DX APM - SaaS - Portuguese - Brazil

Table of Contents

Requisitos de rede do DX SaaS **8**

Novidades no 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** **15**
- **22.6** **16**
- **22.3** **17**
- **22.1** **20**
- **Notas da versão de 2021** **24**
  - 21.11 24
  - 21.6 31
  - 21.4 35
  - 21.1 39
- **Notas da versão de 2020** **41**
  - 20.11 41
  - 20.9 48
  - 20.6 52
  - 20.4 55
  - 20.1 62
- **Notas da versão de 2019** **67**
  - Novembro de 2019 67
  - Outubro de 2019 69
  - Agosto de 2019 70

Introdução **72**

- **Suporte e compatibilidade** **72**
- **Arquitetura do DX APM** **72**
- **Recursos em vídeo do DX APM** **73**
- **Convenções de diretório e nome de arquivo** **75**
- **Personalizações** **76**
- **Artigos da base de conhecimento** **76**

Glossário **79**
Confirmações de software de terceiros - SaaS **100**
Implementando agentes **101**
Configurar o ambiente de monitoramento **102**
Funções e privilégios suportados **103**
Gerar token de segurança **107**
Criar notificações para alertas **108**
Configurar notificações por email para alertas **112**
Configurar universos **113**
Configurar a Exibição da experiência **117**
Definir a forma de monitoramento do ambiente com regras de atributo **122**
Importar regras de atributo em massa 126
Ajustar o monitoramento com alertas **128**
Gerenciar dados de métrica usando módulos de gerenciamento **131**
Criar e trabalhar com módulos de gerenciamento 133
Configurar agrupamentos de métricas no Team Center 138
Criar e configurar alertas simples no Team Center 145
Criar e configurar alertas de resumo 152
Criar e editar calculadoras 155
Configurar a análise diferencial 159
Configurar as extensões do JavaScript **161**
Recomendações de dimensionamento do monitor do Docker **170**
Fazer download de ferramentas adicionais **171**
Ferramenta Importação de agentes 171
Conectar o Workstation 174
Cloud Proxy 176
Métricas de suportabilidade do Cloud Proxy 187
Configurar a estação de trabalho 190
Regras de supressão de rastreamento para ocultar dados confidenciais **192**
Configurar o APM Command Center **192**
Exibir status do agente 193
Exibir relatórios do agente 195
Configurar os aplicativos para integração 196
Gerenciar pacotes de agentes 197
Configurar componentes 199
Pesquisar usando a AQL (ACC Query Language) 200
Usando **202**
Integração de aplicativos para monitoramento **203**
Monitorar o desempenho usando a Exibição da experiência **204**

Investigar problemas usando o Bloco de notas de análise....209
Exibir status do agente e gerenciar cartões de agente....214
Monitorar valores de métrica do agente com a Exibição da métrica....217
Incorporar painéis do DX na exibição da métrica....222
Usar a linha de tempo e o realce....224
Usar a linha do tempo e exibir eventos de mudança....226
Usar os atributos no DX APM....229
Organizar componentes usando perspectivas....232
Exibir relacionamentos entre os componentes do mapa....235
Camadas do mapeamento....239
Identificar áreas problemáticas usando filtros....243
Monitorar a integridade geral do ambiente com o painel....245
Monitorar problemas e anomalias da triagem assistida....248
Triagem assistida e analistas....249
Investigar o baixo desempenho das transações....254
Usar o rastreamento de transação entre processos para resolver problemas....256
Iniciar uma sessão de rastreamento de transação....258
Examinar componentes individuais e dados de rastreamento....259
Diagnosticar problemas de carregamento do recurso....265
Diagnosticar problemas de desempenho do sistema....269
Detectar e analisar erros e paralisações....270
Analisar instantâneos de erro e paralisação....274
Coletar e analisar rastreamentos de transações....278
Analisar rastreamentos e colaborar na análise de problemas....291
Monitorar o desempenho e os eventos do navegador....291
Acessar e compreender a estação de trabalho....300
Visão geral da Estação de trabalho....302
Fazer triagem com a estação de trabalho....306
Guia Navegador de métricas....308
Usar o Rastreador de transações....322
Monitorar com estação de trabalho....342
Diagnosticar o problema com a guia Navegador de métricas....342
Ler e compreender as notificações....344
Compreendendo o desempenho nominal....345
Usar a estação de trabalho....347
Navegando entre painéis no Console....347
Dados históricos e dinâmicos no console da estação de trabalho....353
Métricas do DX APM....356
Métricas BlamePoint....358
Métricas JMX....366

Métricas de transação....368
Sustentabilidade do agente.... 377
Métricas relacionadas à memória....382
Métricas de suportabilidade do agrupamento.... 386
Métricas de suportabilidade da triagem assistida.... 395
Principais métricas de suportabilidade.... 396
Monitoramento do desempenho do CA APM usando métricas de suportabilidade.... 398
Istio Support.... 409
Painéis DX.... 423
Solução de problemas....425
Solução de problemas do agente.... 425
O agente foi iniciado, mas não está visível.... 425
O agente não detecta automaticamente um back-end conhecido....428
O agente que está monitorando um front-end não detecta o back-end automaticamente.... 428
O agente aciona ClassNotFoundException ao carregar extensões dinâmicas....429
Os rastreamentos de transação do agente do navegador e do agente do .NET não são correlacionados.... 429
Valor do URL de ConfigurationServer falha ao ser preenchido....429
O cabeçalho do cookie de resposta do agente do navegador para .NET está sendo decorado?.... 430
Falhas do agente do Java....430
Erro de estouro de pilha do agente do Java.... 431
Sem métricas do .NET depois de ativar a injeção automática de snippet do Agente do navegador para .NET.... 432
Sem detecção automática de back-end devido ao erro insperado de carregamento de extensão....432
Aumento em contagens de métricas....432
Não é possível instrumentar um aplicativo com o DX APM.... 433
O agrupamento de URLs não está funcionando....433
O buildpack do Java no Cloud Foundry não consegue encontrar a versão solicitada do agente Java.... 433
Solução de problemas da caixa de diálogo de download do agente....434
Solução de problemas do DX APM....435
As métricas de componentes não são exibidas....435
A variação de análise diferencial não aparece nos nós.... 435
Não há dados de métrica na Exibição da experiência....435
Dados enviados pelos agentes no mapa estão incompletos ou ausentes.... 436
O mapa não exibe corretamente as informações do agente....437
O mapa mostra apenas 50.000 nós....437
Seletor de atributo do Cartão de experiência não mostra os atributos relacionados ao Docker....437
A propagação de atributo entre camadas não funciona.... 438
Onde procurar possíveis problemas relacionados a mapas.... 438
Solução de problemas de transação.... 438
Um método que nunca sai é identificado como método pai....438
Solução de problemas de estação de trabalho....439

Erro na estação de trabalho ao coletar o novo despejo de segmento.... 439
Alterar os tipos de operação nas calculadoras do Módulo de gerenciamento....440
Painéis têm painéis vazios.... 440
Nenhum resultado de eventos históricos de consulta....440
Solucionar problemas de tempo limite de sessão automática em estação de trabalho....441
Expiração da estação de trabalho durante logon no Gerenciador corporativo.... 441
Referência a APIs....442
API do APM Command Center.... 442
Mensagens de erro da API....447
Recurso do agente....449
Recurso agentUpdateTask....452
Recurso diagnosticReport....453
Recurso diagnosticReportTask....454
Recurso de controlador....455
Mensagens de erro....456
Propriedades pesquisáveis.... 462
Pesquisar usando a linguagem de consulta do Command Center....464
Recurso agentFileOperationTask....469
Recurso de arquivo....470
Recurso de pacote....471
Recurso do componente....473
Recurso agentPackageTask....474
API de hipermídia do DX APM.... 475
Autenticação e autorização da API.... 476
Acessando recursos....477
Recursos de pesquisa e filtragem.... 482
Criando e atualizando recursos....486
Cabeçalhos HTTP comuns....487
Mensagens e códigos de erro....488
API REST do DX APM....490
API de aplicativo.... 494
Regra de atributo.... 498
Gráfico.... 502
Vértice do gráfico....505
Incremental do gráfico.... 511
ID do vértice de gráfico.... 514
Vertexstatus incremental do gráfico....515
Recurso raiz.... 517
Universo....518
Vértice....519

ID do vértice....522
Exemplo da API REST do Java para obter atualizações incrementais.... 524
API REST do SQL....532
API REST do Team Center.... 549
API REST de consulta de métricas....562
Usar URLs públicos abreviados no DX APM....576
Suporte internacional.... 578
Recursos de acessibilidade do produto.... 579
Dados de uso (Telemetria)....582
Aviso legal da documentação.... 586

Requisitos de rede do DX SaaS

A infraestrutura do DX SaaS foi atualizada para aumentar a confiabilidade com o tempo mínimo de inatividade para janelas de manutenção. Essa otimização exige atualizações obrigatórias da configuração da rede para suas políticas de firewall a fim de evitar interrupções na segurança relacionada à rede.A comunicação de entrada (por exemplo, webhook) e de saída (por exemplo, agentes, logs, alarmes, RESTMon) é afetada. Os endereços IP do hardware novo deverão ser permitidos em sua implementação quando o hardware novo for ativado. A falha em permitir a comunicação com os novos endereços IP pode afetar a capacidade de ingerir dados de monitoramento e, dada a natureza de algumas tecnologias de monitoramento, isso pode afetar potencialmente o desempenho do sistema monitorado.

Entre em contato com o administrador da rede para garantir que os endereços IP a seguir sejam permitidos para os respectivos datacenters que estiver utilizando:

> **NOTE**
> Os endereços IP existentes devem permanecer permitidos simultaneamente até novo aviso de que esses endereços não estão mais em uso.

Datacenter dos EUA (https://axa.dxi-na1.saas.broadcom.com)

- Entrada:
  - 34.145.151.0/24
- Saída
  - 34.96.90.96/28
  - 34.150.194.136/29

Datacenter europeu (https://axa.dxi-eu1.saas.broadcom.com)

- Entrada:
  - 34.141.238.0/24
- Saída
  - 34.117.194.112/28
  - 34.141.162.16/29

Novidades no DX APM

Saiba mais sobre os novos recursos, aprimoramentos, problemas conhecidos e correções de defeitos relacionados a cada release do 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
- Notas da versão de 2021
- Notas da versão de 2020
- Notas da versão de 2019

24.9.1

Veja a seguir o novo recurso/aprimoramento do DX APM.

Janela de manutenção na UI do APM

Um ícone de Manutenção será exibido se uma página estiver em manutenção. O ícone Manutenção ficará visível por um período máximo de 7 dias antes de qualquer manutenção futura. Para obter mais informações, consulte Gerenciar dados de métrica usando módulos de gerenciamento.

24.4.1

Esta release se concentra apenas nos defeitos do cliente, além de outros vários defeitos internos.

> **NOTE**
> Como esta é uma release de patch, a UI do produto continuará refletindo a versão de release como 24.3.2.

Veja a seguir a lista de defeitos do cliente que foram corrigidos:

Defeito	Descrição
DE593238	O agente Windows do APMIA está conectado e as métricas são exibidas no APM, no entanto, o valor da métrica `ConnectionState` é 5.
DE597525	Gráfico de visualização de alertas - Quando o usuário clica no botão 'X' da Última Hora e dos Últimos 8 minutos, uma mensagem de erro é gerada na UI.

24.3.2

Veja a seguir os novos recursos e aprimoramentos do DX APM.

- Calculadora de conectividade do agente
- Resumo das contagens de agentes
- UI aprimorada do Módulo de gerenciamento
- Criar uma cópia do módulo de gerenciamento
- Iniciar uma sessão de rastreamento de transações na Exibição da métrica
- API de aplicativo para integração de aplicativos

Calculadora de conectividade do agente

A calculadora de conectividade do agente copia o status de conectividade do agente em um local fixo. Ela está desativada por padrão e precisa ser ativada pelo administrador. Para obter mais informações, consulte Calculadora de conectividade do agente.

Resumo das contagens de agentes

A calculadora também gera um pequeno resumo das contagens de agentes para cada ConnectionState em `Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Agents|Agent States` . Para obter mais informações, consulte Calculadora de conectividade do agente.

UI aprimorada do Módulo de gerenciamento

Agora, é possível atualizar o módulo de gerenciamento com a UI aprimorada. Para obter mais informações, consulte Atualizar um módulo de gerenciamento.

Criar uma cópia do módulo de gerenciamento

Agora, é possível criar uma cópia de um módulo de gerenciamento usando o botão Save as New na página Edit Management Module. Para obter mais informações, consulte Copiar um módulo de gerenciamento.

Iniciar uma sessão de rastreamento de transações na Exibição da métrica

Agora, é possível iniciar uma sessão de rastreamento de transação na página Exibição da métrica especificando os valores na caixa de diálogo Sessão de rastreamento de transação. Para obter mais informações, consulte Iniciar uma sessão de rastreamento de transação.

API de aplicativo para integração de aplicativos

A API de aplicativo é documentada por meio do OpenAPI versão 3. O documento do OpenAPI pode ser baixado de uma instalação do APM. Ele pode ser usado para gerar clientes para várias linguagens ou com alguns clientes `HTTP/REST` interativos. Para obter mais informações, consulte API do aplicativo.

23.12.1

Veja a seguir os novos recursos e aprimoramentos do DX APM.

URL direto para a exibição do grupo de métricas

A página de detalhes dos alarmes no DX Operational Intelligence e no email de notificação Alarmes agora está configurada com o link de exibição Métrica do APM. Esse link fornecerá uma exibição abrangente sobre o período em que o alerta foi disparado, juntamente com o status de outros alertas dentro do mesmo grupo de métricas. Também melhorará a visibilidade e facilitará a investigação, fornecendo uma compreensão mais ampla do comportamento das métricas contextuais durante o período observado. Para obter mais informações, consulte Todos os detalhes dos alarmes.

Despejo de segmento no Navegador de métricas

A seleção de um nó do agente na árvore do navegador de métricas agora exibe a guia **Despejos de segmento**. Essa guia permite coletar despejos de segmento Java (despejos de segmento) e exibir dados de despejo de segmento atuais e históricos. Um despejo de segmento fornece informações sobre todos os segmentos em execução dentro de uma JVM em determinado momento. Para obter mais informações, consulte Exibir uma métrica de agente na Exibição da métrica global.

Limitando o tempo de execução do script nas calculadoras de Javascript

As calculadoras de Javascript que processam os dados de métrica de entrada podem levar tempo e afetar o desempenho do Enterprise Manager no qual a extensão do Javascript é executada. Para proteger o Enterprise Manager contra sobrecarga, especifique o tempo limite do script na origem da extensão. Para obter mais informações, consulte Configurar extensões JavaScript.

> **NOTE**
> Agora, é possível remover as calculadoras de Javascript sem declarar novamente o Enterprise Manager. Também é possível definir o tempo limite para limitar o tempo de execução da calculadora de Javascript.

Subpropriedades para a integração do aplicativo

Agora, é possível selecionar **ADD PROFILE** e definir várias configurações da subpropriedade do agente. Por exemplo, um agente pode monitorar vários bancos de dados de modo que você possa adicionar vários conjuntos de propriedades de conexão do banco de dados. Para obter mais informações, consulte Criar aplicativos.

Criar variáveis na configuração de incorporação do painel

Agora, é possível criar variáveis diretamente na configuração de incorporação do painel. Para obter mais informações, consulte Incorporar painéis do DX na exibição da métrica.

Métricas de suportabilidade do Cloud Proxy

Novas métricas de suportabilidade foram adicionadas ao Cloud Proxy. Você pode usar essas métricas para identificar informações mais granulares sobre sua conexão do Cloud Proxy, como a conexão de rede, o uso da memória e assim por diante. Por exemplo, você pode usá-las para investigar quaisquer problemas de rede.

Para obter mais informações, consulte Métricas de suportabilidade do Cloud Proxy.

Novo estilo de interface do usuário

A interface de usuário completa do APM SaaS foi atualizada para utilizar a cor, a fonte e o estilo de ícone usado pela plataforma principal do DX. O tamanho da fonte foi aumentado em algumas áreas, o que pode reduzir um pouco o espaço de tela utilizável, mas aumentar o contraste e a legibilidade em alguns monitores. Alterar o navegador para 90% de zoom permitirá a restauração do espaço de tela utilizável sem reduzir a legibilidade em alguns monitores.

2023.9.1

Veja a seguir os novos recursos e aprimoramentos do DX APM.

- Exportar e importar módulos de gerenciamento
- Filtragem de referência de objeto nos módulos de gerenciamento
- ACC: interface de usuário unificada
- Problemas conhecidos

Exportar e importar módulos de gerenciamento

Agora, é possível exportar os Módulos de gerenciamento no formato de arquivo .jar e também importar os módulos de gerenciamento existentes como um arquivo .jar. Para obter mais informações, consulte Criar módulos de gerenciamento e trabalhar com eles.

Filtragem de referência de objeto nos módulos de gerenciamento

Agora, você pode clicar no valor de qualquer objeto na tabela Referências ao objeto, na página Módulo de gerenciamento. Você será redirecionado para a exibição filtrada da referência ao objeto selecionado e para o módulo de gerenciamento específico no qual você clicou. Para obter mais informações, consulte Criar módulos de gerenciamento e trabalhar com eles.

ACC: interface de usuário unificada

A interface de usuário do ACC foi reformulada para se unificar com a interface do usuário do Application Performance Management.

Problemas conhecidos

DE559435: a combinação de alertas como "Tudo" não está funcionando corretamente

Sintoma: quando a Combinação de alertas estiver definida como Tudo e o email de alerta estiver configurado, nesse caso, mesmo quando uma métrica violar o limite de várias métricas configuradas, o estado do alerta será alterado para Crítico e o email de alerta será enviado. Além disso, o estado do alerta será alterado para Normal e o email será enviado novamente.

2023.7.1

Veja a seguir os novos recursos e aprimoramentos do DX APM.

- Contagem dinâmica de métricas na árvore de métricas
- Painel ACC para ajustar o redimensionamento da janela do navegador
- URL direto para o grupo de métricas do alarme
- Criar painéis usando atributos capturados
- Universos do DX Operational Intelligence são preenchidos com universos do APM
- Painéis prontos para uso
- Otimizar o desempenho da rede e da CPU no Cloud Proxy

Contagem dinâmica de métricas na árvore de métricas

Se você selecionar um agente ou uma subpasta na árvore de métricas e estiver no modo dinâmico, marque a caixa de seleção **Somente métricas dinâmicas** para ver somente o número de métricas dinâmicas, ou seja, as métricas que o agente está relatando no momento. Para obter mais informações, consulte Exibir uma métrica de agente na Exibição da métrica global.

Painel ACC para ajustar o redimensionamento da janela do navegador

No ACC, agora é possível ajustar o painel de janelas para ver todas as configurações de pacotes com muitas atualizações.

URL direto para o grupo de métricas do alarme

Os detalhes do alarme no DX Operational Intelligence fornecem um arquivo JSON bruto no campo Alarm Attributes, a partir do qual é possível extrair o valor do link Grupo de métricas no APM. Esse link aponta diretamente para o grupo de

métricas configurado no APM, o que causou o alarme/evento. Para obter mais informações, consulte Todos os detalhes dos alarmes.

Criar painéis usando atributos capturados

Agora, é possível criar painéis nos Painéis do DX usando os atributos capturados no Business Payload Analyzer.

Nos Painéis do DX, crie o painel usando as seguintes informações:

- Fonte de dados: **AIOps_Metadata**
- Índice principal: **ao_aum_captured_data_2.0**
- Agrupar por: insira o atributo capturado no seguinte formato: **rr_data@<atributo_capturado>**

Para obter mais informações, consulte a documentação Painéis do DX.

Universos do DX Operational Intelligence são preenchidos com universos do APM

A lista suspensa **All My Universes** agora também preenche os universos do DX Operational Intelligence (exceto o universo All Access). Esses universos são marcados com um identificador OI com seu nome na lista suspensa.

Painéis prontos para uso

Esta release inclui os seguintes painéis prontos para uso do APM nos Painéis do DX. Esses painéis estão disponíveis na pasta APM-MetricView.

- APM: GC Monitor
- APM: GC Heap
- APM: EM Overview
- APM: APIM Embedded Dashboard

É necessário exibir esses painéis na Exibição da métrica do APM. Vá para a pasta na árvore e selecione para exibir o painel como uma guia. Clique na guia para exibir os dados no painel. Para obter mais informações, consulte APM-MetricView.

Otimizar o desempenho da rede e da CPU no Cloud Proxy

Agora, é possível usar `apm.server.compressionLevel` no arquivo application.yml para configurar o nível de compactação para a comunicação do WebSocket entre o Cloud Proxy e o Gateway. Para obter mais informações, consulte Cloud Proxy.

2023.5.1

Veja a seguir os novos recursos e aprimoramentos do DX APM.

- Aprimoramentos na integração de aplicativos
- Aprimoramentos/alterações em painéis incorporados
- Capacidade de pesquisa aprimorada na árvore da métrica
- Documentação do Cloud Proxy
- Defeitos conhecidos

Aprimoramentos na integração de aplicativos

Ao usar a integração de aplicativos ininterruptamente para integrar os aplicativos no DX APM e configurar os pacotes de agentes, agora é possível configurar as opções relacionadas ao sistema operacional selecionado. Para obter mais informações, consulte Integração de aplicativos para monitoramento.

Aprimoramentos/alterações em painéis incorporados

A partir desta release, os seguintes painéis do DX estão incorporados prontos para uso:

- Painel de diagnóstico
- Painel FrontendOverview

Esses painéis são pré-configurados. Na Exibição da métrica, esses painéis aparecerão como guias se você selecionar qualquer métrica que corresponda à condição.

Antes desta release, você tinha que importar e incorporar esses painéis manualmente na Exibição da métrica. Para obter mais informações, consulte Incorporar painéis do DX na exibição da métrica.

Capacidade de pesquisa aprimorada na árvore da métrica

Agora, os usuários podem marcar itens na árvore como favoritos. Um botão chamado Show favorites only foi incorporado à árvore da métrica. Esse botão permite que os usuários filtrem e exibam apenas os objetos marcados como favoritos. Para obter mais informações, consulte Pesquisar métricas na árvore de métricas.

Além disso, a barra de pesquisa detecta automaticamente quando a entrada está no formato de regex e executa uma pesquisa de maneira apropriada.

> **NOTE**
> A opção para utilizar expressões regulares foi eliminada.

Documentação do Cloud Proxy

A documentação do Cloud Proxy agora está disponível na documentação do APM SaaS. Consulte Cloud Proxy.

As informações da release sobre aprimoramentos anteriores do Cloud Proxy permanecerão parte da documentação dos agentes do APM.

Defeitos conhecidos

Veja a seguir o defeito conhecido desta release:

DE559435: a combinação de alertas como "Tudo" não está funcionando corretamente

Sintoma: durante a configuração de alertas, quando você define o valor de **Combinação** como **Tudo** e, se apenas um valor de métrica corresponder ao limite, um alerta será criado, e o status do alerta será transformado em Crítico e posteriormente mudará para normal. Devido a esse comportamento, se as notificações por email forem configuradas, vários emails de alerta serão enviados: primeiro para Risco/cuidado e depois quando o status ficar verde.

23.1

Saiba mais sobre os novos recursos e aprimoramentos do DX APM.

- Novos recursos
  - Integração simplificada de agentes
  - Especificador de métrica sem diferenciação de maiúsculas e minúsculas
  - Suprimir dados privados
  - Remoção do suporte ao idioma japonês
  - Incorporar painéis do DX na exibição da métrica
  - Opções Notificar por métrica individual e Notificação de alerta do disparador desativadas

Novos recursos

Saiba mais sobre os novos recursos e aprimoramentos do DX APM SaaS.

Integração simplificada de agentes

Você pode usar a integração de aplicativos para integrar os aplicativos no DX APM de maneira ininterrupta e configurar os pacotes de agentes facilmente para o seu ambiente. O assistente de integração de aplicativos guia você pela seleção das opções de monitoramento e cria pacotes de agentes. A integração de aplicativos contém os seguintes conceitos:

- **Aplicativo:** permite monitorar o aplicativo, que consiste em uma ou mais camadas.
- **Camada:** denota uma camada específica do aplicativo a ser monitorada. A camada faz referência a um ou mais pacotes de agentes criados com base na seleção de um usuário.

> **NOTE**
> Você ainda pode usar a ADD (caixa de diálogo Download do agente) e o ACC para adicionar aplicativos e configurar pacotes de agentes em seu ambiente.

Para obter mais informações, consulte Integração de aplicativos para monitoramento.

Especificador de métrica sem diferenciação de maiúsculas e minúsculas

Agora, é possível especificar o valor do especificador de métrica sem diferenciação de maiúsculas e minúsculas, especificando o valor do especificador de métrica entre (?i) e (?-i). Por exemplo,

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

Consulte Configurar agrupamentos de métricas no Team Center.

Suprimir dados privados

Agora, é possível definir as regras de supressão de rastreamento para identificar dados confidenciais dos usuários e substituí-los por um texto pré-configurado, como SUPRIMIDO PELO APM. Para obter mais informações, consulte Regras de supressão de rastreamento para ocultar dados confidenciais.

Remoção do suporte ao idioma japonês

A interface de usuário e a documentação do DX APM não são mais localizadas no idioma japonês. Consulte Suporte internacional.

Incorporar painéis do DX na exibição da métrica

Agora, é possível incorporar painéis do DX na exibição da métrica. Você pode incorporar

- **Painéis de métricas de diagnóstico e front-end:** os painéis do DX fornecem arquivos JSON para os painéis que podem ser importados. Depois que os painéis são importados, eles ficam disponíveis na exibição da métrica.
- **Painéis personalizados do DX:** crie um painel personalizado nos painéis do DX e, em seguida, mapeie-o usando o bloco **Painéis do DX** na página **Configurações** do DX APM.Uma vez incorporado, o painel é exibido na página Exibição da métrica.

Para obter mais informações, consulte Incorporar painéis do DX na exibição da métrica.

Opções Notificar por métrica individual e Notificação de alerta do disparador desativadas

O APM relata todas as alterações de estados de alerta para o serviço de alertas e, portanto, os botões Notificar por métrica individual e Notificação de alerta do disparador são redundantes. Portanto, as opções Notificar por métrica individual e Notificação de alerta do disparador foram removidas da página Criar/editar alerta. Para obter mais informações, consulte Criar e configurar alertas simples no Team Center.

Você pode gerenciar todas as notificações de alerta e configurar os detalhes da notificação de alerta do acionador em Políticas na Barra inicial. Consulte Criar política.

22.8

Alterações na documentação

A partir desta release, as informações relacionadas aos agentes serão desvinculadas da documentação do DX APM SaaS.As informações relacionadas aos agentes, que anteriormente estavam disponíveis na seção Implementando agentes, agora estão disponíveis em https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/dx-apm-agents/SaaS.html. Agora, a seção Implementando agentes terá um link que redireciona para a documentação dos agentes do DX APM.

> **NOTE**
> Quaisquer informações relacionadas ao agente que tenham sido marcadas no site anterior do DX APM SaaS não funcionarão. É recomendável criar outros marcadores para informações relacionadas ao agente no site de documentação dos agentes do DX APM. Pesquisar informações relacionadas ao agente por meio do Google fará com que sejam exibidos alguns dos links antigos que não funcionarão. Levará tempo até que o Google indexe a nova documentação do DX APM SaaS e dos agentes do DX APM. É recomendável usar a funcionalidade de pesquisa no site de documentação até que o Google indexe nosso conteúdo.

Criptografia de senha no arquivo de configuração da estação de trabalho

Ao configurar a estação de trabalho, agora é possível usar **transport.http.proxy.username** e **transport.http.proxy.password** para especificar os valores de autenticação, nos quais **transport.http.proxy.password** deve ser criptografado. Para obter mais informações, consulte Configurar a estação de trabalho com autenticação.

Regras de supressão de rastreamento

Agora, é possível definir as regras de supressão de rastreamento para identificar dados confidenciais dos usuários e substituí-los por um texto pré-configurado, como SUPRIMIDO PELO APM.Para obter mais informações, consulte Regras de supressão de rastreamento para ocultar dados confidenciais.

22.6

Aprimoramentos do Infrastructure Agent

Monitoramento do SNMP

SNMPMonitor é uma extensão do APM IA que ajuda a monitorar os dispositivos conectados à rede por meio do protocolo SNMP padrão do setor. Trata-se de uma extensão genérica que pode monitorar qualquer dispositivo ou agente ativado para SNMP. Para obter mais informações, consulte Monitoramento do SNMP.

Serviço CDN do Azure

O Monitor de rede de distribuição de conteúdo do Azure permite monitorar a capacidade de resposta da CDN do Azure ao usar aplicativos, como software de jogos, atualizações de firmware, IoT, aplicativos móveis, mídia de streaming e sites. Para obter mais informações, consulte Serviço CDN do Azure.

Monitoramento aprimorado do Kafka

Adição do seguinte suporte ao monitoramento do Kafka:

- **Suporte à autenticação SASL/PLAIN do agente do Kafka:** adição de suporte para autenticação SASL/PLAIN do agente do Kafka. Você pode ativar essa propriedade para conexões de cliente fornecendo o nome de usuário e a senha.
- **Multilocação do UMA:** adição de suporte para a instalação da equipe de multilocação do UMA. Use esse recurso para monitorar os namespaces.

Para obter mais informações, consulte UMA para monitor do Kafka e Monitoramento do Kafka.

Aprimoramentos do IBM MQ

O Infrastructure Agent do IBM MQ foi aprimorado para fornecer melhor suporte à escalabilidade e à filtragem. O agente pcf depreciado também foi removido. Veja a seguir a lista de outros aprimoramentos.

- Tipos de fila adicionados nas métricas para melhor compreensão
- Configuração de regex atualizada

Para obter mais informações, consulte Monitoramento do IBM WebSphere MQ.

Aprimoramentos do agente do .NET/.NET Core

Suporte ao .Net 6.0

O suporte ao .Net 6.0 foi adicionado a partir dessa release para monitorar o desempenho de aplicativos .Net 6.

Adição de suporte ao WebSocket e Websocket seguro para .NET

O suporte ao WebSocket e ao Websocket seguro foi adicionado para a conexão do agente do .NET com o Cloud Proxy.

Aprimoramentos do agente do Node.js

Os nomes de propriedade para os probes foram padronizados para ativar a implantação fácil do UMA.

Mais informações: Configurações do agente do Node.js

Aprimoramentos do Universal Monitoring Agent

- Adição de suporte para monitoramento e geração de relatórios de eventos de agrupamento.
  Mais informações: Configurar o monitoramento de eventos de agrupamento do UMA - Kubernetes e Configurar o monitoramento de eventos de agrupamento do UMA - OpenShift
- Monitoramento aprimorado do Prometheus com o UMA.
  Mais informações: Ingestão de dados do Prometheus
- Adição do painel Eventos aos painéis do DX no UMA.
  Mais informações: documentação dos Painéis do UMA

22.3

A seção lista os recursos novos, alterados e depreciados no DX APM (Application Performance Management) 22.3.

Suporte ao K8s 1.22 e OSE 4.9

O DX Application Performance Management agora oferece suporte ao Kubernetes 1.22 e ao OpenShift 4.9.

