



DX APM - SaaS - French - France

Table of Contents

Exigences réseau pour DX SaaS.....	8
Nouveautés dans DX APM.....	9
24.9.1.....	9
24.4.1.....	9
24.3.2.....	9
23.12.1.....	10
2023.9.1.....	11
2023.7.1.....	12
2023.5.1.....	13
23.1.....	14
22.8.....	16
22.6.....	16
22.3.....	17
22.1.....	20
Notes de mise à jour 2021.....	24
21.11.....	25
21.6.....	32
21.4.....	36
21.1.....	40
Notes de mise à jour 2020.....	43
20.11.....	43
20.9.....	50
20.6.....	54
20.4.....	57
20.1.....	64
Notes de mise à jour 2019.....	70
Novembre 2019.....	70
Octobre 2019.....	71
Août 2019.....	72
Prise en main.....	74
Support et compatibilité.....	74
Architecture DX APM.....	74
Ressources vidéo de DX APM.....	75
Conventions relatives aux répertoires et noms de fichier.....	77
Personnalisations.....	78
Articles de connaissances.....	78

Glossaire.....	81
Avis relatifs aux logiciels tiers SaaS.....	102
Implémentation d'agents.....	103
Configuration de votre environnement de surveillance.....	104
Rôles et privilèges pris en charge.....	105
Génération d'un jeton de sécurité.....	109
Création de notifications pour les alertes.....	111
Configuration de notifications par courriel pour les alertes.....	115
Configuration des univers.....	115
Configuration de la vue Expérience.....	119
Définition du mode de surveillance de l'environnement à l'aide de règles d'attribut.....	124
Importation des règles d'attribut en bloc.....	128
Ajustement de la surveillance des alertes.....	130
Gestion des données de mesures à l'aide des modules de gestion.....	134
Création et utilisation des modules de gestion.....	136
Configuration des groupements de mesures dans Team Center.....	140
Création et configuration d'alertes simples dans Team Center.....	147
Création et configuration d'alertes récapitulatives.....	154
Création et modification d'outils de calcul.....	157
Configuration de l'analyse différentielle.....	161
Configuration des extensions JavaScript.....	163
Recommandations de dimensionnement de Docker Monitor.....	172
Téléchargement d'outils supplémentaires.....	173
Outil d'importation d'agent.....	173
Connexion de la station de travail.....	176
Proxy cloud.....	179
Mesures de prise en charge du proxy cloud.....	189
Configuration de la station de travail.....	192
Règles de suppression des traces pour le masquage des données sensibles.....	194
Configuration d'APM Command Center.....	195
Affichage du statut de l'agent.....	195
Affichage des rapports d'agent.....	198
Configuration des applications pour l'intégration.....	199
Gestion des packages d'agent.....	199
Configuration des groupes.....	201
Recherche à l'aide du langage de requête ACC (AQL, ACC Query Language).....	202
Utilisation.....	205
Intégration d'applications pour la surveillance.....	206
Surveillance des performances à l'aide de la vue Expérience.....	208

Recherche de solutions aux problèmes à l'aide du carnet d'analyse.....	213
Affichage du statut d'agent et gestion des fiches d'agent.....	218
Surveillance des valeurs de mesures d'agent à l'aide de la vue des mesures.....	221
Intégration de la page Tableaux de bord DX dans la vue des mesures.....	226
Utilisation de la chronologie et de la surbrillance.....	229
Utilisation de la chronologie et affichage des événements de modification.....	230
Utilisation d'attributs dans DX APM.....	234
Organisation des composants à l'aide de perspectives.....	236
Affichage des relations entre les composants dans la carte.....	239
Couches de carte.....	243
Identification des points importants lors de l'utilisation des filtres.....	247
Surveillance de l'intégrité globale de l'environnement à l'aide du tableau de bord.....	249
Surveillance des problèmes et anomalies relatifs au triage assisté.....	252
Tri assisté et analystes.....	253
Examen des performances médiocres des transactions.....	257
Utilisation du suivi des transactions interprocessus pour résoudre des problèmes.....	260
Démarrage d'une session de suivi de transaction.....	261
Examen des différents composants et des données de suivi.....	262
Diagnostic des problèmes de chargement des ressources.....	269
Diagnostic des problèmes de performance système.....	273
Détection et analyse d'erreurs et de blocages.....	274
Analyse des clichés d'erreur et de blocage.....	278
Collecte et analyse des traces de transaction.....	282
Analyse des données de suivi et collaboration pour l'analyse des problèmes.....	295
Surveillance des performances et des événements du navigateur.....	295
Accès à la station de travail et présentation.....	304
Présentation de la station de travail.....	306
Tri à l'aide de la station de travail.....	310
Onglet Navigateur de mesures.....	313
Utilisation de l'outil de suivi de transaction.....	328
Surveillance à l'aide de la station de travail.....	347
Diagnostic de problèmes à l'aide de l'onglet Navigateur de mesures.....	347
Lecture et compréhension des notifications.....	350
Présentation des performances nominales.....	350
Utilisation de la station de travail.....	352
Navigation entre les tableaux de bord de la console.....	352
Données dynamiques et historiques dans la console de la station de travail.....	359
Mesures DX APM.....	362
Mesures BlamePoint.....	364
Mesures JMX.....	372

Mesures de transaction.....	374
Durabilité d'agent.....	383
Mesures liées à la mémoire.....	388
Mesures de prise en charge des clusters.....	393
Mesures de prise en charge du triage assisté.....	402
Mesures de prise en charge principales.....	403
Surveillance des performances de CA APM à l'aide de mesures de prise en charge.....	405
Istio Support.....	416
Tableaux de bord DX.....	429
Dépannage.....	431
Dépannage de l'agent.....	431
Agent démarré mais invisible.....	431
Echec de la détection automatique par l'agent d'un serveur d'arrière-plan connu.....	434
L'agent surveillant un serveur frontal ne détecte pas automatiquement le serveur d'arrière-plan.....	434
Exception ClassNotFoundException levée par l'agent lors du chargement d'extensions dynamiques.....	435
Les suivis de transaction de l'agent de navigateur et de l'agent .NET ne sont pas mis en corrélation.....	435
Echec du remplissage de la valeur de l'URL du serveur de configuration.....	435
L'en-tête de cookie de réponse de l'agent de navigateur pour .NET est-il décoré ?.....	436
Arrêt brutal de l'agent Java.....	436
Erreur de dépassement de pile de l'agent Java.....	437
Absence de mesures .NET après l'activation de l'injection automatique de snippets de l'agent de navigateur pour .NET.....	438
Non-détection des composants d'arrière-plan automatiques en raison d'une erreur inattendue lors du chargement de l'extension.....	438
Pic du nombre de mesures.....	438
Impossible d'instrumenter une application avec DX APM.....	439
Dysfonctionnement du groupement des URL.....	439
Le buildpack Java de Cloud Foundry ne parvient pas à trouver la version de l'agent Java demandée.....	439
Dépannage des problèmes de la boîte de dialogue de téléchargement d'agent.....	440
Dépannage de DX APM.....	441
Non-affichage des mesures de composant.....	441
L'écart de l'analyse différentielle ne s'affiche pas sur les noeuds.....	441
Aucune donnée de mesure dans la vue Expérience.....	441
Données incomplètes ou manquantes envoyées par les agents dans la carte.....	442
Affichage incorrect des informations sur l'agent dans la carte.....	443
La carte affiche seulement 50 000 noeuds.....	443
Absence d'attributs liés à Docker dans le sélecteur d'attributs de fiche d'expérience.....	443
Dysfonctionnement de la propagation intercouche des attributs.....	444
Recherche des problèmes potentiels liés aux cartes.....	444
Dépannage des transactions.....	444

Identification d'une méthode qui ne se ferme jamais en tant que méthode parent.....	444
Dépannage de la station de travail.....	445
Erreur au niveau de la station de travail lors de la collecte d'un nouveau vidage de threads.....	445
Modification des types d'opérations dans les outils de calcul des modules de gestion.....	446
Panneaux vides dans les tableaux de bord.....	446
Aucun résultat pour une requête sur les événements historiques.....	446
Dépannage des problèmes d'expiration de session automatique dans la station de travail.....	447
Expiration du délai de la station de travail lors de la connexion au gestionnaire d'entreprise.....	447
Référence d'API.....	448
API APM Command Center.....	448
Messages d'erreur d'API.....	453
Ressource d'agent.....	455
Ressource agentUpdateTask.....	458
Ressource diagnosticReport.....	458
Ressource diagnosticReportTask.....	460
Ressource de contrôleur.....	461
Messages d'erreur.....	462
Propriétés pouvant faire l'objet d'une recherche.....	468
Recherche à l'aide du langage de requête de Command Center.....	470
Ressource agentFileOperationTask.....	474
Ressource de fichier.....	475
Ressource package.....	476
bundle Resource.....	478
Ressource agentPackageTask.....	479
API hypermédia de DX APM.....	480
Autorisation et authentification des API.....	481
Accès aux ressources.....	482
Recherche et filtrage de ressources.....	487
Création et mise à jour des ressources.....	490
En-têtes HTTP courants.....	492
Messages et codes d'erreur.....	493
API REST de DX APM.....	495
API d'application.....	499
Règle d'attribut.....	503
Graphique.....	507
Graph Vertex.....	510
Graph Incremental.....	516
ID du sommet du graphique.....	519
Graph Vertexstatus Incremental.....	520
Ressource racine.....	522

Univers.....	523
Sommet.....	525
ID du sommet.....	528
Exemple de code Java d'API REST pour l'obtention de mises à jour incrémentielles.....	529
API REST SQL.....	537
API REST du Team Center.....	555
API REST de demande de mesure.....	567
Utilisation des URL publiques courtes dans DX APM.....	581
Prise en charge internationale.....	584
Fonctionnalités d'accessibilité du produit.....	585
Données d'utilisation (télémétrie).....	588
Documentation Legal Notice.....	592

Exigences réseau pour DX SaaS

L'infrastructure DX SaaS est mise à niveau pour augmenter la fiabilité avec un temps d'indisponibilité minimum pour les fenêtres de maintenance. Cette optimisation requiert des mises à jour de configuration réseau obligatoires pour vos politiques de pare-feu afin d'éviter toute interruption de la sécurité liée au réseau. Les communications entrantes (par exemple, webhook) et sortantes (par exemple les agents, les journaux, les alarmes, RESTMon) sont concernées par ces mises à jour. Les adresses IP du nouveau matériel doivent être autorisées dans votre déploiement lorsque le nouveau matériel est activé. Le fait de ne pas autoriser la communication avec les nouvelles adresses IP peut avoir un impact sur la capacité d'ingérer les données de surveillance ce qui pourrait réduire les performances du système surveillé étant donné la nature de certaines technologies de surveillance.

Contactez votre administrateur réseau pour vous assurer que les adresses IP suivantes sont autorisées pour les centres de données respectifs que vous utilisez actuellement :

NOTE

Les adresses IP existantes doivent rester autorisées simultanément jusqu'à nouvel ordre que ces adresses ne sont plus utilisées.

Centre de données Etats-Unis (<https://axa.dxi-na1.saas.broadcom.com>)

- Entrée :
 - 34.145.151.0/24
- Sortie :
 - 34.96.90.96/28
 - 34.150.194.136/29

Centre de données Europe (<https://axa.dxi-eu1.saas.broadcom.com>)

- Entrée :
 - 34.141.238.0/24
- Sortie :
 - 34.117.194.112/28
 - 34.141.162.16/29

Nouveautés dans DX APM

Découvrez les nouvelles fonctionnalités, les améliorations, les problèmes connus et les correctifs de défauts associés à chaque version de DX APM.

- [24.9.1](#)
- [24.4.1](#)
- [24.3.2](#)
- [23.12.1](#)
- [2023.9.1](#)
- [2023.7.1](#)
- [2023.5.1](#)
- [23.1](#)
- [22.8](#)
- [22.6](#)
- [22.3](#)
- [22.1](#)
- [Notes de mise à jour 2021](#)
- [Notes de mise à jour 2020](#)
- [Notes de mise à jour 2019](#)

24.9.1

Nouvelle fonctionnalité ou amélioration de DX APM.

Fenêtre de maintenance dans l'interface utilisateur d'APM

Une icône Maintenance s'affiche si une page est en cours de maintenance. L'icône Maintenance sera visible pendant une période maximale de 7 jours à l'avance pour toute maintenance à venir. Pour plus d'informations, reportez-vous à la section [Gestion des données de mesure à l'aide des modules de gestion](#).

24.4.1

Cette version cible uniquement les défauts client ainsi que plusieurs défauts internes.

NOTE

Etant donné qu'il s'agit d'un patch, l'interface utilisateur du produit continuera de refléter la version 24.3.2.

La liste des défauts client corrigés est la suivante :

Défaut	Description
DE593238	L'agent Windows APMIA est connecté et les mesures s'affichent dans APM. Toutefois, la valeur de mesure <code>ConnectionState</code> est égale à 5.
DE597525	Graphique d'aperçu d'alerte : lorsque l'utilisateur clique sur X dans les menus Dernière heure et 8 dernières minutes, un message d'erreur s'affiche dans l'interface utilisateur.

24.3.2

Les nouvelles fonctionnalités et améliorations ci-après ont été apportées à DX APM.

- [Outil de calcul de connectivité de l'agent](#)
- [Récapitulatif du nombre d'agents](#)
- [Interface utilisateur du module de gestion améliorée](#)
- [Création d'une copie d'un module de gestion](#)
- [Démarrage d'une session de suivi de transaction dans la vue des mesures](#)
- [API d'application pour l'intégration d'applications](#)

Outil de calcul de connectivité de l'agent

L'outil de calcul de connectivité de l'agent copie l'état de connectivité de l'agent à un emplacement fixe. Il est désactivé par défaut et doit être activé par l'administrateur. Pour plus d'informations, reportez-vous à la section [Outil de calcul de connectivité de l'agent](#).

Récapitulatif du nombre d'agents

L'outil de calcul génère également un bref récapitulatif du nombre d'agents pour chaque état de connexion sous `Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Agents|Agent States`. Pour plus d'informations, reportez-vous à la section [Outil de calcul de connectivité de l'agent](#).

Interface utilisateur du module de gestion améliorée

Vous pouvez désormais mettre à jour le module de gestion avec l'interface utilisateur améliorée. Pour plus d'informations, reportez-vous à la section [Mise à jour d'un module de gestion](#).

Création d'une copie d'un module de gestion

Vous pouvez désormais créer une copie d'un module de gestion à l'aide du bouton Enregistrer en tant que nouvel élément sur la page Modifier le module de gestion. Pour plus d'informations, reportez-vous à la section [Copie d'un module de gestion](#).

Démarrage d'une session de suivi de transaction dans la vue des mesures

Vous pouvez désormais démarrer une session de suivi de transaction sur la page Vue des mesures en spécifiant les valeurs dans la boîte de dialogue Session de suivi de transaction. Pour plus d'informations, reportez-vous à la section [Démarrage d'une session de suivi de transaction](#).

API d'application pour l'intégration d'applications

L'API d'application est documentée à l'aide de la version 3 d'OpenAPI. Le document OpenAPI peut être téléchargé à partir d'une installation d'APM. Il peut être utilisé pour générer des clients pour différentes langues ou avec des clients HTTP/REST interactifs. Pour plus d'informations, reportez-vous à la section [API d'application](#).

23.12.1

Les nouvelles fonctionnalités et améliorations ci-après ont été apportées à DX APM.

URL directe vers la vue du groupe de mesures

La page de détails des alarmes dans DX Operational Intelligence et le courriel de notification d'alarmes sont désormais configurés avec le lien de la vue des mesures APM. Ce lien fournit une vue complète de la période au cours de laquelle l'alerte a été déclenchée, ainsi que le statut des autres alertes dans le même groupe de mesures. Il améliorera également la visibilité et facilitera l'enquête en fournissant une compréhension plus large du comportement des mesures contextuelles au cours de la période observée. Pour plus d'informations, reportez-vous à la section [Tous les détails des alarmes](#).

Vidage de threads dans le navigateur de mesures

Sélectionner un nœud d'agent dans l'arborescence du navigateur de mesures affiche désormais l'onglet **Vidages de threads**. Cet onglet vous permet de collecter des vidages de threads Java et d'afficher les données de vidage de threads actuelles et historiques. Un vidage de threads fournit des informations sur tous les threads qui s'exécutent dans une machine virtuelle Java à un moment donné. Pour plus d'informations, reportez-vous à la section [Affichage d'une mesure d'agent dans la vue de mesures globales](#).

Limitation du temps d'exécution des scripts dans les outils de calcul JavaScript

Le traitement des données de mesures entrantes par les outils de calcul JavaScript peut prendre du temps et affecter les performances du gestionnaire d'entreprise lorsque l'extension JavaScript s'exécute. Pour vous protéger contre une surcharge du gestionnaire d'entreprise, spécifiez le délai d'expiration du script dans la source de l'extension. Pour plus d'informations, reportez-vous à la section [Configuration des extensions JavaScript](#).

NOTE

Vous pouvez désormais supprimer les outils de calcul JavaScript sans redémarrer le gestionnaire d'entreprise. Vous pouvez également définir un délai d'expiration pour limiter le temps d'exécution de l'outil de calcul JavaScript.

Sous-propriétés pour l'intégration d'applications

Vous pouvez désormais sélectionner l'option **ADD PROFILE** (Ajouter un profil) et définir plusieurs configurations de la sous-propriété de l'agent. Par exemple, un agent peut surveiller plusieurs bases de données. Vous pouvez donc ajouter plusieurs ensembles de propriétés de connexion de base de données. Pour plus d'informations, reportez-vous à la section [Création d'applications](#).

Création de variables dans la configuration d'intégration de tableau de bord

Vous pouvez désormais créer des variables directement dans la configuration d'intégration de tableau de bord. Pour plus d'informations, reportez-vous à la section [Intégration de la page Tableaux de bord DX dans la vue des mesures](#).

Mesures de prise en charge du proxy cloud

De nouvelles mesures de prise en charge sont ajoutées au proxy cloud. Vous pouvez utiliser ces mesures pour identifier des informations plus détaillées sur votre connexion de proxy cloud, telles que la connexion réseau, l'utilisation de la mémoire, etc. Par exemple, vous pouvez les utiliser pour examiner d'éventuels problèmes de réseau.

Pour plus d'informations, reportez-vous à la section [Mesures de prise en charge du proxy cloud](#).

Nouveau style de l'interface utilisateur

L'interface utilisateur complète d'APM SaaS a été mise à jour pour utiliser les couleurs, les polices et les styles d'icônes utilisés par la plate-forme DX principale. La taille des polices a été augmentée dans certaines zones, ce qui peut réduire l'espace utilisable à l'écran, mais aussi augmenter le contraste et la lisibilité sur certains moniteurs. Définir votre navigateur sur un zoom de 90% permet de restaurer l'espace d'écran utilisable sans réduire la lisibilité sur certains moniteurs.

2023.9.1

Les nouvelles fonctionnalités et améliorations ci-après ont été apportées à DX APM.

- [Exportation et importation des modules de gestion](#)
- [Filtrage des références d'objet dans les modules de gestion](#)
- [ACC : interface utilisateur unifiée](#)
- [Problèmes connus](#)

Exportation et importation des modules de gestion

Vous pouvez désormais exporter les modules de gestion dans le format de fichier .jar et importer un module de gestion existant en tant que fichier .jar. Pour plus d'informations, reportez-vous à la section [Création et utilisation des modules de gestion](#).

Filtrage des références d'objet dans les modules de gestion

Vous pouvez désormais cliquer sur la valeur d'un objet dans le tableau Références d'objets de la page Module de gestion. Elle vous redirige vers la vue filtrée de la référence de l'objet sélectionné et du module de gestion spécifique à partir duquel vous avez effectué la sélection. Pour plus d'informations, reportez-vous à la section [Création et utilisation des modules de gestion](#).

ACC : interface utilisateur unifiée

L'interface utilisateur d'ACC a été repensée afin de s'harmoniser avec l'interface utilisateur d'Application Performance Management.

Problèmes connus

DE559435 : la combinaison d'alertes Toutes ne fonctionne pas correctement.

Symptôme : lorsque la combinaison d'alertes est définie sur Toutes et que le courriel d'alerte est configuré, dans ce cas, même lorsqu'une mesure dépasse le seuil sur plusieurs mesures configurées, l'état de l'alerte passe à Critique et le courriel d'alerte est envoyé. De plus, l'état d'alerte redevient normal et le courriel est à nouveau envoyé.

2023.7.1

Les nouvelles fonctionnalités et améliorations ci-après ont été apportées à DX APM.

- [Nombre de mesures dynamiques dans l'arborescence de mesures](#)
- [Volet ACC pour ajuster le redimensionnement de la fenêtre du navigateur](#)
- [URL directe vers le groupe de mesures de l'alarme](#)
- [Création de tableaux de bord à l'aide d'attributs capturés](#)
- [Remplissage des univers DX Operational Intelligence par les univers APM](#)
- [Tableaux de bord prêts à l'emploi](#)
- [Optimisation des performances du réseau et de l'UC dans le proxy cloud](#)

Nombre de mesures dynamiques dans l'arborescence de mesures

Si vous sélectionnez un agent ou un sous-dossier dans l'arborescence des mesures et que vous êtes en mode dynamique, cochez la case **Live Metric Only** (Mesures dynamiques uniquement) pour afficher le nombre de mesures dynamiques uniquement, c'est-à-dire les mesures signalées par l'agent à ce moment-là. Pour plus d'informations, reportez-vous à la section [Affichage d'une mesure d'agent dans la vue de mesures globales](#).

Volet ACC pour ajuster le redimensionnement de la fenêtre du navigateur

Dans ACC, vous pouvez désormais ajuster le volet de fenêtre pour afficher toutes les configurations des packages avec de nombreuses mises à jour.

URL directe vers le groupe de mesures de l'alarme

Les détails des alarmes dans DX Operational Intelligence fournissent un fichier JSON brut dans le champ Alarm Attributes (Attributs d'alarme) à partir duquel vous pouvez extraire la valeur du lien Groupement de mesures dans APM. Ce lien

pointe directement vers le groupe de mesures configuré dans APM qui a provoqué l'alarme/l'événement. Pour plus d'informations, reportez-vous à la section [Tous les détails des alarmes](#).

Création de tableaux de bord à l'aide d'attributs capturés

Vous pouvez désormais créer des tableaux de bord dans la page Tableaux de bord DX à l'aide des attributs capturés à partir de Business Payload Analyzer.

Sur la page Tableaux de bord DX, créez le tableau de bord à l'aide des informations suivantes :

- Source de données : **AIOPS_Metadata**
- Index principal : **ao_aum_captured_data_2.0**
- Grouper par : entrez l'attribut capturé au format suivant : **rr_data@<captured_attribute>**

Pour plus d'informations, consultez la documentation [Tableaux de bord DX](#).

Remplissage des univers DX Operational Intelligence par les univers APM

La liste déroulante **Tous mes univers** remplit désormais également les univers DX Operational Intelligence (à l'exception de l'univers All Access (Tous les accès)). Ces univers sont marqués d'une balise OI avec leur nom dans la liste déroulante.

Tableaux de bord prêts à l'emploi

Cette version inclut les tableaux de bord APM prêts à l'emploi suivants dans la page Tableaux de bord DX. Ces tableaux de bord sont disponibles dans le dossier APM-MetricView.

- APM : GC Monitor (Moniteur du nettoyage de mémoire)
- APM : GC Heap (Segment de mémoire du nettoyage de mémoire)
- APM : EM Overview (Présentation du gestionnaire d'entreprise)
- APM : APIM Embedded Dashboard (Tableau de bord intégré d'APIM)

Vous devez afficher ces tableaux de bord dans la vue des mesures d'APM. Accédez au dossier dans l'arborescence et choisissez d'afficher le tableau de bord sous forme d'onglet. Cliquez sur l'onglet pour afficher les données dans le tableau de bord. Pour plus d'informations, reportez-vous à la section [APM-MetricView](#).

Optimisation des performances du réseau et de l'UC dans le proxy cloud

Vous pouvez désormais utiliser `apm.server.compressionLevel` dans le fichier `application.yml` pour configurer le niveau de compression pour la communication WebSocket entre le proxy cloud et la passerelle. Pour plus d'informations, reportez-vous à la section [Proxy cloud](#).

2023.5.1

Les nouvelles fonctionnalités et améliorations ci-après ont été apportées à DX APM.

- [Améliorations apportées à l'intégration d'applications](#)
- [Améliorations/modifications apportées aux tableaux de bord intégrés](#)
- [Amélioration de la fonction de recherche dans l'arborescence de mesures](#)
- [Documentation sur le proxy cloud](#)
- [Défauts connus](#)

Améliorations apportées à l'intégration d'applications

Vous pouvez désormais configurer les options associées au système d'exploitation sélectionné lors de l'utilisation transparente de la fonction d'intégration d'applications pour intégrer les applications dans DX APM et pour configurer les packages d'agent. Pour plus d'informations, reportez-vous à la section [Intégration d'applications pour la surveillance](#).

Améliorations/modifications apportées aux tableaux de bord intégrés

À partir de cette version, les tableaux de bord DX suivants sont intégrés prêts à l'emploi :

- Tableau de bord BlamePoint
- Tableau de bord FrontendOverview

Ces tableaux de bord sont préconfigurés. Dans la vue des mesures, ces tableaux de bord s'affichent sous forme d'onglets si vous sélectionnez une mesure qui correspond à la condition.

Avant cette version, vous deviez importer et intégrer ces tableaux de bord manuellement dans la vue des mesures. Pour plus d'informations, reportez-vous à la section [Intégration de la page Tableaux de bord DX dans la vue des mesures](#).

Amélioration de la fonction de recherche dans l'arborescence de mesures

Les utilisateurs peuvent maintenant marquer des éléments comme favoris dans l'arborescence. Un bouton nommé Afficher les favoris uniquement a été intégré dans l'arborescence de mesures. Ce bouton permet aux utilisateurs de filtrer et d'afficher uniquement les objets marqués comme favoris. Pour plus d'informations, reportez-vous à la section [Recherche de mesures dans l'arborescence de mesures](#).

En outre, la barre de recherche détecte automatiquement lorsque l'entrée est au format d'expression régulière et effectue une recherche en conséquence.

NOTE

L'option permettant d'utiliser des expressions régulières a été supprimée.

Documentation sur le proxy cloud

La documentation relative au proxy cloud est désormais disponible dans la documentation d'APM SaaS. Voir [Proxy cloud](#).

Les informations de version des améliorations précédentes apportées au proxy cloud seront conservées dans la [documentation des agents APM](#).

Défauts connus

Le défaut ci-dessous est connu dans cette version :

DE559435 : la combinaison d'alertes Toutes ne fonctionne pas correctement.

Symptôme : lors de la configuration des alertes, si vous définissez la valeur **Combinaison** sur **Toutes** et que seule une valeur de mesure correspond à la limite de seuil, une alerte est créée et son statut passe à Critique, puis à Normale. En raison de ce comportement, si des notifications par message électronique sont configurées, plusieurs messages électroniques d'alerte sont envoyés : un pour l'alerte danger/avertissement et un autre plus tard lorsque l'état passe à Vert.

23.1

Découvrez les nouvelles fonctionnalités et améliorations de DX APM.

- [Nouvelles fonctionnalités](#)

- [Intégration d'agent simplifiée](#)
- [Spécificateur de mesure non sensible à la casse](#)
- [Suppression des données privées](#)
- [Fin de la prise en charge du japonais](#)
- [Intégration de la page Tableaux de bord DX dans la vue des mesures](#)
- [Désactivation des options Notifier par mesure individuelle et Déclencher une notification d'alerte](#)

Nouvelles fonctionnalités

Découvrez les nouvelles fonctionnalités et améliorations de DX APM SaaS.

Intégration d'agent simplifiée

Vous pouvez utiliser l'intégration d'applications pour intégrer les applications dans DX APM de manière transparente et configurer facilement les packages d'agent pour votre environnement. L'assistant Intégration d'applications vous guide dans la sélection des options de surveillance et crée des packages d'agent. L'intégration d'applications repose sur les concepts suivants :

- **Application** : permet de surveiller l'application qui se compose d'un ou de plusieurs niveaux.
- **Niveau** : indique le niveau d'application à surveiller. Le concept de niveau fait référence à un ou plusieurs packages d'agent créés en fonction de l'utilisateur sélectionné.

NOTE

Vous pouvez toujours utiliser l'ADD (boîte de dialogue de téléchargement d'agent) et ACC (APM Command Center) pour ajouter des applications et configurer des packages d'agent dans votre environnement.

Pour plus d'informations, reportez-vous à la section [Intégration d'applications pour la surveillance](#).

Spécificateur de mesure non sensible à la casse

Vous pouvez désormais spécifier le spécificateur de mesure sur une valeur oscillant entre (?i) et (?-i) sans tenir compte de la casse. Par exemple,

```
(?i)jmx(?-i)\|JVM\|Threading:Current Thread Count
```

Voir [Configuration des groupements de mesures dans Team Center](#).

Suppression des données privées

Vous pouvez désormais définir des règles de suppression des traces permettant d'identifier les données sensibles des utilisateurs et les remplacer par du texte préconfiguré, tel que SUPPRESSED BY APM. Pour plus d'informations, reportez-vous à la section [Règles de suppression des traces pour le masquage des données sensibles](#).

Fin de la prise en charge du japonais

L'interface utilisateur et la documentation de DX APM ne sont plus localisées en japonais. Voir [Prise en charge internationale](#).

Intégration de la page Tableaux de bord DX dans la vue des mesures

Vous pouvez désormais intégrer la page Tableaux de bord DX dans la vue des mesures. Vous pouvez intégrer ce qui suit :

- **Tableaux de bord des mesures BlamePoint et des mesures liées aux composants frontaux** : pour ces tableaux de bord, la fonction Tableaux de bord DX fournit des fichiers JSON que vous pouvez importer. Les tableaux de bord sont disponibles dans la vue des mesures une fois qu'ils ont été importés.
- **Tableaux de bord DX personnalisés** : créez un tableau de bord personnalisé sur la page Tableaux de bord DX, puis mappez-le à l'aide de la mosaïque **Tableaux de bord DX** sur la page **Paramètres** de DX APM. Le tableau de bord s'affiche sur la page Vue des mesures une fois qu'il a été intégré.

Pour plus d'informations, reportez-vous à la section [Intégration de la page Tableaux de bord DX dans la vue des mesures](#).

Désactivation des options Notifier par mesure individuelle et Déclencher une notification d'alerte

APM signale chaque modification de l'état d'alerte au service d'alertes, rendant ainsi redondants les boutons Notifier par mesure individuelle et Déclencher une notification d'alerte, qui ont donc été supprimés de la page Créer/Modifier une alerte. Pour plus d'informations, consultez la section [Création et configuration d'alertes simples dans Team Center](#).

Vous pouvez gérer toutes les notifications d'alerte et configurer les détails de notification d'alerte de déclenchement sous Politiques, dans la zone de lancement. Voir [Création d'une politique](#).

22.8

Modifications apportées à la documentation

À partir de cette version, les informations associées aux agents sont découplées de la documentation de DX APM SaaS. Les informations relatives aux agents qui étaient précédemment disponibles dans la section Implémentation des agents sont désormais disponibles à l'adresse suivante : <https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/dx-apm-agents/SaaS.html>. La section Implémentation des agents contient désormais un lien qui mène vers la documentation relative aux agents DX APM.

NOTE

Les informations associées aux agents qui ont été ajoutées aux signets du site DX APM SaaS précédent ne fonctionnent pas. Nous vous recommandons de créer de nouveaux signets pour les informations relatives aux agents à partir du site de documentation des [agents DX APM](#). La recherche d'informations liées aux agents via Google affiche quelques anciens liens qui ne fonctionnent pas. L'indexation de la nouvelle documentation des agents DX APM SaaS et DX APM par Google prend du temps. Nous vous recommandons d'utiliser la fonctionnalité de recherche sur le site de documentation tant que Google n'a pas indexé notre contenu.

Chiffrement du mot de passe dans le fichier de configuration de la station de travail

Lors de la configuration de la station de travail, vous pouvez désormais utiliser **transport.http.proxy.username** et **transport.http.proxy.password** pour spécifier les valeurs d'authentification, où **transport.http.proxy.password** doit être chiffré. Pour plus d'informations, reportez-vous à la section [Configuration de la station de travail avec l'authentification](#).

Règles de suppression des traces

Vous pouvez désormais définir des règles de suppression des traces permettant d'identifier les données sensibles des utilisateurs et les remplacer par du texte préconfiguré, tel que SUPPRESSED BY APM. Pour plus d'informations, reportez-vous à la section [Règles de suppression des traces pour le masquage des données sensibles](#).

22.6

Améliorations apportées à l'agent Infrastructure

Surveillance SNMP

La surveillance SNMP est une extension de l'agent Infrastructure APM qui permet de surveiller les unités connectées au réseau via le protocole SNMP (Simple Network Management Protocol). Il s'agit d'une extension générique qui peut surveiller n'importe quelle unité ou n'importe quel agent activés par SNMP. Pour plus d'informations, voir la section [Surveillance SNMP](#).

Service Azure CDN

La surveillance Azure Content Delivery Network permet de surveiller la réactivité d'Azure CDN lors de l'utilisation d'applications, telles qu'un logiciel de jeu, des mises à jour de microprogramme, l'IoT, des applications mobiles, des médias de diffusion en continu et des sites Web. Pour plus d'informations, reportez-vous à la section [Service Azure CDN](#).

Surveillance Kafka améliorée

Ajout de la prise en charge suivante pour la surveillance Kafka :

- **Prise en charge de l'authentification SASL/PLAIN de l'intermédiaire Kafka** : Ajout de la prise en charge de l'authentification SASL/PLAIN de l'intermédiaire Kafka. Vous pouvez activer cette propriété pour les connexions client en fournissant le nom d'utilisateur et le mot de passe.
- **Hébergement multiclient de l'agent UMA** : Ajout de la prise en charge de l'installation de l'équipe d'hébergement multiclient de l'agent UMA. Utilisez cette fonction pour surveiller les espaces de noms.

Pour plus d'informations, reportez-vous à la section [UMA pour la surveillance Kafka](#) et [Surveillance Kafka](#).

Améliorations apportées à IBM MQ

L'agent Infrastructure IBM MQ a été amélioré pour fournir une meilleure prise en charge de la mise à l'échelle et du filtrage. L'agent pcf obsolète est également supprimé. Voici la liste des autres améliorations apportées.

- Ajout de types de files d'attente dans les mesures pour une meilleure compréhension
- Mise à jour de la configuration des expressions régulières

Pour plus d'informations, reportez-vous à la section [Surveillance IBM WebSphere MQ](#).

Améliorations apportées à l'agent .Net/.Net Core

Prise en charge de .Net 6.0

Depuis cette version, la prise en charge de .Net 6.0 a été ajoutée pour surveiller les performances des applications .Net 6.

Ajout de la prise en charge de WebSocket et de Secure WebSocket pour .NET

La prise en charge de WebSocket et de Secure WebSocket est ajoutée pour la connexion de l'agent .NET avec le proxy cloud.

Améliorations apportées à l'agent Node.js

Les noms des propriétés des sondes sont normalisés pour faciliter le déploiement de l'agent UMA.

Informations complémentaires : [Configurations de l'agent Node.js](#)

Améliorations apportées à l'agent de surveillance universel

- Ajout de la prise en charge de la surveillance et la génération de rapports d'événements de cluster.
Informations complémentaires : [Configuration de la surveillance des événements de cluster de l'agent UMA - Kubernetes](#) et [Configuration de la surveillance des événements de cluster de l'agent UMA - OpenShift](#)
- Surveillance Prometheus améliorée avec l'agent UMA.
Informations complémentaires : [Ingestion de données Prometheus](#)
- Ajout du panneau Événements aux tableaux de bord DX de l'agent UMA.
Informations complémentaires : [Documentation relative aux tableaux de bord de l'agent UMA](#).

22.3

Cette section indique les fonctionnalités nouvelles, modifiées et désapprouvées dans DX Application Performance Management (DX APM) 22.3.

Prise en charge de K8s 1.22 et d'OSE 4.9

DX Application Performance Management prend désormais en charge Kubernetes 1.22 et OpenShift 4.9.

Améliorations apportées à l'agent Node.js

L'agent Node.js contient les améliorations suivantes :

Prise en charge de Redis pour Node.js

DX Application Performance Management prend en charge l'instrumentation des appels Redis avec la sonde Node.js à partir de cette version. La prise en charge de Redis pour Node.js vous permet de visualiser de manière structurée le cycle de vie complet de la transaction des composants frontaux aux composants d'arrière-plan et de surveiller les opérations CRUD sur les terminaux. La sonde permet d'isoler et de trier plus rapidement les problèmes liés à l'application, à la base de données ou à l'infrastructure. Pour plus d'informations, reportez-vous à la section Redis.

Prise en charge de l'infrastructure asynchrone pour l'agent de sonde Node.js

DX Application Performance Management prend désormais en charge la structure asynchrone pour l'agent de sonde Node.js. Cette infrastructure permet de mettre en corrélation les appels asynchrones des composants frontaux avec les composants d'arrière-plan sous le noeud Fragments. Pour plus d'informations, reportez-vous à la section GraphQL.

Prise en charge de la corrélation de l'agent de navigateur Node.js

A partir de cette version, vous pouvez visualiser la corrélation de bout en bout de votre environnement du navigateur à l'application Node.js (module Express JS), afficher les traces corrélées et les mapper pour trier les problèmes plus rapidement. Pour plus d'informations, reportez-vous à la section Prise en charge de l'agent de navigateur dans Node.js.

Améliorations apportées à l'agent .NET

L'agent .NET contient les améliorations suivantes :

Prise en charge de la détection et de la surveillance automatiques des blocages avec les transactions asynchrones .NET

Désormais, DX Application Performance Management détecte et surveille automatiquement les blocages avec les applications .NET asynchrones pour trier et diagnostiquer les problèmes de performances des applications.

Amélioration de la corrélation des traces de bout en bout pour les applications asynchrones .NET

La visibilité des traces de bout en bout a été améliorée pour les transactions asynchrones. Cela simplifie la résolution des problèmes de transaction.

Améliorations apportées à l'agent Infrastructure APM

L'agent Infrastructure APM inclut les améliorations suivantes :

Prise en charge de l'hébergement multiclient Oracle dans l'extension Moniteur de base de données Oracle d'APMIA

DX Application Performance Management prend désormais en charge l'hébergement multiclient Oracle dans l'extension Moniteur de base de données Oracle. Cette fonction surveille les performances des bases de données Oracle activées avec l'option d'hébergement multiclient. Pour plus d'informations, consultez la section Surveillance de la base de données Oracle.

vCenter Application Insight Modules (VCAIM)

VCenter Application Insight Modules (VCAIM) fournit des fonctions permettant de surveiller les systèmes sous le contrôle de VMware vCenter Server. VCAIM peut s'exécuter sur n'importe quel système Windows sur lequel SystemEDGE est installé. VCAIM communique avec vCenter Server pour surveiller tous les serveurs ESX gérés par le serveur VMware vCenter associé.

Pour plus d'informations, reportez-vous à la section vCenter Application Insight Modules.

Surveillance Azure Databricks

La surveillance Azure Databricks permet de surveiller le cluster autonome Spark et les clusters Azure Databricks. Elle permet de surveiller les jobs, les étapes et les tâches d'une application et de vérifier la mémoire et les performances des exécuteurs. La surveillance Azure Databricks peut être utilisée pour le dépannage des problèmes de performance et la caractérisation de la charge de travail.

Pour plus d'informations, reportez-vous à la section [Déploiement de la surveillance Spark sur Azure Databricks](#).

Surveillance Azure Active Directory

La surveillance Azure Active Directory permet de surveiller Azure Active Directory à l'aide de journaux d'audit. Les détails du journal incluent diverses mesures, telles que le nombre d'ajouts de groupes ou le nombre d'ajouts d'utilisateurs. En outre, cette fonction surveille divers attributs, tels que l'ID d'abonnement Azure et l'ID de client hébergé Azure.

Pour plus d'informations, reportez-vous à la section [Surveillance Azure Active Directory](#).

Améliorations apportées à APM Command Center

APM Command Center inclut l'amélioration suivante :

Ajout du lien d'intégration d'un webhook

L'intégration de produits tiers permet d'intégrer ACC à votre infrastructure (par exemple, avec des artefacts) et de fournir le package ACC à l'aide de votre infrastructure. Le serveur de configuration ACC fournit un lien d'intégration de webhooks qui déclenche une application permettant de télécharger le package et de l'importer dans votre infrastructure. Pour plus d'informations, reportez-vous à la section [Configuration et téléchargement d'un package d'agent](#).

Nouveaux tableaux de bord prêts à l'emploi

Les tableaux de bord DX incluent les nouveaux tableaux de bord suivants :

Tableaux de bord Pivotal Cloud Foundry (PCF)

Les tableaux de bord PCF sont une nouvelle catégorie des tableaux de bord DX APM. Cette catégorie inclut les tableaux de bord suivants disponibles dans le dossier Général :

- Informations sur l'application PCF
- Informations sur la machine virtuelle PCF (BOSH)
- Informations sur la cellule PCF
- Informations sur l'espace organisationnel PCF
- Présentation de PCF

Pour plus d'informations, consultez la section [Tableaux de bord PCF](#).

Améliorations apportées aux tableaux de bord UMA et à la visualisation

Les tableaux de bord UMA ont été améliorés de manière à inclure les performances des applications corrélées. Les tableaux de bord corrélés permettent de déterminer rapidement l'impact des conteneurs sur les performances des applications. Pour afficher la liste des améliorations, reportez-vous à la section [Améliorations apportées au tableau de bord](#).

Défauts corrigés

Les problèmes suivants ont été résolus dans cette version :

Défaut DE539968 : `introscope.agent.acc.controller.configurationServer.url` ne parvient pas à extraire les détails de proxy cloud corrects.

Solution : l'URL du proxy cloud dans l'assistant de configuration de package `introscope.agent.acc.controller.configurationServer.url` (URL du serveur de configuration) et `agentManager.url` (URL du

gestionnaire d'événements) ne sont plus visiblement synchronisées dans l'interface utilisateur d'ACC. Toute valeur saisie est prise en compte et les valeurs par défaut sont disponibles dans le package téléchargé.

NOTE

Vous ne pouvez pas dériver la valeur de la propriété `introscope.agent.acc.controller.configurationServer.url` lorsqu'une URL Isengard unique (hôte:port) est fournie pour l'URL du proxy cloud. La propriété reste alors vide.

Défaut DE526430 : après la mise à niveau vers la version 2022.1.0.25, les utilisateurs existants ne s'affichent sur la page Utilisateurs et autorisations.

Symptôme : j'ai mis à niveau le gestionnaire d'entreprise vers la version 2022.1.0.25 et les utilisateurs existants ne sont pas disponibles dans la page Utilisateurs et autorisations.

Solution : connectez-vous au gestionnaire d'entreprise après avoir procédé à la mise à niveau et consultez les utilisateurs existants.

Défaut DE52234 : les perspectives ne basculent pas vers les valeurs par défaut lorsqu'elles sont permutées d'une couche à l'autre dans la page Vue Carte.

Symptôme : j'ai créé trois perspectives pour chaque couche à partir de la page Carte et je les ai définies comme perspectives par défaut pour chaque couche. Lorsque vous basculez entre chaque perspective de la page Carte, la perspective ne change pas.

Défaut DE526577 : l'outil d'importation d'agent a importé un build antérieur à l'agent 10.7.

Symptôme : j'ai importé un agent connecté 10.7 valide à l'aide de l'outil d'importation d'agent et j'ai constaté que la page ACC affiche le package importé de l'ancien build.

Solution : pour contourner ce problème, utilisez la commande `-v <version_bundle>` dans l'outil `import-agent`.

Défaut DE525374 : affichage de packages incorrects lors du basculement d'un package pour l'agent Infrastructure dans l'interface utilisateur ACC.

Symptôme : la liste des packages ne pouvant pas être appliqués à partir de l'interface utilisateur ACC s'est affichée lorsque j'ai cliqué sur le lien pendant le basculement de packages pour l'agent Infrastructure dans l'interface utilisateur ACC.

22.1

Cette section indique les fonctionnalités nouvelles, modifiées et désapprouvées dans DX Application Performance Management (DX APM) 22.1.

Améliorations apportées à l'agent Java

Prise en charge des mesures de moniteur de plate-forme prêtes à l'emploi via JMX

Ajout de la prise en charge des mesures de surveillance de plate-forme prêtes à l'emploi via JMX.

Améliorations apportées à l'agent Node.js

Prise en charge de la corrélation de la base de données Oracle pour l'agent Node.js

Ajout de la prise en charge de la base de données Oracle en tant que base de données d'arrière-plan pour les applications Node.js. La prise en charge améliorée de la base de données d'arrière-plan aide à détecter les composants en aval, enrichissant ainsi la topologie, l'analyse de service et l'analyse des causes premières. Pour plus d'informations, reportez-vous à la section Agent Node.js.

Prise en charge de l'agent de navigateur dans Node.js

La prise en charge de l'agent de navigateur dans les applications Node.js met en corrélation les événements basés sur le navigateur et les applications Node.js et calcule les performances du navigateur lors du traitement des demandes d'applications Node.js. HTTP est le module principal qui traite les demandes en provenance des navigateurs dans Node.js. Pour la communication basée sur le navigateur, tous les modules frontaux interagissent avec ce module. Pour plus d'informations, reportez-vous à la section Prise en charge de l'agent de navigateur dans Node.js.

Améliorations apportées à l'agent PHP

Prise en charge de la corrélation de l'agent PHP et l'agent de navigateur

A partir de cette version, vous pouvez visualiser la corrélation de bout en bout de votre environnement, du navigateur à l'application PHP. Vous pouvez également afficher les traces corrélées et les mapper pour trier les problèmes plus rapidement. Pour plus d'informations, reportez-vous à la section Injection d'extrait dans l'agent de navigateur à l'aide de l'agent PHP.

Améliorations apportées à l'agent Infrastructure

Prise en charge de l'ingestion de traces AWS X-Ray pour AWS Lambda dans l'application DX Application Performance Management

- La surveillance AWS X-Ray permet de surveiller les applications qui s'exécutent sur le cloud AWS. Cette fonction permet de surveiller l'intégrité et les performances de l'infrastructure AWS.
- La prise en charge de la création et de l'utilisation de plusieurs profils ou comptes est désormais introduite pour la surveillance AWS.

Pour plus d'informations, reportez-vous à la section AWS X-Ray.

Livraison de l'extension de surveillance de l'infrastructure pour IBM App Connect Enterprise v12

A partir de cette version, DX Application Performance Management prend en charge la surveillance d'IBM App Connect Enterprise v11 et versions ultérieures (IBM ACE, le successeur d'IBM Integration Bus v10 (IIB)). L'ajout d'IBM App Connect Enterprise v11 a enrichi les plates-formes middleware prises en charge dans DX Application Performance Management. Avec l'agent de surveillance IIB, les utilisateurs APM peuvent désormais surveiller la disponibilité, l'intégrité et les performances d'IBM ACE. Pour plus d'informations, voir la section Surveillance IIB.

Améliorations apportées à l'agent de surveillance universel

Amélioration apportée à la surveillance k8s

L'amélioration de la surveillance k8s fournit des informations sur les autres performances du réseau et du cluster. Les mesures suivantes sont ajoutées dans les données de performances des pods :

- CPU Request Deviation and Memory Request Deviation
- Pod Ready State
- CPU % (rounded)
- Memory % (rounded)

Pour plus d'informations, reportez-vous à la section Données des mesures des pods.

Améliorations apportées à l'agent UMA

Accès/privilèges de sécurité pour le déploiement de l'agent UMA

Vous pouvez ajouter les privilèges de sécurité au déploiement de l'agent UMA à partir de cette version.

Dépannage amélioré de l'agent UMA

Outils et améliorations de l'agent UMA pour une meilleure gestion des déploiements de l'agent UMA.

Prise en charge des dernières versions du conteneur AKS/EKS/GKE

A compter de cette version, l'agent UMA est pris en charge sur les dernières versions des conteneurs suivants pour gérer les performances des environnements de conteneur.

- Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)

Prise en charge du fichier tools.jar de JDK personnalisé pour l'extension AutoAttach de Java

La prise en charge du fichier tools.jar de JDK personnalisé a été ajoutée pour l'agent UMA pour Kubernetes et pour l'agent UMA pour OpenShift. Cette fonctionnalité rend possible l'association à toutes les machines virtuelles Java pour AutoAttach. Pour plus d'informations, reportez-vous aux sections Installation et configuration de l'UMA pour Kubernetes et Installation et configuration de l'UMA pour OpenShift.

Prise en charge de Red Hat OpenJDK pour l'association automatique

A partir de cette version, l'UMA prend désormais en charge Red Hat OpenJDK pour l'association automatique, ce qui vous permet de surveiller les performances des applications conteneurisées basées sur une machine virtuelle Java Red Hat.

Améliorations apportées à la conception de l'association automatique de l'UMA pour Node.js

L'UMA prend en charge la détection automatique des applications Node.js incluses dans la liste blanche à partir de cette version. Par défaut, le moniteur de conteneur d'applications de l'UMA (pod Daemon Set) s'exécute en mode liste blanche, et détecte ainsi automatiquement les applications Node.js incluses dans la liste blanche et les joint.

Certification des commandes pm2 et Forever Start pour l'association automatique de l'UMA Node.js

A partir de cette version, l'UMA prend en charge la surveillance et l'association automatique des applications Node.js à l'aide des commandes pm2 et Forever start dans l'environnement Kubernetes.

Intégration de DX Application Performance Management - Mainframe

Prise en charge de Sysview DB2

A partir de cette version, DX Application Performance Management améliore la visibilité sur les mesures mainframe en prenant en charge la surveillance des performances de la base de données IBM DB2. Les administrateurs peuvent désormais surveiller les KPI de la base de données IBM DB2 et identifier et trier facilement les problèmes. Pour plus d'informations, reportez-vous à la section Intégration DX APM-Mainframe.

Package Kafka avec l'extension Mainframe

A partir de cette version, DX Application Performance Management prend en charge l'extension Intermédiaire Kafka qui gère les instances d'intermédiaire Kafka et Zookeeper ainsi que leur intégration.

Cette extension s'intègre également au mainframe afin de permettre l'ingestion des enregistrements SMF publiés à partir d'un producteur Kafka tel que ZAB à une fréquence élevée dans l'extension Mainframe IA, évitant ainsi la latence réseau.

Pour plus d'informations, reportez-vous à la section Extension Intermédiaire Kafka.

Ajout de la mosaïque Extensions JavaScript dans la page Paramètres

A partir de cette version, une nouvelle mosaïque **Extension JavaScript** a été ajoutée dans la section **Paramètres généraux**. Cette fonction permet d'accéder à la gestion des extensions JavaScript qui peuvent traiter les mesures entrantes avant leur stockage dans DX Application Performance Management. Avec une extension JavaScript, vous pouvez effectuer des calculs, modifier des chemins de mesure, modifier des noms de mesures, copier des données de mesures dans de nouvelles mesures et exécuter des opérations JavaScript générales sur les mesures entrantes. Pour plus d'informations, reportez-vous à la section Configuration des extensions JavaScript.

Modification de la documentation

A partir de cette version, le nouveau **Tableau de bord DX - Site de documentation de SaaS** est désormais disponible en tant que site autonome. Pour plus d'informations, reportez-vous à la section *Tableaux de bord DX pour SaaS*.

Problèmes connus

Défaut DE526430 : après la mise à niveau vers la version 2022.1.0.25, les utilisateurs existants ne s'affichent sur la page Utilisateurs et autorisations.

Symptôme : j'ai mis à niveau le gestionnaire d'entreprise vers la version 2022.1.0.25 et les utilisateurs existants ne sont pas disponibles dans la page Utilisateurs et autorisations.

Solution : connectez-vous au gestionnaire d'entreprise après avoir procédé à la mise à niveau et consultez les utilisateurs existants.

Défaut DE52234 : les perspectives ne basculent pas vers les valeurs par défaut lorsqu'elles sont permutées d'une couche à l'autre dans la page Vue Carte.

Symptôme : j'ai créé trois perspectives pour chaque couche à partir de la page Carte et je les ai définies comme perspectives par défaut pour chaque couche. Lorsque vous basculez entre chaque perspective de la page Carte, la perspective ne change pas.

Solution : il n'existe aucune solution à ce problème.

Défaut DE522903 : affichage d'une erreur par la vue des mesures dans le navigateur et dans la console de débogage

Symptôme : j'ai démarré une session de suivi de transaction pour un agent via l'application WebView. Dans la page Vue des mesures, j'ai consulté l'onglet Traces/Erreur ainsi que les noeuds de mesures des transactions générées d'un agent et j'ai remarqué qu'une erreur s'affiche dans la page du navigateur et dans la console de débogage.

Solution : il n'existe aucune solution à ce problème.

Défaut DE526577 : l'outil d'importation d'agent a importé un build antérieur à l'agent 10.7.

Symptôme : j'ai importé un agent connecté 10.7 valide à l'aide de l'outil d'importation d'agent et j'ai constaté que la page ACC affiche le package importé de l'ancien build.

Solution : pour contourner ce problème, utilisez la commande `-v <version_bundle>` dans l'outil import-agent.

Défaut DE525374 : affichage de packages incorrects lors du basculement d'un package pour l'agent Infrastructure dans l'interface utilisateur ACC.

Symptôme : la liste des packages ne pouvant pas être appliqués à partir de l'interface utilisateur ACC s'est affichée lorsque j'ai cliqué sur le lien pendant le basculement de packages pour l'agent Infrastructure dans l'interface utilisateur ACC.

Solution : il n'existe aucune solution à ce problème.

Défauts corrigés

Les problèmes suivants ont été résolus dans cette version :

Défaut DE521544 : impossibilité d'afficher la liste déroulante des attributs Ajouter une fiche d'expérience.

Symptôme: je me suis connecté à mon client hébergé et j'ai accédé à DX Application Performance Management. J'ai configuré mon agent Java Tomcat, puis j'ai entraîné mon application à générer quelques transactions. Dans **Vue Expérience**, j'ai sélectionné **Ajouter « + »**. Dans la page **Ajouter une fiche d'expérience**, dans la liste déroulante **sélectionner un univers**, j'ai choisi **Your applications** (Vos applications). Au niveau de la puce **use entire universe or apply a filter** (Utiliser tout l'univers et appliquer un filtre), j'ai choisi **Select agent from Application layer** (Sélectionner un agent dans la couche applicative). Sous **Group by section** (Grouper par section), lorsque j'ai sélectionné la liste déroulante **Attribute** (Attribut), la liste était vide. Elle n'affichait aucun attribut de couche. Ce problème survient uniquement avec les agents DX Application Performance Management 21.11.

Solution : sélectionnez la case à cocher **Inclure le noeud d'expérience** dans la page **Ajouter une fiche d'expérience**. Vous pouvez voir la liste déroulante **Attributs** (Attributs), mais uniquement pour la couche **Application** elle-même, pas pour les autres couches.

Défaut DE520944 : affichage incorrect d'un message d'erreur par APM Command Center après la modification de la configuration du package

Symptôme : j'ai utilisé la boîte de dialogue de téléchargement d'agent pour télécharger un agent Infrastructure. J'ai accédé à APM Command Center pour configurer l'agent Infrastructure et j'ai choisi **Packages > Configuration**. J'ai modifié mon package et configuré un mélange de propriétés contrôlées et dynamiques. Certaines propriétés requièrent un redémarrage de l'application gérée, d'autres non. Lorsque j'ai cliqué sur **Basculer**, le message suivant s'est affiché :

`Agent is not using the latest package version. The latest package version must be applied manually.`

Lorsque j'ai appliqué la nouvelle version de package à l'agent, le message d'erreur ci-dessous s'est affiché pour toutes les modifications de configuration contrôlées et dynamiques de l'agent Infrastructure :

`The latest version of package "Infrastructure Agent-apmia-20211117" can only be applied manually. The agent that uses this package will not be displayed. APM Command Center does not support applying newer infrastructure agent package version through user interface.`

Cependant, le package apparaissait toujours dans la liste des versions et j'ai pu appliquer le nouveau package à l'agent en cours d'exécution.

Solution : vous pouvez ignorer ces messages. Toutes les fonctionnalités liées aux packages fonctionnent correctement. Les listes de packages affichent les versions appropriées et aucun problème ne survient lors de l'application de nouveaux packages aux agents exécutés.

Notes de mise à jour 2021

Cette section contient les notes de mise à jour pour 2021.

- [21.11](#)
- [21.6](#)
- [21.4](#)
- [21.1](#)

21.11

Cette section indique les fonctionnalités nouvelles, modifiées et désapprouvées dans DX Application Performance Management (DX APM) 21.11.

Améliorations apportées à la surveillance du cloud

Voici les améliorations liées à la surveillance du cloud dans cette version.

Google Cloud Monitoring

Surveillance Google Cloud Platform Firewall Insights

Vous pouvez maintenant surveiller l'état et les performances du service Firewall Insights, qui fournit des informations sur l'utilisation du pare-feu et sur les problèmes de configuration liés au pare-feu. La surveillance Firewall Insights prend en charge la corrélation entre les éléments d'un cloud privé virtuel (VPC) tels que le projet, la région, la zone et les sous-réseaux. Cette corrélation fournit des mesures qui offrent une expérience holistique en matière de surveillance. Elle vous permet de mieux comprendre et d'optimiser en toute sécurité vos configurations de pare-feu. Vous pouvez également consulter des rapports sur l'utilisation du pare-feu et sur l'impact de diverses règles de pare-feu sur votre réseau VPC.

Informations complémentaires : Surveillance Google Cloud Platform Firewall Insights.

Amazon Web Services (AWS)

Surveillance AWS Virtual Private Cloud

Utilisez la surveillance AWS Virtual Private Cloud pour visualiser votre VPC AWS Cloud Platform et la façon dont vos composants VPC sont connectés. Examinez les mesures pour surveiller l'intégrité et les performances de votre VPC. Cette extension vous aide à comprendre le contexte des applications qui sont connectées à votre VPC et fournit une corrélation application-infrastructure-réseau. Surveillez et analysez les indicateurs clés de performance du VPC AWS Cloud Platform. Ces indicateurs incluent les données entrantes en provenance de la source, les données sortantes en direction de la destination, le nombre de connexions actives et l'allocation des ports d'erreur. **Informations complémentaires** : Service AWS Virtual Private Cloud.

Surveillance AWS Transit Gateway

Le service AWS Transit Gateway vous permet de connecter vos VPC AWS Cloud Platform et leurs réseaux sur site à une seule passerelle. La surveillance AWS Transit Gateway vous fournit des données sur l'intégrité et les performances de votre passerelle AWS Transit. Cette extension met également en corrélation AWS Transit Gateway avec d'autres composants VPC. La surveillance AWS Transit Gateway vous permet de visualiser et de résoudre les problèmes liés aux données de mesures précises sur les activités réseau et les sources de trafic. Ces mesures vous aident à optimiser les allocations de bande passante, à assurer une planification appropriée de la capacité, à résoudre les problèmes et à surveiller la consommation de bande passante. **Informations complémentaires** : Service AWS Transit Gateway.

Surveillance Amazon FSx for Windows File Server

Amazon FSx vous permet de démarrer, d'exécuter et de gérer des systèmes de fichiers grand public et open source dans le cloud AWS. La surveillance Amazon FSx for Windows File Server détecte automatiquement ce service et effectue une opération périodique de synchronisation. Vous pouvez choisir les matrices DX APM à surveiller à l'aide du filtrage de base ou avancé. Vous pouvez utiliser les attributs spécifiques du service Surveillance Amazon FSx for Windows File Server, tels que le type ipAddressm ipAddress, l'ID de VPC et le nom d'hôte de DNS. **Informations complémentaires** : Service AWS FSx for Windows File Server.

Agent Java

Surveillance des performances des composants frontaux d'expérience de l'agent Java

L'agent Java suit désormais les performances des composants frontaux d'expérience dans l'ensemble des transactions. Cette fonctionnalité vous permet d'utiliser le tri assisté pour déterminer la cause première des problèmes de performance des applications. L'agent Java identifie les goulots d'étranglement des performances en mettant en corrélation les anomalies d'application de pile logicielle avec les performances d'expérience médiocres et inacceptables. **Informations complémentaires** : Composants frontaux d'expérience de l'agent Java.

Surveillance Kafka améliorée pour utiliser SSL

L'extension Agent Java de surveillance Kafka permet désormais de surveiller Kafka à l'aide du protocole de sécurité SSL (Secure Socket Layer). **Informations complémentaires** : Surveillance Kafka.

Surveillance de l'agent Java pour Azure App Service

L'agent Java pour Microsoft Azure App Service permet aux entreprises exécutant des applications Java dans Microsoft Azure d'identifier et de résoudre les problèmes de performances. L'agent Java pour Microsoft Azure App Service intègre des mesures de performances dans DX APM pour offrir des fonctions d'analyse intelligente, d'alerte et de visibilité dans un tableau de bord unique. Vous pouvez déployer cette extension de site lorsque vous déployez un conteneur Tomcat dans Azure. Une fois que vous avez déployé l'agent Java pour Microsoft Azure App Service, vous pouvez configurer ses propriétés à l'aide des paramètres du site Azure.

Agent Infrastructure

Nouvelle intégration DX APM-Mainframe

Vous pouvez désormais surveiller les performances de votre environnement mainframe SYSVIEW à l'aide de la nouvelle intégration DX APM-Mainframe. Cette intégration basée sur l'agent Infrastructure DX APM inclut des tableaux de bord Grafana DX prédéfinis, des mesures SYSVIEW et Cross-Enterprise APM (CE APM) ainsi que des alertes pour les mesures SYSVIEW. **Informations complémentaires** : Intégration DX APM-Mainframe.

Nouveaux Data Collectors SystemEDGE

Le nouveau Data Collector SystemEDGE découple SystemEDGE Core de la surveillance d'hôte de l'agent Infrastructure. Toutefois, DX APM continue de prendre en charge tous vos cas d'utilisation de surveillance SystemEDGE hérités et personnalisés après la mise à niveau vers l'agent Infrastructure APM SaaS 21.11. Le Data Collector SystemEDGE vous permet de continuer à utiliser les bibliothèques de base SystemEDGE. A l'avenir, les bibliothèques SystemEDGE seront disponibles uniquement à l'aide des Data Collectors SystemEDGE de l'agent Infrastructure. Les Data Collectors SystemEDGE prennent en charge les communications SNMPv3, fournissant ainsi une authentification et une confidentialité SNMPv améliorées.

DX APM fournit deux Data Collectors SystemEDGE : le Data Collector SystemEDGE autonome et le Data Collector SystemEDGE pour Linux. Le Data Collector SystemEDGE autonome est pris en charge pour AIX, Linux et Windows. SystemEDGE Data Collector pour Linux vous permet de continuer d'utiliser la surveillance d'hôte et de profiter des avantages offerts par un Data Collector SystemEDGE. **Informations complémentaires** : Data Collector SystemEDGE pour Linux.

Exécution de plusieurs agents Infrastructure sur le même ordinateur

Vous pouvez désormais exécuter plusieurs agents Infrastructure sur un seul ordinateur pour répartir la charge afin de gérer la surveillance de nombreux lots. Vous pouvez configurer le nom de service et les ports lorsque vous installez l'agent Infrastructure pour éliminer les conflits à partir de plusieurs agents installés sur le même ordinateur. **Informations complémentaires** : Téléchargement et installation de l'agent Infrastructure sous AIX, Linux et Solaris.

Équilibrage de charge de l'agent Infrastructure pour les environnements Node.js

Vous pouvez désormais équilibrer la charge de plusieurs agents Infrastructure pour obtenir une haute disponibilité dans des environnements cloud et de conteneur Node.js complexes. L'agent UMA fournit une communication HTTP entre la sonde Node.js et l'agent de collecteur HTTP de l'agent UMA. Cette fonctionnalité vous permet de configurer l'équilibrage de charge HTTP pour gérer vos agents Infrastructure. L'équilibreur de charge offre une distribution automatisée du trafic provenant des agents Node.js et à destination de plusieurs agents Collecteur HTTP. Cette distribution empêche la surcharge d'un agent Node.js particulier. **Informations complémentaires** : Agent UMA pour le collecteur HTTP.

Améliorations apportées à la surveillance de journaux

La surveillance de journaux lit désormais les fichiers journaux nouvellement générés après configuration sans avoir à redémarrer l'application gérée. Vous pouvez utiliser des expressions régulières lors de la configuration des noms de fichier journal pour bénéficier d'une meilleure correspondance de noms. La surveillance des journaux peut maintenant lire de manière dynamique les fichiers journaux créés quotidiennement ou à une fréquence plus élevée. DX APM peut désormais lire les erreurs contenues dans les fichiers journaux et créer les mesures Erreurs par intervalle et clichés d'erreur associés. Team Center affiche les traces de transaction d'erreur lorsque vous sélectionnez un vertex de l'agent Moniteur de journaux. **Informations complémentaires** : Surveillance des journaux.

Améliorations apportées à la sécurité de l'agent Infrastructure

L'agent Infrastructure est maintenant pris en charge sur les dernières plates-formes et avec les protocoles de sécurité standard du secteur. Voici quelques exemples : chiffrement AES-256 de bout en bout ; hachage SHA-256 ; SNMPv3, le cas échéant ; mise à niveau vers VS 2017. Par ailleurs, tous les mots de passe stockés dans les fichiers de configuration sont chiffrés, le cas échéant. **Informations complémentaires** : Data Collector SystemEDGE autonome, Surveillance d'hôte sous Linux.

Ajout de la prise en charge de SSL par le service Surveillance MongoDB

Le service Surveillance MongoDB a été amélioré afin d'utiliser le protocole SSL pour des communications plus sécurisées entre le client MongoDB et l'agent Infrastructure. **Informations complémentaires** : Installation et configuration de la surveillance MongoDB.

Agent .NET/.NET Core

Surveillance améliorée de l'agent de navigateur

Par défaut, la surveillance de l'agent de navigateur pour les applications .NET inclut désormais la décoration de réponse basée sur l'en-tête HTTP. Aucune autre configuration manuelle de l'outil de suivi n'est requise pour obtenir la corrélation des traces de transaction de l'agent de navigateur et la corrélation entre les sessions DX AXA et DX APM. **Informations complémentaires** : *Articles DX APM* : Configuration de l'agent de navigateur pour .NET/.NET Core, Configuration de l'injection automatique de snippets de l'agent de navigateur pour l'agent .NET/.NET Core, Configuration de la décoration de cookies de réponse d'agent de navigateur pour .NET/.NET Core/*Articles CA Experience Collector* : Installation de l'agent .NET et Configuration de l'agent de navigateur, Configuration de l'agent de navigateur pour .NET, Propriétés de l'agent de navigateur pour .NET.

Agent de surveillance universel (UMA)

Tableaux de bord DX de l'agent UMA

L'agent UMA fournit désormais des tableaux de bord Grafana DX prédéfinis qui présentent les données de performances de vos environnements Kubernetes. Ces tableaux de bord viennent compléter les tableaux de bord de couche d'infrastructure de Team Center. Les tableaux de bord de l'agent UMA prennent en charge tous les environnements de conteneur, y compris Kubernetes, OpenShift et Docker (ECS). **Informations complémentaires** : Agent de surveillance universel, [Tableaux de bord de l'agent de surveillance universel \(UMA\)](#).

Surveillance des performances du cluster Kafka de l'agent UMA

Vous pouvez désormais surveiller les performances de votre cluster Kafka à l'aide de l'agent UMA. L'agent UMA détecte automatiquement vos pods ZooKeeper et vos pods d'intermédiaire Kafka à l'aide d'annotations et des configurations de votre extension de surveillance Kafka. Vous pouvez configurer SSL pour les intermédiaires Kafka et pour JMX sur SSL.

Améliorations apportées à la surveillance Kubernetes

L'agent UMA fournit désormais des informations plus approfondies sur la surveillance Kubernetes, affichant ainsi davantage de données sur les performances réseau et sur les performances de cluster. Vous pouvez désormais exécuter la surveillance Kubernetes avec la dernière version de Kubernetes. La surveillance Kubernetes inclut désormais la prise en charge des volumes persistants, fournissant ainsi les nouvelles mesures **%UC/Utilisation de la mémoire** et **%Utilisation du disque par pods**. Vous pouvez surveiller les objets StatefulSet de Kubernetes à l'aide des nouvelles mesures **%UC/Mémoire** et **%Utilisation du disque par pods**. Les nouvelles mesures s'affichent également dans les tableaux de bord DX de l'agent UMA.

Prise en charge de l'hébergement multiclient de l'UMA

Vous pouvez désormais déployer et utiliser l'agent UMA dans un environnement d'hébergement multiclient. **Informations complémentaires** : Déploiement de l'agent UMA dans un environnement d'hébergement multiclient.

Gestion des agents de surveillance universels à l'aide d'APM Command Center

Vous pouvez désormais créer et déployer des packages de l'UMA dans APM Command Center. **Informations complémentaires** : Déploiement des packages d'UMA à l'aide d'APM Command Center.

Améliorations apportées à l'interface utilisateur

Affichage des rôles d'univers dans Team Center

Lorsque vous utilisez l'authentification SSO, les rôles que vous pouvez utiliser peuvent varier pour chaque session en fonction de l'IdP externe auquel l'accès est accordé et qui est indiqué dans la réponse SAML. Dans le panneau **Launchpad > Paramètres > Utilisateurs**, vous pouvez consulter vos rôles d'univers spécifiques et vos rôles de client hébergé (Utilisateur, Utilisateur avec pouvoir, Administrateur de clients hébergés). Vous pouvez maintenant également consulter votre rôle de profil actuel dans l'écran supérieur droit de la fenêtre. **Informations complémentaires** : Dans l'article Configuration de l'univers, consultez la section **Configuration de la sécurité de l'univers**.

Nouvelle icône Team Center pour accéder à la page de gestion de l'outil de calcul JavaScript

En tant qu'administrateur de clients hébergés, vous pouvez maintenant cliquer sur une nouvelle icône pour accéder à l'écran **Gestion de l'outil de calcul JavaScript**, dans lequel vous pouvez définir la sécurité de la vue JavaScript. **Informations complémentaires** : Rôles et privilèges pris en charge.

Prise en charge des propriétés multiniveau dans la boîte de dialogue de téléchargement d'agent

La boîte de dialogue de téléchargement d'agent permet désormais de définir des propriétés qui utilisent des configurations multiniveau. Par exemple, la configuration du moniteur de journal utilise un nombre variable d'éléments matchItem, pathPattern et matchPattern. Avec cette nouvelle fonctionnalité, vous pouvez ajouter des sous-propriétés sous des sous-propriétés lors de la configuration des options dans la boîte de dialogue de téléchargement d'agent.

Autres fonctionnalités

Visibilité sur les bases de données MongoDB et Redis pour la surveillance des applications de l'agent Python

L'agent Python DX APM fournit désormais une visibilité améliorée sur les bases de données d'arrière-plan pour les applications Python. Vous pouvez maintenant surveiller vos bases de données MongoDB et Redis pour détecter les composants en aval, en enrichissant la topologie avec des fonctions d'analyse des services et d'analyse des causes premières. Team Center affiche les mesures de performances pour les appels d'arrière-plan et les traces de transaction corrélées. **Informations complémentaires** : Prise en charge de MongoDB, Prise en charge de Redis.

Amélioration du module d'extension Jenkins pour DX APM

Vous pouvez désormais configurer le module d'extension Jenkins pour DX APM en mode principal ou en mode secondaire, en fonction de la configuration de Jenkins. **Informations complémentaires** : Configuration du module d'extension Jenkins pour DX APM.

Plates-formes et fonctionnalités nouvellement prises en charge

Prise en charge d'APM pour SiteMinder (CA APM pour CA SSO) pour AIX 7

Vous pouvez désormais surveiller les performances de l'agent APM pour SSO exécuté sous AIX 7. Désormais, curl est intégré à l'agent Web APM pour SSO pour AIX, qui offre également la prise en charge d'AIX 7 64 bits. **Informations complémentaires** : Dans l'article [APM pour SiteMinder 13.3.0](#), consultez la section **Installation et configuration sur l'agent Web (AIX)**.

Plate-forme de l'agent Infrastructure/Environnements pris en charge et certification

L'agent Infrastructure est maintenant pris en charge sur davantage de plates-formes parmi les plus récentes et avec les protocoles de sécurité standard du secteur. Toutes les fonctionnalités de l'agent Infrastructure sont certifiées pour fonctionner sur ces plates-formes et dans les environnements suivants : Windows 10, Windows 2019, Windows CORE 2019, RHEL 8.x, CentOS 8.x, SLES 15.x, OpenSuse 15 et Ubuntu 20.04. L'agent SystemEDGE de l'agent Infrastructure est pris en charge sur les serveurs RHEL 8.x et Windows 2019. La surveillance d'hôte de l'agent Infrastructure est prise en charge pour Windows 2019. **Informations complémentaires** : Surveillance d'hôte sous Windows, Matrice de prise en charge de l'agent Infrastructure, Dépannage de la surveillance d'hôte.

Agent EP CA APM 10.7 pris en charge avec DX APM SaaS

Avec DX APM, vous pouvez continuer à utiliser les scripts Perl de l'agent EP CA APM 10.7x dans DX APM SaaS. Pour cela, vous devez migrer votre agent EP CA APM 10.7 vers DX APM SaaS. **Informations complémentaires** : dans l'article [Proxy cloud](#), consultez la section **Migration d'agents individuels vers DX APM à l'aide d'un proxy cloud**.

Problèmes connus

Défaut DE521796 : duplication des vertex de transaction métier sur la carte

Symptôme : j'ai téléchargé l'agent Java Tomcat pour DX APM 21.11 avec l'extension d'agent de navigateur DX APM 21.11. J'ai exploré DX APM et j'ai examiné la carte dans Team Center. Pour certains vertex, le vertex de transaction métier de l'agent de navigateur et les transactions métier de l'agent Java sont associés au vertex frontal. Ce problème survient uniquement avec les agents DX APM 21.11.

Solution : assurez-vous que les trois propriétés ci-après sont définies sur **false**.

- **introscope.agent.first.frontend.biz.enabled**

Lorsqu'aucune transaction métier n'a été définie en externe, cette propriété permet à l'agent Java de créer une transaction métier par défaut. L'agent Java identifie le premier composant frontal surveillé.

- **Valeurs** : true ou false
- **Valeur par défaut** : true
- **Exemple** : introscope.agent.first.frontend.biz.enabled=true
- **Remarque** : Aucun redémarrage de l'application surveillée n'est requis.
- **introscope.agent.crossprocess.biz.enabled**
 Cette propriété permet à l'agent Java de transférer les transactions métier des divers processus vers des agents en aval. Elle permet à DX APM de créer des mesures de transaction métier interprocessus pour les agents en aval.
 - **Valeurs** : true ou false
 - **Valeur par défaut** : true
 - **Exemple** : introscope.agent.crossprocess.biz.enabled=true
 - **Remarque** : Aucun redémarrage de l'application surveillée n'est requis.
- **introscope.agent.backend.biz.enabled**
 Cette propriété permet à l'agent Java de collecter les mesures de transaction métier pour les composants d'arrière-plan.
 - **Valeurs** : true ou false
 - **Valeur par défaut** : true
 - **Exemple** : introscope.agent.backend.biz.enabled=true
 - **Remarque** : Aucun redémarrage de l'application surveillée n'est requis.

Défaut DE521742 : anomalies non converties en problèmes

Symptôme : je souhaite surveiller les applications à l'aide des agents DX APM 21.11 sans activer l'agent de navigateur. J'ai remarqué que les anomalies ne sont pas converties en problèmes, y compris lorsque des alertes sont actives pour les noeuds des composants frontaux. Les alertes actives sont à l'état Danger ou Avertissement. De nouveaux vertex de transaction métier ont été créés par l'agent DX APM 21.11. Ces vertex signalent des mesures BlamePoint. Les mesures BlamePoint s'affichent sous le nouveau vertex de transaction métier, qui correspond aux mesures générées par l'agent pour le composant frontal.

J'ai remarqué que les anomalies sont converties en problèmes uniquement lorsque des alertes sont actives pour les nouveaux vertex de transaction métier. Des mesures apparaissent sous le noeud Composant frontal. Toutefois, certaines mesures de transaction métier sont manquantes pour les nouvelles transactions métier. Les mesures manquantes sont toutes des mesures non liées à BlamePoint. En outre, les alertes de composants frontaux par défaut ne sont pas présentes sous le nouveau vertex de transaction métier. Ce problème survient uniquement avec les agents DX APM 21.11.

Solution : créez les alertes de composants frontaux en modifiant le groupement de mesures pour les alertes par défaut. Incluez une nouvelle expression régulière pour les mesures du noeud Secteur d'activité ou créez des alertes personnalisées sur les mesures BlamePoint de la transaction métier. L'agent signale ces mesures sous le noeud d'agent **Secteur d'activité**. Aucune solution n'est disponible pour créer des alertes personnalisées générées sous les mesures non liées à BlamePoint dans le noeud Composant frontal.

Défaut DE521611 : erreur de lien de définition d'alerte lorsque le nom d'alerte contient le signe plus

Symptôme : j'ai créé une alerte dont le nom contient le signe plus (+). Le nom était semblable à celui ci-après : **cpu+Processor1**. J'ai ouvert la page **Paramètres > Alertes > Modifier les alertes** pour tester l'alerte. J'ai ouvert DX Operational Intelligence et j'ai accédé à la page **Toutes les alarmes** pour tester la définition d'alerte. J'ai sélectionné l'alerte **cpu+Processor1**. Dans la section **Présentation**, sous **Attributs personnalisés**, j'ai cliqué sur le lien **Définition d'alerte APM > Définition d'alerte**. Toutefois, la page **Alerte** ne s'est pas ouverte. De plus, dans DX APM, dans la page **Modifier les alertes**, le message d'erreur suivant s'est affiché : *Error fetching alert* (Erreur lors de l'extraction des données). Le même problème survient lorsqu'un nom de module de gestion contient le signe plus.

Solution : n'incluez pas le signe plus dans les alertes et les modules de gestion DX APM.

Défaut DE521571 : exception lors du téléchargement d'un lot d'APM Command Center vers l'agent en cours d'exécution

Symptôme : lorsque j'ai essayé de télécharger un lot APM Command Center vers l'agent Java en cours d'exécution, celui-ci a émis des exceptions semblables à celles ci-dessous.

```
Could not copy file from https://<gateway name>:443/apm/appmap/acc/apm/acc/downloadpackage/70368744219120?format=zip&bundles=70368744216967&task=70368744219123&packageDownloadSecurityToken=<security token> to C:\<download location>\package.tmp. Error details javax.net.ssl.SSLHandshakeException: Received fatal alert: unrecognized_name
```

Remarque : Ce problème survient uniquement avec certaines versions du JDK, par exemple Java 1.8u25.

Solution : il n'existe aucune solution à ce problème.

Défaut DE521544 : impossibilité d'afficher la liste déroulante des attributs Ajouter une fiche d'expérience

Symptôme : je me suis connecté à mon client locataire et j'ai accédé à DX APM. J'ai configuré mon agent Java Tomcat, puis j'ai entraîné mon application à générer quelques transactions. Dans **Vue Expérience**, j'ai sélectionné **Ajouter « + »**. Dans la page **Ajouter une fiche d'expérience**, dans la liste déroulante **sélectionner un univers**, j'ai choisi **Your applications** (Vos applications). Au niveau de la puce **use entire universe or apply a filter** (Utiliser tout l'univers et appliquer un filtre), j'ai choisi **Select agent from Application layer** (Sélectionner un agent dans la couche applicative). Sous **Group by section** (Grouper par section), lorsque j'ai sélectionné la liste déroulante **Attribute** (Attribut), la liste était vide. Elle n'affichait aucun attribut de couche. Ce problème survient uniquement avec les agents DX APM 21.11.

Solution : sélectionnez la case à cocher **Inclure le noeud d'expérience** dans la page **Ajouter une fiche d'expérience**. Vous pouvez voir la liste déroulante **Attributs** (Attributs), mais uniquement pour la couche **Application** elle-même, pas pour les autres couches.

Défaut DE520944 : affichage incorrect d'un message d'erreur par APM Command Center après la modification de la configuration du package

Symptôme : j'ai utilisé la boîte de dialogue de téléchargement d'agent pour télécharger un agent Infrastructure. J'ai accédé à APM Command Center pour configurer l'agent Infrastructure et j'ai choisi **Packages > Configuration**. J'ai modifié mon package, puis j'ai configuré un mélange de propriétés contrôlées et dynamiques. Certaines propriétés requièrent un redémarrage de l'application gérée, d'autres non. Lorsque j'ai cliqué sur **Basculer**, le message suivant s'est affiché :

```
Agent is not using the latest package version.
The latest package version must be applied manually.
```

Lorsque j'ai appliqué la nouvelle version de package à l'agent, le message d'erreur ci-dessous s'est affiché pour toutes les modifications de configuration contrôlées et dynamiques de l'agent Infrastructure :

```
The latest version of package "Infrastructure Agent-apmia-20211117" can only be applied manually. The agent that uses this package will not be displayed. APM Command Center does not support applying newer infrastructure agent package version through user interface.
```

Cependant, le package apparaissait toujours dans la liste des versions et j'ai pu appliquer le nouveau package à l'agent en cours d'exécution.

Solution : vous pouvez ignorer ces messages. Toutes les fonctionnalités liées aux packages fonctionnent correctement. Les listes de packages affichent les versions appropriées et aucun problème ne survient lors de l'application de nouveaux packages aux agents exécutés.

Défaut DE520499 : message d'erreur de données d'ensemble de traces de transaction dans la console de navigateur et notifications

Symptôme : je me suis connecté à mon client locataire et j'ai accédé à DX APM. J'ai connecté mon agent Java Tomcat et j'ai entraîné mon application Java pour générer des traces de transaction. Dans la vue **Mesures**, j'ai sélectionné un nom d'agent et j'ai cliqué sur l'onglet **Traces**. J'ai défini l'heure de **Live** sur plusieurs temps d'historique, par exemple 24 ou 6 heures, sans fermer l'onglet **Traces**. Après quelques minutes, l'exception ci-dessous est apparue dans ma console de navigateur et dans les notifications de navigateur :

```
Error retrieving transaction trace set data. Status Code: undefined Type: undefined Reason: undefined
```

Ce message s'est également affiché dans la vue **Carte** du bas de page de navigateur et de la console de débogage lorsque j'ai sélectionné un vertex.

Solution : il n'existe aucune solution à ce problème.

Défaut DE519466 : valeur zéro incorrecte au niveau de la mesure de temps de réponse moyen MongoDB de l'agent Python

Symptôme : lorsque l'agent Python surveille les opérations de lecture MongoDB, la valeur de la mesure **Temps de réponse moyen (ms)** est de zéro alors qu'elle devrait être supérieure à zéro.

Solution : il n'existe aucune solution à ce problème.

Défaut DE496868 : Mise à niveau - AJOUT de configurations enregistrées : package non disponible après la mise à niveau

Symptôme : je me suis connecté à DX APM et j'ai accédé à la boîte de dialogue de téléchargement d'agent dans Team Center. Auparavant, j'avais créé et enregistré des packages avec des configurations de propriété. J'ai cliqué sur **Paramètres, Agent, Télécharger un agent**. Lorsque j'ai cliqué sur **Configurations de package enregistrées**, seuls les packages existants pour l'agent Infrastructure étaient disponibles. Les packages enregistrés pour tous mes autres agents affichaient le message d'erreur suivant : `Package non disponible`. Exemples d'agents : Tomcat sur les agents Windows et Linux et agents Java. La colonne **Actions** de ces agents n'affichait aucune icône. Par conséquent, je n'ai pas pu modifier ni télécharger ces packages qui ne sont pas liés à l'agent Infrastructure.

Solution : il n'existe aucune solution à ce problème.

21.6

Cette section indique les fonctionnalités nouvelles, modifiées et désapprouvées dans DX APM 21.6.

Améliorations apportées à la surveillance du cloud

Voici les améliorations liées à la surveillance du cloud dans cette version.

Google Cloud Monitoring

Service GCP Cloud VPN

Le service GCP Cloud Virtual Private Network (VPN) vous permet de surveiller l'intégrité et les performances de Google Cloud Platform Cloud VPN. Cette fonctionnalité permet de vous assurer que votre infrastructure cloud est toujours disponible et performante pour respecter les SLA de temps de disponibilité de vos clients.

Google Virtual Private Network (VPN) établit des connexions sécurisées entre les réseaux sur site, les bureaux distants, les unités client et le réseau global Google. Cette fonctionnalité permet à votre organisation de migrer l'hébergement VPN vers le cloud et d'améliorer l'accès aux ressources basées sur le cloud. **Informations complémentaires** : Service Google VPN.

Amazon Web Services (AWS)

AWS Database Migration Service (DMS)

Surveillez l'intégrité et les performances du service AWS Database Migration Service, qui vous permet de migrer de manière transparente plusieurs composants vers vos données dans le cloud AWS. Ces composants incluent les bases de données relationnelles, les entrepôts de données, les bases de données NoSQL et d'autres types de stockages de données. Vous pouvez utiliser le service AWS Database Migration Service pour migrer vos données entre des instances sur site (via une configuration de cloud AWS) ou entre des combinaisons de configurations cloud et sur site.

Ce service vous permet d'effectuer des migrations uniques et de répliquer les modifications en cours pour maintenir la synchronisation des sources et des cibles. **Informations complémentaires** : AWS Database Migration Service.

Agent Java

Amélioration de la journalisation des propriétés de l'agent Java

Vous pouvez examiner les journaux de l'agent Java pour déterminer l'ensemble précis des propriétés de configuration en cours d'utilisation et la source des valeurs de propriété.

Prise en charge de Java 13 et Java 14

L'agent Java prend désormais en charge les versions 13 et 14 de Java.

Prise en charge de JBoss EAP 7.3

L'agent Java prend désormais en charge la version 7.3 de JBoss EAP.

Modification de la configuration par défaut du filtrage automatique des traces de transaction

Le filtrage automatique des traces de transaction n'inclut plus les transactions les plus rapides et les plus lentes dans la configuration par défaut. Ces paramètres peuvent entraîner une surcharge des ressources supérieure à la surcharge normale pour certaines applications. La propriété par défaut actuelle dans le fichier `introscopeagent.profile` est la suivante :

```
introscope.agent.transactiontracer.sampling.enabled.set=random
```

Pour activer le filtrage des transactions les plus rapides et les plus lentes, reportez-vous à la section Configuration du filtrage des traces de transaction.

Informations complémentaires : Configuration des options de trace de transaction automatique.

Agent Infrastructure

Surveillance de base de données IBM DB2

Vous pouvez désormais surveiller les performances de votre base de données IBM DB2 dans un environnement dynamique. La surveillance de base de données IBM DB2 vous offre une visibilité sur les KPI de base de données. Ces informations vous permettent d'isoler les problèmes des composants de l'application et vous aident à résoudre rapidement les problèmes dans l'environnement dynamique.

L'extension de surveillance de base de données IBM DB2 est un système de gestion de bases de données relationnelles prêts pour l'entreprise. Nous avons conçu cette extension pour offrir une résilience, des performances et une rentabilité aux charges de travail transactionnelles. **Informations complémentaires** : Surveillance de base de données IBM DB2.

Extension IBM DataPower

L'extension IBM DataPower est une passerelle multi-canaux unique conçue pour assurer la sécurité, le contrôle et l'intégration. Nous avons optimisé cette extension pour accéder à une gamme complète de charges de travail mobiles, Web, d'API, d'architecture SOA (architecture orientée services), B2B et de cloud. L'extension IBM DataPower vous permet de surveiller les données de performances essentielles relatives à la passerelle DataPower. Vous pouvez identifier de manière proactive les problèmes de performances dans l'environnement et corrélérer rapidement les unités DataPower et les applications d'arrière-plan. **Informations complémentaires** : Extension IBM DataPower.

Surveillance vRealize Operations

Vous pouvez surveiller, dépanner et gérer l'intégrité et la capacité de votre environnement virtuel en appliquant une automatisation basée sur les stratégies. La surveillance vRealize Operations offre une gestion intelligente des opérations avec une visibilité de l'application au stockage dans les infrastructures physiques, virtuelles et cloud. Cette extension collecte les données de performances de chaque objet à chaque niveau de votre environnement virtuel et analyse les données pour fournir des informations en temps réel sur les problèmes de performances. **Informations complémentaires** : Extension vRealize Operations.

Améliorations de la surveillance d'IBM Integration Bus (IIB)

Vous pouvez désormais établir la connexion de surveillance IIB en mode local ou distant pendant la configuration. Les exigences de sécurité définies pour la surveillance d'un objet MQ ont été optimisées pour offrir une surveillance plus sécurisée. **Informations complémentaires** : Installation et configuration de l'extension de surveillance IIB, Mesures de surveillance IIB.

Mesures d'observabilité RESTmon

L'agent Infrastructure a été amélioré pour prendre en charge les mesures d'observabilité RESTmon. Vous pouvez utiliser ces mesures pour autosurveiller les performances de vos déploiements de surveillance cloud. Cette prise en charge fournit des mesures relatives à différentes plates-formes. Nous fournissons des mesures liées au point de terminaison Amazon Web Services, des mesures liées à la surveillance de Google Cloud Platform, des mesures liées à Azure, etc. **Informations complémentaires** : Mesures d'observabilité RESTmon.

Extension de surveillance SiteMinder

DX Application Performance Management (APM) pour CA Single Sign-On (CA SSO) est un package DX APM à usage spécial qui permet de surveiller CA SiteMinder. La nouvelle extension de surveillance DX APM SiteMinder inclut ce package. CA APM pour CA SSO collecte périodiquement les mesures CA SSO et les envoie à l'agent Infrastructure de DX APM. L'extension de surveillance SiteMinder inclut plusieurs tableaux de bord DX fournissant des informations détaillées sur les performances des serveurs proxy et des agents Web. **Informations complémentaires** : Extension de surveillance SiteMinder.

Extension de surveillance Elastic

L'extension de surveillance Elastic vous permet de surveiller les performances du cluster, des nœuds et des index Elastic Search afin d'identifier les problèmes dans votre environnement dynamique. Vous pouvez désormais filtrer les mesures et effectuer des configurations de groupe à l'aide de l'extension de l'agent Infrastructure pour Elastic Search. **Informations complémentaires** : Extension de surveillance Elastic.

Prise en charge de la surveillance de base de données Oracle pour Oracle 19C

L'extension de l'agent Infrastructure pour la surveillance de base de données Oracle prend désormais en charge la version 19C de la base de données Oracle. **Informations complémentaires** : Surveillance de la base de données Oracle

Agent .NET/.NET Core

Améliorations apportées à l'instrumentation intelligente

L'instrumentation intelligente .NET/.NET Core détecte automatiquement les composants frontaux et d'arrière-plan .NET/.NET Core. Après la détection, les outils de suivi des composants frontaux et d'arrière-plan sont ajoutés à un fichier PBD que l'agent .NET recharge. Par défaut, les nouveaux outils de suivi sont désactivés, mais vous pouvez configurer les outils de suivi. Vous pouvez également démarrer des sessions de détection à l'aide d'une session de suivi de transaction. L'instrumentation intelligente .NET/.NET Core inclut également un déclencheur d'UC configurable

qui démarre une session de détection lorsque l'UC utilisateur dépasse un seuil. **Informations complémentaires :** Configuration de l'instrumentation intelligente .NET/.NET Core.

Prise en charge de .NET 5

L'agent .NET/.NET Core prend désormais en charge la version 5 de .NET.

Agent de surveillance universel (UMA)

Mise en package et téléchargement de l'UMA à l'aide d'APM Command Center

Vous pouvez désormais créer un package de l'UMA avec des fonctionnalités de surveillance spécifiques à l'UMA dans APM Command Center. **Informations complémentaires :** Déploiement des packages d'UMA à l'aide d'APM Command Center.

Surveillance de l'utilisation du disque de pod

Vous pouvez désormais surveiller l'utilisation du disque des pods configurés avec des volumes persistants. **Informations complémentaires :** Données de performance des pods.

Attribution de nom automatique de l'agent par l'UMA dans les environnements de conteneur

L'UMA détermine désormais automatiquement un nom d'hôte d'agent approprié pour les agents Java dans les environnements de conteneur. Cette fonctionnalité inclut l'attribution automatique de nom à l'agent Java dans .NET/.NET Core, UMA AutoAttach dans Kubernetes, ECS, OpenShift, etc. **Informations complémentaires :** Installation et configuration de l'UMA pour Kubernetes.

Prise en charge de l'hébergement multiclient de l'UMA

Vous pouvez désormais utiliser l'UMA dans un environnement d'hébergement multiclient.

Fonctionnalité AutoAttach de l'UMA pour l'agent de sonde Node.js

Vous pouvez désormais surveiller toutes vos applications et toutes vos infrastructures s'exécutant dans l'environnement Kubernetes avec un seul agent. La configuration de la fonctionnalité AutoAttach sans réglage ou avec des réglages minimum facilite l'intégration et la détection. La fonctionnalité AutoAttach vous offre une solution unique de gestion et de surveillance des applications natives cloud prêtes à l'emploi sur le cloud hybride. **Informations complémentaires :** Fonctionnalité AutoAttach de l'agent Node.js.

Problème connu

Défaut DE504064 Arrêt brutal de la JVM Windows avec EXCEPTION_ACCESS_VIOLATION

Symptôme : dans certaines circonstances, la machine virtuelle Java peut créer une image mémoire du noyau. Ce problème se produit lorsque DX APM surveille des applications asynchrones.

Solution : pour corriger le problème, effectuez l'une des opérations suivantes :

- Procédez à la mise à niveau vers le dernier patch de la machine virtuelle Java.
La mise à niveau résout généralement ce problème.
- Créez ou mettez à jour un package qui contient le groupe NoRedef approprié pour votre environnement.
Le groupe NoRedef contient le fichier `AgentNoRedefNoRetrans.jar`, qui désactive la redéfinition et la retransformation des classes afin d'éviter d'éventuels problèmes de performances.
Vous pouvez choisir parmi les groupes NoRedef suivants :

- Java Agent NoRedef
- JBoss NoRedef
- Sockets NoRedef
- Tomcat NoRedef
- WebLogic NoRedef
- WebSphere NoRedef

Informations complémentaires : Informations sur AgentRedef dans la section Configuration du serveur WebSphere Application Server, Déploiement des packages d'agent à l'aide d'APM Command Center.

21.4

Cette section indique les fonctionnalités nouvelles, modifiées et désapprouvées dans DX APM 21.4.

Améliorations apportées à la surveillance du cloud

Voici les améliorations liées à la surveillance du cloud dans cette version.

Google Cloud Monitoring

Service Google Cloud Billing

Le service Google Cloud Billing fournit des mesures relatives aux coûts de Google Cloud Platform (GCP), avec des données générées quotidiennement (configurable). Ce service fournit les informations requises pour budgéter les coûts de GCP. Informations complémentaires : Service Google Cloud Billing

Surveillance de GCP avec service Keyless Entry

Ce service vous permet de surveiller les services Google Cloud sans configurer les jetons de sécurité. Au lieu de cela, le service Keyless Entry utilise Google Kubernetes Engine (GKE) Workload Identity pour fournir les autorisations appropriées. **Informations complémentaires** : Google Cloud Monitoring avec service Keyless Entry.

Amazon Web Services (AWS)

Amélioration du service de surveillance AWS EMR

Le service de surveillance AWS EMR prend désormais en charge deux nouvelles mesures. Ces mesures fournissent le statut des applications en cours d'exécution dans le cluster AWS EMR :

- **Statut** : affiche le statut du cluster EMR.
- **Code de statut** : spécifie le motif de l'échec du cluster (cette mesure est disponible uniquement pour les clusters arrêtés).

Informations complémentaires : Service de surveillance AWS EMR.

Amélioration du service de surveillance AWS Glue

Un nouveau message d'erreur de mesure a été ajouté à ce service. Cette mesure affiche le message d'erreur correspondant à l'échec du job Glue. **Informations complémentaires** : Service AWS Glue.

Service Azure Service Usage and Quotas

Le nouveau service Azure Service Usage and Quotas (Utilisation et quotas du service Azure) vous permet d'afficher la limite actuelle d'utilisation et de service des ressources Azure. Vous pouvez afficher l'utilisation et les quotas pour les fournisseurs suivants :

- Calcul
- Stockage
- Réseau
- Azure VMware Solution by cloudSimple

Informations complémentaires : Utilisation et quotas du service Azure.

Agent Java

Filtrage automatique des traces de transaction

DX APM surveille toutes les transactions dans votre environnement. DX APM collecte par défaut les traces de transaction pour les problèmes de performances, les erreurs et les blocages. Le filtrage automatique des traces de transaction vous permet d'examiner les transactions potentiellement problématiques sans devoir exécuter de manière explicite les traces de transaction. DX APM ajoute désormais une configuration supplémentaire pour le filtrage automatique des traces par N plus lents, N plus rapides, etc. **Informations complémentaires** : Configuration des options de trace de transaction automatique.

Attribution de nom à l'agent Java prenant en charge les conteneurs

DX APM détermine désormais automatiquement un nom d'hôte d'agent approprié pour les agents Java dans les environnements de conteneur. DX APM fournit des noms d'agent Java pour les déploiements Kubernetes natifs de l'agent de surveillance universel (UMA) et les déploiements d'agent Java standard non-UMA. **Informations complémentaires** : Attribution de nom à l'agent Java, Installation et configuration de l'UMA pour Kubernetes. Consultez la section sur la résolution des propriétés dynamiques de l'UMA.

Nouveau mode de démarrage de l'agent Java

Vous pouvez désormais éviter le ralentissement du temps de démarrage de l'agent Java en configurant la propriété système `-Dcom.wily.introscope.agent.startup.mode=neo` pour démarrer l'agent Java en mode Neo. Vous pouvez retarder le démarrage de l'agent Java en configurant la propriété système `-Dcom.wily.introscope.agent.startup.delay`. **Informations complémentaires** : Configuration du mode de démarrage.

Agent Infrastructure

Prise en charge des traces de surveillance de base de données SQL Server

Vous pouvez désormais afficher les traces de transaction de la base de données SQL Server dans la **vue Carte** en sélectionnant le nœud de base de données SQL Server correspondant et en cliquant sur l'onglet **Base de données**. Les traces de transaction de base de données SQL Server sont constituées d'événements comprenant différents indicateurs de performances pour la surveillance et la maintenance de votre base de données SQL Server. **Informations complémentaires** : Traces de base de données SQL Server.

Nouvelles mesures d'utilisation de l'UC/segment de mémoire

La surveillance de serveurs JMX distants fournit désormais des mesures relatives à la mémoire de segment utilisée pour l'allocation d'objet. Ces mesures sont activées par défaut et s'affichent ici dans l'arborescence de mesures : `<agent_infrastructure>|<nœud_racine_mesure_jmx>|JVM|Memory|HeapRemote`. La surveillance de serveurs JMX

fournit également des mesures relatives à la mémoire gérée par la JVM utilisée pour stocker des classes chargées et des métadonnées, et pour le traitement interne. Ces mesures sont activées par défaut et s'affichent ici dans l'arborescence de mesures : <agent_infrastructure>|<noeud_racine_mesure_jmx>|JVM|Memory|Non Heap. Vous pouvez également afficher ces nouvelles mesures en tant que mesures JMX standard. **Informations complémentaires** : Surveillance de serveurs JMX distants, Mesures JMX.

Amélioration de la surveillance F5 LTM

La surveillance F5 LTM permet désormais, avec un déploiement d'agent unique, la surveillance de plusieurs instances F5. Pour chaque instance F5, vous devez configurer un profil F5. **Informations complémentaires** : Surveillance F5 LTM.

Prise en charge de l'authentification par couche sécurisée dans la surveillance Redis

L'extension de surveillance Redis prend désormais en charge la surveillance Redis sur SSL. Utilisez les propriétés suivantes pour activer SSL dans la surveillance Redis :

- introscope.agent.redisinfra.profiles.default.sslenabled
- introscope.agent.redisinfra.profiles.default.servercertificate.path

Informations complémentaires : Configuration de l'extension de surveillance Redis.

Amélioration de la surveillance d'hôte

Surveillez les performances des processus d'hôte dédiés en définissant des arguments de processus dans la configuration de surveillance. **Informations complémentaires** : Propriétés de la surveillance d'hôte.

Prise en charge de RHEL 8.2 pour la surveillance d'hôte, SysEDGE

RHEL 8.2 est désormais certifié pour la surveillance d'hôte et SysEDGE. **Informations complémentaires** : Matrice de prise en charge de l'agent Infrastructure.

Prise en charge de NGINX 1.19.X

DX APM prend désormais en charge la version 1.19.0 de NGINX. **Informations complémentaires** : Surveillance NGINX.

Amélioration de la surveillance vCenter

Vous pouvez désormais surveiller la nouvelle mesure **Resource Pool** (Pool de ressources) avec les autres mesures vCenter dans votre environnement vCenter. **Informations complémentaires** : Surveillance vCenter.

Agent .NET/.NET Core

Détection automatique de composants d'arrière-plan

L'agent .NET/.NET Core détecte désormais automatiquement les composants d'arrière-plan sans instrumentation manuelle ou personnalisée. **Informations complémentaires** : Instrumentation intelligente de l'agent .NET/.NET Core.

Agent de surveillance universel (UMA)

Prise en charge d'ECS et de Docker Swarm

L'agent de surveillance universel détecte et surveille désormais automatiquement les conteneurs et l'infrastructure de noeud AWS ECS et Docker Swarm. **Informations complémentaires** : UMA pour AWS ECS, UMA pour Docker Swarm.

Surveillance Kubernetes améliorée

L'agent de surveillance universel fournit désormais des informations plus détaillées sur la surveillance Kubernetes en fournissant les nouvelles fonctions et mesures de surveillance des performances du réseau et du cluster suivantes :

- Mesures réseau : octets en entrée, octets en sortie, octets envoyés et octets reçus
- Surveillance des performances du serveur d'API et etcd
- Surveillance des performances des configurations de déploiement
- Limites d'UC et de mémoire par projet

Fonctionnalités de l'interface utilisateur

Aperçu du groupement de mesures

L'aperçu de la vue des mesures affiche le mode d'aperçu des groupes de mesures configurés. Vous pouvez afficher les données de mesures pertinentes tracées dans le graphique. La fenêtre Aperçu affiche le graphique de données des mesures basé sur le **Spécificateur de l'agent** et le **Spécificateur de mesure** fournis dans le champ **Expressions**. Informations complémentaires : Configuration des groupements de mesures dans Team Center

Aperçu des alertes

L'aperçu des alertes affiche le mode d'aperçu des groupes de mesures configurés. Vous pouvez afficher les données de mesures pertinentes tracées dans le graphique. La fenêtre Aperçu affiche le graphique de données de mesures basé sur le champ **Groupement de mesures**. **Informations complémentaires** : Création et configuration d'alertes simples dans Team Center.

Aperçu des outils de calcul

L'aperçu des outils de calcul affiche le mode d'aperçu des groupes de mesures configurés. Vous pouvez afficher les données de mesures pertinentes tracées dans le graphique. La fenêtre Aperçu affiche le graphique de données de mesures basé sur le champ **Groupement de mesures**. **Informations complémentaires** : Création et modification d'outils de calcul.

Augmentation de la granularité de la sécurité des univers

Désormais, dans chaque univers, des droits individuels sont affectés aux utilisateurs par module de gestion pour modifier des alertes, des outils de calcul et des groupes de mesures. Auparavant, seuls les utilisateurs disposant du rôle Utilisateur avancé ou Administrateur de clients hébergés pouvaient modifier les alertes, les outils de calcul et les groupes de mesures du module de gestion. Désormais, le rôle Utilisateur avancé, les utilisateurs et les groupes d'utilisateurs doivent disposer de l'autorisation d'afficher ou de créer des alertes, des outils de calcul ou des groupes de mesures dans un module de gestion. L'utilisateur avancé peut toujours démarrer manuellement les sessions de suivi de transaction.

Informations complémentaires : Configuration des univers.

Autres fonctionnalités

Augmentation de la sécurité de la boîte de dialogue de téléchargement d'agent, d'APM Command Center et du proxy cloud

Les agents DX APM téléchargés et les contrôleurs ACC sont désormais plus sécurisés. Voici les améliorations :

- La validation de certificat TLS (Transport Layer Security) d'ACC (APM Command Center) a été améliorée pour les communications entre l'agent et le contrôleur ACC. DX APM valide le certificat et le nom d'hôte pour les agents nouveaux et mis à jour, et les contrôleurs ACC qui utilisent la connexion TLS.
- La validation de certificat TLS est activée pour tous les agents que vous téléchargez depuis la boîte de dialogue de téléchargement d'agent.
- Vous pouvez désormais spécifier des référentiels d'approbations personnalisés pour la validation TLS globale et par client hébergé.
- Vous pouvez mettre à jour les agents existants et les contrôleurs ACC avec un nouveau référentiel d'approbations personnalisé.
- Le proxy cloud est désormais configuré pour utiliser le référentiel d'approbations Java par défaut pour la validation de certificat.

Problème connu

Défaut DE502703 : la propriété `introscope.agent.dotnet.monitorAppPools` ne fonctionne pas

Symptôme : j'ai supprimé les marques de commentaire et configuré la propriété

`introscope.agent.dotnet.monitorAppPools` dans le fichier `introscopeagent.profile` de .NET/.NET Core. Par exemple, `introscope.agent.dotnet.monitorAppPools="DefaultAppPool"`. Après avoir redémarré le serveur Web IIS, la propriété n'est pas appliquée.

Solution : pour CA APM 10.7 et versions antérieures, la valeur configurée était placée entre guillemets.

Pour DX APM SaaS et DX APM sur site, la valeur doit être configurée *sans* guillemets. Par exemple, `introscope.agent.dotnet.monitorAppPools=DefaultAppPool`.

Défaut DE499817 : aucune donnée affichée dans la carte, le tableau de bord ou le carnet d'analyse

Symptôme : sélectionnez le choix de perspective vide (une zone gris clair) dans la liste des perspectives. Lorsque cette perspective apparaît, la carte DX APM, le tableau de bord et le **carnet d'analyse de la vue Expérience** n'affichent aucune donnée.

Solution : sélectionnez une perspective valide dans la liste de perspectives, puis actualisez la page.

21.1

Cette section indique les fonctionnalités nouvelles, modifiées et désapprouvées dans DX APM 21.1.

Cette section indique les fonctionnalités nouvelles, modifiées et désapprouvées dans DX APM 21.1.

Améliorations apportées à la surveillance du cloud

Dans cette version, nous avons apporté plusieurs améliorations liées à la surveillance du cloud, dont celles ci-après :

Nouvelle couche réseau

DX APM fournit une nouvelle couche réseau qui met en corrélation les composants d'application, les éléments d'infrastructure et la topologie réseau. Cette corrélation permet d'identifier l'emplacement du goulot d'étranglement des performances : application, infrastructure ou réseau. La carte DX APM inclut désormais une **couche réseau**. Cette couche contient des informations sur les agents Infrastructure et sur leurs extensions cloud. Cette couche affiche les éléments cloud tels que le cloud privé virtuel (VPC), les routeurs, les interconnexions, les sous-réseaux et autres éléments des VPC. **Informations complémentaires** : Couches de carte.

Google Cloud Monitoring

Activez ces services cloud pour afficher les composants et les connexions dans la couche réseau :

- **Service Cloud privé virtuel de Google**

Le service Cloud privé virtuel (VPC, Virtual Private Cloud) de Google fournit une fonctionnalité réseau pour les instances de machine virtuelle (VM) Compute Engine, les conteneurs Google Kubernetes Engine (GKE) et l'environnement flexible App Engine. Il permet de surveiller l'intégrité et les performances du réseau. **Informations complémentaires** : Cloud privé virtuel de Google Cloud.

- **Service Cloud Router de Google**

Le service Google Cloud Router fonctionne via une connexion VPN ou Cloud Interconnect. Cloud Router fournit un routage dynamique en utilisant le protocole BGP (Border Gateway Protocol) pour les réseaux VPC (Virtual Private Cloud) de Google Cloud. Il permet de surveiller l'intégrité et les performances des routeurs cloud dans Google Cloud Platform. **Informations complémentaires** : Google Cloud Router.

- **Service Google Cloud Interconnect**

Le service Google Cloud Interconnect permet de surveiller l'intégrité et les performances de Google Cloud Interconnect dans Google Cloud Platform. **Informations complémentaires** : Google Cloud Interconnect.

Améliorations apportées au service Google Compute Engine

Google Compute Engine prend désormais en charge les mesures de **mise en miroir** et **NAT**. **Informations complémentaires** : Service Google Compute Engine.

Amazon Web Services

Authentification basée sur les rôles AWS sans informations d'identification

L'authentification basée sur les rôles Amazon Web Services (AWS) surveille les comptes AWS sans informations d'identification. Pour utiliser l'authentification basée sur les rôles, créez une stratégie et un rôle sur les comptes AWS pour surveiller l'agent AWS. **Informations complémentaires** : Authentification basée sur les rôles AWS sans informations d'identification.

Agent Java

Extension Oracle Service Bus 12C

L'extension Oracle Service Bus 12C (OSB12) surveille les détails des transactions OSB, les mesures de performances et offre une visibilité complète sur l'intégrité, puis affiche des informations complètes sur les flux de demandes de bout en bout. Elle indique tous les composants OSB présents dans un flux. **Informations complémentaires** : Extension Oracle Service Bus 12C.

Agent Infrastructure

Surveillance vCenter certifiée pour VMware vSphere version 7

L'extension Surveillance vCenter prend désormais en charge VMware vSphere version 7.0. Informations complémentaires : **Surveillance vCenter**

Agent de surveillance universel

Prise en charge de l'agent de surveillance universel pour WebSphere Liberty Profile

Désormais, l'agent de surveillance universel détecte et instrumente automatiquement les conteneurs WebSphere Liberty. **Informations complémentaires** : WebSphere Liberty.

Fonctionnalités de l'interface utilisateur

Cette section présente les fonctionnalités de l'interface utilisateur nouvelles et améliorées.

Filtrage de carte non sensible à la casse

La valeur de filtrage des URL composée pour interroger les vues **Carte** et **Isolement** n'est plus sensible à la casse. Par exemple, si vous recherchez le nom d'hôte **GOOGLE.Com**, DX APM recherche également les valeurs **google.com**.

Arborescences de mesures filtrées par carte

La nouvelle option **Filtrer la vue des mesures par composants de carte** de l'éditeur **Univers** filtre les arborescences de mesures dans le navigateur de mesures par carte. **Informations complémentaires** : Configuration des univers.

Téléchargement d'App Synthetic Monitor à partir de la boîte de dialogue de téléchargement d'agent

Vous pouvez maintenant télécharger le groupe App Synthetic Monitor (ASM) à partir de la boîte de dialogue **Sélectionner l'agent à télécharger** de l'agent Infrastructure.

Améliorations apportées à la boîte de dialogue Sélectionner l'agent à télécharger

La boîte de dialogue **Sélectionner l'agent à télécharger** du site de téléchargement d'agent offre une nouvelle disposition qui permet de mieux faire la différence entre les agents livrés par l'agent Infrastructure et les extensions disponibles.

APM Command Center

Interface utilisateur d'APM Command Center conforme aux critères WCAG 2.0 AA

Des technologies d'assistance sont maintenant disponibles pour parcourir l'interface utilisateur d'APM Command Center. APM Command Center est désormais conforme aux critères WCAG 2.0 AA.

Autres fonctionnalités

Outils de calcul JavaScript persistants

Les outils de calcul JavaScript supportent désormais le calcul continu des mesures pendant l'ensemble des redémarrages et des mises à niveau de DX APM et sans interaction manuelle. Ils sont désormais stockés sur un lecteur persistant.

Tableaux de bord DX : ajout de la prise en charge des fonctions d'agrégation dans l'API NASS

Le langage de requête NassQL offre un moyen flexible d'interroger et de traiter les données de mesure sur le serveur. Il est semblable au langage SQL propre aux bases de données relationnelles. Plusieurs fonctions permettent d'interroger les données de mesure. Vous pouvez utiliser la fonction FROM et grouper les données à l'aide des fonctions WINDOW et GROUP. Vous pouvez également effectuer des opérations plus avancées d'agrégation et de mappage. **Informations complémentaires** : [Référence de requête d'agrégation de mesures](#).

Problème connu

Défaut DE492513 : impossible d'appliquer un nouveau package aux agents dans APM Command Center

Symptôme : dans APM Command Center, j'ai créé un package pour un agent et effectué des opérations de configuration pendant la création. Ensuite, j'ai mis à jour le package. Lorsque j'ai souhaité appliquer le package à mes agents, aucun agent n'était répertorié. Je n'ai donc pas pu appliquer la version de package mise à jour à mes agents connectés.

Solution : utilisez cette solution de contournement pour installer l'agent avec le package mis à jour.

Procédez comme suit :

1. Dans APM Command Center, cliquez sur l'option **Packages** dans le volet de navigation gauche.
2. Dans la liste **Packages**, sélectionnez la version mise à jour de l'agent.
Les informations sur l'agent s'affichent dans le volet central.
3. Dans la section **Versión du package**, recherchez la ligne **Télécharger le package**.
4. Cliquez sur **Télécharger l'archive du package**.
DX APM télécharge le package sur votre ordinateur.
5. Désinstallez l'ancien agent.
6. Installez l'agent avec la dernière version du package.

Notes de mise à jour 2020

Cette section contient les notes de mise à jour pour 2020.

- [20.11](#)
- [20.9](#)
- [20.6](#)
- [20.4](#)
- [20.1](#)

20.11

Cette section indique les fonctionnalités nouvelles, modifiées et désapprouvées dans DX APM 20.11.

Améliorations apportées à la surveillance Java

Les modifications ci-après ont été apportées à l'agent Java.

Surveillance Spring Cloud Gateway

L'extension Spring Cloud Gateway est une passerelle d'API qui fournit un moyen simple et efficace d'acheminer les API.

Informations complémentaires : Extension Spring Cloud Gateway.

Extension WebSphere Portal

L'extension WebSphere Portal permet de créer et de gérer des portails Web. Vous pouvez utiliser cette extension pour créer un portail, qui est une collection de portlets. Un espace désigné est affecté à chaque portlet dans le portail. Vous pouvez créer les portlets en extrayant des données à partir de diverses sources et afficher des données concernant les portlets dans la vue **Mesures**. **Informations complémentaires :** Extension WebSphere Portal.

Prise en charge de MySQL version 8.x

L'agent SQL pour Java surveille désormais les performances des appels d'arrière-plan de base de données pour la version 8.x de MySQL.

PostgreSQL EDB version 4.2

L'agent SQL pour Java surveille désormais les performances des appels d'arrière-plan de base de données pour la version 4.2 de PostgreSQL EDB.

Agent Java amélioré pour la surveillance du serveur d'applications WebSphere

Vous pouvez maintenant utiliser le fichier `Agent.jar` comme fichier JAR du serveur d'applications WebSphere (WAS) pour les versions 8 et ultérieures. Il n'est plus nécessaire de configurer le fichier `AgentNoRedefNoRetrans.jar`.

Informations complémentaires : Serveur d'applications WebSphere.

Sécurité renforcée de l'agent Java

Vous pouvez maintenant utiliser la propriété `agentManager.tls.validateHostname` pour renforcer la sécurité de DX APM en empêchant les attaques potentielles approuvées de type man-in-the-middle. **Informations complémentaires** : Propriétés de l'agent Java.

Améliorations apportées à la fonction de suivi des transactions de l'agent Java

Vous pouvez maintenant utiliser ces deux propriétés pour collecter et utiliser les traces de transaction automatiques de priorité de l'agent Java. Les traces automatiques de priorité sont des traces de transaction qui activent d'autres fonctionnalités essentielles, telles que la détection de la topologie.

- `introscope.agent.deep.automatic.trace.priority.clamp`
Cette propriété permet de limiter le nombre de traces de transaction automatiques de priorité collectées par l'agent pour chaque intervalle de 1 minute.
- `introscope.agent.deep.automatic.trace.detailed.reason`
Cette propriété permet de décorer les traces de transaction automatiques avec le motif détaillé pour lequel l'agent a été déclenché pour la collecte de la trace. Dans le cas contraire, les traces sont entièrement décorées avec un motif récapitulatif.

Informations complémentaires : Propriétés de l'agent Java.

Améliorations apportées à la surveillance de l'agent .NET

Les modifications ci-après ont été apportées à l'agent .NET.

Instrumentation intelligente .NET/.NET Core

L'instrumentation intelligente .NET/.NET Core détecte et instrumente les composants frontaux .NET/.NET Core sans qu'aucune configuration ne soit requise. Elle est activée par défaut et elle démarre lorsque vous commencez une trace de transaction. Vous pouvez configurer les propriétés permettant de contrôler la consignation de piles de threads spécifiques et l'emplacement des fichiers `.pbd` générés. En cas de détection d'un nouveau composant frontal, l'agent .NET/.NET Core ajoute une configuration au fichier `detected-frontends.pbd`. **Informations complémentaires** : Configuration de l'instrumentation intelligente .NET/.NET Core.

Améliorations apportées à l'analyse de la cause première des performances de l'UC .NET/.NET Core

L'agent .NET/.NET Core affiche deux nouvelles mesures qui fournissent davantage d'informations sur les performances de l'UC pour les méthodes .NET. Ces mesures peuvent vous aider à déterminer si un goulot d'étranglement des performances est dû à l'exécution du code de méthode ou au temps d'E/S.

- Temps d'UC utilisateur moyen (ms)
- Temps d'UC système moyen (ms)

Informations complémentaires : Diagnostic des problèmes de performances système.

Mesures de fragment asynchrones et traces de transaction Fragment asynchrones pour ASP.NET et ASP.NET Core

L'agent .NET/.NET Core surveille maintenant les demandes asynchrones dans les applications ASP.NET et ASP.NET Core. Le navigateur de mesures affiche les mesures du composant frontal associé sous les noeuds **Fragments** et **Called Fragments** (Fragments appelés). L'agent collecte également les traces de transaction Fragment. **Informations complémentaires** : Fragments asynchrones .NET/.NET Core.

Extension Automatic Attribute Decoration pour .NET/.NET Core

L'extension Automatic Attribute Decoration incluse dans l'agent NET/.NET Core permet d'ajouter des attributs personnalisés à vos vertex Team Center à partir de votre environnement d'agent. Vous pouvez ainsi contrôler et remplir automatiquement tous les attributs dans les vertex que l'agent gère au niveau de votre environnement. La carte affiche les vertex, vous permettant ainsi d'identifier le canal de communication entre plusieurs vertex dans votre environnement. Les attributs ajoutés vous permettent d'identifier et d'isoler plus facilement un vertex problématique, et donc de réduire le nombre de problèmes et de les résoudre plus rapidement. **Informations complémentaires** : Automatic Attribute Decoration (agent .NET/.NET Core).

Améliorations apportées à la surveillance du cloud

Les modifications ci-après ont été apportées à la surveillance du cloud :

Google Cloud Monitoring

Surveillance Cloud Bigtable

Google Cloud Bigtable permet de stocker de grandes quantités de données à clé unique avec une faible latence. La surveillance Cloud Bigtable inclut un noeud statique nommé **multi-region** de type **GCP Region** (Région GCP). Ce noeud statique permet de connecter les instances GCP Bigtable aux régions applicables. **Informations complémentaires** : Google Cloud Bigtable.

Surveillance Google Memorystore for Memcached

Le service GCP Memorystore for Memcached est hautement évolutif et entièrement géré pour Google Cloud. Vous pouvez surveiller GCP Memorystore for Memcached à l'aide de mesures de statut, d'attributs et de mesures cloud. Pour cet agent, vous pouvez surveiller le groupe de mesures au niveau du noeud. **Informations complémentaires** : Surveillance Google Memorystore for Memcached.

Amazon Web Services

Surveillance AWS SageMaker

AWS SageMaker permet de former, de créer et d'héberger un modèle sur un terminal disponible. Vous pouvez surveiller les performances de SageMaker à l'aide de l'extension de surveillance AWS. **Informations complémentaires** : AWS SageMaker.

Surveillance AWS Athena

Le service Amazon Athena est un service interactif de requête qui simplifie l'analyse des données dans Amazon S3 à l'aide du code SQL standard. Vous pouvez surveiller les mesures à partir de Cloud Watch et de l'API Service. Vous pouvez également surveiller les mesures dérivées. La surveillance AWS Athena prend en charge les groupes de travail, ce qui permet de séparer les utilisateurs, les équipes, les applications ou les charges de travail. **Informations complémentaires** : Service AWS Athena.

Surveillance AWS Step Functions

AWS Step Functions est un service d'orchestration sans serveur. Il permet de combiner des fonctions AWS Lambda et d'autres services AWS pour créer des applications stratégiques via un flux de travaux visuel. Activez ce service pour afficher les mesures Step Functions. **Informations complémentaires** : AWS Step Functions.

Prise en charge de la détection basée sur des balises AWS Services

Le filtrage basé sur des balises permet de surveiller les instances à l'aide de balises spécifiques uniquement pour les services de surveillance AWS suivants :

- Service de surveillance AWS EC2
- Service AWS Classic Load Balancer (CLB)
- Service AWS Network Load Balancer (NLB)
- Service AWS Application Load Balancer (ALB)
- Service AWS S3
- Service de surveillance AWS EBS
- Service AWS Redshift

Informations complémentaires : Filtrage basé sur les balises dans AWS Inventory.

Améliorations apportées à la surveillance de l'infrastructure

Les modifications ci-après ont été apportées à l'agent Infrastructure.

Surveillance Cassandra

L'extension Surveillance Cassandra est une extension de l'agent Infrastructure qui permet de collecter et d'afficher les mesures de cluster de base de données Apache Cassandra. **Informations complémentaires** : Surveillance Cassandra.

Surveillance Vault

L'extension Surveillance Vault est une extension de l'agent Infrastructure qui permet de surveiller les performances du serveur Vault de différentes bibliothèques et de différents sous-systèmes. Elle collecte diverses mesures, notamment concernant l'exécution, le noyau, l'audit, l'arrière-plan de stockage, le traitement des demandes et le moteur de secrets.

Informations complémentaires : Surveillance Vault.

Prise en charge de l'extension IBM Integration Bus (IIB) 10 Trace

L'extension IIB 10 permet de surveiller les performances des flux de messages IBM Integration Bus, en générant des traces et des mesures de transaction. Vous pouvez utiliser cprobe et userexits, fournis par IIB, pour interagir avec les flux de messages sans modifier l'application existante. **Informations complémentaires** : Extension IBM Integration Bus (IIB) 10 Trace.

Surveillance Cloud Foundry améliorée

L'extension de surveillance Cloud Foundry de l'agent Infrastructure signale de nouvelles mesures afin de mieux gérer les performances de Pivotal Cloud Foundry Platform. Par exemple, elle fournit désormais des mesures Auctioneer et BBS LockHeld, User Account and Authentication (UAA), etc. **Informations complémentaires** : Mesures de surveillance Cloud Foundry.

Surveillance améliorée des hôtes pour Windows

L'extension Surveillance d'hôte de l'agent Infrastructure pour Windows inclut désormais toutes les mesures de performances et d'intégrité de SysEdge. **Informations complémentaires** : Surveillance d'hôte pour Windows.

Automatic Attribute Decoration pour l'agent Infrastructure

L'extension Automatic Attribute Decoration est une extension Infrastructure qui permet d'ajouter des attributs personnalisés à vos vertex Team Center à partir de votre environnement d'agent. Vous pouvez ainsi contrôler et remplir automatiquement tous les attributs dans les vertex que l'agent gère au niveau de votre environnement. La carte affiche les vertex, vous permettant ainsi d'identifier le canal de communication entre plusieurs vertex dans votre environnement. Les attributs ajoutés vous permettent d'identifier et d'isoler plus facilement un vertex problématique, et donc de réduire le nombre de problèmes et de les résoudre plus rapidement. **Informations complémentaires** : Automatic Attribute Decoration pour l'agent Infrastructure.

Prise en charge de l'authentification Windows pour la surveillance des serveurs Web IIS

Vous pouvez maintenant configurer l'agent Surveillance de serveur Web IIS à l'aide de l'authentification Windows. **Informations complémentaires** : Configuration de la surveillance de serveur Web à l'aide de l'authentification Windows.

Configuration de l'accès sécurisé pour la surveillance F5 LTM

L'extension Surveillance F5 LTM de l'agent Infrastructure inclut la nouvelle propriété `introscope.agent.f5.tokenAuth` pour l'exécution de l'authentification basée sur les jetons. **Informations complémentaires** : Configuration de l'extension F5 LTM Monitor.

Accès des utilisateurs non root à l'agent Infrastructure

Les utilisateurs non root peuvent désormais installer, démarrer et arrêter l'agent Infrastructure. Certaines commandes de l'agent Infrastructure ont été modifiées. Le tableau ci-dessous répertorie les commandes précédentes et celles mises à jour :

Commande précédente	Commande mise à jour
<code>force_start</code>	<code>console_start</code>
<code>force_stop</code>	<code>console_stop</code> : cette commande a elle aussi été ajoutée pour l'agent Infrastructure basé sur UNIX.
<code>apmia-ca-installer.sh/apmia-ca-installer.bat</code>	<code>APMIACtrl.sh/APMIACtrl.bat</code>

Fonctionnalités de l'agent UMA

Cette section répertorie les fonctionnalités nouvelles et améliorées de l'agent de surveillance universel.

Extension UMA pour sonde Python

L'agent de surveillance universel pour Kubernetes détecte désormais automatiquement vos applications Python et les instrumente, sans qu'aucune modification manuelle de l'image d'application ne soit nécessaire. **Informations complémentaires** : Extension UMA pour sonde Python.

Extension UMA pour sonde NGINX

L'agent de surveillance universel pour Kubernetes détecte désormais automatiquement vos applications NGINX et les instrumente, sans qu'aucune modification manuelle de l'image d'application ne soit nécessaire. **Informations complémentaires** : Extension UMA pour sonde NGINX.

Zipkin Support

DX APM collecte désormais les données d'étendue concernant les applications suivies par le système de suivi distribué Zipkin. L'extension Zipkin Support signale et affiche les mesures de performances, erreurs et traces de transaction des

applications. Zipkin Support est une extension de l'agent Infrastructure qui fournit des données concernant les serveurs frontaux HTTP, d'arrière-plan HTTP et d'arrière-plan de base de données. **Informations complémentaires** : Zipkin Support.

Fonctionnalités de l'agent Node.js

Cette section répertorie les fonctionnalités nouvelles et améliorées de l'agent Node.js.

Surveillance des performances d'exécution de l'agent Node.js dans les déploiements conteneurisés

Vous pouvez désormais installer l'agent Node.js en tant qu'agent autonome sans Python. **Informations complémentaires** : Installation de l'agent de sonde Node.js pour CA Digital Experience Insights.

Prise en charge de MS SQL pour l'agent Node.js

L'agent Node.js prend désormais en charge les appels provenant de la base de données des versions 2016 et 2017 de Microsoft SQL Server. **Informations complémentaires** : Matrice de prise en charge de l'agent Node.js.

Fonctionnalités de l'agent PHP

DX APM prend désormais en charge la version 7.4 de PHP. **Informations complémentaires** : Matrice de prise en charge de l'agent PHP.

Fonctionnalités de l'interface utilisateur

Cette section présente les fonctionnalités de l'interface utilisateur nouvelles et améliorées.

Améliorations apportées à la création d'univers et à l'intégration

Dans la nouvelle vue **Univers**, les administrateurs peuvent accorder différents droits aux utilisateurs et aux groupes d'utilisateurs. Ces droits incluent l'accès à l'univers et le filtrage des sources de mesures. Le filtrage peut être basé sur les domaines (accès aux agents) avec des attributs et des expressions régulières, des composants de carte et des modules de gestion.

En outre, le comportement des univers a été modifié, ce qui a une incidence sur le filtrage des sources de mesures. En raison de cette modification, vous devez reconfigurer les sources de mesures de l'univers pour que le filtrage d'agent appliqué au navigateur de mesures soit correct. Imaginons, par exemple, que votre environnement inclut dix agents actifs. Avant les améliorations apportées aux univers 20.11, quatre agents étaient répertoriés dans l'univers X et s'affichaient dans le navigateur de mesures. Suite aux modifications apportées à l'univers 20.11, l'univers X contient dix agents qui s'affichent tous dans le navigateur de mesures. Vous devez mettre explicitement à jour les sources de mesures de l'univers pour qu'elles affichent à nouveau quatre agents dans l'univers X et pour que quatre agents s'affichent dans le navigateur de mesures.

Informations complémentaires : Configuration des univers.

Agents déconnectés

Vous pouvez maintenant accéder aux données des agents déconnectés. **Informations complémentaires** : Surveillance des valeurs des mesures d'agent avec la vue des mesures.

Tri des attributs dans la fenêtre Perspective

Vous pouvez maintenant faire glisser des attributs et les déposer dans la fenêtre **Perspective** afin de les trier ou de les réorganiser dans la hiérarchie. L'ordre des attributs définit l'ordre d'application des filtres et par conséquent le groupement des vertex. **Informations complémentaires** : Organisation des composants à l'aide de perspectives.

Couleurs de statut des agents

Les agents déconnectés s'affichent maintenant en gris. **Informations complémentaires** : Surveillance des valeurs des mesures d'agent avec la vue des mesures.

Autres fonctionnalités

Exportation des mesures dans la vue des mesures

Vous pouvez désormais exporter les mesures dans la **Vue des mesures**, par exemple, pour combiner différents types de données et créer des graphiques dans Excel. **Informations complémentaires** : Surveillance des valeurs des mesures d'agent avec la vue des mesures.

Problèmes connus

Cette section répertorie les problèmes connus liés à la version actuelle.

Symptôme : je me connecte à un client hébergé après avoir activé l'hébergement pour SAML dans Chrome. Lorsque je me déconnecte, je suis reconnecté.

Solution : ce problème est dû au maintien du même hébergement. Il s'agit du comportement standard pour les applications pour lesquelles l'authentification unique est activée, telles que DX SaaS, MS Office 365, Box, SharePoint et Google. Pour résoudre ce problème, vous devez effacer le cache lorsque vous vous déconnectez pour l'hébergement.

Défaut DE481045 : impossible de se déconnecter du client hébergé SAML de DX SaaS

Symptôme : je me connecte à un client hébergé après avoir activé l'hébergement pour SAML dans Chrome. Lorsque je me déconnecte, je suis reconnecté.

Solution : ce problème est dû au maintien du même hébergement. Il s'agit du comportement standard pour les applications pour lesquelles l'authentification unique est activée, telles que DX SaaS, MS Office 365, Box, SharePoint et Google. Pour résoudre ce problème, vous devez effacer le cache lorsque vous vous déconnectez pour l'hébergement.

Voici la procédure à suivre pour contourner ce problème :

Démarrez une nouvelle session sans vous déconnecter.

- Ouvrez une fenêtre de navigateur en mode de navigation privée et démarrez une nouvelle session.
- Ouvrez un autre navigateur, tel que FireFox, et démarrez une nouvelle session.

Déconnectez-vous et reconnectez-vous pour démarrer une nouvelle session.

- Déconnectez-vous, puis cliquez sur **Sign in with another Tenant** (Se connecter avec un autre client hébergé) après quelques secondes.
- Déconnectez-vous manuellement d'un client hébergé en supprimant le cookie **CA_CLOUD_Management**. Ensuite, connectez-vous à un autre client hébergé.
- Fermez le navigateur et patientez jusqu'à ce que la session expire. Ensuite, connectez-vous à un autre client hébergé.

Défaut DE481045 : difficulté à basculer entre plusieurs clients hébergés SAML de DX SaaS

Symptôme : je peux accéder à plusieurs clients hébergés SAML. Toutefois, je ne peux pas basculer facilement entre eux.

Solution : ce problème de basculement est dû à un problème de déconnexion de DX SaaS. En effet, DX SaaS ne peut pas se déconnecter de plusieurs clients hébergés utilisés à l'aide du même navigateur. Ce problème survient uniquement avec SAML.

Utilisez les mêmes solutions de contournement que pour le problème précédent.

Défaut DE486199 : comportement incorrect lors de la création d'un univers ou de l'enregistrement du filtre de carte en tant qu'univers

Symptômes :

- Lorsque je crée un univers, les comportements indésirables ci-dessous se produisent dans la page **Créer un univers** :
 - Les noms et les descriptions des champs sont parfois remplis automatiquement avec les données d'un univers existant. Lorsque je clique sur **Enregistrer**, la page est enregistrée avec les options par défaut (voir ci-dessous).
 - Le bouton radio **Modules de gestion** passe de la valeur par défaut **Tous les éléments** à **Éléments sélectionnés** lorsque je remplis les champs **Nom*** et **Description**. Lorsque je clique sur **Enregistrer**, la page est enregistrée avec les options par défaut (voir ci-dessous).
- Lorsque j'enregistre le filtre de carte en tant qu'univers, les comportements indésirables ci-dessous se produisent :
 - Le bouton radio **Module de gestion - Filtre** est placé à côté de **Éléments sélectionnés** et non de **Tous les éléments**. Lorsque je clique sur **Enregistrer**, la page est enregistrée avec les options par défaut (voir ci-dessous).
 - Lorsque j'enregistre le filtre de carte en tant qu'univers, le paramètre **Inclure le noeud d'expérience** n'est pas appliqué à l'univers nouvellement créé.

Voici les options par défaut pour l'enregistrement d'un nouvel univers :

- Lorsque l'univers est créé via un clic sur **Nouvel univers**, l'option **Tous les éléments** est sélectionnée dans chaque onglet.
- Lorsque l'univers est créé via un clic sur **Enregistrer en tant qu'univers** dans la page **Carte**, un filtre est rempli dans l'onglet **Composants de carte**. L'option **Tous les éléments** est sélectionnée dans les autres onglets.

Solution : aucune solution de contournement n'est disponible pour ces problèmes.

20.9

Cet article présente les fonctionnalités nouvelles, modifiées et désapprouvées dans DX APM 20.9.

Améliorations apportées à la surveillance Java

Les modifications ci-après ont été apportées à l'agent Java.

Refonte de la prise en charge du service JMX de l'agent Java

L'extension JMX de l'agent Java améliorée est fournie sous forme de package et déployée en tant que nouvelle extension d'agent qui prend en charge les mesures de micromètre et Spring Boot. Vous pouvez configurer de nouvelles propriétés JMX à l'aide d'APM Command Center ou du fichier `bundle.properties` qui se trouve dans le dossier `extensions/deploy`. L'extension améliorée est prise en charge sous Java 7 et version supérieure. Pour Java 6, continuez à utiliser les propriétés JMX du fichier `IntroscopeAgent.profile`.

Définitions améliorées du groupe d'URL frontales

L'agent Java normalise désormais automatiquement les segments dynamiques des URL en définitions d'URL frontale plus significatives et plus utiles.

Détection automatique du nom de l'application Spring Boot

Vous pouvez maintenant configurer l'extension de l'agent Java Surveillance Spring Boot pour détecter automatiquement le nom de l'application Spring Boot.

L'agent SQL prend en charge Oracle 19.x.

L'agent SQL pour Java prend désormais en charge la surveillance des bases de données Oracle 19.x. **Informations complémentaires** : Configuration de la surveillance SQL pour Java.

Prise en charge de l'agent Java Spring Boot Webflux 2.1.x et 2.2.x

DX APM prend désormais en charge Spring Boot Webflux versions 2.1.x et 2.2.x. **Informations complémentaires :** Surveillance des applications réactives Spring Boot .

Prise en charge de Jetty Framework 8.x

L'agent Java prend désormais en charge Jetty Framework 8.x.

Améliorations apportées à la surveillance de l'agent .NET

Les modifications ci-après ont été apportées à l'agent .NET.

Amélioration de la visibilité approfondie sur les performances des applications .NET Core

DX APM ajoute automatiquement une visibilité approfondie sur les applications .NET Core s'exécutant sous Linux, sans qu'aucune instrumentation personnalisée ou manuelle ne soit nécessaire.

Améliorations apportées à la surveillance du cloud

Les modifications ci-après ont été apportées à la surveillance du cloud :

Google Cloud Platform

Prise en charge du service Google Cloud BigQuery

Le service Google Cloud BigQuery permet de visualiser les performances des requêtes BigQuery. **Informations complémentaires :** Service Google Cloud BigQuery.

- Prise en charge du service Google Dataproc

L'extension de surveillance Google Cloud Platform collecte les mesures pour le service Dataproc. **Informations complémentaires :** Google Dataproc.

- Prise en charge du service Google Cloud Load Balancing

L'extension de surveillance Google Cloud Load Balancing collecte les mesures pour le service d'équilibrage de charge. **Informations complémentaires :** Service Google Cloud Load Balancing.

- Prise en charge du service Google Cloud Autoscaler

Google Cloud Autoscaler permet de gérer l'augmentation du trafic tout en réduisant les coûts lorsque le besoin en ressources diminue. **Informations complémentaires :** Google Cloud Autoscaler.

Amazon Web Services

- Détection automatique basée sur les rôles pour les organisations AWS

Prise en charge de la détection automatique basée sur les rôles pour les organisations Amazon Web Services. **Informations complémentaires :** Configuration de la surveillance des organisations AWS

Amazon Web Services (AWS) prend désormais en charge les services ci-après :

- Prise en charge du service AWS Elastic Map Reduce (EMR)

Le service de surveillance AWS EMR offre la flexibilité nécessaire pour exécuter les cas d'utilisation sur des clusters à usage unique et de courte durée qui évoluent automatiquement pour répondre à la demande ou sur des clusters à disponibilité extrêmement élevée et à exécution à long terme à l'aide du nouveau mode de déploiement multimaître. **Informations complémentaires :** Service de Surveillance AWS EMR.

- Prise en charge du service AWS Glue

Le service AWS Glue détecte vos données et stocke les métadonnées associées (par exemple, la définition et le schéma de table) dans le catalogue de données AWS Glue. **Informations complémentaires** : Service AWS Glue.

Améliorations apportées à la surveillance de l'infrastructure

Les modifications ci-après ont été apportées à l'agent Infrastructure.

Extension de surveillance d'hôte distant

L'extension de surveillance d'hôte distant de l'agent Infrastructure permet de récupérer les données de performances d'un système non doté d'un agent. Elle collecte les données de performances du système en envoyant des commandes de CLI à distance. L'extension collecte les mesures relatives à l'utilisation de l'UC, du disque et de la mémoire et concernant la charge, ainsi que les processus pour lesquels l'utilisation des ressources du système surveillé a connu une augmentation minimale. **Informations complémentaires** : Surveillance d'hôte distant.

Surveillance Logstash

L'extension de surveillance Logstash de l'agent Infrastructure permet de surveiller et de collecter des mesures à partir de divers modules d'extension Logstash. **Informations complémentaires** : Extension de surveillance Logstash.

Prise en charge de NGINX 1.18.X

DX APM prend désormais en charge NGINX version 1.18.0. **Informations complémentaires** : Surveillance NGINX.

Surveillance d'hôte

Prise en charge des principales mesures pour la surveillance d'hôte

Les anciennes mesures d'UC, de disque et de mémoire, de processus et de noyau de réseau SysEdge ont été transférées vers l'extension de surveillance d'hôte de l'agent Infrastructure sous Linux. **Informations complémentaires** : Mesures de surveillance d'hôte.

Surveillance des bases de données

Surveillance des bases de données SAP HANA

L'extension de surveillance des bases de données SAP HANA collecte les mesures qui surveillent l'intégrité et les performances des bases de données SAP HANA. **Informations complémentaires** : Surveillance SAP HANA.

Améliorations apportées à la surveillance Python

Les modifications ci-après ont été apportées à l'agent Python.

Appels asynchrones pris en charge pour l'agent Python

L'agent Python prend désormais en charge tous les cadres Python qui utilisent des modules d'instrumentation asynchrones.

Prise en charge de l'agent Python pour l'infrastructure Rasa et le SDK Rasa

Rasa est une infrastructure open source utilisée principalement pour créer des assistants contextuels, c'est-à-dire des applications de chatbot. L'agent Python prend désormais en charge les applications de surveillance basées sur l'infrastructure Rasa. **Informations complémentaires** : Infrastructure Rasa.

Améliorations apportées à l'agent de surveillance universel

Ajout de la prise en charge de l'agent de surveillance universel pour l'extension Node.js

Vous pouvez connecter les applications de sonde à l'agent Data Collector UMA qui s'exécute conjointement à l'ensemble de démons UMA en configurant la variable d'environnement **COLLECTOR_AGENT_HOST** avec un nom de noeud spécifique. **Informations complémentaires** : Agent de surveillance universel pour l'extension Node.js.

Améliorations apportées aux services middleware, ESB et Web de messagerie

Prise en charge d'Apache Camel

L'extension Apache Camel permet de surveiller toutes les applications qui utilisent Apache Camel comme moteur de routage. Les applications peuvent être déployées sur des applications JBoss Fuse, Tomcat ou Spring Boot. **Informations complémentaires** : Apache Camel.

Améliorations apportées à CA API Gateway Agent

Prise en charge de l'agrégation des mesures de service

L'agrégation des mesures de service s'effectue à plusieurs niveaux pour les services demandés. Vous pouvez afficher les mesures au niveau passerelle, au niveau cluster et au niveau EM pour tous les agents. **Informations complémentaires** : Agrégation des mesures de service dans CA API Gateway Agent.

Améliorations apportées à APM Command Center

Remplacement du langage de requête Lucene

Nous avons remplacé la recherche à l'aide du langage de requête Apache Lucene dans APM Command Center par un langage de requête interne à DX APM.

Problèmes connus

Cette section répertorie les problèmes connus liés à la version actuelle.

Défaut DE479068 : rotation de l'arborescence des mesures

Symptôme : dans la **Vue des mesures**, lorsque vous masquez les agents déconnectés, le graphique de mesures se charge, mais pas l'arborescence des mesures.

Solution : Il n'existe aucune solution à ce problème.

Défaut DE478641 : l'alerte de danger générée par la mesure n'affiche pas d'icône Danger

Symptôme : dans la **Vue des mesures**, l'alerte de danger générée par une mesure ne s'affiche pas sous forme d'icône. Cependant, l'icône d'alerte de danger s'affiche correctement si vous basculez entre deux vues de mesures.

Défaut DE477342 : champs de tri assisté non visibles dans la vue Isolement

Symptôme : lorsqu'un agent possède des attributs personnalisés et qu'une alerte est déclenchée, les champs Tri assisté ne sont pas visibles dans la **Vue Isolement** pour l'alerte.

Solution : Il n'existe aucune solution à ce problème.

Défaut DE477272 : aucuns problèmes ou anomalies affichés dans le panneau de droite de la Vue Expérience

Symptôme : dans la **Vue Expérience**, les problèmes et les anomalies s'affichent dans la fiche d'expérience. Toutefois, lorsqu'un problème ou une anomalie sont sélectionnés, le panneau droit de la **Vue Expérience** n'affiche pas les détails.

Solution : Il n'existe aucune solution à ce problème.

Défaut DE476351 : échec des liens vers la documentation d'installation du package APM Command Center

Symptôme : ce problème survient lorsque vous sélectionnez un package existant dans APM Command Center et que vous cliquez sur le lien **ici** dans les instructions d'installation. Une page techdocs.broadcom.com vide ou le portail Tech Docs s'affiche au lieu de la page de documentation des instructions d'installation prévue.

Solution : accédez directement au [site de documentation de DX APM SaaS](#).

Défaut DE449130 : connexion impossible à l'aide d'un compte SAML

Symptôme : les utilisateurs ne peuvent pas se connecter à l'aide des détails du compte SAML.

Solution : générez un jeton public et connectez-vous à l'aide de celui-ci.

20.6

Cette section indique les fonctionnalités nouvelles, modifiées et désapprouvées dans DX APM 20.6.

Fonctionnalités d'agent

Cette section présente les fonctionnalités d'agent nouvelles et améliorées.

Surveillance RabbitMQ

RabbitMQ est un intermédiaire de messages multiplate-forme, qui offre un moyen d'échanger des données entre différentes applications.

L'extension RabbitMQ surveille les performances des nœuds, les échanges de messages, les files d'attente et les connexions des clusters et des systèmes autonomes dans l'infrastructure RabbitMQ. Dans un cluster RabbitMQ, l'extension détecte automatiquement les nœuds du cluster à surveiller. L'extension établit une corrélation entre l'application et l'infrastructure, ce qui vous permet de déboguer les problèmes causés par le serveur RabbitMQ dans une application. Dans la vue Carte, la couche d'infrastructure affiche le mappage entre le cluster et les nœuds. Nous avons également introduit des GIF animés à des fins d'illustration. Pour plus d'informations, consultez la section Surveillance RabbitMQ.

Prise en charge de Mule ESB 4.x

Mule ESB 4.x vous permet d'identifier les flux de communication et leur corrélation dans toutes les communications, y compris dans les communications asynchrones. Vous pouvez également identifier les composants de modélisation propres à Mule ESB. La carte affiche une nouvelle icône Mule au niveau des vertex Mule. Nous avons également introduit des GIF animés à des fins d'illustration. Pour plus d'informations sur Mule ESB 4.x, reportez-vous à la section Mule ESB 4.x.

Surveillance PostgreSQL

La solution de surveillance PostgreSQL pour DX APM vous permet de surveiller les performances et la disponibilité de votre environnement de base de données PostgreSQL. Vous pouvez configurer et utiliser cette extension d'agent Infrastructure pour collecter les mesures de performances liées au serveur PostgreSQL : Utilisation des ressources, Transactions, Débit, Interblocages, etc. L'extension PostgreSQL permet également aux utilisateurs de corréler les performances de l'application avec celles de la base de données PostgreSQL utilisée comme base de données d'arrière-plan. Pour plus d'informations, consultez la section Surveillance PostgreSQL.

Prise en charge de la corrélation du moniteur d'infrastructure WebLogic

L'extension de surveillance de l'infrastructure WebLogic prend désormais en charge la corrélation application-infrastructure. Pour plus d'informations, reportez-vous à la section Attributs de surveillance de l'infrastructure WebLogic.

Mesures de surveillance vCenter

La surveillance vCenter pour DX APM fournit désormais des mesures pour les entités suivantes dans votre environnement vCenter : vCenter, centre de données, cluster, référentiel de données, pools de ressources, cartes NIC virtuelles et physiques, commutateurs virtuels, disques, détecteurs, ESX et VM. Pour plus d'informations, reportez-vous à la section Surveillance vCenter.

Prise en charge d'autres services par la surveillance AWS

La solution de surveillance AWS (Amazon Web Services) pour DX APM prend désormais en charge les nouveaux types de services suivants : Elastic Load Balancing, ElastiCache, Auto Scaling, Kinesis Data Streams, Billing, API Gateway, CloudTrail, Functions, Logic App, Redshift, Cloudwatch Logs, Cloudfront, Cloudwatch Events et Fargate. DX APM fournit la prise en charge de la surveillance basée sur les rôles AWS pour l'ID externe, ce qui empêche toute attaque Confused Deputy dans votre environnement AWS. Pour plus d'informations, voir la section Surveillance Amazon Web Services.

Prise en charge de .NET Core par l'agent de surveillance universel

L'agent de surveillance universel (UMA, Universal Monitoring Agent) pour Kubernetes détecte désormais automatiquement vos applications .NET Core et les instrumente, sans qu'aucune modification manuelle de l'image d'application ne soit nécessaire. L'agent UMA prend en charge la version 3.1 de NET Core et les versions ultérieures.

Prise en charge de l'agent de navigateur .NET Core

Vous pouvez désormais configurer l'injection automatique de snippets de l'agent de navigateur pour l'agent .NET Core. Pour plus d'informations, consultez la section Configuration de l'agent de navigateur pour .NET.

Affichage des données de l'agent UMA pour Kubernetes dans l'arborescence des mesures et dans la carte

L'agent UMA pour Kubernetes dispose de détails supplémentaires sur les données de topologie, d'attributs et de mesures que vous pouvez afficher dans l'arborescence des mesures et dans la carte.

Collecte et affichage des données du composant d'arrière-plan OpenTracing Jaeger par DX APM

DX APM collecte désormais les traces à partir du composant d'arrière-plan OpenTracing Jaeger et signale les données sous forme de mesures DX APM et de traces de transaction.

Utilisation d'annotations pour remplacer les configurations AutoAttach de l'agent UMA

Vous pouvez désormais utiliser des annotations pour remplacer les configurations AutoAttach de l'agent UMA. Voici quelques exemples :

- Vous pouvez remplacer les vérifications de filtre de l'extension AutoAttach pour la mémoire et les machines virtuelles Java.
- Vous pouvez utiliser une annotation pour transférer n'importe quelle configuration de l'agent Java, par exemple pour ajouter des propriétés.
- Si vous souhaitez activer l'agent de navigateur par espace de noms, ajoutez une annotation appropriée. L'extension AutoAttach utilise la nouvelle annotation en tant que configuration et transfère les propriétés pour activer l'agent de navigateur sans redémarrage ni redéploiement.

Fourniture d'une corrélation par l'agent OpenTracing

L'extension d'agent OpenTracing pour l'agent Infrastructure effectue désormais des corrélations dans les étendues Jaeger et les traces de transaction DX APM.

Utilisation de la communication WebSocket par l'agent .NET/.NET Core

L'agent .NET /.NET Core est configuré pour envoyer automatiquement des informations à l'aide du protocole WebSocket. Ce protocole combine efficacité de la communication de socket binaire et compatibilité des proxys et pare-feux de réseau HTTP. Toutes les versions de .NET Core prises en charge, ainsi que .NET Framework 4.5 et versions ultérieures, prennent en charge les communications WebSocket.

Création d'attributs et de noms d'applications .NET/.NET Core personnalisés

Vous pouvez désormais configurer les propriétés `IntroscopeAgent.profile` pour .NET/.NET Core pour afficher les informations suivantes :

- Attributs personnalisés dans l'onglet **Agent** de la carte **Vue de composant**
- Noms d'application personnalisés dans l'onglet **Composant frontal générique** de la carte **Vue de composant**
- Noms d'application personnalisés répertoriés dans le volet **Détails du composant** de l'outil de suivi de transaction

Prise en charge du système d'exploitation Alpine par l'agent .NET Core

L'agent .NET Core peut désormais surveiller les performances de vos applications exécutées sous le système d'exploitation Alpine Linux.

Fonctionnalités de l'interface utilisateur

Cette section présente les fonctionnalités de l'interface utilisateur nouvelles et améliorées.

Expressions de recherche

A mesure que vous saisissez une expression de recherche, vous pouvez en sélectionner une précédemment saisie et qui apparaît dans la liste déroulante de saisie semi-automatique. Pour plus d'informations, reportez-vous à la section Recherche de mesures dans l'arborescence de mesures.

Affichage des agents déconnectés dans la chronologie

Les agents déconnectés apparaissent en gris dans la chronologie.

Tableaux de bord DX App Synthetic Monitor

Les nouveaux tableaux de bord DX App Synthetic Monitor (ASM) prêts à l'emploi fournissent une vue d'ensemble des performances de votre environnement Web. Vous pouvez définir plusieurs moniteurs dans DX ASM pour mesurer les performances de page. Ces tableaux de bord sont désormais disponibles dans DX SaaS :

- **Key Metrics From All Monitor** (Mesures clés de tous les moniteurs) : ce tableau de bord affiche les mesures clés collectées par tous les moniteurs.
- **Key Metrics For Single Monitor** (Mesures clés d'un seul moniteur) : ce tableau de bord affiche les mesures clés collectées par un seul moniteur.

Pour plus d'informations sur les tableaux de bord prêts à l'emploi, reportez-vous à la section Tableaux de bord DX.

Autres fonctionnalités et améliorations

Cette section présente les autres fonctionnalités améliorées.

Améliorations apportées au référentiel de topologies

En tant qu'administrateur, vous pouvez désormais créer des partitions de référentiel de topologies et rééquilibrer les clients hébergés dans les instances de référentiel de topologies.

Problèmes connus

Cette section répertorie les problèmes connus liés à la version actuelle.

Défaut DE466013 : alerte APM - sélection du déclenchement de notifications d'alerte ignorée

Applicable à DX APM SaaS 20.6

Symptôme : ce problème survient après la sélection d'une notification à déclencher lorsque vous créez une alerte. DX APM n'applique pas correctement le déclencheur lorsque le niveau d'alerte change. Par exemple, vous créez une alerte et sélectionnez l'option à notifier **En cas d'augmentation de la sévérité**.

Lorsque la sévérité d'alerte passe de **Critique** à **Majeur**, puis à **OK**, DX APM ne doit pas envoyer de notification d'alerte par courriel. Toutefois, le canal de notification est déclenché, ce qui entraîne l'envoi indu d'une notification par courriel lorsque la sévérité de l'alerte est réduite.

Solution : Il n'existe aucune solution à ce problème.

Défaut DE449130 - connexion impossible à l'aide d'un compte SAML

Applicable à DX APM 20.1, 20.4, 20.6

Symptôme : les utilisateurs ne peuvent pas se connecter à l'aide des détails du compte SAML.

Solution : générez un jeton public et connectez-vous à l'aide de celui-ci.

DE467134 - onglet Affected Metric (Mesure affectée) de DX Operational Intelligence manquant dans la page Analyse des alarmes

Applicable à DX APM 20.6, CA APM 10.7x

Symptôme : ce problème survient lorsque CA APM 10.7x sur site est configuré pour envoyer des alarmes à DX Operational Intelligence SaaS. Vous pouvez afficher les alertes CA 10.7x sur site sur la page **Analyse des alarmes** de DX Operational Intelligence SaaS. Toutefois, l'onglet **Affected Metric** (Mesure affectée) est manquant pour toutes les alertes CA 10.7x sur site. Ce problème ne survient pas lorsque DX APM SaaS envoie des alertes.

Solution : sélectionnez des mesures dans la page **Performance Analytics** (Analyse des performances).

20.4

Cet article présente les fonctionnalités nouvelles, modifiées et désapprouvées dans DX APM 20.4.

Fonctionnalités d'agent

Cette section présente les fonctionnalités d'agent nouvelles et améliorées.

Surveillance Undertow

Vous pouvez désormais utiliser l'extension de surveillance Undertow pour DX APM pour surveiller les performances des applications qui implémentent des gestionnaires HTTP Undertow. Activez cette extension d'agent Java lorsque vous utilisez Undertow et que DX APM n'affiche aucun composant frontal Undertow.

Lorsque vos applications utilisent l'API Servlet, il n'est pas nécessaire d'utiliser la surveillance Undertow, même si vous disposez d'un serveur Undertow sous-jacent. L'extension n'est pas requise dans ce cas, car l'agent Java effectue le suivi des servlets par défaut.

Pour déployer la solution de surveillance Undertow, incluez le groupe **Undertow (Non-Servlets)** lors de la création ou de la modification d'un package dans APM Command Center.

Surveillance Service Mesh d'Istio

DX APM effectue désormais une surveillance de pile complète des déploiements Service Mesh d'Istio. La surveillance Service Mesh d'Istio fournit les informations et fonctionnalités suivantes :

- Données d'intégrité et de performances relatives aux composants Control Plane d'Istio, tels que Mixer, Pilot et Gateway
- Données de performances relatives au composant Data Plane comprenant le proxy Envoy
- Données d'intégrité et de performances relatives aux services
- Détection automatique de la topologie Service Mesh, y compris les performances en termes d'intercommunication entre les microservices et l'infrastructure du conteneur

Surveillance etcd

Vous pouvez désormais surveiller les performances de votre déploiement etcd. DX APM utilise l'agent de surveillance universel configuré pour importer les données Prometheus et signaler les mesures etcd relatives à l'intégrité de votre cluster Kubernetes ou OpenShift.

Amélioration apportée à la surveillance Kubernetes et OpenShift

La génération de rapports sur les performances de la topologie Kubernetes a été améliorée dans DX APM. La carte inclut désormais des nœuds pour les composants Kubernetes, y compris les clusters et les espaces de noms. Les solutions de surveillance Kubernetes et OpenShift incluent désormais des mesures vous permettant de mieux évaluer la capacité de votre cluster. Ces nouvelles mesures vous permettent de déterminer si le cluster Kubernetes et les différents espaces de noms et projets sont sous- ou surprovisionnés.

Surveillance MongoDB

La solution de surveillance MongoDB pour DX APM vous permet de surveiller les performances et la disponibilité de votre environnement MongoDB. L'extension MongoDB de l'agent Infrastructure fournit une visibilité en temps réel des ressources de base de données et vous permet de corréler les mesures de performances de l'application, de l'infrastructure et de la base de données dans une interface unifiée.

Surveillance Google Cloud Platform

La solution de surveillance Google Cloud Platform (GCP) pour DX APM surveille à distance l'intégrité et les performances des services et de l'infrastructure GCP. La solution de surveillance GCP est une extension d'agent Infrastructure qui utilise les API Google StackDriver pour se connecter et détecter les ressources GCP à surveiller. La solution de surveillance GCP prend en charge les services GCP suivants : Google Compute Engine, Google Cloud Storage, Google Cloud SQL et Google Cloud Filestore. Pour plus d'informations, reportez-vous à la section Surveillance Google Cloud Platform.

Service AWS CloudTrail

Le service Amazon Web Services (AWS) CloudTrail pour DX APM vous permet d'effectuer la mise en conformité, la gouvernance, un audit opérationnel et un audit des risques de votre compte AWS. Vous pouvez effectuer la mise en conformité de votre compte AWS en fonction de l'autorité réglementaire interne de votre organisation ou d'une autorité réglementaire tierce. Pour plus d'informations, voir la section Surveillance Amazon Web Services.

Surveillance AWS

La solution de surveillance AWS pour DX APM prend désormais en charge les nouveaux types de services suivants : Elastic Load Balancing, ElastiCache, Auto Scaling, Kinesis Data Streams, Billing, API Gateway, CloudTrail, Functions, Logic App, Redshift et Fargate. Pour plus d'informations, voir la section Surveillance Amazon Web Services.

Surveillance Azure

La surveillance Azure pour DX APM prend désormais en charge les nouveaux types de service suivants : Azure Kubernetes Service, Cost Management, Load Balancer, Azure SQL, Azure Cosmo DB, Event Hub et Service Bus. Pour plus d'informations, reportez-vous à la section Surveillance Azure.

Surveillance de base de données SQL Server

La solution de surveillance de base de données SQL Server pour DX APM vous permet de surveiller les performances et la disponibilité de votre environnement de base de données SQL Server. Vous pouvez configurer et utiliser cette extension d'agent Infrastructure pour collecter les mesures de performances de votre serveur SQL Server liées aux connexions, au gestionnaire de tampons, aux statistiques d'index, etc. La solution de surveillance SQL Server fournit également des mesures de cluster. Pour plus d'informations, voir la section Surveillance de base de données SQL Server.

Surveillance Redis

La solution de surveillance Redis pour DX APM peut surveiller une seule instance d'un serveur Redis et plusieurs clusters.

Les deux principaux composants d'un cluster Redis sont les nœuds maître et esclave. Toutes les données écrites sur le nœud maître sont également enregistrées sur le nœud esclave. L'extension de surveillance Redis d'agent Infrastructure surveille les nœuds maître et esclave. Lorsqu'un nœud esclave est promu nœud maître, la solution de surveillance Redis détecte les modifications et les reflète dans l'interface utilisateur. Pour plus d'informations, reportez-vous à la section Extension de la surveillance Redis.

Extension de surveillance ForgeRock

L'extension d'agent Java ForgeRock pour DX APM est disponible pour tous les agents Java. L'extension surveille ForgeRock Identity Platform, qui comprend des composants de gestion des accès et des passerelles d'identité. Pour plus d'informations, reportez-vous à la section Extension de la surveillance ForgeRock.

Surveillance GraphQL

DX APM surveille désormais les performances de GraphQL version 14.x et versions supérieures sur Node.js. Vous pouvez afficher les mesures en fonction des itinéraires de l'infrastructure GraphQL de Node.js et des informations associées.

Amélioration du mécanisme de connexion entre la surveillance IBM WebSphere MQ et le serveur MQ

DX APM inclut désormais une connexion en mode Liaisons entre l'extension de surveillance IBM WebSphere MQ d'agent Infrastructure et le serveur MQ résidant sur le même ordinateur. Dans ce mode, DX APM ne requiert aucun détail sur l'hôte, le port ni le canal pour établir une connexion avec le serveur MQ. Pour plus d'informations, reportez-vous à la section Configuration de la connexion en mode Liaisons.

Dans DX APM, le processus d'authentification des utilisateurs a également été amélioré pour connecter la surveillance IBM WebSphere MQ et le serveur MQ en mode client-serveur. Vous pouvez désormais exécuter le script `RunMQCommands` et fournir les détails d'authentification ; ainsi, tous les utilisateurs de l'agent Infrastructure pourront accéder au serveur MQ. Pour plus d'informations, reportez-vous à la section Configuration de la connexion client-serveur.

Prise en charge d'Amazon Linux

L'agent Infrastructure est désormais pris en charge sur les versions Amazon Linux suivantes :

- Amazon Linux 2 AMI
- Amazon Linux AMI

Surveillance de l'infrastructure WebLogic

La solution de surveillance de l'infrastructure WebLogic pour DX APM fournit des fonctionnalités de surveillance JMX pour le serveur WebLogic, y compris tous les nœuds de cluster. Pour plus d'informations, reportez-vous à la section Surveillance de l'infrastructure WebLogic.

Business Payload Analyzer

Lorsque vous téléchargez l'outil BT Listener, les propriétés suivantes sont automatiquement configurées :

- **btListener.output.channel.tenantId** : cette propriété est configurée avec l'ID de client hébergé.
- **btListener.output.channel.url** : cette propriété est configurée avec l'URL DXC.

Echantillonnage aléatoire dynamique

DX APM fournit désormais une étape d'échantillonnage intelligent complet. Vous pouvez configurer l'agent Java pour effectuer une collecte dynamique des traces de transaction aléatoires au cours d'une période donnée et intercepter différents types de transactions. Vous pouvez configurer l'agent Java pour collecter les N premières traces de transaction au cours d'une période donnée et/ou un nombre spécifique de traces de transaction aléatoires pendant une période donnée.

Prise en charge de .NET Core 3.1

L'agent .NET Core collecte désormais des données sur les applications .NET Core 3.1. Pour plus d'informations, reportez-vous aux sections Agent .NET/.NET Core et Microsoft .NET Core.

Fonctionnalités de l'interface utilisateur

Cette section présente les fonctionnalités de l'interface utilisateur nouvelles et améliorées.

Tableaux de bord de base de données Oracle pour DX APM

Vous pouvez afficher plusieurs tableaux de bord liés aux performances de la base de données Oracle. Les tableaux de bord Oracle affichent des mesures relatives aux performances de la base de données et à d'autres activités utilisateur qui vous permettent de résoudre les problèmes connexes. Pour plus d'informations, reportez-vous à la section Tableaux de bord de base de données Oracle pour .

Rôle d'utilisateur avancé dans Team Center

Nous avons introduit un rôle d'utilisateur avancé pouvant effectuer des opérations CRUD (créer, lire, mettre à jour, supprimer) sur les alertes, les modules de gestion, les outils de calcul et les groupes de mesures. Pour plus d'informations, reportez-vous à la section Modification d'autorisations, d'application de domaine et d'éléments.

Affichage des mesures à partir d'agents déconnectés

Déplacer la chronologie vers un intervalle de temps écoulé et afficher un agent connecté à cette période vous permet d'obtenir les mesures correspondantes dans la vue contextuelle de carte.

Importation d'agents existants dans APM Command Center

Vous pouvez désormais importer un agent existant à partir de CA APM 10.7 dans APM Command Center à l'aide de l'utilitaire de l'outil d'importation d'agent. Pour plus d'informations, reportez-vous à la section Outil d'importation d'agent.

Colonnes définies par l'utilisateur dans les résultats de recherche de mesures

Vous pouvez désormais afficher ou masquer des colonnes pour personnaliser les résultats de recherche de mesures. Pour plus d'informations, reportez-vous à la section Recherche de mesures dans l'arborescence de mesures.

Modification d'événements en mode dynamique

Le mode **dynamique** de la chronologie vous permet désormais d'afficher des événements de modification liés au statut, à la topologie et aux attributs d'un nœud. Pour plus d'informations, reportez-vous à la section Utilisation de la chronologie et affichage des événements de modification.

Prise en charge du proxy pour les contrôleurs d'agent

En tant qu'administrateur, vous pouvez définir les détails du proxy lors de la configuration du groupe de contrôleurs d'agent dans APM Command Center. Pour configurer le proxy, activez et définissez les propriétés suivantes dans la page de configuration de contrôleur d'agent :

- `com.ca.apm.acc.controller.configurationServer.proxy.host`
- `com.ca.apm.acc.controller.configurationServer.proxy.port`
- `com.ca.apm.acc.controller.configurationServer.proxy.user.name`
- `com.ca.apm.acc.controller.configurationServer.proxy.password`

NOTE

Si vous ne définissez aucune valeur pour ces paramètres, la valeur `agentManager.httpProxy.username` du groupe em-connection est utilisée.

Pour plus d'informations sur la configuration des propriétés de groupe, reportez-vous à la section Configuration des propriétés de groupe et instructions d'installation dans APM Command Center.

Intégrations

Cette section présente les intégrations de produits nouvelles et améliorées.

Intégration du moniteur DX App Synthetic Monitor et de DX APM

Vous pouvez désormais configurer l'intégration du moniteur DX App Synthetic Monitor (ASM) avec DX APM dans APM Command Center. L'intégration s'exécute avec l'agent Infrastructure. Pour plus d'informations, reportez-vous à la section Configuration du moniteur DX App Synthetic Monitor pour DX APM.

Avant d'utiliser les améliorations, configurez les paramètres suivants :

- `asm.metrics.logs=true` (pour les étapes JMeter et WebDriver)
- `asm.metrics.download.full=true` (pour les étapes JMeter et WebDriver)
- `asm.metrics.har.requests=true` (pour les étapes WebDriver uniquement)

Vous pouvez également utiliser les améliorations suivantes :

- **Affichage détaillé des étapes JMeter**
Lorsque Script Monitor exécute le script JMeter, vous pouvez désormais afficher les résultats des étapes JMeter dans la vue des mesures. Pour afficher les résultats d'étapes JMeter, définissez la valeur `asm.reportJTLSubtree` sur `true`.
- **Affichage détaillé des étapes WebDriver**
Lorsque Script Monitor exécute le script WebDriver, vous pouvez désormais afficher les résultats des étapes WebDriver dans la vue des mesures. Pour afficher les résultats d'étapes WebDriver, définissez la valeur `asm.metrics.har.wdm` sur `true`.
- **Mesure de dernière vérification de résultat**
La nouvelle mesure de **dernière vérification de résultat** affiche le dernier statut de la vérification du moniteur. La mesure affiche les états suivants :
 - 0 : Aucune erreur
 - 1 : Erreur
 - 2 : Mode de maintenance

Autres fonctionnalités

Cette section présente les autres fonctionnalités améliorées.

Améliorations apportées au système d'automatisation des tests (TAS)

Vous pouvez utiliser les améliorations apportées au système TAS suivantes :

- **API TAS v2** : vous pouvez désormais exécuter des commandes pour supprimer une partie du référentiel de topologie de façon synchrone ou asynchrone.
- **Authentification utilisateur activée pour les systèmes TAS/NASS** : l'utilisateur connecté à l'aide de droits d'administrateur de clients hébergés ou principal est autorisé à appeler les terminaux TAS/NASS (référentiel de mesures).

Problèmes connus

Cette section répertorie tous les problèmes connus liés à la version actuelle.

Défaut DE459955 : problème lié au nom de la base de données RDS d'Amazon Web Services

Applicable à DX APM SaaS 20.4

Symptôme : un problème DX APM survient lorsque vous n'affectez aucun nom à une base de données lors de la création de l'instance AWS RDS. Ce problème entraîne le dysfonctionnement de la corrélation de la couche applicative avec la couche d'infrastructure pour l'instance de cette base de données dans l'agent Infrastructure.

Solution : il n'existe aucune solution à ce problème.

Défaut DE457462 : lien de configuration de l'agent PHP inactif dans la boîte de dialogue de téléchargement d'agent

Applicable à DX APM SaaS 20.4

Symptôme : dans la page de la boîte de dialogue de téléchargement d'agent Infrastructure pour DX APM, le lien fourni pour accéder aux détails de configuration complète de l'agent PHP est inactif et affiche l'erreur 404.

Solution : Il n'existe aucune solution à ce problème.

Défaut DE457423 : instructions incorrectes dans la boîte de dialogue de téléchargement d'agent pour la surveillance WebLogic de l'agent Infrastructure

Applicable à DX APM SaaS 20.4

Symptôme : dans la page de la boîte de dialogue de téléchargement d'agent Infrastructure, la page d'instructions d'installation du moniteur WebLogic présente une erreur de contenu. Dans la section **DX APM WebLogic Infra Monitor**, les instructions de copie des fichiers .jar sont incorrectes.

Solution : suivez les instructions ci-après pour copier correctement les fichiers .jar.

Procédez comme suit :

1. Accédez au répertoire `<répertoire_base_WL>/lib`.
Répertoire_WL est le répertoire d'installation du serveur WebLogic.
2. Copiez le fichier `wlthint3client.jar`.
3. Collez le fichier `wlthint3client.jar` dans le répertoire `<répertoire_base_APMIA>/lib`.

Défaut DE456625 : perte des modifications apportées au fichier config.json après l'installation de la sonde Node.js

Applicable à DX APM SaaS 20.4, sonde Node.js version 1.10.83

Symptôme : après l'installation de la dernière sonde de l'application Node.js, toutes les modifications que vous avez apportées au fichier `config.json` sont perdues.

Solution : avant d'installer la dernière sonde de l'application Node.js, effectuez les tâches suivantes.

Procédez comme suit :

1. Recherchez le fichier `config.json` à l'emplacement suivant sur le système sur lequel vous avez installé l'application Node.js :

```
<Node.js_Installation_Folder>\node-modules\ca-apm-probe\
```

2. Sauvegardez le fichier `config.json`.
3. Pour installer la dernière sonde Node.js, exécutez la commande suivante sur le système sur lequel vous avez installé l'application Node.js :

```
npm i ca-apm-probe
```
4. Accédez à l'emplacement suivant sur le système sur lequel vous avez installé l'application Node.js :

```
<Node.js_Installation_Folder>\node-modules\ca-apm-probe\
```
5. Entrez les nouvelles propriétés du dernier fichier `config.json` dans le fichier `config.json` de sauvegarde (**étape 2**).
6. Démarrez l'application Node.js.

Défaut DE456154 : problème lors de la corrélation des composants d'arrière-plan avec les composants frontaux de l'application Node.js

Applicable à DX APM SaaS 20.4, sonde Node.js version 1.10.83

Symptôme : lorsque des composants frontaux de l'application Node.js appellent de façon asynchrone plusieurs composants d'arrière-plan, la corrélation ne fonctionne pas dans la vue des mesures ni dans la carte. Toutefois, la corrélation de composants d'arrière-plan et frontaux fonctionne correctement dans les traces de transaction.

Solution : il n'existe aucune solution à ce problème.

Défaut DE456144 : échec du chargement des valeurs de la configuration d'Attribute Decoration lors du démarrage de Node.js

Applicable à DX APM SaaS 20.4, sonde Node.js version 1.10.83

Symptôme : lorsque vous démarrez l'application Node.js, les valeurs de la configuration dans le fichier `config.json` pour l'extension Automatic Attribute Decoration à partir de Node.js ne sont pas chargées dans la sonde Node.js.

Solution : effectuez les tâches suivantes pour charger les valeurs de configuration d'Automatic Attribute Decoration.

Procédez comme suit :

1. Assurez-vous que l'agent Infrastructure est installé.
2. Installez NodeJS `ca-apm-probe` et démarrez l'application Node.js avec la sonde NodeJS.
3. Assurez-vous de configurer la clé d'API publique dans le fichier `introscopeAgent.profile` de l'agent Infrastructure. Pour effectuer la configuration, ouvrez le fichier `introscopeAgent.profile` et mettez à jour la propriété suivante en accédant à l'emplacement du dossier `\apmia\core\config\` :

```
attribute.decoration.apm.access.token
```
4. Ouvrez le fichier `config.json` en accédant à l'emplacement suivant sur le système sur lequel vous avez installé l'application Node.js et la sonde NodeJS `ca-apm-probe` :

```
<Node.js_Installation_Folder>\node-modules\ca-apm-probe\
```
5. Mettez à jour le fichier `config.json`.

NOTE

Remarque : Veillez à apporter quelques modifications au fichier `config.json` ; par exemple, insérez un espace.

6. Enregistrez le fichier `config.json`.

Défaut DE454550 : affichage du nœud d'arrière-plan MongoDB comme composant d'arrière-plan générique dans la carte

Applicable à DX APM SaaS 20.4, MongoDB 2.x, Node.js

Symptôme : le nœud d'arrière-plan MongoDB doit s'afficher en tant que base de données inférée avec l'application Node.js dans la carte. Toutefois, le nœud d'arrière-plan MongoDB s'affiche en tant que composant d'arrière-plan générique.

Solution : Il n'existe aucune solution à ce problème.

Défaut DE450621 : problème lié à la commande Python Django Run

Applicable à DX APM 20.4, Python 3.x

Symptôme : la commande `run` suivante ne fonctionne pas sur le système sur lequel vous avez installé l'application Python Django :

```
ca-apm-runpy python manage.py runserver
```

Solution : utilisez la commande `run` suivante sur le système sur lequel vous avez installé l'application Python Django :

```
ca-apm-runpy gunicorn -w 2 -b :8000 <project-name>.wsgi
```

Défaut DE450599 : affichage d'un agent Python Django inconnu dans la vue des mesures

Applicable à DX APM 20.4, Python 3.x

Symptôme : lorsque vous démarrez l'agent Infrastructure de DX APM, un agent inconnu s'affiche dans la vue des mesures.

Solution : Il n'existe aucune solution à ce problème.

Défaut DE450618 : problème d'affichage des mesures d'URL Python Django

Applicable à DX APM 20.4, Python 3.x

Symptôme : lorsque vous connectez l'application Python Django à l'agent Infrastructure et parcourez l'application Python Django, chaque mesure d'URL (terminal) de l'application Python Django s'affiche en double dans la vue des mesures.

Solution : il n'existe aucune solution à ce problème.

Défaut DE449130 - connexion impossible à l'aide d'un compte SAML

Applicable à DX APM 20.1, 20.4

Symptôme : l'utilisateur ne parvient pas à se connecter à l'aide des détails du compte SAML.

Solution : générez un jeton public et connectez-vous à l'aide de celui-ci.

Défaut DE438579 : dysfonctionnement de la corrélation du moniteur d'hôte avec le nœud d'intégration IIB

Applicable à DX APM SaaS 20.4

Symptôme : la corrélation du moniteur d'hôtes avec le nœud d'intégration IBM Integration Bus (IIB) échoue lorsque la fonctionnalité de surveillance d'hôtes d'infrastructure IIB est activée.

Solution : il n'existe aucune solution à ce problème.

Défaut DE405769 : dysfonctionnement de la corrélation de Mule ESB 3.x avec le proxy

Applicable à DX APM SaaS 20.4, Mule ESB 3.x

Symptôme : la corrélation de l'application Mule ESB 3.x avec le proxy est utilisée par une application imbriquée. La corrélation ne fonctionne pas dans la carte ni dans les traces de transaction.

Solution : Il n'existe aucune solution à ce problème.

20.1

Cette section indique les fonctionnalités nouvelles, modifiées et désapprouvées dans DX APM 20.1.

Fonctionnalités d'agent

Module d'extension du serveur Web Nginx

Business Payload Analyzer comprend désormais un plugin pour le serveurs Web Nginx. Pour plus d'informations sur l'installation et la configuration, voir la section Installation et configuration du module d'extension pour serveur Web Nginx.

Vous pouvez désormais déployer l'agent de surveillance universel pour la fonctionnalité Kubernetes à l'aide d'un opérateur de service Kubernetes.

Utilisation de l'opérateur de service Kubernetes pour le déploiement de l'agent de surveillance universel pour Kubernetes

Vous pouvez désormais déployer l'agent de surveillance universel pour la fonctionnalité Kubernetes à l'aide d'un opérateur de service Kubernetes.

OpenTracing Support

DX APM propose désormais la prise en charge de la surveillance pour les applications OpenTracing. La prise en charge d'OpenTracing permet de signaler les mesures de performances des applications et les traces de transactions collectées à partir d'applications que vous instrumentez à l'aide de Jaeger. DX APM fournit la prise en charge OpenTracing en tant qu'extension de l'agent Infrastructure. Pour plus d'informations, voir la section Prise en charge OpenTracing.

Installation de l'agent Infrastructure sur AIX

Vous pouvez maintenant télécharger et installer l'agent Infrastructure sur la plate-forme AIX. Pour plus d'informations, voir la section Installation de l'agent Infrastructure sur DX APM.

Prise en charge Python 3.x

L'agent python prend désormais en charge python 3.x ainsi que la corrélation entrante et sortante. Vous pouvez désormais afficher la corrélation des flux entrants dans l'application Python avec les flux sortants de l'application Python.

Corrélation prise en charge

- **Corrélation entrante** : s'il existe un appel à partir du flux entrant (Java ou python) vers l'application Python, les agents respectifs instrumentent les deux flux.
- **Corrélation sortante** : s'il existe un appel de l'application Python à l'aval (Java ou python), les agents respectifs instrumentent les deux flux.

Corrélation sortante à l'aide du module de demande

Le module **Demande** est la norme pour la réalisation de requêtes HTTP dans Python. Si une application python invoque le module de demande dans la sonde Python, la sonde est notifiée et les traces correspondantes sont affichées.

Corrélation sortante à l'aide du module Urllib

Urllib.request est le module permettant d'extraire des URL (Uniform Resource Locator) dans Python. Le module urllib.request définit les fonctions et les classes qui aident à ouvrir les URL (principalement HTTP) dans Python. Si une application python invoque ce module dans la sonde Python, la sonde est notifiée et les traces correspondantes sont affichées.

Prise en charge des applications Python dans les conteneurs du Docker

Vous pouvez dorénavant utiliser l'agent Python pour surveiller les applications Django Framework et Flask Framework Python.

Service AWS CloudTrail

L'AWS CloudTrail pour vous permet d'effectuer la mise en conformité, la gouvernance, un audit opérationnel et un audit des risques de votre compte AWS. Vous pouvez effectuer la mise en conformité de votre compte AWS de deux manières. Conformité basée sur l'autorité réglementaire interne de votre organisation ou d'une autorité réglementaire tierce.

IIB Infra Monitoring

Vous pouvez utiliser la surveillance IBM Integration Bus (IIB) pour surveiller l'intégrité et la disponibilité de IIB et les flux de messages correspondants. Comme condition préalable, vous devez utiliser l'un des composants suivants : MQTT, qui est

intégré à IIB ou à IBM MQ. L'extension de surveillance IIB se connecte à l'un des composants pour collecter les mesures de statistiques IIB. Pour plus d'informations, voir la section Surveillance IIB.

Surveillance de base de données SQL Server

La solution de surveillance de base de données SQL Server pour vous permet de surveiller les performances et la disponibilité de votre environnement de base de données SQL Server. Vous pouvez configurer et utiliser cette extension pour collecter les mesures de performances de votre serveur SQL Server liées aux connexions, au gestionnaire de tampons, aux statistiques d'index, etc. Pour plus d'informations, voir la section Surveillance de base de données SQL Server.

Surveillance des bases de données MySQL

L'extension de surveillance de base de données MySQL vous permet de surveiller les performances et la disponibilité de votre environnement de base de données MySQL. Cette extension offre une visibilité en temps réel sur les ressources de base de données critiques. Ces ressources incluent les octets envoyés et reçus, les tentatives, les interruptions ou les échecs de connexion, les données Innodb, les opérations de base de données, l'utilisation des ressources, etc. Pour plus d'informations, voir la section Surveillance des bases de données MySQL.

Prise en charge du suivi des transactions pour la base de données Oracle, Oracle RAC et Oracle EBS

DX APM prend en charge la collecte basée sur les événements de traces de base de données pour les extensions de base de données suivantes : Oracle Database, Oracle Real Application Clusters (RAC) et Oracle E-Business Suite (EBS).

Les extensions de base de données fournissent des traces de base de données basées sur le service de base de données spécifique. Les suivis de base de données fournissent les détails des indicateurs de performance. Les traces affichent également des informations et des statistiques sur l'utilisation de l'extraction, de l'attente, de l'analyse SQL et des ressources, tandis que la base de données correspondante exécute les transactions de base de données pour une transaction métier particulière.

Prise en charge du cadre Koa.js pour Node.js

L'agent Node.js prend en charge Koa.js, qui est la structure Web Node.js nouvelle génération.

Prise en charge de la surveillance NGINX

L'extension de l'agent de surveillance NGINX vous permet de surveiller la version des services hébergés NGINX. Vous pouvez utiliser cette extension avec les autres extensions existantes pour surveiller à la fois la surveillance de l'infrastructure NGINX et les performances des services hébergés sur la version des services hébergés NGINX. Pour plus d'informations, voir la section Surveillance NGINX.

Amélioration de la prise en charge des applications .NET Core

DX APM prend désormais en charge la surveillance des transactions .NET Core asynchrones.

Mesures de surveillance Kafka Lag et Consumer Offset

La surveillance Kafka affiche désormais les performances des décalages des groupes de consommateurs Kafka. La surveillance Kafka utilise les mesures **Lag** et **Current Offset** pour chaque groupe de consommateurs lorsque l'application Kafka subit des performances lentes. Ces mesures peuvent vous aider à déterminer si les performances Kafka lentes sont dues au fait que les utilisateurs ne lisent pas les messages suffisamment rapidement, ce qui entraîne la lecture des messages en attente.

Amélioration de la prise en charge de Java 11

L'agent Java surveille désormais les applications Java 11 sans qu'il soit nécessaire de transférer des arguments de ligne de commande supplémentaires à la commande `-javaagent`.

Améliorations de la surveillance de la corrélation des journaux

La surveillance de la corrélation des journaux prend désormais en charge log4j2. Vous pouvez désormais définir le modèle `param com.ca.apm.log.correlation.mdc.insert.before` avec `%m%n` et `%msg` simultanément. Vous pouvez également définir plusieurs modèles pour `param com.ca.apm.log.correlation.mdc.insert.before`.

Prise en charge des applications Akka et Play

DX APM inclut une extension d'agent Java qui indique les performances Akka et le cadre Play. Cette extension rapporte les mesures de performances de serveur frontal, d'arrière-plan, de corrélation, de contrôleur de lecture et de performances de Akka.

Surveillance Prometheus

L'agent Infrastructure inclut désormais la surveillance Prometheus, qui permet à DX APM d'ingérer à distance les mesures Prometheus. Vous pouvez configurer les propriétés du fichier de la configuration pour l'intégration des mesures directement à partir d'un serveur d'arrière-plan Prometheus. Par exemple, vous pouvez configurer le type de mesure, la requête de mesure, etc. Vous pouvez également configurer la surveillance Prometheus pour l'intégration de mesures à partir d'un exportateur Prometheus.

Surveillance de serveurs JMX distants

L'agent Infrastructure inclut une nouvelle extension de surveillance de serveurs JMX distants. Cette extension vous permet de surveiller à distance les performances des applications Java sur JMX sans nécessiter d'instrumentation d'application directe. Les mesures de performances JMX sont corrélées avec d'autres mesures de performances telles que les performances de l'infrastructure et des applications. Pour plus d'informations, voir la section Surveillance de serveurs JMX à distance.

Couchbase Monitor

L'agent Infrastructure inclut une nouvelle extension de surveillance Couchbase. Cette extension vous permet de surveiller les performances de Couchbase, y compris de surveiller un cluster. Pour plus d'informations, reportez-vous à la section Surveillance Couchbase.

Modes de surveillance de l'agent Java

L'agent Java dispose d'un nouveau mode de surveillance que vous pouvez définir sur **None** (aucun). Le mode None est le mode minimal pour l'agent, ce qui désactive la plupart des fonctionnalités et des mesures. Vous pouvez changer le mode au moment de l'exécution sans nécessiter un redémarrage du serveur d'applications.

Amélioration de la visibilité sur les performances des applications .NET

L'agent NET collecte maintenant automatiquement les traces de pile. Les traces de pile contiennent la pile d'appel de la méthode d'application .NET complète. Les traces de pile apparaissent comme des clichés dans les traces de transaction.

Prise en charge de l'application PHP dans le conteneur du Docker

L'agent PHP prend désormais en charge la surveillance CLI PHP. Vous pouvez utiliser l'agent PHP pour surveiller les scripts PHP exécutés à partir d'un autre script PHP.

Prise en charge des applications Node.js dans les conteneurs du Docker

L'agent Node.js vous permet de surveiller votre application Node.js, ainsi que les bases de données se connectant à votre application Node.js. Par exemple, les bases de données PostgreSQL, MongoDB et MySQL.

Fonctionnalités de l'interface utilisateur

API pour le téléchargement d'agent disponible à partir d'APM Command Center

Vous pouvez maintenant utiliser API APM Command Center pour télécharger les derniers packages à partir d'APM Command Center et personnaliser le comportement du téléchargement en définissant les propriétés requises. Par exemple, au cours du téléchargement, vous pouvez personnaliser la charge utile et définir certaines propriétés comme masquées. Pour plus d'informations, voir la section API APM Command Center.

Agent Java pour les microservices dans APM Command Center

Vous pouvez désormais créer et télécharger l'agent Java pour les microservices à partir d'APM Command Center. Pour plus d'informations, voir la section Déploiement des packages d'agent à l'aide de CA APM Command Center.

Filtre de la vue des mesures à l'aide d'attributs

Dans la vue des mesures, vous pouvez désormais définir des filtres pour les agents en fonction de leurs attributs.

Amélioration des calculatrices

Vous pouvez désormais créer des calculatrices qui utilisent les valeurs d'un groupement de mesures comme entrée, et la moyenne ou la somme des valeurs. Les calculatrices génèrent la valeur résultante en tant que mesure personnalisée dans le navigateur de mesures. Les mesures générées par la calculatrice s'affichent sous un processus virtuel, nommé **Processus de mesure personnalisé**. Le processus de métrique personnalisé s'exécute sur un hôte virtuel nommé **Processus de mesure personnalisé**. Pour plus d'informations, voir la section Créer et modifier des calculatrices.

Exécution de requêtes à l'aide d'API REST

Vous pouvez désormais utiliser les API REST suivantes pour rechercher des mesures et les données associées :

- API REST de demande de mesure

L'API de demande de mesure interroge les mesures pour différentes périodes, fréquences et mesures. Comme d'autres API APM REST, l'interface API REST de demande de mesure utilise une authentification par jeton. Pour plus d'informations, reportez-vous à la section API REST de demande de mesure.

- API REST du Team Center

API REST du Team Center fournit diverses fonctionnalités de requêtes de niveau tableau de bord et de données de mesures. Comme d'autres API REST APMDX APM, l'interface de l'API REST du Team Center utilise un système d'authentification basée sur des jetons. Pour plus d'informations, voir la section API REST du Team Center.

Importation et exportation de définitions de packages d'agent à partir d'APM Command Center

Vous pouvez désormais importer et exporter des définitions de package d'agent d'un client hébergé à un autre. Pour plus d'informations, voir la section Déploiement des packages d'agent à l'aide de CA APM Command Center.

Prise en charge et fonctionnalités dépréciées

DX APM ne prend plus en charge les fonctionnalités suivantes :

- Station de travail de ligne de commande
- Python 2.7
- Détecteur de modifications
- Instrumentation dynamique
- Enterprise Team Center
- Fonctionnalité de montage/démontage de l'agent.

Les agents sont toujours disponibles dans DX APM. Par conséquent, il n'est plus nécessaire de monter ni de démonter les agents.

- La propriété système de l'agent `-DagentProfile` n'est plus prise en charge.

Problèmes connus

Défaut DE449471 - L'URL de la vue d'isolement de l'agent Infrastructure ne s'ouvre pas

Applicable à : DX APM 20.1

Symptôme : la vue **Isolation** ne peut pas être générée pour l'agent Infrastructure. Cette situation se produit lorsque vous naviguez dans **Tableaux de bord**, **Agent**, **Ajouter un filtre**, sélectionnez le nom d'hôte de l'agent Infrastructure dans la liste déroulante, puis sélectionnez **Couche applicative**.

Solution : en fonction de la définition de l'alerte, définissez manuellement le filtre approprié dans la carte.

Défaut DE449130 - connexion impossible à l'aide d'un compte SAML

Applicable à : DX APM 20.1

Symptôme : l'utilisateur ne parvient pas à se connecter à l'aide des détails du compte SAML.

Solution : générez un [jeton public](#) et connectez-vous à l'aide de celui-ci.

Défaut DE440008 - La sélection d'une trace rétablit le volet Trace de la transaction sur haut

Applicable à : DX APM 20.1

Symptôme : ce problème se produit lorsqu'il existe de nombreux suivis dans le volet Trace des transactions de la visionneuse des traces de transaction. Après avoir fait défiler le volet et avoir sélectionné une trace, le volet Traces de transactions se réinitialise en haut.

Solution : faites défiler le volet Traces de transactions et recherchez la trace avec une bordure.

Défaut DE450933 - Erreur de surveillance OpenShift

Symptôme : je veux télécharger la surveillance OpenShift à partir de la boîte de dialogue de téléchargement APM SaaS APM. Je clique sur **OpenShift** sous la catégorie **Cloud Native**. Lorsque vous suivez les instructions et exécutez la commande `oc create -f caagent-openshiftmonitor.yml`, je reçois une erreur.

Comment puis-je résoudre ce problème ?

Solution : dans le fichier `caagent-openshiftmonitor.yml`, supprimez la propriété `- name: dev & readOnly: true`. Exécutez cette commande :

```
oc create -f caagent-openshiftmonitor.yml
```

Défaut DE432585 - Les valeurs des mesures des statistiques sur les ressources de surveillance IBM Integration Bus sont affichées comme cumulatives

Symptôme : les valeurs des mesures des statistiques sur les ressources de surveillance IBM Integration Bus (IIB Monitoring) sont affichées comme **cumulatives** au lieu de **par intervalle**.

Solution : il n'existe aucune solution à ce problème.

Défaut DE448777 - Les statistiques sur les flux de messages et les ressources de surveillance IBM Integration Bus ne sont pas rapportées

Symptôme : lorsque vous redémarrez le QM souscrit, les statistiques sur les flux de messages et de ressources IBM Integration Bus ne sont pas reportées dans DX APM.

Solution : redémarrez l'agent Infrastructure de DX APM.

Défaut DE448618 - Echec du module d'extension Jenkins dans l'environnement DX SaaS

Symptôme : le module d'extension Jenkins, `em.url` ne fonctionne pas DX SaaS après la mise à niveau de DX APMem.url.

Solution : lorsque vous mettez à niveau l'environnement DX SaaS, mettez à jour la valeur de l'URL EM dans le fichier `performance-comparator.properties`.

Procédez comme suit :

1. Connectez-vous à DX SaaS.
2. Cliquez sur **Ouvrir** dans la zone **DX APM**. La page d'accueil de DX APM s'affiche. La page d'accueil affiche l'URL utilisée pour accéder à DX APM dans le navigateur Web.
3. Accédez à `<Espace de travail Jenkins>\<nom job jenkins>\properties\`.
4. Ouvrez le fichier `performance-comparator.properties`.
5. Mettez à jour la valeur de la propriété `em.url` avec la dernière URL EM.

Notes de mise à jour 2019

Cette section contient les notes de mise à jour pour 2019.

- [Novembre 2019](#)
- [Octobre 2019](#)
- [Août 2019](#)

Novembre 2019

26 novembre 2019 - Nouveautés !

Mesures de l'agent Infrastructure pour RedHat

Vous pouvez désormais afficher les mesures du serveur RedHat sur l'UC, les disques, le système de fichiers, la mémoire, le réseau, les processeurs, la pagination, les permutations, les performances du système, etc. *Surveillance réactive Spring Boot*

Cette nouvelle extension d'agent Java surveille les applications Spring Boot Reactive. L'extension instrumente spécifiquement les serveurs HTTP asynchrones Netty, les clients HTTP asynchrones Netty et les structures Spring Boot Reactor Core pour assurer la corrélation entre les threads et le suivi des composants asynchrones. Pour plus d'informations, voir Surveillance des applications Spring Boot Reactive.

Surveillance Oracle RAC

L'extension Oracle RAC vous permet de surveiller les performances et la disponibilité de votre environnement Oracle RAC (Real Application Clusters). Vous pouvez utiliser l'extension Oracle RAC pour déterminer si un service dans une base de données de clusters présente des problèmes de disponibilité. L'extension Oracle RAC offre une visibilité en temps réel sur les ressources de base de données critiques telles que les interblocages, les analyses complètes de tables, les fichiers journaux de rétablissement, les segments de restauration, etc.

Vous pouvez configurer l'extension Oracle RAC et collecter ses mesures de performances afin de vous aider à surveiller votre environnement Oracle RAC. Vous pouvez voir directement la rentabilisation dans des tableaux de bord préconfigurés et des alertes déclenchées par les performances qui vous informent de manière proactive sur les violations potentielles de SLA, avant que les utilisateurs finaux soient affectés. Pour plus d'informations, voir Surveillance Oracle RAC.

Surveillance Oracle EBS

L'extension Oracle E-Business Suite (EBS) vous permet de surveiller les performances et la disponibilité des composants d'Oracle EBS suivants : gestionnaires simultanés, programmes simultanés et gestionnaire de résolution de conflits. Vous pouvez utiliser l'extension Oracle EBS pour examiner les jobs simultanés, les gestionnaires simultanés au niveau du cluster et au niveau du nœud individuel. Pour plus d'informations, consultez la section Surveillance Oracle EBS.

Surveillance IIB

Vous pouvez utiliser la surveillance IBM Integration Bus (IIB) pour surveiller l'intégrité et la disponibilité des applications connectées à IIB et les flux de messages correspondants. Comme condition préalable, IBM MQ doit fonctionner de manière à ce que l'extension IIB Monitoring puisse se connecter à IBM MQ et collecter les statistiques IIB. Pour plus d'informations, voir la section Surveillance IIB.

Extension OkHttp

L'agent Java prend désormais en charge la surveillance OkHttp. OkHttp représente un client HTTP performant prenant en charge le protocole HTTP/2. Ce protocole charge efficacement les données et économise la bande passante. Pour plus d'informations, voir Extension OkHttp.

Mesures liées à Host Monitoring

Outre les mesures de surveillance d'hôte existantes prises en charge par DX APM, les mesures de surveillance d'hôte pour Solaris et RedHat ont été récemment ajoutées. Pour plus d'informations, voir la section Surveillance d'hôte.

Prise en charge de la surveillance NGINX

L'extension de l'agent de surveillance NGINX vous permet de surveiller les versions suivantes du serveur NGINX : NGINX-Plus Version et NGINX Community Version. Vous pouvez utiliser l'extension pour surveiller la surveillance de l'infrastructure NGINX. Pour plus d'informations, voir la section Surveillance NGINX.

Chargement de l'instrumentation dynamique de l'agent NET

L'agent .NET peut désormais charger dynamiquement l'instrumentation sans nécessiter de redémarrage de l'application. Voici quelques exemples :

- Vous pouvez instrumenter une méthode spécifique qui ne correspond pas encore à une définition de sonde existante. Plus spécifiquement, vous pouvez instrumenter des méthodes MVC asynchrones sans redémarrage.
- DX APM peut réévaluer les méthodes et modifier l'instrumentation lorsque vous effectuez les actions suivantes :
 - Placez un nouveau fichier .pbd dans le dossier **hotdeploy**
 - Modifier ou supprimer un fichier .pbd existant.

Services AWS et Azure

- La nouvelle extension d'Amazon Web Services (AWS) prend en charge les nouveaux types de services suivants : calcul, stockage, messagerie, base de données, analyse, services mobiles. Pour plus d'informations, voir la section Surveillance Amazon Web Services.
- La nouvelle extension des services Azure prend en charge les nouveaux types de service suivants : calcul, stockage et analyse. Pour plus d'informations, reportez-vous à la section Surveillance Azure.

Problème connu de l'agent Infrastructure

Défaut DE437143 - Aucune mesure Host Monitor

Applicable à DX APM 10.7 Service Pack 1 (SP1-3), DX APM 11.1.3, Kubernetes et Host Monitor

Symptôme :

Aucune mesure n'apparaît pour le nœud **SystemEdge** dans la **Vue des mesures**. Ce problème survient dans les conditions suivantes :

- Host Monitor est réinstallé à l'aide de l'agent de surveillance universel.
- Le processus CA SystemEdge n'est pas arrêté, même lorsque Kubernetes détruit le pod correspondant.

Solution :

Procédez comme suit :

1. Connectez-vous au nœud **SystemEdge** sur lequel aucune mesure Host Monitor n'est présente.
2. Utilisez la commande suivante pour arrêter le processus SystemEDGE s'il est en cours d'exécution : `ps -ef | grep "SystemEDGE" | grep -v grep`.
3. Redéployez l'agent de surveillance universel.

Octobre 2019

10 octobre 2019 - Nouveautés

Onglets supplémentaires du Navigateur de mesures

Ces nouveaux onglets affichent les traces et les erreurs associées à une transaction métier.

- Onglet **Traces** : cet onglet affiche la liste des transactions métier, les traces associées et les détails des composants.
- Onglet **Erreurs** : cet onglet affiche la liste des transactions métier qui contiennent des erreurs.

Problème connu de l'agent Infrastructure

Défaut DE437143 - Aucune mesure Host Monitor

Applicable à DX APM 10.7 Service Pack 1 (SP1-3), DX APM 11.1.3, Kubernetes et Host Monitor

Symptôme :

Aucune mesure n'apparaît pour le nœud **SystemEdge** dans la **Vue des mesures**. Ce problème survient dans les conditions suivantes :

- Host Monitor est réinstallé à l'aide de l'agent de surveillance universel.
- Le processus CA SystemEdge n'est pas arrêté, même lorsque Kubernetes détruit le pod correspondant.

Solution :

Procédez comme suit :

1. Connectez-vous au nœud **SystemEdge** sur lequel aucune mesure Host Monitor n'est présente.
2. Utilisez la commande suivante pour arrêter le processus SystemEDGE s'il est en cours d'exécution : `ps -ef | grep "SystemEDGE" | grep -v grep`.
3. Redéployez l'agent de surveillance universel.

Août 2019

31 août 2019 - Nouveautés

Prise en charge d'AdoptOpenJDK

CA Technologies, une société Broadcom, adopte davantage de technologies open source dans ses produits. Dans le cadre de cette stratégie, divers produits ont fait l'objet d'implémentations Java open source. Pour s'aligner sur cette orientation de l'entreprise, DX APM a adopté AdoptOpenJDK (11), qui remplace le JDK Oracle.

Problème connu de l'agent Infrastructure

Défaut DE437143 - Aucune mesure Host Monitor

Applicable à DX APM 10.7 Service Pack 1 (SP1-3), DX APM 11.1.3, Kubernetes et Host Monitor

Symptôme :

Aucune mesure n'apparaît pour le nœud **SystemEdge** dans la **Vue des mesures**. Ce problème survient dans les conditions suivantes :

- Host Monitor est réinstallé à l'aide de l'agent de surveillance universel.
- Le processus CA SystemEdge n'est pas arrêté, même lorsque Kubernetes détruit le pod correspondant.

Solution :

Procédez comme suit :

1. Connectez-vous au nœud **SystemEdge** sur lequel aucune mesure Host Monitor n'est présente.
2. Utilisez la commande suivante pour arrêter le processus SystemEDGE s'il est en cours d'exécution : `ps -ef | grep "SystemEDGE" | grep -v grep`.
3. Redéployez l'agent de surveillance universel.

3 août 2019 - Nouveautés

Business Payload Analyzer

Business Payload Analyzer est un système de surveillance d'expérience d'utilisateur final qui vous permet de rechercher des informations dans des services sans avoir à recréer vos applications. Business Payload Analyzer fournit un mécanisme de collecte et de génération de rapports de données enrichies pour effectuer le suivi des flux de travaux entre les services du centre de données. Business Payload Analyzer étudie l'application qu'il surveille et capture les transactions métier et des mesures pour calculer les mesures de performances. Ces mesures fournissent des informations sur l'expérience utilisateur. La collecte des données est automatique et aucune personnalisation n'est requise pour les applications. Toutefois, l'administrateur de l'application peut configurer le système via l'interface

utilisateur pour personnaliser la surveillance. Cette version de Business Payload Analyzer fournit les fonctionnalités clés suivantes :

- Prise en charge de la capture des charges utiles à partir des serveurs Web IIS (.NET) et Apache Tomcat
- Prise en charge prête à l'emploi de la capture d'URL, d'en-têtes HTTP et de formulaires HTML
- Planification du mode de détection périodique, permettant de mettre à jour le modèle de science de données de la fréquence d'occurrence de champ et de valeur
- Détection automatique basée sur l'apprentissage automatique et mise en surbrillance des valeurs de données les plus importantes, qui sont définies comme paramètres d'identification
- Attribution dynamique de nom de transaction métier et identification de la segmentation des utilisateurs (Ex. : balises démographiques telles que la valeur d'un panier, le solde d'un compte et l'ID d'utilisateur)
- Ajustement de la catégorisation de la science des données des champs de charge utile capturée dans une interface graphique simple d'utilisation
- Support fourni à l'administrateur pour le changement de nom et la capture partielle de champs complexes, tels que des cookies
- Intégration de la topologie DX APM
 - Les transactions métier détectées par Business Payload Analyzer s'affichent sous forme d'éléments d'utilisateur final dans le mappage d'applications.
 - Les transactions métier détectées par Business Payload Analyzer apparaissent dans les traces de la visionneuse de transactions métier de Team Center.
 - Les informations démographiques utilisateur de Business Payload Analyzer sont signalées comme paramètres de suivi dans la visionneuse de transactions métier de Team Center.
 - Les transactions métier détectées par Business Payload Analyzer signalent des mesures d'intégrité et de performances dans la visionneuse de mesures de Team Center.

Prise en main

Prise en main de DX APM

Pour...	Procédez comme suit...	Reportez-vous aux ressources suivantes...
En savoir plus sur CA Application Performance Management via des vidéos	Accédez aux canaux YouTube CA Technologies et CA Educate dans consacrés à CA APM.	Ressources vidéos destinées aux analystes
Améliorez vos connaissances sur CA Application Performance Management et votre productivité.	Suivre un cours CA Education, un parcours de formation ou une formation.	DX APM Cours et formations.
Familiarisez-vous avec les termes utilisés dans CA Application Performance Management.	Recherchez des termes et lisez leur définition dans le glossaire.	Glossaire

NOTE

Pour télécharger et configurer le proxy cloud, consultez la documentation relative au [proxy cloud](#).

Support et compatibilité

La page produit de DX APM du site Web du [support de Broadcom/CA](#) fournit le logiciel et la documentation de toutes les versions.

Pour obtenir des informations sur le système, l'environnement d'exploitation et les versions prises en charge, contactez le support Broadcom.

Architecture DX APM

Un environnement d'évaluation DX APM repose sur les composants d'architecture suivants :

- Client hébergé : groupe d'utilisateurs possédant des droits spécifiques leur permettant d'accéder à l'instance logicielle.
- Service : modèle de livraison de logiciels dans lequel le logiciel est concédé sous licence via un abonnement. Le logiciel est hébergé de manière centralisée.
- Pod OpenShift : un ou plusieurs conteneurs déployés sur un hôte. Un pod est l'unité la plus petite pouvant être définie, déployée et gérée.
- Conteneur : conteneur DX APM unique qui regroupe le pilote de charge, le gestionnaire d'entreprise et l'application de démonstration

Un conteneur est affecté à des pods OpenShift dédiés et ces pods dédiés s'exécutent sur des noeuds OpenShift dédiés. Par conséquent, dans l'environnement des versions d'évaluation, la cardinalité Client hébergé-Service-Pod-Conteneur est de 1-1-1-1. Broadcom maintient un ensemble de pods initialisés afin d'accélérer le processus d'intégration des clients hébergés. En cas d'ajout réussi, un pod déjà en cours d'exécution est affecté au client hébergé et un nouveau pod est ajouté dans le pool. Ces pods mis en pool deviennent actifs lorsqu'un client hébergé leur est affecté.

L'architecture inclut les principaux éléments suivants :

- **Mise en réseau**

La transmission des données de client hébergé et des requêtes est assurée via une communication HTTPS (443). L'ensemble des données de client hébergé et du trafic de requête est multiplexé sur une connexion unique, c'est pourquoi la totalité du trafic système est dirigé vers l'adresse *.apm.cloud.ca.com. Ce site héberge un routeur OpenShift. Le routeur OpenShift utilise alors le segment le moins significatif de l'adresse de destination (qui possède un identificateur de client hébergé unique) afin de démultiplexer le terminal de service. Utilisez une liste blanche pour

le système de nom de domaine publics (DNS) *.apm.cloud.ca.com et ne vous fiez pas des adresses IP, car elles changent fréquemment.

- **Stockage des données de client hébergé et de la configuration**

DX APM stocke les différents types de données de surveillance et de constructions de configuration. Tous ces types sont externalisés afin que les conteneurs soient sans état, facilitant ainsi les mises à niveau. D'un point de vue structurel, deux types de données sont stockées : les données basées sur un fichier et les données relationnelles. Les données relationnelles sont stockées dans des instances de la plate-forme Google Cloud Platform.

- **Gestion des services - Moteur de provisionnement**

OpenShift est le moteur de provisionnement. Ce microservice basé sur Java reçoit les événements de cycle de vie et de gestion des clients hébergés en amont (contrôlé par GIS) et effectue les appels d'API OpenShift nécessaires. Pendant l'ajout, le moteur de provisionnement (PE) prépare la structure de répertoires du système de fichiers réseau et le schéma du service de base de données relationnelles pour le client hébergé. La taille du moteur de provisionnement augmente au fur et à mesure que des nouvelles fonctionnalités (de sauvegarde et de migration par exemple) sont ajoutées au cloud DX APM.

Ressources vidéo de DX APM

DX APM inclut une vaste gamme de ressources vidéo qui viennent compléter la documentation et qui présentent les fonctionnalités disponibles dans DX APM.

Les liens ci-dessous mènent à la chaîne YouTube de [CA Technologies](#) qui propose des listes de lecture consacrées à DX APM. Lorsque vous cliquez sur un lien, un nouvel onglet s'ouvre pour afficher la vidéo sur le site YouTube. Pour afficher les vidéos incorporées en mode plein écran, cliquez sur Lire, puis sur le logo YouTube dans la barre d'outils inférieure. Un nouvel onglet s'ouvre directement sur la vidéo YouTube.

Si votre entreprise a bloqué YouTube, contactez votre administrateur.

Vous pouvez utiliser DX APM pour surveiller les performances des applications. Vous pouvez identifier les zones de votre environnement qui subissent une charge élevée et trier les problèmes potentiels avant qu'ils n'affectent l'expérience client. Vous pouvez également utiliser DX APM pour effectuer le suivi des problèmes existants jusqu'à leur résolution.

DX APM : identification de la cause première d'un problème d'application

9 minutes et 46 secondes

Omar vous montre comment parcourir l'interface utilisateur de DX APM pour identifier rapidement la source des problèmes de performances.

DX APM : mise en oeuvre de l'agent de surveillance universel

23 minutes et 53 secondes

Rob vous présente les fonctionnalités de base de l'agent de surveillance universel (UMA) .

DX APM : mise en oeuvre de l'analyse de l'entonnoir

33 minutes et 42 secondes

Harish vous montre comment l'analyse de l'entonnoir peut vous aider à surveiller votre flux de production.

DX APM : présentation et utilisation de la carte et de l'arborescence de mesures

12 minutes et 34 secondes

Nous vous montrons comment parcourir les couches de carte pour comprendre les relations entre les composants. Découvrez les attributs et parcourez l'arborescence de mesures.

Architecture de référence de DX APM : présentation de l'approche du déploiement de DX APM

21 minutes et 5 secondes

Henrik discute du déploiement de DX APM, de la haute disponibilité, des services, de la connectivité et du flux de données.

DX APM Team Center : utilisation des attributs

1 heure 11 minutes et 39 secondes

Andreas vous présente la carte et les attributs en vous expliquant le vocabulaire, la navigation et les meilleures pratiques.

DX APM : présentation de la vue Expérience, du tri assisté et du carnet d'expérience

13 minutes et 11 secondes

Nous décrivons l'utilisation de la vue Expérience et des fiches d'expérience, du tri assisté et du carnet d'expérience.

DX APM : analyse des alarmes : utilisation et correction

28 minutes et 33 secondes

Jan explique les informations sur les alarmes, le filtrage et la réduction du bruit, les types d'alarme et leurs algorithmes, ainsi que la correction des alarmes.

DX APM : procédure de création de services

47 minutes et 14 secondes

Nous vous présentons les services DX APM, l'assistant de création de services, la procédure de création de votre premier service et l'analyse des services.

Procédure de déploiement de l'agent de surveillance universel

8 minutes et 33 secondes

Nous vous expliquons la procédure d'installation de l'agent de surveillance universel, qui instrumente et surveille automatiquement votre cluster Kubernetes.

DX APM : procédure de tri des problèmes de lenteur de connexion

17 minutes et 40 secondes

Nous utilisons une application de démonstration exécutée dans un environnement Kubernetes déployé sur un cloud AWS pour vous guider dans l'utilisation du produit App Experience Analytics. Nous examinons l'expérience utilisateur final d'une application surveillée. Il s'agit par exemple de pannes subies par l'utilisateur final pendant la semaine écoulée ou de sessions connaissant des connexions lentes depuis les dernières 24 heures.

DX APM : obtention d'une meilleure visibilité entre l'application et l'infrastructure

9 minutes et 59 secondes

Omar parcourt les niveaux, les noeuds et les couches de carte en effectuant une démonstration de la capture de mesures à l'aide de balises, ainsi que de la corrélation de mesures.

DX APM : démonstration de la gestion des clusters

10 minutes et 33 secondes

Dominik présente les services de gestion des clusters, le déploiement des services, les services de client hébergé, la création de clients hébergés, les jetons et la surveillance des performances à l'aide de mesures.

Moniteur App Synthetic Monitor : procédure de simulation des transactions stratégiques et des parcours utilisateur

10 minutes et 7 secondes

Dominik présente DX App Synthetic Monitor et effectue une démonstration de la création de moniteurs synthétiques et de scripts pour la réplique de l'expérience de l'utilisateur final.

DX APM : utilisation des modules de gestion dans Team Center

5 minutes et 2 secondes

Nous vous présentons les modules de gestion, qui permettent aux administrateurs d'organiser et de gérer facilement les données de mesure.

Conventions relatives aux répertoires et noms de fichier

La documentation de DX APM utilise les conventions suivantes pour les noms de fichier et les chemins d'accès aux répertoires :

Convention	La Convention fait référence aux éléments suivants
<répertoire_base_agent>	Répertoire de niveau supérieur dans lequel l'agent Introscope est installé ; par défaut, ce répertoire est nommé <code>wily</code> .
<répertoire_base_BdD_APM>	Répertoire de niveau supérieur dans lequel votre serveur d'applications est installé ; ce répertoire est souvent identique à <répertoire_base_agent>.
<AppServer_Home>	Répertoire de base de votre serveur d'applications
<EM_Home>	Répertoire de niveau supérieur dans lequel le gestionnaire d'entreprise est installé
<Installation_Directory>	Répertoire d'installation d'un composant DX APM ou toute autre application lorsqu'il n'est pas installé dans le répertoire par défaut ou standard
<ProductName_Home>	Répertoire d'installation d'un produit tiers ou d'un type d'application Par exemple, vous pouvez vous référer au répertoire de base de votre serveur d'applications WebSphere au format <répertoire_base_WAS>.
<Workstation_Home>	Répertoire de niveau supérieur dans lequel la station de travail est installée ; ce répertoire est souvent identique au répertoire <répertoire_base_EM>.

<File_Name><version><Operating System or other identifier>.<FileType>	Nom de fichier qui inclut des informations d'identification spécifiques ; par exemple, si vous extrayez des fichiers d'un package .tar pour <nom_produit> 10.7.0 sur un système d'exploitation UNIX, téléchargez <nom_produit> 107.0=.0unix.tar . Le nom de fichier apparaît dans cette documentation au format : <nom_produit><10.7.0>.unix.tar .
Séparateur de chemin barre oblique (/)	Séparateur de chemin utilisé dans les noms de répertoire de votre environnement d'exploitation Les environnements UNIX et les exemples dans cette documentation utilisent la barre oblique. Utilisez le séparateur approprié pour votre système d'exploitation.
Variables d'environnement symbole du dollar (\$)	Notation de variable d'environnement utilisée dans votre système d'exploitation Les environnements UNIX et les exemples dans cette documentation utilisent le symbole du dollar (\$). Utilisez le caractère approprié pour votre système d'exploitation.

Personnalisations

DX APM est hautement personnalisable, mais le service de support de Broadcom ne prend pas en charge les personnalisations apportées aux configurations par défaut. Par exemple, vous pouvez personnaliser l'instrumentation des agents, y compris déployer des PBD personnalisées. Vous pouvez créer des outils de calcul JavaScript ainsi que des scripts shell et EPAgent pour des extensions d'agent. Si nous pensons que des personnalisations entraînent un problème au niveau du produit, nous pouvons vous demander de les supprimer ou de les désactiver. Nous pouvons ensuite vous apporter notre aide. Pour obtenir de l'aide sur une personnalisation DX APM nouvelle ou existante, contactez l'architecte de la solution.

Articles de connaissances

Pour afficher la liste complète des articles de connaissances pour DX Application Performance Management, cliquez [ici](#).

Utilisez des filtres de recherche avancée pour affiner vos critères de recherche.

1. Dans la liste des options disponibles sous **Sources**, sélectionnez Knowledge Articles (Articles de connaissances).

Sources	
<input type="checkbox"/> TechDocs	1139422
<input type="checkbox"/> Solutions	503672
<input type="checkbox"/> Community Threads	328165
<input type="checkbox"/> Problems	236777
<input type="checkbox"/> Knowledge Articles	140221
<input type="checkbox"/> Product News	9361

2. Dans les options **Product** (Produit), sélectionnez Application Performance Management.

⋮

Product

▼

🔍 Search

×

<input type="checkbox"/>	ACF2	1550349
<input type="checkbox"/>	CA Automic	1014573
<input type="checkbox"/>	Identity Management Suite	1012945
<input type="checkbox"/>	Application Performance Management	1011866
<input type="checkbox"/>	CA 7 Workload Automation	526756
<input type="checkbox"/>	APCDOC Automated Job Document...	522603
<input type="checkbox"/>	APCDDS Automated Report Balancing	520265
<input type="checkbox"/>	CA Configuration Automation	513009
<input type="checkbox"/>	CA Service Management - Asset Port...	508258

3. Sélectionnez la langue de votre choix.

4. Dans les options **Updated Date** (Date de mise à jour), sélectionnez une durée.

Updated Date

☐ All Time 507268
 ☐ Past Year 4090
 ☒ Past Month 390
 ☐ Past Week 77
 ☐ Past Day 25

5. Les articles de connaissances correspondant aux critères de filtre spécifiés s'affichent.

Glossaire

Ce glossaire fournit une description des termes clés de DX APM.

NOTE

Tous les termes s'appliquent à DX APM sur site, et seuls quelques uns d'entre eux s'appliquent également à DX APM.

agent .NET

L'*agent .NET* collecte des mesures sur les applications Microsoft .NET.

Voir aussi : Common Language Runtime (CLR), .NET Framework

.NET Framework

.NET Framework de Microsoft est un environnement de développement et d'exécution qui permet à différents langages de programmation et bibliothèques de fonctionner ensemble. .NET Framework est basé sur un environnement d'exécution appelé Common Language Runtime (CLR). CLR utilise des langages de programmation comme C#.

Voir aussi : Common Language Runtime (CLR), agent .NET

agent

L'*agent* collecte des mesures relatives aux applications et à l'environnement et les transmet au gestionnaire d'entreprise. Ces applications peuvent être de l'un des types suivants : Java, .NET, PHP ou des applications Web. Une application qui signale des mesures à un agent est dite instrumentée.

Voir aussi : instrumenté, agent Java, agent .NET, agent PHP

Topologie de réseau agent - gestionnaire d'entreprise

La topologie de réseau agent - gestionnaire d'entreprise est la structure réseau de l'environnement DX APM. Cette topologie spécifie quels agents ou groupes d'agents peuvent se connecter aux éléments suivants :

- Gestionnaires d'entreprise autonomes spécifiques
- Collecteurs
- Groupes de collecteurs

équilibrage de charge d'agent

L'*équilibrage de charge d'agent* équilibre la charge de mesures entre les collecteurs dans un environnement en clusters. Les agents spécifiques affectés au MOM égalisent le nombre de mesures dans tous les collecteurs. Les agents spécifiques indiquent aux autres agents qu'ils doivent envoyer leurs données de mesures au collecteur le moins occupé dans le cluster.

Voir aussi : agent, Collecteur, gestionnaire des gestionnaires (Manager of Managers, MoM)

alerte

Une *alerte* est un jeu enregistré de valeurs seuil pour "Avertissement" et "Danger", avec d'autres propriétés associées. Les alertes font partie des objets de base d'un module de gestion, qui enregistre des collections de ces objets afin de les réutiliser. Une alerte comprend généralement des actions qui lui sont associées, mais les actions sont elles-mêmes des objets distincts du module de gestion.

Il convient de faire la distinction entre l'alerte proprement dite (par exemple, le nom de l'alerte associée aux valeurs seuil enregistrées) et :

- un *indicateur d'alerte*, qui est un affichage graphique d'un statut d'alerte
- une *notification d'alerte*, qui est l'une des actions associables à une alerte.

Stockage Amazon EBS

Amazon EBS (Elastic Block Store) est un volume de stockage de niveau bloc qui persiste indépendamment de la durée de vie d'une instance EC2. Nous vous recommandons d'utiliser ce type de stockage dans votre instance afin de pouvoir arrêter et redémarrer votre instance ultérieurement.

Amazon Machine Image

Une *Amazon Machine Image* (AMI) est une image d'ordinateur chiffrée, semblable à un modèle, du lecteur racine d'un ordinateur. Les images AMI contiennent le système d'exploitation et peuvent inclure le logiciel et les couches applicatives, telles que les serveurs de base de données, les intergiciels et les serveurs Web. L'AMI est stockée dans l'Amazon Elastic Block Store ou l'Amazon Simple Storage Service.

Base de données APM

La *base de données APM* est une base de données relationnelle qui stocke les données.

Voir aussi : Base de données SmartStor, Base de données d'événements de transactions

Application Performance Management (APM)

Le produit *DX APM*. DX APM propose une stratégie de gestion des performances des applications qui vous permet de comprendre l'expérience de l'utilisateur final et de mesurer les accords sur les niveaux de service (SLA). Vous pouvez mapper toutes les transactions avec l'infrastructure de bout-en-bout. Vous pouvez également effectuer un tri des incidents et établir un diagnostic des causes premières dans une solution complète et intégrée.

capacité de prise en charge d'une application

DX APM mesure la *capacité de prise en charge* d'une application en mesurant les performances de différents composants de l'application. Les mesures fournissent des informations sur les JVM/CLR, les applications Web et les composants d'arrière-plan.

DX APM propose des mesures de capacité de prise en charge pour vous permettre de répondre aux questions relatives à l'intégrité de vos applications. La capacité de prise en charge d'une application est également appelée l'intégrité de l'application.

App Synthetic Monitor (ASM)

DX APM App Synthetic Monitor (ASM) est un produit qui crée des transactions synthétiques pour compléter la surveillance des transactions dans DX APM. ASM fournit un avertissement précoce des problèmes de disponibilité des applications.

attribut

Les *attributs* sont des étiquettes qui sont appliquées à des noeuds pour différencier les composants et identifier leurs relations avec d'autres composants.

règles d'attribut

Les *règles d'attribut* sont des règles qui automatisent le processus d'ajout d'attributs personnalisés. Seuls les administrateurs peuvent créer des règles d'attribut.

trace de transaction automatique

Lorsque l'instrumentation intelligente est activée, des outils de suivi hautement optimisés et à temps système réduit collectent une *trace de transaction automatique* dans des conditions de déclenchement spécifiques. Une erreur peut être un déclencheur. Autre exemple de déclencheur : dépassement du temps de réponse d'un composant après le déploiement de l'outil de suivi `ComponentTimeAutoTraceTriggerTracer`. Les traces de transaction automatiques affichent des composants à visibilité profonde et présentent des caractéristiques qui diffèrent des traces de transaction non automatiques, comme des traces manuelles et modèles.

AutoProbe

DX APM *AutoProbe* automatise le processus d'instrumentation des applications en ajoutant dynamiquement des sondes à ces applications au moment du démarrage. Les sondes DX APM fournissent les données sources pour les mesures DX APM.

Voir aussi : instrumenté, ProbeBuilder

promotion automatique

Lorsque vous activez la *promotion automatique*, toutes les modifications apportées aux paramètres du Business Payload Analyzer sont automatiquement appliquées.

composant d'arrière-plan

Un *composant d'arrière-plan* est un système externe sur lequel repose une application Web pour une partie de son traitement. Par exemple, un composant d'arrière-plan peut être une base de données, un serveur de messagerie, un système de traitement de transactions ou un système de messagerie. DX APM identifie automatiquement les bases de données, les systèmes JMS et les terminaux HTTP.

Pour les autres systèmes externes, DX APM analyse l'activité des sockets d'applications pour détecter et surveiller les composants d'arrière-plan sans configuration manuelle. Cette fonctionnalité est appelée détection de *composant d'arrière-plan automatique*.

Les mesures de composant d'arrière-plan s'affichent sous le noeud Composants d'arrière-plan dans l'arborescence Navigateur de mesures.

Voir aussi : composant frontal, point d'entrée

temps d'arrière-plan

Le *temps d'arrière-plan* correspond au temps nécessaire au composant Blame suspecté (un composant de base de données, par exemple) du système d'arrière-plan pour se terminer, mesuré à partir des rapports DX APM. Le temps d'arrière-plan d'Introscope est mesuré à partir du composant Java qui appelle le composant d'arrière-plan. Par conséquent, le temps inclut à la fois le temps de traitement du composant d'arrière-plan et le temps réseau éventuel passé à communiquer avec le composant d'arrière-plan.

Voir aussi : composant d'arrière-plan, composant Blame suspect

référence

La *référence* est un ensemble initial de données utilisées à des fins de comparaison ou de contrôle. DX APM utilise des algorithmes de référence pour surveiller les applications Web.

DX APM détermine la couleur d'un indicateur d'alerte dans l'onglet **Présentation** en évaluant les mesures actuelles par rapport à une référence pour ces mesures. Avec un noeud d'agent sélectionné dans l'arborescence centrée sur l'agent, le noeud heuristique affiche les valeurs de mesure correspondant à ces indicateurs.

Pour une mesure donnée, l'algorithme de référence DX APM détermine la prochaine valeur attendue, ainsi que l'écart attendu par rapport à cette valeur. Lorsque l'écart réel dépasse (2x) ou dépasse sensiblement (4x) l'écart attendu, l'outil de référence indique une violation modérée ou sévère. L'élément heuristique associé devient jaune ou rouge.

En interne, l'outil de référence évalue la pente de la série chronologique et détermine la valeur attendue de la pente. Les données récentes ont plus de poids que les données plus anciennes.

Voir aussi : mesures heuristiques, spécification

Blame

DX APM *Blame* est la technologie utilisée pour instrumenter une application. DX APM surveille les interactions des composants et l'utilisation des ressources en marquant les composants frontaux et les composants d'arrière-plan des applications. DX APM fournit également des mesures pour l'examen des problèmes.

Voir aussi : composant d'arrière-plan, composant frontal, instrumenté, outil de suivi de transaction

BT Listener

Le BT Listener (Business Transaction Listener) est un composant Business Payload Analyzer qui filtre et achemine uniquement les données intéressées demandées par le composant BT Diviner (Business Transaction Diviner). Un BT Listener est déployé entre le module d'extension et le BT Diviner. BT Listener est pris en charge sous Windows et Linux.

application business

Une *application business* est un programme logiciel qui automatise un service d'entreprise. DX APM surveille les transactions Web qui sont le produit des applications Web. Une application business fait partie de la hiérarchie de transactions.

service d'entreprise

Dans SOA Performance Management, un service d'entreprise adresse des demandes sortantes aux systèmes d'arrière-plan pour le bus de service d'entreprise.

composant de transaction métier

Un *composant de transaction métier* représente une paire demande/réponse HTTP qui est instrumentée et surveillée afin de suivre l'intégrité d'une transaction métier. Les composants de transaction métier constituent la source de mesures d'intégrité de carte.

Le composant de transaction métier est le seul composant d'identification de la transaction.

Un composant de transaction métier est similaire aux deux composants suivants :

- Transaction (étant donné qu'il s'agit de la transaction d'identification de la transaction métier) ;
- Composant de transaction (étant donné qu'il s'agit du composant d'identification dans la transaction).

Voir aussi : transaction, composant de transaction, hiérarchie de transaction

attributs capturés

Dans Business Payload Analyzer, vous pouvez définir les attributs que vous souhaitez capturer dans chaque transaction, lorsqu'ils sont disponibles, en tant qu'*attributs capturés*. Les attributs capturés avec des valeurs numériques peuvent être analysés dans le temps sous forme d'indicateurs clés de performance dans le Navigateur de mesures ou les tableaux de bord.

Voir : Présentation des attributs Business Payload Analyzer

Règle de capture

Dans Business Payload Analyzer, la *règle de capture* définit les attributs à capturer dans chaque transaction lorsqu'elle est disponible.

clamp

Un *clamp* est une limite configurable du nombre de mesures qui sont renvoyées pour une fonction spécifique. Utilisé dans le clamping de trace de transaction et le clamping de mesure pour divers composants DX APM, comme les agents et le gestionnaire d'entreprise.

Voir aussi : clamp de mesure, outil de suivi de transaction

Collecteur

Un *collecteur* est un gestionnaire d'entreprise utilisé dans un environnement en cluster. Le gestionnaire des gestionnaires (Manager of Managers, MOM) gère les collecteurs dans les environnements en cluster.

Voir aussi : gestionnaire d'entreprise (Enterprise Manager, EM), gestionnaire des gestionnaires (Manager of Managers, MOM)

Common Language Runtime (CLR)

Common Language Runtime (CLR) est l'implémentation Microsoft de l'infrastructure CLI (Common Language Infrastructure). L'objectif de l'infrastructure CLI est de proposer une plate-forme indépendante du langage pour le développement et l'exécution d'applications.

.NET CLR est l'équivalent approximatif de la plate-forme Java JVM.

Voir aussi : agent .NET, .NET Framework

configurer

Dans DX APM, le terme *configurer* a un sens particulier. *Configurer* consiste à définir ou à modifier des valeurs ou des entrées dans des propriétés, des scripts, des PBD, des PBL, etc. Le service de support de Broadcom prend en charge les configurations décrites dans la documentation de DX APM.

Voir aussi : personnaliser

console, station de travail

La *console* est la vue par défaut lors du démarrage de la station de travail. La console contient des tableaux de bord qui affichent des données de performances sous forme de vues graphiques.

Voir aussi : console, station de travail, station de travail

conteneur

Un *conteneur* désigne un environnement d'exécution Java pour des beans entreprise. Un conteneur qui s'exécute sur un serveur EJB (Enterprise JavaBeans) gère le cycle de vie des objets Bean entreprise, coordonne les transactions distribuées et implémente la sécurité des objets.

Voir aussi : transaction

personnaliser

Dans DX APM, le terme *personnaliser* a un sens particulier. *Personnaliser* consiste à programmer une nouvelle forme de surveillance, de création de script, de traitement, de mise en forme d'un module d'extension, etc.

DX APM est hautement personnalisable, mais le service de support de Broadcom ne prend pas en charge les personnalisations apportées aux configurations par défaut. Par exemple, vous pouvez personnaliser l'instrumentation des agents, y compris déployer des PBD personnalisées. Vous pouvez créer des outils de calcul JavaScript ainsi que des scripts shell et EPAgent pour des extensions d'agent. Si nous pensons que des personnalisations entraînent un problème au niveau du produit, nous pouvons vous demander de les supprimer ou de les désactiver. Nous pouvons ensuite vous apporter notre aide. Pour obtenir de l'aide sur une personnalisation DX APM nouvelle ou existante, contactez l'architecte de la solution.

Voir aussi : configurer

tableau de bord

Un *tableau de bord* combine et présente des mesures d'application dans des vues afin de surveiller l'environnement d'application global. Les tableaux de bord fournissent des informations de performances détaillées qui permettent un tri, un diagnostic et une résolution rapides des problèmes pour les applications de production. Dans Team Center, le tableau de bord affiche l'intégrité globale de l'environnement.

Voir aussi : mesure

mesure inactive

Une *mesure inactive* est une mesure sans aucune nouvelle donnée signalée au cours d'une période donnée. La période est configurable.

Voir aussi : mesure dynamique, mesure

composant de visibilité approfondie

Un *composant de visibilité approfondie* est une méthode ou un composant que l'agent détecte et affiche automatiquement sans utiliser de directives ProbeBuilder (ProbeBuilder Directive, PBD). Lorsque l'instrumentation intelligente est activée,

l'agent analyse la complexité des méthodes afin de déterminer les appels et les composants à instrumenter et à afficher comme composants de visibilité approfondie.

analyse différentielle

L'*analyse différentielle* est une approche permettant d'identifier automatiquement les modifications importantes au niveau des performances de vos applications. Les références héritées prédisent les performances normales. L'analyse différentielle recherche un éventuel écart non contrôlé dans le temps de réponse moyen de vos applications frontales et mesures de transaction métier. Un écart non contrôlé se présente sous la forme de pics dans un flux de données normalement stable, un peu comme un sismomètre détecte les tremblements de terre.

planification de détection

La *planification de détection* détermine les éléments à détecter dans la charge utile de l'application Business Payload Analyzer.

attributs ignorés

Dans Business Payload Analyzer, les attributs détectés par le composant BT Listener dans la charge utile de l'application selon la règle de détection sont classés dans la catégorie des attributs ignorés.

Voir : Présentation des attributs Business Payload Analyzer

domaine

Un *domaine* DX APM est une façon de partitionner les agents et la logique de gestion pour définir les informations pouvant être vues par les différents utilisateurs.

réseau double pile

Un *réseau double pile* prend en charge les applications et services IPv4 et IPv6. Cela implique que les hôtes et les routeurs doivent prendre en charge les protocoles IPv4 et IPv6.

L'approche double pile est une manière courante d'introduire le protocole IPv6 dans une architecture IPv4 existante. Cette approche permet aux réseaux de prendre en charge à la fois les protocoles IPv4 et IPv6 pendant la période de transition, en attendant que les applications et services IPv6 deviennent largement disponibles.

DX APM

DX APM est une solution de gestion des performances des applications à l'échelle de l'entreprise qui vous permet d'effectuer les opérations suivantes.

- Surveiller des applications complexes dans des environnements de production 24 heures sur 24, 7 jours sur 7.
- Détecter des problèmes avant qu'ils n'affectent vos clients.
- Résoudre ces problèmes rapidement et de manière collaborative.

Voir aussi : agent, gestionnaire d'entreprise, mesure

propriété dynamique

Une *propriété* dynamique dans les fichiers de configuration DX APM (le fichier `IntroscopeAgent.profile`, par exemple) est déployée dès que le fichier de configuration est enregistré. Il est inutile de redémarrer l'application ou les serveurs d'application pour que la modification prenne effet.

Activation d'application

Les données d'une application sont envoyées au Business Payload Analyzer uniquement lorsque l'application est activée. Pour activer une application, définissez une planification de détection, qui détermine les éléments à détecter dans la charge utile de l'application.

Voir : Présentation des attributs Business Payload Analyzer

extension

Une *extension* DX APM est un code programme (fichier JAR) qui étend les fonctionnalités de base du gestionnaire d'entreprise ou d'un agent.

Voir aussi : gestionnaire d'entreprise, agent

Gestionnaire d'entreprise

Le *gestionnaire d'entreprise* stocke et regroupe les mesures de performances des applications, comme le temps de réponse, la bande passante et l'allocation de mémoire. De nombreux agents, répartis dans toute l'entreprise, collectent et transmettent les mesures d'environnement et d'application au gestionnaire d'entreprise.

Voir aussi : collecteur, gestionnaire des gestionnaires (Manager of Managers, MoM)

point d'entrée

Lorsque l'instrumentation intelligente et la détection automatique de points d'entrée sont activées, DX APM surveille automatiquement les threads qui sont impliqués dans les transactions d'appel de socket client. Les *points d'entrée* sont les points de début de transaction. Les points d'entrée s'affichent dans l'arborescence centrée sur l'agent et les traces de transaction.

Voir aussi : instrumentation intelligente, composant d'arrière-plan automatique

Environmental Performance Agent (EPAgent, EPA)

L'*agent de performance environnementale* (*Environmental Performance Agent, agent EP*) est une version modifiée de l'agent qui permet d'intégrer dans DX APM des données de mesures à partir de sources génériques et non-Java. L'agent EP utilise des scripts simples qui permettent à l'agent de surveiller pratiquement n'importe quel type de sous-système d'application ayant un impact sur les performances. Par exemple, les serveurs d'annuaire, les systèmes d'exploitation, les intergiciels de messagerie et les serveurs de transactions.

Voir aussi : agent, modules d'extension avec état, modules d'extension sans état

cliché d'erreur

ErrorDetector génère un *cliché d'erreur* qui affiche des informations détaillées sur les événements en cours lors de la survenue d'une erreur. Les données sur les clichés d'erreur sont stockées dans la base de données des événements de transaction.

Voir aussi : ErrorDetector

ErrorDetector

ErrorDetector permet au personnel de support des applications de détecter et de diagnostiquer la cause d'erreurs sérieuses susceptibles d'empêcher les utilisateurs de finaliser des transactions Web.

Des erreurs "sérieuses" prédéfinies basées sur les informations contenues dans les spécifications PHP, J2EE et .NET incluent les erreurs suivantes :

- Erreurs HTTP (par exemple, 404 et 500)
- Erreurs d'instruction SQL
- Erreurs de connectivité réseau (erreurs de délai d'expiration)
- Erreurs d'arrière-plan (par exemple, impossible d'envoyer un message via JMS ou impossible d'écrire un message dans la file d'attente).

Voir aussi : cliché d'erreur

événement

Un *événement* DX APM est une action pour laquelle des agents capturent des mesures. Exemples d'événements : traces de transaction, erreurs et blocages.

Voir aussi : ErrorDetector, mesure, blocage, trace de transaction

extension

Les *extensions* sont des applications DX APM qui étendent les fonctionnalités de surveillance des données de l'agent. Les extensions s'intègrent aisément aux composants DX APM par défaut pour offrir une meilleure visibilité sur votre environnement et vos applications surveillées.

Certaines extensions exigent un redémarrage de l'application, d'autres pas. Vous pouvez activer les extensions qui sont fournies avec DX APM.

Federal Information Processing Standards (FIPS)

Les *Federal Information Processing Standards (FIPS)* sont des normes publiques développées par le gouvernement fédéral américain pour être utilisées par toutes les agences gouvernementales non militaires et les entrepreneurs gouvernementaux. De nombreuses normes FIPS sont des versions modifiées des normes utilisées dans le secteur plus vaste des logiciels.

La publication FIPS 140-2, "Security Requirements for Cryptographic Modules" spécifie la norme de sécurité pour les bibliothèques cryptographiques. Cette publication spécifie les algorithmes que les produits logiciels doivent utiliser pour le chiffrement. Le chiffrement affecte le stockage et la vérification des mots de passe. Il affecte aussi la communication de toutes les données sensibles entre les composants d'un produit et entre les produits.

composant frontal

Un *composant frontal* est le composant d'une application qui gère en premier une transaction entrante. Dans les applications J2EE les plus courantes, ce composant est un servlet ou une JSP. Dans certaines instances Java, il peut s'agir d'un EJB ou autre composant. DX APM identifie automatiquement les servlets et JSP comme des composants frontaux, mais pas les autres composants. Pour marquer explicitement un composant comme frontal, utilisez l'outil de suivi `FrontendMarker`.

Voir aussi : composant d'arrière-plan

pile graphique

Dans une trace de transaction, la *pile graphique* est la représentation de l'ordre des transactions des composants de haut en bas. La pile graphique ressemble à un gâteau de mariage à l'envers. Affichez la pile graphique dans la visionneuse des traces de transaction.

Voir aussi : trace de transaction, outil de suivi de transaction

GUID

Le *GUID* (globally unique identifier ou identificateur unique global) est une clé unique produite par `ServletHeaderDecorator`. La clé identifie une transaction dans l'application business surveillée. Le GUID est l'information clé qui met en corrélation certaines transactions.

Vous pouvez créer des GUID de plusieurs manières. Généralement, les GUID sont une combinaison de paramètres uniques basés sur un moment spécifique. Par exemple, un GUID peut être une combinaison d'une adresse IP, d'une adresse MAC réseau, d'une date et d'une heure.

Voir aussi : adresse MAC, `ServletHeaderDecorator`

signal d'activité

Un *signal d'activité* est l'intervalle de temps sur la base duquel les mesures sont vérifiées, généralement en secondes.

mesures heuristiques

Les *mesures heuristiques* DX APM servent à évaluer et à signaler le statut. Ce sont des nombres entiers, mais les nombres entiers sont des symboles de statut et ne mesurent rien. La valeur d'une mesure heuristique est déterminée en comparant les mesures actuelles à une référence pour ces mesures.

Vous pouvez définir des alertes en termes de mesures heuristiques plutôt que de seuils fixes. Le fait de définir des alertes à l'aide de mesures heuristiques en déterminant les valeurs normales pour des indicateurs clés de performance (KPI) déplace la charge de travail de l'administrateur APM vers DX APM.

Voir aussi : référence, mesure

propriété masquée

Une *propriété masquée* est une propriété dans un fichier de configuration. La propriété est uniquement disponible lorsque vous l'ajoutez au fichier de configuration. Exemple de fichier de configuration : fichier `IntroscopeAgent.profile` ou fichier `IntroscopeEnterpriseManager.properties`.

HTTPHeaderDecorator

DX APM *HTTPHeaderDecorator* est une extension d'agent qui augmente les en-têtes de réponse HTTP pour les agents .NET.

Voir aussi : GUID `ServletHeaderDecorator`, outil de suivi de transaction

attributs d'identification

Les attributs que vous voulez inclure dans la règle de nommage des transactions métier peuvent être définis comme attributs d'identification. La règle de nommage attribue aux transactions métier un nom unique qui permet de les identifier dans DX APM.

Voir : Présentation des attributs Business Payload Analyzer

composant d'identification

Le *composant d'identification* est le premier composant de transaction dans l'ensemble des composants de transaction. Le composant d'identification identifie de manière unique le début d'une transaction. Un composant d'identification ne doit pas être un composant d'une autre transaction.

NOTE

Une redirection peut apparaître comme le premier composant d'un enregistrement de transaction, mais elle n'est pas le composant d'identification.

Voir aussi : hiérarchie de transaction

transaction d'identification

La *transaction d'identification* est la première transaction dans un ensemble de transactions métier. La transaction d'identification identifie de manière unique le début d'une transaction métier. Une transaction d'identification ne doit pas être une transaction d'une autre transaction métier.

Voir aussi : hiérarchie de transaction

Type d'instance

Le *type d'instance* est une spécification qui définit la mémoire, l'UC, la capacité de stockage et le coût horaire d'une instance dans AWS (Amazon Web Services). Il est possible de concevoir des types d'instance pour des applications standard ou pour des applications exigeantes en termes d'UC ou de mémoire.

instrumenté

Un code d'application est *instrumenté* lorsque ProbeBuilder insère des sondes, dans le code d'octet, pour envoyer des mesures à l'agent.

Voir aussi : agent, AutoProbe, application gérée, ProbeBuilder

Investigator, station de travail

L'arborescence *Investigator* de la station de travail vous permet d'afficher le statut des applications et du système, de rechercher et de parcourir des données de mesures à l'aide d'une structure arborescente. Vous pouvez avoir plusieurs fenêtres Investigator ouvertes en même temps.

Voir aussi : console, station de travail ; station de travail

Agent Java

L'*agent Java* collecte des mesures dans les environnements Java.

port d'écoute

Un *port d'écoute* sert à simplifier l'administration de l'association entre une fabrique de connexion, une destination et un bean axé sur les messages déployé.

mesure dynamique

Une *mesure dynamique* comporte des données signalées activement par un agent spécifique.

Voir aussi : mesure inactive, mesure

temps logique

Le *temps logique* est la mesure du temps nécessaire au code de programme du composant Blame suspect pour se terminer. Ce temps est basé sur les rapports DX APM.

Voir aussi : composant Blame suspect

Adresse MAC

L'*adresse MAC* (Media Access Control) est une adresse matérielle qui identifie de manière unique chaque nœud d'un réseau.

L'adresse MAC peut être utile pendant le processus de résolution des problèmes. Par exemple, lorsque des serveurs Web sont situés derrière un équilibreur de charge qui masque la véritable identité du serveur Web au niveau de l'IP. Par exemple, dans les environnements d'équilibrage de charge Resonate, tous les serveurs Web ont la même adresse IP. Toutefois, l'adresse MAC envoyée dans la réponse peut identifier de manière unique les serveurs.

application gérée

Lorsqu'une application instrumentée est en cours d'exécution, elle est appelée *application gérée*.

Voir aussi : instrumenté

module de gestion

Un *module de gestion* contient un ensemble d'informations de configuration de surveillance. Les modules de gestion sont répertoriés pour chaque domaine et contiennent des éléments. Les éléments sont des objets qui contiennent des données et les organisent avec une logique de surveillance, comme des alertes, des actions et des tableaux de bord.

Voir aussi : tableau de bord, WebView, station de travail

Gestionnaire des gestionnaires (Manager of Managers, MOM)

Le *gestionnaire des gestionnaires* (Manager of Managers, *MOM*) stocke les mesures signalées par plusieurs gestionnaires d'entreprise. La mise en cluster d'un gestionnaire d'entreprise permet à un gestionnaire d'entreprise (le MOM) de gérer d'autres gestionnaires d'entreprise. Chacun des gestionnaires d'entreprise gérés, appelés collecteurs, collecte des mesures d'agent et, à son tour, transmet ces mesures au MOM.

Voir aussi : collecteur, gestionnaire d'entreprise (Enterprise Manager, EM)

carte

Dans Team Center, la *carte* affiche les relations entre les différents composants au sein de l'environnement.

valeur médiane

La *valeur médiane* est une valeur unique représentant une distribution de données. La valeur médiane est préférée à la valeur moyenne comme représentation à chiffre unique d'une distribution lorsque cette dernière n'est pas une distribution normale (courbe en forme de cloche).

clap de mesure

Un *clap de mesure* est une limite, ou clap, du nombre de mesures sur l'agent et le gestionnaire d'entreprise. Un clap de mesure permet d'éviter les pics au niveau du nombre de mesures signalées (explosions de mesures) sur le gestionnaire d'entreprise.

Voir aussi : agent, clap, mesure

explosion de mesures

Une *explosion de mesures* se produit lorsque de nouvelles mesures apparaissent en grandes quantités sur une courte période. Des définitions de mesures mal configurées peuvent entraîner la modification de métadonnées de mesures avec des changements de valeur de mesure, et s'afficher comme de nouvelles mesures. Par exemple, des chaînes de variables dans une mesure SQL. Des propriétés de connexion d'agent mal configurées pour un ensemble de nouveaux agents peuvent engendrer des milliers de nouvelles mesures qui surchargent le gestionnaire d'entreprise. Ces situations peuvent réduire les performances.

Voir aussi : fuite de mesures, agent, clap, mesure

groupement de mesures

Les *groupements de mesures* sont des objets Module de gestion qui enregistrent les informations suivantes :

- L'*expression de l'agent* : une expression régulière dans Perl 5 qui filtre les entrées dans la mesure en spécifiant les données, y compris l'agent.
- L'*expression de mesure* : une expression régulière dans Perl 5 qui spécifie la ressource (la chaîne de dossiers à l'origine de la mesure) et la mesure.
- Le module de gestion auquel appartient le groupement de mesures.

fuite de mesures

Une *fuite de mesures* se produit lorsque, en raison d'une erreur de configuration DX APM, des agents signalent des mesures pendant une période limitée. Ce problème entraîne une accumulation progressive de métadonnées de mesures sans données de mesures associées.

Voir aussi : explosion de mesures, agent, clamp, mesure, DX APM

limitation de mesures

Une *limitation de mesures* stoppe un agent lorsque sa production de mesures devient excessive.

Voir aussi : agent, clamp, mesure

mesure, DX APM

Une *mesure DX APM* est une mesure des performances des applications. Les types de mesures ci-dessous sont disponibles :

- Bande passante : fichier de niveau CLR et JVM et activité de socket
- Simultanéité : nombre d'appels de méthode démarrés, mais non encore terminés
- Nombre : nombre d'appels de méthode à ce jour
- Exception : capture des exceptions
- Mémoire : mémoire allouée à la JVM ou CLR en cours d'utilisation, à des fins de nettoyage de mémoire
- Taux : nombre d'exécutions de méthode par seconde ou intervalle de temps
- Temps de réponse : durée moyenne d'exécution de méthode en millisecondes
- Méthodes bloquées : nombre de méthodes démarrées, mais dont les durées d'appel ont dépassé un seuil
- Journaux système : surveillent les sorties système et d'erreurs système
- Threads : nombre de threads instrumentés

Voir aussi : clamp de mesure, explosion de mesures, limitation de mesures

port en miroir

Un *port en miroir* est une fonctionnalité logicielle de commutateurs et routeurs réseau.

Voir aussi : tap réseau

Basculement MOM

Un *basculement MOM* se produit lorsque le gestionnaire d'entreprise (MOM) est déconnecté ou s'arrête en raison d'une défaillance matérielle ou réseau. Le basculement a lieu lorsque vous avez configuré un deuxième gestionnaire d'entreprise MOM pour assurer la reprise du premier gestionnaire d'entreprise MOM.

Voir aussi : collecteur, gestionnaire d'entreprise (Enterprise Manager, EM), gestionnaire des gestionnaires (Manager of Managers, MoM)

surveiller, moniteur

Les agents *surveillent* les performances Web de bout en bout, les composants Java et leurs dépendances, les composants CLR et leurs dépendances, les connexions aux systèmes d'arrière-plan, et les niveaux des ressources (y compris les logiciels tiers), ainsi que les ressources des serveurs d'applications.

Voir aussi : agent, synchroniser tous les moniteurs

règle de nommage

Les règles de nommage peuvent également être définies sous forme d'une chaîne d'attributs d'identification. La règle de nommage attribuée aux transactions métier un nom unique qui permet de les identifier dans DX APM.

TAP de réseau

Un *TAP de réseau* est un dispositif matériel qui accède directement au câblage de l'infrastructure. Ce dispositif crée des copies des paquets et les transfère à un ou plusieurs destinataires.

Voir aussi : port en miroir

noeud

Un *noeud* est un emplacement où les informations relatives à certaines mesures sont rassemblées, puis affichées dans l'arborescence du Navigateur de mesures. Par exemple, Investigator affiche le noeud des composants d'arrière-plan ou le noeud d'utilisation de l'UC. En développant le noeud, il est possible d'afficher et de rechercher des informations de mesures plus détaillées. Dans Team Center, un noeud représente directement les transactions métier et les composants cumulés ou surveillés dans un contexte topologique.

Voir aussi : Investigator, station de travail, mesure, station de travail

accord sur les niveaux opérationnels (Operating Level Agreement, OLA)

Un *accord sur les niveaux opérationnels (Operating Level Agreement, OLA)* est un contrat entre une organisation informatique et les groupes de support internes. Les termes du contrat dépendent des besoins des parties impliquées. Les OLA sont utilisés pour gérer les engagements de service des groupes informatiques à des fins de conformité.

opportunité

Une *opportunité* est une zone dans un produit, processus, service ou autre système dans lequel un défaut est susceptible de se produire. En général, plus les produits sont complexes, plus les opportunités de défauts sont nombreuses.

Voir aussi : défaut, spécification

réponse partielle

Une *réponse partielle* signifie qu'une réponse complète n'a pas été observée pour un composant spécifique pendant la période configurable attendue (valeur par défaut : 60 secondes).

Voir aussi : réponse manquante

Origine

L'*origine* est le premier composant dans une série de dépendances indiquant des problèmes de performance. Ce composant est à l'origine de la détérioration des performances dans votre environnement d'application. L'origine est probablement la cause première du problème.

valeur de centile

La *valeur de centile* d'une distribution est un nombre dans lequel un pourcentage de la distribution est inférieur ou égal à cette valeur de centile. Par exemple, le 25e centile (également appelé le quartile inférieur) est un nombre tel que 25 pour cent des valeurs de données se situent en dessous de ce nombre.

Voici un autre exemple. Pour un graphique de temps de réponse, le nombre au 95e centile signifie que 95 % des transactions pendant cette période avaient un temps de réponse à ce niveau ou un niveau inférieur.

perspective

Une *perspective* regroupe des composants de manière logique dans l'interface utilisateur selon leurs attributs partagés.

Agent PHP

L'*agent PHP* collecte des mesures dans les applications PHP.

module d'extension

Le *module d'extension* est l'un des composants Business Payload Analyzer. Business Payload Analyzer comprend des modules d'extension pour les serveurs Web suivants :

- Serveur Web Apache (Windows et Linux)
- Serveur Web IIS
- Serveur Web Nginx

règle de confidentialité

Une règle de confidentialité vous permet de masquer les valeurs de champ que vous ne souhaitez pas afficher dans l'interface utilisateur ou stocker dans la base de données. Vous pouvez par exemple masquer les quatre derniers chiffres du numéro de carte de crédit utilisé pour les transactions, ou hacher la description médicale d'un patient à l'aide de l'algorithme unidirectionnel SHA-256. Pour plus d'informations, consultez la section Menu des actions (Actions Menu).

sonde

Une *sonde* mesure des éléments d'information spécifiques sur une application sans modifier la logique métier de l'application. Un agent est installé sur le même ordinateur que l'application Web instrumentée.

Voir aussi : agent, instrumenté, ProbeBuilder

ProbeBuilder

ProbeBuilder exécute le processus d'instrumentation dans lequel des outils de suivi identifient les mesures collectées par un agent à partir d'applications et des machines virtuelles lors de leur exécution. Les outils de suivi sont définis dans les fichiers PBD (ProbeBuilder Directive).

Voir aussi : agent, AutoProbe, fichier PBD (ProbeBuilder Directive)

directive ProbeBuilder (ProbeBuilder Directive, PBD)

Les fichiers *PBD (ProbeBuilder Directive)* indiquent à ProbeBuilder comment ajouter des sondes aux composants PHP, .NET ou Java pour instrumenter l'application. Les temporisateurs et les compteurs sont des exemples de sondes. Les fichiers PBD gèrent les mesures spécifiques que les agents signalent au gestionnaire d'entreprise.

Il est également possible de créer des directives personnalisées pour suivre les classes et méthodes propres à des applications spécifiques.

Voir aussi : AutoProbe, gestionnaire d'entreprise (EM), ProbeBuilder, listes ProbeBuilder (PBL)

listes ProbeBuilder (ProbeBuilder Lists, PBL)

Un fichier *PBL* (*ProbeBuilder List*) contient une liste de plusieurs fichiers PBD. Plusieurs fichiers PBL peuvent faire référence aux mêmes fichiers PBD.

Voir aussi : AutoProbe, ProbeBuilder, fichier PBD (ProbeBuilder Directive)

ProbeBuilding, dynamique

La fonction *ProbeBuilding dynamique* permet d'apporter des corrections aux fichiers PBD ou de modifier les niveaux de collecte de données pendant le tri sans interrompre le service d'application.

temps de traitement

Dans App Synthetic Monitor, le *temps de traitement* est la période suivant l'envoi de la requête HTTP pendant laquelle l'outil de surveillance attend les premiers octets du résultat.

ServletHeaderDecorator

DX APM *ServletHeaderDecorator* augmente les en-têtes de réponse HTTP des servlets pour les agents Java.

Le GUID est utilisé comme identifiant des transactions. *ServletHeaderDecorator* est une extension d'agent.

Voir aussi : GUID, outil de suivi de transaction

SiteMinder

DX APM *SiteMinder* est une application qui propose des fonctionnalités de sécurité comme l'authentification unique et le contrôle centralisé des accès des utilisateurs aux applications Web.

instrumentation intelligente

L'*instrumentation intelligente* est une méthode utilisée par DX APM pour instrumenter des applications. Cette méthode utilise des outils de suivi hautement optimisés et à temps système réduit. Les outils de suivi permettent aux agents de découvrir et d'instrumenter automatiquement d'autres méthodes pour fournir des composants de visibilité approfondie sans avoir recours aux directives ProbeBuilder (PBD). L'instrumentation intelligente propose également un suivi automatique des transactions.

Voir aussi : trace de transaction automatique, composants de visibilité approfondie

base de données SmartStor

La *base de données SmartStor* est une base de données non relationnelle qui enregistre toutes les données liées aux performances des applications (mesures d'agent) en permanence. Cette base de données permet aux utilisateurs d'analyser des données historiques, d'identifier les causes principales de l'indisponibilité des applications ou de réaliser des analyses de capacité, sans avoir besoin d'une base de données externe.

SmartStor est activée par défaut lors de l'installation de DX APM. Les données SmartStor sont configurées pour devenir obsolètes au fil du temps, pour éviter que le référentiel de données ne devienne trop volumineux. Il existe plusieurs fichiers de données et leur nombre augmente au fur et à mesure que de nouvelles données sont générées.

Voir aussi : base de données APM, base de données d'événements de transaction

spécification

Une *spécification* est une exigence pour une transaction ou un composant de transaction. Si une transaction ou un composant ne respecte pas l'exigence établie dans la spécification associée, elle/il est défini(e) comme un défaut. Par exemple, un défaut de lenteur peut être défini comme tout temps de transaction supérieur à 5,00 secondes.

Voir aussi : défaut, limite de spécification supérieure (upper specification limit)

blocage

Un *blocage* DX APM fait généralement référence à des méthodes qui ont démarré, mais dont les durées d'appel ont dépassé un seuil.

Voir aussi : mesure

bulle de démarrage

Une *bulle de démarrage* est la période temporaire durant laquelle le système enregistre une demande en ressources importante susceptible d'affecter des éléments autres que le signalement de mesures DX APM. Pendant la bulle de démarrage, votre application instrumentée risque de ne plus répondre.

Il se peut également que cela affecte d'autres composants partageant des ressources avec l'application instrumentée ou présents dans le même environnement. La bulle de démarrage peut se manifester avec l'agent .NET lors du démarrage.

Voir aussi : agent .NET

modules d'extension avec état

Les *modules d'extension avec état* sont en principe des scripts présentant un temps important d'exécution (notamment les démons). Les modules d'extension avec état démarrent en même temps que l'agent de performance environnementale (agent EP) et s'exécutent de manière continue, renvoyant des données dans DX APM via le canal de sortie standard du module d'extension. Lorsqu'un module d'extension avec état se termine, EPA le relance.

Voir aussi : Environmental Performance Agent (EPAgent, EPA), modules d'extension sans état

modules d'extension sans état

Les *modules d'extension sans état* sont conçus pour s'exécuter selon une planification récurrente et sont configurés avec la fréquence (spécifiée en tant que délai entre chaque exécution) à laquelle ils doivent être exécutés. Les modules d'extension sans état sont en principe des scripts s'exécutant rapidement, qui collectent simplement des données, les envoient à l'agent EPA via le canal de sortie standard et se ferment. L'agent EPA n'effectue aucune vérification spéciale pour garantir l'exécution d'une seule instance d'un module d'extension à la fois. Les développeurs de modules d'extension doivent donc concevoir leurs modules sans état de manière à ce qu'ils s'exécutent dans un délai relativement court.

Voir aussi : Environmental Performance Agent (EPAgent, EPA), modules d'extension avec état

SuperDomain

Le noeud *SuperDomain* contient les mesures pour tous les agents qui rendent compte au gestionnaire d'entreprise auquel la station de travail est connectée ; il inclut tous les domaines et agents définis par l'utilisateur. Ce noeud est uniquement visible pour les utilisateurs disposant d'un accès SuperDomain. Les mesures sont organisées selon une hiérarchie Hôte|Processus|Agent.

mesures de capacité de prise en charge

Les *mesures de capacité de prise en charge* DX APM aident à garantir le bon fonctionnement du gestionnaire d'entreprise proprement dit. Le gestionnaire d'entreprise génère et collecte des mesures à son sujet qui sont utiles pour évaluer son intégrité et déterminer ses performances sous sa charge de travail.

composant Blame d'arrière-plan suspect

Le *composant Blame d'arrière-plan suspect* est la portion la plus spécifique du temps d'arrière-plan qui est identifiée comme étant la cause suspectée du retard d'une transaction lente. Dans DX APM, le composant d'arrière-plan Blame

suspecté apparaît comme le composant d'arrière-plan le plus large, mais pas nécessairement le plus bas, dans le graphique.

NOTE

Il s'agit du composant d'arrière-plan *le plus bas et le plus lent*, et non du composant d'arrière-plan *le plus lent et le plus bas* dans les graphiques DX APM.

Le composant d'arrière-plan Blame suspect est identifié en considérant le composant d'arrière-plan le plus bas qui prend plus d'un quart du total du temps d'arrière-plan pour s'exécuter.

composant Blame suspect

Le *composant Blame suspect* est la portion la plus spécifique de la logique (ou du code de programme) qui est identifiée comme étant la cause suspectée du retard d'une transaction lente. Dans DX APM, le composant Blame suspecté apparaît comme le composant le plus large, mais pas nécessairement le plus bas, dans le graphique.

NOTE

Il s'agit du composant *le plus bas et le plus lent*, et non du composant *le plus lent et le plus bas* dans les graphiques DX APM.

Le composant Blame suspect est identifié en considérant le composant (non d'arrière-plan) le plus bas qui prend plus d'un quart du total du temps de transaction pour s'exécuter.

mesure de durabilité

Une *mesure de durabilité* fournit des informations sur l'état interne de l'agent plutôt que sur l'application que l'agent surveille. Ces données vous permettent d'examiner le comportement de l'agent.

Team Center

Team Center est une interface utilisateur qui présente un environnement d'application.

délai avant la première réponse

Le *délai avant la première réponse* correspond au temps écoulé entre le *dernier* paquet de la demande et le premier paquet de la réponse pour le composant.

Le délai avant la première réponse varie en fonction du type de défaut suivi :

- Défaut de composant - Le délai avant la première réponse pour ce composant
- Défaut de transaction - Le délai avant la première réponse pour le composant d'identification de la transaction
- Défaut de transaction métier - Le délai avant la première réponse pour le composant d'identification de la transaction d'identification

NOTE

Ce paramètre peut être modifié pour désigner le temps écoulé entre le *premier* paquet de la demande et le premier paquet de la réponse. Si ce paramètre doit déterminer la latence du réseau entrant, contactez le support Broadcom.

La modification de ce paramètre affecte uniquement les nouvelles données. (Les valeurs des données existantes sont basées sur le paramètre de délai avant la première réponse qui était en vigueur au moment de la collecte des données).

chronologie

Dans l'interface utilisateur, la *Chronologie* permet de passer du moment actuel à un point dans le passé afin d'afficher les événements de statut qui se sont produits auparavant. La fonction de chronologie permet de remonter jusqu'à l'origine d'un problème.

transaction

Une *transaction* DX APM désigne l'appel et le traitement d'un service. Il s'agit d'un cycle de traitement complet, où le contexte d'application définit la notion d'achèvement :

- Dans le contexte d'une application Web, il s'agit de l'appel et du traitement d'une URL envoyée à partir d'un navigateur Web.
- Dans le contexte d'un service Web, il s'agit de l'appel et du traitement d'un message SOAP à partir d'un client de services Web.

DX APM peut capturer des transactions et inclure des détails sur la demande envoyée au service ainsi que sur le traitement du service (par exemple, des appels vers une base de données SQL).

Une transaction comprend généralement un composant HTML, suivi éventuellement de sous-composants (par exemple, feuille de style CSS, fichiers JavaScript JS et images JPG). Chaque transaction comporte un composant de transaction d'identification.

Une seule action d'utilisateur peut entraîner une ou plusieurs transactions, qui sont encapsulées dans une transaction métier.

Voir aussi : hiérarchie de transaction

base de données d'événements de transaction

La *base de données d'événements de transaction* contient les données détaillées des transactions. Ces données incluent les traces des transactions, les blocages et les données collectées à partir d'événements déclenchés, tels que les clics d'erreur.

La base de données d'événements de transaction se trouve généralement dans le répertoire des traces et comprend plusieurs fichiers. Un fichier est créé pour chaque jour ; les données sont conservées pour le nombre de jours spécifié.

Voir également : base de données APM, base de données SmartStor, transaction, outil de suivi de transaction

hiérarchie de transaction

Les mesures et informations de DX APM sont organisées selon une *hiérarchie de transaction*. Cette hiérarchie est une façon de convertir les transactions et services d'entreprise en éléments HTTP techniques permettant de créer l'expérience client.

La hiérarchie de transaction de DX APM est la suivante.

Une application business est un programme logiciel qui automatise un service d'entreprise. Chaque transaction (qui utilise un service d'entreprise, une transaction métier et enfin une transaction) est associée à une application business.

Exemple : Siebel

Exemple : Avitek

Un service d'entreprise est un groupe arbitraire de transactions métier.

Exemple : Avitek Financial (inclut les achats, les ventes et les requêtes)

Exemple : Siebel Call Center (inclut la connexion et d'autres transactions métier Siebel)

Une transaction métier est un ensemble de transactions qui représente une seule action utilisateur.

Exemple : Ensemble Achat (peut inclure plusieurs transactions associées à un achat)

Exemple : Ensemble Vente (peut inclure plusieurs transactions associées à une vente)

Une transaction est un ensemble de composants de transaction qui représente généralement une demande auprès du serveur d'applications.

Exemple : Achat (transaction d'achat proprement dite)

Exemple : Demande de prix d'achat (requête associée à un achat)

Un composant de transaction métier est utilisé dans DX APM comme alternative à l'ensemble des transactions et des composants de transaction appartenant à une transaction métier. Le composant de transaction métier correspond au composant de transaction d'identification de la transaction d'identification en fonction de laquelle il est nommé.

Exemple : Soumettre l'achat (l'élément d'identification pour la transaction et la transaction d'identification de la transaction métier)

Un composant de transaction est un élément de bas niveau qui représente une paire requête/réponse HTTP.

Exemple : Soumission d'achat (l'élément d'identification de la transaction qui peut être JavaScript)

Exemple : main.css (un élément de la transaction qui n'est pas d'identification, mais est critique)

Un paramètre de transaction est l'élément du niveau le plus bas dans la hiérarchie ; il s'agit d'une paire nom/valeur HTTP.

Exemple : URL Path=/dir/file.html (l'élément d'identification du composant)

Exemple : Cookie=JSESSIONID

paramètre de transaction

Un *paramètre de transaction* est une paire nom/valeur HTTP, composée d'un type, d'un nom et d'un modèle.

Comme exemples, citons les URL, les cookies ainsi que les paramètres d'interrogation et POST (par exemple : URL Host=www.company.com).

Voir aussi : hiérarchie de transaction

La *taille de transaction* est la taille (en octets) du trafic HTTP observé pour une transaction. La taille inclut l'en-tête HTTP ainsi que les demandes et les réponses HTTP. Elle n'inclut pas les en-têtes Ethernet, IP et TCP.

trace de transaction

Une *trace de transaction* désigne la sortie de l'outil de suivi de transaction. La trace contient une liste des composants appelés pendant une transaction et leur durée correspondante.

Voir aussi : outil de suivi de transaction

durée de trace de transaction

La *durée de trace de transaction* est le temps d'exécution d'une *session de suivi de transaction*. La durée maximale de session de suivi de transaction est une limite de temps. La valeur par défaut est de 30 minutes.

Voir aussi : outil de suivi de transaction

seuil de temps de trace de transaction

Le *seuil de temps de trace de transaction* est la limite de temps d'exécution d'une *transaction*. Lorsqu'une trace de transaction est en cours d'exécution, toutes les transactions qui ne se terminent pas avant d'atteindre le seuil de temps sont suivies.

Le seuil de temps de trace de transaction correspond à un pourcentage qui se base sur la spécification de défaut de lenteur. Par exemple, la spécification de défaut de lenteur est définie sur 8,00 secondes et le seuil de temps de trace de transaction est configuré sur 25 %. Toutes les transactions avec un composant Blame suspect (temps logique) supérieur à 2,00 secondes sont suivies.

Voir aussi : temps logique, composant Blame suspect, outil de suivi de transaction

Outil de suivi de transaction

L'*outil de suivi de transaction* surveille l'activité des différentes transactions lorsqu'elles circulent au niveau des éléments suivants :

- Machine virtuelle Java (JVM) unique
- Plate-forme virtuelle CLR (Common Language Runtime) dans le cas de .NET

L'outil de suivi de transaction réduit le temps requis pour identifier les composants posant problème dans une transaction. Il permet d'effectuer le suivi de l'activité de transaction au niveau des composants.

temps de transfert

Dans App Synthetic Monitor, le *temps de transfert* est le délai nécessaire pour traiter les données de réponse HTTP.

volume de transactions

Le *volume de transactions* est la somme des tailles de toutes les transactions pour une période spécifiée.

tri

Le *tri* désigne le processus assurant les tâches suivantes :

1. Collecte des informations relatives à un problème.
2. Détermination de la sévérité du problème.
3. Affectation du problème à la personne qui pourra le corriger le plus rapidement. La personne qui gère cette étape d'analyse du problème peut être désignée sous le terme de responsable du tri.

univers

Un *univers* est un groupe pertinent de composants qui est adapté aux besoins d'un utilisateur ou d'un groupe spécifique dans l'interface utilisateur.

limite de spécification supérieure (Upper Specification Limit, USL)

La *limite de spécification supérieure* (ou USL) est une valeur numérique définissant la valeur la plus élevée acceptable pour la caractéristique. Par exemple, une USL peut définir le débit de transaction le plus élevé acceptable.

Ensemble de règles de correspondance d'URL

L'ensemble de règles de correspondance d'URL est l'URL à surveiller.

base de données des écarts

La *base de données des écarts* DX APM stocke les états de profil de prévision et d'écart les plus récents pour les mesures évaluées par l'analyse différentielle. Ces profils servent d'entrées pour le moteur de règles interne. Le moteur génère ensuite une intensité d'écart pour les mesures qui s'affichent dans la carte d'analyse différentielle de WebView.

Voir aussi : base de données APM, mesures heuristiques, base de données SmartStor, base de données d'événements de transaction

WebView

WebView présente les arborescences Investigator et les tableaux de bord personnalisables dans une fenêtre de navigateur. WebView permet de consulter les informations stratégiques sans passer par la station de travail. Voir aussi : démarrage Web de la station de travail

station de travail

La *station de travail* vous permet de contrôler DX APM et d'accéder aux mesures de performances. Sur la station de travail, vous pouvez effectuer les actions suivantes et bien d'autres encore :

- Définir des alertes pour des mesures ou des groupes de mesures logiques spécifiques
- Afficher les mesures de performances
- Personnaliser les vues de votre propre environnement

Voir aussi : démarrage Web de la station de travail

démarrage Web de la station de travail

La *station de travail WebStart* utilise Java Web Start pour démarrer la station de travail.

En tant qu'administrateur, vous pouvez créer et configurer des alertes et des actions dans Team Center pour surveiller les performances. Team Center fournit les alertes suivantes :

- Alerte simple
- Alertes récapitulatives

Pour plus d'informations sur la création, la mise à jour, la suppression et la configuration d'alertes simples, consultez la section [Création et configuration d'alertes simples dans Team Center](#).

Avis relatifs aux logiciels tiers SaaS

Cette section contient des contrats de licence de logiciels tiers pour les applications ajoutées/inclues dans la version actuelle de DX APM. Cliquez [ici](#) pour télécharger ces contrats.

Implémentation d'agents

Découvrez la procédure d'implémentation d'un ou de plusieurs agents en fonction des environnements que vous surveillez.

L'*agent* est un composant de collecte de données. Ce composant collecte des informations de performances détaillées sur les applications et l'environnement informatique au fur et à mesure que des transactions sont exécutées. Une application Web qui signale des mesures à un agent est dite instrumentée. Une fois l'application Web instrumentée, l'agent collecte les données et les signale au gestionnaire d'entreprise. Puis, le gestionnaire d'entreprise traite et stocke les données à des fins de génération de rapports en temps réel et historiques. Vous pouvez alors afficher et utiliser les données collectées pour créer des alertes ou intervenir. Vous pouvez modifier la surveillance par défaut pour obtenir l'équilibre requis entre visibilité et performances. Une *extension d'agent* est un code de programme qui étend la fonctionnalité de base de l'agent.

Pour plus d'informations sur l'agent, reportez-vous à la section [Agents DX APM](#).

Utilisez les liens suivants pour accéder à la documentation de certains agents clés :

- [Agent Java](#)
- [Agent .NET/.NET Core](#)
- [Agent Infrastructure](#)
- [Business Payload Analyzer](#)
- [Agent Node.js](#)

Configuration de votre environnement de surveillance

Votre environnement de surveillance vous permet d'identifier, de mesurer et d'évaluer les performances d'une application. Vous pouvez effectuer des tâches pour configurer votre environnement de surveillance afin de répondre à vos besoins.

Création de favoris de paramètres

Vous pouvez marquer des mosaïques dans la page **Paramètres** comme favorites. Cliquez sur l'icône en forme d'épingle dans la mosaïque pour ajouter le paramètre en tant que favori dans le volet de navigation gauche. Pour supprimer le paramètre en tant que favori, cliquez sur l'icône **Supprimer** du paramètre dans le volet de navigation gauche.

Configurations disponibles

Les configurations suivantes sont disponibles dans la page **Paramètres** :

Pour...	Lisez ces informations...
Configuration des paramètres généraux	<ul style="list-style-type: none"> • Configuration et téléchargement d'un package d'agent pour DX APM • Organisation des composants à l'aide de perspectives • Configuration des univers • Définition du mode de surveillance de l'environnement à l'aide de règles d'attribut • Sécurité • Notifications • Téléchargements <ul style="list-style-type: none"> — Télécharger la station de travail — Télécharger le proxy cloud — Outil d'importation d'agent • Remarque : Vous pouvez accéder à l'outil d'importation d'agent uniquement en tant qu'administrateur principal. • Règles de suppression des traces pour le masquage des données sensibles
Configuration des paramètres du module de gestion	<ul style="list-style-type: none"> • Création et utilisation des modules de gestion • Configuration des groupements de mesures dans Team Center • Création et configuration d'alertes simples dans Team Center • Création et modification d'outils de calcul
Configuration des intégrations	<ul style="list-style-type: none"> • Business Payload Analyzer • Configuration de WebView (DX APM sur site uniquement) • APM Command Center (Accès administrateur uniquement) <p>Remarque : WebView est uniquement disponible dans DX APM sur site. Dans DX APM sur site, WebView n'est pas activé par défaut. Toutefois, vous pouvez activer WebView pour des clients hébergés spécifiques lors de la création de client hébergé. Vous pouvez également activer WebView ultérieurement pour tout client hébergé déjà créé. Pour plus d'informations sur l'activation de WebView, reportez-vous à la section Services de client hébergé. L'accès à WebView et à APM Command Center ouvre un nouvel onglet.</p>
Configuration d'autres paramètres	Les agents sont téléchargés à partir de Team Center à partir de la configuration avancée.

Configurations d'environnement supplémentaires

Outre les configurations disponibles dans la page **Paramètres**, vous pouvez effectuer les tâches suivantes pour configurer votre environnement.

- [Création de notifications pour les alertes](#)
- [Configuration de notifications par courriel pour les alertes](#)
- [Configuration de la vue Expérience](#)
- [Ajustement de la surveillance des alertes](#)
- [Configuration de la station de travail](#)
- [Recommandations de dimensionnement de Docker Monitor](#)

Votre environnement de surveillance vous permet d'identifier, de mesurer et d'évaluer les performances d'une application.

Pour plus d'informations sur les tâches que vous pouvez effectuer pour configurer votre environnement de surveillance en fonction de vos besoins, reportez-vous à la section [Configuration de votre environnement de surveillance](#).

Rôles et privilèges pris en charge

Sur la plate-forme DX, les rôles suivants sont pris en charge.

- **Administrateur de clients hébergés**
- **Utilisateur avancé**
- **Utilisateur**

Dans DX APM, ces mêmes rôles sont mappés comme suit :

- Administrateur de clients hébergés → **administrateur APM**
- Utilisateur avancé → **utilisateur APM**
- Utilisateur → **utilisateur APM**

Droits et rôles dans DX APM

Les vues dans Team Center et dans les autres interfaces utilisateur possèdent des niveaux d'accès différents pour chaque rôle.

- [Vue Expérience \(EV\)](#)
- [Vue Agent \(AV\)](#)
- [Perspective](#)
- [Attributs personnalisés](#)
- [Univers](#)
- [Règles](#)
- [Agents](#)
- [Sécurité](#)
- [Alertes](#)
- [Notification](#)
- [Modules de gestion](#)
- [Groupements de mesures et calculateurs](#)
- [Outils de calcul JavaScript](#)
- [Téléchargements](#)
- [AXA dans la boîte de dialogue de téléchargement d'agent](#)
- [Page Paramètres](#)

Vue Expérience (EV)

Action	Administrateur	Utilisateur	Utilisateur avancé
Modifier la position	Oui	Oui	Oui
Ajouter une EV	Oui	Oui	Oui
Définir une EV comme globale	Oui	Non	Non
Modifier une EV	Oui	Oui	Oui
Supprimer une EV	Oui	Oui	Oui
Modifier une EV globale	Oui	Non	Non
Supprimer une EV globale	Oui	Non	Non

Vue Agent (AV)

Action	Administrateur	Utilisateur	Utilisateur avancé
Ajouter une AV	Oui	Oui	Oui
Définir une AV comme globale	Oui	Non	Non
Modifier une AV	Oui	Oui	Oui
Supprimer une AV	Oui	Oui	Oui
Modifier une AV globale	Oui	Non	Non
Supprimer une AV globale	Oui	Non	Non

Perspective

Action	Administrateur	Utilisateur	Utilisateur avancé
Créer une perspective	Oui	Oui	Oui
Modifier une perspective	Oui	Oui	Oui
Définir une perspective comme globale	Oui	Non	Non
Définir une perspective par défaut	Oui	Non	Non
Supprimer une perspective	Oui	Oui	Oui
Personnaliser une perspective	Non	Oui	Oui

Attributs personnalisés

Action	Administrateur	Utilisateur	Utilisateur avancé
Créer	Oui	Non	Oui
Supprimer	Oui	Non	Oui
Modifier	Oui	Non	Oui

Univers

Action	Administrateur	Utilisateur	Utilisateur avancé
Créer un univers	Oui	Non	Non
Renommer un univers	Oui	Non	Non
Modifier la liste des utilisateurs	Oui	Non	Non
Supprimer un univers	Oui	Non	Non

Règles

Action	Administrateur	Utilisateur	Utilisateur avancé
Créer des règles	Oui	Non	Non
Supprimer des règles	Oui	Non	Non
Créer des règles d'entreprise	Oui	Non	Non
Supprimer les règles d'entreprise	Oui	Non	Non
Dupliquer	Oui	Non	Non
Charger des règles	Oui	Non	Non

Agents

Action	Administrateur	Utilisateur	Utilisateur avancé
Télécharger un agent	Oui	Non (Peut être contrôlé par l'administrateur dans Paramètres)	Oui
Effectuer le suivi de tous les agents	Oui	Non	Oui
Effectuer le suivi d'un agent particulier	Oui	Non	Oui
Afficher les détails de la connexion d'agent	Oui	Oui, mais (Le bouton Générer un jeton dépend de la visibilité de la boîte de dialogue de téléchargement d'agent)	Oui

Sécurité

Action	Administrateur	Utilisateur	Utilisateur avancé
Créer un jeton d'API	Oui	Oui	Oui
Générer un jeton d'agent	Oui	Oui : si la boîte de dialogue de téléchargement d'agent est visible. (peut être contrôlé par l'administrateur dans Paramètres)	Oui

Action	Administrateur	Utilisateur	Utilisateur avancé
Créer un jeton de système	Oui	Non	Non
Invalider un jeton	Oui	Le sien	Le sien
Renommer	Oui	Le sien	Le sien
Définir l'expiration	Oui	Le sien	Le sien

Alertes

Action	Administrateur	Utilisateur	Utilisateur avancé
Lire une alerte	Oui	Oui	Oui
Créer une alerte	Oui	Non	Non*
Supprimer une alerte	Oui	Non	Non*
Activer/Désactiver une alerte	Oui	Non	Non*
Modifier une alerte	Oui	Non	Oui

Notification

Action	Administrateur	Utilisateur	Utilisateur avancé
Read	Oui	Oui	Oui
Créer une notification	Oui	Non	Non

Modules de gestion

Action	Administrateur	Utilisateur	Utilisateur avancé
Read	Oui	Oui	Oui
Créer	Oui	Non*	Non*
Modifier	Oui	Non*	Non*
Supprimer	Oui	Non*	Non*

Groupelements de mesures et calculateurs

Action	Administrateur	Utilisateur	Utilisateur avancé
Read	Oui	Oui	Oui
Créer	Oui	Non*	Non*
Supprimer	Oui	Non*	Non*
Modifier	Oui	Non*	Non*

Outils de calcul JavaScript

Action	Administrateur	Utilisateur	Utilisateur avancé
Read	Oui	Oui	Oui
Créer	Oui	Non	Non
Modifier	Oui	Non	Non
Supprimer	Oui	Non	Non

Téléchargements

Action	Administrateur	Utilisateur	Utilisateur avancé
Accéder à la page de téléchargement	Oui	Oui	Oui

AXA dans la boîte de dialogue de téléchargement d'agent

Action	Administrateur	Utilisateur	Utilisateur avancé
Créer une application AXA (dans la boîte de dialogue de téléchargement d'agent)	Oui	Non	Oui

Page Paramètres

Action	Administrateur	Utilisateur	Utilisateur avancé
Accès au centre de commande (vignette ACC)	Oui	Non	Oui

* Ce privilège est le privilège par défaut. Les utilisateurs et les groupes peuvent obtenir des privilèges à l'aide du module de sécurité de l'univers.

Informations complémentaires : [Configuration des univers](#).

La plate-forme DX prend en charge les rôles suivants :

- Administrateur de clients hébergés
- Utilisateur avancé
- Utilisateur

Pour plus d'informations sur les rôles DX APM et leurs privilèges, reportez-vous à la section [Rôles et privilèges pris en charge](#).

Génération d'un jeton de sécurité

Les jetons de sécurité servent à authentifier les demandes et à accorder les autorisations pour les agents. A l'aide des paramètres de **Sécurité**, vous pouvez générer des jetons hors ligne qui n'expirent jamais. Ces jetons sont utilisés pour accéder aux API publiques. Vous pouvez également générer des jetons pour autoriser des agents ou des clients hébergés.

IMPORTANT

La génération de jetons de sécurité est une tâche réservée aux administrateurs. Vous devez être un administrateur principal pour générer le jeton de sécurité. Si vous êtes un client hébergé, contactez l'équipe Broadcom SaaS chargée des opérations pour obtenir un jeton de sécurité.

Génération d'un jeton

Procédez comme suit :

1. Connectez-vous à Team Center et cliquez sur **Paramètres**, puis sur la mosaïque **Sécurité**.
2. Cliquez sur **Générer un nouveau jeton**.
La boîte de dialogue **Nouveau jeton de sécurité d'API** s'affiche.
3. Définissez les informations suivantes :
 - **Etiquette** : nom du jeton de sécurité.
 - Sélectionnez le type de jeton de sécurité :
 - **Agent** : jeton permettant d'autoriser un agent.

NOTE

Les informations d'expiration d'un jeton d'agent sont définies à l'intérieur du jeton. Par conséquent, vous ne pouvez pas modifier l'expiration du jeton une fois que vous l'avez créé.

- **API publique** : jeton permettant d'accéder à une API publique. Vous pouvez définir une date d'expiration pour les jetons de l'API publique ou désactiver l'expiration du jeton.
- **Jeton de client hébergé** : jeton permettant d'accorder l'accès à un client hébergé.

NOTE

Les informations d'expiration d'un jeton de client hébergé sont définies à l'intérieur du jeton. Par conséquent, vous ne pouvez pas modifier l'expiration du jeton une fois que vous l'avez créé.

4. Cliquez sur **Générer un jeton**.
Le système génère un nouveau jeton.

WARNING

Pour des raisons de sécurité, vous ne voyez un jeton qu'une seule fois. Enregistrez le jeton à un emplacement sûr avant de fermer cette boîte de dialogue. Ne communiquez le jeton à aucune personne non autorisée.

Le jeton figure maintenant parmi les autres jetons dans l'onglet **Sécurité**.

Gestion des jetons

Pour chaque jeton, vous pouvez effectuer les actions suivantes :

- **Renommer** : modifier le nom du jeton
- **Révoquer** : retirer l'autorisation aux API ou aux agents
- **Annuler la révocation** : restaurer l'autorisation pour les API ou les agents
- **Définir l'expiration** : pour les API publiques, si vous avez désactivé l'expiration du jeton, puis que vous utilisez l'option **Définir l'expiration**, vous pouvez choisir une date et une heure d'expiration du jeton. Le jeton ne pourra plus être utilisé pour l'autorisation des API publiques au-delà de ces date et heure.

Les jetons de sécurité servent à authentifier les demandes et à accorder les autorisations pour les agents. À l'aide des paramètres de Sécurité, vous pouvez générer des jetons hors ligne qui n'expirent jamais. Ces jetons sont utilisés pour accéder aux API publiques. Vous pouvez également générer des jetons pour autoriser des agents ou des clients hébergés.

Pour plus d'informations sur les jetons de sécurité, consultez la section [Génération d'un jeton de sécurité](#).

Création de notifications pour les alertes

DX APM vous permet de créer des notifications d'alertes. Les notifications peuvent transmettre automatiquement les alertes de CA Application Performance Management via des services internes tels que des listes de distribution à des services externes via l'API REST, ou à PagerDuty, une plate-forme de résolution des incidents.

Pour plus d'informations sur la configuration des notifications par courriel, reportez-vous à la section [Configuration de notifications par courriel pour les alertes](#).

La vidéo suivante indique la terminologie et le flux de travaux utilisés ainsi que des exemples de création de notifications pour les alertes.

PagerDuty

PagerDuty analyse les incidents et envoie des notifications directement aux administrateurs IT chargés de la résolution des problèmes. Utilisez l'intégration avec PagerDuty pour surveiller votre système, identifier les événements critiques via un chemin défini, réagir rapidement et réduire au maximum le temps d'indisponibilité de votre système d'exploitation. Pour plus d'informations sur les fonctionnalités de PagerDuty, rendez-vous sur la page <https://www.pagerduty.com>.

Pour travailler efficacement dans les deux systèmes, suivez ces règles :

- Une alerte dans DX APM déclenche un incident dans PagerDuty. PagerDuty transmet alors l'incident sous forme de ticket à un destinataire désigné.
- L'effacement d'une alerte dans DX APM résout l'incident dans PagerDuty. En revanche, la résolution d'un incident dans PagerDuty n'efface pas l'alerte dans CA Application Performance Management.

Flux de travaux des incidents

Lorsqu'une alerte est générée et correspond aux paramètres de configuration de service, DX APM déclenche automatiquement un incident. Les incidents dans PagerDuty contiennent les informations d'alerte suivantes pour identifier le composant affecté :

- `alertStartTime`
- `alertState`
- `alertName`
- `alertId`
- `vertexId`
- `vertexAttributes` (par exemple, type, nom)

PagerDuty traite ensuite les incidents en fonction des stratégies et des paramètres d'utilisateur configurés.

NOTE

L'effacement d'une alerte dans DX APM résout automatiquement un incident dans PagerDuty. Le délai de notification correspond à la durée pendant laquelle DX APM attend avant de déclencher un incident dans PagerDuty. Le délai de notification est utile pour réduire le nombre d'incidents déclenchés par des alertes transitoires.

Création et modification d'une notification PagerDuty

Pour créer une notification PagerDuty, vous devez disposer d'un compte PagerDuty. Ce dernier vous permet de configurer le comportement des notifications et de recevoir un jeton d'utilisateur d'API unique ainsi qu'une clé d'intégration à utiliser avec DX APM.

Procédez comme suit :

1. Connectez-vous à [PagerDuty](#) ou créez un compte.

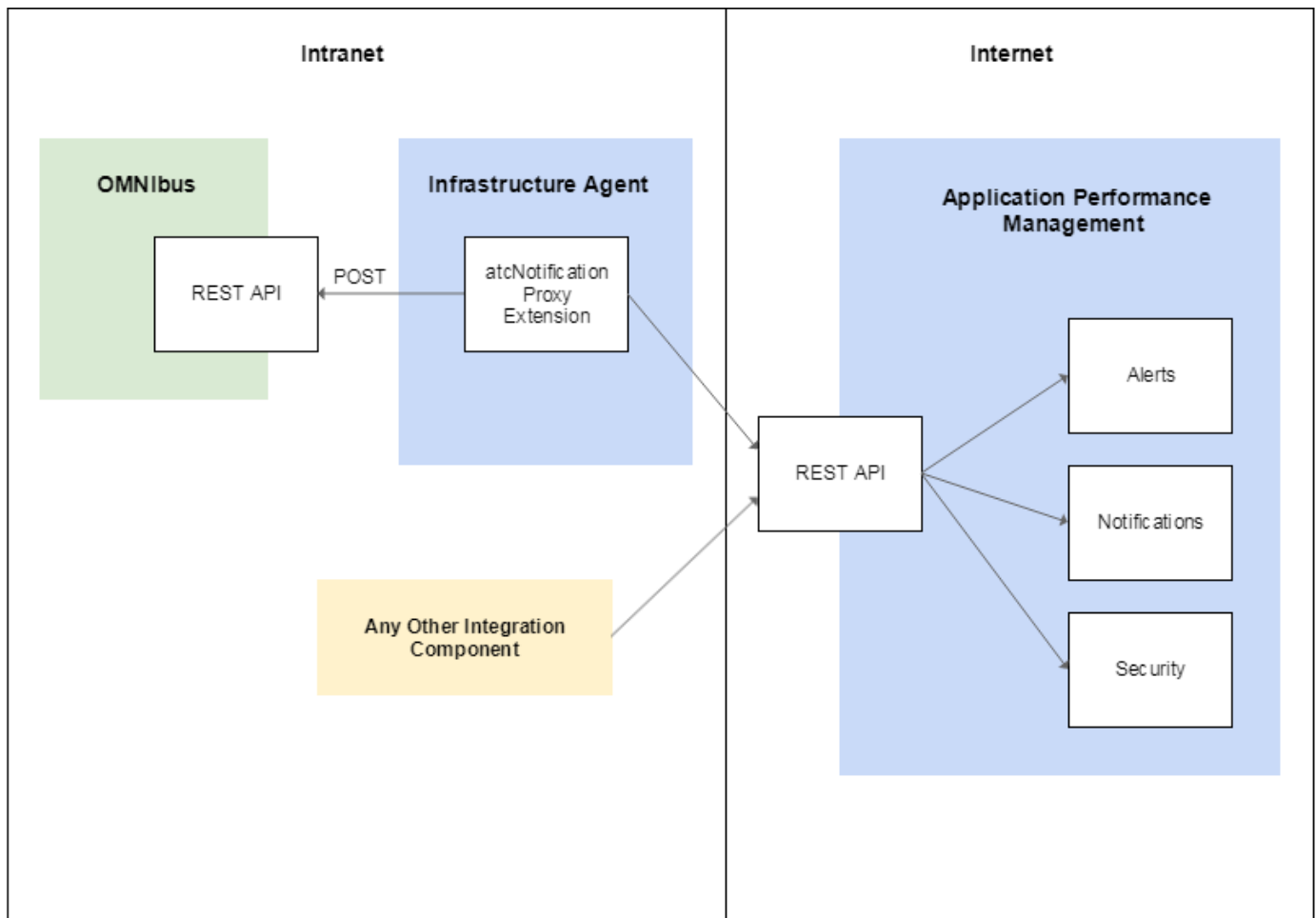
2. Copiez le jeton d'utilisateur d'API et la clé d'intégration à partir de PagerDuty.
3. Dans DX APM, cliquez sur **Notifications**.
4. Cliquez sur **Créer une notification PagerDuty**.
5. Créez un nom de notification.
6. Collez le jeton d'utilisateur d'API et la clé d'intégration de PagerDuty.
7. Sélectionnez la sévérité de la notification.
8. Cliquez sur **Enregistrer**.
9. (Facultatif) Sélectionnez la notification que vous souhaitez modifier et cliquez sur **Modifier**.
10. (Facultatif) Sélectionnez la notification que vous souhaitez supprimer et cliquez sur **Supprimer**.

Vous avez créé et apporté les modifications requises à une notification PagerDuty.

Notifications d'API REST

DX APM vous permet de recevoir des notifications concernant les modifications d'alerte via l'API REST. L'API REST est l'interface de tirage qui permet aux intégrations de s'exécuter derrière les pare-feu de l'entreprise. Utilisez l'API pour intégrer les notifications avec des composants tiers, par exemple divers tableaux de bord. Le diagramme ci-dessous montre l'API REST dans l'infrastructure de CA Application Performance Management.

Figure 1: Notification d'API REST



Création et modification d'une notification d'API REST

Procédez comme suit :

1. Dans DX APM, cliquez sur **Notifications**.
2. Cliquez sur **Créer une notification d'API REST**.
3. Créez un nom de notification.
4. Créez un jeton de proxy unique ou cliquez sur **Générer un jeton**.
5. Cliquez sur **Enregistrer**.
6. (Facultatif) Sélectionnez la notification que vous souhaitez modifier et cliquez sur **Modifier**.
7. (Facultatif) Sélectionnez la notification que vous souhaitez supprimer et cliquez sur **Supprimer**.

Vous avez créé et apporté les modifications requises à une notification d'API REST.

Intégration des notifications d'API REST

Pour intégrer des notifications d'API REST avec des composants tiers, accédez à l'API REST.

Procédez comme suit :

1. Générez un jeton de sécurité dans les **paramètres** de DX APM. Enregistrez le jeton de sécurité quelque part en vue d'une utilisation ultérieure. Pour plus d'informations sur la génération d'un jeton de sécurité, reportez-vous à la section [Autorisation et authentification des API](#).
2. Accédez à **Notifications** et copiez le jeton de proxy de la notification d'API REST que vous souhaitez intégrer. Enregistrez le jeton de proxy quelque part en vue d'une utilisation ultérieure.

NOTE

Vous pouvez utiliser le même jeton de proxy pour plusieurs notifications dans DX APM. L'API REST renvoie les notifications d'alerte de toutes ces configurations de notification. L'appel d'API REST désigne le jeton de proxy `proxyKey`. `proxyKey` identifie le client d'API REST.

3. Définissez la valeur de dernière version sur 0 pour recevoir les états non OK (avertissement ou danger) pour toutes les alertes actives.
4. Copiez le numéro d'hôte à partir de votre URL DX APM. Enregistrez le numéro d'hôte quelque part en vue d'une utilisation ultérieure.
5. Collez le numéro d'hôte, le jeton de sécurité, le jeton de proxy et la dernière version dans la commande POST suivante appeler l'API REST :

POST

Host: `https://<YOUR HOST NUMBER>.apm.cloud.ca.com/apm/appmap/private/graph/recentstatuschanges`

Réponse :

L'API REST envoie un objet JSON en guise de réponse. La réponse contient les modifications d'alerte de toutes les notifications présentant la même valeur de jeton de proxy qui sont survenues après le dernier appel. La réponse renvoie également le champ de version pour l'appel suivant.

Dans la réponse, chaque notification contient les champs suivants :

- **status** : sévérité de l'alerte (OK, CAUTION, DANGER)
- **alertName** : nom de l'alerte
- **time** : occurrence du changement d'état (en millisecondes) depuis le début de l'[heure UTC](#)
- **vertex** : sommet d'alerte, y compris tous les attributs de sommet

Exemple de réponse :

```

{
  "items":
  [
    {
      "vertex":
      {
        "agent":
        [ "CA APM Demo Host|Tomcat|CA APM Demo Agent - Tomcat" ],
        "hostname": [ "ca apm demo host" ],
        "Source cluster": [ "Enterprise Team Center" ],
        "name": [ "Apps|ReportingEngine|URLs|Default" ],
        "agentDomain": [ "SuperDomain" ],
        "IsDemo": [ "Yes" ],
        "processedBy": [ "FrontendVertexIdentifier" ],
        "type": [ "GENERICFRONTEND" ],
        "applicationName": [ "ReportingEngine" ]
      },
      "status": "DANGER",
      "time": 1507025865000,
      "alertName": "SuperDomain:SaaS:Frontend Errors"
    },
    {
      "vertex":
      {
        "agent":
        [ "CA APM Demo Host|Tomcat|CA APM Demo Agent - Tomcat" ],
        "IsExperience": [ "Yes" ],
        "agentDomain": [ "SuperDomain" ],
        "IsDemo": [ "Yes" ],
        "type": [ "GENERICFRONTEND" ],
        "servletMethod": [ "service" ],
        "Experience": [ "Apps|ReportingService|URLs|Default on ca apm demo host (GENERICFRONTEND)" ],
        "hostname": [ "ca apm demo host" ],
        "Source cluster": [ "Enterprise Team Center" ],
        "name": [ "Apps|ReportingService|URLs|Default" ],
        "serviceId": [ "ApplicationService" ],
        "processedBy": [ "FrontendVertexIdentifier" ],
        "applicationName": [ "ReportingService" ]
      },
      "status": "OK",
      "time": 1507025865000,
      "alertName": "SuperDomain:SaaS:Frontend Errors"
    }
  ],
  "version": 1507026459020
}

```

Statut HTTP d'authentification et codes d'erreur

Si l'authentification de la demande échoue, le serveur de ressources renvoie un code d'erreur HTTP et un en-tête de réponse contenant les détails relatifs à l'erreur.

- 401 Unauthorized – votre jeton de sécurité (envoyé dans l'en-tête HTTP) n'est pas valide pour l'URL donnée.
- 403 Forbidden – le jeton proxy ne correspond à aucune configuration de notification.

Pour plus d'informations, reportez-vous aux [définitions des codes de statut HTTP](#).

DX APM vous permet de créer des notifications d'alertes. Les notifications peuvent transmettre automatiquement les alertes de CA Application Performance Management via des services internes tels que des listes de distribution à des services externes via l'API REST, ou à PagerDuty, une plate-forme de résolution des incidents.

Pour plus d'informations sur les notifications, consultez la section [Création de notifications pour les alertes](#).

Configuration de notifications par courriel pour les alertes

Vous pouvez associer une alerte dans DX APM avec les listes prédéfinies de distribution de courriels. Les utilisateurs, dont les administrateurs informatiques, qui sont ajoutés aux listes de distribution sont notifiés lorsque la valeur de mesure dépasse les seuils d'avertissement et de danger.

NOTE

Les seuils d'avertissement et de danger de DX APM sont considérés comme des seuils majeur et critique (respectivement) dans DX SaaS.

Création d'une liste de diffusion

1. Connectez-vous à DX SaaS en tant qu'administrateur de clients hébergés.
2. Dans le volet de navigation gauche, sélectionnez **Notifications** (icône en forme de cloche).
3. Cliquez sur la flèche à la fin de la ligne **Mailing Lists** (Listes de diffusion).
4. Cliquez sur **+ New** (+ Nouveau).
5. Spécifiez le nom de la liste de distribution, puis ajoutez des adresses électroniques.
6. Enregistrez la liste de distribution.

Association d'une liste de distribution à une alerte

Associez une liste de distribution à une alerte dans DX APM.

WARNING

Les modifications apportées aux listes de distribution, comme l'ajout ou la suppression d'une nouvelle adresse, n'apparaissent dans le volet Alertes qu'après 10 minutes. Si votre nouvelle liste de distribution n'apparaît pas dans une alerte, vérifiez de nouveau après 10 minutes.

Procédez comme suit :

1. Dans DX APM, cliquez sur l'icône **Alertes** située dans le volet gauche. Le volet Alertes s'ouvre.
2. Sélectionnez l'alerte à modifier. La liste déroulante Alerte s'ouvre.
3. Cliquez sur le menu déroulant **Notifications**. Une liste de toutes les listes de distribution disponibles s'affiche.
4. Sélectionnez les listes de distribution pour lesquelles des notifications doivent être envoyées concernant cette alerte.

NOTE

Désélectionnez les listes de distribution non valides qui s'affichent en rouge. Les listes de distribution non valides sont maintenant supprimées.

5. Cliquez sur **OK** et sur **Enregistrer l'alerte**.

Configuration des univers

Univers

Les univers permettent à l'administrateur de définir le nombre et le type de composants et de les rassembler dans des groupes faciles à utiliser. Ce groupe ajusté est un univers. Pour des raisons de sécurité, aucune affectation par

défaut à tous les utilisateurs n'est disponible. Pour afficher DX APM, chaque utilisateur doit être alloué à un univers. Si aucun univers n'est associé à l'ID d'utilisateur, l'utilisateur est averti. En tant qu'administrateur, vous êtes chargé de créer des univers pour les utilisateurs. Utilisez l'univers par défaut, appelé **Tous les composants**, ou créez un univers personnalisé.

Pour configurer l'univers, l'administrateur doit effectuer les tâches suivantes :

- Créer un univers adapté aux besoins des utilisateurs ou des groupes d'utilisateurs.
- Appliquer un filtre permettant de sélectionner des données de composant dans l'ensemble de données.
- (Facultatif) Créer plusieurs univers pour créer toute une série d'espaces gérables. Les utilisateurs peuvent facilement basculer entre les espaces et bénéficier ainsi d'une navigation simplifiée dans l'environnement.
- (Facultatif) Vérifier que l'accès utilisateur est limité selon les besoins en matière de sécurité de l'entreprise.

NOTE

Créer un univers basé sur les domaines. Créer un filtre **Sources de mesures** et utiliser la ou les mêmes expressions régulières à partir de la définition de domaine. Créer un filtre pour les composants de carte basé sur l'attribut **agentDomain**, sélectionnez le domaine de votre choix et cliquez sur **Enregistrer**.

En tant qu'administrateur APM, affectez au moins un univers à chaque utilisateur afin que ce dernier puisse accéder au contenu.

Chaque univers se compose de ce qui suit :

- Un nom : identificateur unique
- Une description : texte facultatif décrivant l'univers
- Des filtres :
 - Un filtre Sources de mesures : applicable dans une vue de mesures et dans les graphiques de mesures de la vue Carte.
 - Un filtre Composants de carte : applicable à toutes les vues basées sur la carte, à savoir la vue Carte, la vue Tableau de bord, la vue Expérience et la vue Agent.
 - Un filtre de module de gestion : applicable lors de l'affichage du contenu du module de gestion. Par exemple, les alertes dans la carte ou le tableau de bord. Vous pouvez également définir des définitions d'outils de calcul, de sources de mesures et d'alertes.
- Une liste d'utilisateurs : utilisateurs ayant accès à cet univers

Univers prédéfinis

Certains univers sont créés par défaut :

- L'univers **Tous les composants** est créé automatiquement et contient tous les composants dans la carte, la source de mesure et les modules de gestion.
- L'univers **Entreprise** inclut tous les composants de l'environnement. Cet univers intégré ne peut pas être supprimé ni défini et il est affecté uniquement aux administrateurs à qui il fournit un accès à l'ensemble des données. Cet univers n'est même pas répertorié dans la page **configuration** des univers.

NOTE

- Les utilisateurs peuvent être affectés à plusieurs univers. Dans ce cas, l'univers **All My Universes** (Tous mes univers) est disponible dans la vue **Expérience** et dans la vue **Agents**. Il regroupe les données de tous les univers de tous les utilisateurs..
- La liste déroulante **Tous mes univers** remplit également les univers DX Operational Intelligence (à l'exception de l'univers All Access (Tous les accès)). Ces univers sont marqués d'une balise OI avec leur nom dans la liste déroulante. Vous ne pouvez pas modifier les univers DX Operational Intelligence dans APM.

Deux scénarios d'utilisation différents sont disponibles pour créer des univers :

- **Création d'un univers de navigation** : la création d'un univers de navigation fournit aux utilisateurs de toute une gamme d'environnements filtrés préconfigurés. Les utilisateurs peuvent rapidement basculer entre les environnements pour afficher les différentes zones d'un environnement complexe.
- **Création d'un univers de sécurité** : créez des univers de sécurité dans le but de limiter les composants de l'environnement qu'un utilisateur spécifique peut afficher. Nous vous recommandons de baser le contenu d'un univers de sécurité sur les chemins de transaction. De plus, il est conseillé de créer des attributs personnalisés aux limites qui permettent aux analystes d'identifier la suite du chemin d'accès. Si votre environnement utilise des domaines, l'attribut `agentDomain` est rempli par défaut. Utilisez-le comme condition de filtre pour créer un univers qui correspond aux limitations appliquées aux autorisations du domaine spécifié.

Création d'un univers

Lorsque vous définissez un nouvel univers, vous pouvez accorder des droits différents aux utilisateurs et aux groupes d'utilisateurs. Les droits d'accéder à l'univers, de sélectionner des sources de mesures et des composants de carte, et de gérer des modules.

Procédez comme suit :

1. Tenez compte du contenu que vous voulez définir dans cet univers.
2. Dans le volet gauche, cliquez sur **Univers**, puis sélectionnez **Nouvel univers**.

Une boîte de dialogue s'ouvre.

NOTE

Les définitions ajoutées à un onglet sont propagées à la partie correspondante de l'application. Par exemple, les définitions ajoutées aux composants de carte sont appliquées à la carte. Les définitions ajoutées aux sources de mesures sont appliquées au navigateur de mesures. Les autres parties de l'application ne sont pas affectées.

3. Attribuez un nom à l'univers.
4. (Facultatif) Ajoutez une description pour l'univers.
5. Dans la vue **Accès**, accordez aux utilisateurs et/ou groupes d'utilisateurs différents droits d'accès à cet univers.
 - a. Sélectionnez le droit à accorder :
 - **Lire** : autorise les utilisateurs à consulter les composants sélectionnés dans l'univers.
 - **Modifier** : autorise les utilisateurs à modifier les composants qu'ils sélectionnent dans l'univers et à ajouter des attributs ou des règles aux composants de carte. Ce droit inclut également des droits de lecture.
 - **Gérer** : autorise les utilisateurs à modifier les droits d'accès à l'univers. Les administrateurs utilisent le droit Gérer pour déléguer des droits d'accès à d'autres utilisateurs. Ce droit inclut également des droits de lecture et d'écriture.
 - b. Dans la liste déroulante, sélectionnez l'utilisateur ou le groupe d'utilisateurs auquel vous voulez accorder le droit.
 - c. Cliquez sur **Ajouter un utilisateur** ou sur **Ajouter un groupe** pour ajouter l'utilisateur ou le groupe d'utilisateurs sélectionné à l'univers.
 - d. (Facultatif) Sélectionnez un droit différent et un utilisateur ou un groupe d'utilisateurs, puis ajoutez-les à la liste.
6. Dans la vue **Sources de mesures**,
 - L'option **Filtrer la vue des mesures par composants de carte** filtre les arborescences de mesures dans le navigateur de mesures par carte. Valeur par défaut : **true** (le filtre est appliqué par défaut). Sélectionnez la case à cocher pour désactiver le filtre.
 - Sélectionnez **Toutes les sources de mesures**, y compris les composants futurs. Si vous sélectionnez cette option, l'univers contient toutes les sources de carte (agents) sans qu'aucun filtre ne soit appliqué.
 - Personnalisez les sources de mesures en sélectionnant un sous-ensemble d'agents individuels et/ou en ajoutant une expression régulière. Les expressions régulières sont basées sur le nom d'hôte, le nom de processus et le nom d'agent. Exemples d'expressions :

- myhost\.* - Sélectionne tous les agents s'exécutant sur l'hôte "myhost". Le caractère | (barre verticale) est échappé avec une barre oblique inversée, car il s'agit d'un caractère de contrôle des expressions régulières.
- usnye.* - Sélectionne les agents de tous les hôtes avec le préfixe "usnye".
- .*\\.*\dmn13t.* - Sélectionne tous les agents avec le préfixe "dmn13t".

NOTE

Dans la boîte de dialogue située en bas de la page, cliquez sur **Recharger** pour afficher un aperçu de la sous-arborescence pour les agents sélectionnés.

WARNING

Les sources de mesures des univers créés avant la version 20.11 doivent être reconfigurées.

7. Dans la vue **Composants de carte**, sélectionnez l'une de ces actions :
 - Mappez tous les composants (y compris les composants futurs). Si vous sélectionnez cette option, l'univers contient tous les composants de carte sans qu'aucun filtre ne soit appliqué.
 - Utilisez le filtre **Sources de mesures**. Si vous sélectionnez cette option, l'univers contient tous les composants de carte générés par les agents sélectionnés par le filtre **Sources de mesures**.
 - Personnalisez le filtre. Définissez un filtre de carte pour sélectionner les composants de carte requis. Ce filtre est identique à celui de la vue **Carte**.

NOTE

Pour plus d'informations sur le nœud Expérience, reportez-vous à la section [Surveillance des performances à l'aide de la vue Expérience](#).

8. Dans la vue **Modules de gestion**, effectuez l'une des sélections suivantes :
 - Tous les éléments (y compris les futurs à venir).
 - Un ou plusieurs éléments de la liste.
9. La vue **Infos** est générée après l'enregistrement de l'univers. Cette vue contient une présentation des définitions d'univers. La présentation inclut le nombre de composants dans différentes parties de l'application (par exemple, carte et vue de mesures).
10. Sélectionnez **Enregistrer**.

NOTE

En tant qu'administrateur, vous pouvez également créer un univers directement à partir de la carte de l'univers Enterprise. Définissez les filtres de carte et cliquez sur **Enregistrer en tant qu'univers** dans le coin supérieur droit pour enregistrer les nœuds de carte filtrée en tant qu'univers.

Modification d'un univers**Procédez comme suit :**

1. Dans le volet gauche, cliquez sur **Univers**.
2. Sélectionnez l'univers que vous souhaitez modifier et cliquez sur **Modifier**.
3. Suivez les étapes décrites dans la section [Création d'un univers](#).

Suppression d'un univers**Procédez comme suit :**

1. Dans le volet gauche, cliquez sur **Univers**.
2. Sélectionnez l'univers que vous souhaitez supprimer et cliquez sur **Supprimer**.
3. Confirmez la suppression.

Configuration de la sécurité de l'univers

Dans chaque univers, des droits individuels sont affectés aux utilisateurs pour modifier des alertes, des outils de calcul et des groupes de mesures. Le rôle Utilisateur avancé, les utilisateurs et les groupes d'utilisateurs doivent disposer de l'autorisation d'afficher ou de créer des alertes, des outils de calcul ou des groupes de mesures pour un module de

gestion. L'utilisateur avancé peut démarrer manuellement les sessions de suivi de transaction. L'administrateur de client hébergé dispose de tous les droits. Les droits sont en vigueur uniquement lors de l'affichage de l'univers spécifié. Voici les droits par type d'autorisation :

NOTE

Par défaut, un utilisateur/utilisateur avancé sans autorisation d'accès à un univers ne peut pas voir d'agents/ de mesures dans la vue des mesures. Un utilisateur disposant d'une autorisation de lecture sur un univers peut consulter les mesures de l'agent configurées pour l'univers dans la vue des mesures.

- **lire** : permet à l'utilisateur avancé, à l'utilisateur ou au groupe d'utilisateurs affectés d'afficher les alertes, les outils de calcul et les groupes de mesures du module de gestion.
- **écrire** : permet à l'utilisateur avancé, à l'utilisateur ou au groupe d'utilisateurs affectés d'afficher et de modifier les alertes, les outils de calcul et les groupes de mesures du module de gestion.
- **gérer** : permet à l'utilisateur avancé, à l'utilisateur ou au groupe d'utilisateurs affectés d'afficher et de modifier les alertes, les outils de calcul, les groupes de mesures et les utilisateurs du module de gestion. Les utilisateurs disposant des droits **gérer** peuvent également ajouter des modules de gestion à l'univers.

L'administrateur de clients hébergés doit explicitement accorder à l'univers le chemin d'accès à la source de mesure. Ce chemin permet aux utilisateurs disposant de l'accès à l'univers d'afficher les mesures d'alarme et d'outil de calcul dans l'arborescence des mesures.

L'administrateur a le privilège de choisir les entités auxquelles les utilisateurs ont accès. Cela inclut les mesures, les vertex et les modules de gestion.

- Avec un accès en **lecture**, l'utilisateur peut afficher les entités, mais ne peut pas les modifier.
- Avec un accès en **écriture**, l'utilisateur peut modifier les entités. Il peut, par exemple, modifier le contenu du module de gestion ou ajouter des attributs personnalisés aux vertex.
- **Gérer** l'accès donne à l'utilisateur le privilège de modifier la liste d'accès dans l'univers.

Nous recommandons les paramètres suivants pour vous assurer que les utilisateurs disposent d'un accès correct aux paramètres des modules de gestion :

- N'affectez pas d'utilisateurs à un univers avec un paramètre de portée **Module de gestion** dont la valeur est **Tous les éléments**.
- Ajoutez explicitement des **modules de gestion** dans la portée de tous les univers, à l'exception de l'univers Entreprise. Entreprise est un univers spécial uniquement disponible pour l'administrateur de clients hébergés.

Informations complémentaires : [Rôles et droits pris en charge](#)

Les univers permettent à l'administrateur d'affiner le nombre et le type de composants, et de les rassembler dans des groupes faciles à utiliser appelés univers. Pour afficher DX APM, chaque utilisateur doit être alloué à un univers. En tant qu'administrateur, vous devez créer des univers pour les utilisateurs. Utilisez l'univers par défaut Tous les composants ou créez un univers personnalisé.

Pour plus d'informations sur la gestion et la configuration des univers, reportez-vous à la section [Configuration des univers](#).

Configuration de la vue Expérience

En tant qu'administrateur, configurez les fiches d'expérience dans la vue Expérience. Configurez les fiches afin que les analystes puissent facilement afficher les composants métier les plus critiques qui affectent l'expérience utilisateur final.

Vue Expérience

Les administrateurs sont chargés des tâches suivantes :

- Configuration de l'univers
- Ajout d'une nouvelle fiche d'expérience
- Modification d'une fiche d'expérience
- Partage d'une fiche d'expérience

Fiches de la vue Expérience

Découvrez comment créer une fiche d'expérience dans la vue Expérience. Configurez vos fiches d'expérience pour que l'univers des analystes soit divisé en groupes significatifs.

Configuration de l'univers

Avant de configurer la vue Expérience d'un utilisateur, affectez-lui au moins un univers.

NOTE

La vue Tous mes univers est disponible dans la vue **Expérience** uniquement pour les administrateurs. Pour les autres utilisateurs, la vue Tous mes univers est disponible dans la vue **Agents**, si plusieurs univers sont affectés.

Informations complémentaires :

- [Configuration des univers](#)
- [KB000113376 : des utilisateurs disposant d'un accès en lecture à Team Center ne parviennent pas à afficher la vue Tous mes univers](#)

Ajout d'une nouvelle fiche d'expérience

Prêt à l'emploi, pour un gestionnaire d'entreprise, le système crée deux fiches d'expérience pour chaque univers existant. Les fiches d'expérience pour les applications incluent deux niveaux de détail avec des attributs `Application` et `Name`. Les fiches d'expérience pour les services incluent deux niveaux de détail avec les attributs `Business service` et `Name`. En tant qu'administrateur, créez, mettez à jour ou supprimez autant de fiches d'expérience personnalisées que nécessaire pour les analystes.

NOTE

Les fiches d'expérience ne sont pas créées automatiquement si vous ajoutez un nouvel univers ou si vous connectez un nouveau fournisseur. La création automatique de fiches d'expérience ne constitue qu'une partie d'une installation ou mise à niveau.

Procédez comme suit :

1. Ouvrez la vue Expérience et assurez-vous que vous vous trouvez dans la vue de niveau supérieur.
2. Cliquez sur le bouton + pour ajouter une nouvelle fiche d'expérience.
3. Sélectionnez un univers.
4. Utilisez l'univers complet ou appliquez un filtre.
5. Sélectionnez les attributs. Les fiches d'expérience sont groupées par attributs. Les niveaux de détail de la fiche d'expérience correspondent au nombre d'attributs que vous sélectionnez.

TIP

Nous vous recommandons d'utiliser trois à quatre niveaux d'attributs. Vous pouvez également regrouper plusieurs attributs sous un seul attribut pour surveiller un groupe de composants spécifique. Par exemple, Propriétaire = Joe.

6. Sélectionnez un type de graphique par défaut :
 - a. Histogramme
 - b. Temps de réponse moyen

- c. Volume de transactions
- 7. Nommez la fiche.
- 8. Cochez la case **Rendre cette fiche d'expérience publique**.
- 9. Sélectionnez **Enregistrer**.

L'administrateur peut maintenant consulter les fiches d'expérience dans la vue Expérience.

WARNING

Un message erreur s'affiche lorsque vous tentez d'afficher plus de 500 transactions métier en mode Dynamique ou plus de 50 transactions métier en mode Historique. La vue Expérience limite le nombre de transactions métier pour des raisons de performances. Pour plus d'informations, consultez la rubrique [Aucune donnée de mesure dans la vue Expérience](#).

Modification d'une fiche d'expérience existante

Au niveau supérieur de la vue Expérience, vous pouvez modifier des fiches d'expérience, aussi bien celles par défaut que celles définies par l'utilisateur.

Procédez comme suit :

1. Cliquez sur l'icône de développement située dans l'angle inférieur droit de la fiche.
2. Sélectionnez **Modifier la fiche**.
3. Modifiez les paramètres de fiche selon vos besoins.
4. Sélectionnez **Enregistrer**.

Suppression d'une fiche d'expérience

Au niveau supérieur de la vue Expérience, vous pouvez supprimer des fiches d'expérience, aussi bien celles par défaut que celles définies par l'utilisateur.

Procédez comme suit :

1. Cliquez sur l'icône de développement située dans l'angle inférieur droit de la fiche.
2. Sélectionnez **Modifier la fiche**.
3. Sélectionnez **Supprimer la fiche**. La fiche est supprimée pour tous les utilisateurs qui y ont accès.

Partage d'une fiche d'expérience

Vous pouvez partager une fiche d'expérience avec un utilisateur dans un univers existant.

Procédez comme suit :

1. Vérifiez que l'utilisateur dispose de l'accès à l'univers.
2. Cliquez sur l'icône de développement située dans l'angle inférieur droit de la fiche.
3. Sélectionnez **Modifier la fiche**.
4. Sélectionnez **Rendre cette fiche d'expérience publique**.
5. Sélectionnez **Enregistrer**.
La fiche apparaît dans votre liste de fiches.
6. Envoyez le lien de la fiche d'expérience à l'utilisateur.

NOTE

Vous pouvez partager une fiche d'expérience privée avec un utilisateur du même univers. L'utilisateur peut afficher temporairement la fiche privée.

Propagateur

La vue Expérience permet d'organiser les expériences (noeuds d'expérience) dans des fiches en fonction des attributs. Pour développer la sélection des attributs pour les expériences de groupement, utilisez le propagateur. Le propagateur copie les attributs des composants adjacents qui sont directement connectés à une expérience. Ces attributs sont propagés jusqu'à l'expérience en fonction des règles. Si plusieurs composants sont connectés à une même expérience et que le même attribut est défini plusieurs fois, l'attribut est propagé uniquement si toutes les occurrences de cet attribut possèdent la même valeur. Le propagateur peut également collecter et envoyer des attributs à partir d'autres couches de plan. Par exemple, la propagation intercouche vous permet d'organiser vos expériences en fonction des attributs docker et hôte à partir de la couche d'infrastructure.

Configuration des paramètres du propagateur

Définissez les attributs que vous souhaitez propager à vos expériences à l'aide de la syntaxe RegEx sur les noms d'attribut. Identifiez la source de l'attribut et configurez la propagation intercouche.

Procédez comme suit :

1. Définissez et identifiez les attributs que vous souhaitez propager. Les sources d'attributs disponibles sont les suivantes :

- **GATHERED**
Inclut des attributs définis par l'agent lors de la surveillance du composant.
- **CUSTOM**
Contient des attributs créés manuellement dans l'IU ou définis dans l'API REST.
- **DECORATED**
Regroupe les attributs créés à l'aide de règles d'attribut.

NOTE

Les attributs propagés aux expériences sont toujours Decorated. Ces attributs peuvent être écrasés par des règles d'attribut, l'API REST ou des modifications manuelles apportées à l'IU.

2. Utilisez une liste blanche pour propager certains attributs ou utilisez une liste noire pour bloquer les attributs. Définissez ces règles de propagation globale en modifiant les propriétés suivantes dans le fichier `IntroscopeEnterpriseManager.properties` :

- **introscope.apmserver.atc.propagator.blacklist**

Spécifie les attributs de la liste noire.

Valeur par défaut :

```
introscope.apmserver.atc.propagator.blacklist=CUSTOM\.*;DECORATED\.*;Name;Hostname;Agent;AgentDomain
```

La liste noire par défaut ne propage pas les attributs suivants :

- Attributs personnalisés et décorés
- Name (nom)
- HostName ,
- Agent
- AgentDomain

- **introscope.apmserver.atc.propagator.whitelist**

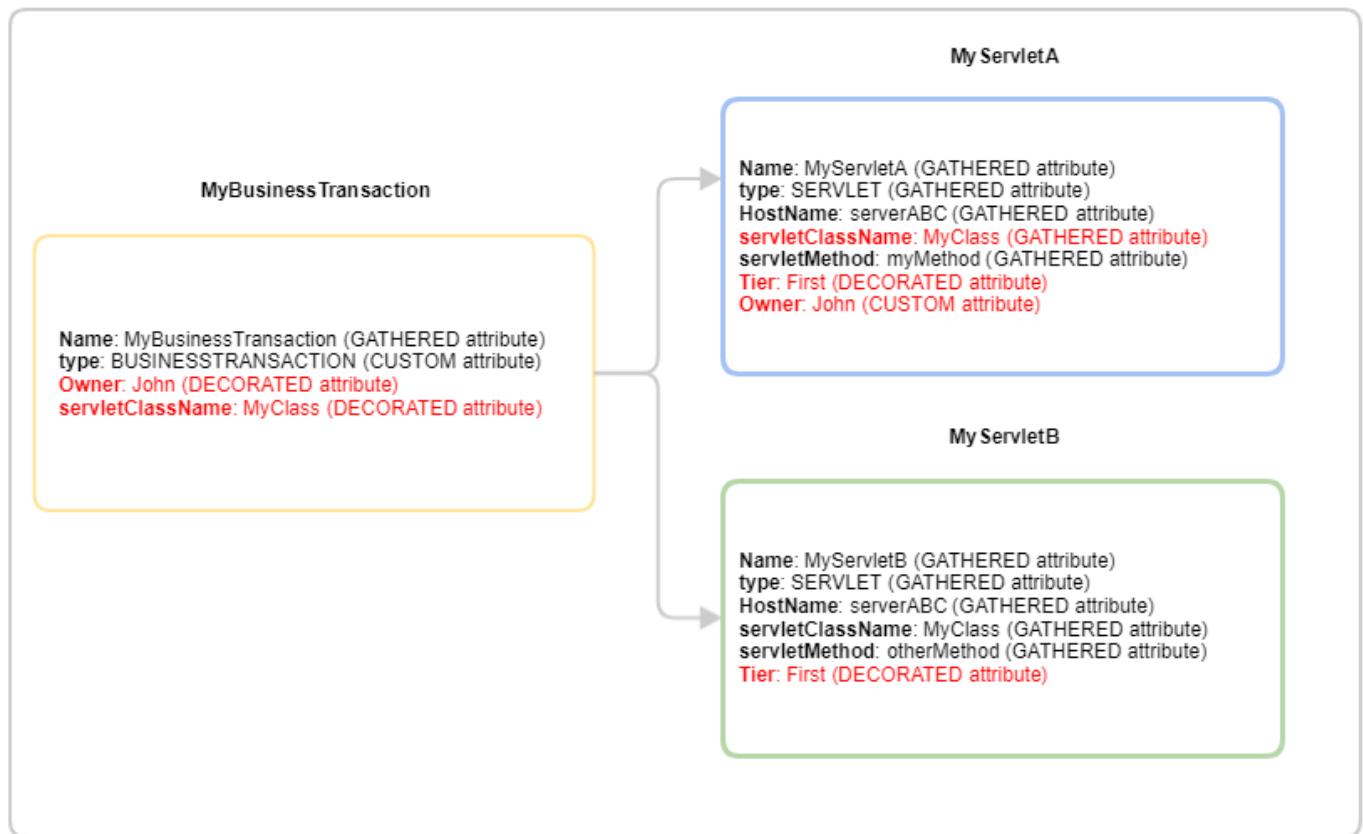
Spécifie les attributs de la liste blanche.

Valeur par défaut :

```
introscope.apmserver.atc.propagator.whitelist=.*Owner
```

La liste blanche par défaut propage l'attribut `Owner` .

Exemple : L'exemple ci-dessous illustre la propagation des attributs `Owner` et `servletClassName` vers une expérience à partir du servlet connecté.

Figure 2: propagateur**Résultats :**

- L'attribut Tier n'est pas propagé, car la liste noire désactive la propagation des attributs personnalisés.
 - L'attribut HostName n'est pas propagé, car il figure lui aussi dans la liste noire.
 - L'attribut servletMethod n'est pas propagé, car les servlets possèdent des valeurs différentes.
 - Owner est propagé, car il n'interfère pas avec MyServletB.
 - servletClassName est propagé, car les deux servlets présentent les mêmes valeurs.
3. Pour configurer la propagation intercouche des attributs, ouvrez le fichier `IntroscopeEnterpriseManager.properties` à partir du répertoire `<répertoire_base_EM>/config`. Spécifiez les couches de carte dans la propriété `introscope.apmserver.atc.propagator.crosslayer` :
Valeur par défaut : `<vide>` La valeur par défaut est une chaîne vide, ce qui signifie que la propagation intercouche est désactivée.

NOTE

Pour activer la propagation à partir de plusieurs couches de carte, séparez chaque couche par une virgule.

Exemple - Dans l'exemple suivant, le propageur est configuré pour récupérer les attributs à partir de la couche d'infrastructure :

```
introscope.apmserver.atc.propagator.crosslayer=INFRASTRUCTURE
```

NOTE**Informations complémentaires :**

- [Définition du mode de surveillance de l'environnement à l'aide de règles d'attribut](#)

Clamp de données

Le clamp de données en mode historique est de 50 expériences contre 500 expériences en mode dynamique. Les expériences sont des transactions métier ou des points d'entrée d'application. Si vous sélectionnez une période en mode historique au cours des dernières 24 heures, le clamp de données en mode dynamique (500 expériences) est appliqué. Les dernières 24 heures sont couvertes par les données mises en cache.

Les administrateurs configurent les fiches d'expérience dans la vue Expérience afin que les analystes puissent facilement afficher les composants critiques pour l'entreprise qui affectent l'expérience de l'utilisateur final.

Pour plus d'informations sur la configuration des fiches d'expérience, consultez la section [Configuration de la vue Expérience](#).

Définition du mode de surveillance de l'environnement à l'aide de règles d'attribut

Les attributs sont des étiquettes appliquées aux composants. Chaque attribut possède un nom et une valeur (colour=rouge, par exemple). Les attributs simplifient l'identification des composants et de leurs relations avec les autres composants. Utilisez des attributs dans les perspectives, mises en surbrillance et filtres pour organiser et afficher les parties de l'environnement d'application surveillé. DX APM vous permet d'affecter un nombre illimité d'attributs aux composants.

Types d'attribut

DX APM propose les types d'attributs suivants :

- **Attributs de base**

Les attributs de base sont automatiquement signalés et affectés à chaque composant à partir de l'agent associé. Par exemple, un composant de base de données peut avoir les attributs de base suivants :

- `datasasename`
- `inferredBackendNode`
- `Name` (nom)
- `fournisseur`
- `Source cluster`
- `Type`

- **Attributs personnalisés**

Affecter des attributs personnalisés à chaque composant, puis ajoutez ces attributs aux perspectives, groupes et filtres. Par exemple, utilisez l'attribut `owner` (propriétaire) pour affecter le composant à un analyste spécifique. Pour afficher les composants qui sont affectés à cet analyste, ajoutez l'attribut `owner` (propriétaire) à un filtre et spécifiez la valeur de filtre.

- **Attributs décorés**

Vous pouvez définir des règles d'attribut qui affectent automatiquement de nouvelles valeurs aux attributs existants. Ces nouveaux attributs dérivés sont appelés des attributs décorés.

Définition d'attributs personnalisés

Définissez un attribut personnalisé pour un composant ou un groupe de composants.

NOTE

Il est recommandé d'affecter des attributs personnalisés à tous les composants de l'environnement. Il est recommandé d'affecter des valeurs à `Owner` (Propriétaire) et à `Location` (Localisation) pour tous les composants.

Procédez comme suit :

1. Dans la **carte**, sélectionnez un composant ou un groupe.

TIP

Vous pouvez ajouter un attribut personnalisé à un composant qui représente un groupe. Le nom et la valeur de l'attribut sont ajoutés à tous les composants de ce groupe. Un message s'affiche dans lequel vous devez indiquer que vous voulez ajouter l'attribut au groupe ou créer une règle d'attribut.

2. Accédez à la section **Attributs personnalisés** du panneau **Vue Composant** et sélectionnez les valeurs pour les attributs personnalisés par défaut suivants :
 - location (localisation)
 - owner (propriétaire)
 - region (région)
 - tier (niveau)
3. (Facultatif) Pour créer un attribut, sélectionnez **<nouveau nom d'attribut>**, puis saisissez le nom d'attribut. Sélectionnez **<nouvelle valeur d'attribut>**, puis affectez une valeur à l'attribut.

NOTE

DX APM reconnaît si une valeur d'attribut est une adresse électronique ou une URL. Une icône d'enveloppe ou de lien apparaît à côté de l'attribut dans le panneau **Vue Composant**. Sélectionnez l'icône pour ouvrir des liens dans un nouvel onglet de navigateur ou pour ouvrir une page de messagerie Outlook.

4. Ajoutez le nouvel attribut aux filtres et aux perspectives.

Le nouvel attribut et la nouvelle valeur apparaissent dans la section **Attributs personnalisés** du panneau **Vue Composant**.

Définition des attributs intercouche

Les attributs affectés aux composants à partir d'une couche spécifique sont également visibles dans les autres couches de DX APM. Par exemple, les attributs affectés aux composants de la couche d'infrastructure sont inclus dans la liste déroulante permettant de filtrer la carte dans la couche applicative. Cette fonctionnalité intercouche offre aux analystes des vues de données qui présentent les relations entre les composants d'application et les composants d'infrastructure connectés. Cette vue de données combinée est également utilisée comme aperçu pour aider à définir et à organiser les rôles de support dans l'organisation. Les administrateurs peuvent affecter des attributs aux composants de la couche d'infrastructure dans la section **Attributs personnalisés** du panneau **Vue Composant** ou en définissant une règle d'attribut.

Exemples**Exemple 1 : Utilisation des attributs intercouche pour faciliter le tri de l'infrastructure**

L'attribut `Owner = Joe Smith` est affecté à tous les composants d'infrastructure dont Joe effectue le support. Cet attribut est ensuite utilisé pour créer la perspective `Joe Smith`. Les analystes utilisent cette perspective et d'autres perspectives `Owner` (Propriétaire) pour identifier qui fournit le support de l'infrastructure pour les applications nécessitant un tri. Ces vues de données permettent également aux analystes d'effectuer le support de l'infrastructure avec des informations clés qui peuvent aboutir à un tri plus rapide.

Exemple 2 : Utilisation des attributs intercouche pour définir des rôles de support

Si les composants de l'hôte de votre environnement observent une convention d'attribution de noms, vous pouvez créer une règle d'attribut pour définir des rôles de support pour les composants d'application. La règle d'attribut suivante affecte Joe Smith à tous les composants d'hôte situés à New York. Une perspective est créée en fonction de cet attribut, ce qui

permet à l'analyste Joe Smith d'afficher les composants d'application affectés et tous les composants d'infrastructure connectés.

Nom de l'attribut personnalisé	Valeur nouvellement affectée	Nom de l'attribut existant	Condition/Opérateur correspondant	Valeur de la condition
Owner	Joe Smith	Hostname (nom d'hôte)	Contient	NY

Les liens suivants fournissent des informations complémentaires sur les couches et sur l'utilisation des attributs dans DX APM :

NOTE

Informations complémentaires :

- [Couches de carte](#)
- [Identification des points importants lors de l'utilisation des filtres](#)
- [Organisation des composants à l'aide de perspectives](#)

Définition des attributs décorés à l'aide de règles d'attribut

Utilisez des règles d'attribut pour automatiser le processus d'ajout d'attributs personnalisés. Une règle utilise les attributs de base et personnalisés qui ont déjà été affectés à un composant. Si l'attribut remplit la condition spécifiée dans la règle, un nom d'attribut personnalisé est créé (ou mis à jour), puis la valeur spécifiée lui est affectée. Par exemple, une règle d'attribut indique que si l'attribut de nom d'hôte d'un composant se termine par le suffixe .cz, l'attribut personnalisé avec le nom Emplacement du service de support doit être créé et la valeur République tchèque doit lui être attribuée. Tous les composants répondant aux critères d'une règle se voient affecter la valeur de l'attribut personnalisé. Les règles affectent l'attribut personnalisé dans l'environnement actuel. Elles affectent également cet attribut à tous les composants répondant aux critères par la suite.

• Règles d'attribut locales

En tant qu'utilisateur, vous pouvez créer des règles d'attribut locales et les appliquer aux composants inclus dans votre univers. La règle applique la valeur du nouvel attribut à tous les composants qui répondent aux critères et qui sont inclus dans l'univers actuel. Ces attributs personnalisés sont réservés à l'univers. Seuls les utilisateurs ayant accès à cet univers et l'administrateur peuvent les afficher.

• Règles d'attribut globales

Les règles d'attribut globales appliquent les valeurs de l'attribut personnalisé à tous les composants répondant aux critères de règle dans l'environnement d'entreprise. Seul l'administrateur peut créer des règles d'attribut globales. Les règles d'attribut globales prévalent sur les règles d'attribut locales. **Exemple** : Créez un attribut local pour définir la valeur d'un attribut Emplacement sur Long Island. Si une règle d'attribut globale est définie pour affecter la valeur d'attribut d'emplacement New York, la valeur indique New York pour tous les utilisateurs.

Définition de règles d'attribut globales

Définissez des règles d'attribut pour affecter automatiquement des attributs aux composants. Les règles d'attribut globales appliquent des attributs personnalisés à tous les composants actuels et futurs qui remplissent les conditions de la définition de règle. Elles s'appliquent à tous les composants dans l'environnement d'entreprise, quel que soit l'univers. Les utilisateurs pour lesquels le composant est affecté à leur univers voient l'attribut personnalisé. Un utilisateur ne peut pas créer de règle d'attribut locale qui remplace une valeur de la règle d'attribut globale.

Procédez comme suit :

1. Sélectionnez l'onglet **Attributs**.
2. Cliquez sur **<nouvelle règle d'attribut>** dans la colonne **Nom de l'attribut personnalisé**, puis remplissez les noms et valeurs de la nouvelle règle.
3. Cliquez n'importe où en dehors de la ligne.

La règle est enregistrée.

Utilisation de l'opérande d'expression régulière avec les règles d'attribut

Utilisez l'opérande Contient une expression régulière dans les cas suivants :

- Les opérandes tels que `Commence par` ou `Contient` ne sont pas suffisants pour créer la règle d'attribut dont vous avez besoin.
- Vous avez besoin d'une nouvelle valeur d'attribut basée sur la valeur d'origine.

L'utilisation d'une expression régulière sur une valeur d'attribut existante permet de créer plusieurs règles d'attribut personnalisées.

Procédez comme suit :

1. Sélectionnez l'onglet **Attributs**.
2. Cliquez sur **<nouvelle règle d'attribut>**.
3. Affectez un nom d'attribut personnalisé.
4. Affectez une valeur de groupe d'expressions régulières à la **valeur affectée récemment**.
5. Sélectionnez le **nom d'attribut existant requis**.
6. Sélectionnez une valeur **Condition/Opérateur correspondant** : `Contient une expression régulière` ou `Ne contient pas une expression régulière`.
7. Entrez l'expression régulière dans **Valeur de la condition** et appuyez sur la touche **Entrée**.

NOTE

L'option **Sensible à la casse** ne peut pas être sélectionnée. Le respect de la casse est défini en fonction d'une expression régulière.

La règle d'attribut est enregistrée et le nombre de composants avec le nouvel attribut s'affiche dans la section **Nombre de composants affectés**.

- Exemple : le nom d'hôte de votre réseau suit la règle `<code pays à 2 lettres><ville><ID numérique>.vendor.com`. Vous pouvez utiliser l'opérande d'expression régulière pour créer des règles d'attribut afin de créer des attributs de pays et de ville distincts à partir du nom d'hôte. La syntaxe `(.)([a-z]*)[0-9]*\.vendor\.com` décrit cette expression régulière. Vous pouvez créer des règles d'attribut afin d'extraire les valeurs des attributs Pays et Ville.

Nom de l'attribut personnalisé	Valeur nouvellement affectée	Nom de l'attribut existant	Condition/Opérateur correspondant	Respecter la casse	Valeur de la condition
Pays	\$1	hostname (nom d'hôte)	ContainsRegex		<code>(.)([a-z]*)[0-9]*\.vendor\.com</code>
Ville	\$2	hostname (nom d'hôte)	ContainsRegex		<code>(.)([a-z]*)[0-9]*\.vendor\.com</code>

- Exemple : deux valeurs de nom d'hôte dans un environnement, `uklondon1234.vendor.com` et `usdallas1234.vendor.com`

La valeur \$1 renvoie les valeurs uk (Royaume-Uni) et us (Etats-Unis), alors que la valeur \$2 renvoie les valeurs london (Londres) et dallas (Dallas). Vous pouvez également créer un lien vers votre documentation en procédant comme dans l'exemple suivant. Sélectionnez un élément de la carte pour afficher un lien vers votre documentation.

Nom de l'attribut personnalisé	Valeur nouvellement affectée	Nom de l'attribut existant	Condition/ Opérateur correspondant	Respecter la casse	Valeur de la condition
Pays	\$1	hostname (nom d'hôte)	ContainsRegEx		(..)([a-z]*)[0-9]*\.\.vendor\.com
Ville	\$2	hostname (nom d'hôte)	ContainsRegEx		(..)([a-z]*)[0-9]*\.\.vendor\.com
URL de la documentation	https://wiki.vendor.com/searchForServerDoc.cgi?host=\$1	hostname (nom d'hôte)	ContainsRegEx		(.*)\.vendor\.com

NOTE

Pour connaître la syntaxe complète des expressions régulières, consultez la documentation [Java RegEx](#). (Facultatif) Recherchez un testeur en ligne d'expressions régulières Java sur Internet.

Importation des règles d'attribut en bloc

DX APM vous permet d'attribuer une description unique à vos composants, qu'ils s'agissent d'hôtes, d'applications ou de composants d'application. Attribuez ces descriptions (attributs personnalisés) dans votre environnement pour tirer pleinement parti des vues Carte et Expérience. Par exemple, fournissez un attribut Propriétaire pour chaque application dans votre environnement. Lorsque vous affichez la vue Carte de vos propriétaires, les applications qu'ils gèrent y sont imbriquées. La définition de cet attribut Propriétaire vous permet de disposer d'une mosaïque qui récapitule les performances de toutes les applications par propriétaire. Vous pouvez ensuite accéder aux détails de la mosaïque pour afficher chaque application qui appartient à ce propriétaire spécifique.

Pour faciliter l'application de ces attributs, vous pouvez utiliser un mécanisme de chargement de règle en bloc. En tant qu'administrateur, vous pouvez créer un ensemble de règles d'attribut externes dans un fichier CSV. Vous pouvez ensuite importer ce fichier pour créer plusieurs règles d'attribut. Cette fonctionnalité vous permet d'utiliser un fichier CSV contenant plusieurs règles d'attribut et de les charger en même temps sur une courte période.

Dans le fichier, spécifiez le nom de l'attribut personnalisé, une virgule et la valeur souhaitée. Ajoutez ensuite une autre virgule et spécifiez l'attribut que vous souhaitez utiliser pour la correspondance à la règle. Ajoutez une autre virgule, puis la valeur attendue de l'attribut correspondant.

En d'autres termes :

```
WHEN Hostname equals my-tradeservice THEN Owner equals Ralph
```

Cette formulation peut être écrite dans le fichier CSV sous la forme :

```
Owner,Ralph,Hostname,my-tradeservice
```

Utilisez le format suivant dans le fichier CSV :

Nom de l'attribut personnalisé que vous souhaitez ajouter. L'attribut peut être un des attributs décorés.	Valeur de l'attribut personnalisé que vous souhaitez ajouter.	Nom de l'attribut de filtre que vous souhaitez mettre en correspondance. Ces attributs sont les attributs de base.	Valeur de l'attribut de filtre que vous souhaitez mettre en correspondance.
--	---	--	---

Ce fichier peut inclure uniquement quatre colonnes. La valeur d'attribut de correspondance dans la troisième colonne doit être un nom d'attribut valide.

Procédez comme suit :

1. Dans un éditeur, créez un fichier CSV en utilisant le format mentionné, par exemple :

```
owner,ralph,Hostname,my-machine-name
location,CA,Hostname,my-machine-name
region,san mateo,Application,my-app-name
country,USA,agent,my-agent-name
```
2. Enregistrez et nommez le fichier en utilisant la convention suivante : `nom_fichier.csv`. Par exemple, sous Windows, utilisez la fonctionnalité Enregistrer sous et enregistrez au format `.csv`. Fermez le fichier.
3. Dans DX APM, passez le curseur sur le volet de gauche et cliquez sur **Attributs**.
4. Cliquez sur **Charger le fichier de la règle d'attribut**.
La boîte de dialogue Charger le fichier CSV de la règle attribut s'affiche.
5. Lisez les instructions de la boîte de dialogue et sélectionnez des univers supplémentaires pour appliquer les règles si vous le souhaitez. Si aucun univers n'est sélectionnée, les règles d'attribut sont uniquement appliquées à l'univers sélectionné actuellement.
6. Cliquez sur **Parcourir** et sélectionnez le fichier CSV à importer. Vous pouvez répéter cette étape pour sélectionner un autre fichier à charger.
7. Cliquez sur **Charger**.
Un message s'affiche et vous informe du statut de chargement du fichier.
8. Cliquez sur **Terminé**.
Les règles d'attribut s'affichent dans la liste des règles d'attribut.

Configuration de règles pour la mise à jour des attributs

Lorsque vous souhaitez mettre à jour les attributs de plusieurs composants (par exemple, pour spécifier le propriétaire de nombreuses applications ou hôtes), le chargement de règles au format CSV peut être plus pratique que de les créer dans l'interface utilisateur. Il n'est pas nécessaire de spécifier uniquement les attributs existants. Vous pouvez créer des attributs répondant à vos besoins pour créer des mosaïques Perspectives et Vue Expérience. Après leur chargement, les règles apparaissent dans la carte.

Exemple :**Fonctionnement des règles**

Dans cet exemple, vous souhaitez affecter l'attribut Owner avec la valeur Eric à deux noms d'hôtes : red et blue. Vous souhaitez également affecter l'attribut Owner avec la valeur Susan au nom d'hôte green.

```
@ruleset, owners-by-hostOwner,Eric,hostname,redOwner,Eric,hostname,blueOwner,Susan,hostname,green
```

`@ruleset, <name>` place ces trois règles dans la portée `owners-by-host`. L'interface utilisateur affiche l'identificateur auquel chaque règle appartient. Chaque règle spécifiée appartient à un groupe avec un identificateur unique : un ensemble de règle (`@ruleset`). Lorsqu'aucun ensemble de règle `@ruleset` n'est spécifié, les règles appartiennent implicitement à un groupe global. Vous devez toujours utiliser les identificateurs de règle ou vous pouvez noter des modifications inopinées dans la portée globale et supprimer involontairement des règles dans les autres portées.

Exemple :**Modification ou suppression d'une règle**

Vous pouvez modifier les règles dans l'interface utilisateur. Vous pouvez également modifier les règles avec des fichiers CSV, mais vous devez faire attention. Dans cet exemple, le nom d'hôte purple spécifie Eric tant que propriétaire, mais les deux autres règles spécifiées dans l'exemple précédent sont supprimées.

```
@ruleset, owners-by-hostOwner,Eric,hostname,purple
```

Si vous spécifiez un identificateur d'ensemble de règles `@ruleset` dans le fichier CSV, vous supprimez toutes les règles qui ne sont pas spécifiées à nouveau. Ce comportement s'applique à toutes les règles et pas seulement aux règles modifiées. Par conséquent, le fichier CSV suivant supprime toutes les règles dans la portée `owners-by-host` :

```
@ruleset, owners-by-host@ruleset, owners-by-appOwner, Foo, Application, Bar
```

WARNING

En raison de ce comportement de règle, nous vous recommandons de conserver une copie principale du fichier CSV et de le modifier uniquement.

Informations complémentaires :

- [Organisation des composants à l'aide de perspectives](#)
- [Configuration de la vue Expérience](#)

Utilisation de stratégies de décoration pour filtrer les règles d'attribut

Les attributs décorés sont créés ou mis à jour automatiquement suivant les règles d'attribut. Une stratégie de décoration permet de définir les règles d'attribut à appliquer à la carte du Team Center. A intervalle régulier, DX APM met à jour tous les noeuds applicables qui respectent les règles de la stratégie de décoration. Les stratégies de décoration vous permettent d'organiser et d'afficher les noeuds dans votre environnement d'application surveillé dans Team Center.

Les options suivantes vous permettent de filtrer différents types de stratégies de décoration :

- Tout : affiche toutes les règles d'attribut que vous avez créées.
- CSV Created Rules (Règles créées dans un CSV) : affiche les règles d'attribut de CSV.
- Manually Created Rules (Règles créées manuellement) : affiche toutes les règles d'attribut créées manuellement dans l'onglet Attribute Rules (Règles d'attribut).

Procédez comme suit :

- Dans DX APM, passez le curseur sur le volet de gauche et cliquez sur **Attributs**.
- Cliquez sur **Attribute Rule:<option>** (Règle d'attribut), puis sélectionnez une stratégie.
La liste des règles d'attribut s'actualise et affiche les règles qui appartiennent à la stratégie.

Informations complémentaires : [Définition du mode de surveillance de l'environnement à l'aide de règles d'attribut](#)

Ajustement de la surveillance des alertes

En tant qu'administrateur APM, vous pouvez créer, modifier et supprimer des alertes. Définissez des seuils de performances pour les mesures afin que les analystes puissent identifier lorsqu'un composant spécifique est en cours de chargement. Créez des alertes et définissez des seuils pour identifier les problèmes avant que l'expérience client ne soit affectée.

Création d'une alerte

En tant qu'administrateur, vous pouvez créer des alertes afin de surveiller efficacement les éventuels problèmes dans votre environnement.

Procédez comme suit :

- Dans le volet de gauche, passez le curseur sur l'icône représentant une cloche, puis cliquez sur **Alertes**.
- Cliquez sur **Créer une alerte**.
- Entrez des valeurs dans les champs **Nom de l'alerte** et **Description**.
- Maintenez le bouton bascule sur **Actif**.
- Entrez des valeurs dans les champs **Spécificateur de l'agent** et **Spécificateur de mesure**.

Spécificateur de l'agent : spécifie une expression régulière qui filtre les informations envoyées à la mesure et spécifie les données jusqu'au nom de l'agent inclus. Cette expression détermine les agents auxquels sont limitées les données regroupées. Par exemple, l'expression `(.*)\WPS2-0[1,2]` recherche des agents de tous les domaines nommés WPS2-01 ou WPS2-02. L'expression d'agent est importante lorsque plusieurs machines virtuelles Java génèrent un rapport sur le même gestionnaire d'entreprise, mais servent à des fins différentes. Par exemple, différents

sites Web dans la même entreprise. Dans ce cas, vous utilisez une expression régulière afin de limiter le groupement de mesures aux agents filtrés.

Spécificateur de mesure : spécifie une expression régulière indiquant la mesure et la ressource. Une ressource est une chaîne de dossiers menant à la mesure. Par exemple, l'expression LDAP\([^\:]*\)\\.*:Response Time\(\ms\) recherche toutes les ressources dans le dossier de ressource LDAP. L'expression recherche uniquement la mesure Temps de réponse (ms) dans ces ressources.

6. (Facultatif) Cliquez sur **+** à côté du champ **Spécificateur de mesure** pour ajouter d'autres champs pour les valeurs de **Spécificateur de l'agent** et **Spécificateur de mesure**.
7. Entrez des valeurs dans les champs **Seuil de danger** et **Seuil d'avertissement**.
8. Cliquez sur **Créer une alerte**.

Vous avez créé une alerte.

Création d'une alerte à partir de la vue des mesures

Vous pouvez créer des alertes dans la page Vue des mesures.

Procédez comme suit :

1. Parcourez l'arborescence des mesures pour sélectionner une mesure, par exemple, **Erreurs par intervalle**.
2. Cliquez avec le bouton droit sur la mesure.
3. Cliquez sur Nouvelle alerte simple à partir de la mesure Erreurs par intervalle.
La page **Alertes** s'affiche. Les champs **Spécificateur de l'agent** et **Spécificateur de mesure** sont renseignés automatiquement.
4. Entrez des valeurs dans les champs **Nom de l'alerte** et **Description**.
5. Entrez des valeurs dans les champs **Seuil de danger** et **Seuil d'avertissement**.
6. Cliquez sur **Créer une alerte**.

Vous avez créé une alerte.

Création d'une alerte avec les options avancées

Procédez comme suit :

1. Dans le volet de gauche, passez le curseur sur l'icône représentant une cloche, puis cliquez sur **Alertes**.
2. Cliquez sur **Créer une alerte**.
3. Entrez des valeurs dans les champs **Nom de l'alerte** et **Description**.
4. Maintenez le bouton bascule sur **Actif**.
5. Entrez des valeurs dans les champs **Spécificateur de l'agent** et **Spécificateur de mesure**.
6. (Facultatif) Cliquez sur **+** à côté du champ **Spécificateur de mesure** pour ajouter d'autres champs pour les valeurs de **Spécificateur de l'agent** et **Spécificateur de mesure**.
7. Cliquez sur **Afficher les options avancées**.
8. Dans la liste déroulante **Combinaison**, sélectionnez l'une des options suivantes :
 - **N'importe quel type** : si une mesure faisant partie du groupement de mesures d'alerte dépasse le seuil, l'alerte est déclenchée.
 - **Tout** : si toutes les mesures faisant partie du groupement de mesures d'alerte dépassent le seuil, l'alerte est déclenchée.
9. Sélectionnez une option dans la liste déroulante **Opérateur de comparaison** :
 - Inférieur à
 - Supérieur à
 - Egal à
 - Non égal à
10. Entrez des valeurs pour les seuils **Danger** et **Avertissement**.

- Seuil : spécifie une valeur qui déclenche une alerte de risque ou une alerte d'avertissement.
- Périodes dépassant le seuil : spécifie le nombre maximum de périodes que le seuil peut dépasser avant qu'une alerte ne soit déclenchée.
- Périodes observées : spécifie le nombre total de périodes surveillées pour chaque itération d'alerte.

11. Cliquez sur **Créer une alerte**.

Vous avez créé une alerte avec les options avancées.

Définition des seuils de danger et d'avertissement

En tant qu'administrateur, vous pouvez définir des seuils de danger et d'avertissement pour les alertes. Une alerte récupère les informations de performances et les compare avec les valeurs de seuil. L'alerte affiche l'un des états suivants :

- **Vert** : aucune des mesures mises en correspondance par l'alerte n'est en violation des seuils de danger et d'avertissement, comme indiqué par la configuration de l'alerte.
- **Jaune** : une alerte signale un état d'avertissement. Une tentative d'utilisation de l'application ou du composant n'offre probablement pas des résultats satisfaisants.
- **Rouge** : une alerte signale un état de danger, c'est-à-dire un problème qui requiert une attention immédiate.
- **Gris** : une alerte ne renvoie aucune donnée. Les mesures mises en correspondance par l'alerte simple ne renvoie aucune donnée (par exemple, lorsque les agents sont déconnectés).
- **N/D** : une alerte ne renvoie aucune donnée. Une alerte simple n'est pas active ou ne correspond à aucune mesure.

Procédez comme suit :

1. Dans le volet de gauche, passez le curseur sur l'icône représentant une cloche, puis cliquez sur **Alertes**.

La page Alertes s'ouvre et répertorie les mesures suivantes :

- **Application Errors** (Erreurs d'application) : nombre d'alertes déclenchées lorsque le seuil d'erreurs d'application est dépassé.
- **Backend Errors** (Erreurs de composant d'arrière-plan) : une alerte est déclenchée lorsque le seuil d'erreurs de composant d'arrière-plan non SQL ou de service Web est dépassé.
- **Etat de la connexion** : une alerte est déclenchée lorsqu'un problème survient sur l'agent DockerMonitor connecté à la configuration Docker.
- **Utilisation de l'UC** : une alerte est déclenchée lorsque le seuil d'utilisation de l'UC est dépassé.
- **Frontend Errors** (Erreurs de composant frontal) : une alerte est déclenchée lorsque le seuil d'erreurs de groupe d'URL de composant frontal est dépassé.
- **Frontend Response Time** (Temps de réponse de composant frontal) : une alerte est déclenchée lorsque le seuil de temps de réponse du groupe URL de composant frontal est dépassé.
- **Frontend Stalls** (Blocages de composant frontal) : une alerte est déclenchée lorsque le seuil de blocages de groupe d'URL de composant frontal est dépassé. Un blocage est une demande de composant frontal qui ne s'est pas terminée pendant une période spécifique (30 secondes par défaut). Les blocages indiquent le blocage d'un thread en raison d'une boucle infinie, d'un interblocage ou de ressources limitées.
- **Heap Used Percent** (Pourcentage d'utilisation de segment de mémoire) : une alerte est déclenchée lorsque le seuil de pourcentage d'utilisation du segment de mémoire est dépassé.
- **Response Time Variance Intensity** (Intensité de l'écart dans les temps de réponse) : une alerte est déclenchée lorsque le seuil d'intensité de l'écart dans les temps de réponse est dépassé.
L'intensité de l'écart est une mesure de stabilité comprise entre 10 et 40 :

- 10 : stable
 - 11 à 25 : relativement stable
 - 25 à 30 : modérément instable
 - 30 à 40 : gravement instable
- **WebService Client Errors** (Erreurs de client de service Web) : une alerte est déclenchée lorsque le seuil d'erreurs de services Web (SOAP ou REST) côté client est dépassé.
 - **WebService Server Errors** (Erreurs de serveur de service Web) : une alerte est déclenchée lorsque le seuil d'erreurs de service Web côté serveur est dépassé.
2. Développez l'alerte que vous voulez configurer.
 3. Dans le champ Seuil de danger, entrez la valeur qui déclenche une alerte Danger.
 4. Dans le champ Avertissement, entrez la valeur qui déclenche une alerte Avertissement.
Les unités correspondent à la valeur utilisée dans le groupement de mesures. Par exemple, si vous créez une alerte simple pour la mesure Temps de réponse moyen, la valeur est exprimée en millisecondes.
 5. Cliquez sur **Enregistrer l'alerte**.

TIP

Conseil : Evitez de définir des seuils pouvant générer des alertes trop fréquentes. Vous souhaitez recevoir une alerte sans être inondé de résultats.

Activation ou désactivation d'alertes

Vous pouvez spécifier les alertes à utiliser pour la surveillance. La page Alertes affiche une liste d'alertes disponibles de façon concise.

Procédez comme suit :

1. Dans le volet de gauche, passez le curseur sur l'icône représentant une cloche, puis cliquez sur **Alertes**.
La page Alertes s'ouvre et répertorie des alertes.
2. Recherchez l'alerte que vous souhaitez activer ou désactiver.
3. (Facultatif) Cliquez sur un nom de colonne pour trier les éléments par valeur d'en-tête.
4. Cliquez sur une ligne pour développer les détails de l'alerte.
5. Définissez le bouton bascule sur **Actif** ou **Inactif**.
6. Cliquez sur **Enregistrer**.

L'alerte est active ou inactive.

Suppression d'une alerte

En tant qu'administrateur, vous pouvez supprimer une alerte dont vous n'avez plus besoin.

Procédez comme suit :

1. Dans le volet de gauche, passez le curseur sur l'icône représentant une cloche, puis cliquez sur **Alertes**.
2. Développez l'alerte que vous voulez supprimer.
3. Cliquez sur **Supprimer**.

Vous avez supprimé une alerte.

Présentation des expressions régulières

Les expressions régulières définissent les mesures à inclure dans la définition de l'alerte. Une expression régulière (Perl RegEx) est une chaîne de texte qui décrit un modèle de recherche.

Spécificateur de l'agent

Un spécificateur d'agent définit les agents à partir desquels l'alerte récupère les données. Par exemple, un spécificateur d'agent applique une alerte uniquement sur les agents de tous les domaines nommés WPS2-01 ou WPS2-02.

Un spécificateur d'agent est utile lorsque plusieurs machines virtuelles Java génèrent un rapport sur le même gestionnaire d'entreprise, mais servent à des fins différentes. Par exemple, à l'exécution de différents sites Web dans la même entreprise. Dans ce cas, vous limitez les agents auxquels sont appliqués le groupement de mesures à l'aide d'expressions régulières pour créer un filtre.

Les spécificateurs d'agent utilisent les parties suivantes :

1. Nom de l'hôte qui exécute le processus à surveiller
2. Nom du processus particulier dans une application ou une instance d'application Java gérée à partir duquel vous souhaitez collecter des données
3. Agent responsable de la collecte des données

Spécificateur de mesure

Un spécificateur de mesure définit les mesures à inclure dans l'alerte. Le spécificateur de mesure filtre toutes les données que les agents fournissent en fonction de leur expression d'agent. Vous devez être plus prudent lorsque vous utilisez les spécificateurs de mesure, car le nombre de mesures filtrées dépasse le nombre d'agents.

Les spécificateurs de mesures utilisent les parties suivantes :

1. Ressources menant à la mesure
2. Nom de la mesure

Gestion des données de mesures à l'aide des modules de gestion

Vous pouvez utiliser des modules de gestion pour gérer et organiser les données de mesures à surveiller. Les modules de gestion sont des collections d'objets et de paramètres.

Modules de gestion

Les modules de gestion pour chaque domaine contiennent des éléments. Les éléments sont des objets qui contiennent et organisent des données de mesures avec la logique de surveillance, pour la présentation dans Team Center. Les éléments sont les suivants :

- Groupements de mesures
- Alertes (qui inclut des alertes simples)
- Modules de gestion
- Calculatrices

Un module de gestion par défaut est intégré au superdomaine lors de l'installation d'Introscope. Ce module de gestion par défaut contient des tableaux de bord préconfigurés qui incluent la logique de surveillance des performances communément utilisée. Création d'autres modules de gestion pour les autres domaines créés.

Le module APM Infrastructure Management qui contient la définition des alertes et d'autres objets couvrant les principales mesures d'intégrité APM est un module utile.

NOTE

Pour afficher les alertes dans Team Center, assurez-vous que les mesures sont mappées vers les noeuds et que l'option Propager vers Team Center est activée. Accédez à Team Center, Management. La case à cocher Propager vers Team Center se trouve dans la définition de l'alerte.

NOTE

Une icône Maintenance sur la page Modules de gestion sous l'onglet Maintenance indique que la page est en cours de maintenance. L'icône Maintenance sera visible pendant une période maximale de 7 jours à l'avance pour toute maintenance à venir.

L'icône de maintenance s'affiche en fonction de l'ordre de priorité suivant :

1. Actif avec l'heure de fin la plus récente
2. Actif avec l'heure de fin la plus courte
3. Planifié avec l'heure de début la plus proche
4. Reste de la planification

Autorisations, application du domaine et modification d'éléments

Les agents sont partitionnés en domaines. Les utilisateurs sont autorisés à accéder à certains domaines et peuvent uniquement créer des éléments et des modules de gestion qui référencent des données dans les domaines auxquels ils appartiennent. Pour créer ou modifier des éléments, vous devez disposer des autorisations appropriées. Pour effectuer la plupart des modifications apportées aux éléments, vous devez disposer des droits d'accès en écriture au domaine dans lequel l'élément est contenu. Certaines fonctions requièrent une autorisation spécifique. Rappelez-vous que lors de la création ou de la modification d'un élément, les éléments dans des domaines individuels peuvent uniquement référencer d'autres éléments dans le même domaine. Les éléments du superdomaine peuvent référencer des éléments dans tout domaine.

Si vous êtes l'utilisateur avancé, vous pouvez effectuer les opérations CRUD sur les alertes, les modules de gestion, les outils de calcul et les groupements de mesures.

Personnalisation des modules de gestion

Utilisez les modules de gestion d'infrastructure par défaut et APM avec de nouveaux déploiements APM. Les modules peuvent être personnalisés pour répondre aux besoins de surveillance de votre organisation. La personnalisation est particulièrement valide pour les déploiements effectuant une mise à niveau à partir de versions antérieures ou de déploiements APM à grande échelle. Vous devez personnaliser les modules de gestion mentionnés précédemment et vos propres modules de gestion avant de passer à la production. Vous pouvez appliquer les paramètres de personnalisation suivants :

- Activation ou désactivation des alertes
- Définition des seuils d'alerte appropriés
- Ajuster les périodes sur un seuil
- Activer ou désactiver la case à cocher **Propager vers Team Center**

Le module Gestion des systèmes de la page d'accueil de Team Center contient des alertes et des groupements de mesures requis pour les appels d'arrière-plan, l'UC, la mémoire et le statut d'intégrité de niveau application. Les administrateurs APM ne sont pas censés ajuster ce module de gestion.

NOTE**Informations complémentaires :**

- [Activation/Désactivation des alertes et des actions](#)

La vidéo ci-après explique comment utiliser les modules de gestion dans APM Team Center :

Vous pouvez utiliser des modules de gestion pour gérer et organiser les données de mesures à surveiller. Les modules de gestion sont des collections d'objets et de paramètres. Cette section couvre les rubriques suivantes :

- Modules de gestion
- Autorisations, application du domaine et modification d'éléments
- Personnalisation des modules de gestion

Pour gérer et organiser les données de mesure pour la surveillance, reportez-vous à la section [Gestion des données de mesure à l'aide des modules de gestion](#).

Création et utilisation des modules de gestion

Les modules de gestion organisent les éléments de manière à faciliter leur recherche, copie et modification. Les modules de gestion sont stockés sous forme de fichiers *.jar* dans votre <répertoire_base_EM>/config/modules. Des modules de gestion peuvent également être présents dans des domaines de sous-répertoires sous le <répertoire_base_EM>/config/modules. Un utilisateur peut définir ces domaines et le fichier Management Module.jar contenus dans ce répertoire.

Vous pouvez définir un module de gestion comme modifiable/non modifiable ou actif/inactif. Lorsqu'un module n'est pas modifiable, les éléments qu'il contient ne le sont pas non plus. Lorsqu'un module de gestion est inactif, les éléments qu'il contient le sont également.

Éléments contenus dans l'éditeur de module de gestion

Le tableau ci-après décrit les éléments de module de gestion :

Élément	Description
module de gestion	Conteneur d'éléments
Alertes	Notifications de problèmes potentiels dans votre application, générées par un processus de comparaison des valeurs de mesure aux valeurs de seuil définies par l'utilisateur et par l'indication d'un statut
Calculatrices	Un outil de calcul effectue la somme ou la moyenne des données de mesures pour générer des mesures personnalisées.
Grouperements de mesures	Objets qui spécifient les mesures concernées ; ils sont utilisés comme blocs de construction pour des éléments tels que des alertes.

Recherche d'éléments de module de gestion

Vous pouvez rechercher un élément de module de gestion à l'aide d'expressions régulières utilisant la syntaxe Lucene.

Remarque : Pour plus d'informations, reportez-vous à la section [Interrogation des événements stockés](#).

Procédez comme suit :

1. Dans l'éditeur de module de gestion, sélectionnez un domaine ou un nœud Module de gestion.
2. Sélectionnez l'onglet **Rechercher**.
3. Dans le volet Filtre, entrez une expression régulière utilisant la syntaxe Lucene.

Remarque : Les caractères spéciaux doivent être échappés. Les chaînes commençant par un astérisque (*) ou un point d'interrogation (?) entraînent une erreur. Ces caractères ne sont pas autorisés au début d'une expression Lucene.

A mesure que vous saisissez une entrée dans le volet **Filtre**, les correspondances s'affichent. Les correspondances s'affichent dans un tableau dans l'onglet **Rechercher**. Ces informations s'affichent pour chaque élément correspondant à la recherche :

- a. Nom de l'élément
- b. Module de gestion auquel l'élément appartient
- c. Domaine auquel le module de gestion appartient

Attribution de noms aux modules de gestion et à leurs éléments

Les règles d'attribution de noms suivantes s'appliquent aux modules de gestion et leurs éléments :

- Les noms des modules de gestion d'un même domaine doivent être uniques.
Vous pouvez utiliser des noms de module de gestion identiques dans des domaines distincts.
- Les noms des éléments de type identique inclus dans un module de gestion unique doivent être uniques.
Par exemple, le nom d'une alerte et d'un outil de calcul peut être **Octets en cours d'utilisation**, mais le nom de deux alertes ne peut pas être **Octets en cours d'utilisation**.
- Des éléments de module de gestion peuvent porter le même nom s'ils se trouvent dans des modules de gestion distincts.
Par exemple, vous pouvez avoir deux alertes nommées **Alerte de servlet A**. Une alerte se trouve dans l'exemple de module de gestion et l'autre dans un module **Module de test** que vous avez créé.

Pour faciliter l'attribution de nom, vous pouvez utiliser l'option **Forcer l'unicité** pour créer et nommer un module de gestion ou un élément :

- Si l'option **Forcer l'unicité** est activée et que vous saisissez un nom non unique, DX APM y ajoute un numéro pour le rendre unique.
Le numéro ajouté s'affiche après la création du modèle de rapport, lorsque vous l'ouvrez dans l'**éditeur de module de gestion**.
- Lorsque l'option **Forcer l'unicité** est désactivée et qu'un nom de modèle de rapport identique existe, DX APM affiche un message d'erreur et le rapport n'est pas créé.

Création d'un module de gestion

Pour créer un module de gestion, effectuez les tâches suivantes :

Procédez comme suit :

1. Dans Team Center, sélectionnez **Modules de gestion**, puis cliquez sur **Créer un module de gestion**.
2. Dans la page Créer un module de gestion, entrez les informations suivantes :
 - a. Dans le champ **Nom du module de gestion**, entrez un nom pour le module de gestion ; ce nom s'affiche dans l'arborescence de l'éditeur de module de gestion.
 - b. Entrez les détails dans le champ **Expression d'agent**. Pour plus d'informations, consultez la section [Définition d'expressions d'agent pour un module de gestion](#).
 - c. Dans le champ **Description**, entrez la description requise permettant d'identifier le module de gestion que vous créez.
 - d. Cliquez sur **Enregistrer**.
Vous venez de créer le module de gestion.
3. Cliquez sur **OK**.
Le module de gestion s'affiche dans l'arborescence de l'**éditeur de module de gestion**. Les modules sont actifs et modifiables au moment de la création.

Mise à jour d'un module de gestion

Pour mettre à jour un module de gestion, effectuez les tâches suivantes :

Procédez comme suit :

1. Dans **Paramètres**, cliquez sur **Modules de gestion**.
2. Les modules de gestion disponibles pour l'utilisateur s'affichent. Vous pouvez également rechercher un module de gestion spécifique à l'aide du filtre.
3. Cliquez sur le nom du module de gestion approprié. La page **Modifier le module de gestion** correspondant s'affiche.
4. Sur la page **Modifier le module de gestion**, mettez à jour les détails suivants :
 - a. Cliquez sur le bouton bascule pour marquer le module de gestion comme actif ou inactif.

- b. Dans le champ **Nom du module de gestion**, entrez un nom pour le module de gestion (le nom s'affiche dans l'arborescence de l'éditeur de module de gestion).
- c. Dans le champ **Description**, mettez à jour la description requise permettant d'identifier le module de gestion que vous créez.
- d. Dans le champ **Nom du fichier Jar**, mettez à jour le nom du fichier `.jar` du module de gestion, à l'aide des caractères alphanumériques sans espace (à des fins de compatibilité avec tous les systèmes d'exploitation).
- e. Mettez à jour les détails du champ **Expression d'agent**. Pour plus d'informations, consultez la section [Définition d'expressions d'agent pour un module de gestion](#).
- f. Le tableau **Aperçu** affiche une liste de tous les agents connectés et leur état (Connecté ou Déconnecté).
- g. L'utilisateur peut basculer vers d'autres paramètres liés à ce module de gestion, tels que les groupements de mesures, les alertes, les alertes récapitulatives, les outils de calcul et l'analyse différentielle, pour les mettre à jour.
- h. Cliquez sur **Enregistrer**.
Le module de gestion est mis à jour.
- i. Dans la boîte de dialogue de confirmation, cliquez sur **OK**.
Le module de gestion mis à jour s'affiche sur la page **Modules de gestion**.

Activation ou désactivation d'un module de gestion

Si le module de gestion est inactif, tout son contenu le sera aussi.

Procédez comme suit :

1. Sélectionnez le module de gestion dans l'arborescence de l'éditeur de module de gestion.
2. Dans le volet Paramètres du module de gestion, sélectionnez ou désélectionnez la case à cocher **Actif**.
3. Cliquez sur **Appliquer**.

Copie d'un module de gestion

Pour copier un module de gestion, effectuez les tâches suivantes :

1. Dans **Paramètres**, cliquez sur **Modules de gestion**.
2. Les modules de gestion disponibles pour l'utilisateur s'affichent. Vous pouvez également rechercher un module de gestion spécifique à l'aide du filtre.
3. Cliquez sur le nom du module de gestion approprié. La page **Modifier le module de gestion** correspondant s'affiche.
4. Sur la page **Modifier le module de gestion**, cliquez sur **Enregistrer en tant que nouvel élément**.
5. Dans la zone **Créer un module de gestion** qui s'affiche, mettez à jour les détails suivants, le cas échéant.
Vous pouvez également ignorer cette étape et cliquer sur **Enregistrer** dans la zone Créer un module de gestion pour créer une copie du module de gestion.

NOTE

La création d'une copie du module de gestion existant copiera les paramètres à partir de l'onglet Propriétés uniquement. Vous devrez peut-être créer d'autres paramètres, si nécessaire.

- a. Cliquez sur le bouton bascule pour marquer le module de gestion comme actif ou inactif.
- b. Dans le champ **Nom du module de gestion**, entrez un nom pour le module de gestion (le nom s'affiche dans l'arborescence de l'éditeur de module de gestion).
- c. Mettez à jour les détails du champ **Expression d'agent**. Pour plus d'informations, consultez la section [Définition d'expressions d'agent pour un module de gestion](#).
- d. Dans le champ **Description**, mettez à jour la description requise permettant d'identifier le module de gestion que vous créez.
- e. Cliquez sur **Enregistrer**.
Vous venez de créer le module de gestion.
- f. Dans la boîte de dialogue de confirmation, cliquez sur **OK**.
Le module de gestion s'affiche sur la page **Modules de gestion**.

Suppression d'un module de gestion

La suppression d'un module de gestion entraîne celle de tous les éléments qu'il contient.

Procédez comme suit :

1. Dans Team Center, sélectionnez **Modules de gestion**.
2. Dans le champ **Rechercher**, entrez le `<nom_module_gestion>` à mettre à jour.
Le champ Rechercher renseigne le `<nom_module_gestion>` de votre choix.
3. Avant de supprimer le module de gestion, désactivez-le. Dans le volet Paramètres du module de gestion, sélectionnez ou désélectionnez la case à cocher **Actif**.
4. Cliquez sur **Appliquer**.
5. Dans le volet gauche, cliquez sur le `<nom_module_gestion>`.
La page *Module de gestion* `<nom_module_gestion>` correspondante s'affiche.
6. Cliquez sur l'icône **Supprimer**.
7. Cliquez sur **Oui**.

Exportation d'un module de gestion

Vous pouvez exporter un module de gestion existant au format de fichier *.jar*.

Procédez comme suit :

1. Dans Team Center, sélectionnez **Modules de gestion**, puis sélectionnez **Exporter**.
Tous les modules de gestion sont répertoriés avec des cases à cocher ajoutées.
2. Sélectionnez les modules de gestion à exporter, puis cliquez sur **Exporter**.
Les modules de gestion exportés sont téléchargés dans un répertoire local portant le nom de fichier modules.zip.
3. Vous pouvez extraire le fichier modules.zip.
Tous les modules de gestion sont disponibles sous forme de fichiers *.jar* individuels.

Importation d'un module de gestion

Vous pouvez importer un module de gestion existant au format de fichier *.jar*.

Procédez comme suit :

1. Dans Team Center, sélectionnez **Modules de gestion**, puis sélectionnez **Importer**.
Une boîte de dialogue s'ouvre.
2. Sélectionnez l'option **Sélectionner un fichier**, puis spécifiez le fichier *.jar*.
3. Cliquez sur **Importer** pour importer le fichier.
Le module de gestion s'affiche dans l'arborescence de l'éditeur de module de gestion. Les modules sont actifs et modifiables au moment de la création.

Définition d'expressions d'agent pour un module de gestion

Les groupements de mesures (et leurs agents et expressions de mesure) filtrent les données correspondant aux critères d'agent et de mesure. Tous les groupements de mesures d'un module de gestion peuvent partager un ensemble unique d'expressions d'agent. Vous pouvez ensuite spécifier, au niveau du groupement de mesures, si vous souhaitez utiliser l'expression d'agent partagé ou les expressions d'agent du groupement de mesures.

L'utilisation d'expressions d'agent du module de gestion simplifie la configuration de la logique de surveillance. Vous pouvez modifier les expressions de mesure et d'agent d'un module de gestion et les appliquer à tous les groupements de mesures qu'il contient. Si vous modifiez le déploiement (par ex., le nom de l'ordinateur), vous pouvez modifier le module de gestion ; le changement s'appliquera à tous les éléments qu'il contient. Vous pouvez également copier un module de gestion configuré et modifier l'expression d'agent pour surveiller un agent différent.

NOTE

Il est recommandé d'utiliser des expressions d'agent de module de gestion ou de groupement de mesures, mais pas une combinaison des deux dans un même module de gestion. Vous pouvez également utiliser uniquement des expressions d'agent de groupement de mesures pour surveiller un ensemble de mesures spécifique d'un ensemble d'agents spécifique.

Procédez comme suit :

1. Dans Team Center, sélectionnez **Modules de gestion**.
2. Dans le champ **Rechercher**, entrez le `<nom_module_gestion>` à mettre à jour.
Le champ Rechercher renseigne le `<nom_module_gestion>` de votre choix.
3. Dans le volet gauche, cliquez sur le `<nom_module_gestion>`.
La page *Module de gestion* `<nom_module_gestion>` correspondante s'affiche. Un champ Expressions d'agent vide apparaît.
4. Vous pouvez fournir des informations sur les expressions d'agent de l'une des deux manières suivantes :
 - Entrez les informations dans une expression régulière.
 - Ouvrez une autre fenêtre Investigator, sélectionnez un agent ou une mesure, puis déplacez les informations par glisser-déplacer dans le champ Expressions d'agent. Une ligne s'affiche dans le champ Expressions d'agent.
5. Cliquez sur **Appliquer**.

NOTE

Les expressions d'agent définies ici ne sont pas automatiquement appliquées aux groupements de mesures. Utilisez les expressions d'agent de module de gestion au lieu des expressions d'agent de groupement de mesures. Pour plus d'informations sur ce processus, reportez-vous à la section [Configuration de groupements de mesures dans Team Center](#).

Configuration de la sécurité du module de gestion

Dans chaque univers, des droits individuels sont affectés aux utilisateurs par module de gestion pour modifier des alertes, des outils de calcul et des groupes de mesures. Le rôle Utilisateur avancé, les utilisateurs et les groupes d'utilisateurs doivent disposer de l'autorisation d'afficher ou de créer des alertes, des outils de calcul ou des groupes de mesures pour un module de gestion.

Suivez les instructions de la section [Configuration d'univers](#) pour définir la sécurité du module de gestion.

Configuration des groupements de mesures dans Team Center

Vous pouvez configurer des groupements de mesures dans Team Center. Les groupements de mesures s'affichent dans la liste des dossiers et représentent les modules de gestion. Chaque dossier contient une liste de groupements de mesures correspondants.

Spécification d'expressions pour les groupements de mesures

Les groupements de mesures sont des objets Module de gestion qui enregistrent les informations suivantes :

- L'*expression de l'agent* : une expression régulière dans Perl 5 qui filtre les entrées dans la mesure en spécifiant les données, y compris l'agent.
- L'*expression de mesure* : il s'agit d'une expression régulière dans le langage Perl 5 qui spécifie la ressource (chaîne de dossiers vers la mesure) et la mesure.
- Le module de gestion auquel appartient le groupement de mesures.

Examinez cet exemple du module de gestion Prise en charge. Le groupement de mesures disk usage (Mo) utilise les expressions suivantes :

- **Expression de l'agent de groupement de mesures :**


```
(.*)\\Custom Metric Process \\(Virtual\\)\\(\\(.*)
```

• Expression de mesure :

```
Enterprise Manager\\|Data Store\\(\\(.*)Disk Usage \\(mb\\)
```

Pour remplir ces champs, vous pouvez saisir les informations à l'aide du langage d'expressions régulières Perl 5 ou sélectionner des mesures et des agents et les déplacer par glisser-déposer à partir d'Investigator vers les champs. Pour spécifier un spécificateur de mesure non sensible à la casse, saisissez une valeur oscillant entre (?i) et (?-i). Par exemple,

```
(?i)jmx(?-i)\\|JVM\\|Threading:Current Thread Count
```

Vous pouvez définir des expressions d'agent par module de gestion. Vous pouvez ensuite appliquer ces expressions d'agent à des groupements de mesures dans un module de gestion.

Par défaut, chaque groupement de mesures utilise ses propres expressions d'agent pour mettre des agents en correspondance. Pour utiliser les expressions d'agent du module de gestion, sélectionnez cette option dans le panneau des paramètres de groupement de mesures. Si vous sélectionnez cette option, les agents correspondants changent automatiquement lorsque les expressions de l'agent du module de gestion sont modifiées.

Structure des noms de mesure

Un nom de mesure complet présente la syntaxe suivante :

```
Domain|Hostname|Process|AgentName|Resource:Metric
```

Par exemple, le nom complet d'une mesure dans une ressource est similaire à l'exemple suivant :

```
Acme|c1737019-a|AcmeUSA|AcmeWest|GC Heap:Bytes In Use
```

Si une mesure se trouve dans deux ressources, le nom sera similaire à l'exemple suivant :

```
Acme|c1737019-a|AcmeUSA|AcmeWest|Servlets|FileServlet:Responses Per Second
```

Si des couches de ressource plus profondes sont présentes, les ressources sont séparées par une barre verticale (|).

Pour plus d'informations sur la création de noms de mesure, reportez-vous à la section Utilisation des variables.

NOTE

Pour les utilisateurs de domaines différents de SuperDomain, le nom de la mesure s'affiche sans les informations de domaine avec la syntaxe suivante : *nom_hôte|processus|nom_agent|ressource:mesure*.
Exemple : c1737019|AcmeUSA|AcmeWest|GC Heap:Bytes In Use

Création d'un groupement de mesures à partir du menu Éléments

Vous pouvez créer un groupement de mesures à partir du menu Éléments.

Procédez comme suit :

1. Dans Team Center, sélectionnez **Groupements de mesures**.
La page de groupements de mesures affiche une liste de mesures regroupées en fonction des modules de gestion.
2. Dans la page Groupements de mesures, sélectionnez **Créer un groupement de mesures**.
3. Dans la page Créer un groupement de mesures, entrez les informations suivantes :
 - a. Dans le champ **Nom du groupement de mesures**, entrez un nom de groupement de mesures unique ; celui-ci s'affichera dans l'arborescence de l'éditeur de module de gestion.
 - b. Dans la liste déroulante, sélectionnez le **module de gestion** qui contiendra le groupement de mesures. Vous pouvez également sélectionner **Créer un module de gestion** pour créer un module de gestion dans une boîte de dialogue distincte.
 - c. Dans le champ **Description**, entrez la description requise permettant d'identifier le groupement de mesures que vous créez.

- d. Sélectionnez les expressions d'agent requises à utiliser :
 - Sélectionnez **Utiliser des expressions de l'agent de module de gestion** pour utiliser les expressions d'agent définies pour le module de gestion.
 - Sélectionnez **Utiliser des expressions de l'agent de groupement de mesures** pour utiliser des expressions d'agent définies pour ce groupement de mesures.
- e. Entrez les informations d'agent et de mesure spécifiques dans les champs d'**expression d'agent de module** et d'**expression de mesure**.
- f. Sélectionnez **Créer**.
Le groupement de mesures est correctement créé.

NOTE

Le groupement de mesures est actif une fois créé et ne peut pas être désactivé.

Personnalisation de groupements de mesures

Vous pouvez personnaliser les expressions régulières dans le groupement de mesures en modifiant les champs Expressions de l'agent de groupement de mesures et Expressions de mesure pour spécifier les mesures à mettre en correspondance.

Règles de modification de groupements de mesures

- Séparez les niveaux successifs de l'arborescence Investigator à l'aide de barres obliques inverses. La barre oblique inverse sert de caractère d'échappement.
- Dans Expressions de l'agent de groupement de mesures : hôte\|processus\|nom_agent, utilisez **([^\|:]*)** pour représenter un segment de ressource.
- Dans **Servlets\|([^\|:]*)Temps de réponse moyen(ms\)**, un caractère d'échappement (barre oblique inverse) est requis pour les séparateurs \| et les parenthèses \(et \).
- Dans **Servlets\|Servlet1:Temps de réponse moyen (ms\)**, vous pouvez inclure des listes d'éléments entre parenthèses à l'aide de barres verticales pour les mettre en correspondance avec une expression.
- Dans **Servlets\|Servlet(1|14|18):Temps de réponse moyen (ms\)**, si aucun dossier de ressources ne figure entre le nom d'agent et la mesure, entrez uniquement le nom de la mesure. Dans le cas contraire, séparez les dossiers de ressources par une barre oblique inverse et insérez le signe des deux-points (:) avant le nom de la mesure.
- Dans Expressions de mesure : **ressource\|sous-ressource:mesure**
- Dans Expressions de mesure : **ressource:mesure**
- Dans Expressions de mesure : **mesure**
- Par exemple, dans Expressions de mesure, spécifiez la durée moyenne de requête JDBC pour un servlet appelé OptionReport comme suit : **Servlets\|OptionReport\|JDBC:Average Query Time**.
- Utilisez **(.*)** pour représenter "tous les types".
- Par exemple, **Cherubim\|PhoneHome\|(.*)** suivi de **Sockets:Output Bandwidth** spécifie la bande passante de sortie de tous les sockets pour toutes les instances du processus PhoneHome exécuté sur l'hôte Cherubim.
- L'entrée **File System:(.*)** dans le champ Expressions de mesure signifie que les données à afficher sont les mesures d'entrée et de sortie du fichier détectées dans Investigator sous File System. En revanche, **File System:File Input Rate** affiche le taux d'entrée du fichier uniquement.
- Utilisez **(.*)\|(.*)\|(.*)** dans le champ Agent pour que le groupement de mesures affiche les données à partir de tout type de serveur, de processus ou d'agent. Vous pouvez indiquer un ou plusieurs segments à mettre en correspondance avec des agents avec un nom d'hôte, de processus ou d'agent spécifique.
- Pour exclure une branche de l'arborescence des mesures, utilisez une antémémoire négative dans l'expression régulière du groupement de mesures. Par exemple, **Agents\|(.*)\|(.*)\|(?!ima_q01)([^\|:]*)ConnectionStatus** exclut le ConnectionStatus de ima_q01, mais affiche toujours le ConnectionStatus d'autres agents.


Procédez comme suit :

1. Dans Team Center, sélectionnez **Grouper les mesures**.
La page de groupements de mesures affiche une liste de mesures regroupées en fonction des modules de gestion.
2. Développez le groupe de mesures à supprimer.
3. Sélectionnez le *nom_groupe_mesures* à supprimer.
La page **Modifier le groupement de mesures : <nom_groupe_mesures>** s'affiche.
4. Modifiez la définition en appliquant les [règles de modification de groupements de mesures](#).
5. Si nécessaire, sélectionnez le **signe Plus (+)** pour spécifier d'autres mesures pour le groupement.
6. Sélectionnez **Appliquer**.