Aprimoramentos do agente do Nodejs

O agente do Nodejs apresenta os seguintes aprimoramentos:

Suporte do Redis para NodeJs

A partir dessa release, o DX Application Performance Management oferece suporte a chamadas de instrumentação do Redis com o probe node.js. O suporte do Redis para Node.Js permite que você visualize todo o ciclo de vida da transação, dos front-ends aos back-ends, de uma maneira estruturada, e monitore as operações de CRUD nos terminais. O probe ajuda a isolar e a fazer a triagem das ocorrências com aplicativos, bancos de dados ou infraestrutura mais rapidamente.Para obter mais informações, consulte Redis

Suporte à estrutura assíncrona para o agente do probe do NodeJs

O DXApplication Performance Management agora oferece suporte à estrutura assíncrona para o agente do probe do NodeJs. Essa estrutura permite correlacionar chamadas assíncronas de front-ends aos back-ends sob o nó Fragments. Para obter mais informações, consulte GraphQL

Suporte para correlação do agente do navegador do Nodejs

A partir dessa release, você pode visualizar a correlação de ponta a ponta do seu ambiente do navegador para o aplicativo Nodejs (módulo express js), bem como pode exibir os rastreamentos correlacionados e mapear para fazer a triagem de ocorrências mais rapidamente. Para obter mais informações, consulte Suporte do agente do navegador no Nodejs.

Aprimoramentos do agente do .NET

O agente do .NET apresenta os seguintes aprimoramentos:

Suporte para detectar e monitorar automaticamente paralisações com transações assíncronas do .Net

O DX Application Performance Management agora detecta e monitora automaticamente paralisações com os aplicativos assíncronos .net para fazer a triagem e diagnosticar problemas de desempenho de aplicativos.

Correlação aprimorada de rastreamento de ponta a ponta para aplicativos assíncronos do .Net

A visibilidade de rastreamento de ponta a ponta para transações assíncronas foi aprimorada. Esse recurso ajuda a solucionar problemas de transação.

Aprimoramentos do APM Infrastructure Agent

O APM Infrastructure Agent apresenta os seguintes aprimoramentos:

Suporte à multilocação Oracle na extensão de monitor Oracle DB no APMIA

O DX Application Performance Management agora oferece suporte à multilocação Oracle na extensão de monitor do Oracle DB. Esse recurso monitora o desempenho dos bancos de dados Oracle ativados com a opção de multilocação. Para obter mais informações, consulte Monitoramento do banco de dados Oracle.

VCAIM (vCenter Application Insight Modules)

O VCAIM (vCenter Application Insight Modules) fornece recursos para monitorar sistemas que estão sob controle do VMware vCenter Server. O VCAIM pode ser executado em qualquer sistema Windows em que o SystemEDGE esteja instalado. O VCAIM se comunica com o vCenter Server para monitorar todos os ESX Servers que o VMware vCenter Server associado gerencia.

Para obter mais informações, consulte vCenter Application Insight Modules.

Monitoramento do Azure Databricks

O monitoramento do Azure Databricks ajuda a monitorar o agrupamento independente do Spark e os agrupamentos do Azure Databricks. Ele ajuda no monitoramento de tarefas, estágios e tarefas de um aplicativo. Ele verifica a memória e o desempenho dos executores. O monitoramento do Azure Databricks pode ser usado para solução de problemas de desempenho e caracterização da carga de trabalho.

Para obter mais informações, consulte Implementar o monitoramento do Spark no Azure Databricks.

Monitoramento do Azure Active Directory

O monitoramento do Azure Active Directory ajuda a monitorar o Azure Active Directory usando os logs de auditoria. Os detalhes do log incluem várias métricas, como contagem de adição de grupos, contagem de adição de usuários, entre outras. Além disso, ele monitora vários atributos, como a ID de assinatura do Azure, a ID do inquilino do Azure, etc.

Para obter mais informações, consulte Monitoramento do Azure Active Directory.

Aprimoramento do APM Command Center

O APM Command Center apresenta os seguintes aprimoramentos:

Adição do link de integração do webhook

A integração de terceiros permite que você integre o ACC à sua infraestrutura (por exemplo, artefato) e entregue o pacote ACC usando a sua infraestrutura. O servidor de configuração do ACC fornece um link de integração do webhook que dispara um aplicativo que faz o download do pacote e o importa na sua infraestrutura. Para obter mais informações, consulte Configurar e baixar um pacote do agente.

Novos painéis do OOTB

Os painéis DX incluem os seguintes novos painéis:

Painéis PCF (Pivotal Cloud Foundry)

Os painéis PCF são uma nova categoria nos painéis DX APM. Essa categoria inclui os painéis a seguir que estão disponíveis na pasta Geral:

- Informações do aplicativo PCF
- Informações do PCF VM (BOSH)
- Informações da célula do PCF
- Informações de OrgSpace do PCF
- Visão geral do PCF

Para obter mais informações, consulte a seção Painéis do PCF.

Aprimoramentos de visualização e painéis do UMA

Os painéis UMA foram aprimorados para incluir o desempenho de aplicativos correlacionados. Os painéis correlacionados ajudam a determinar rapidamente o impacto do desempenho dos recipientes sobre o desempenho do aplicativo. Para ver a lista de aprimoramentos, consulte Aprimoramentos no painel.

Defeitos corrigidos

Os seguintes problemas foram corrigidos nessa release:

Defeito DE539968: **introscope.agent.acc.controller.configurationServer.url falha ao buscar os detalhes do Cloud Proxy correto**

Solução: O URL do Cloud Proxy no assistente de configuração do pacote introscope.agent.acc.controller.configurationServer.url (URL do configserver) e agentManager.url (URL do EM) não é mais visivelmente sincronizado na UI do ACC. Qualquer valor fornecido será considerado, e os valores padrão estão disponíveis no pacote baixado.

> **NOTE**
> Não é possível derivar o valor para a propriedade introscope.agent.acc.controller.configurationServer.url quando um único URL Isengard (host:porta) é fornecido para o URL do Cloud Proxy. Nesse caso, a propriedade será deixada em branco.

Defeito DE526430 – após upgrade para a release 2022.1.0.25, os usuários existentes não aparecem na página Usuários e permissões.

Sintoma: fiz upgrade para o Enterprise Manager 2022.1.0.25 e os usuários existentes não são disponibilizados na página Usuários e permissões.

Solução: efetue logon no Enterprise Manager após o upgrade e exiba os usuários existentes.

Defeito DE52234 – as perspectivas não mudam para o padrão quando alternadas entre camadas na página de exibição do mapeamento

Sintoma: criei três perspectivas para cada camada na página Mapeamento e as defini como as perspectivas padrão para cada camada. Quando você alterna entre as perspectivas na página Mapeamento, a perspectiva não muda.

Defeito DE526577: a ferramenta Importação de agentes importou a compilação mais antiga do Agente 10.7

Sintoma: eu importei o agente conectado válido 10.7 usando a ferramenta Importação de agentes e verifiquei que a página ACC mostra o pacote importado da compilação mais antiga.

Solução: como uma solução alternativa, use `-v<versão-pacote>` da ferramenta import-agent.

Defeito DE525374: os pacotes incorretos são exibidos ao alternar o pacote para o Infrastructure Agent na UI do ACC

Sintoma: embora eu estivesse alternando pacotes do Infrastructure Agent na UI do ACC, clicar no link exibia a lista de pacotes que não podem ser aplicados a partir da UI do ACC.

22.1

A seção lista os recursos novos, alterados e depreciados no DX APM (Application Performance Management) 22.1.

Aprimoramentos do agente do Java

Suporte para métricas do monitor da plataforma OOB por meio do JMX

Adição de suporte para métricas de monitoramento da plataforma OOB por meio do JMX.

Aprimoramentos do agente do Nodejs

Suporte à correlação do Oracle DB para o agente do Nodejs

Adição de suporte ao Oracle DB como um banco de dados de back-end para aplicativos Nodejs. O suporte aprimorado ao banco de dados de back-end ajuda a detectar componentes de downstream, enriquecendo a topologia, a análise de serviços e a análise de causa raiz. Para obter mais informações, consulte Agente do Nodejs.

Suporte ao agente do navegador no Nodejs

O suporte ao agente do navegador em aplicativos Nodejs correlaciona eventos de versão de navegador e aplicativos Nodejs, além de calcular o desempenho do navegador quando solicitações de aplicativos Nodejs são processadas nele. HTTP é o módulo principal que processa solicitações de navegadores no Nodejs. Para a comunicação em versão de navegador, todos os módulos de front-end interagem com esse módulo. Para obter mais informações, consulte Suporte do agente do navegador no Nodejs.

Aprimoramentos do agente de PHP

Suporte para correlação do agente do navegador e do agente do PHP

A partir dessa release, você pode visualizar a correlação de ponta a ponta do seu ambiente, do navegador ao aplicativo PHP. Também é possível exibir os rastreamentos correlacionados e mapear para fazer a triagem de ocorrências mais rapidamente. Para obter mais informações, consulte Injeção de snippet do agente do navegador usando o agente do PHP.

Aprimoramentos do Infrastructure Agent

Suporte para ingestão de rastreamentos do AWS X-Ray para AWS Lambda no DX Application Performance Management

- O monitoramento do AWS X-Ray ajuda a monitorar os aplicativos que são executados na nuvem do AWS. Esse recurso ajuda a monitorar a integridade e o desempenho da infraestrutura do AWS.
- O suporte para criação e uso de vários perfis ou contas agora foi introduzido para o monitoramento do AWS.

Para obter mais informações, consulte AWS X-Ray

Fornecer extensão de monitoramento de infraestrutura para IBM App Connect Enterprise v12

A partir dessa release, o DX Application Performance Management oferece suporte ao monitoramento do IBM App Connect Enterprise v11 e versões superiores (IBM ACE), o sucessor do IBM Integration Bus v10 (IIB). A adição do IBM App Connect Enterprise v11 enriqueceu as plataformas de middleware suportadas no DX Application Performance Management. Usando o IIB Monitoring Agent, os usuários do APM agora podem monitorar a disponibilidade, a integridade e o desempenho do IBM ACE.Para obter mais informações, consulte Monitoramento do IIB.

Aprimoramentos do Universal Monitoring Agent

Aprimoramento no monitoramento do k8s

O aprimoramento do monitoramento do k8s fornece insights sobre o desempenho de outros agrupamentos e rede. As seguintes métricas foram adicionadas aos dados de desempenho do pod:

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

Para obter mais informações, consulte Dados de métricas do pod.

Aprimoramentos do UMA

Acesso/privilégios de segurança para implementação do UMA

Você pode adicionar os privilégios de segurança à implementação do UMA, começando com essa release.

Solução de problemas avançada do UMA

Ferramentas e aprimoramentos do UMA para gerenciar melhor as implementações do UMA.

Suporte para versões mais recentes do recipiente do AKS/EKS/GKE

A partir dessa release, o UMA é suportado nas versões mais recentes dos recipientes a seguir para gerenciar o desempenho dos ambientes do recipiente.

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

Suporte para o tools.jar do JDK personalizado no Auto Attach do Java

O suporte ao tool.jar do jdk personalizado foi adicionado para o UMA para Kubernetes e o UMA para OpenShift. Com essa funcionalidade, você pode permitir a anexação a todos os JVMs para anexo automático. Para obter mais informações, consulte Instalar e configurar o UMA para Kubernetes e Instalar e configurar o UMA para OpenShift.

Suporte ao Red Hat OpenJDK para anexo automático

A partir dessa release, o UMA oferece suporte ao Red Hat OpenJDK para anexo automático, o que permite a você monitorar o desempenho de aplicativos em recipiente com base no JVM do Red Hat.

Aprimoramentos de design de anexo automático do UMA para NodeJS

O UMA oferece suporte à descoberta automática de aplicativos Nodejs na lista branca, começando nessa release. POR PADRÃO, o monitor do recipiente de aplicativos do UMA (pod Daemon Set) é executado no modo de lista branca, que detecta automaticamente e anexa os aplicativos Nodejs na lista branca.

Certificar os comandos pm2 e Forever Start para anexo automático do UMA para NodeJs

O UMA oferece suporte ao monitoramento e ao anexo automático de aplicativos Nodejs usando os comandos pm2 e Forever start no ambiente do Kubernetes, iniciando nessa release.

DX Application Performance Management - integração de mainframe

Suporte ao Sysview DB2

A partir dessa release, o DX Application Performance Management melhorou a visibilidade das métricas de mainframe, oferecendo suporte ao monitoramento de desempenho do banco de dados IBM DB2. Agora os administradores podem monitorar os KPIs do banco de dados IBM DB2, bem como identificar e fazer a triagem das ocorrências sem dificuldades. Para obter mais informações, consulte Integração de mainframe do DX APM.

Pacote Kafka com a extensão de mainframe

A partir dessa release, o DX Application Performance Management oferece suporte à extensão do agente do Kafka que gerencia o agente do Kafka e as instâncias do Zookeeper e sua integração.

Essa extensão também se integra ao mainframe para permitir a ingestão de registros do SMF publicados a partir de um produtor do Kafka, como o ZAB, em uma taxa alta na extensão do mainframe IA, evitando, assim, a latência da rede.

Para obter mais informações, consulte Extensão do agente do Kafka.

Adição do bloco de extensões JavaScript na página Configurações

A partir dessa release, um novo bloco **Extensão JavaScript** foi adicionada sob a seção **Configuração geral**. Esse recurso permite acesso ao gerenciamento de extensões JavaScript que podem processar as métricas de entrada antes de elas serem armazenadas no DX Application Performance Management. Dentro de uma extensão JavaScript, é possível executar cálculos, modificar caminhos de métrica, modificar nomes de métrica, copiar dados de métrica em novas métricas e executar operações JavaScript gerais em relação às métricas de entrada. Para obter mais informações, consulte Configurar extensões JavaScript.

Mudança na documentação

A partir dessa release, um novo **site de documentação dos Painéis DX - SaaS** está disponível como um site autônomo. Para obter mais informações, consulte *SaaS para painéis DX*

Problemas conhecidos

Defeito DE526430 – após upgrade para a release 2022.1.0.25, os usuários existentes não aparecem na página Usuários e permissões.

Sintoma: fiz upgrade para o Enterprise Manager 2022.1.0.25 e os usuários existentes não são disponibilizados na página Usuários e permissões.

Solução: efetue logon no Enterprise Manager após o upgrade e exiba os usuários existentes.

Defeito DE52234 – as perspectivas não mudam para o padrão quando alternadas entre camadas na página de exibição do mapeamento

Sintoma: criei três perspectivas para cada camada na página Mapeamento e as defini como as perspectivas padrão para cada camada. Quando você alterna entre as perspectivas na página Mapeamento, a perspectiva não muda.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE522903: a exibição de métricas gera um erro no navegador e no console do depurador

Sintoma: iniciei uma sessão de rastreamento de transações para um agente por meio do aplicativo WebView. Na página Exibição da métrica, fui até a guia Rastreamentos/Erro e nós de métricas das transações geradas de um agente e vi que um erro apareceu na página do navegador e no console do depurador.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE526577: a ferramenta Importação de agentes importou a compilação mais antiga do Agente 10.7

Sintoma: eu importei o agente conectado válido 10.7 usando a ferramenta Importação de agentes e verifiquei que a página ACC mostra o pacote importado da compilação mais antiga.

Solução: como uma solução alternativa, use `-v<versão-pacote>` da ferramenta import-agent.

Defeito DE525374: os pacotes incorretos são exibidos ao alternar o pacote para o Infrastructure Agent na UI do ACC

Sintoma: embora eu estivesse alternando pacotes do Infrastructure Agent na UI do ACC, clicar no link exibia a lista de pacotes que não podem ser aplicados a partir da UI do ACC.

Solução: não há nenhuma solução alternativa para esse problema.

Defeitos corrigidos

Os seguintes problemas foram corrigidos nessa release:

Defeito DE521544 - a lista suspensa de atributos Adicionar cartão de experiência não é exibida

Sintoma: efetuei logon em meu inquilino e acessei o DX Application Performance Management. Configurei meu agente do Java Tomcat e, em seguida, fiz meu aplicativo gerar algumas transações. Em **Exibição da experiência**, selecionei **Adicionar novo "+"**. Na página **Adicionar cartão de experiência**, na lista suspensa **Selecionar universo**, escolhi **Your applications**. Na lista com marcadores **use entire universe or apply a filter**, escolhi **Select agent from Application layer**. Em **Group by section**, quando selecionei a lista suspensa **Atributo**, a lista estava vazia. A lista não exibe atributos de camada. Esse problema ocorre apenas com os agentes do DX Application Performance Management 21.11.

Solução: marque a caixa de seleção **Incluir o nó da experiência** na página **Adicionar cartão de experiência**. Você pode ver a lista suspensa **Atributos**, mas somente para a camada **Aplicativo**, e não para outras camadas.

Defeito DE520944 - o APM Command Center exibe incorretamente a mensagem de erro após mudanças de configuração do pacote

Sintoma: usei a caixa de diálogo Download do agente para baixar um Infrastructure Agent. Acessei o APM Command Center para configurar o Infrastructure Agent e escolhi **pacotes** > **Configuração**. Editei o pacote e configurei uma mistura de propriedades dinâmicas e estáticas. Algumas propriedades exigem uma reinicialização de aplicativos gerenciados, e outras, não. Quando cliquei em **Alternar**, esta mensagem foi exibida:

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

Quando apliquei a nova versão do pacote ao agente, esta mensagem de erro foi exibida para todas as alterações de configuração estática e dinâmica do Infrastructure Agent:

```
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.
```

No entanto, o pacote ainda é exibido na lista de versões, e eu pude aplicar o novo pacote ao meu agente em execução.

Solução: você pode ignorar essas mensagens. Todas as funcionalidades relacionadas a pacotes funcionam adequadamente. As listas de pacotes exibem as versões corretas, e não há problemas na aplicação de novos pacotes nos agentes em execução.

Notas da versão de 2021

Esta seção contém as notas da versão de 2021.

- 21.11
- 21.6
- 21.4
- 21.1

21.11

Veja a seguir os recursos novos, alterados e depreciados no DX Application Performance Management (DX APM) 21.11.

Aprimoramentos de monitoramento na nuvem

Veja a seguir os aprimoramentos relacionados ao monitoramento da nuvem nesta release.

Google Cloud Monitoring

Monitoramento do Google Cloud Platform Firewall Insights

Agora, é possível monitorar a integridade e o desempenho do Firewall Insights, que fornece informações sobre o uso do firewall e problemas de configuração do firewall. O monitoramento do Firewall Insights oferece suporte à correlação entre os elementos da VPC (Virtual Private Cloud - Nuvem Privada Virtual), como Projeto, Região, Zona e Sub-redes. Essa correlação fornece métricas que proporcionam uma experiência de monitoramento holística. Você pode compreender melhor e otimizar com segurança as configurações do firewall. Também é possível revisar relatórios sobre o uso do firewall e o impacto de várias regras de firewall na sua rede da VPC. **Mais informações:** Monitoramento do Google Cloud Platform Firewall Insights

AWS (Amazon Web Services)

AWS Virtual Private Cloud Monitoring

Use o AWS Virtual Private Cloud Monitoring para visualizar seu AWS Cloud Platform VPC e como os componentes do seu VPC estão conectados. Examine as métricas para monitorar a integridade e o desempenho do VPC. Essa extensão ajuda a entender o contexto dos aplicativos que estão conectados ao seu VPC, fornecendo a correlação entre aplicativos, infraestrutura e rede. Monitore e analise os indicadores chave de desempenho do AWS Cloud Platform VPC. Esses indicadores incluem dados de entrada da origem, dados de saída para o destino, contagem de conexões ativas e alocação de porta de erro. **Mais informações:** Serviço AWS Virtual Private Cloud

AWS Transit Gateway Monitoring

O AWS Transit Gateway é um serviço que permite conectar seus AWS Cloud Platform VPCs e respectivas redes no local a um gateway.O AWS Transit Gateway Monitoring fornece dados sobre o desempenho e a integridade do seu AWS Transit Gateway. Essa extensão também correlaciona o gateway seu AWS Transit Gateway a outros componentes do VPC. O Transit Gateway Monitoring permite que você visualize e resolva problemas com métricas precisas de atividades de rede e fontes de tráfego. Essas métricas ajudam a otimizar as alocações de largura de banda, a garantir o planejamento adequado da capacidade, a resolver os problemas e a monitorar o consumo de largura de banda. **Mais informações:** Serviço AWS Transit Gateway

Amazon FSx Monitoring for Windows File Server

O Amazon FSx permite iniciar, executar e gerenciar sistemas de arquivos comerciais e de código aberto na nuvem AWS.O Amazon FSx Monitoring for Windows File Server detecta automaticamente esse serviço e executa periodicamente uma operação de sincronização. Você pode escolher as matrizes do DX APM a serem monitoradas usando a filtragem Básica e Avançada. É possível usar os atributos específicos do serviço Amazon FSx Monitoring for Windows File Server, como ipAddressm, tipo de ipAddress, ID do VPC e nome do host DNS. **Mais informações:** Serviço AWS FSx for Windows File Server

Agente do Java

Monitorar o desempenho de front-ends na experiência de agente do Java

O agente do Java agora rastreia o desempenho de front-ends da experiência durante as transações. Esse recurso permite usar a triagem assistida para determinar a causa raiz de problemas de desempenho do aplicativo. O agente do Java identifica gargalos de desempenho correlacionando anomalias do aplicativo da pilha de software em busca de desempenho insatisfatório e inaceitável da experiência. **Mais informações:** Front-ends da experiência do agente do Java

Monitoramento do Kafka aprimorado para usar SSL

A extensão do agente do Java Monitoramento do Kafka agora permite monitorar o Kafka usando o protocolo de segurança SSL (Secure Socket Layer). **Mais informações:** Monitoramento do Kafka

Monitorar serviços de aplicativo Azure Java

O agente do Java para serviços de aplicativos do Microsoft Azure permite que as empresas executem aplicativos Java no Microsoft Azure para identificar e resolver problemas de desempenho. O agente do Java para serviços de aplicativos do Microsoft Azure integra métricas de desempenho ao DX APM para análise inteligente, geração de alertas e visibilidade em um único painel. Você pode implementar essa extensão de site ao implementar um recipiente Tomcat no Azure. Após implementação do agente do Java para serviços de aplicativo do Microsoft Azure, é possível configurar as propriedades do agente usando as configurações do site do Azure.

Infrastructure Agent

Nova integração entre o DX APM e o Mainframe

Agora é possível monitorar o desempenho do seu ambiente de mainframe SYSVIEW usando a nova integração entre o DX APM e o Mainframe. Essa integração com base no DX APM Infrastructure Agent inclui painéis Grafana DX prontos para uso, métricas do SYSVIEW e CE APM (Cross-Enterprise APM), bem como alertas para as métricas do SYSVIEW. **Mais informações:** Integração entre o DX APM e o Mainframe

Novos SystemEDGE Data Collectors

O novo SystemEDGE Data Collector separa o SystemEDGE Core do monitoramento de host do Infrastructure Agent. No entanto, o DX APM continua oferecendo suporte a todos os casos de uso de monitoramento com base no SystemEDGE herdados e personalizados após a atualização para o Infrastructure Agent do APM SaaS 21.11. O SystemEDGE Data Collector permite continuar usando as principais bibliotecas do SystemEDGE. No futuro, as bibliotecas do SystemEDGE serão disponibilizadas apenas usando os SystemEDGE Data Collectors do Infrastructure Agent. Os SystemEDGE Data Collectors oferecem suporte ao SNMPv3, fornecendo privacidade e autenticação SNMPv aprimoradas.

O DX APM fornece dois SystemEDGE Data Collectors: o Standalone SystemEDGE Data Collector e o SystemEDGE Data Collector for Linux. O Standalone SystemEDGE Data Collector é suportado em AIX, Linux e Windows. O SystemEDGE Data Collector for Linux permite que você continue usando o monitoramento de host e aplique os benefícios de usar um SystemEDGE Data Collector. **Mais informações:** Coletor de dados SystemEDGE para Linux

Executar vários Infrastructure Agents no mesmo computador
Agora, é possível executar vários Infrastructure Agents em um computador para distribuir a carga de modo a ajudar a gerenciar o monitoramento de muitos componentes. É possível configurar o nome do serviço e as portas ao instalar o Infrastructure Agent para eliminar conflitos de vários agentes instalados no mesmo computador. **Mais informações:** Baixar e instalar o Infrastructure Agent no AIX, Linux e Solaris.

Balanceamento de carga do Infrastructure Agent para ambientes do Node.js
Agora, é possível equilibrar a carga de vários Infrastructure Agents para obter alta disponibilidade em ambientes complexos de recipiente e nuvem do Node.js. O UMA fornece comunicação HTTP entre o probe do Node.js e o agente do coletor de HTTP do UMA. Essa funcionalidade permite configurar o balanceamento de carga HTTP para gerenciar os Infrastructure Agents. O balanceador de carga fornece distribuição automática de tráfego dos agentes do Node.js para vários agentes do coletor de HTTP. Essa distribuição evita a sobrecarga em qualquer agente específico do Node.js. **Mais informações:** UMA para coletor de HTTP

Melhorias no monitoramento de log

O monitoramento de log agora lê os arquivos de log gerados recentemente após a configuração, sem precisar reiniciar o aplicativo gerenciado. É possível configurar nomes de arquivos de log usando expressões regulares (regex) para melhor correspondência de nomes. Agora, o monitoramento de log pode ler dinamicamente os arquivos de log que são criados diariamente ou com mais frequência. O DX APM agora pode ler erros de arquivos de log e criar os instantâneos de erro e a métrica Errors per Interval associada. O Team Center exibe os rastreamentos de transação de erro quando você seleciona um vértice do agente do Monitor de log. **Mais informações:** Monitoramento de log

Aprimoramentos de segurança do Infrastructure Agent

O Infrastructure Agent agora é suportado nas plataformas mais recentes e protocolos de segurança padrão do setor. Veja a seguir alguns exemplos: criptografia AES-256 de ponta a ponta; hash SHA-256; SNMPv3, sempre que aplicável; atualizado para VS 2017; e todas as senhas armazenadas nos arquivos de configuração são criptografadas sempre que aplicável. **Mais informações:** Coletor de dados independente do SystemEDGE, Monitoramento do host

O monitoramento do MongoDB agora oferece suporte a SSL
O monitoramento do MongoDB foi aprimorado para usar SSL para comunicações mais seguras entre o cliente do MongoDB e o Infrastructure Agent. **Mais informações:** Instalar e configurar o monitoramento do MongoDB.

Agente do .NET/.NET Core

Monitoramento aprimorado do agente do navegador

O monitoramento do agente do navegador para aplicativos .NET agora inclui uma decoração de resposta com base em cabeçalho HTTP por padrão. Nenhuma configuração do rastreador manual é necessária para obter correlação de rastreamento de transação do agente do navegador e correlação de sessões do DX AXA para o DX APM. **Mais informações:** *artigos do DX APM*: Configurar o agente do navegador para .NET/.NET Core, Configurar a injeção de snippet automática do agente do navegador para .NET/.NET Core, Configurar a decoração de resposta do agente do navegador para .NET/.NET Core *Artigos do coletor de experiência da CA*: Instalar o agente do .NET e configurar o agente do navegador, Configurar o agente do navegador para .NET, Propriedades do agente do navegador para .NET.

UMA (Universal Monitoring Agent)

Painéis DX para UMA

O UMA agora oferece painéis Grafana DX prontos para uso para apresentar dados de desempenho de seus ambientes Kubernetes. Esses painéis complementam os painéis da camada de infraestrutura do Team Center. Os

painéis do UMA oferecem suporte a todos os ambientes de recipiente, incluindo o Kubernetes, o OpenShift e o Docker (ECS). **Mais informações:** Universal Monitoring Agent, Painéis do UMA (Universal Monitoring Agent)

Monitoramento do desempenho do agrupamento do Kafka para UMA

Agora é possível monitorar o desempenho do agrupamento do Kafka usando o UMA. O UMA detecta automaticamente os pods ZooKeeper e os pods agente do Kafka usando anotações e as configurações da extensão de monitoramento do Kafka. Você pode configurar o SSL para os agentes do Kafka e o JMX por SSL.

Melhorias no monitoramento do Kubernetes

O UMA agora fornece insights mais detalhados sobre o monitoramento do Kubernetes, o que proporciona ainda mais desempenho da rede e dados de desempenho do agrupamento. Agora, é possível executar o monitoramento do Kubernetes na versão mais recente do Kubernetes. O monitoramento do kubernetes agora inclui suporte a volumes persistentes, fornecendo as novas métricas **%CPU/Memory utilization** e **%Disk Utilization by Pods**. Monitore o Kubernetes StatefulSets usando as novas métricas **%CPU/Memory utilization** e **%Disk Utilization by Pods**. As novas métricas também são exibidas nos painéis DX do UMA.

Suporte à multilocação do UMA

Agora, é possível implementar e usar o UMA em um ambiente de multilocação. **Mais informações:** Implementar o UMA em um ambiente de multilocação.

Gerenciar Universal Monitoring Agents usando o APM Command Center

Agora, é possível criar e implementar pacotes de UMA no APM Command Center. **Mais informações**: Implementar pacotes do UMA usando o APM Command Center

Aprimoramentos na interface do usuário

Exibir funções de universo no Team Center

Quando você usa a autenticação SSO, as funções que podem ser executadas podem variar para cada sessão, dependendo do IdP externo que é concedido e fornecido na resposta SAML. No painel **Barra inicial** > **Configurações** > **Usuários**, é possível ver suas funções específicas de universo e suas funções de inquilino (Usuário, Usuário avançado, Administrador de inquilinos). Agora, também é possível ver a função do perfil atual na tela superior direita da janela. **Mais informações:** no artigo Configurar universos, consulte a seção sobre **Configurar a segurança de universos**.

Novo ícone do Team Center para acessar a página de gerenciamento da calculadora de JavaScript

Como administrador de inquilinos, agora é possível clicar em um novo ícone para acessar a tela de **gerenciamento de calculadora de JavaScript**. Você pode definir a segurança da exibição de JavaScript nessa tela. **Mais informações:** Funções e privilégios suportados.

A caixa de diálogo Download do agente oferece suporte a propriedades de vários níveis

A caixa de diálogo Download do agente agora permite que você defina as propriedades que usam configurações de vários níveis. Por exemplo, a configuração do monitor de log usa um número variável de matchitems, pathPatterns e matchpatterns. Usando essa nova funcionalidade, você pode adicionar subpropriedades em subpropriedades ao fazer configurações na caixa de diálogo Download do agente.

Outros recursos

Visibilidade do banco de dados MongoDB e Redis para monitoramento de aplicativos do agente do Python

O agente do Python do DX APM agora fornece visibilidade aprimorada do banco de dados de back-end para seus aplicativos Python. Você pode monitorar os bancos de dados MongoDB e Redis para ajudar a detectar componentes de downstream, aprimorando a topologia com a análise de serviços e a análise de causa raiz. O Team Center exibe as métricas de desempenho para chamadas de back-end e os rastreamentos de transação correlacionados. **Mais informações:** Suporte ao MongoDB, Suporte ao Redis

Aprimoramento do plugin Jenkins do DX APM

Agora você tem a flexibilidade de configurar o plug-in Jenkins do DX APM no modo principal ou secundário, dependendo da configuração do Jenkins. **Mais informações:** Configurar o plug-in Jenkins do DX APM.