Suppression d'un groupe de mesures à partir du menu Éléments

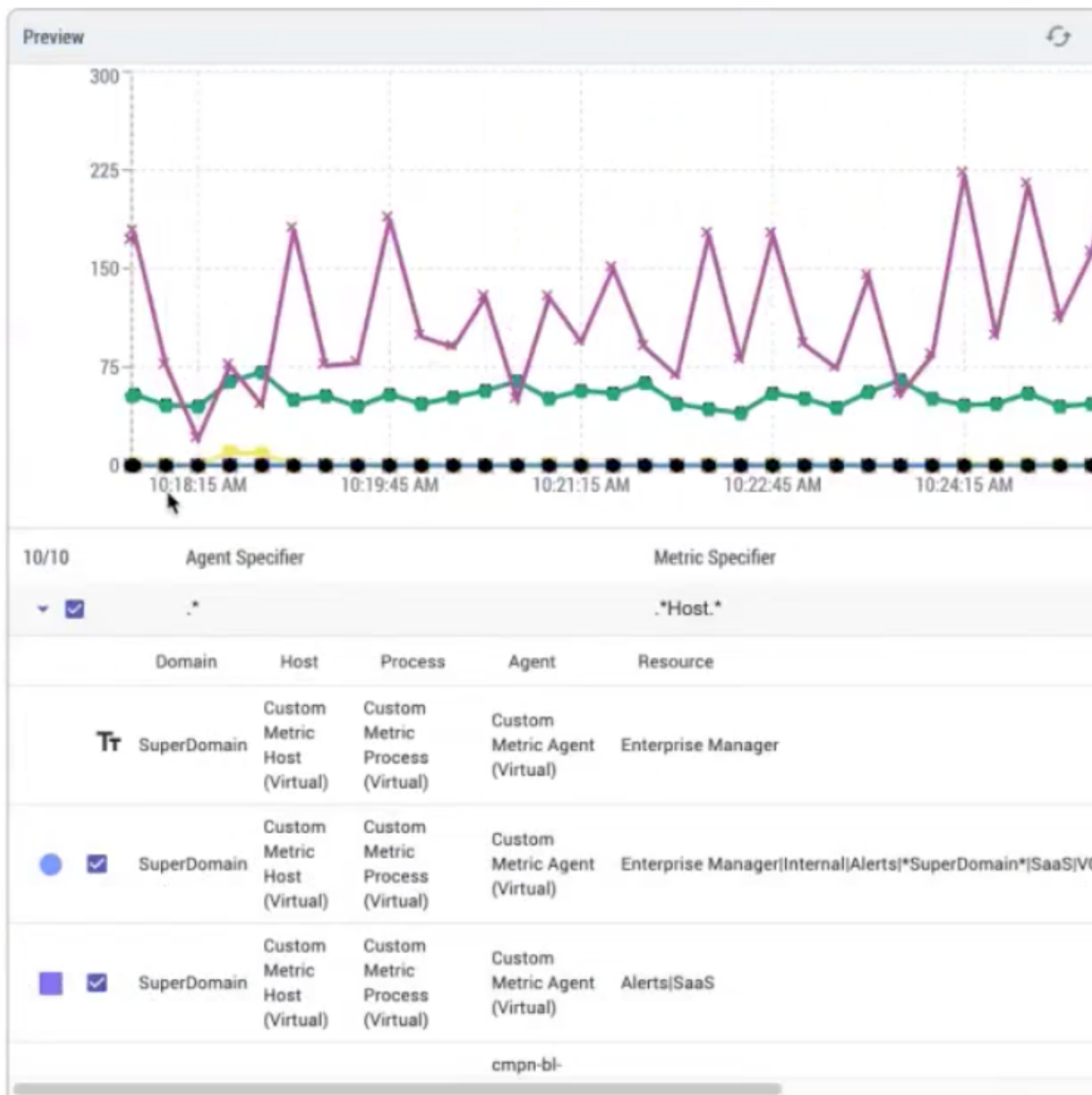
Vous pouvez supprimer un groupement de mesures à partir du menu Éléments.

Procédez comme suit :

1. Dans Team Center, sélectionnez **Grouper les mesures**.
La page de groupements de mesures affiche une liste de mesures regroupées en fonction des modules de gestion.
2. Développez le groupe de mesures à supprimer.
3. Sélectionnez le *nom_groupe_mesures* à supprimer.
La page **Modifier le groupement de mesures : <nom_groupe_mesures>** s'affiche.
4.
Sélectionnez l'icône Supprimer ().
5. Sélectionnez **Oui**.

Aperçu du groupement de mesures

L'aperçu de la vue des mesures affiche le mode d'aperçu des groupes de mesures configurés. Vous pouvez afficher les données de mesures pertinentes tracées dans le graphique. La fenêtre Aperçu affiche le graphique de données des mesures basé sur le **Spécificateur de l'agent** et le **Spécificateur de mesure** fournis dans le champ **Expressions**.



Dans la fenêtre Aperçu, vous pouvez afficher et effectuer les tâches suivantes :

- Spécifiez le **Spécificateur de mesure** et le **Spécificateur de l'agent** dans le champ **Expressions** et l'icône **Actualiser**













est mise en surbrillance. Cliquez sur l'icône Actualiser pour afficher les dernières mesures en fonction des expressions.

- Le tableau Aperçu affiche le nombre total de mesures, le spécificateur d'agent, le spécificateur de mesure et le nombre de mesures à afficher dans le graphique.
- Vous pouvez sélectionner uniquement dix mesures à afficher dans le graphique.
- Vous pouvez personnaliser les colonnes à afficher dans le tableau. Cliquez sur



et sélectionnez les colonnes requises dans la liste.

- Dix couleurs et formes différentes sont disponibles pour distinguer les mesures représentées sur le graphique. Lorsque vous sélectionnez une mesure dans la liste, une couleur et une forme sont automatiquement affectées à une mesure.

	Value	Min	Max	Count
	0	0	0	0
	6	6	6	1
	0	0	0	1
	0	0	0	1
	0	0	0	1
	45	45	45	1
	0	0	0	1
	4	4	4	1
	0	0	0	1
	0	0	0	1
3/31/21 3:21:15 PM				

- Cliquez sur l'icône Plein écran



pour afficher la fenêtre Aperçu en mode plein écran.

- Sur le graphique d'aperçu, l'axe X représente les valeurs de mesure et l'axe Y représente la plage horaire.

Vous pouvez configurer des groupements de mesures dans Team Center. Les groupements de mesures s'affichent dans la liste des dossiers et représentent les modules de gestion. Chaque dossier contient une liste de groupements de mesures correspondants.

Pour plus d'informations sur les éléments suivants, consultez la section [Configuration des groupements de mesures dans Team Center](#).

- Spécification d'expressions pour les groupements de mesures
- Structure des noms de mesure
- Création d'un groupement de mesures à partir du menu Eléments
- Personnalisation de groupements de mesures
- Suppression d'un groupe de mesures à partir du menu Eléments
- Aperçu du groupement de mesures

Création et configuration d'alertes simples dans Team Center

En tant qu'administrateur, vous pouvez créer et configurer des alertes et des actions dans Team Center pour surveiller les performances.

NOTE

N'utilisez pas la méthode standard de création d'alertes APM pour les mesures ingérées directement dans NASS (cela inclut les mesures de prise en charge du proxy cloud APM et toute mesure non APM). Utilisez plutôt la [configuration d'alertes basées sur les mesures](#) de DX OI.

NOTE

Une icône Maintenance sur la page Alertes sous l'onglet Maintenance indique que la page est en cours de maintenance. L'icône Maintenance sera visible pendant une période maximale de 7 jours à l'avance pour toute maintenance à venir.

L'icône de maintenance s'affiche en fonction de l'ordre de priorité suivant :

1. Actif avec l'heure de fin la plus récente
2. Actif avec l'heure de fin la plus courte
3. Planifié avec l'heure de début la plus proche
4. Reste de la planification

Team Center fournit les alertes suivantes :

Alerte simple

Utilise les informations de statut générées par un processus de comparaison pour les comparer aux valeurs de seuil définies par l'utilisateur. La sortie d'une alerte simple est un statut. Les alertes simples peuvent utiliser les délais d'action Danger et Avertissement pour déterminer à quel moment les actions spécifiées doivent être lancées. Une alerte simple peut présenter l'un des états suivants :

- **Not reporting data (Aucune donnée n'est collectée.)**

Cet état est généré si l'alerte simple est inactive, ne correspond à aucune mesure, ou que les mesures correspondantes ne sont pas signalées.

- **Vert (Ok)**
- **Jaune (Avertissement)**
- **Rouge (Danger)**

L'alerte simple est l'alerte de base dans Introscope. Les alertes simples peuvent fournir les données d'une alerte récapitulative. Cette alerte s'affiche sous le nœud Alerts (Alertes) dans l'arborescence Investigator.

Alertes récapitulatives

Agrège le statut de plusieurs alertes simples et d'autres alertes récapitulatives. Cette alerte s'affiche sous le nœud Alerts (Alertes) dans l'arborescence Investigator.

NOTE

Informations complémentaires : [Création et configuration d'alertes récapitulatives](#)

Création d'une alerte simple à partir du menu Éléments

Procédez comme suit :

1. Dans Team Center, sélectionnez **Alertes**, puis **Créer une alerte**.
La page Alertes affiche une liste d'alertes divisées en groupement de mesures.
2. Dans la page Alertes, sélectionnez **Créer une alerte**.
3. Dans la page Créer une alerte, entrez les informations suivantes :
 - a. Dans le champ **Nom de l'alerte**, entrez un nom pour l'alerte simple.

Le nom s'affiche dans l'arborescence de l'éditeur de module de gestion.

TIP

Utilisez des noms d'alerte descriptifs. Nous vous recommandons d'utiliser une convention d'attribution de noms permettant au destinataire de l'alerte d'en identifier la source.

- b. Dans la liste déroulante **Canaux de notification**, sélectionnez le canal à appliquer à l'alerte simple que vous créez.
 - c. Dans la liste déroulante **Module de gestion**, sélectionnez le module à appliquer à l'alerte simple que vous créez. Vous pouvez également sélectionner **Créer un module de gestion** pour créer un module de gestion dans une boîte de dialogue distincte.
 - d. Dans le champ **Description**, entrez la description requise permettant d'identifier l'alerte simple que vous créez.
 - e. Dans le champ **Groupement de mesures**, sélectionnez le groupement de mesures à appliquer à l'alerte simple que vous créez. Vous pouvez également sélectionner **Créer un groupement de mesures** pour créer un **groupement de mesures** dans une boîte de dialogue distincte.
 - f. Dans le champ **Résolution**, spécifiez la durée de résolution en heures, minutes ou secondes. Une alerte utilise les données d'entrée provenant d'un groupement de mesures sélectionné. Pour la période de résolution, l'alerte rassemble les informations et affiche une valeur de synthèse pour cette période. La valeur obtenue dépend du type de données dans la mesure. Par exemple, si la mesure est un taux, la valeur de synthèse est le taux moyen pendant cette période. Si la mesure est un compteur, la valeur correspond à la dernière valeur du compteur. Les valeurs de période de résolution doivent être des incréments de 15 secondes.
 - g. Dans la liste déroulante **Opérateur de comparaison**, sélectionnez une valeur dans la liste déroulante pour la condition déclenchant l'alerte simple. L'opérateur de comparaison (avec les valeurs de seuil Danger et Avertissement) définit la condition qui déclenche l'alerte simple. L'opérateur de comparaison est associé aux valeurs de seuil Danger et Avertissement. Par exemple, si vous souhaitez être averti lorsqu'un temps de réponse moyen de servlet est supérieur à 5 000, utilisez l'opérateur Supérieur à. L'opérateur de comparaison affecte également les valeurs de seuil Avertissement et Danger. Si l'opérateur de comparaison est défini sur Supérieur à, la valeur de seuil Danger doit être supérieure à la valeur de seuil Avertissement. Inversement, si l'opérateur de comparaison est défini sur Inférieur à, la valeur de seuil Danger doit être inférieure à la valeur de seuil Avertissement.
 - h. Dans le champ **Combinaison**, indiquez si une alerte doit être déclenchée lorsqu'une mesure dépasse un seuil ou que toutes les mesures dépassent un seuil. Le champ Combinaison est ignoré lorsque la case à cocher Notifier par mesure individuelle est sélectionnée.
 - i. Dans la section **Seuils**, sélectionnez **Enregistrer**.
Vous venez de créer le module de gestion.
4. Sélectionnez **OK**.

L'alerte simple que vous avez créée est mise en surbrillance dans l'arborescence de l'éditeur de module de gestion et ses paramètres s'affichent dans le volet Paramètres.

Pour plus d'informations sur l'activation de notifications d'alertes, consultez la section [Création de notifications pour les alertes](#). Pour plus d'informations sur la documentation de politique pour la configuration de notifications d'alertes supplémentaires dans Operational Intelligence, reportez-vous à la section [Création d'une politique](#).

Mise à jour d'une alerte simple à partir du menu Eléments

Procédez comme suit :

1. Dans Team Center, sélectionnez **Alertes**. La page Alertes s'affiche avec les alertes divisées en groupement de mesures.
2. Accédez au groupement de mesures de l'alerte à mettre à jour.
3. Sélectionnez le **<Nom_alerte>** à mettre à jour.
4. Dans la page **Modifier l'alerte : <nom_alerte>**, mettez à jour les détails suivants :
 - a. Dans le champ **Nom de l'alerte**, mettez à jour le nom de l'alerte simple.

Le nom s'affiche dans l'arborescence de l'éditeur de module de gestion.

TIP

Utilisez des noms d'alerte descriptifs. Nous vous recommandons d'utiliser une convention d'attribution de noms permettant au destinataire de l'alerte d'en identifier la source.

- b. Dans la liste déroulante **Canaux de notification**, sélectionnez le canal à appliquer à l'alerte simple.
 - c. Dans la liste déroulante **Module de gestion**, sélectionnez le module à appliquer à l'alerte simple. Vous pouvez également sélectionner **Créer un module de gestion** pour créer un module de gestion dans une boîte de dialogue distincte.
 - d. Dans le champ **Description**, mettez à jour la description requise permettant d'identifier l'alerte simple.
 - e. Dans le champ **Groupement de mesures**, sélectionnez le groupement de mesures à appliquer à l'alerte simple. Vous pouvez également sélectionner **Créer un groupement de mesures** pour créer un **groupement de mesures** dans une boîte de dialogue distincte.
 - f. Dans la liste déroulante **Opérateur de comparaison**, sélectionnez une valeur dans la liste déroulante pour la condition déclenchant l'alerte simple. L'opérateur de comparaison (avec les valeurs de seuil Danger et Avertissement) définit la condition qui déclenche l'alerte simple. L'opérateur de comparaison est associé aux valeurs de seuil Danger et Avertissement. Par exemple, si vous souhaitez être averti lorsqu'un temps de réponse moyen de servlet est supérieur à 5 000, utilisez l'opérateur Supérieur à. L'opérateur de comparaison affecte également les valeurs de seuil Avertissement et Danger. Si l'opérateur de comparaison est défini sur Supérieur à, la valeur de seuil Danger doit être supérieure à la valeur de seuil Avertissement. Inversement, si l'opérateur de comparaison est défini sur Inférieur à, la valeur de seuil Danger doit être inférieure à la valeur de seuil Avertissement.
 - g. Dans la section **Seuils**, sélectionnez **Enregistrer**.
Vous venez de créer le module de gestion.
5. Sélectionnez **OK**.

L'alerte simple que vous avez créée est mise en surbrillance dans l'arborescence de l'éditeur de module de gestion et ses paramètres s'affichent dans le volet Paramètres.

Copie d'une alerte simple


Pour copier une alerte simple, effectuez les tâches suivantes.

1. Dans **Paramètres**, cliquez sur **Alertes**.
2. Les modules de gestion disponibles pour l'utilisateur s'affichent. Vous pouvez également rechercher un module de gestion spécifique à l'aide du filtre.
3. Cliquez sur le nom du module de gestion et le nom de l'alerte appropriés.
4. Sur la page **Modifier l'alerte**, cliquez sur **Enregistrer en tant que nouvel élément**.
5. Dans la zone **Créer une alerte** qui s'affiche, mettez à jour les détails suivants, le cas échéant.
Vous pouvez également ignorer cette étape et cliquer sur **Enregistrer** dans la zone Créer une alerte pour créer une copie de l'alerte.
 - a. Cliquez sur le bouton bascule pour marquer l'alerte comme active ou inactive.
 - b. Dans le champ **Nom de l'alerte**, entrez un nom pour l'alerte simple (le nom s'affiche dans l'arborescence de l'éditeur de module de gestion).
 - c. Dans la liste déroulante **Canaux de notification**, sélectionnez le canal à appliquer à l'alerte simple que vous créez.
 - d. Dans la liste déroulante **Module de gestion**, sélectionnez le module à appliquer à l'alerte simple que vous créez. Vous pouvez également sélectionner Créer un module de gestion pour créer un module de gestion dans une boîte de dialogue distincte.
 - e. Dans le champ **Description**, entrez la description requise permettant d'identifier l'alerte simple que vous créez.

- f. Dans le champ **Groupement de mesures**, sélectionnez le groupement de mesures à appliquer à l'alerte simple que vous créez. Vous pouvez également sélectionner Créer un groupement de mesures pour créer un groupement de mesures dans une boîte de dialogue distincte.
- g. Dans le champ **Résolution**, spécifiez la durée de résolution en heures, minutes ou secondes. Une alerte utilise les données d'entrée provenant d'un groupement de mesures sélectionné. Pour la période de résolution, l'alerte rassemble les informations et affiche une valeur de synthèse pour cette période. La valeur obtenue dépend du type de données dans la mesure. Par exemple, si la mesure est un taux, la valeur de synthèse est le taux moyen pendant cette période. Si la mesure est un compteur, la valeur correspond à la dernière valeur du compteur. Les valeurs de période de résolution doivent être des incréments de 15 secondes.
- h. Dans la liste déroulante **Opérateur de comparaison**, sélectionnez une valeur dans la liste déroulante pour la condition déclenchant l'alerte simple. L'opérateur de comparaison (avec les valeurs de seuil Danger et Avertissement) définit la condition qui déclenche l'alerte simple. L'opérateur de comparaison est associé aux valeurs de seuil Danger et Avertissement. Par exemple, si vous souhaitez être averti lorsqu'un temps de réponse moyen de servlet est supérieur à 5 000, utilisez l'opérateur Supérieur à. L'opérateur de comparaison affecte également les valeurs de seuil Avertissement et Danger. Si l'opérateur de comparaison est défini sur Supérieur à, la valeur de seuil Danger doit être supérieure à la valeur de seuil Avertissement. Inversement, si l'opérateur de comparaison est défini sur Inférieur à, la valeur de seuil Danger doit être inférieure à la valeur de seuil Avertissement.
- i. Dans le champ **Combinaison**, indiquez si une alerte doit être déclenchée lorsqu'une mesure dépasse un seuil ou que toutes les mesures dépassent un seuil. Le champ Combinaison est ignoré lorsque la case à cocher Notifier par mesure individuelle est sélectionnée.
- j. Spécifiez les valeurs sous **Seuil de danger** et **Seuil d'avertissement**.
- k. Cliquez sur **Create**.
L'alerte est créée.
- l. Dans la boîte de dialogue de confirmation, cliquez sur **OK**.
L'alerte s'affiche sur la page **Modules de gestion**.

Suppression d'une alerte simple à partir du menu Éléments

Procédez comme suit :

1. Dans Team Center, sélectionnez **Alertes**.
La page Alertes s'affiche avec les alertes divisées en groupement de mesures.
2. Accédez au groupement de mesures de l'alerte à supprimer.
3. Sélectionnez le **<Nom_alerte>** à supprimer.
La page **Modifier l'alerte : <nom_alerte>** s'affiche.
4. Dans la page **Modifier l'alerte : <nom_alerte>**, sélectionnez l'icône Supprimer ().
5. Sélectionnez **Oui**.
6. Sélectionnez **OK**.

L'alerte simple est supprimée.

Configuration des paramètres d'alerte simple

Après avoir créé une alerte simple, définissez les conditions de déclenchement.

Procédez comme suit :

1. Recherchez l'alerte simple que vous avez créée dans l'arborescence de l'éditeur de module de gestion, sous le module de gestion correspondant. Sélectionnez l'alerte simple pour afficher ses paramètres.
2. Dans le volet Paramètres, sélectionnez la case à cocher **Actif** pour activer l'alerte simple. Sélectionnez la case à cocher **Propager vers Team Center** pour afficher les alertes dans Team Center.

3. Utilisez l'opérateur comparaison et les actions Danger et Avertissement pour définir la condition déclenchant l'alerte simple.
Par exemple, si vous souhaitez être averti lorsqu'un temps de réponse moyen de servlet est supérieur à 5 000, utilisez l'opérateur *Supérieur à*.

NOTE

L'opérateur de comparaison affecte également les valeurs de seuil Avertissement et Danger. Si l'opérateur de comparaison est défini sur *Supérieur à*, la valeur de seuil Danger doit être supérieure à la valeur de seuil Avertissement. Inversement, si l'opérateur de comparaison est défini sur *Inférieur à*, la valeur de seuil Danger doit être inférieure à la valeur de seuil Avertissement.

4. Sous les actions Danger ou Avertissement, sélectionnez **Ajouter**.
- Sélectionnez une action, puis cliquez sur **Sélectionner**.
 - Ajoutez une autre action, si nécessaire.
 - Dans le volet Paramètres de l'alerte simple, sélectionnez **Appliquer**.
5. Dans le champ Seuil, entrez une valeur qui déclenche une alerte Danger ou Avertissement.
Les unités des valeurs de seuil Danger correspondent à la valeur utilisée dans le groupement de mesures. Par exemple, pour créer une alerte simple de temps de réponse moyen du servlet, utilisez une valeur en millisecondes.
6. Définissez le nombre de périodes excessives qui déclenche l'alerte. Définissez cette condition dans les champs **Périodes dépassant le seuil** et **Périodes observées**.
Exemple : vous avez saisi les valeurs 8 et 10. L'alerte de danger se déclenche uniquement si la mesure dépasse le seuil de danger dans 8 périodes observées sur 10.

TIP

- Utilisez la propriété *At least N of the last M periods* (Au moins N sur les M dernières périodes) pour définir des alertes de problèmes réels. Cette propriété définit le nombre d'instances nécessaires pour que le seuil Danger déclenche une alerte. Par exemple, dans les environnements de production, les indicateurs clés de performance peuvent atteindre des pics pendant une courte période. Une UC peut atteindre un pic sur une période de 15 secondes, puis revenir à la normale lors de la période de 15 secondes suivante. Ce comportement de performances ne requiert pas d'alerte et peut être exclu à l'aide d'une condition.
- Avant de modifier les seuils existants, nous vous recommandons d'informer les destinataires des alertes. Réduire le seuil d'une alerte active peut entraîner l'envoi de celle-ci.

NOTE

Les alertes seront déclenchées uniquement à la fin de la **période observée** et non dès que le nombre de périodes dépassant le seuil est atteint.

7. Définissez un délai d'action en heures, minutes et secondes.
Les délais d'action Danger et Avertissement déterminent le moment du déclenchement d'une action d'alerte simple.

NOTE

Les délais d'action Danger et Avertissement ne sont pas disponibles sous l'option d'alerte Résolution.

8. Sélectionnez **Appliquer**.
L'alerte simple est créée et s'affiche dans l'arborescence sous le module de gestion correspondant. Ex. : Configuration d'une alerte de déconnexion d'agent

NOTE

Lorsque vous créez une alerte simple à partir d'une mesure, un groupement de mesures est automatiquement créé. Ce groupement de mesures s'affiche dans le même module de gestion.

Configuration d'une alerte de déconnexion d'agent

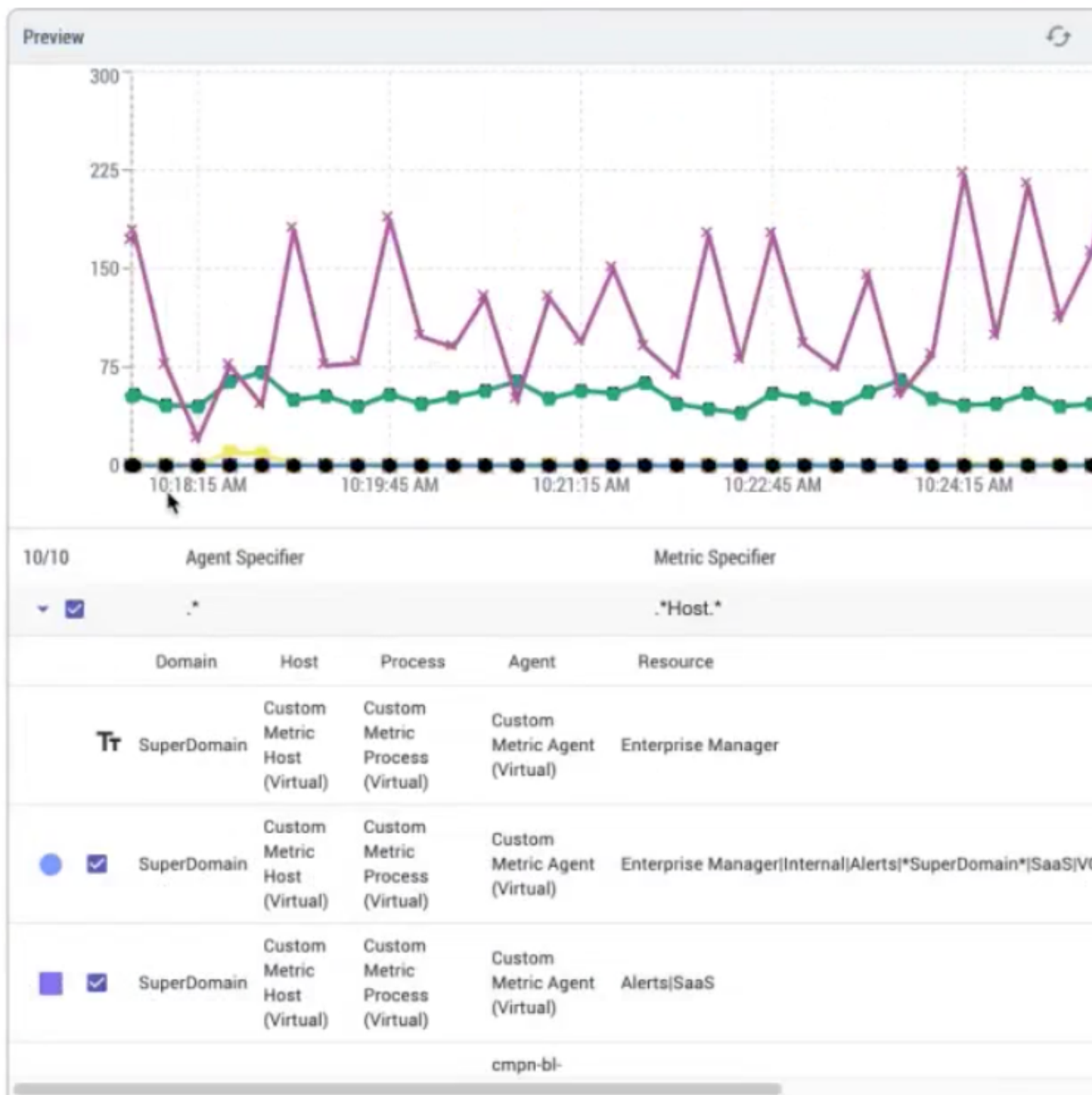
Si un agent se déconnecte du gestionnaire d'entreprise, vous ne pouvez plus collecter ni surveiller ses données. Vous pouvez configurer une alerte pour déclencher une notification qui vous informe en cas de déconnexion.

Procédez comme suit :

1. Dans Team Center, sélectionnez **Groupements de mesures**.
2. Dans la page Groupements de mesures, sélectionnez **Nouveau groupement de mesures**.
3. Cette mesure présente les valeurs suivantes :
 - 3 = déconnecté ; indique que l'agent a été déconnecté manuellement.
 - 2 = connecté, lenteur ou aucune donnée
 - 1 = connecté
 - 0 = démonté ; indique que l'agent a été déconnecté du gestionnaire d'entreprise après une période spécifique. Vous pouvez configurer cette période.
4. Saisissez un nom pour la nouvelle alerte et cliquez sur **OK**.
5. Définissez l'opérateur de comparaison sur **Inférieur à**.
6. Définissez les seuils Danger et Avertissement.
7. Définissez le critère de diffusion de seuil pour l'alerte. **Exemples :**
 - Very Sensitive (Très sensible) (Danger = 2, Avertissement = 2, au moins 1 des 10 dernières périodes)
 - Less Sensitive (Moins sensible) (Danger = 3, Avertissement = 2, au moins 3 des 10 dernières périodes)
8. Sélectionnez **Actif**.
9. Sélectionnez **Appliquer**.

Aperçu des alertes

L'aperçu des alertes affiche le mode d'aperçu des groupes de mesures configurés. Vous pouvez afficher les données de mesures pertinentes tracées dans le graphique. La fenêtre Aperçu affiche le graphique de données de mesures basé sur le champ **Groupement de mesures**.



Dans la fenêtre Aperçu, vous pouvez afficher et effectuer les tâches suivantes :

- Fournissez le filtre pour le champ Groupement de mesures et l'icône **Actualiser**



est mise en surbrillance. Cliquez sur l'icône Actualiser pour afficher les dernières mesures en fonction des expressions.

- Le tableau Aperçu affiche le nombre total de mesures, le spécificateur d'agent, le spécificateur de mesure et le nombre de mesures à afficher dans le graphique.
- Vous pouvez sélectionner uniquement dix mesures à afficher dans le graphique.
- Vous pouvez personnaliser les colonnes à afficher dans le tableau. Cliquez sur



et sélectionnez les colonnes requises dans la liste.

- Dix couleurs et formes différentes sont disponibles pour distinguer les mesures représentées sur le graphique. Lorsque vous sélectionnez une mesure dans la liste, une couleur et une forme sont automatiquement affectées à une mesure.

	Value	Min	Max	Count
	0	0	0	0
	6	6	6	1
	0	0	0	1
	0	0	0	1
	0	0	0	1
	45	45	45	1
	0	0	0	1
	4	4	4	1
	0	0	0	1
	0	0	0	1
3/31/21 3:21:15 PM				

- Cliquez sur l'icône Plein écran



pour afficher la fenêtre Aperçu en mode plein écran.

- Sur le graphique d'aperçu, l'axe X représente les valeurs de mesure et l'axe Y représente la plage horaire.

En tant qu'administrateur, vous pouvez créer et configurer des alertes et des actions dans Team Center pour surveiller les performances. Team Center fournit les alertes suivantes :

- Alerte simple
- Alertes récapitulatives

Pour plus d'informations sur la création, la mise à jour, la suppression et la configuration d'alertes simples, consultez la section [Création et configuration d'alertes simples dans Team Center](#).

Création et configuration d'alertes récapitulatives

Une alerte récapitulative permet d'afficher le statut de plusieurs alertes simples sous-jacentes en un seul statut global. Vous pouvez créer et configurer des alertes récapitulatives dans Team Center, la station de travail ou WebView. Vous pouvez modifier le nom et les alertes simples sous-jacentes dans tous les environnements. Il existe des différences au niveau des notifications et des actions :

- **Team Center** : prise en charge de l'affectation du canal de notification (option préférée)
- **Station de travail** : prise en charge de la création et de l'affectation d'actions de trace de transaction
- **Webview** : prise en charge uniquement de l'affectation d'actions de trace de transaction

Cette section contient les informations suivantes :

- [Alertes récapitulatives](#)
- [Création d'une alerte récapitulative](#)
- [Configuration d'une alerte récapitulative](#)
- [Retards dans les actions de danger et d'avertissement](#)

NOTE

Une icône Maintenance sur la page Alertes récapitulatives indique que la page est en cours de maintenance. L'icône Maintenance sera visible pendant une période maximale de 7 jours à l'avance pour toute maintenance à venir.

L'icône de maintenance s'affiche en fonction de l'ordre de priorité suivant :

1. Actif avec l'heure de fin la plus récente
2. Actif avec l'heure de fin la plus courte
3. Planifié avec l'heure de début la plus proche
4. Reste de la planification

Alertes récapitulatives

Les alertes récapitulatives ne comportent pas de seuils explicites de danger ou d'avertissement ni d'expressions de comparaison, comme c'est le cas pour les alertes simples. Une alerte simple présente l'un des quatre états suivants : sans signalement de données, vert, jaune et rouge.

Icône d'état	Définition	Valeur numérique
Losange ou triangle jaune	Avertissement	2
Octogone ou carré rouge	Danger	3
Disque vert	Normal	1
Disque gris	Sans signalement de données	0

L'état d'alerte récapitulative est le pire état parmi les alertes simples qu'il contient. L'alerte récapitulative peut être définie pour N'importe quel type d'alerte ou Toutes les alertes. L'option N'importe quel type d'alerte utilise l'état maximum de toutes les alertes. L'option Toutes les alertes utilise l'état minimum de toutes les alertes dont l'état est supérieur à 0 (sans signalement de données). Exemple : vous disposez d'une alerte récapitulative qui comprend les alertes suivantes :

- Alerte : A ; État : 0
- Alerte : B ; État : 1
- Alerte : C ; État : 1
- Alerte : D ; État : 2
- Alerte : E ; État : 3

Dans ce cas, l'option N'importe quel type d'alerte adopte l'état 3 et l'option Toutes les alertes l'état 1.

Création d'une alerte récapitulative

Pour Team Center, procédez comme suit :

1. Accédez à **Paramètres**, sélectionnez **Alertes, Alertes récapitulatives**.
2. Cliquez sur **Créer une alerte récapitulative**.

3. Configurez les paramètres d'alertes récapitulatives.

Pour la station de travail ou Webview, procédez comme suit :

1. Dans la fenêtre de l'éditeur de module de gestion, sélectionnez Éléments, Nouvelle alerte, Nouvelle alerte récapitulative.
 2. Saisissez les informations suivantes :
 - **Nom** : permet d'attribuer un nom à l'élément. Pour identifier la source d'un élément, utilisez un nom descriptif.
- NOTE**
Les alertes récapitulatives et simples s'affichent ensemble sous le nœud Alertes. Par conséquent, spécifiez un nom pour distinguer les alertes récapitulatives des alertes simples.
- **Forcer l'unicité** : ajoute un chiffre au nom lorsque ce nom existe déjà dans le module de gestion.
 - **Module de gestion** : spécifie un module de gestion pour contenir l'élément.
3. Cliquez sur OK. L'alerte simple que vous avez créée est mise en surbrillance dans l'arborescence de l'éditeur de module de gestion et ses paramètres s'affichent dans le volet Paramètres.
 4. Configurez les paramètres d'alertes récapitulatives.

Configuration d'une alerte récapitulative

Dans tous les environnements, vous pouvez :

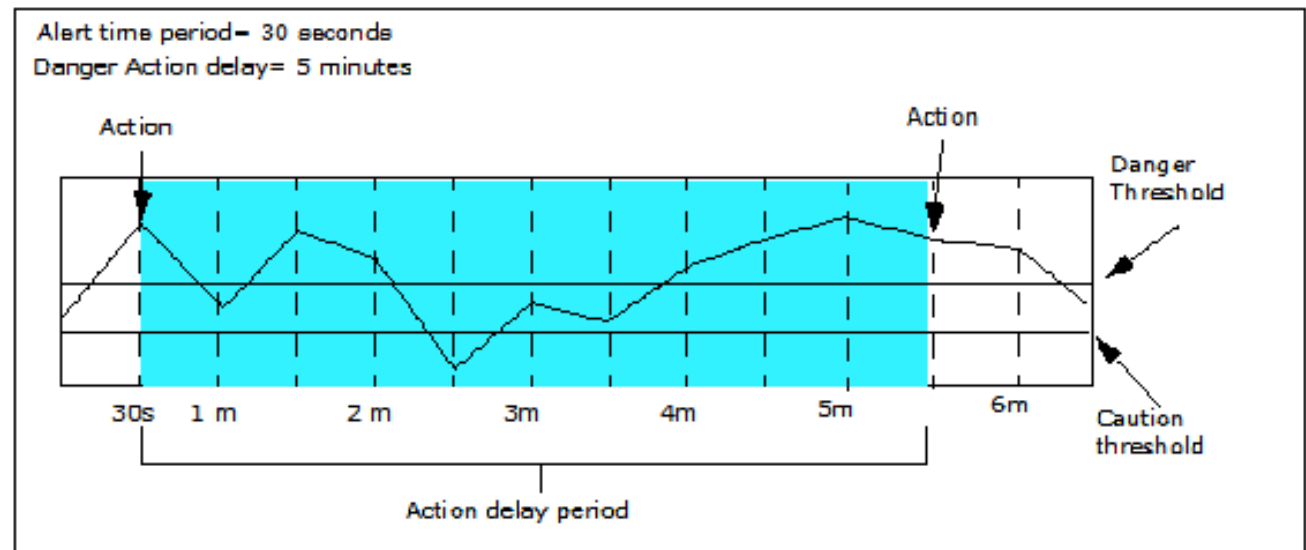
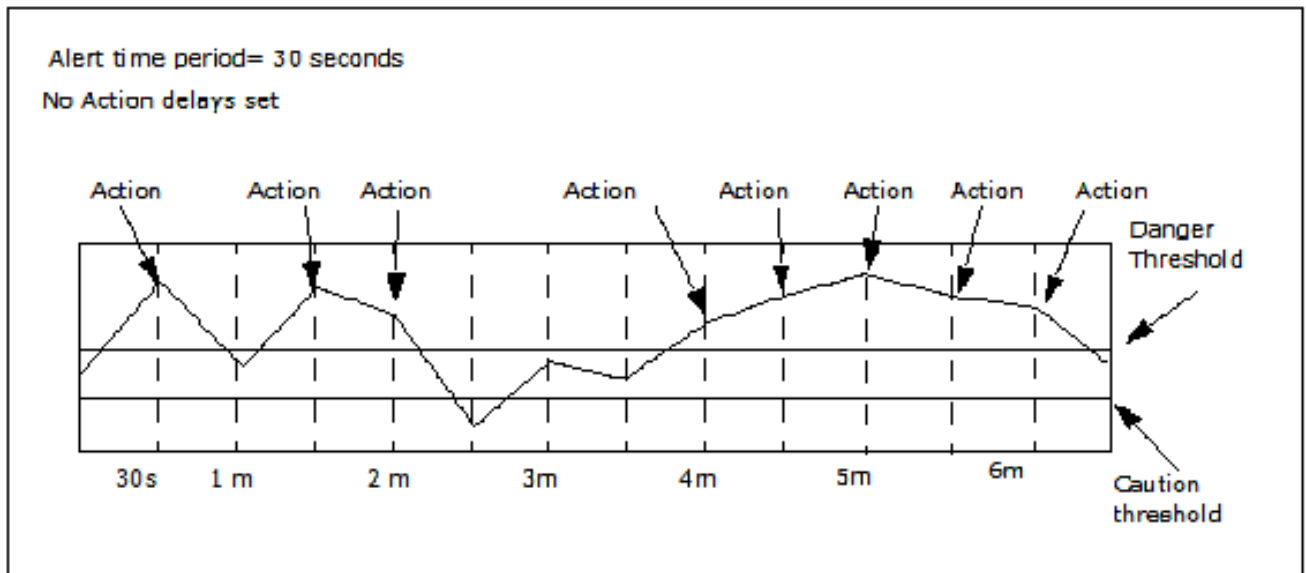
1. Modifier les champs comme il convient. Par exemple, vous pouvez effectuer les actions suivantes :
 - Modifier le nom et sélectionner un module de gestion.
 - Activer ou désactiver l'objet à l'aide de la case à cocher Actif.
2. Affecter des alertes à l'alerte récapitulative. Pour Team Center, utilisez le bouton **Ajouter des alertes**. Pour la station de travail ou Webview, sélectionnez une ou plusieurs alertes et utilisez les flèches pour les déplacer de la liste Disponible vers la liste Inclus.
3. Sélectionner une combinaison pour N'importe quel type d'alerte ou pour Toutes les alertes.

Dans Team Center, vous pouvez affecter un canal de notification. Dans la station de travail ou Webview, vous pouvez affecter une action de trace de transaction et définir un délai d'action.

Retards dans les actions de danger et d'avertissement

(Webview et la station de travail uniquement pour les actions de trace de transaction)

Les délais d'action de danger et d'avertissement déterminent les conditions dans lesquelles les statuts Danger ou Avertissement sont signalés par un résultat de comparaison dans l'action. Ces délais d'action empêchent une saturation des notifications d'alerte. Un délai agit comme un bouton de mise en sommeil pour les notifications d'alerte. Vous pouvez définir un délai entre la première notification d'alerte et les notifications suivantes.



Dans un scénario où la période d'alerte est définie sur 30 secondes, si les informations génèrent un statut d'alerte Danger et que vous avez défini une action pour celui-ci, l'action est déclenchée. Sans délai défini, si le statut Danger persiste, vous êtes averti à chaque fois que le seuil Danger est dépassé. Par exemple, vous recevez une notification huit fois sur une courte période. Les problèmes ne sont généralement pas résolus en un laps de temps aussi court que 30 secondes. Par conséquent, retardez les actions suivantes à l'aide d'un délai d'action. En d'autres termes, avec la même période d'alerte de 30 secondes, si vous définissez un délai d'action de cinq minutes pour le statut Danger, vous recevez la première notification d'alerte au bout de 30 secondes. Toutefois, si l'état Danger se produit à nouveau pendant cette période de suspension d'action de cinq minutes et que le seuil Danger est toujours dépassé à la fin de la période d'interdiction, vous n'êtes informé d'une deuxième action que cinq minutes après la première notification.

Création et modification d'outils de calcul

Les outils de calcul utilisent les valeurs d'un groupement de mesures comme entrée et déterminent la moyenne ou la somme des valeurs. Les outils de calcul affichent la valeur obtenue en tant que mesure personnalisée dans

l'arborescence Investigator. Les mesures générées par un outil de calcul s'affichent sous un processus virtuel, appelé processus de mesures personnalisées. Le processus de mesures personnalisées s'exécute sur un hôte virtuel appelé Hôte de mesures personnalisées.

A propos des outils de calcul

Les outils de calcul peuvent calculer la moyenne ou la somme des valeurs à partir d'un groupement de mesures, puis générer des mesures personnalisées dans l'arborescence Investigator. Les outils de calcul génèrent des mesures qui sont exécutées sur un processus virtuel, appelé processus de mesures personnalisées. Ce processus s'exécute sur un hôte virtuel : l'hôte de mesures personnalisées.

Les mesures de prise en charge collectent les données à l'aide d'outils de calcul. Pour signaler correctement des données, tous les outils de calcul MOM requièrent des données provenant d'au moins un collecteur. Sans données de collecteur, MOM ne peut pas calculer les mesures ni les afficher.

Exemple

Sur un MOM, vous souhaitez afficher la mesure `(.*)\\Custom Metric Process \\(Virtual\\)\\Custom Metric Agent \\(Virtual\\)Enterprise Manager\\Configuration:Number of Metric Groupings`. Vous attendez une valeur de mesure supérieure à 0.

Si aucun collecteur n'est connecté à MOM, la mesure `Number of Metric Groupings` signale 0.

Si au moins un collecteur est connecté à MOM, la mesure `Number of Metric Groupings` signale la valeur correcte.

Outil de calcul JavaScript

Un Outil de calcul JavaScript effectue des calculs complexes, tels que l'écart type et les moyennes non pondérées. Cet outil de calcul présente également les avantages suivants :

- Meilleur contrôle de la fréquence de calcul des mesures
- Gestion des chemins d'accès de la mesure calculée de manière similaire à un agent
- Stockage des calculs précédents et génération des mesures agrégées pendant une période spécifique à l'aide de variables globales
- Evaluation des mesures de chaîne ou production d'une mesure de chaîne calculée

Outil de calcul du module de gestion

L'outil de calcul du module de gestion effectue des calculs simples sur des mesures, tels que la somme, la moyenne, la valeur minimum et la valeur maximum.

L'outil de calcul du module de gestion requiert moins de ressources que les outils de calcul JavaScript. Cet outil de calcul présente également les avantages suivants :

- Nombre de ressources système inférieur à celui de l'outil de calcul JavaScript
- Vous pouvez créer et gérer des outils de calcul. L'accès aux répertoires d'installation n'est pas requis pour créer ou gérer l'outil de calcul du module de gestion.

Création d'un outil de calcul

Vous pouvez créer un outil de calcul pour un groupe de mesures.

Procédez comme suit :

1. Dans Team Center, sélectionnez **Outils de calcul**.
La page Outils de calcul affiche une liste des outils de calcul regroupés en fonction des modules de gestion.
2. Sélectionnez **Créer un outil de calcul**.
La page Créer un outil de calcul s'affiche.

3. Pour modifier un outil de calcul, sélectionnez celui que vous souhaitez mettre à jour.
La page Modifier l'outil de calcul : `<nom_outil_calcul>` s'affiche.
4. Dans la liste déroulante **Module de gestion**, sélectionnez le module à appliquer à l'outil de calcul simple que vous créez. Vous pouvez également sélectionner **Créer un module de gestion** pour créer un module de gestion dans une boîte de dialogue distincte.
5. Dans le champ **Description**, entrez la description requise permettant d'identifier l'outil de calcul simple que vous créez.
6. Dans le champ **Groupement de mesures**, sélectionnez le groupement de mesures à appliquer à l'outil de calcul simple que vous créez. Vous pouvez également sélectionner **Créer un groupement de mesures** pour créer un groupement de mesures dans une boîte de dialogue distincte.

NOTE

- Lorsque l'outil de calcul est créé, un groupement de mesures est automatiquement créé et porte le même nom. Toutefois, pour fournir des données à l'outil de calcul, le groupement de mesures doit être personnalisé.
- Sélectionnez un groupement de mesures qui fournit des valeurs entières. Les outils de calcul ne peuvent pas accepter de valeurs non entières comme entrée. Les types mixtes génèrent des résultats inattendus.

NOTE

Informations complémentaires : [Configuration des groupements de mesures dans Team Center](#)

Outils de calcul et moyennes pondérées

Les outils de calcul Introscope peuvent générer des mesures basées sur des moyennes. Les calculs sont basés sur des moyennes pondérées, non sur des moyennes linéaires. Les moyennes pondérées sont utiles lors de la surveillance des performances de votre application dans un environnement de cluster. Dans ce scénario, vous pouvez afficher un temps de réponse précis entre plusieurs serveurs dont les niveaux de charge sont susceptibles d'être différents.

Exemple :

Vous disposez d'un outil de calcul qui génère une mesure à partir du temps de réponse moyen pour cinq servlets. Une moyenne linéaire permet d'ajouter le temps de réponse pour une période définie et de la diviser par cinq. Une moyenne pondérée attribue un poids supérieur aux servlets qui sont appelés le plus souvent, ce qui améliore sa précision.

Modification des types d'opération dans les outils de calcul du module de gestion

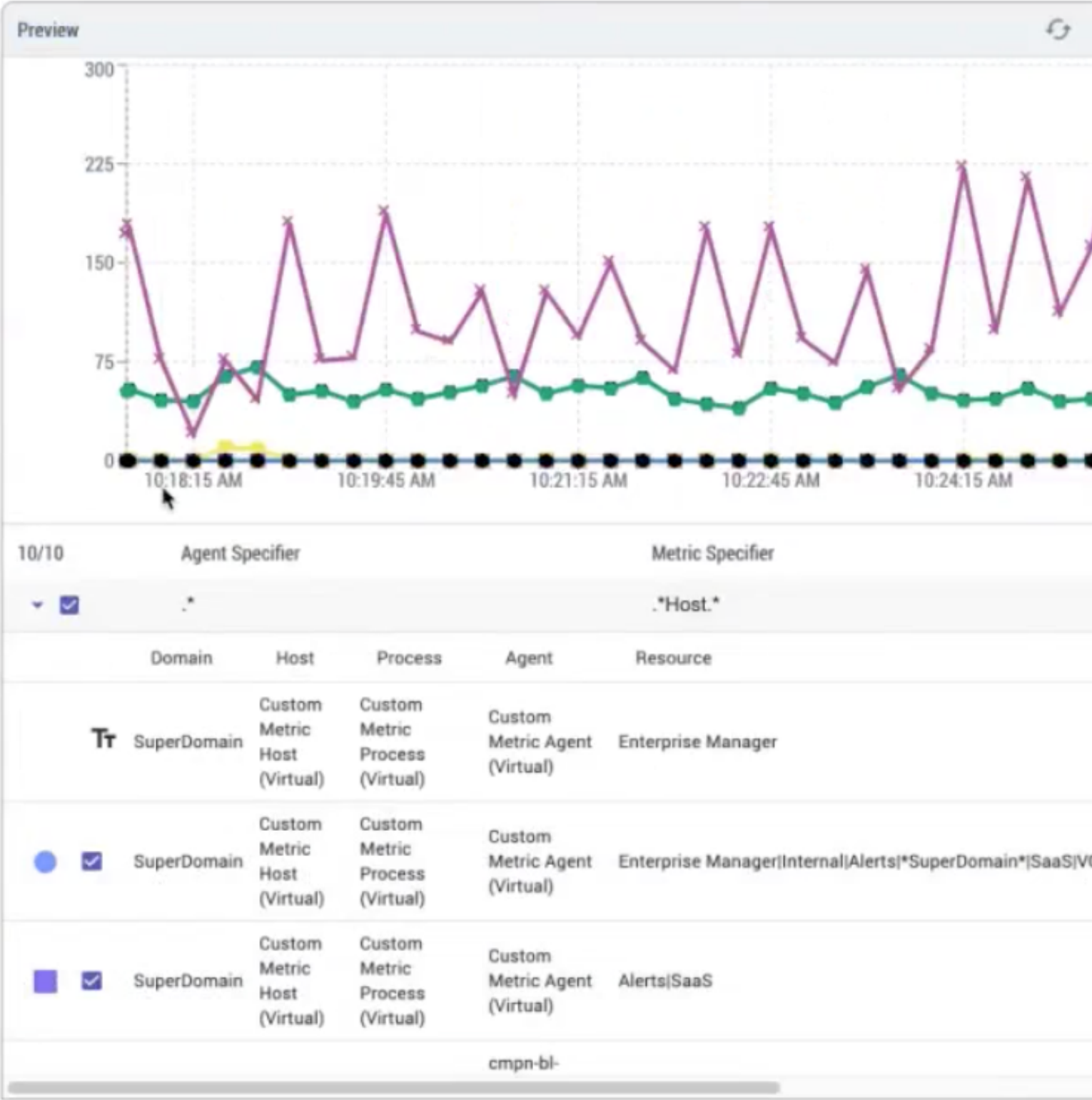
Lorsque vous modifiez un outil de calcul dans un module de gestion, modifiez le type d'opération pour redéfinir la signification de la mesure de sortie de l'outil de calcul. Par exemple, remplacez la valeur MIN par la valeur MAX. Si vous conservez le même nom de mesure de sortie de l'outil de calcul, l'affichage de cette mesure juxtapose les anciennes valeurs dans l'historique (calculée par exemple, par la valeur MIN) avec les nouvelles valeurs (la valeur MAX dans notre exemple). L'affichage de la mesure de sortie ne fournit aucune indication sur l'emplacement où l'altération du traitement a eu lieu. Si cela peut gêner les utilisateurs, renommez la mesure de sortie de l'outil de calcul lorsque vous modifiez le type d'opération.

NOTE

Informations complémentaires : [Modification des types d'opération dans les outils de calcul du module de gestion](#)

Aperçu des outils de calcul

L'aperçu des outils de calcul affiche le mode d'aperçu des groupes de mesures configurés. Vous pouvez afficher les données de mesures pertinentes tracées dans le graphique. La fenêtre Aperçu affiche le graphique de données de mesures basé sur le champ **Groupement de mesures**.



Dans la fenêtre Aperçu, vous pouvez afficher et effectuer les tâches suivantes :

- Fournissez le filtre pour le champ Groupement de mesures et l'icône **Actualiser**



est mise en surbrillance. Cliquez sur l'icône Actualiser pour afficher les dernières mesures en fonction des expressions.

- Le tableau Aperçu affiche le nombre total de mesures, le spécificateur d'agent, le spécificateur de mesure et le nombre de mesures à afficher dans le graphique.
- Vous pouvez sélectionner uniquement dix mesures à afficher dans le graphique.
-



Vous pouvez personnaliser les colonnes à afficher dans le tableau. Cliquez sur et sélectionnez les colonnes requises dans la liste.

- Dix couleurs et formes différentes sont disponibles pour distinguer les mesures représentées sur le graphique. Lorsque vous sélectionnez une mesure dans la liste, une couleur et une forme sont automatiquement affectées à une mesure.

	Value	Min	Max	Count
	0	0	0	0
	6	6	6	1
	0	0	0	1
	0	0	0	1
	0	0	0	1
	45	45	45	1
	0	0	0	1
	4	4	4	1
	0	0	0	1
	0	0	0	1

3/31/21 3:21:15 PM

- Cliquez sur l'icône Plein écran



pour afficher la fenêtre Aperçu en mode plein écran.

- Sur le graphique d'aperçu, l'axe X représente les valeurs de mesure et l'axe Y représente la plage horaire.

Les outils de calcul utilisent les valeurs d'un groupement de mesures comme entrée et déterminent la moyenne ou la somme des valeurs. Les outils de calcul affichent la valeur obtenue en tant que mesure personnalisée dans l'arborescence Investigator. Les mesures générées par l'outil de calcul s'affichent sous un processus virtuel, nommé Processus de mesure personnalisé.

Pour plus d'informations sur les outils de calcul, sur la création d'un outil de calcul et sur la modification des types d'opérations, reportez-vous à la section [Création et modification d'outils de calcul](#).

Configuration de l'analyse différentielle

L'analyse différentielle est activée par défaut. Toutefois, en tant qu'administrateur, vous êtes chargé de configurer les paramètres par défaut ou de créer et configurer des éléments de l'analyse différentielle. En tant que responsable du tri des applications, vous surveillez les performances à l'aide des informations figurant dans la carte ou dans le graphique d'analyse différentielle.

Vérification des prérequis de l'analyse différentielle

Avant d'implémenter l'analyse différentielle, vérifiez que votre implémentation CA APM inclut ce qui suit :

- Un gestionnaire d'entreprise
- Des agents configurés pour les composants frontaux, les composants d'arrière-plan ou les transactions métier des applications ou tout ce qui précède.
- Un moniteur TIM (Transaction Impact Monitor, requis pour l'installation de CA CEM).
- Vous pouvez installer un ou plusieurs moniteurs TIM dans un environnement CA CEM.

Création d'un contrôle différentiel

Les contrôles différentiels sont des éléments destinés à détecter toute instabilité au niveau des mesures correspondantes. Les seuils d'avertissement et de danger contrôlent l'intensité d'écart, qui évalue la stabilité de la mesure. Ce comportement diffère des contrôles différentiels réalisés par les alertes traditionnelles qui combinent un état vert, jaune et rouge et impliquent l'existence de problèmes. Les contrôles différentiels vous permettent de déterminer la quantité d'instabilité à enregistrer pour entrer dans les zones d'intensité d'écart d'avertissement et de danger. Les options avancées permettent d'effectuer un contrôle plus poussé des intensités d'écart de l'analyse différentielle. En général, les utilisateurs de l'analyse différentielle peuvent appliquer des seuils faibles pour afficher le flux complet des modifications de la stabilité ou utiliser des seuils élevés pour limiter la sortie à quelques modifications parmi les plus extrêmes (qui sont susceptibles d'indiquer un problème).

Nous vous recommandons d'utiliser les seuils par défaut pour commencer et de modifier les paramètres de seuil d'alerte par défaut afin d'indiquer les intensités auxquelles vous souhaitez définir une notification.

La carte de l'analyse différentielle s'affiche pour une mesure uniquement s'il existe un contrôle différentiel. Vous créez un élément de contrôle différentiel dans un module de gestion correspondant à votre mesure. Des modules de gestion peuvent exister pour un domaine ou pour tous les domaines ; ils contiennent des éléments qui organisent les données de mesure devant être présentées.

Procédez comme suit :

1. Dans Team Center, sélectionnez **Analyse différentielle**.
La page Analyse différentielle affiche une liste de contrôles d'analyse différentielle regroupés d'après les modules de gestion.
2. Sur la page Analyse différentielle, sélectionnez **Créer un contrôle de l'analyse différentielle**.
La fenêtre Créer un contrôle de l'analyse différentielle s'affiche.
3. Spécifiez les options suivantes et cliquez sur **Créer**.
 - **Actif** : le contrôle de l'analyse différentielle est activé par défaut. Toutefois, vous pouvez configurer son activation ou le désactiver.
 - **Nom** : saisissez un nom pour l'élément Contrôle de l'analyse différentielle.
 - **Module de gestion** : spécifiez le module de gestion auquel appartient cet élément Contrôle de l'analyse différentielle.
 - **Description** : champ facultatif. Entrez une brève description de l'élément Contrôle de l'analyse différentielle.
 - **Groupement de mesures** : effectuez l'une des opérations ci-après pour sélectionner le groupement de mesures.
 - Cliquez sur la liste déroulante **Afficher les filtres** et choisissez tous les modules de gestion à partir desquels vous souhaitez sélectionner le groupement de mesures, puis sélectionnez le groupement de mesures requis dans la liste. Le cas échéant, cliquez sur **Ouvrir** pour modifier le groupement de mesures sélectionné.
 - Sélectionnez le groupement de mesures requis dans la liste des groupements de mesures disponibles. Le cas échéant, cliquez sur **Ouvrir** pour modifier le groupement de mesures sélectionné.
 - Sélectionnez l'icône de liste déroulante dans la liste des groupements de mesures disponibles, puis cliquez sur l'option **Créer un groupement de mesures** disponible au bas de la liste.

La page Créer un groupement de mesures s'affiche. Pour plus d'informations, consultez la section Configuration des groupements de mesures dans Team Center.

- **Seuils** : définissez les options de seuil pour les alertes **Danger** et **Avertissement**. Cette valeur déclenche une alerte de danger ou une alerte d'avertissement.
- **Fenêtre d'évaluation** :
 - **Longueur** : spécifie le nombre de cellules de 15 secondes précédentes qui influencent le poids d'une fenêtre. Le poids total de la fenêtre détermine les régions d'avertissement ou de danger. Chaque cellule de la fenêtre contient le poids le plus élevé de toutes les règles enfreintes au cours de ces 15 secondes, moins toute éventuelle dégradation. La cellule la plus ancienne devient obsolète et est abandonnée au fur et à mesure que de nouvelles cellules sont ajoutées. Valeur par défaut : 20
 - **Dégradation** : spécifie la fréquence à laquelle les règles enfreintes se désintègrent avec leur cellule au fil du temps. Au fur et à mesure que de nouvelles cellules sont ajoutées, la dégradation réduit l'effet des poids précédemment ajoutés dans la fenêtre. Le poids le plus récent est toujours le poids complet. En fonction de la valeur de dégradation, seules les parties des anciens poids sont prises en compte pour le calcul final. Ainsi, chaque cellule de la fenêtre présente un pourcentage de réduction basé sur le niveau de dégradation. Les poids sont réduits sur chaque nouvelle instance ajoutée à la fenêtre en fonction de cette valeur de pourcentage de réduction.

La valeur 100 représente la dégradation la plus rapide et la valeur des violations de règle diminue rapidement au fur et à mesure que les règles vieillissent. Les cellules, classées de la plus récente à la plus ancienne, présentent une réduction progressive de la dégradation de 0 à 100 dans leur poids. Par exemple, la réduction du poids des cellules les plus anciennes est complète. Ce paramètre réduit la probabilité de notification d'avertissement et de danger, en particulier lorsqu'une période d'instabilité s'écoule rapidement.

La valeur 0 représente la sensibilité la plus élevée (aucune dégradation) et les violations conservent leur valeur totale pendant la totalité de la fenêtre. La cellule la plus ancienne possède la même valeur que lorsqu'elle représentait la cellule la plus récente. En utilisant ce paramètre, une courte période d'instabilité peut maintenir le pic dans un état d'avertissement ou de danger jusqu'à son expiration complète et sa disparition de la fenêtre. La valeur par défaut est 20. Les violations de règle récentes comptent un peu plus que les anciennes.
- **Application d'une règle** : spécifie une règle de déclenchement des pics.
 - **Règle 1 : $+3\sigma$** : un point de données unique se situe en dehors de la limite 3σ à partir de la ligne centrale.
 - **Règle 2 : $+2\sigma$ (2/3)** : deux points consécutifs sur trois se trouvent au-delà de la limite 2σ .
 - **Règle 3 : $+1\sigma$ (4/5)** : quatre points consécutifs sur cinq se trouvent au-delà de la limite 1σ .
 - **Règle 4 : $\Delta f(x) \geq 0$ (10/10)** : dix points consécutifs sur dix sont en hausse ou en baisse.

Les contrôles différentiels sont des éléments destinés à détecter toute instabilité au niveau des mesures correspondantes. Les contrôles différentiels vous permettent de déterminer la quantité d'instabilité à enregistrer pour entrer dans les zones d'intensité d'écart d'avertissement et de danger. Les options avancées permettent d'effectuer un contrôle plus poussé des intensités d'écart de l'analyse différentielle.

En général, les utilisateurs de l'analyse différentielle peuvent appliquer des seuils faibles pour afficher le flux complet des modifications de la stabilité ou utiliser des seuils élevés pour limiter la sortie à quelques modifications parmi les plus extrêmes (qui sont susceptibles d'indiquer un problème). L'analyse différentielle est activée par défaut.

Pour plus d'informations sur les conditions préalables et sur la création d'un contrôle différentiel, reportez-vous à la section [Configuration de l'analyse différentielle](#).

Configuration des extensions JavaScript

Une extension JavaScript permet de créer une nouvelle extension et de modifier une extension existante. Cette extension lit les mesures d'entrée et génère des mesures de sortie en fonction des calculs spécifiés dans un fichier texte JavaScript créé par l'utilisateur. Les nouvelles mesures calculées peuvent apparaître dans l'arborescence Investigator, sous l'agent personnalisé virtuel. Les mesures peuvent également s'afficher dans n'importe quel noeud de l'arborescence Investigator, en fonction de la mesure de sortie spécifiée dans le script de l'outil de calcul. Une mesure calculée peut être désactivée,

mais l'outil de calcul qui la produit n'est pas informé de l'état d'arrêt. Le moteur JavaScript du gestionnaire d'entreprise permet de déployer à chaud des outils de calcul JavaScript vers un gestionnaire d'entreprise en cours d'exécution.

- [Accès aux extensions JavaScript](#)
- [Ecriture d'outils de calcul JavaScript](#)
- [Exécution des outils de calcul JavaScript sur le MOM](#)
- [Types de données de mesures](#)

Accès aux extensions JavaScript

Procédez comme suit :

1. Dans l'interface utilisateur de DX Application Performance Management, cliquez sur **Paramètres**.
2. Cliquez sur la mosaïque **Extensions JavaScript**, sous **Paramètres généraux**.
3. Pour créer une extension, cliquez sur **Créer une extension**.
4. Sélectionnez un fichier d'extension et chargez-le.

NOTE

Vous pouvez également modifier l'extension existante, ou bien télécharger ou supprimer une extension.

5. Pour activer ou désactiver le statut, désactivez le bouton de basculement sous la colonne **Statut**.

L'extension JavaScript est créée.

Ecriture d'outils de calcul JavaScript

Les noms des fichiers des outils de calcul JavaScript doivent se terminer par une extension `.js`.

Les outils de calcul JavaScript spécifient des mesures d'entrée et génèrent une ou plusieurs mesures de sortie.

NOTE

Chaque erreur dans un outil de calcul JavaScript est consignée dans le journal EM. Des erreurs fréquentes peuvent saturer le journal EM. Testez vos outils de calcul avant de les déployer en production.

Fonction execute()

Chaque outil de calcul doit avoir une fonction `execute()` qui inclut deux arguments. En outre, des fonctions d'assistance sont disponibles pour vous aider à créer les mesures à renvoyer au gestionnaire d'entreprise. La fonction `execute()` est appelée toutes les 15 secondes par le moteur de script.

Notez ce qui suit pour la fonction `execute()` :

- L'appel de la fonction `execute()` se produit toutes les 15 secondes, même en l'absence de mesures correspondant aux expressions régulières renvoyées (voir plus loin). Cela permet à l'outil de calcul, par exemple, de signaler une mesure pour indiquer que certaines mesures ne sont pas signalées afin de créer une alerte.
- L'appel toutes les 15 secondes est effectué au mieux et il n'est pas garanti qu'il soit exactement de 15 secondes.
- L'appel aux secondes 0, 15, 30 et 45 est le meilleur effort possible, mais n'est pas garanti.
- Les mesures sont horodatées par le gestionnaire d'entreprise lorsqu'elles sont reçues lors du retour de la fonction `execute()`.
- Pour la stabilité du gestionnaire d'entreprise, la durée d'appel de la fonction `execute()` ne doit pas dépasser 7,5 secondes. Au-delà de 15 secondes, il est probable qu'il y ait une instabilité du gestionnaire d'entreprise et des écarts de mesures, car la collecte des mesures du gestionnaire d'entreprise est retardée. Un dépassement constant de 15 secondes peut provoquer un arrêt brutal du gestionnaire d'entreprise.
- La seule mesure de prise en charge qui peut vous alerter sur les outils de calcul entraînant une instabilité est le temps de collecte de l'outil de calcul du gestionnaire d'entreprise, qui ne doit que très occasionnellement dépasser 7,5 secondes et presque jamais 15 secondes.

La syntaxe de la fonction `execute()` est la suivante :


```
function execute(metricData, javascriptResultSetHelper)
```

Où

- **metricData** : tableau des données de mesure fournies à la fonction lorsqu'elle est appelée toutes les 15 secondes avant les intervalles `execute()`.

NOTE

Il convient d'éviter de transmettre de nombreuses mesures à un outil de calcul, car le temps nécessaire à la construction du tableau `MetricData`, et en particulier la mémoire utilisée pour cela, peut empêcher l'achèvement dans les délais du cycle de collecte de 15 secondes du gestionnaire d'entreprise et provoquer une instabilité. La limite dépend de la configuration du gestionnaire d'entreprise. Utilisez le temps de collecte de l'outil de calcul comme indicateur d'instabilité, comme indiqué ci-dessus.

```
{ data[
  { agentName:
    { processURL= string           // Metric source: domain|host|process|agent
      getDomain= string()         // Returns the domain segment of the metric source
    }
    agentMetric:
    { attributeURL= string }       // Metric attribute: metricPath:metricName
    timeslicedValue:
    { dataIsAbsent: boolean()      // Returns false if data is present
      Value: long, int, or string  // The metric's value, count, or average
      Type: int                   // Coded metric value type
      dataPointCount= int         // Count of metric values reported
      minimum: int                // Minimum value reported
      maximum: int                // Maximum value reported
    }
  ] }
```

NOTE

- Ignorez les entrées de données où `data.dataIsAbsent==true`.
- Lorsqu'aucune mesure ne correspond aux expressions régulières de l'agent et de la mesure, `data.length` est égal à 0.
- L'ordre des mesures dans le tableau `metricData` n'est pas défini et peut varier d'un appel à l'autre.
- **javascriptResultSetHelper** : objet qui collecte les nouvelles données de mesures produites par le script et qui les envoie au gestionnaire d'entreprise. Cet objet fournit la fonction `addMetric` en deux versions surchargées :

```
JavascriptResultSetHelper:
{
  addMetric(fullMetricName, value, type, frequency)

  addMetric(fullMetricName, count, value, min, max, type, frequency)
}
```

- `kDefaultFrequency` est utilisé comme entrée dans l'argument de fréquence de la fonction d'assistance `addMetric()`.
- `kIntegerConstant` : mappe vers le type de mesure de constante d'entier.
- `kIntegerFluctuatingCounter` : mappe vers le type de mesure de compteur fluctuant d'entier.
- `kLongConstant` : mappe vers le type de mesure de constante longue.
- `kLongFluctuatingCounter` : mappe vers le type de mesure de compteur fluctuant long.
- `kLongTimestamp` : mappe vers le type de mesure d'horodatage longue.
- `kLongTimestampConstant` : mappe vers le type de mesure de constante d'horodatage longue.
- `kIntegerPercentage` : mappe vers le type de mesure de pourcentage d'entier.
- `kIntegerDuration` : mappe vers le type de mesure de durée d'entier.
- `kLongDuration` : mappe vers le type de mesure de durée longue.
- `kLongIntervalCounter` : mappe vers le type de mesure de compteur d'intervalle long.
- `kStringIndividualEvents` : mappe vers le type de mesure de chaîne.
- `addMetric(metricName, count, value, min, max, metricType, frequency)` : prend en charge la définition de nombre/valeur/min/max d'une valeur de mesure, nécessaire pour les types de mesure Taux et Nombre d'intervalles, où la valeur de la mesure est basée sur le nombre (count).
- `getCustomMetricAgentMetric(agentMetric)` : permet de créer un nom de mesure complet à l'aide de la mesure d'agent fournie et de remplir le reste en fonction du nom de l'agent de mesures personnalisé `SuperDomain`.

NOTE

- Une mesure ne peut être soumise qu'une seule fois. Si des mesures en double (nom uniquement) sont soumises, une erreur `tardy`, `invalid`, or `duplicate metric` (mesure en retard, non valide ou en double) se produit et est consignée dans le journal du gestionnaire d'entreprise.
- Si votre outil de calcul doit agréger des valeurs de mesure, il doit procéder à une agrégation interne pour soumettre une mesure unique qui correspond à la valeur agrégée.
- Si une valeur non valide est transmise, une erreur se produit (avec le message d'erreur JavaScript consigné dans le journal du gestionnaire d'entreprise).
- La version précédente, courte et surchargée, définit implicitement `count=1`.
- Cette dernière version, longue et surchargée, est nécessaire lorsque vous souhaitez soumettre une mesure avec un nombre supérieur à 1, ce qui est généralement requis pour les types de mesure `PerIntervalCounter` et `IntRate` (car celles-ci ont `value==count`, c'est-à-dire que le nombre est pris comme valeur).
- La fonction `execute()` doit renvoyer l'objet `javascriptResultSetHelper` reçu pour soumettre les mesures ajoutées par les appels `addMetric` dans le cycle de récolte des questionnaires d'entreprise, car les appels `addMetric` ajoutent des mesures aux champs masqués de l'objet `javascriptResultSetHelper`.
- Les mesures cachées dans l'objet `javascriptResultSetHelper` ne sont soumises au gestionnaire d'entreprise qu'à la fin de la fonction `execute()`.

Spécification des mesures d'entrée

Le script de l'outil de calcul peut spécifier les mesures d'entrée qu'il reçoit de l'une des deux manières suivantes :

- La méthode de spécification des mesures d'entrée consiste à utiliser une paire de méthodes appelées par le gestionnaire d'entreprise lors du déploiement de l'outil de calcul :
 - fonction `getAgentRegex()` qui doit renvoyer une chaîne contenant une expression régulière pour mettre en correspondance les agents.
 - fonction `getMetricRegex()` qui doit renvoyer une chaîne contenant une expression régulière pour mettre en correspondance les mesures.

```
function getAgentRegex()
{ return "SuperDomain\\|beta.*\\|Infrastructure Agent\\|EPAgent" }
```

```
function getMetricRegex()
```

- Les expressions régulières en JavaScript ont deux formats. Un format chaîne, délimité par des guillemets :
 - `"(.*\\|(.*)*\\|(.*)*"`
 - Dans les chaînes d'expressions régulières, les caractères spéciaux qui sont utilisés de manière littérale doivent être doublement échappés (`\\`) pour adhérer à l'échappement de barre oblique inverse Javascript dans les chaînes. Par conséquent, en JavaScript, `\\` dans une chaîne signifie que la première barre oblique inverse échappe la seconde en laissant cette deuxième barre oblique inverse en place.
 - En dehors des chaînes d'expression régulière, il n'est pas nécessaire d'échapper les caractères spéciaux d'expression régulière.
- L'expression régulière de l'agent peut spécifier les quatre segments d'un chemin source :
 - `Domain | host | process | agent`
 - Les domaines incluent tous les domaines et pas seulement `SuperDomain`.
- Il n'y a pas d'exigences de format pour les expressions régulières utilisées. Par exemple, une expression régulière de l'agent :
 - `".*"`
- inclut les mêmes agents que :
 - `".*\\.|.*\\.|.*\\."`
 - `"(.*)*(.*)*(.*)*(.*)"`
- Si vous vous souciez de l'efficacité des expressions régulières, évitez les retours sur trace en utilisant des correspondances différées (comme dans `.?*`) et des groupes de caractères (comme `[^\\]]`) :
 - `"SuperDomain\\|beta.*?\\|Infrastructure Agent\\|EPAGent"`
 - `"SuperDomain\\|beta[^\\]]*\\|Infrastructure Agent\\|EPAGent"`

Vous pouvez également utiliser la méthode fonction `getMetricSpecifier()`, qui doit renvoyer un spécificateur de mesure complet, c'est-à-dire une expression régulière d'agent et une expression régulière de mesure combinées.

Les expressions régulières créées sous forme de chaînes dans fonction `getAgentRegex()`, fonction `getMetricRegex()` et fonction `getMetricSpecifieur()` doivent utiliser un échappement des caractères différent de celui des autres expressions régulières que vous utilisez dans Introscope. Par exemple, dans les groupements de mesures ou dans la vue de recherche. En effet, tous les caractères d'échappement Java renvoyés depuis ces fonctions JavaScript doivent également être échappés dans JavaScript. Par exemple, `\|` doit être échappé en tant que `\\|` dans JavaScript.

Toutes les fonctions de l'outil de calcul JavaScript ont accès à un journal des variables globales, de type `IModuleFeedbackChannel`. **Exemple :**

Pour utiliser des fonctions JavaScript avancées ou pour garantir la conformité avec ECMA, le moteur de script intègre la bibliothèque JavaScript Mozilla Rhino, version 1.6 R1.

Création des données de mesure de sortie

La création de données de mesure de sortie requiert la spécification des paramètres suivants :

- **Nom de la mesure** : composé de l'agent et du chemin d'accès complet au noeud approprié dans l'arborescence de mesures.
 - Vous pouvez créer un nom d'agent basé sur les données entrantes. Les nouvelles données calculées s'affichent avec les données de mesure signalées par l'agent.
ou
 - Vous pouvez spécifier un nom de mesure d'outil de calcul pour afficher les données de mesure calculées dans leurs propre noeud dans l'arborescence de mesures.
- **Valeur des données** : calculée par le script.
- **Type de données de résultat** : spécifié par une valeur de constante à partir de la classe `com.wily.introscope.spec.metric.MetricTypes`.
- **Fréquence de génération de rapports** : fréquence à laquelle les nouvelles données de mesures sont signalées au gestionnaire d'entreprise et qui peuvent être obtenues à partir des données entrantes ou spécifiées explicitement. Vous pouvez définir la fréquence sur un multiple de la fréquence par défaut du gestionnaire d'entreprise (15 secondes).

Voici une valeur calculée standard à partir d'un script :

```
javascriptResultSetHelper.addMetric(metricName,
heapUsedValue, Packages.com.wily.introscope.spec.metric.MetricTypes.kIntegerFluctuatingCounter, frequency)
```

NOTE

Spécifiez les expressions régulières avec précaution, car elles peuvent potentiellement correspondre à toutes les mesures que vous produisez. Par exemple, une expression régulière `EJB.*Time.*` peut insérer une nouvelle valeur sous EJB. L'expression régulière insère une nouvelle valeur sous EJB lorsqu'une expression régulière correspond à `EJB.*Time.*`. Vous pouvez modifier votre expression régulière pour cela ou supprimer des données de mesures de vos propres mesures.

Ajout d'un outil de calcul JavaScript

Pour installer un nouvel outil de calcul JavaScript, chargez le fichier texte JavaScript dans le gestionnaire d'entreprise à l'aide de la page Extensions JavaScript mentionnées dans la section *Accès aux extensions JavaScript*.

Limitation du temps d'exécution des scripts

Le traitement des données de mesures entrantes par l'outil de calcul peut prendre du temps et affecter les performances du gestionnaire d'entreprise lorsque l'extension JavaScript s'exécute. Pour vous protéger contre une surcharge du gestionnaire d'entreprise, spécifiez le délai d'expiration du script dans la source de l'extension. Par exemple, lors de l'utilisation d'une expression régulière trop générique pour les mesures d'entrée.

Lorsqu'une fonction `getTimeout()` est présente dans la source du script, la valeur qu'elle renvoie est utilisée comme délai d'expiration du script. Si la fonction de délai d'expiration n'est pas incluse dans le script, le délai d'expiration de l'extension Javascript par défaut du gestionnaire d'entreprise est utilisé.

Fonction `getTimeout()`

Utilisez la fonction `getTimeout()` pour spécifier le délai d'exécution du script en millisecondes.

Exemple

Pour utiliser un délai d'expiration de script de 50 ms :

```
function getTimeout() {
    return 50;
```

```
}
```

Exécution des outils de calcul JavaScript sur le MOM

Vous pouvez exécuter un outil de calcul JavaScript sur le MOM pour générer des mesures pour l'agent de mesure personnalisée MOM. L'outil de calcul ne peut pas produire de mesures pour les agents connectés à un collecteur, mais il peut afficher les mesures d'entrée des agents dans les collecteurs.

NOTE

Informations complémentaires : [A propos des outils de calcul](#)

Si un outil de calcul est ajouté, modifié ou supprimé dans un environnement en cluster, MOM propage automatiquement la modification à tous les collecteurs. Cette propagation ne se produit pas lorsque les mises à jour automatiques sont désactivées pour les collecteurs.

Fonction runOnMOM

Un outil de calcul JavaScript qui ne doit pas être exécuté sur le MOM doit implémenter une fonction `runOnMOM` qui renvoie `false`, comme dans l'exemple suivant :

```
// return false if the script should not run on the MOM
// default is true.
function runOnMOM()
{
    return false;
}
```

Si la fonction `runOnMOM` renvoie `true` ou n'est pas implémentée, l'outil de calcul JavaScript s'exécute également sur le MOM.

Les outils de calcul qui renvoient `false` pour cette fonction sont, par défaut, automatiquement propagés pour le déploiement sur tous les collecteurs.

Pour APM 10.8, cette valeur par défaut peut être remplacée par

```
introscope.enterprisemanager.javascript.hotdeploy.collectors.enable= false.
```

Cela permet le déploiement d'ensembles différents et limités d'outils de calcul dans vos collecteurs lorsqu'ils sont utilisés avec une correspondance coordonnée à la configuration des connexions agents à collecteurs permises au sein de `loadbalancing.xml` afin d'obtenir l'effet souhaité de limitation des exécutions des outils de calcul, en fonction du placement des mesures.

Pour DX APM SaaS, ce contrôle n'est pas possible, car la répartition de charge est contrôlée différemment et les clusters le sont de manière interne.

Réduction du nombre d'erreurs de création de mesures consignées

Lorsqu'un outil de calcul s'exécute sur le MOM et crée une mesure pour un agent présent dans les collecteurs, une journalisation unique de l'événement au niveau `WARN` a lieu.

Exemple

```
5/15/07 02:32:20 PM PDT [WARN] [Manager.MetricCalculatorBean] Calculator Registered Metric <ID=7,
JavaScript calculator C:\workspaces\workspaceKrakatau\com.wily.introscope.em.feature\rootFilesMOM\.\scripts
\HeapUsedPercentage.js>. A JavaScript calculator in the MOM cannot output metric data to an agent that exists
in a Collector: SuperDomain\rhart-dt1|EPAgentProcess1|EPAgent15|GC Heap:Heap Used (%) 5/15/07 02:32:20 PM PDT
[WARN] [Manager.MetricCalculatorBean]
```

Les événements ultérieurs sont consignés uniquement au niveau `DEBUG`.

Désactivation de la mise à jour automatique des collecteurs

Les environnements en cluster sont automatiquement définis pour propager un outil de calcul JavaScript ajouté, modifié ou supprimé à tous les collecteurs. Si vous ne souhaitez pas que les outils de calcul soient propagés, contactez le service de support Broadcom pour désactiver cette fonction.

Exemple de création d'un exemple d'outil de calcul

Cet exemple crée un outil de calcul simple qui reçoit une mesure correspondant au nombre cumulé de rejets (depuis le démarrage de l'agent) et produit la valeur delta par intervalle de 15 secondes.

Les quatre premières fonctions de contrat doivent ressembler à ce qui suit :

```
function getAgentRegex() { return ".*" }
function getMetricRegex() { return "GC Heap:Bytes Total" }
function getFrequency()
{ return Packages.com.wily.introscope.spec.metric.Frequency.kDefaultSystemFrequencyInSeconds; }
function runOnMOM() { return false; }
```

Il doit s'exécuter sur les collecteurs, car il doit produire une mesure avec un chemin de mesure comme l'original et un nom de mesure avec delta ajouté (:Rejections Delta). La fonction `execute()` est implémentée comme indiqué en suivant :

```
'use strict';
var savedValues= {} // An object for saved metric values
function execute(metricData, javascriptResultSetHelper)
{
    try
    {
        var metricsReceived= 0;
        for (var i = 0; i < metricData.length; i++)
        {
            var data= metricData[i];
            if (data.timeslicedValue.dataIsAbsent())
                continue;
            metricsReceived++;
            var
                metricSource= data.agentName.processURL,
                metricAttribute= data.agentMetric.attributeURL,
                split= metricAttribute.split(":"),
                metricPath= split[0]=="?"?"":split[0], // Leave empty or prepend a segment pipe
                metricName= split[1] + " Delta",
                metricValue= data.timeslicedValue.value;
            metric= metricSource + metricPath + metricName;
            var savedValue= savedValues[metric]
            if (savedValue) // Iff a saved value is present calculate the delta to submit
            {
                var delta= metricValue - savedValue
                JavascriptResultSetHelper.addMetric(
                    metric, delta,
                    Packages.com.wily.introscope.spec.metric.MetricTypes.LongFluctuatingCounter,
                    Packages.com.wily.introscope.spec.metric.Frequency.getFrequencyInSeconds(15))
                metricsSubmitted++;
            }
            savedValues[metric]= metricValue;
        }
    }
}
```

```

    return javascriptResultSetHelper;
}
catch (e)
{ log.error(e); }
}

```

NOTE

- La variable savedValues se trouve dans une variable globale et est enregistrée dans les appels d'exécution.
- La fonction datalsAbsent() est utilisée pour court-circuiter le traitement ultérieur d'une entrée metricData lorsqu'elle est vraie en continuant avec l'itération suivante.
- L'attribut metricAttribute est fractionné au niveau des deux-points de délimitation afin d'obtenir des valeurs distinctes pour le chemin d'accès et le nom de la mesure. Cela est nécessaire, car pour un chemin de mesure vide, aucun délimiteur de barre verticale ne doit être utilisé lors de la génération de la mesure complète (sinon vous vous retrouveriez avec « |: », ce qui n'est pas valide).

Types de données de mesures

CA APM surveille les performances des applications en les mesurant en plusieurs points dans les sous-systèmes et composants des applications. Les sondes insérées dans le bytecode d'un composant d'application envoient des données aux agents, qui à leur tour les transmettent à Introscope Enterprise Manager. En outre, d'autres sous-systèmes, tels que JMX et PMI, envoient les données collectées par les agents. Le gestionnaire d'entreprise compile ces données en mesures et les affiche dans la station de travail ou WebView. Vous pouvez également exporter les mesures vers une base de données externe. Pour plus d'informations, reportez-vous à la section [Mesures APM](#).

Dans les outils de calcul JavaScript, tous les types de données de mesure sont référencés en ajoutant ce qui suit au début du type de données de mesure : `Packages.com.wily.introscope.spec.metric.MetricTypes`. Par exemple, pour utiliser `kIntegerFluctuatingCounter`, le nom complet doit être `Packages.com.wily.introscope.spec.metric.MetricTypes.kIntegerFluctuatingCounter`.

Les types de données de mesure sont pris en charge par l'agent PHP, l'agent Java, l'agent .NET et l'agent Node.js.

PerIntervalCounter :

kLongIntervalCounter : valeur numérique 64 bits représentant une valeur de mesure par intervalle. Lorsque l'intervalle est agrégé sur plusieurs périodes, la somme la plus élevée est utilisée comme valeur agrégée. Le nombre correspond au nombre d'achèvements (c'est-à-dire de réponses ou d'erreurs) au cours de l'intervalle et sera égal à la valeur.

Exemples de mesures : Réponses par intervalle, Erreurs par intervalle

IntCounter/LongCounter :

kIntegerFluctuatingCounter/kLongFluctuatingCounter : valeur numérique 32/64 bits qui fluctue, mais reste à la dernière valeur connue jusqu'à ce que de nouvelles données soient disponibles. Lorsque l'intervalle est agrégé sur plusieurs périodes, la valeur la plus élevée est utilisée comme valeur agrégée. Le nombre correspond au nombre total d'incrémentations et de décréments de la valeur qui se sont produits pendant cet intervalle.

Exemples de mesures : Nombre de transactions bloquées, Appels simultanés (IntCounter), Octets utilisés (LongCounter)

IntAverage/LongAverage :

kIntegerDuration/kLongDuration : valeur numérique de 32/64 bits représentant la durée. Lorsque l'intervalle est agrégé sur plusieurs périodes, la moyenne pondérée est utilisée comme valeur agrégée. Il s'agit du nombre d'achèvements (par exemple réponses) au cours de l'intervalle, qui est utilisé comme dénominateur pour calculer la valeur (par exemple moyenne).

Exemple de mesure : Temps de réponse moyen (ms)

IntRate :

kIntegerRate : valeur numérique de 32 bits représentant un compteur par seconde. Pour un intervalle de 15 secondes, les 14 secondes ou moins restantes sont tronquées. Lorsque l'intervalle est agrégé sur plusieurs périodes, la moyenne pondérée est utilisée comme valeur agrégée.

Exemple de mesure : Requêtes par seconde

TimeStamp :

kLongTimestamp : valeur d'horodatage qui peut être mise à jour. La valeur est entrée en nombre de millisecondes depuis l'heure d'époque UNIX (1er janvier 1970 à 00:00:00 UTC). Non conservée dans SmartStor.

StringEvent :

kStringIndividualEvents : valeur de chaîne qui peut être mise à jour. Non conservée dans SmartStor.

Exemple de mesure : Actuellement en fuite

IntConstant/LongConstant :

kIntegerConstant/kLongConstant : valeur numérique 32 ou 64 bits qui est initialisée, mais ne change pas.

Exemple de mesure : ID du processus

IntPercentage :

kIntegerPercentage : pourcentage entier (sans décimal). Lorsque l'intervalle est agrégé sur plusieurs périodes, la moyenne est utilisée comme valeur agrégée.

Exemple de mesure : % d'utilisation (processus)

LongTimeStampConstant :

kLongTimestampConstant : valeur d'horodatage initialisée, mais qui ne change pas. La valeur est entrée en nombre de millisecondes depuis l'heure d'époque UNIX (1er janvier 1970 à 00:00:00 UTC). Non conservée dans SmartStor.

Exemple de mesure : Date/heure de lancement

StringConstant :

kStringConstant : valeur de chaîne initialisée, mais qui ne change pas. Non conservée dans SmartStor.

Exemple de mesure : Machine virtuelle

Une extension JavaScript permet de créer une nouvelle extension et de modifier une extension existante. Cette extension lit les mesures d'entrée et génère des mesures de sortie en fonction des calculs spécifiés dans un fichier texte JavaScript créé par l'utilisateur. Les nouvelles mesures calculées peuvent apparaître dans l'arborescence Investigator, sous l'agent personnalisé virtuel. Les mesures peuvent également s'afficher dans n'importe quel noeud de l'arborescence Investigator, en fonction de la mesure de sortie spécifiée dans le script de l'outil de calcul.

Pour plus d'informations sur l'accès aux extensions JavaScript et leur configuration, reportez-vous à la section [Configuration des extensions JavaScript](#).

Recommandations de dimensionnement de Docker Monitor

Pour optimiser les performances de votre environnement Docker surveillé, vous pouvez vous servir des recommandations de dimensionnement suivantes comme référence. Ces recommandations sont simplement fournies à titre indicatif. Aussi, nous ne pouvons pas garantir que les exemples décrits sont optimaux pour votre environnement.

Recommandations de dimensionnement et mesures utiles

- **Allocation en ressources minimale recommandée pour un conteneur Docker Monitor :**
 - **Mémoire** : 650 Mo
 - **UC** : 0,3 pour 25 conteneurs. Pour l'allocation en ressources d'UC, reportez-vous au tableau ci-dessous.
- **Paramètre d'intervalle d'interrogation recommandé** : docker.interval.seconds=90

En règle générale, conteneur Docker Monitor n'utilise pas énormément d'UC. Toutefois, si la mesure **CPU Utilization % (mCore)** indique une utilisation de l'UC supérieure à 80 % pendant plus d'une heure, il est recommandé d'augmenter l'allocation en ressources d'UC. Il est recommandé d'augmenter l'allocation de 0,2 à chaque fois.

La mesure **CPU Throttling** est un autre indicateur montrant que Docker Monitor doit augmenter son allocation en ressources d'UC.

Allocation en ressources minimale

Nombre de conteneurs	Contraintes d'UC	Mémoire (Mo)
25	0,3	650
50	0,5	650
75	0,7	700
100	0,9	700

Téléchargement d'outils supplémentaires

La mosaïque **Téléchargements** vous permet de télécharger et de configurer des outils supplémentaires dans votre environnement de surveillance. Vous pouvez télécharger les outils suivants à partir des **Paramètres**, mosaïque **Téléchargements** :

- **Station de travail** : téléchargez l'outil Station de travail pour effectuer des tâches administratives et accéder aux mesures de performance.
- **Proxy cloud** : téléchargez et configurez le proxy cloud pour Windows ou Linux. Vous pouvez configurer le proxy cloud pour envoyer et recevoir des données collectées par l'agent directement à la passerelle cloud.
- **Outil d'importation d'agent** : téléchargez l'outil d'importation d'agent pour créer un package APM Command Center pour les agents de versions APM antérieures.
- [Configuration de la station de travail](#)
- [Connexion de la station de travail](#)
- [Proxy cloud](#)
- [Outil d'importation d'agent](#)

La mosaïque Téléchargements vous permet de télécharger et de configurer des outils supplémentaires dans votre environnement de surveillance. Les outils Station de travail, Proxy cloud et Outil d'importation d'agent sont disponibles au téléchargement à partir de la mosaïque Téléchargements des paramètres.

Pour plus d'informations sur les téléchargements et les outils disponibles au téléchargement, reportez-vous à la section [Téléchargement d'outils supplémentaires](#).

Outil d'importation d'agent

L'outil d'importation d'agent est un utilitaire de ligne de commande qui vous permet de migrer les agents Java pour CA APM 10.7 créés en tant que fichier .zip vers les derniers agents Java pour DX APM. Dans le processus de migration, un package APM Command Center est créé pour chaque agent tout en conservant les changements de configuration de

la version antérieure. Les modifications conservées incluent celles apportées aux valeurs de propriétés et aux bascules. Vous pouvez ensuite utiliser le package obtenu pour déployer l'agent remplaçant le précédent. La configuration du nouveau package est déjà modifiée pour se connecter à l'instance DX APM de nouvelle génération.

NOTE

Utilisez cet outil uniquement pour les packages d'agent autres que le programme d'installation Java 10.7. Cet outil prend en charge Windows et Linux.

Cet article couvre les rubriques suivantes :

Conditions préalables requises

Open JDK 11.x ou Oracle JDK 11.x

Processus de migration

Lorsque vous exécutez l'utilitaire, il identifie les fichiers et les paramètres utilisés par l'agent sélectionné et crée un package APM Command Center qui inclut des groupes contenant la configuration et les fichiers correspondants. Toutes les mises à jour manuelles apportées aux valeurs de propriété ou aux bascules sont appliquées aux nouveaux groupes si leurs valeurs diffèrent des valeurs par défaut dans le fichier de configuration de l'agent d'origine.

L'utilitaire crée un groupe personnalisé s'il détecte des fichiers, des bascules ou des paramètres de configuration non identifiés. Ce groupe est inclus dans le package créé.

Après la migration, vous pouvez gérer la configuration des agents à partir d'APM Command Center.

NOTE

Pour afficher un agent dans APM Command Center, incluez le groupe de contrôleur d'agent dans l'extension d'agent Java ou l'agent Infrastructure ; le contrôleur d'agent doit également être déployé sur le même hôte.

L'utilitaire est configuré pour utiliser une connexion directe au composant de passerelle cloud de DX APM. Vous pouvez reconfigurer l'utilitaire pour utiliser le proxy cloud local en modifiant la propriété dans le fichier de configuration [application.properties](#) ou à l'aide du [paramètre de ligne de commande](#).

Exécution de l'utilitaire Outil d'importation d'agent

Lors de l'exécution de l'utilitaire Outil d'importation d'agent, vous devez définir uniquement le chemin d'accès au système de fichiers vers le répertoire de l'agent dans le paramètre de ligne de commande. Des options de ligne de commande supplémentaires sont disponibles pour modifier le mode d'exécution de l'utilitaire ou pour sélectionner la configuration appropriée de l'agent.

Procédez comme suit :

1. Accédez à DX APM Team Center, **Paramètres, Téléchargements**.
2. Dans la section **Outil d'importation d'agent**, cliquez sur **Télécharger**.
Le fichier suivant est téléchargé : *apmservices.agentimport-<version>.zip*.
3. Extrayez le contenu du fichier .zip.
Le contenu suivant s'affiche :
 - a. Dossier **lib**
 - b. Fichier **application.properties**
 - c. Fichier de script Windows **import-agent.cmd**
 - d. Fichier de script Linux **import-agent.sh**
4. (Facultatif) Mettez à jour les propriétés requises dans le fichier **application.properties**.

IMPORTANT

Le répertoire de l'agent peut contenir plusieurs profils d'agent ; vous devez donc spécifier le chemin d'accès correct de manière explicite. Par défaut, le fichier *IntroscopeAgent.profile* est utilisé comme fichier de

configuration principal de l'agent. Toutefois, si vous souhaitez utiliser un autre fichier de profil (par ex., *noredef variant*), vous pouvez utiliser le paramètre de ligne de commande *--profile*.

NOTE

L'utilitaire utilise le jeton de sécurité propre au client hébergé actuel, généré lors de son téléchargement. Pour utiliser un autre jeton, générez un jeton d'API publique à partir de Team Center. Pour plus d'informations sur la génération du jeton de sécurité, consultez la rubrique [Génération d'un jeton de sécurité](#). Une fois le jeton généré, remplacez la valeur dans le fichier **application.properties** ou spécifiez-la en tant que paramètre de ligne de commande.

- En fonction de votre système d'exploitation, exécutez le script de démarrage de l'outil de ligne de commande avec le chemin d'accès au répertoire de l'agent qui contient les agents Java pour CA APM 10.7.

Exemple : `import-agent /opt/weblogic/wily`

NOTE

Sous Linux, vous devez mettre à jour l'autorisation de fichier et le rendre exécutable à l'aide de la commande `chmod +x import-agent.sh`.

L'utilitaire identifie l'environnement de l'agent (Ex. : système d'exploitation, version, processus et modifications apportées à la configuration) et crée un package correspondant dans l'instance du serveur de configuration APM Command Center.

NOTE

L'utilitaire crée un package à l'aide des groupes de la dernière version disponible dans APM Command Center.

Paramètres de ligne de commande

Lors de l'extraction des fichiers de l'utilitaire, vous obtenez des scripts pour les systèmes d'exploitation Linux et Windows :

- Linux** : `import-agent.sh`
- Windows** : `import-agent.cmd`

NOTE

Sous Linux, vous devez mettre à jour l'autorisation de fichier et le rendre exécutable à l'aide de la commande `chmod +x import-agent.sh`.

Lorsque vous exécutez le script, le seul paramètre requis est le chemin d'accès au répertoire des agents CA APM 10.7.

Exemple : `/opt/weblogic/wily`

Options de ligne de commande supplémentaires

- `-a, --agentJar <arg>` : utilise le chemin d'accès au fichier .jar de l'agent associé à la racine. Par défaut, le nom du fichier est **Agent.jar**.
- `-f, --force <arg>` : ignore toutes les erreurs et poursuit l'exécution de la commande. Cette option désactive l'optimisation du package.
- `-n, --name <arg>` : nom préfixé pour le package créé et le groupe personnalisé. Par défaut, le nom du package présente le format suivant : *Agent importé- <plate-forme> <processus>*.
- `-p, --profile <arg>` : chemin d'accès au fichier de profil associé à la racine. Par défaut, le chemin d'accès au profil est le suivant : *core/config/IntroscopeAgent.profile*.
- `-t, --token <arg>` : valeur du jeton de sécurité de l'API publique
- `-u, --url <arg>` : passerelle cloud ou URL de base du proxy

Les valeurs d'URL et de jeton sont définies dans le fichier de configuration **application.properties**. Toutefois, vous pouvez remplacer ces valeurs à l'aide des paramètres de ligne de commande, si nécessaire. Pour plus d'informations sur la génération du jeton de sécurité, consultez la rubrique [Génération d'un jeton de sécurité](#).

NOTE

Si vous utilisez une machine virtuelle Java IBM, remplacez la valeur par défaut du fichier JAR de l'agent par le fichier *AgentNoRedefNoRetrans.jar*, car elle est utilisée pour une connexion à JVM à l'aide du paramètre `--agentJar`.

Logging

L'utilitaire fournit une journalisation détaillée pour le suivi de l'identification de groupes spécifiques et de la configuration des propriétés. Il journalise également toutes les demandes REST dans APM Command Center.

Pour activer la journalisation de débogage, activez ou supprimez les marques de commentaire de la propriété suivante dans le fichier de configuration **application.properties** : `logging.level.com=DEBUG`.

L'outil d'importation d'agent est un utilitaire de ligne de commande qui vous permet de migrer les agents Java pour CA APM 10.7 créés en tant que fichier .zip vers les derniers agents Java pour DX APM. Dans le processus de migration, un package APM Command Center est créé pour chaque agent tout en conservant les changements de configuration de la version antérieure.

Pour plus d'informations sur ce qui suit, reportez-vous à la section [Outil d'importation d'agent](#).

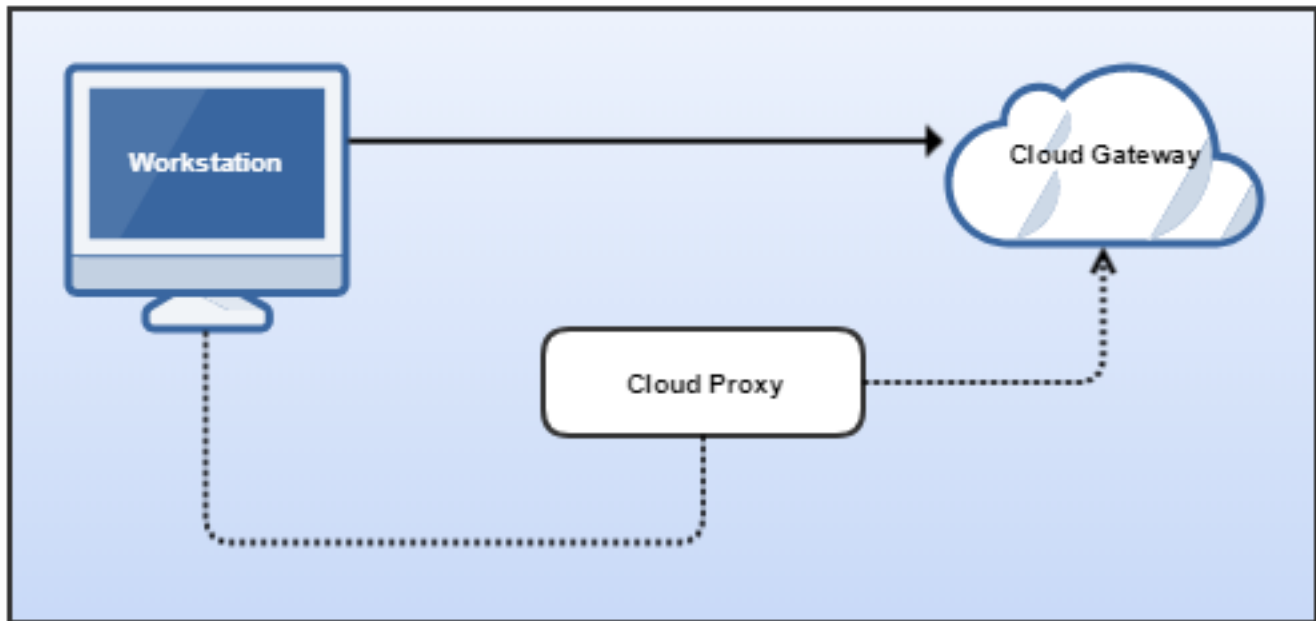
- Processus de migration
- Exécution de l'utilitaire Outil d'importation d'agent
- Paramètres de ligne de commande
- Logging

Connexion de la station de travail

La station de travail est disponible au téléchargement dans la section **Téléchargements** située dans le volet gauche. Par défaut, elle est configurée pour communiquer directement avec la passerelle cloud. Les organisations qui requièrent une communication de canal unique entre le centre de données et la passerelle cloud peuvent relier la station de travail au proxy cloud.

Le diagramme suivant illustre ces deux options :

Figure 3: ConnectWorkstation



Connexion de la station de travail à la passerelle cloud

Conditions préalables requises :

Pour exécuter la station de travail sous Linux, assurez-vous qu'Oracle ou qu'OpenJDK 11.x est installé sur votre ordinateur.

NOTE

Le protocole **Isengard** n'est pas pris en charge pour la passerelle cloud.

Procédez comme suit :

1. Sous **Paramètres, Téléchargements, téléchargez** la station de travail. Décompressez le fichier.
2. Démarrez la station de travail depuis la ligne de commande :
 - (Windows) `start.bat`
 - (Linux) `start.sh`
 La boîte de dialogue de connexion à la station de travail CA Introscope s'affiche.
3. Saisissez votre **mot de passe**.
4. Sélectionnez **Connexion**.
Le tableau de bord de la station de travail s'affiche.

Vous venez de connecter la station de travail à la passerelle cloud.

Connexion de la station de travail au proxy cloud

Conditions préalables requises :

- Pour exécuter la station de travail sous Linux, assurez-vous qu'Oracle 11.x ou qu'OpenJDK 11.x est installé sur votre ordinateur.
- Pour exécuter le proxy cloud, assurez-vous d'avoir installé une version prise en charge de Java (OpenJDK 11.x ou JDK Oracle 11.x) sur votre ordinateur.

Procédez comme suit :

1. Configurez le proxy cloud et vérifiez qu'il est en cours d'exécution.
Pour plus d'informations sur la configuration du proxy cloud, reportez-vous à la section [Configuration du proxy cloud](#).
2. Sous **Paramètres, Téléchargements, téléchargez** la station de travail. Décompressez le fichier.
3. Démarrez la station de travail depuis la ligne de commande :
 - (Windows) `start.bat`
 - (Linux) `start.sh`
 La boîte de dialogue de connexion à la station de travail DX APM Introscope s'affiche.
4. Saisissez l'URL du proxy comme valeur **URL du cloud**. Définissez l'URL du proxy au format suivant :
Par exemple, `ws://<<hôte_proxy_cloud>>:8081`.

TIP

Nous vous recommandons d'utiliser l'un des protocoles suivants (avec l'option de configuration correspondante et les valeurs par défaut) pour la connexion du proxy cloud à la station de travail :

- **apm.server.httpPort**
 - WS 8081
- **apm.server.secureHttpPort**
 - WSS 8444

NOTE

- L'URL cible du proxy est préconfigurée lorsque la fonctionnalité de téléchargement du proxy cloud est exécutée dans l'interface utilisateur graphique.
- Utilisez les protocoles Isengard et HTTP pour la connexion aux agents.

5. Saisissez votre **mot de passe**.
6. Sélectionnez **Connexion**.
Le tableau de bord de la station de travail s'affiche.

Vous venez de connecter la station de travail au proxy cloud.

Redémarrage de la station de travail

Lorsque vous avez fini d'utiliser la station de travail, vous pouvez vous déconnecter de la station de travail ou fermer la station de travail. La déconnexion de la station de travail met fin à la session actuelle, mais n'arrête pas la station de travail. Vous pouvez vous reconnecter à partir de la boîte de dialogue de connexion qui s'affiche par défaut lorsque vous vous déconnectez. La fermeture de la station de travail vous déconnecte de la station de travail et arrête le processus de station de travail. La station de travail enregistre le nombre de fenêtres Investigator et de console ouvertes, pour que la même configuration s'affiche lorsque vous vous reconnectez.

Procédez comme suit :

1. Ouvrez le répertoire dans lequel la station de travail a été extraite.
2. Démarrez la station de travail depuis la ligne de commande :
 - (Windows) `start.bat`
 - (Linux) `start.sh`
 La boîte de dialogue de connexion à la station de travail DX APM Introscope s'affiche.
3. Renseignez les champs obligatoires.
4. Sélectionnez **Connexion**.

Vous venez de redémarrer la station de travail.

NOTE

Informations complémentaires :

- [Présentation de la station de travail](#)

La station de travail est disponible au téléchargement dans la section **Téléchargements** située dans le volet gauche. Par défaut, elle est configurée pour communiquer directement avec la passerelle cloud. Les organisations qui requièrent une communication de canal unique entre le centre de données et la passerelle cloud peuvent relier la station de travail au proxy cloud.

Pour plus d'informations sur les stations de travail, reportez-vous à la section [Connexion de la station de travail](#).

Proxy cloud

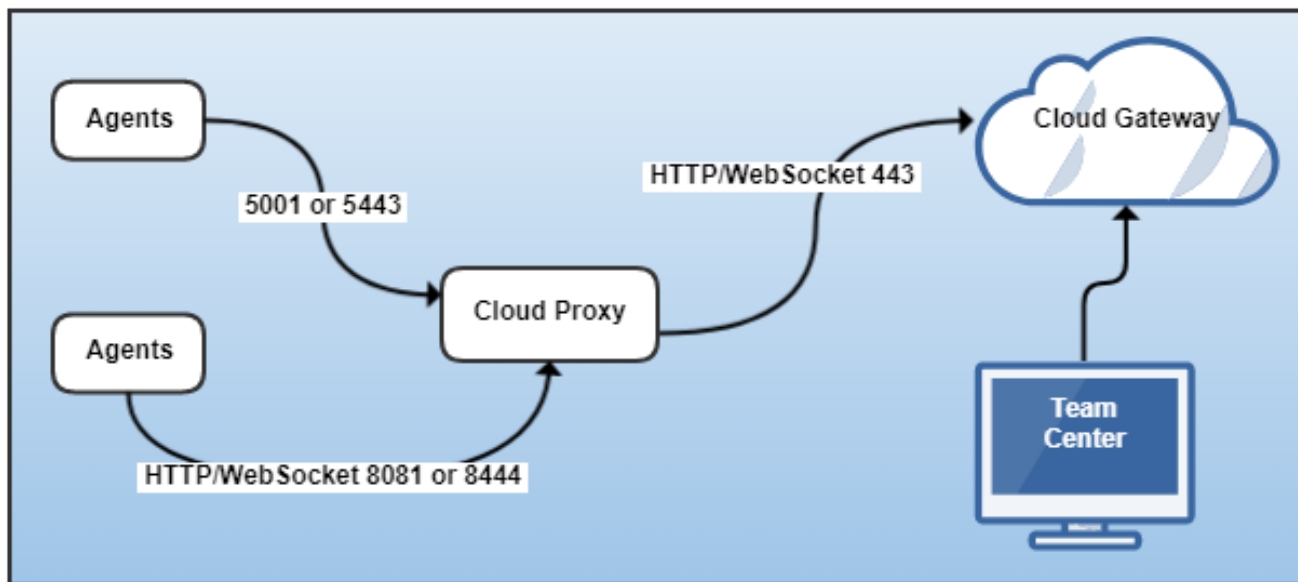
En tant qu'administrateur, téléchargez et configurez un proxy cloud pour migrer tous les agents actuellement connectés à CA APM 9.6 et versions ultérieures et à DX APM. Votre organisation a besoin de communications sortantes sur un proxy HTTP ou d'utiliser les communications à partir d'un nœud spécifique pour configurer le pare-feu. Vous pouvez utiliser le proxy cloud pour effectuer ces configurations. Vous pouvez configurer le proxy cloud en tant que proxy autonome ou l'exécuter dans un conteneur Docker.

NOTE

- Vous pouvez utiliser également le proxy cloud pour vous connecter à la station de travail. Pour plus d'informations, reportez-vous à la section Connexion de la station de travail dans la documentation d'APM.
- N'utilisez pas la méthode standard de création d'alertes APM pour les mesures ingérées directement dans NASS (cela inclut les mesures de prise en charge du proxy cloud APM et toute mesure non APM). Utilisez plutôt la [configuration d'alertes basées sur les mesures](#) de DX OI.

Le diagramme suivant présente les ports disponibles pour le proxy cloud :

Figure 4: Proxy cloud vers passerelle



Cet article contient les rubriques suivantes :

- [Configuration du proxy cloud](#)

- Configuration du service Linux
- Installation du service Windows
- Configuration de la haute disponibilité (HD)
- Connexion des nouveaux agents au proxy cloud
- Migrer des agents individuels vers DX APM à l'aide du proxy cloud
- Journalisation du proxy cloud
- Optimisation des performances du réseau et de l'UC
- Dépannage
- Mesures d'intégrité de la connexion de proxy cloud
- Mesures de prise en charge du proxy cloud

Configuration du proxy cloud

Une seule configuration initiale est requise pour le proxy cloud. Si vous effectuez une migration vers DX APM SaaS à partir d'une version sur site de DX APM, la configuration suivante exécutera la migration de tous les agents actuellement connectés.

Conditions préalables requises :

- Assurez-vous d'avoir installé une version prise en charge de Java (OpenJDK 11.x ou JDK Oracle 11.x) sur votre ordinateur.
- Assurez-vous d'avoir installé une version prise en charge du système d'exploitation sur votre ordinateur : RHEL 7.6 et versions ultérieures, CentOS 7.9 et versions ultérieures, ou Windows Server 2016 et versions ultérieures.
- Pour 4 000 agents par proxy cloud, la taille recommandée est de 4 Go pour le segment de mémoire. Par conséquent, pour 10 000 agents, il est recommandé de configurer trois proxies cloud.
- Allouez 6GBi de mémoire de l'OS pour environ 4 000 agents.

NOTE

6 GBi est une recommandation de dimensionnement par défaut, alors que la machine virtuelle Java utilise 4 GBi de segment de mémoire.

- Assurez-vous que l'espace disque soit suffisant pour stocker les journaux.
- Sur le système d'exploitation hôte, définissez la valeur du nombre maximum de descripteurs de fichier ouverts pour un **processus** sur 16384 ou une version ultérieure.
- Pour connecter 10 000 agents par proxy cloud, la recommandation de dimensionnement par défaut est de 8 GBi lorsque la machine virtuelle Java utilise 6 GBi du segment de mémoire.
Sur le système d'exploitation hôte, définissez le nombre maximum de descripteurs de fichiers ouverts pour un processus sur 61440 ou une valeur ultérieure.
- Pour connecter 15 000 agents par proxy cloud, la recommandation de dimensionnement par défaut est de 12 GBi lorsque la machine virtuelle Java utilise 8 GBi du segment de mémoire.
Sur le système d'exploitation hôte, définissez le nombre maximum de descripteurs de fichiers ouverts pour un processus sur 92160 ou une valeur ultérieure.

Configuration du service Linux

Procédez comme suit :

1. Dans l'interface utilisateur d'ATC, cliquez sur l'icône Paramètres



- ().
2. Sélectionnez **Téléchargements** et téléchargez le proxy cloud sur l'ordinateur sur lequel le gestionnaire d'entreprise MoM est exécuté. Extrayez le fichier.

L'URL cible et le jeton du proxy sont préconfigurés lorsque la fonctionnalité de téléchargement du proxy cloud est exécutée dans l'interface utilisateur d'ATC.

NOTE

Si nécessaire, vous pouvez remplacer le jeton. Dans l'interface utilisateur d'ATC, sous **Sécurité**, sélectionnez **Générer un nouveau jeton**. Assurez-vous que le type de jeton est défini sur **Agent**, puis définissez un délai d'expiration approprié, car la date d'expiration d'un jeton de type **Agent** ne peut pas être modifiée ultérieurement. Ensuite, dans le dossier de configuration, fichier `application.yml`, entrez le nouvel ID de jeton sous la propriété `apm.server.token`.

3. (Facultatif) Dans le fichier `application.yml` sous le dossier de configuration, les propriétés suivantes sont définies par défaut. Configurez les propriétés pour remplacer les ports TCP par défaut.

- `apm.server.port`
Valeur par défaut : 5001
- `apm.server.httpPort`
Valeur par défaut : 8081
- `apm.server.securePort`
Valeur par défaut : 5443
- `apm.server.secureHttpPort`
Valeur par défaut : 8444

NOTE

- Vous pouvez configurer le proxy cloud avec des ports personnalisés, mais le gestionnaire d'entreprise lui-même ajoute des mesures d'hôte et de port du gestionnaire d'entreprise que vous ne pouvez donc définir à partir d'aucun agent.
- En interne, le proxy cloud utilise Isengard, or le serveur Isengard héberge le port `apm.server.port`. Par conséquent, le port `apm.server.port` doit être ouvert pour que les protocoles HTTP/HTTPS puissent se terminer sur le proxy cloud.
- Pour Isengard, la valeur `ulimit` doit être définie sur le double du nombre d'agents. Par exemple, pour prendre en charge 8 000 agents, la valeur recommandée est 16 000.
- Pour les connexions HTTP/HTTPS, la valeur `ulimit` doit correspondre à quatre fois le nombre d'agents.

4. (Facultatif) Pour utiliser votre propre certificat de sécurité, accédez au fichier `application.yml` dans le dossier de configuration. Configurez les propriétés suivantes :

- `apm.server.useSelfSignedCert`
Définissez la valeur sur `false`.
- `apm.server.keyCertChainFile`
Saisissez un chemin d'accès à un fichier de certificat X.509 au format PEM.
- `apm.server.keyFile`
Saisissez un chemin d'accès à un fichier de clé privée PKCS#8 au format PEM. DX APM prend uniquement en charge le format PKCS#8.

NOTE

Par défaut, le proxy cloud utilise un certificat autosigné généré. Nous vous recommandons vivement de générer un certificat approuvé correctement signé. Les certificats autosignés ne doivent pas être utilisés dans des déploiements de production.

5. (Facultatif) Pour configurer un proxy HTTP pour la communication entre le proxy cloud et la passerelle cloud :
- a. Accédez au fichier `application.yml` dans le dossier de configuration. Configurez les propriétés suivantes :
 - `apm.server.httpProxy.host`
Entrez le nom d'hôte du proxy HTTP.
 - `apm.server.httpProxy.port`
Entrez le numéro de port du proxy HTTP.

- b. Si le proxy HTTP requiert une authentification, fournissez un nom d'utilisateur et un mot de passe valides :
 - `apm.server.httpProxy.username`
Entrez un nom d'utilisateur pour accéder au proxy HTTP.
 - `apm.server.httpProxy.password`
Entrez un mot de passe pour accéder au proxy HTTP.
6. (Facultatif) Pour appliquer la communication TLS 1.3 entre le proxy cloud et DX APM SaaS, configurez la valeur du paramètre `apm.server.secureClientProtocol` sur "TLSv1.3".
7. Arrêtez le gestionnaire d'entreprise MoM et tous les collecteurs.
8. Dans la ligne de commande, entrez la commande `apmservices.cloudproxy.sh` pour démarrer le proxy cloud. Le script démarre le processus `apmservices.cloudproxy` en arrière-plan.

NOTE

Pour l'utilisation de l'environnement de production, nous vous recommandons vivement de connecter le script au système de gestion des démons de la plate-forme cible. Par exemple : `init daemon`, `SystemD` ou `Upstart`.

9. Consultez les journaux suivants dans le répertoire des journaux pour vous assurer que le proxy cloud a démarré correctement :

- `logs/cloudproxy.log`
- `logs/apmservices.cloudproxy.wrapper.log`

Vous avez démarré le proxy cloud pour Linux. Si vous avez migré les agents à l'aide du proxy cloud, vous pouvez désormais consulter les agents dans Team Center, **Paramètres**, **Agents**.

NOTE

Les arguments suivants peuvent être utilisés avec `apmservices.cloudproxy.sh` :

Argument	Fonction
start	Démarre le service en arrière-plan.
run	Démarre le service au premier plan.
stop	Arrête le service si le service est en cours d'exécution.
restart	Arrête le service si le service est en cours d'exécution et le redémarre.
status	Imprime le statut en cours d'exécution et arrêté du service.
logs	Suit le journal dans <code>logs/cloudproxy.log</code> .
version	Imprime la version du service.
install	Installez et démarrez <i>apmservices-cloudproxy</i> en tant que service <i>systemd</i> .
uninstall	Arrêtez et désinstallez le service <i>apmservices-cloudproxy systemd</i> .

Installation du service Windows

Procédez comme suit :

1. Sous **Paramètres**, **Téléchargements**, téléchargez le proxy cloud sur l'ordinateur sur lequel le gestionnaire d'entreprise MoM est exécuté. Décompressez le fichier.
L'URL cible et le jeton du proxy sont préconfigurés lorsque la fonctionnalité de téléchargement du proxy cloud est exécutée dans l'interface utilisateur d'ATC.

NOTE

Si nécessaire, vous pouvez remplacer le jeton. Dans l'interface utilisateur d'ATC, sous **Sécurité**, sélectionnez **Générer un nouveau jeton**. Assurez-vous que le type de jeton est défini sur **Agent**, puis définissez un délai d'expiration approprié, car la date d'expiration d'un jeton de type **Agent** ne peut pas être

modifiée ultérieurement. Ensuite, dans le dossier de configuration, fichier `application.yml`, entrez le nouvel ID de jeton sous la propriété `apm.server.token`.

2. (Facultatif) Dans le fichier `application.yml` sous le dossier de configuration, les propriétés suivantes sont définies par défaut. Configurez les propriétés pour remplacer les ports TCP par défaut.

- **`apm.server.port`**
Valeur par défaut : 5001
- **`apm.server.httpPort`**
Valeur par défaut : 8081
- **`apm.server.securePort`**
Valeur par défaut : 5443
- **`apm.server.secureHttpPort`**
Valeur par défaut : 8444

NOTE

- Vous pouvez configurer le proxy cloud avec des ports personnalisés, mais le gestionnaire d'entreprise lui-même ajoute des mesures d'hôte et de port du gestionnaire d'entreprise que vous ne pouvez donc définir à partir d'aucun agent.
- En interne, le proxy cloud utilise Isengard, or le serveur Isengard héberge le port `apm.server.port`. Par conséquent, le port `apm.server.port` doit être ouvert pour que les protocoles HTTP/HTTPS puissent se terminer sur le proxy cloud.
- Pour Isengard, la valeur `ulimit` doit être définie sur le double du nombre d'agents. Par exemple, pour prendre en charge 8 000 agents, la valeur recommandée est 16 000.
- Pour les connexions HTTP/HTTPS, la valeur `ulimit` doit correspondre à quatre fois le nombre d'agents.

3. (Facultatif) Pour utiliser votre propre certificat de sécurité, accédez au fichier `application.yml` dans le dossier de configuration. Configurez les propriétés suivantes :

- **`apm.server.useSelfSignedCert`**
Définissez la valeur sur `false`.
- **`apm.server.keyCertChainFile`**
Saisissez un chemin d'accès à un fichier de certificat X.509 au format PEM.
- **`apm.server.keyFile`**
Saisissez un chemin d'accès à un fichier de clé privée PKCS#8 au format PEM. DX APM prend uniquement en charge le format PKCS#8.

NOTE

Par défaut, le proxy cloud utilise un certificat autosigné généré. Nous vous recommandons vivement de générer un certificat approuvé correctement signé. Les certificats autosignés ne doivent pas être utilisés dans des déploiements de production.

4. (Facultatif) Pour configurer un proxy HTTP pour la communication entre le proxy cloud et la passerelle cloud :

- a. Accédez au fichier `application.yml` dans le dossier de configuration. Configurez les propriétés suivantes :
 - **`apm.server.httpProxy.host`**
Entrez le nom d'hôte du proxy HTTP.
 - **`apm.server.httpProxy.port`**
Entrez le numéro de port du proxy HTTP.
- b. Si le proxy HTTP requiert une authentification, fournissez un nom d'utilisateur et un mot de passe valides :
 - **`apm.server.httpProxy.username`**
Entrez un nom d'utilisateur pour accéder au proxy HTTP.
 - **`apm.server.httpProxy.password`**
Entrez un mot de passe pour accéder au proxy HTTP.

5. (Facultatif) Pour appliquer la communication TLS 1.3 entre le proxy cloud et DX APM SaaS, configurez la valeur du paramètre `apm.server.secureClientProtocol` sur "TLSv1.3".
6. Arrêtez le gestionnaire d'entreprise MoM et tous les collecteurs.
7. Arrêtez le gestionnaire d'entreprise MoM et tous les collecteurs.
8. Installez le service Windows. Exécutez la ligne de commande en tant qu'administrateur et entrez
`apmservices.cloudproxy.exe install`
9. Démarrez le proxy cloud. Exécutez la ligne de commande en tant qu'administrateur et entrez
`apmservices.cloudproxy.exe start`
10. Consultez les journaux suivants dans le répertoire des journaux pour vous assurer que le proxy cloud a démarré correctement :
 - `logs/cloudproxy.log`
 - `logs/apmservices.cloudproxy.wrapper.log`

Vous avez démarré le proxy cloud pour Windows. Si vous avez migré les agents à l'aide du proxy cloud, vous pouvez désormais consulter les agents dans Team Center, **Paramètres, Agents**.

Configuration côté agent pour le proxy cloud

Si vous utilisez le certificat auto-signé, après l'avoir généré, effectuez les étapes suivantes pour que l'agent se connecte au gestionnaire d'entreprise :

Accédez au dossier dans lequel vous avez téléchargé l'agent. Par exemple, le fichier `introscopeAgent.profile` pour Tomcat est disponible sous `<wily\releases\2022.3\core\config>`. De même, pour un agent Infrastructure, le fichier `introscopeAgent.profile` se trouve sous `<apmia\core\config>`.

Copiez le fichier **.jks** du système de proxy cloud vers le système de l'agent. Dans le fichier **IntroscopeAgent.profile** du système de l'agent, indiquez le chemin d'accès où le fichier **.jks** a été copié.

Par exemple, `agentManager.trustStore.1=C:\linux_cp_certs\trust.jks`.

Entrez le mot de passe dans la propriété `agentManager.trustStorePassword.1` du fichier `IntroscopeAgent.profile`.

Par exemple, `agentManager.trustStorePassword.1=changeit`.

Configuration de la haute disponibilité (HD)

Le proxy cloud est un service autonome exécuté dans un environnement de système d'exploitation hôte client. Le gestionnaire de service du système d'exploitation ou une application tierce est requis pour assurer la disponibilité de l'instance. Le proxy cloud fournit une liveness probe via les terminaux HTTP et HTTPs `/supportability/health`. Un équilibreur de charge peut être placé devant les proxys cloud DX APM pour obtenir une haute disponibilité. L'équilibreur de charge s'assure que les reconnections d'agent sont acheminées vers une instance disponible. L'équilibreur de charge équilibre également le nombre de connexions entre les instances.

Configuration requise pour différents protocoles de transport d'agent pour une solution d'équilibrage de la charge tierce :

1. **Agents se connectant via le protocole de transport HTTP/HTTPS** : l'équilibreur de charge doit veiller à ce que les demandes HTTP d'un agent soient équilibrées vers l'instance de proxy cloud en fonction du cookie de session HTTP JSESSIONID. L'instance de proxy cloud conserve un canal WebSocket vers une passerelle APM associée à la session HTTP de l'agent.
2. **Agents se connectant via le protocole de transport WebSocket** : Le transport Agent WebSocket crée une connexion TCP socket stable. La solution tierce doit prendre en charge le protocole WebSocket.
3. **Agents se connectant via le protocole Isengard** : Le protocole Isengard est transféré directement via une connexion par socket TCP. Vous pouvez utiliser un équilibreur de charge réseau ou une technique similaire pour assurer le basculement vers une instance de proxy cloud disponible.

Connexion des nouveaux agents au proxy cloud

Utilisez le proxy cloud pour acheminer les données que les agents collectent vers la passerelle cloud via un canal unique.

Procédez comme suit :

1. Configurez le proxy cloud et vérifiez qu'il est en cours d'exécution.
Pour plus d'informations sur la configuration du proxy cloud, reportez-vous à la section [Configuration du proxy cloud](#).

NOTE

- Il n'est pas nécessaire de configurer le proxy cloud chaque fois que vous connectez un nouvel agent. Une seule configuration initiale est requise pour le proxy cloud.
- Si la connexion de l'agent au proxy cloud est effectuée via ws/wss, assurez-vous que l'agent fournit également la propriété **agentManager.credential**.

2. Téléchargez et déployez l'agent.
Pour plus d'informations sur le téléchargement et le déploiement des agents, consultez la section [Configuration et téléchargement d'un package d'agent](#).

- a. Utilisez le script de démarrage de l'agent pour définir la propriété de l'agent `agentManager.url.1` ou entrez `-D` et l'un des protocoles suivants :

- **WebSocket**

```
-DagentManager.url.1=ws://proxyhost:8081
```

- **WebSocket Secure**

```
-DagentManager.url.1=wss://proxyhost:8444
```

- b. Si l'agent dispose d'une extension de contrôleur, spécifiez la propriété de contrôleur `introscope.agent.acc.controller.configurationServer.url` ou entrez `-D` et l'un des protocoles suivants :

- **HTTP**

```
-Dintroscope.agent.acc.controller.configurationServer.url=http://proxyhost:8081
```

- **HTTPS**

```
-Dintroscope.agent.acc.controller.configurationServer.url=https://proxyhost:8444
```

- c. Démarrez l'agent.

L'agent est maintenant connecté au proxy cloud.

Vous pouvez afficher les agents connectés en cliquant sur **Paramètres, Agents**.

Migration d'agents individuels vers DX APM à l'aide d'un proxy cloud**IMPORTANT**

Exécutez cette procédure si vous souhaitez migrer des agents exécutés sur APM 10.7 (et versions antérieures).
Pour les versions 11 et ultérieures de DX APM, le cluster effectue automatiquement l'équilibrage de charge.

Vous pouvez configurer les détails du proxy Cloud dans le fichier *loadbalancing.xml* de votre installation sur site DX APM et autoriser la migration de chaque agent vers DX APM.

Ajoutez la configuration suivante pour connecter des agents à DX APM via un proxy cloud.

```
<agent-collector name="SendToProxy">
  <agent-specifier>.*\|.*\|.*</agent-specifier>
  <include>
    <collector host="<cloud-proxy-host>" port="5001"/>
  </include>
</agent-collector>
```

NOTE

Pour plus d'informations, reportez-vous à la section Configuration du fichier *loadbalancing.xml* pour les agents autorisés et non autorisés par le gestionnaire d'entreprise dans la documentation d'APM.

Journalisation du proxy cloud

Les journaux de proxy cloud sont disponibles dans le répertoire de journaux à l'emplacement suivant : `logs/cloudproxy.log`. Toutefois, vous pouvez activer des paramètres de journalisation supplémentaires pour afficher des informations de journal plus détaillées.

IMPORTANT

Après une mise à jour des détails de journalisation, vous devez redémarrer le processus Proxy cloud.

Activation du niveau de journalisation DEBUG (DEBOGAGE) ou TRACE (SUIVI)

IMPORTANT

Le niveau de journalisation TRACE fournit des traces de transaction à partir des vidages de threads de tous les paquets passant par le câble, les jetons d'informations confidentielles ou les informations d'identification transférées. Activez la journalisation de niveau TRACE uniquement lorsque le support Broadcom le demande ou lorsque le dépannage approfondi est requis. Désactivez la journalisation de niveau TRACE après avoir terminé les tests.

Option 1 : Ajout d'un paramètre JVM

Niveau de journalisation DEBUG (DEBOGAGE)

Ouvrez `apmservices.cloudproxy.bat/sh`, puis ajoutez le paramètre de machine virtuelle Java :

```
-Dlogging.level.com.ca.apm.cloudproxy=DEBUG
```

Niveau de journalisation TRACE

En général, le niveau de journalisation DEBUG fournit suffisamment de détails, car il consigne la plupart des exceptions de connexion. Cependant, si vous basculez vers le niveau de journalisation TRACE, vous devez ajouter le paramètre de machine Java supplémentaire `SocketProxyWS` pour diagnostiquer les paquets par câble.

Ouvrez `apmservices.cloudproxy.bat/sh`, puis ajoutez le paramètre de machine virtuelle Java :

```
-Dlogging.level.com.ca.apm.cloudproxy=TRACE -Dlogging.level.SocketProxyWS=TRACE
```

Vous trouverez ci-dessous les options de suivi de bas niveau que vous pouvez utiliser pour déboguer les problèmes entrants :

```
-Dlogging.level.CloudProxyIsengard=TRACE - suit les communications entrantes pour tous les ports de communication DX APM internes.
```

```
-Dlogging.level.CloudProxyHTTP=TRACE - suit toutes les communications entrantes des ports HTTP.
```

Pour un débogage spécifique, utilisez les options suivantes :

```
-Dlogging.level.HTTPBinaryTunnel=TRACE - suit les données du protocole HTTP binaire en entrée. Utilisez l'option de débogage des problèmes avec les agents se connectant au proxy via le protocole HTTP binaire.
```

```
-Dlogging.level.HTTPSoapTunnel=TRACE - suit les données du protocole HTTP Soap en entrée. Utilisez l'option de débogage des problèmes avec les agents se connectant au proxy via le protocole HTTP SOAP (agents hérités).
```

```
-Dlogging.level.WSTunnel=TRACE - suit le protocole WebSocket en entrée. Utilisez l'option de débogage des problèmes avec les connexions WS.
```

```
-Dlogging.level.AccHttpProxy=TRACE - suit la communication proxy HTTP d'APM Command Center sur le côté entrant.
```

Option 2 : Ajout d'une propriété masquée

Ouvrez le fichier `./config/application.yml`, puis ajoutez la propriété masquée :

```
logging.level.com.ca.apm.cloudproxy: DEBUG
```

Ou

Ouvrez le fichier `./config/application.yml`, puis ajoutez la propriété masquée :

```
logging.level.com.ca.apm.cloudproxy: TRACE
```

Mise à jour de l'historique et de la taille des fichiers journaux

Ouvrez les fichiers `./config/application.yml`, puis ajoutez les propriétés suivantes :

```
logging.file.max-history: <nombre_jours>
```

Par défaut, un nouveau fichier journal est créé lorsque le précédent atteint 10 Mo. Les fichiers journaux précédents sont conservés pendant 7 jours, sauf si vous modifiez la valeur de ce paramètre.

Exemple : `logging.file.max-history : 14`

Dans cet exemple, les fichiers journaux sont conservés pendant 14 jours.

```
logging.file.total-size-cap:<taille-en-octets-unités-incluses>
```

Où `logging.file.total-size-cap` correspond aux sauvegardes de journal à stocker et est représenté en termes de taille de fichier (Mo, Go).

Définissez la taille de l'archive totale des journaux. Lorsque la taille des archives dépasse ce seuil, les sauvegardes sont supprimées. Les unités prises en charge sont les suivantes : octets, kilo-octets, mégaoctets, gigaoctets et téraoctets.

Exemple : `logging.file.total-size-cap : 1 Go`

Dans cet exemple, les sauvegardes sont supprimées lorsque la taille totale de l'archive des journaux dépasse 1 Go.

IMPORTANT

Par défaut, la taille maximum du fichier journal est définie sur 10 Mo. Si vous voulez mettre à jour cette valeur, vous pouvez utiliser la propriété suivante :

```
logging.file.max-size
```

Optimisation des performances du réseau et de l'UC

Utilisez `apm.server.compressionLevel` dans le fichier `application.yml` pour configurer le niveau de compression pour la communication WebSocket entre le proxy cloud et la passerelle. Vous pouvez définir n'importe quelle valeur comprise entre 0 et 9. Elle équilibre la quantité de données et d'UC utilisée. Par exemple,

```
apm.server.compressionLevel: 1
```

Les valeurs applicables sont les suivantes :

- 6 : valeur par défaut
- 1 : pour atteindre la vitesse réseau constante pour le proxy cloud, mais cela peut augmenter légèrement le trafic réseau.
- 9 : à utiliser pour une meilleure compression
- 0 : pas de compression. Il est recommandé de ne pas utiliser cette valeur, car elle augmente la quantité de données et l'amélioration de l'UC est minime.

NOTE

Redémarrez le proxy cloud après chaque modification de configuration.

Distinction des proxys cloud

Utilisez le préfixe `apm.server.proxyAgentNamePrefix` dans le fichier `application.yml` pour ajouter un préfixe au nom d'hôte de l'agent. Il peut être utilisé pour distinguer plusieurs proxys cloud. Cette fonctionnalité est disponible uniquement pour les communications ws/wss avec la passerelle cloud définies via `apm.server.proxyTarget`.

Dépannage

Symptôme :

Le démarrage du proxy cloud échoue et le message d'erreur suivant apparaît :

```
No provider succeeded to generate a self-signed certificate.
```

Solution :

La génération d'un certificat autosigné n'est pas prise en charge dans les environnements d'exécution IBM J9. Les certificats doivent être générés séparément et fournis au proxy cloud à l'aide des propriétés de configuration indiquées plus haut.

Symptôme :

L'agent ne peut pas se connecter à la passerelle Cloud.

Solution :

Utilisez le nom d'hôte de la passerelle Cloud fournie lors de la définition des règles de pare-feu sortant. L'utilisation d'une adresse IP à la place peut entraîner une interruption de connexion inattendue en cas de changement de l'adresse IP.

Symptôme :

L'agent ne peut pas se connecter à DX APM et le message suivant s'affiche dans le fichier journal du proxy cloud `logs/cloudproxy.log` :

```
java.net.SocketException: Too many open files
```

Solution :

Sur le système d'exploitation hôte, définissez la valeur du nombre maximum de descripteurs de fichier ouverts pour un **processus** sur 16384 ou une version ultérieure. Consultez la documentation de votre système d'exploitation pour en savoir plus sur l'augmentation de la limite des ressources système par processus.

Symptôme :

Le proxy cloud ne parvient pas à transférer la connexion de l'agent ou de la station de travail et le message d'erreur suivant s'affiche :

```
sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.  
SunCertPathBuilderException: unable to find valid certification path to requested target
```

Solution :

Les services DX APM sont déployés avec un certificat auto-signé ou non valide. Pour permettre au proxy cloud de se connecter à ces systèmes, définissez le paramètre **apm.server.proxyInsecure** sur *true* dans le fichier `config/application.yml`, comme indiqué ci-dessous.

Exemple : `apm.server.proxyInsecure: true`

NOTE

L'approbation de certificats non valides présente un sérieux risque de sécurité. Elle doit être utilisée uniquement dans des cas justifiés et désactivée dès qu'un certificat valide est déployé sur l'équilibreur de charge d'avant-plan de la passerelle DX APM.

Mesures d'intégrité du proxy cloud

Vous pouvez surveiller l'intégrité d'une connexion de proxy cloud à l'aide des mesures de connexion. Pour générer les mesures, définissez une valeur de jeton d'agent valide pour le paramètre de configuration `apm.server.token`. Cette section contient également les détails relatifs aux mesures de durabilité signalées à partir du proxy cloud.

Configurez un nom pour les mesures de proxy cloud à l'aide du paramètre de configuration `apm.server.id`. Ce nom s'affiche dans l'arborescence des mesures. Si vous ne configurez pas la valeur de `apm.server.id`, le proxy cloud détecte le nom d'hôte de l'ordinateur (adresse IP) et l'affiche dans l'arborescence des mesures.

NOTE

N'utilisez pas les mesures de durabilité du proxy cloud pour configurer des alertes. Au lieu de cela, vous pouvez utiliser l'interface utilisateur de DX Operational Intelligence SaaS pour configurer les alertes. Reportez-vous à la section [Configuration des alertes basées sur les mesures](#).

Le tableau suivant répertorie certains noms de mesures importants pour un proxy cloud.

Nom de la mesure	Description
SuperDomain apmservices CloudProxy PROXY_ID Agents Active Connections Count	Nombre d'agents connectés via le proxy cloud.
SuperDomain apmservices CloudProxy PROXY_ID Configuration Agent HostName Prefix	Préfixe du nom d'hôte de l'agent. Cette valeur s'affiche uniquement lorsque le préfixe est configuré pour un nom d'hôte d'agent.
SuperDomain apmservices CloudProxy PROXY_ID Beans	Vous pouvez utiliser les propriétés du bean pour un examen approfondi.
SuperDomain apmservices CloudProxy PROXY_ID Resources	Affiche l'utilisation des ressources pour le proxy cloud et l'hôte.
SuperDomain apmservices CloudProxy PROXY_ID Resources System Uptime (ms)	Vous pouvez l'utiliser pour examiner le redémarrage de l'agent.

En tant qu'administrateur, téléchargez et configurez un proxy cloud pour migrer tous les agents actuellement connectés à CA APM 9.6 et versions ultérieures et à DX Application Performance Management. Votre organisation a besoin de communications sortantes sur un proxy HTTP ou d'utiliser les communications à partir d'un nœud spécifique pour configurer le pare-feu. Vous pouvez utiliser le proxy cloud pour effectuer ces configurations. Vous pouvez configurer le proxy cloud en tant que proxy autonome ou l'exécuter dans un conteneur Docker.

Pour plus d'informations sur l'installation, la configuration, la migration, la journalisation et le dépannage des problèmes spécifiques au proxy cloud, reportez-vous à la section [Proxy cloud](#).

Mesures de prise en charge du proxy cloud

Cette page décrit les mesures de prise en charge pour le proxy cloud.

NOTE

Les préfixes suivants sont destinés aux mesures répertoriées ci-dessous : `apmservices | CloudProxy | PROXY_HOSTNAME` ou `apmservices | CloudProxy | PROXY_ID`.

Agents

Nom de la mesure	
Active Connections Count	Nombre d'agents connectés.
Closed per Interval	Nombre de connexions fermées par intervalle.
Connections failed per Interval	La connexion n'a pas été établie.
Connections reset by peer per Interval	Indique que le serveur ou le client distant a fermé la connexion de façon inattendue de charge.
Connections timed out per Interval	La connexion n'a pas été établie dans les délais impartis.

Nom de la mesure	
I/O exceptions per Interval	Nombre d'exceptions d'E/S par intervalle.
Other exceptions per Interval	Nombre d'autres problèmes non spécifiés.
Writes failed per Interval	Nombre d'échecs d'écriture par intervalle.

Beans | SupportabilityManagerPoller

Mesures BlamePoint

Nom de la mesure	
Temps de réponse moyen (ms)	La mesure Average Response Time établit la moyenne des temps de réponse pour satisfaire une demande.
Average Response Time (us)	
Concurrent Invocations	Les appels sont des demandes gérées par l'application et ses différentes parties.
Erreurs par intervalle	Les erreurs correspondent au nombre d'exceptions signalées par la machine.
Réponses par intervalle	Reflète le nombre d'appels terminés dans cet intervalle. Cette mesure concerne les appels terminés pendant un intervalle.
Nombre de blocages	Les demandes bloquées sont celles qui ne sont pas terminées dans un délai donné, cela signifie que son exécution a dépassé le seuil de blocage.
Total Metrics (Mesures totales)	Nombre de mesures signalées par le proxy cloud.

Resources | Buffer Pool

Le chemin Resources | Buffer Pool fournit des mesures de surveillance pour les mémoires tampons directes allouées en dehors du segment de mémoire.

Nom de la mesure	
Buffer Count	Nombre de tampons dans les pools de tampons Java (tampons directs, etc.).
Buffer Total Capacity	Capacité totale de tous les tampons.
Buffer Memory Used	Quantité totale de mémoire utilisée par tous les tampons.

Resources | CPU

Nom de la mesure	
CPU Used (%)	Somme de l'utilisation totale de l'UC en % pour les noyaux individuels. Elle peut varier de 0 à 100.
CPU Used (ms)	Somme de l'utilisation totale de l'UC pour les noyaux individuels en ms par intervalle.
Kernel CPU (%)	Somme de l'utilisation de l'UC en % passé dans le noyau (heure système).
Kernel CPU (ms)	Somme de l'utilisation de l'UC en % passé dans le noyau (heure système) en ms par intervalle.
User CPU (%)	Somme de l'utilisation de l'UC en % passé dans l'espace utilisateur.

Resources | Host | CPU

Nom de la mesure	
CPU Used (%)	Somme de l'utilisation totale de l'UC en % pour les noyaux individuels. Elle
CPU Used (ms)	Somme de l'utilisation totale de l'UC pour les noyaux individuels en ms par i
Idle CPU (%)	Durée pendant laquelle l'UC n'a pas été occupée.
Idle CPU (ms)	
Kernel CPU (%)	Somme de l'utilisation de l'UC en % passé dans le noyau (heure système).
Kernel CPU (ms)	Somme de l'utilisation de l'UC en % passé dans le noyau (heure système) e
Wait CPU (%)	Somme de l'utilisation de l'UC en % passé dans l'espace utilisateur.
Wait CPU (ms)	Temps d'attente de l'UC, par exemple, pour que les opérations d'E/S de diso même si cela ne rend pas un système défectueux, cela limite les performan

Resources | Host | Memory

Ces mesures sont utilisées pour surveiller la mémoire de l'hôte.

Nom de la mesure	
Memory Available (byte)	Quantité de mémoire disponible pour l'allocation à un nouveau processus
Memory Total (byte)	Mémoire physique totale sur l'hôte.
Memory Usage (%)	Mémoire actuellement utilisée par les processus en cours d'exécution.

Resources | Memory

Les mesures sous Resources | Memory surveillent la mémoire utilisée par le processus de la machine virtuelle Java.

Nom de la mesure	
GC Count	Nombre de nettoyage de mémoire de la machine virtuelle Java exécutés p
GC Time (ms)	Durée cumulée des pauses de nettoyage de mémoire par intervalle. Si le performances sont affectées de manière significative.
Memory Heap Committed	Quantité de mémoire dont la disponibilité est garantie pour l'utilisation par
Memory Heap Max	Quantité maximum de mémoire pouvant être utilisée pour la gestion de la APM_HEAP_XMXPCT, APM_HEAP_XMXMIN, APM_HEAP_XMXMAX da
Memory Heap Used	Quantité réelle de mémoire utilisée par le segment de mémoire.
Memory Resident (byte)	Quantité de mémoire occupée par le processus.
Memory Virtual (byte)	Taille de la mémoire virtuelle du processus.
Memory No Heap Committed	Quantité de mémoire maximum dont la disponibilité est garantie pour la m internes.
Memory No Heap Max	Quantité de mémoire maximum la machine virtuelle Java utilisée afin de s
Memory No Heap Used	Quantité de mémoire réelle la machine virtuelle Java utilisée afin de stock

Resources | Storage

Nom de la mesure	
Disk Read (byte)	Octets lus sur le disque par intervalle.
Disk Write (byte)	Octets écrits sur le disque par intervalle.

Resources | System

Nom de la mesure	
Harvest Cycle Duration (ms)	Les mesures de prise en charge collectent la durée de la période.
Uptime (ms)	Nombre de millisecondes écoulées depuis le début de l'instance.

Configuration de la station de travail

En tant qu'administrateur, vous pouvez configurer les options suivantes au niveau de la station de travail :

Exécution de la station de travail en mode documenté

Exécute la station de travail en mode documenté pour créer des messages de journal détaillés à utiliser à des fins de débogage ou de dépannage.

Procédez comme suit :

- Ouvrez le fichier `IntroscopeWorkstation.properties` sous `<répertoire_base_station_travail>/config`.
- Dans la propriété `log4j.logger.Workstation`, remplacez `INFO` par l'instruction suivante :

```
VERBOSE#com.wily.util.feedback.Log4JSeverityLevel
```
- Enregistrez les modifications.

Redirection de la sortie de la station de travail vers un fichier

Définissez le fichier `IntroscopeWorkstation.properties` de manière à rediriger les messages de sortie détaillés vers un fichier journal.

Procédez comme suit :

- Ouvrez le fichier `IntroscopeWorkstation.properties` dans le répertoire `<répertoire_base_station_travail>/config`.
- Dans la propriété `log4j.logger.Workstation`, remplacez `console` par `logfile`. Le paramètre de propriété ci-dessous entraîne par exemple la journalisation des messages détaillés dans un fichier journal par la station de travail :

```
log4j.logger.Workstation=VERBOSE#com.wily.util.feedback.Log4JSeverityLevel,logfile
```
- (Facultatif) Modifiez le nom et l'emplacement du fichier journal de la station de travail à l'aide de la propriété `log4j.appender.logfile.File`.

Configuration de station de travail pour la saisie des valeurs de connexion

Vous pouvez modifier le fichier `Introscope_Workstation.lax` pour saisir les valeurs de connexion et ignorer l'écran de connexion.

Procédez comme suit :

- Ouvrez le fichier `<répertoire_bas_EM>/Introscope_Workstation.lax`.

2. Dans la propriété *lax.command.line.args*, ajoutez des commandes *-login* pour chaque commande de connexion à laquelle une valeur doit être saisie. Par exemple, pour l'authentification locale, cette propriété est similaire à l'instruction suivante :

```
lax.command.line.args=$CMD_LINE_ARGUMENTS$ -loginimmediate
-loginhost foos -loginport 4503 -loginresponse sanderson,45tst87
```

WARNING

Ne supprimez pas la valeur par défaut *\$CMD_LINE_ARGUMENTS\$* du paramètre.

Vous êtes connecté maintenant à la station de travail et une console s'ouvre. En cas d'échec de la connexion, la station de Job ne démarre pas et un message d'erreur est journalisé.

Activation de l'expiration de la session dans la station de travail

L'expiration automatique de la session ajoute un niveau supplémentaire de sécurité en déconnectant les utilisateurs inactifs. Modifiez le fichier *IntroscopeEnterpriseManager.properties* pour activer l'expiration automatique de session.

Procédez comme suit :

1. Ouvrez le fichier *<répertoire_base_EM>/config/IntroscopeEnterpriseManager.properties*.
2. Ajoutez la propriété *introscope.apmserver.ui.inactivityLogoutTimeout* et définissez la valeur (en minutes) sur un nombre entier supérieur à 0 pour activer l'expiration de la session. Par exemple, l'instruction suivante expire la session après 60 minutes :

```
introscope.apmserver.ui.inactivityLogoutTimeout=60
```

NOTE

L'expiration de la session est désactivée par défaut (valeur = 0).

Configuration de la station de travail pour les rapports dans une langue asiatique

Ajoutez les composants suivants pour votre installation de la station de travail afin de générer des rapports Introscope dans des langues qui utilisent des jeux de caractères multi-octet telles que le chinois et japonais.

Génération de rapports aux formats HTML et RTF dans une langue asiatique

(Windows) Installez la prise en charge de langues supplémentaires dans les langues de l'Asie de l'Est. Pour plus d'informations sur la prise en charge linguistique, rendez-vous sur la page <https://msdn.microsoft.com/en-us/goglobal/default>.

Génération de rapports au format PDF dans une langue asiatique

Procédez comme suit :

1. Téléchargez le pack de polices asiatiques d'Acrobat Reader à partir de la page <http://www.adobe.com/support/downloads/product.jsp?platform=windows&product=10>.
2. Installez le pack de polices asiatiques d'Acrobat Reader.

Configuration de la station de travail pour l'utilisation du proxy HTTP avec l'authentification

Utilisez *transport.http.proxy.username* et *transport.http.proxy.password* pour spécifier les valeurs d'authentification, où *transport.http.proxy.password* doit être chiffré. Pour chiffrer le mot de passe, effectuez les opérations ci-après.

Procédez comme suit :

1. Ouvrez le fichier *IntroscopeWorkstation.properties* sous *<répertoire_base_station_travail>/config*.
2. Dans la propriété *transport.http.proxy.password*, saisissez le mot de passe chiffré.
Vous pouvez exécuter la commande suivante pour chiffrer le mot de passe :

```
java -cp plugins\com.wily.core_<VERSION>.jar com.wily.util.properties.PropertiesUtils encrypt <PASSWORD>
```

Où <VERSION> correspond à la version d'APM installée sur la station de travail et où <PASSWORD> est le mot de passe non chiffré.

3. Enregistrez les modifications.

En tant qu'administrateur, vous pouvez configurer les options suivantes au niveau de la station de travail :

- Exécution de la station de travail en mode documenté
- Redirection de la sortie de la station de travail vers un fichier
- Configuration de station de travail pour la saisie des valeurs de connexion
- Activation de l'expiration de la session dans la station de travail
- Configuration de la station de travail pour les rapports dans une langue asiatique
- Configuration de la station de travail pour l'utilisation du proxy HTTP avec l'authentification

Pour plus d'informations sur chaque option de station de travail configurable, reportez-vous à la section [Configuration de la station de travail](#).

Règles de suppression des traces pour le masquage des données sensibles

Les agents exécutés dans des environnements utilisateur envoient plusieurs types de données, dont des données de suivi. Ces données de suivi peuvent contenir des informations confidentielles/personnelles/sensibles que l'utilisateur doit masquer. Vous pouvez définir des règles de suppression des traces permettant d'identifier de telles données et les remplacer par du texte préconfiguré, tel que SUPPRESSED BY APM. Pour chaque client hébergé, vous pouvez ajouter plusieurs règles pour tous les attributs pour lesquels vous souhaitez supprimer la valeur de trace.

Les agents exécutés dans des environnements utilisateur envoient plusieurs types de données, dont des données de suivi. Ces données de suivi peuvent contenir des informations confidentielles/personnelles/sensibles que l'utilisateur doit masquer. Vous pouvez définir des règles de suppression des traces permettant d'identifier de telles données et les remplacer par du texte préconfiguré, tel que SUPPRESSED BY APM.

Pour configurer une règle de suppression des données de trace, reportez-vous à la section [Règles de suppression des traces pour le masquage des données sensibles](#).

Configuration d'une règle de suppression des données de suivi

1. Connectez-vous à Team Center et cliquez sur **Settings** (Paramètres), puis sur la mosaïque **Security** (Sécurité).
2. Cliquez sur **Trace Suppression Rule** (Règle de suppression des traces).
La fenêtre **Trace Suppression Rule** (Règle de suppression des traces) s'affiche. Elle contient toutes les règles actuellement configurées.
3. Cliquez sur **Trace Suppression Rule** (Règle de suppression des traces).
La boîte de dialogue **Edit Trace Suppression** (Modifier la suppression des traces) s'affiche.
4. Saisissez les informations suivantes :
 - **Name** (Nom) : attribuez un nom à la règle de suppression des traces.
 - **Description** : fournit une description appropriée de la règle à configurer.
 - **Configure** (Configurer)
 - **Suppressed Properties** (Propriétés supprimées) : entrez l'attribut pour lequel la valeur de trace doit être masquée dans APM. Par exemple, `FullUrl`. Vous pouvez utiliser l'icône plus pour ajouter plusieurs attributs.
 - **Regular Expression** (Expression régulière) : pour sélectionner plusieurs agents portant des noms similaires, utilisez l'astérisque * comme caractère générique avec les mêmes initiales des agents. Par exemple, pour

sélectionner tous les agents dont le nom commence par `tas-uk`, entrez `tas-uk.*`. Tous les agents qui remplissent les critères apparaissent alors dans la liste **Preview** (Aperçu).

- **Individual Agents** (Agents individuels) : dans cette liste, sélectionnez tous les agents pour lesquels vous souhaitez supprimer la valeur de trace. Tous les agents sélectionnés apparaissent dans la liste **Preview** (Aperçu).

Par exemple, le champ **Suppressed Properties** (Propriétés supprimées) est défini sur `FullUrl` et `tas-uk.*` est défini dans le champ **Regular Expression** (Expression régulière). Les données de suivi de tous les agents dont le nom commence par `tas-uk.*` s'affichent sous forme de texte SUPPRESSED BY APM chaque fois que la valeur de l'attribut `FullUrl` apparaît.

5. Pour enregistrer la règle, sélectionnez **Save** (Enregistrer).

La nouvelle règle apparaît dans la liste des règles de la fenêtre **Trace Suppression Rule** (Règle de suppression des traces).

Configuration d'APM Command Center

APM Command Center vous permet d'effectuer les opérations suivantes :





- Afficher les propriétés de l'agent stocké localement en sélectionnant un agent dans la liste. Chaque agent est vérifié et ses propriétés sont mises à jour toutes les 24 heures (signal d'activité). Reportez-vous à la section [Affichage du statut de l'agent](#).
- Obtenir des informations plus détaillées sur un agent particulier en générant un rapport. Les rapports de diagnostic vous fournissent des informations détaillées sur un agent. Vous pouvez faire défiler les propriétés détaillées de l'agent ou télécharger un fichier ZIP contenant tous les détails, y compris les fichiers journaux et de configuration. Vous pouvez utiliser ce fichier ZIP lorsque vous faites référence à cet agent particulier. Reportez-vous à la section [Affichage des rapports d'agent](#).
- Afficher toutes les applications créées dans DX Application Performance Management. Vous pouvez utiliser ces applications pour les intégrer dans DX APM de manière transparente et pour configurer facilement les packages d'installation de l'agent pour votre environnement. Reportez-vous à la section [Configuration des applications pour l'intégration](#).
- Créer et déployer des packages d'agent sur des serveurs d'applications à partir d'APM Command Center. Les packages d'agent sont un ensemble de fichiers binaires d'agent et de fichiers de configuration au format ZIP ou TAR pouvant être déployés. Chaque package comprend plusieurs groupes. Un *groupe* est une partie compacte d'une fonctionnalité d'agent. Reportez-vous à la section [Gestion des packages d'agent](#).
- Les groupes représentent des sous-ensembles de la fonctionnalité de surveillance d'agent. Les exigences de compatibilité, les interrelations et les dépendances sont définies pour chaque groupe et déterminent les possibilités de combinaison. Pour modifier la configuration d'un agent, modifiez les propriétés de groupe dans un package d'agent existant. Reportez-vous à la section [Configuration des groupes](#).

API RESTful

Pour une interaction automatisée avec DX APM Command Center, vous pouvez utiliser l'API RESTful. Pour plus d'informations, reportez-vous à la section [API APM Command Center](#).

Affichage du statut de l'agent

La page Agents répertorie tous les agents de l'environnement. À l'aide du bouton de téléchargement, vous pouvez télécharger la liste des agents au format CSV. L'icône correspondant au nom de l'agent fournit le statut actuel de l'agent.

- Actif  : l'agent répond dans l'intervalle de pulsation de 24 heures de l'agent contrôleur.
- Actif  : la configuration de l'agent a été récemment modifiée et l'agent doit être redémarré pour que les modifications prennent effet.
- Arrêté  : les agents 10.2 et versions ultérieures communiquent avec le contrôleur d'agent toutes les 60 secondes. Si un agent arrête de signaler des données, il est marqué comme Arrêté.
- Absent(e)  : l'agent n'a pas répondu depuis plus de 24 heures. Si ce n'est pas le comportement attendu, vérifiez que l'agent est en cours d'exécution.

NOTE

- Un agent inactif est supprimé de la liste au bout de sept jours.
- Les données ne sont pas dynamiques. L'application affiche les données valides au moment du dernier contact régulier avec l'agent. Les données peuvent dater d'il y a 24 heures pour les versions antérieures des agents.
- Vous pouvez rechercher un agent spécifique à l'aide de la barre de recherche. Pour plus d'informations, reportez-vous à la section Recherche d'un agent.

Informations sur l'agent

La sélection d'un agent dans la liste fournit les informations suivantes sur l'agent :

- Informations sur l'agent
- Environnement
- Configuration
- Rapport de diagnostic

Environnement

Les informations sur l'environnement incluent les éléments suivants :

- Machine virtuelle Java
- Version de la machine virtuelle Java
- Serveur d'applications
- Version du serveur d'applications
- OS Type
- OS Version

Configuration

Les informations sur la configuration incluent les éléments suivants :

- Name (nom)
- Dernier changement
- Version du package

Vous pouvez également modifier la configuration, modifier un package ou révéler la configuration du package, si disponible.

Pour modifier la configuration d'un agent, sélectionnez l'agent, puis cliquez sur **Modifier** dans la fiche **Configuration**.
(ADD A LINK TO THE SECTION)

Rapport de diagnostic

Vous pouvez générer le rapport de diagnostic d'un agent en sélectionnant le bouton **Générer** dans la fiche Rapports de diagnostic. Une fois le rapport généré, vous pouvez l'afficher ou le télécharger à partir de la page Rapports.

Recherche d'agents

Pour rechercher des agents, utilisez la barre de recherche en haut de la page ACC. Vous pouvez rechercher par propriété d'agent (nom, statut, système d'exploitation, etc.). Vous pouvez également effectuer une recherche globale sur la page Accueil.

Pour rechercher des agents à l'aide du langage de requête ACC, reportez-vous à la section [Recherche à l'aide du langage de requête ACC \(AQL, ACC Query Language\)](#).

Voici des exemples de recherches d'agents :

- `appServerName:Tomcat`
- Recherchez une expression à l'aide de guillemets doubles et de caractères génériques.
`**"Windows Server 2016"**`
- Utilisez les opérateurs ET (par défaut), OU et NON.
`logLevel:info OR logLevel:debug`
- Recherchez les agents Tomcat, mais uniquement ceux dont le nom de serveur ne contient pas le mot linux :
`processName:Tomcat NOT serverName:linux`
- Recherchez les agents dont les valeurs de champ sont comprises entre les limites inférieure et supérieure spécifiées. Utilisez des dates exactes ou une période pour une plage de temps, par exemple des semaines (w), des jours (d), des heures (h), des minutes (m) et des secondes (s).
`lastContact:[-5w TO NOW]`
- Utilisez des parenthèses pour regrouper les opérateurs logiques.
`(osName:windows OR osName:Linux) AND logLevel:info`
- Placez les recherches par expression régulière entre des barres obliques /.

TIP

Vous pouvez copier et coller des expressions de recherche d'agent à partir des mesures WebView.

```
/ACCServer.*01\|Tomcat\|.Agent/
```

Enregistrement de la recherche

Dans la barre de recherche, utilisez l'option **Enregistrer en tant que nouvelle collection** pour enregistrer un modèle de recherche que vous utilisez fréquemment. Vous pouvez également utiliser la recherche enregistrée dans une requête.

Exemple : utilisation de la collecte dans une requête

```
collection:"Tomcat Agents" AND reportName:Linux
```

Propriétés de la recherche d'agent

La propriété par défaut pour la recherche d'agent est `spaName`. Elle contient le nom du serveur, le nom du processus et le nom de l'agent séparés par le caractère |.

Pour rechercher plusieurs propriétés, utilisez la propriété `all`, qui couvre les propriétés d'agent suivantes :

`agentId`, `agentName`, `agentProfile`, `appServerName`, `appServerVersion`, `build`, `emCollectorHost`, `emCollectorPort`, `installPath`, `logLevel`, `osArch`, `osName`, `osVersion`, `packageId`, `packageName`, `packageOriginId`, `packageVersion`, `platformArch`, `platformName`, `platformVersion`, `processName`, `serverName`, `spaName`, `status`, `type`, `version`.

Affichage des rapports d'agent

Tous les rapports générés pour les agents s'affichent sous forme de liste sur la page Rapports. Vous pouvez sélectionner un rapport pour en afficher les détails. Par défaut, les rapports sont disponibles pendant 40 jours.

Vous pouvez également sélectionner un rapport et cliquer sur Télécharger pour le télécharger au format ZIP. Un fichier ZIP contient le rapport complet au format HTML avec toutes les informations que vous pouvez afficher dans la description du rapport. Le fichier ZIP inclut également tous les fichiers journaux et de configuration. Le nom du fichier ZIP contient le nom du rapport et un horodatage pour faciliter l'identification.

Vous pouvez utiliser la barre de recherche en haut de la page pour rechercher un rapport. Vous pouvez effectuer une recherche par propriété de rapport. Vous pouvez également effectuer une recherche globale sur la page Accueil.

Recherche de rapports

Vous pouvez utiliser la barre de recherche en haut de la page pour rechercher un rapport. Vous pouvez effectuer une recherche par propriété de rapport. Vous pouvez également effectuer une recherche globale sur la page Accueil.

Pour rechercher des rapports à l'aide du langage de requête ACC, reportez-vous à la section [Recherche à l'aide du langage de requête ACC \(AQL, ACC Query Language\)](#).

Voici des exemples de recherches de rapports :

- Recherchez par nom de rapport. Utilisez des guillemets pour inclure les espaces.

```
reportName:"ACCDemoWin01|Tomcat|Tomcat Agent-3"
```

- Vous pouvez utiliser les opérateurs ET (par défaut), OU et NON.

```
logLevel:info OR logLevel:debug
```

- Recherchez les rapports des agents Tomcat, mais uniquement ceux dont le nom de serveur ne contient pas le mot linux.

```
processName:Tomcat NOT serverName:linux
```

- Recherchez par dernier contact (5 semaines à aujourd'hui) :

```
lastContact:[-5w TO NOW]
```

- Utilisez des parenthèses pour regrouper les opérateurs logiques.

```
(osName:windows OR osName:Linux) AND logLevel:info
```

Placez les recherches par expression régulière entre des barres obliques /.

TIP

Vous pouvez copier et coller des expressions de recherche d'agent à partir des mesures WebView.

```
/ACCServer.*01\|Tomcat\|.*Agent/
```

Enregistrement de la recherche

Dans la barre de recherche, utilisez l'option **Enregistrer en tant que nouvelle collection** pour enregistrer un modèle de recherche que vous utilisez fréquemment. Vous pouvez également utiliser la recherche enregistrée dans une requête.

Exemple : utilisation de la collecte dans une requête

```
collection:"Tomcat Agents" AND reportName:Linux
```

Propriétés de la recherche d'agent

La propriété par défaut pour la recherche d'agent est spaName. Elle contient le nom du serveur, le nom du processus et le nom de l'agent séparés par le caractère |.

Pour rechercher plusieurs propriétés, utilisez la propriété `all`, qui couvre les propriétés d'agent suivantes :

`agentId`, `agentName`, `agentProfile`, `appServerName`, `appServerVersion`, `build`, `emCollectorHost`, `emCollectorPort`, `installPath`, `logLevel`, `osArch`, `osName`, `osVersion`, `packageId`, `packageName`, `packageOriginId`, `packageVersion`, `platformArch`, `platformName`, `platformVersion`, `processName`, `serverName`, `spaName`, `status`, `type`, `version`.

Configuration des applications pour l'intégration

La page Applications affiche toutes les applications créées dans DX Application Performance Management. Utilisez ces applications pour les intégrer dans DX APM de manière transparente et pour configurer facilement les packages d'installation de l'agent pour votre environnement.

L'intégration d'applications repose sur les concepts suivants :

- **Application** : permet de surveiller l'application qui se compose d'un ou de plusieurs niveaux.
- **Niveau** : indique le niveau d'application à surveiller. Le concept de niveau fait référence à un ou plusieurs packages d'agent créés en fonction de l'utilisateur sélectionné.

Pour créer une application pour l'intégration, reportez-vous à la section [Création d'applications](#).

Recherche d'applications

Vous pouvez utiliser la barre de recherche en haut de la page pour rechercher une application en utilisant uniquement le champ de nom. Comme le champ de nom est l'option de recherche par défaut, il n'est pas nécessaire d'ajouter `name:` dans le champ de recherche.

Pour rechercher des applications à l'aide du langage de requête ACC, reportez-vous à la section [Recherche à l'aide du langage de requête ACC \(AQL, ACC Query Language\)](#).

Voici des exemples de recherches d'application :

- Pour rechercher une application avec le nom Website

```
name:website
```

Ou

```
website
```
- Vous pouvez utiliser les opérateurs ET (par défaut), OU et NON.

```
name:website AND NOT name:testing
```

Ou

```
website AND NOT name:testing
```

Gestion des packages d'agent

Un package est une image d'agent déployable accompagnée des instructions d'installation au format ZIP ou TAR. Le package est généré à partir de groupes qui représentent une fonctionnalité d'agent. Command Center fournit également des packages d'amorçage Java. Le package d'amorçage vous permet de basculer entre différentes versions d'agent sans effort. Pour transférer des définitions de package entre différents locataires, utilisez la fonctionnalité d'exportation/importation.

Dans l'onglet Package, une liste des packages disponibles s'affiche. Une icône en regard du nom du package indique qu'une mise à jour est disponible. Sélectionnez ce package et cliquez sur Mettre à jour pour le mettre à jour.

La page Packages vous permet d'effectuer les opérations suivantes :

- [Création d'un package d'agent](#)
- [Utilisation d'un groupe dans un package](#)
- [Déploiement des packages d'agent](#)
- [Intégration de produits tiers](#)
- [Gestion des packages et groupes d'agents à l'aide d'APM Command Center](#)

La page Package affiche les informations suivantes à propos d'un package.

Package

La fiche Package affiche des informations générales sur le package, telles que le nom, la description et le nombre total d'agents.

Le champ **Nombre total d'agents** indique le nombre d'agents qui utilisent ce package. Vous pouvez accéder à l'onglet **Agents** et consulter les agents qui utilisent ce package.

Version du package

La fiche **Versions** affiche le nombre d'agents qui utilisent chaque version de package. Vous pouvez consulter la date de la dernière modification du package, son nom, la version du package et de l'agent, et si le package est archivé. Cette vue générale vous permet de vous assurer que tous les agents utilisent la dernière version.

NOTE

Vous ne pouvez pas télécharger un package archivé. Vous ne pouvez pas non plus apporter des modifications à la configuration du package archivé. Lorsque vous créez une nouvelle version de package, elle est basée sur la version actuelle (non archivée).

Versions

La fiche de version affiche les informations relatives à chaque mise à jour de package et à l'utilisateur qui l'a mis à jour.

Lorsqu'un package est créé, son numéro de version initial est 1. Après les modifications ultérieures, la version de l'agent reste 1 jusqu'à ce qu'un utilisateur télécharge le package ou l'applique à l'agent. La modification suivante modifie le numéro de version sur 2.

Groupes

La fiche Groupes affiche tous les groupes inclus dans le package sélectionné.

Si un groupe personnalisé est mis à jour vers une version plus récente, un bouton de mise à jour s'affiche dans la colonne Version du panneau Groupes personnalisés. Si une mise à jour d'un groupe personnalisé échoue et que le message d'erreur vous informe que le groupe n'a pas de version plus récente, vous pouvez le mettre à jour manuellement. Cliquez sur **Modifier**, accédez à la vue **Sélectionner des groupes** et remplacez la version du groupe par une version plus récente, le cas échéant.

Recherche de packages

Vous pouvez utiliser la barre de recherche en haut de la page pour rechercher un package. Vous pouvez effectuer une recherche par propriété de package. Vous pouvez également effectuer une recherche globale sur la page Accueil.

Pour rechercher des packages à l'aide du langage de requête ACC, reportez-vous à la section [Recherche à l'aide du langage de requête ACC \(AQL, ACC Query Language\)](#).

Voici des exemples de recherches de package :

- Recherchez par nom de package. Utilisez des guillemets pour inclure les espaces.

```
packageName:tomcatLinux
```

- Vous pouvez utiliser les opérateurs ET (par défaut), OU et NON.

```
logLevel:info OR logLevel:debug
```

- Recherchez les rapports des agents Tomcat, mais uniquement ceux dont le nom de serveur ne contient pas le mot linux.

```
processName:Tomcat NOT serverName:linux
```

- Recherchez par dernier contact (5 semaines à aujourd'hui) :

```
lastContact:[-5w TO NOW]
```

- Utilisez des parenthèses pour regrouper les opérateurs logiques.

```
(osName:windows OR osName:Linux) AND logLevel:info
```

Placez les recherches par expression régulière entre des barres obliques /.

TIP

Vous pouvez copier et coller des expressions de recherche d'agent à partir des mesures WebView.

```
/ACCServer.*01\|Tomcat\|.*Agent/
```

Enregistrement de la recherche

Dans la barre de recherche, utilisez l'option **Enregistrer en tant que nouvelle collection** pour enregistrer un modèle de recherche que vous utilisez fréquemment. Vous pouvez également utiliser la recherche enregistrée dans une requête.

Exemple : utilisation de la collecte dans une requête

```
collection:"Tomcat Agents" AND reportName:Linux
```

Propriétés de la recherche de package

La propriété par défaut pour la recherche de rapport est packageName. Pour rechercher plusieurs propriétés, utilisez la propriété all, qui couvre les propriétés de rapport suivantes :

bundles, comment, emHost, facets, packageName.

Configuration des groupes

Un groupe est un bloc de construction à partir duquel des agents sont créés. Le groupe représente un ensemble compact de fonctionnalités d'agent, par exemple, les services Web SOAP, le servlet ou JSP.

Les groupes peuvent être déployés à chaud ou nécessiter un redémarrage du processus surveillé. Les groupes dynamiques peuvent être déployés à chaud. Vous pouvez déployer le package sur un agent en cours d'exécution sans devoir le redémarrer. Pour déployer le package, ajoutez, supprimez ou mettez à jour un groupe dynamique dans un package d'installation de l'agent. Les groupes dynamiques sont indiqués par une icône Groupe dynamique. Les groupes qui peuvent être appliqués à un agent en cours d'exécution, mais qui nécessitent un redémarrage du processus surveillé sont identifiés par l'icône Redémarrage requis.

Pour afficher la liste des groupes disponibles dans APM Command Center par défaut, reportez-vous à la section [Liste des groupes](#).

Vous pouvez également créer un groupe personnalisé. Pour plus d'informations, consultez la section [Ajout de groupes personnalisés](#). Vous ne pouvez pas modifier les groupes sur la page Groupes. Utilisez la page Packages pour modifier les propriétés de groupe.

Recherche de groupes

Vous pouvez utiliser la barre de recherche en haut de la page pour rechercher un groupe. Vous pouvez effectuer une recherche par propriété de groupe. Vous pouvez également effectuer une recherche globale sur la page Accueil.

Pour rechercher des groupes à l'aide du langage de requête ACC, reportez-vous à la section [Recherche à l'aide du langage de requête ACC \(AQL, ACC Query Language\)](#).

Voici des exemples de recherches de groupe :

- Recherchez par nom de groupe. Utilisez des guillemets pour inclure les espaces.

```
bundleName:"ACCDemoWin01|Tomcat|Tomcat Agent-3"
```

- Vous pouvez utiliser les opérateurs ET (par défaut), OU et NON.

```
logLevel:info OR logLevel:debug
```

- Recherchez les groupes d'agents Tomcat, mais uniquement ceux dont le nom de serveur ne contient pas le mot linux.

```
processName:Tomcat NOT serverName:linux
```

- Recherchez par dernier contact (5 semaines à aujourd'hui) :

```
lastContact:[-5w TO NOW]
```

- Utilisez des parenthèses pour regrouper les opérateurs logiques.

```
(osName:windows OR osName:Linux) AND logLevel:info
```

Placez les recherches par expression régulière entre des barres obliques /.

TIP

Vous pouvez copier et coller des expressions de recherche d'agent à partir des mesures WebView.

```
/ACCServer.*01\|Tomcat\|.Agent/
```

Enregistrement de la recherche

Dans la barre de recherche, utilisez l'option **Enregistrer en tant que nouvelle collection** pour enregistrer un modèle de recherche que vous utilisez fréquemment. Vous pouvez également utiliser la recherche enregistrée dans une requête.

Exemple : utilisation de la collecte dans une requête

```
collection:"Tomcat Agents" AND reportName:Linux
```

Propriétés de la recherche de groupe

La propriété par défaut pour la recherche de groupe est name. Pour rechercher plusieurs propriétés, utilisez la propriété all, qui couvre les propriétés de groupe suivantes :

category, dependencies, description, enhances, facets, name, osName, version.

Recherche à l'aide du langage de requête ACC (AQL, ACC Query Language)

Spécifiez une requête personnalisée dans la barre de recherche en haut de la page d'ACC, qui filtre les éléments affichés dans une vue. La requête personnalisée utilise le langage de requête ACC (AQL), qui remplace le langage Lucene utilisé auparavant. Pour en savoir plus sur les différences entre Lucene et AQL, consultez la section [Propriétés pouvant faire l'objet d'une recherche](#).

Création de requêtes simples

Entrez un mot dans la barre de recherche pour filtrer tous les résultats correspondants en fonction de la requête de mot. La recherche est effectuée sur une propriété par défaut, généralement un nom. Pour rechercher une propriété spécifique, saisissez la requête au format suivant :

```
propertyName:search_query_word
```

Notez que `propertyName` est sensible à la casse. A mesure que vous entrez une valeur, la barre de recherche affiche les propriétés disponibles. Utilisez la propriété `all` pour effectuer une recherche sur plusieurs propriétés.

Exemple : recherche simple

```
osName:windows
```

Créer des requêtes de combinaison

Entrez plusieurs requêtes dans la barre de recherche séparées par des espaces ou entrez plusieurs sous-requêtes à l'aide des opérateurs suivants : ET, OU et NON.

Les opérateurs doivent respecter la casse et vous pouvez utiliser des parenthèses pour les grouper. AND est l'opérateur par défaut pour les requêtes séparées par des espaces.

Exemple : requête combinée avec l'opérateur ET

Les exemples de requête ci-dessous filtrent les résultats dont tous les mots sont trouvés.

```
word1 AND word2 AND word3
word1 AND word2 word3
word1 word2 word3
```

Exemple : requête combinée avec l'opérateur OU

Cet exemple montre comment filtrer les résultats en cas de détection de l'un des mots.

```
word1 OR word2 OR word3
```

Exemple : requête combinée avec l'opérateur NON

Cet exemple filtre les résultats qui ne contiennent pas le mot `myquery`.

```
NOT myquery
```

Vous pouvez utiliser d'autres symboles plutôt que des opérateurs nommés :

Operator	Autres symboles
ET	&&
Ou	
NON	!

Exemple : requête combinée avec des parenthèses

Cet exemple groupe les opérateurs et filtre les résultats.

```
(word1 AND word2) OR word3
word1 AND (word2 OR word3)
```

Autres requêtes de recherche

Vous pouvez utiliser des chaînes, des caractères génériques, des nombres, des expressions régulières et des requêtes de plage comme modèles de recherche pour filtrer les résultats.

Utilisation de chaînes et de caractères génériques

Entrez une chaîne de mots ou de caractères entre guillemets (" ") pour filtrer les résultats de la recherche. Les résultats correspondent exactement à la chaîne de recherche. Vous pouvez utiliser les types de caractères génériques suivants : * pour faire correspondre une sous-chaîne et ? pour faire correspondre un caractère. L'utilisation d'un caractère spécial dans une chaîne est traitée comme un caractère ordinaire.

Exemple : requête de chaîne

La requête ci-dessous filtre tous les résultats qui correspondent exactement à la chaîne.

```
"abc xyz"
```

Exemple : requête de caractère générique

La requête ci-dessous filtre tous les résultats qui contiennent la chaîne de recherche.

```
*"abc xyz"*
```

Exemple : requête combinée de chaîne et de caractère générique

La requête ci-dessous affiche un modèle de recherche utilisant des caractères génériques, une chaîne et un mot unique.

```
word*"quoted string"?
```

Requête de plage

Une requête de plage peut être une plage de nombres, de versions ou de dates.

Exemple : requête de plage

La requête ci-dessous filtre les résultats dans la plage 0 à 5 sur la propriété numérique prop.

```
prop:[0 TO 5]
```

La requête ci-dessous affiche un modèle de recherche avec une plage exclusive et une étoile indiquant qu'aucune limite maximum n'est définie pour la propriété numérique prop.

```
prop prop:{10 TO *}]
```


Utilisation

DX APM vous permet d'utiliser différentes méthodes pour surveiller le statut de vos applications métier et examiner et résoudre les problèmes.

Pour...	Procédez comme suit...	Reportez-vous aux ressources suivantes...
Présentation de la géographie de votre environnement d'application	La vue Expérience permet d'afficher votre environnement d'application à partir de l'univers le plus élevé. Analysez certaines transactions en profondeur à la recherche d'anomalies.	Surveillance des performances à l'aide de la vue Expérience
Affichage d'une vue d'ensemble des valeurs de mesures d'agent	Sélectionnez Vue des mesures et accédez à l' arborescence des mesures d'un hôte de serveur d'applications. Analysez l'arborescence en profondeur et cliquez sur le noeud d'agent que vous souhaitez examiner.	Surveillance des valeurs de mesures d'agent à l'aide de la vue des mesures
Affichage de l'intégrité globale de l'environnement	Accédez au tableau de bord et appliquez la vue Agent ou Expérience. Une vignette Tableau de bord correspond à un groupe rassemblant tous les composants qui partagent un nom et une valeur d'attribut. Les vignettes affichent les statuts d'alerte les plus pertinents de tous les composants du groupe.	Surveillance de l'intégrité globale de l'environnement à l'aide du tableau de bord
Surveillance des problèmes et des anomalies	Utilisez le panneau Assisted Triage (Tri assisté) pour surveiller les problèmes et anomalies. Le panneau Assisted Triage (Tri assisté) identifie les expériences affectées et nomme les preuves indiquées comme problème. Les anomalies sont semblables aux problèmes, mais elles n'affectent pas encore l'expérience utilisateur. Le tri assisté analyse les données d'agent à partir de vos environnements surveillés et identifie les composants communs d'un problème afin de ne pas recevoir un trop grand nombre de problèmes.	Tri assisté et analystes
Examen des problèmes	Utilisez le carnet d'analyse et examinez les problèmes identifiés par le tri assisté.	Recherche de solutions aux problèmes à l'aide du carnet d'analyse
Examen des performances médiocres des transactions	Utilisez la visionneuse des traces de transaction pour connaître les performances des transactions et résoudre les problèmes de performances en identifiant quand, où et pourquoi les performances se détériorent.	Examen des performances médiocres des transactions

Surveillance de l'intégrité et des performances des agents	Utilisez la vue Agents pour surveiller les agents disponibles dans votre environnement. Des fiches d'agent dans la vue présentent les détails d'un agent ou d'un groupe d'agents. Si des agents sont regroupés dans une fiche, les informations sur les mesures sont également groupées.	Affichage du statut d'agent et gestion des fiches d'agent
--	---	---

Intégration d'applications pour la surveillance

Utiliser l'intégration d'applications pour intégrer les applications dans DX APM de manière transparente et pour configurer facilement les packages d'agent pour votre environnement. L'assistant Intégration d'applications vous guide dans la sélection des options de surveillance et crée des packages d'agent. L'intégration d'applications repose sur les concepts suivants :

- **Application** : permet de surveiller l'application qui se compose d'un ou de plusieurs niveaux.
- **Niveau** : indique le niveau d'application à surveiller. Le concept de niveau fait référence à un ou plusieurs packages d'agent créés en fonction de l'utilisateur sélectionné.

Dans la configuration de niveau, chaque étape contient une ou plusieurs options qui mappent vers des fonctionnalités de surveillance concrètes (par exemple, la surveillance des bases de données APMIA et Oracle ou le système d'exploitation Linux). Pour intégrer des applications, configurez ce qui suit :

1. **Détails de l'application** : définissez le nom et la description de l'application à surveiller.
2. **Configuration de niveau** : définissez les options de surveillance du niveau.
3. **Etape de téléchargement** : définissez les artefacts (packages d'agent) à télécharger qui ont été créés à partir des options de surveillance.

Création d'applications

Créez des applications en sélectionnant les options de surveillance et des agents de création pour l'intégration des applications dans DX APM. Vous pouvez ajouter plusieurs niveaux à l'application. Vous pouvez également modifier, cloner ou supprimer l'application.

1. Dans l'interface utilisateur de DX APM, sélectionnez **Settings** (Paramètres).
2. Cliquez sur la mosaïque **Applications**.
3. Si vous utilisez la mosaïque **Applications** pour la première fois, cliquez sur **Get Started** (Prise en main) pour créer

une application. Dans le cas contraire, créez une application en cliquant sur



4. Entrez les détails suivants pour votre application :
 - a) **Application name** (Nom de l'application) : attribuez un nom à l'application. Vous pouvez le modifier à tout moment.
 - b) **Description** : entrez une description de votre application.
5. Cliquez sur **Add Application Tiers** (Ajouter des niveaux d'application).
6. Créez un niveau pour votre application avec les détails ci-dessous.
 - a) **Tier Name** (Nom du niveau) : ajoutez un nom de niveau et une description pour votre niveau d'application.
 - b) **Operating System** (Système d'exploitation) : sélectionnez le système d'exploitation sur lequel votre application s'exécute. Les options suivantes changent en fonction du système d'exploitation sélectionné.
 - c) **Technology Stack** (Pile technologique (facultative)) : sélectionnez la pile technologique sur laquelle votre application s'exécute. Vous pouvez sélectionner plusieurs piles technologiques.
 - d) **Container Type (Optional)** (Type de conteneur (facultatif)) : sélectionnez le type de conteneur pour votre application. Le type de conteneur change en fonction du système d'exploitation.
 - e) **Database** (Base de données (facultative)) : vous pouvez sélectionner une ou plusieurs bases de données sur lesquelles votre application s'exécute. Vous pouvez ajouter plusieurs profils pour les bases de données qui prennent en charge plusieurs connexions et fournissent des paramètres de connexion distincts. Sélectionnez/désélectionnez la case à cocher **Clichés** pour activer/désactiver les clichés de trace de base de données.
 - f) **Webserver** (Serveur Web) : sélectionnez un ou plusieurs serveurs Web sur lesquels votre application s'exécute. Vous pouvez ajouter plusieurs profils pour un serveur Web sélectionné et configurer leurs paramètres séparément.
 - g) **Messaging System** (Système de messagerie) : sélectionnez un système de messagerie que l'application utilise pour la communication. En fonction de votre sélection, fournissez les détails du système de messagerie. Vous pouvez ajouter plusieurs profils pour les systèmes de messagerie qui prennent en charge plusieurs connexions et configurent leurs paramètres séparément.
 - h) **Monitoring** (Surveillance) : sélectionnez les options de surveillance des performances de vos applications. En fonction de votre sélection, fournissez les détails du système de surveillance. Vous pouvez ajouter plusieurs profils pour les systèmes de surveillance qui prennent en charge plusieurs connexions de surveillance et configurent leurs paramètres séparément.
 - i) **Supplémentaire** : des options supplémentaires s'affichent basées sur le système d'exploitation sélectionné. Sélectionnez les fonctionnalités requises et fournissez des détails supplémentaires en fonction de votre sélection. Vous pouvez ajouter plusieurs options pour les fonctionnalités qui prennent en charge plusieurs connexions et configurent leurs détails séparément.
 - j) **Options** : mettez à jour les options en fonction du système d'exploitation sélectionné.
 - k) **Tier Summary** (Récapitulatif des niveaux) : examinez vos configurations de niveau et cliquez sur **Add Tier Now** (Ajouter un niveau maintenant).

Le niveau est créé. Vous pouvez le modifier, le cloner ou le supprimer. Vous pouvez créer et ajouter plusieurs niveaux à l'application.

7. Cliquez sur **Create Application** (Créer une application).
8. Cliquez sur **Done** (Terminé).

L'application est créée avec les niveaux requis. Vous pouvez télécharger une application ou copier le lien de téléchargement. Vous pouvez également télécharger ou consulter les instructions d'installation.

Téléchargement d'applications

A l'aide de la liste déroulante **Télécharger** correspondant à une application, vous pouvez télécharger une application ou copier le lien de téléchargement. Vous pouvez également télécharger ou consulter les instructions d'installation. Le package téléchargé contient ce qui suit :

- Un dossier pour chaque niveau. Chaque dossier contient les packages d'agent configurés pour chaque niveau.
- **Completed.txt** : le package n'est pas téléchargé correctement si ce fichier ne figure pas dans le dossier téléchargé.
- **Info.txt** : ce fichier contient un récapitulatif de tous les packages figurant à l'intérieur des dossiers de niveau.

Surveillance des performances à l'aide de la vue Expérience

DX APM vous permet de comprendre la géographie de votre environnement d'application, qui est vital pour une surveillance et une résolution des problèmes efficaces. CA Application Performance Management fournit un aperçu d'un environnement applicatif. La vue Expérience affiche vos applications surveillées depuis le point de vue de l'expérience.

Les rôles suivants utilisent la vue Expérience :

- Les administrateurs voient l'état de l'environnement.
- Les analystes de niveau un surveillent les problèmes et les avertissements dans l'environnement à l'aide de la vue Expérience.
- Les analystes expérimentés examinent et résolvent les problèmes à l'aide du carnet d'analyse, de la carte et du tableau de bord.

Comprendre le composant frontal en tant qu'expérience

L'expérience est le composant le plus en amont de la transaction, c'est-à-dire le premier composant surveillé de l'ensemble de la transaction. Le noeud d'expérience est le premier composant frontal surveillé et il contient un attribut Expérience. Le noeud d'expérience est le début du chemin de transaction. Une expérience peut être, par exemple, un servlet ou un serveur frontal générique.

Vue Expérience

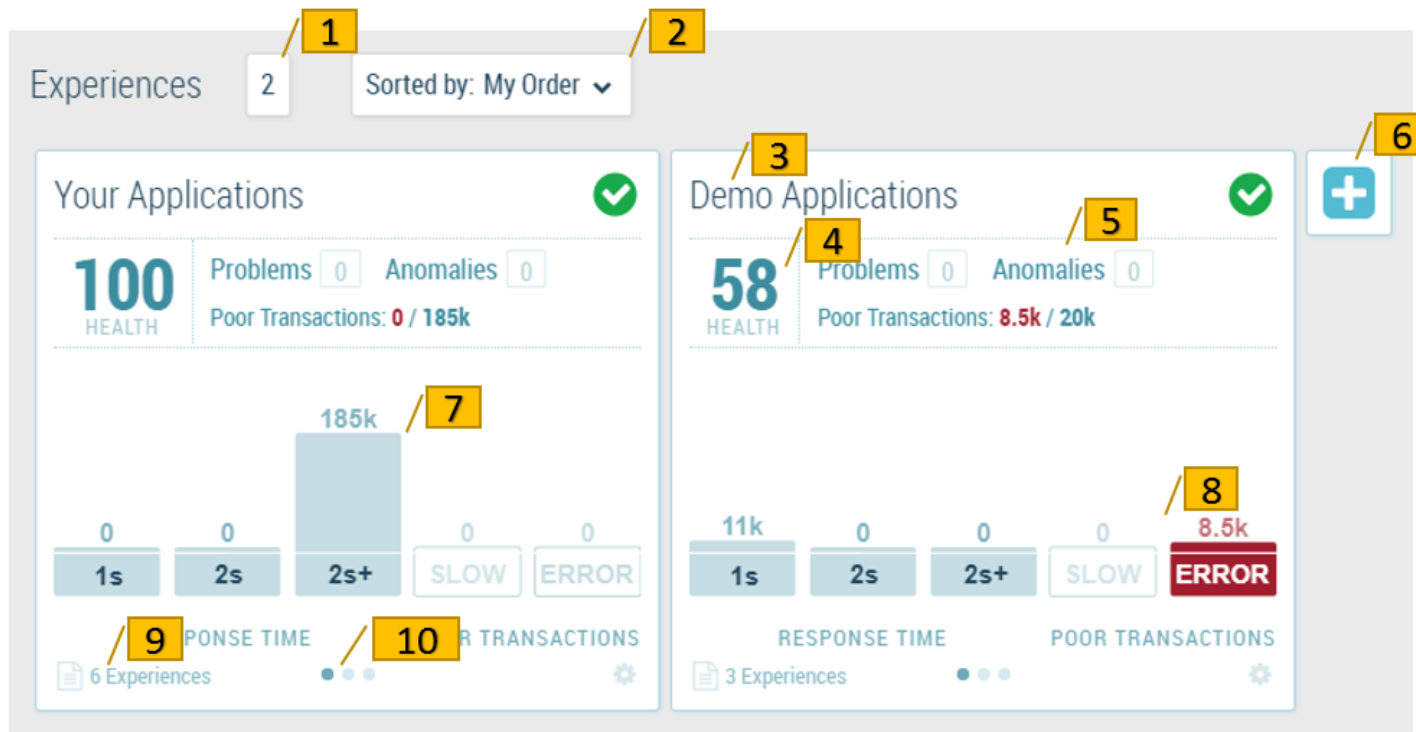
La vue Expérience vous permet de :

- Exclure les parties de l'environnement ne posant aucun problème pour se concentrer sur les problèmes existants.
- Accéder aux niveaux inférieurs de la vue Expérience pour afficher des sections de l'environnement de manière plus détaillée. Les fiches d'expérience affichent le statut de tous les composants desquels vous êtes responsable. Les informations de fiche présentent les expériences en situation de charge. Le tri assisté identifie les zones potentiellement problématiques et affiche le nombre de problèmes et les anomalies.

Types de transaction dans la vue Expérience :

- Transactions saines : valeurs de mesure *Réponses par intervalle* lorsque le noeud d'expérience n'a aucune alerte Attention ou Danger.
- Transactions bloquées : valeurs de mesure *Blocages* du noeud d'expérience.
- Transactions avec erreurs : valeurs de mesure *Erreurs par intervalle* du noeud d'expérience.
- Transactions lentes : valeurs de mesure *Réponses par intervalle* lorsque le noeud d'expérience a une alerte Attention ou Danger pour la mesure Temps de réponse moyen ou une mesure d'analyse différentielle.
- Transactions avec alerte : valeurs de mesure *Réponses par intervalle* lorsque le noeud d'expérience n'a aucune alerte Attention ou Danger pour une mesure autre que la mesure identifiant les transactions lentes.

Le graphique suivant et la légende correspondante permettent de comprendre les différentes fonctionnalités disponibles dans la vue Expérience.



La légende suivante identifie chaque élément de la carte par un numéro et fournit des informations complémentaires :

Numéro	Name (nom)	Informations complémentaires
1	Nombre d'expériences	
2	Trier par	Trie les fiches par nom ou à l'aide du filtre Mon ordre.
3	Fiche d'expérience	Les fiches d'expérience affichent un résumé et identifient le problème et son origine. Les fiches sont définies selon un univers. Le nombre maximum est 1 univers par fiche.

4	INTEGRITE	La zone Indice d'intégrité affiche l'indice d'intégrité global de l'environnement. Le nombre indique le pourcentage de transactions saines par rapport au nombre total de transactions. L'indice indique le volume des transactions saines et médiocres. Le volume des transactions médiocres est la somme de toutes les transactions non saines (lentes, avec erreur, avec alerte, bloquées).
5	Problèmes et anomalies	Indique le nombre de problèmes et d'anomalies. Un problème indique une situation où un ou plusieurs composants dans les transactions associées déclenchent des alertes. Des événements tels que des blocages, des erreurs ou d'autres problèmes affectent les transactions. Une anomalie indique une situation où un ou plusieurs composants dans les transactions associées déclenchent des alertes. Des événements tels que des blocages et des erreurs ont été détectés, mais n'affectent pas les performances des transactions.
6	Ajouter une fiche d'expérience	Cliquez sur le bouton + pour nommer et de configurer une nouvelle fiche d'expérience. Remarque : pour plus d'informations sur l'ajout d'une carte, consultez la section Affichage du statut d'agent et gestion des fiches d'agent
7	Temps de réponse	L'histogramme Temps de réponse affiche le temps de réponse moyen par seconde pour les transactions saines et terminées en : <ul style="list-style-type: none"> • 1s moins de 1 seconde • 2s entre 1 à 2 secondes • 2s+ plus de 2 secondes
8	Transactions médiocres	L'histogramme Transactions médiocres affiche le nombre de transactions médiocres qui se sont produites pendant la période. <ul style="list-style-type: none"> • LENT affiche le nombre de transactions bloquées et lentes. Ces transactions présentent des alertes pour l'analyse différentielle ou pour le temps de réponse moyen. • ERREUR affiche le nombre d'erreurs par intervalle pour l'application.

9	Ouvrir le bloc-notes d'analyse	Le carnet d'analyse affiche les transactions métier pour une fiche d'expérience spécifique. Le nombre de transactions métier s'affiche en regard de l'icône du carnet d'analyse. Remarque : Par défaut, vous ne pouvez pas ouvrir le carnet d'analyse si la fiche d'expérience contient plus de 20 transactions métier.
10	Switch graphs (Changer de graphique)	Les graphiques correspondent au temps de réponse agrégé, au temps de réponse moyen et au volume de transactions.

Surveillance des performances à l'aide de la vue Expérience

La vue Expérience permet de surveiller les performances de votre environnement à partir de l'univers le plus élevé. Vous pouvez accéder aux informations détaillées de transactions spécifiques pour rechercher des anomalies.

Procédez comme suit :

1. Cliquez sur une **fiche d'expérience**.
Les données agrégées pour les groupes de transactions métier associées disponibles dans votre univers s'affichent. Vous pouvez ajouter des fiches, les configurer et les réorganiser.
2. Cliquez sur le **graphique** pour parcourir les graphiques de mesures.
3. Affichez l'**indice d'intégrité**.
La zone Indice d'intégrité affiche l'indice d'intégrité global de l'environnement. Le nombre indique le pourcentage de transactions saines par rapport au nombre total de transactions. Par exemple, l'indice d'intégrité de l'environnement que vous surveillez est 85. Cet indice signifie que 85 % des transactions que vous surveillez sont saines. Les 15 % restants sont médiocres. Les transactions médiocres correspondent à la somme des transactions lentes et ayant échoué.
4. Développez une **fiche**. Des détails complémentaires s'affichent dans le panneau Assisted Triage (Tri assisté). Le panneau Assisted Triage est une liste déroulante située sur la droite qui affiche où se produisent des problèmes et des anomalies. Le moteur de tri assisté identifie les composants communs d'un problème afin de ne pas recevoir un trop grand nombre de problèmes. Le panneau Assisted Triage s'affiche dans la vue Expérience, à l'exception de la page de niveau supérieur.
5. Développez la **story**. Des détails complémentaires s'affichent. Le panneau affiche également les noeuds suspects, mis en surbrillance par le moteur de tri assisté en tant que possibles responsables de la situation.
6. Développez le menu **Problems and Anomalies** (Problèmes et anomalies).
Des détails complémentaires s'affichent.
7. Cliquez sur le **titre** du graphique et explorez le niveau suivant de groupement.
8. Cliquez sur l'icône de **bloc-notes**.
Le carnet d'analyse du groupe de composants s'ouvre.

NOTE

Par défaut, vous ne pouvez pas ouvrir le carnet d'analyse si la Fiche d'expérience contient plus de 20 transactions métier.

Création d'un tri à l'aide de la vue Expérience

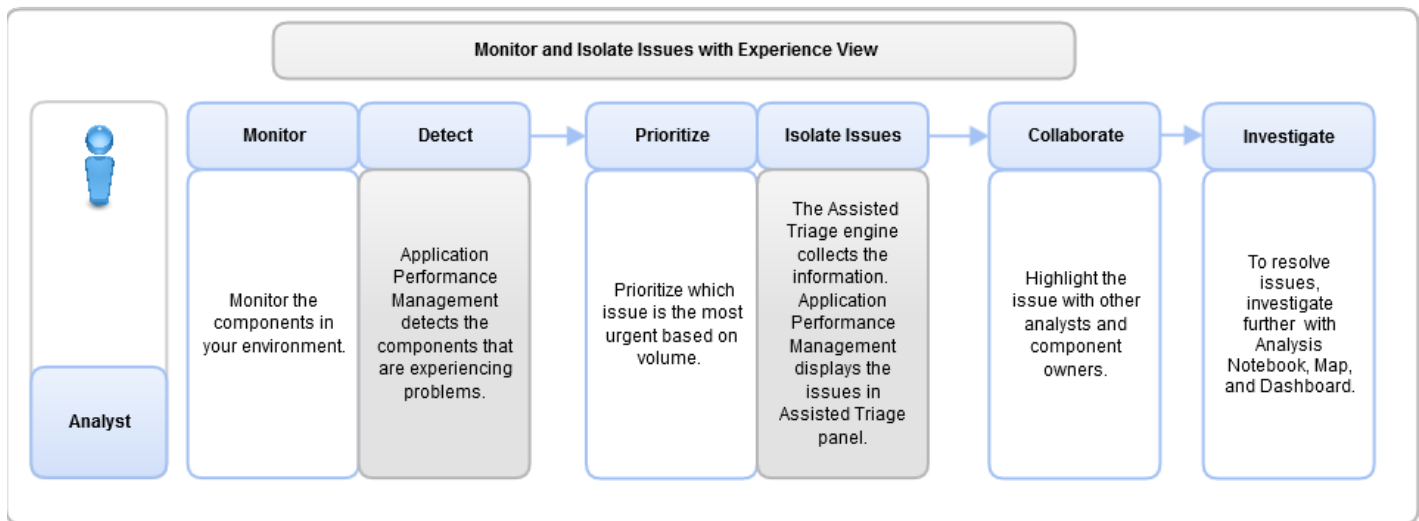
Découvrez comment le panneau Assisted Triage (Tri assisté) signale les problèmes et les anomalies relatifs aux événements dans votre système.

NOTE**Informations complémentaires :****Surveillance des problèmes et anomalies relatifs au Assisted Triage (Tri assisté)****Exemple : surveillance et isolement des problèmes à l'aide de la vue Expérience**

La vue Expérience permet d'afficher le statut de tous les composants de la zone de l'environnement dont vous êtes responsable. Vous pouvez voir les expériences en cours de chargement et accéder aux niveaux inférieurs pour identifier les composants critiques. La fonctionnalité Assisted Triage (Tri assisté) vous aide à identifier les zones posant potentiellement un problème.

Cet exemple présente un flux de travaux d'analyste. En tant qu'analyste, vous êtes informé d'un problème dans l'environnement. Identifiez la cause première des problèmes et les ressources directes pour les résoudre. L'objectif du diagnostic des problèmes est d'identifier l'origine. L'origine est le composant de l'application qui rencontre le premier des problèmes et affecte les autres composants et l'expérience client.

Le diagramme suivant présente le flux de travaux de surveillance d'un environnement et d'isolement des problèmes :

Figure 5: Flux_de_travail_Page_d'accueil

1. Surveillez les composants dans votre environnement.
2. Cliquez sur une **fiche d'expérience** pour afficher plus d'informations dans les niveaux inférieurs de la vue Expérience. Application Performance Management détecte les composants qui rencontrent des problèmes et les transactions lentes ou ayant échoué. La somme des transactions lentes et ayant échoué s'affiche en tant que nombre total d'expériences client médiocres. Les expériences sont classées en fonction du volume de transactions et du volume d'expériences client médiocres.
3. Définit le problème le plus urgent en fonction du volume. Examinez les expériences confrontées aux problèmes d'intégrité les plus graves. Mettez en corrélation l'expérience et les problèmes identifiés dans le panneau Assisted Triage. Hiérarchisez les problèmes à résoudre selon la valeur métier.
Le moteur de tri assisté collecte les informations et affiche les problèmes dans le panneau Assisted Triage (Tri assisté). Le moteur de triage assisté identifie les transactions qui partagent des composants fonctionnant mal. Les composants associés en cours de chargement sont identifiés ensemble en tant que problème dans le panneau Assisted Triage.

4. Consultez des analystes plus expérimentés ou un responsable pour obtenir de l'aide. Utilisez les informations du panneau pour identifier les propriétaires des composants présentant des problèmes. Partagez l'URL avec la personne concernée afin qu'elle puisse afficher la même vue.
5. Recherchez une solution au problème dans le carnet d'analyse, la carte et le tableau de bord.

DX Application Performance Management offre une vue d'ensemble et vous permet de comprendre la géographie de votre environnement d'application, ce qui est vital pour une surveillance et une résolution efficaces des problèmes. La vue Expérience affiche vos applications surveillées depuis le point de vue de l'expérience.

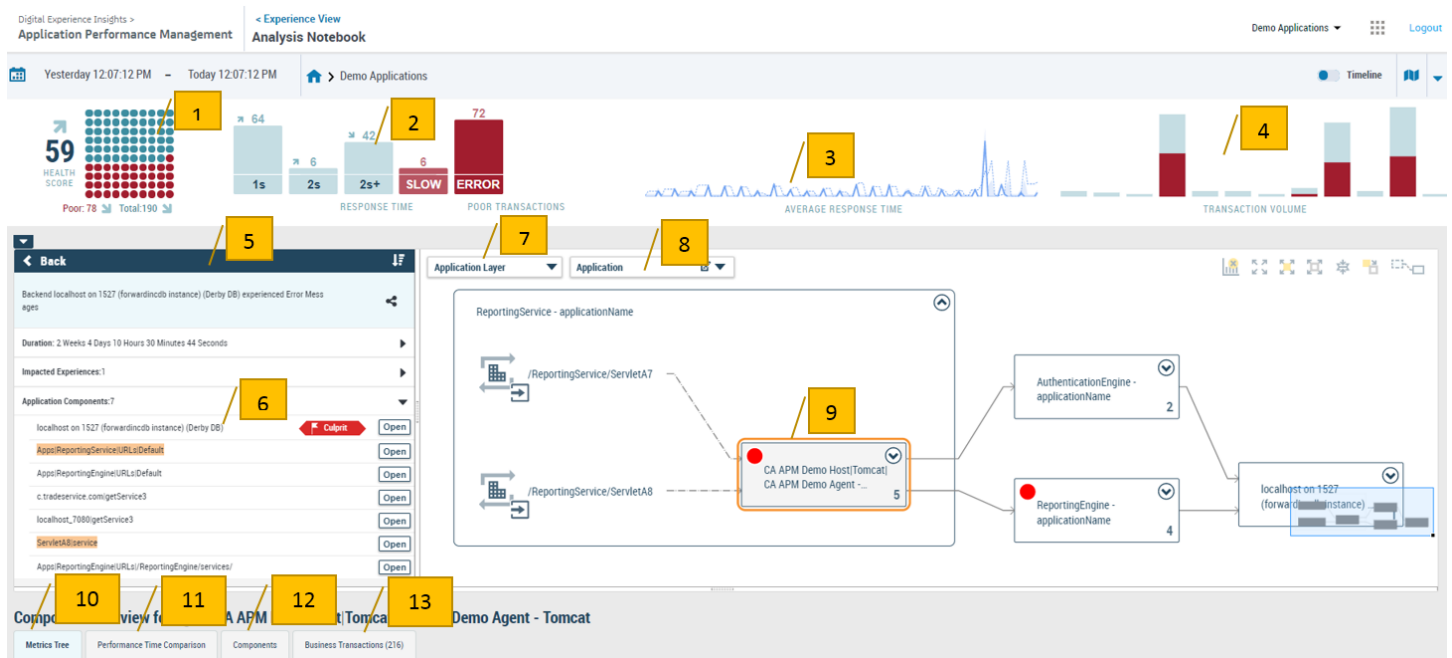
Pour surveiller les performances des applications à l'aide de la vue Expérience, reportez-vous à la section [Surveillance des performances à l'aide de la vue Expérience](#).

Recherche de solutions aux problèmes à l'aide du carnet d'analyse

DX APM permet aux analystes d'effectuer des tâches spécifiques pour leur rôle. Utilisez le carnet d'analyse pour examiner les problèmes.

Carnet d'analyse

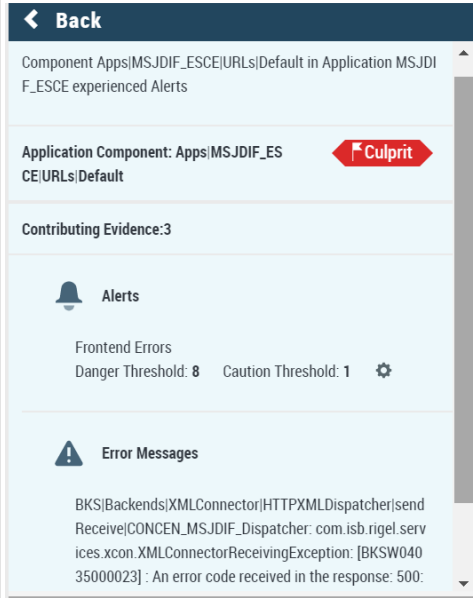
Le graphique suivant et la légende correspondante décrivent les différentes fonctionnalités disponibles dans la vue Carnet d'analyse.



La légende suivante identifie chaque élément par un numéro et fournit des informations complémentaires :

Numéro	Name (nom)	Informations complémentaires
1	INDICE D'INTEGRITE	<p>La zone Indice d'intégrité affiche l'indice d'intégrité global de l'environnement. Le nombre indique le pourcentage de transactions saines par rapport au nombre total de transactions. L'indice indique le volume des transactions saines et médiocres. Le volume des transactions médiocres est la somme de toutes les transactions non saines (lentes, avec erreur, avec alerte, bloquées).</p>
2	Histogramme des temps de réponse agrégés	<p>L'histogramme affiche le temps de réponse moyen par seconde pour les transactions saines et médiocres.</p> <ul style="list-style-type: none"> • 1s Nombre de transactions saines terminées en moins de 1 seconde. • 2s Nombre de transactions saines terminées entre 1 et 2 secondes. • 2s+ Nombre de transactions saines terminées en plus de 2 secondes. • Lent Nombre de transactions bloquées et lentes. Transactions ayant dépassé le seuil d'alerte Temps de réponse moyen. • Erreur Erreurs par valeur de mesure d'intervalle pour le noeud d'expérience <p>Le rouge indique le nombre de transactions qui sont terminées avec une alerte.</p>
3	Données de série chronologique - graphique Temps de réponse moyen	<p>Les données de série chronologique offrent un aperçu des mesures ou une période particulière qui pose problème. Vous n'êtes pas limité à la seule guidance des événements. Placez le curseur sur un pic de mesure dans le comportement des mesures dans le graphique pour le sélectionner, puis effectuez un zoom sur une période qui pose problème. Les mesures de réponses par intervalle et d'erreurs par intervalle sont collectées toutes les 15 secondes.</p> <p>Graphique Temps de réponse moyen</p> <ul style="list-style-type: none"> • La ligne bleue indique le temps de réponse moyen réel. • La ligne en pointillés indique une prévision du temps de réponse moyen. • Les zones ombrées indiquent un écart. Si la valeur de prévision se situe en dehors de la plage de déviation, un événement inhabituel se produit.

4	Données de série chronologique - histogramme Volume de transactions	<p>Les données de série chronologique offrent un aperçu des mesures ou une période particulière qui pose problème. Vous n'êtes pas limité à la seule guidance des événements. Passez la souris sur un pic de mesure dans le graphique pour le sélectionner, puis effectuez un zoom sur une période qui pose problème. Les mesures de réponses par intervalle et d'erreurs par intervalle sont collectées toutes les 15 secondes.</p> <p>Histogramme Volume de transactions</p> <ul style="list-style-type: none">• Divise la période en 12 sections et compare le volume de transactions dans la période sélectionnée.
5	Panneau de tri assisté	<p>Le panneau Assisted Triage (Tri assisté) répertorie les problèmes et les anomalies pour le composant sélectionné.</p>

6	Statut/responsabilité du composant	<p>Cercle rouge : Le composant joue un rôle dans au moins un problème ou une anomalie répertorié(e) dans le panneau Assisted Triage (Tri assisté). Tous les composants d'une story sont traités comme des acteurs.</p> <p>Cercle concentrique rouge : Le composant est responsable d'au moins un problème ou une anomalie répertorié(e) dans le panneau Assisted Triage (Tri assisté). Tous les acteurs sont impliqués, mais un responsable est considéré comme un acteur spécial. Le responsable correspond à la cause première du problème ou de l'anomalie au niveau de l'application ou de la transaction en question. Ce composant peut être à l'origine de la détérioration des performances dans votre environnement d'application.</p> <p>Ouvrir : Cliquez sur Ouvrir pour afficher les détails de la preuve pour l'anomalie. De plus, pour les alertes, vous pouvez afficher les valeurs de seuil et également modifier les paramètres d'alerte. Cliquez sur l'icône des paramètres d'une alerte pour accéder aux paramètres des alertes et les personnaliser.</p> 
7	Couche	Les couches de carte chevauchent différents types de composants de l'environnement dans la carte.
8	Filtre	Un filtre est une liste d'attributs et de valeurs requises qui vous permet d'afficher des composants spécifiques dans la carte.

9	Noeuds et connexions de composants	Les lignes de connexion entre les noeuds correspondent aux statuts suivants : Ligne grise : aucune alerte n'est définie sur le composant d'arrière-plan. Ligne rouge : il existe au moins une alerte rouge sur le composant d'arrière-plan. Les pointillés gris indiquent qu'aucun composant d'arrière-plan n'existe sur la connexion.
10	Arborescence de mesures	Mesure du composant sélectionné affichées dans une arborescence permettant d'effectuer des recherches
11	Comparaison de temps de performance	Mesures pour le composant sélectionné présentées sous forme de tableau
12	Composants	Attributs associés au composant sélectionné.
13	Transactions métier	Transactions métier du composant sélectionné

Recherche de solutions aux problèmes à l'aide du carnet d'analyse

Le carnet d'analyse vous permet d'examiner des problèmes spécifiques.

Procédez comme suit :

- Lorsque vous identifiez une expérience présentant des problèmes potentiels, ouvrez le **carnet d'analyse**.
Le carnet d'analyse affiche les transactions qui sont affectées au format de carte.
- Utilisez La carte **Chronologie** pour afficher les événements et les alertes.
- Groupez la carte selon une perspective prédéfinie ou créez votre propre perspective.
- Recherchez des composants marqués comme problèmes ou anomalies.
 - Un cercle rouge indique que le composant joue un rôle dans au moins un problème ou une anomalie.
 - Un cercle concentrique rouge indique que le composant est responsable d'au moins un problème ou une anomalie.
- Passez la souris sur un **composant**, puis cliquez sur l'icône.
Le **graphique du composant** affiche un maximum de 20 noeuds. Utilisez les **graphiques de composant** pour comparer d'autres mesures dynamiques ou historiques entre des noeuds arbitraires. Le **graphique du composant** contient plus d'informations de mesures que celles disponibles pour chaque composant dans la carte.
 - Histogramme des temps de réponse agrégés
 - Moyenne Sparkline
 - Graphique Volume de transactions
- Cliquez sur un **composant** dans Relationship Flow (Flux de relation).
 - L'onglet **Arborescence de mesures** affiche un sous-ensemble contextuel des mesures pour le composant sélectionné. Pour plus d'informations sur l'utilisation de l'arborescence de mesures, voir la section [Surveillance des valeurs de mesures d'agent à l'aide de la vue des mesures](#).
 - L'onglet **Comparaison de temps de performance** affiche un comparateur Sparkline de mesures. La colonne de droite affiche les mesures de l'heure en cours. La colonne de gauche affiche les mesures pour la même heure d'une période précédente. Vous pouvez définir l'heure de comparaison dans les listes déroulantes. Les données de mesure apparaissent dans la visionneuse de mesures à côté des mesures de comparaison d'une période précédente.
 - L'onglet **Composants** contient les informations relatives aux attributs du composant sélectionné.
 - L'onglet **Transactions métier** contient une liste des transactions.
- Sélectionnez la période pour la comparaison des mesures dans la liste déroulante.

Le moteur de tri assisté analyse les données d'agent à partir de l'environnement surveillé. Le moteur identifie les connexions et les modèles entre des alertes spécifiques qui indiquent un problème de développement. Le panneau de tri assisté affiche les problèmes et anomalies détectés. Les problèmes et les anomalies représentent des situations. Les situations sont groupées par nom d'application responsable et triées dans l'ordre chronologique et par taille. Une anomalie indique une situation dans laquelle un ou plusieurs composants dans les transactions associées déclenchent des alertes d'avertissement.

Un problème indique une situation dans laquelle un ou plusieurs composants dans les transactions associées déclenchent des alertes d'avertissement.

8. Cliquez sur un **problème** ou une **anomalie**.

Des informations détaillées s'affichent. Le composant affecté est mis en surbrillance dans la carte.

Affichage du statut d'agent et gestion des fiches d'agent

Utilisez la vue Agents pour surveiller l'intégrité et les performances des agents disponibles dans votre environnement.

La page de vue d'agents est une vue d'ensemble contenant toutes les informations importantes sur les agents dans un emplacement unique. Dans la vue, les fiches d'agent présentent les détails d'un agent ou d'un groupe d'agents. Si plusieurs agents sont regroupés dans une fiche, les informations sur les mesures sont également groupées. Vous pouvez effectuer les opérations suivantes avec l'agent ou sa fiche :

Affichage du statut de l'agent

La vue d'agents vous permet de déterminer le statut de la connectivité des agents, de détecter tout problème de surcharge ou de collecte de mesures par l'agent. Vous pouvez afficher les informations en temps réel ou sélectionner une période historique.

Procédez comme suit :

1. Cliquez sur **Agents View** (Vue d'agents) dans le volet gauche.
Une fiche présente les détails d'un agent ou d'un groupe d'agents. Si plusieurs agents sont regroupés dans une fiche, les informations sur les mesures sont également groupées. La vue d'agents affiche tous les agents dans l'environnement et les mesures suivantes :
 - **UC**
Affiche le pourcentage d'UC utilisée.
 - **Heap Memory (Segment de mémoire)**
Affiche le pourcentage de mémoire utilisée.
Dans le graphique en courbes de l'UC et du segment de mémoire, passez le curseur sur un pic de mesure. Sélectionnez une période problématique et effectuez un zoom.
 - **GC Time (Durée GC)**
Affiche le pourcentage d'intervalle de temps passé dans l'utilitaire de nettoyage de mémoire pour la période sélectionnée.
 - **Metrics Collected (Mesures collectées)**
Indique le nombre de mesures collectées par les agents.
Si la fiche contient des informations pour un seul agent, des détails d'attribut plus précis tels que le nom d'hôte ou le temps de disponibilité sont affichés. Si la fiche inclut plusieurs agents, elle affichera le nombre d'applications, le nombre d'agents et le nombre de collecteurs.
2. (Facultatif) Cliquez sur le titre de la fiche pour afficher une perspective à partir de laquelle vous souhaitez regrouper les agents. Exemple : Type. La perspective par défaut est Nom.
Les perspectives disponibles sont basées sur des noms d'attribut de manière à grouper les agents en fonction de leurs attributs.
3. (Facultatif) Cliquez sur **Isolation View** (Vue Isolement).
Un nouvel onglet s'ouvre et contient la carte dans la **couche d'infrastructure APM**. La carte affiche les composants qui partagent la valeur d'attribut comme groupe étendu. Une perspective temporaire supprime les niveaux supérieurs

de groupement. La vue d'ensemble applique un filtre de chemins de transaction de façon que la carte affiche l'ensemble des transactions complètes qui transitent par les composants.

4. Ouvrez une fiche d'agent et sélectionnez l'une des options suivantes dans la liste déroulante **Sorted by** (Critère de tri) :
 - **Indice d'intégrité**
Affiche l'intégrité globale des agents. Plusieurs alertes sur les agents surveillent des mesures telles que l'UC ou la connectivité de l'agent. Le pourcentage d'indice d'intégrité calcule les alertes des dernières 24 heures. Si des alertes surveillées sont déclenchées au cours des dernières 24 heures, le pourcentage d'indice d'intégrité baisse. Par exemple, un indice d'intégrité de 100 % signifie qu'aucune alerte n'a été déclenchée dans les dernières 24 heures. Un indice d'intégrité de 50 % signifie qu'au cours des dernières 24 heures, des alertes ont été déclenchées pendant une durée totale de 12 heures.
 - **Connexion**
Indique le nombre d'agents disponibles dans votre environnement et le nombre d'agents déconnectés.
 - **Highest CPU (UC le plus élevé)**
Présente les fiches dont l'utilisation d'UC est la plus élevée en premier.
 - **Highest Memory (Mémoire la plus élevée)**
Présente les fiches dont l'utilisation de mémoire est la plus élevée en premier.
5. (Facultatif) Cliquez sur **View as List** (Afficher sous forme de liste).
Une liste est une alternative aux fiches d'agent qui contient des données supplémentaires et concises sur une seule page. Cliquez sur un nom de colonne à trier. Cliquez sur une ligne pour développer les données d'agent.

Ajout d'une fiche d'agent

Les fiches d'agent vous permettent de diviser vos agents en groupes pertinents en fonction de leurs attributs. Par défaut, vous disposez d'une fiche avec tous les agents. En tant qu'administrateur, vous pouvez ajouter d'autres fiches d'agent.

Procédez comme suit :

1. En haut de la page de vue d'agents, cliquez sur le signe Plus près des fiches d'agent existantes.
Une nouvelle fenêtre **Add Agent Card** (Ajouter une fiche d'agent) s'ouvre.
2. Fournissez un nom pour la fiche et suivez les instructions dans la fenêtre.
 - **Sélection d'un univers**
Dans la plupart des environnements d'entreprise, le nombre total de composants est trop élevé pour les visualiser de manière efficace. Les univers permettent à l'administrateur de définir le nombre et le type de composants et de les rassembler par groupes pertinents. Ce groupe ajusté est un univers. Pour des raisons de sécurité, aucune affectation par défaut à tous les utilisateurs n'est disponible. Pour afficher les informations d'un univers, Vous devez y être alloué.
 - **Application d'un filtre**
Utilisez l'univers complet ou appliquez un filtre.
 - **Inclusion du noeud Experience**
Experience est le premier composant frontal surveillé et le début du chemin de transaction. Un noeud d'expérience contient un attribut supplémentaire appelé Experience. Si vous cochez l'option Include experience node (Inclure un noeud Experience), les résultats filtrés incluent le noeud indiquant le point de départ de la transaction.
 - **Critère de groupement**
Sélectionnez les attributs que vous souhaitez utiliser pour accéder à d'autres niveaux de la fiche d'agent.
 - **Type de graphique par défaut**
UC/Segment de mémoire
Nombre de mesures collectées/Durée GC
Récapitulatif des attributs
3. Si vous souhaitez rendre une fiche publique, sélectionnez **Make this Agent Card public** (Rendre cette fiche d'agent publique).

NOTE

Si vous ne sélectionnez pas cette option, la fiche est privée et vous seul pouvez l'afficher. Si vous sélectionnez cette option, la fiche est publique et tous les utilisateurs ayant accès à l'univers approprié peuvent l'afficher.

4. Cliquez sur **Enregistrer**.

Vous venez d'ajouter une fiche d'agent.

Modification d'une fiche d'agent

Vous pouvez modifier des fiches d'agent, par exemple pour sélectionner différents attributs comme niveaux d'accès.

Procédez comme suit :

1. En haut de la page de vue d'agents, sélectionnez la fiche à modifier.
2. Cliquez sur le bouton Paramètres dans la fiche.
3. Cliquez sur **Edit Card** (Modifier une fiche).
Une nouvelle fenêtre **Edit Agent Card** (Modifier une fiche d'agent) s'ouvre.
4. Modifiez la fiche.
5. Cliquez sur **Enregistrer**.

Vous venez de modifier une fiche d'agent.

Suppression d'une fiche d'agent

Vous pouvez supprimer les fiches d'agent que vous ne souhaitez plus utiliser.

Procédez comme suit :

1. En haut de la page de vue d'agents, sélectionnez la fiche à modifier.
2. Cliquez sur le bouton Paramètres dans la fiche.
3. Cliquez sur **Edit Card** (Modifier une fiche).
Une nouvelle fenêtre **Edit Agent Card** (Modifier une fiche d'agent) s'ouvre.
4. Cliquez sur **Delete Card** (Supprimer une fiche).
5. Dans la fenêtre contextuelle de confirmation de suppression, cliquez sur **Supprimer**.

Vous venez de supprimer une fiche d'agent.

Partage d'une fiche d'agent

En tant qu'administrateur, vous pouvez partager une fiche d'agent avec un utilisateur dans un univers existant.

Procédez comme suit :

1. Vérifiez que l'utilisateur dispose de l'accès à l'univers.
2. Dans la fiche d'agent, sélectionnez **Make this Agent Card public** (Rendre cette fiche d'agent publique).
La fiche apparaît dans votre liste de fiches.
3. Envoyez le lien de la fiche d'agent à l'utilisateur.

NOTE

Vous pouvez partager une fiche d'agent privée avec un utilisateur du même univers. L'utilisateur peut afficher temporairement la fiche privée.

La page Vue Agents est une vue d'ensemble de toutes les informations importantes sur l'agent et permet à l'utilisateur de surveiller l'état et les performances des agents disponibles dans l'environnement. Vous pouvez effectuer les opérations suivantes avec l'agent ou sa fiche :

- Affichage du statut de l'agent
- Ajout d'une fiche d'agent
- Modification d'une fiche d'agent
- Suppression d'une fiche d'agent
- Partage d'une fiche d'agent

Pour plus d'informations sur l'exécution de ces actions, consultez la section [Affichage du statut d'agent et gestion des fiches d'agent](#).

Surveillance des valeurs de mesures d'agent à l'aide de la vue des mesures

En tant qu'administrateur CA APM, utilisez la vue des mesures pour obtenir une présentation claire des valeurs de mesures d'agent. Examinez les agents pour afficher leurs valeurs de mesures pendant une période donnée.

Présentation

DX APM fournit deux vues de mesures :

- **Vue de mesures globales** : contient toutes les mesures de tous les agents connectés à l'infrastructure APM pendant la plage horaire sélectionnée.
- **Vue de mesures contextuelles** : affiche un sous-ensemble de mesures applicables aux composants sélectionnés dans la carte.

Les deux vues contiennent une arborescence qui répertorie les mesures et d'autres informations. Dans DX SaaS, les mesures sont organisées selon une hiérarchie *Hôte | Processus | Agent*. DX APM sur site organise les mesures selon une hiérarchie *Domaine | Hôte | Processus | Agent*.

Présentation de l'arborescence des mesures

Le niveau le plus élevé dans l'arborescence représente des hôtes de serveur d'applications (DX SaaS) ou les domaines (DX APM sur site). Le niveau suivant représente les processus, suivis des agents installés sur des hôtes de serveur d'applications spécifiques. L'arborescence des agents, des ressources et des mesures s'actualise toutes les 60 secondes pour afficher les données de mesure actuelles.

L'arborescence des mesures affiche deux types d'hôtes :

- **Custom Metric Host (Virtual)** (Hôte de mesures personnalisées (Virtual)) : ce noeud représente un hôte virtuel qui contient des mesures non signalées par un agent spécifique. Par exemple, les mesures cumulées s'affichent sous ce noeud. Ce noeud ne correspond pas à un ordinateur hôte physique.
- **Hôtes** : ce noeud représente un ordinateur qui héberge un agent. Chaque noeud hôte contient un noeud de processus pour l'instance de l'application surveillée. Les noeuds de processus eux contiennent des noeuds d'agent. Les noeuds correspondant à des ressources d'application et système contiennent des mesures stockées dans les noeuds d'agent. Les ressources d'application dans les noeuds d'agent diffèrent en fonction du type d'agent (Java ou .NET). Le noeud de haut supérieur représente les composants suivants :
 - Composants de votre application J2EE ou .NET, tels que des servlets, des EJB ou des pages ASP
 - Noeuds système, y compris l'hôte exécutant votre serveur d'applications et l'ordinateur hôte exécutant DX APM

L'arborescence des mesures affiche deux types de mesures :

- **Mesure de chaîne** : la valeur de la mesure est une chaîne. Le graphique des mesures affiche uniquement la valeur en cours à la fin de la période.
- **Mesure numérique** : le graphique affiche les valeurs de mesure, lesquelles incluent les valeurs minimales et maximales, l'écart et l'historique d'état d'alerte associé.

Affichage d'une mesure d'agent dans la vue de mesures globales

Affichez les données en temps réel ou sélectionnez une période pour afficher des données historiques. Comparez, corrélerez et visualisez les valeurs de mesure d'une période spécifique.

Procédez comme suit :

1. Dans DX APM, cliquez sur **Vue des mesures** dans le volet gauche pour ouvrir la vue des mesures globales. L'arborescence de mesures s'ouvre.
2. Sélectionnez un hôte de serveur d'applications.
3. Parcourez l'arborescence et cliquez sur le nœud d'agent que vous souhaitez examiner.

NOTE

Les agents déconnectés sont affichés en gris. Si un agent n'envoie pas de mesure pendant un certain temps, elle devient inactive et s'affiche également en gris.

4. Cliquez sur un dossier dans l'arborescence des mesures pour afficher l'**aperçu des mesures**.

L'**aperçu des mesures** comprend les onglets suivants :

– Graphiques de mesures

Affiche les valeurs de mesure pour les nœuds sélectionnés dans l'arborescence des mesures.

– Nombre de mesures

Contient des informations récapitulatives à propos des mesures contenues dans des sous-dossiers du dossier sélectionné.

1. Cliquez sur une mesure dans le graphique à secteurs ou le tableau pour ouvrir le sous-dossier approprié.
2. Cochez la case **Mesures dynamiques uniquement** pour afficher le nombre de mesures dynamiques, c'est-à-dire les mesures signalées par l'agent à ce moment-là.

– Suivis

Contient la liste de toutes les transactions métier associées.

1. Cliquez sur une transaction métier dans la liste pour afficher les suivis correspondants et les détails des composants.

– Erreurs

Affiche une liste de toutes les transactions métier qui contiennent des erreurs.

1. Cliquez sur une transaction métier pour afficher les détails de l'erreur.

– Vidages de threads

Sélectionnez un nœud d'agent dans l'arborescence du navigateur de mesures pour afficher l'onglet **Vidages de threads**. Cet onglet vous permet de collecter des vidages de threads Java et d'afficher les données de vidage de threads actuelles et historiques. Un vidage de threads fournit des informations sur tous les threads qui s'exécutent dans une machine virtuelle Java à un moment donné. Pour chaque thread, un vidage de threads fournit le nom et l'ID du thread, son état et une trace de pile, qui répertorie toutes les méthodes appelées. L'onglet Vidages de threads inclut les éléments suivants :

- L'en-tête affiche l'heure du vidage de threads.
- Le volet de recherche vous permet de rechercher une chaîne spécifique dans toutes les informations de vidage de threads. Les résultats s'affichent dans le tableau d'informations de thread.
- La liste déroulante des états de threads filtre le tableau d'informations de thread par état de thread. Lorsque vous sélectionnez un état, le tableau des informations de threads est mis à jour.
- Le tableau des informations de threads affiche une liste de tous les threads. Pour chaque thread, il fournit l'ID, le nom, l'état du thread ainsi que la dernière méthode appelée par le thread juste avant le vidage.
- Le tableau de trace de pile de thread affiche toutes les méthodes dans l'ordre d'appel.
- Le graphique à secteurs % de threads par état affiche les threads dans les états suivants : Interbloqués, Bloqués, En cours d'exécution ou En attente.

NOTE

Si vous souhaitez trier les problèmes d'agent, affichez la mesure `<nom_agent> | Threads | Deadlock Count` dans l'arborescence du navigateur de mesures. Cette mesure indique s'il existe des threads interbloqués affectant l'agent. La configuration d'Introscope est requise pour activer la mesure Deadlock Count (Nombre d'interblocages). Pour plus d'informations, reportez-vous à la section [Agent Java](#).

Vous pouvez effectuer les opérations suivantes dans l'onglet Vidages de threads :

- **Collecter nouveau** : pour collecter un vidage de threads.
- **Enregistrer en tant que texte** : pour enregistrer le vidage de threads actuel dans un fichier texte.
- **Charger précédent** : pour charger un vidage de threads unique précédemment collecté et pour afficher l'horodatage et les données associées.

Aucune donnée de vidage de threads n'est affichée tant qu'un vidage de threads n'est pas collecté ou après le redémarrage d'un gestionnaire d'entreprise. Pour désélectionner un thread dans le tableau, maintenez la touche Ctrl enfoncée et cliquez à nouveau sur la ligne.

- (Facultatif) Cliquez sur la loupe pour rechercher des mesures spécifiques dans l'arborescence des mesures.
 - Sélectionnez **Partout** pour effectuer une recherche globale, ou sélectionnez l'option de dossier pour effectuer une recherche locale.
- (Facultatif) Pour masquer des mesures qui ne fournissent aucune donnée actuelle à l'agent, cliquez avec le bouton droit de la souris sur le noeud d'agent, puis cliquez sur **Masquer les mesures grisées**. La mesure n'apparaît pas dans l'arborescence des mesures.

NOTE

L'arborescence des mesures affiche à nouveau la mesure lorsque l'agent commence à recevoir des données actuelles de celle-ci.

- Cliquez sur une mesure, par exemple, **Temps de réponse moyen (ms)**, pour afficher ses valeurs dans le graphique de mesures. S'il existe une alerte sur la mesure, le graphique de mesures affiche l'historique d'état d'alerte sous la forme de bandes de couleur, qui indiquent l'état de l'alerte à un moment donné :
 - **Vert** - OK
 - **Jaune** - Avertissement
 - **Rouge** - Danger
 - **Aucune couleur** - Il n'existe aucune alerte pour la mesure sélectionnée.

NOTE

L'historique d'état d'alerte apparaît dans le graphique de mesures pendant maximum 7 jours. Si vous étendez la période au-delà de 7 jours, les informations relatives à l'état d'alerte n'apparaissent pas.

- (Facultatif) Désélectionnez l'option d'**affichage de l'analyse différentielle** pour masquer la bande d'écart.

NOTE

Si la mesure prend en charge l'analyse différentielle, une bande met automatiquement en évidence l'écart dans la tendance de la mesure.

- (Facultatif) Cliquez sur **Afficher les valeurs Min/Max**. Les valeurs minimum et maximum s'affichent dans le graphique.
- (Facultatif) Sélectionnez plusieurs mesures dans l'arborescence des mesures pour les comparer dans le graphique.
 - Cliquez sur le nom de la mesure en dehors de la case à cocher pour sélectionner une nouvelle valeur.
 - Cliquez sur **Combiner** pour afficher les données de mesures dans un seul graphique.
 - Cliquez sur **Effacer la sélection** pour sélectionner un autre ensemble de mesures.

NOTE

Vous pouvez sélectionner jusqu'à 10 mesures à comparer dans le graphique de mesures.

11. Utilisez la **chronologie** pour sélectionner une période spécifique.
12. Passez le pointeur de la souris sur le graphique et effectuez un zoom sur une période plus courte.

NOTE

La **chronologie** affiche des plages comprises entre 8 minutes minimum et une année maximum.

13. Sélectionnez une période dans la liste déroulante **Résolution** (15 minutes, 30 minutes, 1 heure, 2 heures, 6 heures ou 12 heures) pour afficher les valeurs correspondantes. Les valeurs de période disponibles sont : 15 secondes, 30 secondes, 1 minute, 2 minutes, 5 minutes, 15 minutes, 30 minutes, 1 heure, 2 heures, 6 heures, 12 heures, 1 jour, 7 jours et 14 jours.

NOTE

Les valeurs de période dans la liste déroulante **Résolution** s'affichent en fonction de la période sélectionnée dans la **chronologie**.

14. (Facultatif) Partagez l'URL avec vos collègues pour leur permettre d'afficher la même vue d'une mesure spécifique dans l'arborescence.

Graphiques de mesures personnalisées

Vous pouvez utiliser les options suivantes pour personnaliser le graphique.

- Sélectionnez une période dans la liste déroulante **Résolution** (15 secondes, 30 secondes, 1 minute ou 2 minutes) pour afficher les valeurs correspondantes.
- Cliquez sur **Combiner** et sélectionnez **Tout** pour afficher les données de mesures dans un graphique ou sélectionnez **Par nom** pour afficher les graphiques de mesures catégorisés par nom de mesure. Cette option est activée lorsque vous sélectionnez plusieurs mesures dans l'**arborescence des mesures**.
- Utilisez le bouton de **sélection** pour afficher et configurer les options suivantes :
 - **Affichage des valeurs min./max.** : sélectionnez l'option pour afficher les valeurs minimum et maximum sur le graphique.
 - **Combiner** : sélectionnez plusieurs mesures dans l'arborescence de mesures et sélectionnez une option dans le menu Combiner pour afficher toutes les mesures dans un graphique.
 - **Comparaison de périodes** : comparez les données sur les graphiques à l'aide d'une période prédéfinie ou sélectionnez une période personnalisée.
 - **Ruptures d'axe** : sélectionnez l'option pour afficher les données de la plage minimum à la plage maximum par rapport à la vue par défaut qui affiche les données de 0 à la valeur maximum. Lorsque vous sélectionnez l'option Ruptures d'axe, vous ne pouvez pas afficher les données sur une période. Par conséquent, l'option Comparaison de périodes est supprimée de liste déroulante. En outre, l'option Ruptures d'axe s'affiche uniquement lorsque vous ne combinez pas les graphiques de mesures.
 - **Télécharger** : sélectionnez une ou plusieurs mesures dans l'arborescence des mesures et cliquez sur l'option Télécharger pour télécharger les détails des mesures au format CSV.

Affichage de la vue de mesures contextuelles

Ouvrez la vue de mesures contextuelles à partir de la carte ou du carnet d'analyse pour afficher un sous-ensemble des mesures pour un noeud spécifique dans la carte.

Pour ouvrir la vue de mesures contextuelles à partir de la carte, procédez comme suit :

1. Dans DX APM, cliquez sur **Carte** dans le volet gauche.
2. Dans la carte, sélectionnez un noeud pour lequel vous souhaitez afficher les mesures d'agent.

NOTE

Si vous sélectionnez plusieurs noeuds, l'arborescence des mesures affiche un lien de mesures correspondant aux noeuds sélectionnés.

3. Cliquez sur le panneau **Navigateur de mesures** pour ouvrir l'arborescence des mesures.

Pour ouvrir la vue de mesures contextuelles à partir du carnet d'analyse, procédez comme suit :

1. Dans DX APM, cliquez sur **Vue Expérience** dans le volet gauche.
2. Recherchez une **fiche d'expérience** pour laquelle vous souhaitez afficher les mesures et cliquez sur **Ouvrir un carnet d'analyse**.
Le carnet d'analyse s'affiche.
3. **Ouvrez** un problème ou une anomalie pour afficher la **vue Carte** correspondante.

NOTE

Si le carnet d'analyse affiche un seul problème ou une seule anomalie, la **vue Carte** correspondante s'affiche par défaut.

4. Dans la carte, sélectionnez un noeud pour lequel vous souhaitez afficher les mesures d'agent.

NOTE

Si vous sélectionnez plusieurs noeuds, l'arborescence des mesures affiche un lien de mesures correspondant aux noeuds sélectionnés.

5. Cliquez sur le panneau **Arborescence de mesures** pour ouvrir l'arborescence des mesures.

Recherche de métriques dans l'arborescence de mesures

Dans l'**arborescence de mesures**, vous pouvez rechercher des mesures spécifiques ou utiliser l'expression régulière de l'agent pour filtrer les mesures requises. En outre, la barre de recherche prend en charge la fonctionnalité de recherche en texte intégral. Désormais, la barre de recherche détecte automatiquement si une entrée est au format d'expression régulière et effectue une recherche par expression régulière en conséquence.

NOTE

L'option permettant d'utiliser des expressions régulières a été désapprouvée.

Procédez comme suit :

1. Dans DX APM, cliquez sur **Vue des mesures** dans le volet gauche pour ouvrir la vue des mesures globales. L'**arborescence de mesures** s'ouvre.
2. Dans la zone de texte de recherche à filtrer, saisissez le nom de la mesure. La barre de recherche détecte si l'entrée est au format d'expression régulière et effectue une recherche en conséquence.

NOTE

Vous pouvez également sélectionner une saisie précédente dans la liste déroulante de saisie semi-automatique.

3. Les mesures correspondant aux critères de recherche sont répertoriées dans le volet droit.

NOTE

Cliquez sur le menu à trois points situé à droite de la page de résultats de la recherche pour afficher ou masquer des colonnes dans la vue des résultats de la recherche.

En outre, vous pouvez marquer des éléments comme favoris dans l'arborescence de mesures. Cette fonctionnalité s'étend aux mesures de graphique.

Procédez comme suit :

1. Pour marquer un élément comme favori, placez le curseur sur cet élément dans l'arborescence de mesures. Une étoile s'affiche sur le côté droit de l'élément.
2. Cliquez sur l'icône en forme d'étoile pour marquer l'élément comme favori.
3. La sélection de l'option **Show favorites only** (Afficher les favoris uniquement) affiche uniquement les éléments marqués comme favoris.

DX Application Performance Management offre deux vues de mesures : la vue globale des mesures et la vue contextuelle des mesures.

La vue des mesures fournit une présentation claire des valeurs de mesures d'agent. Examiner les agents est également utile pour afficher leurs valeurs de mesures pendant une période donnée.

Pour plus d'informations sur l'utilisation de la vue des mesures, reportez-vous à la section [Surveillance des valeurs de mesures d'agent à l'aide de la vue des mesures](#).

Intégration de la page Tableaux de bord DX dans la vue des mesures

Vous pouvez créer des tableaux de bord personnalisés dans les tableaux de bord DX à l'aide des mesures APM et les intégrer sur la page Vue des mesures. Dans la vue des mesures, le tableau de bord intégré s'affiche sous forme d'onglet si vous sélectionnez une mesure qui correspond à la condition.

NOTE

Par défaut, les tableaux de bord BlamePoint et Présentation des composants frontaux sont intégrés dans la vue des mesures. Ces tableaux de bord sont préconfigurés et faciles à utiliser.

A un haut niveau,

1. [Créez un tableau de bord](#). Créez le tableau de bord, balisez-le et ajoutez les variables dans Tableaux de bord DX.
2. [Mappez le tableau de bord](#). Mappez le tableau de bord que vous avez créé précédemment et l'emplacement des mesures dans DX APM à l'aide de la mosaïque **Tableaux de bord DX** située sur la page **Paramètres** de DX APM.
3. [Affichez le tableau de bord dans DX APM](#).

Création d'un tableau de bord personnalisé sur la page Tableaux de bord DX

Créez le tableau de bord à l'aide de la source de données **AIOps_Metrics**. Dans le générateur de requêtes, ajoutez les variables **\$Agent** et **\$Attribute**.

Procédez comme suit :

1. Connectez-vous à la page Tableaux de bord DX.
2. Cliquez sur **Créer > Tableau de bord** dans le volet de navigation gauche.
 - a. Cliquez sur **Add an empty panel** (Ajouter un panneau vide).
 - b. Dans le champ **Panel Title**, entrez le titre du panneau.
 - c. Sélectionnez la visualisation.
 - d. Générez la requête :
 - a. Sélectionnez la source de données **AIOps_Metrics**.
 - b. Activez l'option **Advanced Query Builder** (Générateur de requêtes avancées).
 - c. Dans la section **Source Name Specifier** (Spécificateur de nom de source),
 - a. Définissez la valeur Specifier (Spécificateur) sur **EXACT**. Vous pouvez également spécifier le modèle REGEX.
 - b. Définissez la valeur Name (Nom) sur **\$Agent**.

NOTE

Vous pouvez entrer cette variable comme **\$Agent** ou l'ajouter avec des valeurs. Par exemple, vous pouvez saisir **\$Agent:SuperDomain\apm\rh7\197\Infrastructure\Agent**.

- d. Dans la section **Attribute Name Specifier** (Spécificateur de nom d'attribut),
 - a. Définissez la valeur Specifier (Spécificateur) sur **EXACT**. Vous pouvez également spécifier le modèle REGEX.
 - b. Définissez la valeur **Pattern** (Modèle) sur **\$Attribute**.

NOTE

Vous pouvez entrer cette variable comme **\$Attribute** ou l'ajouter avec des valeurs. Par exemple, vous pouvez entrer **\$Attribute: Average Response Time**.

NOTE

En plus de **\$Agent** et **\$Attribute**, vous pouvez également utiliser une variable personnalisée du nom de votre choix.

3. Enregistrez le tableau de bord dans le dossier **APM-MetricView**. Vous pouvez également utiliser le **Dossier personnalisé** pour spécifier un autre dossier dans lequel enregistrer le tableau de bord.
4. Balisez le tableau de bord.
 - a. Cliquez sur l'icône **Paramètres** du tableau de bord.
 - b. Ajoutez la balise sur la page **Paramètres généraux**.

NOTE

Assurez-vous que la balise est unique.

5. Ajoutez la variable **\$Agent** :
 - a. Ouvrez la page **Paramètres généraux**.
 - b. Dans le volet de navigation gauche, cliquez sur **Variables**.
 - c. Saisissez les informations suivantes :
 - a. **Nom** : attribuez un nom à la variable.
 - b. **Type** : définissez la valeur Type sur **Personnalisé**.
 - c. **Valeurs séparées par des virgules** : entrez la valeur d'un agent.
 - d. Cliquez sur **Mettre à jour**.
6. Ajoutez la variable **\$Attribute** :
 - a. Ouvrez la page **Paramètres généraux**.
 - b. Dans le volet de navigation gauche, cliquez sur **Variables**.
 - c. Saisissez les informations suivantes :
 - a. **Nom** : attribuez un nom à la variable.
 - b. **Type** : définissez la valeur Type sur **Personnalisé**.
 - c. **Valeurs séparées par des virgules** : entrez la valeur d'un attribut.

NOTE

Si vous avez utilisé des paramètres personnalisés, vous devez également ajouter les variables correspondantes.

7. Cliquez sur **Mettre à jour**.

Mappage du tableau de bord

Une fois le tableau de bord créé, l'étape suivante consiste à le mapper à l'aide de la mosaïque **Tableaux de bord DX** située sur la page **Paramètres** de **DX APM**.

Procédez comme suit :

1. Connectez-vous à DX Application Performance Management.
2. Cliquez sur **Paramètres** dans le volet de navigation gauche.
3. Cliquez sur **Tableaux de bord DX** sous **Paramètres généraux**.
4. Cliquez sur **Nouveau tableau de bord DX**.
5. Saisissez les informations suivantes :
 - **Actif** : activez le tableau de bord.
 - **Nom de l'onglet** : entrez un nom pour l'onglet du tableau de bord qui sera visible dans la vue des mesures.
 - **Dossier de l'arborescence des mesures** :
 - **Expression du dossier** : entrez l'expression régulière du dossier de mesures.

NOTE

Pour connaître le chemin d'accès complet, accédez à la **Vue des mesures**. Cliquez avec le bouton droit sur le dossier contenant cette mesure et sélectionnez **Copier le chemin d'accès complet en tant qu'expression régulière**.

- **Mesures enfants** : entrez la mesure que le dossier de mesures doit contenir.
 - **Intégration de la page Tableaux de bord DX** :
 - **Balise du tableau de bord** : entrez la balise du tableau de bord à mapper.
 - **Paramètres** : sélectionnez les paramètres requis ci-après.
 - **De** : indique l'heure de début actuelle.
 - **À** : indique l'heure de fin actuelle.
 - **Agent** : indique le chemin de l'agent sélectionné.
 - **Attribut** : indique le chemin de l'attribut sélectionné.
 - **Options avancées** :
 - **Dossier personnalisé** : si vous avez enregistré le tableau de bord dans un autre dossier, spécifiez le nom ici. Pour le dossier APM-MetricView, vous pouvez laisser ce champ vide.
 - **Paramètres personnalisés** : pour utiliser les paramètres personnalisés, configurez les valeurs suivantes :
 - **Nom du paramètre** : nom du paramètre personnalisé.
 - **Expression régulière** : expression régulière utilisée pour exécuter une recherche de correspondance dans le chemin du dossier sélectionné. Elle peut utiliser des groupes de capture (en utilisant des parenthèses ()) ou des groupes de capture nommés (en utilisant la syntaxe (?<nom>pattern)).
 - **Valeur** : spécifiez le groupe qui doit être utilisé à l'aide du signe \$. Exemples : \$1, \$2, \$name.
 - **Valeur par défaut** : valeur par défaut qui sera utilisée si aucune valeur ne correspond dans le chemin du dossier sélectionné à l'aide de l'expression régulière.
6. Cliquez sur **Enregistrer**.
- Le mappage est terminé. Cette page affiche les informations suivantes pour chaque mappage :
- Nom de l'onglet
 - Condition
 - Balise de tableau de bord
 - Active
 - Actions (Afficher, Modifier, Supprimer)

Affichage du tableau de bord dans la vue des mesures

Une fois le tableau de bord mappé dans DX APM, il s'affiche sous forme d'onglet si vous sélectionnez une mesure correspondant à la condition.

Procédez comme suit :

1. Connectez-vous à DX APM.
 2. Ouvrez la mosaïque **Tableaux de bord DX** sur la page **Paramètres**.
 3. Notez le chemin d'accès indiqué dans la colonne **Condition** correspondant au chemin d'accès au tableau de bord.
 4. Dans le volet de navigation gauche, cliquez sur **Vue des mesures**.
 5. Accédez à l'emplacement et sélectionnez le dossier de mesure.
- Le tableau de bord s'affiche sous la forme de l'un des onglets.

Vous pouvez créer des tableaux de bord personnalisés dans les tableaux de bord DX à l'aide des mesures APM et les intégrer sur la page Vue des mesures. Dans la vue des mesures, le tableau de bord intégré s'affiche sous forme d'onglet si vous sélectionnez une mesure qui correspond à la condition.

Pour créer, mapper et afficher un tableau de bord personnalisé dans la vue des mesures, reportez-vous à la section [Intégration de la page Tableaux de bord DX dans la vue des mesures](#).

Utilisation de la chronologie et de la surbrillance

Le mode Chronologie permet de passer du moment actuel à un point dans le passé afin d'afficher les événements de statut qui se sont produits auparavant. La fonction de surbrillance permet d'identifier, dans la carte, les composants qui partagent un ou plusieurs attributs.

Utilisation de la chronologie

La fonction de chronologie permet de remonter jusqu'à l'origine du problème. Utilisez le curseur de chronologie pour vérifier le statut des composants sélectionnés à un moment dans le passé. Passez d'un événement à un autre pour connaître les événements de modification pour la période sélectionnée.

Procédez comme suit :

1. Cliquez sur **Chronologie**.
La chronologie s'affiche. Par défaut, la chronologie fonctionne en mode Temps réel et affiche le récapitulatif agrégé des alertes pour les 8 dernières minutes. La plage horaire est verrouillée et s'actualise toutes les 30 secondes.
2. Pour activer le mode **Historique**, sélectionnez **DYNAMIQUE**, puis désactivez **Live Updates**. Sélectionnez **Appliquer**. La section bleu claire de la chronologie indique la période active. La carte affiche le statut et l'environnement à la fin de la plage horaire. Les barres d'état sur les noeuds affichent les résultats agrégés pour cette période.
3. Modifiez la période en faisant glisser la période active dans la chronologie.
4. Modifiez l'échelle de la chronologie à l'aide de la molette ou via une entrée tactile.
5. Sélectionnez une heure spécifique en cliquant sur la partie supérieure de la chronologie.

NOTE

Cliquer sur la partie supérieure de la chronologie modifie l'heure de fin, mais pas la plage horaire.

Les événements de statut sont affichés sous forme d'icônes dans la chronologie. La vue Carnet d'analyse filtre les événements en fonction du problème ou de l'anomalie que vous sélectionnez. Des récapitulatifs d'alerte affichent les résultats regroupés pour la période jusqu'à la date sélectionnée.

TIP

A tout moment, utilisez les sélecteurs **Heure de début** et **Heure de fin** pour sélectionner une heure spécifique.

6. Cliquez sur un **noeud** pour afficher les événements correspondant dans la période sélectionnée.
7. Sélectionnez **Statut**, **Topologique** ou **Attribut** afin d'inclure ces événements de modification dans la chronologie.

NOTE

La sélection de l'événement de modification est réinitialisée lorsque vous ouvrez le carnet d'analyse.

- a. Cliquez sur une **icône d'événement** ou sur une **icône de groupe d'événements** pour afficher les détails concernant l'événement de modification. Assurez-vous d'avoir sélectionné le noeud approprié dans la carte. Les noeuds qui ne sont pas affectés par les modifications sélectionnées s'affichent grisés dans la carte.
- b. Cliquez sur un **noeud**.
- c. Cliquez sur l'**icône d'événement de modification**.
Les détails de l'événement ou d'une liste chronologique des événements du groupe s'affichent dans le volet droit.

NOTE

La chronologie détecte automatiquement les nouveaux composants chargés dans APM. Sélectionnez **Statut**, **Topologique** ou **Attribut** pour afficher les événements de modification pour les nouveaux composants dans la chronologie.

8. Effectuez un zoom avant ou arrière sur la chronologie pour modifier l'échelle.
 - a. Faites glisser les curseurs de début et de fin pour définir la période de votre choix.
 - b. Faites glisser la période active vers des périodes antérieures ou ultérieures.

- c. Faites glisser la chronologie inactive (grise) pour déplacer la plage visible.
Si la période active n'est pas visible, cliquez sur la valeur de temps. Le marqueur de fin de la période active se déplace vers l'heure que vous avez sélectionnée. Définissez des dates et heures spécifiques à l'aide des sélecteurs situés sur la gauche.
9. Cliquez sur un **événement individuel** pour afficher les noeuds concernés dans la carte. Les noeuds qui ne sont pas affectés sont grisés.
Les barres d'état des noeuds affichent l'état agrégé pour la période sélectionnée. La carte affiche l'environnement pour la période sélectionnée.

Utilisation de la surbrillance

La fonction de surbrillance permet d'identifier, dans la carte, les composants qui partagent un ou plusieurs attributs. Une liste affiche les attributs disponibles pour la surbrillance selon les attributs des composants dans la vue de carte actuelle.

Procédez comme suit :

1. Cliquez sur l'icône **Carte**, puis sur **Surbrillance**.
Une barre de surbrillance est développée.
2. Cliquez sur l'icône en forme de signe **plus** et sélectionnez l'attribut que vous souhaitez mettre en surbrillance.
3. (Facultatif) Cliquez sur l'attribut sélectionné pour le trier ou le filtrer.
La carte affiche l'environnement, y compris les filtres appliqués. La carte s'affiche dans la perspective sélectionnée. La valeur d'attribut sélectionné s'affiche en jaune.

La fonction de chronologie permet de remonter jusqu'à l'origine du problème. Utilisez le curseur de chronologie pour vérifier le statut des composants sélectionnés à un moment dans le passé.

La fonction de surbrillance permet d'identifier, dans la carte, les composants qui partagent un ou plusieurs attributs.

Pour plus d'informations sur la chronologie et la mise en surbrillance, reportez-vous à la section [Utilisation de la chronologie et de la mise en surbrillance](#).

Utilisation de la chronologie et affichage des événements de modification

La chronologie vous permet d'afficher les événements de modification qui se produisent à l'heure actuelle et ceux qui se sont produits auparavant. La fonction de chronologie permet de remonter jusqu'à l'origine du problème.

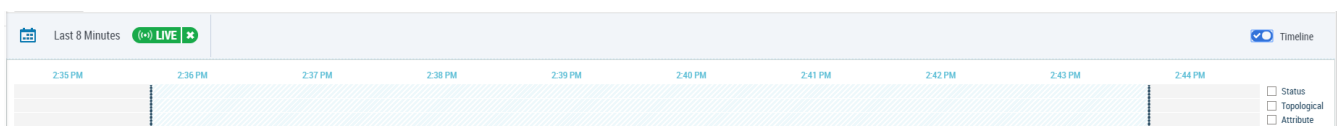
Vous pouvez afficher la chronologie dans les vues suivantes :

- Vue Expérience
- Vue Agents
- Carte
- Tableaux de bord
- Vue des mesures

Cet article couvre les rubriques suivantes :

Actions disponibles dans la chronologie

Lorsque vous activez le bouton bascule **Chronologie** dans une vue, la chronologie s'affiche et la section bleu clair de celle-ci indique la période active. La chronologie est actualisée toutes les 30 secondes.



Vous pouvez effectuer les actions suivantes dans la chronologie :

Déplacement de la chronologie

Cliquez n'importe où dans la zone grise de la chronologie et faites-la glisser pour afficher une période passée, actuelle ou future.

Modification de la période active

Vous pouvez sélectionner la zone bleu clair et la faire glisser pour ajuster la période de temps active. La période active est toujours comprise entre l'heure actuelle et la période précédente.

Ajustement de l'échelle

Pour ajuster l'échelle active, sélectionnez et déplacez les barres horizontales à la fin de la période active. Vous pouvez sélectionner une heure spécifique en cliquant en haut de la chronologie ou de la valeur d'heure. Le fait de cliquer sur une valeur d'heure ou sur la partie supérieure de la chronologie modifie l'heure de fin, mais pas la plage horaire.

Affichage des noeuds et des événements affectés

Vous pouvez afficher les noeuds et les événements affectés à l'aide de la chronologie, de la **carte** ou de la vue **Composant**.

NOTE

La section Événements de la vue **Composant** s'affiche uniquement lorsque vous sélectionnez la case à cocher du ou des événements dans la chronologie.

- **Utilisation de la chronologie**

Lorsque vous sélectionnez un événement dans la chronologie, le noeud sur lequel l'événement s'est produit est mis en surbrillance dans la **carte** ou le **tableau de bord**, et les noeuds restants sont grisés.

Si le panneau **Vue Composant** est visible, le ou les événements que vous sélectionnez dans la chronologie apparaissent en surbrillance en jaune dans la section Événements du panneau.

- **Utilisation de la carte**

Lorsque vous sélectionnez un ou plusieurs noeuds dans la **carte**, les événements correspondants s'affichent dans la section Événements, mais *uniquement* lorsque le panneau **Vue Composant** est visible.

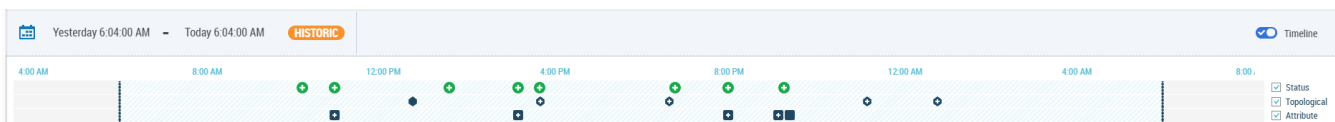
- **Utilisation du panneau Vue Composant**

Pour effectuer une action dans le panneau **Vue Composant**, assurez-vous qu'il est visible.

Lorsque vous sélectionnez un ou plusieurs noeuds dans la **carte**, le panneau affiche tous les événements associés dans la section Événements. La sélection d'un événement dans la chronologie entraîne la mise en surbrillance des événements correspondants en jaune dans la section Événements du panneau. De même, lorsque vous sélectionnez un événement dans la section Événements du panneau, le noeud correspondant est centré et mis en surbrillance dans la **carte**.

Affichage des événements de modification dans la chronologie

Dans la **carte**, les **tableaux de bord** et les vues Carnet, vous pouvez sélectionner et afficher les événements de modification **Statut**, **Topologique** ou **Attribut** dans la chronologie. La vue Carnet d'analyse filtre les événements en fonction du problème ou de l'anomalie que vous sélectionnez. La chronologie détecte automatiquement les nouveaux composants chargés dans DX APM. Les événements de modification sont disponibles lorsque la chronologie affiche des données en temps réel ou historiques. Les événements de modification sélectionnés s'affichent sous forme d'icônes dans la chronologie.



NOTE

La sélection de l'événement de modification est réinitialisée lorsque vous ouvrez le carnet d'analyse.

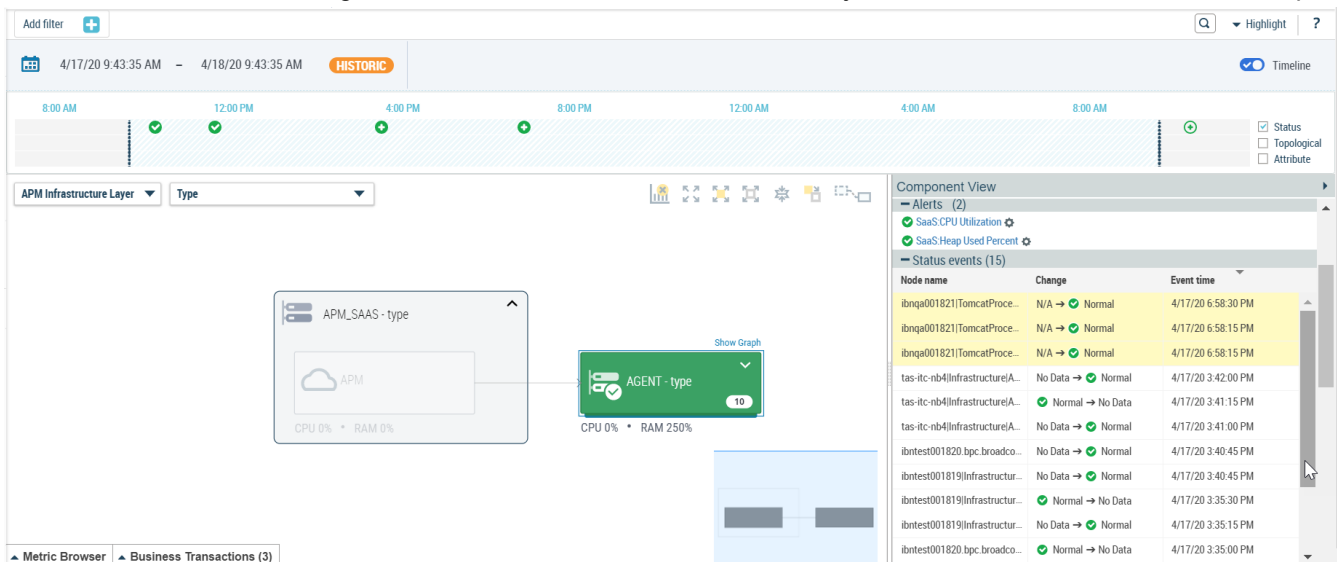
Dans la vue **Carte**, les détails des événements sont disponibles dans la vue **Composant**.

Événements de modification de statut

Dans la vue **Carte** ou **Tableaux de bord**, sélectionnez un noeud, puis sélectionnez la case à cocher **Statut** dans la chronologie pour afficher les événements de modification de statut.

Dans l'image ci-dessous, vous pouvez constater qu'un noeud est sélectionné dans la **carte** et que la case à cocher **Statut** est sélectionnée dans la chronologie. Par conséquent, vous pouvez afficher les événements de modification de statut sous forme d'icônes dans la chronologie, qui représentent le moment où la modification de statut s'est produite pour le noeud sélectionné.

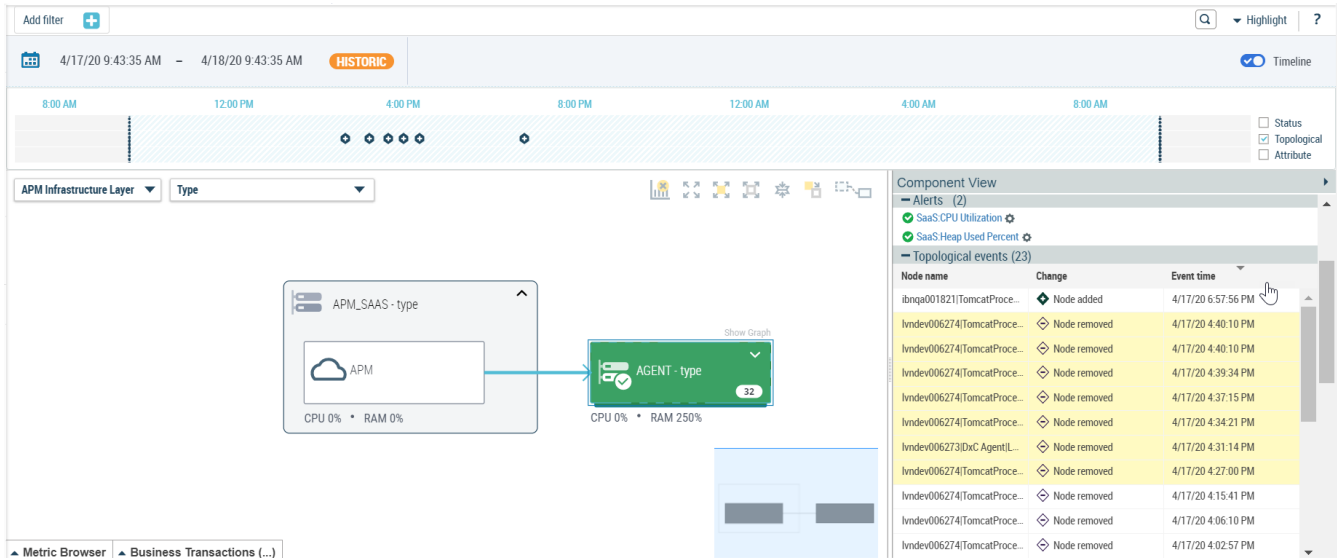
Lorsque vous sélectionnez un noeud dans la **carte**, tous les événements associés s'affichent dans la section Événements du panneau **Vue Composant**, mais *uniquement* si ce dernier est visible. Vous pouvez afficher les détails du statut, par exemple lorsque le noeud est passé de normal à un état où il ne recevait plus de données. De plus, la sélection d'un événement dans la chronologie met en surbrillance les événements en jaune dans la section Événements du panneau.

**Événements de modification topologique**

Dans la vue **Carte** ou **Tableaux de bord**, sélectionnez un noeud, puis sélectionnez la case à cocher **Topologique** dans la chronologie pour afficher les événements de modification topologique. Vous pouvez afficher des détails, tels que la date et l'heure de la suppression ou de l'ajout du noeud dans la topologie.

Dans l'image ci-dessous, vous pouvez constater qu'un noeud est sélectionné dans la **carte** et que la case à cocher **Topologique** est sélectionnée dans la chronologie. Par conséquent, vous pouvez afficher les événements de modification de topologie sous forme d'icônes dans la chronologie, qui représentent le moment où la modification de topologie s'est produite pour le noeud sélectionné.

Lorsque vous sélectionnez un noeud dans la **carte**, tous les événements associés s'affichent dans la section Événements du panneau **Vue Composant**, mais *uniquement* si ce dernier est visible. Tous les événements de modification de topologie qui se sont produits dans le noeud sont répertoriés dans la section **Événements topologiques** de la vue **Composant**. De plus, la sélection d'un événement dans la chronologie met en surbrillance les événements en jaune dans la section Événements du panneau.

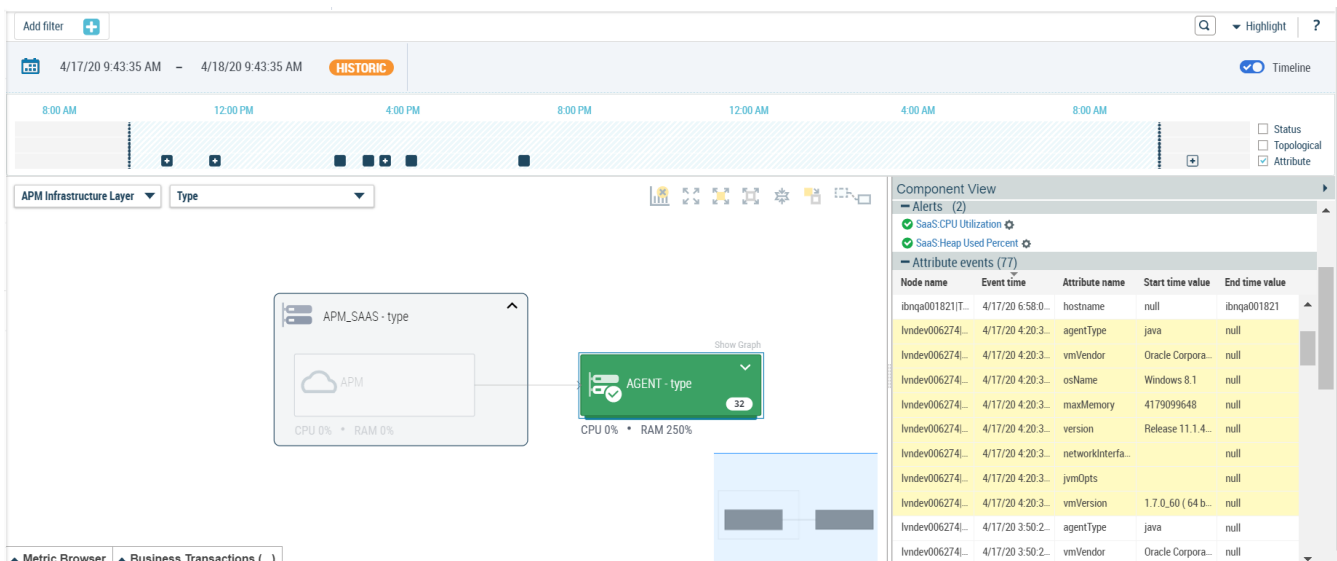


Événements de modification d'attribut

Dans la vue **Carte** ou **Tableaux de bord**, sélectionnez un noeud, puis sélectionnez la case à cocher **Attribut** dans la chronologie pour afficher les événements de modification d'attribut. Vous pouvez afficher des détails, tels que la date et l'heure d'ajout de l'attribut, le nom et la valeur au début et à la fin.

Dans l'image ci-dessous, vous pouvez constater qu'un noeud est sélectionné dans la **carte** et que la case à cocher **Attribut** est sélectionnée dans la chronologie. Par conséquent, vous pouvez afficher les événements de modification d'attribut sous forme d'icônes dans la chronologie, qui représentent le moment où l'attribut a été créé pour le noeud sélectionné.

Lorsque vous sélectionnez un noeud dans la **carte**, tous les événements associés s'affichent dans la section Événements du panneau **Vue Composant**, mais *uniquement* si ce dernier est visible. Tous les événements de modification d'attribut qui se sont produits dans le noeud sont répertoriés dans la section **Événements d'attribut** de la vue **Composant**. De plus, la sélection d'un événement dans la chronologie met en surbrillance les événements en jaune dans la section Événements du panneau. Pour ajouter un attribut personnalisé, vous devez être en mode dynamique.



La chronologie vous permet d'afficher les événements de modification survenus à l'heure actuelle et ceux qui se sont produits auparavant, et vous aide également à rechercher l'origine du problème. La chronologie peut être affichée dans les vues suivantes : Vue Expérience, Vue Agents, Carte, Tableaux de bord et Vue des mesures.

Pour plus d'informations sur les actions disponibles et pour afficher les événements de modification dans la chronologie, reportez-vous à la section [Utilisation de la chronologie et affichage des événements de modification](#).

Utilisation d'attributs dans DX APM

Les attributs sont des balises ou des étiquettes que les agents collectent auprès des composants dans votre environnement d'application. Ils permettent d'afficher la carte sous diverses perspectives, de filtrer ainsi que de mettre en surbrillance des composants. Les attributs simplifient l'identification des composants et de leurs relations avec les autres composants. Chaque attribut a un nom et une valeur.

DX APM collecte des attributs de base pour chaque composant. Les administrateurs peuvent créer des attributs personnalisés en définissant des règles d'attribut. Pour plus d'informations sur la création d'attributs personnalisés, reportez-vous à la section [Définition du mode de surveillance de l'environnement à l'aide de règles d'attribut](#).

NOTE

Tous les attributs s'appliquent à DX APM et seuls certains attributs s'appliquent à DX APM sur site.

Présentation

Chaque composant dans la carte contient un ensemble d'attributs. DX APM établit une distinction entre les types d'attributs suivants :

- Les **attributs communs** sont collectés automatiquement par DX APM et existent pour la plupart des composants.
- Les **attributs personnalisés** vous permettent de définir et de recueillir des informations supplémentaires à l'aide de règles d'attribut.
- Les **attributs d'agent** fournissent des informations sur les composants spécifiques que les agents installés surveillent.
- Les **attributs d'extension** fournissent des informations supplémentaires que les extensions d'agent collectent.

Les attributs disponibles pour une utilisation dans les filtres et les perspectives s'affichent dans la liste déroulante des attributs.

NOTE

Informations complémentaires :

- [Organisation des composants à l'aide de perspectives](#)
- [Identification des points importants lors de l'utilisation des filtres](#)
- [Surveillance de l'intégrité globale de l'environnement à l'aide du tableau de bord](#)

Attributs communs

DX APM collecte les attributs communs suivants :

- `name`
Définit le nom du composant. Cet attribut est dérivé d'un ou de plusieurs autres attributs.
- `type`
(Vertex)
Indique le type de composant du vertex (sommet).
- `Source cluster` Définit le cluster APM auquel le composant envoie ses rapports.
- `agent`

Définit l'identificateur de l'agent (`hostname|process|agentName`). Cet attribut indique l'origine du vertex.

- `hostname`

Définit le nom d'hôte ou de conteneur sur lequel le composant s'exécute.

- `agentDomain`

Définit le domaine de l'agent.

- `processedBy`

Indique le nom de la classe qui a traité et créé ce composant. Cet attribut provient généralement d'une trace de transaction.

- `applicationName`

Définit le nom de l'application. Recherchez le nom de l'application dans la description du déploiement de l'application Web ou examinez le chemin de mesure de l'agent `Frontends|Apps|<nom_application>`.

- `containerId`

(Docker) Indique l'ID du conteneur Docker. La valeur `containerID` est visible dans la couche applicative.

NOTE

Cet ID est présent uniquement si l'agent Java, Node JS, PHP ou Python s'exécute dans le conteneur.

- `remotePort`

Indique le port distant appelé par le composant.

- `backendNode`

Affiche la valeur `true` si le vertex est un composant d'arrière-plan dans une application.

- `remoteName`

Indique le nom de l'hôte distant appelé par le composant.

- `localAddress`

Définit l'adresse IP locale du composant.

- `serviceId`

Identifie le service d'entreprise défini dans CA CEM.

- `Experience`

Indique le nom de l'expérience comme indiqué dans la vue Expérience, par exemple, `Apps|ActivityService|URLs|/api/v1/` on `serv17.ca.com` (GENERICFRONTEND). Cet attribut existe uniquement si la valeur de l'attribut `IsExperience` est `true`. Pour plus d'informations sur les expériences, reportez-vous à la section [Surveillance des performances à l'aide de la vue Expérience](#).

- `IsExperience`

Indique que le vertex est une "Expérience" ou le composant le plus à gauche dans la carte. Pour plus d'informations sur les expériences, reportez-vous à la section [Surveillance des performances à l'aide de la vue Expérience](#).

- `remoteAddress`

Indique l'adresse IP distante appelée par le composant.

- `inferredBackendNode`

Affiche la valeur `true` si ce vertex a été inféré d'une ou de plusieurs connexions à ce composant d'arrière-plan.

- `provider`

Indique le fournisseur de la base de données, par exemple, base de données Postgres, Oracle ou Derby.

- `port`

Indique le port sur lequel la base de données ou le gestionnaire d'entreprise (Enterprise Manager, EM) écoute.

Attributs personnalisés

Les administrateurs peuvent créer des attributs personnalisés au niveau des composants afin que les utilisateurs puissent afficher les perspectives et filtrer la carte en fonction des composants qui partagent le même nom d'attribut. Vous pouvez ajouter un attribut personnalisé à un seul composant ou à une règle d'attribut. Les attributs personnalisés permettent aux utilisateurs d'identifier et d'associer facilement des composants spécifiques. Les analystes peuvent ainsi afficher

les perspectives et filtrer la carte en fonction des composants qui partagent le même nom d'attribut. CA Application Performance Management permet de filtrer le contenu en fonction de n'importe quelle valeur d'attribut. Les attributs affectés aux composants à partir d'une couche spécifique dans DX APM sont également visibles dans les autres couches.

NOTE

Informations complémentaires :

- [Définition du mode de surveillance de l'environnement à l'aide de règles d'attribut](#)
- [Couches de carte](#)

Attributs d'agent

Les agents Java et Node.js collectent uniquement les attributs communs.

Attributs d'extension

Les extensions d'agent Infrastructure collectent des attributs pour des composants d'infrastructure spécifiques. Consultez les liens ci-dessous pour obtenir la liste complète des attributs d'extension disponibles.

NOTE

Informations complémentaires :

- [Amazon Web Services](#)
- [Attributs Azure](#)
- [Attributs Docker](#)
- [Personnalisation des attributs du Docker](#)
- [Attributs et mesures F5 LTM](#)
- [Attributs liés à Host Monitoring](#)
- [Attributs Kubernetes](#)
- [Attributs OpenShift](#)

Les attributs sont des balises ou des étiquettes que les agents collectent auprès des composants dans votre environnement d'application. Ils permettent d'afficher la carte sous diverses perspectives, de filtrer ainsi que de mettre en surbrillance des composants. Les attributs simplifient l'identification des composants et de leurs relations avec les autres composants. Chaque attribut a un nom et une valeur.

Pour plus d'informations sur les attributs, reportez-vous à la section [Utilisation d'attributs dans DX APM](#).

Organisation des composants à l'aide de perspectives

Les perspectives permettent de grouper des composants dans la **carte** et le **tableau de bord** sans les supprimer de l'ensemble de données. Vous pouvez créer des perspectives personnelles réservées à votre univers. Sélectionnez un ou plusieurs attributs partagés pour grouper les composants. Les administrateurs de DX APM peuvent modifier et créer des perspectives à caractère public accessibles à tous les utilisateurs. Les perspectives prêtes à l'emploi permettent de visualiser les composants d'application et d'infrastructure des piles de technologie et services d'hébergement présents dans votre environnement d'application.

Présentation

La liste déroulante Perspectives se trouve dans la **carte** et le **tableau de bord**. Le cadre affiche la perspective actuelle appliquée. Développez la liste déroulante pour afficher les perspectives définies.

- Les perspectives personnelles s'affichent au-dessus de la ligne.
- Les perspectives publiques, définies par l'administrateur, s'affichent sous la ligne.
- Les perspectives prêtes à l'emploi, qui affichent les relations entre les composants qui existent sur les couches, s'affichent sous la ligne. Les perspectives suivantes sont définies comme prêtes à l'emploi :

Couche de carte	Perspective prête à l'emploi							
Couche Application	Type	Valeur par défaut :	Hostname (nom d'hôte)	Utilisateur final, Application	Location	Owner	Jenkins	Infrastructure d'application
Couche d'infrastructure APM	Type							
Couche Infrastructure	Type	Valeur par défaut :						
Couche réseau	Type							

La dernière perspective de la liste déroulante est toujours *Aucune perspective*, qui affiche tous les composants séparément. Combinez une perspective avec des filtres pour supprimer les composants de votre choix de la **carte** et du **tableau de bord**.

NOTE

La perspective par défaut de la couche applicative n'a pas les mêmes attributs que la perspective par défaut de la couche d'infrastructure.

Utilisation des perspectives prêtes à l'emploi

Utilisez les perspectives prêtes à l'emploi pour afficher les composants d'application et leurs composants d'infrastructure associés.

Procédez comme suit :

1. Accédez à la **carte** ou au **tableau de bord**.
2. Affichez les composants d'infrastructure et d'application.
Pour afficher les composants d'infrastructure d'un composant d'application spécifique :
 - a. Dans la liste déroulante en haut, sélectionnez **Couche applicative**.
 - b. Cliquez sur la liste déroulante **Perspectives**, sélectionnez **Infrastructure d'application**.

NOTE

Si votre environnement applicatif utilise des conteneurs Docker, sélectionnez cette perspective pour afficher les conteneurs, les hôtes et les instances de serveur Docker associés.

- c. Sélectionnez un composant d'application dans la **carte** ou le **tableau de bord** pour afficher les composants d'infrastructure associés.
3. Affichez d'autres informations sur les composants dans la **vue Composant**, qui s'ouvre près de la **carte**.

Vous avez utilisé une perspective prête à l'emploi pour afficher les relations entre les composants qui existent sur les couches.

Création d'une perspective personnelle


Les perspectives permettent de grouper des composants en fonction d'un attribut spécifique. Les composants pour lesquels la valeur de cet attribut est identique apparaissent dans des groupes discrets dans la carte. Par exemple, la perspective **Emplacement** comprend trois groupes :

- Tous les composants avec la valeur **Londres**
- Tous les composants avec la valeur **Prague**
- Tous les composants avec la valeur **New York**

Les utilisateurs individuels créent et personnalisent des groupes de perspectives personnelles.

Procédez comme suit :

1. Dans le volet gauche, sélectionnez **Perspectives**.
2. sélectionnez **Créer une perspective**.
3. Attribuez un nom à la perspective.
4. Sélectionnez chaque **couche applicable** sur laquelle la perspective est visible.
5. (Facultatif) Dans **Visibilité**, activez les options requises :
 - Sélectionnez la case **Public** pour activer la visibilité des droits pour d'autres utilisateurs.
 - Sélectionnez la zone **Groupement automatique** pour réorganiser les vertex dans la carte en groupes par défaut.
6. Dans la **Hiérarchie de regroupement**, sélectionnez au moins un attribut.
 Cliquez sur **Ajouter un attribut** pour appliquer des attributs supplémentaires pour le groupement des vertex. Notez que chaque attribut ne peut être ajouté qu'une seule fois.
 Si vous avez activé l'option **Groupement automatique**, le groupement par défaut est d'abord appliqué aux vertex, suivi des attributs sélectionnés dans la section **Hiérarchie de groupement**. Les attributs de la section **Hiérarchie de groupement** sont appliqués dans l'ordre descendant. Si vous supprimez un attribut, la liste est réorganisée et les attributs sont ensuite appliqués dans le nouvel ordre descendant.

Cliquez sur le bouton  en face d'un attribut et faites-le glisser et déposez-le pour trier ou réorganiser les attributs dans la hiérarchie. L'ordre des attributs est important, car il définit l'ordre d'application des filtres et par conséquent le groupement des vertex.

NOTE

Les attributs sont répertoriés sous la couche correspondante. Vous pouvez sélectionner les attributs des couches qui ne sont pas sélectionnées en tant que **Couches applicables** pour une perspective donnée.

7. (Facultatif) Créez un groupe de perspectives multiniveau. Sélectionnez d'autres attributs.
8. Sélectionnez **Enregistrer**.

La perspective s'affiche dans la liste déroulante **Perspectives** de la **carte** lorsque la couche correspondante est sélectionnée.

Personnalisation d'une perspective publique

L'administrateur crée des groupes de perspectives publiques. Ces groupes sont disponibles pour tous les utilisateurs de CA APM. Vous pouvez personnaliser une perspective publique.

Procédez comme suit :

1. Dans le volet gauche, sélectionnez **Perspectives**.
2. Identifiez la perspective publique que vous souhaitez personnaliser, puis sélectionnez **Modifier**.
 Une fenêtre contextuelle s'affiche.
3. (Facultatif) Modifiez le nom de la perspective.
4. (Facultatif) Sélectionnez une autre couche ou ajoutez plusieurs couches sur lesquelles vous souhaitez que la perspective soit visible.

Pour plus d'informations, reportez-vous à la section [Couches de carte](#).

5. Dans la **Hiérarchie de regroupement**, sélectionnez au moins un attribut.
6. (Facultatif) Créez un groupe de perspectives multiniveau. Sélectionnez d'autres attributs.
7. (Facultatif) Sélectionnez **+** pour ajouter des attributs supplémentaires au groupe de perspectives.
8. Sélectionnez **Enregistrer**.

Vous venez de personnaliser une perspective publique. La perspective que vous avez créée est personnelle. Vous pouvez la modifier ou la supprimer. La perspective s'affiche dans la liste déroulante **Perspectives** de la **carte**.

Modification d'une perspective personnelle

Procédez comme suit :

1. Dans le volet gauche, sélectionnez **Perspectives**.
2. Sélectionnez la perspective personnelle et cliquez sur **Modifier**.
Une fenêtre contextuelle s'affiche.
3. (Facultatif) Modifiez le nom de la perspective.
4. (Facultatif) Sélectionnez une autre couche ou ajoutez plusieurs couches sur lesquelles vous souhaitez que la perspective soit visible.
Pour plus d'informations, reportez-vous à la section [Couches de carte](#).
5. Dans la **Hiérarchie de regroupement**, sélectionnez au moins un attribut.
6. (Facultatif) Créez un groupe de perspectives multiniveau. Sélectionnez d'autres attributs.
7. (Facultatif) Sélectionnez **+** pour ajouter des attributs supplémentaires au groupe de perspectives.
8. Sélectionnez **Enregistrer**.

Vous venez de modifier la perspective personnelle.

Suppression d'une perspective personnelle

Procédez comme suit :

1. Dans le volet gauche, sélectionnez **Perspectives**.
2. Identifiez la perspective personnelle et cliquez sur **Supprimer**.
3. Une fenêtre contextuelle de confirmation s'affiche. Sélectionnez **Oui**.

Vous venez de supprimer la perspective personnelle.

Les perspectives permettent de grouper des composants dans la carte et le tableau de bord sans les supprimer de l'ensemble de données. Vous pouvez créer des perspectives personnelles réservées à votre univers. Sélectionnez un ou plusieurs attributs partagés pour grouper les composants. Les administrateurs de DX APM peuvent modifier et créer des perspectives à caractère public accessibles à tous les utilisateurs.

Pour obtenir des informations complémentaires sur les perspectives, consultez [Organisation des composants à l'aide de perspectives](#).

Affichage des relations entre les composants dans la carte

La carte utilise des composants tels que des noeuds, des alertes, le panneau des détails et l'aperçu des performances. Les groupes de composants affichent les informations d'état cumulées pour l'ensemble des composants du groupe concerné. La carte affiche les relations entre les différents composants présents dans l'environnement. L'origine est le premier composant dans une série de dépendances indiquant des problèmes de performance. Ce composant est à l'origine de la détérioration des performances dans votre environnement d'application.

Carte

La carte présente le statut d'alerte, le nom et le type d'icône pour chaque composant. DX APM collecte les informations à partir du gestionnaire d'entreprise et les affiche dans chaque noeud.

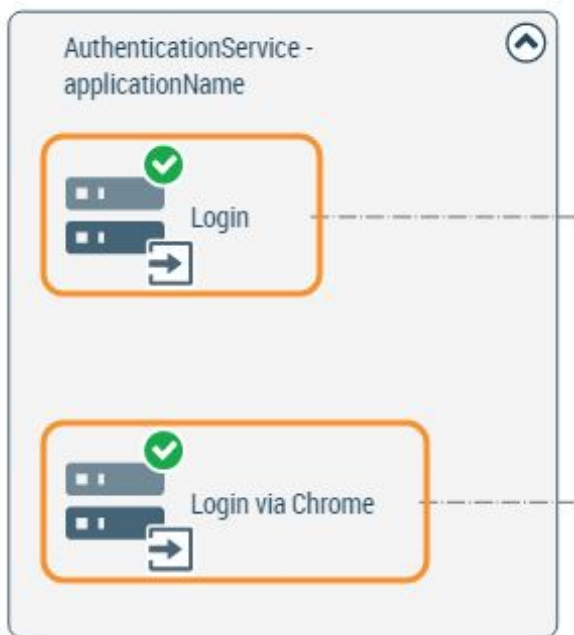
Différentes options vous permettent d'affiner vos recherches dans la carte. Vous pouvez par exemple :

- Afficher la carte sous différentes perspectives.
- Utiliser des filtres pour vous concentrer sur des composants spécifiques.
- Utiliser la vue Composant pour afficher les alertes, mesures et attributs de chaque noeud de la carte. Sélectionnez les onglets pour afficher des informations issues d'autres couches de la carte.
- Utiliser la chronologie pour comparer les informations actuelles et historiques. La chronologie présente des marqueurs signalant les modifications d'alerte, de topologie et d'attribut et vous permet de les inspecter. Les informations sont calculées sur la période spécifiée dans la chronologie. En mode dynamique, la période d'agrégation est de 8 minutes.

DX APM prend en charge les permaliens, qui contiennent tous les détails de la page affichée dans l'URL. Vous pouvez envoyer l'URL de la page à tout autre utilisateur pour qu'il puisse afficher la même vue. Vous pouvez également créer des favoris pour ces URL, afin de revenir à la même vue lors d'une session ultérieure.

Composant frontal en tant qu'expérience

Le noeud d'expérience est le premier composant frontal surveillé et contient un attribut Expérience. Le noeud d'expérience est le début du chemin de transaction. Une expérience peut être, par exemple, un servlet ou un composant frontal générique. La carte affiche un noeud d'expérience avec une icône en forme de flèche. Dans l'exemple ci-dessous, vous pouvez voir des noeuds d'expérience *Login* et *Login via Chrome*.



NOTE

Tous les composants frontaux ne sont pas des expériences. La plupart des noeuds frontaux apparaissent au milieu d'une transaction et ne sont donc pas des expériences.

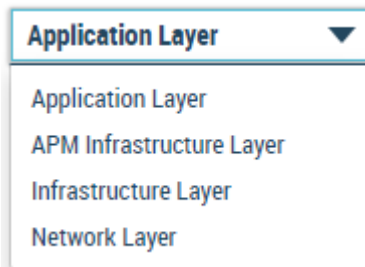
Présentation de la carte

Servez-vous de l'exemple de flux de travaux ci-dessous pour en apprendre davantage sur la carte. Par défaut, la carte s'actualise toutes les 5 minutes pour afficher la nouvelle topologie. Cette fonctionnalité est configurable. Les nouveaux

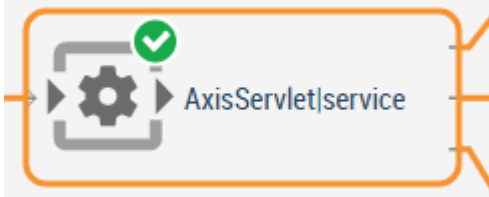
composants se distinguent par leur contour continu de couleur bleue, et les composants supprimés par leur contour bleu en pointillés.

Procédez comme suit :

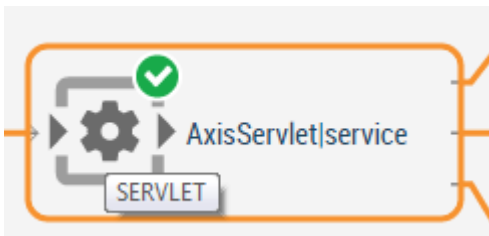
1. Sélectionnez la **couche applicative** pour afficher les composants dans la carte. Les composants correspondent aux fiches d'expérience dans la vue Expérience.



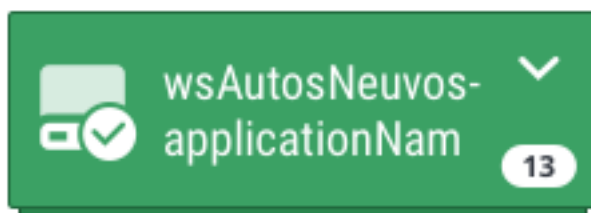
2. Parcourez les noeuds et passez le curseur sur l'un d'eux pour afficher d'autres informations. Le noeud est une représentation des transactions métier et des composants logiciels directement surveillés ou cumulés dans un contexte topologique. La carte prend en charge jusqu'à 50 000 noeuds. Si le nombre de noeuds à afficher sur la carte est suffisant pour affecter les performances, la carte regroupe automatiquement les noeuds. Les groupes ne représentent aucun attribut ou perspective spécifique. Par défaut, les noeuds sont groupés automatiquement lorsque le nombre de noeuds à afficher est supérieur à 150. Ajoutez des filtres ou définissez des perspectives pour réduire le nombre de noeuds à afficher sur la carte. Le graphique de statut affiche le dernier statut signalé à la fin de l'intervalle sélectionné pour ce composant ou ce groupe.



Pour savoir le type d'unité qu'un noeud représente, passez le curseur sur l'icône près du nom de l'unité.



Dans l'exemple suivant, un groupe de noeuds partage l'attribut `applicationName`.



75 tx/min • 324 seconds

- Le nombre 13 indique que le groupe inclut 13 noeuds.
- 75 tx/min indique des réponses par intervalle.
- 324 secondes indique le temps de réponse moyen.

3. Identifiez les connexions :

Les connexions affichées sur la carte peuvent contenir des composants d'arrière-plan.

APM reconnaît les connexions suivantes :

- **Ligne pleine** : un composant d'arrière-plan existe sur la connexion. Sélectionnez la connexion pour afficher les propriétés du composant d'arrière-plan dans la vue Composant.
- **Ligne grise en tirets** : aucun composant d'arrière-plan n'existe sur la connexion. Il n'est pas possible de cliquer sur la connexion.
- (Couche Infrastructure uniquement) **Ligne grise en pointillés** : la ligne présente entre deux noeuds indique que le premier contient le deuxième.
- (Couche Infrastructure uniquement) **Ligne grise** : la ligne présente entre deux dockers signifie que le premier se rapporte au deuxième.

La couleur de la ligne pleine indique l'état d'alerte du composant d'arrière-plan :

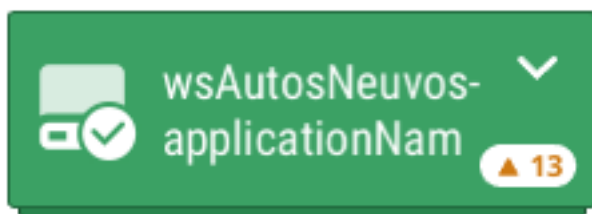
- **Ligne grise** : aucune alerte n'est définie sur le composant d'arrière-plan.
- **Ligne verte** : toutes les alertes sur le composant d'arrière-plan sont vertes.
- **Ligne jaune** : il existe au moins une alerte jaune, mais aucune alerte rouge sur le composant d'arrière-plan.
- **Ligne rouge** : il existe au moins une alerte rouge sur le composant d'arrière-plan.
- **Ligne orange** : une ligne de couleur orange indique une trace de transaction.

4. Groupez les composants de la couche sélectionnée pour identifier les problèmes de performances des composants d'infrastructure partagés (composants intercouche).

La couleur de l'icône de groupe indique l'état d'alerte du composant intercouche :

- **Icône grise** : il existe au moins une alerte verte pour le composant intercouche qui regroupe les composants de la couche sélectionnée.
- **Icône rouge** : il existe au moins une alerte rouge pour le composant intercouche qui regroupe les composants de la couche sélectionnée.
- **Icône jaune** : il existe au moins une alerte jaune pour le composant intercouche qui regroupe les composants de la couche sélectionnée.

Dans l'exemple ci-dessous, les groupes d'agents partagent un hôte. Le nombre 13 indique un composant d'hôte et le nombre 12 les composants d'agent. Le triangle orange représente une application dans un état Avertissement :



75 tx/min • 324 seconds

5. Placez le curseur sur un composant pour afficher la trace de transaction.

La trace de transactions montre tous les composants auxquels une transaction est associée en amont et en aval. Passez le curseur sur un noeud Experience pour afficher le chemin complet de la transaction en surbrillance.

6. Basculez entre les couches de la carte.

- Sélectionnez **Couche d'infrastructure APM** pour afficher les gestionnaires d'entreprise et les agents dans la carte. La vue correspond à la vue Agents. Utilisez cette vue si vous souhaitez afficher, par exemple, les gestionnaires

d'entreprise en cours d'exécution et les agents connectés. Lorsque vous accédez à la vue d'isolement à partir d'une fiche d'agent, la carte affiche la couche d'infrastructure APM.

- Sélectionnez **Couche d'infrastructure** pour afficher l'infrastructure réseau de votre environnement, y compris Docker Monitor.

NOTE

Pour plus d'informations sur les couches de la carte, reportez-vous à la section [Couches de carte](#).

7. Sélectionnez **Navigateur de mesures** pour afficher la vue des mesures.

Analyse des transactions métier

La vue Carte permet de rechercher des composants à surveiller. Dans l'onglet Transactions métier, vous pouvez consulter les récapitulatifs et les détails des traces de transactions associées. Ces informations permettent de comprendre les performances des transactions et de résoudre les problèmes de performances en identifiant quand, où et pourquoi les performances se détériorent.

Procédez comme suit :

1. Sélectionnez des noeuds spécifiques ou des groupes de 1 000 noeuds maximum.
2. Sélectionnez l'onglet **Transactions métier**.
Une liste récapitulative affiche les informations de suivi qui correspondent au composant pour la période sélectionnée dans la chronologie. Les traces affichent les durées. Les traces sont codées au moyen d'une couleur afin d'indiquer les problèmes liés à une transaction. Le rouge, par exemple, indique une erreur. Vous pouvez identifier les méthodes problématiques en notant la durée du suivi. Les opérations de suivi anormalement longues sont probablement la cause des transactions lentes.

NOTE

La liste est actualisée automatiquement lorsque vous utilisez le mode Dynamique.

3. [Examen des performances médiocres des transactions](#)

NOTE

Informations complémentaires :

- [Organisation des composants à l'aide de perspectives](#)
- [Identification des points importants lors de l'utilisation des filtres](#)
- [Surveillance des performances à l'aide de la vue Expérience](#)

La carte utilise des composants tels que des nœuds, des alertes, le panneau de détails et la présentation des performances pour montrer les relations entre les différents composants dans l'environnement. Les groupes de composants affichent les informations d'état cumulées pour l'ensemble des composants du groupe concerné.

Pour plus d'informations sur la carte et sa relation avec les composants, reportez-vous à la section [Affichage des relations entre les composants dans la carte](#).

Couches de carte

En tant qu'administrateur, vous pouvez parcourir rapidement les couches de carte pour identifier la cause première des problèmes de performances. Passez d'une couche à l'autre de la carte pour visualiser les problèmes de performance qui sont causés par des composants d'application, des composants d'infrastructure ou des composants DX APM. Appliquez d'autres filtres pour afficher des types spécifiques de composants dans les couches. Ajustez le nombre et les types de composants pour les rassembler en groupes d'utilisation simple (univers).

Présentation

Les couches de carte chevauchent différents types de composants de l'environnement dans la carte. La carte affiche les composants et leurs connexions dans la couche sélectionnée. Les connexions entre les composants de différentes

couches sont appelées connexions intercouches. Les composants avec connexions intercouches aux composants dans la couche sélectionnée s'affichent à droite dans la **vue Composant**. Par exemple, lorsque vous sélectionnez un composant de servlet dans la carte, la **vue Composant** affiche les propriétés du servlet et les propriétés de l'agent qui le surveille. Vous pouvez également afficher les connexions intercouches sur la carte à l'aide de filtres d'attribut intercouche. Pour plus d'informations, voir la section [Définition du mode de surveillance de l'environnement à l'aide de règles d'attribut](#).

NOTE

DX APM ajoute automatiquement des connexions intercouches entre les agents et les composants d'application surveillés par les agents.

Utilisation des couches de carte

Basculez entre les couches de carte pour afficher les composants d'une couche spécifique. Sélectionnez un composant dans la carte et affichez les connexions intercouches dans la **vue Composant**.

Procédez comme suit :

1. Sélectionnez une couche de carte dans la liste déroulante. Effectuez un choix parmi les couches suivantes :
 - **Couche Application**
Affiche les composants d'application surveillés par les agents APM. Cette couche correspond aux composants de carte de versions antérieures de CA APM.
 - **Couche d'infrastructure APM**
Affiche les composants APM, tels que des agents et des collecteurs.
 - **Couche Infrastructure**
Affiche les hôtes, les instances Docker et d'autres composants physiques. Cette couche contient des informations sur les agents Infrastructure et leurs extensions. La couche d'infrastructure collecte également les informations à partir d'intégrations ; exemple : Unified Infrastructure Management (CA UIM).

NOTE

DX APM sur site vous permet d'intégrer des composants d'autres systèmes dans la couche d'infrastructure à l'aide de l'API REST. CA UIM utilise cette API REST pour l'intégration à DX APM sur site pour permettre à DX APM sur site d'afficher les composants matériels.

- **Couche réseau**
Affiche les éléments du réseau cloud tels que le cloud privé virtuel (VPC), les routeurs, les interconnexions, les sous-réseaux et d'autres éléments des VPC. Cette couche contient des informations sur les agents Infrastructure et sur leurs extensions cloud.

NOTE

Pour afficher les services de surveillance des extensions cloud GCP dans la couche réseau, configurez les services GCP tels que Google Virtual Private Cloud, Google Cloud Interconnect et Google Cloud Router. Pour plus d'informations, reportez-vous à la section [Configuration de l'extension Google Cloud Platform](#).

2. Cliquez sur un composant dans la carte pour ouvrir la **vue Composant**.
3. Basculez entre les onglets de la **vue Composant** pour afficher les propriétés du composant sélectionné et des composants connectés à partir d'autres couches.

Application de filtres dans les couches de carte

Un filtre est une liste d'attributs et de valeurs requises qui vous permet d'afficher des composants spécifiques dans la carte. Appliquez un filtre pour afficher tous les composants de la couche de filtrage qui correspondent aux attributs de filtre. Si vous changez de couche, les composants avec connexions intercouches aux composants filtrés restent visibles dans la carte.

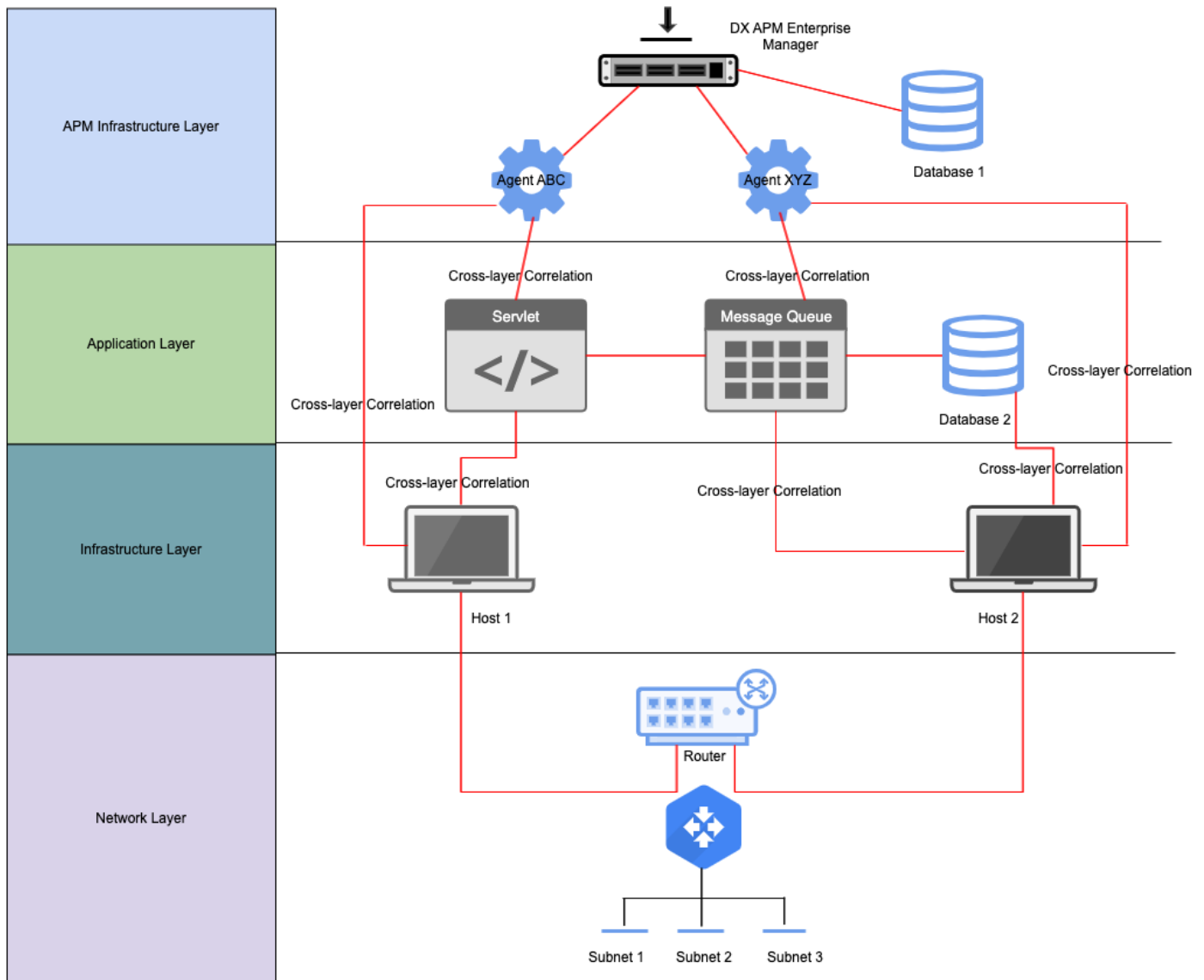
Pour appliquer un filtre à la carte, sélectionnez un attribut de filtre dans la liste des attributs.

NOTE

Les attributs sont répertoriés sous la couche correspondante. Vous pouvez sélectionner des attributs de plusieurs couches.

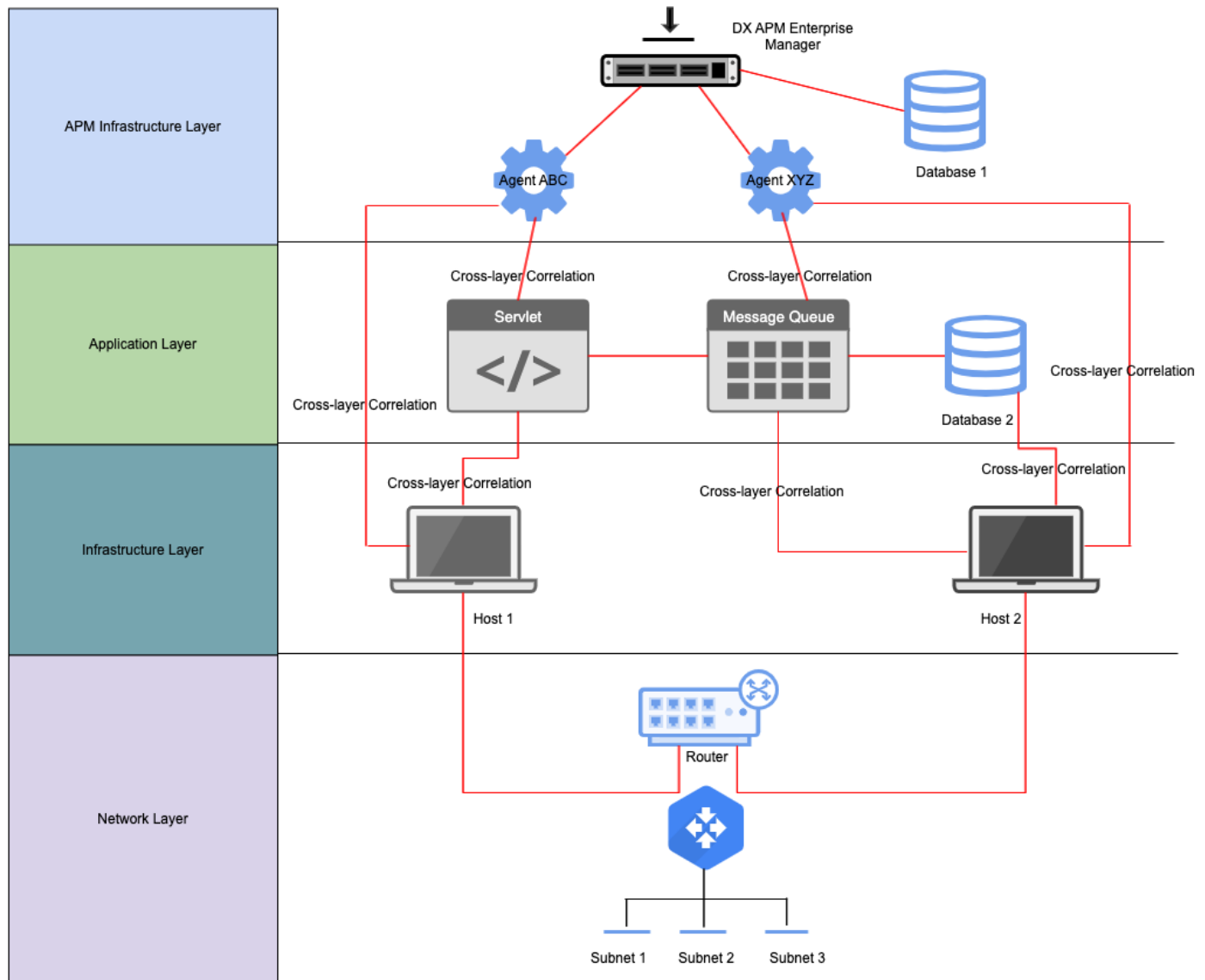
Exemple :

Le diagramme suivant illustre une carte non filtrée qui contient plusieurs connexions intercouches :

Figure 6: Couches de carte 1**Opération :**

Dans la couche d'infrastructure APM, définissez le filtre pour renvoyer les agents dont le nom contient ABC et XYZ.

Résultats : Le diagramme suivant illustre les résultats filtrés pour chaque couche de carte :



NOTE

La couche d'infrastructure APM n'affiche pas de collecteurs ni de bases de données du gestionnaire d'entreprise si la couche de filtrage constitue la couche applicative. Les collecteurs et les bases de données du gestionnaire d'entreprise n'ont pas de connexions intercouchées aux composants d'application. Seuls les composants de type agent ont des connexions intercouchées à la couche applicative.

Application d'univers dans les couches de carte

Après avoir défini un filtre de sélection de composants spécifiques, vous pouvez enregistrer le filtre en tant qu'univers. Autorisez les utilisateurs à accéder à tous les composants de l'univers, y compris les composants à connexions intercouchées aux composants sélectionnés. Pour plus d'informations sur la configuration des univers, voir la section [Configuration des univers](#).

Les exemples suivants présentent des possibilités d'utilisation de filtres dans les couches de carte.

Exemple 1 : Capture de transactions complètes transitant par un domaine spécifique

Cet univers contient les transactions complètes surveillées qui traversent un domaine sélectionné, notamment des composants d'arrière-plan déduits et des noeuds de transaction métier. Cet univers contient également tous les agents qui surveillent les composants d'application.

Procédez comme suit :

1. Sélectionnez la **couche applicative** comme couche de filtrage.
2. Cliquez sur **Ajouter un filtre** et sélectionnez **Suivre le chemin de la transaction**.
3. Sélectionnez **Domaine de l'agent** dans la liste des attributs.
4. Entrez le nom du **domaine de l'agent** dans le **filtre** pour rechercher les transactions de ce domaine.

Exemple 2 : Octroi de l'accès administrateur à l'ensemble des collecteurs du gestionnaire d'entreprise, des bases de données du gestionnaire d'entreprise et des agents à partir d'un domaine spécifique

Cet univers contient les composants requis à partir de la couche d'infrastructure APM, ainsi que les composants d'application que les agents surveillent dans le domaine spécifié. Les résultats n'affichent pas les transactions d'arrière-plan ou métier déduites, car ces transactions ne sont pas surveillées par des agents.

Procédez comme suit :

1. Sélectionnez la **couche d'infrastructure APM** comme couche de filtrage.
2. Cliquez sur **Ajouter un filtre** et sélectionnez l'attribut **Domaine de l'agent**.
3. Entrez le nom du **domaine de l'agent** dans le **filtre**.
4. Cliquez sur le signe **+** pour ajouter un autre élément de filtre et sélectionnez **Ajouter un groupe de filtres**.
5. Sélectionnez **Type** dans la liste des attributs.
6. Sélectionnez toutes les valeurs d'attribut à l'exception de **AGENT** ; par exemple : **EM_COLLECTOR**, **EM_DATABASE**, etc.

La carte affiche les composants et leurs connexions dans la couche sélectionnée. Les couches de carte vous permettent d'identifier la cause première des problèmes de performances. Vous pouvez passer d'une couche à l'autre de la carte pour visualiser les problèmes de performance qui sont causés par des composants d'application, des composants d'infrastructure ou des composants DX APM.

Pour plus d'informations sur les couches de la carte, reportez-vous à la section [Couches de carte](#).

Identification des points importants lors de l'utilisation des filtres

Les filtres vous permettent d'affiner la recherche de composants par nom et valeur d'attribut. Ils suppriment les informations de l'ensemble de données affichés dans le tableau de bord et la carte. Utilisez des filtres pour identifier des points importants dans le cadre de la surveillance de votre environnement. Filtrez les groupes de composants non affectés pour simplifier le tableau de bord et la carte à des fins de triage et de surveillance. Les filtres sont cumulatifs et fonctionnent de gauche à droite. Vous pouvez filtrer les résultats d'un filtre par un autre. Vous pouvez créer des couches de filtres pour accéder rapidement aux zones spécifiques d'un environnement. Les filtres sont persistants entre le tableau de bord et la carte.

Application Performance Management comprend les fonctionnalités de filtre suivantes :

- Filtrer par chemin de transaction
- Filtrer les composants par n'importe quel attribut
- Appliquer plusieurs groupes de filtres
- Inclure le noeud d'expérience dans les résultats du filtre
- Effectuer un glisser-déposer de filtres individuels sur les groupes de filtres

Groupes de filtres et filtres d'attribut

Un groupe de filtres définit l'ensemble des noms et des valeurs d'attributs affichés sur la carte et le tableau de bord. Tous les autres composants sont supprimés de l'ensemble de données. Dans un groupe de filtres unique, chaque condition de

filtre supplémentaires réduit l'ensemble résultant de noeuds affichés. Un filtre d'attribut supprime tous les composants de l'ensemble de données qui n'ont pas de noms et de valeurs d'attributs dans la condition de filtre. Un filtre de chemin de transaction supprime tous les composants de l'ensemble de données qui n'ont pas de valeurs de chemin de transaction dans la condition de filtre.

- Les filtres d'un groupe de filtres unique sont combinés avec un opérateur ET. Chaque condition de filtre peut être un filtre d'attribut ou un filtre de chemin de transaction. Ajoutez un groupe de filtres pour inclure un deuxième ensemble de données filtrées dans la carte et le tableau de bord.
- Les groupes de filtres différents sont combinés avec un opérateur OU. La carte affiche tous les noeuds qui répondent aux critères du groupe de filtres 1 et tous les noeuds qui répondent aux critères du groupe de filtres 2.

Vous pouvez glisser-déposer les conditions de filtre pour modifier les groupes de filtres. Si vous déplacez un filtre de chemin de transaction entre les groupes de filtres à l'aide de la fonction glisser-déposer, le filtre devient un filtre d'attribut. Vous ne pouvez pas déplacer les filtres de chemin de transaction entre les groupes de filtres. Vous pouvez modifier le filtre et sélectionner la case à cocher **Suivre le chemin de la transaction** pour activer les traces de transaction.

Vous pouvez modifier l'ordre des filtres à l'aide de la fonction glisser-déposer. Vous pouvez modifier l'ordre des filtres, les déplacer dans des groupes de filtres et dans des filtres de chemin de transaction, ou en dehors de ceux-ci. La seule restriction est que vous ne pouvez pas déplacer le filtre de chemin de transaction dans son ensemble. Si vous déplacez la dernière condition de filtre en dehors de la trame du filtre de chemin de transaction, la trame disparaît.

NOTE

Informations complémentaires :

- [Définition du mode de surveillance de l'environnement à l'aide de règles d'attribut](#)

Définition d'un filtre de chemin de transaction

Application Performance Management génère des données de carte en échantillonnant les données de suivi de transaction. Il existe un enregistrement pour chaque chemin de transaction qui transite via un composant.

NOTE

Dans les environnements de grande taille, le fait d'identifier toutes les transactions peut entraîner la génération d'un nombre élevé de vertex, ce qui peut avoir un impact sur les performances. Pour empêcher l'explosion des données dans les environnements de grande taille, vous pouvez désactiver cette fonctionnalité.

Un filtre de chemin de transaction identifie tous les composants de tous les chemins de transaction avec des valeurs d'attribut spécifiées dans les critères de filtre. Par exemple, vous voulez afficher dans la carte toutes les transactions qui transiteront par tous les composants dont l'attribut Emplacement est égal à Paris. Si vous définissez un filtre de transaction pour l'emplacement Paris, la carte affiche tous les composants des transactions qui transitent par les noeuds Paris.

NOTE

Les chemins de transaction proviennent du noeud d'expérience, qui constitue le premier composant frontal surveillé ainsi que le début du chemin de transaction. Un noeud d'expérience contient un attribut supplémentaire appelé Experience. Si une transaction est dérivée à un moment, les filtres de chemin de transaction identifient tous les composants de cette transaction. Les filtres de chemin de transaction identifient également les branches, indépendamment de l'emplacement de l'attribut spécifié dans la transaction.

Procédez comme suit :

1. Cliquez sur **Ajouter un filtre**, ajoutez des critères de filtre, puis sélectionnez **Suivre le chemin de la transaction**.
2. (Facultatif) Activez la case à cocher **Inclure le noeud d'expérience**. Le noeud d'expérience est le premier composant frontal surveillé et le début du chemin de la transaction. L'attribut Expérience des filtres contient le noeud d'expérience, y compris tous les autres noeuds du chemin de transaction. Si vous sélectionnez l'option **Inclure le noeud d'expérience**, vous ajoutez tous les noeuds d'expérience qui utilisent les noeuds filtrés.

TIP

Vous pouvez supprimer manuellement des noeuds spécifiques. Affectez un attribut personnalisé au noeud, puis filtrez cet attribut.

Vous définissez un filtre de chemin de transaction.

Création d'un groupe de filtres**Procédez comme suit :**

1. Cliquez sur l'icône plus située près d'un filtre.
Une liste déroulante de noms d'attribut s'affiche.
2. (Facultatif) Sélectionnez l'option **Suivre le chemin de transaction**.
3. Sélectionnez un nom d'attribut à appliquer comme filtre.

NOTE

Les attributs sont répertoriés sous la couche correspondante.

4. Cliquez sur l'icône plus à nouveau. Sélectionnez **Ajouter un groupe de filtres**, puis sélectionnez un nom d'attribut à appliquer comme filtre.
5. Cliquez sur la liste déroulante de condition de filtre et effacez les valeurs d'attribut que le filtre doit supprimer.
Les icônes de statut en regard des valeurs de filtre indiquent le statut d'intégrité des composants associés en mode dynamique uniquement.
6. (Facultatif) Ajoutez d'autres critères de filtre. Cliquez sur l'icône plus dans le cadre bleu et ajoutez d'autres noms d'attributs à la condition de filtre de chemin de transaction.

Vous avez créé un groupe de filtres.

TIP

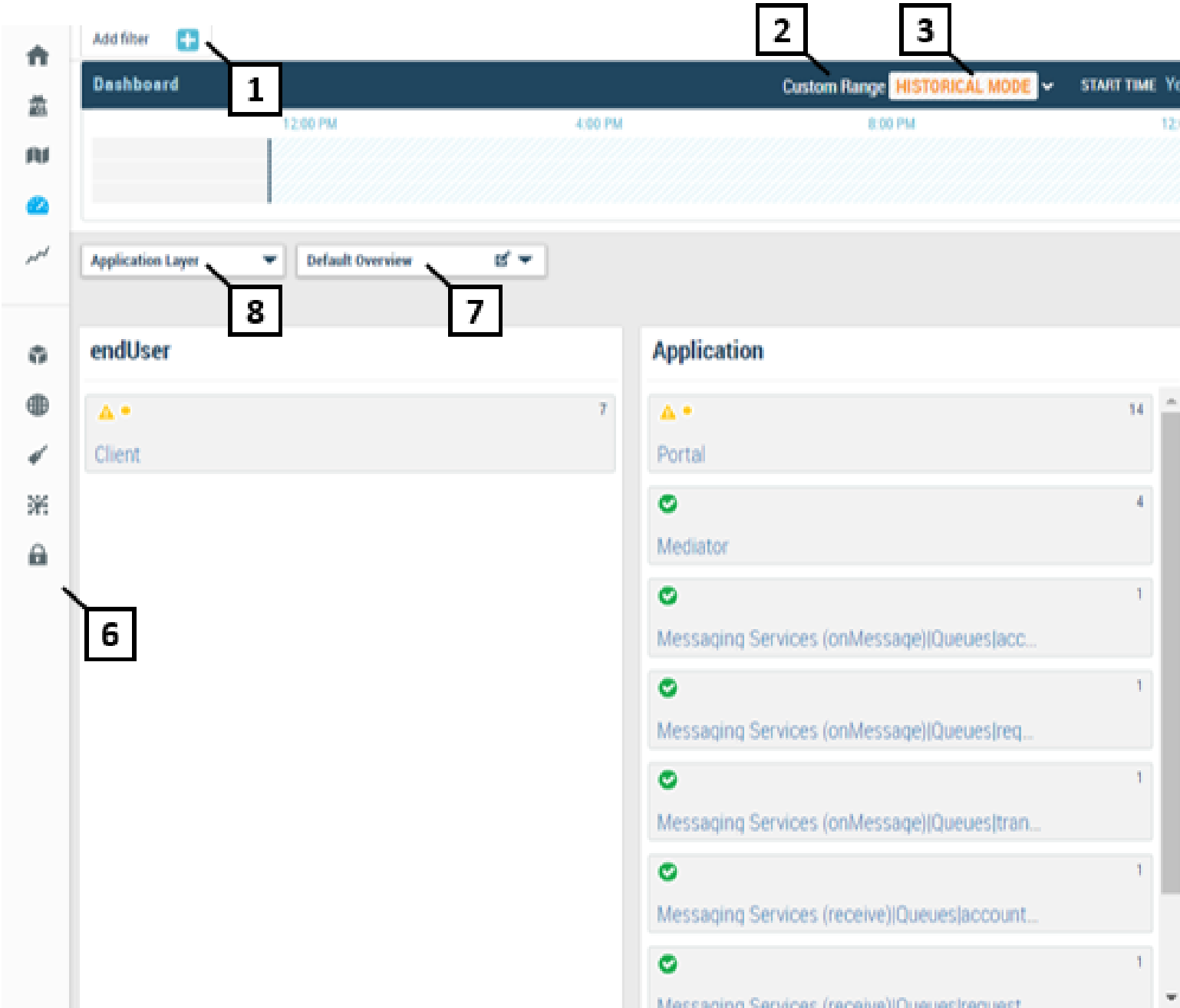
Si vous modifiez le groupe de filtres ultérieurement, enregistrez d'abord l'URL. Vous pouvez utiliser l'URL pour rétablir les paramètres précédents du groupe de filtres.

Surveillance de l'intégrité globale de l'environnement à l'aide du tableau de bord

DX APM fournit une vue d'ensemble d'un environnement d'application. Le tableau de bord montre l'intégrité globale de l'environnement. Une vignette correspond à un groupe rassemblant tous les composants qui partagent un nom et une valeur d'attribut. Les vignettes affichent l'analyse différentielle et le statut d'alerte les plus pertinents de tous les composants du groupe.

Présentation

Les vignettes du tableau de bord sont organisées en colonnes. Chaque colonne représente un attribut de la perspective sélectionnée. Le nom de l'attribut est indiqué dans l'en-tête de la colonne. Chaque vignette figurant dans une colonne affiche l'état de tous les composants présentant une valeur d'attribut spécifique.



La légende suivante identifie chaque élément de la carte par un numéro et fournit des informations complémentaires :

Numéro	Name (nom)	Informations complémentaires
1	Filtre	
2	Plage horaire	Cliquez pour sélectionner une plage horaire personnalisée ou prédéfinie.
3	Mode Chronologie (historique ou dynamique)	

4	Développer ou réduire la chronologie	Sélectionnez Statut , Topologique ou Attribut pour afficher les événements de changement dans la chronologie. Remarque : Par défaut, la chronologie est chargée sans sélection d'événements de changement.
5	Lien vers l'Aide en ligne	
6	Panneau de navigation	
7	Perspectives	Une perspective regroupe les composants de manière logique et repose sur les attributs partagés.
8	Couches	Les couches montrent les composants correspondant aux vues de CA Application Performance Management, par exemple, les vues Agent et Expérience.
9	Statut de l'alerte	Les alertes indiquent l'état de tous les composants du groupe. L'intensité de l'alerte dans le tableau de bord reflète l'intensité de l'état d'alerte. L'état d'alerte dépend des informations supplémentaires provenant du système d'alerte, notamment de la durée pendant laquelle le noeud est affecté et de la mesure dans laquelle les mesures associées dépassent les seuils limites. L'échelle d'alerte compte 5 niveaux, allant de faible à élevé. Lorsqu'aucun niveau n'est spécifié, cela signifie que les données disponibles ne sont pas suffisantes pour tirer une conclusion.
10	Vignette	Les vignettes présentes dans le tableau de bord correspondent à des groupes de composants qui partagent un nom et une valeur d'attribut. Chaque vignette affiche l'analyse différentielle et les résultats d'alerte les plus pertinents de tous les composants du groupe. La valeur d'attribut correspond à l'en-tête de la vignette. Cet en-tête est un lien cliquable. Cliquez sur ce lien pour afficher ce groupe sur la carte.
11	Nombre de vignettes figurant dans ce groupe	

Affichage des couches dans le tableau de bord

Les couches permettent d'appliquer au tableau de bord les vues CA Application Performance Management standard, par exemple, les vues Agent et Expérience. Le tableau de bord vous permet de basculer entre les couches suivantes :

- **Couche Application**
Affiche les composants dans la carte. Les composants correspondent aux fiches d'expérience dans la vue Expérience.
- **Couche APM Infrastructure**
Affiche les gestionnaires d'entreprise et les agents dans le tableau de bord. Cette couche correspond à la vue Agents.
- **Couche Infrastructure**
Affiche l'infrastructure réseau de votre environnement, y compris les moniteurs Docker Monitor.

Affichage des perspectives dans le tableau de bord

Une perspective est un moyen de grouper des composants dans les vues CA Application Performance Management sur la base de leurs attributs partagés. Les perspectives permettent de grouper des composants dans le tableau de bord sans les supprimer de l'ensemble de données. Pour obtenir des informations complémentaires sur les perspectives, consultez [Organisation des composants à l'aide de perspectives](#).

DX Application Performance Management fournit un aperçu d'un environnement d'application. Le tableau de bord montre l'intégrité globale de l'environnement. Une vignette correspond à un groupe rassemblant tous les composants qui partagent un nom et une valeur d'attribut. Les vignettes affichent l'analyse différentielle et le statut d'alerte les plus pertinents de tous les composants du groupe.

Pour plus d'informations sur le tableau de bord, reportez-vous à la section [Surveillance de l'intégrité globale de l'environnement à l'aide du tableau de bord](#).

Surveillance des problèmes et anomalies relatifs au triage assisté

Des informations sur les événements intéressants apparaissent sous la forme de problèmes et d'anomalies (stories) dans la vue Expérience ou le carnet d'analyse. La vue Expérience est un composant de l'environnement à partir duquel une transaction commence. Le triage assisté collecte des preuves pour détecter les problèmes ou les problèmes potentiels de votre environnement. La collecte de preuves peut se trouver au début du processus et les preuves ne pointent pas encore vers une affectation de l'expérience. Ce type de preuve est appelée une *anomalie*. Lorsque le triage assisté a suffisamment d'informations pour identifier les expériences affectées, ce type de preuve est appelé un *problème*. Les anomalies sont semblables aux problèmes, mais elles n'affectent pas encore l'expérience utilisateur.

La vue Expérience ou le carnet d'analyse fournissent des emplacements pratiques permettant de surveiller l'intégralité du système. Dans votre application, plusieurs événements différents se produisent en permanence, mais la plupart ne vous intéressent pas. La fonctionnalité de triage assisté vous permet d'identifier et de hiérarchiser les problèmes en signalant les événements importants dans le système de l'application. Ces événements importants s'affichent sous forme de stories accompagnées de titres dans la vue Expérience ou le carnet d'analyse et expliquent les aspects suivants :

- Quel est le problème potentiel ?
- Qui est affecté par le problème ?
- Qui peut être affecté par le problème (potentiel) ?
- Quels sont les composants concernés par le problème ?
- Quels types d'événements se sont produits pour les composants concernés par le problème ?
- Quand le problème a-t-il commencé et s'est-il terminé ?

Comme pour un journal, vous pouvez consulter les titres régulièrement au cours de la journée. Le niveau d'intérêt d'une expérience est directement lié à vos responsabilités d'analyste. Par exemple, un des cas suivants peut indiquer qu'un problème ou une anomalie requiert votre attention :

- La portée de l'impact client est grave. Le triage assisté évalue souvent l'impact à l'aide des informations QUI.
- La portée de l'impact client n'est pas spécifiée ou l'expérience est mal définie. Par exemple, si les informations OU indiquent une application ou une transaction clé, vous devrez peut-être obtenir davantage d'informations.

Procédez comme suit :

1. Cliquez sur le bouton **Vue Expérience**.
La vue Expérience affiche les fiches d'expérience individuelles. Chaque fiche affiche un récapitulatif. Ce récapitulatif représente l'aspect QUOI et explique le POURQUOI. Les éléments en rouge indiquent les points importants, tels que les échecs de transaction.
2. Accédez à la page et cliquez sur l'icône **Ouvrir un carnet d'analyse** sur une fiche de votre choix. Les problèmes et les anomalies apparaissent dans le panneau du triage assisté. Le moteur de triage assisté identifie les transactions qui partagent des composants fonctionnant mal.

NOTE

Lorsque vous explorez une fiche d'expérience en passant d'une vue à l'autre, les stories du tri assisté peuvent modifier les problèmes en anomalies. Une transaction métier peut indiquer un problème et zéro anomalie. Lorsque vous analysez en profondeur une fiche d'expérience, une nouvelle fiche peut afficher zéro problème et une anomalie.

Ce comportement se produit, car une story du triage assisté peut être un problème pour des transactions métier et une anomalie pour d'autres. L'une des transactions métier qui présente un problème masque les autres transactions métier pour les afficher comme des anomalies. Lorsque vous analysez en profondeur une transaction organisationnelle, l'anomalie masquée dans la vue précédente est désormais visible.

3. Parcourez le volet et consultez les détails concernant un problème ou une anomalie qui vous intéresse. Cliquez sur **Ouvrir** près d'un problème ou d'une anomalie.
Le flux de relation affiche les chemins de transaction des expériences sélectionnées. Cette carte fournit le contexte de l'événement qui s'est produit, notamment les informations d'emplacement. CA APM affiche *uniquement* le sous-ensemble de la carte globale de l'application où se situe le problème ou l'anomalie. Par exemple, la durée du problème et les composants affectés. Le responsable s'affiche dans le panneau Assisted Triage (Tri assisté) et dans la carte.

TIP

Utilisez la liste déroulante **Perspective** et créez ou sélectionnez une perspective. Vous pouvez utiliser les perspectives pour regrouper des composants en fonction de leurs attributs partagés.

La carte Relationship Flow (Flux de relation) réduit la vue.

4. Dans le panneau Assisted Triage (Tri assisté), développez **Durée**, **Expériences affectées** ou **Composants de l'application** et recherchez la cause première du problème. Cliquez sur **Ouvrir** pour afficher les données probantes de contribution.
5. [Continuez vos recherches à l'aide des différentes options dans le carnet d'analyse.](#)

Tri assisté et analystes

La fonctionnalité de tri assisté est un moteur et un générateur de stories. Elle identifie les événements les plus significatifs qui se sont produits dans vos systèmes et fournit des informations contextualisées (stories) sur ces événements. Ces stories sont présentées sous la forme de problèmes et d'anomalies avec des titres. La nature fiable et intelligente des stories générées par le tri assisté vous maintient informé de l'état de votre domaine de surveillance.

Fonctionnement du tri assisté

La fonctionnalité de tri assisté crée des problèmes et des anomalies relatifs aux événements de votre système. Elle réagit aux types d'événements suivants :

- Blocages
- Errors
- Alertes
- Temps de réponse instables

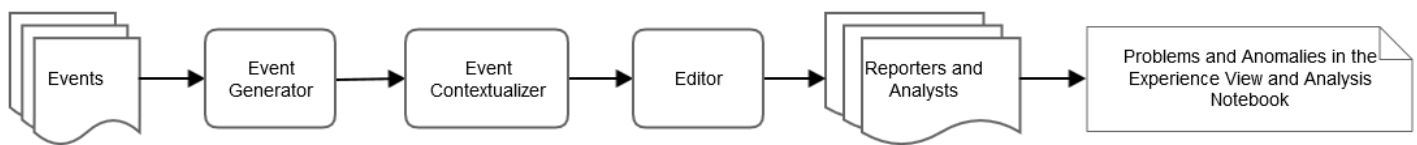
Les problèmes et les anomalies décrivent les aspects d'un ou de plusieurs événements. Par exemple, les aspects incluent notamment :

- **QUOI** : résume l'événement, y compris les causes suspectées (**POURQUOI**). Ces informations s'affichent sous la forme d'un titre pour un problème ou une anomalie dans la vue Expérience et le bloc-notes d'analyse.
- **OU** : identifie une occurrence d'événement. En général, des informations telles que le nom d'hôte et d'agent. OU peut comprendre d'autres informations lorsqu'elles sont disponibles.
- **QUI** : identifie les transactions affectées ou susceptibles de l'être. Cet aspect détermine également le nombre de transactions affectées.
- **QUAND** : enregistre une occurrence d'événement. En général, le début et la fin d'un événement de blocage, d'erreur ou d'instabilité.
- **POURQUOI** : décrit une occurrence d'événement. Par exemple, l'instruction suivante indique un problème de taux d'appels élevé :

```
Potential high call ratio from ViewOrders|service to 138.0.0.1_7080|getService 2 in the order of 214980
```

Le diagramme suivant et les étapes correspondantes décrivent le fonctionnement du tri assisté :

Figure 7: Architecture de tri assisté



1. Les événements du système APM se produisent sous la forme d'intensité d'écart, d'erreurs, de blocages, d'alertes APM, etc. Un événement contient un suspect potentiel à l'origine du problème.
2. Un générateur d'événements collecte les données d'événement de différentes sources et les envoie au processeur d'événements.
3. L'outil de contextualisation d'événement reçoit les événements des générateurs d'un cluster, les traite, puis réunit tous les événements associés dans un contexte. Les informations de contexte incluent l'impact potentiel du composant le plus à gauche et toutes les transactions effectuées sur le composant. L'outil de contextualisation transfère ces informations de contexte à l'éditeur.
4. L'éditeur assure le suivi des différents contextes et affecte un générateur de rapports par contexte d'événement spécifique pour une analyse plus approfondie.
5. Les générateurs de rapports connaissent les différents types d'analystes disponibles dans le système et leur envoient le contexte pour analyse. Les analystes analysent le contexte, recherchent les types d'événements, les schémas et déterminent l'impact potentiel, puis chaque analyste crée une instruction. Les analystes collaborent pour enregistrer des preuves ou créer des stories à partir des instructions, puis stockent les données dans la base de données APM. Les stories sont purgées de la base de données lorsqu'elles dépassent 62 jours.
6. Les stories s'affichent sous la forme de problèmes ou d'anomalies dans la vue Expérience et le bloc-notes d'analyse.

NOTE

Le gestionnaire d'entreprise génère et collecte les mesures relatives aux composants du tri assisté. Ces mesures de prise en charge sont utiles pour évaluer l'intégrité du gestionnaire d'entreprise.

Analystes

Les analystes peuvent être comparés à des spécialistes en médecine qui savent diagnostiquer les différentes maladies. Le tri assisté utilise les types principaux d'analystes suivants. Chaque type d'analyste inclut des analystes spécifiques.

Les *analystes d'événements* recherchent certains types d'événement et créent des instructions qui servent de preuves. Exemples d'analystes d'événements :

- Un analyste différentiel recherche l'intensité d'écart.
- Un analyste d'erreur recherche des événements d'erreur dans les contextes.
- Un analyste d'événements de ressource surveille les événements d'alerte sur les ressources système.

Les *analystes de modèles* recherchent des modèles dans le contexte et créent des instructions de modèle. Ces instructions constituent une partie d'un récapitulatif de story. Exemples d'analystes de modèles :

- Un analyste par défaut détermine le composant le plus complet dans un contexte (selon le mappage des relations). L'analyste par défaut est également appelé Identificateur de zone.
- Un analyste de taux d'appels élevé recherche le composant le plus complet dans le contexte donné (selon le mappage des relations). Il détermine si le composant appelle les noeuds d'arrière-plan un nombre inhabituel de fois.

Les instructions des analystes constituent un récapitulatif de story.

Exemple de story : analyste par défaut (identificateur de zone)

Cet exemple présente une story d'analyste par défaut (identificateur de zone). Cet analyste est toujours en fonctionnement, même si d'autres analystes spécifiques identifient des modèles. L'analyste par défaut identifie une zone probable. La zone peut être un serveur frontal, un serveur d'arrière-plan ou un composant interne entre eux. Par exemple, une instruction de l'analyste par défaut ressemble au titre suivant :

```
Problem isolated to {type} {component}
```

{type} peut être un serveur frontal, une transaction métier, un composant interne ou un serveur d'arrière-plan.

{component} est le nom du composant impliqué dans la zone.

Par exemple, considérez les composants suivants dans le système :

- Serveur frontal F
- Serveur d'arrière-plan B
- Composant interne M

Tous ces composants sont liés par la transaction métier F-> M-> B.

La séquence d'événements suivante se produit dans le flux de transactions :

1. Des événements qui correspondent uniquement au serveur frontal F se produisent.
La story d'analyste par défaut signale un événement isolé sur le serveur frontal F.
2. Un événement se produit pour le composant interne M.
L'analyste par défaut associe ces deux événements, car ils se trouvent dans le même flux de transactions. L'analyste indique : Problème isolé sur le composant interne M.
3. Un événement se produit pour le serveur d'arrière-plan B.
L'analyste par défaut regroupe les trois événements et indique : Problème isolé sur le serveur d'arrière-plan B.

Dans les anomalies et les problèmes de la vue Expérience et du bloc-notes d'analyse, recherchez un titre incluant le type de composant, par exemple :

```
Problem isolated to internal component AxisServlet|service
```

Ce titre décrit une story d'analyste par défaut. Par exemple, les détails peuvent décrire un problème dans la zone entre les transactions du serveur frontal et du serveur d'arrière-plan pour l'application ACME.

Exemple de story : Taux d'appels élevé

Cet exemple explique comment la fonctionnalité de tri assisté signale une story de taux d'appels élevé. Une story de taux d'appels élevé se produit lorsqu'un composant client envoie un trop grand nombre de transactions, entraînant le ralentissement de la transaction sous-jacente qui l'a initialisé. Autrement dit, lorsque le taux appelant/appelé équivaut à une valeur faible pour l'appelant et à un nombre élevé pour l'appelé (par exemple, 1:20). Ce nombre indique qu'un appel à l'appelant entraîne 20 appels à l'appelé. L'analyste de modèles signale des stories de taux d'appels élevé pour les noeuds/composants de serveur d'arrière-plan, tels que des bases de données ou des clients de services Web.

Les symptômes suivants peuvent indiquer un problème de taux d'appels élevé :

- La latence est élevée avant un composant dans la pile d'appels, mais la latence du composant est faible, ce qui indique un taux d'appels élevé pour le composant, ou avant le composant.
- Transactions à latence élevée avec modèles de type code à barres : un composant A appelle un composant B à plusieurs reprises dans un court intervalle. Ce comportement entraîne une latence normale pour le composant B, mais une latence élevée pour le composant A.

Dans les anomalies et les problèmes de la vue Expérience et du bloc-notes d'analyse, identifiez un titre de taux d'appels élevé. Par exemple, les anomalies et les problèmes présentent le titre suivant :

```
Potential high call ratio from {culprit.name} to {calledComp.name} in the order of {ratio}
```

Ce titre décrit une story de taux d'appels élevé. Par exemple, les détails peuvent décrire un problème de latence pour la connexion client à une base de données à New York.

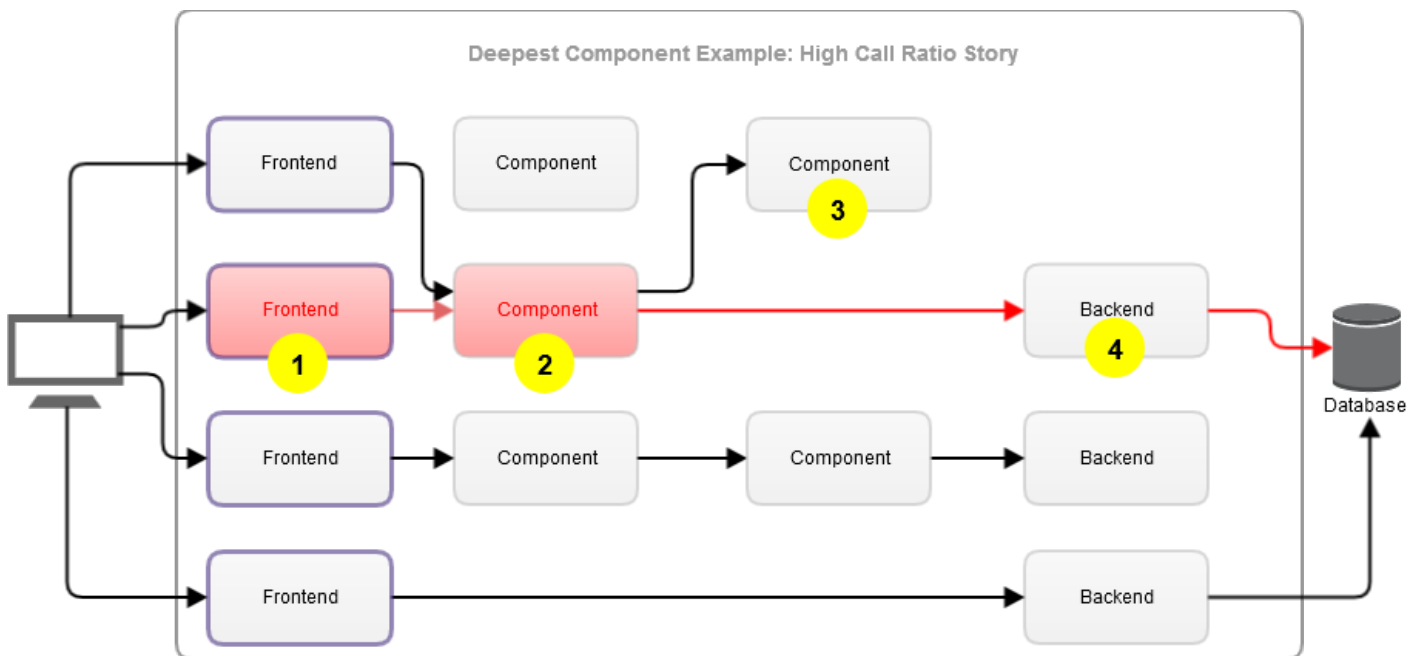
Exemple : procédure permettant à un analyste de déterminer le composant le plus complet d'une story de taux d'appels élevé

L'exemple suivant présente la procédure que suit un analyste de modèles pour rechercher le composant le plus complet dans une story de taux d'appels élevé :

1. L'analyse différentielle a déclenché une alerte : une transaction est ralentie et fait dorénavant partie d'une story.
2. Un événement s'est produit sur le chemin d'appel à partir de la transaction. L'analyste recherche le composant le plus complet dans le contexte.
3. Un composant est une impasse, car il n'appelle aucun serveur d'arrière-plan. L'analyste l'ignore.
4. Un composant appelle un serveur d'arrière-plan. A l'aide des données historiques, l'analyste compare le nombre de réponses par intervalle dans le composant appelant au nombre de réponses par intervalle pour les appels aux serveur d'arrière-plan. Si le taux d'appels de la transaction est élevé (par exemple, supérieur à 1:50), il est anormalement élevé et pourrait affecter les performances de l'application.

D'autres composants peuvent également avoir un taux d'appels élevé à la base de données. L'analyste diagnostique uniquement le taux élevé lorsque des composants se trouvent sur le chemin d'appel d'un serveur frontal. L'analyste n'est pas concerné par l'application entière, mais se concentre plutôt sur une story identifiée.

Figure 8: Exemple de composant le plus complet : story Taux d'appels élevé



Prise en charge de l'analyste des événements de ressource

La fonctionnalité de tri assisté utilise un analyste d'événements de ressource pour surveiller les alertes au niveau des événements de ressource, tels que ceux relatifs à l'UC et à la mémoire, comme suit :

1. Une application rencontre des problèmes de ressources système.
2. Les événements de ressource sont répertoriés comme suspects pour le problème ou l'anomalie.
3. Un composant de ressource/d'infrastructure est identifié comme responsable potentiel.

Les analystes de ressources prennent en charge les agents pour DX APM et l'agent DX APM Infrastructure. Le tri assisté fournit le contexte pour les informations d'infrastructure signalées par l'agent Infrastructure pour une application. Les alertes qui sont déclenchées sur des composants de l'infrastructure sont intégrées à des stories de tri assisté (preuves). Exemple :

1. L'exécution d'une UC est élevée sur un serveur, ce qui provoque peut-être un ralentissement de l'application.
2. L'agent Infrastructure signale ce problème.
3. Le tri assisté associe ce problème de ressource à l'application et au composant d'infrastructure concernés.
4. Le composant d'infrastructure est répertorié comme responsable potentiel au niveau de l'infrastructure.

NOTE

Les étapes préalables suivantes sont requises au niveau de l'analyste d'événements de ressource :

1. Vérifiez que la fonction de surveillance de l'agent DX APM Infrastructure est activée et que les alertes sont mappées vers les composants d'infrastructure.
2. Dans la vue Carte, sélectionnez **Couche applicative** pour afficher les composants d'application.
3. Dans la carte, cliquez sur un composant d'application.
Des valeurs de corrélation doivent exister et inclure le composant d'infrastructure correspondant.

Informations complémentaires :

[Couches de carte](#)

[Agent Infrastructure](#)

Examen des performances médiocres des transactions

Les données de mesure, comme le temps de réponse moyen d'un composant important, peuvent vous informer sur l'expérience des clients qui utilisent ce composant. Toutefois, ces données ne permettent pas de comprendre les causes de performances anormalement lentes. En cas de transactions lentes, un suivi des transactions peut être l'équivalent d'une radiographie par rayons x, car il permet d'afficher les détails qui ne sont pas visibles de la surface et de déterminer le temps passé à chaque étape de la transaction de manière détaillée. Application Performance Management (auparavant Wily Introscope) est un pionnier du suivi de transaction permettant une visibilité approfondie des transactions. Le suivi de transaction permet de surveiller l'activité de chaque transaction lorsqu'elles circulent sur les applications surveillées par l'agent. Les données de mesure vous informe de l'existence d'un goulot d'étranglement dans le trafic, alors que le suivi de transaction peut vous informer de l'expérience d'une seule transaction : où elle a été retardée, pendant combien de temps et éventuellement les causes du retard. Les informations de suivi de transaction sont stockées afin que vous puissiez les consulter plusieurs heures ou jours après leur première occurrence.

Recherche de suivis de transactions lentes ou ayant échoué

En tant qu'analyste, la **vue Expérience** vous fournit des suivis de transaction utiles à examiner. Dans l'onglet **Transactions métier**, vous pouvez consulter les récapitulatifs et les détails des traces de transactions. Ces informations permettent de comprendre les performances des transactions et de résoudre les problèmes de performances en identifiant quand, où et pourquoi les performances se détériorent.

Procédez comme suit :

1. Dans le volet gauche, cliquez sur **Vue Expérience**.

La vue Expérience affiche les fiches d'expérience individuelles. Chaque fiche affiche un récapitulatif. Les éléments en rouge indiquent des transactions lentes ou ayant échoué.

NOTE

Pour plus d'informations sur la vue Expérience, reportez-vous à la section [Surveillance des performances à l'aide de la vue Expérience](#).

TIP

Vous pouvez également démarrer votre enquête à partir de la carte. Dans le volet gauche, cliquez sur **Carte** et ignorez l'étape suivante.

2. Parcourez les fiches et cliquez sur l'icône de **carnet** au niveau de la fiche de votre choix.

Le carnet d'analyse indique des détails concernant l'expérience.

3. Dans le volet **PROBLEMES**, cliquez sur **Ouvrir** près d'un problème qui vous intéresse.

- Un cercle rouge indique que le composant joue un rôle dans au moins un problème ou une anomalie. Tous les composants d'une story sont traités comme des acteurs.

- Un cercle concentrique rouge indique que le composant est responsable d'au moins un problème ou une anomalie. Tous les acteurs sont impliqués, mais un responsable est considéré comme un acteur spécial. Le responsable correspond à la cause première du problème ou de l'anomalie au niveau de l'application ou de la transaction en question.

Ce composant peut être à l'origine de la détérioration des performances dans votre environnement d'application.

Le flux de relation affiche les chemins de transaction des expériences sélectionnées. Cette carte fournit le contexte de l'événement qui s'est produit.

4. Cliquez sur des noeuds spécifiques ou des groupes de 1 000 noeuds maximum. Sélectionnez la **couche applicative** ou la **couche d'infrastructure APM** dans la carte pour afficher tous les suivis collectés par hôte, agent ou application. Le graphique **Présentation du composant** apparaît et affiche les transactions saines et médiocres.

Pour accéder à l'Aide du graphique de composant, cliquez ici...

Le graphique de composant affiche un maximum de 20 noeuds. Utilisez les graphiques de composant pour comparer les mesures en temps réel ou historiques entre des noeuds arbitraires. Le graphique de composant contient plus d'informations de mesures que celles disponibles pour chaque composant dans la carte. Utilisez les options de commutateur (points) en bas du graphique pour afficher les informations suivantes.

- Histogramme Temps de réponse : l'histogramme affiche le temps de réponse moyen agrégé par seconde pour les transactions saines et médiocres. L'histogramme vous permet de comparer les données et identifier les tendances facilement, par exemple, l'augmentation ou la réduction du nombre de suivis.
- Graphique sparkline Temps de réponse moyen : le graphique sparkline indique la forme générale de la variation dans le temps des mesures BlamePoint d'un composant. Le graphique sparkline affiche des informations pour la période active sélectionnée dans la chronologie. Passez le curseur sur n'importe quel point du graphique sparkline pour afficher une valeur numérique.
- Graphique Volume de transactions : le graphique à barres permet de déterminer rapidement le niveau de volume des transactions. Les barres facilitent également l'identification des tendances de volume.

Le composant est mis en surbrillance dans le volet **AFFECTED APPLICATION COMPONENTS** (Composants d'application concernés).

5. Cliquez sur l'onglet **Transactions métier**.

Une liste récapitulative affiche les informations de suivi qui correspondent au composant pour la période sélectionnée dans la chronologie. Les traces des composants inférés sont répertoriées, bien que ces transactions ne soient pas surveillées par des agents. Par exemple, les composants inférés peuvent être des composants d'arrière-plan, des services Web ou des sockets. Les traces affichent la durée et présentent un code couleur. Chaque couleur indique une caractéristique associée à une transaction ; par exemple, le rouge indique une erreur. Vous pouvez identifier

les méthodes problématiques en notant la durée du suivi. Les opérations de suivi anormalement longues sont probablement la cause des transactions lentes.

NOTE

La liste est actualisée automatiquement lorsque vous utilisez le mode Dynamique.

La liste affiche les informations de suivi suivantes pour 2 000 traces maximum.

URL : URL appelée pour lancer la transaction ou chemin d'accès au composant qui a initialisé la transaction.

Nom : nom du composant de haut niveau, par exemple : Valeur par défaut.

Horodatage : heure de début, selon l'horloge système de l'hôte de l'agent, de l'appel du composant sélectionné.

Durée : Durée d'exécution (en millisecondes) du composant sélectionné


Type de trace : type de trace (Autre, Erreur ou Cliché).

ID d'utilisateur : ID de l'utilisateur connecté qui exécute la transaction.

Ces informations vous aident à comprendre la séquence des appels dans une période et à évaluer les performances.

Remarque : Toutes les informations sur les composants de visibilité approfondie ne sont pas disponibles.

6. Effectuez une ou plusieurs actions :

- Cliquez sur le **bouton contextuel**  pour ouvrir la visionneuse dans une boîte de dialogue de vue complète. Appuyez sur **Echap** pour fermer la boîte de dialogue.

- Sélectionnez une option dans la liste déroulante **Type de trace** pour classer les informations de suivi par caractéristiques. Un suivi peut avoir plusieurs caractéristiques :

Autre : renvoie tous les suivis de transaction autres que les suivis avec des erreurs ou des blocages. La couleur orange clair



indique qu'une analyse différentielle a déclenché une alerte : une transaction comporte un écart non contrôlé.

Erreur : renvoie les suivis de transaction avec une caractéristique d'erreur. Une erreur est une exception signalée par les codes d'erreur JVM ou HTTP. Elles incluent par exemple, un statut d'erreur HTTP, une exception SQL ou une exception Java. Si le type de suivi est Normal, mais qu'une erreur déclenche un suivi de transaction automatique, le composant est indiqué comme une erreur et il est inclus dans le nombre total d'erreurs.

Les traces de transaction comportant un message d'erreur de type `Transaction bloquée` sont également renvoyées. Un blocage est une transaction, ou un composant d'une transaction, qui ne s'est pas terminée dans les délais impartis.

Cliché : renvoie toutes les transactions qui comportent des clichés.

- Cliquez sur un **en-tête de colonne**.

La liste trie les suivis par type de colonne, par exemple, par ID d'utilisateur. Il n'est pas possible de trier le type de trace en cliquant sur l'en-tête de colonne.

Remarque : L'ID d'utilisateur est l'identification de l'utilisateur connecté qui exécute la transaction (si ce champ configuré et que l'ID est disponible).

7. Examinez les différents composants et les données de suivi. Vous pouvez consulter la séquence d'appel et examiner le code pour déterminer la cause d'un problème.

Informations complémentaires :

[Utilisation du suivi des transactions interprocessus pour résoudre des problèmes](#)

[Démarrage d'une session de suivi de transaction](#)

[Examen des différents composants et des données de suivi](#)

[Diagnostic des problèmes de chargement des ressources](#)

[Diagnostic des problèmes de performance système](#)

[Détection et analyse d'erreurs et de blocages](#)

[Analyse des clichés d'erreur et de blocage](#)

[Analyse des données de suivi et collaboration pour l'analyse des problèmes](#)

Utilisation du suivi des transactions interprocessus pour résoudre des problèmes

Souvent, les transactions passent par plusieurs machines virtuelles Java, CLR, instances Node.js ou services d'application, en fonction de l'environnement. Le traitement passe par n'importe quelle combinaison de machine virtuelle Java, CLR, instance Node.js ou serveur d'applications à une autre. L'identification du chemin complet d'une transaction nécessite de tracer les appels synchrones et asynchrones à travers différentes instances de machine virtuelle Java, CLR ou Node.js. Pour pouvoir tracer des transactions sur plusieurs plates-formes, l'exécution d'un agent pris en charge est parfois aussi nécessaire. Le *suivi des transactions inter-processus* identifie le chemin complet des transactions sur plusieurs plates-formes. Cette fonctionnalité vous permet de consulter des informations lorsque des transactions appellent des méthodes sur plusieurs machines virtuelles Java ou CLR s'exécutant sur différents serveurs.

NOTE

Le suivi des transactions inter-processus est pris en charge dans les traces de transaction exécutées manuellement et échantillonnées, ainsi que dans d'autres traces de transaction utilisant le filtrage d'agent.

Le suivi des transactions inter-processus dans les traces de transaction automatiques est pris en charge uniquement pour les applications Java.

Corrélation de transactions

Les applications distribuées sont complexes. En règle générale, les transactions mono-utilisateur s'étendent sur plusieurs threads exécutés sur différents CLR ou machines virtuelles Java d'agent. Souvent, une même transaction inclut à la fois des appels synchrones et asynchrones. L'agent doit également tenir compte des appels de transaction individuels pour présenter le chemin complet d'une transaction comme une unité logique.

Les transactions se composent généralement d'une série d'appels et de réponses transmis d'un processus à un autre. Souvent, plusieurs processus d'une même transaction appellent différents serveurs logiques ou physiques. Les processus peuvent également être distribués de manière à s'exécuter sur différents composants ou systèmes d'arrière-plan. L'assemblage d'une transaction complète nécessite un agent pour identifier tous les processus inclus et déterminer l'ordre des appels. L'agent requiert également des informations sur les threads, ainsi que sur les appels synchrones et asynchrones.

Pour pouvoir tracer le chemin complet d'une transaction incluant des appels inter-processus, l'agent doit connecter les processus de manière logique. L'agent utilise un *identificateur de corrélation* (ID de corrélation), qui met en corrélation, ou crée une vue connectée, des processus. L'agent effectue la connexion en insérant l'identificateur de corrélation dans la transaction. L'identificateur de corrélation peut être transmis d'un processus à un autre. Cette association de processus permet à l'agent d'identifier les composants frontaux et d'arrière qui font partie d'une même transaction. Dans la section **Détails du composant** de la visionneuse des traces de transaction, l'ID de corrélation est la valeur de la propriété Données multiprocessus.

Pour pouvoir assembler une transaction complète, un agent doit également déterminer à quel moment un processus d'une transaction en appelle un autre. Vous pouvez voir l'ordre dans lequel les composants frontaux et d'arrière-plan s'appellent dans une transaction. Pour les transactions synchrones, l'ordre peut aider à identifier les relations appelant-appelé. Pour les transactions asynchrones, l'ordre peut aider à identifier un flux de travaux sur plusieurs processus pour des segments de transaction client et serveur complexes. La combinaison de l'identificateur de corrélation et de l'ordre des appels fournit une *trace de transaction corrélée* ou *trace corrélée*.

Le suivi des transactions inter-processus prend également en charge les corrélations multi-threads au sein du même processus.

L'agent gère automatiquement l'ensemble de données de l'identificateur de corrélations et transmet les informations au gestionnaire d'entreprise. Le gestionnaire d'entreprise génère la représentation graphique des transactions sélectionnées qu'affiche la visionneuse des traces de transaction.

Utilisation du traçage des transactions pour résoudre des problèmes

Le processus ci-dessous explique comment vous pouvez examiner des transactions dans la visionneuse des traces de transaction, afin d'identifier la cause première de certains problèmes.

1. Lorsque la visionneuse des traces de transaction affiche une pile graphique, l'agent a tracé les processus connexes dans un événement de trace sélectionné. Les processus qui font l'objet d'un suivi par différents agents s'affichent dans différentes zones grisées.
2. Vous pouvez examiner les composants liés pour visualiser les transactions inter-processus ou inter-machines virtuelles Java. Par exemple, vous pouvez vérifier si une transaction donnée a quitté un processus, puis en a intégré un autre.
3. Vous pouvez également déterminer les appels qui sont à l'origine de transactions lentes et bloquées.

Exemple de traçage de transactions inter-processus

Cet exemple décrit comment le suivi des transactions inter-processus peut vous aider à identifier et évaluer les problèmes rapidement et efficacement.

1. Vous examinez la trace d'une transaction problématique et remarquez un temps d'exécution de 6 secondes (6 000 ms).
2. Dans la pile graphique, vous constatez des appels d'une méthode côté client, `dataservice.yourcompany.net/invoke`, à une méthode côté serveur, `thirdparty.mycompany.net/invoke`.
3. Vous remarquez que le service Web côté serveur passe un grand nombre d'appels à un service Web tiers. Etant donné que service Web tiers est non instrumenté, son temps d'exécution n'apparaît pas explicitement dans la trace.
4. La pile graphique montre que le composant d'arrière-plan du service Web tiers traite des demandes répétées qui se succèdent rapidement. Ce comportement indique que la logique de programmation, par exemple une boucle imbriquée, est probablement la cause des appels répétés au niveau du service côté serveur. Vous avez déterminé que l'opération d'appel côté serveur est responsable de la majorité du temps d'exécution globale des transactions.
5. Fort de ces informations, vous contactez le propriétaire de l'application du service Web côté serveur.
6. Le propriétaire demande une analyse de la logique applicative qui appelle le composant d'arrière-plan du service web tiers.

Démarrage d'une session de suivi de transaction

Pour exécuter une session de suivi de transaction manuellement, spécifiez les agents pour lesquels vous souhaitez effectuer le suivi des transactions et la période de capture des données. Une fois la session de suivi de transaction lancée, les transactions correspondant aux critères de filtre s'affichent dans la visionneuse des traces de transaction. Les événements de transaction incluent des traces et des erreurs de transaction.

Lorsque le suivi est lancé pendant une durée, la session s'arrête à la fin de la période spécifiée.

NOTE

Vous pouvez uniquement démarrer une session de suivi pour un agent spécifié pendant une période donnée. Si vous redémarrez une session de suivi active, une notification vous rappelle que la session de suivi de transaction est déjà active pour l'agent et affiche le temps restant dans celle-ci. Vous pouvez lancer un nouveau suivi pour le même agent après la fin d'une session de suivi active.

Par exemple : La session de suivi de transaction est actuellement active pour l'agent - Temps restant : moins d'une minute.

Vous pouvez démarrer la session de suivi de transaction sur la page Agents ou la page Vue des mesures.

Pour démarrer la session de suivi de transaction sur la page **Agents**, procédez comme suit :

1. Dans le volet gauche sous **Paramètres**, cliquez sur **Agents**.
La page Agents s'affiche et répertorie les agents.
2. (Facultatif) Cliquez sur la flèche **Applications**.
Toutes les applications surveillées par l'agent sont répertoriées.
3. Sélectionnez un ou plusieurs agents pour lesquels vous souhaitez effectuer un suivi de transactions :
 - Pour suivre tous les agents, cliquez sur **Effectuer le suivi de tous les agents**. Cette option permet d'effectuer le suivi des agents pris en charge et actuellement connectés, ainsi que des agents qui se connectent pendant la session de suivi.
 - Pour suivre des agents sélectionnés, cliquez sur **Effectuer le suivi de l'agent** pour un agent.
 La session de suivi de transaction s'affiche.
4. Spécifiez des valeurs pour le suivi de transactions dans les champs de la boîte de dialogue ou acceptez les valeurs par défaut et cliquez sur **Lancer** :
 - Spécifiez la **durée minimum des transactions** en millisecondes pour le suivi de transactions. La valeur par défaut est 1000 millisecondes. La valeur minimum est 1 milliseconde.
 - Spécifiez la **durée de la session de suivi** en minutes. La valeur par défaut est 1 minute avec une durée maximum de 5 minutes pour une session de suivi.
 Un volet affiche le statut de la session.
5. (Facultatif) Fermez la boîte de dialogue après le lancement d'un suivi. L'exécution de la session de suivi continue en arrière-plan.

Pour démarrer la session de suivi de transaction sur la page **Vue des mesures**, procédez comme suit :

1. Dans le volet gauche, cliquez sur **Vue des mesures**.
2. Dans l'onglet **Arborescence de mesures**, recherchez l'agent pour lequel vous souhaitez effectuer le suivi de transaction.
3. Cliquez avec le bouton droit de la souris sur l'agent, puis sur l'option Agent de suivi : <Nom>. La boîte de dialogue Session de suivi de transaction s'affiche.
4. Spécifiez les valeurs de la trace de transaction dans la boîte de dialogue.
 - Spécifiez la **durée minimum des transactions** en millisecondes pour le suivi de transactions. La valeur par défaut est 1000 millisecondes. La valeur minimum est 1 milliseconde.
 - Spécifiez la **durée de la session de suivi** en minutes. La valeur par défaut est 1 minute avec une durée maximum de 5 minutes pour une session de suivi.
5. Cliquez sur **Démarrer**. Le message de confirmation La session de suivi de transaction a démarré s'affiche.
6. Cliquez sur **Annuler** pour fermer la boîte de dialogue et revenir à la page **Vue des mesures**.

Examen des différents composants et des données de suivi

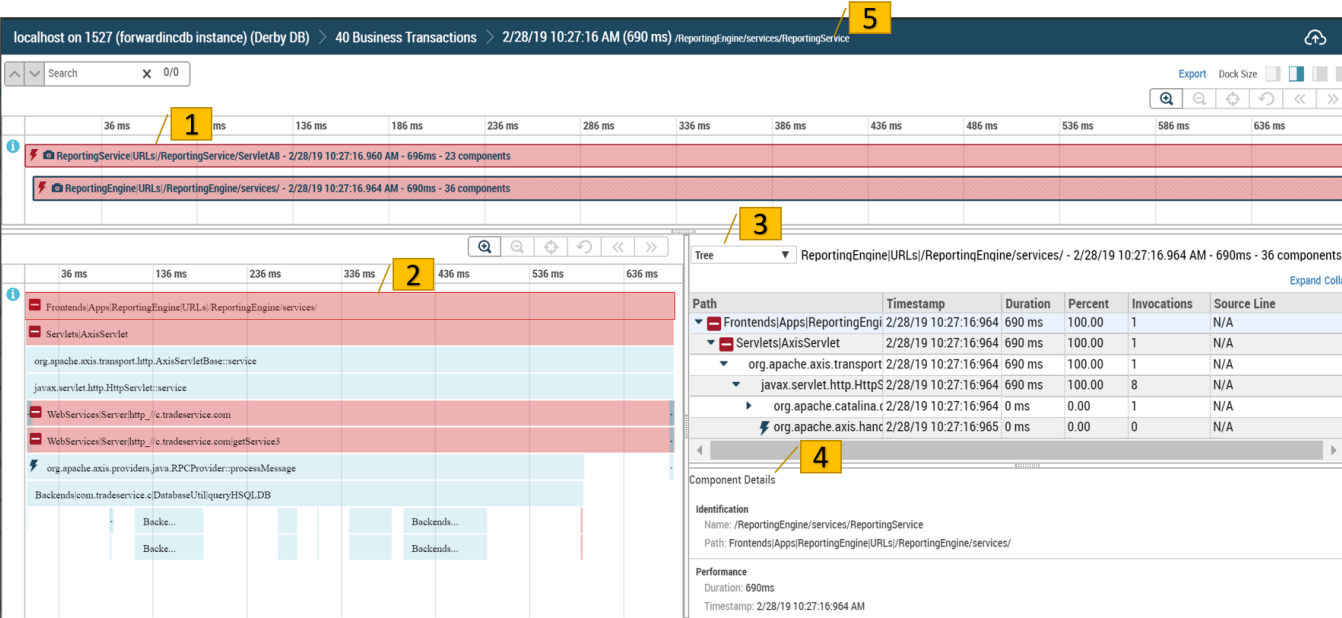
Vous pouvez consulter les informations détaillées sur vos données de suivi pour connaître les raisons de la lenteur ou de l'interruption de vos transactions. La visionneuse des traces de transaction affiche différentes représentations des données qui vous permettent d'identifier les composants peu performants.

Procédez comme suit :

1. Dans la carte ou le carnet d'analyse, accédez à l'onglet **Transactions métier**.
2. Cliquez sur l'onglet **Transactions métier**.
3. Cliquez sur une ligne dans la liste des traces de transaction.
La visionneuse des traces de transaction affiche 4 volets qui contiennent des informations sur les traces de transaction et les composants.

- Les **traces de transaction** s'affichent dans le volet supérieur.
- Les **détails des traces de transaction** s'affichent dans le volet inférieur gauche.
- Le volet inférieur droit est divisé en 2 sous-volets :
 - Les **informations de transaction** relatives à la trace de transaction sélectionnée s'affichent dans le sous-volet supérieur droit.
 - Les **détails de composant** s'affichent dans le sous-volet inférieur droit.

Le graphique suivant et la légende correspondante permettent de comprendre les différentes fonctionnalités disponibles dans la visionneuse des traces de





transaction.

La légende suivante identifie chaque élément par un numéro et fournit des informations complémentaires :

Numéro	Name (nom)	Informations complémentaires
1	Traces de transaction	Examinez chaque trace de transaction. S'il en existe plusieurs, les informations relatives à la trace de transaction sélectionnée s'affichent dans les autres volets.
2	Volet de détails des traces de transaction	Ce volet affiche la pile graphique, c'est-à-dire l'ordre des transactions des composants de haut en bas. La pile graphique ressemble à un gâteau de mariage à l'envers.

3	Volet Informations sur la transaction	Ce volet affiche des informations sur la trace de transaction sélectionnée. Notez que le chemin d'accès à droite de la liste déroulante correspond au chemin de la trace de transaction sélectionné dans le volet Trace de la transaction. Vous pouvez choisir les vues suivantes dans la liste déroulante : Arborescence , Récapitulatif , Temporisation du navigateur , Propriétés système et Cliché .
4	Détails du composant	Ce volet fournit des informations sur le composant sélectionné dans la pile graphique. Si vous n'en avez sélectionné aucun, les informations sur le premier composant de la pile graphique s'afficheront.
5	Chemin de navigation	Chemin d'accès situé au-dessus de la visionneuse des traces de transaction.

La pile graphique et les données de trace de transaction affichent des informations qui vous permettent d'évaluer les performances. Par exemple :

Relations d'appel entre les composants	<p>Les lignes des composants s'affichent de haut en bas dans l'ordre des appels.</p> <p>Remarque : Les termes appel et composant sont synonymes. Lorsque vous sélectionnez un composant, vous sélectionnez un appel dans la transaction.</p> <p>Un appel peut créer des appels enfants, qui composent la pile ou profondeur :</p> <p>1 ligne = 1 ou plusieurs appels = 1 ou plusieurs composants pouvant créer des appels enfants ou des invocations</p> <p>L'arborescence présente une correspondance unique des données :</p> <p>1 ligne = 1 appel = 1 composant</p> <p>La vue résumé affiche des données cumulées, non une correspondance unique :</p> <p>1 ligne = chemin d'accès</p> <p>Le chemin d'accès correspond à l'étiquette de l'appel et le niveau dans la pile. Par exemple, un appel Connexion a été passé 5 fois à un niveau identique de la pile. Vous pouvez observer 5 composants dans la même ligne. L'arborescence présente 5 lignes. Le nombre dans la vue Récapitulatif est 5 et la colonne Durée totale affiche la somme de la durée des 5 appels.</p>
Erreurs et clichés	<p>Le carré rouge contenant une icône de signe moins blanc  indique qu'un composant présente une erreur.</p> <p>L'icône représentant un appareil photo  identifie une transaction à laquelle un cliché d'erreur ou de blocage est associé.</p> <p>Remarque : pour plus d'informations, reportez-vous au document Analyse des clichés d'erreur et de blocage.</p>
Points d'entrée	<p>En général, les points d'entrée apparaissent comme le premier composant d'une transaction. S'il s'agit d'une transaction métier, elle apparaît comme le premier composant suivi du point d'entrée.</p>
Séquence de transactions	<p>La position des composants de gauche à droite indique la séquence. Le temps horloge relatif (en millisecondes) s'affiche en haut de la transaction. Si la durée du suivi est suffisamment importante, elle s'affiche en secondes, heures et jours.</p>

Données de transactions inter-processus et multi-JVM	<p>Un identificateur unique (ID de corrélation) lie les transactions des serveurs frontaux et d'arrière-plan suivis. La séquence repose sur l'ordre dans lequel les serveurs frontaux appellent les composants d'arrière-plan dans une transaction. L'ID de corrélation permet de déterminer les appels pouvant être à l'origine d'une transaction lente ou bloquée. Dans la section Détails du composant de la visionneuse des traces de transaction, l'ID de corrélation est la valeur de la propriété Données multiprocessus.</p> <p>Dans la visionneuse, diverses piles graphiques affichent les processus associés à l'événement de suivi sélectionné. Les processus qui font l'objet d'un suivi par différents agents s'affichent dans différentes zones grisées. Examinez les composants liés dans un suivi de transactions pour afficher les transactions inter-processus ou multi-JVM. Par exemple, vous pouvez vérifier si une transaction donnée a omis un processus et en a intégré un autre. Vous pouvez également déterminer les appels pouvant être à l'origine de transactions lentes et bloquées.</p> <p>Remarque : pour plus d'informations sur la corrélation de transactions, consultez la section Use Cross-Process Transaction Tracing to Solve Problems (Utilisation du suivi des transactions multiprocessus pour résoudre les problèmes).</p>
Composants de visibilité approfondie	<p>Une icône représentant un éclair indique un composant de visibilité approfondie. Ce type de composant correspond à une méthode ou un composant automatiquement détecté sans utiliser les directives ProbeBuilder. CA Application Performance Management analyse la complexité des méthodes afin de déterminer les appels et les composants à instrumenter et à afficher comme composants de visibilité approfondie.</p>
Visibilité d'écart d'exécution	<p>La visibilité d'écart d'exécution permet aux agents d'instrumenter automatiquement des applications et de les surveiller en fonction de leurs performances d'exécution.</p> <p>Remarque : pour plus d'informations, consultez la page Configuration de l'instrumentation intelligente.</p>

4. (Facultatif) Effectuez l'une ou plusieurs des actions suivantes :

- Saisissez une chaîne de texte pour filtrer les traces dans le champ Rechercher. La recherche correspond aux informations contenues dans l'ensemble des traces de transaction et des composants. Les résultats s'affichent dans toutes les vues et dans les propriétés du volet **Détails du composant**. La recherche renvoie également des correspondances partielles. Par exemple, les critères de recherche concernent `node1` . La vue **Récapitulatif** affiche les traces pour `node1` , `node124` et `node1_323` .
Les vues et la pile graphique affichent tous les composants connexes. Les composants correspondant à la recherche sont mis en surbrillance en jaune dans la pile. Le cas échéant, l'arrière-plan du texte correspondant apparaît en jaune dans les vues.
- Passez le curseur sur l'**icône d'informations** (rond bleu contenant un i).
Une info-bulle affiche le nom complet de l'agent. L'icône d'informations et la ligne correspondante représentent chaque agent.

5. Examinez de haut en bas les traces de transaction capturées par l'agent.

NOTE

Si le nombre de traces collectées est excessif, un message indique que la Visionneuse des traces de transaction ne peut pas les afficher. Par exemple, dans Internet Explorer, une fenêtre contextuelle explique que le fichier JSON est trop volumineux pour être chargé.

- Passez la souris sur une trace ou un composant pour afficher une info-bulle contenant le récapitulatif des informations de trace de transaction. L'info-bulle est utile en cas d'affichage partiel du composant.
- Utilisez les fonctions de navigation pour ajuster la vue.
Cliquez ici pour afficher l'aide sur la navigation...

La fonction Zoom avant (Maj + signe égal) modifie l'échelle et permet d'afficher plus de détails.

La fonction Zoom arrière (Maj + signe moins) modifie l'échelle pour afficher moins de détails.

La fonction Réinitialiser (Maj + R) rétablit l'état des données de la visionneuse sur sa valeur initiale.

La fonction Centrer (Maj + C) permet de centrer les données de la visionneuse.

La fonction Faire défiler vers la gauche (Maj + flèche gauche) déplace le curseur vers la gauche.

La fonction Faire défiler vers la droite (Maj + flèche droite) déplace le curseur vers la droite.

La fonction Sélectionner suivant (flèche vers le bas) sélectionne la ligne suivante.

La fonction Sélectionner précédent (flèche vers le haut) sélectionne la ligne précédente.

Utilisez les séparateurs des **volets** pour afficher celui qui vous intéresse. Double-cliquez sur un séparateur pour réduire ou agrandir les volets supérieur et inférieur à gauche.

Cliquez sur une option de **Taille de l'ancrage** pour augmenter ou diminuer la taille des volets gauche et droit.

Notez qu'un élément sélectionné dans une représentation l'est automatiquement dans les autres représentations (et vice versa) lorsque des informations sont associées. Par exemple, cliquez sur une ligne dans la pile graphique. La pile graphique, l'élément Informations sur la transaction, le volet **Détails du composant** et les vues associées affichent des informations correspondant à cette ligne.

6. Cliquez sur la trace de transaction de votre choix.
Vous pouvez sélectionner une seule trace de transaction à la fois.
7. Examinez les composants de la pile graphique de haut en bas pour connaître la séquence des appels pendant une période donnée. Un temps de transaction de composant anormalement long peut indiquer la cause première du problème. Notez que le nom et le premier numéro de ligne du fichier source Java de la méthode Java instrumentée apparaissent entre parenthèses.
Les lignes rouges indiquent une condition d'erreur. Les lignes en bleu clair indiquent qu'aucun problème n'existe. Les lignes en orange clair indiquent qu'une analyse différentielle a déclenché une alerte. Les lignes orange foncé indiquent un blocage. Les lignes jaunes indiquent les résultats de la recherche.
Les transactions de 0 milliseconde apparaissent sous la forme d'un point avec un arrière-plan bleu clair.
8. Cliquez sur un composant de votre choix.
Dans la partie inférieure droite, les volets **Informations sur la transaction** et **Détails du composant** affichent des informations détaillées dans leurs sous-volets respectifs.
9. Dans le sous-volet supérieur, sélectionnez une option dans la liste déroulante **SELECT A VIEW (sélectionner une vue)** pour afficher diverses représentations des données. Le comportement de sélection varie pour chaque vue. Par exemple, la vue **Arborescence** répertorie les chemins des traces de transaction, tandis que la vue **Temporisateur du navigateur** affiche les données des pages matérielles et les ressources associées aux pages logicielles. Par conséquent, les informations que vous pouvez sélectionner pour ces vues sont différentes.

Arborescence

L'**arborescence** répertorie les chemins de trace dans l'ordre hiérarchique des appels. Chaque chemin inclut le nom des classes et des méthodes d'un appel. Vous pouvez afficher les changements survenus entre un point de départ et un point final d'une trace. Les données Chemin, Horodatage, Durée, Pourcentage et Appels

s'affichent dans des colonnes pouvant faire l'objet d'un tri. (La colonne Ligne source n'est pas triable.) Certaines traces d'un composant peuvent ne pas contenir d'informations sur la ligne source. Dans ce cas, la colonne Ligne source indique N/D (Non disponible). Ajustez la quantité d'informations qui s'affiche en développant ou en réduisant les chemins. Des icônes de couleur indiquent le type de trace. Par exemple, la couleur orange clair



indique qu'une analyse différentielle a déclenché une alerte : une transaction comporte un écart non contrôlé.

L'**arborescence** vous permet de parcourir les données et d'accéder à des composants spécifiques pour identifier des problèmes de performances. Les valeurs des données permettent de connaître le mode d'affectation d'une valeur initiale par une série de valeurs intermédiaires.

Récapitulatif

La vue **Récapitulatif** affiche des données dont les couleurs indiquent le type de trace. Les valeurs de taux d'appel supérieures sont des nuances approfondies, car les appels s'affichent les uns au-dessus des autres. Ce récapitulatif visuel vous permet d'identifier les problèmes instantanément. Après avoir identifié un problème, vous pouvez utiliser l'**arborescence** pour examiner les détails de ce type d'appel.

Les données de colonne affichent les totaux pour chaque ligne. Exemple : un composant est appelé 100 fois sur la ligne de niveau 4 d'une transaction. Le nombre de lignes de niveau 4 est de 100. Chaque appel est de 2 millisecondes, la durée totale est donc de 200 millisecondes (100 x 2). La valeur de la durée totale dans le chemin de navigation peut différer de celle figurant dans le **récapitulatif**. Cette différence peut se produire, car la valeur de chemin de navigation inclut tous les suivis corrélés à partir d'un composant d'arrière-plan tandis que la valeur de la vue **Récapitulatif** ne les inclut pas.

Browser Timing (Délai du navigateur)

Le délai du navigateur affiche les données de pages matérielles et leurs ressources, ainsi que celles des ressources associées à des pages logicielles. Les données des pages logicielles n'apparaissent pas.

NOTE

Pour plus d'informations sur le délai du navigateur, consultez la page [Diagnose Resource Load Issues](#) (Diagnostic des problèmes de performances système).

Propriétés système

Les propriétés système indiquent les données de surveillance du temps d'UC et de la contention de threads pour les traces de transaction dans la méthode de servlet.

NOTE

Pour plus d'informations sur les propriétés système, consultez la page [Diagnose System Performance Issues](#) (Diagnostic des problèmes de performances système).

Cliché

Le cliché fournit des informations sur les clichés de blocage et d'erreur.

NOTE

Pour plus d'informations sur les clichés d'erreur et de blocage, consultez la page [Analyze Error and Stall Snapshots](#) (Analyse des clichés d'erreurs et de blocage).

10. Examinez le volet **Détails du composant**.

Pour obtenir les détails du composant, cliquez ici...

NOTE

Toutes les informations sur les composants de visibilité approfondie ne sont pas disponibles.

Nom : Nom du composant ; par ex. : Valeur par défaut

Chemin : nom de ressource complet du composant, par exemple : `Frontends|Apps|AuthenticationService|URLs|Default`

Durée : Durée d'exécution (en millisecondes) du composant sélectionné

Horodatage (relatif) : heure de début (en fonction de l'horloge système) de l'appel du composant racine

Pourcentage de la durée : pourcentage de la durée totale des transactions

Propriétés système : les données de temps permettent de diagnostiquer les threads de méthode pour identifier les problèmes de performance. Les zones de couleur identifient les différentes propriétés système. Un histogramme (graphique à barres) représente les valeurs de données de ces propriétés système. Lorsque les valeurs sont égales à 0 ms, le graphique affiche une ligne noire. Chaque propriété système et sa valeur sont répertoriées sous le graphique.

Propriétés : liste des propriétés facultatives du composant, y compris la propriété suivante :

- Ligne source (agent Java uniquement) : nom et premier numéro de ligne du fichier source Java de la méthode Java instrumentée. L'agent Java ne collecte pas les numéros de ligne de code qui appellent la méthode Java instrumentée. Les images mémoire de pile de threads d'exception standard dans les débogueurs et les images mémoire du noyau affichent généralement ces numéros de ligne.

TIP

Cliquez sur **Développer** pour développer l'arborescence complète. Cliquez sur **Réduire** pour réduire l'arborescence complète. Cliquez sur la flèche vers la droite près d'un composant pour afficher un seul sous-composant.

Redimensionnez une colonne pour afficher plus ou moins d'informations.

Passez la souris sur un **nom de colonne** ou un **segment de graphique de propriétés système** pour afficher une info-bulle contenant des informations sur l'élément.

11. Déterminez la cause première du problème de performance des applications. Utilisez les informations d'identification pour collecter des détails spécifiques concernant le problème. En règle générale, vous recherchez les composants d'exécution les plus longs et approfondis dans votre suivi. Exemple :

- Appel unique à une base de données
- Appels nombreux et rapides qui contribuent à une latence élevée

Vous pouvez contacter le personnel affecté aux opérations pour solliciter un examen du code d'application. Le personnel déterminera s'il existe un problème de code ou de dépendance d'application.

NOTE

Informations complémentaires : [Analyse des données de suivi et collaboration pour l'analyse des problèmes](#)

Diagnostic des problèmes de chargement des ressources

Pour diagnostiquer les problèmes de performance d'une page Web, vous devez examiner le timing des ressources téléchargées par vos fichiers HTML et JavaScript. Dans la visionneuse des traces de transaction, l'onglet **Temporisation du navigateur** permet de visualiser les ressources téléchargées en réponse aux requêtes HTTP associées à une trace. Cet onglet inclut les données générées de manière cumulée et séquentielle au cours d'une trace de transaction. Vous pouvez consulter des informations détaillées à propos de vos données de trace. Vous pouvez consulter les données des pages matérielles et de leurs ressources, ainsi que celles des ressources associées à des pages logicielles. (Les données relatives à une page logicielle proprement dite ne sont pas visibles.) Les ressources sont grisées par défaut, tandis que chaque phase possède sa propre couleur. Cette représentation en cascade permet de comprendre de quelle manière différents facteurs contribuent à une trace de transaction. Cette vue fonctionne de la même façon qu'une vue en cascade dans les outils de développement de votre navigateur.

NOTE

Informations complémentaires : [Examen des différents composants et données de suivi](#)

Procédez comme suit :

1. Dans l'onglet **Transactions métier**, cliquez sur la trace de transaction qui vous intéresse. Les différents composants de transaction s'affichent dans la pile graphique **Détails de la transaction**.
2. Examinez les composants de la pile graphique de haut en bas pour connaître la séquence des appels pendant une période donnée. Un temps de transaction de composant anormalement long peut indiquer la cause première du problème.

3. Cliquez sur un composant de votre choix.
4. Dans le volet **Informations sur la transaction**, sélectionnez **Temporisation du navigateur** dans la liste déroulante de **sélection de vue**.
5. Passez en revue les informations figurant dans la vue pour diagnostiquer les problèmes de chargement des ressources :

La vue **Temporisation du navigateur** se compose de trois parties :

- Une zone récapitulative contenant des informations à propos du composant de la trace qui a déclenché le téléchargement de ressources.
- Une chronologie vous permet de réduire la période concernée afin de vous concentrer sur des ressources spécifiques. La chronologie vous permet de visualiser toutes les ressources en contexte et de limiter la période affichée dans la grille. Vous pouvez modifier la plage en déplaçant les indicateurs situés aux extrémités ou en faisant glisser la ligne entière au milieu.
- Une grille affichant une ligne de détail pour chaque ressource.

La grille inclut les types de lignes suivants :

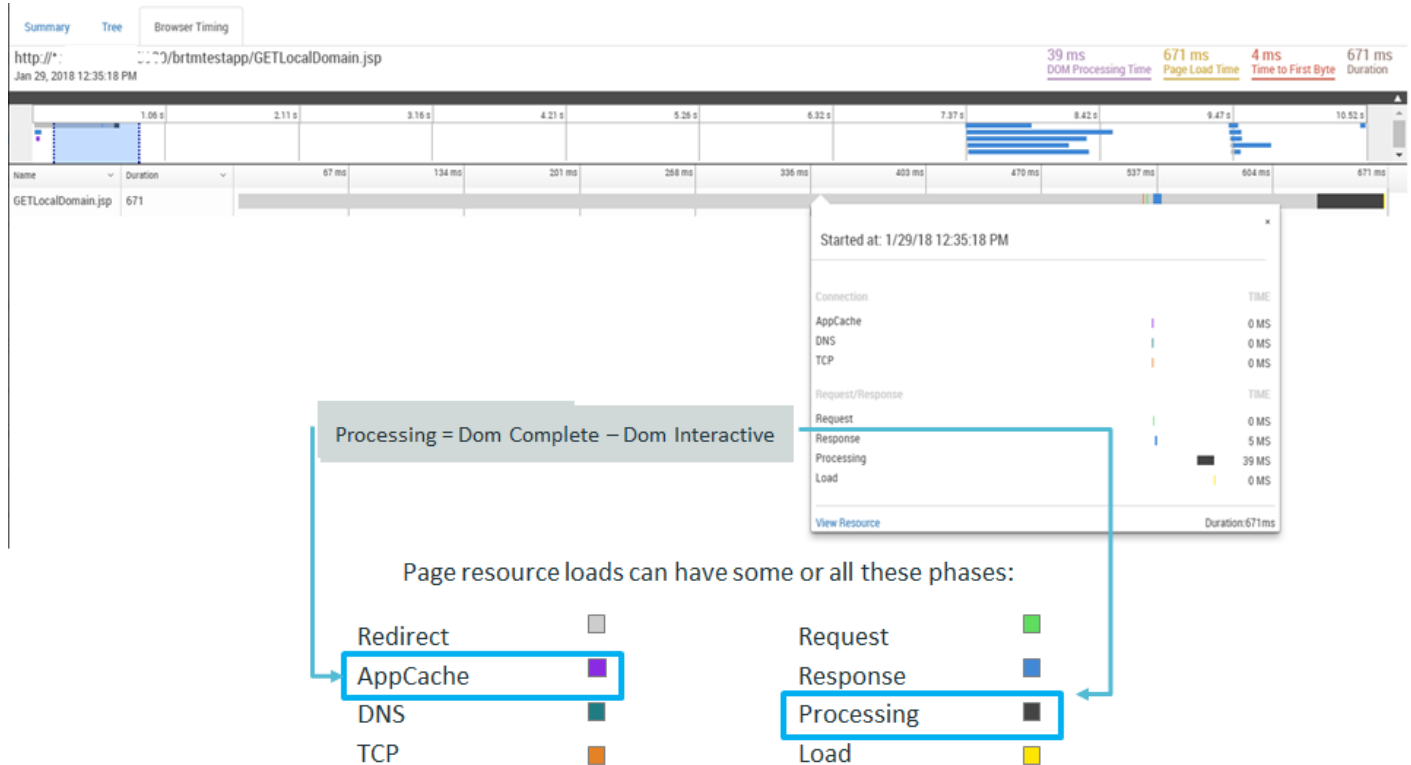
- Lignes de chargement de page
Lorsque la trace sélectionnée correspond à un chargement de page matérielle, la page proprement dite est représentée dans la grille. (Un chargement de page logicielle met simplement à jour la page existante à l'aide de JavaScript.) La dernière colonne de la grille indique la plage horaire sélectionnée, divisée en dix périodes égales. La barre grise représente la durée totale du chargement de la page, tandis que les bandes de couleur correspondent aux différentes "phases" du chargement. La somme des durées des différentes phases ne peut pas être égale à la durée globale du chargement de la page, car la durée globale inclut la temporisation du navigateur. La durée de temporisation du navigateur inclut les durées liées au réseau et la commutation contextuelle du navigateur. Pour afficher la répartition des durées d'une trace, passez le curseur sur la phase.