Plataformas e recursos recentemente suportados

Suporte do APM para o SiteMinder (CA APM para CA SSO) para AIX 7

Agora é possível monitorar o desempenho do APM SSO em execução no AIX 7. Agora, a rotação é agrupada com o agente web do APM para SSO para AIX, que também tem suporte para o AIX 7 de 64 bits. **Mais informações:** no artigo APM for SiteMinder 13.3.0, consulte a seção **Instalação e configuração no agente web (AIX)**.

Suporte e certificação do ambiente/plataforma do Infrastructure Agent

O Infrastructure Agent agora é suportado nas plataformas e nos protocolos de segurança padrão do setor mais recentes. Todas as funcionalidades do Infrastructure Agent são certificadas para trabalhar nestas plataformas e nestes ambientes: Windows 10, Windows 2019, Windows CORE 2019, RHEL 8.x, CentOS 8.x, SLES 15.x, OpenSuse 15 e Ubuntu 20.04. O SystemEDGE do Infrastructure Agent é suportado no servidor RHEL 8.x e Windows 2019. O monitoramento de host do Infrastructure Agent é suportado no Windows 2019. **Mais informações:** Monitoramento de host no Windows, Matriz de suportabilidade do Infrastructure Agent, Solução de problemas do monitoramento de host

CA APM 10.7 EPAgent suportado no DX APM SaaS

O DX APM permite continuar usando os scripts do CA APM 10.7x EPAgent Perl no DX APM SaaS. Você faz isso ao migrar seu CA APM 10.7 EPAgent para o DX APM SaaS. **Mais informações:** no artigo do Cloud Proxy, consulte a seção **Migrar agentes individuais para o DX APM usando o Cloud Proxy**.

Problemas conhecidos

Defeito DE521796 - duplicação de vértices de transações comerciais no mapa

Sintoma: baixei o agente do Java Tomcat do DX APM 21.11 com a extensão Agente do navegador do DX APM 21.11. Naveguei pelo DX APM e observei o mapa no Team Center. Para alguns vértices, o vértice da transação comercial do agente do navegador e as transações comerciais do agente do Java estão associados ao vértice de front-end. Esse problema ocorre apenas com os agentes do DX APM 21.11.

Solução: certifique-se de que as três propriedades estejam definidas como **false**:

- **introscope.agent.first.frontend.biz.enabled**
  Quando não há transações comerciais definidas externamente, essa propriedade permite que o agente do Java crie uma transação comercial padrão. O agente do Java identifica o primeiro front-end monitorado.

  - **Valores:** true/false
  - **Padrão:** true
  - **Exemplo:** introscope.agent.first.frontend.biz.enabled=true
  - **Observação:** não é necessário reiniciar o aplicativo monitorado.
- **introscope.agent.crossprocess.biz.enabled**
  Essa propriedade permite que o agente do Java encaminhe transações comerciais entre processos para agentes de downstream. Essa propriedade permite que o DX APM crie métricas de transação comercial entre processos para os agentes de downstream.
  - **Valores:** true/false
  - **Padrão:** true
  - **Exemplo:** introscope.agent.crossprocess.biz.enabled=true
  - **Observação:** não é necessário reiniciar o aplicativo monitorado.
- **introscope.agent.backend.biz.enabled**
  Essa propriedade permite que o agente do Java colete métricas de transação comercial para componentes de back-end.
  - **Valores:** true/false
  - **Padrão:** true
  - **Exemplo:** introscope.agent.backend.biz.enabled=true
  - **Observação:** não é necessário reiniciar o aplicativo monitorado.

Defeito DE521742 - anomalias não convertidas em problemas

Sintoma: eu queria monitorar aplicativos usando agentes do DX APM 21.11 sem que o agente do navegador fosse ativado. Percebi que as anomalias não estão sendo convertidas em problemas, mesmo quando meus nós de front-end têm alertas ativos. Os alertas ativos têm um estado de Risco ou Cuidado. Novos vértices de transação comercial foram criados pelo agente do DX APM 21.11. Esses vértices relatam as métricas de diagnóstico. As métricas de diagnóstico são exibidas sob o novo vértice de transação comercial, que são métricas correspondentes que o agente gera para o front-end.

Percebi que as anomalias foram convertidas em problemas somente quando os novos vértices de transação comercial tinham alertas ativos. Vejo métricas sob o nó de Frontend; no entanto, há métricas de transação comercial ausentes para as novas transações comerciais. As métricas ausentes são todas as métricas que não são de diagnóstico. Além disso, os alertas de front-end padrão não estão presentes sob o novo vértice de transação comercial. Esse problema ocorre apenas com os agentes do DX APM 21.11.

Solução: crie os alertas de front-end alterando o agrupamento de métricas para os alertas padrão. Inclua um novo regex de métricas de nós de segmento comercial ou crie alertas personalizados nas métricas de diagnóstico de transação comercial. O agente relata essas métricas no nó **Segmento comercial** do nó do agente. Não temos nenhuma solução alternativa para a criação de alertas personalizados que são gerados sob as métricas de não diagnóstico do nó de front-end.

Defeito DE521611 - erro de link de definição de alerta quando o nome do alerta contém o sinal de mais

Sintoma: criei um alerta e o nome contém o sinal de mais (**+**). O nome era semelhante a este nome: **cpu+Processor1**. Abri a página **Configurações** > **Alertas** > **Editar alertas** para testar o alerta. Abri o DX Operational Intelligence e fui para a página **Todos os alarmes** para testar a definição de alerta. Selecionei meu alerta **cpu+Processor1**. Na seção **Visão geral**, em **Atributos personalizados**, cliquei no link **Definição do alerta do APM > Definição do alerta**. No entanto, a página **Alerta** não pôde ser aberta. E, no DX APM, na página **Editar alertas**, esta mensagem de erro é exibida: `Error fetching alert`. O mesmo problema ocorre quando um nome de módulo de gerenciamento contém o sinal de adição.

Solução: não inclua o sinal de adição nos módulos de gerenciamento e de alertas do DX APM.

Defeito DE521571 - exceção ao baixar o componente do APM Command Center para execução do agente

Sintoma: quando eu estava tentando baixar um componente do APM Command Center para o meu agente do Java em execução, o agente gerou exceções semelhantes a esta mensagem:

```
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
```

Observação: esse problema ocorre apenas com determinadas versões do JDK, por exemplo, o Java 1.8u25.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE521544 - a lista suspensa de atributos de Adicionar cartão de experiência não é exibida

Sintoma: fiz logon em meu inquilino e acessei o DX APM. Configurei meu agente do Java Tomcat e, em seguida, fiz meu aplicativo gerar algumas transações. Em **Exibição da experiência**, selecionei **Adicionar novo "+"**. Na página **Adicionar cartão de experiência**, na lista suspensa **selecionar universo**, escolhi **Your applications**. Na lista com marcadores **use entire universe or apply a filter**, escolhi **Select agent from Application layer**. Em **Group by section**, quando selecionei a lista suspensa **Atributo**, a lista estava vazia. A lista não exibe atributos de camada. Esse problema ocorre apenas com os agentes do DX APM 21.11.

Solução: marque a caixa de seleção **Incluir o nó da experiência** na página **Adicionar cartão de experiência**. Você pode ver a lista suspensa **Atributos**, mas somente para a camada **Aplicativo**, e não para outras camadas.

Defeito DE520944 - o APM Command Center exibe incorretamente a mensagem de erro após mudanças de configuração do pacote

Sintoma: usei a caixa de diálogo Download do agente para baixar um Infrastructure Agent. Acessei o APM Command Center para configurar o Infrastructure Agent e escolhi **pacotes** > **Configuração**. Editei meu pacote e configurei uma mistura de propriedades dinâmicas e estáticas. Algumas propriedades exigem uma reinicialização do aplicativo gerenciado, e outras não. Quando cliquei em **Alternar**, esta mensagem foi exibida:

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

Quando apliquei a nova versão do pacote ao agente, esta mensagem de erro foi exibida para todas as alterações de configuração estática e dinâmica do Infrastructure Agent:

```
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.
```

No entanto, o pacote ainda é exibido na lista de versões, e eu pude aplicar o novo pacote ao meu agente em execução.

Solução: você pode ignorar essas mensagens. Todas as funcionalidades relacionadas a pacotes funcionam adequadamente. As listas de pacotes exibem as versões corretas, e não há problemas na aplicação de novos pacotes nos agentes em execução.

Defeito DE520499 - mensagem de erro de dados do conjunto de rastreamentos de transação no console do navegador e em notificações

Sintoma: fiz logon em meu inquilino e acessei o DX APM. Conectei meu agente do Java Tomcat e fiz meu aplicativo Java gerar alguns rastreamentos de transação. Na exibição **Métrica**, selecionei um nome de agente e cliquei na guia **Rastreamentos**. Alterei a hora de **Dinâmico** para várias horas históricas, por exemplo, 24 ou 6 horas, mantendo a guia **Rastreamentos** aberta. Após alguns minutos, esta exceção apareceu no console do navegador e nas notificações do navegador:

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

Essa mensagem também é exibida no rodapé do navegador e no console do depurador na exibição **Mapeamento** quando seleciono um vértice.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE519466 - o valor zero da métrica do tempo médio de resposta do MongoDB para o agente do Python está incorreto

Sintoma: quando o agente do Python está monitorando operações de leitura do MongoDB, o valor da métrica **Average Response Time (ms)** é zero quando o valor deve ser maior que zero.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE496868 - atualização - ADICIONAR configurações salvas: o pacote não está disponível após a atualização

Sintoma: efetuei logon no DX APM e fui até a caixa de diálogo Download do agente no Team Center. Anteriormente, eu tinha criado e salvo pacotes com as configurações de propriedade. Cliquei em **Configurações**, **Agente**, **Fazer download de agente**. Quando cliquei em **Configurações de pacote salvas**, somente os pacotes existentes do Infrastructure Agent estavam disponíveis. Os pacotes salvos para todos os meus outros agentes exibiram esta mensagem de erro: `Package is not available`. Os exemplos do agente são o Tomcat nos agentes do Windows e Linux e nos agentes do Java. A coluna **Ações** para esses agentes não exibe ícones. Portanto, não foi possível editar nem baixar esses pacotes não relacionados ao Infrastructure Agent.

Solução: não há nenhuma solução alternativa para esse problema.

21.6

Veja a seguir os recursos novos, alterados e obsoletos no DX APM 21.6.

Aprimoramentos de monitoramento na nuvem

Veja a seguir os aprimoramentos relacionados ao monitoramento da nuvem nesta release.

Google Cloud Monitoring

Serviço GCP Cloud VPN

O serviço GCP Cloud VPN (Virtual Private Network) permite monitorar a integridade e o desempenho do Google Cloud Platform Cloud VPN. Esse recurso ajuda a garantir que a sua infraestrutura na nuvem esteja sempre disponível e que atenda aos SLAs de tempo de atividade do seu cliente.

O Google VPN (Virtual Private Network) estabelece conexões seguras entre suas redes no local, escritórios remotos, dispositivos cliente e a rede global Google. Esse recurso permite que a sua organização migre sua hospedagem de VPN para a nuvem, melhorando, assim, o acesso a seus recursos com base na nuvem. **Mais informações:** Serviço Google VPN

AWS (Amazon Web Services)

AWS DMS (Database Migration Service)

Agora, monitore a integridade e o desempenho do serviço AWS Database Migration, que permite que você migre ininterruptamente vários componentes para os seus dados no AWS Cloud. Esses componentes incluem bancos de dados relacionais, data warehouses, bancos de dados NoSQL e outros tipos de armazenamento de dados. Você pode usar o AWS Database Migration Service para migrar os dados entre as instâncias locais (por meio de uma configuração do AWS Cloud) ou entre combinações de configurações na nuvem e no local. Esse serviço permite que você execute migrações casuais e replique as alterações contínuas para manter as origens e os destinos sincronizados. **Mais informações:** AWS Database Migration Service

Agente do Java

Registro em log aprimorado da propriedade do agente do Java

Agora, é possível examinar os logs do agente do Java para determinar o conjunto preciso de propriedades de configuração em uso e a origem dos valores de propriedade.

Suporte ao Java 13 e Java 14

O agente do Java agora oferece suporte às versões 13 e 14 do Java.

Suporte ao JBoss EAP 7.3

O agente do Java agora oferece suporte ao JBoss EAP versão 7.3.

Alteração padrão da filtragem automática de rastreamento de transação

A filtragem automática de rastreamento de transação não inclui mais as transações fastestn e slowestn na configuração padrão. Essas configurações podem gerar sobrecarga de recursos mais alta do que o normal para determinados aplicativos. Este é o padrão da propriedade atual no arquivo `introscopeagent.profile`:

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

Consulte Configurar a filtragem de rastreamento de transação para ativar a filtragem das transações fastestn e slowestn.

Mais informações: Configurar opções automáticas do rastreamento de transação

Infrastructure Agent

Monitoramento do banco de dados do IBM DB2

Agora é possível monitorar o desempenho do banco de dados do IBM DB2 em seu ambiente dinâmico. O monitoramento do banco de dados do IBM DB2 fornece visibilidade dos KPIs do banco de dados. Essas informações permitem isolar os problemas dos componentes do aplicativo e ajudam a resolver problemas rapidamente no ambiente dinâmico.

A extensão de monitoramento do banco de dados do IBM DB2 é um sistema de gerenciamento de banco de dados relacional pronto para a empresa. Criamos essa extensão para fornecer resiliência, desempenho e economia para suas cargas de trabalho transacionais. **Mais informações:** Monitoramento do banco de dados do IBM DB2

Extensão do IBM DataPower

A extensão do IBM DataPower é um gateway único multicanal que foi desenvolvido para fornecer segurança, controle e integração. Otimizamos essa extensão para acessar uma gama completa de cargas de trabalho de dispositivos móveis, web, API (Application Programming Interface - Interface de Programação de Aplicativos), SOA (Service-Oriented Architecture - Arquitetura Orientada a Serviços), B2B e nuvem. A extensão do IBM DataPower permite monitorar dados essenciais de desempenho sobre o gateway do DataPower. Você pode identificar de forma proativa os problemas de desempenho no ambiente e correlacionar rapidamente os dispositivos do DataPower aos aplicativos de back-end. **Mais informações:** Extensão do IBM DataPower

Monitoramento do vRealize Operations

Você pode monitorar, solucionar problemas e gerenciar a integridade e a capacidade do seu ambiente virtual aplicando a automação com base em política. O monitoramento do vRealize Operations oferece gerenciamento inteligente de operações com visibilidade do aplicativo ao armazenamento em infraestruturas físicas, virtuais e na nuvem. Essa extensão coleta dados de desempenho de cada objeto em cada nível do seu ambiente virtual. A extensão analisa os

dados para fornecer informações em tempo real sobre os problemas de desempenho. **Mais informações:** Extensão do vRealize Operations

Aprimoramentos de monitoramento do IIB (IBM Integration Bus)

Agora, é possível estabelecer a conexão de monitoramento do IIB usando o modo local ou remoto durante a configuração. Os requisitos de segurança definidos para monitorar um objeto MQ foram otimizados para fornecer um monitoramento mais seguro. **Mais informações:** Instalar e configurar a extensão de monitoramento do IIB, Métricas de monitoramento do IIB

Métricas de observabilidade do RESTmon

O Infrastructure Agent foi aprimorado para oferecer suporte às métricas de observabilidade do RESTmon. Você pode usar essas métricas para monitorar automaticamente o desempenho de suas implementações de monitoramento na nuvem. Esse suporte fornece métricas sobre várias plataformas. Fornecemos métricas relacionadas ao endpoint do Amazon Web Services, métricas relacionadas ao monitoramento do Google Cloud Platform, métricas relacionadas ao Azure, entre outras. **Mais informações:** Métricas de observabilidade do RESTmon

Extensão de monitoramento do SiteMinder

O DX APM (Application Performance Management) para CA SSO (CA Single Sign-On) é um pacote de propósito especial do DX APM para monitorar o CA SiteMinder. A nova extensão de monitoramento do SiteMinder do DX APM inclui este pacote. O CA APM para CA SSO coleta periodicamente métricas do CA SSO e as envia ao DX APM Infrastructure Agent. A extensão de monitoramento do SiteMinder inclui vários painéis DX que fornecem insights de desempenho sobre servidores proxy e agentes web. **Mais informações:** Extensão de monitoramento do SiteMinder

Extensão de monitoramento do Elastic

A extensão de monitoramento do Elastic permite monitorar o desempenho do agrupamento de cluster, nós e índices do Elastic Search para identificar problemas no seu ambiente dinâmico. Agora, é possível filtrar as métricas e executar configurações de grupo usando a extensão do Infrastructure Agent para Elastic Search. **Mais informações:** Extensão de monitoramento do Elastic

Suporte ao monitoramento do banco de dados Oracle para Oracle 19C

A extensão do Infrastructure Agent para monitoramento de banco de dados Oracle agora oferece suporte ao banco de dados Oracle versão 19C. Mais informações: Monitoramento do banco de dados Oracle

Agente do .NET/.NET Core

Aprimoramentos de instrumentação inteligente

A instrumentação inteligente do .NET/.NET Core detecta automaticamente os front-ends e back-ends do .NET/.NET Core. Após a detecção, os rastreadores de front-end e back-end são adicionados a um arquivo PBD que o agente do .NET recarrega. Por padrão, os novos rastreadores estão desativados, no entanto, você pode configurá-los. Você também pode iniciar sessões de detecção usando uma sessão de rastreamento de transação. A instrumentação inteligente do .NET/.NET Core também inclui um disparador de CPU configurável que inicia uma sessão de detecção quando a CPU do usuário excede um limite. **Mais informações:** Configurar a instrumentação inteligente do .NET/.NET Core.

Suporte ao .NET 5

O agente do .NET/.NET Core agora oferece suporte ao .NET versão 5.

UMA (Universal Monitoring Agent)

Empacotar e baixar o UMA usando o APM Command Center

Agora, é possível criar um pacote do UMA com recursos de monitoramento específicos do UMA no APM Command Center. **Mais informações**: Implementar pacotes do UMA usando o APM Command Center.

Monitoramento do uso do disco do pod

Agora, é possível monitorar o uso do disco de pods configurados com volumes persistentes. **Mais informações**: Dados de desempenho do pod

Nomenclatura automática de agente do UMA em ambientes de recipiente

Agora, o UMA determina um nome de host do agente apropriado para os agentes em execução em ambientes do recipiente. Esse recurso inclui a nomenclatura automática do agente do Java no .NET/.NET Core; AutoAttach do UMA no Kubernetes, ECS, OpenShift, etc. **Mais informações**: Instalar e configurar o UMA para Kubernetes.

Suporte à multilocação do UMA

Agora, é possível usar o UMA em um ambiente de multilocação.

Recurso AutoAttach do UMA para o agente do probe do Node.js

Agora, você pode monitorar todos os seus aplicativos e a infraestrutura em execução no ambiente do Kubernetes com um único agente. O recurso AutoAttach quase sem toque ou configuração mínima de toque permite a facilidade de integração e detecção. O recurso AutoAttach oferece uma solução única para o gerenciamento e o monitoramento de aplicativos nativos de nuvem prontos para uso na nuvem híbrida. **Mais informações:** AutoAttach do agente do Node.js

Problema conhecido

Defeito DE504064 - pane da JVM no Windows com EXCEPTION_ACCESS_VIOLATION

Sintoma: em determinadas circunstâncias, a JVM pode executar um despejo de núcleo. Esse problema ocorre quando o DX APM está monitorando aplicativos assíncronos.

Solução: como solução alternativa, execute *uma* destas ações:

- Faça upgrade para o patch JVM mais recente.
  Normalmente, fazer upgrade resolve esse problema.
- Crie ou atualize um pacote que contenha o componente NoRedef apropriado para o seu ambiente.
  O componente NoRedef contém o arquivo `AgentNoRedefNoRetrans.jar` , que desativa a redefinição e retransformação da classe para evitar possíveis problemas de desempenho.
  Você pode escolher dentre estes componentes do NoRedef:
  - NoRedef para agente do Java
  - NoRedef para JBoss
  - NoRedef para soquetes
  - NoRedef para Tomcat
  - NoRedef para WebLogic
  - NoRedef para WebSphere

  Mais informações: Informações sobre o AgentRedef em Configurar o WebSphere Application Server; Implementar pacotes do agente usando o APM Command Center

21.4

Veja a seguir os recursos novos, alterados e obsoletos no DX APM 21.4.

Aprimoramentos de monitoramento na nuvem

Veja a seguir os aprimoramentos relacionados ao monitoramento da nuvem nesta release.

Google Cloud Monitoring

Serviço Google Cloud Billing

O serviço Google Cloud Billing fornece métricas sobre o custo do GCP (Google Cloud Platform), com dados gerados diariamente (configuráveis). Esse serviço fornece as informações necessárias para orçar o custo do GCP. Mais informações: Serviço Google Cloud Billing

Monitoramento do GCP com entrada sem chave

Esse serviço permite que você monitore os serviços do Google Cloud sem configurar os tokens de segurança. Em vez disso, o serviço de entrada sem chave usa a identidade de carga de trabalho do GKE (Google Kubernetes Engine) para fornecer as permissões corretas. **Mais informações:** Google Cloud Monitoring com entrada sem chave

AWS (Amazon Web Services)

Aprimoramento do serviço AWS EMR Monitoring

O serviço AWS EMR Monitoring agora oferece suporte a duas novas métricas. Essas métricas fornecem o status dos aplicativos em execução no cluster do AWS EMR:

- **State:** mostra o estado do cluster EMR.
- **Status Code:** especifica o motivo da falha do cluster (essa métrica está disponível somente para clusters encerrados).

Mais informações: Serviço AWS EMR Monitoring

Aprimoramento do serviço AWS Glue Service Monitoring

Uma nova métrica, Error Message, foi adicionada nesse serviço. Essa métrica exibe a mensagem de erro real para a falha da rotina Glue. **Mais informações:** Serviço AWS Glue

Serviço de cotas e uso de serviços do Azure

O novo serviço Cotas e uso de serviços do Azure ajuda você a ver o limite atual de uso e serviço dos recursos do Azure. Você pode exibir o uso e as cotas para esses provedores:

- Computação
- Armazenamento
- Network
- Solução Azure VMware by CloudSimple

Mais informações: Cotas e uso de serviços do Azure

Agente do Java

Filtragem automática de rastreamento de transação

O DX APM monitora todas as transações em seu ambiente. O DX APM coleta rastreamentos de transação em busca de problemas de desempenho, erros e paralisações. A filtragem automática do rastreamento de transação permite que você examine transações potencialmente problemáticas sem executar explicitamente rastreamentos de transação. Agora, o DX APM inclui configurações adicionais para rastreamentos de filtragem automática por N mais lentos, N mais rápidos, e assim por diante. **Mais informações:** Configurar opções automáticas do rastreamento de transação

Nomenclatura do agente do Java com reconhecimento de recipiente

Agora, o DX APM determina automaticamente um nome de host do agente apropriado para os agentes do Java nos ambientes do recipiente. O DX APM fornece a nomenclatura do agente do Java para as implementações nativas do Kubernetes no UMA (Universal Monitoring Agent) e implementações padrão do agente do Java fora do UMA. **Mais informações:** Nomenclatura do agente do Java, Instalar e configurar o UMA para Kubernetes. Consulte a seção sobre resolução de propriedade dinâmica do UMA.

Novo modo de inicialização do agente do Java

Agora é possível evitar a lentidão no tempo de inicialização do agente do Java configurando a propriedade do sistema `-Dcom.wily.introscope.agent.startup.mode=neo` para iniciar o agente do Java no modo Neo. Você pode adiar a inicialização do agente do Java configurando a propriedade do sistema `-Dcom.wily.introscope.agent.startup.delay`. **Mais informações:** Configurar o modo de inicialização

Infrastructure Agent

Suporte a rastreamentos do monitoramento de banco de dados do SQL Server

Agora, é possível exibir os rastreamentos de transação do banco de dados do SQL Server na **exibição do mapeamento** selecionando o nó do banco de dados do SQL Server correspondente e clicando na guia **Banco de dados**. Os rastreamentos de transação do banco de dados do SQL Server consistem em eventos com vários indicadores de desempenho para monitorar e manter o banco de dados do SQL Server. **Mais informações:** Rastreamentos do banco de dados do SQL Server

Novas métricas de utilização de CPU/memória heap

O monitoramento remoto do JMX agora fornece métricas sobre a memória heap usada para a alocação de objeto. Essas métricas são ativadas por padrão e são exibidas aqui na árvore de métricas: <infra-agent>|<jmx-metric-root-node>|JVM|Memory|HeapO monitoramento remoto do JMX agora também fornece métricas sobre a memória gerenciada pela JVM que é usada para armazenar classes e metadados carregados e para processamento interno. Essas métricas são ativadas por padrão e exibidas aqui na árvore de métricas: <infra-agent>|<jmx-metric-root-node>|JVM|Memory|Non HeapVocê também pode exibir essas novas métricas como métricas padrão JMX. **Mais informações**: Monitoramento remoto do JMX, Métricas JMX

Aprimoramento do monitoramento do F5 LTM

O monitoramento do F5 LTM agora permite, com uma única implementação do agente, o monitoramento de várias instâncias do F5. Para cada instância do F5, você deve configurar um perfil do F5. **Mais informações:** Monitoramento do F5 LTM

Suporte à autenticação de camada segura no monitoramento do Redis

A extensão de monitoramento do Redis agora oferece suporte ao monitoramento do Redis por SSL. Use essas propriedades para ativar o SSL no monitoramento do Redis:

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

Mais informações: Configurar a extensão de monitoramento do Redis

Aprimoramento do monitoramento de host
Monitore o desempenho de processos de host dedicados definindo argumentos de processo na configuração de monitoramento. **Mais informações:** Propriedades do monitoramento de host

Suporte ao RHEL 8.2 para monitoramento de host, SysEDGE

O RHEL 8.2 agora está certificado para monitoramento de host e SysEDGE. **Mais informações:** Matriz de suportabilidade do Infrastructure Agent

Suporte ao NGINX 1.19.X
O DX APM agora oferece suporte ao NGINX versão 1.19.0. **Mais informações:** Monitoramento do NGINX

Aprimoramento do monitoramento do vCenter
Agora, é possível monitorar a nova métrica **Resource Pool** com as outras métricas do vCenter em seu ambiente vCenter. Mais informações: Monitoramento do vCenter

Agente do .NET/.NET Core

Detecção automática de back-end

O agente do .NET/.NET Core agora detecta back-ends automaticamente sem exigir instrumentação manual ou personalizada. **Mais informações:** Instrumentação inteligente do agente do .NET/.NET Core

UMA (Universal Monitoring Agent)

Suporte para ECS e Docker Swarm

O Universal Monitoring Agent agora detecta e monitora automaticamente os recipientes e a infraestrutura de nós do AWS ECS e do Docker Swarm. **Mais informações:** UMA para AWS ECS; UMA para Docker Swarm

Monitoramento aprimorado do Kubernetes

O Universal Monitoring Agent agora fornece insights mais aprofundados a partir do monitoramento de Kubernetes ao oferecer esses novos recursos e métricas de monitoramento de desempenho de rede e de cluster:

- Métricas de rede: bytes que entram, bytes que saem, bytes enviados e bytes recebidos
- Monitora o servidor de API e o desempenho do etcd
- Monitora o desempenho das configurações de implementação
- Limites de CPU e memória por projeto

Recursos da UI

Visualização do agrupamento de métricas

A visualização da exibição da métrica mostra o modo de visualização dos grupos de métricas configurados. É possível exibir os dados de métricas relevantes que são plotados no gráfico. A janela Visualização mostra o gráfico de dados de métricas com base no **Especificador de agente** e no **Especificador de métrica** fornecidos no campo **Expressões**. Mais informações: Configurar agrupamentos de métricas no Team Center

Visualização de alertas

A visualização de alertas exibe o modo de visualização dos grupos de métricas configurados. É possível exibir os dados de métricas relevantes que são plotados no gráfico. A janela de visualização mostra o gráfico de dados de métricas com base no campo **Agrupamento de métricas**. **Mais informações:** Criar e configurar alertas simples no Team Center

Visualização de calculadoras

A visualização de calculadoras exibe o modo de visualização dos grupos de métricas configurados. É possível exibir os dados de métricas relevantes que são plotados no gráfico. A janela de visualização mostra o gráfico de dados de métricas com base no campo **Agrupamento de métricas**. **Mais informações:** Criar e editar calculadoras

Maior granularidade da segurança de universos

Agora, em cada universo, os usuários recebem direitos individuais por módulo de gerenciamento para editar alertas, calculadoras e grupos de métricas. Anteriormente, apenas os usuários atribuídos como o Usuário avançado ou o Administrador de inquilinos podiam modificar todos os alertas, calculadoras e grupos de métricas do módulo de gerenciamento. Agora, a função de Usuário avançado, os usuários e os grupos de usuários devem receber permissão para exibir ou criar alertas, calculadoras ou grupos de métricas em um módulo de gerenciamento. O Usuário avançado continua podendo iniciar manualmente as sessões de rastreamento de transação. **Mais informações:** Configurar universos.

Outros recursos

Mais segurança para a caixa de diálogo de download do agente, APM Command Center, Cloud Proxy

Os agentes do DX APM e os controladores ACC baixados agora são mais seguros. Veja a seguir os aprimoramentos:

- A validação do certificado de TLS (Transport Layer Security) do ACC (APM Command Center) foi aprimorada para as comunicações do agente e do controlador ACC. Agora, o DX APM valida o certificado e o nome do host para agentes novos e atualizados e controladores ACC que usam a conexão TLS.
- A validação do certificado TLS agora está ativada para todos os agentes que você baixa pela caixa de diálogo de download do agente.
- Agora, é possível especificar truststores personalizados para validação de TLS por inquilino e globalmente.
- Você pode atualizar os agentes existentes e os controladores ACC com um novo truststore personalizado.
- O Cloud Proxy agora vem configurado para usar o truststore padrão do Java para validação de certificado.

Problema conhecido

Defeito DE502703 - a propriedade introscope.agent.dotnet.monitorAppPools não funciona

Sintoma: Removi o comentário e configurei a propriedade `introscope.agent.dotnet.monitorAppPools` no arquivo `introscopeagent.profile` do .NET/.NET Core. Por exemplo, `introscope.agent.dotnet.monitorAppPools=”DefaultAppPool”` . Depois que reiniciei o servidor web do IIS, a propriedade não entrou em vigor.

Solução: No CA APM 10.7 e anterior, o valor configurado tinha que ser colocado entre aspas.
No DX APM SaaS e DX APM On-premise, o valor deve ser configurado *sem* aspas. Por exemplo, `introscope.agent.dotnet.monitorAppPools=DefaultAppPool` .

Defeito DE499817 - nenhum dado é exibido no mapa, no painel nem no bloco de notas de análise

Sintoma: Selecione a opção de perspectiva vazia (uma caixa cinza claro) na lista perspectivas. Quando essa perspectiva é exibida, o **Bloco de notas de análise da Exibição da experiência**, o painel e o mapa do DX APM não exibem nenhum dado.

Solução: Selecione uma perspectiva válida na lista perspectivas e, em seguida, atualize a página.

21.1

Veja a seguir os recursos novos, alterados e obsoletos no DX APM 21.1.

Veja a seguir os recursos novos, alterados e obsoletos no DX APM 21.1.