Les chargements des ressources d'une page peuvent inclure l'ensemble ou une partie des phases suivantes :

- – Redirection
- AppCache
- DNS
- TCP
- Requête
- Réponse
- Traitement
- Chargement

L'agent de navigateur signale directement la plupart des phases, mais deux d'entre elles sont calculées comme indiqué dans le graphique ci-dessous :

- AppCache : DNS (recherche de domaine) – extraction
- Traitement : Dom Complete – Dom Interactive

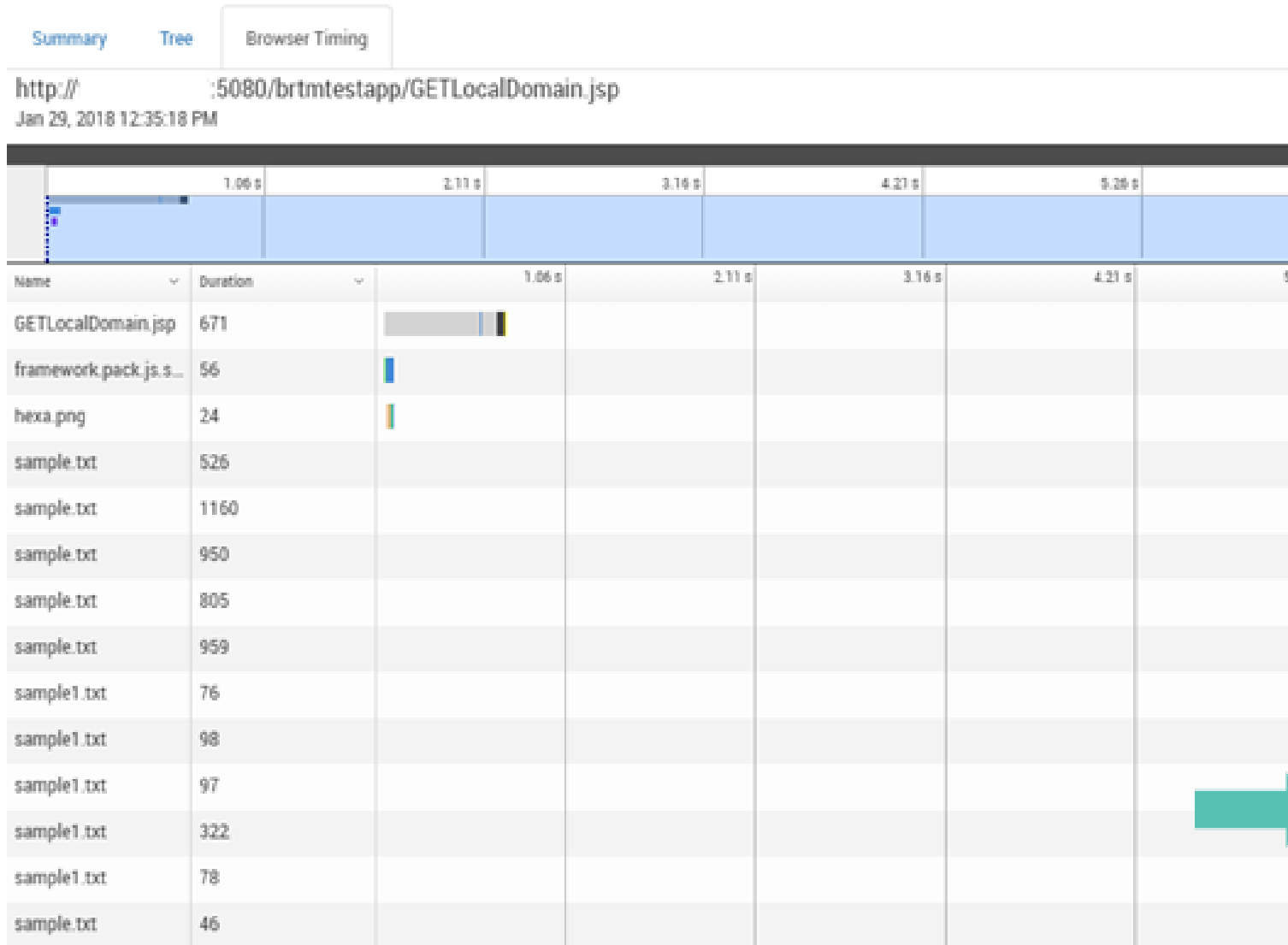


- Lignes de chargement de ressources

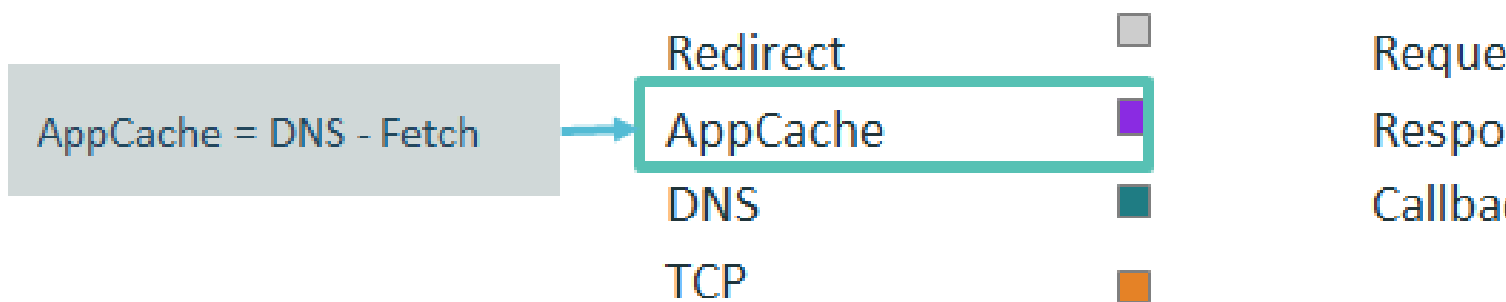
Comme les phases de ressources ne sont pas affichées dans la pile (graphique à secteurs), vous ne pouvez pas visualiser les données brutes des phases. Chaque ressource téléchargée par la page correspond à une ligne dans la grille des temporisations du navigateur. Comme pour les chargements de page, vous pouvez consulter des informations plus détaillées pour chaque ressource en passant la souris sur le graphique correspondant dans la grille. Les chargements de ressource peuvent inclure l'ensemble ou une partie des phases suivantes :

- AppCache
- DNS
- TCP
- Requête
- Réponse
- Durée d'exécution du rappel

Les ressources téléchargées par la page s'affichent de la même manière que les chargements de page, mais les phases sont légèrement différentes. L'agent de navigateur signale toutes les phases, sauf AppCache. La phase AppCache est calculée comme suit : DNS – extraction. Le graphique ci-dessous illustre les phases de chargement de ressources.



Resource loads can have some o



Il se peut que les valeurs des traces de ressource ne correspondent aux valeurs de temps des mêmes traces dans l'onglet Réseau Firefox. Par ailleurs, la vue **Temporisation du navigateur** n'inclut pas certaines des ressources affichées dans l'onglet Réseau. Les incohérences de valeurs concernent toutes les ressources, car la valeur de temps sous l'onglet Firefox Network correspond à la période allant du début de la demande jusqu'à la fin de la réponse. Toutefois, la durée de temporisation du navigateur inclut les durées liées au réseau et la commutation contextuelle du navigateur. Les ressources manquantes dans la vue Temporisation du navigateur sont filtrées par défaut (paramètre non configurable). Ces ressources incluent les requêtes du client pour la configuration du profil et pour l'envoi des réponses de mesures. L'onglet Temporisation du navigateur n'inclut pas les mesures de page pour les ressources requises par l'agent de navigateur. La valeur de durée totale peut ne pas correspondre sur tous les navigateurs, car la durée d'exécution du rappel est ajoutée pour ajuster la valeur de durée.

NOTE

La temporisation peut être arrondie sur une valeur supérieure ou inférieure d'une milliseconde.

Diagnostic des problèmes de performance système

La vue Propriétés système de la vue Visionneuse des traces de transaction indique les données de surveillance du temps d'UC et de la contention de threads pour les traces de transaction dans les méthodes de l'API de servlet.

NOTE

Informations complémentaires : [Examen des différents composants et données de suivi](#)

Les méthodes s'exécutent souvent lorsque l'utilisateur clique sur un lien, soumet un formulaire ou exécute un autre type d'action sur un site Web. Les propriétés système peuvent vous aider à comprendre la source d'un ralentissement, un serveur bloqué ou une utilisation anormalement élevée de l'UC, par exemple :

- DX APM affiche les mesures de blocage, mais aucune transaction n'apparaît lors de l'exécution d'une trace de transaction. Cette situation peut se produire, car les transactions ne se terminent pas et le gestionnaire d'entreprise reçoit des informations incomplètes concernant le blocage du serveur de l'agent.
- L'UC n'est pas trop sollicitée par une application. pourtant, les temps de réponse sont longs. Cela peut indiquer que tous les threads en fonctionnement sont bloqués, interbloqués ou en attente.
- Le chargement d'une méthode est lent. Un thread peut utiliser une grande quantité d'UC.

Les données de temps/durée permettent de diagnostiquer les threads de méthode à la recherche de problèmes de performance.

Procédez comme suit :

1. Dans l'onglet **Transactions métier**, cliquez sur la trace de transaction qui vous intéresse.
Les différents composants de transaction s'affichent dans une pile graphique, dans le volet **Détails de la transaction**.
2. Dans le volet **Informations sur la transaction**, sélectionnez **Propriétés système** dans la liste déroulante de **sélection de vue**.
3. Examinez les informations figurant dans la grille. Les valeurs de données indiquent la durée (en millisecondes) ainsi que le pourcentage de temps total passé dans chaque méthode ou thread. Recherchez les valeurs élevées afin d'identifier les threads qui utilisent une puissance de traitement élevée, qui sont en attente ou qui sont bloqués.

TIP

Lorsque vous cliquez sur une ligne dans la grille, la trace correspondante est mise en surbrillance dans la pile graphique et inversement.

Mesures liées à l'agent Java

Temps total d'UC : temps d'UC total pour le thread actuel, pour tous les threads ou pour aucun thread. La valeur correspond à la somme du temps d'UC système et du temps d'UC utilisateur.

Temps d'UC utilisateur : temps que le processeur a passé à exécuter le code de programme ou le code dans les bibliothèques pour une transaction lorsque la JVM prend en charge la mesure du temps d'UC.

Temps d'UC système : temps passé à exécuter du code dans le noyau du système d'exploitation d'une transaction d'application surveillée lorsque la JVM prend en charge la mesure du temps d'UC.

Délai d'attente : durée approximative qu'un thread de transaction a passé dans l'état WAITING ou TIMED_WAITING lorsque la JVM prend en charge la surveillance de contentions de threads.

Bloqué : durée approximative qu'un thread a passé dans l'état BLOCKED lorsque la JVM prend en charge la surveillance de contentions de threads.

Autre : durée approximative passée autre que la somme des temps d'UC, durée du blocage et délai d'attente.

Mémoire allouée : nombre approximatif d'octets alloués au segment de mémoire de threads de transaction lorsque la JVM prend en charge la mesure de l'allocation de la mémoire de threads.

Chemin : nom de ressource complet du thread.

Mesures liées à l'agent .NET/.NET Core

Temps d'UC utilisateur : temps que le processeur a passé à exécuter le code de programme ou le code dans les bibliothèques pour une transaction lorsque le CLR .NET/.NET Core prend en charge la mesure du temps d'UC.

Temps d'UC système : temps passé à exécuter du code dans le noyau du système d'exploitation d'une transaction d'application surveillée lorsque le CLR .NET/.NET Core prend en charge la mesure du temps d'UC.

4. Vous trouverez plus de détails sur les **propriétés système** dans le volet **Détail du composant**. Les valeurs de temps sont exprimées en millisecondes. Les propriétés suivantes s'appliquent au temps système :

Block Time (ms) : durée approximative qu'un thread a passé dans l'état BLOCKED lorsque la JVM prend en charge la surveillance de la contention de threads.

CPU System Time (ms) : temps passé à exécuter du code dans le noyau du système d'exploitation d'une transaction d'application surveillée lorsque la JVM prend en charge la mesure du temps d'UC.

CPU Time (ms) : temps d'UC total pour le thread actuel, pour tous les threads ou pour aucun thread. La valeur correspond à la somme du temps d'UC système et du temps d'UC utilisateur.

CPU User Time (ms) : temps que le processeur a passé à exécuter le code de programme ou le code dans les bibliothèques pour une transaction lorsque la JVM prend en charge la mesure du temps d'UC.

Other Time (ms) : temps approximatif écoulé autre que la somme des valeurs CPU Time (Temps d'UC), Blocked Time (Temps bloqué) et Wait Time (Temps d'attente).

Wait Time (ms) : durée approximative qu'un thread de transaction a passé dans l'état WAITING ou TIMED_WAITING lorsque la JVM prend en charge la surveillance de contentions de threads.

Détection et analyse d'erreurs et de blocages

Un *blocage* est une transaction, ou un composant d'une transaction, qui ne s'est pas terminée dans les délais impartis. Lorsque vous avez déterminé l'emplacement d'une transaction ou d'un composant bloqué, vous pouvez effectuer les opérations suivantes :

Procédure d'analyse d'erreurs et de blocages

Utilisation de ce scénario

Utilisez ce scénario lorsque vous rencontrez un problème de performances des applications, tel qu'il s'affiche dans le tableau de bord DX Application Performance Management ou lorsqu'il vous est signalé dans une notification.

Conditions préalables

Avant de commencer, isolez l'emplacement du problème.

Les agents collectent des données sur les transactions et les envoient au gestionnaire d'entreprise pour leur traitement et leur affichage. Ces données incluent des informations relatives aux erreurs et aux blocages d'application.

Erreur

Une erreur est une exception signalée par les codes d'erreur JVM ou HTTP. Exemple :

- Un statut d'erreur HTTP, tel que 404 Page Not Found

- Une exception SQL
- Une exception Java

Blocage

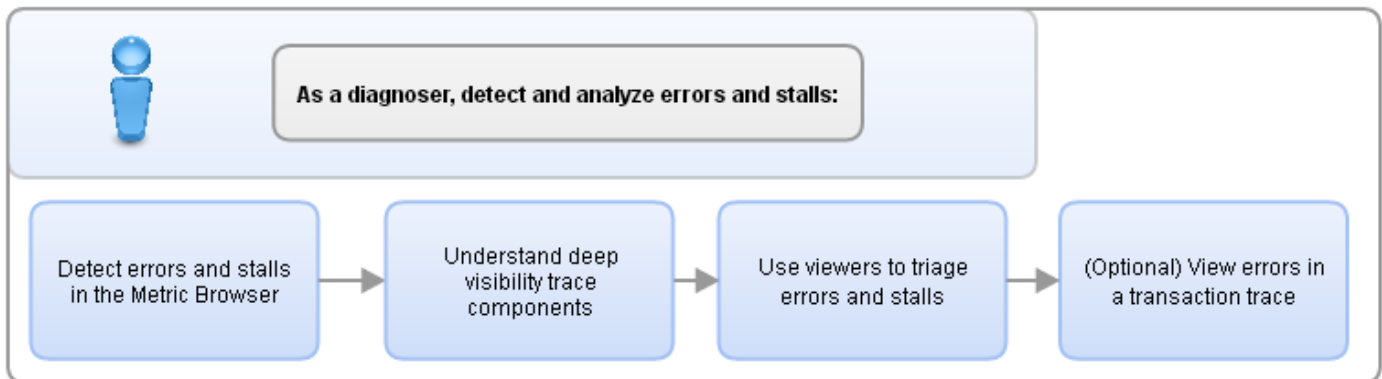
Un blocage est une transaction, ou un composant d'une transaction, qui ne s'est pas terminée dans les délais impartis.

Vous pouvez effectuer les tâches suivantes :

- Détecter la cause des erreurs et des blocages majeurs au moment où ils se produisent, procéder à leur triage, et surveiller les événements associés.
- Déterminer la fréquence et la nature des erreurs.
- Déterminer la cause première d'un problème.

Le diagramme suivant décrit la procédure d'analyse des erreurs et des blocages pour identifier la cause première d'un problème de performances.

Figure 9: 9.8 Détection et analyse d'erreurs et de blocages



Procédez comme suit :

1. Détectez les erreurs et les blocages dans la vue des mesures.
2. Examinez les composants de trace de visibilité approfondie.
3. Utilisez des visionneuses pour trier les erreurs et les blocages.
4. (Facultatif) Affichez les erreurs dans une trace de transaction.

Détection des erreurs et des blocages dans la vue des mesures

Vous pouvez détecter et trier la cause des erreurs et blocages majeurs lorsqu'ils se produisent. Vous pouvez surveiller les agents et composants en affichant des informations détaillées dans l'onglet **Vue des mesures**.

DX Application Performance Management met à jour l'affichage des informations d'erreur et de blocage toutes les 15 secondes.

Procédez comme suit :

1. Accédez à Team Center.
2. Dans la **Vue des mesures**, accédez à l'agent ou au composant que vous voulez surveiller et sélectionnez l'onglet **Erreurs** en bas de la page.

L'onglet **Erreurs** contient les données signalées par un agent sur une machine virtuelle Java (JVM) ou un environnement CLR .NET. Si des erreurs ou des blocages sont signalés pour l'agent ou le composant, une liste connexe s'affiche.

- Description de l'onglet Erreur sélectionné.
- 3. Sélectionnez l'onglet **Traces**.
Description de l'onglet Traces sélectionné.
- 4. Cliquez sur Horodatage pour effectuer le tri. Les nouveaux blocages ou erreurs s'affichent dans l'ordre de tri.

Composants de trace de visibilité approfondie

Lorsque l'instrumentation intelligente est activée, les agents détectent et collectent automatiquement des informations détaillées sur les composants de transaction au niveau de la méthode. Les agents détectent et instrumentent automatiquement les composants de visibilité approfondie, sans utiliser de fichiers de directives ProbeBuilder (PBD). Les composants de visibilité approfondie que vous affichez dans les transactions bloquées contiennent uniquement le nom de classe, le nom de la méthode et la durée. Vous pouvez configurer la profondeur et la portée de la visibilité approfondie de trace en fonction de votre environnement et de vos besoins. Par exemple, configurez l'agent pour détecter et instrumenter automatiquement une quantité faible, moyenne ou élevée du code d'application. Pour plus d'informations, reportez-vous à la page [Configuration de l'instrumentation intelligente](#).

NOTE

L'instrumentation intelligente est disponible uniquement pour les agents Java et non pour les agents .NET.

Détection des erreurs dans la vue des mesures

Les agents collectent des données sur les transactions et les envoient au gestionnaire d'entreprise pour leur traitement et leur affichage dans une visionneuse de données. Ces données incluent des informations relatives aux erreurs d'application. Vous pouvez détecter et trier la cause des erreurs lorsqu'elles se produisent. Vous pouvez surveiller les agents et composants en affichant des informations détaillées dans l'onglet **Vue des mesures**.

DX Application Performance Management met à jour l'affichage des informations d'erreur toutes les 15 secondes.

Procédez comme suit :

1. Accédez à Team Center.
2. Dans la **Vue des mesures**, accédez à l'agent ou au composant que vous voulez surveiller.
3. Recherchez la mesures Erreurs par intervalle. Si la valeur :
= 0, il n'existe aucune erreur.
> 0, passez à l'étape 4 : sélectionnez l'onglet Traces.
4. Sélectionnez l'onglet **Traces**.
5. Pour trier les lignes par le contenu d'une colonne, cliquez sur son en-tête. Les nouvelles traces s'affichent dans l'ordre de tri. Les erreurs dans la liste des traces apparaissent en rouge.
6. Affichez le message d'erreur dans la trace de transaction collectée automatiquement par Introscope.
Si vous ne voyez pas les traces de transaction automatiques, reportez-vous à la section Traces de transaction collectées de manière automatique.
7. Sélectionnez l'onglet **Erreurs**.
L'onglet Erreurs contient les données générées par un agent sur une machine virtuelle Java (JVM) ou un environnement CLR .NET. Si des erreurs sont signalées pour l'agent ou le composant, une liste connexe s'affiche. Pour trier les lignes par le contenu d'une colonne, cliquez sur son en-tête. Les nouvelles erreurs s'affichent dans l'ordre de tri.
8. Sélectionnez un cliché d'erreur pour obtenir plus d'informations sur l'erreur, y compris le chemin d'appel et les paramètres. Utilisez les observateurs d'erreurs en direct et d'événements historiques pour trier les problèmes.

Affichage d'erreurs dans une trace de transaction

Vous pouvez afficher des informations sur les erreurs, y compris des composants de visibilité approfondie, dans une trace de transaction.

Les deux méthodes ci-dessous permettent de collecter les traces de transaction et consulter les informations sur les erreurs :

- Exécutez manuellement une trace de transaction.
- Lorsque l'instrumentation intelligente est activée, Introscope collecte automatiquement une trace de transaction en cas d'erreur.
Lorsqu'une erreur déclenche une trace de transaction automatique, les détails de composant suivants s'affichent :
 - Le composant ayant levé l'exception inclut les propriétés du composant.
 - Le premier composant dans la trace de transaction affiche la propriété Auto Trace Trigger Criteria en tant qu'erreur.

Procédez comme suit :

1. Accédez à Team Center.
2. Cliquez sur **Vue des mesures**.
3. Sélectionnez une application dans l'arborescence des mesures.
4. Cliquez sur l'onglet **Error View** (Vue des erreurs) dans le volet inférieur.
Remarque : En mode dynamique, l'onglet Traces répertorie les événements de trace de transaction pour les 20 dernières minutes. En d'autres termes, les événements de trace de transaction de plus de 20 minutes ne s'affichent pas en mode dynamique.
5. Sélectionnez l'une des erreurs répertoriées pour afficher des informations détaillées.
Un écran affiche la description complète de l'erreur sélectionnée.

The screenshot displays the Introscope Error View interface. At the top, a breadcrumb shows the path: > 43 Business Transactions > 7/4/23 2:53:00 PM (2 ms) /demobank/CAbankOnline/img/irbcm.gif. Below this is a search bar and navigation controls. The main area shows a transaction trace with a red bar indicating an error. The trace is divided into three segments: 0 ms, 1 ms, and 2 ms. The 2 ms segment is highlighted with a red bar and contains the text: Apache-Axis|URLs|Resources - 7/4/23 2:53:00.796 PM - 2 ms - 7 components. Below the trace, a table lists the components of the transaction. The table has columns: Path, Timestamp, Duration, Percent, Invocations, and Source Line. The components are: Frontends|Apps|Apache-Axis|URLs|Resources (2 ms, 100.00%, 1 invocation, HttpServlet.java:591), Servlets|DefaultServlet (HttpServlet) (2 ms, 100.00%, 1 invocation, HttpServlet.java:591), and org.apache.catalin (1 ms, 50.00%, 1 invocation, DefaultServlet.java:). The bottom right panel shows the 'Component Details' for the selected component, including its Name, Path, and Performance (Duration: 2 ms).

Path	Timestamp	Duration	Percent	Invocations	Source Line
Frontends Apps Apache-Axis URLs Resources	7/4/23 2:53:00:796 PM	2 ms	100.00	1	HttpServlet.java:591
Servlets DefaultServlet (HttpServlet)	7/4/23 2:53:00:796 PM	2 ms	100.00	1	HttpServlet.java:591
org.apache.catalin	7/4/23 2:53:00:797 PM	1 ms	50.00	1	DefaultServlet.java:

Component Details

Identification

Name: /demobank/CAbankOnline/img/irbcm.gif
Path: Frontends|Apps|Apache-Axis|URLs|Resources

Performance

Duration: 2 ms

6. Déterminez la cause première du problème de performance des applications.
Utilisez les informations d'identification dans les onglets disponibles pour collecter des détails spécifiques concernant le problème. Affichez les champs suivants : Horodatage, Durée, Description, ID d'utilisateur (si un ID est associé au problème), Message d'erreur, Durée d'appel et Chemin.

Vous pouvez effectuer les opérations suivantes :

- Trier les colonnes pour rechercher les appels ou méthodes qui présentent les temps de réponse les plus longs ou le plus grand nombre d'erreurs
- Utiliser l'onglet Rechercher pour filtrer les résultats
- Utiliser les messages d'erreur et d'autres informations pour en savoir plus sur le problème

Après avoir identifié les composants à l'origine du problème, le personnel chargé des opérations peut demander une modification du code de l'application pour le résoudre.

Analyse des clichés d'erreur et de blocage

Les agents détectent et collectent automatiquement des informations détaillées sur les composants des transactions au niveau de la méthode. Ces données incluent des informations relatives aux erreurs et aux blocages d'application :

- **Erreur**

Dans une application, certains événements peuvent causer des erreurs de transaction, par exemple :

- un statut d'erreur HTTP tel que "404 Not Found"
- une exception sur une méthode
- une exception sur du code non instrumenté tel qu'un composant profond
- l'implémentation d'un outil de suivi d'erreurs personnalisé sur une logique de communication ou structure

- **Blocage**

Un blocage est une transaction, ou un composant d'une transaction, qui ne s'est pas terminée dans les délais impartis.

Un *cliché* indique les traces de transaction d'une erreur ou d'un blocage, ainsi que des informations relatives à ce qu'il s'est passé lorsque l'événement est survenu.

Une transaction peut inclure des erreurs et des blocages déclenchant les clichés associés. Prenons, par exemple, une transaction qui inclut 100 appels. L'appel 3 commence à s'exécuter lentement, puis déclenche un cliché de blocage. Après quelques appels supplémentaires, l'appel 6 présente une erreur, ce qui déclenche un cliché d'erreur. L'appel 81 rencontre une autre erreur, ce qui déclenche un autre cliché d'erreur.

Dans la visionneuse des traces de transaction, la vue **Arborescence** affiche tous les chemins possibles dans une transaction pour les appels. La vue **Cliché** affiche un chemin via une transaction. Il s'agit du chemin d'appel direct d'un blocage ou d'une erreur spécifique. La vue **Arborescence** inclut donc généralement plusieurs couches d'appel, tandis que la vue Cliché englobe les clichés d'erreur et de blocage dans une même couche.

NOTE

Informations complémentaires : [Examen des différents composants et données de suivi](#)


Examen des clichés pour l'étude des erreurs et des blocages

Un cliché permet d'effectuer les tâches suivantes :

- Détecter la cause des erreurs et des blocages majeurs au moment où ils se produisent, procéder à leur triage, et surveiller les événements associés.
- Déterminer la fréquence et la nature des erreurs.
- Déterminer la cause première d'un problème.

Procédez comme suit :

1. Sous l'onglet **Transactions métier**, sélectionnez **Cliché** dans la liste déroulante **Type de trace**.
2. Sélectionnez la trace que vous souhaitez examiner.
Les différents composants de transaction s'affichent dans une pile graphique (graphique à secteurs) **Détails de la transaction**.

Une ligne rouge et une case rouge avec une icône de signe moins blanc  identifient les traces présentant une erreur.

3. Dans la pile graphique, vous pouvez consulter les caractéristiques du cliché à l'aide des identificateurs suivants :
Une icône en forme d'appareil photo



indique une transaction normale à laquelle un ou plusieurs cliché sont associés.

Un préfixe **Cliché d'erreur** avant le nom de composant identifie une seule transaction avec un cliché, mais sans chemin de trace vers une erreur ou un blocage. Une transaction peut n'avoir aucune trace associée dans les cas suivants :

- Vous utilisez un agent qui n'a pas été mis à jour vers la version actuelle.
- Un problème survient dans la transaction avant que les informations de corrélation ne soient extraites de la charge utile de la requête. Le cas échéant, les informations de trace ne sont pas incluses dans l'événement.
- L'agent ne signale pas toutes les traces, car il repose sur un système d'échantillonnage. Par défaut, les agents échantillonnent le comportement des transactions en traçant régulièrement chaque URL normalisée unique dans une application. Un événement d'erreur sans trace de transaction peut survenir à cause de l'implémentation de la détection des erreurs (outil de suivi d'agent), ou parce qu'un seuil de clamp a été atteint pour les traces sur le gestionnaire d'entreprise ou l'agent.

4. Dans le volet **Trace de transaction**, sélectionnez la trace de votre choix.
5. Dans le volet **Informations sur la transaction**, sélectionnez **Cliché** dans la liste déroulante.

La vue **Cliché** répertorie les chemins de trace dans l'ordre hiérarchique des appels. Dans la grille, une trace est comme un arbre qui compte différentes branches qui comportent elles-mêmes des feuilles. Un cliché est un chemin qui va de branche en branche jusqu'à une feuille. Vous pouvez avoir plusieurs clichés qui sont chacun représentés comme racine de la grille. Un cliché vous permet de détecter les erreurs ou blocages survenus sur différentes branches. L'arborescence développée prend le nom du cliché et indique à quel endroit le problème est survenu dans le chemin d'appel. L'arborescence vous permet de parcourir l'examen des données et d'accéder à des composants spécifiques pour identifier des problèmes de performance. Les valeurs des données permettent de connaître le mode d'affectation d'une valeur initiale par une série de valeurs intermédiaires. La valeur **Type de cliché** est Erreur ou Blocage.

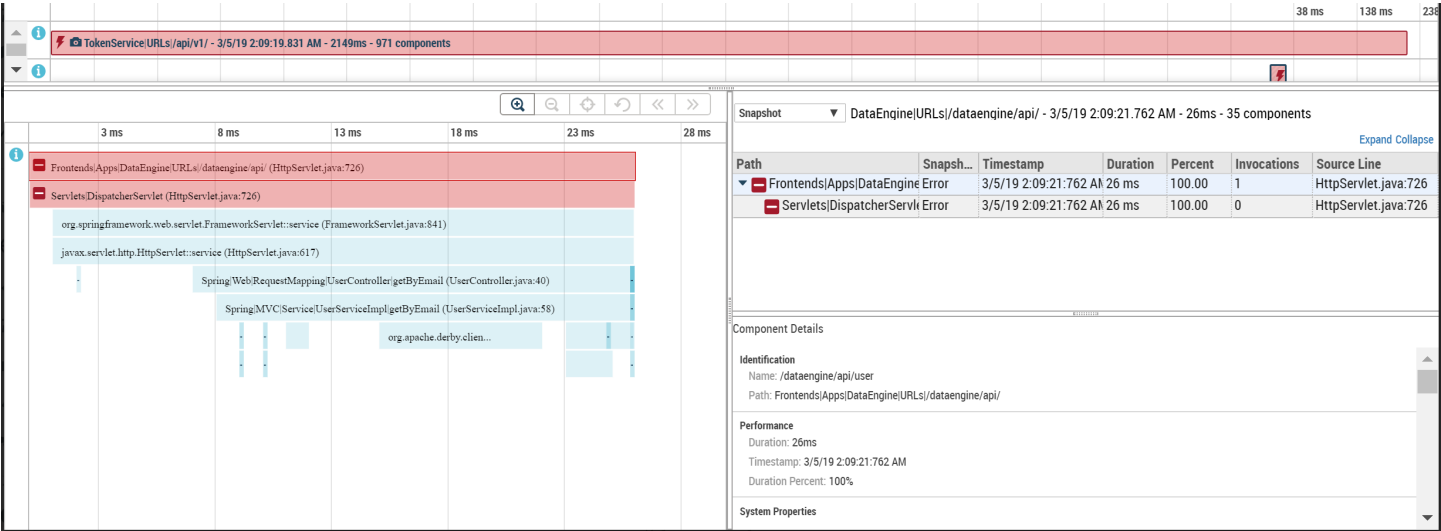
TIP

Lorsque vous cliquez sur une ligne dans la grille, la trace correspondante est mise en surbrillance dans la pile graphique et inversement.

6. Examinez le cliché pour identifier la cause première d'un problème.
7. Identifiez les composants visiblement à l'origine du problème. Le personnel opérationnel peut demander une modification du code de l'application pour résoudre le problème.

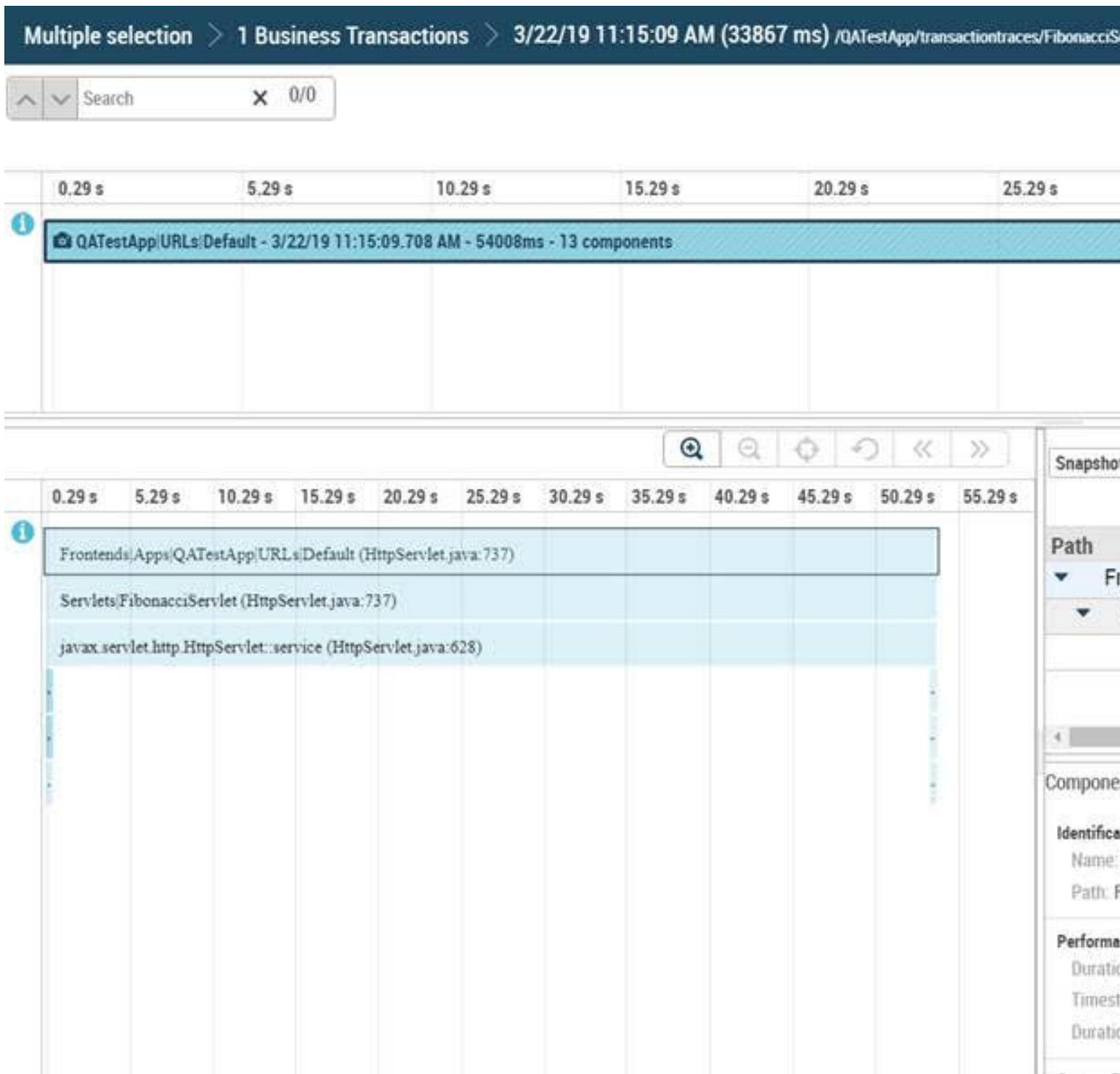
Exemple : Transaction avec cliché d'erreur associé

Le graphique ci-dessous affiche une transaction avec un cliché d'erreur associé. Notez l'apparition d'une icône en forme de caméra sur la gauche de la trace de transaction et de la valeur **Erreur** dans la colonne **Cliché**.



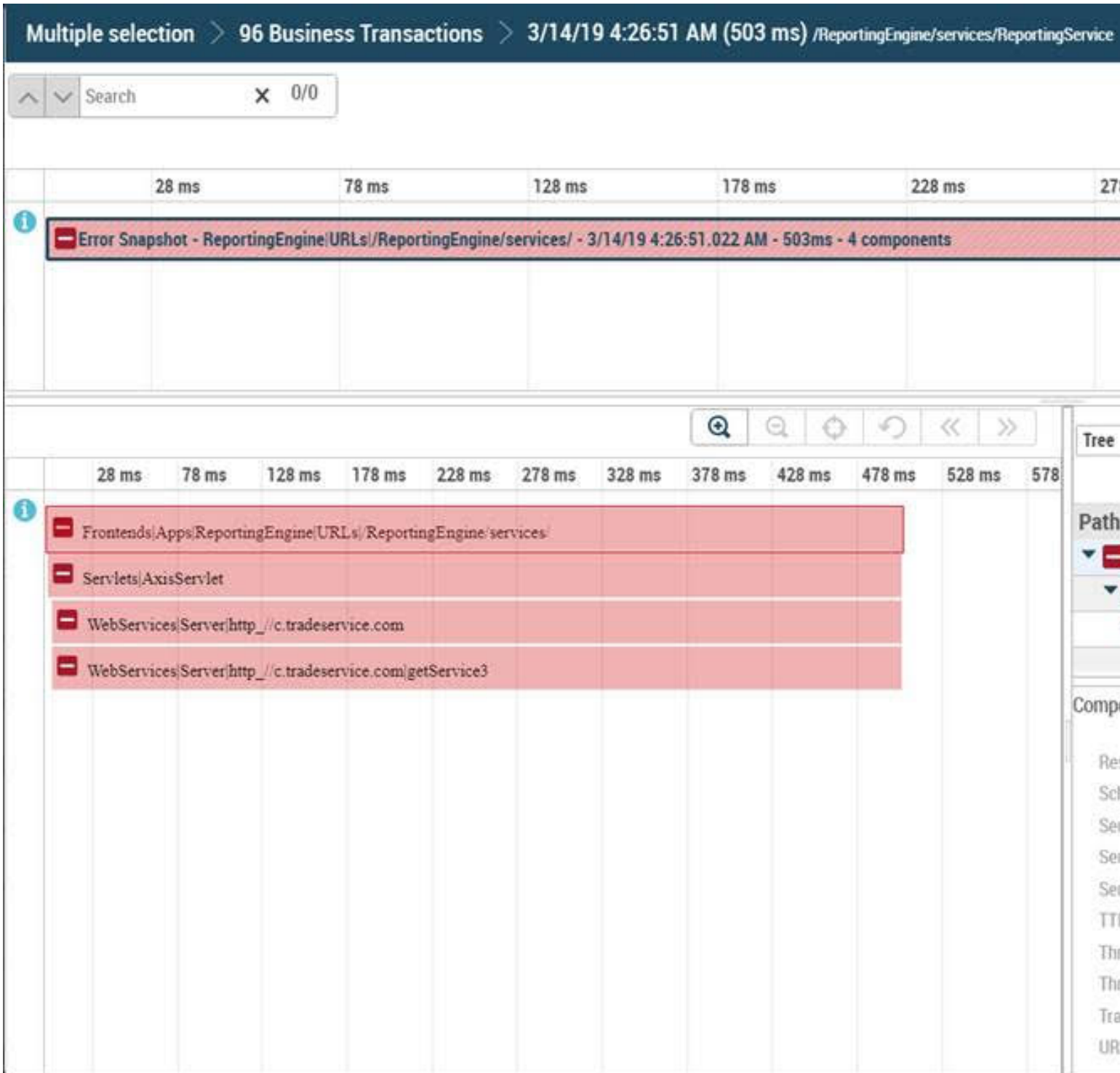
Exemple : Transaction avec cliché de blocage associé

Le graphique ci-dessous représente une transaction normale avec un cliché de blocage associé. Notez l'apparition d'une icône en forme d'appareil photo et de la valeur **Blocage** dans la colonne **Cliché**.



Exemple : Transaction unique avec un cliché, mais sans trace associée vers une erreur ou un blocage

Le graphique ci-dessous représente une transaction unique avec un cliché, mais sans chemin de trace associé vers une erreur ou un blocage. Un préfixe **Cliché erreur** apparaît, mais pas d'icône en forme d'appareil photo.



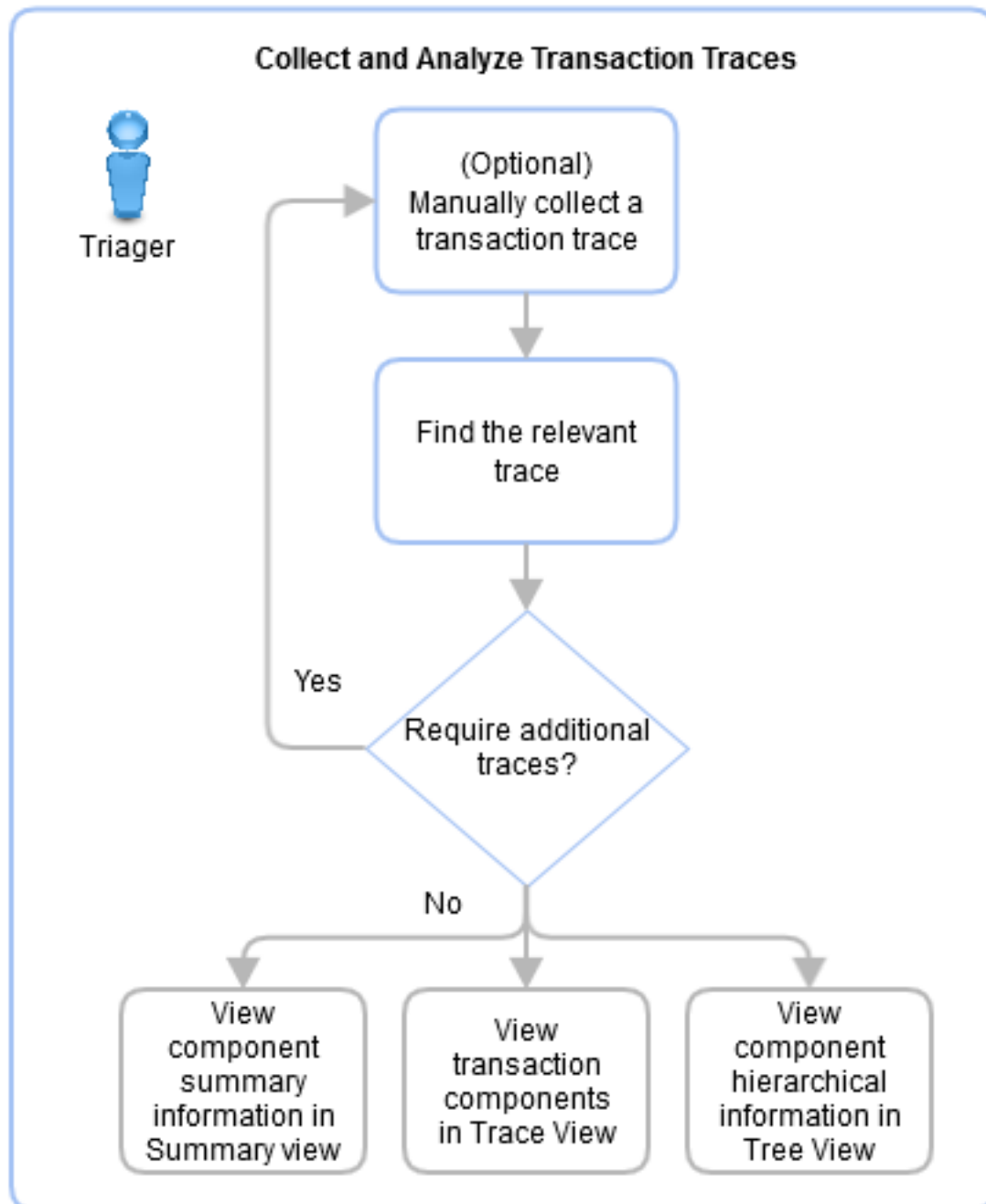
Collecte et analyse des traces de transaction

En tant que responsable du diagnostic, du triage ou de l'administration, vous affichez les informations détaillées sur les composants de suivi de transactions tels que les méthodes. Ces informations vous aident à identifier la cause première des problèmes de performances des applications. Avec l'outil de suivi de transaction, vous pouvez examiner les traces de

transaction collectées automatiquement ou manuellement. Les informations s'affichent parce que les composants sont instrumentés à l'aide de directives PBD ou parce que l'instrumentation intelligente est activée.

Ce diagramme illustre la procédure d'identification de la cause première des problèmes de performances des applications et indique des informations détaillées sur les composants de transaction.

Figure 10: Procédure de collecte et d'analyse des traces de transaction



Présentation du suivi des transactions

L'outil de suivi de transaction surveille l'activité des différentes transactions lorsqu'elles circulent dans les limites des agents pris en charge. Les agents prennent en charge la surveillance des applications Java, .NET et Node.js. Le suivi des transactions interprocessus surveille les appels de transaction entre différentes instances JVM (Java Virtual Machine), CLR (Common Language Runtime) et Node.js. La surveillance peut avoir lieu sur des ordinateurs locaux ou distants. L'affichage des détails des transactions interprocessus permet d'effectuer un examen des problèmes dans les processus de transaction.

Modes disponibles de collecte des traces de transaction :

- [Introscope collecte automatiquement les traces de transaction.](#)
 - Lorsque l'instrumentation intelligente est activée, Introscope collecte automatiquement les traces de transaction dans plusieurs circonstances.

Remarque : L'instrumentation intelligente est disponible uniquement pour les agents Java, PHP et Node.js et pas pour les agents .NET.
 - Introscope collecte régulièrement un [échantillon de trace de transaction](#).
- [Collecte manuelle d'une trace de transaction](#)

Après le lancement d'une session de suivi de transaction, les transactions correspondant aux critères de filtre s'affichent dans la station de travail ou dans WebView. Vous pouvez afficher les informations de trace dans l'onglet Outil de suivi de transaction, y compris les événements de transaction de type traces de transaction et erreurs de transaction.

Traces de transaction collectées de manière automatique

Lorsque l'[instrumentation intelligente](#) est activée, Introscope collecte automatiquement une trace de transaction dans les circonstances suivantes :

- Une analyse différentielle détecte un problème d'instabilité de l'application.

Remarque : Les traces de transaction automatiques de l'analyse différentielle requièrent la version 10.0 ou supérieure de l'agent.
- Une erreur se produit.
- L'outil de suivi `ComponentTimeAutoTraceTriggerTracer` est déployé et le délai de réponse d'un composant est dépassé.
- Une API déclenche une trace de transaction automatique basée sur des critères personnalisés.

Informations complémentaires : contactez les [services d'implémentation de CA APM](#).

Les outils de suivi optimisés et à surcharge faible collectent les traces de transaction automatiques. Les traces automatiques supposent une surcharge de performances moindre que pour l'exécution manuelle, l'échantillonnage et autres traces de transaction. Les autres types de suivi de transaction utilisent un filtrage d'agent qui ajoute une surcharge.

Les traces de transaction automatiques présentent les caractéristiques suivantes :

- Elles sont prises en charge pour les agents Java, PHP et Node.js. L'agent .NET n'est, lui, pas pris en charge.
- Tous les composants instrumentés par des directives PBD possèdent une mesure associée dans l'arborescence Investigator. Aucune mesure n'est associée aux composants de visibilité approfondie.
- Les [composants de visibilité approfondie](#) incluent uniquement le nom de classe, le nom de méthode et la durée. Pour les composants frontaux et d'arrière-plan (par exemple, les servlets, services Web, appels SQL), le nom est formaté selon la configuration des directives PBD.
- Elles incluent les traces de transaction interprocessus

Remarque : Les transactions interprocessus dans les traces de transaction automatiques sont prises en charge uniquement pour les applications Java.
- Les traces de transaction automatiques n'affichent pas certaines propriétés de détails des composants que les autres types de traces de transaction affichent.
- Les propriétés suivantes s'affichent sous `ComponentProperties` :

- Le type de trace est Normal.
- Si une erreur a déclenché la trace de transaction, le composant qui a généré l'exception inclut les propriétés du composant.
- Le premier composant dans la trace de transaction affiche la propriété `Auto Trace Trigger Criteria`.

Si vous ne voyez pas les traces de transaction automatiques, cela peut être dû à l'une des raisons suivantes :

- L'[instrumentation intelligente](#) n'est pas activée.
- Le nombre de traces de transaction automatiques par limite d'intervalle (propriété `agent.deep.automatic.trace.clamp`) est dépassé.

NOTE

Informations complémentaires : [Durabilité d'agent](#)

Introscope collecte uniquement la trace manuelle si des filtres manuels correspondent à une trace automatique pendant l'exécution manuelle d'une trace.

Transactions multiprocessus dans les traces de transaction automatiques

L'affichage des transactions interprocessus dans les traces de transaction automatiques permet d'évaluer les transactions interniveaux. Vous pouvez déterminer le niveau à l'origine du goulot d'étranglement pour une transaction problématique.

NOTE

Le suivi des transactions inter-processus dans les traces de transaction automatiques est pris en charge uniquement pour les applications Java.

Agents en amont et en aval

Les agents qui surveillent les transactions peuvent être en amont, en aval ou les deux par rapport à d'autres agents surveillant la même transaction. Les agents en amont peuvent réaliser des appels interprocessus aux agents en aval. Les appels de transaction peuvent parcourir plusieurs processus. Par conséquent, les agents surveillant les processus entre le premier appel de transaction et le dernier appel de transaction sont placés aussi bien en aval qu'en amont par rapport aux autres agents. Voici un exemple :

1. Vous examinez la trace d'une transaction problématique et remarquez un temps d'exécution de 6 secondes (6 000 ms).
2. La **vue Suivi** affiche les appels d'une méthode côté client (`dataservice.yourcompany.net/invoke`) à une méthode côté serveur (`thirdparty.mycompany.net/invoke`).
3. Vous remarquez que la méthode côté serveur passe un grand nombre d'appels au service Web tiers

`3PP site data`

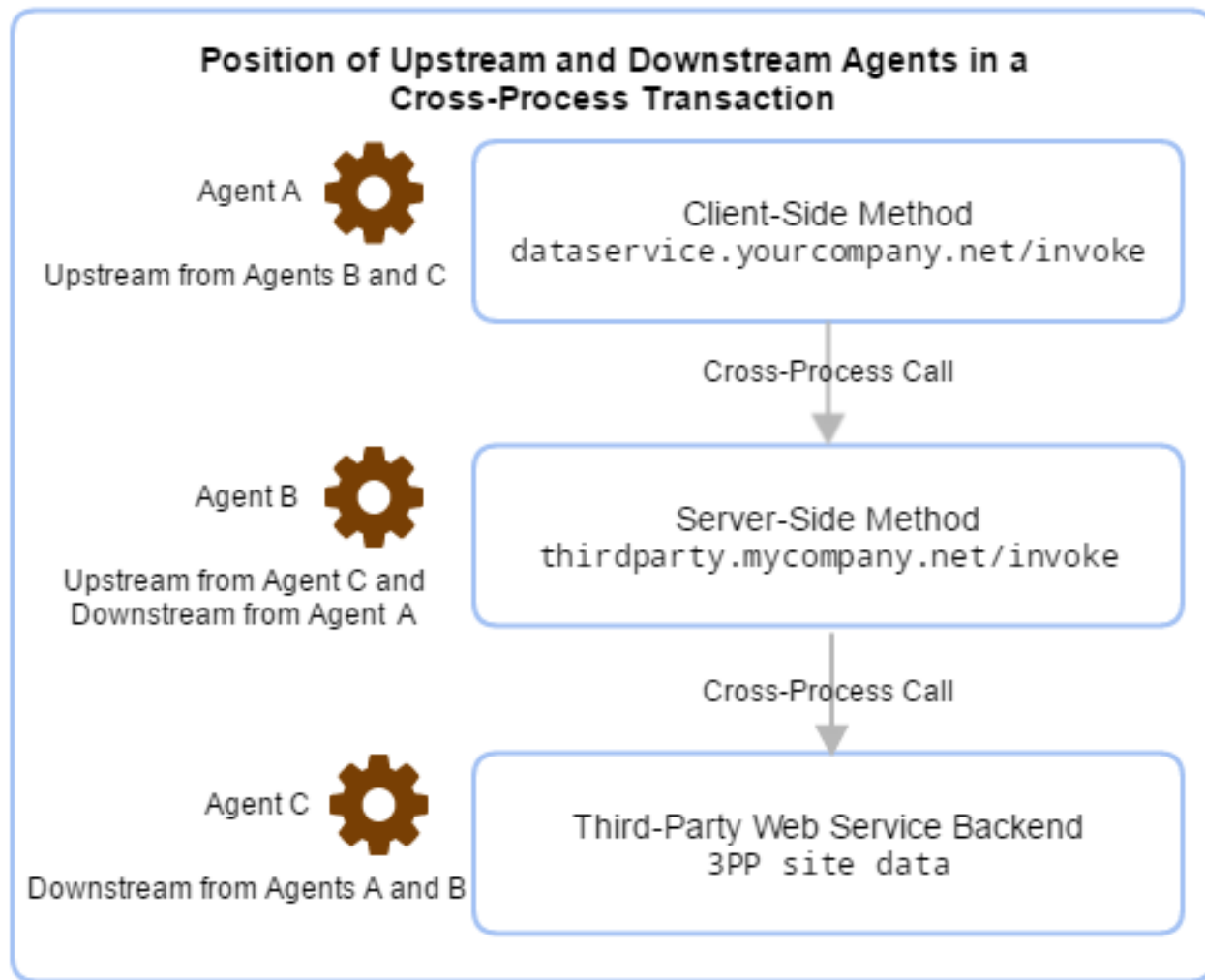
, qui est instrumenté.

4. La **vue Suivi** indique que

`3PP site data`

le serveur d'arrière-plan du service Web traite des demandes répétées qui se succèdent rapidement. Ce comportement indique que la logique de programmation, par exemple une boucle imbriquée, est probablement la cause des appels répétés au niveau du service côté serveur. Vous avez déterminé que l'opération d'appel côté serveur est responsable de la majorité du temps d'exécution globale des transactions.

Le graphique ci-dessous indique les positions des agents dans cet exemple de transaction interprocessus.

Figure 11: Diagramme d'agents en amont et en aval

Les agents signalent les problèmes lorsqu'ils les rencontrent et démarrent parfois les traces de transaction. Lorsque le suivi de transaction automatique n'incluait pas les appels interprocessus, seuls les agents en amont pouvaient signaler les problèmes et collecter les traces de transaction.

Visibilité avant le suivi interprocessus dans les traces de transaction automatiques

Un agent proche du début d'une transaction ne sait pas si la transaction présente un problème en aval. A la fin de la transaction, un agent en aval signale un éventuel problème en aval à l'agent en amont le plus proche. Tout ce que ces agents en amont savent est que cette transaction est inachevée tant qu'aucun agent en aval n'a signalé sa finalisation. A l'achèvement de la transaction, l'agent en amont le plus proche du début de la transaction signale les problèmes rencontrés au gestionnaire d'entreprise sous forme de traces de transaction. Lorsque le suivi de transaction automatique n'incluait pas la surveillance des appels interprocessus, les agents en aval détectant des problèmes n'envoyaient jamais les traces de transaction au gestionnaire d'entreprise. Les problèmes détectés par les agents en aval ne pouvant pas être signalés à l'agent le plus en amont n'étaient pas signalés. Cette situation se traduisait par un important manque de visibilité sur les problèmes des applications.

Visibilité de bout-en-bout avec le suivi interprocessus dans les traces de transaction automatiques

Grâce à la prise en charge du suivi interprocessus, les agents Java peuvent utiliser la mise en cache intelligente pour envoyer des traces de transaction automatiques pour les transactions interprocessus en aval qui posent problème. Cette fonctionnalité offre une visibilité de bout-en-bout pour les transactions Java.

Les agents en amont et en aval qui détectent des transactions problématiques peuvent déclencher des traces de transaction automatiques. Ils peuvent également envoyer des informations de trace de transaction au gestionnaire d'entreprise. Les agents qui déclenchent des traces automatiques décident à la fin de la transaction s'ils doivent ou non envoyer une trace au gestionnaire d'entreprise. Le moment de cette prise de décision est particulièrement utile pour l'analyse différentielle lorsque les seuils de référence du gestionnaire d'entreprise déclenchent des traces de transaction automatiques.

Les transactions peuvent utiliser un protocole pris en charge, HTTP ou SOAP par exemple, pour appeler un service dans le même processus. Dans ce cas, les agents réalisant des appels interprocessus peuvent être placés aussi bien en amont qu'en aval par rapport aux autres agents. Lorsqu'un agent en amont collecte une trace de transaction automatique, tous les agents en aval participants collectent eux aussi les traces de transaction automatiques. La fonction de suivi des transactions interprocessus collecte uniquement les traces vous permettant de trier les problèmes en vue de l'analyse de leurs causes premières.

Lorsqu'un agent en amont déclenche une trace, la propriété

`Component Details Auto Tracing Triggered`

affiche le type de déclencheur, une erreur par exemple. Lorsqu'un agent en aval déclenche la collecte des traces automatiques, la propriété

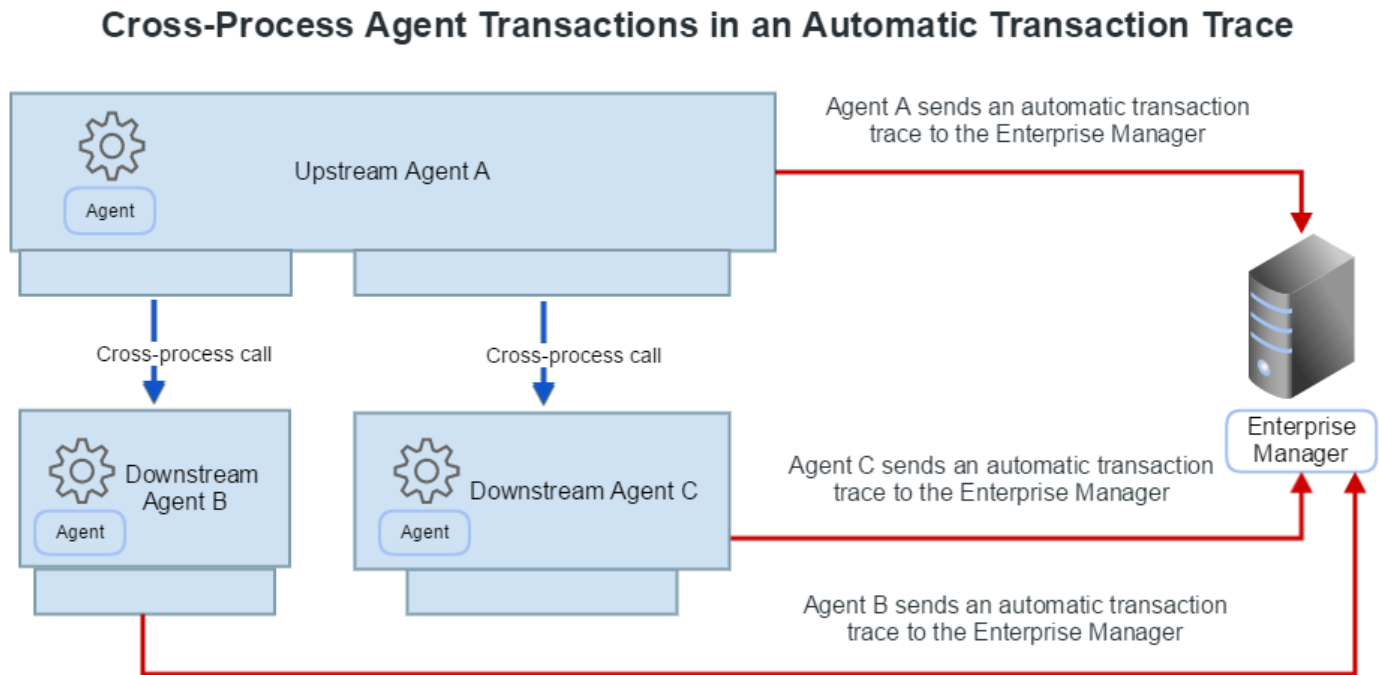
`Component Details Auto Tracing Triggered`

la propriété est

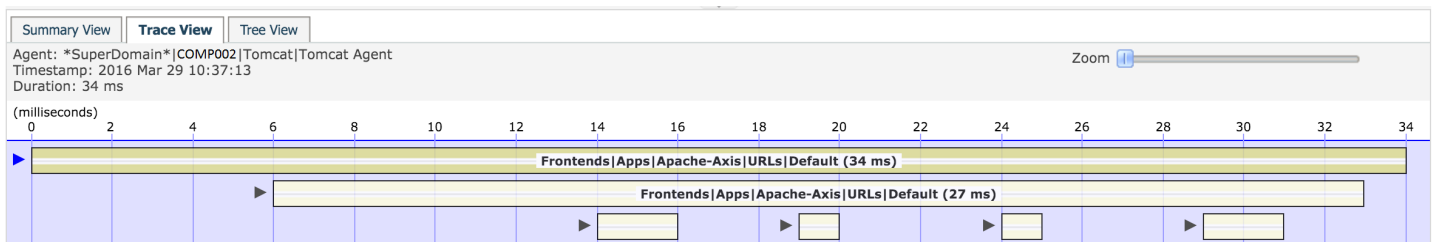
`Cross Process Trigger`

Exemple : corrélation des traces de transaction interprocessus des agents dans les traces de transaction automatiques

Un agent en amont par rapport aux autres agents détecte un problème. L'agent en amont déclenche la collecte d'une trace de transaction automatique et indique aux agents en aval de faire de même. Tous les agents envoient leurs traces de transaction automatiques au gestionnaire d'entreprise. Ensemble, les agents créent une transaction interprocessus corrélée, comme illustré dans le diagramme ci-après.

Figure 12: Les transactions interprocessus déclenchent le suivi automatique - agent

Les traces de transaction automatiques prennent également en charge la corrélation interthreads au sein du même processus. Les appels de thread peuvent parcourir plusieurs transactions. Une transaction dans un processus peut parcourir différents threads. Le graphique ci-dessous illustre quatre threads interprocessus dans la ligne du bas d'une trace de transaction automatique.

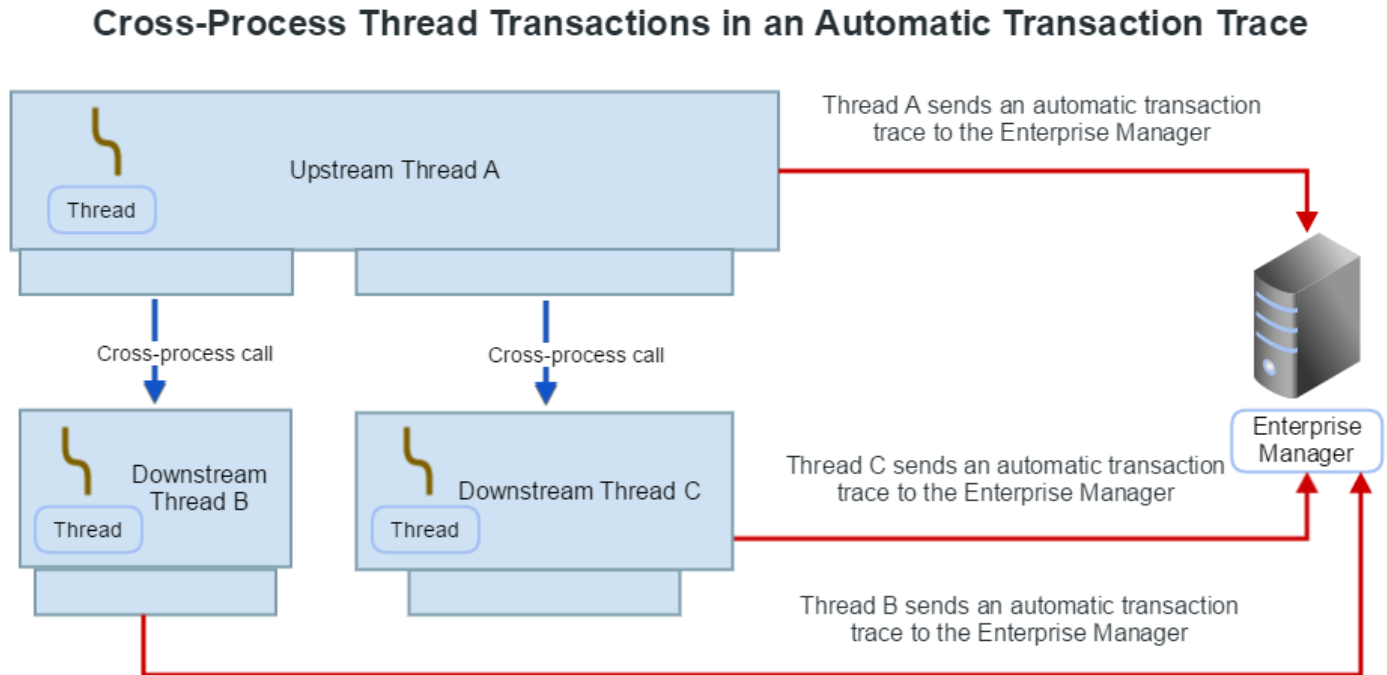


Les threads en amont peuvent déclencher des traces de transaction automatique à tout moment, avant ou après l'appel des threads en aval. Les détails de transaction varient selon que le thread est en amont ou en aval par rapport au thread de déclenchement initial dans la transaction.

Exemple : corrélation des traces de transaction interprocessus des threads dans les traces de transaction automatiques

Un thread en amont détecte un problème. Le thread en amont déclenche la collecte d'une trace de transaction automatique et indique aux threads en aval de faire de même. Tous les threads envoient leurs traces de transaction automatiques au gestionnaire d'entreprise. Ensemble, les threads forment une transaction interprocessus corrélée.

Figure 13: Transaction interprocessus dans un suivi automatique 2



Collecte automatique d'une trace de transaction basée sur l'instabilité des applications

La fonction d'analyse différentielle suit la stabilité de vos applications. Par défaut, l'analyse différentielle recherche un éventuel écart non contrôlé dans le temps de réponse moyen de vos mesures de transaction frontale et métier. La carte d'analyse différentielle permet d'explorer visuellement la stabilité et la réactivité de nombreuses applications. Chaque bande de la carte correspond à une mesure unique. Dans une période calme et stable, la bande prend la forme d'une légère ombre. Au fur et à mesure que la stabilité se détériore, l'ombre de la bande devient progressivement plus noire en fonction de la sévérité de l'instabilité. Une bande unique permet donc de connaître la stabilité d'une application ou transaction métier unique au fil du temps. La carte affiche les bandes les plus instables dans la partie supérieure.

Lorsqu'une application devient légèrement instable, l'analyse différentielle en informe l'agent, qui est préparé pour la collecte des traces de transaction automatiques associées. Généralement, l'agent collecte les traces de transaction jusqu'à ce que l'application devienne stable. Toutefois, l'agent peut décider de ne pas collecter de trace de transaction lorsque la période d'instabilité est brève. Reportez-vous à ces traces de transaction pour obtenir des informations détaillées concernant la modification de la stabilité et pour déterminer la cause première de cette variation.

NOTE

Les traces de transaction automatiques de l'analyse différentielle requièrent la version 10.0 ou supérieure de l'agent.

Procédez comme suit :

1. Dans APM Team Center, cliquez sur **WebView**.
APM WebView s'affiche.
2. Cliquez sur **Investigator**.
Une arborescence présente une vue hiérarchique de votre système.
3. Dans cette arborescence, sélectionnez l'agent pour lequel vous souhaitez afficher les informations de performances, par exemple :

SuperDomain | Host | Process | Agent | Frontends | Apps | App Name

4. Cliquez sur l'onglet **Analyse différentielle**.
La carte affiche une représentation graphique des données de performances ainsi que les 8 dernières minutes de données. Les 100 premières mesures problématiques s'affichent par ordre décroissant d'instabilité. Les données sont actualisées lorsque vous interrogez ou modifiez la période ou lorsque vous sélectionnez un autre noeud.
5. Cliquez sur la bande de votre choix dans la carte.
Le graphique d'analyse différentielle s'affiche. Il vous permet de comprendre la stabilité des mesures dans la chronologie que la bande représente. Ce graphique indique le statut du composant surveillé, ce qui vous permet de détecter rapidement les performances normales et anormales.
Une ligne représente une valeur de mesure réelle.
Les régions grisées correspondent aux bandes d'écart 1, 2 et 3. Plus la bande est foncée, plus l'écart est élevé par rapport à la valeur prévue. Lorsqu'elle apparaît en blanc, la mesure dépasse les prévisions. Les mesures qui s'affichent au-dessus de la zone blanche du bas ont dépassé la valeur prévue. Par exemple, si la mesure dépasse la bande supérieure, cela signifie qu'elle dépasse de trois fois l'écart standard.
6. Passez le curseur de votre souris sur la ligne.
Des info-bulles affichent la valeur des mesures.
7. Cliquez sur le lien hypertexte correspondant à la mesure qui vous intéresse, par exemple, Temps de réponse moyen.
8. Dans le navigateur de mesures, cliquez sur le noeud de dossier juste au-dessus de la mesure, puis sur l'onglet **Traces**.
Vous pouvez afficher les traces de transaction automatiques engendrées par l'instabilité.
9. (Facultatif) Cliquez sur d'autres noeuds pour afficher les traces de transaction générées par la fonction d'analyse différentielle.
Dans cet exemple, cliquez sur le noeud **Composants frontaux**, puis sur l'onglet **Traces** pour afficher les traces automatiques pour toutes vos applications frontales.

Vous pouvez configurer l'analyse différentielle pour des points d'entrée et d'autres mesures d'application.

Déclenchement du suivi automatique des transactions en cas de dépassement du temps de réponse du composant

Vous pouvez déployer un PBD pour déclencher automatiquement une trace de transaction lorsque le temps de réponse du composant a été dépassé. Pour cela, vous créez une entrée PBD avec un outil de suivi pour collecter les informations de trace automatique. Par exemple, pour collecter les informations de trace lorsque le temps de réponse d'un servlet spécifique dépasse 10 secondes. Utilisez l'option d'outil de suivi `ComponentTimeAutoTraceTriggerTracer` pour configurer cette fonctionnalité.

NOTE

Informations complémentaires : [Configuration des options de trace de transaction](#)

Collecte manuelle d'une trace de transaction

Pour exécuter une session de suivi de transaction manuellement, spécifiez les agents pour lesquels vous souhaitez effectuer le suivi des transactions et la période de capture des données. Spécifiez des filtres pour limiter le suivi des transactions qui ont dépassé le seuil de temps d'exécution, qui correspondent aux valeurs de paramètre ou qui contiennent des erreurs. Une fois la session de suivi de transaction lancée, les transactions correspondant aux critères de filtre s'affichent dans la table de transaction. Les événements de transaction incluent des traces et des erreurs de transaction.

Vous devez disposer d'une autorisation `run_tracer` pour exécuter une nouvelle session de suivi de transaction.

Procédez comme suit :

1. Dans APM Team Center, cliquez sur **WebView**.
APM WebView s'affiche.

2. Cliquez sur **Outils**, puis sur **Outil de suivi de transaction**.
3. Cliquez sur **Démarrer la session de suivi**.
4. Dans la zone Effectuer le suivi de transactions :
 - Spécifiez la durée minimale de la trace de transaction. Dans la liste déroulante, sélectionnez millisecondes ou secondes. La valeur par défaut est 5000 millisecondes.
 - (Facultatif) Spécifiez l'une des conditions de filtre ci-dessous pour la trace de transaction.
 - **Est égal à**
Valeur de paramètre qui correspond aux chaînes suivies.
 - **N'est pas égal**
Valeur de paramètre qui ne correspond pas à la chaîne suivie. Les transactions qui n'incluent pas le paramètre auquel le filtre s'applique sont elles aussi suivies.
 - **Contains** : valeur de paramètre contenant la chaîne suivie
 - **Starts with** : valeur de paramètre qui commence par la chaîne suivie
 - **Finit par**
Valeur de paramètre qui finit par la chaîne suivie.
 - **Existe**
Les transactions qui incluent le paramètre auquel le filtre s'applique sont suivies, quelle que soit la valeur du paramètre.
 - **N'existe pas**
Les transactions qui n'incluent pas le paramètre auquel le filtre s'applique sont suivies.
5. Entrez la durée de la session de suivi.
6. Dans la zone **Effectuer le suivi d'agents**, sélectionnez un ou plusieurs agents pour lesquels les transactions doivent être suivies :
 - Pour suivre tous les agents, cliquez sur **Effectuer le suivi de tous les agents pris en charge**. Cette option permet d'effectuer le suivi des agents pris en charge et actuellement connectés, ainsi que des agents qui se connectent pendant la session de suivi.
 - Pour suivre les agents sélectionnés, cliquez sur **Effectuer le suivi des agents sélectionnés** et sélectionnez des agents dans la liste (**Ctrl + clic** pour sélectionner plusieurs agents).
7. Cliquez sur **OK** pour démarrer la session de suivi de transaction.
Une fois la session démarrée, la barre d'état située dans le panneau inférieur affiche les informations suivantes :
 - Nombre de transactions suivies et description brève de la configuration de la trace.
 - Temps restant dans la session.
 En mode dynamique, l'onglet **Traces** répertorie les événements de trace de transaction pour les 20 dernières minutes. En d'autres termes, les événements de trace de transaction de plus de 20 minutes ne s'affichent pas en mode dynamique. Un maximum de 500 événements de trace de transaction sont répertoriés.

Arrêt, redémarrage et basculement des sessions de suivi de transaction

Vous pouvez gérer la session de suivi dans l'onglet **Outil de suivi de transaction** comme suit :

- Cliquez sur **Arrêter le suivi** pour finaliser la session.
- Cliquez sur **Redémarrer la trace** pour continuer à suivre les transactions dans les agents cibles en utilisant les mêmes conditions. Vous pouvez redémarrer une session de suivi de transaction :
 - Après l'expiration d'une session.
 - Pour redémarrer une session que vous avez arrêtée.
 - Pour redémarrer une session en cours.
- Cliquez sur **Changer de trace** pour sélectionner une autre session de suivi à exécuter.

Recherche de la trace pertinente

Vous examinez une trace unique pour collecter les informations concernant le problème d'application.

Procédez comme suit :

1. Analysez les informations de l'activité de suivi pour la session de suivi dans la table de transaction. Sélectionnez une ligne de table pour afficher d'autres détails.
2. Réexécutez, arrêtez, redémarrez ou basculez les sessions de suivi, si nécessaire.
3. Examinez les onglets **Vue récapitulative**, **Vue Suivi** et **Vue Arborescence** dans le volet inférieur. Les informations peuvent vous aider à diagnostiquer et à trier les problèmes d'application et les problèmes de performances.

Description des points d'entrée

La détection automatique des points d'entrée permet de rapidement surveiller et trier les applications Java sans configurer manuellement les directives ProbeBuilder.

Lorsque l'instrumentation intelligente et la détection de points d'entrée sont activées, Introscope surveille les threads qui sont impliqués dans les transactions d'appel de socket client. L'instrumentation intelligente et la détection des points d'entrée sont activées par défaut. Les *points d'entrée* sont les points de début de transaction. Un moteur de règles dans l'agent identifie les points d'entrée candidats. L'agent instrumente et surveille le point d'entrée candidat apparu le plus tôt dans le thread de transaction. Un point d'entrée qu'un agent détecte et conserve est activé pour la surveillance par tous les agents utilisant le même répertoire d'installation. Toutefois, lorsque plusieurs agents partagent l'instrumentation, la génération de rapports sur les mesures dépend des machines virtuelles Java exécutant les mêmes classes de code ou Framework sur le serveur d'applications.

Voici quelques exemples de transactions dans lesquelles la détection des points d'entrée offre automatiquement une visibilité :

- Piles et infrastructures technologiques que l'instrumentation Introscope ne surveille pas déjà
- Appels d'API personnalisés ou propriétaires
- Threads d'arrière-plan qui consomment des ressources critiques et peuvent réduire les performances globales de l'application

NOTE

La détection des points d'entrée ne prend pas en charge le protocole UDP (User Datagram Protocol).

L'agent enregistre les points d'entrée dans le fichier `AutoPersist.pbd`, qui est conservé dans le répertoire `<répertoire_base_agent>\core\config\hotdeploy`.

WARNING

L'utilisateur système qui exécute le serveur d'applications requiert un accès en lecture/écriture au répertoire / hotdeploy. Ces autorisations permettent à l'agent d'écrire des données dans le fichier

```
AutoPersist.pbd
```

Les points d'entrée diffèrent des composants frontaux. L'agent Java détecte automatiquement les points d'entrée, qui se trouvent à proximité du début du chemin d'appel de transaction. Les composants frontaux sont définis manuellement dans les directives PBD et peuvent se trouver n'importe où dans un chemin d'appel de transaction.

WARNING

N'apportez pas de modifications manuelles au fichier

```
AutoPersist.pbd
```

. Toutefois, vous pouvez copier les points d'entrée détectés et les utiliser dans une autre directive PBD.

Les mesures des points d'entrée s'affichent dans l'arborescence centrée sur l'agent, dans le sous-noeud Point d'entrée automatique, sous le noeud de l'agent.

NOTE

Vérifiez que la propriété `introscope.autoprobe.dynamicinstrument.enabled` dans le fichier `IntroscopeAgent.profile` est définie sur `true`. Cette configuration permet à l'agent de signaler des mesures de point d'entrée sans devoir redémarrer l'application.

Introscope signale les cinq mesures Blame standard pour chaque point d'entrée. Les points d'entrée s'affichent dans les traces de transaction, mais pas dans la carte. Les noms de point d'entrée respectent le format suivant : `entry point <nom-classe _ nom-méthode>`. Introscope signale [les mesures de prise en charge de la détection des points d'entrée](#).

Vous pouvez [configurer la collecte de points d'entrée](#). Par exemple, une propriété de configuration limite le nombre de points d'entrée que le fichier `AutoPersist.pbd` peut conserver.

NOTE

Informations complémentaires : [Création de fichiers PBD pour la conversion de points d'entrée en composants frontaux](#)

Présentation des composants d'arrière-plan automatiques

Lorsque la *détection automatique des composants d'arrière-plan* est activée, l'agent détecte et surveille automatiquement les composants d'arrière-plan d'application sans qu'aucune configuration manuelle ne soit requise.

Un moteur de détection dans l'agent identifie les composants d'arrière-plan automatiques candidats. Les composants d'arrière-plan automatiques qu'un agent détecte et conserve sont activés pour la surveillance par tous les agents utilisant le même répertoire d'installation.

Voici quelques exemples de composants d'arrière-plan que la détection des composants d'arrière-plan automatiques peut trouver et surveiller :

- Piles et infrastructures technologiques en arrière-plan que l'agent ne surveille pas déjà. MongoDB et Cassandra sont des exemples de composants d'arrière-plan non SQL.
- Composants d'arrière-plan propriétaires ou personnalisés

L'agent enregistre les composants d'arrière-plan automatiques dans le fichier `AutoPersist.pbd`, qui est conservé dans le répertoire `<répertoire_base_agent>\core\config\hotdeploy`.

WARNING

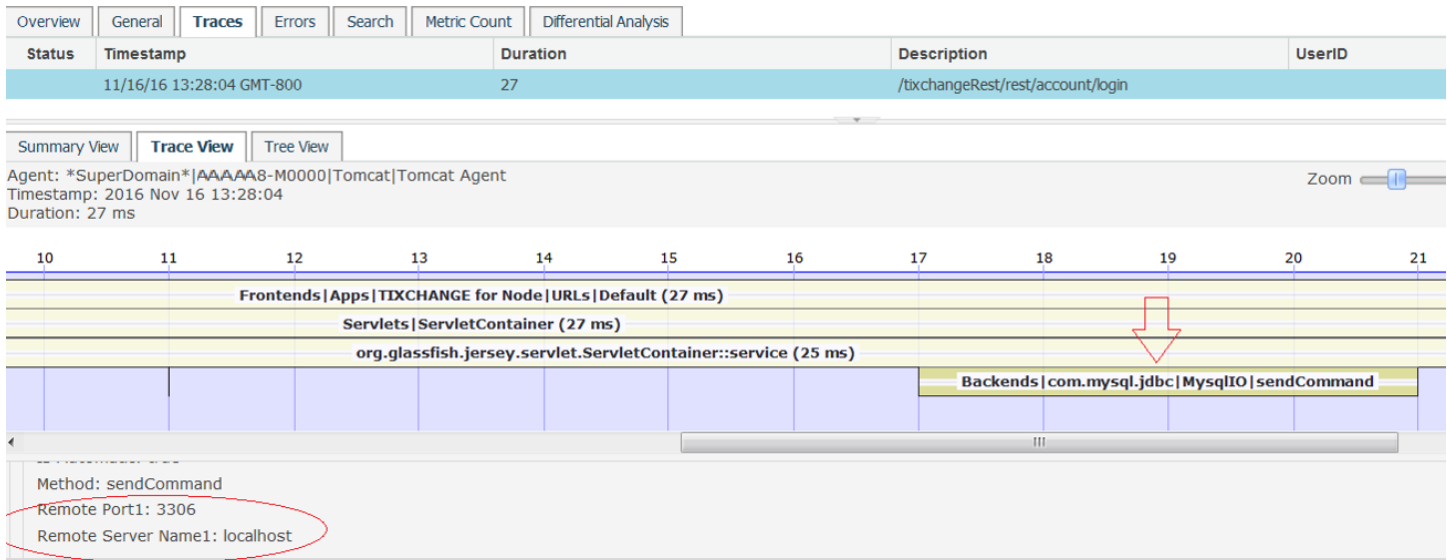
- L'utilisateur système qui exécute le serveur d'applications requiert un accès en lecture/écriture sur le répertoire `/hotdeploy`. Ces autorisations permettent à l'agent d'écrire des données dans le fichier `AutoPersist.pbd`.
- N'apportez pas de modifications manuelles au fichier `AutoPersist.pbd`. Toutefois, vous pouvez copier des composants d'arrière-plan automatiques détectés et les utiliser dans un autre fichier PBD.

Vous pouvez [configurer la détection des composants d'arrière-plan automatiques](#). Par exemple, une propriété de configuration limite le nombre de composants d'arrière-plan automatiques que le fichier `AutoPersist.pbd` peut conserver.

Dans la vue **Suivi**, les paramètres de `port distant` et de `nom de serveur distant` apparaissent dans les **détails du composant**.

Notez le chemin d'appel d'arrière-plan et les paramètres dans cette trace de transaction :

- Le composant de trace de transaction pour le chemin d'appel d'arrière-plan est : `Backends|com.mysql.jdbc|MySQLIO|sendCommand`.
- Le paramètre de port distant est `3306` et le paramètre d'hôte serveur distant est `Name1: localhost`.



Présentation des composants de visibilité approfondie

Lorsque l'instrumentation intelligente est activée, les agents détectent et collectent automatiquement des informations détaillées sur les composants de transaction au niveau de la méthode. Les agents détectent et instrumentent automatiquement les composants de visibilité approfondie, sans utiliser de fichiers de directives ProbeBuilder (PBD). Introscope analyse la complexité des méthodes afin de déterminer les appels et les composants à instrumenter et à afficher comme composants de visibilité approfondie.

Remarque : L'instrumentation intelligente est disponible uniquement pour les agents Java et pas pour les agents .NET.

Choses à savoir à propos des composants de visibilité approfondie :

- Une icône représentant un éclair indique un composant de visibilité approfondie. L'étiquette Composant de trace profonde s'affiche également dans l'info-bulle lorsque vous passez le curseur de votre souris sur ce composant.
- Les composants de visibilité approfondie n'incluent pas de liens vers les mesures. Aucune donnée de mesure ne s'affiche dans l'arborescence Investigator ou dans la carte.
- Ils contiennent uniquement le nom de classe, le nom de méthode et la durée.
- Les propriétés suivantes s'affichent dans les détails du composant :
 - Instrumentation Level (Niveau d'instrumentation)
Niveau d'instrumentation intelligente auquel une transaction a été détectée.
 - Method Level Score (Indice du niveau de méthode)
Niveau d'instrumentation intelligente qui est en corrélation avec l'indice que l'algorithme d'évaluation Introscope affecte à la méthode d'un composant de visibilité approfondie. Introscope peut afficher les méthodes de composant de visibilité approfondie dont les indices varient dans une trace de transaction, une erreur ou un blocage. Par exemple, une transaction détectée à l'aide d'un niveau moyen peut afficher les méthodes dont les indices de niveau sont à la fois moyens et faibles.

Utilisez ces propriétés pour comprendre la profondeur de la visibilité de l'instrumentation intelligente d'une trace de transaction et des méthodes dans une trace. Par exemple, vous pouvez comparer le nombre de méthodes que l'instrumentation intelligente détecte à deux niveaux d'infrastructure différents. Vous pouvez noter le niveau d'instrumentation intelligente auquel Introscope a évalué des méthodes spécifiques. Vous pouvez ajuster la solution de surveillance pour la surveillance de visibilité, l'équilibrage de charge et la visibilité souhaités.

Les composants instrumentés et les composants de visibilité approfondie standard peuvent apparaître dans une session de suivi de transaction.

Vous pouvez configurer la profondeur de la visibilité de l'instrumentation intelligente d'après votre environnement et vos exigences.

Analyse des données de suivi et collaboration pour l'analyse des problèmes

Vous pouvez exporter le fichier JSON (JavaScript Object Notation) pour un ou plusieurs suivis de transaction. Utilisez un simple éditeur ou recherchez dans le fichier un composant ou les paramètres d'un composant. Partagez le fichier par courriel ou sur un lecteur réseau partagé pour permettre aux utilisateurs de collaborer pour l'analyse des problèmes. Un autre utilisateur peut charger le fichier exporté pour afficher les mêmes informations. Cette perspective partagée facilite la collaboration afin de déterminer rapidement si un composant est disponible ou rencontre des problèmes de performances. Par exemple, vous pouvez examiner si les utilisateurs peuvent se connecter, extraire les données ou les afficher. Vous pouvez voir les temps de réponse des utilisateurs et les causes des problèmes lorsqu'ils se produisent.

Pour exporter ou charger un fichier JSON de suivi, utilisez l'onglet **Transactions métier**. Pour ouvrir l'onglet, utilisez le Carnet d'analyse, puis cliquez sur le problème de votre choix.

Exportation d'un fichier JSON de suivi

Exportez les données de suivi dans un fichier JSON à des fins d'analyse ou de partage.

Procédez comme suit :

1. Cliquez sur l'onglet **Transactions métier**.
2. Cliquez sur un segment de transaction ou un composant qui vous intéresse, puis sur **Charger**.
Le nom du fichier téléchargé s'affiche au bas de la page.
3. (Facultatif) Ouvrez le fichier et analysez les données :
 - Utilisez un éditeur tel que [JSON Editor Online](#).
 - Faites glisser le fichier dans Chrome.

NOTE

Les informations de la vue **Cliché** ne sont pas disponibles dans le fichier JSON exporté.

Chargement d'un fichier JSON de suivi

Chargez les données de suivi dans un fichier JSON pour afficher une perspective partagée.

Procédez comme suit :

1. Cliquez sur l'onglet **Transactions métier**.
Une liste affiche les données de suivi qui correspondent au composant.
2. Cliquez sur l'icône **Charger le fichier de suivi JSON**  pour charger les données de liste ou cliquez sur un segment de transaction de votre choix, puis sur l'icône **Charger le fichier de suivi JSON**.
3. Recherchez et sélectionnez le fichier <nom>.json et cliquez sur **Ouvrir**.

NOTE

La taille maximum autorisée du fichier JSON est 52,4288 Mo. La pile graphique Détails de la transaction reflète les données JSON chargées.

Surveillance des performances et des événements du navigateur

L'agent de navigateur permet de surveiller les mesures et les erreurs relatives aux performances de chargement de pages Web. Vous pouvez identifier la cause de la dégradation des performances du navigateur, du réseau ou du serveur d'applications.

En tant que propriétaire de l'application, suivez ces étapes générales :

1. Utilisez les procédures standard pour surveiller les performances :

NOTE

[Surveillance des performances à l'aide de la vue Expérience](#)

[Examen des performances médiocres des transactions](#)

[Diagnostic des problèmes de chargement des ressources](#)

2. Lisez et utilisez les informations supplémentaires ci-dessous, spécifiques de l'agent de navigateur :

Surveillance des performances de l'application avec l'agent de navigateur

Vous pouvez surveiller le temps de réponse du navigateur pour votre application gérée et examiner vos applications sous diverses perspectives telles que celle des services d'entreprise et de leurs dépendances. Une carte est automatiquement générée à partir des performances et de l'analyse des mesures, erreurs et événements.

NOTE

Seules les mesures de chargement de pages s'affichent dans la carte. Les mesures relatives aux infrastructures structurelles de type AJAX n'apparaissent pas dans la carte.

Procédez comme suit :

1. Dans le volet gauche, cliquez sur **Vue Expérience**.
La vue Expérience affiche les fiches d'expérience individuelles. Chaque fiche affiche un récapitulatif. Les éléments en rouge indiquent des transactions lentes ou ayant échoué.
2. Parcourez les fiches et cliquez sur l'icône de **carnet** au niveau de la fiche de votre choix.
Le carnet d'analyse indique des détails concernant l'expérience. Le flux de relation affiche les chemins de transaction des expériences sélectionnées. Cette carte fournit le contexte de l'événement qui s'est produit.
3. (Facultatif) Dans la liste déroulante **Perspective**, sélectionnez **Type**.
4. Analysez la carte et identifiez le premier composant (composant le plus à gauche) dans une série de dépendances indiquant des problèmes de performance. Ce composant peut être à l'origine de la détérioration des performances dans votre environnement d'application.
5. Cliquez sur un **composant** dans la carte.
L'onglet Mesures affiche les mesures BlamePoint et W3C.
6. (Facultatif) Dans l'onglet **Mesures**, cliquez sur un **nom de mesure**, par exemple Correspondances de page par intervalle.
L'arborescence des mesures s'ouvre et indique la mesure spécifique.
7. Utilisez ces informations pour étudier les problèmes de performances.

Analyse des mesures de l'agent de navigateur

Les applications dont les performances sont médiocres peuvent détériorer l'expérience de l'utilisateur final. Vous pouvez afficher les données actives dans l'arborescence de mesures et simplifier ainsi l'analyse et la résolution des problèmes de performances. L'arborescence des mesures, des ressources et des agents s'actualise toutes les 15 secondes pour afficher les données de mesure actuelles.

Toutes les mesures de l'agent de navigateur s'affichent à l'emplacement suivant :

- Noeud **Agent Dx**, **Segment de marché**. Les descriptions de chemin de mesure dans les sections suivantes indiquent les chemins de l'**agent Dx**.

NOTE

Toutes les valeurs de mesure de l'agent de navigateur sont arrondies. Ajoutez un lien vers la section Calculs de l'agent de navigateur ou ajoutez individuellement les valeurs de chaque sous-rubrique ci-dessous aux calculs spécifiques.

Mesures de chargement de la page

L'agent Navigateur signale les temps de réponse et les événements du navigateur pour les pages Web. Le cas échéant, il signale les temps de réponse de son propre navigateur. Des limitations s'appliquent à certains navigateurs :

- Aucun déchargement de page précédente n'est associé pour une page initiale.
- Si un chargement de page attend que l'utilisateur saisisse du texte, cette période est incluse dans la mesure Durée moyenne de chargement de la page (ms).

Le tableau ci-dessous décrit le mode de calcul des mesures de chargement de page pour les navigateurs. La colonne Calcul de mesure indique le calcul mathématique que l'agent de navigateur utilise pour obtenir une mesure spécifique. Par exemple, la durée moyenne de rendu de la page (ms) s'obtient par soustraction de la durée de deux événements à partir du navigateur : loadEventEnd et domComplete.

Mesure	Description	Calcul de mesure
Durée moyenne de rendu de la page (ms)	Temps nécessaire pour le rendu du contenu après le traitement du modèle d'objet de document (DOM).	Durée loadEventEnd - durée domComplete
Temps moyen d'établissement de la connexion (ms)	Durée que le navigateur met pour établir la connexion TCP au serveur.	Durée connectEnd - durée connectStart
Temps de recherche de domaine moyen (ms)	Durée que le navigateur met pour effectuer la recherche du service de noms pour le domaine de la page Web actuelle.	Durée domainLookupEnd - durée domainLookupStart
Temps de traitement DOM moyen (ms)	Durée qui s'écoule entre le début de la navigation et le traitement du modèle d'objet de document (DOM) par le navigateur. Remarque : Cette durée n'indique pas le moment où tous les objets dans le DOM sont extraits et chargés.	Durée domComplete - durée domLoading
Durée moyenne de chargement de la page (ms)	Durée qui s'écoule entre le début de la navigation et le chargement de tous les composants par le navigateur et l'affichage de la totalité de la page.	Durée loadEventEnd - durée navigationStart
Durée moyenne de déchargement de la page précédente (ms)	Durée nécessaire pour le déchargement de la page affichée précédemment. Aucune valeur n'est disponible s'il n'existe aucune page à décharger (par exemple, lorsqu'une session de navigateur est lancée).	Durée unloadEventEnd - durée unloadEventStart
Délai moyen avant le premier octet (ms)	Durée que met le navigateur pour recevoir le premier octet de la réponse en provenance du cache du serveur ou du cache de l'application.	Durée responseStart - durée requestStart
Délai moyen avant le dernier octet (ms)	Durée que met le navigateur pour recevoir le dernier octet de la réponse en provenance du cache du serveur ou du cache de l'application.	Durée responseEnd - durée requestStart
Erreurs JavaScript par intervalle	Nombre d'occurrences d'une erreur JavaScript dans la page Web surveillée au cours d'un intervalle donné.	Non applicable
Clics sur la page par intervalle	Nombre de fois où la page Web surveillée a été demandée au cours d'un intervalle donné.	Non applicable

Durée moyenne de blocage de la page	Durée que la demande de page a passé à attendre avant d'avoir pu être distribuée.	(durée connectStart - durée domainLookupEnd) + (durée requestStart - durée connectEnd)
-------------------------------------	---	--

L'agent de navigateur utilise les seuils où les mesures de navigateur ne peuvent pas être créées ni signalées. Les mesures de seuil de chargement de page, les mesures asynchrones et les mesures de fonction JavaScript possèdent des seuils par défaut qui sont configurables. Les durées du navigateur doivent respecter les limites de seuil pour que les mesures puissent être créées.

Les mesures de navigateur peuvent ne pas être créées dans l'arborescence de mesures, car elles ne sont pas collectées. Elles n'apparaissent alors pas dans la carte. Par exemple, si la valeur Délai moyen avant le dernier octet (ms) ne s'affiche pas dans l'arborescence des mesures, elle n'apparaît pas dans la carte.

L'agent Navigateur signale les temps de réponse et les événements du navigateur pour les pages Web. Le cas échéant, il utilise l'API Mesure des durées Navigation W3C pour signaler les temps de réponse de son navigateur. Cette API est une interface implémentée par les navigateurs les plus récents. Des limitations s'appliquent à certains de ces navigateurs :

- Aucun déchargement de page précédente n'est associé pour une page initiale.
- Si un chargement de page attend que l'utilisateur saisisse du texte, cette période est incluse dans la mesure Durée moyenne de chargement de la page (ms).

Lorsqu'une transaction métier n'est pas démarrée pour la page de niveau supérieur, les mesures s'affichent à l'emplacement suivant :

- Business Segment | <Page_URL_HOST>/<Page_URL_PORT> | <Page_URL_Path>

Lorsqu'une transaction métier est démarrée pour la page de niveau supérieur, les mesures s'affichent à l'emplacement suivant :

- Business Segment | <Business_Service> | <Business_Transaction> | <Business_Transaction_Component> | Browser

NOTE

Lorsque des erreurs surviennent, l'agent de navigateur incrémente la mesure Erreurs de page par intervalle dans le chemin des mesures de page. Cette mesure indique le nombre total d'erreurs JavaScript et AJAX sur la page.

Mesures de chargement de page logicielle

Les applications à page unique réalisent une demande de page unique pour extraire l'ensemble du contenu de cette page au chargement de la page initiale. Les applications peuvent alors obtenir les ressources à partir du serveur de façon dynamique et mettre à jour l'interface utilisateur suite aux interactions de l'utilisateur. De nombreuses applications à page unique utilisent des propriétés de hachage des API d'historique HTML5 et de l'emplacement URI pour indiquer la navigation utilisateur logique sur la même page Web. Ce type de navigation utilisateur logique qui déclenche des modifications de l'itinéraire sans recharger la page entière est désigné sous le nom de navigation parmi les pages logicielles. L'agent de navigateur surveille la durée de chargement des pages logicielles et signale la mesure Durée moyenne de chargement de la page (ms). Il surveille également le nombre de fois où la page logicielle surveillée a été visitée au cours d'un intervalle donné. L'agent de navigateur indique ce nombre sous forme de mesure Correspondances de page par intervalle. Ces informations fournissent une visibilité plus complète sur l'expérience de l'utilisateur final des applications à page unique.

Les mesures suivantes sont disponibles pour les applications à page unique et la navigation parmi les pages logicielles. Ces calculs de mesure utilisent les variables suivantes :

- TSPE = Heure de début de la navigation dans les pages logicielles (modification de l'itinéraire sans chargement de page)
- TSPS = Heure de finalisation du chargement de page logicielle

Mesure	Description	Calcul de mesure
Durée moyenne de chargement de la page (ms)	Durée moyenne entre le début de la navigation dans les pages logicielles (modification de l'itinéraire sans chargement de page) et la fin du chargement de la page logicielle.	TSPE - TSPS
Clics sur la page par intervalle	Nombre de fois où la page logicielle surveillée a été visitée au cours d'un intervalle donné.	Non applicable

Lorsqu'une navigation dans les pages logicielles a lieu, les mesures Durée moyenne de chargement de la page (ms) et Correspondances de page par intervalle s'affichent sous le noeud Hachage de page logicielle de la page de niveau supérieur :

- Business Segment | <Page_URL_HOST>/<Page_URL_PORT> | <Page_URL_Path> | <Page_Path> | <Soft_Page_Hash>

Lorsqu'une transaction métier est lancée pour la page de niveau supérieur, les mesures de page logicielle s'affichent à l'emplacement suivant :

- Business Segment | <Business_Service> | <Business_Transaction> | <Business_Transaction_Component> | Browser | <Soft_Page_Hash>

Mesures AJAX

Pour les applications Web, l'agent de navigateur peut fournir les temps de réponse du navigateur pour les pages Web dynamiques dans les infrastructures structurales telles qu'AJAX (Asynchronous JavaScript and XML).

L'agent de navigateur ne prend pas en charge les éléments suivants :

- Rappels AJAX imbriqués
- Demandes AJAX synchrones
- Fonctions de rappel telles que `XMLHttpRequest.onerror` et `XMLHttpRequest.ontimeout` . (Les heures d'exécution de rappel sont prises en charge pour `XMLHttpRequest.onreadystatechange` et `XMLHttpRequest.onload`.)
- Icône

NOTE

Pour plus d'informations sur la prise en charge, reportez-vous à la [matrice de compatibilité du produit](#).

Les mesures suivantes sont disponibles pour les infrastructures utilisant AJAX. Ces calculs de mesure utilisent les variables suivantes :

- TSE = Heure de fin de l'appel d'envoi AJAX
- TFB = Heure de réception du premier octet de la réponse du serveur par le navigateur
- TLB = Heure de réception du dernier octet de la réponse du serveur par le navigateur
- TCS = Heure de début de l'exécution du rappel AJAX
- TCE = Heure de fin de l'exécution du rappel AJAX

Mesure	Description	Calcul de mesure
Durée moyenne d'exécution du rappel (ms)	Durée moyenne nécessaire aux fonctions de rappel <code>XMLHttpRequest.onreadystatechange</code> ou <code>XMLHttpRequest.onload</code> pour traiter la réponse du serveur.	TCE - TCS
Nombre d'appels par intervalle	Nombre total de fois où la demande AJAX a été effectuée dans un intervalle donné.	Non applicable
Délai moyen avant le premier octet (ms)	Durée moyenne écoulée entre le moment où la demande AJAX est émise pour une ressource HTTP et la réception du premier octet de la réponse du serveur.	TFB - TSE
Durée moyenne de chargement de la ressource (ms)	Durée moyenne écoulée entre le moment où la demande AJAX est émise pour une ressource HTTP et la fin du rappel AJAX (fonction responsable de la réception et du traitement des données du serveur).	TCE - TSE
Temps de téléchargement de réponse moyen (ms)	Durée moyenne écoulée entre la réception du premier octet et du dernier octet de la réponse du serveur.	TLB - TFB

NOTE

Pour les appels AJAX, les mesures Temps de téléchargement de réponse moyen (ms) et Durée moyenne d'exécution du rappel (ms) sont signalées indépendamment l'une de l'autre. Ces mesures ne peuvent pas être signalées en raison de limitations au niveau de certaines infrastructures AJAX, en particulier pour les appels AJAX via jQuery 1.x.

- L'agent de navigateur peut ne pas signaler la mesure Durée moyenne d'exécution du rappel (ms) pour le premier appel AJAX.
- L'agent de navigateur peut ne pas signaler de valeur pour les propriétés Temps de téléchargement de réponse moyen (ms) et Délai moyen avant le premier octet (ms).

Un appel AJAX peut avoir lieu dans la page de niveau supérieur ou dans la page logicielle. Les mesures AJAX sont réparties par demandes asynchrones et par demandes synchrones :

Mesures AJAX synchrones

Lorsqu'une transaction métier n'est pas démarrée pour la page de niveau supérieur, les mesures AJAX s'affichent sous le noeud Ressources de la page.

- Business Segment | <HOST/PORT> | <Page_Path> | Resources | AJAX Call | Sync | <AJAX_URL_HOST>/<AJAX_URL_PORT> | <AJAX_URL_Path>
- Business Segment | <HOST/PORT> | <Page_Path> | <Soft_Page_Hash> | Resources | AJAX Call | Sync | <AJAX_URL_HOST>/<AJAX_URL_PORT> | <AJAX_URL_Path>

Lorsqu'une transaction métier est démarrée pour la page de niveau supérieur, les mesures AJAX s'affichent à l'emplacement suivant :

- Business Segment | <Business_Service> | <Business_Transaction> | <Business_Transaction_Component> | Browser | Resources | AJAX Call | Sync | <AJAX_URL_HOST>/<AJAX_URL_PORT> | <AJAX_URL_Path>
- Business Segment | <Business_Service> | <Business_Transaction> | <Business_Transaction_Component> | Browser | <Soft_Page_Hash> | Resources | AJAX Call | Sync | <AJAX_URL_HOST>/<AJAX_URL_PORT> | <AJAX_URL_Path>

Lorsqu'une transaction métier est démarrée pour l'appel AJAX, elle a priorité sur la transaction métier qui est lancée pour la page de niveau supérieur. Les mesures AJAX s'affichent à l'emplacement suivant :

- Business Segment | <Business_Service_AJAX> | <Business_Transaction_AJAX> | <Business_Transaction_Component_AJAX> | Browser | Resources | AJAX Call | Sync | <AJAX_URL_HOST>/<AJAX_URL_PORT> | <AJAX_URL_Path>

Mesures AJAX asynchrones

Lorsqu'une transaction métier n'est pas démarrée pour la page de niveau supérieur, les mesures AJAX s'affichent sous le noeud Ressources de la page.

- Business Segment | <HOST/PORT> | <Page_Path> | Resources | AJAX Call | Async | <AJAX_URL_HOST>/<AJAX_URL_PORT> | <AJAX_URL_Path>
- Business Segment | <HOST/PORT> | <Page_Path> | <Soft_Page_Hash> | Resources | AJAX Call | Async | <AJAX_URL_HOST>/<AJAX_URL_PORT> | <AJAX_URL_Path>

Lorsqu'une transaction métier est démarrée pour la page de niveau supérieur, les mesures AJAX s'affichent à l'emplacement suivant :

- Business Segment | <Business_Service> | <Business_Transaction> | <Business_Transaction_Component> | Browser | Resources | AJAX Call | Async | <AJAX_URL_HOST>/<AJAX_URL_PORT> | <AJAX_URL_Path>
- Business Segment | <Business_Service> | <Business_Transaction> | <Business_Transaction_Component> | Browser | <Soft_Page_Hash> | Resources | AJAX Call | Async | <AJAX_URL_HOST>/<AJAX_URL_PORT> | <AJAX_URL_Path>

Lorsqu'une transaction métier est démarrée pour l'appel AJAX, elle a priorité sur la transaction métier qui est lancée pour la page de niveau supérieur. Les mesures AJAX s'affichent à l'emplacement suivant :

- Business Segment | <Business_Service_AJAX> | <Business_Transaction_AJAX> | <Business_Transaction_Component_AJAX> | Browser | Resources | AJAX Call | Async | <AJAX_URL_HOST>/<AJAX_URL_PORT> | <AJAX_URL_Path>

NOTE

Lorsqu'un appel AJAX contient une erreur, l'agent de navigateur incrémente la mesure Erreurs de ressource par intervalle sous le chemin de mesure AJAX.

Mesures de ressource Web

L'agent de navigateur signale les mesures de ressource Web pour toutes les ressources dans la page, de type image, CSS, JavaScript, etc. Les pages Web sont créées à partir du contenu qui n'est pas affichable à partir du téléchargement initial de la page elle-même. Ce contenu peut prendre la forme d'images, de sons ou d'autres supports. Par exemple, une application Web peut utiliser les services de distribution de contenu pour héberger des images et peut également intégrer des publicités. Ces éléments sous-jacents que la page référence et télécharge sont appelés des ressources. En tant qu'analyste, vous devez savoir si les performances médiocres d'une application trouvent leur origine dans l'application ou dans les ressources Web, qui peuvent être fournies par un tiers.

Les mesures de ressource Web de toutes les autres ressources dans la page s'affichent sous le noeud Ressources, HTML de la page :

- Business Segment | <Page_URL_HOST>/<Page_URL_PORT> | <Page_URL_Path> | <Page_Path> | Resources | HTML | <Resource_URL_HOST>/<Resource_URL_PORT> | <Resource_URL_Path>
- Business Segment | <Page_URL_HOST>/<Page_URL_PORT> | <Page_URL_Path> | <Soft_Page_Hash> | Resources | HTML | <Resource_URL_HOST>/<Resource_URL_PORT> | <Resource_URL_Path>

Lorsqu'une transaction métier est lancée pour la page, les mesures de ressource Web s'affichent à l'emplacement suivant :

- Business Segment | <Business_Service> | <Business_Transaction> | <Business_Transaction_Component> | Browser | Resources | HTML | <Resource_URL_HOST>/<Resource_URL_PORT> | <Resource_URL_Path>
- Business Segment | <Business_Service> | <Business_Transaction> | <Business_Transaction_Component> | Browser | <Soft_Page_Hash> | Resources | HTML | <Resource_URL_HOST>/<Resource_URL_PORT> | <Resource_URL_Path>

Procédez comme suit :

1. Dans le volet gauche, cliquez sur **Mesures**.
L'arborescence des mesures répertorie les mesures et autres informations sous forme d'arborescence. Les noeuds de haut niveau apparaissant immédiatement sous les noeuds de domaine représentent les agents installés sur des hôtes de serveur d'applications individuels ou l'équivalent. Un noeud est un emplacement où les informations sur les mesures sont rassemblées, puis affichées dans l'arborescence axée sur l'agent. Lorsque vous développez un noeud, vous pouvez afficher et rechercher des informations plus détaillées sur les mesures.
2. Développez le noeud **DxC Agent, Secteur d'activité**.
L'arborescence des mesures, des ressources et des agents s'actualise toutes les 15 secondes pour afficher les données de mesure actuelles.
3. Explorez les noeuds pour afficher les mesures de navigateur.
4. (Facultatif) Partagez l'URL avec vos collègues pour leur permettre d'afficher la même vue d'une mesure spécifique dans l'arborescence.

Analyse des erreurs

Les applications Web utilisent JavaScript pour réaliser des actions dont celles ci-dessous :

- Acceptation des informations d'utilisateur
- Création d'effets transitoires
- Rendu, voire présentation de données complexes

Une section non fonctionnelle d'une page Web est probablement à l'origine d'une erreur JavaScript ou AJAX. La solution de surveillance des erreurs JavaScript et AJAX incluse dans l'agent de navigateur offre une visibilité dans ces situations erronées.

Erreurs JavaScript

Le traitement des erreurs JavaScript peut avoir lieu localement à l'aide de blocs try ou catch ou globalement grâce à des gestionnaires d'événements. L'agent de navigateur utilise un gestionnaire global d'erreurs pour capturer toutes les erreurs JavaScript non interceptées dans la fenêtre de navigateur actuelle. L'agent Navigateur peut :

- Signaler le nombre d'erreurs JavaScript dans la mesure Erreurs de page par intervalle. Cette mesure s'affiche sous le chemin de mesure de page dans le contexte de transaction métier ou d'URL approprié.
- Collecter les informations concernant les erreurs JavaScript personnalisées et natives dans la fenêtre de navigateur, telles que le numéro de ligne et de colonne, l'horodatage et la trace de pile de l'erreur.
- Générer des clichés d'erreur par erreur avec les détails de l'erreur.

Erreurs AJAX

Les codes de statut AJAX peuvent indiquer un problème au niveau de vos terminaux AJAX. L'agent de navigateur signale tous les appels AJAX pour lesquels les codes de statut HTTP de réponse ci-dessous apparaissent comme des erreurs AJAX :

- Erreur Client 4XX
- Erreur Serveur 5xx

L'agent de navigateur capture également des informations sur une réponse d'erreur destinée à vous aider à comprendre les problèmes pour chacun de vos appels AJAX. L'agent Navigateur peut :

- Signaler le nombre total d'erreurs AJAX dans la page dans la mesure Erreurs de page par intervalle. Cette mesure s'affiche sous le chemin de mesure de page dans le contexte de transaction métier ou d'URL approprié.
- Signaler les erreurs de ressource par intervalle sous le chemin de mesure AJAX dans la transaction métier ou le contexte d'URL approprié(e).
- Capturer des informations sur une réponse d'erreur :
 - Code de statut de réponse, par exemple 404
 - Texte de statut de réponse, par exemple Introuvable
 - Messages d'erreur personnalisés en provenance de jQuery, par exemple un message d'erreur d'analyseur JSON et une trace de pile

Analyse des erreurs à partir du cliché d'erreur

L'agent de navigateur crée un cliché d'erreur JavaScript ou AJAX individuel par erreur. Chaque erreur qui a lieu sur une page Web surveillée dans le délai spécifique contient les informations suivantes :

- Nom du navigateur
- Version du navigateur
- URL de la page Web dans laquelle l'erreur s'est produite
- Description de l'erreur signalée par le navigateur
- Numéro de ligne de l'erreur signalée par le navigateur
- Numéro de colonne de l'erreur signalée par le navigateur
- Nom de fichier source signalé par le navigateur

Consultez le cliché d'erreur pour en savoir plus sur l'erreur, notamment pour connaître le chemin d'appel et les paramètres. Toutes les 15 secondes, un cliché d'erreur individuel affiche les erreurs JavaScript ou AJAX qui se sont produites dans cet intervalle.

Procédez comme suit :

1. Cliquez sur l'onglet **Transactions métier**.
Une liste récapitulative affiche les traces qui correspondent au composant. Les segments affichent les durées. Les segments sont codés au moyen d'une couleur afin d'indiquer les problèmes liés à une transaction. Le rouge, par exemple, indique une erreur.
2. Cliquez sur la trace de transaction de votre choix.
Les composants de transaction individuels s'affichent dans une pile graphique (graphique à secteurs).
3. Cliquez sur le secteur d'activité rouge de votre choix, sur une erreur JavaScript par exemple :
Secteur d'activité | <chemin_page> ou <transaction métier>/jserrors/error_SyntaxError.jsp (0 ms)
4. Affichez les **détails du composant** et les détails de l'erreur.

NOTE

Certains navigateurs ne fournissent pas de trace de pile. C'est le cas, par exemple, d'Internet Explorer 10, de Microsoft Edge et de Safari 9.x.

5. Identifiez les composants qui sont à l'origine du problème et suivez le processus de résolution de problèmes mis en place par votre organisation.

Accès à la station de travail et présentation

La station de travail est disponible dans DX APM. Cet article présente la procédure d'accès à la station de travail, l'emplacement des fonctions qui ont été déplacées et les fonctions qui ne sont pas disponibles.

- [Accès à la station de travail](#)
- [Présentation de la station de travail](#)

Accès à la station de travail

Vous pouvez télécharger la station de travail à partir de l'interface utilisateur. Pour plus d'informations sur le téléchargement et la connexion de la station de travail, consultez la rubrique [Connexion de la station de travail](#).

Présentation de la station de travail

Le tableau suivant décrit les fonctions non disponibles dans la station de travail. Utilisez la colonne Informations complémentaires pour savoir comment effectuer des tâches similaires dans l'interface utilisateur.

Table 1:

Fonction (Emplacement)	Description		Supprimée de la station de travail	Disponible dans l'interface utilisateur	Informations complémentaires
Carte de tri d'application (Investigator de la station de travail)	Présente une vue graphique de votre application gérée et affiche les erreurs et l'intégrité de cette application.		Oui	Oui	<ul style="list-style-type: none"> • Affichage des relations entre les composants dans la carte • Surveillance des performances à l'aide de la vue Expérience
Préférences de l'utilisateur > onglet Investigator (Station de travail, toutes les vues)	Permet d'activer ou de désactiver la fonction d'actualisation automatique pour l'affichage de la carte de tri d'application.		Oui	Oui	<ul style="list-style-type: none"> • Utilisation de la chronologie et de la surbrillance
Mappage des dépendances SOA (Investigator de la station de travail, navigateur de mesures, feuilles d'agent)	Fournit une représentation visuelle des services déployés dans l'environnement SOA et permet de surveiller et différents composants et connaître leur relation.		Oui	Non	N/D

Fonction (Emplacement)	Description		Supprimée de la station de travail	Disponible dans l'interface utilisateur	Informations complémentaires
Carte d'emplacement (Investigator de la station de travail, navigateur de mesures, feuilles d'hôte et d'agent)	Permet d'afficher la configuration et de surveiller les performances de votre infrastructure.		Oui	Oui	<ul style="list-style-type: none"> Affichage des relations entre les composants dans la carte Couches de carte
Arrêter le gestionnaire d'entreprise (Station de travail, Editeur de module de gestion, Gestionnaire)	Permet d'arrêter le gestionnaire d'entreprise de la station de travail et de vous déconnecter de la station de travail.		Oui	Non	N/D
Publier dans la MIB (Station de travail, Editeur de module de gestion, Gestionnaire)	Permet de capturer les données de mesures stockées dans les collections SNMP.		Oui	Non	N/D
Nouvelle action (Station de travail, Editeur de module de gestion, Eléments)	Permet de créer : <ul style="list-style-type: none"> Une action de notification de console Une action de notification SNMP Une action d'envoi de courriel SMTP Une action de commande Shell Une action d'alerte SNMP 		Oui		<ul style="list-style-type: none"> Création et configuration d'actions de notification dans Team Center
Nouvelle session de suivi de transaction (Station de travail, toutes les vues)	Effectue le suivi de l'activité des transactions dans une application de production.		Oui	Oui	<ul style="list-style-type: none"> Démarrage d'une session de suivi de transaction Affichage des relations entre les composants dans la carte
Nouvelle visionneuse d'erreurs dynamique (Station de travail, toutes les vues)	Permet de rechercher des erreurs sur tous les agents surveillés par un gestionnaire d'entreprise en mode <i>dynamique</i> .		Oui	Oui	<ul style="list-style-type: none"> Recherche de solutions aux problèmes à l'aide du carnet d'analyse

Fonction (Emplacement)	Description		Supprimée de la station de travail	Disponible dans l'interface utilisateur	Informations complémentaires
Interrogation des événements historiques (Station de travail, toutes les vues)	Permet de rechercher des erreurs sur tous les agents surveillés par un gestionnaire d'entreprise en mode <i>historique</i> .		Oui	Oui	<ul style="list-style-type: none"> Recherche de solutions aux problèmes à l'aide du carnet d'analyse
Console de statut APM (Station de travail, toutes les vues)	Permet d'afficher des événements et des statuts importants pour un gestionnaire d'entreprise autonome ou en cluster.		Oui	Non	N/D

Présentation de la station de travail

La station de travail fournit un outil Investigator et une console pour l'affichage des données et de l'intégrité de l'application.

Via ProbeBuilder, DX APM ajoute des sondes d'agent à une application Java, PHP ou .NET. AutoProbe automatise ce processus et ProbeBuilder ajoute de manière dynamique des sondes au démarrage de l'application. Les fichiers PBD (ProbeBuilder Directive) indiquent à ProbeBuilder la procédure d'ajout des sondes, telles que des temporisateurs et des compteurs, aux composants Java, PHP ou .NET. Les sondes instrumentent l'application Web.

Les sondes mesurent des éléments d'information spécifiques d'une application sans modifier la logique métier de celle-ci. Un agent est installé sur le même ordinateur que l'application instrumentée. L'application Java se transforme en *application instrumentée* après l'installation de sondes dans le bytecode. Lorsqu'elle est exécutée avec des sondes, l'application Java devient une application gérée.

DX APM détecte et instrumente automatiquement les composants supplémentaires sans les directives ProbeBuilder définies.

Lors de l'exécution d'une application gérée, les sondes transmettent les données collectées à l'agent. L'agent collecte alors les données et les résume avant de les envoyer au gestionnaire d'entreprise.

Les données collectées par le gestionnaire d'entreprise sont accessibles via une ou plusieurs stations de travail. Vous pouvez utiliser la station de travail pour afficher les données de performances. Vous pouvez également configurer le gestionnaire d'entreprise pour qu'il effectue certaines tâches telles que la création d'alertes ou la collecte des informations en vue de leur analyse ultérieure.

Lorsqu'une application gérée est exécutée, les agents collectent les données de performances en temps réel et les envoient au gestionnaire d'entreprise. La station de travail permet d'effectuer les tâches suivantes :

- Configuration du gestionnaire d'entreprise
- Organisation des mesures
- Affichage des informations sélectionnées dans un format pratique

Surveillance des performances à l'aide des outils de la station de travail

Les outils de la station de travail simplifie la surveillance des performances de l'application grâce aux tâches suivantes :

- Filtrage et affichage des mesures de performance pour divers éléments du système sur lequel est exécutée votre application
- Navigation en profondeur afin de découvrir la cause première des problèmes de performances du système
- Création de vues graphiques des mesures

Accès aux différentes vues des données de mesure

La station de travail permet d'afficher les données de mesure sous différentes formes. Les utilisateurs autorisés peuvent effectuer des opérations d'administration et de configuration. La station de travail présente les informations dans les fenêtres suivantes :

- **Console**
Affiche les données dans des tableaux de bord, qui contiennent des visionneuses de données.
- **Investigator**
Présente les arborescences d'agents, d'applications, de ressources et de mesures.
- **Editeur de module de gestion**
Présente une arborescence des modules de gestion, permettant ainsi de créer et de modifier ces derniers.
- **Editeur de tableau de bord**
Permet aux utilisateurs disposant d'autorisations en *écriture* pour un domaine (ou superdomaine) de créer et de modifier des visionneuses de données et autres objets du tableau de bord tels que les images importées, les formes, les lignes ou encore le texte.
- **Visionneuses de données**
Présentation visuelle des données en fonction du type.

Connexion de la station de travail

La station de travail est disponible au téléchargement dans la section **Téléchargements** située dans le volet gauche. Par défaut, elle est configurée pour communiquer directement avec la passerelle cloud. Toutefois, les organisations qui requièrent une communication de canal unique entre le centre de données et la passerelle cloud peuvent relier la station de travail au proxy cloud.

A propos de la console de la station de travail

La console est la vue par défaut lorsque vous démarrez la station de travail. Elle contient des tableaux de bord qui affiche les données de performances dans des vues graphiques. Les tableaux de bord sont des outils de base pour l'affichage des données de gestion dans DX APM.

Le module de gestion par défaut fournit plusieurs modèles de tableaux de bord. Les utilisateurs autorisés peuvent créer des tableaux de bord personnalisés à l'aide de l'éditeur de tableau de bord.

Vous pouvez ouvrir plusieurs fenêtres Console à la fois.

Pour ouvrir une nouvelle fenêtre Console :

- Sélectionnez Poste de travail > Nouvelle console.

A propos de l'outil Investigator de la station de travail

Investigator permet d'afficher des mesures sur les applications et leurs serveurs d'arrière-plan de différentes façons. Vous pouvez avoir plusieurs fenêtres Investigator ouvertes en même temps.

Pour ouvrir une nouvelle fenêtre Investigator :

- Sélectionnez Station de travail > Nouvel Investigator.

Investigator s'ouvre et affiche des données sur votre application Java ou .NET.

Vous pouvez également ouvrir une fenêtre Investigator à partir de la console en double-cliquant sur certains éléments du tableau de bord, selon le mode de création de l'élément.

Onglet Navigateur de mesures

L'onglet Navigateur de mesures affiche une vue centrée sur l'agent de vos applications surveillées. Il permet d'effectuer les tâches suivantes :

- Affichage des applications et des mesures organisées dans une arborescence hiérarchique
- Surveillance des mesures détaillées pour chaque couche de technologie
- Utilisez la fonction de suivi des transactions pour trier les anomalies au niveau des performances de l'application.

A propos de l'éditeur de module de gestion

L'éditeur de module de gestion permet de créer ou de modifier un module de gestion, qui contient un ensemble d'informations sur la configuration de la surveillance dans DX APM. Les modules de gestion sont répertoriés pour chaque domaine.

Remarque : Si vous disposez d'une licence complète de DX APM, vous pouvez créer, modifier ou supprimer des informations dans l'éditeur de module de gestion. Si vous ne possédez pas de licence de ce type, vous pouvez uniquement afficher les informations.

L'arborescence de l'éditeur de module de gestion répertorie les modules de gestion déployés sur le gestionnaire d'entreprise par domaine.

La partie droite de l'éditeur de module de gestion présente les paramètres de configuration actuels pour l'élément sélectionné dans l'arborescence.

Les utilisateurs autorisés peuvent modifier les éléments dans l'éditeur de module de gestion.

A propos de l'éditeur de tableau de bord

L'éditeur de tableau de bord fournit des outils de création et de disposition des visionneuses de données, des formes, des lignes, des zones de texte et des connecteurs. Les utilisateurs disposant des autorisations appropriées peuvent créer et modifier des tableaux de bord et des objets de tableau de bord tels que les images importées, les formes, les lignes et le texte.

A propos des visionneuses de données

Les visionneuses de données dans l'onglet Navigateur de mesures ou dans un tableau de bord affichent les données provenant d'une application DX APM sous forme visuelle. Les visionneuses de données peuvent afficher les données d'une mesure, d'une ressource ou d'un élément, par exemple, une alerte.

Remarque : La valeur de temps indiquée sur les visionneuses de données correspond à l'horloge de l'ordinateur hébergeant le gestionnaire d'entreprise. Toutefois, elle est réglée sur le fuseau horaire dans lequel la station de travail est exécutée.

Types de visionneuses de données

Un type de visionneuse de données par défaut et d'autres visionneuses sont affectés aux types de données.

Type de données	Type de visionneuse de données par défaut	Peut également être affiché en tant que
Mesure	Graphique	Compteur de numérotations, graphique à barres, égaliseur graphique, visionneuse de chaîne, visionneuse de texte

Groupelement de mesures	Graphique	Graphique à barres, visionneuse de chaîne
Alerte	Indicateur d'alerte	Graphique, graphique à barres ou visionneuse de chaîne
Calculatrice	Graphique	Compteur de numérotations, graphique à barres, égaliseur graphique, visionneuse de chaîne

Selon le type de mesure ou d'élément, la station de travail peut afficher les données dans une visionneuse de données avec les types d'affichage de vue présentés ici.

Graphique

Les graphiques tracent les valeurs dans le temps. Dans les vues en temps réel, le graphique affiche de façon dynamique la dernière période prise en charge dans le graphique.

Si le graphique affiche une alerte, les seuils d'avertissement et de danger apparaissent sous forme de lignes jaunes et rouges, respectivement.

Vous pouvez modifier l'échelle des graphiques lors de l'affichage de données actives afin de consulter les données dans un affichage plus lisible.

Graphique à barres

Les graphiques à barres affichent les valeurs de données actuelles sous forme de barres horizontales. Il s'agit de l'affichage par défaut des vues N principaux filtrés.

Si un graphique à barres affiche une alerte, les barres sont vertes, jaunes ou rouges selon le statut de l'alerte.

Le graphique à barres est disponible pour l'affichage des données actives uniquement.

Egaliseur graphique

Les égaliseurs graphiques indiquent la valeur actuelle des données ainsi que les niveaux élevés récents.

Visionneuse de chaîne

Les visionneuses de chaîne peuvent afficher une valeur sous forme de ligne de texte. Elles permettent d'afficher des valeurs dans un espace relativement réduit. Vous pouvez également utiliser une visionneuse de chaîne pour les valeurs simples qui ne changent pas, telles que l'heure de lancement ou l'adresse IP.

Remarque : Avec les mesures dynamiques provenant des agents connectés, la plupart des données sont valides uniquement pour la dernière tranche de 15 secondes. Lorsqu'un agent se déconnecte, les mesures de chaîne n'affichent aucune valeur. Toutefois, certaines mesures constantes, telles que l'heure de lancement d'origine de l'agent, restent valides que l'agent soit connecté ou non.

Visionneuse de texte

Les visionneuses de texte affichent le texte des données lorsque de nouvelles valeurs sont ajoutées, par exemple, un journal système ou d'exceptions.

A propos des alertes et des indicateurs d'alerte

Les indicateurs d'alerte indiquent si une mesure a franchi un seuil :

- Disque vert = statut normal
- Losange jaune = seuil dépassé (avertissement)
- Octogone rouge = seuil dépassé (danger)
- Disque gris = alerte sans données

Les indicateurs d'alerte ci-dessus peuvent apparaître sous forme de tableau de trois indicateurs dans lequel l'indicateur actif indique le statut. Dans la plupart des cas, ils apparaissent comme un indicateur unique qui change de couleur et de forme d'après son statut.

Les indicateurs d'alerte peuvent apparaître dans plusieurs modes et emplacements :

- Dans les tableaux de bord
- Dans l'onglet Présentation
- En tant que lignes de seuil dans un graphique
- En tant que couleurs dans les cellules de table lorsque cette fonctionnalité est prise en charge
- A la place des noeuds d'arborescence

Différence entre les *alertes* et les *indicateurs d'alerte*

Il est important de comprendre ce qu'est une alerte. Veillez à faire la distinction entre :

- L'**alerte** elle-même dont la définition inclut des attributs enregistrée tels que :
 - des valeurs de seuil
 - le groupement de mesures auquel elle est liée
 - le module de gestion auquel elle appartient
- L'**indicateur d'alerte**, qui est un affichage graphique d'un statut d'alerte

Tri à l'aide de la station de travail

L'Investigator de la station de travail fournit une vue centrée sur l'agent permettant d'examiner les mesures et d'identifier les causes des problèmes potentiels dans votre environnement.

Fonctionnalités générales d'Investigator

Astuces de navigation

Pour ouvrir Investigator :

- Sélectionnez **Station de travail > Nouvel Investigator**.

Pour naviguer en avant et en arrière :

- Les flèches avant et arrière se trouvent dans le coin supérieur droit. Utilisez ces boutons pour avancer ou reculer entre les éléments de l'arborescence hiérarchique affichée précédemment.
- Sélectionnez une option dans les listes déroulantes en regard des flèches avant et arrière dans l'angle supérieur droit d'Investigator.

Volets d'Investigator

Investigator contient deux volets :

- Une arborescence hiérarchique dans un volet étroit sur la gauche
- Un volet de visionneuse plus grand sur le côté droit
 - Le contenu du volet de visionneuse varie selon le type d'élément sélectionné dans l'arborescence hiérarchique.
 - Un ou plusieurs onglets constituent le volet de visionneuse. Chaque onglet affiche une vue différente.

Les graphiques de mesures constituent la méthode la plus courante d'afficher les mesures, mais ne sont cependant pas la seule façon de le faire. Pour les mesures, une vue des données de mesures s'affiche. Chaque type de mesure a une vue par défaut dans le volet de visionneuse.

Info-bulles

Les info-bulles identifient les chemins et les valeurs de mesures dans les arborescences hiérarchiques et les volets de visionneuse. Pour accéder aux info-bulles dans l'onglet Navigateur de mesures, passez la souris sur le nom de la mesure dans une zone de légende de visionneuse de données.

Vous pouvez afficher différents types d'informations dans l'infobulle, en fonction de l'élément de l'interface utilisateur sur lequel se trouve le curseur. Ces informations peuvent inclure les données suivantes :

- Nom complet de la mesure, sa valeur et ses valeurs minimum et maximum
- Nombre de points de données signalés dans la tranche horaire sélectionnée
- Un horodatage de la valeur la plus proche du curseur ou une note de comparaison
- Par exemple, Valeur trop haute lorsque la valeur de mesure dépasse un seuil défini.

NOTE

Les infobulles ne sont plus disponibles à partir des noeuds.

Vue centrée sur l'agent

Un agent est un composant logiciel installé sur un hôte sur lequel une application est déployée. L'agent collecte les mesures d'applications et d'environnement, et les transmet au gestionnaire d'entreprise. L'onglet Navigateur de mesures permet de parcourir la liste complète des mesures que signale un agent unique. Chaque application dont les données sont signalées par un agent s'affiche dans une arborescence hiérarchique sous un noeud appelé **Frontends (Composants frontaux)**.

La vue centrée sur l'agent contient les sections suivantes :

- *L'arborescence centrée sur l'agent* à gauche fournit des informations sur chaque hôte et application que gère le gestionnaire d'entreprise. Les mesures qui apparaissent dans l'arborescence centrée sur l'agent dépendent des facteurs suivants :
 - Ressources utilisées par les applications.
 - Données que les agents Introscope sont configurés pour signaler.
- Le *volet Visionneuse* à droite présente les détails, souvent sous forme de graphique, de la ressource ou de la mesure dans l'arborescence. Vous pouvez sélectionner les onglets Afficher pour ouvrir les différentes vues de données. Les onglets disponibles dépendent de l'élément sélectionné dans l'arborescence. Pour certaines vues, vous pouvez disposer d'options permettant de contrôler les données affichées dans la visionneuse dans la partie inférieure du volet Visionneuse.
- Un tableau en bas du volet Visionneuse affiche les données dans un format tabulaire. Les données affichées dans le tableau dépendent de la sélection effectuée dans l'arborescence ou le volet Visionneuse.

Clamp des mesures de l'agent

Une icône d'agent affichant un ruban rouge indique un agent avec une limite de mesures. Un agent est limité lorsque le nombre de mesures qu'il génèrent est supérieur au nombre de mesures que le gestionnaire d'entreprise peut traiter. Une fois que les mesures de l'agent sont limitées, il est impossible de savoir quelles mesures sont signalées. Les mesures peuvent être limitées du côté de l'agent ou du côté du gestionnaire d'entreprise. Lorsqu'une mesure basée sur un agent est limitée, les messages figurant dans les journaux indiquent qu'une limite a été appliquée et qu'aucune nouvelle valeur de mesure n'est signalée. Lorsqu'une mesure basée sur le gestionnaire d'entreprise est limitée, toutes les mesures signalées avant l'application de la limite continuent d'envoyer des valeurs, mais aucun nouveau type de mesure n'est

traité. La mesure de capacité de prise en charge d'un agent limité renvoie une valeur de 1. Un agent limité indique qu'une instrumentation trop élevée est activée. Ajustez le niveau de l'instrumentation dans la configuration de l'agent.

Un agent limité peut également indiquer une explosion des mesures. Dans ce cas, les composants des agents signalent constamment des mesures qui varient. Pour plus d'informations sur les explosions de mesures, reportez-vous à la section [Explosion des mesures](#).

Noeud SuperDomain

Le noeud **SuperDomain** inclut les mesures de tous les agents qui renvoient des données au gestionnaire d'entreprise auquel la station de travail est connectée. Les mesures sont organisées selon une hiérarchie `Hôte | Processus | Agent`.

Les noeuds figurant sous le noeud **SuperDomain** sont des hôtes virtuels et physiques.

- **Hôte de mesure personnalisé (virtuel)** Ce noeud ne correspond pas à un ordinateur hôte physique. Il s'agit d'un hôte virtuel qui contient les mesures qui ne sont pas signalées par un agent spécifique. Par exemple, les mesures personnalisées s'affichent sous le noeud Custom Metric Host (Hôte de mesure personnalisée). Les mesures personnalisées peuvent provenir d'outils de calcul que vous avez configurés ou d'agents agrégés configurés.
- **Hôtes** Un noeud par ordinateur hébergeant un agent. Chaque noeud d'hôte contient un noeud de processus pour l'instance de l'application surveillée. Le noeud de processus contient un noeud d'agent. Le noeud d'agent contient les noeuds qui correspondent aux applications et aux ressources système contenant les mesures.

Remarque : Les ressources d'application qui s'affichent dans le noeud d'agent varient en fonction du type d'agent (Java ou .NET).

Le noeud SuperDomain inclut tous les domaines et les agents définis par l'utilisateur. L'administrateur du gestionnaire d'entreprise peut configurer le gestionnaire d'entreprise de sorte à afficher les domaines enfants avec des autorisations distinctes.

Les mesures affichées dans l'arborescence centrée sur l'agent dépendent des deux facteurs suivants :

- Directives ProbeBuilder utilisées pour instrumenter l'application
- Activité d'exécution de l'application

Une mesure apparaît uniquement dans l'arborescence lorsque l'agent commence à la signaler. La mesure reste visible dans l'arborescence, même si l'agent arrête de la signaler.

Lorsque les mesures sont de différents types, elles peuvent porter le même nom dans Investigator et donc apparaître deux fois. Dans cette situation, comme pour toutes les mesures, les mesures inactives sont grisées.

Outils de surveillance de l'intégrité du gestionnaire d'entreprise

Mesures de capacité de prise en charge

Les mesures de capacité de prise en charge offrent des informations sur l'état du gestionnaire d'entreprise et sur l'ordinateur sur lequel il s'exécute. Vous pouvez les afficher dans le chemin d'accès `SuperDomain | Custom Metric Host | Custom Metric Agent | Enterprise Manager`.

Noeud Domaines

L'administrateur DX APM peut organiser les agents qui fournissent des données au gestionnaire d'entreprise en domaines. Dans ce cas, le noeud de domaine de l'arborescence centrée sur l'agent contient les sous-noeuds de chaque domaine. Chaque noeud de domaine est structuré dans la même hiérarchie `Host | Process | Agent` que le noeud SuperDomain. Chaque noeud de domaine peut également contenir un noeud Custom Metric Agent (Agent de mesure personnalisée) pour les mesures personnalisées.

Portée des autorisations d'utilisateur sur les éléments affichables

L'administrateur DX APM affecte des autorisations pour les domaines et les composants que les utilisateurs de la station de travail peuvent afficher. Ces autorisations sont disponibles uniquement lorsqu'un administrateur les a configuré les à l'aide de Enterprise Enablement Manager.

Le contenu de l'onglet **Navigateur de mesures** est basé sur les autorisations d'utilisateur du domaine :

- Les utilisateurs disposant des autorisations `SuperDomain` (autorisation de lecture au minimum) affichent tous les domaines de l'arborescence centrée sur l'agent pour le gestionnaire d'entreprise.
- Les utilisateurs disposant des autorisations sur plusieurs domaines affichent les informations de domaine des domaines figurant dans l'arborescence centrée sur l'agent.
- Les utilisateurs disposant des autorisations sur un domaine unique ne peuvent pas consulter les informations de domaine dans l'arborescence centrée sur l'agent. Ils peuvent uniquement afficher les dossiers des modules de mesures et de gestion.

Onglet Navigateur de mesures

L'onglet Navigateur de mesures répertorie les mesures et les autres informations sous forme d'arborescence. Les noeuds de haut niveau apparaissant immédiatement sous les noeuds de domaine représentent les agents installés sur des hôtes de serveur d'applications individuels ou l'équivalent.

Les noeuds de haut niveau représentent différents composants, notamment :

- Composants de votre application J2EE, PHP ou .NET, tels que des servlets, des EJB ou des pages ASP
- Noeuds système, y compris l'hôte exécutant votre serveur d'applications et l'ordinateur hôte exécutant DX APM
- Événements, défauts et autres occurrences spécifiques

Vous pouvez afficher les données dynamiques dans Investigator ou sélectionner une période pour afficher les données historiques. Par défaut, la vue dynamique des données s'affiche.

Mesures dans l'onglet Navigateur de mesures

Les mesures par défaut que la station de travail affiche dans l'onglet Navigateur de mesures varient selon le noeud sélectionné dans l'arborescence hiérarchique.

Mesures standard

Pour les composants d'application frontaux et d'arrière-plan surveillés, ainsi que de nombreux autres composants d'application, Introscope affiche les cinq mesures standards, parfois appelées [mesures BlamePoint](#) :

- Temps de réponse moyen (ms) : mesure de la vitesse de réponse des applications.
- Appels simultanés : nombre de demandes traitées à un moment donné.
- Erreurs par intervalle : nombre d'erreurs qui se produisent au cours d'un créneau spécifique.
- Réponses par intervalle : nombre de demandes terminées au cours d'un créneau spécifique.
- Nombre de transactions bloquées : nombre de demandes bloquées ou non terminées, qui n'ont pas été terminées avant le seuil de temps spécifié.

Outre les cinq mesures standards, et parfois en lieu et place de celles-ci, Introscope collecte et affiche d'autres [mesures pertinentes](#) pour le noeud.

Composants frontaux et d'arrière-plan

Par défaut, Introscope définit un composant frontal en tant que fichier .war ou .jsp qui gère d'abord une transaction entrante vers une application. Dans une application .NET, l'équivalent serait une page ASP.

Un *composant d'arrière-plan* est un système externe sur lequel repose une application Web pour une partie de son traitement. Généralement, il s'agit d'une base de données, mais il peut s'agir d'un système externe tel qu'un serveur de messagerie, un système de traitement de transactions (par exemple, IBM CICS ou BEA Tuxedo) ou un système de messagerie (par exemple, MQSeries). Introscope identifie automatiquement les bases de données en tant que systèmes d'arrière-plan en fonction de leur nom. Pour les autres systèmes externes, Introscope analyse l'activité des sockets de l'application et nomme le composant d'arrière-plan en fonction de l'adresse IP et du port que l'application utilise pour ses communications.

Afficher les mesures pour les composants d'arrière-plan

Le noeud Serveurs d'arrière-plan de l'arborescence du Navigateur de mesures contient un noeud pour chaque serveur d'arrière-plan, y compris ceux automatiquement détectés par Introscope, ou marqués explicitement en tant que serveurs d'arrière-plan lors de la phase ProbeBuilding.

Généralement, ceux-ci sont une base de données, mais il peut s'agir d'un système externe tel qu'un serveur de messagerie, un système de traitement de transactions (par exemple, IBM CICS ou BEA Tuxedo) ou un système de messagerie (par exemple, MQSeries).

Mesures du serveur d'arrière-plan de base de données

Lorsque le système d'arrière-plan est une base de données, ces mesures reflètent l'activité et les performances du serveur d'arrière-plan sur toutes les applications qu'il traite :

- Temps de réponse moyen (ms)
- Concurrent Invocations
- Erreurs par intervalle
- Nombre de connexions : nombre de connexions à la base de données pendant un intervalle donné.
- Réponses par intervalle
- Nombre de blocages

Format de nom du serveur d'arrière-plan de base de données

Cette section explique la convention d'attribution de noms d'Introscope pour les serveurs d'arrière-plan de base de données.

Oracle

Le nom du serveur d'arrière-plan est une concaténation de la chaîne de SID Oracle, de l'hôte et du port de la base de données délimités par un trait d'union et la chaîne (*Oracle DB*).

Exemple :

```
PRODORCL3 sfoprod6.globex.com-1521 (Oracle DB)
```

DB/2

Le nom du serveur d'arrière-plan est une concaténation de la chaîne DBName et de la chaîne (*DB/2 DB*).

Exemple :

```
Inventory4 (DB/2 DB)
```

Microsoft SQL Server

Le nom du serveur d'arrière-plan peut être une concaténation du nom de base de données, du nom d'instance, de l'hôte et du port de la base de données délimités par un trait d'union et de la chaîne (*MS SQL Server DB*), selon la configuration du pilote de base de données.

Si le pilote a un nom de base de données et un nom d'instance, le nom du serveur d'arrière-plan dans Investigator ressemble à cela :

PRODORCL3 (instance Mx22) on prod6.globex.com-1521 (MS SQL Server DB)

Si le pilote n'a aucun nom de base de données, le nom du serveur d'arrière-plan dans Investigator ressemble à cela :

SQLServer on prod6.globex.com-1521 (MS SQL Server DB)

Si le pilote a un nom de base de données, mais aucun nom d'instance, le nom du serveur d'arrière-plan dans Investigator ressemble à cela :

PRODORCL3 on prod6.globex.com-1521 (MS SQL Server DB)

Si le pilote a un nom d'instance, mais aucun nom de base de données, le nom du serveur d'arrière-plan dans Investigator ressemble à cela :

(instance Mx22) on prod6.globex.com-1521 (MS SQL Server DB)

Valeurs par défaut et de secours

Dans les cas où le pilote de base de données ne prend pas en charge l'interrogation du nom de base de données, le nom de la base de données est défini par défaut sur l'URL JDBC, et les deux-points (:) sont remplacés par le caractère de pourcentage (%). Dans certains cas, même cette valeur de secours n'est pas disponible, et le nom de base de données est défini par défaut sur le nom de classe du pilote de base de données. Le comportement exact dépend du fournisseur et de la version du pilote de base de données.

Autres mesures de serveurs d'arrière-plan

Chaque système d'arrière-plan peut également être configuré pour générer des rapports sur les mesures suivantes :

- Validations
- Restaurations
- SQL

Mesures d'alerte dans l'arborescence centrée sur l'agent

Chaque couleur d'alerte a une valeur de mesure :

- Gris : 0, aucune donnée n'est disponible
- Vert : 1, OK
- Jaune : 2, avertissement
- Rouge : 3, danger

Le tableau suivant présente la manière dont les mesures gèrent les valeurs d'alerte dans l'onglet Présentation.

Type de mesure	Signification d'un indicateur jaune	Signification d'un indicateur rouge
Utilisateur	Les erreurs de serveur frontal sont anormales. Le temps de réponse du serveur frontal est anormal. Le nombre de transactions bloquées du serveur frontal est anormal.	Les erreurs du serveur frontal sont <i>très</i> anormales. Le nombre de transactions bloquées du serveur frontal est <i>très</i> anormal.
Machine virtuelle	L'utilisation d'UC agrégée est anormale et supérieure à 30 pour cent. L'utilisation du pool de connexions JDBC est anormale.	L'utilisation d'UC agrégée est <i>très</i> anormale et supérieure à 50 pour cent. L'utilisation du pool de connexions JDBC est <i>très</i> anormale.

Récapitulatif des serveurs d'arrière-plan	Le temps de réponse du serveur d'arrière-plan est anormal. Le nombre d'erreurs du serveur d'arrière-plan est anormal. Le nombre de transactions bloquées du serveur d'arrière-plan est anormal.	Le nombre d'erreurs du serveur d'arrière-plan est <i>très</i> anormal. Le nombre de transactions bloquées du serveur d'arrière-plan est <i>très</i> anormal.
---	---	---

Vous pouvez afficher les mesures d'alerte en sélectionnant les mesures Utilisateur, Machine virtuelle, Serveurs d'arrière-plan|*Nom_serveur_arrière-plan*, sous le noeud d'analyse heuristique d'Investigator.

Les mesures sous-jacentes dont dépendent les mesures d'alerte s'affichent dans les dossiers Utilisateur, Machine virtuelle, Serveurs d'arrière-plan|*Nom_serveur_arrière-plan* dans l'arborescence.

Administration des connexions de l'agent à partir de la station de travail

Vous pouvez émettre des commandes directement à partir de la station de travail afin de démonter ou d'arrêter des agents ou des mesures.

Lorsqu'un agent est déployé sur un serveur d'applications, il démarre automatiquement au démarrage du serveur d'applications et s'affiche dans l'arborescence Navigateur de mesures sous le gestionnaire d'entreprise vers lequel il renvoie les données de mesure. Lorsque l'agent s'affiche dans l'arborescence, il est considéré comme *monté*.

Lorsqu'un serveur d'applications tombe en panne, l'agent arrête automatiquement d'envoyer des données au gestionnaire d'entreprise. Cet agent est considéré comme *déconnecté* et apparaîtra dans le Navigateur de mesures en gris au lieu d'une autre couleur.

Un agent déconnecté apparaîtra toujours monté dans l'arborescence Navigateur de mesures, et vous pouvez parcourir les mesures signalées avant sa déconnexion. Si vous souhaitez le supprimer de l'arborescence Navigateur de mesures, vous devez *démonter* l'agent.

Pour démonter un agent :

1. Cliquez avec le bouton droit de la souris sur un agent déconnecté.
2. Sélectionnez Démonter <nom_agent>.
L'agent disparaît de l'arborescence de navigation.

Si vous souhaitez afficher les données historiques stockées dans la base de données SmartStor pour un agent qui a été démonté, vous pouvez remonter l'agent afin qu'il s'affiche à nouveau dans l'arborescence Navigateur de mesures.

Pour remonter un agent déconnecté :

1. Sélectionnez Gestionnaire > Monter un agent.
La boîte de dialogue Sélecteur d'agent s'affiche.
2. Dans la liste, sélectionnez l'agent à remonter.
3. Cliquez sur OK.

L'arborescence Navigateur de mesures affiche les agents déconnectés et vous pouvez parcourir les données stockées dans la base de données SmartStor.

Si vous souhaitez que le gestionnaire d'entreprise arrête le stockage des données d'un agent en cours d'exécution, vous pouvez arrêter la collecte de données sans arrêter le serveur d'applications en sélectionnant la commande Arrêter.

Remarque : La commande Arrêter n'arrête pas réellement l'agent, mais la connexion entre un agent en cours d'exécution et le gestionnaire d'entreprise.

Pour arrêter la connexion à un agent en cours d'exécution :

1. Cliquez avec le bouton droit de la souris sur un agent connecté.
2. Choisissez Arrêter <nom_agent>.

L'agent continue de s'exécuter sur le serveur d'applications à condition que ce dernier soit en cours d'exécution, mais le gestionnaire d'entreprise n'y est plus connecté et ne stocke plus les données de mesures correspondantes.

Une fois que vous arrêtez la connexion à un agent, vous pouvez réactiver la connexion.

Pour activer la connexion à un agent arrêté :

1. Cliquez avec le bouton droit de la souris sur un agent arrêté.
2. Sélectionnez Activer tous les composants d'agent.

La connexion entre l'agent et le gestionnaire d'entreprise est rouverte et l'agent commence à envoyer des données au gestionnaire d'entreprise. Notez que vous devrez patienter entre 30 et 45 secondes pour que les données s'affichent dans la station de travail.

Remarque : La commande Activer tous les composants d'agent fonctionne uniquement si vous avez préalablement arrêté la connexion d'agent via la station de travail en utilisant la commande Arrêter *<nom_agent>*.

Vues dans l'onglet Navigateur de mesures

Lorsque l'onglet Navigateur de mesures est sélectionné dans le volet gauche d'Investigator, les vues qui apparaissent dans le volet droit varient en fonction de la ressource ou de la mesure sélectionnée dans l'arborescence de l'onglet Navigateur de mesures. Selon le type de noeud sélectionné, les onglets affichés sont associés à une ou plusieurs des vues suivantes :

- Onglet Général
- Onglets Présentation
- Onglet Rechercher
- Onglet Traces
- Onglet Erreurs
- Onglet Nombre de mesures
- Onglet Vidages de threads

Onglet Général

Lorsque vous sélectionnez une mesure, l'onglet Général affiche une vue graphique de la mesure : pour les données dynamiques ou pour une période historique sélectionnée. Reportez-vous à la section [Affichage des données historiques dans l'onglet Navigateur de mesures](#) pour obtenir une explication sur la manière de sélectionner des plages de données historiques et les afficher.

Pour certains noeuds dans l'arborescence, l'onglet Général affiche le chemin d'accès à cet objet de noeud dans la hiérarchie d'Investigator. Par exemple, lorsque le noeud Composants frontaux est sélectionné, l'onglet Général indique le chemin d'accès suivant :

```
*SuperDomain* | HostName | ProcessName | AgentName | Frontends
```

Pour certains autres noeuds dans l'arborescence, l'onglet Général affiche la vue des 10 éléments les plus lents du noeud sélectionné. Par exemple, lorsque le noeud EJB est sélectionné, l'onglet Général indique les temps de réponse des dix principaux composants appelés du noeud EJB sélectionné.

Dix mesures les plus lentes ou les moins performantes

Lorsque vous sélectionnez certaines ressources dans Investigator, l'onglet Général du volet Visionneuse affiche les dix mesures les plus lentes/moins performantes de la ressource sélectionnée. Les ressources Java incluent les servlets, JSP, EJB et JDBC. Pour .NET, les ressources incluent ASP.NET, ADO.NET et les composants de service.

Ces mesures apparaissent dans un graphique à barres dans le volet de la visionneuse Investigator.

Vous pouvez également afficher les temps de réponse des dix premiers composants appelés d'un servlet, EJB ou JSP sélectionné pour Java, ou d'ASP.NET, ADO.NET et des composants de service pour .NET.

Si vous voyez moins de dix barres dans le graphique à barres, il y a moins de dix composants surveillés sous cette ressource. Si les mesures ne contiennent aucun donnée, les noms des mesures s'affichent dans le volet de la visionneuse, mais il n'y a aucune barre de données.

Onglets Présentation

Investigator récapitule les informations dans un onglet Présentation pour :

- L'application globale : reportez-vous à la section Présentation de l'application.
- L'intégrité du gestionnaire d'entreprise : reportez-vous à la section Présentation du gestionnaire d'entreprise.
- Les données des pages ASP.NET : reportez-vous la section Présentation d'ASP. NET.
- Les données EJB : reportez-vous à la section Présentation de l'EJB.
- Les données des composants frontaux d'application : reportez-vous à la section Présentation des composants frontaux.
- Les données des systèmes d'arrière-plan d'application : reportez-vous à la section Présentation des composants d'arrière-plan.
- Le segment mémoire GC (Garbage Collection, nettoyage de la mémoire) : reportez-vous à la section Présentation du segment de mémoire GC.
- Le nombre d'instances de classes Java instanciées sur la machine virtuelle Java : reportez-vous à la section Nombre d'instances.
- Les données de JavaNIO : reportez-vous à la section Présentation de JavaNIO.
- Les données des composants JTA : reportez-vous à la section Présentation de JTA.
- Les données de servlets : reportez-vous à la section Présentation du servlet.
- Les connexions de socket : reportez-vous à la section Présentation du socket.
- Les données Struts : reportez-vous à la section Présentation des données Struts.
- Les données des threads en cours d'exécution : reportez-vous à la section Présentation des threads.
- Les données des composants XML : reportez-vous à la section Présentation du contenu XML.

NOTE

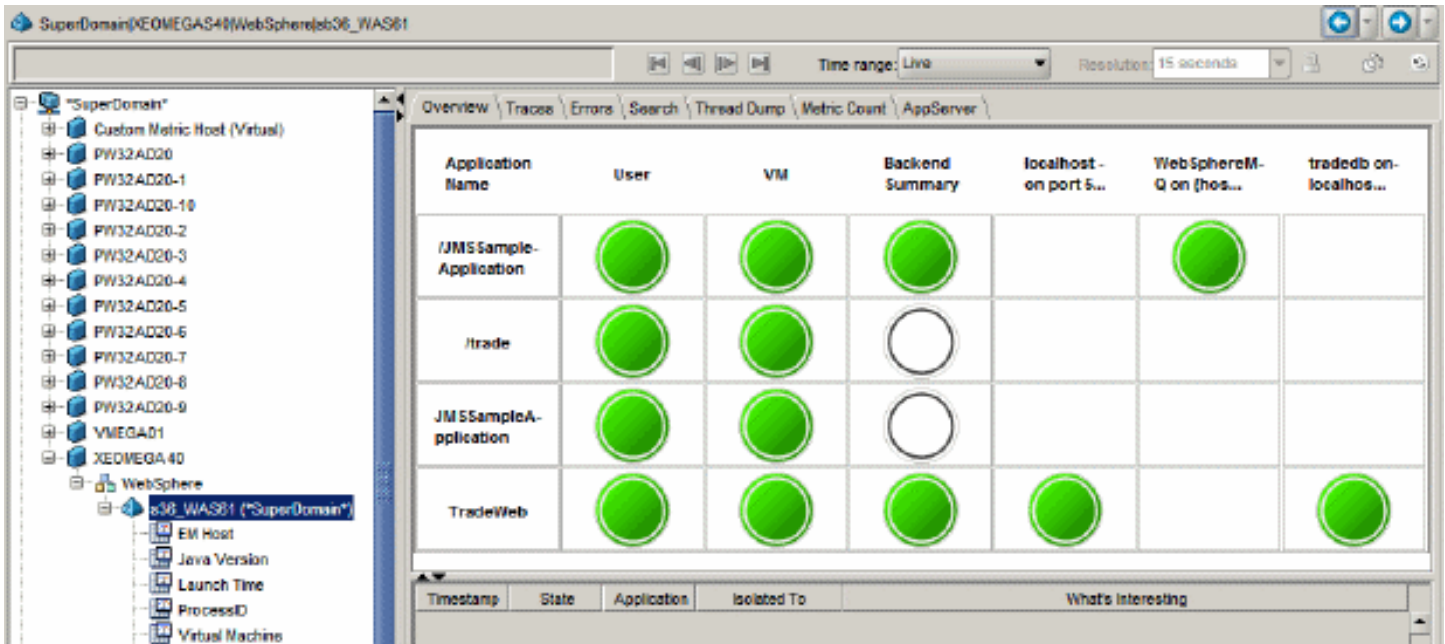
Les onglets Présentation affichent la valeur de mesure actuelle lorsqu'ils sont affichés en **mode dynamique**. Lorsqu'ils sont affichés en **Mode historique**, ils affichent les valeurs de mesures agrégées (valeurs moyennes ou cumulées, selon le type de mesure) pour la période sélectionnée.

Présentation de l'application

La présentation de l'application est disponible lorsque vous sélectionnez un agent dans l'arborescence centrée sur l'agent et activez la surveillance et le tri des applications. Elle affiche des indicateurs d'intégrité de haut niveau et un journal des événements liés et des informations historiques sur la mesure.

L'onglet Présentation affiche une ligne d'indicateurs pour chaque application gérée par l'agent sélectionné. Introscope présente les données de chaque application détectée : lorsqu'un servlet s'exécute, Introscope effectue un appel vers *getServletContextName()* de l'interface *ServletContext* pour déterminer le nom de l'application. Après le démarrage de l'application, l'onglet Présentation se met automatiquement à jour pour afficher une ligne d'indicateurs correspondants.

La figure ci-dessous présente l'onglet Présentation pour un agent sur un serveur d'applications WebSphere nommé `s36_WAS61` :



La figure comprend quatre applications gérées par l'agent, une par ligne du tableau. Pour cette application, vous pouvez afficher des alertes indiquant l'état des éléments :

Utilisateur : indique le degré potentiel de satisfaction des interactions entre les utilisateurs finals et l'application. Le niveau de satisfaction dépend des erreurs, des blocages, des temps de réponse et des attentes.

- Vert : interactions normales et satisfaisantes des utilisateurs avec l'application.
- Jaune : une tentative d'utilisation de l'application n'offre probablement pas de résultats satisfaisants (par exemple, en raison de temps de réponse médiocres ou d'erreurs).
- Rouge : indique un problème de disponibilité grave et qu'une tentative d'utilisation de l'application va probablement échouer.

Machine virtuelle : indique l'intégrité et la disponibilité des ressources de serveur, telles que les pools de ressources et l'UC.

- Vert : intégrité normale des ressources de serveur.
- Jaune : limitations ou interruptions des ressources.
- Rouge : limitations ou interruptions graves des ressources.

Récapitulatif des serveurs d'arrière-plan : indique l'intégrité et la disponibilité la moins performante de tous les serveurs d'arrière-plan auxquels l'application accède. Par exemple, si un des trois serveurs d'arrière-plan a une limitation ou une interruption importante des ressources, l'indicateur All Backends (Tous les serveurs d'arrière-plan) est rouge. L'objectif de l'indicateur All Backends est de permettre à l'utilisateur d'évaluer rapidement avec un minimum de défilement de page, si des serveurs d'arrière-plan ont des problèmes qui requièrent un examen.

- Vert : intégrité et disponibilité normales des serveurs d'arrière-plan de tous les serveurs d'arrière-plan auxquels l'application accède.
- Jaune : au moins un serveur d'arrière-plan auquel accède l'application rencontre une erreur ou un blocage, ou présente des temps de réponse plus médiocres que ceux attendus.
- Rouge : au moins un serveur d'arrière-plan auquel accède l'application rencontre des limitations ou des interruptions de ressources graves.

Serveurs d'arrière-plan : aucun indicateur à droite de l'indicateur Récapitulatif des serveurs d'arrière-plan ne correspond aux serveurs d'arrière-plan.

- Vert : intégrité et disponibilité normales du serveur d'arrière-plan.
- Jaune : erreurs ou blocages du serveur d'arrière-plan, ou celui-ci présente des temps de réponse plus médiocres que ceux attendus.
- Rouge : limitations ou interruptions graves des ressources du serveur d'arrière-plan.

Les indicateurs sont actualisés toutes les 15 secondes. Les lignes sont triées par couleur : celles avec des indicateurs rouges précèdent celles avec des indicateurs jaunes, qui précèdent celles avec des indicateurs verts, afin de réduire le défilement nécessaire pour identifier les problèmes potentiels. Dans une catégorie de couleur, les lignes sont classées par ordre alphabétique selon le nom de l'application.

Utilisation des alertes pour afficher davantage de données

Vous pouvez double-cliquer sur une alerte dans l'onglet Présentation pour afficher les données sous-jacentes pour ce niveau d'application. Par exemple, si vous double-cliquez sur l'alerte Utilisateur, la station de travail affiche le noeud URL pour cet agent.

Mesures de présentation de l'application en mode historique

Dans une plage historique, une couleur d'alerte reflète la pire valeur de l'analyse heuristique à un moment de cette plage. Par exemple, si à un moment de la plage historique, l'analyse heuristique de l'utilisateur pour un agent est jaune, mais jamais rouge, l'onglet Présentation de cette plage historique est jaune.

Mesures de présentation de l'application pour un agent virtuel

Pour les agents virtuels, l'analyse heuristique est évaluée en fonction des mesures de l'agent virtuel. Pour cette raison, l'onglet Présentation d'un agent virtuel peut indiquer une valeur différente que celle des agents physiques de l'agent virtuel.

Par exemple, l'onglet Présentation d'un agent virtuel peut afficher une alerte Utilisateur verte, même si l'onglet Présentation de l'un des agents dans cet agent virtuel affiche une alerte Utilisateur jaune.

Les mesures heuristiques sont générées uniquement si les mesures analysées existent. Par exemple, si l'agent virtuel est configuré pour ne pas inclure les mesures d'UC, JMX ou WebSphere PMI, il n'y a aucun dossier Machine virtuelle et l'alerte Machine virtuelle reste grise.

Présentation du gestionnaire d'entreprise

Vous pouvez afficher un ensemble de mesures sur le gestionnaire d'entreprise en sélectionnant le noeud Gestionnaire d'entreprise sous Custom Metric Agent (Agent de mesure personnalisée).

Présentation d'ASP.NET

Dans les environnements où Introscope surveille une application .NET, un noeud ASP.NET dans l'arborescence centrée sur l'agent vous permet de surveiller les mesures des composants d'application.

Présentation de l'EJB

La présentation de l'EJB (Enterprise Java Beans) répertorie les statistiques des beans d'entité, des beans de session et des beans générés par message.

Présentation des composants frontaux

Les présentations pour les noeuds de composants frontaux affichent les mesures des applications sous la forme de graphiques et les statistiques relatives aux transactions de l'application :

Les programmes affichés par Investigator sous le noeud Frontends (Composants frontaux) représentent les composants d'une application qui gèrent une transaction entrante en premier.

Présentation des composants d'arrière-plan

Les présentations pour les noeuds de composants d'arrière-plan affichent les vues graphiques des mesures de base de données et une vue de tableau du contenu SQL sous le noeud.

Présentation du segment de mémoire GC

La présentation du segment de mémoire GC (Garbage Collection, nettoyage de la mémoire) indique l'utilisation du segment de mémoire.

Onglet Présentation du moniteur GC

Cliquer sur le noeud GC Monitor (Moniteur GC) dans l'arborescence Navigateur de mesures affiche l'onglet Présentation du moniteur GC dans le volet de la visionneuse. L'onglet Présentation affiche trois volets :

- Haut : un indicateur d'alerte pour la mesure Pourcentage du segment de mémoire Java utilisé pour la machine virtuelle Java.
- Milieu : une vue tabulaire des utilitaires de nettoyage de mémoire de la machine virtuelle Java.
- Bas : vue tabulaire des pools de mémoire de la machine virtuelle Java.

Remarque : L'indicateur d'alerte dans le volet supérieur de l'onglet Présentation et la couleur qui apparaît en fond dans les cellules du tableau des volets au milieu et en bas dépendent des seuils d'avertissement et de risque prédéfinis. Les utilisateurs ne peuvent pas réinitialiser ces seuils.

Lorsque vous sélectionnez un des noeuds Garbage Collector (Utilitaire de nettoyage de mémoire) ou Memory Pool (Pool de mémoire), les graphiques affichent les mêmes mesures affichées dans l'onglet Présentation.

Pour plus d'informations :

- consultez la section sur [l'utilisation des mesures de moniteur GC](#) pour ajuster l'allocation de mémoire de la machine virtuelle Java.

Activation/désactivation du moniteur GC

Les mesures du moniteur GC sont activées par défaut.

Pour les désactiver :

1. Ouvrez le fichier *IntroscopeAgent.profile*.
2. Définissez la valeur de la propriété `introscope.agent.gcmonitor.enable` sur `false`.
3. Enregistrez et fermez le fichier.

Remarque : Il s'agit d'une propriété configurable à chaud. Les modifications apportées ne nécessitent aucun redémarrage du gestionnaire d'entreprise.

Pour plus d'informations sur la modification du fichier `IntroscopeAgent.profile`, reportez-vous à la section [Agent Java](#).

Nombre d'instances

L'onglet de présentation Nombre d'instances affiche les classes instanciées sur la machine virtuelle Java.

Présentation JavaNIO

La présentation de la fonctionnalité NIO répertorie les tableaux pour les datagrammes et les canaux, notamment les mesures de client et de serveur. Lorsque le noeud JavaNIO est sélectionné, l'onglet Présentation affiche des informations générales sur le noeud sélectionné, y compris tous les ports comportant une activité NIO.

Présentation des canaux NIO

L'onglet Présentation du noeud Channels (Canaux) affiche les informations sur le client et le serveur pour les datagrammes et les sockets.

Présentation des sockets NIO

L'onglet Présentation du noeud Sockets affiche des graphiques pour les données de bande passante en entrée et en sortie, les lecteurs simultanés, les données d'enregistreurs ainsi que les informations sur le client et le serveur pour les sockets.

Présentation des datagrammes NIO

L'onglet Présentation du noeud Datagrams (Datagrammes) affiche des graphiques pour les données de bande passante en entrée et en sortie, les lecteurs simultanés, les données d'enregistreurs ainsi que les informations sur le client et le serveur pour les datagrammes.

Présentation de JTA

L'onglet Présentation de JTA affiche les données relatives aux composants JTA.

Présentation du servlet

La Présentation du servlet affiche un tableau des servlets dans le noeud. Lorsque vous sélectionnez un servlet, Investigator affiche les statistiques dans un graphique.

Sélectionnez un servlet pour afficher l'onglet récapitulatif Présentation.

Présentation du socket

La présentation des sockets (à ne pas confondre avec la présentation des sockets NIO) répertorie les tableaux pour les sockets de client et de serveur, ainsi que les informations de socket pour chaque port. Lorsque le noeud Socket est sélectionné dans l'arborescence centrée sur l'agent, le volet de visionneuse à droite affiche tous les ports avec des sockets actifs. Sélectionner un port dans le tableau de serveur en haut du volet de visionneuse affiche les ports de client du serveur dans le tableau Client de la partie inférieure. Sélectionner un port dans l'arborescence centrée sur l'agent affiche les graphiques de mesures relatifs aux événements et à la charge.

Présentation des données Struts

L'onglet Présentation des données Struts affiche une vue d'ensemble des composants Struts, y compris le temps de réponse moyen pour tous les composants.

Sélectionner un des noeuds de composant affiche un aperçu des mesures pour ce noeud.

Présentation des threads

La page Présentation des threads affiche tous les threads actifs en cours de traitement par un agent.

Présentation du contenu XML

L'onglet Présentation pour le noeud XML présente les mesures des composants XML.

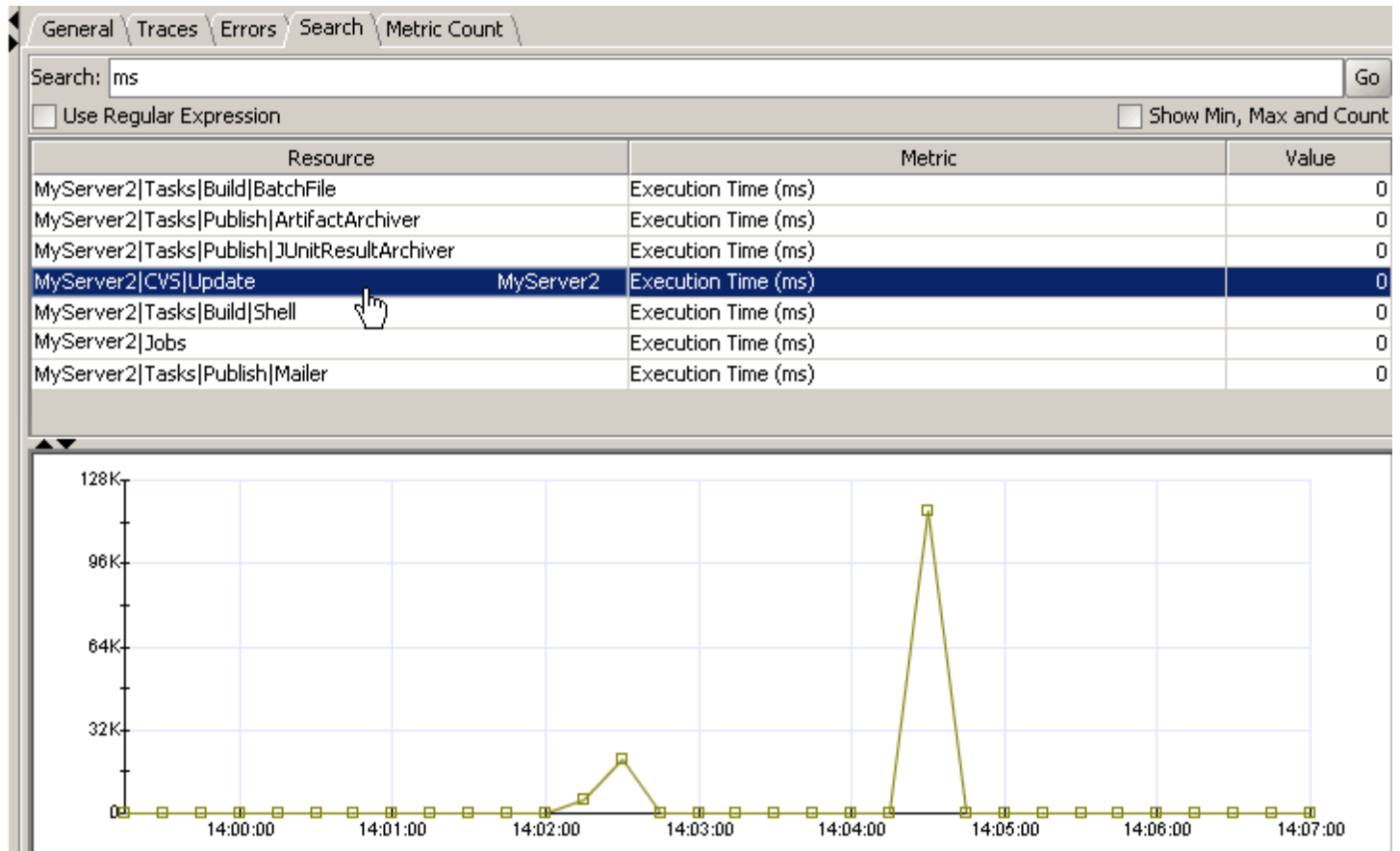
Autres onglets

Outre les onglets Présentation, d'autres onglets incluent les onglets Rechercher, Traces, Erreurs et Nombre de mesures.

Onglet Rechercher

L'onglet Rechercher est disponible lorsque vous sélectionnez un noeud dans l'arborescence centrée sur l'agent qui contient des mesures. Il vous permet de rechercher rapidement des mesures.

La figure ci-dessous présente l'onglet Rechercher dans le volet de visionneuse.



Points à noter :

- Le noeud sélectionné dans l'arborescence centrée sur l'agent permet de définir la portée d'une recherche. Par exemple, si vous sélectionnez Frontends (Composants frontaux) dans l'arborescence, la recherche sera effectuée uniquement sur les ressources sous ce noeud.
- Vous pouvez entrer une chaîne ou une expression régulière dans le champ Rechercher.
- Si vous entrez une expression régulière, cochez la case Utiliser une expression régulière.

Remarque : Les expressions régulières ne peuvent pas filtrer les données par agent. Il est donc impossible de rechercher un nom d'agent, un nom d'hôte ou un nom de processus.

Le volet droit répertorie les ressources avec les mesures correspondant à l'argument de recherche et la valeur pour chacun. Pour afficher les colonnes Min, Max. et Nombre, cliquez sur Afficher min., max. et nombre.

Si vous cliquez sur une mesure dans la liste, une vue apparaît dans la partie inférieure du volet droit.

Si vous cliquez sur un autre noeud qui contient des mesures, l'argument de recherche utilisé dans la recherche précédente reste actif et est appliqué au noeud nouvellement sélectionné.

Pour plus d'informations sur l'utilisation de la recherche, reportez-vous à la section [Utilisation de la recherche](#).

Onglet Traces

L'onglet Traces, disponible lorsqu'une ressource ou un composant est sélectionné dans l'arborescence centrée sur l'agent, est similaire à l'outil de suivi de transaction (reportez-vous à la section [Utilisation de l'outil de suivi de transaction](#)). L'onglet Traces répertorie les événements de trace de transaction enregistrés pour la ressource ou le composant sélectionné.

Remarque : La période par défaut pour les traces en mode dynamique est de 20 minutes. Les traces âgées de plus de 20 minutes ne sont pas affichées en mode dynamique, car elles sont obsolètes après plus de 20 minutes.

Définition de l'unité de durée

Par défaut, l'onglet Traces affiche la durée des transactions et des composants de transaction en millisecondes (ms).

Vous pouvez modifier cette unité comme suit :

- secondes
- microsecondes (µs)

Pour modifier l'unité de la colonne Durée sous l'onglet Traces :

1. Cliquez sur l'en-tête de colonne Durée (ms).
2. Dans le menu déroulant, sélectionnez l'une des options suivantes :
 - secondes
 - millisecondes (par défaut)
 - microsecondes

L'onglet Traces affiche la nouvelle unité dans l'en-tête de colonne, puis affiche la durée à l'aide de la nouvelle unité dans toutes les vues de transaction (y compris dans la visionneuse des traces de transaction, reportez-vous à la section [Utilisation de la visionneuse des traces de transaction](#)).

Onglet Erreurs

L'onglet Erreurs disponible lorsqu'une ressource ou un composant est sélectionné dans l'arborescence centrée sur l'agent, répertorie les erreurs et leurs détails pour l'élément sélectionné. L'onglet Erreurs permet au personnel de support de détecter et de diagnostiquer la cause des erreurs lorsqu'elles se produisent, de déterminer la fréquence et la nature des erreurs qui peuvent empêcher les utilisateurs finals de mener à bien des transactions Web, et de fournir des informations spécifiques sur la cause première aux développeurs.

Remarque : Pour afficher l'onglet Erreurs, ErrorDetector doit être activé. Pour plus d'informations sur l'activation d'ErrorDetector, reportez-vous à la section [Configuration d'ErrorDetector](#).

La moitié supérieure de l'onglet Erreurs affiche l'heure, la description et le type de chaque erreur. La moitié inférieure de l'onglet affiche des informations détaillées sur chaque composant impliqué dans l'erreur sélectionnée dans la liste ci-dessus.

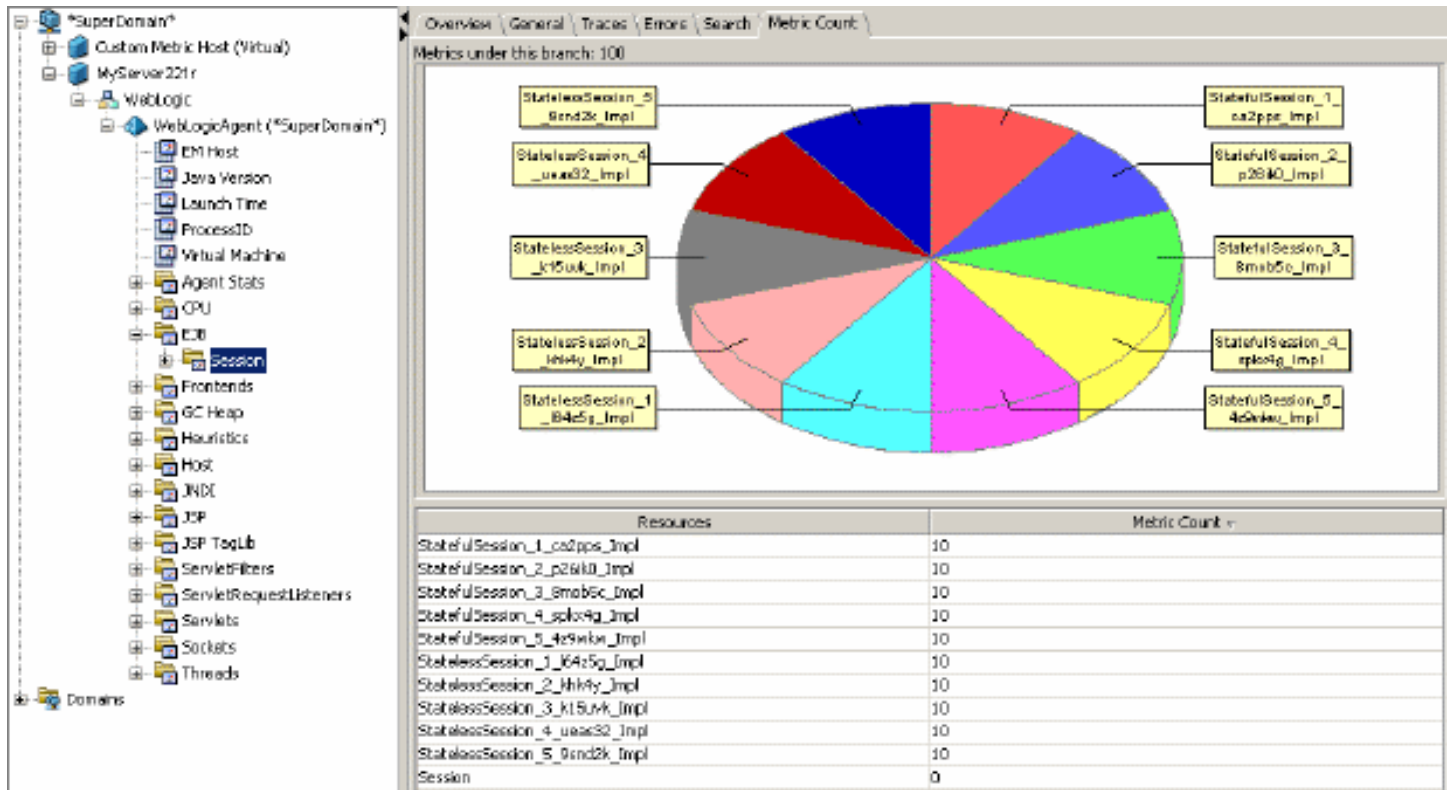
Onglet Nombre de mesures

Plusieurs noeuds de l'arborescence centrée sur l'agent comportent un onglet Nombre de mesures, qui affiche un graphique à secteurs de la distribution des mesures pour le noeud.

La figure ci-dessous présente le graphique à secteurs, avec un tableau des mêmes données au-dessous.

Le graphique à secteurs affiche un maximum de 50 tranches. Lorsqu'il y a plus de 50 ressources dans le noeud sélectionné :

- Le graphique affiche les ressources avec les 50 valeurs les plus élevées.
- Outre les tranches qui représentent les 50 valeurs les plus élevées, une tranche supplémentaire est définie comme Toutes les autres mesures pour afficher la proportion des mesures avec des données en dehors des 50 principales valeurs signalées.
- La barre de statut affiche le message Affichage des 50 premières ressources. Les ressources restantes sont groupées dans Toutes les autres mesures.



Lorsque vous passez la souris sur une zone du graphique à secteurs, une infobulle affiche le nombre et le pourcentage.

Les étiquettes longues seront tronquées, mais lorsque vous sélectionnez une tranche du graphique, le nom complet de la ressource apparaît dans le tableau sous le graphique.

L'onglet Nombre de mesures affiche tous les nombres de mesures pour la période sélectionnée, y compris les mesures des agents déconnectés au cours de la même période.

Les mesures des agents déconnectés s'affichent dans le nombre de mesures pendant 30 minutes. Si la période sélectionnée est inférieure à 30 minutes, les mesures des agents déconnectés disparaissent après 30 minutes. Si la période sélectionnée est plus élevée, les mesures des agents déconnectés restent affichées pendant la période complète.

Vue de l'onglet Ressources

L'onglet Ressources contient des graphiques des mesures de ressources. L'onglet Ressources apparaît dans l'arborescence Navigateur de mesures, lorsque l'agent est sélectionné.

Remarque :

- Bien que les graphiques pour toutes les mesures de ressource s'affichent dans la vue de l'onglet Ressources, ils n'affichent aucune donnée lorsque les classes des mesures ne sont pas disponibles pour l'agent.
- La source d'origine de la mesure qui s'affiche dans les graphiques Threads utilisés et Connexions JDBC en cours d'utilisation peut varier d'un agent à un autre, selon le type de l'agent (WebLogic, Tomcat, .NET, etc) et le mappage spécifié dans le fichier ResourceMetricMap.properties.

Dans l'arborescence Navigateur de mesures, ils s'affichent sous le noeud de l'agent comme suit :

Figure 14: nom de l'agent



Onglet Vidages de threads

Chaque nœud de l'agent sur l'arborescence Navigateur de mesures comporte un onglet Vidages de threads. Cet onglet vous permet de collecter des vidages de threads Java et d'afficher les données de vidage de threads actuelles et historiques. Un vidage de threads fournit des informations sur tous les threads qui s'exécutent dans une machine virtuelle Java à un moment donné. Pour chaque thread, un vidage de threads fournit le nom et l'ID du thread, son état et une trace de pile, qui répertorie toutes les méthodes appelées.

L'onglet Vidages de threads inclut les éléments suivants :

- L'en-tête affiche l'heure du vidage de threads.
- La barre de récapitulatif du vidage de threads affiche le nombre total de threads ainsi que le nombre de threads en attente, bloqués et en cours d'exécution.
- Le volet de recherche vous permet de rechercher une chaîne spécifique dans toutes les informations de vidage de threads. Les résultats s'affichent dans le tableau d'informations de thread.
- La liste déroulante des états de threads filtre le tableau d'informations de thread par état de thread. Lorsque vous sélectionnez un état, le tableau des informations de threads est mis à jour.
- Le tableau des informations de threads affiche une liste de tous les threads. Pour chaque thread, il fournit l'ID, le nom, l'état du thread ainsi que la dernière méthode appelée par le thread juste avant le vidage.
- Le tableau de trace de pile de thread affiche toutes les méthodes dans l'ordre d'appel.
- Le graphique à secteurs % de threads par état affiche les threads dans les états suivants : Interbloqués, Bloqués, En cours d'exécution ou En attente.
 - Lorsque vous passez la souris sur une zone, une infobulle affiche le nombre et le pourcentage de threads dans chaque état.

L'onglet Vidages de threads est visible dans l'arborescence Navigateur de mesures lorsque vous avez sélectionné un nœud d'agent.

Remarque : Si vous souhaitez trier des problèmes d'agent, affichez la mesure <nom_agent>|Threads|Deadlock Count dans l'arborescence Navigateur de mesures. Cette mesure indique s'il existe des threads interbloqués affectant l'agent.

La configuration d'Introscope est requise pour activer la mesure Deadlock Count (Nombre d'interblocages). Pour plus d'informations, reportez-vous à la section [Agent Java](#).

Vous pouvez cliquer sur :

- Collecter nouveau pour collecter un vidage de threads.
- Enregistrer en tant que texte pour enregistrer le vidage de threads actuel dans un fichier texte.
- Charger précédent pour charger un vidage de threads unique précédemment collecté et pour afficher l'horodatage et les données associées.

Aucune donnée de vidage de threads n'est affichée tant qu'un vidage de threads n'est pas collecté ou après le redémarrage d'un gestionnaire d'entreprise.

L'onglet Vidages de threads est disponible en mode dynamique. Aucune données historiques de vidage de threads n'est affichée en mode historique.

Utilisation des infobulles pour afficher des noms et des valeurs de mesures dans une visionneuse de données

Dans une visionneuse de données, vous pouvez passer la souris sur un point d'un diagramme pour ouvrir une infobulle.

Pour ouvrir une infobulle :

- Passez la souris sur un élément dans l'arborescence de mesures du poste de travail ou dans une visionneuse de données, tel qu'un point dans un graphique.

Un point de données particulier dans le graphique affiche :

- Nom de la mesure
- Valeur exacte de la mesure
- Valeurs minimum/maximum pour la mesure sur la période représentée par le point de données. Au lieu d'arrondir sur une valeur à l'aide d'un K pour les milliers ou d'un M pour les millions, les infobulles affichent les valeurs exactes. Cette procédure est expliquée dans la section Conséquence d'une période sur les points de données ci-dessous.
- Nombre d'intervalles de 15 secondes représentés par le point de données.
- Date et heure du point de données dans le graphique.

Appuyer sur F2 lorsqu'une infobulle est active vous permet de cliquer sur le texte du lien hypertexte. Ce faisant, une fenêtre Investigator s'ouvre avec l'arborescence développée sur la mesure indiquée dans l'infobulle.

Conséquence d'une période sur les points de données

Chaque point de données sur un graphique représente une répartition égale de la durée couverte par le graphique. Si la période est définie sur Dynamique (comme dans l'illustration ci-dessus), chaque point de données représente un intervalle de 15 secondes.

Si la période est définie sur une autre valeur, l'intervalle représenté par chaque point de données sera différent. Si la période est définie sur deux heures, par exemple :

- Chaque point de données représente un intervalle de deux minutes ou huit intervalles de 15 secondes.
- Comme il y a huit intervalles de 15 secondes dans deux minutes, le nombre de chaque point de données est 8.

L'onglet Navigateur de mesures répertorie les mesures et les autres informations sous forme d'arborescence. Les noeuds de haut niveau apparaissant immédiatement sous les noeuds de domaine représentent les agents installés sur des hôtes de serveur d'applications individuels ou l'équivalent.

Pour plus d'informations sur les mesures, reportez-vous à la section [Onglet Navigateur de mesures](#).

Utilisation de l'outil de suivi de transaction

Les utilisateurs de la station de travail disposant des autorisations appropriées utilisent l'outil de suivi de transaction pour suivre l'activité des transactions dans une application de production. Les transactions sont identifiées à mesure qu'elles circulent via une machine virtuelle Java ou un moteur CLR (Common Language Runtime) dans un environnement .NET.

L'outil de suivi de transaction permet de capturer les transactions qui remplissent certains critères. Il examine ensuite les appels effectués dans l'ensemble du système pour cette transaction. L'interface utilisateur graphique vous permet de facilement trier les pannes d'applications et les problèmes de performances.

Les méthodes de collecte des traces de transaction sont les suivantes :

- Utilisez l'outil de suivi de transaction.

Pour exécuter une session de suivi de transaction, spécifiez les agents pour lesquels vous souhaitez effectuer le suivi des transactions et la période de capture des données. Vous pouvez spécifier des options de filtre pour limiter le suivi des transactions. Vous pouvez filtrer les transactions qui ont dépassé le seuil de temps d'exécution, qui correspondent aux valeurs de paramètre ou qui contiennent des erreurs.

Une fois la session de suivi de transaction lancée, les transactions correspondant aux critères de filtre s'affichent dans la table de transaction. Les événements de transaction incluent des traces et des erreurs de transaction.

- L'agent collecte automatiquement les traces de transaction.

Lorsque l'instrumentation intelligente est activée, l'agent collecte automatiquement une trace de transaction dans plusieurs circonstances.

L'outil de suivi de transaction peut suivre les transactions synchrones qui dépassent les limites dans les environnements de serveur d'applications homogène prenant en charge cette fonctionnalité :

- WebLogic Server 8.0 et versions ultérieures
- WebSphere 6.x

Dans d'autres environnements, les transactions peuvent être suivies dans les limites d'une seule machine virtuelle ou d'un moteur CLR unique.

Vous affichez les résultats d'une requête de suivi de transaction interprocessus dans l'onglet Vue Suivi de la visionneuse des traces de transaction.

DX APM enregistre les données de session de suivi de transaction dans la base de données des événements de transaction pour la durée spécifiée. Les données sont régulièrement définies comme étant obsolètes afin de réduire la surcharge.

Vous pouvez configurer l'agent pour capturer les données de trace de transaction en fonction des valeurs des variables ASP.NET ou du servlet. Les variables incluent les en-têtes de demande HTTP, les paramètres de demande, les attributs de session, l'ID de session, le nom d'utilisateur, les URL et les chaînes de requête d'URL. En outre, par défaut, les agents recueillent des exemples de transaction.

NOTE

L'état de fermeture des mesures n'affecte pas les données de trace de transaction. Lorsqu'un agent géré est désactivé, celui-ci ne signale pas les données de trace de transaction. Il peut être désactivé lors d'une session de suivi de transaction. Dans ce cas, l'agent signale les données collectées avant la demande de fermeture.

Echantillonnage des traces de transactions

Par défaut, les agents échantillonnent le comportement des transactions en suivant chaque URL normalisée unique dans une application une fois par heure. Vous pouvez afficher et analyser les traces échantillonnées d'une période historique sélectionnée :

- dans la station de travail
- dans l'onglet **Traces** du navigateur de mesures

Vous pouvez également configurer l'échantillonnage de trace de transaction, même si aucun groupe d'URL n'est configuré. Vous spécifiez le nombre de transactions à échantillonner sur une période. La valeur par défaut est une transaction toutes les 2 minutes.

L'échantillonnage des informations de suivi de transaction est activé par défaut. Vous pouvez désactiver le comportement, modifier la période d'échantillonnage ou annuler la mise en mode aléatoire de la période d'échantillonnage si nécessaire.

NOTE

Informations complémentaires : [Configuration des options de trace de transaction](#) (agent Java) ou [Options de l'outil de suivi de transaction](#) (agent .NET).

Surcharge de trace de transaction

Une session de suivi de transaction affecte la surcharge du début du traitement de toutes les transactions jusqu'à la fin de la session. Vous pouvez spécifier le seuil d'exécution à la milliseconde, mais cela augmente la charge du système.

Les fonctionnalités de l'outil de suivi de transaction réduisent la probabilité qu'une session de suivi impose une surcharge inacceptable :

- **Délai d'expiration de la session de suivi de transaction** : une session de suivi de transaction expire après une période définie par l'utilisateur pour que l'administrateur ne puisse pas accidentellement laisser activé l'outil de suivi de transaction et affecter les performances sur une longue période. A la fin du délai d'expiration, l'agent arrête le suivi des nouvelles transactions et termine le suivi des transactions en cours d'exécution.
- **Logique anti-saturation** : pour empêcher une surcharge excessive, la logique anti-saturation de l'agent limite le nombre de transactions suivies par intervalle de 15 secondes à 200. Une fois cette limite dépassée, l'agent enregistre que le seuil anti-saturation a été dépassé. Il ne signale plus les données de suivi de transaction au gestionnaire d'entreprise jusqu'à ce que l'expiration de la période de 15 secondes. Une fois la période de 15 secondes expirée, la logique anti-saturation reprend la génération de rapports.

Traces de transaction collectées de manière automatique

Lorsque l'instrumentation intelligente est activée, l'agent collecte automatiquement une trace de transaction dans les cas suivants :

- Une erreur se produit.
- L'analyse différentielle détecte une instabilité de l'application et la limite de fixation de suivi automatique par intervalle n'est pas dépassée.
Remarque : Le suivi automatique des transactions selon l'analyse différentielle nécessite un agent 10.0 au minimum.
- L'outil de suivi `ComponentTimeAutoTraceTriggerTracer` est déployé et le délai de réponse d'un composant est dépassé.
- Une API déclenche des suivis de transaction automatique en fonction des critères personnalisés. Pour plus d'informations, contactez les [services d'implémentation de DX APM](#).

Les outils de suivi optimisés et à surcharge faible collectent les suivis de transactions automatiques. Les informations de suivi automatique supposent une surcharge de performances moindre que pour l'exécution manuelle, l'échantillonnage et les autres suivis de transaction. Les autres types de suivi de transaction utilisent un filtrage d'agent qui ajoute une surcharge. Le suivi automatique des transactions n'affiche pas toutes les propriétés détaillées du composant que les autres types de suivi de transaction affichent.

Les traces de transaction automatiques présentent les caractéristiques suivantes :

- Tous les composants instrumentés par des directives PBD possèdent une mesure associée dans l'arborescence du navigateur de mesures. Aucune mesure n'est associée aux composants de visibilité approfondie.
- Les [composants de visibilité approfondie](#) incluent uniquement le nom de classe, le nom de méthode et la durée. Pour les composants frontaux et d'arrière-plan (par exemple, les servlets, services Web, appels SQL), le nom est formaté selon la configuration des directives PBD.
- Les propriétés suivantes s'affichent dans les détails du composant :
 - Le **type de trace** est **Normal**.
 - Si une erreur a déclenché la trace de transaction, le composant qui a généré l'exception inclut les propriétés du composant.
 - Le premier composant dans la trace de transaction affiche la propriété `Auto Trace Trigger Criteria` (Critères du déclencheur de suivi automatique).
- Prise en charge du suivi des transactions interprocessus

NOTE

Informations complémentaires :

- La section [Configuration de l'instrumentation intelligente](#) décrit la configuration des transactions interprocessus dans les traces de transaction automatiques.

Si vous ne voyez pas les traces de transaction automatiques, cela peut être dû à l'une des raisons suivantes :

- L'instrumentation intelligente n'est pas activée.

NOTE

L'instrumentation intelligente est disponible uniquement pour les agents Java et non pour les agents .NET.

- Un agent en mode hérité surveille la machine virtuelle Java. Le mode hérité ne prend pas en charge les fonctionnalités d'instrumentation intelligente.
- La valeur limite du nombre de traces de transaction automatiques par intervalle (propriété `agent.deep.automatic.trace.clamp`) est dépassée. Reportez-vous à la mesure de prise en charge `Deep Tracing|Auto Tracing: Clamped: Clamped Traces`

NOTE

Informations complémentaires :

- [Configuration de l'instrumentation intelligente](#)
- [Propriétés de l'instrumentation intelligente](#)

Si des filtres manuels correspondent à une trace de transaction automatique pendant l'exécution manuelle d'une trace, l'agent collecte uniquement la trace manuelle.

Suivi automatique des transactions en cas de dépassement du temps de réponse du composant

Vous pouvez déployer un PBD pour déclencher automatiquement le suivi de transaction lorsque le temps de réponse du composant a été dépassé. Pour cela, vous créez une entrée PBD avec un outil de suivi pour collecter les informations de suivi automatique. Par exemple, pour collecter les informations de suivi lorsque le temps de réponse d'un servlet spécifique dépasse 10 secondes. Utilisez l'option d'outil de suivi `ComponentTimeAutoTraceTriggerTracer` pour configurer cette fonctionnalité.

NOTE

Informations complémentaires : [Configuration des options de trace de transaction](#)

Lorsque `ComponentTimeAutoTraceTriggerTracer` déclenche une trace de transaction, le premier composant de la trace inclut la propriété des détails de composant `Auto Trace Trigger Criteria` (Critères du déclencheur de suivi automatique). Cette propriété affiche **Response Time <nom_composant> Threshold Value exceeded <valeur>**.

Composants de visibilité approfondie

Lorsque l'instrumentation intelligente est activée, les agents détectent et collectent automatiquement des informations détaillées sur les composants de transaction au niveau de la méthode. Les agents détectent et instrumentent automatiquement les composants de visibilité approfondie, sans utiliser de fichiers de directives ProbeBuilder (PBD). L'agent analyse la complexité des méthodes afin d'identifier les appels et les composants à instrumenter et à afficher comme composants de visibilité approfondie.

NOTE

L'instrumentation intelligente est disponible uniquement pour les agents Java et non pour les agents .NET.

Choses à savoir à propos des composants de visibilité approfondie :

- Les composants de visibilité approfondie n'incluent pas de liens vers les mesures. Aucune donnée de mesure ne s'affiche dans l'arborescence du navigateur de mesures.
- Ils contiennent uniquement le nom de classe, le nom de méthode et la durée.
- Les [propriétés de détails composant](#) suivantes s'affichent dans la vue **Suivi** :
 - La propriété nommée `Is Unmonitored` indique un composant de visibilité approfondie.
 - Instrumentation Level (Niveau de l'instrumentation) : niveau de l'instrumentation intelligente auquel une transaction a été détectée.
 - Method Score Level (Niveau d'indice de méthode) : niveau d'instrumentation intelligente qui est en corrélation avec l'indice que l'algorithme d'évaluation DX APM affecte à la méthode d'un composant de visibilité approfondie. DX APM peut afficher les méthodes de composant de visibilité approfondie dont les indices varient dans une trace de transaction, une erreur ou un blocage. Par exemple, une transaction détectée à l'aide d'un niveau moyen peut afficher les méthodes dont les niveaux d'indice sont à la fois moyens et faibles. Utilisez les propriétés Instrumentation Level et Method Score Level pour déterminer la profondeur de la visibilité d'instrumentation intelligente d'une trace de transaction. Vous pouvez également déterminer la profondeur de visibilité des méthodes dans une trace. Par exemple, vous pouvez comparer le nombre de méthodes que l'instrumentation intelligente détecte à deux niveaux d'infrastructure différents. Vous pouvez noter le niveau d'instrumentation intelligente auquel DX APM évalue certaines méthodes spécifiques. Vous pouvez ajuster la solution de surveillance pour la surveillance de visibilité, l'équilibrage de charge et la visibilité souhaités.
- L'icône représentant un éclair qui identifie les composants de visibilité approfondie ne s'affiche pas dans la station de travail.

Vous pouvez [configurer la profondeur de la visibilité de l'instrumentation intelligente](#) d'après votre environnement et vos exigences. Par exemple, configurez l'agent pour détecter et instrumenter automatiquement une quantité faible, moyenne ou élevée du code d'application.

Points d'entrée

La détection automatique des points d'entrée permet de rapidement surveiller et trier les applications Java sans configurer manuellement les directives ProbeBuilder.

Lorsque l'instrumentation intelligente et la détection de points d'entrée sont activées, l'agent surveille les threads qui sont impliqués dans les transactions d'appel de socket client. L'instrumentation intelligente et la détection des points d'entrée sont activées par défaut. Les *points d'entrée* sont les points de début de transaction. Un moteur de règles dans l'agent identifie les points d'entrée candidats. L'agent instrumente et surveille le point d'entrée candidat apparu le plus tôt dans le thread de transaction. Un point d'entrée qu'un agent détecte et conserve est activé pour la surveillance par tous les agents utilisant le même répertoire d'installation. Toutefois, la génération de rapports de mesure de point d'entrée requiert les mêmes classes de code ou de structure dans les autres machines virtuelles Java du serveur d'applications.

Voici quelques exemples de transactions dans lesquelles la détection des points d'entrée offre automatiquement une visibilité :

- Piles et infrastructures technologiques que l'instrumentation DX APM ne surveille pas déjà
- Appels d'API personnalisés ou propriétaires
- Threads d'arrière-plan qui consomment des ressources critiques et peuvent réduire les performances globales de l'application

NOTE

La détection des points d'entrée ne prend pas en charge le protocole UDP (User Datagram Protocol).

L'agent enregistre les points d'entrée dans le fichier `AutoPersist.pbd`, qui est conservé dans le répertoire `<répertoire_base_agent>\core\config\hotdeploy`.

WARNING

L'utilisateur système qui exécute le serveur d'applications requiert un accès en lecture/écriture au répertoire `hotdeploy`. Ces autorisations permettent à l'agent d'écrire des données dans le fichier `AutoPersist.pbd`.

Les points d'entrée diffèrent des composants frontaux. L'agent Java détecte automatiquement les points d'entrée, qui se trouvent à proximité du début du chemin d'appel de transaction. Les composants frontaux sont définis manuellement dans les directives PBD et peuvent se trouver n'importe où dans un chemin d'appel de transaction.

WARNING

N'apportez pas de modifications manuelles au fichier `AutoPersist.pbd`. Toutefois, vous pouvez copier les points d'entrée détectés et les utiliser dans une autre directive PBD.

Les mesures des points d'entrée s'affichent dans l'arborescence centrée sur l'agent, dans le sous-nœud **Point d'entrée automatique**, sous le nœud de l'agent.

NOTE

Vérifiez que la propriété `introscope.autoprobe.dynamicinstrument.enabled` dans `IntroscopeAgent.profile` est définie sur `true`. Cette configuration permet à l'agent de signaler des mesures de point d'entrée sans devoir redémarrer l'application.

L'agent signale les cinq mesures BlamePoint standard pour chaque point d'entrée. Les points d'entrée s'affichent dans les traces de transaction. Les noms de point d'entrée respectent le format suivant : `entry point <nom_classe _ nom_méthode>`. L'agent signale les mesures de [prise en charge des points d'entrée](#).

Vous pouvez [configurer la collecte de points d'entrée](#). Par exemple, une propriété de configuration limite le nombre de points d'entrée que le fichier `AutoPersist.pbd` peut conserver.

NOTE

Informations complémentaires : [Création de fichiers PBD pour la conversion de points d'entrée en composants frontaux](#)

Composants d'arrière-plan automatiques

Lorsque la *détection automatique des composants d'arrière-plan* est activée, l'agent détecte et surveille automatiquement les composants d'arrière-plan d'application sans qu'aucune configuration manuelle ne soit requise.

Un moteur de détection dans l'agent identifie les composants d'arrière-plan automatiques candidats. Les composants d'arrière-plan automatiques qu'un agent détecte et conserve sont activés pour la surveillance par tous les agents utilisant le même répertoire d'installation.

Voici quelques exemples de composants d'arrière-plan que la détection des composants d'arrière-plan automatiques peut trouver et surveiller :

- Piles et infrastructures technologiques en arrière-plan que l'agent ne surveille pas déjà. MongoDB et Cassandra sont des exemples de composants d'arrière-plan non SQL.
- Composants d'arrière-plan propriétaires ou personnalisés

L'agent enregistre les composants d'arrière-plan automatiques dans le fichier `AutoPersist.pbd`, qui est conservé dans le répertoire `<répertoire_base_agent>\core\config\hotdeploy`.

WARNING

- L'utilisateur système qui exécute le serveur d'applications requiert un accès en lecture/écriture sur le répertoire `/hotdeploy`. Ces autorisations permettent à l'agent d'écrire des données dans le fichier `AutoPersist.pbd`.
- N'apportez pas de modifications manuelles au fichier `AutoPersist.pbd`. Toutefois, vous pouvez copier des composants d'arrière-plan automatiques détectés et les utiliser dans un autre fichier PBD.

Vous pouvez [configurer la détection des composants d'arrière-plan automatiques](#). Par exemple, une propriété de configuration limite le nombre de composants d'arrière-plan automatiques que le fichier `AutoPersist.pbd` peut conserver.

Dans la vue **Suivi**, les paramètres de `port distant` et de `nom de serveur distant` apparaissent dans les **détails du composant**.

Démarrage, arrêt et redémarrage d'une trace de transaction

Contenu

Pour exécuter une session de trace de transaction manuellement, spécifiez les agents pour lesquels vous souhaitez effectuer le suivi des transactions et la période de capture des données. Vous pouvez spécifier des options de filtre pour limiter le suivi des transactions suivantes :

- Les transactions qui dépassent un seuil de délai d'exécution que vous définissez.
- Les transactions qui correspondent aux valeurs de paramètre tel que l'ID d'utilisateur, les informations des en-têtes de demande, etc.
- Les transactions comprenant des erreurs, si `ErrorDetector` est activé.

Lors du démarrage de la session de suivi de transaction, Introscope capture les données de trace de transaction spécifiées dans le profil de l'agent, pour chaque transaction. Les transactions qui correspondent aux critères de filtre s'affichent dans la fenêtre Visionneuse des traces de transaction et sont enregistrées dans la base de données des événements de transaction.

Démarrage d'une session de suivi de transaction

Pour démarrer une session de suivi de transaction :

1. Sélectionnez Poste de travail > Nouvelle session de suivi de transaction.
La fenêtre Nouvelle session de suivi de transaction s'ouvre.
2. Dans la section Effectuer le suivi de transactions de la fenêtre, spécifiez la durée minimum des transactions à suivre. Dans la liste déroulante, sélectionnez millisecondes ou secondes.
Remarque : Les durées définies sur une unité sous les secondes peuvent affecter les performances.
3. Pour spécifier un filtre de transaction, cochez la case à gauche du menu déroulant grisé ID d'utilisateur dans la section *Effectuer le suivi de transactions*, puis sélectionnez un type dans la liste :
 - ID d'utilisateur : entrez un opérateur et une valeur de paramètre.
 - ID de session : entrez un opérateur et une valeur de paramètre.
 - URL ou Requête d'URL : entrez un opérateur et une valeur de paramètre.
 - En-tête de demande : entrez un nom de type de données, une condition et une valeur.
 - Paramètre de la demande : entrez un nom de type de données, un opérateur et une valeur de paramètre.
 - Attribut de session : entrez un nom de type de données, un opérateur et une valeur de paramètre.**Remarque :** Les données sont uniquement disponibles pour une utilisation dans les filtres si l'agent est configuré pour les capturer.

Les conditions de filtre sont les suivantes :

- est égal à : les transactions pour lesquelles la valeur du paramètre correspond à la chaîne spécifiée sont suivies.
- n'est pas égal : les transactions pour lesquelles la valeur du paramètre ne correspond pas à la chaîne spécifiée sont suivies.

Remarque : Les transactions qui n'incluent pas le paramètre auquel le filtre s'applique sont également suivies.

- contient : les transactions pour lesquelles la valeur du paramètre contient la chaîne spécifiée sont suivies.
- ne contient pas : les transactions pour lesquelles la valeur du paramètre ne contient pas la chaîne spécifiée sont suivies.

Remarque : Les transactions qui n'incluent pas le paramètre auquel le filtre s'applique sont également suivies.

- commence par : les transactions pour lesquelles la valeur du paramètre commence par la chaîne spécifiée sont suivies.
- finit par : les transactions pour lesquelles la valeur du paramètre finit par la chaîne spécifiée sont suivies.
- existe : les transactions qui incluent le paramètre auquel le filtre s'applique sont suivies, quelle que soit la valeur du paramètre.
- n'existe pas : les transactions qui n'incluent pas le paramètre auquel le filtre s'applique sont suivies.

4. Spécifie la durée de la session de suivi en minutes.

5. Dans la section Effectuer le suivi d'agents, sélectionnez un ou plusieurs agents pour lesquels effectuer le suivi des transactions :

- Pour suivre tous les agents qui prennent en charge le suivi de transactions, sélectionnez Effectuer le suivi de tous les agents pris en charge. Cette option permet d'effectuer le suivi des agents pris en charge et actuellement connectés, ainsi que des agents qui se connectent pendant la session de suivi.
- Pour suivre les agents sélectionnés, sélectionnez Effectuer le suivi des agents sélectionnés et sélectionnez des agents dans la liste (Ctrl + clic pour sélectionner plusieurs agents).

6. Sélectionnez OK pour démarrer la session de suivi de transaction.

Les résultats du suivi de transaction s'affichent dans la [Visionneuse des traces de transaction](#).

En mode dynamique, les événements de trace de transaction des 20 dernières minutes sont affichés. En d'autres termes, les événements de trace de transaction de plus de 20 minutes ne s'affichent pas en mode dynamique. Un maximum de 500 événements de trace de transaction sont affichés.

Arrêt d'une session de suivi de transaction

Pour arrêter une session de suivi de transaction :

- Cliquez sur Arrêter.
- Vous pouvez également sélectionner Suivi > Arrêter la session de suivi.

Redémarrage d'une session de suivi de transaction

Redémarrer la session de suivi de transaction réinitialise le délai d'expiration pour la période définie par l'utilisateur et permet de continuer le suivi des transactions dans les agents cibles en utilisant les mêmes critères de seuil.

Vous pouvez redémarrer une session de suivi de transaction :

- Après l'expiration d'une session.
- Pour redémarrer une session que vous avez arrêtée.
- Pour redémarrer une session en cours.

Pour redémarrer une session de suivi de transaction :

- Cliquez sur Redémarrer.
- Vous pouvez également sélectionner Suivi > Redémarrer la session de suivi.

Utilisation de la visionneuse des traces de transaction

La visionneuse des traces de transaction affiche les informations de suivi des transactions qui répondent aux critères spécifiés pour la session de suivi.

Le tableau dans le volet supérieur de la visionneuse des traces de transaction répertorie les transactions suivies lors de la session. Vous pouvez trier les lignes par colonne en cliquant sur l'en-tête de colonne. Les nouvelles transactions sont insérées dans le tableau dans l'ordre de tri.

Cette table répertorie les colonnes figurant dans la table des transactions :

Champ	Description
Type	Type d'informations de la ligne de trace : Trace de transaction (T) Erreur (E) Exemple (R) Transaction sélectionnée lors d'un échantillonnage aléatoire Bloqué (S) Transaction bloquée Les données d'erreur s'affichent uniquement si ErrorDetector est activé. Astérisque Si un astérisque s'affiche après le symbole de type, certains composants dans la transaction ont été tronqués ou sont limités . Seules les transactions de type T et E peuvent être limitées. Les types répertoriés ici s'appliquent aux transactions disponibles en mode dynamique. Lors de l'interrogation des transactions historiques, les autres types de transaction sont disponibles.
Domaine	Domaine auquel l'agent suivi est mappé.
Host	Hôte sur lequel s'exécute l'agent suivi.
Processus	Nom du processus d'agent
Agent	Nom de l'agent
Horodatage	Heure de début, selon l'horloge système de l'agent, de l'appel du composant racine.
Durée	Heure d'exécution d'horloge du composant racine.
Description	URL appelée pour lancer la transaction ou chemin d'accès Introscope au composant qui a initialisé la transaction.
ID d'utilisateur	ID de l'utilisateur connecté qui exécute la transaction (s'il est configuré et disponible).

La fenêtre Outil de suivi de transaction contient trois onglets :

- Vue récapitulative
- Vue Suivi
- Arborescence

Vue récapitulative

La première fois que vous sélectionnez une transaction dans la table des transactions, la vue récapitulative s'ouvre. Lorsque vous sélectionnez une transaction ouverte auparavant, elle s'ouvre dans la vue la plus récemment sélectionnée.

Ces informations s'affiche pour la transaction actuellement sélectionnée dans chaque onglet :

- Nom complet de l'agent
- Heure de début, selon l'horloge système de l'agent, de l'appel du composant racine.
- Durée d'exécution du composant racine en millisecondes

La vue récapitulative affiche des mesures pour les composants dans la transaction sélectionnée. Les mesures peuvent inclure le chemin d'accès, le nombre d'appels, la durée de l'appel en millisecondes ainsi que les durées d'appel moyenne, minimum et maximum. Double-cliquez sur une des mesures qui figurent dans la vue de table pour ouvrir la mesure dans l'arborescence de navigation.

Au bas de la fenêtre Suivi, la barre de statut de la trace de transaction affiche :

- Nombre de transactions collectées dans la session.
- Critères de filtre pour la session de suivi de transaction.
- Temps restant avant l'expiration de la session en cours.

NOTE

Pour les composants de transaction corrélés, les onglets Vue récapitulative et Arborescence affichent uniquement la portée de la première machine virtuelle Java. L'onglet Vue Suivi affiche l'ensemble de la portée des composants de transaction associés. Tenez compte de cette limitation lorsque vous passez de l'onglet Vue Suivi aux autres vues d'onglet.

Vue Suivi

La Vue Suivi affiche une transaction sélectionnée dans une pile graphique des composants constituant la transaction. Lorsque vous sélectionnez un des composants, vous affichez les détails du composant dans le volet inférieur de la visionneuse.

Contenu de la Vue Suivi :

- Chaque composant dans la transaction sous forme de barre
- Pourcentage de la durée d'exécution totale des transactions de chaque composant
- Relations d'appel entre les composants
Les barres des composants s'affichent de haut en bas dans l'ordre des appels.
- Séquence de transactions au fil du temps
La position des composants de gauche à droite indique la séquence. Le temps horloge relatif, en millisecondes, s'affiche en haut du cliché de transaction.
- Composants de visibilité approfondie. Introscope détecte automatiquement ces composants et les instrumente à l'aide de l'instrumentation intelligente sans recourir à un PBD.

NOTE

L'instrumentation intelligente est disponible uniquement pour les agents Java et non pour les agents .NET.

- Erreurs dans les transactions (Détection et analyse d'erreurs et de blocages). Si ErrorDetector est activé.
Les sections rouges dans le cliché de transaction indiquent des erreurs dans les transactions.

NOTE

La période par défaut pour les traces en mode dynamique est de 20 minutes. Les traces de transaction de plus de 20 minutes ne s'affichent pas en mode dynamique. Les traces ne sont pas affichées, car elles sont obsolètes après plus de 20 minutes.

Dans la Vue Suivi, vous pouvez effectuer les actions suivantes :

- Placez le curseur sur un composant pour ouvrir une info-bulle.
- Cliquez avec le bouton droit de la souris sur un composant pour ouvrir l'arborescence de mesures et afficher les mesures de composants.
- Sélectionnez un composant dans la Vue Suivi pour ouvrir le volet Détails du composant de transaction.

Détails du composant de transaction

Les détails du composant affichés dans la Vue Suivi sont les suivants :

- **Type** Composant de haut niveau (par exemple, EJB, servlet, JSP dans un environnement Java et ASPX dans un environnement .NET).
- **Nom** Nom du composant.
- **Chemin** Nom complet de la ressource du composant.
- **Durée** Durée d'exécution du composant sélectionné. L'unité par défaut est la milliseconde.
- **Horodatage (relatif)** Heure de début, selon l'horloge système de l'hôte de l'agent, de l'appel du composant sélectionné.
- **% du temps de transaction total** Pourcentage de la durée totale de transaction requise par le composant sélectionné.
- **Propriétés** Propriétés facultatives signalées par le composant (par exemple, URL, Requête d'URL, SQL dynamique) ou définies pour la collecte dans le profil d'agent (ID d'utilisateur, En-tête de demande, Paramètre de la demande ou Attribut de session). Vous pouvez sélectionner le texte d'un champ dans les détails des propriétés et le copier à l'aide de la combinaison de touches CTRL + C.

Propriété	Description
User ID (ID d'utilisateur pour servlet, JSP, ASPX)	ID de l'utilisateur qui appelle la demande de servlet HTTP.
URL (servlet, JSP, ASPX)	URL transmise au servlet ou JSP, à l'exception de la chaîne de requête (texte après le délimiteur ? dans l'URL).
URL Query (Requête d'URL pour servlet, JSP, ASPX)	Partie de l'URL qui spécifie les paramètres de requête dans la demande HTTP (texte après le délimiteur ? dans l'URL).
Session ID (ID de la session pour servlet, JSP, ASPX)	ID de la session HTTP associée à la demande de servlet, le cas échéant.
Dynamic SQL (instructions JDBC ou ADO.NET dynamiques, lorsque l'agent SQL est installé).	Instruction SQL dynamique généralisée, comme elle apparaîtrait sous forme agrégée dans l'agent SQL.
Callable SQL (Instruction SQL sur appel - instructions JDBC ou ADO.NET sur appel, lorsque l'agent SQL est installé)	Instruction SQL sur appel (avec le ? toujours présent)
Prepared SQL (Instruction SQL préparée - instructions JDBC ou ADO.NET préparées, lorsque l'agent SQL est installé)	Instructions SQL préparées (avec le ? toujours présent)
Method (outils de suivi responsables ; tout sauf les instructions de servlets, JSP et JDBC pour Java, ASPX et ADO.NET pour .NET)	Nom de la méthode suivie
Is Unmonitored (Non surveillé)	L'instrumentation intelligente détecte le nom du composant suivi. Aucune mesure n'est collectée pour ce composant.
Trace Truncated (Trace tronquée)	La trace de transaction est tronquée à la dernière méthode dans la trace. La troncation est généralement due à des appels récursifs approfondis.

Auto Trace Trigger Criteria (Critères du déclencheur de suivi automatique)	<p>Déclencheur qui indique à Introscope de collecter une trace de transaction automatique. Par exemple, si une erreur se produit ou qu'un temps de réponse de composant est dépassé lorsque le traceur <code>ComponentTimeAutoTraceTriggerTracer</code> est déployé.</p> <p>Lorsque <code>ComponentTimeAutoTraceTriggerTracer</code> est le déclencheur, <code>Auto Trace Trigger Criteria</code> (Critères du déclencheur de suivi automatique) affiche <code>Response time of <nom_composant> exceeds threshold <valeur></code> (Le temps de réponse de <code><nom_composant></code> dépasse le seuil <code><valeur></code>).</p> <p><code>Auto Trace Trigger Criteria</code> affiche les déclencheurs suivants lorsque les agents collectent des transactions interprocessus dans les traces de transaction automatiques :</p> <ul style="list-style-type: none"> Lorsqu'un agent en amont déclenche une transaction interprocessus, <code>Auto Trace Trigger Criteria</code> (Critères du déclencheur de suivi automatique) affiche le déclencheur Introscope. Par exemple, <code>error</code> (erreur) ou <code>Response time of <nom_composant> exceeds threshold <valeur></code> (Le temps de réponse de <code><nom_composant></code> dépasse le seuil <code><valeur></code>). Lorsqu'un agent en aval déclenche une transaction interprocessus, <code>Auto Trace Trigger Criteria</code> (Critères du déclencheur de suivi automatique) affiche le déclencheur <code>interprocessus</code>.
Instrumentation Level (Niveau d'instrumentation)	Niveau d'instrumentation intelligente auquel une transaction est détectée.
Method Level Score (Indice du niveau de méthode)	Niveau d'instrumentation intelligente qui est en corrélation avec l'indice que l'algorithme d'évaluation Introscope affecte à la méthode d'un composant de visibilité approfondie. Introscope peut afficher les méthodes de composant de visibilité approfondie dont les indices varient dans une trace de transaction, une erreur ou un blocage. Par exemple, une transaction détectée à l'aide d'un niveau moyen peut afficher les méthodes dont les indices de niveau sont moyens et faibles.

Info-bulles dans la visionneuse des traces de transaction

Vous pouvez passer le curseur sur les composants ou les couches de la représentation graphique d'une transaction. Une info-bulle affiche les détails du composant.

L'info-bulle affiche les informations suivantes :

- Chemin
- Durée
- Horodatage (relatif)
- % du temps de transaction total

Vue de séquence

L'onglet Vue de séquence affiche les composants de transaction dans l'ordre dans lequel un processus appelle les composants.

ID de corrélation dans les transactions interprocessus

La station de Introscope utilise un identificateur unique (ID de corrélation) pour lier les transactions des serveurs frontaux et d'arrière-plan suivis. L'ordre selon lequel les serveurs frontaux appellent les serveurs d'arrière-plan dans une transaction détermine le séquençement de cet ID.

Vous pouvez utiliser l'ID de corrélation pour reconnaître et suivre le chemin d'accès des composants liés dans une trace de transaction. Cette information permet de déterminer les appels pouvant être à l'origine d'une transaction lente ou bloquée.

NOTE

Informations complémentaires : [Utilisation du suivi des transactions interprocessus pour résoudre des problèmes.](#)

Transactions limitées

Une propriété de limitation empêche les résultats de trace de transaction inhabituels de consommer trop de cycles. La limite des composants de trace de transaction est définie par défaut sur 5 000. Cette propriété, `introscope.agent.transactiontrace.componentCountClamp`, est spécifiée dans `IntroscopeAgent.profile`. Vous pouvez configurer les propriétés de l'[agent Java](#) et de l'[agent .NET](#).

Les composants de trace de transaction qui dépassent les limites `introscope.agent.transactiontrace.componentCountClamp` sont signalés par un astérisque.

Points à noter :

- La première ligne de traces est sélectionnée.
- Le symbole de type est marqué par un astérisque. L'astérisque indique que certains composants dans la transaction ont été tronqués ou limités.
- Une info-bulle indique le nombre de composants tronqués. Dans l'exemple ci-dessus, 15 des composants de la trace sélectionnée dépassaient le nombre spécifié par la propriété `introscope.agent.transactiontrace.componentCountClamp`.
- Les composants non tronqués s'affichent dans l'onglet Vue récapitulative en bas de la visionneuse.
- Chaque agent comprend une valeur heuristique `IsClamped` (0=non limité et 1=limité).

Apparence du fichier XML exporté en cas de limitation des transactions

Lorsqu'un composant de trace est limité, le format du fichier XML exporté est correct et inclut un paramètre semblable au paramètre suivant :

```
<Parameter Value="15" Name="Components Not Shown"/>
```

Pour afficher une info-bulle contenant des informations complémentaires sur une trace :

1. Sélectionnez l'une des traces de la table.
2. Placez le curseur sur la trace sélectionnée.
L'info-bulle affiche le type de trace et le nombre de composants tronqués ou limités.

Pour trier les traces par type :

- Cliquez sur l'en-tête de la colonne Type dans la table.

Recherche de transactions limitées

Vous pouvez rechercher des transactions limitées en effectuant une requête d'événement historique. Utilisez un exemple de chaîne dans votre requête, comme dans l'exemple suivant :

```
componentsNotShown:[1 TO 9999]
```

Utiliser une chaîne garantit que la requête renvoie des traces comprenant des transactions limitées.

NOTE

Les recherches de la visionneuse d'événements historiques utilisent la syntaxe Lucene. Les règles de syntaxe suivantes s'appliquent donc aux requêtes d'événements historiques :

- Le mot TO dans la chaîne est sensible à la casse.
- La syntaxe de recherche est lexicographique, et non numérique. C'est pourquoi le fait d'effectuer une requête historique à l'aide du filtre de requête `componentNotShown` peut renvoyer des résultats incorrects.
- Les chaînes commençant par * (astérisque) ou par ? (point d'interrogation) ne sont pas autorisées.

Affichage des erreurs dans l'outil de suivi de transaction

Lorsque [Détection et analyse d'erreurs et de blocages](#) est activé, vous pouvez utiliser l'outil de suivi de transaction pour identifier et afficher les erreurs.

A propos de l'arborescence dans l'outil de suivi de transaction

Afficher les composants de transaction dans une vue hiérarchique d'informations. Vous pouvez accéder au composant et identifier les problèmes de performances.

Vous pouvez afficher les composants instrumentés à l'aide de PBD et les composants de visibilité approfondie. Introscope détecte et utilise automatiquement les composants de visibilité approfondie sans utiliser de PBD.

NOTE

L'instrumentation intelligente est disponible uniquement pour les agents Java et non pour les agents .NET.

Procédez comme suit :

1. Dans WebView, cliquez sur Outils, Outil de suivi de transaction.
2. Sélectionnez une trace de transaction dans la table.
3. Cliquez sur l'onglet Arborescence dans le volet inférieur.
4. Développez un noeud dans l'arborescence.
Chaque noeud dans l'arborescence affiche le composant, le nom, la durée et le pourcentage de la durée totale de transaction. La couleur de l'icône en forme de cercle indique la durée :
 - Rouge : durée du composant > 25 % de la durée totale
 - Jaune : durée du composant > 9 % < 25 % de la durée totale
 - Vert : durée du composant < = 9 % de la durée totale



Dans le graphique, vous pouvez suivre les indicateurs circulaires rouges dans l'arborescence. Vous pouvez consulter les méthodes impliquées dans la majeure partie du temps de transaction. Par exemple, la méthode `AxisServer::invoke` a pris 95 % des 37 ms qu'il a fallu à la transaction pour s'exécuter.

Les composants de trace qui supposent uniquement une petite partie de la durée de transaction sont signalés par une icône verte.

5. Sélectionnez un composant pour afficher les informations suivantes dans la zone Détails du composant :
 - Type de composant, nom et chemin
 - Durée, horodatage et durée totale de transaction

NOTE

Pour les composants de transaction corrélés, les onglets Vue récapitulative et Arborescence affichent uniquement la portée de la première machine virtuelle Java. L'onglet Vue Suivi affiche l'ensemble de la portée des composants de transaction associés. Tenez compte de cette limitation lorsque vous passez de l'onglet Vue Suivi aux autres vues d'onglet.

Données agrégées pour plusieurs transactions

Dans l'outil de suivi de transaction, vous pouvez sélectionner plusieurs transactions pour afficher les données agrégées pour tous les composants dans les traces.

Procédez comme suit :

1. Ouvrez une liste de transactions en exécutant une trace de transaction.
2. Sélectionnez plusieurs transactions à l'aide des combinaisons CTRL + clic ou MAJ + clic.
3. Ouvrez l'arborescence ou la vue récapitulative pour afficher les données de transactions agrégées.
 - L'outil de suivi de transaction affiche les données agrégées dans la table.
Vous devrez peut-être faire défiler la page pour afficher toutes les données.
 - L'arborescence affiche les données agrégées.
Dans l'arborescence, l'outil de suivi de transaction ajoute un noeud si les transactions sélectionnées ne partagent pas un noeud racine commun. Le noeud est appelé Root.

NOTE**Informations complémentaires :**

- [Impression, enregistrement et exportation des informations de suivi des transactionshttps://techdocs.broadcom.com](https://techdocs.broadcom.com)

Interrogation des événements stockés

Les résultats de la session de suivi de transaction sont stockés automatiquement dans la base de données des événements de transaction. Les événements de transactions incluent les traces de transactions et les erreurs, y compris les blocages (si vous avez installé Introscope Error Detector). La base de données des événements de transaction contient les traces de transactions qui ont été automatiquement échantillonnées par Introscope. La base de données contient également les résultats des sessions de suivi de transaction que vous exécutez.

La base de données des événements de transaction prend en charge les types de requêtes suivants :

- événements historiques (simple) : reportez-vous à la section Interrogation des événements historiques.
- événements similaires (à la sélection)
- événements corrélés (à la sélection)

Remarque : Assurez-vous d'exécuter plusieurs sessions de suivi de transaction avant d'utiliser la requête d'historique, afin que des données soient disponibles pour l'interrogation.

Syntaxe de la requête

Les sections suivantes décrivent comment utiliser la fonctionnalité de requête d'historique pour interroger des erreurs stockées. La fonctionnalité de requête :

- **Respecte la casse** : pour les chaînes de requêtes ou les valeurs des options de requête.
- **Prend en charge le caractère astérisque (*)** : entrez une partie d'un terme de recherche suivi par un astérisque. (Vous ne pouvez pas commencer une recherche par l'astérisque.) Par exemple, pour rechercher les erreurs associées à un composant dont le nom inclut la chaîne Shopping, utilisez la chaîne de requête Shopping*.
- **Prend en charge les opérateurs booléens** : les termes à rechercher peuvent utiliser la logique booléenne, telle que les groupements AND, OR, NOT et ().
- **Prend en charge les conditions d'exclusion** : utilisez +JDBC-CICS pour rechercher des transactions avec JDBC, mais sans CICS.
- **Prise en charge des options de requête** : utilisez les options décrites dans la section Options de requête et la syntaxe pour limiter les événements d'erreur de requête qui se produisent dans un délai spécifique, ou qui sont associés à certains utilisateurs ou à des éléments de l'environnement d'hébergement (tels qu'identifiés par le domaine, l'agent, l'hôte et le processus).

Interrogation des événements historiques

Vous pouvez interroger les événements de transaction historiques.

Procédez comme suit :

1. Sélectionnez Poste de travail > Interroger les événements historiques.
La visionneuse des requêtes historique s'ouvre.
Le champ Requête affiche, dans une liste déroulante, jusqu'à douze recherches précédentes de la session en cours, ou des sessions précédentes du même utilisateur de la station de travail. Cela vous permet de sélectionner l'une des recherches enregistrées au lieu d'avoir à ressaisir l'entrée.
Conseil : Par défaut, le champ garde en mémoire jusqu'à douze recherches. Vous pouvez définir un nombre différent de recherches à garder en mémoire dans le champ en modifiant la propriété `introscope.workstation.historical.query.history.limit` dans le fichier *IntroscopeWorkstation.properties*.
2. Dans le champ Requête, entrez une combinaison des éléments suivants :
 - *Type d'option de requête* : pour inclure tous les événements de transaction qui correspondent au type spécifié.
 - Chaîne de requête : pour rechercher les erreurs qui contiennent ou correspondent à une chaîne. Si vous ne saisissez pas une chaîne de requête, tous les événements d'erreur sont renvoyés.
 - Options de requête : pour limiter votre recherche aux paramètres d'événement, tels que définis dans les options de requête et la syntaxe.**Conseil** : Lorsque vous saisissez une entrée dans le champ Requête, les recherches affichées dans la liste déroulante seront limitées à celles qui correspondent à ce que vous avez saisi.
3. Utilisez l'option Période pour filtrer les requêtes selon une période, le cas échéant. Pour obtenir une explication sur l'utilisation de l'option Période, reportez-vous à la section [Affichage des données historiques](#).
Si vous ne sélectionnez pas une période, la requête utilise la valeur par défaut Tout et n'applique aucun filtre.
4. Cliquez sur OK.
Les transactions qui correspondent à la requête sont affichées dans la fenêtre Requête historique : le format est identique à la visionneuse des traces de transaction. Pour plus d'informations, reportez-vous à la section [Utilisation de la visionneuse des traces de transaction](#).
Remarque : Vous pouvez afficher uniquement 500 événements. Si plus de 500 événements correspondent à la requête, les 500 plus anciens s'affichent.

Options de requête et syntaxe

Les requêtes utilisent la syntaxe d'expressions régulières Lucene pour rechercher et remplacer les chaînes de texte.

Remarque : Pour plus d'informations sur la syntaxe Lucene, consultez le site Web Lucene (lucene.apache.org) et recherchez query syntax.

Champ	Description	Exemple
agent	Limite la recherche aux événements signalés par un agent particulier.	agent:ControlledRangeAgent
domaine	Limite la recherche aux événements liés aux composants d'un domaine donné.	domain:AcmeWest
fullAgent	Limite la recherche aux événements signalés par des agents spécifiques, tels que spécifiés par le chemin complet correspondant : <i>domain process host agent</i> .	fullAgent:AcmeWest Custom Metric Host ControlledRange Agent
host	Limite la recherche aux événements qui se sont produits sur un hôte particulier.	host:Wmiddle01
process	Limite la recherche aux erreurs liées aux composants dans une application donnée.	process:Custom Metric Host
root	Limite la recherche aux événements associés à des composants spécifiques, tels que spécifiés par le chemin de la mesure.	root:servlets accountServlet
type	Spécifie le type d'événement à inclure dans les résultats de la requête. errorsnapshot : limite la recherche aux événements d'erreur. normal : renvoie les événements de transaction capturés dans les traces de transactions initiées par les utilisateurs. sampled : renvoie les événements de transaction capturés à la suite de l'échantillonnage de transaction d'Introscope par défaut.	type:errorsnapshot type:normal type:sampled
url	Limite la recherche aux événements associés avec le préfixe de chemin d'accès d'URL de transaction spécifiée. Le préfixe de chemin est la partie de l'URL qui suit le nom d'hôte. Dans l'URL suivante : <i>http://burger1.com/bWar/burgerServlet?ViewItem&category=11776&item=55562630&rd=1</i> le préfixe de chemin est : <i>/bWar/burgerServlet</i>	url:/bWar/burgerServlet

urlParams	Limite la recherche aux événements associés aux paramètres d'URL de transaction spécifiée. Paramètres URL suivis d'un point d'interrogation (?) dans l'URL. Dans cette URL : http://ubuy.com/ws/shoppingServlet?category=734&item=3772&tc=photo la partie de paramètre d'URL est la suivante : ?category=734&item=3772&tc=photo Remarque : urlParams ne peut pas commencer par un caractère générique.	urlParams:category=734*
user	Limite la recherche aux événements des transactions associées au nom d'utilisateur spécifié.	user:jdoe
duration	Limite la recherche par durée d'événement (en millisecondes par défaut).	
componentsNotShown	Limite la recherche aux événements où un composant donné n'est pas affiché.	
durationencoded	Aucune définition fournie	
time	Limite la recherche aux événements avant ou après un certain temps.	time:[yyyyMMddHH] where y=year, M=month, d=date, and H=hour of day
tracelD	Limite la recherche aux événements avec un ID de suivi spécifié.	tracelD:1340419311156\3957 Remarque : Une barre oblique inversée (\) est requise avant le second deux-points (:).

Si les caractères spéciaux suivants font partie de votre requête, la syntaxe Lucene vous permet de les échapper par une barre oblique inversée (\) :

+ - & | ! () { } [] ^ " ~ * ? : \

Par exemple, pour rechercher (1+1):2, saisissez la requête :

\(1\+1\)\:2

Remarque : L'astérisque (*) et le point d'interrogation (?) ne sont pas pris en charge au début d'une requête.

Recherche d'événements similaires

Dans Introscope, vous pouvez rechercher les événements similaires à un événement sélectionné. Par exemple, des événements similaires peuvent être des événements contenant les mêmes composants (Servlet > EJB > SQL) avec des temps de réponse différents. Introscope considère que des événements sont similaires si 60 % de leurs chaînes (noms de composants, noms de tables SQL, etc.) correspondent.

Remarque : Même si un type d'événement de transaction est sélectionné, les transactions et les erreurs peuvent être renvoyées dans les résultats (les erreurs sont uniquement renvoyées si ErrorDetector est installé).

Procédez comme suit :

1. Lorsqu'une fenêtre de résultats de requête est ouverte, sélectionnez une ligne de table.
2. Sélectionnez Suivi > Événements similaires.

Introscope répertorie les événements similaires dans la fenêtre Requête historique.

Recherche des événements corrélés

Dans Introscope, vous pouvez rechercher les événements corrélés : ceux qui font partie d'une même transaction plus grande. Par exemple, un événement temps de réponse de navigateur est corrélé avec un événement de transaction servlet.

Remarque : Même si un événement de type transaction est sélectionné, les transactions et les erreurs peuvent être renvoyées dans les résultats.

Procédez comme suit :

1. Lorsqu'une fenêtre de résultats de requête est ouverte, sélectionnez une ligne de table.
2. Sélectionnez Suivi > Événements corrélés.

Introscope répertorie les événements corrélés dans la fenêtre Requête historique.

Impression, enregistrement et exportation des informations de suivi des transactions

Vous pouvez effectuer les actions suivantes avec les informations de suivi des transactions :

- Imprimer une fenêtre de trace de transaction.
- Enregistrer les données de suivi des transactions dans un fichier XML que vous pouvez ouvrir plus tard dans une fenêtre Trace de transaction.
- Exporter des données de suivi des transactions dans un fichier texte pour l'examiner dans un éditeur de texte.

Impression d'une fenêtre Trace de transaction

Procédez comme suit :

1. Sélectionnez Poste de travail > Imprimer.
La fenêtre de mise en page s'ouvre. Les valeurs d'impression par défaut sont la taille de lettre et l'orientation portrait.
2. Cliquez sur OK pour continuer, ou modifier les options, puis cliquez sur OK.
La fenêtre Imprimer s'affiche.
3. Sélectionnez les options d'impression, puis cliquez sur OK.

Remarque : L'impression d'une plage de pages n'est pas prise en charge (tout est imprimé sur une page).

L'intégralité du contenu de la fenêtre Trace de transaction est imprimée à l'échelle pour tenir sur une seule page.

Enregistrement des données de trace de transaction

Enregistrez les données de trace de transaction dans un fichier XML. Ultérieurement, vous pouvez ouvrir le fichier dans une fenêtre de trace de transaction pour reproduire la trace de transaction.

Procédez comme suit :

1. Dans la visionneuse des traces de transaction, sélectionnez les traces de transaction à enregistrer :
 - CTRL + clic pour sélectionner plusieurs traces de transaction.
 - Modifier > Tout sélectionner pour sélectionner toutes les traces de transaction dans la fenêtre.
2. Cliquez sur Enregistrer sous.
3. Ouvrez le fichier ou sélectionnez un emplacement dans lequel vous souhaitez enregistrer le fichier.
4. Si vous enregistrez le fichier, entrez un nom de fichier, puis cliquez sur Enregistrer.

Ouverture des données XML de l'outil de suivi des transactions enregistrées

Vous pouvez ouvrir et afficher les données de trace de transaction enregistrées dans une nouvelle fenêtre Trace de transaction. Vous pouvez partager les fichiers enregistrés par courriel ou les stocker sur un lecteur réseau partagé. Partager des fichiers permet aux utilisateurs de collaborer pour l'analyse des problèmes.

Lors de l'ouverture des données de trace de transaction enregistrées :

- Vous ne pouvez pas redémarrer la session de suivi de transaction affichée.
- Les liens des composants de trace de transaction vers les chemins des mesures ne sont pas disponibles si les chemins de mesures ne sont pas actifs dans le gestionnaire d'entreprise auquel la station de travail est connectée.

Pour ouvrir les données de trace de transaction enregistrées dans un fichier XML :

1. Sélectionnez Poste de travail > Interroger les événements historiques.
2. Sélectionnez Suivi > Ouvrir les événements enregistrés (XML).
3. Sélectionnez le fichier XML dans la fenêtre du navigateur, puis cliquez sur Ouvrir.
Les données dans le fichier XML s'affichent dans une nouvelle fenêtre Requête historique.

Remarque : Lorsque vous affichez les événements historiques enregistrés dans un fichier XML, les événements corrélés sont affichés, mais ne le sont pas en tant qu'événements corrélés. Pour afficher la corrélation des événements historiques dans une trace de transaction, affichez une trace active (reportez-vous à la section [Interrogations des événements corrélés](#)).

Vous pouvez désormais effectuer les actions suivantes :

- Exporter une trace de transaction dans un fichier texte
- Sélectionner les traces de transaction dans les données et les enregistrer dans un nouveau fichier XML

Exportation d'une trace de transaction dans un fichier texte

Pour exporter des traces de transaction dans un fichier texte :

1. Dans la visionneuse des traces de transaction, sélectionnez les traces de transaction à exporter :
 - CTRL + clic pour sélectionner plusieurs traces de transaction
 - Modifier > Tout sélectionner pour sélectionner toutes les traces de transaction dans la fenêtre.
2. Sélectionnez Suivi > Exporter.
3. Sélectionnez un emplacement dans lequel enregistrer le fichier et nommez le fichier (*nom par défaut : <type_composant_racine>_<nom_composant_racine>.txt*), puis cliquez sur OK.

Exemple de fichier XML de trace de transaction

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TransactionTracerSession EndDate="2005-03-15T17:28:13.953-08:00" Version="0.1" Duration="32"
  StartDate="2005-03-15T17:28:13.921-08:00" User="Admin">
  <TransactionTrace Duration="32" Domain="SuperDomain" EndDate="2005-03-15T17:28:13.953-08:00"
    AgentName="WebLogic Agent" Host="rnadimpalli-dt3" StartDate="2005-03-15T17:28:13.921-08:00"
    Process="WebLogic">
    <CalledComponent MetricPath="Servlets|ActionServlet" ComponentName="ActionServlet" Duration="32"
      ComponentType="Servlets" RelativeTimestamp="0">
      <CalledComponents>
        <CalledComponent MetricPath="JSP|__register" ComponentName="__register" Duration="16"
          ComponentType="JSP" RelativeTimestamp="16">
          <CalledComponents>
            <CalledComponent MetricPath="JSP TagLib|HtmlTag|doStartTag" ComponentName="doStartTag"
              Duration="0" ComponentType="JSP TagLib" RelativeTimestamp="16">
              <Parameters>
                <Parameter Value="doStartTag" Name="Method"/>
              </Parameters>
            </CalledComponent>
            <CalledComponent MetricPath="JSP TagLib|BaseTag|doStartTag" ComponentName="doStartTag"
              Duration="0" ComponentType="JSP TagLib" RelativeTimestamp="16">
              <Parameters>
```

```

        <Parameter Value="doStartTag" Name="Method"/>
    </Parameters>
</CalledComponent>
<CalledComponent MetricPath="JSP TagLib|MessageTag|doStartTag"
ComponentName="doStartTag" Duration="0" ComponentType="JSP TagLib" RelativeTimestamp="16">
    <Parameters>
        <Parameter Value="doStartTag" Name="Method"/>
    </Parameters>
</CalledComponent>
<CalledComponent MetricPath="JSP TagLib|MessageTag|doStartTag"
ComponentName="doStartTag" Duration="0" ComponentType="JSP TagLib" RelativeTimestamp="16">
    <Parameters>
        <Parameter Value="doStartTag" Name="Method"/>
    </Parameters>
</CalledComponent>
</TransactionTrace>
</TransactionTracerSession>

```

Surveillance à l'aide de la station de travail

Les utilisateurs de DX APM savent que DX APM fonctionne de manière optimale non seulement lors de l'analyse des problèmes d'application, mais également pour la surveillance des performances nominales des applications. Lorsque vous connaissez les performances nominales pour votre application, vous êtes alors mieux préparé pour comprendre les signaux liés aux problèmes et erreurs de performances de vos applications.

Cette section couvre les rubriques suivantes :

- [Présentation des performances nominales](#)
- [Lecture et compréhension des notifications](#)
- [Diagnostic de problèmes à l'aide de l'onglet Navigateur de mesures](#)

Diagnostic de problèmes à l'aide de l'onglet Navigateur de mesures

Les outils dans l'onglet de navigateur de mesures vous permettent de rechercher et d'identifier les problèmes à résoudre.

Contenu

L'onglet **Navigateur de mesures** contient les outils suivants qui vous permettent d'obtenir plus d'informations sur un problème :

- Mesures historiques
- Recherche
- Outil de suivi de transaction

Utilisation de mesures dynamiques et historiques

Par défaut, les vues contiennent des mesures dynamiques et les données s'actualisent toutes les 15 secondes. Les données qui ne s'affichent pas dans un graphique dynamique sont enregistrées par le gestionnaire d'entreprise en tant que données historiques. Pour diagnostiquer un problème qui peut être survenu dans les minutes ou les heures précédentes, affichez les données historiques.

Affichage des données historiques dans l'onglet Navigateur de mesures

Pour afficher des données historiques, sélectionnez une période. L'utilisation d'une période peut vous aider à identifier rapidement l'heure à laquelle un problème est survenu. Par exemple, vous pensez que le problème est survenu au cours de la dernière heure. Vous définissez la période sur une heure et regardez les données antérieures à l'heure actuelle. Si vous ne voyez aucun problème dans cette période, vous pouvez utiliser les contrôles pour avancer ou reculer. Déplacez la période jusqu'à ce que vous trouviez l'heure à laquelle le problème est survenu.

Pour afficher les données historiques :

1. Sélectionnez la mesure ou le tableau de bord pour lequel vous souhaitez afficher les données historiques.
2. Sélectionnez une plage de temps pour la vue historique dans le menu déroulant **Période**.
Les données s'affichent pour cette période. La période utilise la durée que vous avez sélectionnée et définit l'heure de fin sur l'heure actuelle.
Remarque : DX APM applique la période que vous sélectionnez pour afficher les données historiques à d'autres mesures et tableaux de bord dans la même fenêtre. Cette période s'applique à toutes les nouvelles fenêtres que vous ouvrez.
3. Pour sélectionner une résolution et ajuster le niveau de détail de la vue, augmentez ou diminuez le nombre de points de données qui s'affichent.
Chaque plage prédéfinie est associée à une résolution par défaut. En général, vous n'avez pas besoin de modifier la résolution. Modifiez la résolution pour obtenir un plus grand niveau de détails ou une granularité des données plus élevée.
4. Vous pouvez ajuster une période après l'avoir sélectionnée. Utilisez les contrôles pour faire défiler les incréments en fonction de la période que vous avez sélectionnée :
 - Faites glisser le curseur sur la barre de temps pour modifier la plage de temps.
 - Cliquez sur les flèches pour avancer ou reculer dans le temps.
Les flèches simples déplacent la période vers l'arrière ou vers l'avant par petits incréments. Les doubles flèches déplacent la période vers l'arrière ou vers l'avant par incréments qui correspondent à la taille de la période sélectionnée.
 - Cliquez sur l'icône **Réinitialiser** pour définir l'heure de fin de la plage sur l'heure actuelle.

Utilisation du zoom sur les données historiques dans des graphiques

Vous pouvez effectuer un zoom avant sur des données historiques affichées dans un graphique.

Pour effectuer un zoom avant sur des données dans un graphique :

- Effectuez l'une des actions suivantes :
 - Cliquez sur une position dans le graphique et faites-la glisser pour spécifier la plage de temps.
 - Cliquez avec le bouton sur le graphique, puis cliquez sur **Zoomer** pour ajuster les données.

Les données s'actualisent dans la visionneuse en fonction de la nouvelle requête et la nouvelle période s'affiche dans la visionneuse.

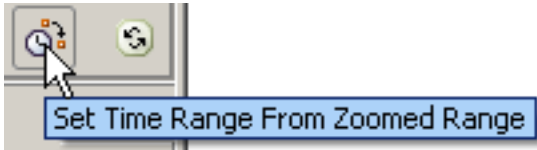
Pour effectuer un zoom arrière :

1. Cliquez avec le bouton droit sur le graphique zoomé.
2. Cliquez sur **Zoom arrière** ou **Zoom arrière extrême**.

La plage de temps globale dans la fenêtre et la commande de plage de temps ne sont pas automatiquement modifiées lorsque vous zoomez sur des données. Par exemple, vous effectuez un zoom avant sur une période de 10 minutes sur un graphique dont la période est définie sur 1 heure. Le graphique affiche la période de 10 minutes, mais le contrôle reste sur 1 heure. La barre temporelle affiche toujours la période de 1 heure.

Pour faire correspondre la plage de temps globale et la commande de plage de temps à la vue zoomée :

- Cliquez sur le bouton **Définir la plage de temps à partir de la plage zoomée** :



Utilisation de la recherche

L'onglet Rechercher (voir section [Onglet Rechercher](#)) est activé pour chaque nœud de l'arborescence du navigateur de mesures. Cet onglet vous permet de rechercher des mesures sous un nœud particulier.

Pour utiliser l'onglet Rechercher :

1. Sélectionnez un nœud dans l'arborescence du navigateur de mesures.
2. Sélectionnez l'onglet Rechercher.

Pour utiliser la recherche de texte brut :

1. Entrez une chaîne dans le volet de recherche.
2. Cliquez sur **OK** ou appuyez sur **Entrée**.
Les résultats de recherche s'affichent sous forme de tableau. Les résultats affichent toutes les ressources dont le nom inclut la chaîne de recherche.

TIP

Sélectionner l'une des mesures répertoriées dans le tableau affiche un graphique présentant une vue en temps réel de la mesure.

Pour afficher les résultats, notamment leurs valeurs min, max et nombre :

- Sélectionnez **Afficher min., max. et nombre**.

TIP

Après avoir lancé la recherche, vous pouvez sélectionner **Afficher min., max. et nombre** et les résultats s'actualisent avec les nouvelles colonnes.

Utilisation des expressions régulières

Le volet Rechercher accepte toute expression régulière en langage Perl 5.

TIP

Le langage Perl 5 permet également de définir des groupements de mesures.

Pour utiliser des expressions régulières dans la recherche :

1. Sélectionnez **Utiliser une expression régulière**.
2. Entrez une expression régulière dans le volet Rechercher.
3. Cliquez sur **OK** ou appuyez sur **Entrée**.
L'onglet **Rechercher** affiche les résultats.

Utilisation de la trace de transaction

L'outil de suivi de transaction est un outil puissant permettant de suivre l'activité des transactions à mesure qu'elles passent par une application. Vous exécutez des traces de transactions pour surveiller les transactions qui se produisent dans une machine virtuelle Java (JVM) dans un environnement Java ou dans un environnement CLR (Common Language Runtime) dans un environnement .NET.

Reportez-vous à la section [Utilisation de l'outil de suivi de transaction](#).

Lecture et compréhension des notifications

Notifications d'alertes dans les tableaux de bord

La forme la plus évidente est une notification visuelle dans un tableau de bord de console. L'illustration ci-dessous représente un tableau de bord comprenant un graphique unique qui a été configuré avec une ligne jaune indiquant un seuil d'avertissement de 3 000 ms et un seuil de risque de 4 000 ms.

Le graphique indique :

- Le temps de réponse moyen a dépassé le seuil d'avertissement plusieurs fois au cours des dernières minutes.
- Le temps de réponse moyen a dépassé le seuil de risque une fois, il y a deux minutes environ.
- En fonction de la mesure la plus récente, les performances de l'application sont dans l'état Avertissement.

Les indicateurs sous le graphique constituent une autre manière d'indiquer le statut d'alerte. La façon dont vos tableaux de bord s'affichent dépend de la manière dont vous ou votre administrateur les avez configurés.

Lorsque vous voyez un tableau de bord indiquant une condition Avertissement ou Danger, l'indicateur d'alerte cumule généralement des mesures de plusieurs sources. La tâche doit consister à déterminer quelles mesures sous-jacentes sont à l'origine de la condition.

Pour modifier une vue d'alerte :

- Affichez une alerte dans le volet Aperçu d'Investigator et sélectionnez Propriétés > Vue Alerte.

Messages d'alerte

Les messages d'alerte sont déclenchés par une action qui est associée à un statut d'alerte. Ces alertes s'affichent automatiquement. Vous pouvez également afficher des messages d'alerte en sélectionnant Station de travail > Afficher les messages d'alerte.

Présentation des performances nominales

Savoir à quoi ressemblent les performances standard des applications vous permet de vous familiariser avec le système, ainsi qu'avec les outils et les utilitaires DX APM. Ces connaissances vous permettent d'élargir le contexte afin de mieux comprendre les problèmes inévitables. Lorsqu'un problème survient, vous possédez les connaissances nécessaires pour l'identifier.

Trois différents noeuds de l'arborescence du navigateur de mesures sont particulièrement utiles pour surveiller les performances des applications. Ces noeuds, **GC Heap**, **Frontends** et **Backends**, peuvent être considérés comme les signes vitaux de votre application.

Surveillance des performances avec les mesures GC Heap

Le nettoyage de mémoire, abrégé GC pour Garbage Collection, est le processus de libération de mémoire réservée par les objets qui ne sont plus en cours d'utilisation. Une fois que la mémoire est libérée, elle est utilisable par d'autres objets. Les mesures **GC Heap** (Segment de mémoire GC) fournissent un excellent outil pour la surveillance et la compréhension des performances des applications.

GC Heap|Bytes In Use

Les mesures GC Heap|Bytes In Use (Segment de mémoire GC|Octets utilisés) spécifient la quantité de mémoire actuellement utilisée par les objets.

GC Heap|Bytes Total

Les mesures GC Heap|Bytes Total (Segment de mémoire GC|Nombre total d'octets) indiquent la quantité totale de mémoire que la machine virtuelle Java alloue.

Allouer une quantité de mémoire trop faible ou trop élevée à la machine virtuelle Java peut entraîner des problèmes de performances. Pour résumer, vous pouvez appliquer les recommandations suivantes :

- Lorsque vous allouez une mémoire insuffisante, le processus GC s'exécute plus fréquemment, donnant lieu à des problèmes de dégradation des performances courts, mais fréquents.
- Lorsque vous allouez trop de mémoire, l'exécution du processus GC prend relativement longtemps et entraîne une dégradation des performances sur cette période.

Vous pouvez utiliser ces mesures pour déterminer la taille appropriée du segment de mémoire.

Une fois que vous avez déterminé la taille appropriée, vous pouvez surveiller les mesures GC Head dans le temps afin de comprendre à quoi ressemblent les performances nominales. La mesure **Bytes In Use** (Octets utilisés) doit afficher des augmentations et réductions périodiques. Dans le temps, les mesures montrent des résultats répétés, mais aucune trace de fuite de mémoire.

Surveillance des performances à l'aide des mesures GC Monitor

GC Monitor fournit un ensemble de mesures sur le fonctionnement interne de la machine virtuelle Java, y compris l'allocation de mémoire et les taux de croissance de segment de mémoire. GC Monitor permet d'allouer le segment de mémoire JVM en vérifiant que tous les utilitaires de nettoyage de mémoire et les pools de mémoire sont alloués correctement. De cette façon, vous pouvez détecter les problèmes de nettoyage de mémoire qui affectent les performances.

Machines virtuelles Java prises en charge

GC Monitor prend en charge uniquement les machines virtuelles Java suivantes :

- Machine virtuelle Java Sun, version 1.5.0 ou supérieure, 32 et 64 bits
- IBM, version 1.5.0 ou supérieure, 32 et 64 bits

Pour utiliser les mesures GC Monitor afin d'ajuster l'allocation de mémoire :

1. Dans l'arborescence Navigateur de mesures, accédez au noeud de l'agent sur l'hôte dont vous souhaitez surveiller l'activité de nettoyage de mémoire. Développez le noeud **GC Monitor**.
2. Surveillez l'utilisation des mesures et le pool de mémoire de chaque utilitaire de nettoyage de mémoire.
3. Selon les mesures, réallouez la taille du pool de mémoire pour améliorer l'efficacité du nettoyage de mémoire.

Si vous avez besoin de directives pour vous aider à réallouer la taille du pool de mémoire, consultez la documentation appropriée de votre machine virtuelle Java.

Surveillance des performances à l'aide des mesures de composants frontaux

Vous pouvez utiliser le noeud **Frontends** de deux façons pour surveiller les performances générales des applications : surveiller les mesures standards et noter les URL principales.

Surveillance des mesures de composants frontaux standard

DX APM affiche les [cinq mesures BlamePoint de base](#) pour chaque composant frontal. Consultez ces mesures dans l'arborescence du navigateur de mesures, sous `Frontends|Applications|<nom_composant_frontal>`.

Performances optimales

Une application fonctionne bien lorsqu'un volume élevé de demandes traitées (**réponses par intervalle**) correspond à une latence faible (un **temps de réponse moyen** faible). Une performance optimale est d'environ une seconde par transaction.

Performances problématiques

Les méthodes simultanées sont des méthodes qui ont démarré au cours d'un intervalle, mais ne se sont pas finalisées pendant cet intervalle. Vous souhaitez que les méthodes se terminent rapidement, c'est pourquoi il n'est pas souhaitable

d'obtenir un nombre anormalement élevé d'appels simultanés. Vous pouvez constater des pics temporaires dans les appels simultanés, mais la mesure doit renvoyer zéro dans chaque cas. La mesure qui renvoie une valeur différente de zéro peut indiquer un goulot d'étranglement des threads, un nombre de connexions à la base de données ou une autre ressource partagée.

Reconnaissance des transactions les moins performantes

Un bon moyen pour surveiller les performances consiste à déterminer quelles sont les transactions qui sont constamment lentes. Vous pouvez configurer une visionneuse de données pour afficher les transactions les plus lentes dans un graphique à barres.

Un des meilleurs moyens d'afficher les transactions les plus lentes consiste à configurer les groupes d'URL comme base pour le regroupement des mesures.

Surveillance des performances à l'aide des mesures de serveurs d'arrière-plan

Le noeud **Backends** de l'arborescence du navigateur de mesures affiche les cinq mesures standard pour chaque système d'arrière-plan connecté.

Deux mesures différentes sous le noeud **Backends** permettent de reconnaître les performances nominales.

Fréquence de traitement des instructions SQL

Savoir quelles instructions SQL sont le plus traitées est un bon moyen pour vous familiariser avec les performances des applications.

Pour examiner la fréquence de traitement des instructions SQL comme mesure des performances :

1. Sous le noeud **Backends**, ouvrez le noeud de l'application à surveiller.
2. Sous l'application, ouvrez le noeud de l'application à surveiller.
L'onglet **Présentation** affiche une liste des requêtes et des autres instructions SQL en cours d'exécution sur la ressource de base de données.
3. Dans la section **Requêtes** du volet droit, cliquez sur l'en-tête de colonne **Réponses** pour trier le tableau par nombre de réponses.
4. Notez les requêtes SQL les plus envoyées.

Modèles de connexion de base de données

Déterminez quels sont les modèles de connexion de base de données d'application et soyez informé lorsqu'un modèle est rompu.

La façon dont votre application établit et gère les connexions de base de données dépend de la plate-forme.

Utilisation de la station de travail

La console de la station de travail affiche des informations sur les mesures dans les tableaux de bord. Les tableaux de bord sont des fenêtres préconfigurées qui présentent des vues graphiques des mesures de performances et de disponibilité actuelles ou historiques.

Lorsque vous ouvrez la console, celle-ci affiche les données de performances et de disponibilité en temps réel. Vous pouvez afficher les données historiques en sélectionnant une période.

Navigation entre les tableaux de bord de la console

Contenu

Vous pouvez sélectionner des tableaux de bord de Console de différentes manières :

- Liste déroulante de tableaux de bord
- Boutons Suivant et Précédent
- Liste des historiques
- Bouton Accueil
- Liens hypertextes

Liste déroulante de tableaux de bord

Vous pouvez sélectionner des tableaux de bord dans la liste déroulante en haut de la page Console. Vous pouvez entrer tout ou partie du nom du tableau de bord, afin de limiter les sélections dans la liste.

Une fois que vous avez affiché plusieurs tableaux de bord, vous pouvez naviguer entre eux :

- A l'aide des flèches avant et arrière
- A l'aide de la liste déroulante en regard des flèches avant et arrière
- Si vous avez défini un tableau de bord d'accueil dans vos préférences d'utilisateur, vous pouvez l'ouvrir en cliquant sur Accueil.

Navigation à l'aide de liens hypertextes

Vous pouvez utiliser des liens hypertextes pour naviguer entre les tableaux de bord Introscope et Investigator :

- Liens hypertextes automatiques : Introscope associe automatiquement une visionneuse de données au groupement de mesures sur lequel elle est basée. Le menu Liens de la visionneuse contient un lien vers la définition du groupement de mesures sous-jacent dans l'éditeur de module de gestion. De même, les tableaux de bord contenant des visionneuses de données basée sur le même groupement de mesures sont automatiquement liés, et vous pouvez naviguer entre eux à l'aide du menu liens.
- Liens hypertextes personnalisés : vous pouvez définir des liens personnalisés pour les éléments du tableau de bord, pour les associer à d'autres tableaux de bord et pages Web. Vous pouvez définir des liens personnalisés si vous disposez des droits de modification du tableau de bord.

Remarque : Certains tableaux de bord de la console prêts à l'emploi, par exemple, Capacité EM, ne contiennent pas automatiquement de liens vers les données sous-jacentes. Modifiez ces tableaux de bord par défaut ou créez des tableaux de bord avec des liens.

Pour afficher une liste des liens de tableau de bord disponibles :

1. Cliquez avec le bouton droit de la souris sur un objet de tableau de bord.
2. Sélectionnez Propriétés > liens.

Si aucun lien n'est disponible pour un objet, le menu Liens est désactivé.

Pour suivre les liens du tableau de bord :

1. Passez la souris sur un objet de tableau de bord qui comporte un lien hypertexte.
Le pointeur prend la forme d'une main.
2. Double-cliquez sur l'objet pour suivre le lien vers la cible par défaut.

Création de favoris de tableau de bord

Pour simplifier l'accès aux tableaux de bord que vous utilisez souvent, vous pouvez les ajouter au menu Favoris de la console.

Pour ajouter un tableau de bord à vos favoris :

1. Accédez au tableau de bord.
2. Sélectionnez Favoris > Ajouter aux favoris.

Remarque : Les liens favoris ne sont pas conservés lorsque vous renommez ou supprimez un tableau de bord favori. Mettez le lien à jour ou supprimez l'ancien lien, puis créez-en un autre.

Pour supprimer un tableau de bord des favoris :

1. Dans la console, sélectionnez Favoris > Organiser les favoris.
2. Sélectionnez un tableau de bord.
3. Sélectionnez Supprimer.

Pour modifier la liste des favoris :

1. Dans la console, sélectionnez Favoris > Organiser les favoris.
2. Sélectionnez un tableau de bord.
3. Sélectionnez Modifier.

Lancement d'Investigator à partir de la console

Si vous visualisez les données en temps réel dans la console, puis lancez l'Investigator de la station de travail à partir de cette console, vous pouvez également afficher les données dynamiques dans Investigator. Toutefois, dans Investigator, la valeur par défaut pour la période est de 8 minutes et la résolution est de 15 secondes. Vous n'avez pas la possibilité d'entrer une période et une résolution personnalisées pour le mode dynamique dans Investigator.

Si vous visualisez les données historiques dans la console, puis lancer l'Investigator de station de travail à partir de la console, vous pouvez également afficher les données historiques dans Investigator pour la même période et résolution que vous avez sélectionnées pour les données historiques dans la console.

Lancement de la console à partir d'Investigator

Si vous visualisez les données dynamiques dans Investigator et lancez la console de la station de travail à partir d'Investigator, vous pouvez également afficher les données dynamiques dans la console. Toutefois, dans la console, la valeur par défaut pour la période est de 8 minutes et la résolution est de 15 secondes. Vous pouvez entrer une période et une résolution personnalisées pour le mode dynamique dans la console.

Si vous visualisez les données historiques dans Investigator, puis lancer la console de la station de travail à partir d'Investigator, vous pouvez également afficher les données historiques dans la console pour la même période et résolution que vous avez sélectionnées pour les données historiques dans Investigator.

Autres informations dans les tableaux de bord

Lorsque vous souhaitez en savoir plus sur les données présentées dans les tableaux de bord, vous pouvez utiliser des raccourcis pour obtenir plus d'informations.

Procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur un graphique ou une alerte, sélectionnez liens, puis accédez à l'alerte correspondante dans le module de gestion ou un autre tableau de bord associé au graphique ou à l'alerte.
2. Double-cliquez sur une mesure à partir du graphique affichant les N principales données de mesure (par exemple, les 10 ou 25 principales les plus lentes) pour afficher ses détails dans Investigator.

Filtrage par agent à l'aide de la loupe de la console

Vous utilisez la loupe de la console pour filtrer les données de mesure pour les agents qui renvoient des données. Dans un tableau de bord qui affiche des données pour plusieurs agents, vous pouvez utiliser la loupe de la console pour afficher uniquement les données des agents sélectionnés.

Lorsque vous appliquez la loupe de la console, le filtre est appliqué jusqu'à la fermeture de la fenêtre Console, la déconnexion de la station de travail ou l'utilisation de la commande Effacer les loupes.

Application de la loupe de la console

Pour appliquer la loupe de la console :

1. Cliquez sur la loupe (ou sélectionnez Tableau de bord, Loupe).
Si la console est en mode dynamique, la boîte de dialogue répertorie les agents actuellement connectés. Si vous affichez une période de données historiques, la boîte de dialogue répertorie les agents connectés pour la plage historique sélectionnée.
2. Dans la boîte de dialogue Sélectionner des agents, sélectionnez un agent unique ou plusieurs agents (sélectionnez-les et faites-les glisser, utilisez CTRL + clic) sur lesquels appliquer le filtre.
Remarque : Vous pouvez commencer à saisir un nom d'agent, un nom d'hôte ou un nom de processus dans le champ Rechercher. Lorsque vous saisissez un nom, la liste des agents est filtrée pour correspondre à ce que vous saisissez.
3. Sélectionnez Appliquer ou appuyez sur Entrée.
Le tableau de bord s'actualise pour afficher uniquement les données pour le ou les agents sélectionnés. La flèche située sur la loupe passe du bleu clair au noir lorsque celle-ci est appliquée.

Widgets non pris en charge

Certains widgets de tableau de bord ne prennent pas en charge la fonctionnalité de loupe :

- Graphiques basés sur les outils de calcul
- Les graphiques dépendant d'un agent virtuel sont basés sur une alerte simple. Cela inclut le graphique Top 10 Connected Agents (10 premiers agents connectés) du tableau de bord Présentation.

Remarque : Lorsque vous modifiez un tableau de bord pour ajouter une nouvelle alerte simple et qu'une loupe est appliquée au tableau de bord, un certain temps peut s'écouler avant que la nouvelle alerte affiche les données de statut.

Effacement de la loupe de la console

Pour effacer la loupe de la console :

1. Sélectionnez Loupe.
2. Désactivez la loupe en cliquant sur Effacer dans la boîte de dialogue Appliquer la loupe de la console.

Loupe de la console et vues d'onglet dans les tableaux de bord

L'effet d'une loupe de console sur une vue Investigator dans un tableau de bord dépend du type d'élément d'arborescence auquel est associé la vue.

Si l'élément Investigator associé à la vue est :	et...	alors
un domaine	un agent unique est sélectionné dans la loupe...	... l'association d'éléments est définie sur une sélection d'agent unique. Si la vue ne prend pas en charge la sélection d'agent, un message d'erreur s'affiche.
un agent	un agent unique est sélectionné dans la loupe...	... l'association d'éléments est définie sur une sélection d'agent unique.
une mesure	un agent unique est sélectionné dans la loupe...	... la même mesure sur l'agent sélectionné devient la sélection actuelle. Si cette mesure n'existe pas, un message d'erreur s'affiche.
un chemin de mesure	un agent unique est sélectionné dans la loupe...	...le même chemin de mesure sur l'agent sélectionné devient la sélection actuelle. Si le chemin n'existe pas, un message d'erreur s'affiche.

un autre type d'élément		un message d'erreur s'affiche.
-------------------------	--	--------------------------------

Si plusieurs agents sont sélectionnés, un message d'erreur s'affiche.

Si l'agent auquel la loupe est appliquée est un agent virtuel, la vue affiche les données pour cet agent, s'il prend en charge ce type de sélection. Vous pouvez déterminer quelles vues sont prises en charge pour un type d'élément spécifique en sélectionnant un élément dans l'arborescence et en observant les onglets des vues disponibles.

Un agent virtuel est un groupe d'agents physiques configurés pour être un agent unique, ce qui permet d'obtenir une vue cumulée des mesures renvoyées par ceux-ci.

Manipulation du contenu des visionneuses de données

Les visionneuses de données dans le volet de visionneuse d'Investigator ou dans un tableau de bord, affichent les données d'une application gérée sous forme visuelle. Les données s'affichent dans une visionneuse de données en fonction du type de données : par exemple, les mesures s'affichent sous forme de graphiques et les alertes sous forme d'indicateurs de couleur. Les visionneuses de données peuvent afficher les données d'une mesure, d'une ressource ou d'un élément, par exemple, une alerte.

Dans les visionneuses de données, vous pouvez :

- Afficher les valeurs des mesures minimum/maximum dans un graphique
- Afficher ou masquer les données de mesure dans un graphique
- Modifier l'échelle des graphiques
- Déplacer les mesures à l'avant ou à l'arrière des graphiques
- Exporter les données

Affichage des valeurs de mesures minimum/maximum dans un graphique

Vous pouvez configurer un graphique pour afficher les valeurs minimum et maximum.

Pour afficher les valeurs minimum et maximum des mesures et des groupements de mesures dans un graphique :

1. Sélectionnez un graphique dans la console.
2. Vous affichez les valeurs minimum et maximum de deux façons :
 - Cliquez avec le bouton droit de la souris sur la visionneuse de données et sélectionnez Afficher minimum et maximum.
 - Sélectionnez le menu Propriétés, puis Afficher minimum et maximum.

Remarque : Cette modification s'applique uniquement lorsque vous affichez le tableau de bord actuel. Si vous ouvrez une console ou basculez vers un autre tableau de bord, ce paramètre rétablit les valeurs par défaut et n'affiche plus les valeurs de mesures minimum et maximum. Pour afficher les valeurs de mesures minimum et maximum par défaut dans un graphique, activez cette option lorsque vous modifiez un tableau de bord avec l'éditeur de tableau de bord.

Affichage/masquage des données de mesures dans un diagramme

Si vous visualisez les données de plusieurs mesures dans un graphique, vous pouvez afficher ou masquer des données de mesure particulières.

Pour afficher ou masquer une mesure dans un graphique :

1. Affichez un graphique dans le tableau de bord de la console.
2. Vous pouvez effectuer les opérations suivantes :
 - Afficher la mesure en sélectionnant la case correspondante.
 - Masquer la mesure en désélectionnant la case correspondante.

Remarque : Les options d'affichage et de masquage de mesures ne sont pas disponibles lorsque les graphiques ou les graphiques à barres affichent des données triées ou filtrées.

Modification de l'échelle des graphiques

Vous pouvez modifier l'échelle des graphiques lors de l'affichage des données dynamiques dans la station de travail, afin de fournir une vue plus lisible. Vous modifiez l'échelle d'un graphique en définissant une valeur minimum et maximum pour l'axe des données du graphique.

La fonctionnalité de mise à l'échelle de graphique est disponible uniquement pour les graphiques en mode dynamique. Elle n'est pas disponible pour tout autre type de visionneuse, tel qu'un graphique à barres, un graphique des dix principaux éléments ou une visionneuse de chaîne.

Remarque : Les modifications de l'échelle d'un graphique sont temporaires. Les paramètres ne sont pas enregistrés avec le tableau de bord. Lorsque vous sélectionnez un tableau de bord ou fermez la fenêtre Console, Introscope ignore les paramètres et rétablit les options d'échelle appliquées lors de la création du tableau de bord.

Pour afficher l'échelle d'un graphique :

- Cliquez sur un graphique pour le sélectionner, puis :
- Sélectionnez Visionneuse > Options de mise à l'échelle.
- Vous pouvez également cliquer sur le graphique et sélectionnez Options de mise à l'échelle dans le menu contextuel. La boîte de dialogue Options des données s'ouvre.

Définir les valeurs par défaut de mise à l'échelle automatique minimum et maximum fournit une vue plus lisible des graphiques mode dynamique.

Pour effectuer une mise à l'échelle en utilisant les valeurs minimum et maximum :

1. Cliquez sur un graphique pour le sélectionner, puis :
 - Sélectionnez Visionneuse > Options de mise à l'échelle.
 - Vous pouvez également cliquer sur le graphique et sélectionnez Options de mise à l'échelle dans le menu contextuel.
2. Entrez les valeurs minimum et maximum pour l'axe des données du graphique.
3. Sélectionnez OK.
Par exemple, si les valeurs de données de graphique se trouvent principalement entre 350 et 550, mais que l'axe du graphique affiche 0 - 1 000, il peut s'avérer utile de définir la valeur de mise à l'échelle minimum sur 300 et celle maximum sur 600 pour une vue optimisée des données pertinentes.

Pour forcer les valeurs minimum et maximum :

1. Cliquez sur un graphique pour le sélectionner.
2. Sélectionnez Visionneuse > Options de mise à l'échelle.
3. Sélectionnez Epingler à sur les côtés Minimum et Maximum de la boîte de dialogue, puis entrez une valeur pour les points minimum et maximum de l'accès aux données.
4. Sélectionnez OK.

Définir des valeurs minimum et maximum pour un graphique affichant des données dynamiques est toutefois risqué, s'il existe une chance que les données dépassent les valeurs que vous définissez.

Pour éviter ce problème, utilisez l'option Echelle automatique pour définir la mise à l'échelle automatique du graphique en fonction des données affichées.

Pour effectuer une mise à l'échelle à l'aide de l'option Echelle automatique :

1. Cliquez sur un graphique pour le sélectionner.
2. Sélectionnez Visionneuse > Options de mise à l'échelle.
3. Sélectionnez Echelle automatique sur les côtés Minimum et Maximum de la boîte de dialogue.
4. Sélectionnez OK.

L'axe de données obtenu est réinitialisé en fonction des données du graphique. Cela entraîne souvent des creux et des pics dans le graphique.

Vous pouvez également définir les options de mise à l'échelle sur Développement automatique. Cette option utilise 0 en bas de l'axe de données, et développe et met à l'échelle automatiquement l'axe des données pour afficher toutes les données de la période.

Pour effectuer un développement automatique :

1. Cliquez sur un graphique pour le sélectionner.
2. Sélectionnez Visionneuse > Options de mise à l'échelle.
3. Sélectionnez Développement automatique sur les côtés Minimum et Maximum de la boîte de dialogue.
4. Sélectionnez OK.

Déplacement des mesures à l'avant ou à l'arrière dans un graphique

Lorsqu'un graphique contient plusieurs mesures, il est possible que certains points de données se superposent. Vous pouvez utiliser les options Ramener au premier plan ou Envoyer à l'arrière-plan pour choisir les mesures qui s'affichent dans la partie supérieure de la liste des mesures.

Remarque : Les options Ramener au premier plan ou Envoyer à l'arrière-plan ne sont pas disponibles lorsque vous affichez des graphiques contenant des données triées ou filtrées.

Pour modifier l'ordre de chevauchement des mesures dans un graphique :

1. Ouvrez la console et affichez un graphique dans un tableau de bord.
2. Cliquez avec le bouton droit de la souris sur l'étiquette de la mesure pour la modifier, puis choisissez une option dans le menu :
 - Ramener au premier plan (déplace la mesure sélectionnée vers la partie supérieure de la liste des mesures)
 - Envoyer à l'arrière-plan (déplace la mesure sélectionnée vers la partie inférieure de la liste des mesures)
 La mesure est déplacée vers l'emplacement choisi.

Copie d'une visionneuse de données dans le Presse-papiers

Vous pouvez copier un cliché des données d'une visionneuse de données vers le Presse-papiers sous forme d'image bitmap. Vous pouvez ensuite coller l'image dans un courriel, un autre document ou une application qui prend en charge les images bitmap. Cette fonctionnalité est pratique si, par exemple, vous souhaitez montrer les données d'une visionneuse de données à un collègue ou les utiliser dans une présentation.

Pour copier une visionneuse de données dans le Presse-papiers :

1. Ouvrez une console et sélectionnez une visionneuse de données.
2. Sélectionnez Visionneuse > Copier dans le Presse-papiers en tant qu'image.

Remarque : Vous ne pouvez pas copier plusieurs visionneuses de données.

Exportation des données des visionneuses de données

Vous pouvez prendre un cliché des données actuelles dans une visionneuse de données et les exporter vers un fichier CSV. Vous pouvez exporter les données de tous les types de visionneuse de données à l'exception de celle d'alerte.

Pour exporter les données d'une visionneuse de données :

1. Dans la console, sélectionnez une visionneuse de données.
2. Sélectionnez Visionneuse > Exporter les données.
3. Dans la boîte de dialogue Enregistrer, sélectionnez un emplacement dans lequel enregistrer le fichier .csv, cliquez sur Enregistrer.

Données dynamiques et historiques dans la console de la station de travail

Vous pouvez afficher des données dynamiques dans la console ou sélectionner une période pour afficher des données historiques. Par défaut, la vue dynamique des données s'affiche.

Pour vérifier si le mode dynamique est activé dans la station de travail, utilisez la liste déroulante Période.

Affichage des données de requête dynamiques dans la console de la station de travail

Procédez comme suit :

- Cliquez sur Dynamique pour activer ce mode et afficher les données actives.

La valeur par défaut de la plage de temps est de 8 minutes et la résolution est de 15 secondes. Vous ne pouvez pas définir une plage de temps et une résolution personnalisées lorsque la console est en mode dynamique.

Remarque : Cliquez sur Dynamique pour désactiver ce mode et sélectionnez une plage de temps et une résolution dans la liste déroulante pour afficher des données historiques. Vous pouvez également entrer une plage de temps personnalisée.

Pour afficher les données de requête dynamiques et historiques dans la console de la station de travail :

- Pour afficher les données de requête dynamiques d'une plage supérieure à 8 minutes, modifiez la propriété `introscope.enterprisemanager.workstation.extendedLiveQuery` dans le fichier `IntroscopeEnterpriseManager.properties` du répertoire `<répertoire_base_EM>\config` comme suit :

`introscope.enterprisemanager.workstation.extendedLiveQuery=true`

Lorsque cette propriété est définie sur `true`, vous pouvez utiliser les listes déroulantes Période et Résolution dans le tableau de bord de la station de travail en mode dynamique. Ces options vous permettent d'entrer une plage de temps et une résolution personnalisées pour le mode dynamique au lieu d'utiliser la plage de temps de 8 minutes et la résolution de 15 secondes par défaut.

Vous pouvez définir la plage de temps sur une période supérieure à 8 minutes (par défaut).

Remarque : La période maximum pour laquelle vous pouvez afficher des données dynamiques est de 30 jours. Si vous entrez une période supérieure à 30 jours, elle sera réinitialisée sur 8 minutes par défaut. Le nombre de points de données affichés dans le tableau de bord correspond au calcul Période/Résolution. Si le résultat de Période/Résolution est inférieur à 2, la résolution est définie sur 15 secondes par défaut.

WARNING

Définir une période supérieure à 8 minutes peut affecter les performances du gestionnaire d'entreprise en raison des opérations E/S sur le disque requises pour extraire les données à partir de SmartStor.

Activation et désactivation du mode dynamique

Dans la console de la station de travail, le mode dynamique est activé par défaut. Vous pouvez activer ou désactiver le mode dynamique en cliquant sur le bouton Dynamique.

Remarque : Lorsque la console est en mode dynamique et que la résolution est de 15 secondes, la résolution indiquée dans la console (barre d'outils) est utilisée pour afficher les données dynamiques. Lorsque la console est en mode dynamique et que la résolution est supérieure à 15 secondes, la résolution du widget est utilisée pour afficher les données dynamiques.

Affichage des données historiques

Pour afficher des données historiques, sélectionnez une période. Lorsque vous sélectionnez une période, Introscope affiche immédiatement les données de celle-ci, définit l'heure de fin sur l'heure actuelle et calcule la durée en fonction de votre sélection de période.

Pour passer des données dynamiques aux données historiques :

- Cliquez sur le bouton Dynamique.

Lorsque le mode dynamique est désactivé, vous pouvez effectuer les actions suivantes :

- Sélectionner une période et une résolution dans les listes déroulantes
- Entrer une période personnalisée
- Afficher des données historiques

Les commandes de plage de temps peuvent vous permettre d'identifier l'heure à laquelle un problème est survenu. Par exemple, si vous pensez que le problème est survenu au cours de la dernière heure, vous pouvez définir la plage de temps sur une heure spécifique et examiner les données de l'heure antérieure. Si le problème survenu n'apparaît dans cette plage de temps, utilisez les commandes pour avancer ou remonter dans le temps et recherchez l'heure du problème.

Pour afficher les données historiques :

1. Sélectionnez la mesure ou le tableau de bord pour lequel vous souhaitez afficher les données historiques.
2. Sélectionnez une plage de temps pour la vue historique dans la liste déroulante Période.
IntroScope utilise la durée sélectionnée dans la liste déroulante Période et définit l'heure de fin sur l'heure actuelle pour afficher les données de cette plage.
Remarque : Si votre période historique inclut une année, quatre chiffres sont requis.
Par exemple, si votre période commence à 04:06:45 et que sa durée est de 8 minutes, l'heure de fin de la plage sera définie sur 04:06:45 et l'heure de début sur 03:59:30.
Remarque : Lorsque vous utilisez le contrôle de la plage de temps pour afficher des données historiques, la plage que vous sélectionnez est appliquée à d'autres mesures ou tableaux de bord affichés dans la même fenêtre et toutes celles que vous ouvrez.
3. Pour sélectionner une résolution et ajuster le niveau de détail de la vue, augmentez ou diminuez le nombre de points de données qui s'affichent.
Chaque plage prédéfinie est associée à une résolution par défaut. En règle générale, il n'est pas nécessaire de modifier ce paramètre. Modifier la résolution est utile lorsque vous devez obtenir un niveau supérieur de détail ou de précision des données qui s'affichent par défaut.
Vous pouvez alors effectuer les actions suivantes :
 - Sélectionner une plage prédéfinie dans la liste déroulante, ou
 - Entrer une valeur dans le champ Résolution. Saisissez des valeurs numériques, suivies de la durée (secondes, minutes, heures ou jours). Exemple : 90 secondes.
4. Après avoir sélectionné une période, vous pouvez la modifier à l'aide des commandes de plage.

Les alertes en mode historique ne reflètent pas l'état de l'alerte historique.

Les valeurs d'alerte ne sont capturées dans aucune base de données ; par conséquent, si un tableau de bord en mode historique contient des alertes, elles ne reflètent *pas* l'état historique. Si des données d'alertes sont actuellement signalées, les alertes correspondent aux valeurs dynamiques, non historiques.

Commandes de période

Vous pouvez utiliser des commandes de plage de temps pour effectuer un défilement des valeurs par incréments qui reposent sur la période sélectionnée.

Curseur

Faites glisser le curseur sur la barre de temps pour modifier la plage de temps.

Flèches



Cliquez sur les flèches pour avancer ou reculer dans le temps.

Les flèches simples avancent ou remontent par petits incréments ; les flèches doubles avancent ou remontent par incréments temporels relatifs à l'heure de la plage de temps sélectionnée.

Icône Réinitialiser



Cliquez sur l'icône Réinitialiser pour définir l'heure de fin de la plage sur l'heure actuelle.

Icône Verrouiller



Cliquer sur l'icône Verrouiller pour conserver la résolution sélectionnée lors de la définition de différentes plages en effectuant un zoom sur les données.

Définition d'une plage de temps personnalisée

Pour définir une plage de temps personnalisée pour afficher des données historiques :

1. Sélectionnez la mesure ou le tableau de bord pour lequel vous souhaitez afficher les données historiques.
2. Sélectionnez Plage personnalisée dans la liste déroulante Période.
La fenêtre Plage personnalisée apparaît et indique la date actuelle (jour en cours) entourée d'un contour.
3. Sélectionnez des dates :
 - a. Utilisez les commandes de calendrier pour sélectionner les dates et heures de début et de fin.
 - b. Utilisez les commandes de menu en haut du calendrier pour sélectionner le mois, l'année et la date dans le calendrier et saisissez l'heure dans le champ Heure au bas du calendrier.
 - c. Cliquez sur OK.
 La station de travail affiche les données de la plage personnalisée.

Zoom sur les données historiques dans des graphiques

Lorsque vous affichez des données historiques dans un graphique, vous pouvez effectuer un zoom avant sur les données en cliquant sur une position dans le graphique et en la faisant glisser pour spécifier la plage.

Introscope actualise les données dans la visionneuse en fonction de la nouvelle requête ; la nouvelle plage de temps s'affiche alors dans la visionneuse.

La plage de temps globale dans la fenêtre et la commande de plage de temps ne sont pas automatiquement modifiées lorsque vous zoomez sur des données. Par exemple, si vous effectuez un zoom avant sur une période de 10 minutes dans un graphique dont la plage de temps est définie sur 1 heure, le graphique affiche la période de 10 minutes, mais la commande reste définie sur 1 heure et la barre affiche toujours la plage de temps.

Pour modifier les actions de zoom par défaut, procédez de l'une des manières suivantes :

- Faites correspondre la plage de temps globale et la commande de plage de temps à la vue zoomée : sélectionnez Visionneuse > Définir la plage de temps à partir de la plage zoomée, ou cliquez sur l'icône Définir la plage de temps à partir de la plage zoomée.
- Verrouillez la résolution sélectionnée en cliquant sur l'icône Verrouiller.
- Lorsque vous effectuez un zoom, maintenez la touche Maj enfoncée pour limiter le zoom à l'axe de temps.

Mesures DX APM

DX APM affiche les données de performances applicatives collectées auprès des systèmes locaux et distants sous la forme de mesures.

Fourniture des mesures par DX APM

DX APM surveille les performances applicatives de différentes méthodes au fur et à mesure que divers composants d'application les exécutent.

1. Les sondes qui sont insérées dans le bytecode des composants d'application transmettent des données aux agents.
2. Les agents communiquent les données au gestionnaire d'entreprise. D'autres sous-systèmes, tels que JMX et PMI, transmettent également les données collectées par les agents.
3. Le gestionnaire d'entreprise compile ces données dans des mesures qui représentent les performances des applications telles que mesurées en de nombreux points des sous-systèmes applicatifs.

NOTE

Le gestionnaire d'entreprise enregistre les heures de performance des événements système dans un fichier journal des performances, à savoir <répertoire_base_EM>/logs/perflog.txt. Alternative aux mesures présentées dans Investigator, le fichier perflog.txt peut contenir des informations utiles.

4. Les mesures s'affichent dans l'interface utilisateur.
5. Vous pouvez exporter les mesures vers une base de données externe.

Terminologie courante

Pour comprendre les mesures, découvrez comment DX APM utilise certains termes courants.

Pour d'autres termes, reportez-vous au [Glossaire DX APM](#).

composant d'arrière-plan

Un composant d'arrière-plan est un système externe, tel qu'une base de données, un serveur de messagerie, un système de traitement des transactions (par exemple, CICS ou Tuxedo) ou un système de messagerie (par exemple, WebSphere MQ).

accès concurrentiel et appels simultanés

Les méthodes simultanées sont des méthodes qui ont démarré au cours d'un intervalle, mais ne se sont pas finalisées pendant cet intervalle. Etant donné que vous souhaitez que les méthodes se terminent rapidement, il est préférable de ne pas avoir un nombre anormalement élevé d'appels simultanés.

erreurs

Erreurs générées par l'application ou le système surveillé.

événements

Un événement est une action pour laquelle les agents capturent des données en plus des mesures. Exemples d'événements : traces de transaction, erreurs et blocages. L'agent enregistre les événements dans certaines situations, notamment :

- Traces de transaction
- Blocages
- Erreurs - Capture les exceptions renvoyées/détectées et suit tous les emplacements où ces exceptions sont renvoyées et détectées.

NOTE

Désactivez la détection des exceptions en production, car elle peut entraîner une dégradation significative des performances.

composant frontal

Un composant frontal est le composant d'une application qui gère en premier une requête entrante. Le composant peut être un servlet, une page JSP, une base de données de gestion, un objet EJB ou un autre composant.

Harvest

Harvest est le processus au cours duquel Introscope collecte des données auprès des collecteurs.

interval (intervalle)

Un intervalle est une période définie par l'utilisateur pour définir des mesures moyennes. Dans Introscope, cette période est généralement de 7,5 secondes. Certains des systèmes surveillés capturent des données selon des intervalles différents.

réponse

Une réponse se rapporte toujours à l'exécution d'une méthode. Une réponse est mesurée en tant que :

- nombre - le nombre de transactions terminées pendant l'intervalle.
- durée - Le temps qu'il a fallu pour exécuter une méthode, en millisecondes.

Le nombre de réponses par intervalle est la mesure de débit standard d'Introscope.

temps de réponse

Le temps de réponse est la période nécessaire pour exécuter une méthode, qui est mesurée en tant que :

- temps de réponse moyen (ms) - La durée moyenne, en millisecondes, nécessaire pour exécuter la méthode pendant l'intervalle.
- temps de réponse, minimum et maximum - Les temps de réponse les plus faibles et les plus élevés pendant l'intervalle.

taux

Le taux est le nombre d'exécutions de méthodes par seconde ou intervalle de temps.

blocage

Un blocage est une instance où le temps d'appel d'une méthode a dépassé un seuil défini par un administrateur.

Types de mesures

Les différents types de mesures sont les suivants :

- [Mesures de type Nombre](#)
- [Mesures de type Pourcentage](#)
- [Données de type Chaîne](#)

Mesures de type Nombre

Un nombre est un entier. Par exemple, un nombre peut représenter :

- Le nombre de points de données dont la moyenne a été calculée pour une mesure.
- Le nombre d'événements depuis un point donné dans le temps.
- Le nombre de threads en cours d'utilisation.

Comme exemples de mesures de type Nombre, citons le nombre d'erreurs et de blocages.

Mesures de type Pourcentage

Les *pourcentages* permettent de mesurer l'utilisation des ressources par rapport aux ressources maximales disponibles. Exemples :

- L'utilisation de l'UC
- Le pourcentage de temps passé dans les nettoyages de mémoire au cours des 15 dernières minutes

Données de type Chaîne

Outre les mesures et les états, Introscope collecte des informations qui identifient les systèmes et applications surveillés. Comme exemples de ce type de données, citons les noms de composants système tels que le nom d'une base de données, les versions JVM ou les adresses IP.

Mesures BlamePoint

DX APM utilise cinq mesures standard appelées *Mesures BlamePoint*. Les mesures BlamePoint fournissent une orientation initiale pour permettre aux trieurs d'identifier les experts système susceptibles d'aider à la résolution d'un problème.

Remarque : Les mesures BlamePoint sont également appelées mesures standard.

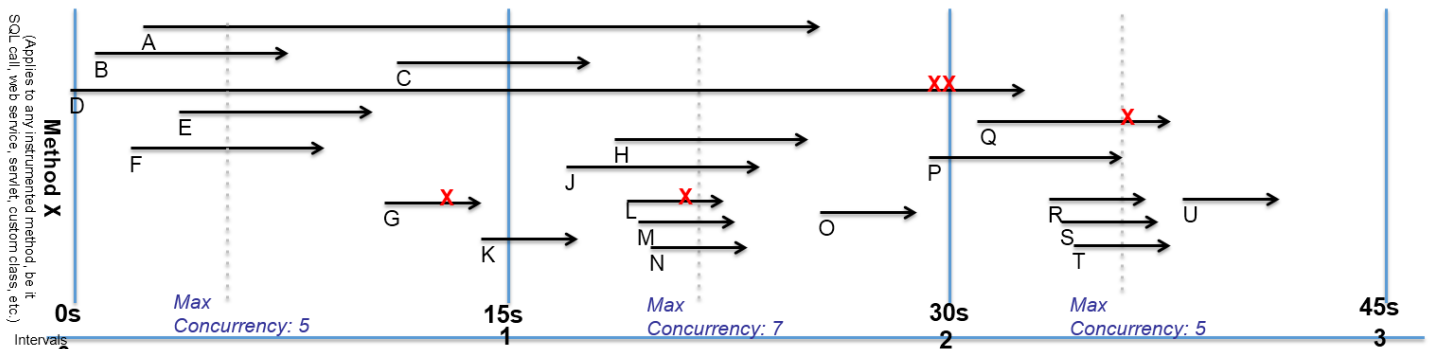
CA APM fournit ces mesures lorsque des méthodes Java sont surveillées ; par exemple :

- Composants frontaux
- Composants d'arrière-plan
- SQL
- Servlets
- Services Web (y compris la mesure d'erreur SOAP)
- EJB
- JSP
- Toutes les classes/méthodes Java personnalisées

Les méthodes les plus instrumentées signalent les cinq mesures suivantes :

L'exemple suivant illustre le signalement des mesures BlamePoint par APM pour les méthodes Java :

BlamePoint Metrics



Average Response Time (ms)

Interval 1: <small> B,E,F,G
Interval 2: <longer> A,C,H,J,K,L,M,N,O
Interval 3: <even longer> P,Q,R,S,T,U

Value is average of all finished invocations of a method or component. Count is number of transactions finished that interval. Min and Max are fastest and slowest measurements respectively.

Errors Per Interval (X)

Interval 1: 1 – G
Interval 2: 2 – L,D
Interval 3: 1 – Q

Any exception caught in the stack will be reported and a snapshot gathered (14 days).

Responses Per Interval

Interval 1: 4 – B,E,F,G
Interval 2: 9 – A,C,H,J,K,L,M,N,O
Interval 3: 6 – P,Q,R,S,T,U

Value reflects number of invocations finished in that interval. Min, Max, and Count all agree with value. Count of Average Response Time is identical to Responses Per Interval.

Stall Count (XX)

Interval 2: 1 – D

When methods take too long (30 sec default), they indicate a stuck thread, usually due to infinite loop, deadlock, or constrained resources. Snapshots are gathered (14 days).

Concurrent Invocations

Interval 1: 4 – A,C,D,K (max: 5 – A,B,D,E,F)
Interval 2: 2 – P,Q (max: 7 – A,D,H,J,L,M,N)
Interval 3: 0 – <none> (max: 5 – Q,P,R,S,T)

Min is the minimum number of threads in a method or component over the interval. Max is the peak number of threads. Value is the final sampling of how many threads were in the method at the end of the interval. Count is the total of entries and exits to the method.

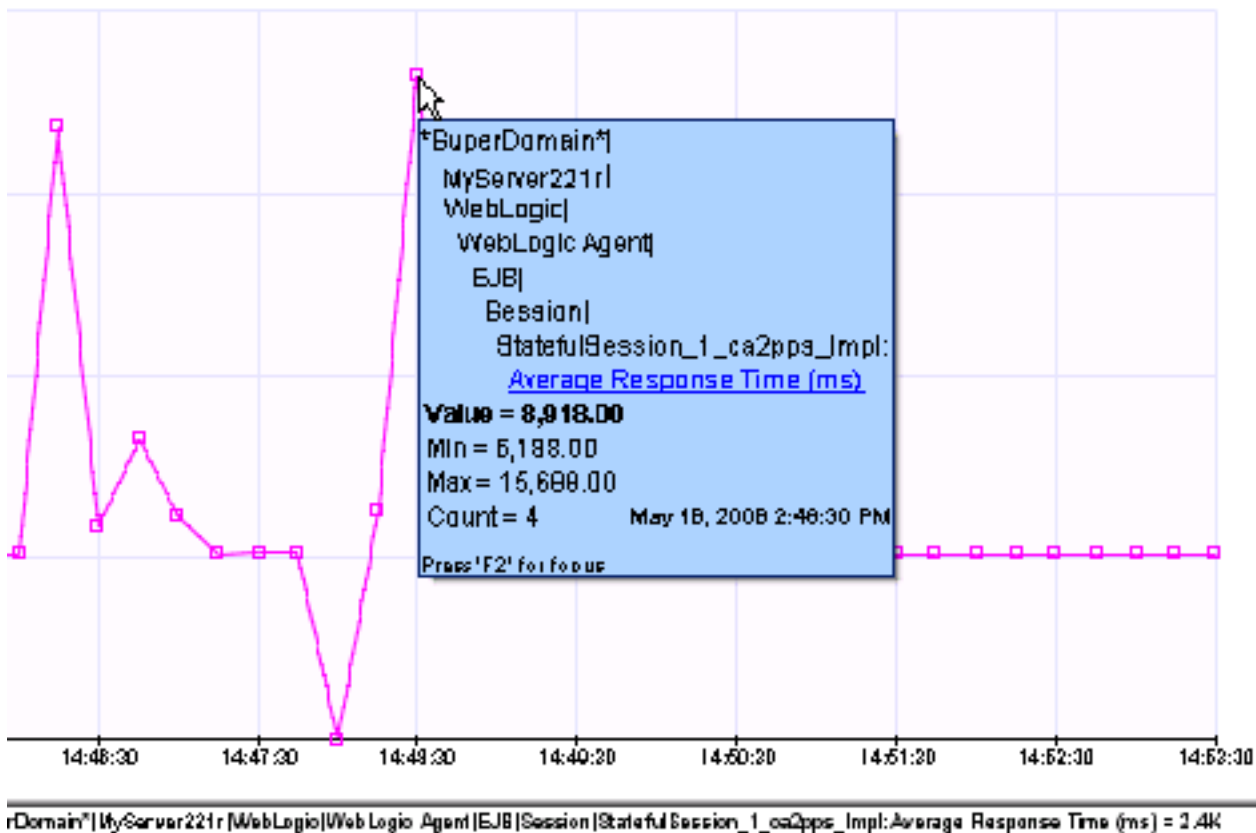
AKA Work in Process. When more work comes in than is being completed, this metric increases, indicating the "Pig-in-a-Python" analogy. If the metric spikes and then returns, this indicates a bottleneck (perhaps due to load) that was temporary.

Temps de réponse moyen (ms)

La mesure Temps de réponse moyen établit la moyenne des temps de réponse de toutes les demandes terminées pendant un intervalle. Le temps de réponse est la période requise pour satisfaire une demande. Ce temps fournit une mesure de base de la vitesse de réponse des applications, par conséquent :

- Il est souhaitable d'obtenir des temps de réponse faibles.
- Un temps de réponse élevé indique un problème.

Remarque : La durée du temps de réponse moyen est identique à la valeur Réponses par intervalle.



L'illustration présente un graphique de temps de réponse moyen pour une session EJB, tel qu'il apparaît dans la station de travail. Points à noter :

- Pour afficher une info-bulle contenant des informations complémentaires sur un point de données, passez le curseur sur celui-ci.
- Par exemple :
 - La valeur de point de données 8919 ms est le temps de réponse moyen des demandes terminées pendant l'intervalle.
 - Le nombre 4 indique que quatre demandes ont été terminées pendant l'intervalle sélectionné.
- En plus de la valeur et du nombre, chaque point de données possède des données Minimum et Maximum.
 - Minimum est la valeur unique la plus faible des demandes représentées dans le nombre. Dans cet exemple, il s'agit de la demande qui a pris le moins de temps à terminer.
 - Maximum est la valeur unique la plus élevée des demandes représentées dans le nombre. Dans cet exemple, il s'agit de la demande qui a pris le plus de temps à terminer.

Tenez compte des informations suivantes sur le temps de réponse moyen :

- **Tri basé sur le temps de réponse moyen**
Utilisez les tendances du temps de réponse moyen, combinées aux modifications apportées dans d'autres mesures, pour identifier et diagnostiquer les problèmes.
- **Problèmes spécifiques**
Lorsqu'ils sont accompagnés d'un nombre faible de threads disponibles, les temps de réponse moyens constamment élevés peuvent indiquer les problèmes suivants :
 - Code inefficace

- Surutilisation du système externe
- Composant d'arrière-plan lent
- Nombre excessif de couches
- **Problèmes périodiques**

Des pics réguliers dans un graphique indiquent des temps de réponse moyens élevés, qui reviennent ensuite à la normale. Lorsqu'ils sont accompagnés d'un nombre faible de threads disponibles, les temps de réponse moyens régulièrement élevés peuvent indiquer les problèmes suivants :

 - Fuites GC fréquentes
 - Goulot d'étranglement du composant d'arrière-plan lié à la charge

Lorsqu'ils sont accompagnés d'une lecture de l'utilisation de l'UC faible, les temps de réponse moyens régulièrement élevés peuvent indiquer les problèmes suivants :

 - Goulot d'étranglement interne
- **Problèmes progressifs**

Une augmentation continue dans le temps de réponse moyen sur une longue période, lorsqu'il est accompagné d'une lecture faible de Réponses par intervalle, peut indiquer une fuite de mémoire.

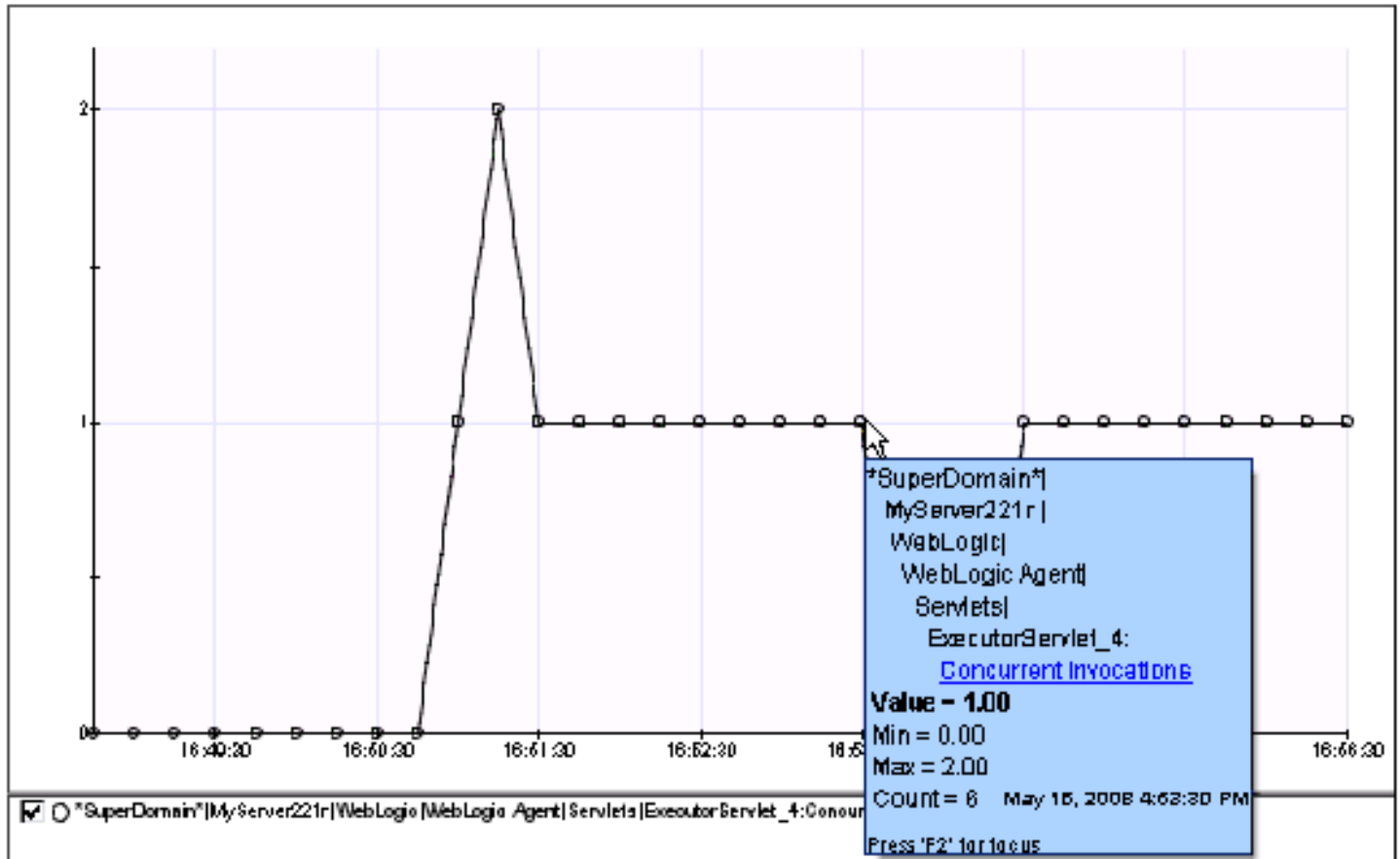
Appels simultanés

Les appels sont des demandes gérées par l'application et ses différentes parties. Les appels simultanés sont les demandes traitées à un moment donné.

DX APM calcule la mesure d'appels simultanés en comptant le nombre de demandes en cours de traitement à la fin d'un intervalle spécifique.

- Il est souhaitable d'obtenir une valeur faible d'appels simultanés.
- Une valeur élevée d'appels simultanés suggère un problème.

Les appels simultanés démarrent pendant un intervalle, mais ne sont pas finalisés au cours de celui-ci. Vous souhaitez que les méthodes se terminent rapidement, c'est pourquoi il n'est pas souhaitable d'obtenir un nombre anormalement élevé d'appels simultanés. Des pics temporaires peuvent se produire dans les appels simultanés, mais la mesure doit renvoyer zéro dans chaque cas. Une mesure qui renvoie une valeur différente de zéro peut indiquer un goulot d'étranglement des threads, un nombre de connexions à la base de données ou une autre ressource partagée.



Dans l'illustration, la valeur 1 indique qu'une demande est toujours en cours de traitement à la fin de l'intervalle sélectionné. Les demandes toujours en cours à la fin de l'intervalle sélectionné sont susceptibles de se terminer pendant les intervalles ultérieurs. Les demandes non terminées avant la fin des seuils spécifiés sont appelées blocages (voir la section [Nombre de blocages](#)).

Tenez compte des informations suivantes relatives aux appels simultanés :

- **Tri basé sur les appels simultanés**

Utilisez les tendances des appels simultanés, combinées aux modifications apportées dans d'autres mesures, pour identifier et diagnostiquer les problèmes.

- **Problèmes spécifiques**

Des valeurs d'appels simultanés constamment élevées peuvent indiquer les problèmes suivants : surutilisation du système externe, composant d'arrière-plan lent.

Lorsqu'elles sont accompagnées d'une lecture de réponses par intervalle faible, des valeurs élevées d'appels simultanés peuvent indiquer les problèmes suivants :

- Code inefficace
- Nombre excessif de couches

- **Problèmes périodiques**

Des valeurs d'appels simultanés régulièrement élevées apparaissent dans un graphique qui présente des pics réguliers, puis revient à la normale. Ce pic peut indiquer un goulot d'étranglement du composant d'arrière-plan lié à la charge.

Lorsqu'elles sont accompagnées d'une lecture de connexions disponibles faible, des valeurs d'appels simultanés régulièrement élevées peuvent indiquer des fuites de mémoire fréquemment nettoyée.

Lorsqu'elles sont accompagnées d'une lecture faible du nombre de threads disponibles, des valeurs d'appels simultanés régulièrement élevées peuvent indiquer un goulot d'étranglement interne.

- **Problèmes progressifs**

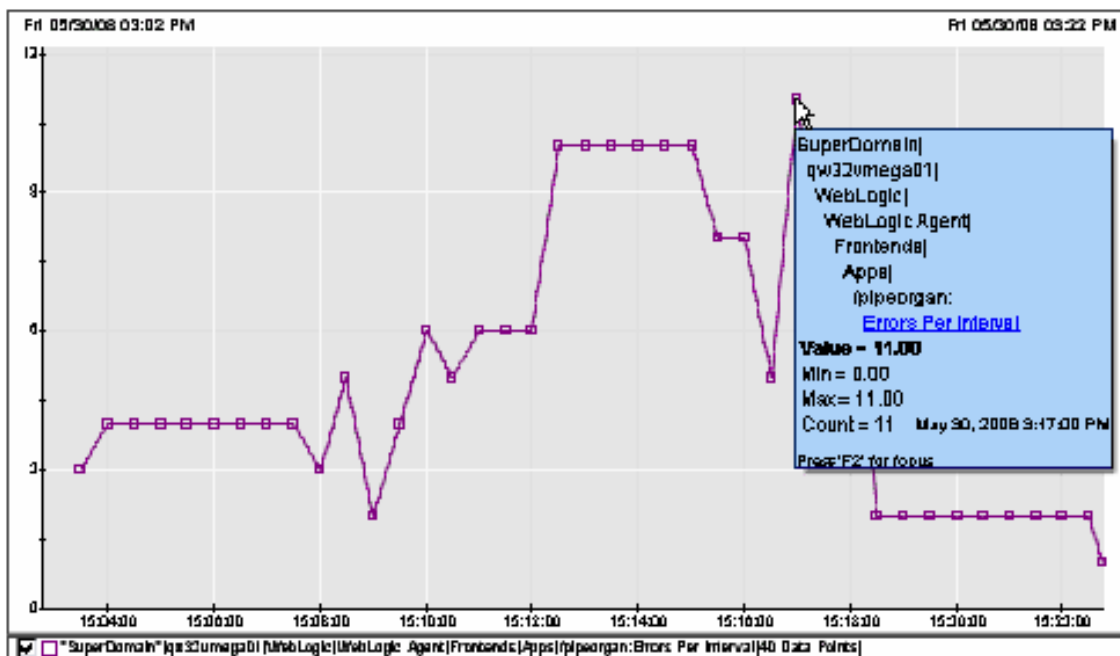
Une augmentation continue des appels simultanés sur une longue période, notamment lorsqu'elle est accompagnée d'une lecture de réponses par intervalle faible, peut indiquer une fuite de threads.

Erreurs par intervalle

Les erreurs représentent le nombre d'exceptions signalées par les codes d'erreur JVM et HTTP. Exemples d'erreurs :

- Statut 404 Page introuvable, signalé par le serveur HTTP
- Exception SQL
- Exception Java

Il est souhaitable d'obtenir un nombre d'erreurs faible.



La mesure est un nombre simple d'erreurs signalées pendant l'intervalle. L'illustration présente un point de données sélectionné avec la valeur 11, ce qui signifie que 11 erreurs ont été signalées pendant ce créneau. Cette mesure étant un nombre simple, les valeurs Minimum et Maximum sont toujours identiques.

Le chemin de mesure sous le graphique identifie l'application signalant l'exception. Pour plus d'informations sur les erreurs affichées dans un graphique, examinez les journaux de cette application.

Dans le cas de systèmes avec la fonction ErrorDetector activée, les erreurs génèrent également des clichés. Les clichés d'erreur fournissent des détails sur les événements lorsqu'une erreur s'est produite. Ces informations sont stockées dans la base de données des événements de transaction. Un nombre élevé d'erreurs génère une quantité de documents élevée. Éviter la génération de ces informations permet également de réduire le nombre d'erreurs.

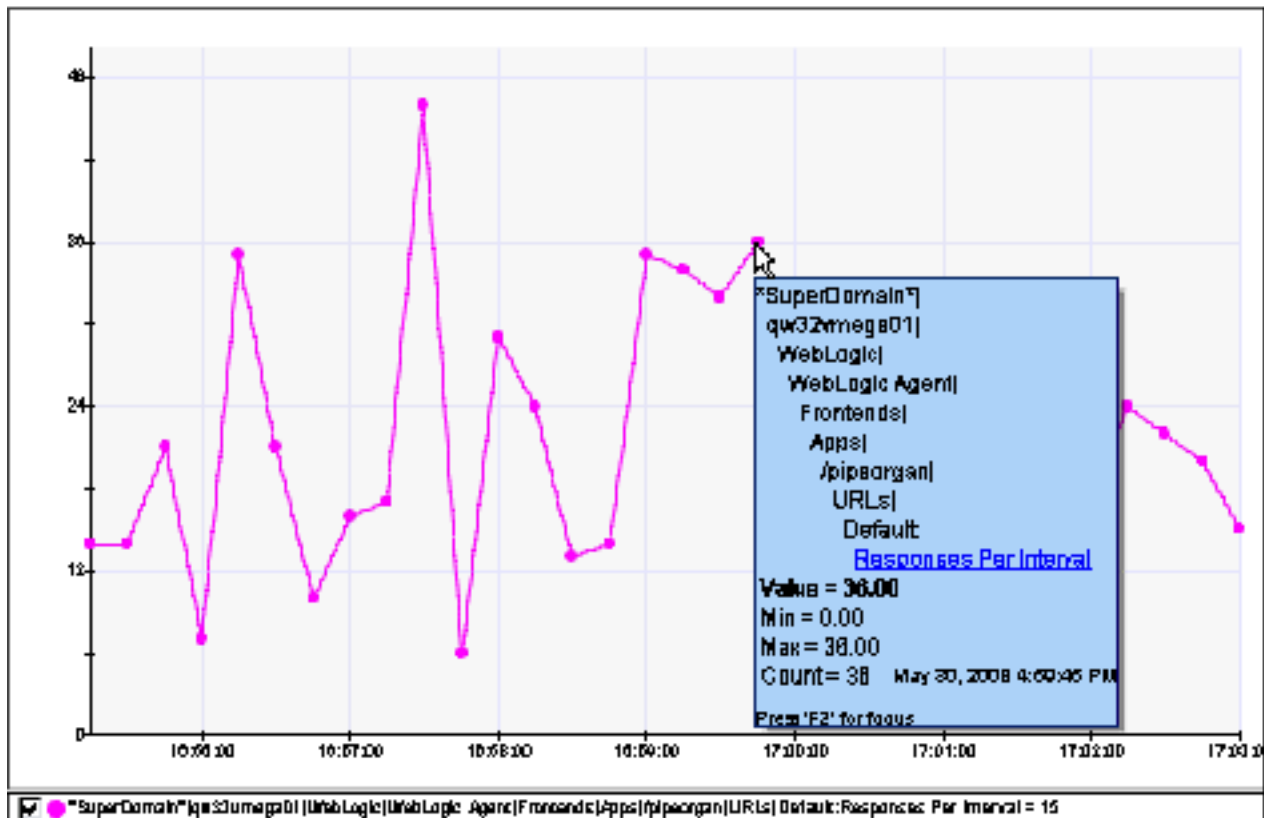
Réponses par intervalle

La mesure de réponses par intervalle reflète le nombre d'appels terminés dans cet intervalle. Cette mesure concerne le débit de données et donc les performances d'application. La mesure est un nombre simple des demandes terminées pendant un intervalle.

- La valeur de la mesure de réponses par intervalle est toujours identique au nombre pour la mesure de temps de réponse moyen.
- La mesure de réponses par intervalle est de type IntCounter. Cette mesure ne représente pas la moyenne du nombre de réponses ; il s'agira toujours de la valeur Maximum du nombre de réponses pendant l'intervalle.

En règle générale :

- Il est souhaitable d'obtenir un nombre élevé.
- Il n'est pas souhaitable d'obtenir un nombre faible.
- Un pic inattendu dans les réponses peut indiquer une surutilisation du système externe, telle qu'une attaque de type déni de service sur un site Web.



Dans l'illustration, l'info-bulle affiche la valeur du points de données sélectionné. Cette mesure étant un nombre simple, les valeurs Minimum et Maximum de la mesure sont toujours identiques.

Tenez compte des informations suivantes sur les réponses par intervalle :

- **Tri basé sur les réponses par intervalle**
Utilisez les tendances des réponses par intervalle, combinées aux modifications apportées dans d'autres mesures, pour identifier et diagnostiquer les problèmes.
- **Problèmes spécifiques**
Des valeurs de réponses par intervalle constamment élevées peuvent indiquer une utilisation excessive du système externe.

Nombre de blocages

Les demandes bloquées sont des demandes non terminées dans un délai spécifié. Le seuil de blocage par défaut est de 30 secondes. Lorsqu'une demande est comptée comme bloquée, cela signifie que son exécution a dépassé le seuil de blocage.

- Il est souhaitable d'obtenir un nombre faible.
- Il n'est pas souhaitable d'obtenir un nombre élevé.

Les blocages peuvent représenter les cas suivants. Ce blocage peut s'expliquer par d'autres raisons, mais les scénarios suivants sont les plus courants.

- **Thread dans une boucle infinie**

Parfois, les programmeurs écrivent un code dans lequel une boucle ne parvient pas à sortir normalement. Lorsqu'un thread entre dans une boucle infinie, le nombre de blocages des composants à l'origine de l'appel augmente. Les boucles infinies ont pour caractéristique supplémentaire de rendre un noyau d'UC occupé. Par exemple, dans un système silencieux comptant quatre noyaux, si un thread entre dans une boucle infinie, l'utilisation totale de l'UC peut augmenter d'environ 25 %. Si un deuxième thread entre dans la boucle infinie, l'UC augmente de 50 %, etc.

- **Thread en longue attente ou thread qui n'expire jamais**

Lorsqu'un thread tente d'ouvrir une ressource telle qu'un socket pour un système distant, le programmeur peut indiquer qu'il doit s'arrêter après un nombre spécifique de secondes. Si cette période est suffisante (ex. : cinq minutes), le nombre de blocages augmente et reste incrémenté pendant les cinq minutes. Dans certains cas, la tentative de connexion n'expire jamais, auquel cas le thread reste occupé et le nombre de blocages ne baisse jamais. Dans de nombreux systèmes, des threads se bloquent de cette manière pour des raisons de routine. Ce comportement explique pourquoi le nombre de blocages peut parfois être différent de zéro pour un composant, même lorsque le système est inactif. Tenez compte du nombre de threads ordinaires et traitez le problème concernant les changements anormaux uniquement.

- **Thread non impliqué dans un interblocage ou un verrou actif**

Les programmeurs utilisent des verrous pour éviter tout endommagement des données. Parfois l'ordre d'acquisition des verrous peut être incorrect, auquel cas le programme peut développer un interblocage. Un interblocage signifie qu'au moins deux threads sont bloqués, chacun d'eux étant dans l'attente de l'avancement de l'autre. Les threads ne peuvent pas avancer sans les ressources déjà extraites par les autres threads. Les interblocages sont des pannes système catastrophiques dans quasiment tous les cas de figure. Les images mémoire de thread constituent souvent la technique la plus utile pour identifier le code endommagé. Un verrou actif est un interblocage dans lequel un ou plusieurs threads utilisent activement l'UC. Les interblocages se distinguent des boucles infinies dans le sens où une boucle infinie est uniquement le résultat d'une condition d'interruption d'une boucle, tandis qu'un interblocage implique la sémantique de verrouillage, ou code synchronisé, de l'application dans laquelle il se produit.

Remarque : Des informations sur les événements de blocage sont stockés dans la base de données des événements de transaction.

Tenez compte des informations suivantes sur le nombre de blocages :

- **Mesure du nombre de blocages**

Le suivi des transactions peut afficher plusieurs demandes non terminées pendant le délai spécifié (blocages), mais Investigator affiche un nombre de blocages différent.

Cela est dû au fait que le nombre de blocages est enregistré comme valeur de point (à un moment donné pendant un intervalle) et non comme valeur de plage (pour une période). Plusieurs valeurs de blocage peuvent représenter des transactions longues terminées pendant un intervalle, mais seul le nombre disponible à un moment donné est utilisé comme point de données.

- **Tri basé sur le nombre de blocages**

Utilisez les tendances du nombre de blocages, combinées aux modifications apportées dans d'autres mesures, pour identifier et diagnostiquer les problèmes.

- **Problèmes spécifiques**

Des valeurs de nombre de blocages constamment élevées peuvent indiquer un système en arrière-plan lent.

- **Problèmes périodiques**

Des valeurs de nombre de blocages régulièrement élevées peuvent indiquer un goulot d'étranglement du composant d'arrière-plan lié à la charge.

- **Problèmes progressifs**

Une augmentation continue des valeurs de nombre de blocages sur une longue période, notamment lorsqu'elle est accompagnée d'un nombre faible de threads disponibles, peut indiquer une fuite de ressource (threads).

Mesures JMX

Les mesures suivantes sont disponibles dans l'arborescence Investigator sous le noeud JMX au format : JMX\|(.*)|(Type=)?<Nom du MBean>:<Nom de l'attribut>.

- **ServerRuntime: OpenSocketsCurrentCount**
Nombre actuel de sockets ouverts sur le serveur.
- **ServerRuntime: SocketsOpenedTotalCount**
Nombre total de sockets qui ont été ouverts sur le serveur.
- **ExecuteQueueRuntime: ExecuteThreadCurrentIdleCount**
Nombre de threads inactifs affectés à la file d'attente.
- **ExecuteQueueRuntime: PendingRequestCurrentCount**
Nombre de demandes en attente dans la file d'attente.
- **ExecuteQueueRuntime: ServicedRequestTotalCount**
Nombre de demandes traitées par cette file d'attente.
- **JDBCDataSourceRuntime: ActiveConnectionsCurrentCount**
Nombre de connexions JDBC en cours d'utilisation dans cette source de données.
- **JDBCDataSourceRuntime: ConnectionsTotalCount**
Nombre total de connexions JDBC créées dans cette source de données depuis son déploiement.
- **JDBCDataSourceRuntime: LeakedConnectionCount**
Nombre de connexions JDBC en fuite.
- **JDBCDataSourceRuntime: WaitingForConnectionCurrentCount**
Nombre de demandes de connexion en attente d'une connexion JDBC.
- **JDBCDataSourceRuntime: NumAvailable**
Nombre de connexions JDBC actuellement disponibles dans cette source de données.
- **EJBCacheRuntime: ActivationCount**
Nombre total de beans de cette interface d'accueil EJB étant activés.
- **EJBCacheRuntime: CacheAccessCount**
Nombre total de tentatives d'accès à un bean à partir de ce cache.
- **EJBCacheRuntime: CachedBeansCurrentCount**
Nombre actuel de beans de cette interface d'accueil EJB figurant dans le cache EJB.
- **EJBCacheRuntime: CacheHitCount**
Nombre de tentatives d'accès au cache réussies.
- **EJBLockingRuntime: TimeoutTotalCount**
Nombre total de threads expirés en attente de verrou sur un bean.
- **EJBPoolRuntime: BeansInUseCount**
Nombre d'instances de bean de ce pool en cours d'utilisation.
- **EJBPoolRuntime: IdleBeansCount**
Nombre d'instances de bean de ce pool actuellement disponibles.
- **EJBPoolRuntime: TimeoutTotalCount**
Nombre total de threads expirés en attente d'un bean disponible à partir de ce pool.
- **EJBPoolRuntime: WaiterCurrentCount**
Calcule le nombre de threads en attente d'une instance de bean disponible du pool libre.
- **EJBTransactionRuntime: TransactionCommittedTotalCount**

Nombre total de transactions validées pour ce EJB.

- **JMSRuntime: ConnectionsTotalCount**
Nombre total de connexions JMS établies avec ce serveur WebLogic après la dernière réinitialisation.
- **JMSRuntime: JMSServersCurrentCount**
Nombre total de serveurs JMS déployés sur cette instance de serveur WebLogic.
- **JMSPooledConnectionRuntime: NumAvailable**
Nombre de sessions JMS disponibles dans le pool non actuellement utilisées.
- **JMSDestinationRuntime: BytesReceivedCount**
Nombre d'octets reçus sur cette destination après la dernière réinitialisation.
- **JMSDestinationRuntime: ConsumersTotalCount**
Nombre total de consommateurs ayant accédé à cette destination après la dernière réinitialisation.
- **JMSDestinationRuntime: MessagesReceivedCount**
Nombre de messages reçus sur cette destination après la dernière réinitialisation.
- **JMSDestinationRuntime: BytesCurrentCount**
Nombre actuel d'octets stockés dans la destination.
- **JMSDestinationRuntime: ConsumersCurrentCount**
Nombre actuel de consommateurs accédant à cette destination.
- **JMSDestinationRuntime: MessagesCurrentCount**
Nombre actuel de messages dans la destination.
- **JMSDurableSubscriberRuntime: MessagesReceivedCount**
Nombre de messages reçus par cet abonné durable après la dernière réinitialisation.
- **JMSDurableSubscriberRuntime: BytesCurrentCount**
Nombre d'octets reçus par cet abonné durable.
- **JMSDurableSubscriberRuntime: MessagesCurrentCount**
Nombre de messages toujours disponibles pour cet abonné durable.
- **JMSServerRuntime: BytesReceivedCount**
Nombre total d'octets reçus par ce serveur JMS après la dernière réinitialisation.
- **JMSServerRuntime: BytesCurrentCount**
Nombre actuel d'octets stockés sur ce serveur JMS.
- **JMSConnectionRuntime: SessionsCurrentCount**
Nombre actuel de sessions pour cette connexion.
- **TransactionNameRuntime: TransactionAbandonedTotalCount**
Nombre total de transactions abandonnées après la dernière réinitialisation.
- **TransactionNameRuntime: TransactionCommittedTotalCount**
Nombre total de transactions validées après la dernière réinitialisation.
- **TransactionNameRuntime: TransactionHeuristicsTotalCount**
Nombre total de transactions terminées avec un statut heuristique après la dernière réinitialisation.
- **TransactionNameRuntime: TransactionRolledBackTotalCount**
Nombre total de transactions annulées après la dernière réinitialisation.
- **TransactionNameRuntime: TransactionRolledBackTimeoutTotalCount**
Nombre total de transactions annulées en raison d'une expiration de délai après la dernière réinitialisation.
- **TransactionNameRuntime: TransactionTotalCount**
Nombre total de transactions traitées (validées/annulées/heuristiques) depuis la dernière réinitialisation.
- **TransactionResourceRuntime: TransactionCommittedTotalCount**
Nombre total de transactions validées depuis la dernière réinitialisation.
- **TransactionResourceRuntime: TransactionHeuristicsTotalCount**
Nombre total de transactions terminées avec un statut heuristique depuis la dernière réinitialisation.
- **TransactionResourceRuntime: TransactionRolledBackTotalCount**
Nombre total de transactions annulées depuis la dernière réinitialisation.
- **TransactionResourceRuntime: TransactionRolledBackTimeoutTotalCount**

Nombre total de transactions annulées en raison d'une expiration de délai depuis la dernière réinitialisation.

- **TransactionResourceRuntime: TransactionTotalCount**
Nombre total de transactions traitées (validées/annulées/heuristiques) depuis la dernière réinitialisation.
- **JTARuntime: TransactionAbandonedTotalCount**
Nombre total de transactions abandonnées depuis la dernière réinitialisation.
- **JTARuntime: TransactionCommittedTotalCount**
Nombre total de transactions validées depuis la dernière réinitialisation.
- **JTARuntime: TransactionHeuristicsTotalCount**
Nombre total de transactions terminées avec un statut heuristique depuis la dernière réinitialisation.
- **JTARuntime: TransactionRolledBackTotalCount**
Nombre total de transactions annulées depuis la dernière réinitialisation.
- **JTARuntime: TransactionRolledBackTimeoutTotalCount**
Nombre total de transactions annulées en raison d'une expiration de délai depuis la dernière réinitialisation.
- **JTARuntime: TransactionTotalCount**
Nombre total de transactions traitées (validées/annulées/heuristiques) depuis la dernière réinitialisation.
- **Server: IdleConnectionTimeout**
Valeur actuelle de l'expiration de session HTTP.

Mesures d'agrégat JMX

Les mesures suivantes sont disponibles dans l'arborescence Investigator sous le noeud WebLogic, JMX Aggregate :

- **Thread Pool: Waiting Request Count**
Calcule le nombre total de threads demandant une instance disponible du pool libre.
- **JDBC Connection Pool: Waiting Thread Count**
Calcule le nombre total de threads en attente d'une instance de connexion disponible du pool libre.
- **EJB Pool: Waiting Thread Count**
Calcule le nombre total de threads en attente d'une instance de bean disponible du pool libre.

Mesures de transaction

Les mesures de transaction mesurent une partie spécifique d'une transaction. En fonction de votre architecture système, les mesures Java suivantes peuvent apparaître dans Investigator. La plupart s'affichent dans l'arborescence des mesures.

L'agent Java indique également le contexte de votre application Java comme des attributs d'exécution pour les vertices (sommets) Team Center. L'ensemble des attributs signalés par l'agent Java sont les [attributs communs](#), qui existent pour la plupart des composants. DX APM regroupe automatiquement les attributs communs. Vous pouvez créer [vos propres perspectives](#) à l'aide des attributs Java.

NOTE

Certaines de ces mesures, telles que Database et XML, s'appliquent à l'agent NET également.

EJB

Si votre architecture intègre des beans EJB (Enterprise JavaBeans), ils peuvent être des types suivants :

- Bean EJB Entity
- Bean EJB Session
- Bean EJB en fonction des messages

Pour chacune de ces types, les deux mesures suivantes s'affichent :

- Durée moyenne d'appel de méthode (ms)
- Appels de méthode par intervalle

Pour chaque classe ou méthode EJB qui apparaît comme noeud enfant sous des types EJB, le gestionnaire d'entreprise fournit les cinq mesures BlamePoint :

- Temps de réponse moyen (ms)
- Appels simultanés
- Erreurs par intervalle
- Réponses par intervalle
- Nombre de blocages

Servlets

Le noeud de servlets affiche généralement les cinq mesures de base BlamePoint pour chaque servlet appelé par l'application surveillée :

- Temps de réponse moyen (ms)
- Appels simultanés
- Erreurs par intervalle
- Réponses par intervalle
- Nombre de blocages

Le noeud de servlets affiche également les mesures liées à l'UC :

NOTE

Les mesures ci-dessous liées à l'UC ne sont pas prises en charge pour les servlets asynchrones.

- Durée moyenne de blocage (ms)
Durée approximative (en ms) qu'un thread a passé dans l'état BLOCKED lorsque la JVM prend en charge la surveillance de la contention de threads.
- Moyenne d'octets allouée
Nombre approximatif d'octets alloués au segment de mémoire de threads de transaction lorsque la JVM prend en charge la mesure de l'allocation de la mémoire de threads.

NOTE

Les machines virtuelles Java IBM ne prennent pas en charge cette mesure.

- Temps d'UC système moyen (ms)
Durée d'exécution du code dans le noyau du système d'exploitation d'une transaction d'application surveillée lorsque la JVM prend en charge la mesure du temps d'UC.
- Temps d'UC utilisateur moyen (ms)
Temps passé par le processeur à exécuter le code de programme ou le code dans les bibliothèques pour une transaction lorsque la JVM prend en charge la mesure du temps d'UC.
- Temps d'attente moyen (ms)
Durée approximative (en ms) qu'un thread de transaction a passé dans l'état WAITING ou TIMED_WAITING lorsque la JVM prend en charge la surveillance de contentions de threads.

JSP (Java Server Pages)

Temps de réponse moyen (ms)

Temps de réponse moyen des méthodes `_jspService()` de tous les fichiers JSP exécutés dans la machine virtuelle Java. La moyenne des temps de réponse de tous les fichiers JSP est établie pour calculer cette valeur.

Réponses par intervalle

Nombre d'appels terminés des méthodes `_jspService` de tous les fichiers JSP exécutés dans la machine virtuelle Java au cours des 15 dernières secondes.

Temps de réponse moyen (ms) par nom de classe

Temps de réponse moyen (en ms) du JSP identifié par le nom de classe. Tous les appels de la méthode `_jspService()` sont chronométrés et la moyenne calculée pour obtenir cette valeur.

Réponses par intervalle

Nombre d'appels terminés de la méthode `_jspService()` du fichier JSP identifié par le nom de classe au cours des 15 dernières secondes.

Réponses par seconde

Fréquence d'exécution des méthodes `_jspService()` de tous les fichiers JSP exécutés dans la machine virtuelle Java.

Réponses par seconde par nom de classe

Fréquence d'exécution des appels de la méthode `_jspService()` du fichier JSP identifié par un nom de classe spécifique.

Méthodes bloquées par nom de classe et par nom de méthode

Nombre de fichiers JSP qui dépassent le seuil défini pour exécuter la méthode `_jspService()`.

Appels simultanés

Nombre de threads exécutant la méthode `_jspService()`.

Bibliothèques de balises JSP (TagLib JSP)

Les bibliothèques de balises sont des collections de balises personnalisées, utilisées dans les pages JSP pour appeler des actions personnalisées. La spécification JSP prévoit six actions standard. Une action personnalisée est une action non incluse dans l'ensemble des six actions standard. Exemples de tâches appelées par des actions personnalisées : contrôle de formulaire, accès à des systèmes externes tels que des bases de données et une messagerie et contrôle de flux.

Les mesures suivantes sont disponibles pour les bibliothèques de balises JSP :

- Durée moyenne d'appel de méthode (ms)
- Appels de méthode par intervalle
- Durée moyenne d'appel de méthode (ms) par nom de classe et nom de méthode
- Appels de méthode par intervalle et par nom de classe
- Appels de méthode par intervalle, par nom de classe et nom de méthode
- Appels de méthode par seconde
- Appels de méthode par seconde par nom de classe
- Appels de méthode par seconde, par nom de classe et nom de méthode
- Appels de méthode simultanés
- Appels de méthode simultanés par nom de classe
- Appels de méthode simultanés par nom de classe et nom de méthode
- Méthodes bloquées pendant plus de 30 secondes par nom de classe et nom de méthode
- Durée moyenne d'appel de méthode (ms)

Bibliothèque de balises d'E/S JSP

- Nombre d'avertissements
- Nombre d'exceptions

RMI (Remote Method Invocations, appels de méthode à distance)

Les appels de méthode à distance sont des appels de méthodes d'objets Java distribués, qui peuvent exister dans plusieurs hôtes.

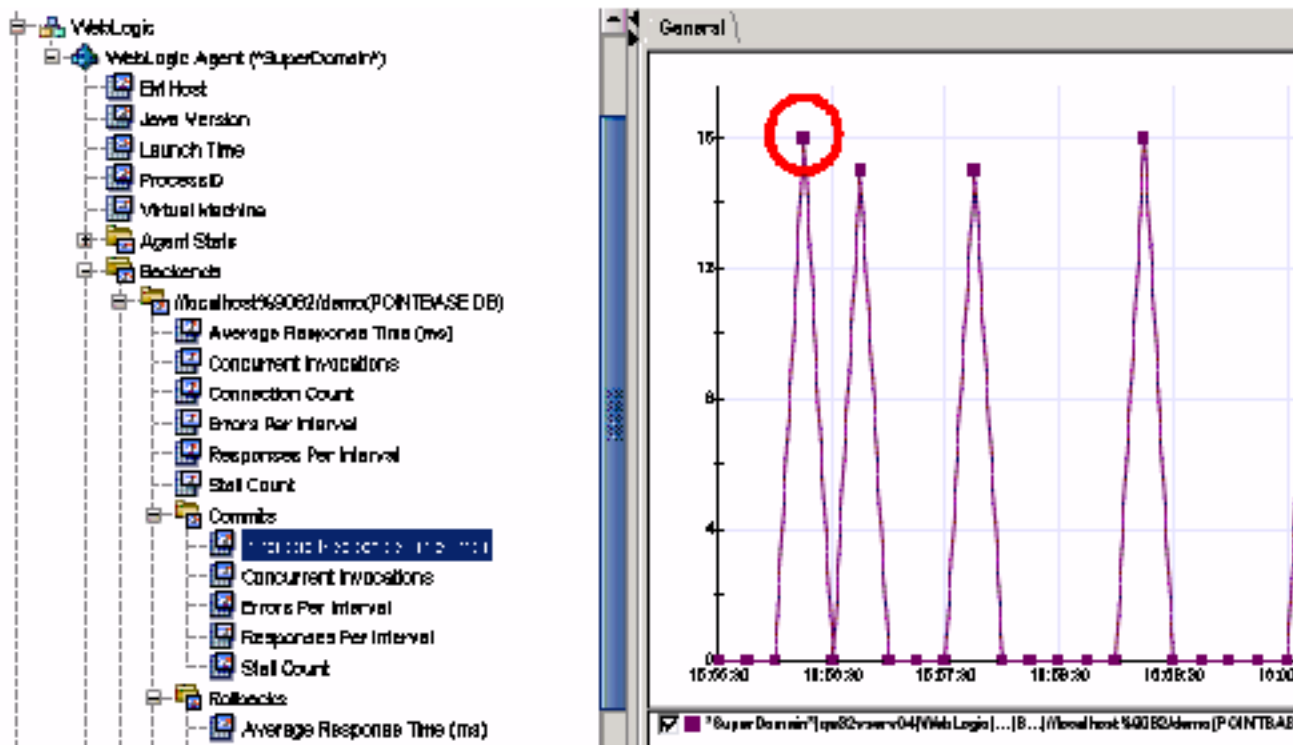
Les mesures suivantes sont disponibles pour les clients et serveurs RMI.

- Durée moyenne d'appel de méthode (ms)
- Appels de méthode par intervalle
- Durée moyenne d'appel de méthode (ms) par nom de classe
- Appels de méthode par intervalle et par nom de classe
- Appels de méthode par seconde
- Appels de méthode par seconde par nom de classe
- Méthodes bloquées pendant plus de 30 secondes
- Appels de méthode simultanés
- Appels de méthode simultanés par nom de classe

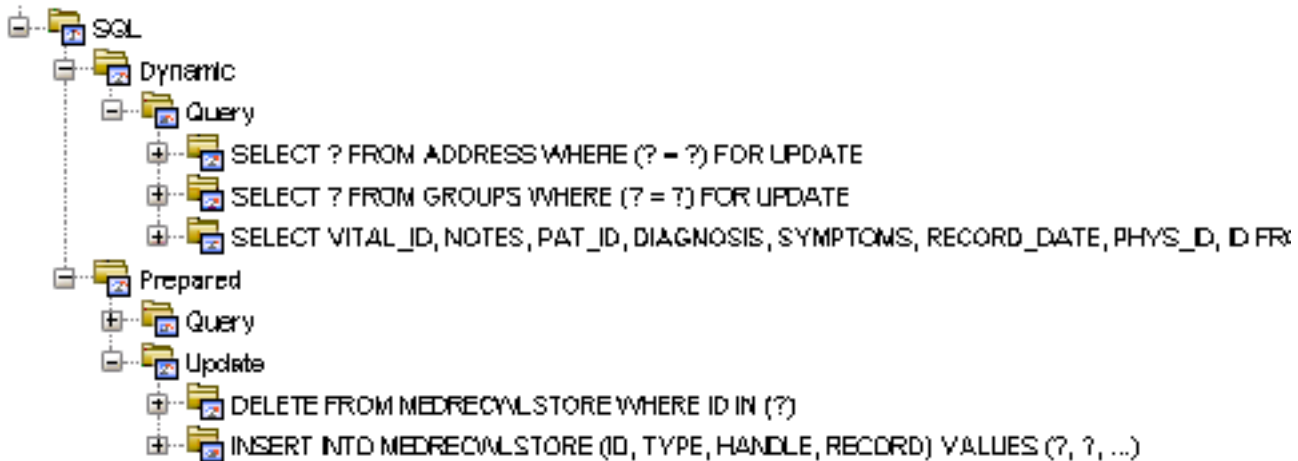
Mesures de base de données (SQL)

Chaque composant d'arrière-plan de base de données peut être configuré pour signaler les mesures suivantes :

- Validations : chaque transaction requête-réponse terminée est appelée *validation*. Les cinq mesures standard sont collectées et affichées pour toutes les transactions de validation dans un intervalle donné. Par exemple, dans la capture d'écran ci-après, le point de données entouré indique le temps de réponse moyen pour toutes les transactions de base de données validées dans cet intervalle.



- Restaurations : une restauration est une transaction de requête-réponse terminée avec des erreurs. Les cinq mesures standard sont collectées et affichées pour toutes les transactions annulées dans un intervalle donné.
- SQL :



Pour chacune des instructions traitées par la base de données pendant un intervalle, l'agent signale les six mesures suivantes :

- Temps de réponse moyen (ms)
- Appels simultanés
- Erreurs par intervalle
- Nombre d'objets de connexion active
- Réponses par intervalle
- Nombre de blocages

Points à noter :

- Les instructions sont séparées par un sous-noeud selon qu'elles soient préparées ou dynamiques.
- Chaque type d'instruction SQL, telle que GRANT, UPDATE, QUERY, REVOKE, DROP est répertorié sous un sous-noeud de du type d'instruction.

Composants d'arrière-plan automatiques

Le chemin des mesures de composants d'arrière-plan automatiques est légèrement différent de celui des mesures de composants d'arrière-plan standard.

Backends|<Package Java>|<nom_classe> |<méthode>

Par exemple : Composants d'arrière-plan|com.mysql.jdbc|MySQLIO|sendCommand

Les mesures récapitulatives pour différents composants d'arrière-plan d'un même package Java s'affichent ici :

Composants d'arrière-plan|<Package Java>

Par exemple : Composants d'arrière-plan|com.mysql.jdbc

Introscope signale des mesures de prise en charge de composants d'arrière-plan automatiques.

XML (Extensible Markup Language)

Les mesures XML peuvent être des types suivants.

SAX

- SAX : durée moyenne d'appel de méthode (ms)
- SAX : appels de méthode par intervalle
- SAX : durée moyenne d'appel de méthode (ms) par nom de classe
- SAX : appels de méthode par intervalle et par nom de classe
- SAX : appels de méthode par seconde
- SAX : appels de méthode par seconde par nom de classe
- SAX : méthodes bloquées pendant plus de 30 secondes par nom de classe et nom de méthode
- SAX : appels de méthode simultanés
- SAX : appels de méthode simultanés par nom de classe

XSLT

- XSLT : durée moyenne d'appel de méthode (ms)
- XSLT : appels de méthode par intervalle
- XSLT : durée moyenne d'appel de méthode (ms) par nom de classe
- XSLT : appels de méthode par intervalle et par nom de classe
- XSLT : appels de méthode par seconde
- XSLT : appels de méthode par seconde par nom de classe
- XSLT : méthodes bloquées pendant plus de 30 secondes par nom de classe et nom de méthode
- XSLT : appels de méthode simultanés
- XSLT : appels de méthode simultanés par nom de classe

JAXM

- JAXM|Listener: durée moyenne d'appel de méthode (ms)
- JAXM|Listener : appels de méthode par intervalle
- JAXM|Listener : durée moyenne d'appel de méthode (ms) par nom de classe
- JAXM|Listener : appels de méthode par intervalle et par nom de classe
- JAXM|Listener : appels de méthode par seconde
- JAXM|Listener : appels de méthode par seconde par nom de classe
- JAXM|Listener : méthodes bloquées pendant plus de 30 secondes par nom de classe et nom de méthode
- JAXM|Listener : appels de méthode simultanés
- JAXM|Listener : appels de méthode simultanés par nom de classe

Connecteur J2EE

- Durée moyenne d'appel de méthode (ms)
- Appels de méthode par intervalle
- Durée moyenne d'appel de méthode (ms) par nom de classe
- Appels de méthode par intervalle
- Appels de méthode par seconde
- Appels de méthode par seconde par nom de classe
- Nombre de méthodes bloquées pendant plus de 30 secondes par nom de classe et nom de méthode
- Appels de méthode simultanés
- Appels de méthode simultanés par nom de classe

JTA (Java Transaction API)

- Durée moyenne d'appel de méthode (ms)
- Appels de méthode par intervalle
- Durée moyenne d'appel de méthode (ms) par nom de classe
- Appels de méthode par intervalle et par nom de classe
- Appels de méthode par seconde
- Appels de méthode par seconde par nom de classe
- Méthodes bloquées pendant plus de 30 secondes par nom de classe et nom de méthode
- Appels de méthode simultanés

JNDI (Java Naming and Directory Interface)

Les mesures JNDI incluent :

- [JNDI lookup](#)
- [JNDI lookupLink](#)
- [JNDI search](#)
- [JNDI called metrics](#)

Recherche JNDI

- Lookup : durée moyenne d'appel de méthode Context (ms)
- Lookup : appels de méthode Context par intervalle
- Lookup : durée moyenne d'appel de méthode Context (ms) par nom de classe
- Lookup : appels de méthode Context par intervalle par nom de classe
- Lookup : appels de méthode Context par seconde
- Lookup : appels de méthode Context par seconde par nom de classe
- Lookup : méthodes Context bloquées pendant plus de 30 secondes par nom de classe et nom de méthode
- Lookup : Appels de méthode Context simultanés
- Lookup : appels de méthode Context simultanés par nom de classe

JNDI lookupLink

- lookupLink : durée moyenne d'appel de méthode Context (ms)
- lookupLink : appels de méthode Context par intervalle
- lookupLink : durée moyenne d'appel de méthode Context (ms) par nom de classe
- lookupLink : appels de méthode Context par intervalle par nom de classe
- lookupLink : appels de méthode Context par seconde
- lookupLink : appels de méthode Context par seconde par nom de classe
- lookupLink : méthodes Context bloquées pendant plus de 30 secondes par nom de classe et nom de méthode
- lookupLink : Appels de méthode Context simultanés
- lookupLink : appels de méthode Context simultanés par nom de classe

JNDI Search

- Search : durée moyenne d'appel de méthode Context (ms)
- Search : appels de méthode Context par intervalle
- Search : durée moyenne d'appel de méthode Context (ms) par nom de classe
- Search : appels de méthode Context par intervalle par nom de classe
- Search : appels de méthode Context par seconde
- Search : appels de méthode Context par seconde par nom de classe
- Search : méthodes Context bloquées pendant plus de 30 secondes par nom de classe et nom de méthode
- Search : appels de méthode Context simultanés
- Search : appels de méthode Context simultanés par nom de classe

JNDI Called Metrics

- Système de fichiers d'E/S

JMS (Java Messaging Service)

JMS présente quatre sous-noeuds :

- écouteur de messages
- consommateur de messages
- éditeur de thèmes
- expéditeur de file d'attente

Les mesures suivantes peuvent apparaître sous l'un des sous-noeuds :

- Durée moyenne d'appel de méthode (ms)
- Appels de méthode par intervalle
- Durée moyenne d'appel de méthode (ms) par nom de classe
- Appels de méthode par intervalle et par nom de classe
- Appels de méthode par seconde
- Appels de méthode par seconde par nom de classe
- Méthodes bloquées pendant plus de 30 secondes par nom de classe et nom de méthode
- Appels de méthode simultanés
- Appels de méthode simultanés par nom de classe

Pour les API de réception JMS synchrones, les mesures suivantes sont signalées sous le noeud de composants d'arrière-plan dans Investigator :

- [Messages reçus par intervalle](#)
- [Erreurs par intervalle](#)
- [Temps de traitement du message estimé \(ms\)](#)

Les valeurs des mesures `{queueName}` et `{topicName}` sont cumulées dans les valeurs des noeuds Queues et Topics, respectivement.

Messages reçus par intervalle

La mesure Messages Received Per Interval est incrémentée d'un point chaque fois que la méthode `receive()` est exécutée avec une valeur de retour non nulle.

Erreurs par intervalle

La mesure Erreurs par intervalle est incrémentée d'un point lorsque l'une des méthodes instrumentées renvoie une exception. De plus, ErrorDetector génère un cliché d'erreur.

NOTE

Lorsque la méthode `receive()` d'IBM WebSphere MQ JMS finit avec une exception `MQRC_NO_MSG_AVAILABLE`, APM ne signale pas certains résultats. La mesure Erreurs par intervalle n'est pas incrémentée et ErrorDetector ne génère aucun cliché d'erreur.

Temps de traitement du message estimé (ms)

Cette mesure indique le temps approximatif entre la finalisation correcte de la méthode `receive()` avec une valeur de retour non nulle et le début de l'appel suivant de la méthode `receive()`. Cette mesure collecte des données lorsque les méthodes sont présentes sur le même objet consommateur et le même thread. Lorsque l'agent ne parvient pas à identifier la réception suivante, l'outil de suivi JMS utilise la méthode parente d'appel de réception JMS pour calculer la valeur de la mesure. Dans ce cas, la valeur de mesure est la durée entre la fin de la réception en cours et la fin de la méthode parente. Ce n'est qu'après l'identification et l'instrumentation correcte de la méthode parente de réception JMS à l'aide de `JMSReceiveParentTracer` que l'agent peut générer une trace de transaction. La trace affiche la valeur de la durée de traitement de la mesure. Consultez la section suivante.

Instrumentation et identification de la méthode parente

La méthode parente d'un appel JMS `Receive` est la méthode chargée de traiter le message reçu par l'appel JMS `Receive`. Parfois, l'outil de suivi ne trouve pas d'appel `receive` après celui en cours. Dans ce cas, l'identification de la méthode parente est essentielle à la fourniture de la valeur de mesure et du suivi des transactions.

L'identification de la méthode parente fonctionne comme suit :

1. Dans une trace de pile collectée dans l'outil de suivi de la méthode `receive`, les classes peuvent être étiquetées à l'aide de la méthode `run` ou `call`. Les classes étiquetées implémentent la méthode des interfaces `java.lang.Runnable` ou la méthode `java.lang.Callable`. Les classes étiquetées avec la méthode `run` ou `call` sont identifiées comme méthodes parentes. Si plusieurs méthodes parentes sont présentes dans la trace de pile, la méthode la plus proche de l'appel `receive` est marquée comme parente.

NOTE

Introscope ignore divers composants lors de l'identification de la classe parente et de la méthode à partir de la trace de pile. Introscope ignore toutes les classes JDK, les méthodes et classes Lambda dynamiques et les classes proxy.

2. Une trace de pile peut ne contenir aucune méthode `run` ou `call` utilisable par l'agent pour identifier la méthode parente. Dans ce cas, l'agent établit l'identification sur la valeur d'index constante. Par défaut, la classe au niveau de l'index 7 est identifiée comme la méthode parente. Si la classe au niveau de l'index 7 est une classe JDK, Lambda dynamique ou proxy, Introscope l'ignore. Introscope prend en compte la classe de l'index inférieur suivant (plus proche de l'appel `receive`) et recommence jusqu'à marquer une classe comme parente. Les classes parentes identifiées sont stockées dans le fichier `JMSParentMethodPersist.pbd` sous le répertoire `<répertoire_base_agent>\core\hotdeploy`.

NOTE

Informations complémentaires : [Identification d'une méthode qui ne se ferme jamais en tant que méthode parente](#)

JavaMail

JavaMail présente deux sous-noeuds :

- JavaMail (Send)
- JavaMail (sendMessage)

Les mesures suivantes peuvent apparaître sous les sous-noeuds Send ou sendMessage :

- Transport : durée moyenne d'appel de méthode (ms)
- Transport : appels de méthode par intervalle
- Transport : durée moyenne d'appel de méthode (ms) par nom de classe
- Transport : appels de méthode par intervalle et par nom de classe
- Transport : appels de méthode par seconde
- Transport : appels de méthode par seconde par nom de classe
- Transport : méthodes bloquées pendant plus de 30 secondes par nom de classe et nom de méthode
- Transport : appels de méthode simultanés
- Transport : appels de méthode simultanés par nom de classe

CORBA

- Durée moyenne d'appel de méthode (ms)
- Appels de méthode par intervalle
- Durée moyenne d'appel de méthode (ms) par nom de classe
- Appels de méthode par intervalle et par nom de classe
- Appels de méthode par seconde
- Méthodes bloquées dans une classe pendant plus de 30 secondes
- Appels de méthode simultanés
- Appels de méthode simultanés par nom de classe

Struts

- Durée moyenne d'appel de méthode (ms)
- Appels de méthode par intervalle
- Durée moyenne d'appel de méthode (ms) par nom de classe et nom de méthode
- Appels de méthode par intervalle et par nom de classe
- Appels de méthode par seconde
- Appels de méthode par seconde par nom de classe
- Méthodes bloquées pendant plus de 30 secondes par nom de classe et nom de méthode
- Appels de méthode simultanés
- Appels de méthode simultanés par nom de classe

Durabilité d'agent

Les mesures du durabilité d'agent apparaissent sous le noeud **Agent Stats**. Ces mesures fournissent des informations sur l'état interne de l'agent plutôt que sur l'application qu'il surveille. Les mesures du durabilité d'agent peuvent indiquer des données utiles lors de l'examen du comportement d'un agent.

Mesures de durabilité de suivi détaillé

Le sous-noeud **Deep Tracing** est situé sous le sous-noeud **Sustainability**. Le sous-noeud Deep Tracing affiche les mesures suivantes sur les ressources d'agent utilisées pour fournir une visibilité détaillée du suivi des transactions :

Mesure de visibilité détaillée du suivi des transactions et de durabilité d'instrumentation intelligente**Analyzed Methods Count**

Nombre total de méthodes analysées par Introscope à des fins d'instrumentation intelligente. Ce nombre inclut les méthodes instrumentées ou non par la solution d'instrumentation intelligente.

Average Component Array Size

Taille de la structure interne de tableau de données du composant d'instrumentation intelligente, signalée par les transactions en temps réel.

Average Component Count Per Transaction

Nombre moyen de composants Blame et de visibilité détaillée par transaction.

Average Deep Component Count Per Transaction

Nombre moyen de composants de visibilité détaillées par transaction.

Classes Processed Per Interval

Nombre de classes traitées par ProbeBuilder à des fins d'instrumentation intelligente.

Instrumented Methods Count

Nombre total de méthodes actuellement instrumentées par l'instrumentation intelligente.

Max Instrumentable Methods Count

Nombre maximum de méthodes qualifiées par Introscope pour l'instrumentation lorsque le niveau d'instrumentation intelligente est élevé.

ProbeInfo Collection Size

Taille de la liste interne de tableaux ProbeInfo Collection.

Auto Tracing: Cached Transaction Count Per Interval

Nombre de transactions placées dans un cache interne par intervalle de 15 secondes.

Auto Tracing: Clamped Traces

Nombre de suivis automatiques de transactions limités et non envoyés au gestionnaire d'entreprise ou affichés dans l'interface utilisateur.

Auto Tracing: Downstream GUID Count Per Interval

Nombre d'identificateurs de trace en aval ajoutés à un cache interne par intervalle de 15 secondes.

Auto Tracing: Sent Traces

Nombre de suivis automatiques de transactions envoyés au gestionnaire d'entreprise et affichés dans l'interface utilisateur.

Auto Tracing: Trace Cache Hits

Nombre de suivis automatiques de transactions envoyés à partir d'un agent en aval par intervalle de 15 secondes.

Auto Tracing: Trace Cache Misses

Nombre d'identificateurs de suivi qui ne correspondent à aucun identificateur dans un cache interne par intervalle de 15 secondes.

Auto Tracing: Upstream GUID Count Per Interval

Nombre d'identificateurs de trace en amont ajoutés à un cache interne par intervalle de 15 secondes.

Instrumentation Level: Number Of Candidate Classes For Reinstrumentation

Nombre total de classes potentielles à recharger après une modification du niveau d'instrumentation intelligente. Ce nombre ne change pas lorsqu'Introscope traite une modification du niveau. A la fin du traitement, le nombre affiche zéro.

Instrumentation Level: Current Instrumentation Level

Niveau actuel de l'instrumentation intelligente. Valeurs : 1 = faible, 2 = moyen, 3 = élevé. Lorsqu'Introscope traite un changement du niveau X au niveau Y, la valeur de mesure affiche le niveau X jusqu'à la fin du traitement.

Mesure de durabilité de détection de points d'entrée**Entry Point Detection: Analyzed Stack Snapshots**

Nombre total de piles de threads analysées pour détecter d'éventuels points d'entrée candidats après le démarrage de l'application surveillée.

Entry Point Detection: Candidates Discarded

Nombre total de candidats suivis et rejetés avant de devenir des points d'entrée, car jugés inappropriés.

Entry Point Detection: Entry Points Discarded

Nombre de points d'entrée rejetés par l'agent, car jugés inappropriés. Ces points d'entrée sont définitivement ignorés.

Entry Point Detection: Entry Points Discovered

Nombre de points d'entrée détectés par cet agent après le démarrage de l'application surveillée.

Entry Point Detection: Initial Candidates Current

Nombre actuel de points d'entrée candidats détectés par l'agent, mais non encore traités par le moteur de règles.

Entry Point Detection: Initial Candidates Total

Nombre total de points d'entrée candidats détectés par l'agent après le démarrage de l'application surveillée.

Entry Point Detection: Stack Snapshot Queue Length

Nombre actuel de clichés de pile de threads collectés, en attente de recherche d'éventuels points d'entrée candidats.

Entry Point Detection: Total Entry Points

Nombre total de points d'entrée dans AutoPersist.pbd.

Entry Point Detection: Total Entry Points Discarded

Nombre total de points d'entrée exclus et ignorés qui sont conservés dans AutoPersist.pbd.

Entry Point Detection: Tracked Candidates Current

Nombre actuel de points d'entrée candidats suivis par l'agent à des fins de performances.

Entry Point Detection: Tracked Candidates Total

Nombre total de points d'entrée candidats suivis par l'agent après le démarrage de l'application surveillée.

Entry Point Detection: Tracked Threads

Nombre actuel de threads suivis par l'agent en vue de la détection d'éventuels points d'entrée.

Mesures de durabilité de détection automatique de serveur d'arrière-plan

Automatic Backend Detection: Analyzed Stack Snapshots (Détection automatique de serveur d'arrière-plan : Clichés de pile analysés)

Nombre total de clichés de pile analysés en vue de la détection de serveurs d'arrière-plan candidats après le démarrage de l'application surveillée.

Automatic Backend Detection: Backends Discovered (Détection automatique de serveur d'arrière-plan : Serveurs d'arrière-plan détectés)

Nombre total de serveurs d'arrière-plan détectés par l'agent après le démarrage de l'application surveillée.

Automatic Backend Detection: Backends Persisted

Nombre total de serveurs d'arrière-plan conservés dans AutoPersist.pbd.

Mesures de durabilité des extensions

Les mesures de durabilité des extensions se trouvent sous le sous-noeud **Extension Bundles**, qui se trouve sous le sous-noeud **Sustainability**. Les mesures d'extensions fournissent des informations sur les extensions d'agent. Les mesures fournissent des options de déploiement d'extension et de chargement/déchargement de données.

Mesures spécifiques au déploiement des extensions

Deployment|Count|All Cycles:Count

Nombre total de cycles de déploiement survenus après le démarrage de l'agent. Chaque cycle commence par l'acquisition d'un verrou de déploiement et se termine par la libération du verrou.

Deployment|Count|Failed Cycles:Count

Nombre total d'échecs de cycle de déploiement après le démarrage de l'agent. Chaque cycle commence par l'acquisition d'un verrou de déploiement et se termine par la libération du verrou. Les cycles de déploiement peuvent échouer pour plusieurs raisons. Exemple : décompression d'un fichier .tar source d'erreurs, suppression d'un fichier .tar, calcul des sommes de contrôle, etc.

Une valeur supérieure à zéro et croissante indique que l'outil de déploiement d'extension rencontre des difficultés pour décompresser une ou plusieurs extensions.

Deployment|Count|Successful Cycles:Count

Nombre total de cycles de déploiement correctement exécutés après le démarrage de l'agent. Chaque cycle commence par l'acquisition d'un verrou de déploiement et se termine par la libération du verrou. En principe, cette valeur devrait être identique à la valeur de la mesure All Cycles Count.

Deployment|Current Cycle|Status

Statut de l'exécution du thread `ExtensionDeployer` pour déployer/annuler le déploiement des extensions à partir de leur fichier .tar vers le répertoire `<répertoire_base_agent>/extensions/deploy/`. Cette mesure présente deux valeurs possibles : la valeur 0 indique que l'extension est déployée et la valeur 1 que l'extension est en cours de déploiement. Dans l'idéal, la valeur doit indiquer 0, c'est-à-dire le statut d'extension déployée. Lorsque la valeur de la mesure indique 1 pendant plusieurs longues minutes, le thread `ExtensionDeployer` est interbloqué. Vérifiez le thread, puis redémarrez l'application surveillée.

Deployment|Last Cycle|Time (milliseconds)

Durée (en millisecondes) du dernier cycle de déploiement `ExtensionDeployer`. Cette valeur représente la durée passée entre l'acquisition et la libération du verrou de déploiement.

Mesures de chargement d'extensions

Failed: Count

Nombre total d'échecs de chargement d'extensions. L'échec peut être entraîné par une combinaison de fichiers PBD ou JAR défectueux, ou d'un autre artefact d'extension facultatif.

Une valeur supérieure à 0 signifie qu'une extension n'a pas été chargée, probablement en raison d'un conflit PBD.

Loaded: Count

Nombre total d'extensions correctement chargées.

Total: Count

Nombre total d'extensions d'agent dans le répertoire `<répertoire_base_agent>/extensions`.

Mesures de durabilité de JMX Clamp

Le sous-noeud **JMX Clamp** se trouve sous le sous-noeud **Sustainability**.

Clamp Status

Lorsque la valeur de la propriété `introscope.agent.jmx.clamp` est égale ou supérieure au niveau du seuil, cette mesure est définie sur 1. Lorsque la valeur de la propriété est inférieur au seuil, la mesure est définie sur 0.

Mesures de visibilité d'écart d'exécution de l'instrumentation intelligente

Le sous-noeud **Runtime Visibility** se trouve sous le sous-noeud **Sustainability**.

Gaps Found Per Interval

Nombre d'écarts détectés par le composant de visibilité d'écart d'exécution pendant l'intervalle. L'intervalle est déterminé par la propriété `introscope.agent.deep.instrumentation.visibility.processor.interval`.

Runtime Components Per Transaction

Nombre moyen de composants de visibilité d'écart d'exécution par transaction de 15 secondes.

Methods Instrumented Per Interval

Nombre de méthodes instrumentées par la solution de visibilité d'écart d'exécution pendant l'intervalle. L'intervalle est déterminé par la propriété `introscope.agent.deep.instrumentation.visibility.processor.interval`.

Methods UnInstrumented Per Interval

Nombre de méthodes non instrumentées par le composant de visibilité d'écart d'exécution pendant l'intervalle. L'intervalle est déterminé par la propriété `introscope.agent.deep.instrumentation.visibility.processor.interval`.

Total Methods Instrumented

Nombre de méthodes actuellement instrumentées par le composant de visibilité d'écart d'exécution.

Mesures de durabilité SQL

Le sous-noeud **SQL** se trouve sous le sous-noeud **Sustainability**.

SQL: SQL Statement Count

Nombre actuel d'instructions SQL uniques pour lesquelles l'agent a créé des mesures.

Mesures de journalisation de la durabilité

Les mesures de journalisation de la durabilité sont situées sous le sous-noeud **Configuration**, sous **Sustainability**. Ces mesures fournissent le nombre d'avertissements et d'erreurs signalés par l'agent dans le fichier journal.

AutoProbe Errors Count

Cette mesure présente deux valeurs : la valeur 0 indique qu'aucun échec d'AutoProbe ne s'est produit et la valeur 1 indique que des échecs d'AutoProbe ont été signalés.

Error Count

Nombre total d'erreurs signalées par l'agent dans le fichier **IntroscopeAgent.log** depuis le démarrage de l'agent.

Erreurs par intervalle

Nombre total d'erreurs signalées par l'agent dans le fichier **IntroscopeAgent.log** pendant l'intervalle actuel de génération de rapports.

Warnings Count

Nombre total d'avertissements signalés par l'agent dans le fichier **IntroscopeAgent.log** depuis le démarrage de l'agent.

Warnings Per Interval

Nombre total d'avertissements signalés par l'agent dans le fichier **IntroscopeAgent.log** pendant l'intervalle actuel de génération de rapports.

Mesures du gestionnaire de surcharge

Les mesures du gestionnaire de surcharge sont disponibles sous le sous-noeud **Sustainability**. Elles indiquent si l'agent collecte ou non les données de surveillance sur le serveur d'applications. Cela est contrôlé par la propriété `introscope.agent.overhead.level`. Pour plus d'informations sur cette propriété, reportez-vous à la section [Propriétés de l'agent Java](#).

Mode de surcharge

La valeur 1 indique que la surveillance d'agent standard est activée sur le serveur d'applications, la valeur 0 qu'elle ne l'est pas.

Mesures liées à la mémoire

Les mesures liées à la mémoire apportent des informations sur la fonction Nettoyage de la mémoire (GC).

NOTE

- Toutes les mesures répertoriées s'appliquent à DX APM sur site et seules certaines mesures s'appliquent à DX APM SaaS.
- Les nombres d'instances présentent une caractéristique spéciale : ils ne sont pas signalés par défaut. Les nombre d'instances sont associés à la mémoire (renvoient uniquement le nombre et non la taille) et génèrent des données concernant les objets transactionnels.

Nettoyage de la mémoire (GC)

L'opération de nettoyage de la mémoire consiste à récupérer automatiquement la mémoire dédiée aux objets qui ne sont plus utilisés par une application. Lorsque le processus trouve un objet qui n'est pas utilisé, la mémoire est libérée. Lorsque le processus trouve un objet qui est toujours utilisé, il le copie dans un pool de mémoires dernière génération. Un pool de mémoires nouvelle génération est rempli et un nettoyage de la mémoire léger a lieu. Les objets actifs sont copiés dans le pool de mémoires du deuxième espace restant. Si ce deuxième espace restant n'est pas suffisamment volumineux pour contenir tous les objets, les objets actifs sont également copiés dans des espaces de pool de mémoires à long terme.

Le nettoyage de la mémoire pouvait avoir lieu très souvent, ce qui augmentait la quantité de mémoire réclamée. La surcharge dédiée au processus était alors excessive. A l'inverse, lorsqu'il n'avait pas lieu suffisamment souvent, le nettoyage de la mémoire ne libérait pas suffisamment de mémoire. De plus, une surcharge significative était nécessaire pour l'exécution du processus GC. Par conséquent, le nettoyage de la mémoire est plus efficace lorsque la période s'écoule avant les nettoyages de la mémoire mineurs. L'efficacité équilibre le nombre d'objets nettoyés avec la quantité de surcharge requise pour les nettoyer.

Lors d'un processus efficace de nettoyage de la mémoire, les pools de mémoires nouvelle génération possèdent la taille appropriée. Si les pools de mémoires sont de trop petite taille, le nettoyage automatique de la mémoire a lieu trop souvent. Si les pools de mémoires sont trop volumineux, le nombre d'objets inutilisés qui s'accumulent est excessif. Cette accumulation oblige le processus GC moins fréquent à utiliser une charge excessive lors de son exécution. La surcharge peut provoquer un pic du pourcentage de temps consacré au nettoyage.

- **Mesures liées au segment de mémoire GC** : par défaut, Introscope génère des mesures liées au segment de mémoire GC. Ces mesures utilisent les octets comme unité de mesure.
- **Mesures liées au moniteur GC** : ces mesures fournissent des informations supplémentaires sur l'utilisation de la mémoire. Elles sont collectées ou générées uniquement après avoir été activées par un administrateur.
- **Les mesures de type Fichiers système, UDP et Sockets** sont liées au débit de données.

Mesures liées au segment de mémoire GC

Ces mesures sont activées par défaut.

- **GC Heap|Bytes In Use**
Les mesures GC Heap|Bytes In Use (Segment de mémoire GC|Octets utilisés) spécifient la quantité de mémoire actuellement utilisée par les objets.
- **GC Heap|Bytes Total**
Les mesures GC Heap|Bytes Total (Segment de mémoire GC|Nombre total d'octets) indiquent la quantité totale de mémoire que la machine virtuelle Java alloue.
Comparez cette mesure avec la mesure Current Capacity (bytes) (Capacité actuelle (octets)), qui est disponible lorsque le DX APMmoniteur GC est activé. La mesure Current Capacity (bytes) (Capacité actuelle (octets)) fournit des informations sur la quantité de mémoire engagée pour tous les segments de mémoire de la machine virtuelle Java. La mesure Bytes Total (Nombre total d'octets) indique la quantité de mémoire engagée pour la machine virtuelle Java totale.

Mesures liées au moniteur GC

Les mesures liées au moniteur GC offre des informations sur les utilitaires de nettoyage de mémoire et les pools de mémoires, aidant ainsi à détecter les problèmes de nettoyage de la mémoire qui réduisent les performances.

Les mesures liées au moniteur GC s'affichent dans le navigateur de mesures directement sous le noeud **GC Heap** (Segment de mémoire GC). Les mesures sont activées par défaut. Certaines mesures incluent un seuil prédéfini qui déclenche des indicateurs d'alerte dans l'onglet **GC Monitor Overview** (Présentation du moniteur GC).

NOTE

Pour plus d'informations sur les limitations du moniteur GC et sur les machines virtuelles Java prises en charge, consultez la Matrice de compatibilité du produit.

Mesures génériques

Les mesures génériques sont les suivantes :

- **GC Policy (Stratégie GC)**
Identifie le nom des déchets pour la machine virtuelle Java.
- **JVM Type (Type de machine virtuelle Java)**
Identifie la machine virtuelle Java surveillée.
- **Percentage of Java Heap Used (Pourcentage de segment de mémoire Java utilisé)**
Indique le pourcentage de segment de mémoire disponible utilisé sur l'ordinateur sur lequel l'agent est déployé.
 - Le seuil d'avertissement est de 60 %.
 - Le seuil de danger est de 80 %.

Par défaut, la machine virtuelle augmente ou diminue le segment de mémoire à chaque nettoyage. Cette action permet de maintenir la proportion d'espace disponible des objets actifs dans une plage spécifique. La plage ciblée est définie via les paramètres, comme suit :

- `-XX:MinHeapFreeRatio=<minimum>`
- `-XX:MaxHeapFreeRatio=<maximum>`

La taille totale est basée sur `-Xms` et `-Xmx` .

La taille par défaut est souvent insuffisante.

WARNING

Conservez la mesure sous 60 pour cent. Si la mesure dépasse 80 %, ajustez la taille du segment de mémoire de la machine virtuelle Java. Pour accorder une mémoire suffisante à un prix abordable à la machine virtuelle, ajustez les paramètres `-Xms` et `-Xmx`.

Les valeurs par défaut de la plage ciblée oscillent entre 30 et 70 %. Les applications plus volumineuses rencontrent souvent des problèmes avec les valeurs par défaut. L'un de ces problèmes est le démarrage lent, qui se produit lorsque le segment de mémoire initial est de taille réduite et qu'il doit être redimensionné au fur et à mesure que plusieurs opérations de nettoyage ont lieu. La définition des paramètres `-Xms` et `-Xmx` sur la même valeur augmente la prévisibilité en évitant à la machine virtuelle d'avoir à prendre la décision la plus importante concernant le dimensionnement. D'autre part, la machine virtuelle ne peut pas compenser les sélections médiocres.

Veillez à augmenter la mémoire au fur et à mesure que vous augmentez le nombre de processeurs, car l'allocation peut être traitée en parallèle.

Mesures liées à l'utilitaire de nettoyage de mémoire

Les mesures liées à l'utilitaire de nettoyage de mémoire sont les suivantes :

- **GC Algorithm (Algorithme GC)**
Affiche l'algorithme de nettoyage de la mémoire pour le gestionnaire de mémoire correspondant.
- **GC Invocation Per Interval (Appels GC par intervalle)**
Indique le nombre d'opérations de nettoyage de la mémoire qui ont eu lieu à chaque intervalle de 15 secondes. La mesure est agrégée et calculée à partir de la mesure de nombre total d'appels GC, en traçant la différence entre l'intervalle actuel et l'intervalle le plus récent.
Cette mesure indique la collecte par intervalle qui s'effectue au niveau du pool de mémoires. Si la mesure augmente au fil du temps, cela signifie que des opérations de nettoyage ont lieu fréquemment dans un pool de mémoires et que la taille n'est pas adaptée. L'augmentation de la taille du pool de mémoires permet d'espacer les opérations de nettoyage.
- **GC Invocation Total Count (Nombre total d'appels GC)**
Nombre de nettoyages de la mémoire qui ont eu lieu depuis le démarrage de la machine virtuelle Java.
Cette mesure indique le nombre d'opérations de nettoyage depuis le démarrage du serveur. La valeur de la mesure s'accroît lentement à intervalles réguliers.
Les pics au niveau de cette mesure indiquent que les nettoyages ont lieu fréquemment, ce qui a un impact sur le débit global des applications. Pour réduire la fréquence des opérations de nettoyage de la mémoire et augmenter le débit, augmentez la taille du pool de mémoires.
- **GC Time Per Interval (ms) (Délai GC par intervalle (ms))**
Affiche la durée du nettoyage de la mémoire pendant l'intervalle de 15 secondes. Cette mesure agrégée est calculée à partir de la mesure de délai total GC en traçant la différence au niveau du délai GC entre l'intervalle actuel et l'intervalle le plus récent.
Dans des circonstances normales, cette mesure reste stable ou s'accroît lentement au fur et à mesure que la durée de nettoyage de la mémoire augmente.
Une augmentation importante indique que la durée d'exécution des applications est lente et qu'elle augmente les temps de pause des opérations de nettoyage de la mémoire. Afin d'éviter que ce problème ne survienne, configurez la mémoire maximum à l'aide de l'indicateur `-Xmx` sur une valeur optimale. Le réglage des valeurs appropriées entraîne la diminution des temps de pause des opérations de nettoyage de la mémoire et l'amélioration du débit GC. Si la mémoire est trop élevée, la fréquence GC diminue et le débit/efficacité GC augmente. Toutefois, l'application subit un temps de pause long, étant donné que le système tente de maintenir un espace de segment de mémoire trop volumineux. La définition de la taille de segment de mémoire sur une valeur optimale garantit des temps de pause et des durées de nettoyage de la mémoire faibles.
- **Memory Reclaimed Per Interval**

Calcule et signale la quantité de mémoire en octets récupérée par un utilitaire de nettoyage de mémoire pendant l'intervalle actuel. Lorsque plusieurs appels d'un utilitaire de nettoyage de mémoire sont présents, cette mesure affiche la somme de toutes les mémoires d'appels d'utilitaire de nettoyage de mémoire.

- **Percentage of Heap Used After GC Invocation**

Calcule et signale le pourcentage de segment de mémoire utilisé par la machine virtuelle Java après l'événement de nettoyage de la mémoire. La mesure affiche une valeur de 0 pour les intervalles sans appel de nettoyage de la mémoire. Lorsque plusieurs appels d'un utilitaire de nettoyage de mémoire sont présents dans un intervalle, cette mesure affiche le pourcentage moyen de segment de mémoire de tous d'appels.

DX APM prend en charge cette mesure sur les versions 1.7 et ultérieures de la machine virtuelle Java Oracle.

- **Pourcentage de temps passé dans GC au cours des 15 dernières minutes**

Affiche une mesure agrégée calculée à l'aide d'un calculateur du gestionnaire d'entreprise. Le pourcentage de cette valeur est calculé à l'aide de la formule suivante :

```
(total GC time spent/length of time in ms) * 100
```

Exemple avec un intervalle de 15 minutes :

```
45600 / (15*60*1000) * 100 = 5 %
```

Une augmentation importante du délai indique que la durée d'exécution des applications est lente et qu'elle augmente les temps de pause des opérations de nettoyage de la mémoire. Configurez la mémoire maximum à l'aide de l'indicateur `-Xmx` sur une valeur optimale.

Une mesure stable qui augmente soudainement indique qu'une opération ponctuelle de nettoyage de la mémoire a pris plus de temps que le temps habituel. Après ce pic, la mesure revient à sa valeur normale et aucune action n'est requise.

- **Total GC Time (ms) (Durée totale GC (ms))**

Affiche la durée totale du processus de nettoyage de la mémoire, en millisecondes.

Dans des circonstances normales, la mesure augmente progressivement.

Une augmentation importante du délai indique que la durée d'exécution des applications est lente et qu'elle augmente les temps de pause des opérations de nettoyage de la mémoire. Afin d'éviter que ce problème ne survienne, configurez la mémoire maximum à l'aide de l'indicateur `-Xmx` sur une valeur optimale. Le réglage des valeurs appropriées entraîne la diminution des temps de pause des opérations de nettoyage de la mémoire et l'amélioration du débit GC.

Activation et utilisation des mesures GC Morel

Le nettoyage de la mémoire et la gestion de la mémoire peuvent réduire considérablement les performances d'une application. Les mesures de base liées au segment de mémoire GC sont disponibles par défaut. Vous pouvez activer des mesures facultatives afin de fournir d'autres informations sur le traitement des opérations de nettoyage de la mémoire et sur l'utilisation du pool de mémoires. Ces mesures supplémentaires s'affichent sous le noeud **GC Monitor** du navigateur de mesures lorsqu'elles sont activées. Les mesures GC Monitor apportent des informations permettant d'optimiser l'allocation du pool de mémoires et le traitement des opérations de nettoyage de la mémoire. Par conséquent, vous activez généralement ces mesures pour une utilisation spécifique. Par exemple, lors du développement ou du test d'applications, ou de la recherche de problèmes de performances des applications. Dans la plupart des cas, les mesures ne sont pas utilisées pour la gestion en temps réel des applications dans un environnement de production et elles sont désactivées par défaut.

Lorsque la propriété `introscope.agent.gcmonitor.enable` est définie sur `true` (valeur par défaut), vous pouvez afficher d'autres informations sur les pools de mémoires et sur les utilitaires de nettoyage de mémoire pour la machine virtuelle Java que vous surveillez.

Mesures liées au pool de mémoires

Les mesures liées au pool de mémoires sont les suivantes :

- **Amount of Space Used (bytes) (Quantité d'espace utilisé (octets))**

Affiche la quantité d'espace mémoire utilisé. Cette valeur inclut la taille de tous les objets présents dans le pool, accessibles comme inaccessibles.

Dans des circonstances normales, la mesure augmente progressivement. Elle peut diminuer lorsque le nettoyage de la mémoire est terminé et que de la mémoire est réclamée.

Un pic temporaire suivi d'une valeur normale peut signaler la présence d'un problème de mémoire.

En cas d'augmentation rapide, la mesure peut atteindre la limite maximum de mémoire, ce qui produit des exceptions de mémoire insuffisante. Afin d'éviter que ce problème ne survienne, définissez la taille maximum du pool de mémoires sur une valeur inférieure.

- **Current Capacity (bytes) (Capacité actuelle (octets))**

Quantité de mémoire allouée pour ce pool et pour tous les segments de mémoire de la machine virtuelle Java. Cette quantité de mémoire est garantie pour la machine virtuelle Java à utiliser.

NOTE

L'ajout des mesures Current Capacity à partir des segments de mémoire équivaut presque à la mesure Bytes Total (reportez-vous aux [mesures GC Heap](#)). Si la quantité d'espace atteint la capacité actuelle, des exceptions de mémoire insuffisante sont levées. Afin d'éviter que ce problème ne survienne, planifiez la quantité d'espace nécessaire pour la gestion des opérations quotidiennes et des pics inattendus.

- **Growth Rate (Taux de croissance)**

Taux moyen de croissance de la mémoire utilisée, exprimée en octets/seconde ; dans un pool de mémoires, cette valeur est exprimée en octets par seconde au cours de la dernière minute. Cette mesure agrégée est calculée comme suit :

- Via la recherche de la dernière valeur du point de données, en octets (lastValue).
- Via la recherche de la première valeur du point de données, en octets (firstValue).

Cette mesure inclut également l'espace dans l'intervalle de 1 minute le plus récent. Le taux est calculé à l'aide de la formule suivante :

```
(lastValue - firstValue) / 60
```

Cette mesure s'accroît lentement, reste stable ou diminue si la mémoire inutilisée est renvoyée au pool.

Une augmentation importante de cette mesure dans un délai de 15 minutes ou plus indique que la mémoire n'est pas recyclée après le nettoyage de la mémoire. Ce comportement traduit une éventuelle fuite de mémoire. Un contrôle plus approfondi est nécessaire.

- **Maximum Capacity (bytes) (Capacité maximum (octets))**

Quantité maximum de mémoire (en octets) utilisée pour la gestion de la mémoire. La disponibilité de cette quantité de mémoire n'est pas garantie pour la gestion de mémoire si cette quantité dépasse la capacité actuelle (quantité de mémoire allouée).

Cette mesure est constante au fil du temps.

- **Memory Type (Type de mémoire)**

Type de mémoire : peut correspondre à l'une des valeurs suivantes :

- Heap (Segment de mémoire)
- Non-Heap (Autre qu'un segment de mémoire)

- **Percentage of Maximum Capacity Currently Used (Pourcentage de capacité maximum actuellement utilisée)**

Affiche le pourcentage d'utilisation actuelle de la mémoire (au-dessus de la quantité maximum). Cette mesure indique le pourcentage de mémoire utilisée au fil du temps.

Cette mesure s'accroît lentement, reste stable ou diminue si la mémoire inutilisée est renvoyée au pool.

Si la mesure dépasse 70 à 80 %, définissez la mémoire maximum sur une valeur plus élevée et optimale.

Système de fichiers, Sockets, UDP

Les mesures de type Réponses par intervalle, Système de fichiers, Socket et UDP sont des mesures liées au débit de données. Elles sont exprimées en octets par seconde :

Système de fichiers

- Taux de sortie des fichiers (octets par seconde)
- Taux d'entrée des fichiers (octets par seconde)

UDP (User Datagram Protocol)

- Bande passante de sortie (octets par seconde)
- Bande passante d'entrée (octets par seconde)

Sockets (nombre total et informations spécifiques de l'hôte/port)

- Bande passante de sortie (octets par seconde)
- Bande passante d'entrée (octets par seconde)

Un grand nombre de mesures liées au port indique que les mesures liées au taux de socket doivent être désactivées, car cette situation traduit probablement un problème d'explosion des mesures.

Nombre d'instances

Les mesures liées au nombre d'instances calculent le nombre d'instances d'objet d'une classe particulière au niveau du segment de mémoire.

- Nombre approximatif d'instances par nom de package et de classe

Mesures de prise en charge des clusters

Un cluster intègre les ressources de deux unités informatiques ou plus (qui autrement pourraient fonctionner séparément) dans un but commun. La création de clusters permet à un gestionnaire d'entreprise de gérer d'autres gestionnaires d'entreprise ou de servir de gestionnaire des gestionnaires (MOM, Manager of Managers). APM mesure la capacité de prise en charge des applications en mesurant les performances des différents composants de l'application et fournit les mesures suivantes :

Les données suivantes sont signalées pour l'ordinateur hébergeant le gestionnaire d'entreprise et pour chaque ordinateur avec des méthodes instrumentées.

- Hôte d'EM : nom d'hôte du serveur du gestionnaire d'entreprise
- Port d'EM : port du gestionnaire d'entreprise auquel l'agent est connecté
- Java Version

Les mesures de prise en charge affichent des informations sur le gestionnaire d'entreprise plutôt que sur l'application qu'il surveille. Ces mesures s'affichent dans l'arborescence Investigator, sous :

Hôte de mesure personnalisé (virtuel)

Custom Metric Process (Virtual)

Custom Metric Agent (Virtual)(SuperDomain)

Sous ce niveau, les mesures de prise en charge sont organisées dans cette hiérarchie. Les définitions de certaines de ces mesures suivent la liste.

Noeud de l'agent

Les agents ont la hiérarchie suivante :

```
<Host_Name>
  <Process_Name>
    <Agent_Name>
```

<Process_Name> et <Agent_Name> sont configurables dans IntroscopeAgent.profile.

Les mesures suivantes sont disponibles pour chaque `<Agent_Name>` :

- `ConnectionStatus`, avec l'une des valeurs suivantes :
 - 3 = déconnecté
 - 2 = connecté, lent ou aucune donnée
 - 1 = connecté
 - 0 = démonté
- `IsClamped`, avec l'une des valeurs suivantes :
 - 1 = limité
 - 0 = non limité

Remarque : Pour plus d'informations sur le verrouillage des mesures, reportez-vous à la section [Utilisation de la visionneuse des traces de transaction](#).

- Nombre de mesures
- Raw Metric Count

Outil de calcul de connectivité de l'agent

L'outil de calcul de connectivité de l'agent copie l'état de connectivité de l'agent à un emplacement fixe. Actuellement, l'état est stocké dans le dossier Collecteurs, mais lorsque l'agent se reconnecte à un autre collecteur, la mesure continue d'être collectée sous un autre dossier. Dans ce cas, l'outil de calcul de connectivité de l'agent copie tous les états du dossier Collecteurs vers le dossier MOM, un seul emplacement permanent.

NOTE

L'outil de calcul de connectivité de l'agent est désactivé par défaut et doit être activé par l'administrateur sur l'instance MOM et le redémarrage MOM en définissant la propriété `introscope.apm.calculator.agentconnectivity.enabled=true`.

L'outil de calcul génère les mesures suivantes dans `Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|<nom_agent>`:

- `Uptime` : valeur qui augmente régulièrement et qui est utile pour voir quand exactement l'agent se connecte. Elle tombe à 0 lorsque l'agent se déconnecte.
- `Metrics` : nombre de mesures brutes fournies par un agent.
- `ConnectionState` : connectivité de l'agent. Il peut s'agir de l'une des valeurs entières suivantes :
 - 4 - Alive : l'agent est connecté et envoie des mesures.
 - 5 - Stopped : l'agent a été arrêté de manière appropriée.
 - 6 - Reconnected : l'agent a basculé sur un autre collecteur.
 - 7 - Interrupted : l'agent ne s'est pas déconnecté de manière appropriée, mais APM ne reçoit aucune mesure de sa part.
 - 8 - AgedOut : l'agent est arrêté ou interrompu pendant plus de 24 heures.

L'outil de calcul génère également un bref récapitulatif du nombre d'agents pour chaque état de connexion sous `Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Agents|Agent States`.

Mesures de l'agent

<Agent_Name> | ErrorSnapshot Events Per Interval

Nombre total d'événements de cliché d'erreur par agent par intervalle.

Nœud Gestionnaire d'entreprise

Sous le nœud Gestionnaire d'entreprise, les mesures de prise en charge suivantes sont disponibles :

- Host
- Name (nom)
- Overall Capacity (%)
- Port
- UC
 - EM CPU Used (%)
- Configuration
 - Agent Clusters Metric Load
 - Number of Agent Clusters
 - Number of Map Entity Metric Groupings
 - Number of Metric Groupings
- Connexions
 - Disallowed Agents Clamped : indique si le nombre maximum d'agents interdits, connecté au MOM, au collecteur ou au gestionnaire d'entreprise autonome spécifié, a été dépassé. Si la valeur est 0, la limite n'est pas appliquée. Si la valeur est 1, la limite est appliquée.
 - EM Historical Metric Clamped
 - EM Live Metric Clamped
 - Mesure Max Number of Agent Connection Limit Exceeded Per Interval : indique si le nombre maximum d'agents, connectés au MOM, au collecteur ou au gestionnaire d'entreprise autonome, a été dépassé. Si la valeur est 0, la limite n'est pas appliquée. Si la valeur est 1, la limite est appliquée.
 - Metrics From External Agents : affiche le nombre de mesures EM générées par les agents virtuels EM.
 - Metrics Queued (%)
 - Number of Agents
 - Number of Applications : nombre d'applications d'agent signalant actuellement des données.
 - Number of Disallowed Agents : affiche le nombre d'agents interdits connectés au MOM, au collecteur ou au gestionnaire d'entreprise autonome spécifié. Les agents connectés en mode passif n'envoient aucune donnée de mesure.
 - Number of Events Processed
 - Number of Events Processed Limit Exceeded
 - Number of Metrics Handled : nombre de mesures entrantes traitées par intervalle de 15 secondes. Ce nombre varie, mais il peut être identique à la valeur de la mesure Number of Metrics. Une valeur inférieure à celle de Number of Metrics indique que le gestionnaire d'entreprise peut être surchargé et ne traite pas les données entrantes assez rapidement.
 - Number of Metrics : affiche la charge totale des mesures sur le gestionnaire d'entreprise.
 - Number of Unique Applications
 - Number of Workstations

Noeud Data Store (Référentiel de données)

Sous le nœud Data Store, les mesures suivantes sont disponibles :

- SmartStor
 - Metrics Appended To Query Per Interval
 - Metrics Converted From Spool to Query Per Interval
 - SmartStor Disk Usage (mb)
 - MetaData
 - Agent Metric Cache Size
Nombre de mesures d'agent dans le cache.
 - Tasks

- Converting Spool To Data
- Data Append
- Reperiodizing
- Transactions
 - TT Database Disk usage (mb)
- Volume Space Free
 - Baseline Volume Free (mb)
 - Log Volume Free (mb)
 - SmartStor Archive Volume Free (mb)
 - SmartStor Data Volume Free (mb)
 - Traces Volume Free (mb)

Sous-noeud Intégrité

- CPU Capacity (%) : pourcentage d'UC utilisé. Par exemple, 300 % signifie que trois noyaux de processeur sont entièrement utilisés.
- GC Capacity (%)
- Harvest Capacity (%)
- Heap Capacity (%)
- Incoming Data Capacity (%)
- SmartStor Capacity (%)

Sous-noeud Internal (Interne)

Les mesures suivantes s'affichent sous le sous-noeud Internal :

- Number of Connection Tickets
- Number of Dependent Calculator Input Metrics
Nombre total de mesures utilisées en tant qu'entrées dans les outils de calcul dépendants. Les outils de calcul dépendants utilisent en tant qu'entrées des valeurs de mesures produites par d'autres outils de calcul. Ce nombre fait référence à toutes les mesures envoyées aux outils de calcul dépendants, et pas uniquement aux mesures produites par d'autres outils de calcul.
- Number of Non-Dependent Calculator Input Metrics
Nombre total de mesures utilisées en tant qu'entrées dans les outils de calcul non dépendants. Les outils de calcul non dépendants n'utilisent aucune valeur de mesures produite par d'autres outils de calcul. Par exemple, les mesures provenant des agents.
- Number of Metric Data Queries per Interval
- Number of Queued Async Data Queries
- Number of Registered Async Data Queries
- Number of Registered Async MG Queries
- Number of Registered Async Path Queries
- Number of Transaction Trace Action Sessions
- Number of Transaction Trace Session Clients
- AlertID
- Query memory in transit (bytes)
- Alertes
 - *<nom_module_gestion>*
 - Agent Connection Status
 - Number of Evaluated Metrics
 - Total Number of Evaluated Metrics

Nombre total de mesures évaluées pour toutes les alertes.

- Calculatrices

- Total Number of Evaluated Metrics

Nombre total de mesures évaluées pour tous les outils de calcul. Cette mesure est la somme de Number of Dependent Calculator Input Metrics et de Number of Non Dependent Calculator Input Metrics. Lorsque ce nombre est élevé, le gestionnaire d'entreprise effectue de nombreux calculs en temps réel, ce qui peut surcharger les ressources d'UC.

- `<nom_outil_calcul>` | Total Number of Evaluated Metrics
Nombre total de mesures évaluées pour un outil de calcul.

NOTE

Cette mesure s'affiche dans Investigator uniquement lorsque l'outil de calcul est défini.

- GC Heap

- Collecteurs

- `<nom_collecteur>`

- Collection Count Per Interval
 - GC Duration (ms)

- Pools

- Harvest

- Alert Action Processing Time (ms)

Temps pris par le gestionnaire d'entreprise à traiter toutes les actions d'alerte.

- Calculator Queries Wait Time (ms)

Temps écoulé avant que le thread de requête de l'outil de calcul ne termine sa tâche actuelle, y compris l'attente de la fin de la boucle de requête hors outil de calcul. Le traitement de la nouvelle requête de l'outil de calcul démarre à la fin de toutes les livraisons de créneaux hors outil de calcul précédentes aux clients.

- Non Calculator Queries Delivery Time (ms)

Temps pris par le gestionnaire d'entreprise pour exécuter et livrer des requêtes hors outil de calcul à tous les clients demandeurs dans un créneau.

Une fois que toutes les requêtes d'outil de calcul sont exécutées, le gestionnaire d'entreprise exécute des requêtes hors outil de calcul et envoie les résultats à tous les clients qui les ont demandés.

- Non Calculator Queries Excess Time (ms)

Temps d'attente excessif pour le traitement des requêtes hors outil de calcul au-delà d'un créneau.

Les clients envoient des requêtes hors outil de calcul au gestionnaire d'entreprise, qui renvoie les résultats. Si ce processus ne se termine pas dans un créneau précis, il est retenté jusqu'à ce qu'il soit terminé. Cette mesure indique la durée au-delà de laquelle le traitement des requêtes hors outil de calcul s'est étendu.

- Metrics From All Agents

Nombre total de mesures uniques générées par tous les agents connectés qui ont envoyé des données au cours du dernier créneau. Ce nombre n'inclut pas les mesures historiques. Les paramètres de clamp n'affectent pas ce nombre.

- Spooling Data File Write Time (ms)

Temps pris par le gestionnaire d'entreprise pour écrire les données collectées dans le fichier de spooling (.spool) dans un créneau.

- Spooling Preparation Time (ms)

Temps pris par le gestionnaire d'entreprise pour préparer l'écriture des données collectées dans le fichier de spooling (.spool) dans un créneau.

- Management Module Calculators

- Total Number of Evaluated Metrics

Nombre de mesures utilisées en tant qu'entrées dans les outils de calcul du module de gestion.

- Messaging

- Active Incoming Threads
- Active Outgoing Threads
- Corrupted Messages Per Interval
- Post Offices
 - *<Nom_bureau_poste>*
 - Number of Mailboxes
 - Queued Messages
- Groupe de mesures
 - Metric Matches Per Interval
Nombre total de mesures évaluées dans toutes les requêtes au cours du dernier créneau.
 - Queued Queries Per Interval
Nombre de requêtes en attente de traitement dans l'intervalle de cycle de collecte. La valeur est généralement de zéro après le démarrage.
- Query
 - Cache Queries Duration (ms)
 - Cache Queries Per Interval
 - SmartStor Queries Duration (ms)
 - SmartStor Queries Per Interval
- Threads
 - *<nom_thread>*
 - Blocked Count
 - Blocked Time (ms)
 - CPU Time (ms)
 - User Time (ms)
 - Nombre d'attentes
 - Wait Time (ms)

Sous-noeud Problèmes

Modules de gestion

- Nombre d'avertissements

Sous-noeud Tâches

Harvest Duration (ms)

SmartStor Duration (ms)

Mesures de collecte

Harvest Capacity

La mesure Harvest Capacity affiche le pourcentage de temps nécessaire pour la collecte de données dans un créneau de 15 secondes. Par exemple, si la collecte de données prend 15 secondes, la valeur de la mesure sera de 100. Investigator affiche cette mesure à l'emplacement suivant :

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Health | Harvest Capacity (ms)
```

Harvest Duration

La mesure Harvest Duration indique la durée en millisecondes (pendant un créneau de 15 secondes) consacrée à la collecte de données. Cette mesure est généralement un bon indicateur permettant de déterminer si le gestionnaire

d'entreprise arrive à traiter la charge de travail actuelle. Cette mesure est disponible à l'emplacement suivant dans l'arborescence Investigator :

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Tasks | Harvest Duration (ms)
```

Incoming Data Capacity (%)

Capacité du gestionnaire d'entreprise à gérer les données entrantes. La mesure est calculée en multipliant la capacité totale de mesure par 2. Par exemple, si 150 000 mesures figurent dans la file d'attente en attente de traitement et que le gestionnaire d'entreprise peut gérer 300 000 mesures, la valeur d'Incoming Data Capacity est de 25 %.

Cette mesure est disponible à l'emplacement suivant dans l'arborescence du navigateur de mesures :

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Health | Incoming Data Capacity (%)
```

Mesures de collecteur

Les mesures suivantes sont des mesures de collecteur.