Aprimoramentos de monitoramento na nuvem

Nesta release, fizemos vários aprimoramentos que estão relacionados ao monitoramento na nuvem, incluindo estes que se seguem:

Nova camada de rede

O DX APM fornece uma nova camada de rede, que correlaciona componentes do aplicativo, elementos da infraestrutura e topologia de rede. Essa correlação ajuda a identificar se o gargalo de desempenho está em um aplicativo, na infraestrutura ou na rede. O mapeamento do DX APM agora inclui uma **camada de rede**. A camada de rede contém informações do Infrastructure Agent e suas extensões de nuvem. Essa camada mostra os elementos da nuvem, como VPC (Virtual Private Cloud - Nuvem Privada Virtual), roteadores, interconexões, sub-redes e outros elementos de VPCs da nuvem. **Mais informações:** Camadas do mapa

Google Cloud Monitoring

Habilite estes serviços de nuvem para exibir os componentes e as conexões na camada de rede:

- **Serviço Google Virtual Private Cloud**
  O Google VPC (Virtual Private Cloud) fornece funcionalidade de rede para instâncias de VM (Virtual Machine - Máquina Virtual) do Compute Engine, recipientes do GKE (Google Kubernetes Engine) e o ambiente flexível do App Engine. O serviço Google Virtual Private Cloud permite monitorar a integridade e o desempenho da rede. **Mais informações:** Virtual Private Cloud do Google Cloud
- **Serviço de roteadores do Google Cloud**
  O Google Cloud Router é um serviço que funciona por conexões do Cloud VPN ou Cloud Interconnect. O Cloud Router fornece roteamento dinâmico usando o protocolo BGP para suas redes de VPC (Virtual Private Cloud) do Google Cloud. Usando esse serviço, é possível monitorar a integridade e o desempenho dos roteadores de nuvem no Google Cloud Platform.**Mais informações:** Roteadores do Google Cloud
- **Serviço Google Cloud Interconnect**
  O serviço Google Cloud Interconnect permite monitorar a integridade e o desempenho do Google Cloud Interconnect no Google Cloud Platform. **Mais informações:** Google Cloud Interconnect

Aprimoramento do serviço Google Compute Engine

Agora, o Google Compute Engine oferece suporte às **métricas de espelhamento** e **métricas nat**. **Mais informações:** Serviço Google Compute Engine.

Amazon Web Services

Autenticação com base em função sem credenciais do AWS

A autenticação com base em função do AWS (Amazon Web Services) monitora contas do AWS sem exigir credenciais. Para usar a autenticação com base em função, crie uma política e função nas contas do AWS para monitorar o agente do AWS. **Mais informações:** Autenticação com base em função sem credenciais do AWS

Agente do Java

Extensão do Oracle Services Bus 12C

A extensão do Oracle Service Bus 12C (OSB12) monitora os detalhes da transação OSB, as métricas de desempenho e os insights de integridade profunda relatando informações completas sobre fluxos completos de solicitação. A extensão exibe todos os componentes do OSB em um fluxo. **Mais informações:** Extensão do Oracle Service Bus 12C

Infrastructure Agent

Monitoramento do vCenter certificado para o VMware vSphere versão 7

A extensão de monitoramento do vCenter agora oferece suporte ao VMware vSphere versão 7.0. **Mais informações:** Monitoramento do vCenter

Universal Monitoring Agent

Suporte ao Universal Monitoring Agent para o perfil do WebSphere Liberty

O Universal Monitoring Agent agora detecta e instrumenta automaticamente recipientes do WebSphere Liberty. **Mais informações**: WebSphere Liberty

Recursos da UI

Esta seção lista os recursos da UI novos e aprimorados.

Filtragem de mapa sem diferenciação de maiúsculas e minúsculas

O valor da filtragem de URL composto para consultar as exibições de **Mapa** e **Isolamento** agora não diferencia maiúsculas de minúsculas. Por exemplo, se você consultar o nome de host **GOOglE.Com**, o DX APM também consultará os valores de **google.com**.

Árvores de métrica filtradas por mapeamento

A nova opção **Filtrar a exibição de métricas por componentes de mapeamento** no editor **Universo** filtra árvores de métricas no Navegador de métricas por mapeamento. **Mais informações:** Configurar universos.

Fazer download do App Synthetic Monitor na caixa de diálogo de download do agente

Agora, você pode fazer download do pacote ASM (App Synthetic Monitor) na caixa de diálogo **Selecione o agente para download** do Infrastructure Agent.

Aprimoramentos na caixa de diálogo Selecione o agente para download

A caixa de diálogo **Selecione o agente para download** no site da caixa de diálogo de download do agente tem um novo layout para melhor diferenciação entre os agentes entregues pelo Infrastructure Agent e as extensões disponíveis.

APM Command Center

UI do APM Command Center em conformidade com o WCAG 2.0 AA

Agora, você pode usar tecnologias de auxílio para percorrer a UI do APM Command Center. O APM Command Center agora está em conformidade com os critérios do WCAG 2.0 AA.

Outros recursos

Calculadoras JavaScript persistentes

As calculadoras JavaScript agora oferecem suporte ao cálculo contínuo de métricas entre as reinicializações e atualizações do DX APM sem qualquer interação manual. As calculadoras agora são armazenadas em uma unidade persistente.

Painéis DX – adição de suporte para funções de agregação na API NASS

A linguagem de consulta NassQL fornece uma maneira flexível de consultar e processar dados de métrica no servidor. A linguagem de consulta NassQL é semelhante à linguagem SQL conhecida de bancos de dados relacionais. Você pode consultar os dados da métrica usando diversas funções. É possível usar a função FROM e agrupar dados usando as funções WINDOW e GROUP. Também é possível agregar e mapear usando funções. **Mais informações:** Referência de consulta a agregações de métrica.

Problema conhecido

DefeitoDE492513 - não é possível aplicar novo pacote aos agentes no APM Command Center

Sintoma: no APM Command Center, criei um pacote para um agente e executei algumas configurações durante a criação. Em seguida, atualizei o pacote. Quando fui aplicar o pacote aos meus agentes, nenhum agente estava listado. Portanto, não foi possível aplicar a versão atualizada do pacote aos meus agentes conectados.

Solução: use essa solução alternativa para instalar o agente com o pacote atualizado.

Siga estas etapas:

1. No APM Command Center, clique em **Pacotes** no painel de navegação esquerdo.
2. Selecione a versão atualizada do agente na lista **Pacotes**.
   As informações do agente são exibidas no painel central.
3. Na seção **Versão do pacote**, encontre a linha **Baixar pacote**.
4. Clique em **Fazer download do arquivo do pacote**.
   O DX APM faz download do pacote no seu computador.
5. Desinstale o agente antigo.
6. Instale o agente com a versão de pacote mais recente.

Notas da versão de 2020

Esta seção contém as notas da versão de 2020.

- 20.11
- 20.9
- 20.6
- 20.4
- 20.1

20.11

Veja a seguir os recursos novos, alterados e obsoletos no DX APM 20.11.

Aprimoramentos do monitoramento do Java

O agente do Java inclui estas alterações:

Monitoramento do Spring Cloud Gateway

A extensão do Spring Cloud Gateway é um gateway de API que fornece uma maneira simples, porém, eficaz de rotear as APIs. **Mais informações:** extensão do Spring Cloud Gateway.

Extensão do WebSphere Portal

A extensão do WebSphere Portal ajuda você a criar e gerenciar portais da web. É possível usar essa extensão para criar um portal, que é um conjunto de portlets. Cada portlet é recebe um espaço designado no portal. Você pode criar os portlets buscando dados em várias fontes e exibir dados sobre os portlets na **exibição de métricas**. **Mais informações:** extensão do WebSphere Portal.

Suporte ao MySQL versão 8.x

O Agente para SQL do Java agora monitora o desempenho das chamadas de back-end do banco de dados para o MySQL versão 8.x.

PostgreSQL EDB versão 4.2

O Agente para SQL do Java agora monitora o desempenho das chamadas de back-end do banco de dados para o PostgreSQL EDB versão 4.2.

Agente do Java aprimorado para monitoramento do WebSphere Application Server

Agora você pode usar o arquivo Agent.jar como o arquivo JAR para o WAS (WebSphere Application Server) versões 8 e superiores. Não é mais necessário configurar o arquivo `AgentNoRedefNoRetrans.jar` . **Mais informações**: WebSphere Application Server.

Mais segurança no agente do Java

Agora, é possível usar a propriedade `agentManager.tls.validateHostname` para aumentar a segurança do DX APM impedindo ataques man-in-the-middle potencialmente confiáveis. **Mais informações**: propriedades do agente do Java.

Aprimoramentos de rastreamento de transação do agente do Java

Agora, você pode usar estas duas propriedades para coletar e decorar rastreamentos automáticos de transações de prioridade do agente do Java. Os rastreamentos automáticos de prioridade são rastreamentos de transação que ativam outros recursos essenciais, como a detecção de topologia.

- introscope.agent.deep.automatic.trace.priority.clamp
  Essa propriedade limita o número de rastreamentos automáticos de transações de prioridade que o agente coleta por intervalo de um minuto.
- introscope.agent.deep.automatic.trace.detailed.reason
  Essa propriedade permite que os rastreamentos automáticos de transações sejam decorados com o motivo detalhado pelo qual o agente foi disparado para coletar o rastreamento. Caso contrário, os rastreamentos são decorados com um motivo resumido.

Mais informações: propriedades do agente do Java.

Aprimoramentos de monitoramento do agente do .NET

O agente do .NET inclui estas alterações:

Instrumentação inteligente do .NET/.NET Core

A instrumentação inteligente do .NET/.NET Core detecta e instrumenta front-ends do .NET/.NET Core sem exigir qualquer configuração. A instrumentação inteligente do .NET/.NET Core é ativada por padrão quando você inicia um rastreamento de transação. É possível configurar as propriedades para controlar o registro em log de pilhas de segmentos específicas e o local dos arquivos .pbd gerados. Ao detectar um novo front-end, o agente do .NET/.NET Core adiciona mais configuração ao `detected-frontends.pbd` . **Mais informações:** Configurar a instrumentação inteligente do .NET/.NET Core.

Aprimoramento da análise de causa raiz do desempenho da CPU do .NET/.NET Core

O agente do .NET/.NET Core relata duas novas métricas que fornecem mais informações sobre o desempenho da CPU relacionadas aos métodos do .NET. Essas métricas podem ajudar a determinar se um gargalo de desempenho se deve à execução do código do método ou à hora de E/S.

- Average User CPU Time (ms)
- Average System CPU Time (ms)

Mais informações: Diagnosticar problemas de desempenho do sistema.

Métricas de fragmento assíncrono e rastreamentos de transação de fragmento assíncrono para ASP.NET e ASP.NET Core

O agente do .NET/.NET Core agora monitora solicitações assíncronas nos aplicativos ASP.NET e ASP.NET Core. O navegador de métricas exibe as métricas de front-end sob os nós **Fragments** e **Called Fragments**. O agente também coleta rastreamentos de transação de fragmento. **Mais informações:** Fragmentos assíncronos de .NET/.NET Core.

Automatic Attribute Decoration para .NET/.NET Core

O Automatic Attribute Decoration está incluído no agente do NET/.NET Core para permitir que você adicione atributos personalizados do seu ambiente de agente aos vértices do Team Center. Com o Automatic Attribute Decoration, é possível controlar e preencher automaticamente todos os atributos para os vértices que o agente gerencia no seu ambiente. O mapa exibe os vértices, permitindo que você identifique o canal de comunicação entre vários vértices no ambiente. Os atributos adicionados permitem identificar e isolar com mais facilidade um vértice problemático, promovendo a mitigação e a resolução mais rápidas do problema. **Mais informações:** Automatic Attribute Decoration (agente do .NET/.NET Core).

Aprimoramentos de monitoramento na nuvem

O monitoramento na nuvem inclui estas alterações:

Google Cloud Monitoring

Monitoramento do Cloud Bigtable

O Google Cloud Bigtable ajuda a armazenar grandes quantidades de dados de chave única com latência baixa. O monitoramento do Cloud Bigtable inclui um nó estático que é chamado de **multi-region** do tipo **GCP Region**. Esse nó estático permite conectar as instâncias do GCP Bigtable às regiões aplicáveis. **Mais informações:** Google Cloud Bigtable.

Monitoramento do Google Memorystore para Memcached

O GCP Memorystore para Memcached é um serviço Memcached altamente dimensionável e totalmente gerenciado para o Google Cloud. Você pode monitorar o GCP Memorystore para Memcached usando as métricas de status, os atributos

e as métricas de nuvem. Para esse agente, é possível monitorar o grupo de métricas no nível de nó. **Mais informações**: Google Memorystore para monitoramento do Memcached.

Amazon Web Services

Monitoramento do AWS SageMaker

O AWS SageMaker permite treinar, criar e hospedar um modelo em um terminal disponível. É possível monitorar o desempenho do SageMaker usando a extensão de monitoramento do AWS. **Mais informações:** AWS SageMaker.

Monitoramento do AWS Athena

O Amazon Athena é um serviço de consulta interativo que facilita a análise de dados no Amazon S3 usando SQL padrão. Você pode monitorar as métricas no Cloud Watch e na API de serviço. Também é possível monitorar as métricas derivadas. O monitoramento do AWS Athena oferece suporte ao grupo de trabalho, o que ajuda a separar usuários, equipes, aplicativos ou cargas de trabalho. **Mais informações:** Serviço AWS Athena.

Monitoramento do AWS Step Functions

O AWS Step Functions é um serviço de orquestração sem servidor. Esse serviço permite combinar as funções do AWS Lambda e outros serviços AWS para criar aplicativos essenciais para os negócios por meio de um fluxo de trabalho visual. Ative esse serviço para ver as métricas do Step Functions. **Mais informações:** AWS Step Functions.

Suporte à detecção com base em marca dos serviços AWS

A filtragem com base em marca ajuda a monitorar instâncias apenas com marcas específicas para os seguintes serviços de monitoramento do AWS:

- Serviço de monitoramento do AWS EC2
- Serviço AWS CLB (Classic Load Balancer)
- Serviço AWS NLB (Network Load Balancer)
- Serviço AWS ALB (Application Load Balancer)
- Serviço AWS S3
- Serviço de monitoramento EBS do AWS
- Serviço do AWS Redshift

Mais informações: Filtragem com base em marca do AWS Inventory.

Aprimoramentos do monitoramento da infraestrutura

O Infrastructure Agent inclui estas alterações:

Monitoramento do Cassandra
O monitoramento do Cassandra é uma extensão do Infrastructure Agent que coleta e exibe as métricas de agrupamento do banco de dados do Apache Cassandra. **Mais informações:** Monitoramento do Cassandra.

Monitoramento do Vault

O monitoramento do Vault é uma extensão do Infrastructure Agent que permite monitorar o desempenho do servidor do Vault de diferentes bibliotecas e subsistemas. Essa extensão coleta várias métricas, incluindo de tempo de execução, núcleo, auditoria, back-end de armazenamento, controle de solicitações e mecanismo de segredos. **Mais informações:** Monitoramento do Vault

Suporte à extensão de rastreamento do IIB (IBM Integration Bus) dez

A extensão do IIB 10 ajuda a monitorar o desempenho dos fluxos de mensagens do IBM Integration Bus, gerando métricas e rastreamentos de transação. Você pode usar cppprobe e userexits, que são fornecidos pelo IIB, para interagir com fluxos de mensagens sem modificar o aplicativo existente. **Mais informações:** Extensão de rastreamento do IIB (IBM Integration Bus) 10.

Monitoramento aprimorado do Cloud Foundry

A extensão do Infrastructure Agent de monitoramento do Cloud Foundry relata novas métricas para que seja possível gerenciar melhor o desempenho da plataforma Pivotal Cloud Foundry. Por exemplo, o monitoramento do Cloud Foundry agora fornece as métricas Auctioneer e BBS LockHeld, métricas UAA (User Account and Authentication) e muito mais. **Mais informações**: Métricas de monitoramento do Cloud Foundry.

Monitoramento avançado de host para Windows

A extensão do Infrastructure Agent de monitoramento de host para Windows agora inclui todas as métricas de desempenho e integridade do SysEdge. **Mais informações**: Monitoramento de host para Windows

Automatic Attribute Decoration para Infrastructure Agent

O Automatic Attribute Decoration é uma extensão do Infrastructure Agent que permite adicionar atributos personalizados do ambiente de agente aos vértices do Team Center. Com o Automatic Attribute Decoration, é possível controlar e preencher automaticamente todos os atributos para os vértices que o agente gerencia no seu ambiente. O mapa exibe os vértices, permitindo que você identifique o canal de comunicação entre vários vértices no ambiente. Os atributos adicionados permitem identificar e isolar com mais facilidade um vértice problemático, promovendo a mitigação e a resolução mais rápidas do problema. **Mais informações:** Automatic Attribute Decoration para Infrastructure Agent.

Suporte à autenticação do Windows para monitoramento do servidor web do IIS

Agora, você pode configurar o monitor do servidor web do IIB usando a autenticação do Windows. **Mais informações:** Configurar o monitoramento do servidor web usando a autenticação do Windows.

Configurar acesso seguro para monitoramento do F5 LTM

A extensão do Infrastructure Agent de monitoramento do F5 LTM inclui a nova propriedade `introscope.agent.f5.tokenAuth` para executar autenticação com base em token. **Mais informações:** Configurar o monitoramento de LTM do F5.

Acesso ao Infrastructure Agent do usuário não raiz

Agora, os usuários não raiz podem instalar, iniciar e interromper o Infrastructure Agent. Alguns comandos do Infrastructure Agent mudaram. Esta tabela lista os comandos antigos e atualizados:

Comando antigo	Comando atualizado
force_start	console_start
force_stop	console_stop Esse comando também é adicionado para o Infrastructure Agent com base em UNIX.
apmia-ca-installer.sh / apmia-ca-installer.bat	APMIACtrl.sh / APMIACtrl.bat

Recursos do UMA

Esta seção lista os recursos novos e aprimorados do Universal Monitoring Agent.

Extensão UMA para o probe Python

Agora, o Universal Monitoring Agent para Kubernetes detecta e instrumenta automaticamente seus aplicativos Python sem exigir qualquer mudança manual na imagem do aplicativo. **Mais informações:** Extensão UMA para o probe Python.

Extensão UMA para o probe NGINX

Agora, o Universal Monitoring Agent para Kubernetes detecta e instrumenta automaticamente seus aplicativos NGNIX sem exigir qualquer mudança manual na imagem do aplicativo. **Mais informações:** Extensão UMA para o probe NGINX.

Zipkin Support

Agora, o DX APM coleta dados de extensão sobre aplicativos que são rastreados pelo Zipkin, um sistema de rastreamento distribuído. O Zipkin Support relata e exibe métricas de desempenho, erros e rastreamentos de transação. O Zipkin Support é uma extensão do Infrastructure Agent que fornece dados sobre front-ends HTTP, back-ends HTTP e back-ends de banco de dados. **Mais informações**: Zipkin Support.

Recursos do agente do Node.js

Esta seção lista os recursos novos e aprimorados do agente do Node.js.

Monitorar desempenho do tempo de execução do Node.js em implantações em recipiente

Agora, você pode instalar o Node.js como um agente autônomo sem o Python. **Mais informações:** arquivo Install the Node.js Probe Agent for CA Digital Experience Insights.dita.

Suporte do MS SQL para o agente do Node.js

O agente do Node.js agora oferece suporte a chamadas do banco de dados Microsoft SQL Server versões 2016 e 2017. **Mais informações**: Matriz de suportabilidade do agente do Node.js.

Recursos do agente do PHP

Agora, o DX APM oferece suporte à versão 7.4 do PHP. **Mais informações**: Matriz de suportabilidade do agente de PHP.

Recursos da UI

Esta seção lista os recursos da UI novos e aprimorados.

Aprimoramentos na criação e integração de universos

Na nova exibição **Universos**, os administradores podem conceder diferentes direitos aos usuários e grupos de usuários. Os direitos incluem o acesso ao universo e a filtragem das origens da métrica. A filtragem pode ter como base os domínios (acesso aos agentes) com atributos e expressões regulares, componentes de mapa e módulos de gerenciamento.

Além disso, o comportamento dos universos mudou, afetando a filtragem das origens da métrica. Devido à mudança, é necessário reconfigurar as origens da métrica do universo para que a filtragem correta do agente seja aplicada ao navegador de métricas. Por exemplo, digamos que o ambiente tenha dez agentes ativos. Antes dos aprimoramentos dos universos 20.11, você tinha quatro agentes listados em Universo X e em exibição no navegador de métricas. Após as mudanças do universo 20.11, o Universo X contém dez agentes e todos são exibidos no navegador de métricas. É preciso atualizar explicitamente as origens da métrica do universo para que os quatro agentes sejam listados no Universo X e exibidos no navegador de métricas novamente.

Mais informações: Configurar universos.

Agentes desconectados

Agora, você pode acessar dados de agentes desconectados. **Mais informações**: Monitorar valores de métrica do agente com a exibição da métrica.

Classificando atributos na janela Perspectiva

Agora, você pode arrastar e soltar atributos na janela **Perspectiva** para classificar ou reorganizar os atributos na hierarquia. A ordem de atributos define a ordem na qual os filtros são aplicados e, portanto, o agrupamento de vértices. **Mais informações**: Organizar componentes usando perspectivas.

Cores de status dos agentes

Agentes desconectados agora são exibidos em cinza. **Mais informações**: Monitorar valores de métrica do agente com a exibição da métrica.

Outros recursos

Exportar métricas na exibição da métrica

Agora, você pode exportar as métricas em **Exibição da métrica** para, por exemplo, combinar diferentes tipos de dados e criar gráficos no Excel. **Mais informações**: Monitorar valores de métrica do agente com a exibição da métrica.

Problemas conhecidos

Esta seção lista os problemas conhecidos da release atual.

Sintoma: efetuo logon em um inquilino com a locação ativada para SAML no Chrome. Quando efetuo logoff, sou conectado de volta.

Solução: esse problema ocorre quando se mantém a mesma locação. Esse comportamento é comum a aplicativos que são ativados para SSO, como o DX SaaS. Exemplos de outros aplicativos incluem MS Office 365, Box, SharePoint e Google.A solução é limpar o cache da locação ao efetuar logoff.

Defeito DE481045 - não é possível efetuar logoff do inquilino SAML do DX SaaS

Sintoma: efetuo logon em um inquilino com a locação ativada para SAML no Chrome. Quando efetuo logoff, sou conectado de volta.

Solução: esse problema ocorre quando se mantém a mesma locação. Esse comportamento é comum a aplicativos que são ativados para SSO, como o DX SaaS. Exemplos de outros aplicativos incluem MS Office 365, Box, SharePoint e Google.A solução é limpar o cache da locação ao efetuar logoff.

Veja a seguir as soluções alternativas:

Inicie uma nova sessão sem efetuar logoff.

- Abra uma janela anônima do navegador e inicie uma nova sessão.
- Abra outro navegador, como o FireFox, e inicie uma nova sessão.

Efetue logoff e logon novamente para iniciar uma nova sessão.

- Efetue logoff e, após alguns segundos, clique em **Sign in with another Tenant**.
- Efetue logoff manualmente de um inquilino excluindo o cookie **CA_CLOUD_Management**. Em seguida, efetue logon em outro inquilino.
- Feche o navegador e aguarde até atingir o tempo limite da sessão. Em seguida, efetue logon em outro inquilino.

Defeito DE481045 - dificuldade de alternar entre vários inquilinos SAML do DX SaaS

Sintoma: consigo acessar vários inquilinos SAML, no entanto, não consigo alternar facilmente entre eles.

Solução: o problema de alternância aparentemente é efeito colateral de um problema de logoff do DX SaaS. O DX SaaS não pode efetuar logoff de vários inquilinos que estão sendo acessados usando o mesmo navegador. Esse problema ocorre apenas quando o SAML é usado.

Use as mesmas soluções alternativas do problema anterior.

Defeito DE486199 - comportamento incorreto ao criar um universo ou ao salvar o filtro de mapa como um universo

Sintomas:

- Quando crio um universo, esses comportamentos indesejados ocorrem na página **Criar universo**:
  - Às vezes, os nomes e as descrições dos campos são preenchidos automaticamente com os dados de um universo existente. Quando clico em **Salvar**, a página é salva com as opções padrão (veja a seguir).
  - O padrão do botão de opções **Módulos de gerenciamento** de **Todos os itens** muda para **Itens selecionados** quando preencho os campos **Nome*** e **Descrição**. Quando clico em **Salvar**, a página é salva com as opções padrão (veja a seguir).
- Quando salvo o filtro de mapa como um universo, ocorrem estes comportamentos indesejados:
  - O botão de opções **Filtro do módulo de gerenciamento** é posicionado ao lado dos **Itens selecionados**, em vez de **Todos os itens**. Quando clico em **Salvar**, a página é salva com as opções padrão (veja a seguir).
  - Quando salvo o filtro de mapa como um universo, a configuração **incluir o nó da experiência** não é aplicada ao universo recentemente criado.

Veja a seguir as opções padrão para salvar um novo universo:

- Quando o universo é criado com o clique no botão **Novo universo**, a opção **Todos os itens** é selecionada em cada guia.
- Quando o universo é criado com o clique no botão **Salvar como universo** na página **Mapeamento**, um filtro é preenchido na guia **Componentes** de **Mapeamento**. Outras guias têm a opção **Todos os itens** selecionada.

Solução: esses problemas não têm uma solução alternativa.

20.9

Estes são recursos novos, alterados e obsoletos no DX APM 20.9.

Aprimoramentos do monitoramento do Java

O agente do Java inclui estas alterações:

Suporte à JMX do agente do Java reformulada

A extensão JMX do agente do Java aprimorada é empacotada e implantada como uma nova extensão do agente que oferece suporte às métricas Spring Boot e de micrômetro. Você pode configurar novas propriedades de JMX usando o APM Command Center ou, no arquivo `bundle.properties` da pasta `extensions/deploy`. A extensão aprimorada é suportada no Java 7 e superior. Para Java 6, continue usando as propriedades de JMX em `IntroscopeAgent.profile`.

Definições aprimoradas do grupo de URLs de front-end

Agora, o agente do Java normaliza automaticamente os segmentos dinâmicos de URLs para definições de URL de front-end mais significativas e úteis.

Detecção automática do nome de aplicativo Spring Boot

Agora, você pode configurar a extensão do agente do Java para monitoramento do Spring Boot para detectar automaticamente o nome de aplicativo Spring Boot.

O Agente para SQL oferece suporte ao Oracle 19.x

O Agente para SQL do Java agora oferece suporte ao monitoramento de bancos de dados do Oracle 19.x. **Mais informações:** Configurar monitoramento de SQL para Java.

Suporte ao Spring Boot Webflux 2.1.x e 2.2.x do agente do Java

O DX APM oferece suporte ao Spring Boot Webflux versões 2.1.x e 2.2.x. **Mais informações:** Monitoramento do aplicativo reativo Spring Boot.

Suporte ao Jetty Framework 8.x

Agora, o agente do Java oferece suporte ao Jetty Framework 8.x.

Aprimoramentos de monitoramento do agente do .NET

O agente do .NET inclui estas alterações:

Visibilidade aprimorada mais detalhada do desempenho do aplicativo .NET Core

O DX APM inclui automaticamente visibilidade mais detalhada dos aplicativos .NET Core que são executados em Linux, sem exigir qualquer instrumentação manual ou personalizada.

Aprimoramentos de monitoramento na nuvem

O monitoramento na nuvem inclui estas alterações:

Google Cloud Platform

Suporte ao serviço BigQuery do Google Cloud

O serviço BigQuery do Google Cloud permite visualizar o desempenho de consultas do BigQuery. **Mais informações:** Serviço BigQuery do Google Cloud.

- Suporte ao serviço Dataproc do Google

A extensão de monitoramento do Google Cloud Platform coleta métricas para o serviço Dataproc. **Mais informações:** Google Dataproc.

- Suporte ao serviço de balanceamento de carga do Google Cloud

A extensão de monitoramento do Google Cloud Platform coleta métricas para o serviço de balanceamento de carga. **Mais informações:** seção Serviço de balanceamento de carga do Google Cloud.

- Suporte ao serviço de escalação automática do Google Cloud

O Google Cloud Autoscaling ajuda você a controlar um aumento no tráfego e a reduzir custos quando a necessidade de recursos for menor. **Mais informações:** Escalação automática do Google Cloud.

Amazon Web Services

- Detecção automática com base em função para organizações AWS

Suporte à detecção automática com base em função para organizações Amazon Web Services. **Mais informações**: Configurar monitoramento da organização AWS

O AWS (Amazon Web Services) agora oferece suporte a estes serviços:

- Suporte ao serviço AWS EMR (Elastic Map Reduce)

O serviço de monitoramento do AWS EMR fornece a flexibilidade para executar casos de uso em agrupamentos efêmeros de finalidade única que são dimensionados automaticamente para atender à demanda, ou em agrupamentos de execução longa altamente disponíveis usando o novo modo de implementação com vários mestres. **Mais informações:** Serviço de monitoramento do AWS EMR.

- Suporte ao Serviço AWS Glue

O serviço AWS Glue detecta seus dados e armazena os metadados associados (por exemplo, definição e esquema de tabela) no catálogo de dados do AWS Glue. **Mais informações:** Serviço AWS Glue.

Aprimoramentos do monitoramento da infraestrutura

O Infrastructure Agent inclui estas alterações:

Extensão de monitoramento de host remoto

A extensão Infrastructure Agent do monitoramento de host remoto permite a recuperação de dados de desempenho sobre um sistema sem um agente no sistema. O monitoramento de host remoto coleta os dados de desempenho do sistema enviando comandos de CLI remotamente.A extensão coleta métricas sobre a utilização de CPU, disco, uso de memória e carga, além de processos com aumento mínimo na utilização de recursos do sistema monitorado. **Mais informações:** Monitoramento de host remoto.

Monitoramento do Logtash

A extensão Infrastructure Agent do monitoramento do Logtash permite monitorar e coletar métricas de vários plugins do Logtash. **Mais informações:** Extensão de monitoramento do Logtash.

Suporte ao NGINX 1.18.X

O DX APM agora oferece suporte ao NGINX versão 1.1.8.0. **Mais informações:** Monitoramento do NGINX

Monitoramento de host

Suporte a métricas principais para monitoramento de host

As antigas métricas principais de CPU, disco e memória, processo e rede do SysEdge foram transferidas para o monitoramento de host do Infrastructure Agent no Linux. **Mais informações:** Métricas de monitoramento de host.

Monitoramento de banco de dados

Monitoramento de bancos de dados SAP HANA

A extensão de monitoramento de banco de dados SAP HANA coleta métricas que monitoram a integridade e o desempenho de bancos de dados SAP HANA. **Mais informações:** Monitoramento de SAP HANA

Aprimoramento do monitoramento do Python

O agente do Python inclui estas alterações:

Chamadas assíncronas suportadas pelo agente do Python

Agora, o agente do Python oferece suporte a todas as estruturas do Python que usam módulos de instrumentação assíncrona.

Suporte ao agente do Python para SDK do Rasa e estrutura Rasa

Rasa é um estrutura de código aberto usada basicamente para criar assistentes contextuais, isto é, aplicativos de bot de bate-papo. O agente do Python agora oferece suporte a aplicativos de monitoramento com base na estrutura Rasa. **Mais informações:** seção Estrutura Rasa.