- **EM Live Metric Clamped**

Indique si le nombre de mesures dynamiques traitées par le gestionnaire d'entreprise est inférieur ou supérieur à la limite maximum spécifiée dans la propriété `introscope.enterprisemanager.metrics.live.limit` pour les verrouillages du gestionnaire d'entreprise. La valeur de la mesure est 0 si le nombre de mesures dynamiques pour le gestionnaire d'entreprise est inférieur à la limite spécifiée. La valeur de la mesure est 1 si le nombre de mesures dynamiques pour le gestionnaire d'entreprise est supérieur à la limite spécifiée.

NOTE

Vous pouvez définir la limite pour la propriété `introscope.enterprisemanager.metrics.live.limit` dans le fichier `apm-events-thresholds-config.xml`. Le fichier `apm-events-thresholds-config.xml` se trouve dans le répertoire `<répertoire_base_EM>\config`.

- **EM Historical Metric Clamped**

Indique si le nombre de mesures dynamiques traitées par le gestionnaire d'entreprise est inférieur ou supérieur à la limite maximum spécifiée dans la propriété `introscope.enterprisemanager.metrics.historical.limit` pour les verrouillages du gestionnaire d'entreprise. La valeur de la mesure est 0 si le nombre de mesures dynamiques pour le gestionnaire d'entreprise est inférieur à la limite spécifiée. La valeur de la mesure est 1 si le nombre de mesures dynamiques pour le gestionnaire d'entreprise est supérieur à la limite spécifiée.

NOTE

Vous pouvez définir la limite pour la propriété `introscope.enterprisemanager.metrics.historical.limit` dans le fichier `apm-events-thresholds-config.xml`. Le fichier `apm-events-thresholds-config.xml` se trouve dans le répertoire `<répertoire_base_EM>\config`.

- **Max Number of Agent Connection Limit Exceeded Per Interval**

Nombre de fois que la limite définie dans la propriété `introscope.enterprisemanager.agent.connection.limit` a été dépassée pendant un intervalle spécifique.

NOTE

Vous pouvez définir la limite pour la propriété `introscope.enterprisemanager.agent.connection.limit` dans le fichier `apm-events-thresholds-config.xml`. Le fichier `apm-events-thresholds-config.xml` se trouve dans le répertoire `<répertoire_base_EM>\config`.

- **Number of Events Processed**

Indique le nombre total d'événements tels que les traces de transaction et les erreurs que le gestionnaire d'entreprise traite dans chaque intervalle.

- **Number of Events Processed Limit Exceeded**

Nombre de fois que la limite définie dans la propriété `introscope.enterprisemanager.events.limit` a été dépassée pendant un intervalle spécifique.

NOTE

Vous pouvez définir la limite pour la propriété `introscope.enterprisemanager.events.limit` dans le fichier `apm-events-thresholds-config.xml`. Le fichier `apm-events-thresholds-config.xml` se trouve dans le répertoire `<répertoire_base_EM>\config`.

Mesures relatives aux requêtes

Data Points Retrieved From Disk Per Interval

Nombre de points de données récupérés à partir de SmartStor par intervalle.

Data Points Returned Per Interval

Nombre de points de données renvoyés par le gestionnaire d'entreprise aux clients par intervalle.

Metrics Read From Disk Per Interval

Nombre de mesures lues à partir de SmartStor par intervalle.

Metrics Returned Per Interval

Nombre de mesures uniques renvoyées par le gestionnaire d'entreprise aux clients.

Queries Exceeding Max Data Points Read From Disk Limit Per Interval

Indique si le nombre maximum de points de données de mesure spécifiés dans la propriété `introscope.enterprisemanager.query.datapointlimit` qu'un gestionnaire d'entreprise renvoie pour une requête par lot particulière est dépassé. Si le nombre de points de données de mesure que le gestionnaire d'entreprise renvoie est inférieur à la limite spécifiée, la valeur de la mesure est 0. Si le nombre de points de données de mesure que le gestionnaire d'entreprise renvoie est supérieur à la limite spécifiée, la valeur de la mesure est 1.

NOTE

Définissez la limite pour la propriété

```
introscope.enterprisemanager.query.datapointlimit
```

dans le fichier

```
IntroscopeEnterpriseManager.properties
```

. Localisez le fichier

```
IntroscopeEnterpriseManager.properties
```

dans le répertoire

```
<EM_Home>\config
```

.

Queries Exceeding Max Data Points Returned Limit Per Interval

Indique si le nombre maximum de points de données de mesure spécifiés dans la propriété `queryintroscope.enterprisemanager.query.returneddatapointlimit` qu'un gestionnaire d'entreprise renvoie pour une requête par lot particulière est dépassé. Si le nombre de points de données de mesure que le gestionnaire d'entreprise renvoie est inférieur à la limite spécifiée, la valeur de la mesure est 0. Si le nombre de points de données de mesure que le gestionnaire d'entreprise renvoie est supérieur à la limite spécifiée, la valeur de la mesure est 1.

NOTE

Définissez la limite pour la propriété

```
introscope.enterprisemanager.query.returneddatapointlimit
```

dans le fichier

```
IntroscopeEnterpriseManager.properties
```

. Le fichier

```
IntroscopeEnterpriseManager.properties
```

se trouve dans le répertoire

```
<EM_Home>\config
```

.

Mesure Converting Spool To Data

La mesure Converting Spool to Data permet de suivre si la tâche de conversion du spool en données est en cours d'exécution. Cette mesure est disponible à l'emplacement suivant dans l'arborescence Investigator :

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Data Store | SmartStor | Tasks | Converting Spool to Data
```

Si la valeur de cette mesure est 1 pendant plus de 10 minutes par heure, elle indique que la réorganisation du fichier de spool SmartStor prend trop de temps.

Mesure Overall Capacity (%)

La mesure Overall Capacity (%) du gestionnaire d'entreprise estime le pourcentage de capacité consommée par le gestionnaire d'entreprise. Cette mesure est disponible à l'emplacement suivant dans l'arborescence Investigator :

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager: Overall Capacity (%)
```

La mesure Overall Capacity (%) est une valeur maximum des mesures CPU Capacity (%), Harvest Capacity (%), Heap Capacity (%), SmartStor Capacity (%), Incoming Data Capacity (%) et GC Capacity (%).

Mesure SmartStor Capacity (%)

La mesure SmartStor Capacity (%) affiche le pourcentage de temps nécessaire pour le processus d'écriture de SmartStor dans un créneau de 15 secondes (où 15 secondes est égal à 100 %).

Cette mesure est disponible à l'emplacement suivant dans l'arborescence Investigator :

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Health | SmartStor Capacity (%)
```

Mesure Heap Capacity (%)

La mesure Heap Capacity (%) est déterminée par le pourcentage de segment de mémoire actuellement utilisé par la machine virtuelle Java (basé sur la mesure GC Heap: In Use Post GC (Mb)).

Mesure Number of Agents

Cette mesure affiche le nombre d'agents actuellement connectés. Elle est disponible à l'emplacement suivant :

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Connections
```

Number of Metrics

Cette mesure affiche la charge totale des mesures sur le gestionnaire d'entreprise. Elle est disponible à l'emplacement suivant :

Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Connections

Mesures de prise en charge du triage assisté

APM fournit des mesures de prise en charge du triage assisté en mesurant les performances des différents composants de l'application de triage assisté. Le gestionnaire d'entreprise génère et collecte les mesures relatives aux composants du tri assisté. Ces mesures de prise en charge sont utiles pour évaluer l'intégrité du gestionnaire d'entreprise.

Note : pour plus d'informations sur le triage assisté, reportez-vous à la section [Surveillance des problèmes et anomalies relatifs au triage assisté](#).

Surveillance des performances des composants de triage assisté

Les mesures de prise en charge du triage assisté permettent de surveiller les performances des différents composants du triage assisté.

D'autres mesures peuvent s'afficher, par exemple :

- Mesures pour les événements d'analyse différentielle créés lorsque l'intensité d'écart dépasse une certaine valeur
- Mesures des événements d'erreur créés lorsque le triage assisté reçoit une erreur de clic ou de blocage

Procédez comme suit :

1. Dans APM Team Center, cliquez sur le lien **WebView**.
2. Cliquez sur l'onglet **INVESTIGATOR**.
3. Développez le nœud du domaine qui vous intéresse.
4. Accédez au nœud **Enterprise Manager, Assisted Triage**.
5. Développez un nœud qui vous intéresse, par exemple **Event Generator**.

Les mesures de prise en charge pour le générateur d'événements s'affichent. Par exemple :

DA : Average Processing Time (ms)

Cette mesure fournit le temps de traitement moyen, en millisecondes, des événements d'analyse différentielle (DA) reçus par le processeur d'événements de triage assisté.

Générateur d'événements

Le triage assisté utilise des générateurs d'événements qui génèrent des événements et dépendent de différents types de sources. Par exemple, les alertes APM sont une source et sont définies par les administrateurs dans les modules de gestion. Voici quelques exemples d'événements :

- Événements d'analyse différentielle créés lorsque l'intensité d'écart dépasse une certaine valeur.
- Événements d'erreur et de blocage

APM fournit les mesures suivantes pour la surveillance du composant générateur d'événements. Les mesures suivantes s'affichent sous le nœud Event Generator dans Investigator :

Enterprise Manager | Assisted Triage | Event Generator | <Metric>

- **DA : Average Processing Time (ms)**
Fournit le temps de traitement moyen, en millisecondes, des événements d'analyse différentielle (DA) reçus par le processeur d'événements de triage assisté.
- **DA : Raw States Received Per Interval**
Fournit le nombre d'événements d'analyse différentielle (DA) reçus par le processeur d'événements de triage assisté par intervalle.
- **DA : Events Sent Per Interval**

Fournit le nombre d'événements d'analyse différentielle (DA) agrégés qui sont renvoyés au processeur d'événements DA.

- **Alert : Average Processing Time (ms)**
Fournit le temps de traitement moyen, en millisecondes, de tous les événements d'alerte traités par le générateur d'alertes.
- **Alert : Raw Alert States Received Per Interval**
Fournit le nombre d'alertes reçues par intervalle par le générateur d'alertes.
- **Alert : Events Sent Per Interval**
Fournit le nombre d'événements d'alerte agrégés qui sont renvoyés aux processeurs d'événements de triage assisté.

Mesures de prise en charge principales

Les mesures de prise en charge permettent d'évaluer les problèmes de performances impliquant le gestionnaire d'entreprise. Les cinq mesures de prise en charge suivantes entraînent généralement des problèmes de performances dans divers environnements APM.

SmartStor Duration (ms)

Nom du chemin de la mesure : `SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Enterprise Manager|Tasks:Smartstor Duration (ms)`

Description : temps nécessaire au gestionnaire d'entreprise ou au collecteur pour enregistrer les données collectées sur le disque.

Produit : APM

Composant : gestionnaire d'entreprise

Version : toutes les versions prises en charge

Impact : si cette mesure dépasse 1 seconde, le gestionnaire d'entreprise ou les collecteurs rencontrent peut-être des problèmes de performances liés aux E/S. Si la mesure est supérieure à 3,5 secondes, d'autres tâches dans le gestionnaire d'entreprise ou le collecteur peuvent être retardées.

Configuration : configurez un disque distinct (contrôleur) pour les données SmartStor en modifiant la propriété `introscope.enterprisemanager.smartstor.directory` dans le fichier `config/IntroscopeEnterpriseManager.properties`.

Plage : Sain : < 1 000 ms, Danger : > 3 500 ms, Danger extrême : > 15 s.

Correction : chaque base de données SmartStor doit résider sur un disque physique dédié distinct. Nous recommandons fortement d'utiliser un disque SSD avec une vitesse de lecture/écriture de 220 Mbits/s pour une taille de bloc de 4 Ko.

Harvest Duration (ms)

Nom du chemin de la mesure : `SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Enterprise Manager|Tasks:Harvest Duration (ms)`

Description : temps nécessaire au gestionnaire d'entreprise ou au collecteur pour agréger les mesures d'intervalle de 15 secondes en vue de leur écriture dans la base de données SmartStor.

Produit : APM

Composant : gestionnaire d'entreprise

Version : toutes les versions prises en charge

Impact : si cette mesure dépasse 1 seconde, le gestionnaire d'entreprise sur les MOM ou les collecteurs rencontrent peut-être des problèmes de performances. Vérifiez les valeurs pour les mesures `Enterprise Manager|Internal|`

Calculators:Total Number of Evaluated Metrics et Enterprise Manager|Internal:Number of [Non] Dependent Calculator Input Metric . Si les valeurs sont supérieures à 3,5 secondes, d'autres tâches dans le gestionnaire d'entreprise ou le collecteur peuvent être retardées.

Configuration :

- Vérifiez les nombres de mesures suivants pour déterminer si le nombre de mesures surcharge le gestionnaire d'entreprise :
 - SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Enterprise Manager|Connections:Number of Metrics
 - Enterprise Manager|Internal|Harvest: Metrics From All Agents
- Réduisez le nombre de mesures dans les alertes et les outils de calcul.

Plage : Sain : < 1 000 ms, Danger : > 3 500 ms, Danger extrême : > 15 s.

Correction : réduisez les composants suivants :

- Mesures dans les alertes et les outils de calcul
- Requêtes CLW
- Connexions à la station de travail

GC Duration (ms)

Nom du chemin de la mesure : SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Enterprise Manager|ApplicationTriageMap|Ontology engine:Average Process Time (ms)

Description : temps que la machine virtuelle Java passe à libérer de la mémoire inutilisée (nettoyage de la mémoire) dans un intervalle de 15 secondes.

Produit : APM

Composant : gestionnaire d'entreprise

Version : toutes les versions prises en charge

Impact : si cette mesure dépasse 1 seconde, le gestionnaire d'entreprise sur les MOM ou les collecteurs rencontrent peut-être des problèmes de performances. Vous pouvez augmenter la taille du segment de mémoire et modifier les paramètres ou les algorithmes de nettoyage de la mémoire (GC).

Plage : Sain : < 1 000 ms, Danger : > 3 500 ms.

Correction : contactez le service de support de CA.

Ontology Engine:Average Process Time (ms)

Nom du chemin de la mesure : SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Enterprise Manager|ApplicationTriageMap|Ontology engine:Average Process Time (ms)

Description : temps nécessaire au gestionnaire d'entreprise pour traiter les modifications apportées à la carte topologique dans un intervalle de 15 secondes.

Produit : APM

Composant : gestionnaire d'entreprise

Version : toutes les versions prises en charge

Impact : si cette mesure dépasse 1 seconde, le gestionnaire d'entreprise sur les MOM ou les collecteurs rencontrent peut-être des problèmes de performances.

Configuration : N/D

Plage : Sain : < 1 000 ms, Danger : > 3 500 ms.

Correction : contactez le service de support de CA.

Surveillance des performances de CA APM à l'aide de mesures de prise en charge

Surveillez les performances du déploiement d'APM à l'aide des outils de surveillance des performances d'APM. Pour surveiller efficacement votre environnement de production, il est important que vos gestionnaires d'entreprise (EM) soient dans un état sain.

CA APM fournit les outils suivants pour vous permettre de détecter les problèmes et d'empêcher des modifications inattendues de compromettre votre environnement de surveillance :

- Mesures de prise en charge
- Alertes

Surveillance des performances à l'aide des mesures de prise en charge du gestionnaire d'entreprise

Toutes les 15 secondes, le gestionnaire d'entreprise collecte et enregistre des mesures d'intégrité le concernant. Vous pouvez afficher ces mesures pour résoudre les problèmes de performances du gestionnaire d'entreprise en examinant les sources suivantes :

- Arborescence du navigateur de mesures Investigator
- Fichier journal
- Onglet Présentation du gestionnaire d'entreprise

Affichage des mesures de prise en charge dans l'arborescence du navigateur de mesures

Pour un gestionnaire d'entreprise autonome ou un MOM, les mesures de prise en charge s'affichent dans l'arborescence du navigateur de mesures, sous le niveau supérieur **SuperDomain** :

```
Custom Metric Host (Virtual)
  Custom Metric Process (Virtual)
    Custom Metric Agent (Virtual) (SuperDomain)
      Enterprise Manager
```

Dans un environnement en cluster, les mesures de prise en charge du collecteur ont un chemin de mesure identique, mais le niveau d'agent de mesure personnalisée inclut le nom de l'ordinateur et le port du collecteur.

L'exemple suivant présente une arborescence Investigator doté d'un MOM et d'un collecteur :

```
Custom Metric Host (Virtual)
  Custom Metric Process (Virtual)
    Custom Metric Agent (Virtual) (SuperDomain)
      Enterprise Manager
    Custom Metric Agent (Virtual) (Collector1@5001) (SuperDomain)
      Enterprise Manager
```

Affichage des mesures de prise en charge dans le fichier journal

Par défaut, les gestionnaires d'entreprise enregistrent les mesures de prise en charge dans un fichier journal nommé `perflog.txt`. Les mesures de prise en charge sont générées toutes les 15 secondes. L'emplacement par défaut de ce fichier est le répertoire `<répertoire_base_EM>/logs`.

Par défaut, `perflog.txt` est généré en mode compressé. Les valeurs sont séparées par des virgules avec des en-têtes de colonne. Dans ce format, `perflog.txt` peut être facilement importé dans une feuille de calcul à des fins d'analyse.

La désactivation du mode compressé entraîne l'écriture de `perflog.txt` par le gestionnaire d'entreprise dans un format plus détaillé, destiné à une meilleure lisibilité humaine.

Procédez comme suit :

1. Ouvrez le fichier `IntroscopeEnterpriseManager.properties`.
2. Définissez les valeurs de configuration suivantes :
 - `introscope.enterprisemanager.performance.compressed=false`
 - `log4j.logger.Manager.Performance=DEBUG, performance, logfile`
3. Enregistrez et fermez le fichier `IntroscopeEnterpriseManager.properties`.

Affichage des mesures de prise en charge dans l'onglet Présentation du gestionnaire d'entreprise

Pour afficher des informations récapitulatives sur les mesures de prise en charge d'un gestionnaire d'entreprise, sélectionnez le dossier Gestionnaire d'entreprise dans l'arborescence du navigateur de mesures. Ces informations incluent un onglet Présentation, qui affiche des graphiques illustrant les mesures de prise en charge les plus importantes dans une vue unique. L'onglet Présentation du gestionnaire d'entreprise est un outil utile pour une analyse rapide de la charge du gestionnaire d'entreprise et de l'utilisation des ressources.

Exécution d'un contrôle de l'intégrité des performances du cluster APM

En tant qu'administrateur, utilisez le fichier `perflog.txt` pour révéler les problèmes d'intégrité courants qui affectent les collecteurs d'un cluster. Le contrôle de l'intégrité des performances standard comprend les étapes suivantes :

- **Vérification de la taille de la file d'attente des messages**
- **Vérification de la taille maximum du segment de mémoire**
- Analyse

NOTE

Pour un contrôle de l'intégrité complet de votre environnement de cluster, contactez CA Services.

Vérification de la taille de la file d'attente des messages

Procédez comme suit :

1. Ouvrez le fichier `IntroscopeEnterpriseManagerSupport.log` et recherchez `transport.outgoingMessageQueueSize`.

NOTE

Si le fichier journal ne contient aucune entrée pour cette mesure, la taille de la file d'attente de messages par défaut est de 3 000.

2. Pour améliorer le débit de la file d'attente de messages entre le MOM et les collecteurs, ouvrez les fichiers `IntroscopeEnterpriseManager.properties` pour le MOM et tous les collecteurs :
 - a. Augmentez la valeur de la propriété `transport.outgoingMessageQueueSize` à 6000.
 - b. Définissez la valeur de `transport.override.isengard.high.concurrency.pool.min.size` sur 10.
 - c. Définissez `transport.override.isengard.high.concurrency.pool.max.size` sur 10.

WARNING

L'augmentation de la file d'attente de messages et de la taille du pool au-delà d'un certain point peut entraîner la consommation par Introscope de ressources supplémentaires. Ne définissez pas

`transport.outgoingMessageQueueSize` sur une valeur supérieure à 9000. La taille minimum et maximum du pool ne doit pas dépasser 20 personnes.

3. Redémarrez tous les gestionnaires d'entreprise.

Vérification de la taille maximum du segment de mémoire

Procédez comme suit :

1. Dans les paramètres de démarrage de la machine virtuelle Java, vérifiez que la taille de segment de mémoire initiale (`-Xms`) et la taille de segment de mémoire maximum (`-Xmx`) correspondent pour le MOM et tous les collecteurs. Ces valeurs doivent être aussi élevées que possible compte tenu de la machine virtuelle Java déployée et de la RAM disponible. Par exemple, pour un gestionnaire d'entreprise qui s'exécute sur une machine virtuelle Java 32 bits, la limite de segment de mémoire maximum est de 1,5 Go sous Windows ou de 2 Go sous Linux.

NOTE

Si le gestionnaire d'entreprise s'exécute sur une machine virtuelle Java 64 bits, la taille maximum du segment de mémoire est limitée uniquement par la quantité de RAM disponible.

2. Pour définir la taille du segment de mémoire, ouvrez le fichier `Introscope_Enterprise_Manager.lax` dans le répertoire `<répertoire_base_EM>` et modifiez la propriété `lax.nl.java.option.additional`.

Exemple : dans cet exemple,

`-Xms`

et

`-Xmx`

sont tous deux définis sur 1024m.

```
lax.nl.java.option.additional=-Xms1024m -Xmx1024m
```

3. Redémarrez le gestionnaire d'entreprise.

Analyse de Perflog.xlsx

Pour effectuer une analyse supplémentaire dans Microsoft Excel, convertissez le fichier `perflog.txt` au format `.xlsx`.

Procédez comme suit :

1. Renommez le fichier `<répertoire_base_EM>/logs/perflog.txt` en `perflog.csv`.
2. Ouvrez `perflog.csv` avec Microsoft Excel et effectuez les étapes de formatage suivantes :
 - a. Sélectionnez la première ligne qui contient les mosaïques :
 - a. Cliquez avec le bouton droit de la souris sur la ligne et sélectionnez **Formater les cellules...**
 - b. Sélectionnez **Alignement**, puis **Renvoyer à la ligne**.
 - c. Sélectionnez **OK**.
 - b. Supprimez toutes les lignes au-dessus de la ligne contenant les mosaïques.
 - c. Sélectionnez **Afficher**, **Figer les volets**, puis **Figer la ligne supérieure**.
 - d. Sélectionnez la première ligne qui contient les mosaïques, puis sélectionnez **Données**, **Filtrer** pour ajouter des filtres aux colonnes.
 - e. Sélectionnez les valeurs des filtres et faites défiler le contenu de la fenêtre de filtre.
 - f. Cliquez sur **Fichier**, puis sélectionnez **Enregistrer sous** et enregistrez le fichier au format `.xlsx`.

Analysez le fichier converti à l'aide de filtres sur les colonnes de mesure de performances suivantes :

- **Total JVM Memory (colonne B)**

Indique la mémoire totale disponible pour la machine virtuelle Java. Si le segment de mémoire initial (`-Xms`) et le segment de mémoire maximum (`-Xmx`) sont égaux, la valeur reste relativement inchangée dans le temps. Cette

intégrité est due au fait que le segment de mémoire maximum est alloué immédiatement après le démarrage et non pas via la collecte de la machine virtuelle Java.

- **Total JVM Free Memory (colonne C)**

Indique la quantité de mémoire disponible de la machine virtuelle Java pendant un intervalle donné. Si la mémoire libre tombe à un nombre à deux chiffres ou moins sur le collecteur, augmentez la taille du segment de mémoire disponible pour la machine virtuelle Java. Ajoutez de la mémoire au serveur si nécessaire. Si vous avez déjà alloué suffisamment de mémoire à la machine virtuelle Java, examinez les autres colonnes de la feuille de calcul. Ce problème est rare sur un MOM.

- **Harvest Duration (colonne F)**

Indique la durée de la collecte. Cette mesure indique le temps que le collecteur passe à agréger les mesures d'intervalle de 15 secondes avant de les enregistrer dans la base de données SmartStor. Par exemple, si la durée de la collecte dépasse fréquemment 3 000 ms (3 secondes), le collecteur a probablement des difficultés à agréger les mesures d'intervalle entrant.

- **Smartstor Duration (colonne G)** Indique la durée SmartStor. Cette mesure indique le temps que le collecteur passe à écrire les données collectées sur le disque. Corrigez les valeurs supérieures à 5 000 ms (5 secondes).

NOTE

Nous vous recommandons d'utiliser un disque séparé sur un contrôleur dédié pour stocker les données SmartStor. Vérifiez l'emplacement du répertoire `/data` de SmartStor pour vous assurer que la base de données SmartStor ne partage pas le disque avec le gestionnaire d'entreprise. Vérifiez que la propriété `introscope.enterprisemanager.smartstor.dedicatedcontroller` est définie sur `true` dans le fichier `IntroscopeEnterpriseManager.properties`.

Mesures de prise en charge importantes du gestionnaire d'entreprise

Les mesures de prise en charge suivantes sont utiles pour prédire les tendances, détecter les problèmes et identifier les causes profondes des problèmes de capacité du gestionnaire d'entreprise. Chaque mesure est décrite avec des informations sur son utilisation.

NOTE

Informations complémentaires :

- [Mesures de prise en charge principales](#)

Harvest Duration

La mesure `Harvest Duration` indique la durée en millisecondes (pendant un créneau de 15 secondes) consacrée à la collecte de données. Cette mesure est généralement un bon indicateur permettant de déterminer si le gestionnaire d'entreprise arrive à traiter la charge de travail actuelle.

Étant donné que le temps d'exécution de l'outil de calcul est une composante majeure de la durée de la collecte, la mesure `Harvest Duration` est une estimation pertinente de l'utilisation de l'UC. Une valeur optimale de la mesure `Harvest Duration` est inférieure à 3 500 ms (3,5 secondes). Une valeur supérieure à 7 500 ms (7,5 secondes) indique que le gestionnaire d'entreprise ne dispose pas d'une capacité d'UC suffisante pour la charge de la mesure et de l'outil de calcul.

Vous pouvez afficher la mesure aux emplacements suivants :

- Arborescence du navigateur de mesures sous `Enterprise Manager | Tasks`
- `perflog.txt` sous `Performance.Harvest.HarvestDuration`

SmartStor Duration

La mesure `SmartStor Duration` indique le temps nécessaire à l'écriture des mesures reçues et générées au cours d'un créneau dans la base de données SmartStor.

La mesure `SmartStor Duration` est un indicateur des performances d'écriture d'E/S du disque SmartStor. Les valeurs incohérentes indiquent un conflit pour les ressources liées au disque. Des valeurs constamment élevées indiquent une bande passante d'écriture sur disque insuffisante pour la charge de mesure traitée.

Dans les conditions standard du gestionnaire d'entreprise, la valeur moyenne de `SmartStor Duration` doit être inférieure à 3 500 ms (3,5 secondes). La valeur de `SmartStor Duration` *doit* être inférieure à 15 000 ms (15 secondes). Une valeur de mesure supérieure à 15 secondes indique un gestionnaire d'entreprise lourdement surchargé.

Vous pouvez afficher la mesure aux emplacements suivants :

- Arborescence du navigateur de mesures sous Enterprise Manager | Tasks
- `perflog.txt` sous `Performance.SmartStor.Duration`

Number of Collector Metrics

La mesure `Number of Collector Metrics` indique le nombre total de mesures actuellement suivies dans un cluster. Cette mesure est la somme des valeurs de la mesure de prise en charge Enterprise Manager | Connections | `Number of Metrics` pour tous les collecteurs du cluster.

Vous pouvez afficher la mesure aux emplacements suivants :

- Arborescence du navigateur de mesures sous Enterprise Manager | MOM | Number of Collector Metrics
- `perflog.txt` sous `Performance.MOM.NumberOfCollectorMetrics`

Collector Metrics Received Per Interval

La mesure `Collector Metrics Received Per Interval` correspond à la somme des points de données de mesure de collecteur reçus par MOM chaque période de 15 secondes. Les points de données proviennent des sources suivantes :

- Abonnements aux mesures pour le compte des modules de gestion, par exemple, tableaux de bord, outils de calculs, alertes
- Requêtes générées par les clients, par exemple, requêtes Station de travail et CLW
- Requêtes pour les mesures générées par les alertes et les outils de calcul intégrés

La mesure `Collector Metrics Received Per Interval` est un indicateur de la charge de requête du cluster et de la consommation de bande passante réseau pour la communication entre le collecteur et le MOM. Des variations sont attendues. Des pics importants indiquent une forte activité de requête spontanée. La valeur `Collector Metrics Received Per Interval` correspond approximativement au nombre de mesures traitées par les outils de calcul.

Vous pouvez afficher la mesure aux emplacements suivants :

- Arborescence du navigateur de mesures sous Enterprise Manager | MOM | Collector Metrics Received Per Interval
- `perflog.txt` sous `Performance.MOM.CollectorMetricsReceivedPerInterval`

Alerts: Total Number of Evaluated Metrics

Les alertes sont des *outils de calcul dépendants*, car les alertes fonctionnent selon la sortie d'autres outils de calcul. Les outils de calcul dépendants ne peuvent pas être exécutés en parallèle avec les outils de calcul qui fournissent leur entrée. Pour cette raison, les alertes peuvent prolonger la durée de collecte plus que les outils de calcul non dépendants. La mesure de prise en charge Alerts: Total Number of Evaluated Metrics affiche le nombre de mesures que les alertes ont traitées au cours de chaque créneau.

Vous pouvez afficher la mesure dans l'arborescence du navigateur de mesures, sous Enterprise Manager | Internal | Alerts.

Si une augmentation de la durée de collecte est corrélée à une augmentation des mesures évaluées par les alertes, vous pouvez augmenter la capacité du gestionnaire d'entreprise en optimisant les alertes. Pour identifier les alertes qui consomment le plus de ressources, recherchez et triez par valeur toutes les mesures dont le nom correspond à l'expression régulière suivante :

```
(.*)Enterprise Manager|Internal|(.*)Alerts(.*)Number of Evaluated Metrics
```

Si Introscope dispose d'alertes évaluant un grand nombre de mesures (en particulier celles provenant de plusieurs collecteurs multiples), envisagez d'effectuer les actions suivantes :

- Désactiver les alertes qui apportent peu de valeur.
- Ajuster les expressions régulières dans les groupes de mesures d'alerte pour inclure uniquement les mesures minimum requises pour indiquer la condition d'alerte.
- Diviser les alertes qui évaluent les mesures de plusieurs collecteurs en plusieurs alertes qui évaluent uniquement les mesures d'un seul collecteur. Cette action ne réduit pas nécessairement le nombre de mesures traitées par le MOM, mais améliore les performances des requêtes dans le cluster.

Overall Capacity (%)

La mesure `Overall Capacity (%)` estime le pourcentage de capacité consommée par le gestionnaire d'entreprise.

Vous pouvez afficher la mesure dans l'arborescence du navigateur de mesures, sous `Enterprise Manager |`.

La mesure `Overall Capacity (%)` est calculée en partie à partir des mesures de contribution suivantes, que vous pouvez afficher dans l'arborescence du navigateur de mesures sous `Enterprise Manager | Health`:

- CPU Capacity (%)
- GC Capacity (%)
- Harvest Capacity (%)
- [Heap Capacity \(%\) metric](#)
- Incoming Data Capacity (%)
- SmartStor Capacity (%)

La mesure `Overall Capacity (%)` a plus d'intérêt sur une longue période plutôt que pour un créneau spécifique de 15 secondes. La mesure `Overall Capacity (%)` étant basée sur des mesures en temps réel, sa valeur peut atteindre un pic supérieur à 100 %. Le pic peut se produire, par exemple, en raison d'une brève surcharge du sous-système d'E/S matériel. Cependant, le gestionnaire d'entreprise a tendance à se remettre automatiquement de ces situations de pic lorsqu'elles ne durent pas longtemps. En général, un pic de 200 %, par exemple, n'est pas préoccupant s'il est transitoire. Cependant, sur une longue période, la moyenne idéale de `Overall Capacity (%)` est inférieure ou égale à 75 %.

Au cours des périodes où la mesure `Overall Capacity (%)` atteint des valeurs élevées, au moins une des autres mesures de contribution présente probablement également un pic. L'examen et la compréhension de la source du pic secondaire peuvent permettre d'identifier la cause première du problème de ressource. Par exemple, vous pouvez résoudre le problème en examinant la mesure [Heap Capacity \(%\)](#) qui alimente la mesure `Overall Capacity (%)`.

L'affichage de la mesure `Overall Capacity (%)` en mode Historique est utile pour obtenir une vue comparative générale du statut de la capacité du gestionnaire d'entreprise. Cependant, la charge de travail du gestionnaire d'entreprise est complexe et divers aspects de celle-ci affectent la mesure `Overall Capacity (%)` de différentes manières non linéaires. Par exemple, la durée des tâches de maintenance de SmartStor (conversion du spool en données et repériodisation) peut être un indicateur important de la capacité du gestionnaire d'entreprise. Toutefois, ces tâches de maintenance ne participent pas directement au calcul de la mesure `Overall Capacity (%)`. Les tâches de maintenance de SmartStor entraînent une augmentation de l'utilisation de l'UC et du segment de mémoire. L'augmentation de l'utilisation se traduit par une augmentation du pourcentage de capacité. Cependant, l'ampleur de l'augmentation ne reflète pas l'intégralité de l'impact des problèmes de maintenance de SmartStor.

La mesure `Overall Capacity (%)` se concentre principalement sur la façon dont un gestionnaire d'entreprise gère la charge de travail des mesures d'agent. Cette mesure n'évalue pas directement la capacité en fonction des données

de CA CEM. Par exemple, la mesure `Overall Capacity (%)` ne reflète pas les services du gestionnaire d'entreprise surchargés ni les problèmes d'E/S de base de données APM.

Heap Capacity (%)

La mesure `Heap Capacity (%)` indique la quantité du segment de mémoire alloué en cours d'utilisation. Cette mesure est normalisée à 75 % du segment de mémoire alloué afin de fournir une mémoire tampon de sécurité et d'éviter les arrêts brutaux. Une valeur de mesure de 100 signifie que le segment de mémoire alloué n'est utilisé qu'à 75 %.

La mesure `Heap Capacity (%)` vous permet d'évaluer si le segment de mémoire alloué à un gestionnaire d'entreprise est suffisant pour la charge. Cette mesure vous permet également de détecter les tendances affectant l'utilisation du segment de mémoire. Parfois, une utilisation élevée de l'UC ou une durée de collecte élevée, ou les deux, peuvent résulter d'une utilisation élevée du segment de mémoire.

Vous pouvez afficher la mesure dans l'arborescence du navigateur de mesures, sous `Enterprise Manager | Health`.

Number of Historical Metrics

La mesure `Number of Historical Metrics` correspond au nombre total de mesures qu'un gestionnaire d'entreprise a vues et conservées dans SmartStor. Ce nombre augmente lorsque les agents signalent de nouvelles mesures et diminue lorsque les mesures expirent dans SmartStor. La déconnexion temporaire d'un agent et l'envoi de nouvelles données à une mesure existante ne modifient pas ce nombre.

Le nombre de mesures historiques affecte les performances des requêtes d'historique et la surcharge de repériodisation nocturne de SmartStor. Une valeur croissante peut indiquer les problèmes suivants :

- **Fuite de mesures**
Augmentation progressive du nombre de mesures en raison d'un environnement de surveillance instable avec des connexions d'agent non contrôlées
- **Explosion de mesures**
Augmentation rapide du nombre de mesures en raison de l'apparition de nombreux nouveaux agents ou de mesures d'agent SQL incorrectement spécifiées

Vous pouvez afficher la mesure dans l'arborescence du navigateur de mesures, sous `Enterprise Manager | Connections`.

Partial Metrics without Data

La mesure `Partial Metrics without Data` indique le nombre de mesures d'agent qui ne sont plus signalées en direct. Ces mesures consomment une partie du segment de mémoire et affectent négativement les performances des requêtes en contribuant au nombre de la mesure `Historical Metrics`.

Les pénalités de performances sont mineures, sauf si la valeur de la mesure `Partial Metrics without Data` devient importante.

Si vous rencontrez des problèmes liés à la réactivité des requêtes d'historique ou à des longs délais de repériodisation SmartStor, comparez la valeur de la mesure `Partial Metrics without Data` à la valeur de la mesure `Partial Metrics with Data`. Vous pouvez afficher la mesure `Partial Metrics with Data` dans l'arborescence du navigateur de mesures, sous `Enterprise Manager | Data Store | SmartStor | MetaData`. Si la mesure `Partial Metrics without Data` se rapproche de la valeur de la mesure `Partial Metrics with Data`, utilisez les outils SmartStor pour supprimer les métadonnées de mesure inutiles.

Vous pouvez afficher la mesure à l'emplacement suivant :

- Arborescence du navigateur de mesures sous `Enterprise Manager | Data Store | SmartStor | MetaData`

Number of Traces in Insert Queue

Le gestionnaire d'entreprise tente d'insérer tous les événements entrants dans une file d'attente d'insertion de trace de transaction. La mesure `Number of Traces in Insert Queue` dans la file d'attente d'insertion affiche le nombre moyen d'événements dans la file d'attente au cours du créneau précédent.

La mesure `Number of Traces in Insert Queue` indique si le gestionnaire d'entreprise applique le processus de trace de transactions. Si la file d'attente d'insertion de trace de transaction est pleine lorsqu'un nouvel événement arrive, l'événement est abandonné. Vous pouvez afficher la mesure `Transactions: Number of Dropped Per Interval` pour afficher le nombre de traces de transaction que le gestionnaire d'entreprise n'a pas pu gérer pendant l'intervalle et qui ont été abandonnées.

Vous pouvez afficher la mesure `Transactions: Number of Dropped Per Interval` aux emplacements suivants :

- Arborescence du navigateur de mesures sous `Enterprise Manager | Data Store | Transactions`
- `perflog.txt` sous `Performance.Transactions.Num.Dropped.Per.Interval`

Vous pouvez afficher la mesure `Number of Traces in Insert Queue` aux emplacements suivants :

- Arborescence du navigateur de mesures sous `Enterprise Manager | Data Store | Transactions`
- `perflog.txt` sous `Performance.Transactions.TT.Queue.Size`

SmartStor Queries Per Interval

La mesure `SmartStor Queries Per Interval` affiche le nombre de requêtes pour les données de mesure reçues au cours du créneau précédent.

Le solde des écritures de mesure comparées aux requêtes de mesure détermine les exigences de configuration de disque SmartStor.

Pour évaluer les performances de votre charge de requête de mesure, examinez les mesures suivantes :

- `Mesure SmartStor Queries per Interval`
- `Mesure SmartStor Queries Duration (ms)`
Cette mesure affiche la durée moyenne de requête au cours du créneau précédent.

Vous pouvez afficher la mesure `SmartStor Queries Duration (ms)` et la mesure `SmartStor Queries per Interval` aux emplacements suivants :

- Arborescence du navigateur de mesures sous `Enterprise Manager | Internal | Query`
- `perflog.txt`

Autres mesures de prise en charge du gestionnaire d'entreprise

Utilisez la liste suivante d'autres mesures de prise en charge utiles.

- **EM CPU Used (%)**
Utilisation du processeur par les threads du gestionnaire d'entreprise (EM) au cours de la période mesurée. Dans un créneau de 15 secondes, l'utilisation est la suivante : $\langle \text{ms de processeur utilisés par l'EM} \rangle / (15000 * \langle \text{nombre de processeurs} \rangle)$.
Situé dans l'arborescence Investigator sous `Enterprise Manager|CPU`.

NOTE

Ce nombre ne reflète pas l'utilisation totale du processeur pendant le créneau. Cette mesure mesure uniquement la participation du gestionnaire d'entreprise à l'utilisation totale du processeur.

- **Number of Agents**
Nombre d'agents actuellement connectés.
Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|Connections`.
- **Harvest Capacity (%)**

Pourcentage de temps nécessaire à la collecte de données dans un créneau de 15 000 ms (15 secondes), où 100 % correspond aux 15 secondes complètes. Par exemple, si la durée de la collecte est de 15 000 ms, la valeur de la mesure est de 100.

NOTE

Dans un environnement de surveillance sain, la capacité de collecte reste inférieure à 25 %.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|Health`.

- **Number of Metrics**

Charge de mesure sur un gestionnaire d'entreprise. Lorsqu'un agent se déconnecte, ce nombre diminue.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|Connections`.

- **SmartStor Capacity (%)**

Pourcentage de temps que dure le processus d'écriture SmartStor dans un créneau de 15 000 ms (15 secondes), où 100 % correspond aux 15 secondes complètes. Par exemple, si la durée de l'écriture SmartStor est de 15 000 ms, la valeur de la mesure est de 100.

NOTE

Dans un environnement de surveillance sain, la capacité SmartStor reste inférieure à 25 %.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|Health`.

- **Active Incoming Threads**

Nombre de threads traitant activement les messages des clients.

La mesure Active Incoming Threads fournit des informations sur la simultanéité de l'exécution de requête. Plusieurs requêtes de mesure simultanées peuvent interférer avec d'autres activités SmartStor et augmenter la durée de SmartStor.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|Internal|Messaging`.

- **Active Outgoing Threads**

Nombre de threads livrant activement des données aux clients.

Cette mesure est un indicateur de la simultanéité des requêtes. Une augmentation du nombre de threads travaillant sur la livraison des données peut indiquer des problèmes réseau.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|Internal|Messaging`.

- **Number of Dependent Calculator Input Metrics**

Nombre total de mesures utilisées en tant qu'entrées dans les outils de calcul dépendants.

Les outils de calcul dépendants fonctionnent sur des valeurs de mesure produites par d'autres outils de calcul. Les entrées dans les outils de calcul dépendants peuvent également inclure des valeurs de mesure signalées par les agents. Ce nombre fait référence à toutes les mesures envoyées aux outils de calcul dépendants, et pas uniquement aux mesures produites par d'autres outils de calcul.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|Internal`.

- **Number of Non Dependent Calculator Input Metrics**

Nombre total de mesures utilisées en tant qu'entrées dans les outils de calcul non dépendants.

Les outils de calcul non dépendants fonctionnent sur les mesures signalées par les agents et non sur les mesures émises par d'autres outils de calcul.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|Internal`.

- **Total Number of Evaluated Metrics (Calculators)**

Nombre total de mesures évaluées pour tous les outils de calcul. Cette mesure est la somme des mesures Number of Dependent Calculator Input Metrics et Number of Non-dependent Calculator Input Metrics.

Lorsque ce nombre est élevé, le gestionnaire d'entreprise effectue de nombreux calculs en temps réel, ce qui peut surcharger les ressources d'UC.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager | InternalCalculators`.

- **<nom_outil_calcul> | Total Number of Evaluated Metrics**

Nombre total de mesures évaluées pour un outil de calcul.

La valeur de cette mesure indique la proportion à laquelle l'outil de calcul associé contribue à la durée de la collecte. Concentrez-vous sur les outils de calcul qui évaluent un grand nombre de mesures pour optimiser la capacité du gestionnaire d'entreprise.

NOTE

Cette mesure s'affiche dans Investigator uniquement lorsque l'outil de calcul est défini.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager | Internal`.

- **Alert Action Processing Time (ms)**

Temps pris par le gestionnaire d'entreprise à traiter toutes les actions d'alerte.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager | Internal | Harvest`.

- **Calculator Queries Wait Time (ms)**

Temps pris par le thread de requête de l'outil de calcul à terminer sa tâche actuelle, y compris l'attente de la fin de la boucle de requête hors outil de calcul.

Le traitement de la nouvelle requête de l'outil de calcul démarre à la fin de toutes les livraisons de créneaux hors outil de calcul précédentes aux clients. Lorsque ce nombre est élevé, le gestionnaire d'entreprise effectue de nombreux calculs en temps réel, ce qui peut surcharger les ressources d'UC.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager | Internal | Harvest`.

- **Non Calculator Queries Delivery Time (ms)**

Temps pris par le gestionnaire d'entreprise pour exécuter et livrer des requêtes hors outil de calcul à tous les clients demandeurs dans un créneau.

Une fois que toutes les requêtes d'outil de calcul sont exécutées, le gestionnaire d'entreprise exécute les requêtes hors outil de calcul. Il envoie ensuite les résultats à tous les clients qui les ont demandés. Lorsque ce nombre atteint des pics, le gestionnaire d'entreprise envoie de nombreux résultats de requête hors outil de calcul aux clients, ce qui peut entraîner une surcharge du réseau.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager | Internal | Harvest`.

- **Non Calculator Queries Excess Time (ms)**

Temps d'attente excessif pour le traitement des requêtes hors outil de calcul au-delà d'un créneau.

Les clients envoient des requêtes hors outil de calcul au gestionnaire d'entreprise, qui renvoie les résultats. Si ce processus ne se termine pas dans un créneau précis, il est retenté jusqu'à ce qu'il soit terminé. Cette mesure indique la durée au-delà de laquelle le traitement des requêtes hors outil de calcul s'est étendu.

Utilisez cette mesure pour déterminer si les requêtes hors outil de calcul surchargent un gestionnaire d'entreprise.

Cette valeur de mesure est généralement égale à 0 lorsqu'Introscope est soumis à une charge réduite. Une valeur supérieure à 0 indique que le gestionnaire d'entreprise est surchargé et incapable de traiter les requêtes de mesures dans un créneau.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager | Internal | Harvest`.

- **Metrics From All Agents**

Nombre total de mesures uniques générées par tous les agents connectés qui ont envoyé des données au cours du dernier créneau. Ce nombre n'inclut pas les mesures historiques. Les paramètres de clamp n'affectent pas ce nombre. Lorsque la limite `introscope.enterprisemanager.agent.metrics.limit` est déclenchée, la valeur de cette mesure vous indique de combien la limite a été dépassée.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager | Internal | Harvest`.

- **Spooling Data File Write Time (ms)**

Temps pris par le gestionnaire d'entreprise pour écrire les données collectées dans le fichier de spooling (`.spool`) dans un créneau.

Utilisez cette mesure pour surveiller le cycle de collecte.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|Internal|Harvest`.

- **Spooling Preparation Time (ms)**

Temps pris par le gestionnaire d'entreprise pour préparer l'écriture des données collectées dans le fichier de spooling (`.spool`) dans un créneau.

Utilisez cette mesure pour surveiller le cycle de collecte.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|Internal|Harvest`.

- **Total Number of Evaluated Metrics (Management Module Calculators)**

Nombre de mesures utilisées en tant qu'entrées dans les outils de calcul du module de gestion.

Lorsque ce nombre augmente, cela indique qu'une requête ou un outil de calcul avec une requête correspond à un trop grand nombre de mesures.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|InternalManagement Module Calculators`.

- **Metric Matches Per Interval**

Nombre total de mesures évaluées dans toutes les requêtes au cours du dernier créneau.

Cette mesure affiche une valeur lorsque les actions suivantes se produisent :

- De nouveaux agents se connectent au gestionnaire d'entreprise.
- Les expressions régulières sont utilisées dans les requêtes internes et générées par l'utilisateur, y compris dans les groupements de mesures du module de gestion.
- Les utilisateurs sélectionnent des mesures dans l'arborescence du navigateur de mesures.
- Les utilisateurs ouvrent des tableaux de bord contenant des graphiques.

Lorsque cette valeur de mesure est élevée, de nombreuses requêtes se produisent en peu de temps.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|InternalMetric Group`.

- **Queued Queries Per Interval**

Nombre de requêtes en attente de traitement dans l'intervalle de cycle de collecte. La valeur est généralement de zéro après le démarrage.

Affichez la mesure dans l'arborescence du navigateur de mesures sous `Enterprise Manager|InternalMetric Group`.

Mesures de prise en charge du pool de connexions de la base de données APM

Les services du gestionnaire d'entreprise fournissent des mesures qui décrivent l'allocation et l'utilisation des pools de connexions de la base de données APM. Ces pools permettent l'échange de données entre les services du gestionnaire d'entreprise et la base de données APM. Les mesures de prise en charge du pool de connexions de la base de données APM s'affichent dans l'arborescence Investigator de la station de travail sous :

```
Custom Metric Agent|Enterprise Manager|Internal|Database|Connection Pools
```

Elles sont également disponibles dans le fichier journal `tessperflog.txt` et portent le préfixe `Internal.Database.Connection Pools`.

Des mesures sont fournies pour les sources de données APM :

Le nom `apmDataSource` identifie la source de données APM.

La liste suivante décrit les mesures de prise en charge du pool de connexions de la base de données APM :

- **numBusyConnections**
Nombre de connexions en cours d'utilisation
- **numConnections**

Nombre de connexions ouvertes

- **numIdleConnections**
Nombre de connexions ouvertes et non utilisées
- **numUnclosedOrphanedConnections**
Nombre de connexions ouvertes non utilisées après le dépassement d'un délai d'expiration
- **threadPoolNumTasksPending**
Nombre de tâches en file d'attente en attente d'une connexion

Surveillance des connexions aux stations de travail à l'aide des mesures de prise en charge

La mesure de prise en charge `Connections: Number of Workstations` affiche le nombre actuel de connexions de stations de travail. Pour les collecteurs dans un environnement en cluster, la valeur de cette mesure est 0.

Consultez la mesure `Connections: Number of Workstations` ici dans l'arborescence du navigateur de mesures :

```
*SuperDomain*|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|
Custom Metric Agent (Virtual) (*SuperDomain*)|Enterprise Manager|
Connections: Number of Workstations
```

NOTE

La mesure

`Connections: Number of Workstations`

ne reflète pas les connexions Command Line Workstation ou WebView.

Istio Support

DX APM Istio Support signale les mesures et les traces de transaction à partir d'applications (généralement des microservices) instrumentées à l'aide d'outils de suivi compatibles avec OpenTracing.

[Istio](#) est un service Mesh open source et indépendant du fournisseur utilisé par les entreprises pour réduire la complexité de leurs environnements hybrides cloud et multicloud. Istio injecte un proxy sidecar dans le pod dans lequel un conteneur d'applications est en cours d'exécution. Le proxy sidecar surveille les demandes d'application (généralement les microservices) du trafic réseau entrant et sortant.

DX APM étend l'importateur Prometheus de l'agent de surveillance universel (UMA) pour signaler les données de demande de proxy sidecar Istio. Istio Support signale les mesures d'intégrité Istio et des applications, et affiche les traces de transaction et les données de carte de Team Center.

Versions d'Istio prises en charge

- Istio 1.4.x

Activation du composant d'arrière-plan de l'importateur Prometheus prenant en charge Istio

Activez le composant d'arrière-plan Istio Support Prometheus Importer avant d'installer l'UMA.

Procédez comme suit :

1. Ouvrez le fichier approprié pour votre environnement dans un éditeur de texte :
 - (Opérateur de l'UMA) Accédez au répertoire `uma-operator` et ouvrez le fichier `uma_cr.yaml`.
 - (Graphique Helm) Accédez au répertoire `helm-chart/uma` et ouvrez le fichier `values.yaml`.
 - (Fichier YAML de l'UMA) Accédez au fichier YAML de l'application `ca-uma-agent.yaml`.
2. (Opérateur de l'agent UMA/graphique Helm) Configurez la propriété `prometheus.backend.enabled`.

NOTE

Ignorez cette étape si vous utilisez le fichier YAML de l'UMA pour installer celui-ci. Par défaut, le fichier `ca-uma-agent.yaml` active la prise en charge du composant d'arrière-plan de l'importateur Prometheus.

- a. Recherchez la propriété `prometheus.backend.enabled`.
 - b. Définissez la propriété `prometheus.backend.enabled` sur `true`. La valeur par défaut est `false`.
3. Définissez l'URL du composant d'arrière-plan de l'importateur Prometheus.
- a. (Opérateur de l'UMA/graphique Helm) Dans le fichier approprié (`uma_cr.yaml` pour l'opérateur UMA, `values.yaml` pour le graphique Helm), ajoutez l'URL du composant d'arrière-plan de l'importateur Prometheus après `url` : Reportez-vous à la section suivante du fichier :
 - b. (Opérateur de l'UMA/graphique Helm) Lorsque l'URL du composant d'arrière-plan de l'importateur Prometheus est protégée, fournissez le nom d'utilisateur et le mot de passe.
- Dans le fichier approprié (`uma_cr.yaml` pour l'opérateur UMA/`values.yaml` pour le graphique Helm), indiquez les informations d'identification dans les propriétés `username` et `password` dans les sections du fichier suivantes :

```
container: | prometheus: | backend: | endPoint: | url: <URL>
```

```
container: | prometheus: > backend: | endPoint: | username: | and prometheus: | backend: | endPoint: |
username:
```

```
container: | prometheus: | backend: > endPoint: | username: | and prometheus: | backend: | endPoint: |
password:
```

Exemples de paramètres pour les fichiers `uma_cr.yaml` et `values.yaml` :

```
container:
  prometheus:
    Exporter:
      enabled: false
    backend:
      enabled: true
      endPoint:
        url: http://10.80.89.157:30007/
        username:
        password:
        token:
      configFiles:
      metricAlias: container_name=container,pod_name=pod
```

(Fichier YAML de l'UMA)

Dans le fichier YAML de l'application, définissez la propriété `Prometheus_server_url` sur `Prometheus_server_url`: "`<URL>`". Veillez à inclure des guillemets droits avant et après l'URL. Voici un exemple :

```
Prometheus_server_url: "http://10.80.89.157:30007/"
```

Installation de Istio Support à l'aide de l'agent UMA

Après avoir configuré la connexion au composant d'arrière-plan Prometheus, installez l'UMA à l'aide de l'une des options suivantes :

- Opérateur Kubernetes
- Graphique Helm
- Fichier YAML de l'UMA

Pour installer l'agent de surveillance universel, reportez-vous à la section [Installation et configuration de l'agent de surveillance universel pour Kubernetes](#).

Mesures Istio

L'UMA déploie le pod **cluster-performance-prometheus** avec l'importateur Prometheus activé, comme illustré dans la capture d'écran d'exemple suivante :

NAME	READY	STATUS	RESTARTS	AGE
pod/app-container-monitor-bndgx	2/2	Running	0	21h
pod/app-container-monitor-rngq5	2/2	Running	0	21h
pod/app-container-monitor-tsmhg	2/2	Running	0	21h
pod/cluster-performance-prometheus-5bbb87b6bf-q4lbv	1/1	Running	0	21h
pod/cluster-info-8668861491-mb5tt	1/1	Running	0	21h
pod/container-monitor-8655dfd798-ffs4q	1/1	Running	0	21h

L'agent DX APM Prometheus récupère les mesures auprès du serveur Prometheus et les signale sous le noeud **Istio**. Le chemin du navigateur de mesures est le suivant :

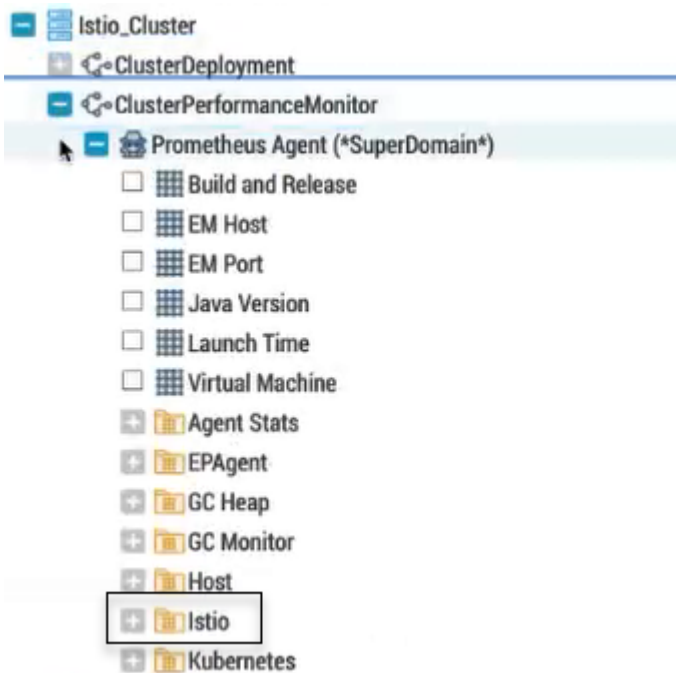
SuperDomain | <nom_cluster> | ClusterPerformanceMonitor | Prometheus Agent | Istio

Indiquez le nom du cluster dans la propriété `clusterName` du fichier `uma_cr.yaml` (opérateur de l'uma) ou du fichier `values.yaml` (graphique Helm).

- Exemple : `DevelopmentCluster`
- Valeur par défaut : `SandBox`

Dans ce cas, le chemin du navigateur de mesures est SuperDomain | ?DevelopmentCluster? or ?SandBox? | ClusterPerformanceMonitor | Prometheus Agent | Istio

Après avoir installé l'UMA, DX APM affiche le noeud **Istio** sous le noeud **Prometheus Agent** (Agent Prometheus) comme illustré dans la capture d'écran suivante :



Istio Support fournit deux catégories de mesures. La première catégorie concerne les mesures de services et de charge de travail, qui fournissent des données de performances sur les applications s'exécutant sur le service Mesh Istio. La deuxième catégorie concerne les mesures d'intégrité spécifiques à Istio.

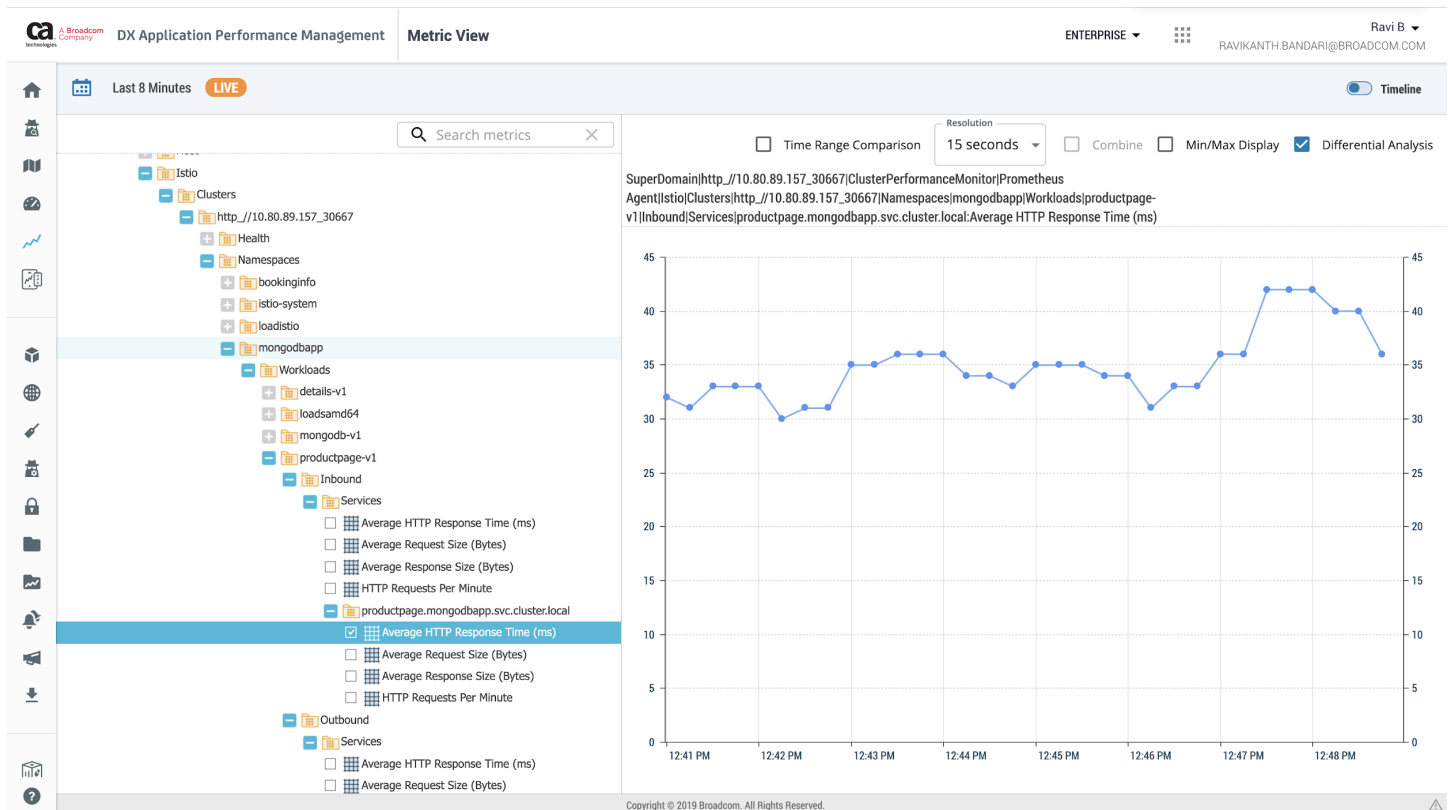
Services et mesures de charge de travail Istio Support

Dans Istio Support, le terme *service* fait référence à un service Kubernetes ou OpenShift. Une *charge de travail* fait référence à un déploiement Kubernetes ou OpenShift. Les termes *entrant* et *sortant* se rapportent au trafic réseau entrant ou sortant d'un service ou d'une charge de travail Kubernetes ou OpenShift.

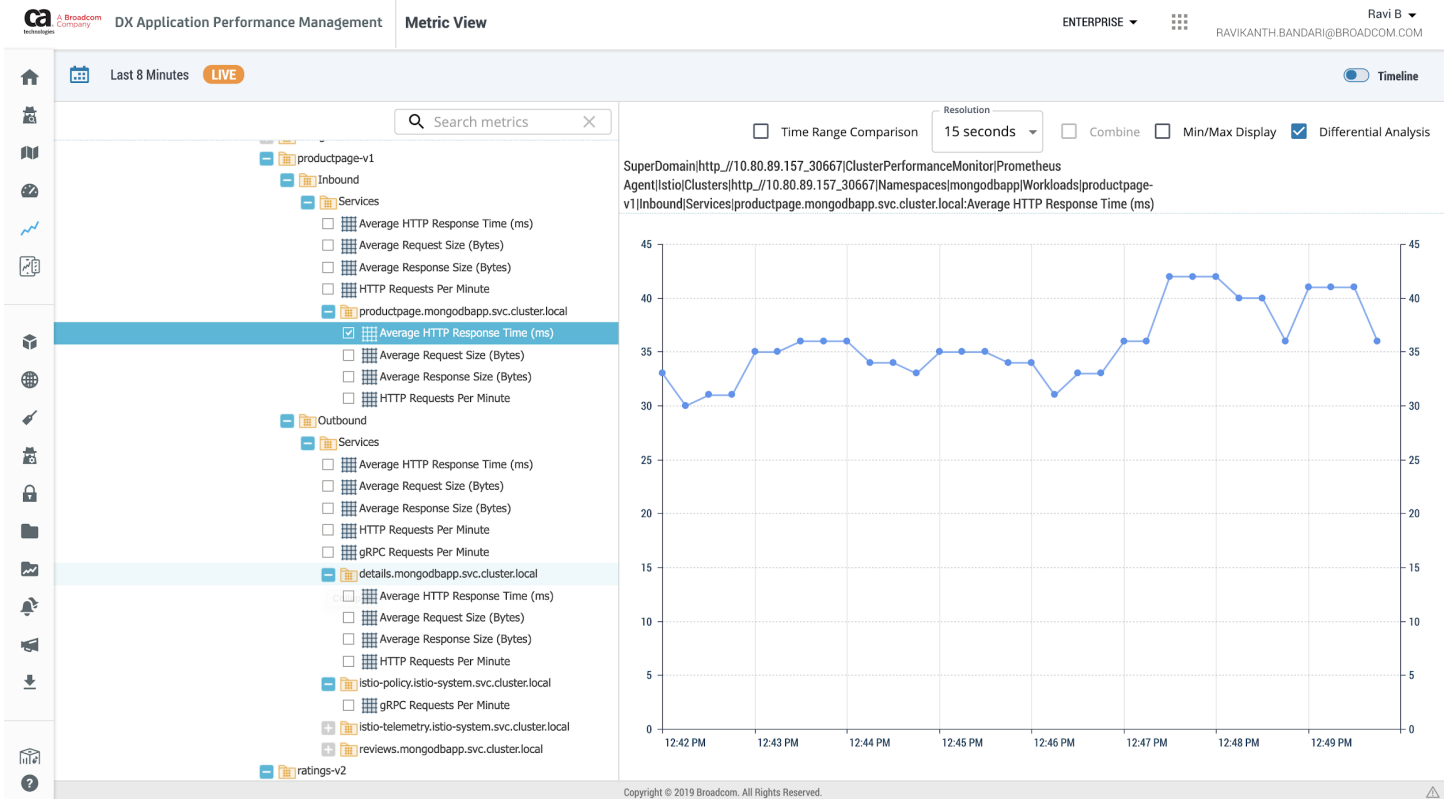
Istio Support signale ces mesures par service ou par charge de travail. Il ne signale pas toutes les mesures pour chaque service ou charge de travail. Les mesures que Istio Support signale dépendent du type de trafic qui passe par le service ou la charge de travail : HTTP, Google Remote Procedure Call (gRPC) et Transmission Control Protocol (TCP). Par exemple, lorsque le trafic HTTP et gRPC est acheminé via un service ou une charge de travail, Istio Support signale toutes les mesures liées aux protocoles HTTP et gRPC. Le chemin du navigateur de mesures pour les mesures de services et de charge de travail est le suivant :

SuperDomain | <nom_cluster> | ClusterPerformanceMonitor | Prometheus Agent | Istio | Clusters | <URL_composant_arrière-plan_importateur_Prometheus> | namespaces | <nom_application> | Workloads | <nom_charge_de_travail> | Inbound/Outbound | Services | <nom_service> |

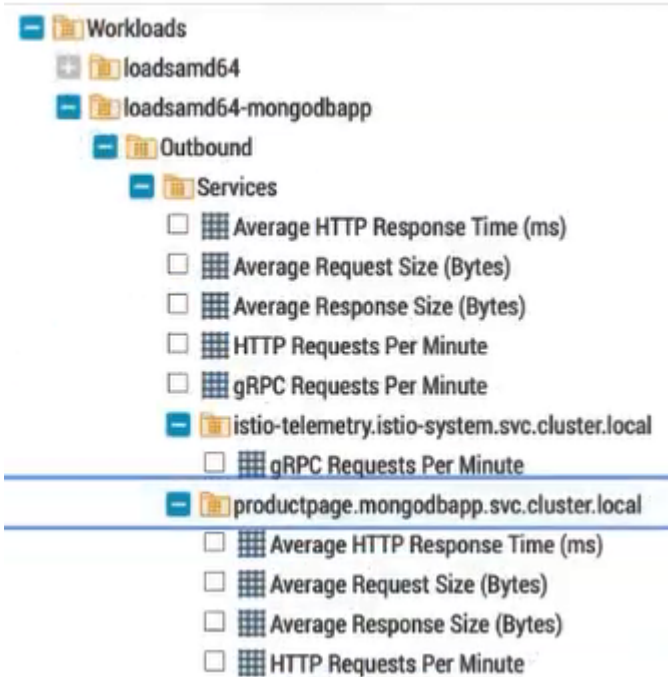
Dans la première des deux captures d'écran suivantes, le navigateur de mesures affiche les mesures pour tous les services **entrants** et certains **services sortants** pour l'application **mongodbapp**. Dans les deux captures d'écran, le graphique affiche les données de la mesure **Average Response Time** pour l'application **mongodbapp**, la charge de travail **productpage-v1** et le service entrant **productpage.mongodbapp.svc.cluster.local**. Notez que la charge de travail **productpage-v1** dispose également de services entrants et sortants.



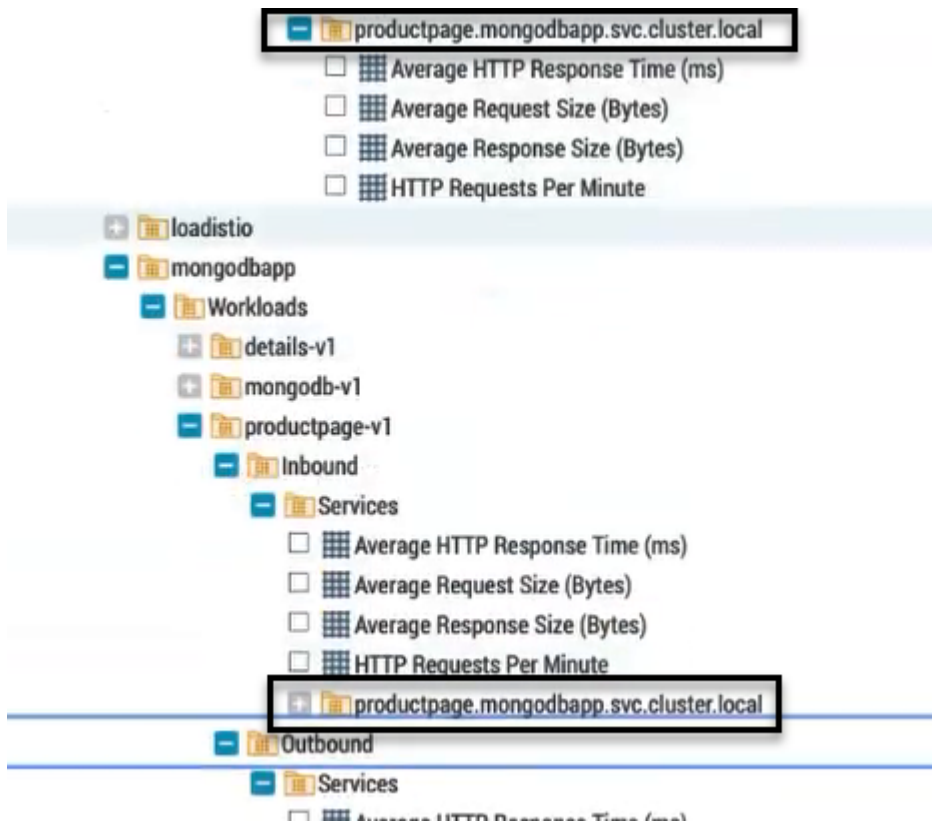
Dans la capture d'écran suivante, le navigateur de mesures affiche les mesures pour certains services **entrants** et tous les **services sortants** pour l'application **mongodbapp**.



Parfois, une charge de travail comprend seulement du trafic sortant. Dans cette capture d'écran, le navigateur de mesures affiche la charge de travail MongoDB **loadsamd64-mongod**. Cette charge de travail comprend uniquement une communication sortante, qui envoie le trafic à deux services : un pour la télémétrie (**istio-telemetry.istio-system.svc.cluster.local**) et une page de produit (**productpage.mongodbapp.svc.cluster.local**).



Dans la capture d'écran suivante, vous pouvez remarquer que le trafic entrant indique que la demande provient du service **productpage.mongodb.svc.cluster.local**.



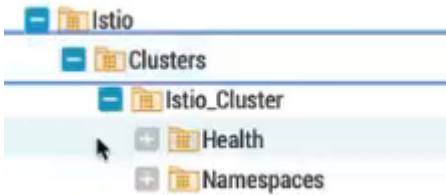
Les mesures de service et de charge de travail ci-dessous sont utilisées dans Istio Support :

- Average HTTP Response Time (ms)
- Average Request Size (Bytes)
- Average Response Size (Bytes)
- HTTP Requests Per Minute
- HTTP Errors Per Minute
- gRPC Errors Per Minute
- gRPC Requests Per Minute
- TCP Bytes Received Per Minute
- TCP Bytes Sent Per Minute
- TCP Connections Closed Per Minute
- TCP Connections Opened Per Minute

Mesures liées à l'intégrité de Istio Support

Les mesures d'intégrité de Istio Support fournissent des informations sur les performances spécifiques à Istio et s'affichent dans le répertoire **Intégrité**. Le chemin complet du navigateur de mesures est le suivant :

SuperDomain | *<nom_cluster>* | ClusterPerformanceMonitor | Prometheus Agent | Istio | Clusters | Istio Cluster ou *<URL de composant d'arrière-plan Prometheus Importer>* | Health



Les mesures d'intégrité sont récupérées auprès des composants Istio Citadel, Pilot et Galley. Le tableau suivant décrit les mesures d'intégrité par composant :

Mesures relatives à Citadel

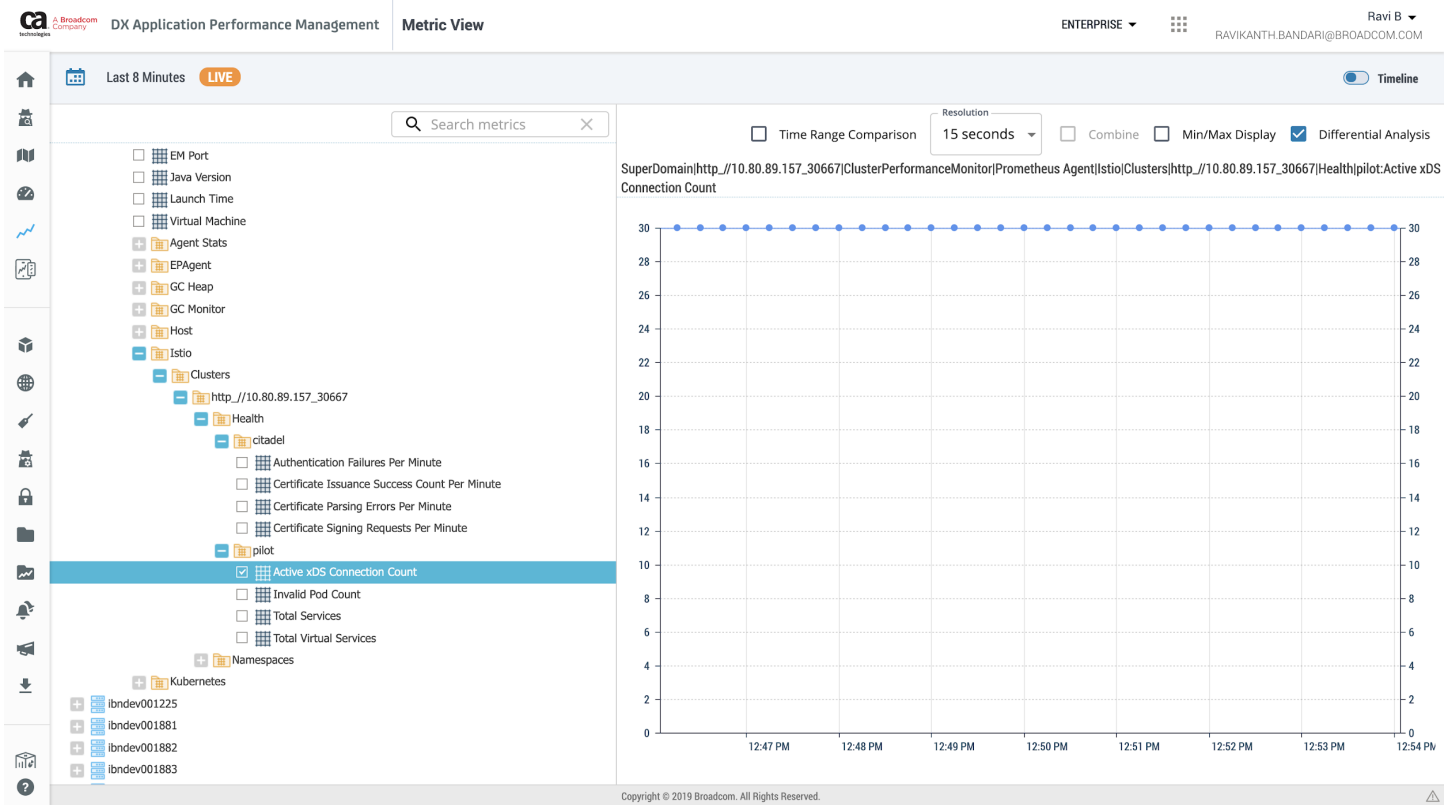
- **Authentication Failures Per Minute**
Nombre d'échecs d'authentification par minute.
- **Certificate Issuance Success Count Per Minute**
Nombre de certificats dont l'émission a réussi par minute.
- **Certificate Parsing Errors Per Minute**
Nombre d'erreurs par minute qui se produisent lors de l'analyse des demandes de signature de certificat (CSR).
- **Certificate Signing Requests Per Minute**
Nombre de demandes de signature de certificat reçues par le serveur Citadel par minute.

Mesures relatives à Pilot

- **Active xDS Connection Count**
Nombre de terminaux/proxys Envoy connectés à l'instance Pilot à l'aide du [protocole XDS Envoy](#).
- **Invalid Pod Count**
Nombre de proxys qui ne sont sélectionnés par aucun service. Cette mesure d'erreur se produit lorsque la liste des terminaux pour un service n'est pas mise à jour dans l'instance Pilot.
- **Total Services**
Nombre total de services que l'instance Pilot reconnaît.
- **Total Virtual Services**
Nombre total de services virtuels que l'instance Pilot reconnaît.

Mesure relative à Galley

- **Validation Failures Per Minute**
Nombre d'échecs de validations par le webhook de validation de configuration par minute.

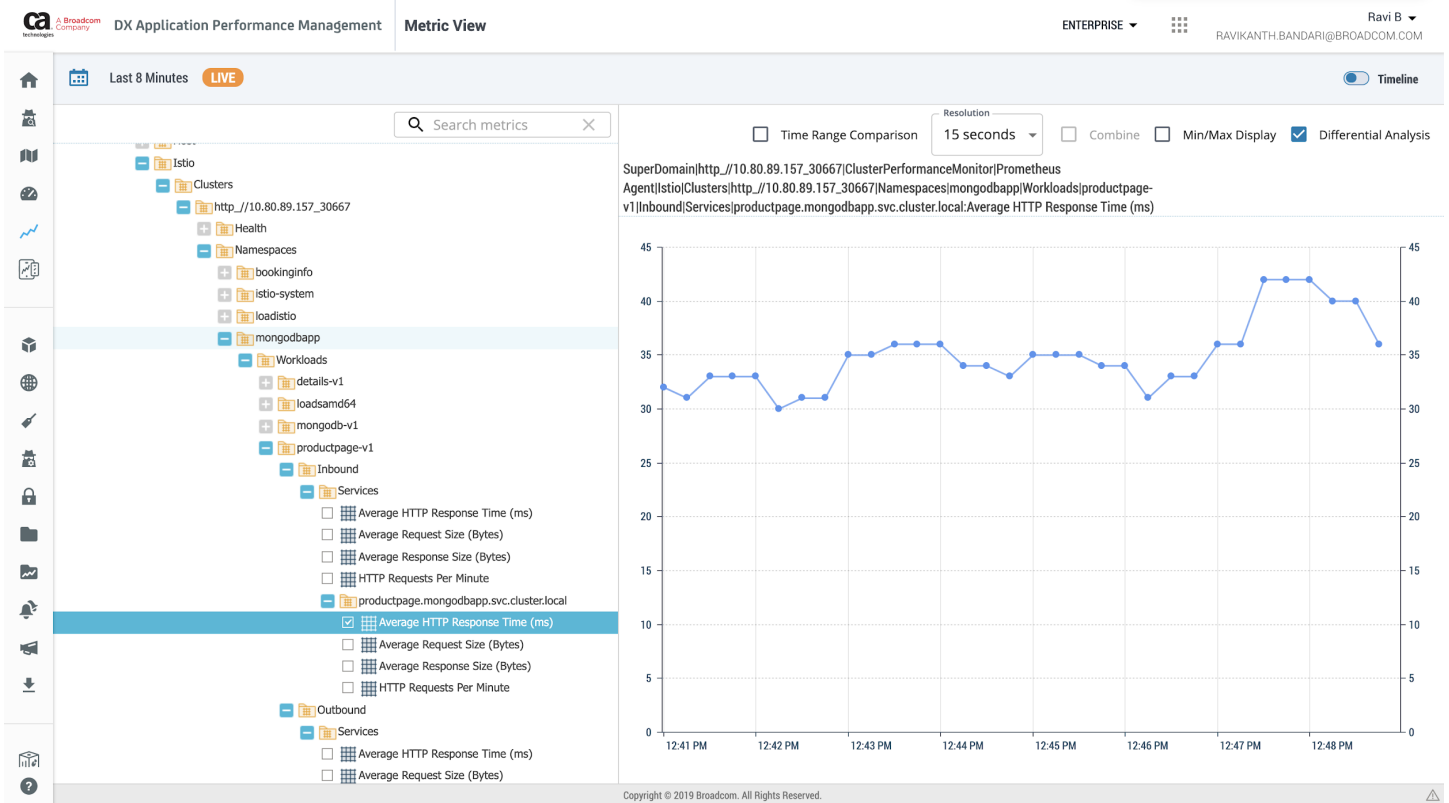


Istio Support affiché dans la carte

Istio Support permet de visualiser la topologie Istio Service Mes dans la carte, qui affiche des services spécifiques qui communiquent entre eux.

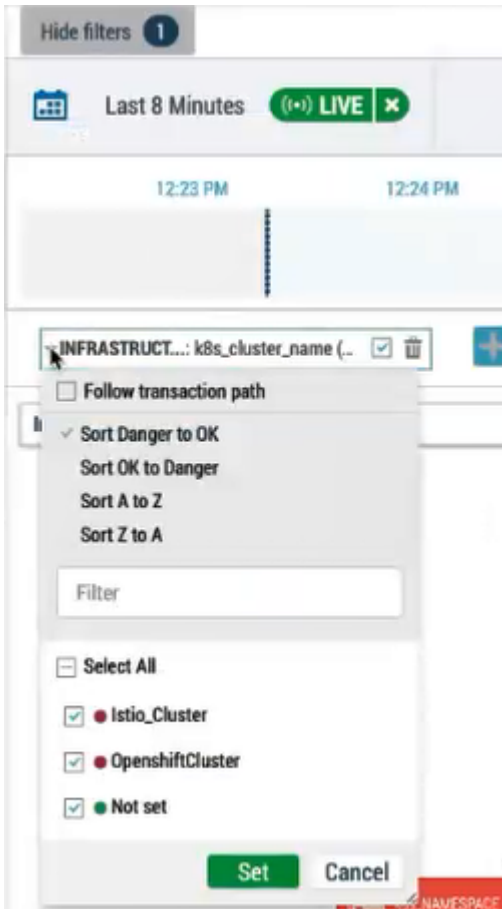
Dans la capture d'écran suivante, la couche **Infrastructure** de la carte affiche huit minutes de flux de trafic réseau Istio dans un cluster Kubernetes.

424



Utilisation de filtres pour affiner l'affichage des composants Istio Support dans la carte

Vous pouvez appliquer des filtres pour que la carte affiche des données plus spécifiques à votre examen en cours. Par exemple, vous pouvez définir un filtre pour le nom du cluster. Dans la capture d'écran, l'utilisateur a sélectionné deux noms de cluster : **Istio_Cluster** et **OpenshiftCluster**.



Procédez comme suit :

1. Dans la partie supérieure gauche de la carte, cliquez sur le côté gauche de la liste déroulante de la couche de carte **Infrastructure**.
2. Définissez un ou plusieurs filtres.
3. Cliquez sur **Définir**.

La carte affiche plus ou moins de données selon vos paramètres de filtre.

Informations complémentaires : [Couches de la carte](#).

Affichage des taux de trafic et des latences du réseau Istio Support

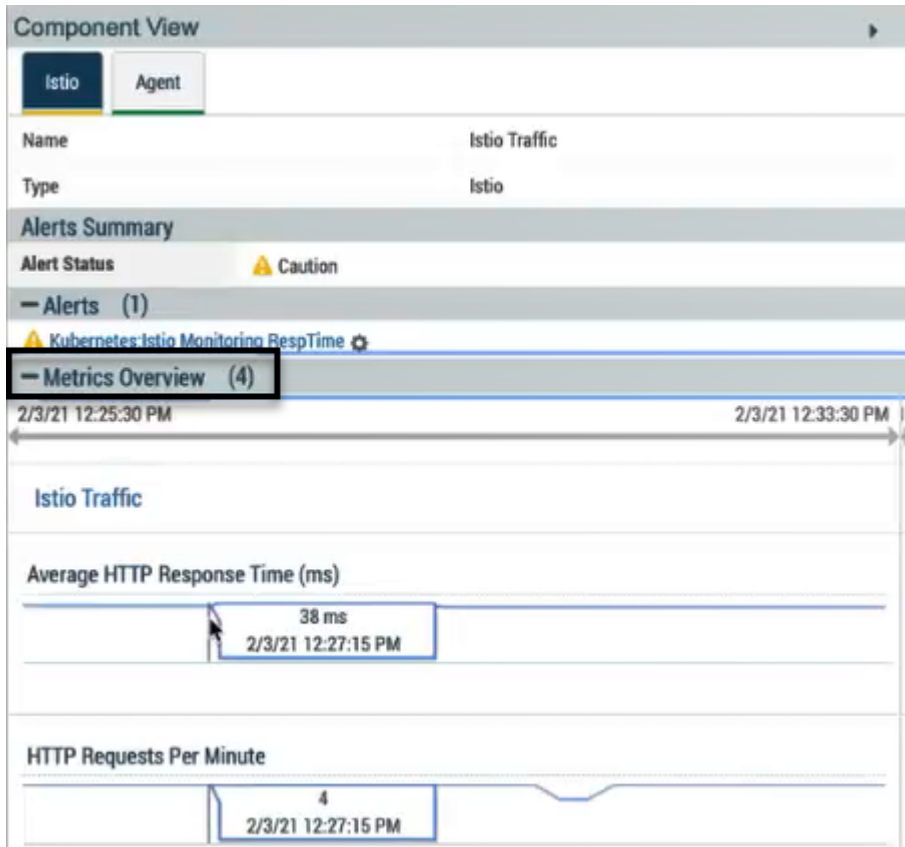
Cliquez sur un arc (ligne connectant deux composants) pour afficher la **Vue Composant**, dans laquelle vous pouvez afficher des mesures sur les taux et les latences du trafic réseau entre les composants. Dans la capture d'écran suivante, l'utilisateur a cliqué sur la ligne indiquant le trafic entrant la charge de travail **productpage-v1**. (Cette partie du trafic a déjà été présentée dans les captures d'écran précédentes utilisées comme exemples.) La **Vue Composant** s'ouvre et affiche les données relatives à une alerte et aux 18 **Attributs de base** associés à la **Présentation des mesures**.

The screenshot displays the DX APM interface. On the left, a service graph shows a component 'productpage-v1' with a green status icon. A yellow line connects this component to the 'Component View' panel on the right. The 'Component View' panel has two tabs: 'Istio' (selected) and 'Agent'. It displays the following information:

- Name:** Istio Traffic
- Type:** Istio
- Alerts Summary:** Alert Status is **Caution** (yellow triangle icon).
- Alerts (1):** A single alert is listed: **Kubernetes:Istio Monitoring RespTime** with a gear icon for settings.
- Metrics Overview:** A section titled **Basic Attributes (18)** is expanded, showing a table of attributes and their live values.

Name	Live Value
agent	Istio_Cluster ClusterPerformanceMonitor Prometh-
backendNode	true
cluster_name	Istio_Cluster
Istio_Connection_Security_Policy	mutual_tls
k8s_agent_data_source	prometheus
k8s_cluster_name	Istio_Cluster
k8s_destination_name	productpage-v1
k8s_destination_project	mongodbapp

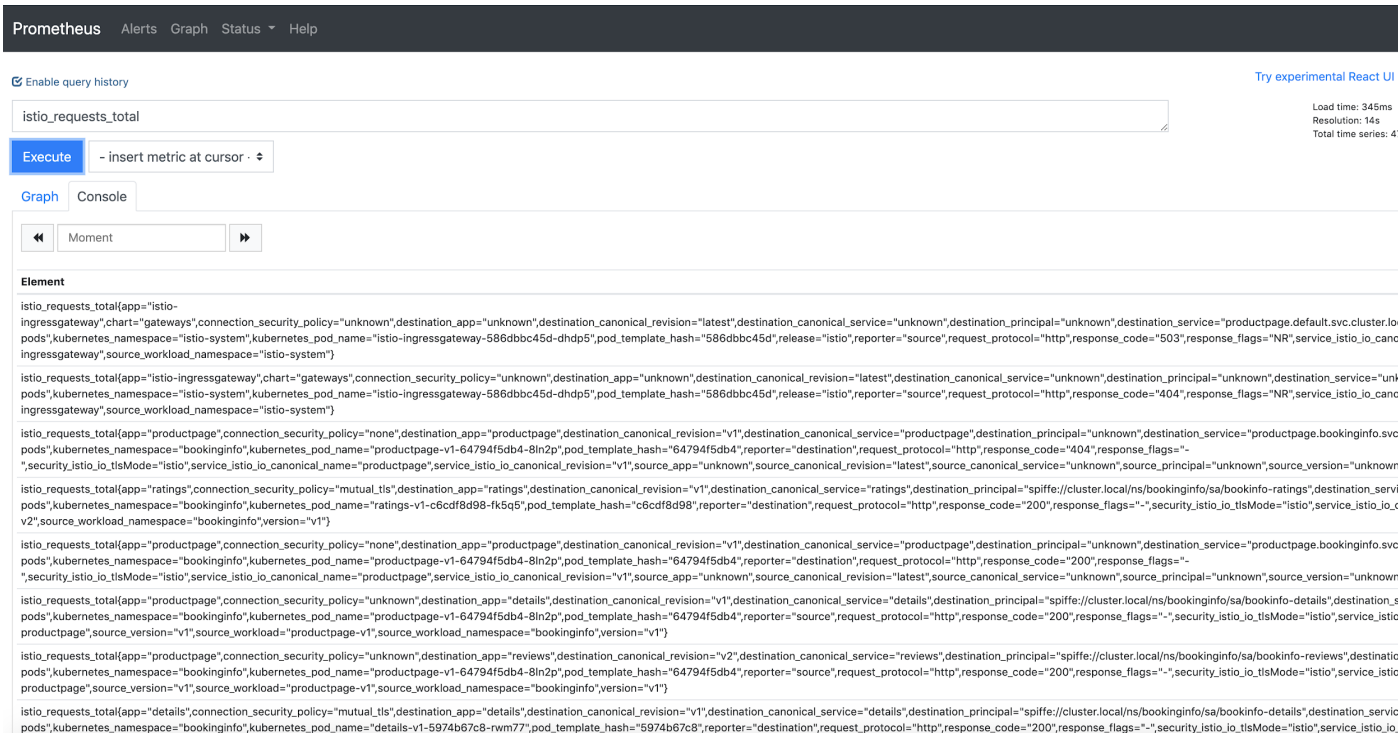
L'utilisateur a cliqué sur un arc à un autre moment pour afficher la **Vue Composant** et les mesures d'une charge de travail spécifique dans la **Présentation des mesures**. L'utilisateur souhaite examiner les mesures **Average HTTP Response Time** et **HTTP Requests Per Minute** pour une heure spécifique, comme indiqué dans la capture d'écran suivante.



Résolution des problèmes liés à Istio Support

Que ce passe-t-il ? Quel type de problèmes liés à Istio Support surviennent ? Effectuez les tâches de dépannage suivantes :

- Vérifiez les journaux du pod **cluster-performance-prometheus** et recherchez les erreurs de connexion au serveur Prometheus. S'il y a des erreurs de connexion, assurez-vous que l'utilisateur, le mot de passe et le jeton Prometheus sont corrects.
- Assurez-vous que les mesures Istio sont signalées dans Prometheus. Pour cela, connectez-vous à l'URL Prometheus et exécutez la requête **istio_requests_total**. Qu'est-ce qui apparaît dans la console ?

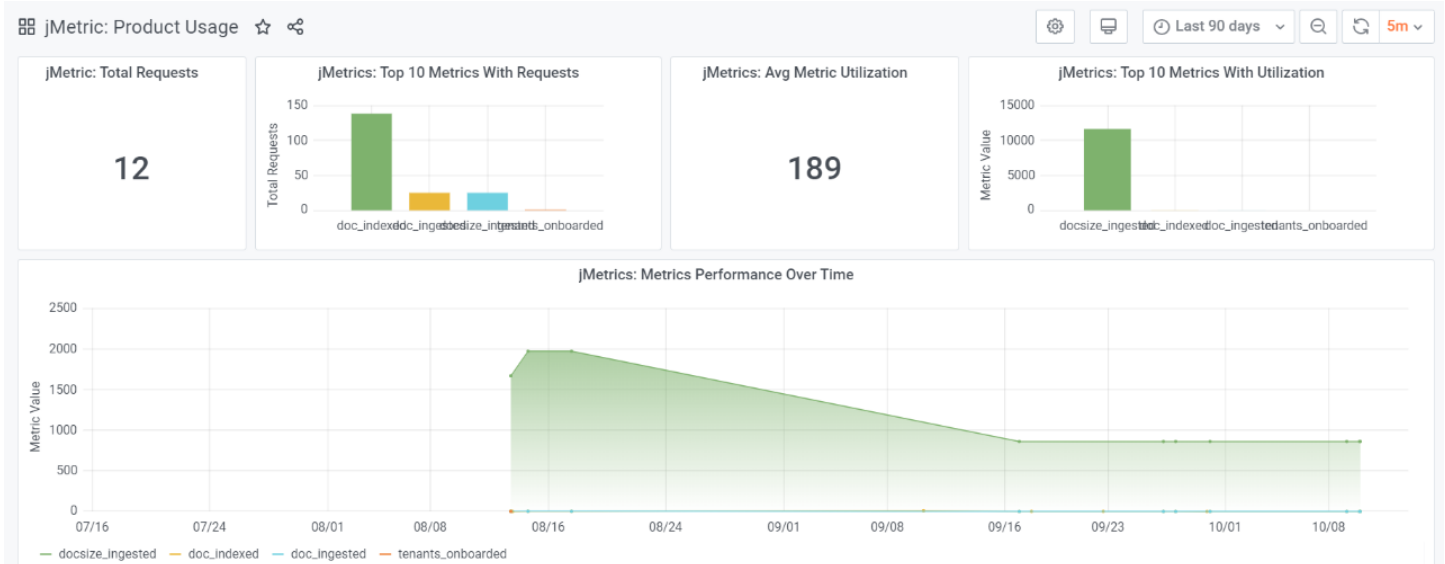


Voici un exemple pour les fichiers uma_cr.yaml et values.yaml

```
container:
  prometheus:
    exporter:
      enabled: false
    backend:
      enabled: true
    endPoint:
      url: http://10.80.89.157:30007/
      username:
      password:
      token:
      configFiles:
    metricAlias: container_name=container,pod_name=pod
```

Tableaux de bord DX

Les tableaux de bord DX sont une plate-forme de visualisation conçue pour rechercher, afficher et interagir avec les données stockées. A l'aide des tableaux de bord DX, vous pouvez créer des rapports métier complets permettant de visualiser les analyses en temps réel. Chaque *tableau de bord DX* est un ensemble de panneaux disposés dans un modèle de grille. Chaque panneau du tableau de bord interagit avec les données de la source de données et permet de visualiser vos données. Un tableau de bord permet également d'accéder aux détails.



Les tableaux de bord DX offrent les avantages suivants :

- Permet de visualiser l'inventaire, l'intégrité, les alarmes, les mesures et les journaux.
- Prise en charge de l'hébergement multient
- Prise en charge des annotations graphiques
- Possibilité, pour les utilisateurs, d'accéder aux différentes couches
- Possibilité de décortiquer le lac de données AIOps

NOTE

Les sources de données des tableaux de bord DX ne sont pas prises en charge avec une instance externe de Grafana. Cependant, vous pouvez déployer des tableaux de bord DX en tant qu'instance autonome et vous connecter à l'une des sources de données. Pour plus d'aide, contactez le **support Broadcom**.

Pour plus d'informations sur les tableaux de bord DX, reportez-vous à la documentation relative aux [tableaux de bord DX](#).

Dépannage

La section Dépannage vous permet de résoudre les symptômes problématiques dans votre implémentation.

Informations complémentaires : [Approche globale de la résolution des problèmes liés à DX Application Performance Management](#).

- [Dépannage de l'agent](#)
- [Dépannage de DX APM](#)
- [Dépannage des transactions](#)
- [Dépannage de la station de travail](#)

Dépannage de l'agent

Les informations de dépannage de l'agent comprennent les questions fréquemment posées ou associent les symptômes que rencontre l'utilisateur à une ou plusieurs solutions.

Général

- [Agent démarré mais invisible](#)
- [Echec de la détection automatique par l'agent d'un serveur d'arrière-plan connu](#)
- [L'agent surveillant un serveur frontal ne détecte pas automatiquement le serveur d'arrière-plan](#)
- [Exception ClassNotFoundException levée par l'agent lors du chargement d'extensions dynamiques](#)
- [Dépannage des problèmes de la boîte de dialogue de téléchargement d'agent](#)
- [L'en-tête de cookie de réponse de l'agent de navigateur pour .NET est-il décoré ?](#)
- [Echec du remplissage de la valeur de l'URL du serveur de configuration](#)
- [Pic du nombre de mesures](#)

Agent Java

- [Dysfonctionnement du groupement des URL](#)
- [Impossible d'instrumenter une application avec DX APM](#)
- [Arrêt brutal de l'agent Java](#)
- [Erreur de dépassement de pile de l'agent Java](#)
- [Non-détection des composants d'arrière-plan automatiques en raison d'une erreur inattendue lors du chargement de l'extension](#)
- [Le buildpack Java de Cloud Foundry ne parvient pas à trouver la version de l'agent Java demandée](#)
- [Panne du contrôleur ACC lors de la génération du rapport de diagnostic](#)

agent .NET

- [Les suivis de transaction de l'agent de navigateur et de l'agent .NET ne sont pas mis en corrélation](#)
- [Absence de mesures .NET après l'activation de l'injection automatique de snippets de l'agent de navigateur pour .NET](#)

Agent démarré mais invisible

L'agent DX APM démarre correctement, mais il n'est pas visible dans le navigateur de mesures, WebView ou le Team Center.

Symptôme :

L'agent DX APM démarre correctement, mais il n'est pas visible dans le navigateur de mesures, WebView ou le Team Center. La version du gestionnaire d'entreprise est la version 10.7.

L'agent est l'un des deux suivants :

- un agent DX APM SaaS version 20.x ou supérieure
- un agent sur site DX APM version 11.x supérieure

Ce symptôme s'applique à tout type d'agent, agent Java, agent .NET, extensions de surveillance de l'agent Infrastructure, etc.

Le journal d'agent inclut des messages d'erreur similaires aux exemples suivants :

- Le journal indique que l'agent est connecté, mais en mode non autorisé.

```
1/10/20 12:00:46 PM EST [INFO] [IntroscopeAgent.IsengardServerConnectionManager]
Connected controllable Agent to the Introscope Enterprise Manager at
em:5001,com.wily.isengard.postofficehub.link.net.DefaultSocketFactory. Host = "muntest000477",
```

```
Process = "TomcatProcess", Agent Name = "QAtestapp", Active = "false". 1/10/20
12:00:46 PM EST [INFO] [IntroscopeAgent.ConnectionThread] Connected to
em:5001,com.wily.isengard.postofficehub.link.net.DefaultSocketFactory in disallowed mode.
```

- Le journal indique que l'agent ne peut pas se connecter en raison de l'incompatibilité d'un client.

```
3/24/20 09:41:05 AM UTC [WARN] [IntroscopeAgent.ConnectionThread] Failed to connect to the Introscope
Enterprise Manager at em:5001,com.wily.isengard.postofficehub.link.net.DefaultSocketFactory
(com.wily.isengard.postofficehub.auth.FailedToAuthenticateException:Invalid credentials for group name
'Agent'. Perhaps the client is not compatible with the server.).
```

Solution :

L'agent de version supérieure tente de se connecter au gestionnaire d'entreprise CA APM 10.7, mais il n'y parvient pas en raison d'une incompatibilité de version. Mettez à jour le fichier `IntroscopeAgent.profile` pour l'agent DX APM SaaS ou de l'agent sur site DX APM, en fonction de votre environnement. Cette solution s'applique à tout type d'agent, agent Java, agent .NET, extensions de l'agent Infrastructure, etc.

Configuration de tous les agents excepté des applications Java dans Cloud Foundry

1. Accédez au fichier `<répertoire_base_agent>\releases\<numéro_version>\core\config\IntroscopeAgent.profile` de l'agent SaaS DX APM ou de l'agent sur site DX APM.
2. Ouvrez le fichier `IntroscopeAgent.profile` dans un éditeur de texte.
3. Ajoutez la propriété `introscope.agent.connection.compatibility.version=10.7`.
4. Annulez la définition de la propriété `agentManager.credential`.

La configuration `introscope.agent.connection.compatibility.version=10.7` fournit une compatibilité uniquement lorsque la propriété `agentManager.credential` est commentée ou non configurée. Voici deux exemples :

```
#agentManager.credential=<your agent token>
agentManager.credential=
```

Si vous ne parvient pas à définir correctement `agentManager.credential`, une erreur **FailedToAuthenticateException** se produit.

NOTE

Lors de la configuration des informations d'identification de l'agent à l'aide du fichier `IntroscopeAgent.profile` ou des arguments de machine virtuelle, n'utilisez pas de guillemets doubles (") pour saisir une valeur vide pour la propriété `agentManager.credential`. Par exemple, `agentManager.credential=`.

5. Supprimez le protocole **ws://** ou **wss://** du début de la propriété `agentManager.url`.

Pour utiliser l'agent DX APM avec un gestionnaire d'entreprise CA APM 10.7, vous devez supprimer le protocole **ws** de la propriété `agentManager.url.1`. Ce changement de configuration permet à l'agent DX APM d'utiliser le protocole TCP par défaut de CA APM 10.7 pour la communication par socket directe.

Exemple de configuration incorrecte :

```
agentManager.url.1=ws://apmhost:5001
```

Exemple de configuration correcte :

```
agentManager.url.1=apmhost:5001
```

Si vous ne supprimez pas le protocole **ws** de la chaîne de propriété, un message d'erreur semblable à celui ci-après s'affiche :

```
9/25/20 08:00:02 PM EDT [WARN] [IntroscopeAgent.ConnectionThread] Failed
to connect to the Introscope Enterprise Manager at <APM services gateway
URL>,com.wily.isengard.client.transport.websocket.WebSocketFactory (java.io.IOException:Connection
```

6. Enregistrez le fichier `IntroscopeAgent.profile`.

7. Redémarrez l'application gérée.

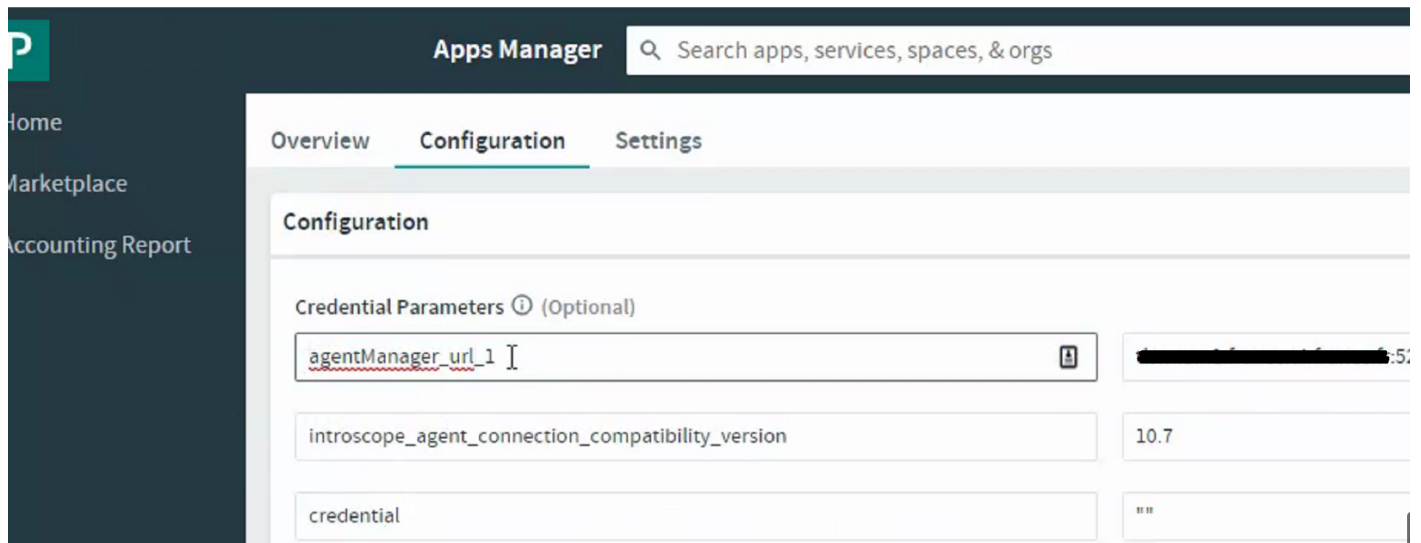
Applications Java dans Cloud Foundry

Lorsque vous surveillez des applications Java dans Cloud Foundry, configurez la compatibilité à l'aide de l'une des options ci-dessous :

- Exécutez cette commande dans une ligne de commande Cloud Foundry :

```
cf cups introscope -p '{"agent_manager_url":"host:port",
"introscope_agent_connection_compatibility_version":"10.7", "credential":""}'
```

- Mettez à jour la configuration dans Pivotal Web Services (PWS) Apps Manager en procédant comme illustré dans ce graphique et comme décrit dans les étapes suivantes.



- Accédez à l'onglet **Configuration**.
- Dans le champ **Credential Parameters (Optional)** (Paramètres d'informations d'identification (facultatif)), entrez la valeur suivante :
`agentManager_url_1`
- Assurez-vous que le champ à *droite* du champ **Credential Parameters (Optional)** (Paramètres d'informations d'identification (facultatif)) est vide.
- Dans le champ *sous* le champ **Credential Parameters (Optional)** (Paramètres d'informations d'identification (facultatif)), entrez la valeur suivante :
`introscope_agent_connection_compatibility_version`
- Dans le champ à *droite* de `introscope_agent_connection_compatibility_version`, entrez la valeur suivante :

10.7

6. Dans le champ *sous* de `introscope_agent_connection_compatibility_version`, entrez la valeur suivante :

`credential`

7. Dans le champ à *droite* de `credential`, saisissez cette valeur (apostrophes doubles) :
""

NOTE

Lors de la configuration des informations d'identification de l'agent pour les applications Java dans Cloud Foundry à l'aide de l'interface utilisateur de Pivotal Web Services (PWS) Apps Manager, utilisez des guillemets doubles ("") pour saisir une valeur vide pour la propriété `agentManager.credential`. Par exemple, `agentManager.credential=""`.

8. Enregistrez la configuration.
9. Redémarrez l'application gérée.

Echec de la détection automatique par l'agent d'un serveur d'arrière-plan connu

Symptôme

Je sais qu'une transaction inclut un serveur d'arrière-plan surveillé, mais l'agent ne le détecte pas automatiquement.

Le journal de niveau INFO de l'agent ne contient pas les messages sur la détection de candidats d'arrière-plan. Je pensais pourtant pouvoir y trouver un message comme l'exemple suivant :

```
[INFO] [IntroscopeAgent.AutomaticBackendDetection] Backend Candidates: [<my-expected backend1>,<my-expected backend2>...]
```

Ces mesures de durabilité de l'agent affichent la valeur 0 :

- Automatic Backend Detection: Analyzed Stack Snapshots (Détection automatique de serveur d'arrière-plan : Clichés de pile analysés)
- Automatic Backend Detection: Backends Discovered (Détection automatique de serveur d'arrière-plan : Serveurs d'arrière-plan détectés)

Solution

La détection automatique de serveur d'arrière-plan requiert que l'agent détecte d'abord et surveille un type de serveur frontal. Vérifiez que la transaction surveille un serveur frontal, un point d'entrée ou un composant personnalisé.

NOTE

L'agent peut avoir besoin de quelques minutes pour détecter et gérer automatiquement une transaction qui inclut des serveurs d'arrière-plan automatiques.

L'agent surveillant un serveur frontal ne détecte pas automatiquement le serveur d'arrière-plan

Symptôme

Une transaction que j'analyse comprend un serveur frontal surveillé et un serveur d'arrière-plan non surveillé. L'agent ne détecte pas le serveur d'arrière-plan.

Valeurs de mesures de prise en charge de l'agent approprié :

- Sustainability|Automatic Backend Detection: Analyzed Stack Snapshots is > 0.
- Sustainability|Automatic Backend Detection: Backends Discovered is 0.

Solution

Ajoutez une instrumentation personnalisée pour surveiller le serveur d'arrière-plan.

Il est possible que la détection automatique de composants d'arrière-plan ne détecte pas les composants d'arrière-plan dans les cas peu fréquents, par exemple, lors d'appels de communication de socket via des sockets datagramme.

Exception ClassNotFoundException levée par l'agent lors du chargement d'extensions dynamiques

Symptôme

Lorsque vous supprimez rapidement des extensions dynamiques et que vous les ajoutez au répertoire `<répertoire_base_agent>/extensions/deploy`, l'agent génère l'erreur `ClassNotFoundException`. Le journal d'agent affiche un message d'erreur similaire au suivant :

```
9/30/16 01:41:43 AM PDT [ERROR] [IntroscopeAgent.Agent] Unable to create tracer factories for the following
class (library not found): com.wily.introscope.agent.trace.test.tracer.TestTracer3
```

Solution

1. Déchargez toutes les extensions dynamiques dans le répertoire `<répertoire_base_agent>/extensions/deploy` en attente de chargement pour le déploiement.
2. Vérifiez que toutes les extensions dynamiques sont déchargées.
3. Rechargez les extensions dynamiques dans le répertoire `<répertoire_base_agent>/extensions/deploy`.

Les suivis de transaction de l'agent de navigateur et de l'agent .NET ne sont pas mis en corrélation

Symptôme

Le suivi de transaction de l'agent de navigateur n'est pas mis en corrélation avec le suivi de transaction de l'agent .NET. Ce problème survient, car l'agent .NET ignore automatiquement le codage `.gzip`.

Solution

Examinez le type de contenu de réponse pour la propriété d'encodage non prise en charge :

```
introscope.agent.browseragent.encodings.skip.
```

Echec du remplissage de la valeur de l'URL du serveur de configuration

Symptôme

L'URL de serveur de configuration définie sur le contrôleur Agent dans ACC est manquante lorsque vous téléchargez le package et que vous le déployez sur les serveurs.

Ce problème survient lorsqu'aucun schéma (HTTPS ou WS(S)) n'est ajouté à l'URL. La chaîne de connexion est considérée comme héritée et utilisée pour la communication Isengard (le port par défaut est 5001). Le contrôleur ACC communique uniquement par le biais de l'appel REST via HTTP(S)/WS(S).

Solution

Vous devez activer HTTP(S)/WS(S) sur le proxy cloud en suivant l'un des processus suivants :

- Activez HTTP(S)/WS(S) sur le proxy cloud et utilisez une connexion via HTTP(S)/WS(S). Vous pouvez mettre à jour le proxy cloud dans le volet de création de package pour que l'URL de connexion soit définie pour les groupes em-connection et acc-controller.
- Activez HTTP(S)/WS(S) sur le proxy cloud et définissez l'URL de connexion dans la propriété `introscope.agent.acc.controller.configurationServer.url` du groupe acc-controller.

L'en-tête de cookie de réponse de l'agent de navigateur pour .NET est-il décoré ?

L'en-tête de cookie de réponse de l'agent de navigateur pour .NET est-il décoré ?

Symptôme :

Je ne parviens pas à déterminer si l'en-tête de cookie de réponse de l'agent de navigateur pour .NET est décoré.

Solution :

Examinez si l'agent .NET a envoyé le cookie de réponse. Appuyez sur la touche **<F12>** et vérifiez dans le navigateur.

Arrêt brutal de l'agent Java

Symptôme

L'agent Java s'arrête brutalement, se bloque ou entraîne une surcharge ou une utilisation élevée de l'UC.

Solution

Les problèmes rencontrés par l'agent peuvent être le résultat de :

- Une configuration non prise en charge.
- Un bogue de machine virtuelle Java qui se produit à cause de l'utilisation de DX APM du mécanisme d'instrumentation de plate-forme Java pour la surveillance.
- Une explosion du nombre des instrumentations ou des mesures

Pour résoudre ces problèmes, essayez les propositions suivantes :

- Un élément a-t-il été mis à jour récemment ?
- Y a-t-il une instrumentation ou une extension personnalisée implémentée par les services professionnels de Broadcom ?
- La configuration est-elle prise en charge ?
- Déterminez si le problème est lié à un bogue de l'instrumentation ou de la machine virtuelle Java comme suit :
 - a. Arrêtez le serveur d'applications.
 - b. Ouvrez `IntroscopeAgent.profile` et définissez le paramètre `introscope.autoprobe.enable=false`.
 - c. Démarrez le serveur d'applications.

Si le problème persiste, il n'est PAS lié à l'instrumentation de DX APM. Essayez les solutions suivantes :

 - Essayez de basculer de `-javaagent` vers `-Xbootclasspath`.
 - Procédez à la mise à niveau vers la dernière version de JVM ou utilisez une autre JVM.
 - Ouvrez un incident auprès du support du fournisseur de machine virtuelle Java.
- Pour vous aider à identifier la cause du problème, réduisez temporairement le nombre d'instrumentations :
 - a. Arrêtez le serveur d'applications.
 - b. Ouvrez `IntroscopeAgent.profile` et définissez le paramètre `introscope.autoprobe.enable=false`.
- Certaines applications utilisent un nombre élevé de chaînes d'instruction SQL uniques, en particulier lors de la génération dynamique de la requête SQL. Cette action entraîne une explosion du nombre de mesures de l'agent SQL. A des fins de test, désactivez l'agent SQL en supprimant le fichier `<répertoire_base_agent>`

`core/ext/SQLAgent.jar` du répertoire de l'AGENT. Si cette action n'est pas possible, définissez `introscope.agent.sqlagent.sql.maxlength=120` (valeur par défaut, 990).

Ne définissez aucune limite pour la longueur des instructions SQL autres que celles imposées par la base de données, car `maxlength` permet de tronquer la longueur des instructions SQL. L'objectif de cette action est d'empêcher une explosion du nombre des mesures SQL.

- Désactivez les outils de suivi du réseau, du système de fichiers et des mesures de système de fichiers dans `toggles.PBD`. Leur activation n'est pas recommandée dans un environnement de production.


```
# TurnOn: SocketTracing
# TurnOn: UDPTracing
# TurnOn: FileSystemTracing
```
- Désactivez la collecte de données JMX. L'interrogation d'un grand nombre de mesures JMX supposent une utilisation intensive de l'UC.

Si possible, définissez `introscope.agent.jmx.enable=false`.

Ne définissez jamais la chaîne de filtre sur null (par exemple, `introscope.agent.jmx.name.filter=`)

Un seul agent peut produire des dizaines de milliers de mesures JMX si aucun filtre n'est défini.
- Désactivez les autres modules complémentaires de l'agent Java, tels que `ErrorDetector`, `Leakhunter` ou d'autres extensions.

`Leakhunter` est un outil de diagnostic, pas un outil de surveillance. Recommandation : ne l'activez pas dans un environnement de production.

Les extensions peuvent générer un grand nombre de mesures, ce qui peut entraîner une surcharge élevée.
- Désactivez les `.pbd` personnalisés restants.

Évitez d'utiliser les directives `TraceAllMethodsOfClass` et `TraceComplexMethodsOfClass`.

Choisissez avec précaution les méthodes à surveiller.

Collectez les informations suivantes avant de contacter le support clientèle de Broadcom si le problème persiste :

- `<répertoire_base_agent>/logs` dans un fichier `.zip`
- `IntroscopeAgent.profile`
- Générez cinq images mémoire de thread sur le serveur d'applications en cas de surcharge, de mémoire insuffisante, de blocage ou d'utilisation élevée d'UC, espacés de 5 à 10 secondes.
- Pour les problèmes de surcharge, générer une image de segment mémoire. Pour la JVM Sun, ajoutez le paramètre de machine virtuelle Java suivant :


```
XX:+HeapDumpOnOutOfMemoryError
```

Redémarrez l'agent.
- Activez le journal GC. Pour la JVM Sun, ajoutez les paramètres de machine virtuelle Java suivants :


```
-Xloggc:<File_Name>.log -XX:+PrintGCDetails
```
- Fichiers journaux du serveur d'applications à envoyer au support de Broadcom :
 - `WebSphere` : `System.out`, `system.err`, `native_stdout`, `native_stderr`, et `server.xml`
 - `WebLogic` : fichier journal et script de démarrage du serveur d'applications
 - `Tomcat` : fichier journal et `catalina.sh/bat`
 - `JBoss` : fichier journal et `run.bat/sh`
- Image mémoire de l'intégralité du noyau, le cas échéant

Erreur de dépassement de pile de l'agent Java

Valide pour : DX APM 8.x, 9.x

Symptôme

Une transaction échoue sur une application surveillée et un message `StackOverflowError` est enregistré dans le journal du serveur d'applications.

Solution

L'agent ajoute des instructions à une application en cours d'exécution. Lorsqu'une application avec un chemin d'appel récursif approfondi a une taille de pile proche de la valeur maximale, les instructions de l'agent ajouté peuvent dépasser la limite de taille de la pile.

1. Augmentez la taille de pile de la machine virtuelle Java dans l'argument de démarrage Java `-Xss`. Exemple :
`-Xss10024k`
2. Redémarrez le serveur d'applications.

Absence de mesures .NET après l'activation de l'injection automatique de snippets de l'agent de navigateur pour .NET

Symptôme :

Je ne vois pas aucune mesure .NET après l'activation de l'injection automatique de snippets de l'agent de navigateur pour .NET.

Solution :

Examinez la source dans votre navigateur. Recherchez la balise du script de l'agent de navigateur.

Non-détection des composants d'arrière-plan automatiques en raison d'une erreur inattendue lors du chargement de l'extension

Symptôme

Les composants d'arrière-plan automatiques ne sont pas détectés. Un message d'erreur similaire à l'exemple ci-dessous s'affiche dans le journal de l'agent, car la version de la machine virtuelle Java n'est pas compatible.

```
[ERREUR] [Agent.Introscope.Agent] Erreur inattendue du chargement de l'extension
java.lang.UnsupportedClassVersionError: com/wily/introscope/agent/intelligent/entrypoint/
tracers/AbstractDetectionHelperTracer : Version 51.0 major.minor non prise en charge
```

Solution

Vérifiez que la version de la machine virtuelle Java est 1.7 ou une version ultérieure.

Pic du nombre de mesures

Symptôme

Les valeurs de pic sont des valeurs cumulées et non distinctes.

Solution

L'API Web Timing signale le temps réseau dans le cadre d'un téléchargement de page précédente. L'agent de navigateur (anciennement BRTM) ne peut pas exclure ces valeurs.

Impossible d'instrumenter une application avec DX APM

Symptôme

Je ne parviens pas à instrumenter une application avec DX APM.

Solution

Vérifiez les éléments suivants :

- Le script de démarrage ou les fichiers de configuration du serveur d'applications contiennent les deux entrées clés de DX APM :

```
-javaagent and - Dcom.wily.introscope.agentProfile
```
- Un fichier journal existe sous `\wily\logs` . Si c'est le cas, examinez le fichier `Autoprobe.log` . Si la taille est 0 ou 1 Ko, vous utilisez probablement un fichier `.pbd` personnalisé ou vous en avez modifié un de manière incorrecte.

Données à collecter avant de contacter le support Broadcom

Si vous avez appliqué les suggestions précédentes et que vous rencontrez encore des problèmes, collectez les données suivantes avant de contacter le support Broadcom. Ces informations permettront au support Broadcom de vous aider de manière efficace.

- `<répertoire_base_agent>\logs` dans un fichier `.zip`
- Fichier journal du serveur d'applications
- Script de démarrage ou fichier de configuration du serveur d'applications qui contient les entrées de DX APM

Dysfonctionnement du groupement des URL

Symptôme

Le groupement des URL ne fonctionne pas.

Solution

Examinez les problèmes connus dans les Notes de publication sur le [regroupement des URL](#). Testez le problème à l'aide d'une définition de groupement d'URL simple.

Collectez les informations suivantes avant de contacter le support clientèle si le problème persiste :

- `<répertoire_base_EM>/logs/*` dans un fichier `.zip`. Ces fichiers vous aident à déterminer si le problème est lié aux performances.
- Fichier `IntroscopeAgent.profile`
- Capture d'écran de l'exemple d'onglet Investigator des URL

Le buildpack Java de Cloud Foundry ne parvient pas à trouver la version de l'agent Java demandée

Symptôme

Lors du déploiement d'une application Java sur Cloud Foundry, vous devez mettre à jour le fichier manifeste de l'application vers la version 10.x en exécutant la commande suivante :

```
JBP_CONFIG_INTROSCOPE_AGENT: '{ version: 10.x.0_xx}
```

Vous exécutez la commande **cf push** pour obtenir le buildpack Java contenant l'agent Java 10.x. L'interface de ligne de commande de Cloud Foundry affiche un message **No version resolvable error** similaire à l'exemple ci-dessous :

```
[Buildpack]      ERROR Detect failed with exception #<RuntimeError: Introscope Agent error: No version
resolvable for '10.7.0_70' in 10.5.2_15, 10.5.1_6, 10.5.0_20, 10.3.0_15, 10.2.0_27, 10.1.0_15, 10.0.0_16>
Introscope Agent error: No version resolvable for '10.7.0_70' in 10.5.2_15, 10.5.1_6, 10.5.0_20, 10.3.0_15,
10.2.0_27, 10.1.0_15, 10.0.0_16 [meta-buildpack] No other buildpack selected
[Buildpack]      ERROR Detect failed with exception #<RuntimeError: Introscope Agent error: No version
resolvable for '10.7.0_70' in 10.5.2_15, 10.5.1_6, 10.5.0_20, 10.3.0_15, 10.2.0_27, 10.1.0_15, 10.0.0_16>
Introscope Agent error: No version resolvable for '10.7.0_70' in 10.5.2_15, 10.5.1_6, 10.5.0_20, 10.3.0_15,
10.2.0_27, 10.1.0_15, 10.0.0_16
Error staging application: An app was not successfully detected by any available buildpack
FAILED
[root
```

Solution

Vous utilisez un buildpack Java hors ligne. Les buildpacks hors ligne ne contiennent pas toutes les versions de l'agent Java. Si vous souhaitez utiliser une version antérieure ou ultérieure de l'agent Java, téléchargez et utilisez la version appropriée du buildpack hors ligne.

Les buildpacks Java hors ligne peuvent être téléchargés ici : <https://github.com/cloudfoundry/java-buildpack/releases>. Vous pouvez également utiliser le buildpack Java en ligne.

NOTE

Informations complémentaires : [Déploiement et surveillance d'une application Java sur Cloud Foundry](#)

Dépannage des problèmes de la boîte de dialogue de téléchargement d'agent

La liste suivante répertorie les causes possibles des problèmes d'affichage et les actions à effectuer pour les corriger :

- **Les propriétés de configuration ne s'affichent pas.**
 - Examinez le journal ACC pour consulter les erreurs et avertissements relatifs au contenu de la boîte de dialogue de téléchargement.
 - Analysez le fichier downloadPackageConfig.json et recherchez les erreurs de configuration.
- **Le contenu n'est pas localisé.**
 - Examinez le journal ACC pour consulter les erreurs et avertissements relatifs au contenu de la boîte de dialogue de téléchargement.
 - Examinez les fichiers de propriétés pour les clés manquantes ou non localisées.
- **Le format des instructions d'installation est incorrect.**
 - Vérifiez la syntaxe du contenu Markdown dans le fichier de propriétés.
 - Assurez-vous que les clés d'instructions d'installation ont un suffixe Markdown.
- **La liste des applications AXA n'est pas visible dans la configuration de l'agent de navigateur.**
 - **Cause possible :**
 - AXA n'est pas disponible.
 - L'intégration AXA n'est pas correctement configurée.
 - **Essayez ce qui suit :**
 - Vérifiez la configuration d'EM.
 - Recherchez des erreurs dans la console de développeur du navigateur.

Dépannage de DX APM

Les informations de dépannage de DX APM comprennent les questions fréquemment posées ou associent les symptômes que rencontre l'utilisateur à une ou plusieurs solutions.

[Non-affichage des mesures de composant](#)

[L'écart de l'analyse différentielle ne s'affiche pas sur les noeuds](#)

[Aucune donnée de mesure dans la vue Expérience](#)

[Données incomplètes ou manquantes envoyées par les agents dans la carte](#)

[Affichage incorrect des informations sur l'agent dans la carte](#)

[La carte affiche seulement 50 000 noeuds](#)

[Absence d'attributs liés à Docker dans le sélecteur d'attributs de fiche d'expérience](#)

[Dysfonctionnement de la propagation intercouche des attributs](#)

[Recherche des problèmes potentiels liés aux cartes](#)

Non-affichage des mesures de composant

Symptôme

Les mesures ne sont pas affichées pour un composant.

Solution

Nommez les composants avec un maximum de 250 caractères. Si un nom de composant dépasse 250 caractères, il est tronqué à 250 caractères. Par conséquent, les noeuds associés n'affichent pas les mesures et les alertes associées lorsque l'attribut de nom est utilisé pour calculer la mesure. Par exemple, SOCKET, EJBCLIENT, DATABASE, BUSINESSTRANSACTION, GENERICBACKEND, GENERICFRONTEND.

L'écart de l'analyse différentielle ne s'affiche pas sur les noeuds

Symptôme

Les mesures de l'écart de l'analyse différentielle n'apparaissent pas sur les noeuds.

Solution

Le statut de l'analyse différentielle n'est pas associé à une mesure lorsque le chemin de la mesure dépasse 1 000 caractères. Les configurations de l'analyse différentielle et la barre d'analyse différentielle ne sont pas visibles dans la présentation des performances de ces mesures.

Aucune donnée de mesure dans la vue Expérience

Symptôme

Impossible d'afficher les données dans la vue Expérience. L'erreur suivante apparaît dans le navigateur :

```
That's a lot of data. The number of metrics exceeds the display maximum.
```

Ce message erreur s'affiche lorsque vous tentez d'afficher plus de 500 transactions métier en mode Dynamique ou plus de 50 transactions métier en mode Historique. La vue Expérience limite le nombre de transactions métier pour des raisons de performances.

Solution

Il existe plusieurs façons de limiter le nombre de transactions métier affichées.

- Accédez à d'autres niveaux des fiches d'expérience. Le niveau suivant affiche les mesures, car le nombre de transactions métier est moindre.
- Appliquez des filtres au niveau supérieur des fiches d'expérience.
- Créez des univers avec moins de transactions métier.

Données incomplètes ou manquantes envoyées par les agents dans la carte

Symptôme

Après la connexion d'un nouvel agent ou le déploiement d'une nouvelle application, la topologie correspondante n'apparaît pas dans la carte, ou seules des données partielles s'affichent immédiatement. Les données complètes s'affichent après une ou deux minutes.

Solution

Lancez un suivi de transactions sur l'agent pour accélérer la collection initiale des données dans la **vue Carte**. Lorsque vous exécutez un suivi de transactions sur un agent, vous collectez un volume de traces élevé. Cette action permet au serveur de recréer rapidement la vue Carte. Pour exécuter une session de suivi de transaction manuellement, spécifiez les agents pour lesquels vous souhaitez effectuer le suivi des transactions et la période de capture des données. Une fois la session de suivi de transaction lancée, les transactions correspondant aux critères de filtre s'affichent dans la visionneuse des traces de transaction. Les événements de transaction incluent des traces et des erreurs de transaction.

Lorsque le suivi est lancé pendant une durée, la session s'arrête à la fin de la période spécifiée. Vous pouvez uniquement démarrer une session de suivi pour un agent spécifié pendant une période donnée. Si vous relancez une session de suivi active, une notification vous rappelle que la session de suivi de transaction est déjà active pour l'agent. La notification affiche le temps restant dans la session active. Vous pouvez lancer un nouveau suivi pour l'agent même après la fin d'une session de suivi active.

Procédez comme suit :

1. Dans le volet gauche sous Paramètres, cliquez sur **Agents**.
La page Agents s'affiche et répertorie les agents.
2. (Facultatif) Cliquez sur la flèche **Applications**.
Toutes les applications surveillées par l'agent sont répertoriées.
3. Sélectionnez un ou plusieurs agents pour lesquels vous souhaitez effectuer un suivi de transactions :
 - Pour suivre tous les agents, cliquez sur **Effectuer le suivi de tous les agents**. Cette option permet d'effectuer le suivi des agents pris en charge et actuellement connectés, ainsi que des agents qui se connectent pendant la session de suivi.
 - Pour suivre des agents sélectionnés, cliquez sur **Effectuer le suivi de l'agent** pour un agent.
La session de suivi de transaction s'affiche.
4. Spécifiez des valeurs pour le suivi de transactions dans les champs de la boîte de dialogue ou acceptez les valeurs par défaut et cliquez sur **Lancer** :
 - Spécifiez la **durée minimum des transactions** en millisecondes pour le suivi de transactions. La valeur par défaut est 1000 millisecondes. La valeur minimum est 1 milliseconde.
 - Spécifiez la **durée de la session de suivi** en minutes. La valeur par défaut est 1 minute avec une durée maximum de 5 minutes pour une session de suivi.

Un volet affiche le statut de la session.

5. (Facultatif) Fermez la boîte de dialogue après le lancement d'un suivi.
L'exécution de la session de suivi continue en arrière-plan.

NOTE

Informations complémentaires :

[Analyse des données de suivi et collaboration pour l'analyse des problèmes](#)

Affichage incorrect des informations sur l'agent dans la carte

Symptôme

La carte n'affiche pas correctement les informations sur l'agent.

Solution

Synchronisez les horloges système pour tous les agents que surveille DX APM pour un chemin transactionnel spécifique.

Nous vous recommandons de synchroniser les horloges de vos serveurs d'applications à l'aide du protocole NTP (Network Time Protocol).

La carte affiche seulement 50 000 noeuds

Symptôme

La carte affiche seulement 50 000 noeuds.

Solution

DX APM est configuré pour afficher les cartes avec un maximum de 50 000 noeuds afin de maintenir les performances. Au-delà de cette limite, les données sont bloquées.

Procédez comme suit :

1. Cliquez sur Tableau de bord.
2. Ajoutez des filtres pour réduire le nombre de noeuds affichés sous 50 000.

Absence d'attributs liés à Docker dans le sélecteur d'attributs de fiche d'expérience

Symptôme

Lorsque vous créez ou modifiez une fiche d'expérience, les attributs liés à Docker ne figurent pas dans la liste déroulante.

Solution

Dans la **vue Carte**, consultez Expérience pour vérifier si une Expérience contient des attributs qui n'apparaissent pas dans la liste déroulante.

NOTE

Informations complémentaires :

- [KB000115511 : Attributs et fiches d'expérience de Docker pour APM 10.7](#)
- [Configuration de la vue Expérience](#)

Dysfonctionnement de la propagation intercouche des attributs

Symptôme

La propagation des attributs de la couche Infrastructure vers la couche Application ne fonctionne pas.

Solution

Consultez la **Vue Composants** pour vérifier que les noeuds relatifs sont connectés et qu'ils partagent les attributs.

NOTE

Informations complémentaires :

- [KB000115511 : Attributs et fiches d'expérience de Docker pour APM 10.7](#)
- [Configuration de la vue Expérience](#)

Recherche des problèmes potentiels liés aux cartes

Vous pouvez vérifier les points suivants pour rechercher d'éventuels problèmes liés aux cartes :

- Ouvrez la console du développeur et recherchez des exceptions.
- En cas d'erreur de serveur interne 500, recherchez des informations supplémentaires dans la réponse du serveur.

Dépannage des transactions

Les informations de dépannage des transactions comprennent les questions fréquemment posées ou associent les symptômes que rencontre l'utilisateur à une ou plusieurs solutions.

[Identification d'une méthode qui ne se ferme jamais en tant que méthode parent](#)

Identification d'une méthode qui ne se ferme jamais en tant que méthode parent

Symptôme

Après avoir identifié la méthode parent d'un appel JMS Receive comme indiqué dans la section [Mesures de transaction](#), une méthode qui ne se ferme jamais est identifiée en tant que parent.

Solution

Définissez la méthode parent manuellement en utilisant l'une des procédures suivantes :

- Ouvrez le fichier `JMSParentMethodPersist.pbd` dans le dossier **hotdeploy** dans un éditeur de texte et ajoutez la définition de suivi de méthode parent dans la partie inférieure :

```
TraceOneMethodOfClass: <class name> <method> JMSReceiveParentTracer "JMSParentInstrumentation"
```

- Définissez la valeur d'index constante (reportez-vous à l'étape 2 ci-dessus) sur la valeur qui appartient à la méthode correcte parent telle qu'elle apparaît dans la trace de pile en modifiant la valeur de la propriété `jms.receive.parent.lookupFallback.maximumDepth` dans le fichier de profil d'agent.

Dépannage de la station de travail

Les informations de dépannage de la station de travail comprennent les questions fréquemment posées ou associent les symptômes que rencontre l'utilisateur à une ou plusieurs solutions. Voici quelques-uns des articles de dépannage :

[Erreur au niveau de la station de travail lors de la collecte d'un nouveau vidage de threads](#)

[Modification des types d'opérations dans les outils de calcul des modules de gestion](#)

[Panneaux vides dans les tableaux de bord](#)

[Aucun résultat pour une requête sur les événements historiques](#)

[Dépannage des problèmes d'expiration de session automatique dans la station de travail](#)

[Expiration du délai de la station de travail lors de la connexion au gestionnaire d'entreprise](#)

Erreur au niveau de la station de travail lors de la collecte d'un nouveau vidage de threads

Erreur au niveau de la station de travail

Symptôme : lorsque l'agent Tomcat s'exécute avec une taille de segment de mémoire de 50 Mo, l'erreur **ConnectionExceptionErrorStatus** apparaît dans la station de travail et les journaux EM affichent le journal d'erreurs ci-après.

```
[ERROR] [PO:main Mailman 5] [Manager.MessageServiceClient] Exception: java.lang.OutOfMemoryError: Java
heap space calling method: com.wily.isengard.messageprimitives.service.MessageServiceCallMessage:
{com.wily.introscope.threaddump.common.IAgentThreadDumpService.getThreadDump, v1, [lvnqa002872|TomcatProcess|
Tomcat Agent, manual], source: Server.main:409, remoteHost: {Unknown}}
com.wily.isengard.messageprimitives.ConnectionException
    at
com.wily.isengard.messageprimitives.service.MessageServiceClient.sendRequest(MessageServiceClient.java:197)
    at com.wily.isengard.messageprimitives.service.MessageServiceClient.invoke(MessageServiceClient.java:359)
    at com.sun.proxy.$Proxy269.getThreadDump(Unknown Source)
    at com.wily.introscope.threaddump.em.ThreadDumpImpl.getAgentThreadDump(ThreadDumpImpl.java:142)
    at com.wily.introscope.threaddump.em.ThreadDumpImpl.getThreadDump(ThreadDumpImpl.java:265)
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
    at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
    at java.lang.reflect.Method.invoke(Method.java:498)
    at com.wily.isengard.messageprimitives.MethodCallUtilities.callInterface(MethodCallUtilities.java:75)
    at com.wily.isengard.messageprimitives.MethodCallUtilities.callInterface(MethodCallUtilities.java:29)
    at com.wily.isengard.messageprimitives.service.MessageService.attemptMethodCall(MessageService.java:183)
    at
com.wily.isengard.messageprimitives.service.MessageService.handleMethodCallMessage(MessageService.java:135)
    at com.wily.isengard.messageprimitives.service.MessageService.receiveMessage(MessageService.java:161)
    at com.wily.isengard.postoffice.Mailbox.handleMessage(Mailbox.java:252)
    at com.wily.isengard.postoffice.PostOffice.deliverInternal(PostOffice.java:532)
    at com.wily.isengard.postoffice.PostOffice.access$2(PostOffice.java:478)
    at com.wily.isengard.postoffice.PostOffice$DeliveryItem.run(PostOffice.java:886)
    at com.wily.EDU.oswego.cs.dl.util.concurrent.PooledExecutor$Worker.run(PooledExecutor.java:728)
    at java.lang.Thread.run(Thread.java:750)
Caused by: java.lang.OutOfMemoryError: Java heap space
```

Résolution

Augmentez le tas sur le serveur d'applications (agent exécutant le serveur). Cette erreur s'affiche uniquement lorsque la machine virtuelle Java (serveur d'applications) est exécutée avec un espace de tas faible.

Modification des types d'opérations dans les outils de calcul des modules de gestion**Symptôme**

Lorsque vous modifiez un outil de calcul dans un module de gestion, la modification du type d'opération redéfinit la signification de la mesure de sortie pour l'outil de calcul. Imaginons, par exemple, que vous avez basculé le type d'opération de MIN à MAX et que vous avez conservé le nom de sortie de la mesure dans l'outil de calcul. La mesure de sortie affiche les anciennes valeurs dans l'historique (la valeur MIN dans notre exemple) avec les nouvelles valeurs (la valeur MAX dans notre exemple). Aucune indication n'apparaît sur l'endroit où l'altération du traitement a eu lieu.

Solution

Renommez la mesure de sortie de l'outil de calcul lorsque vous modifiez le type d'opération si vous pensez que ces valeurs prêtent à confusion.

Panneaux vides dans les tableaux de bord**Symptôme**

Les tableaux de bord incluent des panneaux vides.

Solution

La présence de panneaux vides est due au fait que votre application n'utilise pas ces mesures.

Par défaut, les tableaux de bord affichent un ensemble général de mesures de performances.

Aucun résultat pour une requête sur les événements historiques**Symptôme**

Aucun résultat ne s'affiche lorsque j'effectue une requête sur les événements historiques.

Solution

- Le problème se produit-il en utilisant des filtres de base, tels que type:sampled ? Cela permet de confirmer que les données sont écrites dans la base de données traces.
- Le problème peut être lié à un index de traces endommagé. Arrêtez le gestionnaire d'entreprise, supprimez le répertoire \traces\index et exécutez l'outil de réindexation pour réindexer la base de données de traces.

Données à collecter avant de contacter le support Broadcom

Si vous avez appliqué les suggestions précédentes et que vous rencontrez encore des problèmes, collectez les données suivantes avant de contacter le support Broadcom. Ces informations permettront au support Broadcom de vous aider de manière efficace.

- <répertoire_base_gestionnaire_entreprise>/logs/* dans un fichier .zip
- <répertoire_base_agent>/logs/* et IntroscopeAgent.profile dans un fichier .zip
- Capture d'écran de la fenêtre Outil de suivi de transaction et détails de la classe attendue

Dépannage des problèmes d'expiration de session automatique dans la station de travail

Symptômes

Le délai d'expiration de la session automatique est endommagé et présente au moins l'un des symptômes suivants :

- Les fenêtres de la station de travail ne se ferment pas automatiquement une fois la période d'inactivité atteinte.
- Aucun message de déconnexion ne s'affiche dans la fenêtre de connexion.

Solution

Seuls les administrateurs DX SaaS peuvent modifier le fichier <répertoire_base_EM>/config/IntroscopeEnterpriseManager.properties. Contactez votre administrateur pour vous assurer que la valeur de la propriété introscope.apmserver.ui.inactivityLogoutTimeout est définie sur un nombre entier supérieur à 0 pour activer le délai d'expiration de la session.

Solution

Ouvrez le fichier IntroscopeWorkstation.log ou un fichier journal distinct qui effectue le suivi des événements de station de travail. Vérifiez que les messages suivants sont présents dans le fichier journal :

- **Session timeout configured to <x> minute(s)**
Indique que les paramètres de délai d'expiration de session automatique sont configurés correctement.
- **User activity check: there has been no user action for more than several minutes, therefore logging out.**
Notification de l'expiration du délai de session.

Expiration du délai de la station de travail lors de la connexion au gestionnaire d'entreprise

Symptôme

Expiration du délai de la station de travail lors de la connexion au gestionnaire d'entreprise.

Solution

Le délai de connexion par défaut pour la station de travail est de 60 secondes. Le délai de connexion de la station de travail peut expirer pour les raisons suivantes :

- Latence du réseau entre le poste de travail et le gestionnaire d'entreprise
- La station de travail a une grande quantité de données à récupérer (mesures, modules de gestion) et 60 secondes n'est pas une durée suffisante pour récupérer toutes ces données, même dans des conditions de réseau normales.

Vous pouvez augmenter le délai d'expiration de connexion du client en ajoutant la propriété suivante dans le fichier IntroscopeEnterpriseManager.properties :

```
introscope.enterprisemanager.workstation.timeout=[value in seconds]
```

Redémarrez le gestionnaire d'entreprise pour que les modifications prennent effet.

Référence d'API

CA Application Performance Management comprend l'ensemble d'API de services Web suivantes :

Ces API sont destinées aux utilisateurs suivants :

- Développeurs et administrateurs de CA Application Performance Management
- CA Technologies ou développeurs, services professionnels ou ingénieurs préventes tiers
- Chaque API de services Web de CA Application Performance Management permet aux développeurs et aux administrateurs d'étendre leurs solutions de gestion des applications. Elle peuvent récupérer des informations pertinentes à partir de CA Application Performance Management et intégrer des données à des solutions tierces ou personnalisées.

API APM Command Center

Cet article présente les API RESTful implémentées pour APM Command Center. Les verbes et les paramètres de demande HTTP pris en charge sont répertoriés pour chaque service Web disponible.

Cette section fournit une présentation des API RESTful implémentées pour APM Command Center. Les verbes et les paramètres de requête HTTP pris en charge sont répertoriés pour chaque service Web disponible. Nous vous recommandons également de lire la section [API hypermédia d'APM](#) pour obtenir des informations générales sur l'implémentation d'API RESTful dans DX APM.

Téléchargement du dernier package à partir d'APM Command Center

L'API Command Center vous permet de télécharger les derniers packages à partir d'APM Command Center et de personnaliser le comportement du téléchargement en définissant les propriétés requises. Par exemple, au cours du téléchargement, vous pouvez personnaliser la charge utile et définir certaines propriétés comme masquées.

Vous pouvez obtenir l'URL de téléchargement du package à partir de l'emplacement suivant : **ACC, Packages, Ecran de détails du package, URL du package**.

Les terminaux de téléchargement des packages ont été étendus pour ajouter une demande POST. Exemple :

```
POST /acc/apm/acc/downloadpackage/uid/SsApAZq75k3G/version/latest?
format=archive&layout=bootstrap_preferred&packageDownloadSecurityToken=d19a78c5a88bfe750f3a7a4bc
```

Dans la charge utile, définissez la liste des propriétés JSON au format suivant :

```
{
  "list" : [ {

    "propertyName" : "com.wily.introscope.agent.soapexception.analyzer.enabled",
    "propertyValue" : "false",
  }, {
    "propertyName" : "com.wily.introscope.agent.soapheaderinsertion.enabled",
    "propertyValue" : "true",
    "hidden" : "true" // optional attribute of boolean type - default value is false
  },
  {
    "propertyName" : "introscope.agent.agentName",
    "propertyValue" : "OverriddenAgent",
    "bundleName" : "tomcat", // optional attribute
    "hidden" : "false" // optional attribute of boolean type - default value is false
  }
]
```

```

    }, {
      "propertyName" : "instrument.HTTPServletTracing",
      "propertyValue" : "Off",
      "bundleName" : "servlets", // optional attribute
      "hidden" : "false" // optional attribute of boolean type - default value is false
    },
    "allowOnlyExistingProperties" : "false" // optional attribute, default value is false
  }

```

Vous pouvez également définir des propriétés supplémentaires dans la charge utile.

Nom de propriété	Description	Exemple/valeur par défaut
bundleName	Facultatif Définit le nom du groupe.	La liste des groupes compris dans le package spécifique avec l'ID 2 (UID : SsApAZq75k3G) peut être obtenue par le terminal : <ul style="list-style-type: none"> GET /acc/apm/acc/package/2/bundles
propertyName	Obligatoire Définit le nom de la propriété.	La liste des noms de la propriété bundleName spécifiée (à savoir le groupe dont l'ID est 91) peut être obtenue par le terminal : <ul style="list-style-type: none"> /acc/apm/acc/package/2/bundles/91/profile
propertyValue	Obligatoire Définit la valeur de la propriété.	Aucune
hidden	Facultatif Définissez une valeur booléenne, true ou false si vous voulez masquer le paramètre pendant le téléchargement du package. Si vous définissez la valeur sur true , la valeur sera mise en commentaire dans l'archive du package de résultats.	Valeur par défaut : false
allowOnlyExistingProperties	Facultatif Définit une valeur booléenne : true ou false . Si vous définissez la valeur sur true , les validations au cours du téléchargement renvoient l'erreur HTTP 400 si le nom de propriété spécifié dans le corps du message ne figure dans aucune des propriétés du groupe de packages. Nous vous recommandons de définir la propriété sur true si vous voulez remplacer uniquement les propriétés existantes et exécuter la vérification de validation lors de l'appel REST.	Valeur par défaut : false

Validation et dépannage

Lorsque le terminal termine la validation, il renvoie le package binaire au format .zip ou .tar, en fonction de la plate-forme utilisée (Windows ou UNIX/Linux). Ce package contient les paramètres remplacés ou nouveaux avec le code de réponse 200 OK.

Toutefois, en cas d'échec de la validation, le code de réponse 400 BAD REQUEST est renvoyé à l'utilisateur avec le message d'erreur détaillé.

APM Command Center prend en charge les services Web RESTful publics ci-après :

Les URL des ressources présentent le format suivant :

`https://<hôte_client_hébergé_APM>/apm/appmap/acc/apm/acc/<nom_ressource>`

L'hôte du client hébergé APM Command Center comprend le nom du pod du gestionnaire d'entreprise dans Kubernetes et le nom DNS du routeur Kubernetes. Par exemple : 10-778046.KUBERNETES-ROUTER ; le premier numéro correspond au numéro du client hébergé. Le second numéro diffère pour chaque client hébergé. KUBERNETES-ROUTER est le routeur Kubernetes installé.

Le tableau suivant indique toutes les ressources d'API APM Command Center disponibles ainsi que les verbes HTTP et les paramètres qu'elles prennent en charge.

Ressource	Verbes HTTP						Paramètres				
	GET	HEAD	POST	DELETE	OPTIONS	format	projection	page	size	sort	q
agent Fournit une liste des agents gérés, y compris leurs propriétés.	Oui	Oui	Non	Non	Oui	JSON, CSV	liste	Oui	Oui	Oui	Oui
agentUpdateTask Permet de modifier le niveau de journalisation d'un agent spécifique.	Oui	Oui	Oui	Non	Oui	JSON	Non	Oui	Oui	Oui	Non

diagnosticReport Fournit une liste des rapports de diagnostic et la possibilité de télécharger les rapports.		Oui	Non	Non	Oui	JSON, ZIP	liste	Oui	Oui	Oui	Oui
diagnosticReportTask Permet de générer un nouveau rapport de diagnostic pour un agent.		Oui	Oui	Non	Oui	JSON	Non	Oui	Oui	Oui	Non
contrôleur Fournit une liste des contrôleurs d'agent connectés au serveur de configuration.	Oui	Oui	Non	Non	Oui	JSON, CSV	Non	Oui	Oui	Oui	Non
agentFileOperationTask Permet d'envoyer (ou de supprimer) un fichier dans un répertoire sur un système distant.	Oui	Oui	Oui	Non	Oui	JSON	Non	Oui	Oui	Oui	Non

fichier Fournit une liste des fichiers stockés sur le serveur de configuration.	Oui	Oui	Oui	Oui	Oui	JSON	Non	Oui	Oui	Oui	Non
auditRecord Fournit une liste des enregistrements d'audit associés aux opérations qui modifient l'environnement.	Oui	Oui	Non	Non	Oui	JSON	liste	Oui	Oui	Oui	Oui
package Fournit une liste des packages d'agent créés.	Oui	Oui	Oui	Oui	Oui	ZIP, TAR, archive	liste	Oui	Oui	Oui	Oui
agentPackageTask Permet de distribuer des groupes d'agents vers le répertoire d'installation de l'agent.	Oui	Oui	Oui	Non	Oui	JSON	Non	Oui	Oui	Oui	Non
groupe Fournit une liste des groupes d'agents disponibles.	Oui	Oui	Oui	Oui	Oui	JSON, archive	Non	Oui	Oui	Oui	Oui

Notez que le format des paramètres projection, page, size, sort et q sont sensibles à la casse et doivent être saisis en lettres minuscules ; par exemple, le format CSV ne fonctionnera pas.

Authentification

Un jeton de sécurité est une chaîne de texte générée de manière aléatoire et dont la fonctionnalité est quasiment la même que celle d'un mot de passe. Il permet à l'API d'accéder au service Web de Command Center.

Vous pouvez générer autant de jetons que nécessaire. Vous pouvez modifier la description d'un jeton ou supprimer un jeton à l'aide du bouton Modifier. Seule la suppression des jetons permet de les révoquer. Tous les utilisateurs peuvent supprimer le jeton de leur choix.

Vous pouvez également consulter la date de création d'un jeton et la date à laquelle il a été utilisé pour la dernière fois.

Procédez comme suit :

1. Dans l'interface utilisateur de DX APM, sélectionnez l'onglet **Sécurité**.
2. Cliquez sur **Générer un nouveau jeton**.
3. Sélectionnez **API publique**.
4. (Facultatif) Sélectionnez la date d'expiration du jeton.
5. Cliquez sur **Générer un jeton**.
6. Copiez le jeton généré.

Remarque : Vérifiez que le jeton est immédiatement stocké à des fins d'utilisation ultérieure. Vous ne pouvez pas l'afficher à nouveau dans l'interface utilisateur DX APM.

7. Utilisez le jeton dans l'en-tête de la demande d'autorisation. Pour plus d'informations, consultez la section [Authentification et autorisation d'API](#).

Informations complémentaires :

- [Messages et codes des erreurs générales liées à l'API](#)
- [Messages d'erreur d'API de Command Center](#)

Messages d'erreur d'API

Cette section indique les messages d'erreur d'API renvoyés par DX APM Command Center. Pour obtenir une synthèse de tous les messages et codes d'erreur de l'API DX APM Hypermedia, consultez la section [Codes et messages d'erreur](#).

EA0100 à EA0599

Les erreurs dans la plage comprise entre EA0100 et EA0599 sont des codes de statut HTTP standard. Pour plus d'informations, reportez-vous au document [RFC 7231](#).

EA1001

Requête de recherche incorrecte

Motif :

Code renvoyé lorsqu'une demande de filtre ou de recherche échoue en raison d'une requête non conforme à la syntaxe Lucene.

EA1002

Package actuellement utilisé par {0} agents

Motif :

Vous n'êtes pas autorisé à supprimer les packages auxquels des agents font référence actuellement.

EA3100**Mise à jour d'agent en cours : {agent id}****Motif :**

Une autre tâche de mise à jour d'agent est en cours sur cet agent particulier.

Solution :

Attendez que la tâche de mise à jour actuelle soit finie.

EA3101**Mise à niveau déjà en cours pour le contrôleur sur {serverName}****Motif :**

Une seule tâche ControllerUpgradeTask peut être exécutée à la fois sur un contrôleur d'agent. Une tentative de démarrage d'une nouvelle tâche ControllerUpgradeTask a été effectuée alors qu'une telle tâche est déjà en cours d'exécution, ce qui entraîne l'affichage de ce message d'erreur.

Solution :

Attendez que la tâche de mise à niveau actuelle soit finie.

EA3102**Fichier déjà mis à jour pour l'agent****Motif :**

Une seule tâche AgentFileOperationTask peut être exécutée à la fois pour la même combinaison de fichiers d'agent et de destination.

Solution :

Attendez que la tâche d'opération actuelle soit finie.

EA3103**Le contrôleur n'est pas connecté****Motif :**

Vous avez essayé de mettre à niveau un contrôleur d'agent qui n'est pas en cours d'exécution. Il est impossible de démarrer une tâche ControllerUpgradeTask pour les contrôleurs d'agent qui ne sont pas en cours d'exécution.

Solution :

Démarrez le contrôleur d'agent.

EA3104**La mise à niveau automatique du contrôleur n'est pas autorisée****Motif :**

Il est impossible d'activer la mise à niveau automatique du contrôleur d'agent, car l'envoi du package du contrôleur d'agent est désactivé.

Solution :

Pour obtenir les directives à suivre, consultez la section Dépannage du processus de mise à niveau.

EA3105

Le package a été archivé et ne peut pas être utilisé pour cette opération

Motif :

Vous ne pouvez utiliser de packages archivés pour aucune opération. Par exemple, vous ne parvenez pas à télécharger un package archivé.

Solution :

Choisissez un autre package à télécharger ou décompresser le package demandé et réessayez.

EA3108

Le filtre nommé {name} est utilisé par d'autres filtres : {otherFilters}.

Motif :

Le filtre nommé ne peut pas être supprimé, car il est utilisé (il y est fait référence) par d'autres filtres.

Ressource d'agent

Ce service Web renvoie des informations sur les agents enregistrés dans APM Command Center (ACC). Verbes pris en charge : GET, HEAD, OPTIONS. Paramètres pris en charge : [page](#), [size](#), [sort](#), [q](#), [format](#), [projection](#)

GET

```
GET https://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/agent
```

Utilisez la demande suivante pour obtenir des informations sur l'agent avec l'ID 2 uniquement :

```
GET https://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/agent/2
```

HEAD

La méthode HEAD renvoie des en-têtes contenant des informations sur le service, notamment sur les champs de recherche autorisés.

```
HEAD https://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/agent
```

Exemple de réponse :

```
Cache-Control → public, no-cache, must-revalidate, max-age=43,200Expires → Thu, 30 Apr 2015 20:12:13 GMTServer → Jetty(8.1.15.v20140411)X-CA-ACC-SEARCH-FIELDS → agentId, agentName, processName, version, status, type, build, logLevel,emCollectorHost, emCollectorPort, appServerName, appServerVersion, platformName,platformVersion, platformArch, osName, osVersion, osArch, serverName, agentProfileX-Frame-Options → DENY
```

Propriétés de ressource - Les propriétés suivantes contenant des informations sur la ressource sont disponibles :

Nom de propriété	Type	Description	API Version
tenant	nombre entier	ID du client hébergé	1.1
ID (identification)	nombre entier	ID interne de la ressource d'agent	1.0
agentName	chaîne	Nom de l'agent qu'il fournit lors de son enregistrement dans ACC ; fait partie de l'agent triple.	1.0

Nom de propriété	Type	Description	API Version
serverName	chaîne	Serveur sur lequel l'agent enregistré réside ; fait partie de l'agent triple.	1.0
processName	chaîne	Nom du processus de l'agent, connu de l'agent et d'EM ; fait partie de l'agent triple.	1.0
status	énumération	Indique si l'agent est considéré actif (valeurs possibles : ACTIVE ou AWAY). Par défaut, ACTIVE indique que l'agent a été détecté au cours des dernières 24 heures.	1.0
type	énumération	Type de l'agent, tel qu'indiqué à l'ACC dans le cadre de l'enregistrement de l'agent ; Actuellement, il s'agit toujours de JavaAgent.	1.0
version	chaîne	Version de l'agent définie dans son fichier manifeste (par ex. : 9.7.1).	1.0
build	chaîne	Compilation de l'agent défini dans son fichier manifeste	1.0
logLevel	énumération	Niveau de journalisation actuel de l'agent (FATAL, ERROR, WARN, INFO, VERBOSE, DEBUG, TRACE)	1.0
registrationTimestamp	date	Heure à laquelle l'agent s'est enregistré dans ACC, représentée au format UTC	1.0
registrationUnixTimestamp	date	Heure à laquelle l'agent s'est enregistré dans ACC, représentée au format Unix	1.0
lastContact	date	Dernière heure à laquelle l'agent a contacté l'ACC, représentée au format UTC	1.0
emCollectorHost	chaîne	Nom du collecteur EM auquel l'agent est connecté et connu de l'agent	1.0
emCollectorPort	nombre entier	Port du collecteur EM auquel l'agent est connecté et connu de l'agent	1.0
appServerName	chaîne	Serveur d'applications sur lequel l'agent est exécuté (si connu) ; par ex. : Apache Tomcat	1.0

Nom de propriété	Type	Description	API Version
appServerVersion	chaîne	Version du serveur d'applications sur lequel l'agent est exécuté (si connue)	1.0
platformName	chaîne	Plate-forme sur laquelle l'agent est exécuté (Java Runtime) ; par ex. Oracle Corporation	1.0
platformVersion	chaîne	Version de la plate-forme (Java Runtime) sur laquelle l'agent est exécuté, par ex. : 1.7.0.	1.0
platformArch	chaîne	Architecture de la plate-forme (Java Runtime) sur laquelle l'agent est exécuté si elle est détectable	1.0
osName	chaîne	Système d'exploitation sur lequel l'agent est exécuté (Windows, RedHat, etc.)	1.0
osVersion	chaîne	Version du système d'exploitation sur lequel l'agent est exécuté	1.0
osArch	chaîne	Architecture de processeur du système d'exploitation sur lequel l'agent est exécuté ; par ex. : amd64	1.0
metricCount	nombre entier	Estimation par l'agent du nombre de mesures qu'il collecte	1.0
registrationErrors	tableau de chaînes	Erreurs renvoyées par des modules d'extension lors de la détection d'informations supplémentaires sur l'agent	1.0
installPath	chaîne	Chemin d'accès complet à l'emplacement d'installation de l'agent	1.0
agentProfile	chaîne	Chemin d'accès complet au profil de l'agent	1.0
platformProperties	carte	Paires clé-valeur des propriétés du système Java connues de l'agent	1.0
environmentVariables	carte	Paires clé-valeur des variables d'environnement connues du processus de l'agent	1.0
controllerId	UUID	UUID du contrôleur ACC auquel cet agent est connecté	1.0

Ressource agentUpdateTask

Le service Web agentUpdateTask peut être utilisé pour mettre à jour le profil d'agent (actuellement limité à la modification du niveau de journalisation).

Le service Web agentUpdateTask peut être utilisé pour mettre à jour le profil d'agent (actuellement limité à la modification du niveau de journalisation). Vous pouvez également utiliser la ressource pour répertorier toutes les demandes précédentes. Verbes pris en charge : GET, HEAD, POST, OPTIONS. Paramètres pris en charge : [page](#), [size](#), [sort](#).

accès aux ressources GET

```
GET https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/agentUpdateTask/
```

POST

La méthode POST vous permet de mettre à jour le profil d'agent. Dans l'exemple suivant, le niveau de journalisation de l'agent avec l'ID 1 est remplacé par info :

```
POST https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/agentUpdateTask{ "agent":  
  "agent/1", "property" : "log4j.logger.IntroscopeAgent", "value": "INFO"}
```

Propriétés de ressource - Les propriétés suivantes contenant des informations sur la ressource sont disponibles :

Nom de propriété	Type	Description	API Version
tenant	nombre entier	ID du client hébergé	1.1
status	énumération	Statut de l'opération (Suit la définition de la ressource de tâche.)	1.0
creationTimestamp	date	Heure de la création de la ressource (format UTC)	1.0
completionTimestamp	date	Heure de fin de l'opération (format UTC)	1.0
expectedDuration	nombre entier	Durée attendue de l'exécution de l'opération en cours	1.0
propriété	chaîne	Propriété du profil en cours de mise à jour	1.0
value	chaîne	Valeur demandée	1.0
currentValue	chaîne	Valeur de l'agent connue	1.0
pendingValue	chaîne	Dernière valeur écrite dans le profil	1.0
agentId	nombre entier	Identificateur unique de l'agent sur lequel l'opération est effectuée	1.0
user	chaîne	Utilisateur qui a initié l'opération	1.0
updateErrors	tableau	Tableau d'erreurs renvoyées lors de l'opération	1.0

Ressource diagnosticReport

Ce service Web renvoie des informations sur les rapports de diagnostic.

Ce service Web renvoie des informations sur les rapports de diagnostic. Un rapport de diagnostic contient des informations complètes sur un agent. Verbes pris en charge : GET, HEAD, OPTIONS. Paramètres pris en charge : [page](#), [size](#), [sort](#), [projection](#), [q](#).

GET

GET https://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/diagnosticReport/

Propriétés de ressource - Les propriétés suivantes contenant des informations sur la ressource sont disponibles :

Table 2:

Nom de propriété	Type	Description	API Version
tenant	nombre entier	ID du client hébergé	1.1
ID (identification)	nombre entier	ID interne de la ressource diagnosticReport	1.0
reportName	chaîne	Nom d'affichage du rapport	1.0
requestTimestamp	date	Heure à laquelle le rapport a été demandé (format UTC)	1.0
completionTimestamp	date	Heure à laquelle le rapport a été terminé (format UTC)	1.0
generationDuration	nombre entier	Temps total (en millisecondes) requis pour générer le rapport	1.0
status	énumération	Statut de la génération du rapport	1.0
commandCenterInfo	carte	Paires clé-valeur fournissant des informations sur le serveur de configuration et le contrôleur d'agent utilisés pour générer le rapport	1.0
agentProfile	carte	Paires clé-valeur fournissant des informations sur le profil utilisé pour configurer l'agent. Inclut un lien vers le contenu.	1.0
generationErrors	tableau	Tableau d'erreurs rencontrées lors de la génération du rapport	1.0
agentProperties	carte	Paires clé-valeur représentant les informations sur l'agent lors de la génération du rapport (copiées à partir de la ressource d'agent)	1.0
environmentVariables	carte	Paires clé-valeur représentant les variables d'environnement connues de l'agent au moment de la génération du rapport (copiées à partir de la ressource d'agent)	1.0

Nom de propriété	Type	Description	API Version
platformProperties	carte	Paires clé-valeur représentant les propriétés de la plate-forme (propriétés du système Java) connues de l'agent au moment de la génération du rapport (copiées à partir de la ressource d'agent)	1.0
platformParameters	chaîne	Ligne de commande utilisée pour lancer le processus sous lequel l'agent est exécuté	1.0
extensionDirectory	chaîne	Chemin complet du répertoire des extensions de l'agent	1.0
extensionFiles	carte	Sous-ressource contenant les détails des fichiers d'extension exécutés dans l'agent, notamment le nom, la date de modification, la taille et la version	1.0
logFiles	carte	Sous-ressource contenant les détails des fichiers journaux de l'agent, notamment le nom, le chemin, la date de modification, la taille et le lien vers le contenu	1.0
pbdPblFiles	carte	Sous-ressource contenant les détails des fichiers PBD exécutés dans l'agent, notamment le nom, la date de modification, la taille et le lien vers le contenu	1.0

Ressource diagnosticReportTask

Le service Web diagnosticReportTask peut être utilisé pour demander un rapport de diagnostic.

Le service Web diagnosticReportTask peut être utilisé pour demander un rapport de diagnostic. La création d'une ressource diagnosticReportTask lance la génération d'un rapport. Pour surveiller la progression de la génération du rapport, récupérez (interrogez) la ressource diagnosticReportTask créée. Vous pouvez également utiliser la ressource pour répertorier toutes les demandes précédentes. Verbes pris en charge : GET, HEAD, POST, OPTIONS. Paramètres pris en charge : [page](#), [size](#), [sort](#).

GET

La requête suivante renvoie des informations sur le job de rapport de diagnostic avec l'ID 2 :

```
GET https://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/diagnosticReportTask/2/
```

POST La méthode POST vous permet de commencer à générer un rapport de diagnostic pour un agent spécifié. Voici un exemple de demande qui crée un job de rapport de diagnostic pour l'agent avec l'ID 1 :

```
POST /apm/acc/diagnosticReportTask HTTP/1.1Host: localhost:8443Content-Length: 19Accept: application/json, text/plain, */*Origin: https://localhost:8443X-Requested-With: XMLHttpRequestUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
```



```
(KHTML, like Gecko) Chrome/42.0.2311.90 Safari/537.36 Content-Type: application/json; charset=UTF-8 Referer: https://localhost:8443/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.8,cs;q=0.6,fr;q=0.4,de;q=0.2,nl;q=0.2 { "agent" : "agent/1" }
```

Propriétés de ressource - Les propriétés suivantes contenant des informations sur la ressource sont disponibles :

Nom de propriété	Type	Description	API Version
tenant	nombre entier	ID du client hébergé	1.1
ID (identification)	nombre entier	Identificateur unique de cette ressource	1.0
status	énumération	Statut de l'opération (Suit la définition de la ressource de tâche.)	1.0
creationTimestamp	date	Heure de la création de la ressource (format UTC)	1.0
completionTimestamp	date	Heure de fin de l'opération (format UTC)	1.0
expectedDuration	nombre entier	Durée attendue de l'exécution de l'opération en cours	1.0
diagReportId	nombre entier	Identificateur unique de la ressource diagnosticReport créée	1.0
agentId	nombre entier	Identificateur unique de l'agent sur lequel l'opération est effectuée	1.0

Ressource de contrôleur

Ce service Web renvoie des informations sur les contrôleurs d'agent connectés au serveur de configuration.

Ce service Web renvoie des informations sur les contrôleurs d'agent connectés au serveur de configuration. Verbes pris en charge : GET, HEAD, OPTIONS. Paramètres pris en charge : [page](#), [size](#), [sort](#).

GET

```
GET https://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/controller
```

Propriétés de ressource - Les propriétés suivantes contenant des informations sur la ressource sont disponibles :

Nom de propriété	Type	Description	API Version
tenant	nombre entier	ID du client hébergé	1.1
ID (identification)	UUID	UUID de la ressource de contrôleur	1.0
version	chaîne	Version du contrôleur d'agent, telle que définie dans son fichier manifeste	1.0
messagingApiVersion	nombre entier	Version maximum de l'interface de messagerie prise en charge par ce contrôleur	1.0

Nom de propriété	Type	Description	API Version
buildNo	chaîne	Numéro de compilation du contrôleur, tel que défini dans son fichier manifeste	1.0
hostNames	tableau de chaînes	Tableau contenant tous les noms d'hôte connus pour ce contrôleur	1.0
ipAddresses	tableau de chaînes	Tableau contenant toutes les adresses IP connues (v4 et v6) pour ce contrôleur	1.0
osArch	chaîne	Architecture du système d'exploitation sous lequel le contrôleur est exécuté ; par ex. : amd64	1.0
osName	chaîne	Nom du système d'exploitation sous lequel le contrôleur est exécuté ; par ex. : Windows Server 2008 R2	1.0
osVersion	chaîne	Version du système d'exploitation sous lequel le contrôleur est exécuté, par ex. 6.1.	1.0
registrationTimestamp	date	Date et heure (au format UTC) auxquelles le contrôleur s'est enregistré auprès du serveur de configuration	1.0
registrationUnixTimestamp	date	Date et heure (au format UNIX) auxquelles le contrôleur s'est enregistré auprès du serveur de configuration	1.0
pluginRuntimeVersion	nombre entier	Version maximum de l'exécution du module d'extension prise en charge par ce contrôleur (utilisée pour déterminer la compatibilité des scripts)	1.0
pluginsUpdatable	Valeur booléenne	Indique si le contrôleur autorise l'envoi de nouvelles versions de modules d'extension.	1.0

Messages d'erreur

Cette section explique les messages d'erreur liés à DX APM Command Center.

EC1001

Impossible d'enregistrer le module d'extension {0} : {1}

Le contrôleur d'agent dispose d'un module d'extension qui n'est pas à jour et il n'est pas parvenu à enregistrer le module d'extension mis à jour téléchargé à partir du serveur DX APM Command Center.

Motif :

L'espace disque disponible est insuffisant sur l'hôte sur lequel le contrôleur d'agent est exécuté ou le contrôleur d'agent est exécuté en tant qu'utilisateur non autorisé à écrire dans le répertoire plugins.

Solution :

Vérifiez l'espace disque disponible sur l'hôte du contrôleur d'agent et assurez-vous que l'utilisateur qui exécute le contrôleur d'agent dispose des autorisations write nécessaires pour écrire dans le répertoire plugins et dans les fichiers qui s'y trouvent.

EC1002**La mise à niveau du contrôleur ne s'est pas terminée dans le délai imparti****Motif :**

La tâche de mise à niveau du contrôleur d'agent a été lancée, mais le contrôleur ne s'est pas enregistré auprès du serveur dans le délai prévu.

Solution :

Si le contrôleur ne s'est toujours pas reconnecté, consultez le fichier upgrade.log sur le système de contrôleur pour savoir pourquoi.

EC1003**Echec de la mise à niveau du contrôleur, la version reste inchangée.****Motif :**

L'opération de mise à niveau du contrôleur d'agent a été lancée, mais la mise à niveau n'a pas pu se terminer. La version d'origine a été restaurée.

Causes fréquentes de cette erreur :

- Espace insuffisant sur le système de fichiers
- Contrôleur non autorisé à écrire dans un répertoire accessible pendant le processus de mise à niveau (généralement, le répertoire d'installation /tmp et Controller).
- L'un des fichiers est verrouillé par un processus existant. Cette erreur se produit plus souvent sur les systèmes d'exploitation Windows. Assurez-vous qu'aucune fenêtre d'explorateur ou invite de commande n'utilise ou ne bloque le répertoire de mise à niveau du contrôleur.

Solution :

Générez un rapport de diagnostic pour l'un des agents sur ce serveur et consultez le fichier upgrade.log sur la carte Fichiers journaux du contrôleur. Examinez le message d'erreur et essayez de résoudre le problème.

EC1004**Les groupes suivants n'ont pas été ajoutés : {0}**

Un package a été envoyé à un agent, mais il n'a pas pu ajouter tous les groupes à partir du package.

Motif :

Un package contenant de nouveaux groupes a été envoyé à un agent en cours d'exécution. Cependant, l'agent n'est pas parvenu à ajouter la totalité de ces groupes. Les groupes n'ayant pas pu être ajoutés sont indiqués dans le message.

Solution :

L'exécution d'un rapport de diagnostic pour l'agent permet d'examiner à distance les fichiers journaux de l'agent. Ces journaux indiquent la raison pour laquelle le groupe n'a pas pu être chargé, par exemple, si le groupe est endommagé.

EC1005

Les groupes suivants n'ont pas été supprimés : {0}

Un package a été envoyé à un agent, mais il n'a pas pu supprimer tous les groupes requis à partir du package.

Motif :

Un package a été envoyé à un agent contenant moins de groupes que ceux actuellement utilisés par l'agent. Ces groupes doivent être supprimés de l'agent en cours d'exécution. Cependant, l'agent n'est pas parvenu à supprimer la totalité de ces groupes. Les groupes n'ayant pas pu être supprimés sont indiqués dans le message.

Solution :

L'exécution d'un rapport de diagnostic pour l'agent permet d'examiner à distance les fichiers journaux de l'agent. Ces journaux indiquent la raison pour laquelle le groupe n'a pas pu être supprimé, par exemple, si le répertoire du groupe est déjà utilisé.

EP1000

Le processus {0} n'est pas accessible

Il est impossible d'accéder au processus du serveur d'applications.

Motif :

Le processus du serveur d'applications n'est plus en cours d'exécution ou le contrôleur d'agent ne dispose pas des privilèges suffisants pour afficher le processus.

Solution :

Vérifiez si le processus du serveur d'applications est en cours d'exécution à l'aide de l'ID de processus donné. Si c'est le cas, assurez-vous que le contrôleur d'agent s'exécute avec l'autorisation suffisante pour afficher ce processus, par exemple, s'il s'exécute en prenant l'identité du même utilisateur (user) ou en utilisant le même groupe (group).

EP1001

{0} n'existe pas

Le fichier ou le répertoire n'existe pas.

Motif :

Le fichier spécifié est introuvable.

Solution :

Si le fichier se rapporte à un fichier de directives ProbeBuilder, assurez-vous qu'il existe et qu'il a été correctement nommé dans toutes les listes de directives ProbeBuilder.

EP1002

Autorisation refusée pour la lecture de {0}

Le fichier ou le répertoire n'a pas pu être lu.

Motif :

Le contrôleur d'agent n'est pas autorisé à lire le fichier nommé.

Solution :

Le contrôleur d'agent doit être exécuté avec l'autorisation suffisante pour lire les fichiers générés par l'agent APM. Par exemple, le contrôleur d'agent doit s'exécuter en utilisant le même utilisateur que le serveur d'applications ou en utilisant le même groupe.

EP1003**Une erreur d'E/S est survenue lors de la lecture de {0}**

Le fichier indiqué n'a pas pu être lu.

Motif :

Le fichier a pu être verrouillé par un autre processus ou le contrôleur d'agent n'est pas autorisé à lire le fichier.

Solution :

Le contrôleur d'agent doit être exécuté avec l'autorisation suffisante pour lire les fichiers générés par l'agent APM. Par exemple, le contrôleur d'agent doit s'exécuter en utilisant le même utilisateur que le serveur d'applications ou en utilisant le même groupe.

EP1004**Le SE {0} n'est pas pris en charge**

Le contrôleur d'agent ne peut pas déterminer les paramètres de ligne de commande pour l'ID de processus spécifié, car le système d'exploitation actuel n'est pas pris en charge.

Solution :

Contactez le service de support de CA pour savoir quand ce système d'exploitation devrait être pris en charge.

EP1005**Impossible de déterminer le serveur d'app {0}. Détails de l'erreur : {1}**

Le type du serveur d'applications n'a pas pu être déterminé.

Motif :

Le type ou la version du serveur d'applications ne sont pas encore pris en charge ou le contrôleur d'agent ne dispose pas des privilèges suffisants pour déterminer le type de serveur. L'erreur contient d'autres détails sur sa cause.

Solution :

Assurez-vous que le contrôleur d'agent dispose des autorisations suffisantes pour accéder aux fichiers du serveur d'applications. Par exemple, le contrôleur d'agent doit s'exécuter en utilisant le même utilisateur que le serveur d'applications ou en utilisant le même groupe.

EP1006**Valeur de la propriété introscope.autoprobe.directivesFile manquante dans {0}.****Motif :**

La propriété introscope.autoprobe.directivesFile n'est pas définie ou est vide dans le fichier IntroscopeAgent.profile.

Solution :

Vérifiez la validité du fichier IntroscopeAgent.profile.

EP1007**Autorisation refusée lors de l'écriture sur {0}**

Motif :

Le contrôleur d'agent ne dispose pas de droits d'accès suffisants pour écrire dans le fichier nommé. Cette situation peut se produire dans plusieurs circonstances :

- Tentative de modification du niveau de journalisation de l'agent Introscope
- Tentative de mise à niveau de l'installation du contrôleur d'agent
- Tentative de copie d'un fichier dans le répertoire d'installation de l'agent Introscope

Solution :

Assurez-vous que le contrôleur d'agent est en cours d'exécution avec les autorisations suffisantes pour écrire dans ce fichier et dans ce répertoire. Par exemple, vérifiez qu'il s'exécute avec le même utilisateur (user) ou le même groupe (group).

EP1010**Impossible de copier le fichier de {0} vers {1}. Détails de l'erreur {2}**

L'URL {0} n'est pas accessible en raison de problèmes réseau. Consultez les détails de l'erreur {2}.

Motif :

Vous avez appliqué un nouveau package d'agent ou mis à niveau le contrôleur.

Solution :

Assurez-vous que la connexion réseau est établie entre le contrôleur et le serveur Command Center. Réessayez.

EP1012**La version {0} existe déjà.****Motif :**

Ce message est renvoyé lorsque le répertoire de version a été créé manuellement pendant l'application du package d'agent.

Solution :

Redémarrez l'agent pour le redécouvrir afin qu'il puisse s'enregistrer correctement.

EP1013**L'agent n'est pas de type agent d'amorçage.****Motif :**

La mise à jour de l'agent échoue, car il ne s'agit pas d'un agent d'amorçage, mais Command Center a enregistré l'agent comme pouvant être amorcé.

Solution :

Redémarrez l'agent pour le redécouvrir afin qu'il puisse s'enregistrer correctement.

EP2000**Echec du script avec le message {1}**

Un problème a été détecté lors de la tentative de récupération des détails concernant un agent.

Motif :

Ce problème peut avoir de nombreuses causes. Une erreur de syntaxe 'est peut-être produite au niveau du script exécuté (pour les scripts personnalisés uniquement). Des problèmes sont peut-être survenus lors de l'accès aux fichiers dont le script a besoin.

Enfin, vous utilisez peut être une version ou une implémentation de Java non prise en charge.

ES1000

Echec de la modification du niveau de journal

Motif :

Un autre utilisateur a modifié le niveau de journalisation pour le même agent en même temps. Le module d'extension Contrôleur d'agent a déjà mis à jour le fichier IntroscopeAgent.profile avec le nouveau niveau de journalisation défini par l'autre utilisateur, mais la modification n'était pas encore reflétée dans l'interface utilisateur.

Solution :

Vérifiez le niveau de journalisation actuel et appliquez à nouveau la modification, le cas échéant.

ES1002

Erreur : {0} s'est produite lors de la création de la demande de modification de l'agent.

Motif :

La demande de modification des propriétés a échoué et le job de modification des propriétés n'a pas démarré.

Solution :

Ce problème est probablement lié à un composant d'arrière-plan. Consultez le fichier journal et contactez votre administrateur système.

EU3106

Le package {packageName} n'existe pas.

Motif :

Le package utilisé par cet agent n'est pas connu de DX APM Command Center.

EU3400

Une expiration s'est produite {0}

Motif :

Votre connexion est lente ou le serveur n'est pas disponible.

Solution :

Si le problème persiste ou si vous accédez à APM Command Center au moyen d'une connexion lente, envisagez d'augmenter le délai d'expiration de la demande défini par défaut sur 10 secondes (10 000 ms).

Pour cela, ajoutez la propriété suivante au fichier config/apmccsrv.properties du serveur de configuration et définissez sa valeur sur 30 000 afin de définir le délai d'expiration sur 30 secondes :

```
com.ca.apm.acc.ui.requestTimeout=30000
```

Redémarrez le serveur de configuration pour que la modification prenne effet.

Propriétés pouvant faire l'objet d'une recherche

Cette section répertorie toutes les propriétés que vous pouvez utiliser dans les recherches d'agents, de rapports, de packages ou de groupes dans l'interface utilisateur de DX APM Command Center.

Le tableau suivant répertorie les propriétés qui peuvent être utilisées dans une recherche. Dans la première colonne, vous trouverez la chaîne de recherche que vous devez entrer dans la zone de recherche (les chaînes correspondent aux appels d'API). La deuxième colonne affiche le nom correspondant de la propriété telle qu'il apparaît sur les fiches dans l'interface utilisateur.

Pour plus d'informations sur la recherche à l'aide du langage de requête du centre de commandes, consultez la section [Recherche à l'aide du langage de requête de Command Center](#).

Le modèle suivant est utilisé : Nom de la page - (Nom de la fiche) - Nom du champ.

Chaîne de recherche	Champ de l'interface utilisateur correspondant	Remarques
agentCompatibility	Groupes - Compatibilité	Versions de l'agent avec lesquelles le groupe est compatible. La recherche de plage n'est pas prise en charge. Entrez 10 pour obtenir des groupes compatibles avec toutes les versions 10.x.
agentId	N/D	Identificateur unique de l'agent.
agentName	Agents, Rapports - Nom de l'agent	
agentProfile	Rapports - Agent Profile Directory (Répertoire de profil d'agent)	Chemin d'accès au profil d'agent.
agentProfile.name	Rapports - Agent Profile Name (Nom de profil d'agent)	Renvoie des rapports pour les agents avec le nom de profil spécifié.
agentVersion	Packages - Version de l'agent	Renvoie les packages conçus pour les agents de la version correspondante.
appServerName	Agents - Serveur d'applications	Nom du serveur d'applications sur lequel l'agent est en cours d'exécution.
appServerVersion	Agents - Version du serveur d'applications	Version du serveur d'applications sur lequel l'agent est en cours d'exécution.
author	Groupes - Auteur	Renvoie les groupes créés par l'utilisateur spécifié.
build	N/D	
category	Groupes - Catégorie	Catégorie du groupe : core, environment, feature, custom
Collections	N/D	Utilise une chaîne de recherche enregistrée en tant que collection.
comment	Packages - Commentaire	Renvoie les packages contenant le commentaire spécifié.
controllerId	N/D	Renvoie les agents connectés au contrôleur d'agent spécifié.
deleted	N/D	Renvoie une liste des groupes supprimés ou actifs. Utilisez true ou false.
dependencies	Groupes - Dépendances	Renvoie les groupes qui dépendent des facettes spécifiées.
description	Groupes - Description	Renvoie les groupes avec la description spécifiée.

dynamic	Groupes - Peut être déployé sans redémarrage	Indique si le groupe est explicitement déployable à chaud. Les valeurs valides pour la recherche sont true et false.
emCollectorHost	Agents - Gestionnaire d'entreprise	Hôte du collecteur du gestionnaire d'entreprise
emCollectorPort	Agents - Gestionnaire d'entreprise	Port du collecteur du gestionnaire d'entreprise
enhances	Goupes - Améliorations	Renvoie les groupes qui améliorent les facettes spécifiées.
environmentVariables.value	Rapports - Variables d'environnement	Mappage des variables d'environnement (paires clé-valeur). Seules les valeurs sont recherchées.
extensionFiles.name	Rapports - Répertoire d'extensions	Chemin d'accès au répertoire d'extension d'un agent. Seul le nom du fichier peut faire l'objet d'une recherche.
facets	Groupes - Facettes	Renvoie les groupes qui contiennent les facettes spécifiées.
ID (identification)	N/D	ID littéral du groupe tel qu'utilisé dans la définition de package.
installPath	N/D	Renvoie les agents installés sur le chemin spécifié.
isBootstrapped	N/D	Renvoie les agents qui peuvent être mis à jour par une mise à jour d'amorçage à froid.
lastContact	Agents - Dernier contact	
logLevel	Agents - Niveau de journal	Valeurs : unknown, info, trace, debug, warn, error
name (nom)	N/D	Nom du groupe et non pas le nom d'affichage indiqué dans le champ Nom de la page Groupes.
osArch	Rapports - Propriétés du système Java	Architecture du système d'exploitation. Exemple : x64
osName	Agents - Type de SE, Rapports - SE, Packages - Type de SE	Nom du système d'exploitation. Exemple : Linux. Pour les groupes, les valeurs de recherche sont unix ou windows.
osVersion	Agents - Version du SE, Rapports - Version du SE	Version du système d'exploitation.
packageName	Agents - Package - Nom, Packages - Nom	Renvoie les packages correspondant à la chaîne de recherche et à tous les agents qui utilisent le package.
packageVersion	Agents - Package - Version du package	Renvoie tous les agents qui utilisent la version de package spécifiée.
pbdPblFiles.name	Rapports - Directives liées à ProbeBuilder	Liste des fichiers d'un agent lors de la génération du rapport. Contient uniquement des fichiers PBD et PBL, et seul le nom de fichier peut faire l'objet d'une recherche.
platformArch	N/D	Architecture de plate-forme. Exemple : x86
platformName	Agents - Environnement - JVM	Plate-forme sur laquelle l'agent est en cours d'exécution (Open Java, Oracle Java, .Net 4.0).

platformParameters	Rapports - Propriétés du système Java	Chaîne de paramètres de plate-forme. Utilisez les paramètres de démarrage de la machine virtuelle Java ou un équivalent pour .Net.
platformProperties.value	Rapports - Propriétés du système Java	Mappage des propriétés de la plate-forme (paires clé-valeur). Utilisez les propriétés du système de la machine virtuelle Java ou un équivalent pour .Net. Seules les valeurs sont recherchées.
platformVersion	Agents - Environnement - Version de la machine virtuelle Java	
process	Packages - Environnement - Processus	Renvoie les packages conçus pour le serveur d'applications spécifié.
processName	Agents - Nom du processus, Rapports - Agent - Nom du processus	Renvoie les agents (et leurs rapports) qui s'exécutent sur le serveur d'applications spécifié.
reportName	Rapports - Nom du rapport	
restartRequired	N/D (icône à côté du nom de l'agent)	Renvoie une liste des agents modifiés récemment qui requièrent un redémarrage pour que les modifications prennent effet.
serverName	Agents - Nom du serveur, Rapports - Agent - Nom du serveur	Renvoie les agents (et leurs rapports) qui s'exécutent sur le serveur spécifié.
specificationVersion	N/D	Version des métadonnées utilisées dans le groupe.
status	Agents - Etat de l'agent	Etat de l'agent. Valeurs : actif, arrêté, absent(e)
type	N/D	Type d'agent (par exemple, agent Java).
version	Agents - Version de l'agent, Rapports - Version de l'agent, Groupes - Version	Renvoie les agents de la version correspondante ou les rapports générés pour les agents ou les groupes de la version correspondante.