Aprimoramentos do Universal Monitoring Agent

Adição de suporte ao Universal Monitoring Agent para extensão Node.js

Você pode conectar os aplicativos de probe ao agente do coletor de dados do UMA, que é executado como parte do daemon Set do UMA, ao configurar a variável de ambiente **COLLECTOR_AGENT_HOST** com um nome de nó específico. **Mais informações:** seção Universal Monitoring Agent para extensão do Node.js.

Middleware de troca de mensagens, ESB e Web Services Enhancements

Suporte ao Apache Camel

A extensão Apache Camel permite monitorar todos os aplicativos que usam o Apache Camel como um mecanismo de roteamento. Os aplicativos podem ser implementados em aplicativos JBoss Fuse, Tomcat ou Spring Boot. **Mais informações:** Apache Camel

Aprimoramento do agente de gateway de API

Suporte à agregação de métricas de serviço

A agregação de métricas de serviço executa a agregação de métricas em vários níveis para serviços solicitados. Você pode exibir as métricas no nível de gateway, cluster e EM nos agentes. **Mais informações: seção** Agregação de métricas de serviço em Agente do CA API Gateway.

Aprimoramentos do APM Command Center

Substituição da linguagem de consulta do Lucene

Substituímos a pesquisa da linguagem de consulta do Apache Lucene no APM Command Center por uma linguagem de consulta que é interna no DX APM.

Problemas conhecidos

Esta seção lista os problemas conhecidos da release atual.

Defeito DE479068 - a árvore de métricas fica girando

Sintoma: em **Exibição da métrica**, quando você oculta agentes desconectados, o gráfico de métricas é carregado. No entanto, a árvore de métricas não é carregada.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE478641 - alerta de perigo gerado pela métrica não exibe o ícone de risco

Sintoma: em **Exibição da métrica**, um alerta de risco que é gerado por uma métrica não é exibido como um ícone. No entanto, se você alternar entre duas exibições de métricas quaisquer, o ícone de alerta de risco será exibido.

Defeito DE477342 - campos de triagem assistida não ficam visíveis na exibição de isolamento

Sintoma: quando um agente tem atributos personalizados e um alerta é disparado, os campos de triagem assistida não ficam visíveis na **exibição de isolamento** do alerta.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE477272 - problemas ou anomalias não estão sendo exibidos no painel direito Exibição da experiência

Sintoma: em **Exibição da experiência**, os problemas e anomalias são exibidos no cartão de experiência. No entanto, quando um problema ou anomalia é selecionado, o painel direito **Exibição da experiência** não mostra os detalhes.

Solução: não há nenhuma solução alternativa para esse problema.

DefeitoDE476351 - falha nos links para a documentação de instalação do pacote do APM Command Center

Sintoma: esse problema acontece ao selecionar um pacote existente no APM Command Center e clicar no link **aqui** nas instruções de instalação. Ou uma página em branco de techdocs.broadcom.com, ou um portal de documentos técnicos é exibido no lugar da página esperada da documentação de instruções de instalação.

Solução: vá diretamente para o site de documentação do DX APM SaaS.

Defeito DE449130 - não é possível efetuar logon usando a conta de SAML (Security Assertion Markup Language)

Sintoma: os usuários não podem efetuar logon ao usar os detalhes da conta SAML.

Solução: gere um token público e efetue logon usando o token.

20.6

Veja a seguir os recursos novos, alterados e depreciados no DX APM 20.6.

Recursos do agente

Esta seção lista os recursos novos e aprimorados relacionados ao agente.

Monitoramento do RabbitMQ

RabbitMQ é um agente de mensagens que atua entre plataformas e oferece uma maneira de trocar dados entre diferentes aplicativos.

A extensão do RabbitMQ monitora o desempenho dos nós, as trocas de mensagens, as filas e as conexões dos agrupamentos e dos sistemas independentes na infraestrutura do RabbitMQ. A extensão detecta automaticamente os nós em um agrupamento do RabbitMQ a serem monitorados. A extensão estabelece um aplicativo para a correlação de infraestrutura, que permite depurar os problemas causados pelo servidor do RabbitMQ em um aplicativo. Na Exibição do mapeamento, a camada de infraestrutura exibe o mapeamento entre o agrupamento e os nós.Também apresentamos GIFs animados como um meio de ilustração.Para obter mais informações, consulte Monitoramento do RabbitMQ.

Suporte ao Mule ESB 4.x

O Mule ESB 4.x permite identificar os fluxos de comunicação e suas correlações entre todas as comunicações, incluindo a comunicação assíncrona. Você também pode identificar os componentes de modelagem específicos do Mule ESB. O mapa exibe um novo ícone Mule nos vértices do Mule.Também apresentamos GIFs animados como um meio de ilustração.Para obter mais informações sobre o Mule ESB 4.x, consulte Mule ESB 4.x.

Monitoramento do PostgreSQL

O Monitoramento do PostgreSQL no DX APM permite monitorar o desempenho e a disponibilidade do ambiente de banco de dados PostgreSQL. É possível configurar e usar essa extensão do Infrastructure Agent para coletar estas métricas de desempenho relacionadas ao servidor do PostgreSQL: utilização de recursos, transações, taxa de transferência, bloqueios e muito mais. A extensão do PostgreSQL também permite que os usuários correlacionem o desempenho do aplicativo para o banco de dados com o desempenho real do banco de dados. Para obter mais informações, consulte Monitoramento do PostgreSQL.

Suporte à correlação do WebLogic Infrastructure Monitor

A extensão do WebLogic Infrastructure Monitor agora oferece suporte à correlação entre o aplicativo e a infraestrutura. Para obter mais informações, consulte Atributos do WebLogic Infrastructure Monitor.

Novas métricas do Monitoramento do vCenter

O Monitoramento do vCenter no DX APM agora fornece métricas para estas entidades em seu ambiente vCenter: vCenter, datacenter, agrupamento, repositório de dados, pools de recursos, NICs virtuais e físicas, comutadores virtuais, discos, sensores, ESX e VM. Para obter mais informações, consulte Monitoramento do vCenter.

Monitoramento do AWS oferece suporte a mais serviços

O Monitoramento do AWS (Amazon Web Services) no DX APM agora oferece suporte a estes novos tipos de serviço: Elastic Load Balancing, Elastic Cache, Auto Scaling, Kinesis Data Streams, Billing, API Gateway, CloudTrail, Functions, Logic App, Redshift, Cloudwatch Logs, Cloudfront, Cloudwatch Events e Fargate. O DX APM fornece suporte ao monitoramento com base em função do AWS para ID externa, o que permite evitar ataques confused deputy (representante confuso) em seu ambiente AWS. Para obter mais informações, consulte Monitoramento do Amazon Web Services.

O Universal Monitoring Agent oferece suporte ao .NET Core

O UMA (Universal Monitoring Agent) for Kubernetes agora detecta e instrumenta automaticamente os aplicativos do .NET Core sem exigir nenhuma alteração manual na imagem do aplicativo. O UMA oferece suporte ao NET Core versão 3.1 e superior.

Suporte ao agente do navegador do .NET Core

Agora é possível configurar a injeção automática de snippet do agente do navegador para o agente do .NET Core. Para obter mais informações, consulte Configurar o agente do navegador para .NET.

Exibir dados do UMA for Kubernetes na Árvore de métricas e no Mapa

O UMA (Universal Monitoring Agent) for Kubernetes tem dados de métrica, topologia e atributos do Kubernetes mais detalhados que podem ser exibidos na Árvore de métricas e no Mapa.

DX APM coleta e exibe dados de back-end do OpenTracing Jaeger

Agora, o DX APM coleta os rastreamentos de back-end do OpenTracing Jaeger e relata os dados como métricas e rastreamentos de transação do DX APM.

Usar anotações para sobrepor configurações do AutoAttach do UMA

Agora, é possível usar anotações para substituir as configurações de extensão Anexação automática do UMA. Eis alguns exemplos:

- Você pode sobrepor as verificações de filtro da extensão AutoAttach para memória e JVMs.
- Você pode usar a anotação para passar qualquer configuração do agente do Java, como adição de propriedades.
- Você deseja ativar o agente do navegador por namespace. Para isso, adicione uma anotação adequada. A extensão AutoAttach usa a nova anotação como uma configuração e passa as propriedades para ativar o agente do navegador sem exigir qualquer reinicialização ou reimplementação.

Agente do OpenTracing fornece correlação

A extensão Agente do OpenTracing do Infrastructure Agent agora é correlacionada entre spans do Jaeger e rastreamentos de transação do DX APM.

Agente do .NET/.NET Core usa a comunicação WebsSocket

O agente do .NET/.NET Core está configurado para enviar informações automaticamente usando o protocolo WebsSocket. Esse protocolo combina a eficiência da comunicação do soquete binário com a compatibilidade de firewalls e proxies de rede HTTP. Qualquer versão suportada pelo .NET Core e .NET Framework 4.5 e posterior oferece suporte à comunicação WebSocket.

Criar nomes de aplicativo e atributos personalizados do .NET/.NET Core

Agora, é possível configurar as propriedades `IntroscopeAgent.profile` do .NET/.NET Core para exibir estas informações:

- Atributos personalizados na guia **Agente** da **Exibição de componentes** do mapa
- Nomes de aplicativo personalizados na guia **Front-end genérico** da **Exibição de componentes** do mapa
- Nomes de aplicativo personalizados listados no painel **Detalhes do componente** do Rastreador de transações

Suporte ao agente do .NET Core para o sistema operacional Alpine

O agente do .NET Core agora pode monitorar o desempenho dos aplicativos em execução no sistema operacional Alpine Linux.

Recursos da UI

Esta seção lista os recursos da UI novos e aprimorados.

Frases de pesquisa

À medida que você digita a frase de pesquisa, é possível selecionar uma frase de pesquisa anterior que aparece na lista suspensa de preenchimento automático. Para obter mais informações, consulte Pesquisar métricas na árvore de métricas.

Exibir agentes desconectados na linha do tempo

Os agentes desconectados são exibidos em cinza na linha do tempo.

Painéis do DX App Synthetic Monitor

Novos painéis prontos para uso do DX ASM (App Synthetic Monitor) fornecem uma visão geral do seu desempenho no ambiente da web. É possível definir vários monitores no DX ASM para medir o desempenho da página. Esses painéis agora estão disponíveis no DX SaaS:

- **Key Metrics From All Monitors**: esse painel exibe as principais métricas coletadas por todos os monitores.
- **Key Metrics From Single Monitor**: esse painel exibe as principais métricas coletadas por um único monitor.

Para obter mais informações sobre os painéis prontos para uso, consulte Painéis DX.

Outros recursos e aprimoramentos

Esta seção lista outros recursos aprimorados.

Aprimoramentos no repositório de topologia

Como administrador, você pode criar partições do repositório de topologia e reequilibrar inquilinos entre instâncias do repositório de topologia.

Problemas conhecidos

Esta seção lista os problemas conhecidos da release atual.

Defeito DE466013: alerta do APM - opção de alerta de notificações do disparador ignorada

Válido para: DX APM SaaS 20.6

Sintoma: esse problema ocorre após a seleção de uma notificação de alerta do disparador durante a criação de um novo alerta. O DX APM não aplica o disparador corretamente quando o nível de alerta é alterado. Por exemplo, você cria um alerta e seleciona a opção para ser notificado **Quando a gravidade aumentar**.

Quando a gravidade do alerta realmente muda de **Crítica** para **Grave** e para **OK**, o DX APM não deve enviar uma notificação por email de alerta. No entanto, o canal de notificação é disparado, enviando incorretamente uma notificação por email quando a gravidade do alerta é reduzida.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE449130 - não é possível efetuar logon usando a conta de SAML (Security Assertion Markup Language)

Válido para: DX APM 20.1, 20.4, 20.6

Sintoma: os usuários não podem efetuar logon ao usar os detalhes da conta SAML.

Solução: gere um token público e efetue logon usando o token.

DE467134 - ausência da guia Affected Metric na página Análise do alarme do DX Operational Intelligence

Válido para: DX APM 20.6, CA APM 10.7x

Sintoma: esses problemas ocorrem quando o CA APM 10.7x local está configurado para enviar alarmes ao DX Operational Intelligence SaaS.Você pode ver os alertas do CA 10.7x local na página **Análise do alarme** do DX Operational Intelligence. No entanto, a guia **Affected Metric** está ausente para todos os alertas do CA 10.7x local.Esse problema não ocorre quando o DX APM SaaS envia alertas.

Solução: selecione Métricas na página **Performance Analytics**.

20.4

Esses são recursos novos, alterados e obsoletos no DX APM 20.4

Recursos do agente

Esta seção lista os recursos novos e aprimorados relacionados ao agente.

Monitoramento do Undertow

Agora você pode usar o Monitoramento do Undertow no DX APM para monitorar o desempenho de seus aplicativos que implementam manipuladores HTTP Undertow.Você ativa essa extensão do agente do Java quando usa o Undertow, e o DX APM não exibe qualquer front-end Undertow.

Quando os aplicativos usam a API do servlet, não é necessário usar o Monitoramento do Undertow, mesmo quando você tem um servidor subjacente do Undertow. A extensão não é necessária nesse caso, pois o agente do Java rastreia servlets por padrão.

Para implantar o Monitoramento do Undertow, inclua o componente **Undertow (Non-Servlets)** ao criar ou editar um pacote no APM Command Center.

Monitoramento de service mesh do Istio

Agora, o DX APM realiza o monitoramento de pilha completa das implantações de service mesh do Istio. O Monitoramento de service mesh do Istio fornece estas informações e funcionalidades:

- Dados de integridade e desempenho sobre os componentes do plano de controle do Istio, como Mixer, Pilot e Gateway
- Dados de desempenho sobre o plano de dados que inclui o proxy Envoy
- Dados de integridade e desempenho sobre serviços
- Detecção automática da topologia do seu service mesh, incluindo intercomunicação entre o desempenho da infraestrutura do recipiente e os microsserviços

Monitoramento do etcd

Agora, você pode monitorar o desempenho de sua implantação do etcd. O DX APM usa o Universal Monitoring Agent configurado para importar dados do Prometheus e relatar métricas do etcd sobre a integridade do Kubernetes ou do agrupamento do OpenShift.

Monitoramento aprimorado do Kubernetes e OpenShift

O DX APM agora inclui relatórios aprimorados de desempenho da topologia do Kubernetes. O mapa inclui nós para componentes do Kubernetes, incluindo agrupamentos e namespaces. O monitoramento do Kubernetes e do OpenShift agora inclui métricas para que você avalie melhor sua capacidade do agrupamento. Métricas adicionais ajudam a determinar se o agrupamento do Kubernetes, bem como os diferentes namespaces e projetos, estão subprovisionados ou superprovisionados.

Monitoramento do MongoDB

O Monitoramento do MongoDB no DX APM permite monitorar o desempenho e a disponibilidade do seu ambiente MongoDB.A extensão do Infrastructure Agent do MongoDB fornece visibilidade em tempo real dos recursos do banco de dados e ajuda a correlacionar as métricas de desempenho do aplicativo, da infraestrutura e do banco de dados em uma interface unificada.

Monitoramento do Google Cloud Platform

O Monitoramento do GCP (Google Cloud Platform) no DX APM monitora remotamente a integridade e o desempenho da infraestrutura e dos serviços do GCP. O Monitoramento do GCP é uma extensão do Infrastructure Agent que usa as APIs do Google Stackdriver para conectar e detectar os recursos do GCP a serem monitorados. O Monitoramento do GCP oferece suporte aos seguintes serviços do GCP: Google Compute Engine, Google Cloud Storage, Google Cloud SQL e Google Cloud Filestore. Para obter mais informações, consulte Monitoramento do Google Cloud Platform.

Serviço do AWS CloudTrail

O serviço AWS (Amazon Web Services) CloudTrail no DX APM permite executar tarefas de conformidade, governança, auditoria operacional e auditoria de risco da sua conta do AWS. Você pode executar a conformidade da sua conta do AWS com base na autoridade regulatória interna da sua organização ou em uma autoridade regulatória de terceiros.Para obter mais informações, consulte Monitoramento do Amazon Web Services.

Monitoramento do AWS

O Monitoramento do AWS no DX APM agora oferece suporte a estes novos tipos de serviço: Elastic Load Balancing, Elastic Cache, Auto Scaling, Kinesis Data Streams, Billing, API Gateway, CloudTrail, Functions, Logic App, Redshift e Fargate. Para obter mais informações, consulte Monitoramento do Amazon Web Services.

Monitoramento do Azure

O Monitoramento do Azure no DX APM agora oferece suporte a estes novos tipos de serviço: Serviço de Kubernetes do Azure, Gerenciamento de Custos, Load Balancer, Azure SQL, Azure Cosmo DB, Hub de Eventos e Barramento de Serviço. Para obter mais informações, consulte Monitoramento do Azure

Monitoramento do banco de dados SQL Server

O Monitoramento do banco de dados SQL Server no DX APM permite monitorar o desempenho e a disponibilidade do ambiente de banco de dados SQL Server. É possível configurar e usar essa extensão do Infrastructure Agent para coletar as métricas de desempenho do SQL Server relacionadas a conexões, gerenciador de buffer, estatísticas de índice e muito mais. O Monitoramento do SQL Server também fornece métricas de agrupamento. Para obter mais informações, consulte Monitoramento do banco de dados SQL Server.

Monitoramento do Redis

O Monitoramento do Redis no DX APM pode monitorar uma única instância de um servidor do Redis e de vários agrupamentos.

Os dois componentes principais em um agrupamento do Redis são os nós mestre e subordinado. Todos os dados gravados no nó mestre também são salvos no nó subordinado. A extensão do Infrastructure Agent do Monitoramento do Redis monitora os nós mestre e subordinado. Quando um nó subordinado é promovido a nó mestre, o Monitoramento do Redis detecta as alterações e as reflete na interface do usuário. Para obter mais informações, consulte Extensão do Monitoramento do Redis.

Extensão do Monitoramento do ForgeRock

A extensão do agente do Java do ForgeRock no DX APM está disponível como parte de todos os agentes do Java. A extensão monitora a plataforma de identidade ForgeRock, que inclui os componentes Identity Gateway (gateway de identidade) e Access Management (gerenciamento de acesso). Para obter mais informações, consulte Extensão do Monitoramento do ForgeRock.

Monitoramento do GraphQL

O DX APM agora monitora o desempenho do GraphQL versão 14.x e superior no Node.js. Você pode ver métricas com base nas rotas da estrutura do GraphQL do Node.js e nas informações relacionadas.

Aprimoramento do mecanismo de conexão entre o Monitoramento do IBM WebSphere MQ e o servidor MQ

Agora, o DX APM inclui a conexão Modo de vinculações entre a extensão do Infrastructure Agent do Monitoramento do IBM WebSphere MQ e o servidor MQ que reside na mesma máquina. Nesse modo, o DX APM não exige detalhes de canal, host ou porta para estabelecer uma conexão com o servidor MQ. Para obter mais informações, consulte Configuração da conexão Modo de vinculações.

O DX APM também aprimorou o processo de autenticação de usuário para conectar o Monitoramento do IBM WebSphere MQ e o servidor do MQ no modo cliente/servidor. Agora, é possível executar o script `RunMQCommands` e fornecer os detalhes de autenticação, o que permite que qualquer usuário do Infrastructure Agent acesse o servidor MQ. Para obter mais informações, consulte Configuração de conexão cliente/servidor.

Suporte ao Amazon Linux

O Infrastructure Agent agora é suportado nestas versões do Amazon Linux:

- Amazon Linux 2 AMI
- Amazon Linux AMI

Monitoramento da infraestrutura do WebLogic

O Monitoramento da infraestrutura do WebLogic no DX APM fornece recursos de monitoramento JMX para o servidor do WebLogic, incluindo todos os nós do agrupamento.Para obter mais informações, consulte Monitoramento da infraestrutura do WebLogic.

Business Payload Analyzer

Quando você faz download do BT Listener, as seguintes propriedades são configuradas automaticamente:

- **btListener.output.channel.tenantId:** essa propriedade é configurada com a ID do inquilino.
- **btListener.output.channel.url:** essa propriedade é configurada com o URL DXC.

Amostragem dinâmica aleatória

Agora, o DX APM fornece uma etapa rumo à amostragem inteligente completa. Você pode configurar o agente do Java para coletar dinamicamente os rastreamentos de transações aleatórias em um determinado período a fim de capturar diferentes tipos de transação.É possível configurar o agente do Java para coletar os N primeiros rastreamentos de transação em um determinado período, um número específico de rastreamentos de transação de amostra aleatórios em um determinado período, ou ambos.

Suporte ao .NET Core 3.1

O .NET Core Agent agora coleta dados sobre aplicativos .NET Core 3.1.Para obter mais informações, consulte .NET/.NET Core Agent e Microsoft .NET Core.

Recursos da UI

Esta seção lista os recursos novos e aprimorados relacionados à UI.

Painéis do banco de dados Oracle no DX APM

É possível ver vários painéis relacionados ao desempenho do banco de dados Oracle. Os painéis Oracle exibem métricas relacionadas ao desempenho do banco de dados e a outras atividades do usuário que ajudam você a solucionar problemas de banco de dados.Para obter mais informações, consulte Painéis de banco de dados Oracle no .

Função de usuário avançado no Team Center

Incluímos uma função de usuário avançado que pode executar operações CRUD em alertas, módulos de gerenciamento, calculadoras e agrupamentos de métricas. Para obter mais informações, consulte Permissões, aplicação de domínio e edição de elementos.

Exibir métricas de agentes desconectados

Ao mover a linha do tempo para um intervalo de tempo passado e exibir um agente conectado naquele momento, você pode ver as métricas correspondentes na exibição contextual do mapa.

Importar agentes existentes para o APM Command Center

Agora, é possível importar um agente existente do CA APM 10.7 para o APM Command Center usando o utilitário Import Agent Tool. Para obter mais informações, consulte Agent Import Tool.

Colunas definidas pelo usuário nos resultados da pesquisa de métricas

Agora é possível mostrar ou ocultar colunas para personalizar os resultados da pesquisa de métricas.Para obter mais informações, consulte Pesquisar métricas na árvore de métricas.

Alteração de evento no modo dinâmico

No modo **Dinâmico** da linha do tempo, agora você pode exibir eventos de mudança relacionados ao status, à topologia e aos atributos de um nó.Para obter mais informações, consulte Usar linha do tempo e exibir eventos de mudança.

Suporte ao proxy para controlador de agente

Como administrador, você pode definir os detalhes do proxy ao configurar o componente Controlador de agente no APM Command Center. Para configurar o proxy, ative e defina as seguintes propriedades na página de configuração do Controlador de agente:

- 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**
> Caso você não defina os valores das configurações, eles serão extraídos de `agentManager.httpProxy.username` no pacote em-connection.

Para obter mais informações sobre como configurar as propriedades do complemento, consulte Configurar as propriedades do complemento e as instruções de instalação no APM Command Center.

Integrações

Esta seção lista as integrações de produto novas e aprimoradas.

Integração do DX App Synthetic Monitor e DX APM

Agora, você pode configurar a integração do DX ASM (App Synthetic Monitor) ao DX APM no APM Command Center. A integração é executada como parte do Infrastructure Agent. Para obter mais informações, consulte Configurar o DX App Synthetic Monitor para o DX APM.

Configure os seguintes pré-requisitos antes de usar os aprimoramentos:

- `asm.metrics.logs=true` (para as etapas do JMeter e WebDriver)
- `asm.metrics.download.full=true` (para as etapas do JMeter e WebDriver)
- `asm.metrics.har.requests=true` (somente para etapas do WebDriver)

Também é possível usar estes aprimoramentos:

- Exibir etapas detalhadas do JMeter
  Quando o Monitor de script executa o script JMeter, é possível exibir os resultados das etapas do JMeter na Exibição da métrica. Para exibir os resultados da etapa do JMeter, defina o valor de `asm.reportJTLSubtree` como `true` .
- Exibir etapas detalhadas do WebDriver
  Quando o Monitor de script executa o script WebDriver, é possível exibir os resultados das etapas do WebDriver na Exibição da métrica. Para exibir, os resultados das etapas do WebDriver, defina `asm.metrics.har.wdm` como `true` .
- Métrica Last Result Check
  A nova métrica **Last Result Check** exibe o último status da verificação do monitor.
  Veja a seguir os estados exibidos pela métrica:
  - 0: Sem erros
  - 1: Erro
  - 2: Modo de manutenção

Outros recursos

Esta seção lista outros recursos aprimorados.

Aprimoramentos do TAS (Test Automation System - Sistema de Automação de Teste)

Você pode usar estes aprimoramentos do TAS:

- **TAS API v2**: agora, é possível executar comandos para excluir uma parte do repositório de topologia de modo síncrono ou assíncrono.
- **Autenticação de usuário ativada para TAS/NASS:** o usuário conectado com direitos de administrador de inquilinos ou de administrador principal está autorizado a chamar os terminais de TAS/NASS (repositório de métricas).

Problemas conhecidos

Esta seção lista todos os problemas conhecidos com a release atual.

Defeito DE459955 - problema com o nome do banco de dados RDS do Amazon Web Services

Válido para: DX APM SaaS 20.4

Sintoma: um problema no DX APM ocorre quando você não atribui um nome a um banco de dados durante a criação da instância RDS do AWS.O problema resulta na correlação da Camada do aplicativo à Camada de infraestrutura que não está funcionando para a instância do banco de dados no Infrastructure Agent.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE457462 - link de configuração do agente de PHP inativo na caixa de diálogo de download do agente

Válido para: DX APM SaaS 20.4

Sintoma: na página da caixa de diálogo de download do agente para o DX APM Infrastructure Agent, o link fornecido para acessar os detalhes de configuração completa do agente de PHP está inativo e exibe o erro 404.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE457423 - instruções incorretas na caixa de diálogo de download do agente para monitoramento do WebLogic no Infrastructure Agent

Válido para: DX APM SaaS 20.4

Sintoma: na página da caixa de diálogo de download do agente para fazer download do Infrastructure Agent, a página de instruções de instalação do Monitor do WebLogic contém um erro de conteúdo.Na seção **Monitor de infraestrutura do WebLogic no DX APM**, as instruções para copiar os arquivos jar estão incorretas.

Solução: use estas instruções para copiar corretamente os arquivos jar.

Siga estas etapas:

1. Vá para o diretório `<PASTA_PRINCIPAL_WL>/lib` .
   `PASTA_PRINCIPAL_WL` é o diretório em que o WebLogic Server está instalado.
2. Copie o arquivo `wlthint3client.jar` .
3. Cole o arquivo `wlthint3client.jar` no diretório `<pasta_principal_APMIA>/lib` .

Defeito DE456625 - alterações no arquivo Config.json são perdidas após instalação do probe Node.js

Válido para: DX APM SaaS 20.4, probe NodeJS versão 1.10.83

Sintoma: depois de instalar o probe mais recente do aplicativo Node.js, todas as alterações feitas no arquivo `config.json` serão perdidas.

Solução: antes de instalar o probe mais recente do aplicativo Node.js, execute as tarefas a seguir.

Siga estas etapas:

1. Localize o arquivo `config.json` indo até o seguinte local do sistema, onde você instalou o aplicativo Node.js:
   ```
   <Node.js_Installation_Folder>\node-modules\ca-apm-probe\
   ```
2. Faça backup do arquivo `config.json` .
3. Instale o probe Node.js mais recente executando o seguinte comando no sistema em que você instalou o aplicativo Node.js:
   ```
   npm i ca-apm-probe
   ```
4. Vá até o seguinte local do sistema, no qual você instalou o aplicativo Node.js:
   ```
   <Node.js_Installation_Folder>\node-modules\ca-apm-probe\
   ```
5. Informe as novas propriedades do arquivo `config.json` mais recente no arquivo `config.json` de backup (consulte a **etapa 2**).

6. Inicie o aplicativo Node.js.

Defeito DE456154 - problema ao correlacionar back-ends com front-ends para o aplicativo Node.js

Válido para: DX APM SaaS 20.4, probe NodeJS versão 1.10.83

Sintoma: quando front-ends do aplicativo Node.js chamam de modo assíncrono mais de um back-end, a correlação não funciona na Exibição da métrica nem no mapa. No entanto, a correlação do back-end com o front-end funciona conforme esperado em rastreamentos de transação.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE456144 - os valores de configuração de decoração do atributo não são carregados na inicialização do Node.js

Válido para: DX APM SaaS 20.4, probe NodeJS versão 1.10.83

Sintoma: quando você inicia o aplicativo Node.js, os valores de configuração no arquivo `config.json` para o Automatic Attribute Decoration do Node.js não são carregados no probe Node.js.

Solução: execute as tarefas a seguir para carregar os valores de configuração do Automatic Attribute Decoration.

Siga estas etapas:

1. Verifique se o Infrastructure Agent está instalado.
2. Instale o `NodeJS ca-apm-probe` e inicie o aplicativo Node.js com o probe NodeJS.
3. Certifique-se de configurar a chave da API pública no arquivo `introscopeAgent.profile` do Infrastructure Agent. Para configurar, no arquivo `introscopeAgent.profile` , atualize a seguinte propriedade indo até o local da pasta, `\apmia\core\config\` :
   ```
   attribute.decoration.apm.access.token
   ```
4. Abra o arquivo `config.json` indo até o seguinte local no sistema, onde você instalou o aplicativo Node.js e o probe `NodeJS ca-apm-probe` :
   ```
   <Node.js_Installation_Folder>\node-modules\ca-apm-probe\
   ```
5. Atualize o arquivo `config.json` .

   NOTE
   Observação: certifique-se de editar o arquivo `config.json` com algumas mudanças (como inserir um espaço).
6. Salve o arquivo `config.json` .

Defeito DE454550 - o nó de back-end do MongoDB é exibido como um back-end genérico no mapa

Válido para: DX APM SaaS 20.4, MongoDB 2.x, Node.js

Sintoma: o nó de back-end do MongoDB deve ser exibido como um banco de dados inferido com Node.js no mapa. No entanto, o nó de back-end do MongoDB é exibido como um back-end genérico.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE450621 - problema no comando de execução do Python Django

Válido para: DX APM 20.4, Python 3.x

Sintoma: o comando `run` a seguir não funciona no sistema em que você instalou o aplicativo Python Django:
```
ca-apm-runpy python manage.py runserver
```
Solução: use o seguinte comando `run` no sistema em que você instalou o aplicativo Python Django:
```
ca-apm-runpy gunicorn -w 2 -b :8000 <project-name>.wsgi
```

Defeito DE450599 - agente desconhecido do Python Django é mostrado na Exibição da métrica

Válido para: DX APM 20.4, Python 3.x

Sintoma: quando você inicia o Infrastructure Agent do DX APM, um agente desconhecido é mostrado na Exibição da métrica.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE450618 - problema de exibição das métricas de URL do Python Django

Válido para: DX APM 20.4, Python 3.x

Sintoma: ao conectar o aplicativo Python Django ao Infrastructure Agent e procurar o aplicativo Python Django. Cada métrica de URL (terminal) do aplicativo Python Django é mostrada duas vezes na Exibição da métrica.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE449130 - não é possível efetuar logon usando a conta de SAML (Security Assertion Markup Language)

Válido para: DX APM 20.1, 20.4

Sintoma: o usuário não consegue efetuar logon ao usar os detalhes da conta de SAML.

Solução: gere um token público e efetue logon usando o token.

Defeito DE438579 - a correlação do monitor de host com o nó IIB Integration não funciona

Válido para: DX APM SaaS 20.4

Sintoma: a correlação do monitor do host com o nó IIB (IBM Integration Bus) **Integration** não funciona quando o recurso de monitoramento do host da infraestrutura do IIB está ativado.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE405769 - correlação do Mule ESB 3.x com o proxy não funciona

Válido para: DX APM SaaS 20.4, Mule ESB 3.x

Sintoma: a correlação do aplicativo Mule ESB 3.x com o proxy é usada por um aplicativo aninhado. A correlação não funciona no mapa e em rastreamentos de transação.

Solução: não há nenhuma solução alternativa para esse problema.

20.1

Veja a seguir os recursos novos, alterados e obsoletos no DX APM 20.1.

Recursos do agente

Plugin do servidor web do Nginx

Agora, o Business Payload Analyzer inclui um plugin para o servidor web do Nginx. Para obter mais informações sobre a instalação e a configuração, consulte a seção Instalar e configurar o plugin do servidor web do Nginx.

Agora, é possível implantar todas as funcionalidades do UMA (Universal Monitoring Agent) for Kubernetes usando um operador de serviço do Kubernetes.

Use o operador de serviço do Kubernetes para implantar o Universal Monitoring Agent for Kubernetes

Agora, é possível implantar todas as funcionalidades do UMA (Universal Monitoring Agent) for Kubernetes usando um operador de serviço do Kubernetes.

Suporte do OpenTracing

Agora, o DX APM oferece suporte ao monitoramento de aplicativos OpenTracing. O suporte do OpenTracing relata métricas de desempenho de aplicativos e rastreamentos de transação que são coletados de aplicativos instrumentados com o Jaeger. O DX APM fornece suporte do OpenTracing como uma extensão do Infrastructure Agent. Para obter mais informações, consulte Suporte do OpenTracing.

Instalar o Infrastructure Agent no AIX

Agora, é possível baixar e instalar o Infrastructure Agent na plataforma do AIX. Para obter mais informações, consulte Instalar o Infrastructure Agent no DX APM.

Suporte ao Python 3.x

Agora, o agente do Python oferece suporte ao Python 3.x e à correlação de entrada e de saída. Agora, é possível exibir a correlação de fluxos de entrada no aplicativo Python com fluxos de saída do aplicativo Python.

Correlação suportada

- **Correlação de entrada:** se houver qualquer chamada do fluxo de entrada (Java ou Python) para o aplicativo Python, os respectivos agentes instrumentarão ambos os fluxos.
- **Correlação de saída:** se houver qualquer chamada do aplicativo Python para o downstream (Java ou Python), os respectivos agentes instrumentarão ambos os fluxos.

Correlação de saída usando o módulo de solicitação

O módulo de **solicitações** é o padrão para fazer solicitações HTTP no Python. Se qualquer aplicativo Python chamar o módulo de solicitações no probe Python, o probe será notificado e os rastreamentos correspondentes serão exibidos.

Correlação de saída usando o módulo Urllib

Urllib.request é o módulo de busca de URLs (Uniform Resource Locators - Localizadores Uniformes de Recursos) no Python. O módulo urllib.request define as funções e as classes que ajudam na abertura de URLs (principalmente o HTTP) no Python. Se qualquer aplicativo Python chamar este módulo no probe Python, o probe será notificado e os rastreamentos correspondentes serão exibidos.

Suporte a aplicativos Python em recipientes do Docker

Agora, é possível usar o agente do Python para monitorar os aplicativos Python Django Framework e Flask Framework.

Serviço do AWS CloudTrail

O serviço do AWS CloudTrail permite executar auditorias operacionais, de conformidade de governança e de risco da conta do AWS. Você pode executar a conformidade de sua conta do AWS de duas maneiras. Conformidade com base na autoridade de regulamentação interna da sua organização ou em uma autoridade de regulamentação de terceiros.

Monitoramento da infraestrutura do IIB

Você pode usar o monitoramento do IIB (IBM Integration Bus) para monitorar a integridade e a disponibilidade do IIB e os fluxos de mensagens correspondentes. Como pré-requisito, é preciso usar um dos seguintes componentes: MQTT, que é integrado ao IIB ou ao IBM MQ.A extensão de monitoramento do IIB se conecta a um dos componentes para coletar as métricas de estatísticas do IIB.Para obter mais informações, consulte Monitoramento do IIB.

Monitoramento do banco de dados SQL Server

O monitoramento do banco de dados SQL Server permite monitorar o desempenho e a disponibilidade do ambiente de banco de dados SQL Server. Configure e use essa extensão para coletar as métricas de desempenho do SQL Server que estão relacionadas às conexões, ao gerenciador de buffer, às estatísticas de índice e muito mais.Para obter mais informações, consulte Monitoramento do banco de dados SQL Server.

Monitoramento de banco de dados MySQL

A extensão de monitoramento do banco de dados MySQL permite monitorar o desempenho e a disponibilidade do ambiente de banco de dados MySQL. Essa extensão fornece visibilidade em tempo real dos recursos críticos do banco de dados. Esses recursos incluem bytes enviados e recebidos; conexões tentadas, canceladas ou que falharam; insights do InnoDB; operações do banco de dados; utilização de recursos; e muito mais. Para obter mais informações, consulte Monitoramento do banco de dados MySQL.

Suporte ao rastreamento de transação do banco de dados Oracle, Oracle RAC e Oracle EBS

O DX APM oferece suporte à coleta orientada a eventos de rastreamentos do bancos de dados para as seguintes extensões de banco de dados: banco de dados Oracle, RAC (Real Application Clusters) e Oracle EBS (E-Business Suite).

As extensões de banco de dados fornecem rastreamentos de banco de dados de acordo com o serviço específico. Os rastreamentos do banco de dados fornecem os detalhes dos indicadores de desempenho. Os rastreamentos também mostram detalhes e estatísticas de busca, espera, análise do SQL e utilização de recursos, enquanto o respectivo banco de dados executa as transações de banco de dados para uma transação de negócios específica.

Suporte a Koa.js Framework para Node.js

O agente do Node.js oferece suporte a Koa.js, que é a estrutura web do Node.js da próxima geração.

Suporte ao monitoramento do NGINX

A extensão do agente de monitoramento do NGINX permite que você monitore a versão dos serviços hospedados do NGINX. Você pode usar essa extensão juntamente com outras extensões existentes para fazer o monitoramento da infraestrutura do NGINX e do desempenho dos serviços que são hospedados na versão de serviços hospedados do NGINX. Para obter mais informações, consulte Monitoramento do NGINX.

Suporte aprimorado a aplicativos do .NET Core

Agora, o DX APM oferece suporte ao monitoramento de transações assíncronas do .NET Core.

Métricas do intervalo de monitoramento e de defasagem de consumidores do Kafka

Agora, o monitoramento do Kafka relata o desempenho da defasagem dos grupos de consumidores do Kafka. O monitoramento do Kafka usa as métricas de **intervalo** e **defasagem atual** para cada grupo de consumidores quando o aplicativo Kafka tem baixo desempenho. Essas métricas podem ajudar a determinar se o baixo desempenho do Kafka se deve ao fato de que os consumidores não leem as mensagens com rapidez suficiente, resultando em mensagens aguardando para serem lidas.

Suporte aprimorado ao Java 11

Agora, o agente do Java monitora os aplicativos Java 11 sem a necessidade de transmitir nenhum argumento adicional de linha de comando para o comando `-javaagent` .

Aprimoramentos no monitoramento da correlação de log

Agora, o monitoramento da correlação de log oferece suporte a log4j2. Agora, é possível definir o padrão `param com.ca.apm.log.correlation.mdc.insert.before` com `%m%n` e `%msg` ao mesmo tempo. Você também pode definir vários padrões para `param com.ca.apm.log.correlation.mdc.insert.before` .

Suporte a aplicativos Akka e Play

O DX APM inclui uma extensão do agente do Java que relata o Akka de desempenho e a estrutura do Play. Esta extensão relata as métricas de desempenho do Akka e de front-end, back-end, correlação e do controlador do Play.

Monitoramento do Prometheus

Agora, o Infrastructure Agent inclui o monitoramento do Prometheus, que permite ao DX APM incluir remotamente as métricas do Prometheus. É possível configurar as propriedades do arquivo de configuração para incluir as métricas diretamente a partir de um back-end do Prometheus. Por exemplo, você pode configurar o tipo de métrica, a consulta da métrica e assim por diante. Também é possível configurar o monitoramento do Prometheus para incluir as métricas de um exportador do Prometheus.

Monitoramento do JMX remoto

O Infrastructure Agent contém a nova extensão de monitoramento do JMX remoto. Essa extensão permite que você monitore remotamente o desempenho de aplicativos Java por meio do JMX sem exigir qualquer instrumentação direta do aplicativo. As métricas de desempenho do JMX são correlacionadas com outras métricas de desempenho, como o desempenho da infraestrutura e do aplicativo. Para obter mais informações, consulte Monitoramento do JMX remoto.

Monitoramento do Couchbase

O Infrastructure Agent contém a nova extensão de monitoramento do Couchbase. Essa extensão permite monitorar o desempenho do Couchbase, incluindo o monitoramento de um cluster. Para obter mais informações, consulte Monitoramento do Couchbase.

Modos de monitoramento do agente do Java

O agente do Java tem um novo modo de monitoramento que pode ser definido como **Nenhum**. O modo Nenhum é o modo mínimo do agente, que desativa a maior parte das funcionalidades e das métricas. É possível alterar o modo em tempo de execução sem que seja necessário reiniciar o servidor de aplicativos.

Visibilidade aprimorada do desempenho do aplicativo .NET

Agora, o agente do .NET coleta automaticamente os rastreamentos de pilha. Os rastreamentos de pilha contêm toda a pilha de chamadas de método do aplicativo .NET. Os rastreamentos de pilha são exibidos como instantâneos nos rastreamentos de transação.

Suporte a aplicativos PHP no recipiente do Docker

Atualmente, o agente do PHP oferece suporte ao monitoramento da CLI (Command Line Interface) do PHP. Você pode usar o agente do PHP para monitorar os scripts do PHP que são executados a partir de outro script do PHP.

Suporte ao aplicativo Node.js em recipientes do Docker

O agente do Node.js permite monitorar o aplicativo Node.js juntamente com os bancos de dados que se conectam ao Node.js. Por exemplo, os bancos de dados PostgreSQL, MongoDB e MySQL.

Recursos da UI

API para o download de agentes disponível no APM Command Center

Agora, é possível usar a API do APM Command Center para fazer download dos pacotes mais recentes do APM Command Center e personalizar o comportamento do download definindo as propriedades necessárias. Por exemplo, durante o download, é possível personalizar a carga e definir determinadas propriedades como ocultas. Para obter mais informações, consulte API do APM Command Center.

Agente do Java para microsserviços no APM Command Center

Agora, é possível criar e baixar o agente do Java para microsserviços a partir do APM Command Center. Para obter mais informações, consulte Implantar pacotes de agentes usando o APM Command Center.

Filtrar a exibição de métricas usando atributos

Na exibição da métrica, agora é possível definir filtros para agentes com base em seus atributos.

Aprimoramento de calculadoras

Agora, é possível criar calculadoras que levem os valores de um agrupamento de métricas como entrada e que façam a média ou a soma dos valores. As calculadoras geram a saída do valor resultante como uma métrica personalizada no navegador de métricas. As métricas geradas pela calculadora são exibidas em um processo virtual denominado **Custom Metric Process**. O processo de métricas personalizadas é executado em um host virtual chamado **Custom Metric Host**. Para obter mais informações, consulte Criar e editar calculadoras.

Executar consultas usando a API REST

Agora, é possível usar as seguintes APIs REST para consultar métricas e dados relacionados:

- API REST de consulta de métricas

A API de consulta de métricas consulta as métricas de diferentes intervalos de tempo, frequências e métricas. Assim como outras APIs REST do APM, a interface da API REST de consulta de métricas usa a autenticação com base em token. Para obter mais informações, consulte API REST da consulta de métricas.

- API REST do Team Center

A API REST do Team Center fornece várias funcionalidades no nível do painel e de consulta de dados de métrica. Assim como outras APIs REST do DX APM, a interface da API REST do Team Center usa a autenticação com base em token.Para obter mais informações, consulte API REST do Team Center.

Importar e exportar definições do pacote do agente do APM Command Center

Agora, é possível importar e exportar definições do pacote do agente de um inquilino para outro.Para obter mais informações, consulte Implantar pacotes de agentes usando o APM Command Center.

Suporte e recursos obsoletos

O DX APM não oferece mais suporte aos seguintes recursos e funcionalidades:

- Estação de trabalho da linha de comando
- Python 2.7
- ChangeDetector
- Instrumentação dinâmica
- Enterprise Team Center
- Recurso de montagem/desmontagem do agente.
  Os agentes estão sempre disponíveis no DX APM, portanto, não há mais necessidade de montar e desmontar agentes.
- A propriedade de sistema `-DagentProfile` do agente do Java não é mais suportada.

Problemas conhecidos

Defeito DE449471- O URL de exibição de isolamento do Infrastructure Agent não abre

Válido para: DX APM 20.1

Sintoma: a exibição de **isolamento** não é gerada para o Infrastructure Agent. Essa situação ocorre quando você vai de **Painéis**, **Agente**, **Adicionar filtro**, seleciona o nome do host do Infrastructure Agent na lista suspensa e, em seguida, seleciona **Camada do aplicativo**.

Solução: com base na definição do alerta, defina manualmente o filtro correto no mapeamento.

Defeito DE449130 - não é possível efetuar logon usando a conta de SAML (Security Assertion Markup Language)

Válido para: DX APM 20.1

Sintoma: o usuário não consegue efetuar logon ao usar os detalhes da conta de SAML.

Solução: gere um token público e efetue logon usando o token.

Defeito DE440008 - Selecionar um rastreamento faz com que o painel de rastreamento de transação seja redefinido para o topo

Válido para: DX APM 20.1

Sintoma: esse problema ocorre quando há muitos rastreamentos no painel Rastreamentos de transação do Visualizador do rastreamento de transação. Após rolar o painel para baixo e selecionar um rastreamento, o painel Rastreamentos de transação é redefinido para o topo.

Solução: role para baixo o painel Rastreamentos de transação e procure o rastreamento com uma borda.

Defeito DE450933 - Erro de monitoramento do OpenShift

Sintoma: desejo fazer download do monitoramento do OpenShift na caixa de diálogo de download do APM SaaS. Clico em **Openshift** na categoria **Nativo da nuvem.** Ao seguir as instruções e executar o comando `oc create -f caagent-openshiftmonitor.yml` , recebo um erro.

Como posso resolver o problema?

Solução: no arquivo `caagent-openshiftmonitor.yml` , remova a propriedade `-name: dev & readOnly: true` . Execute este comando:

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

Defeito DE432585 - os valores das métricas de estatísticas do recurso de monitoramento do IIB (IBM Integration Bus) são exibidos como cumulativos

Sintoma: os valores das métricas de monitoramento do IIB (IBM Integration Bus) para as estatísticas do recurso são exibidos como **cumulativos** e não **por intervalo**.

Solução: não há nenhuma solução alternativa para esse problema.

Defeito DE448777 - O fluxo de mensagens de monitoramento do IIB (IBM Integration Bus) e as estatísticas do recurso não são relatados

Sintoma: ao reiniciar o Gerenciador de filas assinado, o fluxo de mensagens e as estatísticas de recursos do IIB (IBM Integration Bus) não são relatados no DX APM.

Solução: reinicie o DX APM Infrastructure Agent.

Defeito DE448618 - O plugin Jenkins falha no ambiente do DX SaaS

Sintoma: o plugin do Jenkins, `em.url` , não funciona no DX SaaS após a atualização do DX APM.

Solução: ao atualizar o ambiente do DX SaaS, atualize o valor de URL do EM no arquivo `performance-comparator.properties` .

Siga estas etapas:

1. Efetue logon no DX SaaS.
2. Clique em **Abrir** na caixa**DX APM** . A página inicial do DX APM é exibida. A página inicial exibe o URL usado para acessar o DX APM no navegador web.
3. Vá para `<Espaço de trabalho do Jenkins>\<nome da tarefa do jenkins>\properties\.`
4. Abra o arquivo `performance-comparator.properties` .
5. Atualize o valor da propriedade `em.url` com o URL do EM mais recente.

Notas da versão de 2019

Esta seção contém as notas da versão de 2019.

- Novembro de 2019
- Outubro de 2019
- Agosto de 2019

Novembro de 2019

26 de novembro de 2019 - O que há de novo

Métricas do Infrastructure Agent para Red Hat

Agora, é possível exibir as métricas do servidor do Red Hat relativas a CPU, discos, sistema de arquivos, memória, rede, processadores, paginação, troca, desempenho do sistema e muito mais.*Monitoramento reativo do Spring Boot*

Essa nova extensão do agente do Java monitora os aplicativos reativos do Spring Boot. A extensão instrumenta especificamente os servidores e clientes HTTP assíncronos Netty e as estruturas Reactor Core para Spring Boot para fazer a correlação entre segmentos e o rastreamento de componentes assíncronos.Para obter mais informações, consulte Monitoramento de aplicativos reativos do Spring Boot.

Monitoramento do banco de dados Oracle RAC

A extensão do Oracle RAC permite monitorar o desempenho e a disponibilidade do ambiente Oracle RAC (Real Application Clusters). Você pode usar a extensão do Oracle RAC para verificar se algum serviço em um banco de dados do agrupamento tem problemas de disponibilidade. A extensão do Oracle RAC fornece visibilidade em tempo real de recursos críticos de banco de dados, como bloqueios, verificações de tabela completa, arquivos redo log, segmentos de reversão e muito mais.

É possível configurar a extensão do Oracle RAC para coletar as métricas de desempenho do Oracle RAC para ajudá-lo a monitorar o ambiente Oracle RAC. Você pode ver de imediato o tempo levado para agregação de valor em painéis pré-configurados e alertas disparados por desempenho que o notificam de forma proativa sobre possíveis violações de SLA, antes que os usuários finais sejam afetados. Para obter mais informações, consulte Monitoramento do banco de dados Oracle RAC.

Monitoramento do banco de dados Oracle EBS

A extensão do Oracle EBS (E-Business Suite) permite que você monitore o desempenho e a disponibilidade dos seguintes componentes do Oracle EBS: gerenciadores simultâneos, programas simultâneos e o gerenciador de resolução de conflitos.Você pode usar a extensão do Oracle EBS para revisar as tarefas simultâneas e os gerenciadores simultâneos no nível do agrupamento e no nível do nó individual. Para obter mais informações, consulte Monitoramento do banco de dados Oracle EBS.

Monitoramento do IIB

Você pode usar o monitoramento do IIB (IBM Integration Bus) para monitorar a integridade e a disponibilidade dos aplicativos conectados ao IIB e os fluxos de mensagens correspondentes. Como pré-requisito, o IBM MQ deve estar em execução para que a extensão de monitoramento do IIB possa se conectar ao IBM MQ e coletar as métricas de estatísticas do IIB. Para obter mais informações, consulte Monitoramento do IIB.

Extensão do OkHttp

Agora, o agente do Java oferece suporte ao monitoramento do OkHttp. OkHttp representa um cliente HTTP eficiente que oferece suporte ao protocolo HTTP/2. Esse protocolo carrega os dados de maneira efetiva e poupa a largura de banda. Para obter mais informações, consulte Extensão do OkHttp.

Métricas de monitoramento do host

Além das métricas de monitoramento de host existentes que o DX APM suporta, as métricas de monitoramento do host para Solaris e Red Hat foram adicionadas recentemente. Para obter mais informações, consulte Monitoramento do host.

Suporte ao monitoramento do NGINX

A extensão do agente de monitoramento do NGINX permite monitorar as seguintes versões do NGINX Server: NGINX Plus e NGINX Community. Você pode usar a extensão para fazer o monitoramento da infraestrutura do NGINX. Para obter mais informações, consulte Monitoramento do NGINX.

Carregamento da instrumentação dinâmica do agente do .NET

Agora, o agente do .NET pode carregar dinamicamente a instrumentação sem exigir reinicializações de aplicativos. Eis alguns exemplos:

- É possível instrumentar um método específico que ainda não corresponda a uma definição de probe existente. Especificamente, é possível instrumentar métodos assíncronos do MVC sem precisar de uma reinicialização.
- O DX APM poderá reavaliar os métodos e modificar a instrumentação quando você executar estas ações:
  - Coloque um novo arquivo .pbd na pasta **hotdeploy**
  - Altere ou remova um arquivo .pbd existente.

Serviços do AWS e do Azure

- A nova extensão do AWS (Amazon Web Services) oferece suporte aos seguintes novos tipos de serviço: computação, armazenamento, troca de mensagens, banco de dados, análises e serviços móveis. Para obter mais informações, consulte Monitoramento do Amazon Web Services.
- A nova extensão de serviços do Azure oferece suporte aos seguintes novos tipos de serviço: computação, armazenamento e análises. Para obter mais informações, consulte Monitoramento do Azure

Problema conhecido do Infrastructure Agent

Defeito DE437143 - Não há métricas do Monitor do host

Válido para:DX APM 10,7 Service Pack 1 (SP1-3),DX APM 11.1.3, Kubernetes e Monitor do host

Sintoma:

Nenhuma métrica é exibida no nó **SystemEdge** da **Exibição da métrica**. Esse problema ocorre nestas condições:

- O Monitor do host é reinstalado por meio do Universal Monitoring Agent
- O processo do CA SystemEdge não é interrompido mesmo quando o Kubernetes destrói o pod correspondente.

Solução:

Siga estas etapas:

1. Efetue logon no nó do **SystemEdge** em que não haja métricas do Monitor do host presentes.
2. Use este comando para encerrar o processo do SystemEDGE se ele estiver em execução: `ps -ef | grep "SystemEDGE" |grep -v grep`
3. Reimplante o Universal Monitoring Agent.

Outubro de 2019

10 de outubro de 2019 - O que há de novo

Guias adicionais do Navegador de métricas

Essas novas guias exibem rastreamentos e erros relacionados a uma transação comercial.

- Guia **Rastreamentos**: esta guia exibe a lista de transações comerciais, os rastreamentos associados e os detalhes do componente.
- Guia **Erros**: esta guia exibe a lista de transações comerciais que contêm erros

Problema conhecido do Infrastructure Agent

Defeito DE437143 - Não há métricas do Monitor do host

Válido para:DX APM 10,7 Service Pack 1 (SP1-3),DX APM 11.1.3, Kubernetes e Monitor do host

Sintoma:

Nenhuma métrica é exibida no nó **SystemEdge** da **Exibição da métrica**. Esse problema ocorre nestas condições:

- O Monitor do host é reinstalado por meio do Universal Monitoring Agent
- O processo do CA SystemEdge não é interrompido mesmo quando o Kubernetes destrói o pod correspondente.

Solução:

Siga estas etapas:

1. Efetue logon no nó do **SystemEdge** em que não haja métricas do Monitor do host presentes.
2. Use este comando para encerrar o processo do SystemEDGE se ele estiver em execução: `ps -ef | grep "SystemEDGE" |grep -v grep`
3. Reimplante o Universal Monitoring Agent.

Agosto de 2019

31 de agosto de 2019 - Novidades!

Suporte para AdoptOpenJDK

A CA Technologies, uma empresa da Broadcom, está mudando para adotar mais tecnologias de código aberto em seus produtos. Como parte dessa estratégia, vários produtos começaram a usar implementações de código-fonte aberto do Java. Para alinhar-se com essa direção corporativa, DX APM adotou o AdoptOpenJDK (11), substituindo o Oracle JDK.

Problema conhecido do Infrastructure Agent

Defeito DE437143 - Não há métricas do Monitor do host

Válido para:DX APM 10,7 Service Pack 1 (SP1-3),DX APM 11.1.3, Kubernetes e Monitor do host

Sintoma:

Nenhuma métrica é exibida no nó **SystemEdge** da **Exibição da métrica**. Esse problema ocorre nestas condições:

- O Monitor do host é reinstalado por meio do Universal Monitoring Agent
- O processo do CA SystemEdge não é interrompido mesmo quando o Kubernetes destrói o pod correspondente.

Solução:

Siga estas etapas:

1. Efetue logon no nó do **SystemEdge** em que não haja métricas do Monitor do host presentes.
2. Use este comando para encerrar o processo do SystemEDGE se ele estiver em execução: `ps -ef | grep "SystemEDGE" |grep -v grep`
3. Reimplante o Universal Monitoring Agent.

3 de agosto de 2019 - Novidades!

Business Payload Analyzer

O Business Payload Analyzer é um sistema de monitoramento de experiência do usuário final que permite acompanhar os serviços para obter informações sem a necessidade de recriar os aplicativos. O Business Payload Analyzer oferece um avançado mecanismo de coleta de dados e geração de relatórios para acompanhar os fluxos de trabalho entre os serviços do Data Center. O Business Payload Analyzer analisa o aplicativo que monitora e captura as transações de negócios e as métricas para calcular as métricas de desempenho. Estas métricas fornecem informações sobre a experiência do usuário. A coleta de dados é automática e não é necessária nenhuma personalização para os aplicativos. No entanto, o administrador do aplicativo pode configurar o sistema por meio da interface do usuário para qualquer monitoramento personalizado.Os recursos principais a seguir estão disponíveis nesta release do Business Payload Analyzer:

- Suporte para capturar cargas dos servidores web do IIS (.NET) e do Apache Tomcat.
- Suporte pronto para uso para captura de URL, cabeçalhos HTTP e formulários HTML.
- Modo de detecção periódica programada para atualizar o modelo de ciência de dados do campo e a frequência de ocorrência do valor.
- Detecção automática com base em aprendizado do computador e realce dos valores de dados mais importantes, que são definidos como parâmetros de identificação.
- Nomenclatura do Business Transaction (BT) e identificação da segmentação do usuário (ou seja, marcas demográficas, como o valor do carrinho de compras, o saldo da conta e a ID do usuário).
- Capacidade de ajustar a categorização da ciência dos dados dos campos de carga capturada em uma interface gráfica fácil de usar.
- Suporte ao administrador para a renomeação e a captura parcial de campos complexos, como cookies.
- DX APM Integração de topologia.

- As transações comerciais detectadas pelo Business Payload Analyzer são exibidas como elementos do usuário final no mapeamento de aplicativo.
- As transações comerciais detectadas pelo Business Payload Analyzer são exibidas nos rastreamentos do Visualizador de transações comerciais do Team Center.
- As informações demográficas do usuário do Business Payload Analyzer são relatadas como parâmetros de rastreamento no Visualizador de transações comerciais no Team Center.
- As transações comerciais detectadas pelo Business Payload Analyzer relatam integridade e métricas de desempenho para o visualizador de métricas do Team Center.

Introdução

Introdução ao DX APM:

Se desejar...	Fazer isso...	Leia isso...
Saiba mais sobre o Application Performance Management por meio de vídeos.	Vá para os canais CA Technologies e CA Educate do YouTube nas listas de reprodução do APM.	Recursos de vídeo para analistas
Aprimore o seu conhecimento e a sua produtividade sobre o Application Performance Management.	Faça um curso do CA Education, siga um caminho de aprendizagem e faça o treinamento.	DX APM Education and Training (em inglês)
Familiarize-se com os termos do Application Performance Management.	Localize os termos e leia suas definições no Glossário.	Glossário

NOTE
Para baixar e configurar o Cloud Proxy, consulte a documentação do Cloud Proxy.

Suporte e compatibilidade

A página do produto DX APM no site de Suporte da Broadcom/CA fornece o software e a documentação para todas as releases.

Para obter informações sobre o sistema, o ambiente operacional e as versões suportadas, entre em contato com o suporte da Broadcom.

Arquitetura do DX APM

Um ambiente de avaliação do DX APM conta com os seguintes componentes de arquitetura:

- Inquilino: um grupo de usuários que compartilham o acesso com privilégios específicos à instância do software.
- Serviço: um modelo de entrega de software em que o software é licenciado por assinatura. O software é hospedado centralmente.
- OpenShift Pod: um ou mais recipientes que são implantados juntos em um host. Um pod é a menor unidade que pode ser definida, implantada e gerenciada.
- Recipiente: um único recipiente do DX APM que agrupa o Enterprise Manager, o aplicativo de demonstração e o driver de carga.

Um recipiente é atribuído a pods dedicados do OpenShift, e esses pods dedicados são executados em nós dedicados do OpenShift. Portanto, no ambiente de avaliação, a cardinalidade de Inquilino - Serviço - Pod - Recipiente é: 1-1-1-1. A Broadcom mantém um pod inicializado definido para acelerar o processo de integração de inquilinos. Após a integração bem-sucedida, um pod que já esteja em execução é atribuído ao inquilino, e o pool obtém um novo pod. Esses pods agrupados ficam ociosos até um inquilino ser atribuído a eles.

A arquitetura inclui os seguintes itens-chave:

- **Rede**
  A comunicação de consultas e dados do inquilino é obtida com o HTTPS (443). Todo o tráfego de consulta e dados de inquilino é multiplexado por uma única conexão, portanto, todo o tráfego do sistema é direcionado para *.apm.cloud.ca.com. Esse site hospeda um roteador do OpenShift. O roteador do OpenShift, por sua vez, usa o segmento menos significativo do endereço de destino, que carrega um identificador de inquilino exclusivo para

remover a multiplexação do terminal do serviço. Use uma lista branca para o DNS (Domain Name System - Sistema de Nome de Domínio) público *.apm.cloud.ca.com e não dependa de endereços IP, pois eles mudam com frequência.

- **Armazenamento de dados de inquilino e configuração**
  O DX APM armazena tipos diferentes de construção de configuração e dados de monitoramento. Todos esses tipos são externalizados para que os recipientes sejam apresentados sem estado para facilitar as atualizações. Do ponto de vista estrutural, dois tipos de dado são armazenados: com base em arquivo e relacional. Os dados relacionais são armazenados em instâncias do Google Cloud Platform.
- **Gerenciamento de serviços - mecanismo de provisionamento**
  O OpenShift é o mecanismo de provisionamento. Esse microsserviço com base em Java recebe os eventos de gerenciamento e ciclo de vida de inquilinos de forma ascendente (controlado pelo GIS) e realiza as chamadas necessárias à API do OpenShift. Durante a integração, o PE (Provisioning Engine - Mecanismo de Provisionamento) prepara a estrutura de pastas do sistema de arquivos de rede e o esquema do RDS (Relational Database Service) para o inquilino. O mecanismo de provisionamento cresce e torna-se mais rico, conforme novas funcionalidades, como backups e migração, são adicionadas ao DX APM Cloud.

Recursos em vídeo do DX APM

O DX APM tem uma ampla seleção de recursos em vídeo disponíveis para complementar a documentação e demonstrar os recursos do DX APM.

Os links abaixo o levarão às listas de reprodução do DX APM no canal da CA Technologies no YouTube.Quando você clicar em um link, uma nova guia será aberta e o conectará ao vídeo no YouTube.Para visualizar vídeos incorporados em tela cheia, clique no botão de reprodução e, em seguida, clique no logotipo do YouTube, na barra de ferramentas inferior. Uma nova guia será aberta com o vídeo diretamente do YouTube.

Se a sua empresa tiver bloqueado o YouTube, entre em contato com o administrador.