Recherche à l'aide du langage de requête de Command Center

Spécifiez une requête personnalisée dans la barre de recherche en haut de la page de Command Center (ACC), qui filtre les éléments affichés dans une vue. La requête personnalisée utilise le langage de requête ACC (AQL), qui remplace le langage Lucene utilisé auparavant. Pour en savoir plus sur les différences entre Lucene et AQL, consultez la section [Propriétés de recherche](#).

Création de requêtes simples

Entrez un mot dans la barre de recherche pour filtrer tous les résultats correspondants en fonction de la requête de mot. La recherche est effectuée sur une propriété par défaut, généralement un nom.

Pour rechercher une propriété spécifique, entrez la requête au format suivant : **propertyName:mot_requête_recherche**

NOTE

La valeur **propertyName** doit respecter la casse. A mesure que vous entrez une valeur, la barre de recherche affiche les propriétés disponibles. Utilisez la propriété **all** pour effectuer une recherche sur plusieurs propriétés.

Recherche simple - Exemple :

```
osName:windows
```

Propriétés associées aux entités

Le tableau ci-dessous répertorie les propriétés par défaut, les propriétés disponibles et les propriétés recherchées lors de l'utilisation du mot clé **all**.

Entité	Propriété par défaut	Propriétés du mot clé all	Propriétés disponibles
Agent	spaName Cette propriété effectue une recherche sur serverName, processName et agentName.	agentId, agentName, agentProfile, appServerName, appServerVersion, build, emCollectorHost, emCollectorPort, installPath, logLevel, osArch, osName, osVersion, packageId, packageName, packageOriginId, packageVersion, platformArch, platformName, platformVersion, processName, serverName, spaName, status, type, version	agentId, agentName, agentProfile, all, appServerName, appServerVersion, build, controllerId, emCollectorHost, emCollectorPort, homePath, installPath, isBootstrapped, isFromTeamCenter, lastContact, logLevel, osArch, osName, osVersion, packageId, packageName, packageOrigin, packageOriginId, packageVersion, platformArch, platformName, platformVersion, processName, restartRequired, serverName, spaName, status, type, version
Rapport de diagnostic	reportName	agentName, agentProfile.name, environmentVariables.value, platformProperties.value, reportName, serverName	agentId, agentName, agentProfile, agentProfile.name, all, appServerName, appServerVersion, build, controllerId, controllerLastContact, dynamicExtensionFiles.name, emCollectorHost, emCollectorPort, environmentVariables.value, extensionFiles.name, generatedPackageId, id, installPath, lastContact, logLevel, metricCount, osArch, osName, osVersion, packageId, packageName, pbdPblFiles.name, platformArch, platformName, platformParameters, platformProperties.value, platformVersion, processName, registrationTimestamp, registrationUnixTimestamp, reportName, serverName, spaName, status, type, uid, version
Package	packageName	bundles, comment, emHost, facets, packageName	agentVersion, all, bundles, comment, draft, emHost, exported, facets, id, isAutogenerated, isFromTeamCenter, latest, modified, originId, osName, packageName, process, version

Entité	Propriété par défaut	Propriétés du mot clé all	Propriétés disponibles
Groupe	name (nom)	category, dependencies, description, enhances, facets, name, osName, version, displayName	agentVersionFrom, agentVersionTo, all, author, category, deleted, dependencies, description, dynamic, enhances, facets, id, name, osName, secondaryOsName, specificationVersion, type, version, versionLong, displayName

Créer des requêtes de combinaison

Entrez plusieurs requêtes dans la barre de recherche séparées par des espaces ou entrez plusieurs sous-requêtes à l'aide des opérateurs AND, OR, NOT.

Les opérateurs doivent respecter la casse et vous pouvez utiliser des parenthèses pour les grouper. AND est l'opérateur par défaut pour les requêtes séparées par des espaces.

Requête combinée avec l'opérateur AND – Exemple

Les exemples de requête ci-dessous filtrent les résultats dont tous les mots sont trouvés.

```
word1 AND word2 AND word3
word1 AND word2 word3
word1 word2 word3
```

Requête combinée avec l'opérateur OR – Exemple

Cet exemple indique comment filtrer les résultats en cas de détection de l'un des mots.

```
word1 OR word2 OR word3
```

Requête combinée avec l'opérateur NOT – Exemple

Cet exemple filtre les résultats qui ne contiennent pas le mot *myquery*.

```
NOT myquery
```

Vous pouvez utiliser d'autres symboles plutôt que des opérateurs nommés :

Operator	Autres symboles
ET	&&
Ou	
NON	! ou -

Requête combinée avec un autre symbole – Exemple

Cet exemple filtre les résultats qui ne contiennent pas le mot *myquery*.

```
-myquery
```

Requête combinée avec parenthèses – Exemple

Cet exemple groupe les opérateurs et filtre les résultats.

```
(word1 AND word2) OR word3
word1 AND (word2 OR word3)
```

Autres requêtes de recherche

Vous pouvez utiliser des chaînes, des caractères génériques, des nombres, des expressions régulières et des requêtes de plage comme modèles de recherche pour filtrer les résultats.

Utilisation de chaînes et de caractères génériques

Entrez une chaîne de mots ou de caractères entre guillemets (" ") ou séparés au moyen d'une barre oblique (/) pour filtrer les résultats de la recherche. Les résultats correspondent exactement à la chaîne de recherche. Les caractères génériques vous permettent de filtrer les résultats qui contiennent la chaîne. Vous pouvez utiliser les types de caractères génériques suivants : * pour faire correspondre une sous-chaîne et ? pour faire correspondre un caractère. L'utilisation d'un caractère spécial dans une chaîne est traitée comme un caractère ordinaire.

Requête de chaîne – Exemple

La requête ci-dessous filtre tous les résultats qui correspondent **exactement** à la chaîne.

```
"abc xyz"
```

Requête de caractère générique – Exemple

La requête ci-dessous filtre **tous** les résultats qui contiennent la chaîne de recherche.

```
*"abc xyz"*
```

Requête combinée de chaîne et de caractère générique – Exemple

La requête ci-dessous affiche un modèle de recherche utilisant des caractères génériques, une chaîne et un mot unique.

```
word*"quoted string"?
```

Requête de plage

Une requête de plage peut être une plage de nombres, de versions ou de dates.

La requête ci-dessous filtre les résultats dans la plage **0 à 5** sur la propriété numérique **prop**.

```
prop:[0 TO 5]
```

La requête ci-dessous affiche un modèle de recherche avec une plage exclusive et une étoile indiquant qu'aucune limite maximum n'est définie pour la propriété numérique **prop**.

```
prop:{10 TO *}]
```

Enregistrement de la recherche

Dans la barre de recherche, utilisez l'option **Enregistrer en tant que nouvelle collection** pour enregistrer un modèle de recherche que vous utilisez fréquemment. Vous pouvez également utiliser la recherche enregistrée dans une requête.

Utilisation d'une collection dans une requête – Exemple

```
collection:"Tomcat Agents" AND reportName:Linux
```

Expression régulière

La requête par expression régulière permet d'effectuer une recherche à l'aide d'une expression régulière. Elle commence et se termine par une barre oblique. Vous pouvez saisir une barre oblique inverse pour placer le caractère suivant de

l'expression régulière entre guillemets doubles. Vous pouvez inclure une barre oblique comme caractère dans une requête.

Exemple : `name:/^test [3-4][0-9]/`

Ressource agentFileOperationTask

Ce service Web peut être utilisé pour envoyer des fichiers (par ex. : fichiers de configuration d'agent) vers un répertoire d'agent sur un système distant.

Ce service Web peut être utilisé pour envoyer des fichiers (par ex. : fichiers de configuration d'agent) vers un répertoire d'agent sur un système distant. Il vous permet également de supprimer un fichier d'un répertoire. Cette ressource peut également être utilisée pour obtenir une liste des opérations de copie de fichier effectuées sur un agent.

Verbes pris en charge : GET, HEAD, POST, DELETE, OPTIONS. Paramètres pris en charge : [page](#), [size](#), [sort](#)

NOTE

Par défaut, les méthodes POST et DELETE, ainsi que le transfert de fichiers vers la ressource de fichier d'API sont désactivés et une réponse indiquant Not Allowed est générée. Pour activer cette fonctionnalité, modifiez le fichier `apmccsrv.properties`.

La demande POST suivante copie le fichier avec l'ID 12 dans le répertoire config de l'agent avec l'ID 2 en tant que fichier `my-new-app.pbd`. Cette demande est envoyée à partir du serveur sur lequel l'agent est exécuté.

```
POST https://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/agentFileOperationTask{
  "agent" : "agent/2", "file" : "file/12", "destination" : "core/config/my-new-app.pbd",
  "operation":"COPY"}
```

La demande suivante supprime le fichier de configuration `my-new-app.pbd`.

```
POST https://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/agentFileOperationTask{
  "agent" : "agent/2", "destination" : "core/config/my-new-app.pbd",
  "operation":"DELETE"}
```

Notez que vous pouvez uniquement publier des fichiers déjà transmis à la [ressource de fichier](#) du serveur de configuration (URL `https://<client hébergé ACC>/apm/appmap/acc/apm/acc/file`) ou des fichiers inclus dans un rapport de diagnostic. Propriétés de ressource - Les propriétés suivantes contenant des informations sur la ressource sont disponibles :

Nom de propriété	Type	Description	API Version
tenant	nombre entier	ID du client hébergé	1.1
status	énumération	Statut de l'opération (Suit la définition de la ressource de tâche.)	1.0
creationTimestamp	date	Heure de la création de la ressource (format UTC)	1.0
completionTimestamp	date	Heure de fin de l'opération (format UTC)	1.0
expectedDuration	nombre entier	Durée attendue de l'exécution de l'opération en cours	1.0
source	chaîne	Fichier à envoyer à l'agent, lié au répertoire <code>fileUploads</code> du serveur de configuration	1.0

Nom de propriété	Type	Description	API Version
destination	chaîne	Emplacement du fichier à mettre à jour ou supprimer, lié au répertoire d'installation de l'agent	1.0
operation	énumération	Opération que vous souhaitez effectuer : copie ou suppression	1.0
agentId	nombre entier	Identificateur unique de l'agent sur lequel l'opération est effectuée	1.0
user	chaîne	Utilisateur qui a initié l'opération	1.0
updateErrors	tableau	Tableau d'erreurs renvoyées lors de l'opération	1.0

Ressource de fichier

Ce service Web renvoie des informations sur les fichiers stockés sur le serveur de configuration.

Ce service Web renvoie des informations sur les fichiers stockés sur le serveur de configuration. Les fichiers sont principalement liés aux rapports de diagnostic (fichiers journaux, profils d'agent et fichiers PBD), mais cette ressource est également utilisée comme stockage pour les fichiers destinés à être publiés sur des systèmes distants. Les fichiers peuvent être chargés vers cette ressource à l'aide de la méthode POST.

Verbes pris en charge : GET, POST, DELETE, OPTIONS

Paramètres pris en charge : [page](#), [size](#), [sort](#)

GET

```
GET https://<ACC_tenant_host>/apm/appmap/acc/apm/acc/file/
```

POST

Exemple de chargement de fichier à l'aide d'une commande curl :

```
curl -k -H "Authorization:Bearer 3f77f1e5-6985-4019-8f49-af1ed04e0119" -F name=my-new-app.pbd -F file=@mylocalFile.pbd https://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/file
```

Vous obtenez une réponse similaire à ce qui suit :

```
{  "id": 32,  "name": "my-new-app.pbd",  "size": 6797,  "createdBy": "user@example.com",  "modified": "2015-06-23T09:55:22.096+01:00",  "_links": {    "content": {      "href": "https://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/file/1/content"    }  } }
```

La valeur id est un identifiant du fichier que vous utiliserez ultérieurement dans la demande POST agentFileOperationTask pour le champ file (par exemple, file : file/32).

Propriétés de la ressource

Les propriétés suivantes contenant des informations sur la ressource sont disponibles :

Nom de propriété	Type	Description	API Version
tenant	nombre entier	ID du client hébergé	1.1
ID (identification)	nombre entier	Identificateur unique de cette ressource	1.1
name (nom)	chaîne	Nom du fichier.	1.1
size	nombre entier	Taille en octets du fichier décompressé.	1.1
createdBy (créé par)	chaîne	Nom de l'utilisateur qui a enregistré le fichier. Valeur nulle dans un rapport de diagnostic.	1.1
modified (modifié)	date	Heure de modification du fichier. Défini sur « heure actuelle » si le fichier a été enregistré par un utilisateur.	1.1
fichier	fichier multipartite	Paramètre de formulaire utilisé dans les commandes POST exécutées pour charger la ressource de fichier.	1.1

Ressource package

Ce service Web renvoie des informations sur les packages d'agent disponibles dans APM Command Center.

Ce service Web renvoie des informations sur les packages d'agent disponibles dans APM Command Center. Vous pouvez également télécharger ces packages au format ZIP ou TAR. Verbes pris en charge : GET, HEAD, POST, PATCH, DELETE, OPTIONS

Paramètres pris en charge : [page](#), [size](#), [sort](#), [q](#), format, [projection](#)

GET

```
GET https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/package
```

Utilisez la requête suivante pour obtenir des informations sur le package avec l'ID 1 :

```
GET https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/package/1
```

Pour télécharger le package, accédez au lien disponible sur la page de détails du package Command Center dans l'interface utilisateur.

Utilisez la requête suivante pour obtenir les instructions d'installation (au format Markdown) pour le package :

```
GET https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/package/1/installInstructions
```

Utilisez la requête suivante pour obtenir des informations sur les groupes contenus dans le package :

```
GET https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/package/1/bundles
```

Utilisez la requête suivante pour obtenir des informations sur les groupes requis pour le package :

```
GET https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/package/1/requiredBundles
```

Utilisez la requête suivante pour obtenir des informations sur tous les groupes compatibles avec le package, y compris ceux qui sont déjà inclus dans celui-ci :

```
GET https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/package/1/compatibleBundles
```


Utilisez la requête suivante pour obtenir des informations sur tous les packages compatibles avec le package spécifié :

GET `https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/package/1/compatiblePackages`

POST La requête suivante crée un package d'agent avec les propriétés spécifiées.

POST `https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/package{ "name": "WebSphere Windows Package", "description": "Example WebSphere Package", "environment": { "osName": "windows", "process": "websphere", "agentVersion": "10.2" }}`

PATCH Les requêtes PATCH vous permettent d'ajouter ou de mettre à jour une propriété de groupe dans le package.

L'exemple suivant met à jour les propriétés `patched.via.rest.api` et `introscope.agent.acc.port` avec les valeurs indiquées :

PATCH `https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/package/111{ "bundleOverrides": { "acc": { "preamble": null, "properties": [{ "name": "new.via.ui", "description": null, "type": null, "value": "yes it is", "validator": null, "hidden": false, "id": null }, { "name": "patched.via.rest.api", "value": "from a patch" }, { "name": "introscope.agent.acc.port", "value": 55555 }] } }`

DELETE La requête suivante supprime le package d'agent avec l'ID 2 :

DELETE `https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/package/2`

Propriétés de la ressource

Les propriétés suivantes contenant des informations sur la ressource sont disponibles :

Nom de propriété	Type	Description	API Version
tenant	nombre entier	ID du client hébergé	1.1
ID (identification)	nombre entier	Identificateur unique de cette ressource	1.1
name (nom)	chaîne	Nom du package.	1.1
description	chaîne	Commentaire pour le package saisi par l'utilisateur.	1.1
version	nombre entier	Numéro de version de ce package (incrémenté après le téléchargement du package modifié).	1.1
bundles	sous-ressource	Groupes contenus dans le package.	1.1
emHost	chaîne	Nom d'hôte ou adresse IP et port des gestionnaires d'entreprise auxquels l'agent se connecte.	1.1
latest	Valeur booléenne	Indique la version actuelle du package.	1.1
origin	nombre entier	ID de la version originale du package.	1.1
draft	Valeur booléenne	Indique si le package doit être disponible pour utilisation.	1.1

bundle Resource

Ce service Web renvoie des informations sur les groupes disponibles dans APM Command Center. Verbes pris en charge : GET, HEAD, POST, DELETE, OPTIONS. Paramètres pris en charge : [page](#), [size](#), [sort](#), [q](#)

GET

```
GET https://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/bundle
```

POST

Ceci est un exemple de chargement de groupe à l'aide d'une commande Curl :

```
curl -k -H "Authorization:Bearer <jeton>" -F file=@leakhunter-10.5.tar.gzhttps://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/bundle
```

Vous obtenez une réponse similaire à ce qui suit :

```
{ "id": 26, "name": "leakhunter", "addedBy": null, "author": "Not Specified",
  "displayName": "Leak Hunter", "description": "This bundle tracks the size of most
  default Java Collections.", "version": "10.5", "agentVersion": "10.5", "path":
  "leakhunter-10.5.tar.gz", "facets": [ "leakhunter" ], "dependencies": [ "java-agent",
  "process" ], "enhances": [], "excludes": [], "compatibility": { "osName": null,
  "agentVersion": "10.5" }, "specificationVersion": "1", "type": "java", "dynamic":
  null, "links": { "self": { "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/
  bundle/26" }, "profile": { "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/
  bundle/26/profile" }, "download": { "href": "https://<ACC tenant host>/apm/appmap/acc/apm/
  acc/bundle/26?format=archive" } } }
```

DELETE

La demande suivante supprime le groupe avec l'ID 21 :

```
DELETE https://<hôte_client_hébergé_ACC>/apm/appmap/acc/apm/acc/bundle/21
```

Lorsqu'un groupe est supprimé :

- Il n'est plus visible lors de l'exécution d'une opération GET sur la ressource.
- Il n'est plus répertorié en tant que groupe disponible lors de la création ou de la modification d'un package.
- Il s'affiche dans les packages existants qui l'utilisent, mais sera marqué comme groupe supprimé. Une fois le groupe supprimé d'un package, vous ne pouvez plus le rajouter.

Remarque : Vous ne pouvez pas supprimer des propriétés principales lbundles.Resource.

Les propriétés suivantes contenant des informations sur la ressource sont disponibles :

Nom de propriété	Type	Description	API Version
tenant	nombre entier	ID du client hébergé	1.1
ID (identification)	nombre entier	Identificateur unique de la ressource	1.1
name (nom)	chaîne	Nom interne du groupe	1.1
displayName	chaîne	Nom du groupement au format convivial	1.1
description	chaîne	Description courte du groupe	1.1
version	chaîne	Version du groupe	1.1
agentVersion	chaîne	Version de l'agent APM pour lequel le groupe est conçu	1.1

Nom de propriété	Type	Description	API Version
chemin	chaîne	chemin d'accès au fichier d'archive du groupe	1.1
facets	tableau	Liste des facettes identifiant le groupe	1.1
dependencies	tableau	Liste des facettes dont le groupe dépend	1.1
enhances	tableau	Liste des facettes améliorées par le groupe	1.1
compatibility	sous-ressource	Définit les contraintes de compatibilité du groupe comme osName et agentVersion.	1.1
specificationVersion	chaîne	Version de spécification de métadonnées du groupe	1.1
type	chaîne	Type de groupe ; actuellement, il s'agit toujours de java.	1.1
deleted	Valeur booléenne	Détermine si le groupe est supprimé (true) ou actif (nul ou false).	1.1
category	chaîne	Catégorie du groupe : core, environment, feature, custom	1.1

Ressource agentPackageTask

Vous pouvez utiliser le service Web agentPackageTask pour mettre à jour un package d'agent avec des groupes (modifiés ou nouveaux) déployables à chaud.

Vous pouvez utiliser le service Web agentPackageTask pour mettre à jour un package d'agent avec des groupes (modifiés ou nouveaux) déployables à chaud. Ce service Web propose un package contenant les modifications apportées au répertoire d'installation de l'agent APM. Verbes pris en charge : GET, HEAD, POST, OPTIONS. Paramètres pris en charge : [page](#), [size](#), [sort](#).

GET

GET `https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/agentPackageTask/`

POST L'API REST suivante lance une demande push. Les groupes ne peuvent pas être déployés directement vers des agents ; ils doivent être inclus dans un package qui leur sera transmis. Spécifiez l'ID de l'agent à mettre à jour et l'ID du package à livrer.

POST `https://<hôte client hébergé ACC>/apm/appmap/acc/apm/acc/agentPackageTask{agent: agent/1,package: package/5}`

Propriétés de ressource - Les propriétés suivantes contenant des informations sur la ressource sont disponibles :

Nom de propriété	Type	Description	API Version
tenant	nombre entier	ID du client hébergé	1.1
agent	nombre entier	Identificateur unique de l'agent sur lequel l'opération est effectuée	1.1

Nom de propriété	Type	Description	API Version
package	nombre entier	Identificateur unique du package déployé sur l'agent	1.1
status	énumération	Statut de la demande	1.1
extStatus	chaîne	Décrit le statut d'échec. Conformément aux directives de l'API REST, un seul état d'échec est imposé. Développe la cause des erreurs, telle que l'absence de réponse du contrôleur ou le non-réenregistrement de l'agent en temps voulu.	1.1
creationTimestamp	date	Heure de la création de la ressource (format UTC)	1.1
completionTimestamp	date	Heure de fin de l'opération (format UTC)	1.1
expectedDuration	nombre entier	Durée attendue de l'exécution de l'opération en cours	1.1
user	chaîne	Utilisateur qui a initié l'opération	1.1
updateErrors	tableau	Tableau d'erreurs liées au module d'extension, telles que des problèmes d'autorisation lors de la copie de groupes dans le répertoire Wily	1.1
addedBundles	tableau	Liste des noms de groupe en cours d'ajout (peut être vide)	1.1
removedBundles	tableau	Liste des noms de groupe en cours de suppression (peut être vide)	1.1

API hypermédia de DX APM

DX APM fournit plusieurs API hypermédia qui peuvent être utilisées par les utilisateurs. Cette section décrit les concepts élémentaires et les mécanismes communs partagés par les API hypermédia de DX APM :

L'architecture d'application REST HATEOAS (Hypermedia As The Engine Of Application State) permet à un client d'interagir avec DX APM via un hypermédia. Pour pouvoir utiliser une API hypermédia vous devez uniquement connaître l'[URL de base](#). Toutes les ressources et les actions disponibles sont fournies dynamiquement par le serveur d'applications lorsque vous travaillez.

Les API RESTful de DX APM utilisent HTTP en tant que protocole par défaut et HAL ([Hypertext Application Language](#)) et [JSON](#) pour les représentations.

Notez que certaines fonctionnalités décrites dans cette spécification sont implémentées par toutes les API. Pour plus d'informations sur chaque API, reportez-vous à la section [API REST de DX APM](#).

Vous pouvez utiliser plusieurs outils pour interagir avec les API hypermédia de DX APM. Exemple :

- Extension Postman pour Chrome
- cURL (outil de ligne de commande)
- Langages de script (Python)

Codes de statut de réponse

L'API renvoie les codes de statut HTTP avec la réponse.

En général, les codes de statut HTTP sont regroupés dans plusieurs catégories distinctes :

- Les codes **1xx** sont informatifs.
- Les codes **2xx** indiquent une réussite.
- Les codes **3xx** indiquent une redirection.
- Les codes **4xx** indiquent des erreurs du client (le client a entraîné une erreur).
- Les codes **5xx** définissent des erreurs côté serveur (le serveur a entraîné une erreur).

Le tableau suivant présente les codes de statut d'opération réussie en fonction de la méthode utilisée :

Method	Valeur renvoyée en cas de réussite	En-tête accompagné	Corps de la réponse
GET	200 OK	variable	variable
POST	201 Créé	Emplacement : renvoie à la ressource créée	vide
POST - asynchrone	202 Accepté	Emplacement : renvoie à une ressource qui sera créée sous peu	vide
POST	200 OK	-	ressource créée
PUT (nouvelle ressource)	201 Créé	Emplacement : renvoie à la ressource créée	vide
PUT (nouvelle ressource)	200 OK	-	ressource créée
PUT (nouvelle ressource) - asynchrone	202 Accepté	Emplacement : renvoie à une ressource qui sera créée sous peu	vide
PUT (ressource existante)	204 Aucun contenu	-	vide
PUT (ressource existante) - asynchrone	202 Accepté	Emplacement : renvoie à une ressource qui sera mise à jour sous peu	vide
PATCH	204 Aucun contenu	-	vide
PATCH - asynchrone	202 Accepté	-	vide
DELETE	200 OK	-	-
DELETE - asynchrone	202 Accepté	-	-

Autorisation et authentification des API

L'authentification des API RESTful d'APM repose sur des jetons de porteur qui peuvent être créés dans l'interface utilisateur de l'application associée. Le jeton permet aux API d'accéder aux services Web de l'application.

Les clients peuvent créer des jetons associés à leur compte. En outre, à condition qu'ils soient authentifiés et autorisés, ils peuvent également mettre à jour, extraire et supprimer (révoquer) les jetons qu'ils possèdent ou auxquels ils ont accès en lecture/écriture.

Création de jetons de porteur

Pour connaître la procédure à suivre pour créer un jeton de porteur, consultez la documentation de l'API concernée.

Utilisation des jetons de porteur

Le client doit envoyer un jeton avec chaque demande. La démonstration d'un jeton suffit au serveur de ressources pour authentifier le client et appliquer des règles d'autorisation à la demande.

Le jeton de porteur est envoyé au serveur de ressources dans le champ d'en-tête de la demande d'autorisation.

Exemple :

```
GET /resource HTTP/1.1
Host: server.example.com
Authorization: Bearer f47ac10b-58cc-4378-a567-0e02b2c3d479
```

Statut HTTP d'authentification et codes d'erreur

Si l'authentification de la demande échoue pour une quelconque raison, le serveur de ressources renvoie un code d'erreur HTTP pertinent et un en-tête de réponse contenant les détails relatifs à l'erreur.

- 401 Non autorisé
- 403 Interdit

Pour plus d'informations, rendez-vous sur la [page consacrée aux définitions de code des statuts HTTP](#) (en anglais).

Accès aux ressources

La récupération des ressources peut être implémentée à l'aide de simples requêtes HTTP GET. Ouvrez l'URL de base dans votre navigateur Web pour récupérer la ressource racine qui vous indique les ressources et les actions disponibles. Vous pouvez demander des ressources spécifiques ou des collections de ressources ; vous pouvez contrôler la pagination ou trier, filtrer et rechercher les ressources.

Les API RESTful de DX APM prennent en charge le type de média Internet HAL et par défaut un document au format HAL est renvoyé. Certaines API peuvent également prendre en charge d'autres formats ; par ex. : application/xml, texte/csv, texte/brut, etc.

Ressource racine

Toutes les API publiques de DX APM présentent une ressource racine. La ressource racine contient des liens (HAL) vers toutes les ressources disponibles ainsi que d'autres informations telles que les métadonnées, versions etc.

Vous pouvez récupérer la ressource racine en accédant à l'URL de base de l'API.

```
GET https://<host>:<port>/apm/<service>
```

Par exemple, utilisez la demande suivante pour obtenir la ressource racine de APM Command Center :

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc
```

La ressource racine suivante est reçue comme réponse :

```
{
  "vendor": "Broadcom",
  "apiVersion": "1.0.1",
  "serverVersion": "10.0.1",
  "serviceProvider": "com.ca.apm.acc",
  "_links": {
    "controller": {
      "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/controller{?page,size,sort}",
      "templated": true
    }
  },
}
```

```

    .
    .
    .
  }
}
}

```

La ressource racine inclut les informations suivantes :

- fournisseur : Broadcom
- apiVersion : version d'API
- serverVersion : la version de l'application/du composant qui présente sa logique applicative via l'API RESTful.
- serviceProvider : nom complet du service
- _links : liste des liens vers toutes les ressources disponibles

Collection de ressources

Le client peut demander des ressources spécifiques ou une collection de ressources. Les collections sont représentées sous forme de tableaux (selon le format JSON) de ressources spécifiques.

```
GET https://<host>:<port>/apm/<service>/resource
```

Un tableau de ressources spécifiques est intégré à la propriété `_embedded` de la ressource :

```

{
  "_links": {
    << list of related links >>
  },
  "_embedded": {
    "<< resource name >>": [
      {
        << resource 1 data >>
      },
      {
        << resource 2 data >>
      },
      .....
    ]
  },
  "_page" : {
    <paging information>
  }
}

```

Lorsqu'une ressource est requise, la réponse contient uniquement la ressource demandée.

```
GET https://<host>:<port>/apm/<service>/resource/1
```

Exemple de réponse :

```

{
  "id": 1,
  "serverName": "ACCserver01",
  "agentName": "Tomcat Agent",
  "status": "ACTIVE",
  "processName": "Tomcat",

```

```

    "_links": {
      "self": {
        "href": "/agent/1{?projection}",
        "templated": true
      },
      "reports": {
        "href": "agent/1/report"
      },
      "agentUpdateTasks": {
        "href": "/agent/1/agentUpdateTask"
      }
    }
  }
}

```

Paramètres de demande courants

Pour accéder à des collections de ressources, le nombre de ressources peut être excessif et affecter l'utilisation. Par conséquent, les clients peuvent utiliser les propriétés suivantes comme paramètres d'interrogation HTTP GET pour rendre les demandes plus précises :

- [page et size](#)
- [sort](#)
- [projection](#)
- [format](#)
- [q](#)

Page et Size (taille)

Vous pouvez contrôler les pages renvoyées ou le nombre de résultats contenus dans une page. Par défaut, les 20 premiers résultats sont renvoyés.

Utilisez les paramètres suivants :

- **page**
Nombre de pages à renvoyer (Par défaut, 0 indique la première page renvoyée.)
- **size**
Taille de page requise. Si le paramètre de taille est défini sur 0, toutes les ressources sont affichées.

Exemples :

La demande suivante renvoie les 50 premiers résultats :

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?page=0&size=50
```

La demande suivante renvoie 51 à 60 résultats :

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?page=5&size=10
```

Sort

Les collections peuvent être triées par propriétés de ressource spécifiques. Les clients peuvent utiliser le paramètre sort pour contrôler le tri.

Exemples :

La demande suivante trie les agents par nom :


```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?sort=agentName
```

La demande suivante récupère la première ressource d'agent (size=1) de la liste triée par nom d'agent dans l'ordre décroissant et par emplacement d'installation dans l'ordre croissant. Notez que l'ordre des paramètres est pris en compte.

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?
sort=name,DESC&sort=installPath,ASC&size=1
```

Projection

Les prévisions renvoient un sous-ensemble prédéfini des données. Il existe deux types de prévisions :

- **Prévisions statiques**

Les prévisions statiques sont des sous-ensembles prédéfinis contenant les propriétés disponibles de la ressource. Elles portent un nom descriptif et peuvent être transmises par le paramètre HTTP projection lors de la demande d'une collection de ressources ou d'une ressource spécifique.

- **Prévisions dynamiques**

Les prévisions dynamiques permettent au client de définir explicitement les propriétés de ressource à renvoyer. Si des ressources dynamiques sont utilisées, le paramètre HTTP fields (champs) définit une liste séparée par des virgules des champs de ressources attendus.

Lorsqu'elles sont disponibles, les prévisions sont décrites dans la documentation d'API correspondante.

Exemple :

La demande suivante renvoie une liste d'agents avec des informations de base :

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?projection=list
```

Exemple de réponse :

```
{  "_links": {
    "self": {
      "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?
projection=list{&q,page,size,sort,projection,format}",
      "templated": true
    }
  },  "_embedded": {
    "agent": [
      {
        "id": 1,
        "serverName": "ACCLinuxServer01",
        "status": "ACTIVE",
        "processName": "Tomcat",
        "agentName": "Tomcat Agent",
        "_links": {
          "self": {
            "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent/1{?projection}",
            "templated": true
          },
          "controller": {
            "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent/1/controller"
          },
          "diagnosticReports": {
            "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent/1/diagnosticReports"
          },
          "agentUpdateTasks": {
```

```

        "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent/1/agentUpdateTasks"
    }
}
},
{
    "id": 2,
    "serverName": "ACCWinServer01",
    "status": "ACTIVE",
    "processName": "Tomcat",
    "agentName": "Tomcat Agent",
    "_links": {
        "self": {
            "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent/2{?projection}",
            "templated": true
        },
        "controller": {
            "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent/2/controller"
        },
        "diagnosticReports": {
            "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent/2/diagnosticReports"
        },
        "agentUpdateTasks": {
            "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent/2/agentUpdateTasks"
        }
    }
}
}
], "page": {
    "size": 20,
    "totalElements": 2,
    "totalPages": 1,
    "number": 0 }}

```

Format

Renvoie les données au format spécifié. Le paramètre format est prioritaire sur l'en-tête HTTP Accept, qui est le mécanisme par défaut utilisé pour demander un format spécifique (Ex. : Accept: text/csv; q=1.0).

Exemple :

La demande suivante renvoie des informations sur les agents au format CSV :

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?format=csv
```

Exemple de réponse :

```

"id","agentName","serverName","processName","status","type","version","build","logLevel","registries"
"1","Tomcat Agent","ACCLinuxServer01","Tomcat","ACTIVE","JavaAgent","9.7.1","16","INFO","2015-04-29
05:15:46 +0100","2015-04-30 05:20:45 +0100","ACCWinServer01","5001","Apache
Tomcat","5.5.34.0","Oracle Corporation","1.7.0",,"Red Hat Enterprise Linux
Server","6.1, kernel 2.6.32-131.0.15.el6.x86_64","amd64","59"

```

```
"2","Tomcat
Agent","ACCWinServer01","Tomcat","ACTIVE","JavaAgent","9.7.1","16","INFO","2015-04-29
05:16:26 +0100","2015-04-30 05:16:26 +0100","ACCWinServer01","5001","Apache
Tomcat","5.5.34.0","Oracle Corporation","1.7.0_51",,"Windows Server 2008
R2","6.1","amd64","66"
```

q

Recherche ou filtrage de collection. Cette option permet de transmettre des [requêtes de filtrage ou de recherche](#) au serveur de ressources.

Date et heure

La date et l'heure sont représentées au format [ISO 8601](#).

Recherche et filtrage de ressources

La fonctionnalité de **recherche** permet à un client de récupérer des informations à partir de l'API. Il en résulte généralement un document contenant plusieurs ressources différentes.

La recherche utilise une ressource explicite (/search) qui accepte des demandes GET qui transfèrent la chaîne de recherche comme valeur du paramètre d'interrogation q HTTP ou des demandes POST qui envoient la chaîne de recherche avec le corps de la demande. La réponse contient un document JSON avec les résultats au format `_ressources` intégrées.

Le **filtrage** est la capacité de l'API à renvoyer un ensemble filtré d'une ressource spécifique.

Le filtrage est implémenté dans chaque ressource qui le prend en charge. Les ressources qui prennent en charge le filtrage indiquent la fonctionnalité de filtrage dans les liens basés sur un modèle HAL (Notez le paramètre q dans l'exemple suivant.) :

```
{
  "_links": {
    "self": {
      "href": "/agent{?q,page,projection,size,sort}",
      "templated": true
    }
  }
}
...
...
}
```

Les clients peuvent utiliser les fonctionnalités de filtrage d'une ressource à l'aide d'une demande POST (qui transfère la chaîne de recherche comme valeur du paramètre d'interrogation q HTTP) ou d'une demande POST (qui envoie la chaîne de recherche avec le corps de la demande).

Exemple :

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=agentName:Tomcat
```

NOTE

La ressource de recherche n'est pas toujours disponible dans une API, ni la fonctionnalité de filtrage. Les utilisateurs doivent lire la documentation de chaque API pour vérifier la disponibilité de ces fonctionnalités.

La [syntaxe Lucene](#) est prise en charge pour la recherche et le filtrage. Les paragraphes suivants décrivent la syntaxe de chaîne de requête prise en charge par les API RESTful de CA APM.

Termes

Une requête peut comporter un seul terme ou une phrase placée entre guillemets doubles. Vous pouvez combiner plusieurs termes à des opérateurs booléens pour former une requête plus complexe.

Champs

Lorsque vous lancez une recherche, vous pouvez spécifier un champ. Vous pouvez rechercher un champ en saisissant son nom suivi par deux-points, puis le terme que vous recherchez. Utilisez des guillemets pour les expressions de plusieurs mots. Si aucun champ n'est spécifié, la recherche s'applique à tous les champs.

Exemple :

La requête suivante recherche tous les agents nommés Apache Tomcat :

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=agentName:"Apache Tomcat"
```

Recherches de caractère générique

La fonctionnalité de recherche prend en charge les recherches de caractères génériques uniques ou multiples dans des termes individuels (mais non dans des requêtes de phrase) :

- Pour effectuer une recherche de caractère générique unique, utilisez le signe ?.
- Pour effectuer une recherche de caractères génériques multiples, utilisez le signe *.

Exemple :

La requête suivante recherche tous les agents exécutés sur un serveur dont le nom contient le terme Linux :

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=serverName:*Linux*
```

Recherches d'expression régulière

La fonctionnalité de recherche peut prendre en charge les recherches d'expression régulière correspondant à un modèle entre barres obliques (/). La syntaxe peut changer d'une version à l'autre, mais la syntaxe actuellement prise en charge est documentée dans la classe [RegExp](#).

Exemple :

La requête suivante recherche des rapports dont le nom inclut les caractères indiqués. Les deux chaînes ACCServerWin01|Tomcat|Tomcat Agent et ACCServerLinux01|Tomcat|Bobcat Agent correspondent à cette requête.

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/diagnosticReport?q=/ACCServer.*01\|Tomcat\|.*Agent/
```

Recherches de plage

Les requêtes de plage vous permettent de mettre en correspondance des documents dont les valeurs de champ entre les limites supérieure et inférieure spécifiées par la requête de plage. Les requêtes peuvent inclure ou exclure des limites inférieures et supérieures. Les requêtes de plage inclusives sont indiquées entre crochets et les requêtes de plage exclusives entre accolades. Le tri est effectué de façon lexicographique.

En plus des dates exactes, vous pouvez également utiliser des périodes, telles que semaines (w), des jours (d), des heures (h), des minutes (m) et des secondes (s).

Exemples :

La requête suivante recherche tous les agents dont le dernier horodatage de contact est compris entre le 1er avril 2015 (inclus) et la date du jour en cours :

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=lastContact:[2015-04-01 TO NOW]
```

La requête suivante recherche tous les agents dont le dernier horodatage de contact est compris entre le 1er avril et le 1er juin 2015, à exclusion des jours mentionnés :

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=lastContact:{2015-04-01 TO 2015-06-01}
```

La requête suivante recherche les agents dont l'horodatage lastContact date de moins de cinq jours :

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=lastContact:[-5d TO NOW]
```

La requête suivante recherche les agents dont l'horodatage lastContact datant d'au moins deux jours, mais de moins de cinq semaines :

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=lastContact:[-5w TO -2d]
```

Amélioration d'un terme

La syntaxe de recherche peut fournir un niveau de pertinence des documents correspondants en fonction des termes trouvés. Pour améliorer un terme, utilisez le signe du caret (^) avec un facteur d'amélioration (un nombre) à la fin du terme recherché. Plus le facteur d'amélioration est élevé, plus le terme sera pertinent.

Opérateurs booléens

Les opérateurs booléens permettent de combiner des termes à l'aide d'opérateurs logiques.

- **Ou**

L'opérateur OU est l'opérateur de conjonction par défaut. En d'autres termes, si aucun opérateur booléen n'est placé entre deux termes, l'opérateur OU est utilisé. L'opérateur OU relie deux termes et recherche un document correspondant si l'un des termes existe dans un document. Le symbole || peut être utilisé à la place du mot OU.

- **ET**

L'opérateur ET met en correspondance des documents dans lesquels les deux termes existent dans le texte d'un document. Le symbole && peut être utilisé à la place du mot ET.

- **+**

L'opérateur + (ou requis) requiert que le terme suivant le symbole + figure dans le champ d'un seul document.

- **NON**

L'opérateur NON exclut les documents qui contiennent le terme suivant NON. Le signe ! peut être utilisé à la place du mot NON.

- **-**

L'opérateur - (ou interdit) exclut les documents qui contiennent le terme suivant le signe -.

Exemples :

La requête suivante recherche les agents dont le nom est Tomcat et le niveau de journalisation est défini sur debug :

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=agentName:Tomcat AND
logLevel:debug
```

La requête suivante recherche tous les agents actifs exécutés sur un serveur Linux :

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=osName:Linux NOT status:away
```

La requête suivante recherche les ressources qui doivent contenir le terme Linux et peuvent contenir le terme server :

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=+Linux server
```

Groupement

La syntaxe prend en charge l'utilisation des parenthèses pour grouper des clauses et former ainsi des sous-requêtes. Cela peut être utile pour contrôler la logique booléenne d'une requête.

Exemple :

La requête suivante recherche les agents dont le nom est Tomcat et qui s'exécutent sur le serveur d'application 5.4 ou 5.5 :

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=(appServerVersion:5.5* OR
appServerVersion:5.4*) AND agentName:Tomcat
```

Groupement de champs

La syntaxe prend en charge l'utilisation des parenthèses pour grouper des clauses multiples dans un champ unique.

Exemple :

La requête suivante recherche les agents exécutés sur des serveurs Windows ou Linux :

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=osName:(Windows OR Linux)
```

Echappement de caractères spéciaux

La syntaxe prend en charge l'échappement des caractères spéciaux suivants : + - && || ! () { } [] ^ " ~ * ? : \ /

Pour échapper ces caractères, utilisez une barre oblique inverse (\) devant ceux-ci.

Création et mise à jour des ressources

Les ressources sont créées à l'aide de requêtes HTTP PUT ou POST :

- POST est utilisé lorsque le client n'a pas besoin de spécifier l'ID de la ressource générée. L'API crée l'ID et la renvoie au client.
- PUT est utilisé lorsque l'ID est connu du client.

Une ressource peut être mise à jour à l'aide de PUT ou PATCH :

- PUT requiert une représentation complète de l'entité à fournir, mais les champs facultatifs peuvent être omis, auquel cas le serveur de ressources conserve les valeurs existantes. Le champ Content-Type définit le type de média Internet de la représentation.
- PATCH est interprété par le serveur de ressources en tant que demande pour appliquer un patch à une ressource existante. Le corps de la demande doit contenir toutes les informations requises pour la modification.

NOTE

Certaines ressources ne prennent pas en charge ces méthodes, car elles sont en lecture seule. Reportez-vous à la documentation de l'API correspondante avant d'utiliser des demandes non sécurisés (créer, mettre à jour, supprimer).

Récapitulatif de la méthode HTTP

Le tableau suivant vous permet de décider quelle méthode HTTP utiliser pour la création, la mise à jour ou la suppression des ressources.

Action	Méthode HTTP	URL	Corps de la demande
Création d'une ressource sans spécifier l'ID	POST	Utilisez l'URL de collecte ; par ex. : <code>http://host:port/apm/acc/agents</code> .	Ajoutez toutes les propriétés non nulles de la ressource dans la charge utile. L'omission d'une propriété entraîne l'utilisation de sa valeur par défaut, si cela est autorisé, ou une erreur si la propriété n'a pas de valeur par défaut.
Création d'une ressource avec un ID spécifique	PUT	Spécifiez l'ID exact dans l'URL. Par exemple, <code>http://host:port/apm/acc/agents/14</code> pour créer un agent avec l'ID 14.	Ajoutez toutes les propriétés non nulles de la ressource dans la charge utile. L'omission d'une propriété entraîne l'utilisation de sa valeur par défaut, si cela est autorisé, ou une erreur si la propriété n'a pas de valeur par défaut.
Mise à jour d'une ressource avec une autre (mise à jour complète)	PUT	Spécifiez l'ID exact dans l'URL. Par exemple, <code>http://host:port/apm/acc/agents/14</code> pour créer un agent avec l'ID 14.	Ajoutez toutes les propriétés non nulles de la ressource dans la charge utile. L'omission d'une propriété entraîne l'utilisation de sa valeur par défaut, si cela est autorisé, ou une erreur si la propriété n'a pas de valeur par défaut.
Mise à jour partielle d'une ressource	PATCH	Spécifiez l'ID exact dans l'URL. Par exemple, <code>http://host:port/apm/acc/agents/14</code> pour créer un agent avec l'ID 14.	Ajoutez uniquement les propriétés que vous souhaitez mettre à jour. L'omission d'une propriété signifie que le serveur utilisera la valeur actuelle de la ressource.
Suppression d'une ressource	DELETE	Spécifiez l'ID exact dans l'URL. Par exemple, <code>http://host:port/apm/acc/agents/14</code> pour supprimer un agent avec l'ID 14.	N/D

Exemples

Pour obtenir des exemples d'utilisation de méthode POST, PUT ou PATCH, consultez la documentation des implémentations d'API spécifiques.

En-têtes HTTP courants

En-têtes de demande

Le tableau suivant répertorie les en-têtes de requête HTTP généralement pris en charge par les API RESTful de DX APM.

En-tête HTTP	Cas d'utilisation/objectif
Accept-Language	Le client demande une langue spécifique pour l'utiliser lors de la création des représentations. Le champ de l'en-tête de demande Accept-Language est similaire au champ Accepter, mais limite l'ensemble des langues naturelles privilégiées comme réponse à la demande.
Content-Type	Utilisé lorsque le client envoie un corps de message avec une demande POST/PUT/PATCH. Décrit le type de média Internet utilisé pour coder le corps de la requête HTTP.
Authorization	Utilisé lorsque le client souhaite authentifier la demande. Le client envoie les informations d'identification contenant les détails d'authentification.
Accept-Encoding	Le client demande au serveur d'utiliser la compression de réponses (si possible).
Host	En-tête obligatoire suivant protocole HTTP. Le champ d'en-tête de demande host spécifie l'hôte Internet et le numéro de port de la ressource demandée, obtenus à partir de l'URI d'origine fournie par l'utilisateur ou la ressource de référence.
If-None-Match	Le client utilise cet en-tête pour envoyer la valeur de balise électronique de la représentation mise en cache.
If-Match	Le client souhaite traiter l'opération demandée (Ex. : supprimer) uniquement si une précondition de balise électronique correspond. L'en-tête contient la valeur de réponse de balise électronique d'un appel précédent. Le serveur doit agir uniquement si aucun autre client n'a modifié la ressource.
If-Modified-Since	Le client utilise cet en-tête pour envoyer la date de la dernière modification de la ressource mise en cache.

En-têtes de réponse

Le tableau suivant répertorie les en-têtes de réponse HTTP que le serveur peut renvoyer.

En-tête HTTP	Cas d'utilisation/objectif
Content-Type	Décrit le type de média Internet utilisé pour coder le corps de la réponse HTTP.
Content-Encoding	Si cet en-tête est présent, la valeur indique des codages de contenu supplémentaires qui ont été appliqués à l'entité (Ex. : compression au format .gzip).
Cache-Control	Le champ d'en-tête général Cache-Control permet de spécifier les directives qui doivent être respectées par tous les mécanismes mis en cache avec la chaîne de demande/réponse.

Informations complémentaires :

Pour plus d'informations sur les définitions de champ d'en-tête, rendez-vous sur le [site Web W3C](#).

Messages et codes d'erreur

Pour chaque opération dont le résultat est inattendu, l'API renvoie une erreur contenant les éléments suivants :

- Code d'erreur
- Message d'erreur
- Horodatage
- Un lien vers la documentation contenant la description complète de l'erreur

Exemple de message d'erreur :

```
{  "_links": {  "description": {  "href": "http://wiki.ca.com/.../Errors#ES1001"  }  },  "errorCode":
  "ES1001",  "errorMessage": "Invalid parameter: serverNames",  "timestamp": "2015-04-12T18:51:19+01:00"}
```

Plages de codes d'erreur

Les codes d'erreur d'API commencent par les lettres EA suivies de quatre chiffres. Les erreurs sont classées en deux catégories : erreurs courantes (pour toutes les API) et erreurs spécifiques à une ressource. Pour obtenir les descriptions des erreurs spécifiques aux ressources, consultez la documentation de l'API correspondante.

Plage de codes d'erreur	Fournisseur de la ressource
1000 - 1014	Codes d'erreur EPAgent hérités
EA0000 - EA0999	Erreurs standard du secteur (Codes de statut HTTP)
EA1000 - EA1999	Erreurs générales d'API CA APM
EA2000 - EA2999	Erreurs d'API REST du gestionnaire d'entreprise
EA3000 - EA3999	Erreurs d'API REST du centre de commande
EA4000 - EA4999	Nouveaux codes d'erreur EPAgent

Erreurs Standard du secteur

Les erreurs dans la plage comprise entre EA0100 et EA0599 sont des codes de statut HTTP standard. Pour plus d'informations, reportez-vous au document [RFC 7231](#).

Erreurs générales d'API CA APM

Code d'erreur (plage)	Description	Utilisation
EA1001	Requête de recherche incorrecte	Code renvoyé lorsqu'une demande de filtre ou de recherche échoue en raison d'une requête non conforme à la syntaxe Lucene.

Messages et codes d'erreur spécifiques à l'API

ErrorCode	Type d'erreur
403 Interdit	
1000	ACCESS_FORBIDDEN
1001	LOGIN_FAILED
405 Méthode non autorisée	
2000	METHOD_NOT_ALLOWED
2001	ATTRIBUTE_CANNOT_BE_DELETED
2002	ATTRIBUTE_CANNOT_BE_UPDATED
400 Demande incorrecte	
3000	BAD_REQUEST
3100	INVALID_INPUT_SYNTAX
3110	MISSING_REQUIRED_PARAMETER
3111	MISSING_ATTRIBUTE_NAME
3112	MISSING_ATTRIBUTE_VALUE
3113	MISSING_VERTEX_IDS
3120	INVALID_PARAMETER_VALUE
3121	INVALID_DATE_FORMAT
3122	REGEX_SYNTAX_ERROR
404 Élément introuvable	
4000	RESOURCE_NOT_FOUND
4001	APPLICATION_NOT_FOUND
4002	ATTRIBUTE_NOT_FOUND
4003	BUSINESS_SERVICE_NOT_FOUND
4004	BUSINESS_TRANSACTION_NOT_FOUND
4005	DECORATION_POLICY_NOT_FOUND
4006	GROUPING_NOT_FOUND
4007	VERTEX_NOT_FOUND
4008	SETTINGS_NOT_FOUND
4009	UNIVERSE_NOT_FOUND
409 Conflit	
5000	CONFLICT
5100	OUTDATED_RESOURCE
5101	OUTDATED_DECORATION_POLICY
5102	OUTDATED_GROUPING
5103	OUTDATED_SETTINGS
5104	UNEXPECTED_NODE_STATE
5105	FOLLOWERS_TOKEN_INVALID

ErrorCode	Type d'erreur
5106	FOLLOWER_UNREACHABLE
5107	MASTER_IS_UNREACHABLE
5200	LAST_RECORD_CANNOT_BE_DELETED
500 Erreur interne au serveur	
6 000	INTERNAL_SERVER_ERROR
415 Type de support non pris en charge	
7000	UNSUPPORTED_MEDIA_TYPE
503 Service non disponible	
8000	SERVICE_UNAVAILABLE
8001	ACC_SERVER_UNAVAILABLE

API REST de DX APM

Utilisez l'API REST de DX APM dans les scripts automatisés pour créer, mettre à jour et supprimer des attributs vertex. Les verbes et les paramètres de requête HTTP pris en charge sont répertoriés pour chaque service Web disponible.

NOTE

Informations complémentaires : [API hypermédia de DX APM](#)

DX APM prend en charge les services Web RESTful publics ci-après :

- [Règle d'attribut](#)
- [Graphique](#)
- [Graph Vertex](#)
- [Graph Incremental](#)
- [ID du sommet du graphique](#)
- [Graph Vertexstatus Incremental](#)
- [Ressource racine](#)
- [Univers](#)
- [Sommet](#)
- [ID du sommet](#)
- [Exemple de code Java d'API REST pour l'obtention de mises à jour incrémentielles](#)

Cette API inclut des **nouvelles** ressources qui n'étaient pas disponibles précédemment. Les ressources root, /vertex/ et /vertex/{id} d'origine sont prises en charge. Nous vous conseillons de migrer vers la nouvelle interface pour tirer le meilleur parti des nouvelles fonctionnalités.

Toutes les URL de ressource respectent les formats suivants :

- DX APM On Premise :
http://{hostname}:8081/{tenantId}/apm/atc/api/
- DX SaaS :
https://{hostname}/{tenantId}/apm/atc/api/

Le tableau suivant indique toutes les ressources d'API REST de DX APM disponibles ainsi que les verbes HTTP et les paramètres qu'elles prennent en charge.

Ressource	Description	Verbes HTTP	Paramètres	Autres
/tenantId/apm/atc/api/vertex (collection)	Représente une collection de vertex.	<ul style="list-style-type: none"> GET : Oui POST : Non PATCH : Oui PUT : Non DELETE : Non 	<ul style="list-style-type: none"> /vertex? projection=full : pour récupérer la projection complète /vertex? projection=compact : pour récupérer la projection compacte 	<ul style="list-style-type: none"> Convivialité d'ETC : Non Horodatage : Oui Filtrage : Oui
/tenantId/apm/atc/api/vertex/{id}	Représente un agent.	<ul style="list-style-type: none"> GET : Oui POST : Non PATCH : Oui PUT : Non DELETE : Non 	Non	<ul style="list-style-type: none"> Convivialité d'ETC : Non Horodatage : Oui Filtrage : Non
/tenantId/apm/atc/api/	Représente un agent.	<ul style="list-style-type: none"> GET : Oui POST : Non PATCH : Non PUT : Non DELETE : Non 	Non	<ul style="list-style-type: none"> Convivialité d'ETC : Oui Horodatage : Non Filtrage : Non
/tenantId/apm/atc/api/graph/vertex	Représente une collection de vertex	<ul style="list-style-type: none"> GET : Oui POST : Non PATCH : Oui PUT : Non DELETE : Non 	<ul style="list-style-type: none"> /vertex? timestamp=1970-01-01T00:00:01Z : récupère le cliché à une date spécifique. La date et l'heure actuelles sont utilisées par défaut. /vertex? projection=full : pour récupérer la projection complète /vertex? projection=compact : pour récupérer la projection compacte /vertex : la charge spécifie une requête. 	<ul style="list-style-type: none"> Convivialité d'ETC : Oui Horodatage : Oui Filtrage : Oui
/tenantId/apm/atc/api/graph/vertex/{id}	Représente un vertex unique	<ul style="list-style-type: none"> GET : Oui POST : Non PATCH : Oui PUT : Non DELETE : Non 	/vertex? timestamp=1970-01-01T00:00:01Z : récupère le cliché à une date spécifique. La date et l'heure actuelles sont utilisées par défaut.	<ul style="list-style-type: none"> Convivialité d'ETC : Oui Horodatage : Oui Filtrage : Non

Ressource	Description	Verbes HTTP	Paramètres	Autres
/tenantId/apm/atc/api/graph	Représente un graphique contenant des vertex et des arcs	<ul style="list-style-type: none"> GET : Oui POST : Non PATCH : Non PUT : Non DELETE : Non 	<ul style="list-style-type: none"> GET /tenantId/apm/atc/api/graph : renvoie les vertex, les statuts de vertex et les arcs pour la date et l'heure actuelles. Filtrage au format JSON, comme pour /graph/vertex /graph?timestamp=1970-01-01T00:00:01Z : récupère le cliché à une date spécifique. La date et l'heure actuelles sont utilisées par défaut. Renvoie une erreur pour une date future. 	<ul style="list-style-type: none"> Convivialité d'ETC : Oui Horodatage : Oui Filtrage : Oui
/tenantId/apm/atc/api/graph/incremental	Mises à jour des vertex et des arcs depuis le dernier appel	<ul style="list-style-type: none"> GET : Oui POST : Non PATCH : Non PUT : Non DELETE : Non 	<ul style="list-style-type: none"> GET /tenantId/apm/atc/api/graph/incremental?sinceVersion=0 : cet appel initial renvoie les vertex et les arcs pour la date et l'heure actuelles. La réponse inclut la propriété lastVersion permettant d'obtenir les mises à jour incrémentielles. GET /tenantId/apm/atc/api/graph/incremental?sinceVersion=XXXVersion4 : renvoie toutes les modifications incrémentielles apportées depuis la version XXXVersion4. La réponse contient des informations sur les vertex et arcs mis à jour et supprimés. 	<ul style="list-style-type: none"> Convivialité d'ETC : Oui Horodatage : Non Filtrage : Oui

Ressource	Description	Verbes HTTP	Paramètres	Autres
/{{tenantId}}/apm/atc/api/graph/vertexstatus/incremental	Cliché + mises à jour incrémentielles des statuts de vertex	<ul style="list-style-type: none"> GET : Oui POST : Non PATCH : Non PUT : Non DELETE : Non 	<ul style="list-style-type: none"> GET /{{tenantId}}/apm/atc/api/vertexstatus/incremental?sinceVersion=0 : cet appel initial renvoie tous les statuts à partir de la date et de l'heure actuelles. La réponse inclut la propriété lastVersion permettant d'obtenir les mises à jour incrémentielles. GET /{{tenantId}}/apm/atc/api/vertexstatus/incremental?sinceVersion=XXXVersion4 : renvoie toutes les modifications incrémentielles apportées depuis la version XXXVersion4. La réponse contient des informations sur les statuts mis à jour. 	<ul style="list-style-type: none"> Convivialité d'ETC : Oui Horodatage : Non Filtrage : Non
/{{tenantId}}/apm/atc/api/apmData/query	Sert d'interface d'interrogation réelle. Vous pouvez transmettre des requêtes SQL à l'aide des fonctionnalités renvoyées par la table de schéma.	<ul style="list-style-type: none"> GET : Non POST : Oui PATCH : Non PUT : Non DELETE : Non 	<ul style="list-style-type: none"> POST http://<EM Host>:8081/{{tenantId}}/apm/atc/api/apmData/query {"query" : "select agent_host, agent_process, agent_name, count(metric_path) from metrics where agent_name Like " group by agent_host, agent_process, agent_name"} : renvoie plusieurs mesures groupées par hôte d'agent. 	<ul style="list-style-type: none"> Convivialité d'ETC : Oui Horodatage : Oui Filtrage : Oui
/{{tenantId}}/apm/atc/api/apmData/schema	Décrit toutes les tables virtuelles connues que l'interface peut renvoyer.	<ul style="list-style-type: none"> GET : Oui POST : Non PATCH : Non PUT : Non DELETE : Non 	GET http://<hôte_EM>:8081/{{tenantId}}/apm/atc/api/apmData/schema : renvoie le schéma de base de données.	<ul style="list-style-type: none"> Convivialité d'ETC : Oui Horodatage : Oui Filtrage : Oui

Remarque : Les paramètres sont sensibles à la casse et doivent être saisis en minuscules.

Filtrage pris en charge dans la syntaxe Lucene

- Prise en charge du filtrage dans la syntaxe Lucene. Une description complète de la syntaxe est disponible à l'adresse : https://lucene.apache.org/core/4_7_0/queryparser/org/apache/lucene/queryparser/classic/package-summary.html

Authentification

Un jeton de sécurité est une chaîne de texte générée de manière aléatoire et dont la fonctionnalité est quasiment la même que celle d'un mot de passe. Il permet à l'API d'accéder au service Web de DX APM. Vous pouvez générer autant de jetons que nécessaire. Vous pouvez définir un délai d'expiration pour un jeton et révoquer un jeton. Les jetons peuvent être révoqués à tout moment et par n'importe quel utilisateur. Toutefois, ils sont permanents et ne disparaissent jamais de la liste sous l'onglet **Sécurité**.

Procédez comme suit :

1. Dans l'interface utilisateur, sélectionnez **Paramètres, Sécurité**.
2. Cliquez sur **Générer un nouveau jeton**.
3. Définissez l'expiration et ajoutez une étiquette.
4. Sélectionnez **API publique** comme **Type**.
5. Cliquez sur **Générer un jeton**.

WARNING

Pour des raisons de sécurité, il n'est pas possible d'afficher le même jeton plusieurs fois. Le jeton s'affiche uniquement après avoir cliqué sur **Nouveau jeton**.

6. [Utilisez le jeton dans l'en-tête de la demande d'autorisation.](#)

NOTE

Informations complémentaires :

- [Autorisation et authentification des API](#)
- [Messages et codes des erreurs générales liées à l'API](#)

Configuration

NOTE

La configuration de l'API REST de DX APM est disponible uniquement dans DX APM On-Premise.

API d'application

L'API d'application est documentée à l'aide de la version 3 d'OpenAPI. Le document OpenAPI peut être téléchargé à partir d'une installation d'APM. Il peut être utilisé pour générer des clients pour différentes langues ou avec des clients HTTP/REST interactifs.

Suivez la procédure mentionnée ci-dessous pour accéder au document OpenAPI 3 décrivant l'API publique APM Config Server pour l'intégration d'applications et l'utiliser pour générer un client Java typé à l'aide d'openapi-generator.

Procédez comme suit :

1. Téléchargez le document OpenAPI actuel.
 - a. Connectez-vous en tant qu'utilisateur autorisé à accéder à APM Config Server.
 - b. Ouvrez l'URL `https://<HOST>/acc/apm/acc/versioned.api.json` et téléchargez-le.

NOTE

Dans l'URL ci-dessus, remplacez <HOST> par le nom d'hôte/nom DNS approprié.

2. Créez un script pour télécharger et exécuter `openapi-generator`. Ce script est destiné au shell Bash, mais il peut être adapté pour fonctionner dans d'autres environnements. Placez-le dans un nouveau répertoire et donnez-lui un nom, par exemple `generate.sh`.

```
#!/bin/bash

if [ ! -f openapi-generator-cli*.jar ]; then
  wget https://repo1.maven.org/maven2/org/openapitools/openapi-generator-cli/7.1.0/openapi-generator-cli-7.1.0.jar
```



```

        final OnboardingConfigurationDto applicationTiersConfiguration =
applicationApi.getApplicationTiersConfiguration(true, false, null);
        final String versionHash = applicationTiersConfiguration.getVersionHash();

        ApplicationRestDto applicationRestDto = new ApplicationRestDto();
        applicationRestDto.setName("My application created through API test");
        applicationRestDto.setDescription("description");
        System.out.println("Creating the application.");
        ApplicationRestDto createdApplication = applicationApi.createApplication(null,
applicationRestDto);

        final TierRestDto tierRestDto = new TierRestDto();
        tierRestDto.setName("My DB tier");
        tierRestDto.setActive(true);
        tierRestDto.setDescription("DB tier");
        tierRestDto.setVersionHash(versionHash);
        // The tier's overrides field contains a user selection and needs to conform to current
configuration retrieved above.
        // In code below the overrides are set with assumption that configuration of the Postgres
// will not change incompatibly.
        final ArrayList<TierRestDtoOverridesInner> overrides = new ArrayList<>();
        final TierRestDtoOverridesInner override1 = new TierRestDtoOverridesInner();
        override1.setKey("operatingSystem");
        final ArrayList<TierUserChoiceItemDto> osValue = new ArrayList<>();
        final TierUserChoiceItemDto osValueItem = new TierUserChoiceItemDto();
        osValueItem.setItemId("osUnix");
        osValueItem.setOverrides(new TreeMap<>());
        osValue.add(osValueItem);
        override1.setValue(osValue);
        overrides.add(override1);
        final TierRestDtoOverridesInner override2 = new TierRestDtoOverridesInner();
        override2.setKey("options");
        final ArrayList<TierUserChoiceItemDto> optionsValue = new ArrayList<>();
        final TierUserChoiceItemDto optionsValueUseDecoration = new TierUserChoiceItemDto();
        optionsValueUseDecoration.setItemId("useDecoration");
        optionsValueUseDecoration.setOverrides(new TreeMap<>());
        optionsValue.add(optionsValueUseDecoration);
        final TierUserChoiceItemDto optionsValueUseOpenTracingJava = new TierUserChoiceItemDto();
        optionsValueUseOpenTracingJava.setItemId("useOpenTracingJava");
        final TreeMap<String, List<TierUserChoiceItemPropertyDto>> optionsValueUseOpenTracingJavaMap = new
TreeMap<>();
        final ArrayList<TierUserChoiceItemPropertyDto> optionsValueUseOpenTracingJavaMapValue = new
ArrayList<>();
        final TierUserChoiceItemPropertyDto openTracingJavaEnable = new TierUserChoiceItemPropertyDto();
        openTracingJavaEnable.setName("introscope.agent.opentracing.enable");
        openTracingJavaEnable.setValue("false");
        openTracingJavaEnable.setValueType(TierConfigurationItemPropertyValueTypes.BOOLEAN);
        optionsValueUseOpenTracingJavaMapValue.add(openTracingJavaEnable);
        optionsValueUseOpenTracingJavaMap.put("open-tracing-java",
optionsValueUseOpenTracingJavaMapValue);
        optionsValueUseOpenTracingJava.setOverrides(optionsValueUseOpenTracingJavaMap);
        optionsValue.add(optionsValueUseOpenTracingJava);
        final TierUserChoiceItemDto optionsValueHttpCollectorAgent = new TierUserChoiceItemDto();

```

```

optionsValueHttpCollectorIagent.setItemId("useHttpCollectorIagent");
optionsValueHttpCollectorIagent.setOverrides(new TreeMap<>());
optionsValue.add(optionsValueHttpCollectorIagent);
override2.setValue(optionsValue);
overrides.add(override2);
final TierRestDtoOverridesInner override3 = new TierRestDtoOverridesInner();
override3.setKey("database");
final ArrayList<TierUserChoiceItemDto> databaseValue = new ArrayList<>();
final TierUserChoiceItemDto databaseValuePostgres = new TierUserChoiceItemDto();
databaseValuePostgres.setItemId("postgresql");
final TreeMap<String, List<TierUserChoiceItemPropertyDto>> databaseValuePostgresMap = new
TreeMap<>();
final ArrayList<TierUserChoiceItemPropertyDto> databaseValuePostgresMapValue = new ArrayList<>();
final TierUserChoiceItemPropertyDto profiles = new TierUserChoiceItemPropertyDto();
profiles.setName("introscope.agent.dbmonitor.postgresql.profiles");
profiles.setValue("db1");
profiles.setSubPropertyRoot(true);
databaseValuePostgresMapValue.add(profiles);
final TierUserChoiceItemPropertyDto dbInstanceName = new TierUserChoiceItemPropertyDto();
dbInstanceName.setName("introscope.agent.dbmonitor.postgresql.profiles.db1.instanceName");
dbInstanceName.setValue("mydbname");
databaseValuePostgresMapValue.add(dbInstanceName);
final TierUserChoiceItemPropertyDto dbHostName = new TierUserChoiceItemPropertyDto();
dbHostName.setName("introscope.agent.dbmonitor.postgresql.profiles.db1.hostName");
dbHostName.setValue("myPostgresHostname");
databaseValuePostgresMapValue.add(dbHostName);
final TierUserChoiceItemPropertyDto dbPort = new TierUserChoiceItemPropertyDto();
dbPort.setName("introscope.agent.dbmonitor.postgresql.profiles.db1.port");
dbPort.setValue("5432");
dbPort.setValueType(TierConfigurationItemPropertyValueTypes.NUMBER);
databaseValuePostgresMapValue.add(dbPort);
final TierUserChoiceItemPropertyDto dbUserName = new TierUserChoiceItemPropertyDto();
dbUserName.setName("introscope.agent.dbmonitor.postgresql.profiles.db1.userName");
dbUserName.setValue("myPostgresUsername");
databaseValuePostgresMapValue.add(dbUserName);
final TierUserChoiceItemPropertyDto dbPassword = new TierUserChoiceItemPropertyDto();
dbPassword.setName("introscope.agent.dbmonitor.postgresql.profiles.db1.password");
dbPassword.setValue("myPostgresPassword");
dbPassword.setValueType(TierConfigurationItemPropertyValueTypes.PASSWORD);
databaseValuePostgresMapValue.add(dbPassword);
databaseValuePostgresMap.put("PostgreSQL", databaseValuePostgresMapValue);
databaseValuePostgres.setOverrides(databaseValuePostgresMap);
databaseValue.add(databaseValuePostgres);
override3.setValue(databaseValue);
overrides.add(override3);
tierRestDto.setOverrides(overrides);
System.out.println("Creating tier with postgres DB.");
final TierRestDto createdTier =
applicationApi.createApplicationTier(createdApplication.getEntityId(), null, tierRestDto);

final DraftChangeListDto draftChangeListDto = new DraftChangeListDto();
final DraftChangeDto itemsItem = new DraftChangeDto();
itemsItem.setId(createdTier.getEntityId());

```

```

        itemsItem.setType(DraftChangeItemType.TIER);
        draftChangeListDto.addItemItem(itemsItem);
        System.out.println("Publishing the application.");
        applicationApi.publishApplication(createdApplication.getEntityId(), draftChangeListDto);

        System.out.println("Creation is complete.");
    }
}

```

NOTE

Le programme Java utilisera le client généré pour créer une application, y ajouter un niveau qui décrit la configuration de l'agent Infrastructure pour Linux afin de surveiller une base de données PostgresDB.

5. Obtenez un jeton d'API dans l'interface utilisateur d'APM ATC. Accédez à **Paramètres > Sécurité > Générer un nouveau jeton**. Sélectionnez le type API publique.
6. Mettez à jour l'appel à la méthode `setBearerToken` avec un jeton valide dans la source de la classe `ClientTestTool`.
7. Compilez et exécutez la classe `ClientTestTool`.
 - a. Pour cela, vous pouvez utiliser n'importe quel IDE qui prend en charge Java et Maven.
 - b. Vous pouvez le faire via Java et Maven directement sur la ligne de commande.
 - a. Effectuez la compilation avec la commande `mvn clean install` dans le répertoire `spring-openapi-generator-api-client`.
 - b. Exécutez `mvn exec:exec -Dexec.executable=java -Dexec.args="-cp %classpath com.example.ClientTestTool"`.
8. Le résultat doit être une nouvelle application avec un niveau qui définit le moniteur d'infrastructure PostgresDB pour Linux.

NOTE

Si vous souhaitez utiliser le document OpenAPI pour générer un client avec un modèle typé avec d'autres langages/infrastructures cibles, assurez-vous que les propriétés d'objet JSON inconnues sont ignorées lors de la désérialisation et que le client envoie correctement les en-têtes Accept et Content-Type conformément au document OpenAPI pour assurer la compatibilité avec les futures versions d'APM.

Dépannage

Symptôme	Solution
Pour APM sur site, le client peut échouer avec une exception <code>javax.net.ssl.SSLHandshakeException</code> lorsqu'APM est configuré avec un certificat HTTPS auto-signé ou signé par une autorité de certification non publique.	Vous avez besoin d'un référentiel d'approbations avec un certificat correspondant à ce qui est utilisé sur le serveur pour connecter le client. Par exemple, un référentiel d'approbations nommé <code>trust.jks</code> (dans le répertoire <code>spring-openapi-generator-api-client</code>) sera utilisé : <pre> mvn exec:exec -Dexec.executable=java -Dexec.args="-cp %classpath -Djavax.net.ssl.trustStore=trust.jks -Djavax.net.ssl.trustStorePassword=changeit com.example.ClientTestTool" </pre>

Règle d'attribut

Directives relatives aux méthodes Post et Put - Utilisez les directives suivantes pour créer (POST) et mettre à jour (PUT) des règles d'attribut.

Les directives et les méthodes suivantes sont disponibles pour cette ressource :

- Directives relatives aux méthodes Post et Put
- Méthodes

Directives relatives aux méthodes Post et Put

Utilisez les directives suivantes pour créer (POST) et mettre à jour (PUT) des règles d'attribut.

Champs de charge utile

Les champs suivants sont obligatoires pour toutes les demandes de charge utile :

layer (couche)	existingName	customName	customValue	operator	operand
----------------	--------------	------------	-------------	----------	---------

Valeurs de champ

Operator

Les valeurs suivantes sont autorisées pour le champ `operator` :

Remarque : Les valeurs terminées par `_CI` ne sont pas sensibles à la casse.

EQUALS	EQUALS_CI	NOT_EQUALS	NOT_EQUALS_CI
STARTS_WITH	STARTS_WITH_CI	ENDS_WITH	ENDS_WITH_CI
CONTAINS	CONTAINS_CI	NOT_CONTAINS	NOT_CONTAINS_CI
IS_EMPTY	IS_NOT_EMPTY	REGEX	NOT_REGEX

Remarque : Si la valeur `operator` est égale à `IS_EMPTY` ou `IS_NOT_EMPTY` , la valeur `operand` doit être une chaîne vide :

```
"operator": "IS_NOT_EMPTY",
"operand": "",
```

Couche

Les valeurs suivantes sont autorisées pour le champ `layer` :

ATC	APM_INFRASTRUCTURE	INFRASTRUCTURE
-----	--------------------	----------------

UniverseId

Si vous fournissez une valeur nulle pour le champ `UniverseId` ou si vous ne spécifiez pas le champ `UniverseId` , la règle d'attribut est créée dans Enterprise Universe. Si la règle d'attribut existe déjà, elle sera transférée à Enterprise Universe.

Enabled

Si vous ne spécifiez pas le champ `enabled` , la valeur sera définie sur `false` par défaut. Cette valeur `false` permet de désactiver la visibilité de la règle d'attribut dans l'interface utilisateur graphique.

Id et _links

Les champs `Id` et `_links` sont en lecture seule. Si vous fournissez des valeurs pour ces champs, elles seront ignorées.

outputclass="bc-h2" id="Methods">Methods

Méthodes

GET /{tenantId}/apm/atc/api/attribute/rule

Cette méthode renvoie la liste des règles d'attribut pour tous les univers auxquels un utilisateur a accès.

```

{
  "_embedded": {
    "attributeRule": [
      {
        "existingName": "agent",
        "operator": "NOT_EQUALS",
        "operand": "sampleValue|Tomcat|Tomcat Agent",
        "customName": "sampleAttribute",
        "customValue": "sampleValue",
        "universeId": null,
        "layer": "ATC",
        "enabled": true,
        "_links": {
          "parent": {
            "href": "http://localhost/{tenantId}/apm/atc/api/attribute/rule"
          },
          "self": {
            "href": "http://localhost/{tenantId}/apm/atc/api/attribute/rule/DP165"
          }
        },
        "id": "DP165"
      },
      { ... },
      { ... }
    ]
  },
  "_links": {
    "self": {
      "href": "http://localhost/{tenantId}/apm/atc/api/attribute/rule"
    },
    "parent": {
      "href": "http://localhost/{tenantId}/apm/atc/api"
    }
  }
}

```

GET **{tenantId}/apm/atc/api/attribute/rule/{id}**

Cette méthode utilise un ID de règle d'attribut pour renvoyer une règle d'attribut unique.

```

{
  "existingName": "agent",
  "operator": "IS_EMPTY",
  "operand": "",
  "customName": "aaaa",
  "customValue": "aaaa",
  "universeId": "UNFWEnterprise Team Center",
  "layer": "APM_INFRASTRUCTURE",
  "enabled": true,
  "_links": {
    "parent": {
      "href": "http://localhost/{tenantId}/apm/atc/api/attribute/rule"
    },

```

```

"self": {
  "href": "http://localhost/{tenantId}/apm/atc/api/attribute/rule/DP235"
},
"id": "DP235"
}

```

POST /{tenantId}/apm/atc/api/attribute/rule

Cette méthode crée une règle d'attribut. Voici un exemple de la charge utile de la demande :

```

{
  "existingName": "agent",
  "operator": "IS_NOT_EMPTY",
  "operand": "",
  "customName": "aaaa",
  "customValue": "aaaa",
  "universeId": null,
  "layer": "APM_INFRASTRUCTURE",
  "enabled": false
}

```

Voici un exemple de réponse :

```

{
  "existingName": "agent",
  "operator": "IS_NOT_EMPTY",
  "operand": "",
  "customName": "aaaa",
  "customValue": "aaaa",
  "universeId": null,
  "layer": "APM_INFRASTRUCTURE",
  "enabled": false,
  "_links": {
    "parent": {
      "href": "http://localhost/{tenantId}/apm/atc/api/attribute/rule"
    },
    "self": {
      "href": "http://localhost/{tenantId}/apm/atc/api/attribute/rule/DP244"
    }
  },
  "id": "DP244"
}

```

PUT /{tenantId}/apm/atc/api/attribute/rule/{id}

Cette méthode utilise un ID de règle d'attribut pour mettre à jour la règle d'attribut qui correspond à l'ID fourni. Voici un exemple de la charge utile de la demande :

```

{
  "existingName": "agent",
  "operator": "CONTAINS",
  "operand": "name",
  "customName": "sample",
  "customValue": "2144",
}

```

```

"universeId":null,
"layer":"ATC",
"enabled":true
}

```

Voici un exemple de réponse :

```

{
  "existingName": "agent",
  "operator": "CONTAINS",
  "operand": "name",
  "customName": "sample",
  "customValue": "2144",
  "universeId": null,
  "layer": "ATC",
  "enabled": true,
  "_links": {
    "parent": {
      "href": "http://localhost/{tenantId}/apm/atc/api/attribute/rule"
    },
    "self": {
      "href": "http://localhost/{tenantId}/apm/atc/api/attribute/rule/DP170"
    }
  },
  "id": "DP170"
}

```

DELETE /{tenantId}/apm/atc/api/attribute/rule/{id}

Cette méthode utilise un ID de règle d'attribut pour supprimer la règle d'attribut qui correspond à l'ID fourni.

Graphique

Cette ressource renvoie un graphique complet comprenant les sommets, les statuts de sommet et les arêtes en fonction de l'horodatage et des critères de filtrage spécifiés. Vous pouvez utiliser vos propres scripts ou une bibliothèque de produits tiers pour analyser le graphique et extraire les informations dont vous avez besoin. Par exemple, les sommets en amont, les sommets en aval ou le chemin le plus court entre deux sommets.

- Joint les graphiques dans tous les univers auxquels vous avez accès.
- Si ETC sert plusieurs clusters, le terminal fusionne les sommets multicluster.
- Permet les requêtes d'historique à partir de l'horodatage. Les attributs, les alertes et les autres champs ont un historique. La date et l'heure actuelles sont utilisées par défaut.

Vous pouvez appeler ce terminal de deux façons :

1. Formule GET simple si vous n'avez pas besoin de filtre.
2. GET /{tenantId}/apm/atc/api/graph?timestamp=2016-01-01T00:00:01Z
3. L'option POST est utile si vous avez besoin d'un filtre. La condition de filtre est ensuite envoyée en tant que charge utile POST. Pour plus d'informations sur les filtres, consultez la section [Vertex de graphique](#).
4. POST /{tenantId}/apm/atc/api/graph/vertex?timestamp=2016-01-01T00:00:01ZContent-Type: application/json

```

{
  "includeStartPoint": false,
  "outputLayer": "ATC",
  "attributesToInclude": ["city"] ,
  "orItems": [
    {

```

```

        "andItems": [
            {
                "itemType" : "attributeFilter",
                "attributeName": "city",
                "attributeOperator": "IN",
                "values": [ null, "Paris", "London" ],
                "layer": "ATC"
            }
        ]
    }
}

{
  "_embedded": {
    "vertex": [
      {
        "timestamp": "2016-09-13T07:33:01.827Z",
        "attributes": {
          "name1": [ "value1" ],
          "name2": [ "value2" ],
          ...
        },
        "status": {
          "vertexStatus": "OK",
          "alerts": [
            {
              "alertName": "SuperDomain:NowhereBank:Engine - Average Response Time (ms)",
              "state": "OK"
            },
            {
              "alertName": "SuperDomain:Default:Frontend Stalls",
              "state": "OK"
            },
            {
              "alertName": "SuperDomain:NowhereBank:Engine - Errors Per Interval",
              "state": "OK"
            },
            {
              "alertName": "SuperDomain:Default:Response Time Variance Intensity",
              "state": "OK"
            },
            {
              "alertName": "SuperDomain:Default:Frontend Errors",
              "state": "OK"
            }
          ]
        },
        "_links": {
          "parent": {
            "href": "http://tas-cz-nc6.ca.com:8081/{tenantId}/apm/atc/api/graph"
          },
          "self": {
            "href": "http://tas-cz-nc6.ca.com:8081/{tenantId}/apm/atc/api/graph/vertex/Enterprise%20Team%20Center%3A8"
          }
        },
        "id": "Enterprise Team Center:8"
      }
    ]
  }
}

```



```
    },
    ...
  ],
  "edge": [
    {
      "sourceId": "Enterprise Team Center:9",
      "targetId": "Enterprise Team Center:8",
      "businessTransactionId": null
    },
    {
      "sourceId": "Enterprise Team Center:8",
      "targetId": "Enterprise Team Center:6",
      "businessTransactionId": null
    },
    ...
  ]
},
"_links": {
  "self": {
    "href": "http://tas-cz-nc6.ca.com:8081/{tenantId}/apm/atc/api/graph"
  },
  "parent": {
    "href": "http://tas-cz-nc6.ca.com:8081/{tenantId}/apm/atc/api"
  }
}}
```

Graph Vertex

Cette ressource renvoie la liste des sommets en fonction des critères de filtrage spécifiés et de la prévision.

- Permet les requêtes d'historique à partir de l'horodatage. Les attributs, les alertes et les autres champs ont un historique. La date et l'heure actuelles sont utilisées par défaut.
- Prend en charge les prévisions statiques compact et full. La valeur par défaut est compact.

Vous pouvez appeler ce terminal de deux façons :

1. Formule GET simple si vous n'utilisez pas de filtre.
GET `/{{tenantId}}/apm/atc/api/graph/vertex?timestamp=2016-01-01T00:00:01Z&projection=full`

2. L'option POST est utile si vous utilisez le filtre. La condition de filtre est ensuite envoyée en tant que charge utile POST.

POST `/{tenantId}/apm/atc/api/graph/vertex?timestamp=2016-01-01T00:00:01Z&projection=fullContent-Type: application/json`

```
{
  "includeStartPoint": false,
  "outputLayer": "ATC",
  "attributesToInclude": ["city"] ,
  "orItems": [
    {
      "andItems": [
        {
          "itemType" : "attributeFilter",
          "attributeName": "city",
          "attributeOperator": "IN",
          "values": [ null, "Paris", "London" ],
          "layer": "ATC"
        }
      ]
    }
  ]
}
```

Format de filtre et fonctionnalités

1. Opérations prises en charge : IN, NOT_IN, MATCHES, NOT_MATCHES
2. IN : correspondance exacte

```
// filter for vertices where attribute named "city" is undefined or equals to "Paris" or "London"
{
  "includeStartPoint": false,
  "orItems": [
    {
      "andItems": [
        {
          "itemType" : "attributeFilter",
          "attributeName": "city",
          "attributeOperator": "IN",
          "values": [ null, "Paris", "London" ] //null means undefined
        }
      ]
    }
  ]
}
```

NOT_IN : non égal.

```
// filter for vertices where attribute named "city" is not "Paris" or undefined
{
  "includeStartPoint": false,
  "orItems": [
    {
      "andItems": [
        {
          "itemType" : "attributeFilter",
          "attributeName": "city",

```

```

        "attributeOperator": "NOT_IN",
        "values": [ "Paris", null ] //null means undefined
    }
}
]
}
]
}

```

MATCHES : correspondance avec caractère générique *. Un astérisque (*) dans le modèle peut correspondre à la valeur zéro ou à plusieurs caractères.

```

// filter for vertices where attribute named "city" matches "P*s" wildcard.
{
    "includeStartPoint": false,
    "orItems":[
        {
            "andItems":[
                {
                    "itemType" : "attributeFilter",
                    "attributeName": "city",
                    "attributeOperator": "MATCHES",
                    "values": [ "P*s" ]
                }
            ]
        }
    ]
}

```

NOT_MATCHES : le caractère générique ne renvoie aucune correspondance.

```

// filter for vertices where attribute named "city" does not match "P*s" wildcard. The resultset will also
include vertices where "city" attribute is undefined.
{
    "includeStartPoint": false,
    "orItems":[
        {
            "andItems":[
                {
                    "itemType" : "attributeFilter",
                    "attributeName": "city",
                    "attributeOperator": "MATCHES",
                    "values": [ "P*s" ]
                }
            ]
        }
    ]
}

// To exclude vertices where "city" attribute is undefined add corresponding condition to the filter
{
    "includeStartPoint": false,
    "orItems":[
        {
            "andItems":[

```

```

        {
            "itemType" : "attributeFilter",
            "attributeName": "city",
            "attributeOperator": "MATCHES",
            "values": [ "P*s" ]
        },
        {
            "itemType" : "attributeFilter",
            "attributeName": "city",
            "attributeOperator": "NOT_IN",
            "values": [ null ]
        }
    ]
}
]
}

```

Le filtre peut combiner plusieurs conditions de filtrage :

```

{
    "includeStartPoint": false, //true if Include request start point
    "orItems":[
        {
            "andItems":[
                {
                    "itemType" : "attributeFilter", //can be "attributeFilter" or "btCoverage"
                    "attributeName": "Attr1",
                    "attributeOperator": "IN",
                    "values": ["value1","value2", null]
                },
                {
                    "itemType" : "btCoverage",
                    "andItemsForBtCoverage": [
                        {
                            "attributeName": "Attr2",
                            "attributeOperator": "IN",
                            "values": ["value1","value2"]
                        }
                    ]
                }
            ],
        },
        {
            "itemType" : "attributeFilter",
            "attributeName": "Name",
            "attributeOperator": "NOT_IN",
            "values": ["value1"]
        }
    ]
},
{
    "andItems":[
        {
            "itemType" : "btCoverage",
            "andItemsForBtCoverage": [

```

```

        {
            "attributeName": "Attr2",
            "attributeOperator": "MATCHES",
            "values": ["val*", "us*active"]
        }
    ],
},
{
    "itemType" : "btCoverage",
    "andItemsForBtCoverage": [
        {
            "attributeName": "Business Service",
            "attributeOperator": "IN",
            "values": ["value1"]
        },
        {
            "attributeName": "Hostname",
            "attributeOperator": "IN",
            "values": ["value1", "value2"]
        }
    ]
}
],
},
]
}

```

Le filtre attributeName prend en charge

- Les noms d'attribut de sommet valides. Par exemple, agent ou hostname.
- serviceld : pour filtrer par service d'entreprise, tel qu'il apparaît dans l'interface utilisateur
- transactionId : pour filtrer par transaction métier, telle qu'elle apparaît dans l'interface utilisateur

Prévisions

Compact (par défaut)

```

?{
  "_embedded": {
    "vertex": [
      {
        "timestamp": "2016-05-12T08:10:55.738Z",
        "attributes": {
          "agent": ["turyu01-win04|NowhereBank|Mediator"],
          "hostname": ["turyu01-win04"],
          "Source cluster": ["Enterprise Team Center"],
          "name": ["Backends|Queue|requestValidation"],
          "agentDomain": ["SuperDomain"],
          "Attr1": ["newValue"],
          "Attr2": ["newValue2"],
          "processedBy": ["BackendVertexIdentifier"],
          "type": ["GENERICBACKEND"],
          "applicationname": ["Mediator"]
        }
      },

```

```

    "_links": {
      "parent": {
        "href": "http://localhost:8081/{tenantId}/apm/atc/api/graph/vertex"
      },
      "self": {
        "href": "http://localhost:8081/{tenantId}/apm/atc/api/graph/vertex/Enterprise%20Team%20Center%3A8"
      }
    },
    "id": "Enterprise Team Center:8"
  },
  {...},
  {...}
]
},
"_links": {
  "self": {
    "href": "http://localhost:8081/{tenantId}/apm/atc/api/graph/vertex"
  },
  "parent": {
    "href": "http://localhost:8081/{tenantId}/apm/atc/api"
  }
}
}

```

Full

```

?{
  "_embedded": {
    "vertex": [
      {
        "timestamp": "2016-05-12T08:15:42.683Z",
        "attributes": [
          {
            "name": "agentDomain",
            "value": "SuperDomain",
            "type": "GATHERED"
          },
          {
            "name": "Attr2",
            "value": "newValue2",
            "type": "CUSTOM"
          },
          {
            "name": "Attr2",
            "value": "newValue3",
            "type": "DECORATED"
          }
        ],
        "_links": {
          "parent": {
            "href": "http://localhost:8081/{tenantId}/apm/atc/api/graph/vertex"
          },
          "self": {

```

```

        "href": "http://localhost:8081/{tenantId}/apm/atc/api/graph/vertex/Enterprise%20Team%20Center%3A8"
    },
    "id": "Enterprise Team Center:8"
},
{...},
{...}
]
},
"_links": {
  "self": {
    "href": "http://localhost:8081/{tenantId}/apm/atc/api/graph/vertex"
  },
  "parent": {
    "href": "http://localhost:8081/{tenantId}/apm/atc/api"
  }
}
}

```

Patch

Met à jour les valeurs d'attribut pour un sommet particulier.

- Les noms d'attribut doivent être uniques. Les attributs dupliqués sont ignorés.
- La valeur Null supprime l'attribut.
- Si un attribut existe pour un sommet donné, il est mis à jour. Dans le cas contraire, la fonction PATCH crée un attribut personnalisé.
- Les attributs personnalisés peuvent être créés, mis à jour ou supprimés. Si la fonction PATCH crée un attribut, il est toujours personnalisé.
- Les attributs personnalisés créés par des règles d'attribut peuvent être mis à jour.
- Les attributs de base ne peuvent pas être mis à jour ou supprimés.

Exemple de charge utile de demande :

```

?{ "items" : [
  {
    "id": "Enterprise Team Center:8",
    "attributes": {
      "Attr1": ["newValue", "newValue2"],
      "Attr2": null
    }
  },
  {...},
  {...}
]
}

```

Graph Incremental

Renvoie les mises à jour incrémentielles de la structure du graphique. Chaque réponse contient la propriété **lastVersion** à utiliser pour l'appel suivant.

- Joint les graphiques dans tous les univers auxquels vous avez accès.
- La réponse ne contient pas toutes les mises à jour. S'il existe plusieurs mises à jour du même vertex/arc, seule la dernière mise à jour en vigueur est signalée.
- Dans une installation multicluster, procédez à la corrélation intercluster côté consommateur (voir exemple).

GET `/{{tenantId}}/apm/atc/api/graph/incremental?sinceVersion=0`

Ce premier appel renvoie les vertex et les arcs à compter du jour en cours. La réponse inclut la propriété **lastVersion** permettant d'obtenir les mises à jour incrémentielles. Mettez les résultats en cache côté consommateur sous forme de cliché initial.

```
{
  "_embedded": {
    "vertex": [ //all vertices as of right now
      {
        "id": "Enterprise Team Center:8",
        "externalId": "ApplicationService:Mediator"?
        "startTime":"2015-04-12T09:59:12.221Z" ,
        "attributes": {
          "name1": ["value1"],
          "name2": ["value2"],
          "name3": ["value3"]
        },
        "_links": {
          "self": {
            "href": "http://tas-cz-nc6.ca.com:8081/{{tenantId}}/apm/atc/api/graph/vertex/Enterprise%20Team%20Center%3A8"
          }
        }
      },
      ...
    ],
    "removedVertex": [ ], //empty for initial snapshot
    "edge": [
      {
        "sourceId": "Enterprise Team Center:9",
        "targetId": "Enterprise Team Center:10",
        "businessTransactionId": "Enterprise Team Center:1",
        "startTime":"2015-04-12T09:59:12.221Z"
      },
      {
        "sourceId": "Enterprise Team Center:15",
        "targetId": "Enterprise Team Center:16",
        "businessTransactionId": "Enterprise Team Center:1",
        "startTime":"2015-04-12T09:59:12.221Z"
      },
      {...}
    ],
    "removedEdge": [], //empty for initial snapshot
  },
  "_links": {
    "self": {
      "href": "http://tas-cz-nc6.ca.com:8081/{{tenantId}}/apm/atc/api/graph/incremental"
    },
  },
}
```

GET /{tenantId}/apm/atc/api/graph/incremental?sinceVersion=XXXXXXXXXXZZZZZ

Renvoie les modifications incrémentielles depuis le dernier appel. Le dernier appel est identifié par le champ **lastVersion** dans la réponse.

La réponse contient des informations sur les vertex et les arcs nouveaux, modifiés et supprimés. Appliquez la réponse au cliqué. Maintenez la mise en cache côté consommateur. Voir exemple ci-dessous :

518

[illegible]

ID du sommet du graphique

Représente un sommet unique identifié par un ID

```
{
  "timestamp": "2016-05-12T08:27:06.851Z",
  "attributes": [
    {
      "name": "agentDomain",
      "value": "SuperDomain",
      "type": "GATHERED"
    },
    {
      "name": "Attr1",
```

```

    "value": "newValue3",
    "type": "CUSTOM"
  },
  {
    "name": "Attr2",
    "value": "newValue3",
    "type": "DECORATED"
  }
],
"_links": {
  "parent": {
    "href": "http://localhost:8081/{tenantId}/apm/atc/api/graph/vertex"
  },
  "self": {
    "href": "http://localhost:8081/{tenantId}/apm/atc/api/graph/vertex/Enterprise%20Team%20Center%3A8"
  }
},
"id": "Enterprise Team Center:8"
}

```

Patch

Met à jour les valeurs d'attribut pour un sommet particulier.

- Les noms d'attribut doivent être uniques. Les attributs dupliqués sont ignorés.
- La valeur Null supprime l'attribut.
- Si un attribut existe pour un sommet donné, il est mis à jour. Dans le cas contraire, la fonction PATCH crée un attribut personnalisé.
- Les attributs personnalisés peuvent être créés, mis à jour ou supprimés. Si la fonction PATCH crée un attribut, il est toujours personnalisé.
- Les attributs personnalisés créés par des règles d'attribut peuvent être mis à jour.
- Les attributs de base ne peuvent pas être mis à jour ou supprimés.

Exemple de charge utile de demande :

```

{
  "attributes": {
    "Attr1": ["newValue3", "newVal3"],
    "Attr2": null
  }
}

```

Graph Vertexstatus Incremental

Renvoie les mises à jour incrémentielles des statuts vertex. Chaque réponse contient la propriété **lastVersion** à utiliser pour l'appel suivant.

- Joint les statuts vertex dans tous les univers auxquels l'utilisateur a accès
- La réponse ne contient pas toutes les mises à jour. S'il existe plusieurs mises à jour du même statut, seule la dernière mise à jour en vigueur est signalée.

GET /{tenantId}/apm/atc/api/graph/vertexstatus/incremental?sinceVersion=0

```
?{
  "_embedded": {
    "status": {
      "alerts": [
        {
          "vertexId": "Enterprise Team Center:8",
          "alertName": "custom alert #8",
          "state": "OK",
          "startTime": "2015-04-12T09:59:12.221Z"
        },
        {
          "vertexId": "Enterprise Team Center:8",
          "alertName": "custom alert #1",
          "state": "DANGER",
          "startTime": "2015-04-12T09:59:12.221Z"
        },
        {...}
      ]
    }
  },
  "_links": {
    "self": {
      "href": "http://tas-cz-nc6.ca.com:8081/{tenantId}/apm/atc/api/graph/vertexstatus/incremental"
    },
    "parent": {
      "href": "http://tas-cz-nc6.ca.com:8081/{tenantId}/apm/atc/api"
    },
    "next": {
      "href": "http://tas-cz-nc6.ca.com:8081/{tenantId}/apm/atc/api/graph/vertexstatus/incremental?
sinceVersion=eyJ0eXB1IjoiVkVSVEVYU1RBVFTTIiwidmVyc2lvdnMiOnsidGFzLWN6LW51ZC5jYS5jb206ODA4MSI6MTQ3Mzc1NDMzMDQ1MSwidGFzLW
"
    },
    "lastVersion":
      "eyJ0eXB1IjoiVkVSVEVYU1RBVFTTIiwidmVyc2lvdnMiOnsidGFzLWN6LW51ZC5jYS5jb206ODA4MSI6MTQ3Mzc1NDMzMDQ1MSwidGFzLWN6LW5jMC5jY
means reset the cache
  }
}
```

Renvoie les modifications incrémentielles depuis le dernier appel. Le dernier appel est identifié par le champ **lastVersion** dans la réponse.

La réponse contient des informations sur les vertex et les arcs nouveaux, modifiés et supprimés. Appliquez cette réponse au cliché. Maintenez la mise en cache côté consommateur. Voir exemple ci-dessous :

521

NOTE

- Répétez les appels pour obtenir les mises à jour incrémentielles aussi souvent que nécessaire. Chaque fois que vous réalisez un appel, toutes les modifications sont implémentées sans fixation ni pagination. Les charges utiles extra volumineuses sont gérées avec un fichier JSON de réponse de diffusion en continu plutôt que d'être conservées en mémoire.
- Vous pouvez, à tout moment, obtenir un cliché actualisé des données. Utilisez **GET /{tenantId}/apm/atc/api/graph/incremental?sinceVersion=0**. Par exemple, cet appel peut être utilisé si votre application est redémarrée. Il offre une nouvelle propriété lastVersion permettant d'obtenir les mises à jour incrémentielles.

Renvoie la liste des options disponibles pour l'API accompagnées d'informations générales la concernant. La ressource est publiquement accessible via SSL et aucun jeton d'autorisation n'est requis. La ressource racine sert de point de départ pour explorer l'API, en associant tous les chemins disponibles qui sont accessibles. Le lien vers une ressource peut être un modèle d'URI. Dans ce cas, la ressource contient une propriété `templated:true`. Si la propriété n'est pas présente ou que sa valeur est différent, la ressource contient une URI simple.

Exemple de réponse :

```

{
  "serviceProvider": "com.ca.apm.appmap",
  "serverVersion": "Release 10.1.0.0 (Build 28)",
  "apiVersion": "1.0.0",
  "vendor": "Broadcom",
  "_links": {
    "self": {
      "href": "https://test.ca.com:8443/{tenantId}/apm/atc/api"
    },
    "doc": {
      "href": "https://wiki.ca.com/display/APMDEVOPS101/APM+REST+API"
    },
    "vertex": [
      {
        "href": "https://test.ca.com:8443/{tenantId}/apm/atc/api/vertex{?timestamp,q,projection}",
        "templated": true
      },
      {
        "href": "https://test.ca.com:8443/{tenantId}/apm/atc/api/vertex/{id}{?timestamp}",
        "templated": true
      }
    ]
  }
}

```

Propriétés de la ressource :

Nom de propriété	Type	Description	API Version
serviceProvider	Chaîne	Décrit le fournisseur du service : com.ca.apm.appmap	1.0.0
serverVersion	Chaîne	Version du serveur fournissant l'API (version APM)	1.0.0
apiVersion	Chaîne	Version de l'API	1.0.0
vendor	Chaîne	Fournisseur du service : Broadcom	1.0.0
_links	Tableau	Répertorie toutes les options disponibles pour cette API.	1.0.0
_links.self	Lien HAL	Contient l'URL vers la ressource racine même	1.0.0
_links.doc	Lien HAL	Contient l'URL vers la documentation de l'API publique	1.0.0
_links.* Par exemple : vertex	Lien HAL	Affiche tous les terminaux disponibles pour une ressource donnée.	1.0.0

Univers

Cette ressource renvoie des propriétés de base pour des univers particuliers ou pour tous les univers auxquels un utilisateur a accès.

Cette ressource renvoie des propriétés de base pour des univers particuliers ou pour tous les univers auxquels un utilisateur a accès.

Vous pouvez appeler ce terminal de deux façons :

- **GET /{ID_client_hébergé}/apm/atc/api/universe**

Renvoie la liste des univers auxquels un utilisateur a accès.

```
{
  "_embedded": {
    "universe": [
      {
        "name": "TestUniverse",
        "_links": {
          "parent": {
            "href": "http://localhost/{tenantId}/apm/atc/api/universe"
          },
          "self": {
            "href": "http://localhost/{tenantId}/apm/atc/api/universe/UN172"
          }
        },
        "id": "UN172"
      },
      {
        "name": "sampleValue components",
        "_links": {
          "parent": {
            "href": "http://localhost/{tenantId}/apm/atc/api/universe"
          },
          "self": {
            "href": "http://localhost/{tenantId}/apm/atc/api/universe/UNFWEnterprise%20Team%20Center"
          }
        },
        "id": "UNFWEnterprise Team Center"
      }
    ]
  },
  "_links": {
    "self": {
      "href": "http://localhost/{tenantId}/apm/atc/api/universe"
    },
    "parent": {
      "href": "http://localhost/{tenantId}/apm/atc/api"
    }
  }
}
```

- **GET /{ID_client_hébergé}/apm/atc/api/universe/{ID}**

Renvoie les propriétés de l'univers dont l'ID est fourni.

```
{
  "name": "TestUniverse",
  "_links": {
    "parent": {
      "href": "http://localhost/{tenantId}/apm/atc/api/universe"
    },
    "self": {
      "href": "http://localhost/{tenantId}/apm/atc/api/universe/UN172"
    }
  }
}
```



```

    },
    "id": "UN172"
  }
}

```

Sommet

Renvoie la liste des sommets en fonction des critères de filtrage spécifiés et de la prévision.

- Permet les requêtes d'historique à partir de l'horodatage. Les attributs, les alertes et les autres champs ont un historique. La date et l'heure actuelles sont utilisées par défaut.
- Prend en charge les prévisions statiques compact et full. La valeur par défaut est compact.

Verbes pris en charge : GET, PATCH

Paramètres pris en charge : projection, timestamp, q

GET

Filtrage de collecte pris en charge

Par horodatage pour récupérer un cliché de la collection à la date et heure de l'horodatage. La date et l'heure actuelles sont utilisées par défaut.

- GET /{tenantId}/apm/atc/api/vertex?timestamp:1970-01-01T00:00:01Z
- Prise en charge du filtrage dans la syntaxe Lucene. Une description complète de la syntaxe est disponible à l'adresse : https://lucene.apache.org/core/4_7_0/queryparser/org/apache/lucene/queryparser/classic/package-summary.html

Exemples de filtrage :

- GET /{tenantId}/apm/atc/api/vertex?q=city:Paris AND sky:blue : vous pouvez combiner des expressions de filtrage à l'aide d'opérateurs logiques
- GET /{tenantId}/apm/atc/api/vertex?q=(city:Paris AND sky:blue) OR (city:London AND sky:grey) : groupement des expressions logiques à l'aide d'accolades
- GET /{tenantId}/apm/atc/api/vertex?q=sky\ color:deep\ : les espaces et autres caractères spéciaux doivent être échappés.

/vertex/ prend en charge les prévisions full et compact. La valeur par défaut est compact.

Full

```

?{
  "_links": {
    "self": { "href": "http://localhost:8081/{tenantId}/apm/atc/api/vertex"},
    "parent": { "href": "http://localhost:8081/{tenantId}/apm/atc/api"}
  },
  "_embedded": {
    "vertex": [
      {
        "id": "497",
        "timestamp": "2015-05-14T09:59:12.221Z",
        "attributes": [
          {
            "name": "applicationName",
            "value": "AuthenticationService",
            "type": "GATHERED"
          },
          {
            "name": "type",

```

```

        "value": "SERVLET",
        "type": "GATHERED"
    },
    {
        "name": "servletClassName",
        "value": "DefaultServlet",
        "type": "GATHERED"
    },
    {
        "name": "city",
        "value": "Paris",
        "type": "CUSTOM"
    }
],
"_links": {
    "parent": { "href": "http://localhost:8081/{tenantId}/apm/atc/api/vertex" },
    "self": { "href": "http://localhost:8081/{tenantId}/apm/atc/api/vertex/497" }
},
{
    "id": "480",
    "timestamp": "2015-05-14T09:59:12.221Z",
    "attributes": [
        {
            "name": "name",
            "value": "Place Order",
            "type": "GATHERED"
        },
        {
            "name": "type",
            "value": "BUSINESSTRANSACTION",
            "type": "GATHERED"
        },
        {
            "name": "serviceId",
            "value": "Trading Service",
            "type": "GATHERED"
        },
        {
            "name": "city",
            "value": "Paris",
            "type": "CUSTOM"
        }
    ],
    "_links": {
        "parent": { "href": "http://localhost:8081/{tenantId}/apm/atc/api/vertex" },
        "self": { "href": "http://localhost:8081/{tenantId}/apm/atc/api/vertex/480" }
    }
}
]
}
}

```

Compact

```
? {
  "_links": {
    "self": {"href": "http://localhost:8081/{tenantId}/apm/atc/api/vertex"},
    "parent": {"href": "http://localhost:8081/{tenantId}/apm/atc/api"}
  },
  "_embedded": {
    "vertex": [
      {
        "id": "516",
        "timestamp": "2015-05-14T10:43:10.163Z",
        "attributes": {
          "name": "WebService|Auth",
          "applicationName": "AuthenticationEngine",
          "hostname": "webserver.ca.com",
          "type": "SERVLET",
          "agent": "tas-cz-n8d|Tomcat|Tomcat Agent",
          "servletClassName": "DefaultServlet",
          "ipAddress": "10.0.0.1"
        },
        "_links": {
          "parent": {"href": "http://localhost:8081/{tenantId}/apm/atc/api/vertex"},
          "self": {"href": "http://localhost:8081/{tenantId}/apm/atc/api/vertex/516"}
        }
      }
    ]
  }
}
```

PATCH

Met à jour les valeurs d'attribut pour un sommet particulier.

- Les noms d'attribut doivent être uniques. Les attributs dupliqués sont ignorés.
- Si un attribut existe pour un sommet donné, il est mis à jour. Dans le cas contraire, la fonction PATCH crée un attribut personnalisé avec un nom donné.
- Les attributs personnalisés peuvent être créés, mis à jour ou supprimés. Les attributs créés par la fonction PATCH sont toujours personnalisés.
- Les attributs décorés peuvent être mis à jour. Si vous les mettez à jour, ils deviennent des attributs personnalisés.
- Les attributs collectés ne peuvent pas être mis à jour ni supprimés.

Exemple de charge utile de demande :

- Les noms d'attribut fournis doivent être uniques. La fonction PATCH ignore les attributs dupliqués.

```
[{
  "id": "3",
  "attributes": {
    "Attr1": "newValue",
    "Attr2": null // NULL deletes attribute
  }
},
...]
```

Paramètres pris en charge

Nom de propriété	Type	Description
vertex	tableau	tableau des sommets : varie en fonction de la prévision.

ID du sommet

La ressource renvoie des informations détaillées pour un sommet unique.

La structure de retour est la même que dans GET /vertex :

Verbes pris en charge : tous

Paramètres pris en charge : id, timestamp, attributes

GET

```
{
  "id": "497",
  "timestamp": "2015-05-14T09:59:12.221Z",
  "attributes": [
    {
      "name": "applicationName",
      "value": "AuthenticationService",
      "type": "GATHERED"
    },
    {
      "name": "type",
      "value": "SERVLET",
      "type": "GATHERED"
    },
    {
      "name": "servletClassName",
      "value": "DefaultServlet",
      "type": "GATHERED"
    }
  ],
  "_links": {
    "parent": { "href": "<xref href='http://localhost:8081/{tenantId}/apm/atc/api/vertex'
scope='external'>http://localhost:8081/{tenantId}/apm/atc/api/vertex</xref> ",
    "self": { "href": "<xref href='http://localhost:8081/{tenantId}/apm/atc/api/vertex/497'
scope='external'>http://localhost:8081/{tenantId}/apm/atc/api/vertex/497</xref>"
  }
}
```

Paramètres HTTP supplémentaires

- timestamp : récupère un cliché de la ressource à la date et heure de l'horodatage. La date et l'heure actuelles sont utilisées par défaut. GET /{tenantId}/apm/atc/api/vertex/123?timestamp=1970-01-01T00:00:01Z

PATCH

Met à jour les valeurs d'attribut pour un sommet particulier.

- Les noms d'attribut doivent être uniques. Les attributs dupliqués sont ignorés.
- Si un attribut existe pour un sommet donné, il est mis à jour. Dans le cas contraire, la fonction PATCH crée un attribut personnalisé avec un nom donné.
- Les attributs personnalisés peuvent être créés, mis à jour ou supprimés. Les attributs créés par la fonction PATCH sont toujours personnalisés.
- Les attributs décorés peuvent être mis à jour. Si vous les mettez à jour, ils deviennent des attributs personnalisés.
- Les attributs collectés ne peuvent pas être mis à jour ni supprimés.

Exemple de charge utile de demande :

- Les noms d'attribut fournis doivent être uniques. La fonction PATCH ignore les attributs dupliqués.

```
{
  "attributes": {
    "Attr1": "newValue",
    "Attr2": null // NULL deletes attribute
  }
}
```

Paramètres pris en charge

Nom de propriété	Type	Description
ID (identification)	Tableau d'une chaîne unique	ID du sommet
Horodatage	Horodatage	<i>Horodatage du cliché servi au format 1970-01-01T00:00:01Z</i>
attributes	Tableau	Liste de tous les attributs définis sur le sommet
attributes.name	Chaîne	Nom de l'attribut
attributes.value	Chaîne	Valeur de l'attribut
attributes.type	Chaîne	Type d'attribut. Les types actuellement pris en charge sont CUSTOM, DECORATED et GATHERED.

Exemple de code Java d'API REST pour l'obtention de mises à jour incrémentielles

L'exemple suivant présente l'utilisation de l'API REST publique pour obtenir des mises à jour incrémentielles.

```
package com.mycompany.app;
import java.net.URI;
import org.apache.http.HttpEntity;
import org.apache.http.HttpHost;
import org.apache.http.HttpResponse;
import org.apache.http.client.methods.HttpGet;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;
import org.apache.http.util.EntityUtils;
import com.fasterxml.jackson.databind.JsonNode;
import com.fasterxml.jackson.databind.ObjectMapper;
public class IncrementalExample {
    public static void main(String[] args) throws Exception {
        final CloseableHttpClient httpClient = HttpClients.createDefault();
```

```

// specify the host, protocol, and port
HttpHost target = new HttpHost("test.ca.com", 8081, "http");
String lastVersionForGraph = "0";
String lastVersionForVertexStatus = "0";
final GraphCache gc = new GraphCache();
for (;;) {
    try {
        final HttpGet request = new HttpGet();
        request.addHeader("Content-Type", "application/json");
        request.addHeader("Authorization", "Bearer f47ac10b-58cc-4372-a567-0e02b2c3d479");
        request.addHeader("Accept", "application/hal+json");
        if ("0".equals(lastVersionForGraph) || "0".equals(lastVersionForVertexStatus)) {
            lastVersionForGraph = "0";
            lastVersionForVertexStatus = "0";
            // reset cache, REST has decided to send you full snapshot
            gc.clear();
        }

        // query graph updates
        request.setURI(URI.create("/{tenantId}/apm/atc/api/graph/incremental?sinceVersion="
            + lastVersionForGraph));
        // execute the request
        final HttpResponse httpResponse = httpClient.execute(target, request);
        if (httpResponse.getStatusLine().getStatusCode() != 200) {
            throw new IllegalStateException("Error polling graph changes == "
                + httpResponse.getStatusLine());
        }
        final HttpEntity entity = httpResponse.getEntity();
        final String result = EntityUtils.toString(entity);
        // parse the results
        final ObjectMapper mapper = new ObjectMapper();
        final JsonNode tree = mapper.readTree(result);
        lastVersionForGraph = tree.get("lastVersion").asText();
        final long newVertices = tree.get("_embedded").get("vertex").size();
        final long removedVertices = tree.get("_embedded").get("removedVertex").size();
        final long newEdges = tree.get("_embedded").get("edge").size();
        final long removedEdges = tree.get("_embedded").get("removedEdge").size();
        System.out.println("polled graph changes == [" + newVertices + ", " + newEdges
            + ", " + removedVertices + ", " + removedEdges + "]");
        // apply changes to cache
        gc.applyGraphChanges(tree);
    }

    // query vertex status updates
    request.setURI(URI
        .create("/{tenantId}/apm/atc/api/graph/vertexstatus/incremental?sinceVersion="
            + lastVersionForVertexStatus));
    // execute the request
    final HttpResponse httpResponse = httpClient.execute(target, request);
    if (httpResponse.getStatusLine().getStatusCode() != 200) {
        throw new IllegalStateException("Error polling vertex status changes == "
            + httpResponse.getStatusLine());
    }
}

```

```

        final HttpEntity entity = httpResponse.getEntity();
        final String result = EntityUtils.toString(entity);
        // parse the results
        final ObjectMapper mapper = new ObjectMapper();
        final JsonNode tree = mapper.readTree(result);
        lastVersionForVertexStatus = tree.get("lastVersion").asText();
        final long changes = tree.get("_embedded").get("status").get("alerts").size();
        System.out.println("polled vertex status changes == " + changes);
        // apply changes to cache
        gc.applyVertexStatusChanges(tree);
    }
    final GraphCache.Graph g = gc.getGraphForUI();
} catch (java.net.ConnectException | IllegalStateException e) {
    e.printStackTrace();
    System.out.println("Will try to reretrieve complete graph at next call");
    lastVersionForGraph = "0";
    lastVersionForVertexStatus = "0";
} catch (Throwable t) {
    System.out.println("Unknown error : " + t);
    t.printStackTrace();
    break;
}
if (!"0".equals(lastVersionForGraph)) {
    Thread.sleep(10000);
}
}
httpClient.close();
}

?
package com.mycompany.app;
import java.util.ArrayList;
import java.util.Collection;
import java.util.HashMap;
import java.util.HashSet;
import java.util.Iterator;
import java.util.List;
import java.util.Locale;
import java.util.Map;
import java.util.Set;
import java.util.Map.Entry;
import com.fasterxml.jackson.databind.JsonNode;
import com.google.common.collect.ArrayListMultimap;
import com.google.common.collect.Multimap;
/**
 * Example of simple cache holder which applies changes in the order they arrive, with no regard to
 * the timestamp of the change.
 * Keeps only latest snapshot, not the historical data
 * Includes all vertices and edges with no filtering them by type
 */
public class GraphCache {
    private Map<String, Vertex> vertices = new HashMap<String, Vertex>();

```

```

private List<Edge> edges = new ArrayList<Edge>();
private final static String CCC_VERTEX_IDENTIFICATION = "CCC.VertexIdentification"
    .toLowerCase(Locale.US);
/**
 * resets the cache
 */
public void clear() {
    vertices.clear();
    edges.clear();
}
/**
 * parses output from GET /graph/incremental and applies it
 */
public void applyGraphChanges(JsonNode jsonTree) throws Exception {
    // added and changed vertices
    for (final JsonNode json : jsonTree.get("_embedded").get("vertex")) {
        // parse Vertex
        final Vertex v = new Vertex();
        v.setVertexId(json.get("id").asText());
        v.setExternalId(json.get("externalId").asText());
        final Iterator<Entry<String, JsonNode>> attributes = json.get("attributes").fields();
        while (attributes.hasNext()) {
            final Map.Entry<String, JsonNode> entry = attributes.next();
            final Iterator<JsonNode> values = entry.getValue().elements();
            while (values.hasNext()) {
                final JsonNode attrValue = values.next();
                v.getAttributes().put(entry.getKey(), attrValue.asText());
            }
        }
        // update graph
        vertices.put(v.getVertexId(), v);
        System.out.println("Added new vertex : '" + v + "'");
    }
    // removed vertices
    for (final JsonNode json : jsonTree.get("_embedded").get("removedVertex")) {
        // parse Vertex
        final String vertexId = json.get("id").asText();
        // update graph
        if (vertices.containsKey(vertexId)) {
            vertices.remove(vertexId);
        } else {
            System.out.println("Ignored delete for missing vertex " + json);
        }
    }
    // added and changed edges
    for (final JsonNode json : jsonTree.get("_embedded").get("edge")) {
        // parse Edge
        final Edge e = new Edge();
        e.setSourceId(json.get("sourceId").asText());
        e.setTargetId(json.get("targetId").asText());
        e.setBusinessTransactionId(json.get("businessTransactionId").asText());
        // update graph
        edges.add(e);
    }
}

```



```

        System.out.println("Added new edge : " + e);
    }
    // removed edges
    for (final JsonNode json : jsonTree.get("_embedded").get("removedEdge")) {
        // parse Edge
        final String sourceId = json.get("sourceId").asText();
        final String targetId = json.get("targetId").asText();
        final String businessTransactionId = json.get("businessTransactionId").asText();
        // update graph
        boolean wasRemoved = false;
        final Iterator<Edge> it = edges.iterator();
        while (it.hasNext()) {
            final Edge e = it.next();
            if (!e.getSourceId().equals(sourceId)) {
                continue;
            }
            if (!e.getTargetId().equals(targetId)) {
                continue;
            }
            boolean btEquals =
                (businessTransactionId == null
                 ? e.getBusinessTransactionId() == null
                 : businessTransactionId.equals(e.getBusinessTransactionId()));
            if (btEquals) {
                it.remove();
                wasRemoved = true;
            }
        }
        if (!wasRemoved) {
            System.out.println("Ignored delete for missing edge " + json);
        }
    }
}
/**
 * parses output from GET /graph/vertexstatus/incremental and applies it
 */
public void applyVertexStatusChanges(JsonNode jsonTree) throws Exception {
    // parse alert updates
    for (final JsonNode json : jsonTree.get("_embedded").get("status").get("alerts")) {
        // parse Edge
        final String vertexId = json.get("vertexId").asText();
        final String alertName = json.get("alertName").asText();
        final String state = json.get("state").asText();
        // update graph
        final Vertex v = vertices.get(vertexId);
        if (v != null) {
            v.getAlerts().put(alertName, state);
            System.out.println("set alert state for vertex '" + vertexId + "' : " + alertName
                               + " --> " + state);
        } else {
            System.out.println("Ignored alert for missing vertex '" + vertexId + "'");
        }
    }
}

```

```

}
/**
 * returns current snapshot with vertices correlated by externalId
 */
public Graph getGraphForUI() throws Exception {
    System.out.println("before CCC : total vertices : " + vertices.size() + " , total edges : "
        + edges.size());
    final Graph ret = new Graph();
    ret.getEdges().addAll(edges);
    ret.getVertices().putAll(vertices);
    correlateByExternalId(ret);
    System.out.println("after CCC : total vertices : " + ret.getVertices().size()
        + " , total edges : " + ret.getEdges().size());
    return ret;
}

private static void correlateByExternalId(Graph mergeGraph) {
    Multimap<String, Vertex> verticesByExternalID = ArrayListMultimap.create();
    Map<String, Vertex> removedVertices = new HashMap<String, Vertex>();
    // map vertices by external_id
    for (Vertex v : mergeGraph.getVertices().values()) {
        String externalId = v.getExternalId();
        if (externalId == null) {
            continue;
        }
        verticesByExternalID.put(externalId, v);
    }
    // create CC vertices by merging original vertices by external_id
    for (Map.Entry<String, Collection<Vertex>> entry : verticesByExternalID.asMap().entrySet()) {
        Collection<Vertex> v2 = entry.getValue();
        if (v2.size() < 2) {
            continue;
        }
        // We have CC vertex. Let's create merged one
        String externalId = entry.getKey();
        Vertex ccVertex = mergeVertices(externalId, v2);
        mergeGraph.getVertices().put(ccVertex.getVertexId(), ccVertex);
        // Collect source vertices to be removed as they are replaced by a CC vertex
        for (Vertex toRemove : v2) {
            removedVertices.put(toRemove.getVertexId(), toRemove);
        }
    }
    // Let's fixup edges
    List<Edge> ccEdges = new ArrayList<Edge>();
    Iterator<Edge> it = mergeGraph.getEdges().iterator();
    for (; it.hasNext();) {
        Edge e = it.next();
        Vertex source = removedVertices.get(e.getSourceId());
        Vertex target = removedVertices.get(e.getTargetId());
        Vertex bt = removedVertices.get(e.getBusinessTransactionId());
        source = source == null ? null : mergeGraph.getVertices().get(source.getExternalId());
        target = target == null ? null : mergeGraph.getVertices().get(target.getExternalId());
        bt = bt == null ? null : mergeGraph.getVertices().get(bt.getExternalId());
        if (source != null || target != null || bt != null) {

```

```

        // Cross cluster edge detected
        Edge ccEdge = createCrossClusterEdge(e, source, target, bt);
        ccEdges.add(ccEdge);
        it.remove();
    }
}
mergeGraph.getEdges().addAll(ccEdges);
// Remove source vertices replaced by CC vertices
for (String vertexIdToRemove : removedVertices.keySet()) {
    mergeGraph.getVertices().remove(vertexIdToRemove);
}
// check for CCC "stub" vertices and remove them, remove the corresponding edges as well
Set<String> stubVertexIds = new HashSet<String>();
for (Vertex v : mergeGraph.getVertices().values()) {
    if (v.getAttributes().containsKey(CCC_VERTEX_IDENTIFICATION)) {
        stubVertexIds.add(v.getVertexId());
    }
}
for (String stubVertexId : stubVertexIds) {
    mergeGraph.getVertices().remove(stubVertexId);
    mergeGraph.getEdges().removeIf(
        e -> e.getSourceId().equals(stubVertexId) || e.getTargetId().equals(stubVertexId));
}
}

private static Vertex mergeVertices(String externalId, Collection<Vertex> vertices) {
    if (vertices.size() < 2) {
        throw new IllegalArgumentException("vertices size is expected to be at least 2");
    }
    final Vertex ret = new Vertex();
    ret.setVertexId(externalId);
    for (Vertex v : vertices) {
        ret.getAlerts().putAll(v.getAlerts());
        // we want to suppress CCC vertex attributes completely
        if (!v.getAttributes().containsKey(CCC_VERTEX_IDENTIFICATION)) {
            ret.getAttributes().putAll(v.getAttributes());
        }
    }
    return ret;
}

private static Edge createCrossClusterEdge(Edge edge, Vertex source, Vertex target, Vertex bt) {
    final Edge ret = new Edge();
    ret.setSourceId(source != null ? source.getVertexId() : edge.getSourceId());
    ret.setTargetId(target != null ? target.getVertexId() : edge.getTargetId());
    ret.setBusinessTransactionId(bt != null ? bt.getVertexId() : edge
        .getBusinessTransactionId());
    return ret;
}

/**
 * Vertices and Edges for UI
 */
public static class Graph {
    private Map<String, Vertex> vertices = new HashMap<String, Vertex>();
    private List<Edge> edges = new ArrayList<Edge>();

```

```

    public Map<String, Vertex> getVertices() {
        return vertices;
    }
    public List<Edge> getEdges() {
        return edges;
    }
}
/**
 * single vertex
 */
public static class Vertex {
    private String vertexId;
    private String externalId;
    private Multimap<String, String> attributes = ArrayListMultimap.create();
    private Map<String, String> alerts = new HashMap<>();
    public void setVertexId(String vertexId) {
        this.vertexId = vertexId;
    }
    public String getVertexId() {
        return this.vertexId;
    }
    public void setExternalId(String externalId) {
        this.externalId = externalId;
    }
    public String getExternalId() {
        return this.externalId;
    }
    public Multimap<String, String> getAttributes() {
        return attributes;
    }
    public Map<String, String> getAlerts() {
        return alerts;
    }
    @Override
    public String toString() {
        StringBuilder sb = new StringBuilder();
        sb.append("Vertex [vertexId=");
        sb.append(vertexId);
        sb.append(", externalId=");
        sb.append(externalId);
        sb.append(", attributes=");
        sb.append(attributes);
        sb.append(", alerts=");
        sb.append(alerts);
        sb.append("]");
        return sb.toString();
    }
}
/**
 * single edge
 */
public static class Edge {
    private String sourceId;

```

```

    private String targetId;
    private String businessTransactionId;
    public void setSourceId(String sourceId) {
        this.sourceId = sourceId;
    }
    public String getSourceId() {
        return sourceId;
    }
    public void setTargetId(String targetId) {
        this.targetId = targetId;
    }
    public String getTargetId() {
        return targetId;
    }
    public void setBusinessTransactionId(String businessTransactionId) {
        this.businessTransactionId = businessTransactionId;
    }
    public String getBusinessTransactionId() {
        return businessTransactionId;
    }
    @Override
    public String toString() {
        StringBuilder builder = new StringBuilder();
        builder.append("Edge [sourceId=");
        builder.append(sourceId);
        builder.append(", targetId=");
        builder.append(targetId);
        builder.append(", businessTransactionId=");
        builder.append(businessTransactionId);
        builder.append("]");
        return builder.toString();
    }
}

```

API REST SQL

L'API REST SQL publique permet d'extraire des données de mesures brutes de CA APM et de les intégrer avec des outils personnalisés. Comme d'autres API REST APM, l'interface de l'API REST SQL utilise un système d'authentification basée sur des jetons. Cette API REST s'exécute dans les modes de gestionnaire d'entreprise (Enterprise Manager, EM) suivants :

- Autonome
- Collecteur
- Gestionnaire des gestionnaires (Manager of Managers, MOM)
- Enterprise Team Center

NOTE

- La fonction d'API REST SQL a été introduite dans le Service Pack 1 (SP1) 10.7.
- Cette fonctionnalité ne fournit pas toutes les fonctions SQL telles que les jointures et les sous-sélections.

IMPORTANT

Utilisez l'API REST SQL publique *uniquement* pour extraire les données de mesure d'APM. Pour extraire les données de mesure APM ou non APM, utilisez l'[API REST de requête de mesure](#).

Connexion à l'API REST SQL

Procédez comme suit :

1. Connectez-vous à Team Center et cliquez sur **Sécurité**.
2. Cliquez sur **Générer un nouveau jeton**.
Une boîte de dialogue s'affiche.
3. Entrez l'**étiquette** (nom) et sélectionnez **API publique** pour l'option **Type**.
4. Définissez la date d'expiration ou sélectionnez **N'expire jamais**.
5. Cliquez sur **Générer un jeton**.
Le système génère un nouveau jeton.

WARNING

Pour des raisons de sécurité, vous ne voyez un jeton qu'une seule fois. Enregistrez le jeton à un emplacement sûr avant de fermer cette boîte de dialogue. Ne communiquez le jeton à aucune personne non autorisée.

Le jeton figure maintenant parmi les autres jetons dans l'onglet **Sécurité**.

6. Testez la connexion avec une requête quelconque, par exemple :

```
URL
    http://<EM Host>:8081/{tenantId}/apm/atc/api/apmData/schema

GET

Header
    Accept: application/json
    Authorization: Bearer <Security Token>
```

Vous êtes maintenant connecté à l'API REST.

Mesures de capacité de prise en charge

Le nom des mesures de capacité de prise en charge de l'API REST SQL contient le préfixe `Enterprise Manager | Data Store | SQL API`. Le tableau suivant répertorie les mesures de capacité de prise en charge disponibles :

Nom de la mesure de capacité de prise en charge	Description
Temps de réponse moyen (ms)	Temps moyen nécessaire pour traiter la requête entrante
Octets envoyés par intervalle	Nombre d'octets envoyés en conséquence au cours d'un intervalle
Réponses par intervalle	Requêtes réussies au cours d'un intervalle
Appels simultanés	Nombre de connexions parallèles à un terminal de requête
Connexions limitées par intervalle	Nombre de connexions rejetées en raison de la limite de clamps
Erreurs par intervalle	Nombre de requêtes ayant échoué au cours d'un intervalle

Ressources de l'API REST

L'API REST SQL contient les ressources suivantes :

```
/ {tenantId} /apm/atc/api/apmData/schema
```

Décrit toutes les tables virtuelles connues que l'interface peut renvoyer.

`/ {tenantId} /apm/atc/api/apmData/query`

Sert d'interface d'interrogation réelle. Vous pouvez transmettre des requêtes SQL à l'aide des fonctionnalités renvoyées par la table de schéma.

Vous pouvez définir des requêtes à l'aide des fonctions count, minimum, maximum et average. Les fonctions d'agrégation suivantes sont uniquement prises en charge dans la colonne `agg_value` de la table `metric_data` : `sum`, `apm_average` et `apm_aggregate`. Les fonctions d'agrégation produisent les résultats suivants :

- La fonction d'agrégation `sum` fournit la somme des valeurs de la colonne `agg_values`.
- La fonction `apm_aggregate` fournit la somme ou la moyenne pondérée en fonction des mesures interrogées.
- La fonction `apm_average` fournit uniquement la moyenne pondérée.

Exemples de requête

Utilisez les exemples suivants pour interroger l'API :

- Exemple 1 : **obtention du nombre de mesures groupées par hôte d'agent**

Cet exemple utilise une demande POST sur la ressource `/ {tenantId} /apm/atc/api/apmData/query`.

```
URL
    http://<EM Host>:8081/{tenantId}/apm/atc/api/apmData/queryVerb
POST
Header
    Accept: application/json
    Content-Type: application/json
    Authorization: Bearer <Security Token>Data
    { "query" : "select agent_host, agent_process, agent_name, count(metric_path) from metrics where
agent_name Like ' ' group by agent_host, agent_process, agent_name" }
```

Exemple 2 : obtention d'un schéma

Cet exemple utilise une demande GET sur la ressource `/ {tenantId} /apm/atc/api/apmData/schema`.

```
{
  "tables": [
    {
      "name": "metric_data",
      "columns": [
        {
          "name": "source_name",
          "type": "string",
          "whereCapabilities": [
            "=",
            "<",
            ">",
            "<=",
            ">=",
            "<>",
            "!=",
            "BETWEEN",
            "LIKE",
            "LIKE_REGEX"
          ]
        }
      ]
    }
  ],
}
```

```
{
  "name": "agent_host",
  "type": "string",
  "whereCapabilities": [
    "=",
    "<",
    ">",
    "<=",
    ">=",
    "<>",
    "!=",
    "BETWEEN",
    "LIKE",
    "LIKE_REGEX"
  ]
},
{
  "name": "agent_process",
  "type": "string",
  "whereCapabilities": [
    "=",
    "<",
    ">",
    "<=",
    ">=",
    "<>",
    "!=",
    "BETWEEN",
    "LIKE",
    "LIKE_REGEX"
  ]
},
{
  "name": "agent_name",
  "type": "string",
  "whereCapabilities": [
    "=",
    "<",
    ">",
    "<=",
    ">=",
    "<>",
    "!=",
    "BETWEEN",
    "LIKE",
    "LIKE_REGEX"
  ]
},
{
  "name": "domain_name",
  "type": "string",
  "whereCapabilities": [
    "=",
```



```

        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "metric_path",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "metric_attribute",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "attribute_type",
    "type": "long",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",

```

```

        "!=" ,
        "BETWEEN"
    ]
},
{
    "name": "frequency",
    "type": "long",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=" ,
        "BETWEEN"
    ]
},
{
    "name": "ts",
    "type": "timestamp",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=" ,
        "BETWEEN"
    ]
},
{
    "name": "min_value",
    "type": "long",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=" ,
        "BETWEEN"
    ]
},
{
    "name": "max_value",
    "type": "long",
    "whereCapabilities": [
        "=",
        "<",
        ">",

```

```

        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN"
    ]
},
{
    "name": "value_count",
    "type": "long",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN"
    ]
},
{
    "name": "agg_value",
    "type": "long",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN"
    ]
}
]
},
{
    "name": "metrics",
    "columns": [
        {
            "name": "source_name",
            "type": "string",
            "whereCapabilities": [
                "=",
                "<",
                ">",
                "<=",
                ">=",
                "<>",
                "!=",
                "BETWEEN",
                "LIKE",
            ]
        }
    ]
}

```

```

        "LIKE_REGEX"
    ]
},
{
    "name": "agent_host",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "agent_process",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "agent_name",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "domain_name",

```

```

        "type": "string",
        "whereCapabilities": [
            "=",
            "<",
            ">",
            "<=",
            ">=",
            "<>",
            "!=",
            "BETWEEN",
            "LIKE",
            "LIKE_REGEX"
        ]
    },
    {
        "name": "metric_path",
        "type": "string",
        "whereCapabilities": [
            "=",
            "<",
            ">",
            "<=",
            ">=",
            "<>",
            "!=",
            "BETWEEN",
            "LIKE",
            "LIKE_REGEX"
        ]
    },
    {
        "name": "metric_attribute",
        "type": "string",
        "whereCapabilities": [
            "=",
            "<",
            ">",
            "<=",
            ">=",
            "<>",
            "!=",
            "BETWEEN",
            "LIKE",
            "LIKE_REGEX"
        ]
    },
    {
        "name": "attribute_type",
        "type": "long",
        "whereCapabilities": [
            "=",
            "<",
            ">",

```

```

        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN"
    ]
},
{
    "name": "first_seen",
    "type": "timestamp",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN"
    ]
},
{
    "name": "last_seen",
    "type": "timestamp",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN"
    ]
}
]
},
{
    "name": "sources",
    "columns": [
        {
            "name": "source_name",
            "type": "string",
            "whereCapabilities": [
                "=",
                "<",
                ">",
                "<=",
                ">=",
                "<>",
                "!=",
                "BETWEEN",
                "LIKE",
            ]
        }
    ]
}

```

```

        "LIKE_REGEX"
    ]
},
{
    "name": "status",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "type",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
}
]
}
]]

```

- **Exemple 3 : obtention des données de mesures avec une clause where**

Cet exemple utilise une demande POST sur la ressource `{tenantId}/apm/atc/api/apmData/query`.

```

{
    "query" : "select <Columns> from metric_data <Where Clause>"
}

```

Résultat :

```

{
    "columns" : [

```

```
{
  "name" : "metric",
  "type" : "string"
},
{
  "name" : "AVG(value)",
  "type" : "double"
}
],
"rows" : [
  [ "host|process|agent|Average Response Time(ms)", 1025.69 ],

  [ "host|process|agent|CPU:Utilization %(process)", 12.25 ]

]]
```

- **Exemple 4 : obtention des données de mesures à l'aide d'une fonction d'agrégation**

Cet exemple utilise une demande POST sur la ressource `{tenantId}/apm/atc/api/apmData/query`.

```
{
  "query": "select sum(agg_value),apm_aggregate(agg_value),apm_average(agg_value) from metric_data where
agent_host='ibndev001382' and domain_name like '%Super%' metric_attribute like '%Average System CPU Time
(ms)%' and ts > 1587473084000"
}
```

Résultat :

```
{
  "columns": [
    {
      "name": "sum(agg_value)",
      "type": "long"
    },
    {
      "name": "apm_aggregate(agg_value)",
      "type": "long"
    },
    {
      "name": "apm_average(agg_value)",
      "type": "long"
    }
  ],
  "rows": [
    [
      149616118,
      149616118,
      443949
    ]
  ]
}
```


Exemples de requête d'URL

Utilisez les exemples suivants pour interroger l'API dans cURL :

- **Exemple 1 : obtention d'un schéma**

```
curl -Lk -H "Authorization: Bearer $TOKEN" -H "Accept: application/json" -H "Content-Type: application/json" \
http://$EM_HOST:8081/{tenantId}/apm/atc/api/apmData/schema
```

- **Exemple 2 : obtention d'un schéma lisible par l'Homme sans fonctionnalités where**

```
curl -Lk -H "Authorization: Bearer $TOKEN" -H "Accept: application/json" -H "Content-Type: application/json" \
http://$EM_HOST:8081/{tenantId}/apm/atc/api/apmData/schema | sed
's/,"whereCapabilities":[[[^\]] *[]] //g' | python -mjson.tool
```

- **Exemple 3 : obtention de toutes les sources**

```
curl -Lk -H "Authorization: Bearer $TOKEN" -H "Accept: application/json" -H "Content-Type: application/json" \
http://$EM_HOST:8081/{tenantId}/apm/atc/api/apmData/query -d '{ "query" : "select *
from sources;" }'
```

Résultat :

```
{ "columns": [ { "name": "source_name", "type": "string" }, { "name": "status", "type": "string" },
{ "name": "type", "type": "string" } ],
"rows": [ [ "<>:8081", "connected", "agc" ],
[ "EM Host 1@5001", "connected", "collector" ],
[ "EM Host 2:8081", "connected", "standalone" ],
[ "EM Host 3:8081", "connected", "mom" ],
[ "EM Host 4:8081", "connected", "standalone" ],
[ "EM Host 5@5001", "connected", "collector" ],
[ "EM Host 6@5001", "connected", "collector" ]
] }
```

- **Exemple 4 : obtention de toutes les mesures pour les agents comportant des caractères spécifiques dans la colonne agent_process**

```
curl -Lk -H "Authorization: Bearer $TOKEN" -H "Accept: application/json" -H "Content-Type: application/json" \
http://$EM_HOST:8081/{tenantId}/apm/atc/api/apmData/query -d "{ \"query\" : \"select
* from metrics where agent_process LIKE '%Nowhere%'\" }"
```

Résultat :

```
{ "columns": [ { "name": "source_name", "type": "string" },
{ "name": "agent_host", "type": "string" }, { "name": "agent_process", "type": "string" },
{ "name": "agent_name", "type": "string" }, { "name": "domain_name", "type":
"string" }, { "name": "metric_path", "type": "string" },
{ "name": "metric_attribute", "type": "string" }, { "name": "attribute_type", "type": "long" },
{ "name": "first_seen", "type": "timestamp" }, { "name": "last_seen", "type": "timestamp" } ]
, "rows": [ [ "Collector Host 1@5001", "Agent Host 1", "Nowhere
Bank", "Engine", "SuperDomain", "Launch Time", "Launch
Time", 2066, 1521511260000, 1521565710000 ]
, [ "Collector Host 2:8081", "Agent Host 2", "Nowhere
Bank", "Mediator", "SuperDomain", "Launch Time", "Launch
Time", 2066, 1521511515000, 1521565710000 ]
, [ "Collector Host 3@5001", "Agent Host 3", "Nowhere
Bank", "Mediator", "SuperDomain", "Launch Time", "Launch
Time", 2066, 1521511560000, 1521565710000 ]
, [ "Collector Host 4@5001", "Agent Host 4", "Nowhere
Bank", "Engine", "SuperDomain", "CPU:Processor Count", "Processor
Count", 17, 1521511260000, 1521565710000 ]
, [ "Collector Host 5:8081", "Agent Host 5", "Nowhere
Bank", "Mediator", "SuperDomain", "CPU:Processor Count", "Processor
Count", 17, 1521511515000, 1521565710000 ]
, [ "Collector Host 6@5001", "Agent Host 6", "Nowhere
Bank", "Portal", "SuperDomain", "Launch Time", "Launch
Time", 2066, 1521511500000, 1521565710000 ]
, [ "Collector Host 7@5001", "Agent Host 7", "Nowhere
Bank", "Engine", "SuperDomain", "CPU:Utilization % (process)", "Utilization %
(process)", 4097, 1521511260000, 1521565710000 ]
, ... ] }
```

- **Exemple 5 : obtention du nombre de mesures groupées par agents**

```
curl -Lk -H "Authorization: Bearer $TOKEN" -H "Accept: application/json" -H "Content-Type: application/json" \
http://$EM_HOST:8081/{tenantId}/apm/atc/api/apmData/query \
-d "{ \"query\" : \"select agent_host, agent_process, agent_name, count(metric_path)
from metrics group by agent_host, agent_process, agent_name \" }"
```

Résultat :

```
{ "columns": [{"name": "agent_host", "type": "string"},
{"name": "agent_process", "type": "string"}, {"name": "agent_name", "type": "string"},
{"name": "count(metric_path)", "type": "long"}]

, "rows": [{"usilca31", "Cross-Enterprise APM Process", "Cross-Enterprise APM Agent
HEY", 4768]

, ["EM Host 1", "CTG Client 2", "CICSTestDriver", 119]

, ["Custom Metric Host (Virtual)", "Custom Metric Process (Virtual)", "Custom Metric
Agent (Virtual) (Custom Host 1@5001)", 1008]

, ["EM Host 2", "Nowhere Bank", "Portal", 302]

, ["Custom Metric Host (Virtual)", "Custom Metric Process (Virtual)", "Custom Metric
Agent (Virtual)", 7234]

, ["Custom Metric Host (Virtual)", "Custom Metric Process (Virtual)", "Custom Metric
Agent (Virtual) (Custom Host 2@5001)", 1131]

, ["Custom Metric Host (Virtual)", "Custom Metric Process (Virtual)", "Custom Business
Application Agent (Virtual) (Custom Host 3@5001)", 76]

, ["EM Host 3", "Infrastructure", "Agent", 231]

, ["EM Host 4", "Collector", "Agent", 80]

, ["EM Host 5", "Tomcat", "Tomcat Agent", 360]

, ["EM Host 6", "Collector", "Agent", 344]

, ["EM Host 7", "Nowhere Bank", "Mediator", 269]

, ["EM Host 8", "Nowhere Bank", "Portal", 302]

, ["EM Host 9", "Agent", "UnnamedAgent", 12]

, ["Custom Metric Host (Virtual)", "Custom Metric Process (Virtual)", "Custom Metric
Agent (Virtual) (Custom Host 4@5001)", 1186]
```

```
,["EM Host 10","Nowhere Bank","Engine",283]
,["EM Host 11","WebSphere","WebSphere Agent",601]
,["Custom Metric Host (Virtual)","Custom Metric Process (Virtual)","Custom Business
Application Agent (Virtual)",873]
,["EM Host 12","Nowhere Bank","Engine",283]
,["EM Host 13","Tomcat","Tomcat Agent",806]
,["EM Host 14","CTG Client 1","CICSTestDriver",119]
,["Custom Metric Host (Virtual)","Custom Metric Process (Virtual)","Custom Business
Application Agent (Virtual) (Custom Host 5@5001)",242]
,["EM Host 15","Tomcat-MathApp-BA-PO","Tomcat-MathApp-BA-PO",1489]
,["EM Host 16","DxC Agent","Logstash-APM-Plugin",306]
,["EM Host 17","Nowhere Bank","Engine",283]
,["EM Host 18","Nowhere Bank","Mediator",261]
,["EM Host 19","CEM","Default Application",107]
,["tradeservice-app","Tomcat","CA APM Demo Agent - Tomcat",763]
,["EM Host 20","Nowhere Bank","Portal",302]
,["EM Host 21","Nowhere Bank","Mediator",269]
,["Custom Metric Host (Virtual)","Custom Metric Process (Virtual)","Custom Business
Application Agent (Virtual) (Custom Host 6@5001)",76]
]}
}
```

- **Exemple 6 : obtention de toutes les données de mesures au cours de la dernière heure**

NOTE

Cette requête renvoie un très grand fichier JSON. Elle doit donc être exécutée avec précaution.

```
ONE_HOUR_AGO=`echo $(date "+%s")*1000 " - 60*60*1000" | bc `; curl -Lk -H
  "Authorization: Bearer $TOKEN" \
-H "Accept: application/json" -H "Content-Type: application/json" http://<EM
Host>:8081/{tenantId}/apm/atc/api/apmData/query \
-d "{ \"query\" : \"select * from metric_data where ts >= ${ONE_HOUR_AGO}\" }"
```

- **Exemple 7 : obtention de la valeur maximale, regroupée par chemin de mesure, à partir des données de mesures pour toutes les mesures moyennes (ms)**

```
curl -Lk -H "Authorization: Bearer $TOKEN" -H "Accept: application/json" -H "Content-Type: application/json" \
http://$EM_HOST:8081/{tenantId}/apm/atc/api/apmData/query \
-d "{ \"query\" : \"select metric_path, max(agg_value) from metric_data where metric_attribute LIKE 'Average%(ms)' group by metric_path \" }"
```

Résultat :

```
{ "columns": [{"name": "metric_path", "type": "string"}, {"name": "max(agg_value)", "type": "long"}],
"rows": [{"Business Segment|tas-cz-n148/9091|/brtmtestapp/spa/|#/green|Resources|AJAX Call|Async|tas-cz-n148/9091|/brtmtestapp/sample.txt:Average Callback Execution Time (ms)", 4}, {"Backends|WebService at http_//localhost_8080:Average Response Time (ms)", 4856}, {"By Frontend|CICSTestDriver_RunUOW|Backend Calls|System localhost on port 2006:Average Response Time (ms)", 0}, {"Frontends|Apps|TradeService|URLs|/TradeService/PlaceOrder|Called Backends|System localhost on port 3456:Average Response Time (ms)", 105}, {"Backends|WebService at PipeOrganWebService_2:Average Response Time (ms)", 128}, {"Frontends|Apps|ReportingService|URLs|Default|Called Backends|WebServices:Average Response Time (ms)", 177}, {"Enterprise Manager|Internal|Messaging|PostOffices|Server.WatchedAgentPO|Messages|com.wily.isengard.messageprimitives.service.MessageServiceCallMessage:Average Process Time (ms)", 73}, {"Enterprise Manager|Internal|Messaging|PostOffices|Server.main|Messages|com.wily.isengard.messageprimitives.service.MessageServiceCallMessage|com.wily.introscope.spec.server.beans.transactiontrace.ITransactionTraceService:Average Process Time (ms)", 40}, {"By Business Service|tas-cz-n148/9091|/brtmtestapp/HTTP304.html_AJAXCalls|Browser:Average Response Time (ms)", 18}]
```

- **Exemple 8 : obtention de l'utilisation moyenne de l'UC pour les agents**

```
curl -Lk -H "Authorization: Bearer $TOKEN" -H "Accept: application/json" -H "Content-Type: application/json" http://$EM_HOST:8081/{tenantId}/apm/atc/api/apmData/query \
```

```
-d "{ \"query\" : \"select agent_host, agent_process, avg(agg_value) from metric_data
where metric_path like '%CPU:Utilization%' group by agent_host, agent_process\" }"
```

Résultat :

```
{ "columns": [{"name": "agent_host", "type": "string"},
{"name": "agent_process", "type": "string"}, {"name": "avg(agg_value)", "type": "long"}]
, "rows": [{"Collector Host 1", "CTG Client 2", 4}
, ["Collector Host 2", "WebSphere", 8]
, ["Collector Host 3", "Nowhere Bank", 3]
, ["Collector Host 4", "Tomcat", 3]
, ["Collector Host 5", "Nowhere Bank", 2]
, ["Collector Host 6", "Nowhere Bank", 1]
, ["Collector Host 7", "CTG Client 1", 7]
, ["Collector Host 8", "Tomcat", 24]
, ["Collector Host 9", "Tomcat-MathApp-BA-PO", 0]
]}
```

- Exemple 9 : **obtention du nombre maximum de mesures pour les collecteurs**

```
curl -Lk -H "Authorization: Bearer $TOKEN " -H "Accept: application/json" -H
"Content-Type: application/json" http://$EM_HOST:8081/{tenantId}/apm/atc/api/
apmData/query \
```

```
-d "{ \"query\" : \"select agent_name, max(agg_value) from metric_data where
metric_path like '%Connections:Number of Metrics' group by agent_name\" }"
```

Résultat :

```
{ "columns": [{"name": "agent_name", "type": "string"},
{"name": "max(agg_value)", "type": "long"}]
, "rows": [{"Custom Metric Agent (Virtual)", 8756}
, ["Custom Metric Agent (Virtual) (Collector Host 1@5001)", 1990]
, ["Custom Metric Agent (Virtual) (Collector Host 2@5001)", 2117]
```

```
,["Custom Metric Agent (Virtual) (Collector Host 3@5001)",5141]
]}
```

API REST du Team Center

Utilisez l'API REST de Team Center pour fournir différentes fonctionnalités de requêtes de niveau tableau de bord et de données de mesures. Comme d'autres API REST APM, l'interface de l'API REST du Team Center utilise un système d'authentification basée sur des jetons. Pour plus d'informations sur la procédure d'obtention d'un jeton, consultez la rubrique [Génération d'un jeton de sécurité](#).

L'API REST du Team Center contient les ressources suivantes :

Ressource	Description	Exemple
/atc/private/apmData/query	Obtient les données de mesure à l'aide de la requête de syntaxe SQL standard dans la charge utile.	POST /atc/private/apmData/query
/atc/private/apmData/schema	Obtient les fonctionnalités de schéma SQL (c.-à-d. les tables prises en charge, les détails des colonnes) que vous pouvez utiliser dans la requête SQL REST .	GET /atc/private/apmData/schema

IMPORTANT

Utilisez l'[API REST SQL](#) publique *uniquement* pour extraire les données de mesure d'APM. Pour extraire les données de mesure APM ou non APM, utilisez l'[API REST de requête de mesure](#).

Ressources de l'API REST du Team Center

Vous pouvez définir des requêtes à l'aide des fonctions count, minimum, maximum et average. Les fonctions d'agrégation suivantes sont uniquement prises en charge dans la colonne agg_value de la table metric_data : sum, apm_average et apm_aggregate.

Les fonctions d'agrégation produisent les résultats suivants :

- La fonction d'agrégation sum fournit la somme des valeurs de la colonne agg_values.
- La fonction apm_aggregate fournit la somme ou la moyenne pondérée en fonction des mesures interrogées.
- La fonction apm_average fournit uniquement la moyenne pondérée.

L'API REST du Team Center contient les ressources suivantes :

Ressource 1 :

```
/atc/private/apmData/query
```

Obtient les données de mesure à l'aide de la requête de syntaxe SQL standard dans la charge utile.

Exemple : POST /atc/private/apmData/query

Charge utile :

```
{ "query": <SQLQuery(string)> //sql query string} // Example:{ "query": "select * from metric_data where ts >=
1572518520000 and ts <= 1572518535000"}
```

Réponse :

```
{
  "columns": [ // The columns specified in the query or all the columns(*) of the table as per the schema
    {
      "name": "source_name",
      // Source name of the metric, empty as it is no longer valid
    }
  ]
}
```

```

        "type": "string"
    },
    {
        "name": "agent_host",
        // Host name of the agent
        "type": "string"
        // Indicates the type of column value
    },
    {
        "name": "agent_process",
        // Process name
        "type": "string"
    },
    {
        "name": "agent_name",
        // Agent name of the metric
        "type": "string"
    },
    {
        "name": "domain_name",
        // Domain name of the metric
        "type": "string"
    },
    {
        "name": "metric_path",
        // Metric path containing folder name and metric attribute
        "type": "string"
    },
    {
        "name": "metric_attribute",
        // Attribute name of the metric
        "type": "string"
    },
    {
        "name": "attribute_type",
        // Integer that defines type of metric
        "type": "long"
    },
    {
        "name": "frequency",
        // Width of interval in number of seconds
        "type": "long"
    },
    {
        "name": "ts",
        // Denotes timestamp of the metric
        "type": "timestamp"
    },
    {
        "name": "min_value",
        // min value of the metric
        "type": "long"
    },
    },

```



```

    {
        "name": "max_value",
        // max value of the metric
        "type": "long"
    },
    {
        "name": "value_count",
        // Count of metric occurrences
        "type": "long"
    },
    {
        "name": "agg_value",
        // aggregate value of the metric
        "type": "long"
    }
],
"rows": [
    [
        <empty(string)>,
        <agent_host(string)>,
        <agent_process(string)>,
        <agent_name(string)>,
        <domain_name(string)>,
        <metric_path(string)>,
        <metric_attribute(string)>,
        <attribute_type(long)>,
        <frequency(long)>,
        <first_ts_value(timestamp)>,
        <min_value(long)>,
        <max_value(long)>,
        <value_count>,
        <agg_value(long)>
    ]
    //next row
  ] // Example:{
"columns": [
  {
    "name": "source_name",
    "type": "string"
  },
  {
    "name": "agent_host",
    "type": "string"
  },
  {
    "name": "agent_process",
    "type": "string"
  },
  {
    "name": "agent_name",
    "type": "string"
  },
  {

```

```

        "name": "domain_name",
        "type": "string"
    },
    {
        "name": "metric_path",
        "type": "string"
    },
    {
        "name": "metric_attribute",
        "type": "string"
    },
    {
        "name": "attribute_type",
        "type": "long"
    },
    {
        "name": "frequency",
        "type": "long"
    },
    {
        "name": "ts",
        "type": "timestamp"
    },
    {
        "name": "min_value",
        "type": "long"
    },
    {
        "name": "max_value",
        "type": "long"
    },
    {
        "name": "value_count",
        "type": "long"
    },
    {
        "name": "agg_value",
        "type": "long"
    }
],
"rows": [
    [
        "",
        "brtlvltsl719sl",
        "WebLogic",
        "WLP_LOGIN_MOBILE_PROD/WLP_LOGIN_MOBILE_PROD_Cluster/WLP_LOGIN_MOBILE_PROD_Srv23",
        "SuperDomain",
        "WebServices|Client|http://www.gvt.com.br/CustomerManagement/CustomerInformationManagement/
CustomerProfileManagement:SOAP Faults Per Interval",
        "SOAP Faults Per Interval",
        8194,
        15000,
        1572518520000,

```

```

    0,
    0,
    0,
    0
  ],
  [
    "",
    "brtlvltsl719sl",
    "WebLogic",
    "WLP_LOGIN_MOBILE_PROD/WLP_LOGIN_MOBILE_PROD_Cluster/WLP_LOGIN_MOBILE_PROD_Srv23",
    "SuperDomain",
    "WebServices|Client|http_//www.gvt.com.br/CustomerManagement/CustomerInformationManagement/
CustomerProfileManagement:SOAP Faults Per Interval",
    "SOAP Faults Per Interval",
    8194,
    15000,
    1572518535000,
    0,
    0,
    0,
    0
  ]
]}

```

Ressource 2 :

/atc/private/apmData/schema

Obtient les fonctionnalités de schéma SQL (c.-à-d. les tables prises en charge, les détails des colonnes) que vous pouvez utiliser dans la [requête SQL REST](#).

Exemple : GET /atc/private/apmData/schema

Réponse :

```

{
  "tables": [
    {
      "name": "metric_data",
      "columns": [
        {
          "name": "source_name",
          "type": "string",
          "whereCapabilities": [
            "=",
            "<",
            ">",
            "<=",
            ">=",
            "<>",
            "!=",
            "BETWEEN",
            "LIKE",
            "LIKE_REGEX"
          ]
        }
      ]
    }
  ],

```

```
{
  "name": "agent_host",
  "type": "string",
  "whereCapabilities": [
    "=",
    "<",
    ">",
    "<=",
    ">=",
    "<>",
    "!=",
    "BETWEEN",
    "LIKE",
    "LIKE_REGEX"
  ]
},
{
  "name": "agent_process",
  "type": "string",
  "whereCapabilities": [
    "=",
    "<",
    ">",
    "<=",
    ">=",
    "<>",
    "!=",
    "BETWEEN",
    "LIKE",
    "LIKE_REGEX"
  ]
},
{
  "name": "agent_name",
  "type": "string",
  "whereCapabilities": [
    "=",
    "<",
    ">",
    "<=",
    ">=",
    "<>",
    "!=",
    "BETWEEN",
    "LIKE",
    "LIKE_REGEX"
  ]
},
{
  "name": "domain_name",
  "type": "string",
  "whereCapabilities": [
    "=",
```

```

        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "metric_path",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "metric_attribute",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "attribute_type",
    "type": "long",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",

```

```

        "!=" ,
        "BETWEEN"
    ]
},
{
    "name": "frequency",
    "type": "long",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=" ,
        "BETWEEN"
    ]
},
{
    "name": "ts",
    "type": "timestamp",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=" ,
        "BETWEEN"
    ]
},
{
    "name": "min_value",
    "type": "long",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=" ,
        "BETWEEN"
    ]
},
{
    "name": "max_value",
    "type": "long",
    "whereCapabilities": [
        "=",
        "<",
        ">",

```

```

        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN"
    ]
},
{
    "name": "value_count",
    "type": "long",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN"
    ]
},
{
    "name": "agg_value",
    "type": "long",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN"
    ]
}
]
},
{
    "name": "metrics",
    "columns": [
        {
            "name": "source_name",
            "type": "string",
            "whereCapabilities": [
                "=",
                "<",
                ">",
                "<=",
                ">=",
                "<>",
                "!=",
                "BETWEEN",
                "LIKE",
            ]
        }
    ]
}

```

```

        "LIKE_REGEX"
    ]
},
{
    "name": "agent_host",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "agent_process",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "agent_name",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "domain_name",

```



```

        "type": "string",
        "whereCapabilities": [
            "=",
            "<",
            ">",
            "<=",
            ">=",
            "<>",
            "!=",
            "BETWEEN",
            "LIKE",
            "LIKE_REGEX"
        ]
    },
    {
        "name": "metric_path",
        "type": "string",
        "whereCapabilities": [
            "=",
            "<",
            ">",
            "<=",
            ">=",
            "<>",
            "!=",
            "BETWEEN",
            "LIKE",
            "LIKE_REGEX"
        ]
    },
    {
        "name": "metric_attribute",
        "type": "string",
        "whereCapabilities": [
            "=",
            "<",
            ">",
            "<=",
            ">=",
            "<>",
            "!=",
            "BETWEEN",
            "LIKE",
            "LIKE_REGEX"
        ]
    },
    {
        "name": "attribute_type",
        "type": "long",
        "whereCapabilities": [
            "=",
            "<",
            ">",

```

```

        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN"
    ]
},
{
    "name": "first_seen",
    "type": "timestamp",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN"
    ]
},
{
    "name": "last_seen",
    "type": "timestamp",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN"
    ]
}
]
},
{
    "name": "sources",
    "columns": [
        {
            "name": "source_name",
            "type": "string",
            "whereCapabilities": [
                "=",
                "<",
                ">",
                "<=",
                ">=",
                "<>",
                "!=",
                "BETWEEN",
                "LIKE",
            ]
        }
    ]
}

```

```

        "LIKE_REGEX"
    ]
},
{
    "name": "status",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
},
{
    "name": "type",
    "type": "string",
    "whereCapabilities": [
        "=",
        "<",
        ">",
        "<=",
        ">=",
        "<>",
        "!=",
        "BETWEEN",
        "LIKE",
        "LIKE_REGEX"
    ]
}
]
}
]]

```

API REST de demande de mesure

API REST de demande de mesure Utilisez l'API de demande de mesure pour interroger les mesures des différentes périodes, fréquences et métriques. Comme d'autres API APM REST, l'interface API REST de demande de mesure utilise une authentification par jeton. Pour plus d'informations sur la procédure d'obtention d'un jeton, consultez la rubrique [Génération d'un jeton de sécurité](#).

L'API contient les ressources suivantes :

Ressource	Description	Exemple
/metrics/queryMetric	Exécutez une demande de mesures et récupérez les valeurs de mesures en fonction des critères de demande et de la période spécifiées. La <SpécificateurDeDemande> peut être toute combinaison de Spécifications de la demande.	POST /metrics/queryMetric

IMPORTANT

Vous pouvez utiliser l'API REST de demande de mesure pour générer des données de mesures APM ou non APM. Vous pouvez également utiliser l'API REST SQL publique pour générer des données de mesures APM. Pour plus d'informations sur la génération de données de mesures APM à l'aide de l'API REST SQL publique, reportez-vous à la section [API REST SQL](#).

Exemple : POST /metrics/queryMetric

Charge utile :

```
{
  "querySpecififier": <QuerySpecififier>,
  "queryRange": {
    "endTime": <time(unixTimestamp/seconds)>, // End time of range (default is current time - NOW)
    "rangeSize": <seconds>, // Width of range to be returned
    "frequency": <seconds> // Specifies requested frequency (default is 15 seconds)
  },
  "clampSize": <size> // default is 500
}

// Example:
{
  "querySpecififier": {
    "op": "SPEC",
    "sourceNameSpecififier": {
      "op": "EXACT",
      "names": [
        "SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)"
      ]
    },
    "attributeNameSpecififier": {
      "op": "REGEX",
      "pattern": "Enterprise Manager:.*"
    }
  },
  "queryRange": {
    "endTime": 1571823645,
    "rangeSize": 120,
    "frequency": 15
  },
  "clampSize": 100
}
```

Réponse :

```

{
  "metrics": [{
    "id": <MetricId(string)>,
    "source": <SourceName(string)>,
    "attribute": <AttributeName(string)>,
    "attributes": <Attributes_Optional(NameValue Pairs - strings)>,
    "type": <type(32bit Integer)>,
    "values": [
      [<time(unixTimestamp/seconds)>, <interval/seconds>, <min>, <max>, <value>, <count>]
      // next data point
    ]
  }
  // next metric
]
}

// Example:
{
  "metrics": [
    {
      "id": "0P-BAB-B-jt9BQG",
      "source": "SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)",
      "attribute": "Enterprise Manager:Overall Capacity (%)",
      "attributes" : { // attributes are optional
        "attribName1" : "attribValue1",
        "hostname" : "test.broadcom.com"
      },
      "type":2050,
      "values": [
        [1518521415, 15, 2, 4, 3, 4],
        [1518521430, 15, 2, 3, 3, 4],
        [1518521445, 15, 3, 4, 3, 4],
        [1518521460, 15, 2, 5, 3, 4],
        [1518521475, 15, 2, 3, 3, 4],
        [1518521490, 15, 86, 86, 86, 1],
        [1518521505, 15, 5, 19, 11, 4],
        [1518521520, 15, 4, 51, 17, 5],
        [1518521535, 15, 3, 11, 7, 4]]
      ]
    }
  ]
}

```

Cumuls pris en charge

L'API prend en charge les spécificateurs d'agrégation suivants :

- MetricSpecifieur directe
- MetricSpecifieur de bucket

MetricSpecifieur directe

TopK : Obtenez le top N des X les moins performants, où les exemples de X dans l'APM sont les URL, les backends, les frontends, etc.

Exemples :

1. Obtention des deux URL les plus performantes
2. Obtention des deux MVJ les plus consommatrices de mémoire

Exemple : POST /metrics/queryMetric

Charge utile : Deux URL principales les moins performantes basées sur le temps de réponse moyen (MS)

```
{
  "querySpecifier": {
    "op": "SPEC",
    "sourceNameSpecifier": {
      "op": "ALL"
    },
    "attributeNameSpecifier": {
      "op": "REGEX",
      "pattern": "Frontends.*"
    }
  },
  "queryRange": {
    "endTime": 1571823645,
    "rangeSize": 120,
    "frequency": 15
  },
  "aggregations": [
    {
      "input": {
        "op": "TOPK",
        "limit": "2",
        "includeAggregateTimeSeries": false
      }
    }
  ]
}
```

Réponse :

```
{
  "aggregations": {
    "TOPK": [
      {
        "key": "SuperDomain|Host1|Process1|Agent1|Frontends|Apps|App1|URLs|URL1:Average Response Time (ms)",
        "ids": [
          "p-BQ-B-2gnVbE"
        ],
        "metric": {
          "sourceName": "SuperDomain|Host1|Process1|Agent1",
          "type": 268436481,
          "attributeName": "Frontends|Apps|App1|URLs|URL1:Average Response Time (ms)",
          "attributes": {
            "installer": "DXI",
            "productName": "APM"
          }
        }
      }
    ]
  }
}
```

```
    }  
  },  
  "values": [  
    [  
      1571823645,  
      15,  
      2,  
      4,  
      3,  
      4  
    ],  
    [  
      1571823660,  
      15,  
      2,  
      3,  
      3,  
      4  
    ],  
    [  
      1571823675,  
      15,  
      3,  
      4,  
      3,  
      4  
    ],  
    [  
      1571823690,  
      15,  
      2,  
      5,  
      3,  
      4  
    ],  
    [  
      1571823705,  
      15,  
      2,  
      3,  
      3,  
      4  
    ],  
    [  
      1571823720,  
      15,  
      86,  
      86,  
      86,  
      1  
    ],  
    [  
      1571823735,
```

```

        15,
        5,
        19,
        11,
        4
    ],
    [
        1571823750,
        15,
        4,
        51,
        17,
        5
    ],
    [
        1571823765,
        15,
        3,
        11,
        7,
        4
    ]
],
"aggregateValues": [
    [
        1571823765,
        120,
        2,
        86,
        9,
        34
    ]
]
},
{
    "key": "SuperDomain|Host1|Process1|Agent2|Frontends|Apps|App1|URLs|URL2:Average Response Time (ms)",
    "ids": [
        "q-CS-F-3vnFcr"
    ],
    "metric" : {
        "sourceName": "SuperDomain|Host1|Process1|Agent2",
        "type": 268436481,
        "attributeName": "Frontends|Apps|App1|URLs|URL1:Average Response Time (ms)",
        "attributes": {
            "installer": "DXI",
            "productName": "APM"
        }
    },
    "values": [
        [
            1571823645,
            15,
            2,

```



```
4,  
3,  
4  
],  
[  
  1571823660,  
  15,  
  2,  
  3,  
  3,  
  4  
],  
[  
  1571823675,  
  15,  
  3,  
  4,  
  3,  
  4  
],  
[  
  1571823690,  
  15,  
  2,  
  5,  
  3,  
  4  
],  
[  
  1571823705,  
  15,  
  2,  
  3,  
  3,  
  4  
],  
[  
  1571823720,  
  15,  
  87,  
  87,  
  87,  
  1  
],  
[  
  1571823735,  
  15,  
  5,  
  21,  
  13,  
  4  
],  
[
```

```

        1571823750,
        15,
        4,
        59,
        12,
        5
    ],
    [
        1571823765,
        15,
        3,
        12,
        5,
        4
    ]
],
"aggregateValues": [
    [
        1571823765,
        120,
        2,
        87,
        8,
        34
    ]
]
}
]
}
}
}

```

BottomK : Obtenez le bottom N le moins performant X où les exemples de X dans l'APM sont les URL, les composants d'arrière-plan, les composants frontaux, etc.

Charge utile : Les deux URL bottom les plus performantes basées sur le temps de réponse moyen (MS)

```

{
  "querySpecifier": {
    "op": "SPEC",
    "sourceNameSpecifier": {
      "op": "ALL"
    },
    "attributeNameSpecifier": {
      "op": "REGEX",
      "pattern": "Frontends\\|Apps\\|[^\\|]*\\|URLs\\|[^\\|]*:Average Response Time \\(ms\\)"
    }
  },
  "queryRange": {
    "endTime": 1571823645,
    "rangeSize": 120,
    "frequency": 15
  },
  "aggregations": [

```

```

    {
      "input": {
        "op": "BOTATOMK",
        "limit": "10",
        "includeAggregateTimeSeries": true
      }
    }
  ]
}

```

Réponse :

```

{
  "aggregations": {
    "BOTATOMK": [
      {
        "key": "SuperDomain|Host1|Process1|Agent2|Frontends|Apps|App1|URLs|URL2:Average Response Time (ms)",
        "ids": [
          "q-CS-F-3vnFcr"
        ],
        "metric": {
          "sourceName": "SuperDomain|Host1|Process1|Agent2",
          "type": 268436481,
          "attributeName": "Frontends|Apps|App1|URLs|URL1:Average Response Time (ms)",
          "attributes": {
            "installer": "DXI",
            "productName": "APM"
          }
        },
        "values": [
          [
            1571823645,
            15,
            2,
            4,
            3,
            4
          ],
          [
            1571823660,
            15,
            2,
            3,
            3,
            4
          ],
          [
            1571823675,
            15,
            3,
            4,
            3,
            4
          ]
        ]
      }
    ]
  }
}

```

```
[
  1571823690,
  15,
  2,
  5,
  3,
  4
],
[
  1571823705,
  15,
  2,
  3,
  3,
  4
],
[
  1571823720,
  15,
  87,
  87,
  87,
  1
],
[
  1571823735,
  15,
  5,
  21,
  13,
  4
],
[
  1571823750,
  15,
  4,
  59,
  12,
  5
],
[
  1571823765,
  15,
  3,
  12,
  5,
  4
]
],
"aggregateValues": [
  [
    1571823765,
    120,
```

```

        2,
        87,
        8,
        34
    ]
}
},
{
    "key": "SuperDomain|Host1|Process1|Agent1|Frontends|Apps|App1|URLs|URL1:Average Response Time (ms)",
    "ids": [
        "p-BQ-B-2gnVbE"
    ],
    "metric": {
        "sourceName": "SuperDomain|Host1|Process1|Agent1",
        "type": 268436481,
        "attributeName": "Frontends|Apps|App1|URLs|URL1:Average Response Time (ms)",
        "attributes": {
            "installer": "DXI",
            "productName": "APM"
        }
    },
    "values": [
        [
            1571823645,
            15,
            2,
            4,
            3,
            4
        ],
        [
            1571823660,
            15,
            2,
            3,
            3,
            4
        ],
        [
            1571823675,
            15,
            3,
            4,
            3,
            4
        ],
        [
            1571823690,
            15,
            2,
            5,
            3,
            4
        ]
    ]
}

```

```
],  
[  
  1571823705,  
  15,  
  2,  
  3,  
  3,  
  4  
],  
[  
  1571823720,  
  15,  
  86,  
  86,  
  86,  
  1  
],  
[  
  1571823735,  
  15,  
  5,  
  19,  
  11,  
  4  
],  
[  
  1571823750,  
  15,  
  4,  
  51,  
  17,  
  5  
],  
[  
  1571823765,  
  15,  
  3,  
  11,  
  7,  
  4  
]  
],  
"aggregateValues": [  
  [  
    1571823765,  
    120,  
    2,  
    86,  
    9,  
    34  
  ]  
]  
}
```

```

    ]
  }
}

```

MetricSpecifieur de bucket

Groupez X dans Y et obtenez les N principaux dans Y. Par exemple, obtenez les 10 premières machines virtuelles Java servant le nombre maximum de demandes, où le nombre maximum de demandes correspond à la somme des réponses de tous les points d'entrée.

Exemple : POST /metrics/queryMetric

Charge utile : Top 2 des MVJ en fonction du nombre de demandes servies (regrouper les composants frontaux dans les MVJ et obtenez le top 10 des MVJ)

```

{
  "querySpecifieur": {
    "op": "SPEC",
    "sourceNameSpecifieur": {
      "op": "ALL"
    },
    "attributeNameSpecifieur": {
      "op": "AND",
      "specifieurs": [
        {
          "op": "REGEX",
          "pattern": "Frontends\\|Apps\\|[^\\|]*:Responses Per Interval"
        },
        {
          "op": "ATTRIBUTE",
          "expressions": [
            {
              "name": "processType",
              "values": [
                "Java"
              ],
              "operator": "MATCHES",
              "comparator": "LEXICAL"
            }
          ]
        }
      ]
    }
  },
  "queryRange": {
    "endTime": 1571823645,
    "rangeSize": 30,
    "frequency": 15
  },
  "aggregations": [
    {
      "input": {
        "op": "TOPK",
        "input": {
          "op": "BUCKET_ATTRIBUTE",

```

```

        "value": "APPNAME"
      },
      "limit": "10",
      "includeAggregateTimeSeries": true
    }
  ]
}

```

Valeurs prises en charge pour l'opération de compartiment :

Opération(OP)	Valeur
ATTRIBUT_BUCKET	<Custom AttributeName>
SOURCE_BUCKET	<ul style="list-style-type: none"> hostname (nom d'hôte) domaine Processus agent
BUCKET_ATTRIBUTE_NAME	<ul style="list-style-type: none"> metricpath (chemin de la mesure) metricname

Réponse :

```

{
  "aggregations": {
    "TOPK": [
      {
        "key": "Process1",
        "ids": [
          "p-BQ-B-2gnVbE",
          "p-BQ-B-2gnVbF"
        ],
        "values": [
          [
            1571823645,
            15,
            34,
            34,
            34,
            34
          ],
          [
            1571823660,
            15,
            27,
            27,
            27,
            27
          ]
        ],
        "aggregateValues": [
          [
            1571823645,

```



```

        30,
        61,
        61,
        61,
        61
    ]
}
{
    "key": "Process2",
    "ids": [
        "p-BQ-B-2gnVbG",
        "p-BQ-B-2gnVbH"
    ],
    "values": [
        [
            1571823645,
            15,
            24,
            24,
            24,
            24
        ],
        [
            1571823660,
            15,
            27,
            27,
            27,
            27
        ]
    ],
    "aggregateValues": [
        [
            1571823645,
            30,
            51,
            51,
            51,
            51
        ]
    ]
}
]
}
}

```

Utilisation des URL publiques courtes dans DX APM

DX APM vous fournit des URL publiques courtes afin d'éviter de devoir couper les URL longues et de faciliter leur utilisation. Vous pouvez utiliser ces URL pour envoyer directement d'autres utilisateurs à des dispositions préconfigurées dans DX APM. Vous pouvez fournir aux autres utilisateurs des URL courtes pour les vues Carte et Mesures. En outre, vous pouvez également utiliser les URL publiques courtes dans les alertes et les notifications par courriel.

NOTE

Les utilisateurs ne peuvent pas accéder à ces liens sans nom d'utilisateur et mot de passe pour DX APM.

Les paramètres d'URL complètes peuvent changer au fil du temps. Vous pouvez utiliser les paramètres suivants pour mapper les URL publiques.

Pour plus d'informations sur les paramètres des API, reportez-vous à la section [Référence d'API](#).

Itinéraires

Le tableau suivant présente le mappage de l'itinéraire public à l'itinéraire interne.

Itinéraire public	DX APMItinéraire interne
/public/vertex	/map
/public/alerts	/alert
/public/metrics	/metrics

Paramètres

Utilisez les paramètres publics suivants pour définir des valeurs spécifiques.

Itinéraire	Paramètre public	Obligatoire	Valeur	Valeur par défaut
/public/vertex	ID (identification)	Oui	ID de vertex	
	endTime	Non	Heure de fin en millisecondes	Mode dynamique si l'heure de fin n'est pas spécifiée
	plage	Non	Plage en millisecondes	480000
	layer (couche)	Non	[ATC APM_INFRASTRUCTURE]	ATC
/public/alerts	name (nom)	Oui	<<domain name>>:<<management module>>:<<AlertName>>	
/public/metrics	éléments	Oui	Ensemble de chemins de mesures délimités par des virgules	
	endTime	Non	Heure de fin en millisecondes	
	plage	Non	Plage en millisecondes	480000

Exemples

Les exemples suivants présentent la procédure de mappage des URL raccourcies.

```
https://<<apmservices-gateway url>>/{tenantID}/apm/atc/#/public/vertex?
id=72&endTime=1534752446000&range=86400000&layer=ATC
```

```
https://<<apmservices-gateway url>>/{tenantID}/apm/atc/#/public/alerts?name=SuperDomain:Cassandra:Connection
%20Status
```

`https://<<apmservices-gateway url>>/{tenantID}/apm/atc/#/public/metrics?items=["SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|APM Alert Summaries:Caution Alerts","SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|APM Alert Summaries:Caution Triage Map Alerts"]&endTime=1534752446000&range=86400000`

Prise en charge internationale

Un produit internationalisé est un produit anglais qui fonctionne correctement dans les versions localisées du système d'exploitation et des produits tiers requis. Un produit internationalisé prend également en charge les données linguistiques locales pour l'entrée et la sortie. Les produits internationalisés offrent également la possibilité de spécifier les conventions régionales applicables au format de date, d'heure, de devise et de valeurs numériques.

Un produit traduit est un produit internationalisé qui inclut la prise en charge, dans la langue locale, de l'interface utilisateur, de l'Aide en ligne et de toute autre documentation du produit. Un produit traduit inclut également les paramètres linguistiques régionaux par défaut applicables au format de date, d'heure, de devise et de valeurs numériques. Un produit traduit est parfois désigné sous le nom de produit localisé.

Application Performance Management DX prend en charge les options d'internationalisation suivantes. Le produit est entièrement localisé et prend en charge les paramètres régionaux applicables à la date, à l'heure et aux valeurs numériques. L'interface utilisateur est disponible dans les langues suivantes :

- Anglais
- Français
- Portugais (Brésil)
- Espagnol

La documentation du produit est disponible dans les langues suivantes :

- Anglais
- Français
- Portugais (Brésil)
- Espagnol

Fonctionnalités d'accessibilité du produit

Nous nous engageons à ce que tous les clients, quelle que soit leur capacité, puissent utiliser nos produits et la documentation associée pour réaliser leurs tâches professionnelles. Cette section décrit les fonctionnalités d'accessibilité de DX Application Performance Management.

Améliorations du produit

DX APM propose des améliorations de l'accessibilité dans les domaines suivants :

- Affichage
- Sound
- Keyboard
- Mouse

Les informations suivantes s'appliquent aux applications Windows et Macintosh. Les applications Java s'exécutent sur plusieurs systèmes d'exploitation hôte, qui peuvent déjà disposer de technologies d'assistance. Pour que ces technologies d'assistance fonctionnent, deux fonctionnalités de la machine virtuelle Java (JVM) doivent être disponibles pour permettre d'accéder aux programmes écrits en JPL. Les technologies d'assistance dépendent de la prise en charge de l'accessibilité Java disponible dans la JVM. Les technologies d'assistance doivent également disposer d'un pont entre elles dans leurs environnements natifs. Ce pont a une extrémité dans la JVM et l'autre dans la plate-forme native. Par conséquent, le pont est légèrement différent pour chaque plate-forme à laquelle se connecte la JVM. Sun développe à la fois le côté JPL et le côté Win32 de ce pont.

Affichage

Pour augmenter la visibilité sur l'affichage de votre ordinateur, vous pouvez ajuster les options suivantes :

- **Font style, color, and size of items**

Définit la couleur de police, la taille et d'autres combinaisons visuelles.

- **Screen resolution**

Définit le nombre de pixels pour agrandir des objets dans la fenêtre.

- **Cursor width and blink rate**

Définit la largeur et la fréquence de clignotement du curseur pour améliorer sa visibilité ou réduire le clignotement.

- **Icon size**

Définit la taille des icônes. Vous pouvez agrandir les icônes pour améliorer leur visibilité ou la réduire pour augmenter l'espace sur l'écran.

- **High contrast schemes**

Définit les combinaisons de couleurs. Vous pouvez sélectionner les couleurs les plus faciles à voir.

Sound

Pour utiliser le son comme alternative visuelle ou pour rendre les sons plus faciles à entendre ou distinguer, ajustez les options suivantes :

- **Volume**

Définit le volume de l'ordinateur.

- **Text-to-Speech**

Définit les options d'écoute de commande de l'ordinateur et de lecture de texte.

- **Warnings**

Définit les avertissements visuels.

- **Notices**

Définit les informations audio ou visuelles lorsque les fonctionnalités d'accessibilité sont activées ou désactivées.

- **Schemes**

Associe des sons à des événements système spécifiques.

- **Captions**

Affiche des légendes pour les sons et la synthèse vocale.

Keyboard

Vous pouvez effectuer les réglages de clavier suivants :

- **Repeat Rate**

Définit la vitesse de répétition des caractères lorsqu'une touche est enfoncée.

- **Tones**

Définit les sons lorsque vous appuyez sur certaines touches.

- **Sticky Keys**

Définit la touche modificatrice (MAJ, Ctrl, Alt ou touche Windows), pour les combinaisons de raccourci. Les touches rémanentes sont actives jusqu'à ce qu'une autre touche soit enfoncée.

Mouse

Vous pouvez utiliser les options suivantes pour rendre la souris plus rapide et facile à utiliser :

- **Click Speed**

Définit la vitesse du clic pour effectuer une sélection.

- **Click Lock**

Définit la souris pour sélectionner ou déplacer du contenu sans maintenir le bouton de la souris enfoncé.

- **Reverse Action**

Définit la fonction inverse contrôlée par les touches gauche et droite de la souris.

- **Blink Rate**

Définit la vitesse de clignotement du curseur.

- **Pointer Options**

Vous permet de définir les comportements suivants :

- – Masquer le pointeur pendant la saisie
- – Afficher l'emplacement du pointeur
- – Définir la vitesse de déplacement du pointeur sur l'écran
- – Sélectionner la taille et la couleur du pointeur pour une meilleure visibilité
- – Déplacer le pointeur vers un emplacement par défaut dans une boîte de dialogue

Raccourcis clavier

DX APM prend en charge les raccourcis clavier suivants :

- **CTRL + X** - Couper
- **CTRL + C** - Copier
- **CTRL + K** - Rechercher l'élément suivant
- **CTRL + F** - Rechercher et remplacer
- **CTRL + V** - Coller
- **CTRL + S** - Enregistrer
- **CTRL + MAJ + S** - Tout enregistrer
- **CTRL + D** - Supprimer la ligne
- **CTRL + flèche vers la droite** - Mot suivant
- **CTRL + flèche vers le bas** - Parcourir les lignes vers le bas
- **Fin** - Fin de ligne

Raccourcis clavier des vidéos de produits

La documentation de DX APM inclut des didacticiels vidéo du produit hébergés sur YouTube. Lorsque vous affichez ces vidéos du produit, vous pouvez utiliser les raccourcis clavier suivants :

- **Tabulation** - Défilement avant dans les fonctions
- **Tabulation + MAJ** - Défilement arrière
- **Entrée** - Sélectionne la fonction mise en surbrillance dans une liste
- **Flèche avant** et **Flèche arrière** - Contrôlent le volume de la vidéo

Données d'utilisation (télémétrie)

La télémétrie est un élément fondamental du modèle PLA (Contrat de licence de portefeuille) de logiciels pour l'entreprise. La condition initiale de l'effort de télémétrie est de collecter et signaler l'utilisation quotidienne spécifique au produit pour le soutien du nouveau modèle de consommation. Vous devez activer la télémétrie et partager les données d'utilisation si votre organisation est un client Broadcom en vertu du PLA de logiciels pour l'entreprise. Cet article décrit comment activer la télémétrie et acheminer les données d'utilisation vers le portail Usage Reporting Portal. Pour plus d'informations, consultez la section [Portail Usage Reporting Portal](#).

- [Données collectées par la télémétrie](#)
- [Fréquence de collecte des données](#)
- [Paramètres d'utilisateur dans IntroscopeEnterpriseManager.properties](#)
- [Configuration du proxy HTTP](#)
- [Calcul des mesures de licence](#)
- [Procédure de signalement automatique des données d'utilisation](#)
- [Procédure de signalement manuel des données d'utilisation](#)

Données collectées par la télémétrie

La télémétrie collecte deux types de détails pour chaque client PLA :

- **Données client** : ces données identifient le client et le site client via l'ID de site. Les données incluent également un ID de contre-passation facultatif qui permet d'identifier la division ou le groupe auxquels l'utilisation doit être facturée.
- **Données d'utilisation** : les données d'utilisation réelles basées sur la consommation sont collectées. Vous devez activer le chargement des données d'utilisation. Pour plus d'informations sur les données d'utilisation collectées, consultez la documentation produit correspondante.

NOTE

La télémétrie ne collecte pas d'informations d'identification personnelle (IIP) ni d'informations sensibles. Pour en savoir plus sur la collecte et l'utilisation de vos informations, consultez notre [déclaration de confidentialité](#).

Fréquence de collecte des données

Par défaut, la télémétrie collecte et stocke les données tous les jours à 12 h. Si le planificateur n'est pas actif à 12 h, les données sont collectées uniquement lors de l'exécution du planificateur le jour suivant. Les données sont collectées une seule fois par jour.

Paramètres d'utilisateur dans IntroscopeEnterpriseManager.properties

Pour charger les données, l'utilisateur doit configurer les propriétés suivantes dans le fichier `IntroscopeEnterpriseManager.properties`, puis définir la valeur de `introscope.platelemetry.upload.enabled` (configurable à chaud) sur `true`. Les propriétés suivantes sont configurables.

Nom de propriété	Description
<code>introscope.platelemetry.instance.</code>	ID généré en interne pour chaque instance du produit.
<code>introscope.platelemetry.customer.</code>	Nom de domaine du client (ne doit pas être une adresse électronique).
<code>introscope.platelemetry.customer.</code>	ID de site client.
<code>introscope.platelemetry.customer.</code>	Indicateur permettant de déterminer si une installation ou une mise à niveau est liée à l'utilisation incrémentielle du PLA (valeur par défaut : <code>false</code>).

Nom de propriété	Description
<code>introscope.platelemetry.customer_id</code>	Facultatif. Utilisé pour identifier la division ou le groupe pour référencer l'utilisation à signaler sur broadcom.com.

Configuration du proxy HTTP

Pour obtenir une description des propriétés EM standard pour un proxy HTTP, telles que `transport.http.proxy.host`, `transport.http.proxy.port`, `transport.http.proxy.username` et `transport.http.proxy.password` (valeur chiffrée), reportez-vous à la section [Configuration de la station de travail](#).

Données collectées

Les données suivantes sont collectées pour DX Application Performance Management :

- Unités

Les tableaux suivants affichent les charges utiles de télémétrie :

Table 3: Charges utiles de télémétrie

Propriétés de charge utile de télémétrie	Description
<code>domain_name</code>	Nom de domaine (par exemple, href="http://customer.com/">customer.com, bank.eu).
<code>site_id</code>	ID de site d'entreprise que le client utilise pour accéder au site de support. Pour obtenir l'ID de site à partir du portail de support, accédez à Mon compte, Profil, Support CA (onglet), ID de site de connexion.
<code>pla_agreement</code>	Valeur booléenne sous forme numérique (1 == true, 0 == false). Cette valeur indique si le client participe à l'abonnement Contrat de licence de portefeuille.
<code>chargeback_id</code>	Valeur fournie par le client au groupe d'identités ou à la zone d'imputation pour utilisation interne, notamment pour la facturation aux groupes.
<code>product_sku</code>	La valeur de SKU spécifique du produit est fournie à la bibliothèque sous-jacente par le produit lors de son initialisation.
<code>sku_description</code>	Description du SKU du produit fournie à la bibliothèque sous-jacente par le produit lors de son initialisation.
<code>product_version</code>	Version du produit.
<code>instance_id</code>	UUID généré par le produit lors de la première installation. Plusieurs installations requièrent des produits pour générer une nouvelle valeur d'ID d'instance à chaque fois.
<code>multiple telemetry metrics key_name</code>	Toutes les paires clé/valeur contiennent un préfixe d'espace de noms pour les rendre uniques par rapport aux valeurs ci-dessus. La télémétrie doit être le préfixe de cette propriété. Des paires clé/valeur sont ajoutées à la charge utile. Ces paires clé/valeur contiennent des mesures d'utilisation spécifiques au produit.
<code>date_collected</code>	Date de collecte des données de télémétrie. Le format de date AAAA-MM-JJ (par exemple, 2018-02-20) est utilisé.

Variables d'environnement

Le tableau suivant répertorie les variables utilisées pour la télémétrie, avec des exemples :

Variable	Description
APPMANAGER_TELEMETRY_ENVTYPE=onpremise	Cette variable correspond au type d'installation.
APPMANAGER_TELEMETRY_CUSTOMERINFO=PROPERTIES_PATH\package\to/customer/info/file>	Cette variable définit le chemin des propriétés d'informations client.
APPMANAGER_TELEMETRY_UPLOADENABLE=false	Cette variable est utilisée pour charger les données de télémétrie.

Calcul des mesures de licence

Les mesures DX Application Performance Management sont calculées comme suit pour chaque agent d'application :

Applications	Mappage
Java	Chaque instance en cours d'exécution d'une machine virtuelle Java (JVM) surveillée consomme 4 unités.
.NET et .NET CorePS	Chaque instance de système d'exploitation exécutant une application .Net ou CLR (Common Language Runtime) surveillée consomme 4 unités.
PHP	Chaque instance en cours d'exécution de l'agent de sonde PHP consomme 2 unités.
Node.js	Chaque processus Node.js surveillé consomme 0,4 unité.
Python	Chaque instance de système d'exploitation exécutant une application Python surveillée consomme 4 unités.

Procédure de signalement automatique des données d'utilisation

Une fois l'installation terminée, configurez l'envoi des données de télémétrie à Broadcom.com.

Procédez comme suit :

1. Copiez le contenu du fichier **opt/dxplatelemetry/configcommon/esdplatelemetry_onpreminfo.properties.template** dans le fichier **opt/dxplatelemetry/configcommon/esdplatelemetry_onpreminfo.properties**.
2. Modifiez le fichier **opt/dxplatelemetry/configcommon/esdplatelemetry_onpreminfo.properties** et remplissez les clés suivantes avec les informations correctes :
 - **dxitenantid** : entrez l'ID de client hébergé pour stocker les données de télémétrie PLA dans NASS.

NOTE

- Entrez l'ID de client hébergé et non l'ID de cohorte.
 - La valeur **dxitenantid** est sensible à la casse.
- **perform_upload** : détermine si les calculs de télémétrie de PLA sont envoyés à Broadcom.com. Entrez True pour charger les calculs de télémétrie. Valeurs : true ou false
3. Redémarrez le pod de télémétrie de PLA pour terminer la configuration.

Procédure de signalement manuel des données d'utilisation

Vous pouvez signaler l'utilisation des données de télémétrie manuellement en procédant comme suit. Vous ne devez signaler l'utilisation manuellement que si vous êtes un client PLA et qu'il existe une raison valable pour laquelle vous ne pouvez pas configurer la télémétrie pour signaler automatiquement l'utilisation.

Vous pouvez configurer cela dans le cadre des étapes de post-installation. Pour connaître la procédure complète, reportez-vous à la section [Populate Information and Configure Telemetry](#). Vous devrez peut-être également configurer l'utilisation des données de télémétrie à l'aide de l'API du collecteur d'utilisation du produit. Pour plus d'informations sur l'utilisation de cette API, reportez-vous à la section [Product Usage Collector](#).

Documentation Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b) (3), as applicable, or their successors.

Copyright © 2005–2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