Você pode usar o DX APM para monitorar o desempenho do aplicativo. Você pode identificar áreas do seu ambiente que estão ficando sobrecarregadas e fazer a triagem de possíveis problemas antes que eles afetem a experiência do cliente. Também é possível usar o DX APM para rastrear problemas existentes na resolução.

DX APM: How to Identify the Root Cause of an App Issue

9 minutos e 46 segundos

Omar mostra como navegar na interface do DX APM para determinar rapidamente a origem dos problemas de desempenho.

DX APM: Getting Started Using the Universal Monitoring Agent (vídeo em inglês)

23 minutos e 53 segundos

Rob apresenta os recursos básicos do UMA (Universal Monitoring Agent) do .

DX APM: Getting Started with Funnel Analysis (vídeo em inglês)

33 minutos e 42 segundos

Harish mostra como a análise do funil pode ajudá-lo a monitorar o fluxo de negócios.

DX APM: Understanding and Using the Map and Metric Tree (vídeo em inglês)

12 minutos e 34 segundos

Mostraremos como navegar em camadas do mapeamento para ver os relacionamentos entre os componentes. Saiba mais sobre os atributos e navegue na árvore de métricas.

DX APM Reference Architecture: Understanding the Approach to DX APM Deployment (vídeo em inglês)

21 minutos e 05 segundos

Henrik discute a implantação, a alta disponibilidade, os serviços, a conectividade e o fluxo de dados do DX APM.

DX APM Team Center: How To Use Attributes (vídeo em inglês)

1 hora, 11 minutos e 39 segundos

Andreas apresenta o mapeamento e os atributos explicando o vocabulário, a navegação e as práticas recomendadas.

DX APM: Understanding Experience View, Assisted Triage, and Experience Notebook (vídeo em inglês)

13 minutos e 11 segundos

Descrevemos o uso da Exibição da experiência, dos cartões de experiência, da triagem assistida e do bloco de anotações de experiência.

DX APM: Alarm Analytics: Understanding and Remediation (vídeo em inglês)

28 minutos e 33 segundos

Jan explica insights sobre alarmes, a filtragem e redução de ruídos, os tipos de alarme e seus algoritmos e a correção de alarmes.

DX APM: How to Create Services (vídeo em inglês)

47 minutos e 14 segundos

Apresentamos os serviços do DX APM, o assistente de criação de serviços, como criar seu primeiro serviço e as análises de serviços.

How to Deploy the Universal Monitoring Agent (vídeo em inglês)

8 minutos e 33 segundos

Ensinamos como instalar o UMA (Universal Monitoring Agent), que instrumenta e monitora automaticamente o agrupamento do Kubernetes.

DX APM: How to Triage a Slow Login (vídeo em inglês)

17 minutos e 40 segundos

Usamos um aplicativo de demonstração em execução em um ambiente Kubernetes implantado na nuvem do AWS para orientá-lo por meio do produto CA App Experience Analytics. Examinamos a experiência do usuário final com um aplicativo monitorado. Por exemplo, o usuário final enfrenta falhas durante a última semana ou sessões com logons lentos nas últimas 24 horas.

DX APM: Gaining App-to-Infra Visibility (vídeo em inglês)

9 minutos e 59 segundos

Omar navega pelos níveis do mapeamento, nós e camadas, demonstrando a captura de métricas por meio de marcas e a correlação de métricas.

DX APM: Cluster Management Demo (vídeo em inglês)

10 minutos e 33 segundos

Dominik apresenta serviços de gerenciamento de agrupamentos, implantação de serviços, serviços de inquilino, criação de inquilinos, tokens e monitoramento de desempenho usando métricas.

App Synthetic Monitor: How to Simulate Business Critical Transactions and User Journeys (vídeo em inglês)

10 minutos e 07 segundos

Dominik presenta o DX App Synthetic Monitor e demonstra como criar monitores e scripts sintéticos para replicar a experiência do usuário final.

DX APM: Working with Management Modules in Team Center (vídeo em inglês)

5 minutos e 02 segundos

Apresentamos os módulos de gerenciamento, que permitem aos administradores organizar e gerenciar com facilidade os dados de métrica.

Convenções de diretório e nome de arquivo

A documentação do DX APM usa as seguintes convenções em nomes de arquivo e caminhos de diretório:

Convenção	A convenção refere-se a(o)
<Pasta_principal_do_agente>	Diretório de nível superior em que o agente do Introscope está instalado. Esse diretório é denominado `wily` por padrão.
<Pasta_principal_Db_APM>	Diretório de nível superior em que o servidor de aplicativos está instalado. Geralmente, esse diretório é o mesmo que <pasta_principal_do_agente>.
<AppServer_Home>	O diretório da pasta principal do servidor de aplicativos.
<EM_Home>	O diretório de nível superior em que o Enterprise Manager está instalado.
<Installation_Directory>	O diretório de instalação de um componente do DX APM ou outro aplicativo quando não instalado no diretório padrão ou de costume.
<ProductName_Home>	O diretório de instalação de um produto ou tipo de aplicativo de terceiros. Por exemplo, você pode se referir ao diretório da pasta principal do seu WebSphere Application Server como <pasta_principal_do_WAS>.
<Workstation_Home>	O diretório de nível superior em que a Estação de trabalho está instalada. Geralmente, esse diretório é o mesmo que <pasta_principal_do_EM>.

`<File_Name><version><Operating System or other identifier>.<FileType>`	Um nome de arquivo que inclui informações de identificação específicas. Por exemplo, se você extrair arquivos de um pacote tar para <nome_do_produto> 10.7.0 em um sistema operacional UNIX, baixe `<nome_do_produto> 107.0=.0unix.tar.` O nome do arquivo é exibido nesta documentação como: `<nome_do_produto><10.7.0>.unix.tar`
Barra como separador de caminho (*/*)	O separador de caminho usado nos nomes de diretório para o seu ambiente operacional. Os ambientes e exemplos do UNIX usam a barra em toda esta documentação. Use o separador apropriado para o seu sistema operacional.
Cifrão ($) como variáveis de ambiente	A notação de variável de ambiente usada em seu sistema operacional. Os ambientes e exemplos do UNIX usam o cifrão ($) em toda esta documentação. Use o caractere apropriado para o seu sistema operacional.

Personalizações

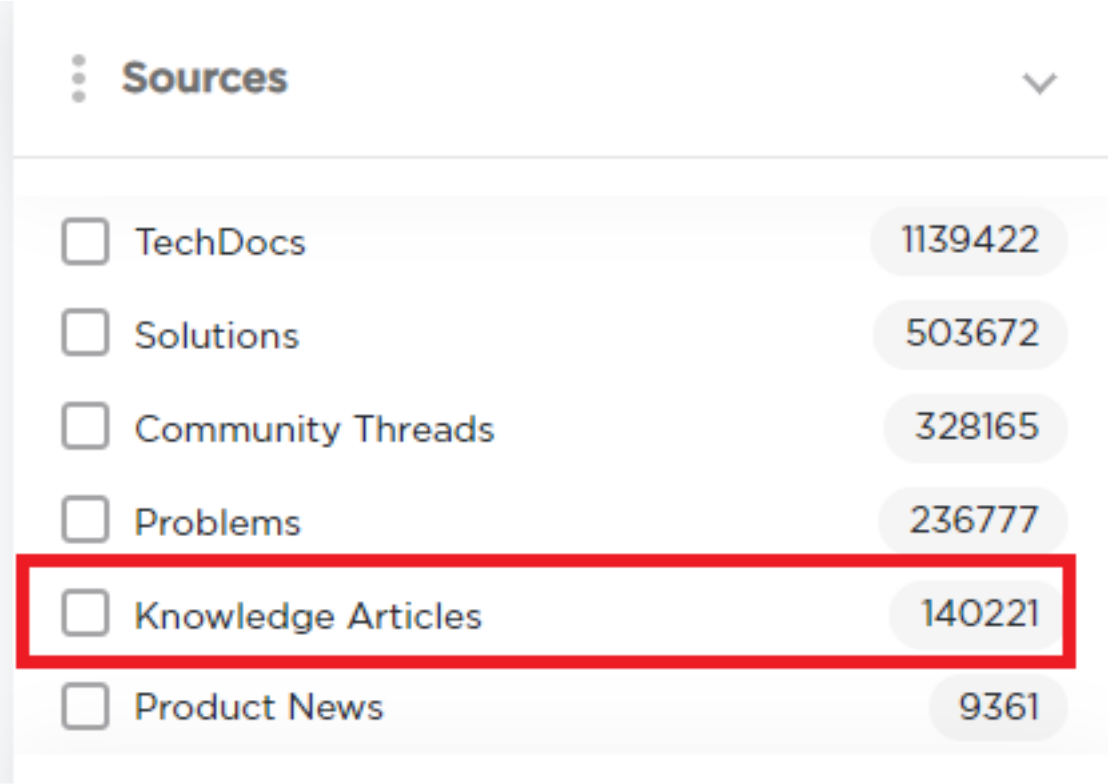
O DX APM é altamente personalizável. No entanto, o Suporte da Broadcom não oferece suporte a personalizações que são feitas para configurações prontas para uso. Por exemplo, você pode personalizar a instrumentação do agente, incluindo a implantação de PBDs personalizados. É possível criar calculadoras de JavaScript personalizadas, bem como scripts de shell e EPAgent para extensões de agente. Quando acreditamos que as personalizações estão causando um problema no produto, podemos pode pedir que você as remova ou as desative. Depois, consideramos oferecer mais ajuda. Para obter ajuda com uma personalização nova ou existente do DX APM, entre em contato com o arquiteto da solução do cliente.

Artigos da base de conhecimento

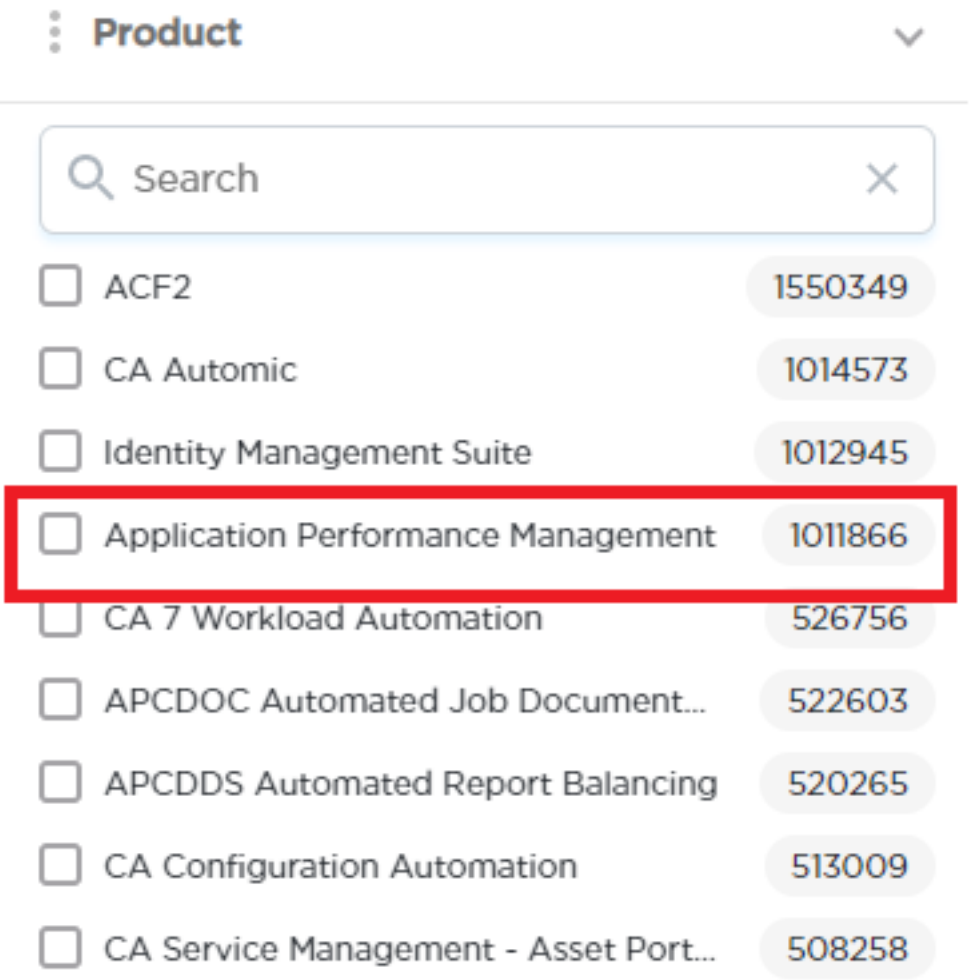
Para exibir a lista completa de artigos da base de conhecimento para o DX Application Performance Management, clique aqui.

Use os filtros de pesquisa avançada para refinar os critérios de pesquisa.

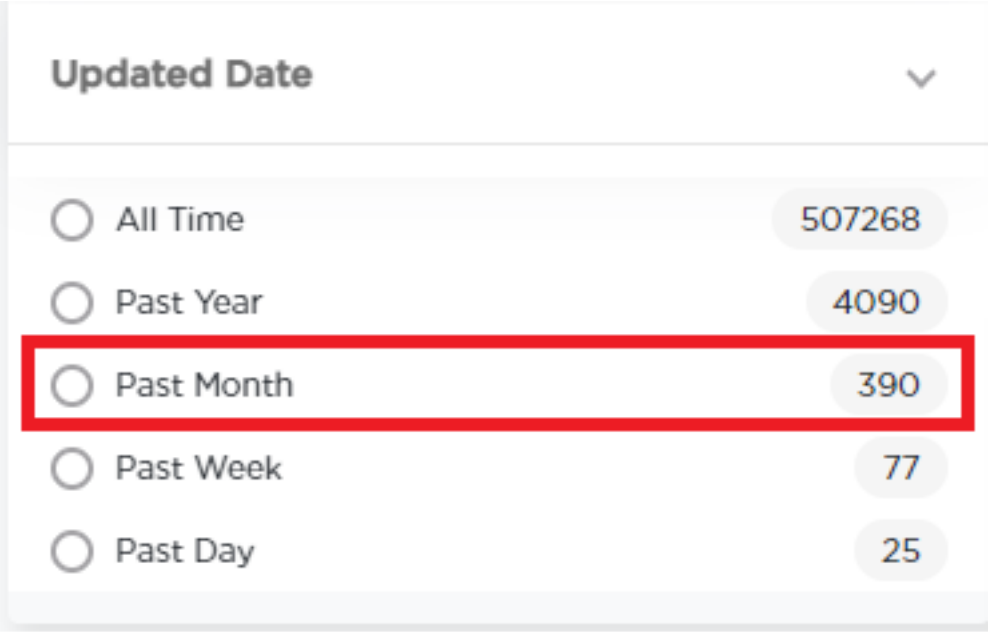
1. Selecione artigos de conhecimento na lista de opções disponíveis em **Origens.**



2. Selecione o Application Performance Management nas opções do **produto**.



3. Selecione o idioma necessário.
4. Selecione a duração necessária nas opções **Updated Date**.



5. Os artigos de conhecimento relevantes para os critérios de filtro especificados são exibidos.

Glossário

Este glossário fornece descrições dos principais termos do DX APM.

> **NOTE**
> Todos os termos se aplicam ao DX APM local e apenas alguns termos se aplicam ao DX APM.

Agente do .NET

O *agente do .NET* coleta métricas sobre aplicativos Microsoft .NET.

Consulte também: CLR (Common Language Runtime) e .NET Framework

.NET Framework

O Microsoft *.NET Framework* é um ambiente de desenvolvimento e execução que permite que diferentes linguagens de programação e bibliotecas trabalhem em conjunto. O .NET Framework baseia-se em um ambiente de tempo de execução que é conhecido como CLR (Common Language). O CLR usa linguagens de programação, como C#.

Consulte também: CLR (Common Language Runtime), Agente do .NET

agente

O *agente* coleta métricas de aplicativo e ambientais e as retransmite ao Enterprise Manager. Esses aplicativos podem ser de qualquer um dos tipos: Java, .NET, PHP ou aplicativos web. Um aplicativo que relata métricas a um agente é designado como instrumentado.

Consulte também: Instrumentado, Agente do Java, Agente do .NET, Agente do PHP

agente - topologia de rede do Gerenciador corporativo

O agente - topologia de rede do Enterprise Manager é a estrutura de rede do ambiente do DX APM. Essa topologia especifica quais agentes ou grupos de agentes podem se conectar a:

- Gerenciadores corporativos independentes específicos
- Coletores
- Grupos de coletores

balanceamento de carga do agente

O *balanceamento de carga do agente* equilibra a carga de métricas entre os Coletores em um ambiente agrupado. Agentes específicos, que são atribuídos ao MOM, equivalem à contagem de métricas entre os coletores. Os agentes específicos direcionam outros agentes para enviar seus dados de métricas para o coletor menos sobrecarregado no agrupamento.

Consulte também: agente, Coletor, MOM (Manager of Managers - Gerenciador de Gerenciadores)

alerta

Um *alerta* é um conjunto salvo de valores de limite para "Cuidado" e "Risco", com outras propriedades concomitantes. Um alerta é um dos objetos base em um Módulo de gerenciamento, que salva as coletas desses objetos para reutilização. Um alerta geralmente tem ações associadas a ele, mas as ações em si são objetos distintos do Módulo de gerenciamento.

Faça a distinção entre o alerta em si (por exemplo, o nome do alerta que é associado aos valores de limite salvos) e:

- *Indicador de alertas*, que é uma exibição gráfica do status do alerta
- *Notificação de alertas*, que é uma das ações possíveis para associação a um alerta.

armazenamento do Amazon EBS

O Amazon EBS (Elastic Block Store) é um volume de armazenamento no nível de bloco que persiste independentemente do tempo de vida útil de uma instância do EC2. É recomendável usar esse tipo de armazenamento em sua instância para que você possa interromper e reiniciar a instância posteriormente.

Imagem de máquina da Amazon

Uma AMI (*Amazon Machine Image - Imagem de máquina da Amazon*) é uma imagem de computador criptografada, semelhante a um modelo, da unidade raiz de um computador. As AMIs contêm o sistema operacional e podem incluir software e camadas do aplicativo. Exemplos de camadas são servidores de banco de dados, middleware e servidores web. A AMI é armazenada no Amazon Elastic Block Store ou Amazon Simple Storage Service.

banco de dados do APM

O *banco de dados do APM* é um banco de dados relacional que armazena dados.

Consulte também: banco de dados SmartStor, banco de dados Eventos de transação

Application Performance Management (APM)

O produto *DX APM*. O DX APM fornece uma estratégia de gerenciamento de desempenho de aplicativos que permite que você entenda a experiência do usuário final e avalie os SLAs (Service Level Agreements - Acordos de Nível de Serviço). É possível mapear todas as transações para a infraestrutura completa. Você também pode realizar a triagem de incidentes e o diagnóstico de causa raiz em uma solução completa e integrada.

suportabilidade do aplicativo

O DX APM avalia a *suportabilidade do aplicativo* medindo o desempenho de vários componentes do aplicativo. As métricas fornecem informações sobre JVM/CLR, aplicativos web e sistemas de back-end.

O DX APM fornece métricas de suportabilidade para que você possa responder às perguntas sobre a integridade dos aplicativos. A suportabilidade do aplicativo também é conhecida como integridade do aplicativo.

App Synthetic Monitor (ASM)

O *DX APM ASM (App Synthetic Monitor)* é um produto que cria transações sintéticas para complementar o monitoramento de transações no DX APM. O ASM fornece, com antecedência, um aviso sobre problemas de disponibilidade do aplicativo.

atributo

Atributos são rótulos que são aplicados a nós em diferentes componentes e identificam suas relações com outros componentes.

regras de atributo

Regras de atributo são regras que automatizam o processo de adição de atributos personalizados. Somente os administradores podem criar regras de atributo.

rastreamento automático de transação

Quando a instrumentação inteligente é ativada, os rastreadores altamente otimizados de baixa sobrecarga coletam um *rastreamento automático de transação* sob condições específicas do disparador. Um erro pode ser um disparador. Outro exemplo de disparador é quando o rastreador `ComponentTimeAutoTraceTriggerTracer` é implementado e o tempo de resposta do componente é excedido. Os rastreamentos automáticos de transação exibem componentes de visibilidade profunda e têm características que diferem dos rastreamentos não automáticos de transação, como rastreamentos manuais e de exemplo.

AutoProbe

O *AutoProbe* do DX APM automatiza o processo de instrumentação do aplicativo adicionando probes dinamicamente ao aplicativo na inicialização. Os probes do DX APM fornecem os dados de origem para as métricas do DX APM.

Consulte também: instrumentado, ProbeBuilder

Promoção automática

Quando você ativa *Promoção automática*, todas as alterações feitas nas configurações do Business Payload Analyzer são aplicadas automaticamente.

back-end

Um *back-end* é um sistema externo do qual um aplicativo web depende para alguma parte de seu processamento. Por exemplo, um back-end pode ser um banco de dados, um servidor de email, um sistema de processamento de transações ou um sistema de troca de mensagens. O DX APM identifica automaticamente bancos de dados, sistemas JMS e terminais HTTP.

Para outros sistemas externos, o DX APM analisa a atividade de soquete do aplicativo a fim de detectar e monitorar back-ends *sem configuração manual*. Esse recurso é chamado de detecção *automática de back-end*.

As métricas de back-end são exibidas sob o nó Backends na árvore do Navegador de métricas.

Consulte também: front-end, ponto de entrada

tempo de back-end

O *tempo de back-end* é a medida de tempo que o componente Blame suspeito (por exemplo, um componente de banco de dados) do sistema back-end leva para ser concluído, com base no relatório do DX APM. O tempo de back-end é medido no componente Java que invoca o back-end. Portanto, o tempo inclui o tempo de processamento do back-end e qualquer tempo de rede gasto se comunicando com o back-end.

Consulte também: back-end, componente Blame suspeito

linha de base

A *linha de base* é um conjunto inicial de dados usado como uma comparação ou um controle. O DX APM usa algoritmos de linha de base para monitorar aplicativos web.

O DX APM determina a cor de um indicador de alerta na guia **Visão geral**, avaliando métricas atuais em relação a uma linha de base para essas métricas. Com um nó de agente selecionado na árvore centrada no agente, o nó Heuristics mostra os valores de métricas relacionados a esses indicadores.

Para uma determinada métrica, o algoritmo de linha de base do DX APM determina o próximo valor esperado e o desvio esperado desse valor. Quando o desvio real exceder (2x) ou exceder significativamente (4x) o desvio esperado, a linha de base indicará uma violação moderada ou grave.A heurística associada se torna amarela ou vermelha.

Internamente, a linha de base avalia a inclinação da série temporal e determina o valor esperado da inclinação. Os dados mais recentes recebem mais peso do que os dados mais antigos.

Consulte também: métricas heurísticas, especificação

Blame

O *Blame* do DX APM é a tecnologia usada para instrumentar um aplicativo. O DX APM rastreia as interações do componente e a utilização de recursos marcando front-ends e back-ends do aplicativo. O DX APM também fornece métricas para investigações de problemas.

Consulte também: back-end, front-end, instrumentado, Rastreador de transações

BT Listener

O BT Listener (Business Transaction Listener) é um componente do Business Payload Analyzer que filtra e roteia somente os dados de interesse solicitados pelo BT Diviner. Um BT Listener é implantado entre o plugin e o BT Diviner. O BT Listener é suportado no Windows e no Linux.

aplicativo comercial

Um *aplicativo comercial* é um programa de software que automatiza um serviço comercial. O DX APM monitora transações web, que são o produto de aplicativos web. Um aplicativo comercial faz parte da hierarquia de transações.

serviço comercial

No SOA Performance Management, um serviço comercial faz solicitações de saída aos sistemas de back-end para o barramento de serviço corporativo.

componente da transação comercial

Um *componente de transação comercial* representa um par de solicitação/resposta HTTP que é instrumentado e monitorado para rastrear a integridade de uma transação comercial. Os componentes da transação comercial são a origem das métricas de integridade do mapeamento.

O componente da transação comercial é o único componente de identificação da transação.

Um componente da transação comercial é semelhante a estes dois componentes:

- Transação (pois trata-se de uma transação de identificação da transação comercial).
- Componente da transação (pois trata-se de um componente de identificação em uma transação).

Consulte também: transação, componente da transação, hierarquia de transações

atributos capturados

No Business Payload Analyzer, você pode definir os atributos que deseja capturar em cada transação quando disponíveis como *atributos capturados*.Os atributos capturados com valores numéricos, com o tempo, podem virar tendência como KPIs no Navegador de métricas ou painéis.

Consulte: Introdução aos atributos do Business Payload Analyzer

Regra de captura

No Business Payload Analyzer, a *regra de captura* define os atributos a serem capturados em cada transação, quando disponíveis.

limite

Um *limite* é o número configurável de métricas que são retornadas para uma função específica. Usada na definição de limite do rastreamento de transação e na definição de limite da métrica para vários componentes do DX APM, como agentes, e do Enterprise Manager.

Consulte também: limite de métrica, Rastreador de transações

Coletor

Um *coletor* é um Enterprise Manager usado em um ambiente agrupado. O MOM (Manager of Managers) gerencia os coletores em ambientes agrupados.

Consulte também: Enterprise Manager, MOM (Manager of Managers)

CLR (Common Language Runtime)

CLR (*Common Language Runtime*) é a implementação da CLI (Common Language Infrastructure) pela Microsoft. A finalidade da CLI é fornecer uma plataforma independente de linguagem para execução e desenvolvimento de aplicativos.

O .NET CLR, em linhas gerais, é equivalente à JVM da plataforma Java.

Consulte também: Agente do .NET, .NET Framework

configurar

No DX APM, *configurar* tem uma definição específica. *Configurar* é definir ou alterar valores ou entradas em propriedades, scripts, PBDs, PBLs, etc. O Suporte da Broadcom oferece suporte a configurações descritas na documentação do DX APM.

Consulte também: personalizar

Console, Estação de trabalho

O *console* é a exibição padrão quando a estação de trabalho é iniciada. O console contém painéis que mostram dados de desempenho em exibições gráficas.

Consulte também: painel, Estação de trabalho, Workstation

recipiente

Um *recipiente* se refere a um ambiente de tempo de execução Java para beans corporativos. Um recipiente que é executado em um servidor EJB (Enterprise JavaBeans) gerencia os ciclos de vida dos objetos de bean corporativo, coordena transações distribuídas e implementa a segurança do objeto.

Consulte também: transação

personalizar

No DX APM, *personalizar* tem uma definição específica. *Personalizar* é programar uma nova forma de monitorar, criar script, processar, formatar um plugin, etc.

O DX APM é altamente personalizável. No entanto, o Suporte da Broadcom não oferece suporte a personalizações que são feitas para configurações prontas para uso. Por exemplo, você pode personalizar a instrumentação do agente, incluindo a implantação de PBDs personalizados. É possível criar calculadoras de JavaScript personalizadas, bem como scripts de shell e EPAgent para extensões de agente. Quando acreditamos que as personalizações estão causando um problema no produto, podemos pode pedir que você as remova ou as desative. Depois, consideramos oferecer mais ajuda. Para obter ajuda com uma personalização nova ou existente do DX APM, entre em contato com o arquiteto da solução do cliente.

Consulte também: configurar

painel

Um *painel* combina e apresenta métricas de aplicativo em exibições para monitorar o ambiente geral do aplicativo. Os painéis fornecem informações detalhadas de desempenho que são necessárias para triagem, diagnóstico e resolução ágeis de problemas para aplicativos de produção. No Team Center, o Painel mostra a integridade geral do ambiente.

Consulte também: métrica

métrica inativa

Uma *métrica inativa* não apresenta relato de dados novos dentro de um determinado período. A quantidade de tempo pode ser configurada.

Consulte também: métrica dinâmica, métrica

componente de visibilidade profunda

Um *componente de visibilidade profunda* é um método ou componente que o agente detecta e exibe automaticamente sem o uso de PBDs (ProbeBuilder Directives - Diretivas do ProbeBuilder). Quando a instrumentação inteligente está ativada, o agente analisa métodos para a sua complexidade a fim de determinar as chamadas e os componentes a serem instrumentados e exibidos como componentes de visibilidade profunda.

Análise diferencial

A *Análise diferencial* é uma abordagem para identificar automaticamente alterações importantes no desempenho dos aplicativos. A criação de linhas de base herdadas prevê o que é normal. A Análise diferencial procura variação não controlada no Tempo médio de resposta dos aplicativos de front-end e das métricas de transação comercial. A variação não controlada aparece como picos em alguma forma de fluxo de dados estável, o que não é muito diferente de como um sismógrafo detecta terremotos.

programação de detecção

Uma *programação de detecção* determina o que deve ser detectado na atividade do aplicativo Business Payload Analyzer.

atributos desconsiderados

No Business Payload Analyzer, os atributos que o BT Listener detecta na atividade do aplicativo com base na regra de detecção são categorizados como atributos desconsiderados.

Consulte: Introdução aos atributos do Business Payload Analyzer

domínio

Um *domínio* do DX APM é uma maneira de particionar a lógica de gerenciamento e agentes, de modo a definir quais usuários podem ver quais informações.

rede de pilha dual

Em uma *rede de pilha dual*, aplicativos e serviços IPv4 e IPv6 são suportados. Isso exige hosts e roteadores para implementar os protocolos IPv4 e IPv6.

A abordagem de pilha dual é uma forma comum de introduzir o IPv6 em uma arquitetura IPv4 existente. Essa abordagem permite que as redes ofereçam suporte ao IPv4 e IPv6 durante o período de transição, aguardando que serviços e aplicativos IPv6 se tornem disponíveis mais prontamente.

DX APM

O *DX APM* é uma solução de gerenciamento corporativo de desempenho de aplicativos que permite:

- Monitorar aplicativos complexos em ambientes de produção 24 horas por dias, 7 dias por semana.
- Detectar problemas antes que eles afetem os clientes.
- Resolver esses problemas de maneira rápida e colaborativa.

Consulte também: agente, Enterprise Manager, métrica

propriedade dinâmica

Uma *propriedade* dinâmica nos arquivos de configuração do DX APM (por exemplo, o arquivo `IntroscopeAgent.profile`) é implantada assim que o arquivo de configuração é salvo. Não é necessário reiniciar o aplicativo ou os servidores de aplicativos para que a alteração entre em vigor.

ativar aplicativo

Os dados de um aplicativo são enviados ao Business Payload Analyzer somente quando o aplicativo é ativado. Para ativar um aplicativo, defina a programação de detecção que determina o que deve ser detectado na atividade do aplicativo.

Consulte: Introdução aos atributos do Business Payload Analyzer

extensão

Uma *extensão* do DX APM é um código de programa (arquivo JAR) que estende a funcionalidade básica do Enterprise Manager ou de um agente.

Consulte também: Enterprise Manager, Agente

Gerenciador corporativo

O *Gerenciador corporativo* armazena e agrega métricas de desempenho do aplicativo, como tempo de resposta, largura de banda e alocação de memória. Vários agentes, espalhados por toda a empresa, coletam e retransmitem métricas de aplicativos e do ambiente e as reportam ao Gerenciador corporativo.

Consulte também: Coletor, MOM (Manager of Managers - Gerenciador de Gerenciadores)

ponto de entrada

Quando a detecção automática do ponto de entrada e a instrumentação inteligente estão ativadas, o DX APM monitora automaticamente os segmentos que estão envolvidos nas transações de chamada de soquete do cliente. Os *pontos de entrada* são os pontos de início da transação. Os pontos de entrada são exibidos na árvore centrada no agente e nos rastreamentos de transação.

Consulte também: instrumentação inteligente, back-end automático

EPAgent, EPA (Environmental Performance Agent - Agente de Desempenho Ambiental)

O *EPAgent, EPA (Environmental Performance Agent - Agente de Desempenho Ambiental)* é uma versão modificada do agente que ajuda a integrar dados de métrica de origens genéricas e não Java ao DX APM. O EPA usa scripts simples que permitam ao agente monitorar praticamente qualquer tipo de subsistema de aplicativo que tenha um impacto no desempenho. Por exemplo, servidores de diretório, sistemas operacionais, middleware de troca de mensagens e servidores de transação.

Consulte também: agente, plugins com estado, plugins sem estado

instantâneo de erro

O ErrorDetector gera um *instantâneo de erro*, que exibe informações detalhadas sobre o que estava acontecendo quando um erro ocorreu. Os dados do instantâneo de erro são armazenados no banco de dados Evento de transação.

Consulte também: ErrorDetector

ErrorDetector

O *ErrorDetector* permite que a equipe de suporte do aplicativo detecte e diagnostique a causa de erros graves, o que pode impedir que usuários concluam transações web.

Os erros "graves" predefinidos que se baseiam em informações que estão contidas nas especificações PHP, J2EE e .NET incluem estes erros:

- Erros HTTP (por exemplo, 404 e 500)
- Erros de instrução SQL
- Erros de conectividade de rede (erros de tempo limite)
- Erros de back-end (por exemplo, não é possível enviar uma mensagem por meio do JMS, não é possível gravar uma mensagem na fila de mensagens).

Consulte também: instantâneo de erro

evento

Um *evento* do DX APM é qualquer ação para a qual os agentes capturam métricas. Exemplos incluem rastreamentos de transação, erros e paralisações.

Consulte também: ErrorDetector, métrica, paralisação, rastreamento de transação

extensão

As *extensões* são aplicativos do DX APM que *estendem* os recursos de monitoramento de dados do agente. As extensões integram-se facilmente aos componentes padrão do DX APM, fornecendo mais visibilidade do ambiente e de seus aplicativos monitorados.

Algumas extensões exigem uma reinicialização do aplicativos, e outras não. É possível ativar as extensões que são fornecidas com o DX APM.

FIPS (Federal Information Processing Standards - Padrões de Processamento de Informações Federais)

O *FIPS* são padrões publicamente anunciados. O governo federal dos EUA desenvolveu esses padrões para serem usados por todas as agências governamentais não militares e prestadores de serviços públicos. Muitos padrões FIPS são versões modificadas dos padrões usados no setor mais amplo de software.

A publicação do FIPS 140-2, "Security Requirements for Cryptographic Modules" (Requisitos de segurança para módulos criptográficos), especifica o padrão de segurança para as bibliotecas criptográficas. Essa publicação especifica os algoritmos que os produtos de software devem usar para criptografia. A criptografia afeta o armazenamento e verificação de senha. Ela também afeta a comunicação de todos os dados confidenciais entre componentes de um produto e entre produtos.

front-end

Um *front-end* é o componente de um aplicativo que primeiro manipula uma transação de entrada. Em aplicativos J2EE mais comuns, esse componente é um servlet ou um JSP. Em algumas instâncias de Java, ele pode ser um EJB ou algum outro componente. O DX APM identifica automaticamente os servlets e JSPs como front-ends, mas não qualquer outro componente. Para marcar um componente explicitamente como front-end, use o rastreador `FrontendMarker` .

Consulte também: back-end

pilha gráfica

Em um rastreamento de transação, a *pilha gráfica* é a representação da ordem dos componentes da transação de cima para baixo. Você pode se referir à pilha gráfica como "bolo de casamento", pois a representação pode se parecer com um bolo de casamento de cabeça para baixo. A pilha gráfica é vista no Visualizador do rastreamento de transação.

Consulte também: rastreamento de transação, Rastreador de transações

GUID

O *GUID* (Globally Unique Identifier - Identificador Global Exclusivo) é uma chave exclusiva gerada por `ServletHeaderDecorator` . A chave identifica uma transação no aplicativo comercial monitorado. O GUID é a principal informação que correlaciona algumas transações.

Os GUIDs podem ser criados de várias maneiras. Normalmente, os GUIDs são uma combinação de configurações exclusivas que se baseiam em um horário específico. Por exemplo, um GUID pode ser uma combinação de um endereço IP, endereço MAC de rede, data e hora.

Consulte também: endereço MAC, ServletHeaderDecorator

sinal de monitoramento

Um *sinal de monitoramento* é o intervalo de tempo de quando as métricas são verificadas, normalmente, em segundos.

métricas heurísticas

As *métricas heurísticas* do DX APM são usadas para avaliar e relatar status. Elas são números inteiros, que são símbolos de status e não de medição. O valor de uma métrica heurística é determinado pela avaliação de métricas atuais em relação a uma linha de base para essas métricas.

Você pode definir alertas em termos de métricas heurísticas em vez de limites fixos. Definir alertas usando métricas heurísticas determinando os valores normais de KPIs (Key Performance Indicators - Indicadores Chave de Desempenho) muda o trabalho do administrador do APM para o DX APM.

Consulte também: linha de base, métrica

propriedade oculta

Uma *propriedade oculta* é uma propriedade em um arquivo de configuração. A propriedade é disponibilizada para uso somente quando você a adiciona ao arquivo de configuração. Por exemplo, um arquivo de configuração é o arquivo IntroscopeAgent.profile ou o arquivo IntroscopeEnterpriseManager.properties.

HTTPHeaderDecorator

O *HTTPHeaderDecorator* do DX APM é uma extensão do agente que aumenta os cabeçalhos de resposta HTTP para os agentes do .NET.

Consulte também: GUID, ServletHeaderDecorator, Rastreador de transações

atributos de identificação

Os atributos que você deseja incluídos na regra de nomenclatura de transação comercial podem ser definidos como atributos de identificação.A regra de nomenclatura nomeia uma transação comercial de maneira exclusiva que ajuda a identificá-la no DX APM.

Consulte: Introdução aos atributos do Business Payload Analyzer

componente de identificação

O *componente de identificação* é o primeiro componente de transação no conjunto de componentes de transação. O componente de identificação identifica exclusivamente o início de uma transação. Um componente de identificação não deve ser um componente de qualquer outra transação.

> **NOTE**
> Um redirecionamento pode ser exibido como o primeiro componente em um registro de transação, porém, ele não é o componente de identificação.

Consulte também: hierarquia de transações

transação de identificação

A *transação de identificação* é a primeira transação em um conjunto de transações comerciais. A transação de identificação identifica exclusivamente o início de uma transação comercial. Uma transação de identificação não deve ser uma transação de qualquer outra transação comercial.

Consulte também: hierarquia de transações

Tipo de instância

O *Tipo de instância* é uma especificação que define a capacidade da memória, da CPU e do armazenamento, bem como o custo por hora de uma instância no AWS (Amazon Web Services). Os tipos de instância podem ser criados para aplicativos padrão ou aplicativos que fazem uso intenso de CPU e memória.

instrumentado

O código de aplicativo é *instrumentado* quando o ProbeBuilder insere probes, dentro do código de byte, para enviar métricas ao agente.

Consulte também: agente, AutoProbe, aplicativo gerenciado, ProbeBuilder

Investigador, Estação de trabalho

O *Investigador* da Estação de trabalho permite exibir o status do sistema e do aplicativo, pesquisar os dados de métrica e navegar por eles usando uma estrutura em árvore. Você pode ter mais de uma janela do investigador aberta simultaneamente.

Consulte também: Console, Estação de trabalho; Workstation

Agente do Java

O *agente do Java* coleta métricas em ambientes Java.

porta de escuta

Uma *porta de escuta* é usada para simplificar a administração da associação entre uma fábrica de conexão, o destino e o bean orientado a mensagens implantado.

métrica dinâmica

Uma *métrica dinâmica* relata dados de maneira ativa de um agente específico.

Consulte também: métrica inativa, métrica

tempo lógico

O *tempo lógico* é a medida de tempo que o código do programa do componente Blame suspeito leva para ser concluído. Esse tempo tem como base a geração de relatórios do DX APM.

Consulte também: componente Blame suspeito

endereço MAC

O *endereço de MAC* (endereço Media Access Control) é um endereço de hardware que identifica exclusivamente cada nó de uma rede.

O endereço MAC pode ser útil durante o processo de resolução de problemas. Por exemplo, quando os servidores web estão localizados atrás de um balanceador de carga que mascara a verdadeira identidade do servidor web no nível de IP. Por exemplo, em ambientes de balanceamento de carga Resonate, todos os servidores web parecem ter o mesmo endereço IP. No entanto, o endereço MAC que é enviado na resposta pode identificar com exclusividade os servidores.

aplicativo gerenciado

Quando um aplicativo instrumentado está em execução, ele é chamado de *aplicativo gerenciado*.

Consulte também: instrumentado

Módulo de gerenciamento

Um *Módulo de gerenciamento* contém um conjunto de informações de configuração de monitoramento. Os Módulos de gerenciamento são listados para cada domínio e contêm elementos. Os elementos são objetos que contêm e organizam dados com lógica de monitoramento como alertas, ações e painéis.

Consulte também: painel. WebView, Estação de trabalho

MOM (Manager of Managers - Gerenciador de Gerenciadores)

O *MOM* (*Manager of Managers*) armazena métricas conforme relatadas por vários Enteprise Managers. O agrupamento de Gerenciadores corporativos permite que um Gerenciador corporativo - o MOM - gerencie outros Gerenciadores corporativos. Cada um dos Gerenciadores corporativos gerenciados, chamados Coletores, coleta métricas de agente e depois as retransmite ao MOM.

Consulte também: Coletor, EM (Enterprise Manager - Gerenciador Corporativo)

mapa

No Team Center, o *mapa* mostra os relacionamentos entre componentes individuais no ambiente.

valor mediano

O *valor mediano* é um único valor que representa uma distribuição de dados. O valor mediano é preferível ao valor médio como uma representação de número único de uma distribuição quando esta não é uma distribuição normal (curva em sino).

limite de métrica

Um *limite de métrica* é um limite no número de métricas do agente e no Gerenciador corporativo. Um limite de métrica ajuda a evitar picos no número de métricas relatadas (explosões de métrica) no Gerenciador corporativo.

Consulte também: agente, limite, métrica

explosão de métrica

Uma *explosão de métrica* ocorre quando novas métricas são exibidas em grandes números em um curto período. As definições de métrica configuradas incorretamente podem fazer com que os metadados da métrica mudem com as alterações do valor da métrica e sejam exibidos como novas métricas. Por exemplo, sequências de caracteres variáveis em uma métrica SQL. As propriedades de conexão do agente configuradas incorretamente para um conjunto de novos agentes podem fazer com que milhares de novas métricas sobrecarreguem o Gerenciador corporativo. Essas situações podem reduzir o desempenho.

Consulte também: vazamento de métrica, agente, limite, métrica

agrupamento de métricas

Os *agrupamentos de métricas* são objetos do Módulo de gerenciamento que salvam estas informações:

- A *expressão do agente* -- uma expressão regular em Perl 5 que filtra entradas na métrica especificando os dados até, e inclusive, o nome do agente.
- A *expressão da métrica* -- uma expressão regular em Perl 5 que especifica o recurso (a cadeia de pastas que leva à métrica) e a métrica.
- O Módulo de gerenciamento ao qual o agrupamento de métricas pertence.

vazamento de métrica

Um *vazamento de métrica* ocorre quando uma configuração incorreta do DX APM resulta em agentes relatando métricas por um tempo limitado. Esse problema resulta em um acúmulo gradual de metadados de métrica sem dados de métrica associados.

Consulte também: explosão de métrica, agente, limite, métrica, DX APM

aceleração de métrica

Uma *aceleração de métrica* interrompe um agente quando a sua saída de métrica se torna excessiva.

Consulte também: agente, limite, métrica

metric, DX APM

Uma *métrica do DX APM* é uma medida do desempenho do aplicativo. Estes são os tipos de métrica:

- Largura de banda - atividade de soquete e arquivo no nível de CLR e JVM
- Simultaneidade - número de invocações de método que foram iniciadas, mas ainda não foram finalizadas
- Contagem - número de invocações de método até o dia atual
- Exceção - exceções de captura
- Memória – memória que é alocada para a JVM ou CLR em uso, conforme relação com a coleta de lixo
- Taxa - número de execuções de método por segundo ou intervalo de tempo
- Tempo de resposta - tempo médio de execução do método em milissegundos
- Métodos paralisados — número de métodos que foram iniciados, mas cujos tempos de invocação excederam um limite.
- Logs do sistema — monitoram a saída do sistema e de erros do sistema.
- Segmentos — número de segmentos instrumentados

Consulte também: limite de métrica, explosão de métrica, aceleração de métrica

porta espelhada

Uma *porta espelhada* é um recurso de software de comutadores e roteadores de rede.

Consulte também: exploração de rede

tolerância a falhas do MOM

A *tolerância a falhas do MOM* ocorre quando o Enterprise Manager do MOM é desconectado ou desativado devido a uma falha de rede ou hardware. A tolerância a falhas ocorre quando você configurou um segundo Gerenciador corporativo do MOM para assumir o controle do primeiro Gerenciador corporativo do MOM.

Consulte também: Coletor, EM (Enterprise Manager - Gerenciador Corporativo), MOM (Manager of Managers - Gerenciador de Gerenciadores)

monitor

Os agentes *monitoram* todo o desempenho da web, componentes Java e suas dependências, componentes CLR e suas dependências, conexões com sistema back-end, recursos do servidor de aplicativos e os níveis de recurso (incluindo software de terceiros).

Consulte também: agente, sincronizar todos os monitores

regra de nomenclatura

Uma regra de nomenclatura também pode ser definida como uma sequência de caracteres dos atributos de identificação. A regra de nomenclatura nomeia uma transação comercial de maneira exclusiva que ajuda a identificá-la no DX APM.

exploração de rede

Uma *exploração de rede* é um dispositivo de hardware que explora diretamente o cabeamento da infraestrutura. Esse dispositivo cria cópias de pacotes e as encaminha a um ou mais destinos.

Consulte também: porta espelhada

nó

Um *nó* é o local em que informações específicas da métrica são reunidas e mostradas na exibição em árvore Navegador de métricas. Por exemplo, o Investigador mostra o nó de back-ends ou o nó de utilização da CPU. Quando o nó é expandido, informações mais detalhadas podem ser exibidas e pesquisadas. No Team Center, um nó representa componentes diretamente monitorados e agregados e transações comerciais em um contexto topológico.

Consulte também: Investigador, Estação de trabalho, métrica, Workstation

OLA (Operating Level Agreement - Acordo de Nível Operacional)

Um *OLA* é um acordo entre uma organização de TI e os grupos de suporte internos. Os termos do contrato dependem das necessidades das partes envolvidas. Os OLAs são usados para gerenciar a conformidade dos compromissos de serviço por grupos de TI.

oportunidade

Uma *oportunidade* é qualquer área dentro de um produto, processo, serviço ou outro sistema onde pode ocorrer um defeito. Em geral, produtos mais complexos significam mais oportunidades de defeitos.

Consulte também: defeito, especificação

resposta parcial

Uma *resposta parcial* significa que uma resposta completa não foi observada para um componente específico dentro do período configurável esperado (o padrão é de 60 segundos).

Consulte também: resposta ausente

Paciente zero

O *Paciente zero* é o primeiro componente de uma série de dependências que indica problemas de desempenho. Esse componente parece ser a origem da degradação do desempenho em seu ambiente de aplicativos. O Paciente zero provavelmente é a causa raiz do problema.

valor do percentil

O *valor do percentil* de uma distribuição é um número em que uma porcentagem da distribuição é inferior ou igual ao valor desse percentil. Por exemplo, o 25º percentil (também conhecido como o quartil inferior) é onde 25% dos valores de dados ficam abaixo dele.

Este é outro exemplo. Para um gráfico de tempo de resposta, o número no 95º percentil significa que 95% das transações nesse período tiveram um tempo de resposta nesse nível ou abaixo.

perspectiva

Uma *perspectiva* agrupa componentes de modo lógico na interface do usuário. Os grupos se baseiam em seus atributos compartilhados.

Agente do PHP

O *Agente do PHP* coleta métricas em aplicativos PHP.

plugin

O *plugin* é um dos componentes do Business Payload Analyzer. O Business Payload Analyzer inclui plugins para estes servidores web:

- Servidor web Apache (Windows e Linux)
- Servidor web do IIS
- Servidor web Nginx

regra de privacidade

Uma regra de privacidade permite mascarar valores de campo que você não deseja que sejam exibidos na UI nem armazenados no banco de dados. Por exemplo, é possível mascarar os últimos quatro dígitos do número do cartão de crédito usado para transações ou usar hash unidirecional SHA-256 para a descrição médica de um paciente. Para obter mais informações, consulte a seção Menu Ações.

probe

Um *probe* mede partes de informações específicas sobre um aplicativo sem alterar a lógica comercial do aplicativo. Um agente é instalado no mesmo computador que o aplicativo web instrumentado.

Consulte também: agente, instrumentado, ProbeBuilder

ProbeBuilder

O *ProbeBuilder* executa o processo de instrumentação, no qual rastreadores identificam as métricas que um agente coleta de aplicativos e as máquinas virtuais no tempo de execução. Os rastreadores são definidos nos arquivos PBD (ProbeBuilder Directives - Diretivas do ProbeBuilder).

Consulte também: agente, AutoProbe, PBD (ProbeBuilder Directive - Diretiva do ProbeBuilder)

PBD (ProbeBuilder Directive - Diretivas do ProbeBuilder)

Os arquivos *ProbeBuilder Directive (PBD)* informam o ProbeBuilder como adicionar probes a componentes PHP, .NET ou Java para instrumentar o aplicativo. Exemplos de probes são temporizadores e contadores.Os arquivos de Diretivas do ProbeBuilder administram as métricas específicas que os agentes relatam ao Gerenciador corporativo.

As Diretivas personalizadas também podem ser criadas para rastrear classes e métodos exclusivos a aplicativos específicos.

Consulte também: AutoProbe, EM (Enterprise Manager - Gerenciador Corporativo), ProbeBuilder, PBL (ProbeBuilder Lists - Listas do ProbeBuilder)

PBL (ProbeBuilder Lists - Listas do ProbeBuilder)

Um arquivo *PBL* contém uma lista de vários arquivos de Diretivas do ProbeBuilder. Vários arquivos PBL podem se referir aos mesmos arquivos PBD.

Consulte também: AutoProbe, ProbeBuilder, PBD (ProbeBuilder Directive - Diretiva do ProbeBuilder)

ProbeBuilding, dinâmico

O *ProbeBuilding dinâmico* é útil para fazer correções em PBDs ou para alterar os níveis de coleta de dados durante a triagem sem interromper o serviço de aplicativo.

tempo de processamento

No App Synthetic Monitor, o *tempo de processamento* é o período depois que a solicitação HTTP é enviada e o monitor aguarda pelos primeiros bytes do resultado.

ServletHeaderDecorator

O *ServletHeaderDecorator* do DX APM amplia os cabeçalhos de resposta HTTP usando servlets de agentes Java.

O GUID é usado como o identificador de transação. O ServletHeaderDecorator é uma extensão de agente.

Consulte também: GUID, Rastreador de transações

SiteMinder

O *SiteMinder* do DX APM é um aplicativo que fornece recursos de segurança, como logon único e controle centralizado de acesso do usuário aos aplicativos web.

instrumentação inteligente

A *instrumentação inteligente* é um método que o DX APM usa para instrumentar aplicativos. Esse método usa rastreadores de sobrecarga baixa altamente otimizados. Os rastreadores permitem que agentes detectem e instrumentem automaticamente mais métodos para fornecer componentes de visibilidade profunda sem o uso de PBDs (ProbeBuilder Directives - Diretivas do ProbeBuilder). A instrumentação inteligente também fornece o rastreamento automático de transação.

Consulte também: rastreamento automático de transação, componentes de visibilidade profunda

banco de dados SmartStor

O *banco de dados SmartStor* é um banco de dados não relacional que registra todos os dados de desempenho do aplicativo (métricas do agente) o tempo todo. Esse banco de dados permite aos usuários analisar dados históricos, identificar causas raiz do tempo de inatividade do aplicativo ou executar análise de capacidade sem a necessidade de um banco de dados externo.

O SmartStor é ativado por padrão durante a instalação do DX APM. Os dados do SmartStor são definidos para expirar ao longo do tempo, de modo que o repositório de dados não fique excessivamente grande. Há vários arquivos de dados e eles aumentam em número à medida que mais dados são gerados.

Consulte também: banco de dados do APM, banco de dados Eventos de transação

especificação

Uma *especificação* é um requisito para uma transação ou um componente de uma transação. Se uma transação ou um componente não atender ao requisito que foi estabelecido na especificação relacionada, sua definição será "com defeito". Por exemplo, um defeito de lentidão pode ser definido como qualquer transação com tempo superior a 5 segundos.

Consulte também: defeito, limite de especificação superior

paralisação

Uma *paralisação* do DX APM normalmente se refere aos métodos que foram iniciados, mas com tempos de invocação que excederam um limite.

Consulte também: métrica

bolhas de inicialização

Uma *bolha de inicialização* é o limite de tempo temporário quando há alta demanda de recursos que pode afetar mais do que os relatórios de métricas do DX APM. Durante a bolha de inicialização, o aplicativo instrumentado poderá não responder.

É possível que outros componentes, que compartilham recursos com o aplicativo instrumentado ou que estejam no mesmo ambiente, sejam afetados. As bolhas de inicialização podem ser observadas com o Agente do .NET no tempo de inicialização.

Consulte também: Agente do .NET

plugins com estado

É esperado que os *plugins com estado* sejam scripts de execução longa (como daemons). Os plugins com estado são iniciados quando o EPAgent (Environment Performance Agent - Agente de Desempenho do Ambiente) é iniciado e executado para sempre, alimentando dados no DX APM por meio do canal de standard output do plugin. Quando um plugin com estado é encerrado, o EPA o reinicia.

Consulte também: EPAgent, EPA (Environmental Performance Agent - Agente de Desempenho Ambiental), plugins sem estado

plugins sem estado

Os *plugins sem estado* foram desenvolvidos para execução em uma programação recorrente e são configurados com a frequência (especificada como atraso entre execuções) na qual eles devem ser executados. Espera-se que os plugins sejam scripts de execução curta que simplesmente coletem alguns dados, os enviem ao EPA por meio do canal de standard output e sejam encerrados. O EPA não faz nenhuma verificação especial de erro para garantir que apenas uma instância de um plugin sem estado seja executada por vez, de modo que os desenvolvedores de plugins devem desenvolver seus plugins sem estado para execução e conclusão em um limite de tempo razoavelmente curto.

Consulte também: EPAgent, EPA (Environmental Performance Agent - Agente de Desempenho Ambiental), plugins com estado

SuperDomain

O nó *SuperDomain* contém métricas para todos os agentes que se reportam ao Gerenciador corporativo ao qual a Estação de trabalho está conectada e inclui todos os domínios e agentes definidos pelo usuário. Esse nó pode ser visto somente pelos usuários com acesso ao SuperDomain. As métricas são organizadas em uma hierarquia Host|Processo|Agente.

métricas de suportabilidade

As *métricas de suportabilidade* do DX APM ajudam a oferecer suporte ao funcionamento íntegro do Enterprise Manager em si. O Gerenciador corporativo gera e coleta métricas sobre si mesmo que são úteis na avaliação de sua integridade e na identificação de como está o seu desempenho tendo em vista a sua carga de trabalho.

componente de back-end Blame suspeito

O *componente de back-end Blame suspeito* é a parte mais específica do tempo de back-end que é identificado como sendo a causa suspeita do atraso em uma transação lenta. No DX APM, o componente de back-end Blame suspeito é exibido como o componente de back-end mais amplo, mas não necessariamente o mais baixo, no gráfico.

> **NOTE**
> Ele é o componente de back-end *mais baixo e lento*, e não o componente de back-end *mais lento e baixo* nos gráficos do DX APM.

O componente de back-end Blame suspeito é identificado por usar o componente de back-end mais baixo que leva mais de 1/4 do tempo geral de back-end para ser concluído.

componente Blame suspeito

O *componente Blame suspeito* é a parte mais específica da lógica (ou do código do programa) que é identificada como sendo a causa suspeita do atraso em uma transação lenta. No DX APM, o componente Blame suspeito é exibido como o componente mais amplo, mas não necessariamente o mais baixo, no gráfico.

> **NOTE**
> Ele é o componente *mais lento e baixo*, e não o componente *mais baixo e lento* nos gráficos do DX APM.

O componente Blame suspeito é identificado por usar o componente mais baixo (não de back-end) que leva mais de 1/4 do tempo geral de transação para ser concluído.

métrica de sustentabilidade

Uma *métrica de sustentabilidade* fornece informações sobre o estado interno do agente, e não do aplicativo que o agente está monitorando. Esses dados podem ajudar a investigar o comportamento do agente.

Team Center

O *Team Center* é uma interface do usuário que fornece uma visão geral de um ambiente de aplicativos.

tempo da primeira resposta

O *tempo da primeira resposta* é o tempo decorrido desde o *último* pacote da solicitação até o primeiro pacote da resposta para o componente.

O tempo da primeira resposta varia de acordo com o tipo de defeito que está sendo rastreado:

- Defeito de componente, o tempo da primeira resposta para esse componente
- Defeitos de transação, o tempo da primeira resposta para o componente de identificação da transação
- Defeito de transação comercial, o tempo da primeira resposta para o componente de identificação da transação de identificação

> **NOTE**
> Essa configuração pode ser alterada para o *primeiro* pacote da solicitação para o primeiro pacote da resposta. Se precisar dessa configuração para determinar a latência de entrada da rede, entre em contato com o Suporte da Broadcom.
>
> Alterar essa configuração afeta apenas os dados novos. (Os valores de dados existente se baseiam na configuração do tempo da primeira resposta que estava em vigor no momento em que os dados foram coletados.)

linha de tempo

Na interface do usuário, a *Linha do tempo* permite que você passe do modo dinâmico para o passado e veja quais eventos de status ocorreram. A Linha de tempo ajuda a investigar onde um problema começou.

transação

Uma *transação* do DX APM é a invocação e o processamento de um serviço. Trata-se de um ciclo completo de processamento, onde o contexto do aplicativo define a conclusão:

- No contexto de um aplicativo web, é a invocação e o processamento de um URL enviado de um navegador.
- No contexto de um serviço web, é a invocação e o processamento de uma mensagem SOAP de um cliente de serviços web.

O DX APM pode capturar transações, bem como incluir detalhes sobre a solicitação que foi feita nos serviços e os detalhes que estão relacionados ao processamento do serviço, como chamadas feitas a um banco de dados SQL.

Uma transação geralmente consiste em um componente HTML, seguido por zero ou mais subcomponentes (por exemplo, folha de estilo CSS, arquivos JS JavaScript, imagens GIFs e JPG). Para cada transação, há um componente de transação de identificação.

Uma única ação do usuário pode resultar em uma ou várias transações, que são encapsuladas em uma transação comercial.

Consulte também: hierarquia de transações

banco de dados Eventos de transação

O *banco de dados Eventos de transação* contém dados detalhados da transação. Esses dados incluem rastreamentos de transação, paralisações e dados que são coletados de eventos disparados, como instantâneos de erro.

O banco de dados Eventos de transação geralmente reside no diretório de rastreamentos e inclui vários arquivos. É criado um arquivo por dia, e os dados são mantidos pelo número de dias especificado.

Consulte também: banco de dados do APM, banco de dados SmartStor, transação, Rastreador de transações

hierarquia de transações

As métricas e informações do DX APM são organizadas em uma *hierarquia de transações*. Essa hierarquia é uma maneira de converter serviços e transações comerciais em elementos HTTP técnicos que criam a experiência do cliente.

A hierarquia de transações do DX APM é:

Um aplicativo comercial é um programa de software que automatiza um serviço comercial. Todas as transações (que usam serviço comercial, transação comercial e, por fim, transação) são associadas a uma aplicativo comercial.
Exemplo: Siebel
Exemplo: Avitek

Um serviço comercial é um grupo arbitrário de transações comerciais.
Exemplo: Avitek Financial (inclui compra, venda, consulta)
Exemplo: Siebel Call Center (inclui logon, além de outras transações comerciais Siebel)

Uma transação comercial é um conjunto de transações que representa uma ação do usuário.
Exemplo: conjunto relacionado à compra (pode incluir várias transações relacionadas à compra)
Exemplo: conjunto relacionado à venda (pode incluir várias transações relacionadas à venda)

Uma transação é um conjunto de componentes de transação que geralmente representa uma solicitação ao servidor de aplicativos.
Exemplo: compra (a transação real de compra)
Exemplo: consulta ao preço para compra (uma consulta relacionada à compra)

Um componente de transação comercial é usado no DX APM como uma alternativa ao conjunto completo de transações e componentes de transação que pertencem a uma transação comercial. O componente de transação comercial corresponde ao componente de transação de identificação da transação de identificação, para a qual é denominado.
Exemplo: enviar compra (o elemento de identificação da transação *e* a transação de identificação da transação comercial)

Um componente de transação é um elemento de nível baixo que representa um par de solicitação/resposta HTTP.
Exemplo: enviar compra (o elemento de identificação da transação que pode ser JavaScript)
Exemplo: main.css (um elemento de não identificação, mas essencial da transação)

Um parâmetro de transação é o elemento de nível mais baixo na hierarquia; um par de nome/valor HTTP.
Exemplo: caminho do URL=/dir/file.html (o elemento de identificação do componente)
Exemplo: Cookie=JSESSIONID

parâmetro de transação

Um *parâmetro de transação* é um par de nome/valor HTTP, que consiste em um tipo, um nome e um padrão. Os exemplos incluem URL, consulta, publicação e cookie (por exemplo: host do URL=www.company.com).

Consulte também: hierarquia de transações

O *tamanho da transação* é o tamanho, em bytes, do tráfego HTTP observado para uma transação. O tamanho inclui o cabeçalho HTTP, bem como as solicitações e respostas HTTP. O tamanho não inclui Ethernet, IP e cabeçalhos TCP.

rastreamento de transação

Um *rastreamento de transação* é a saída do Rastreador de transações. O rastreamento contém uma lista de componentes que são chamados durante uma transação, e seus tempos de duração associados.

Consulte também: Rastreador de transações

duração do rastreamento de transação

A *duração do rastreamento de transação* é o tempo de execução para a *sessão de rastreamento de transação*. A duração máxima da sessão de rastreamento de transação é um limite de tempo. O valor padrão é de 30 minutos.

Consulte também: Rastreador de transações

limite de tempo de rastreamento de transação

O *limite de tempo de rastreamento de transação* é o limite de tempo da execução para a *transação*. Quando um rastreamento de transação está em execução, todas as transações que não foram concluídas dentro do limite são rastreadas.

O limite de tempo de rastreamento de transação é uma porcentagem, que se baseia na especificação do defeito de lentidão. Por exemplo, a especificação do defeito de lentidão é definida para 8 segundos e o limite de tempo de rastreamento de transação é definido para 25%. Todas as transações com um componente Blame suspeito (tempo lógico) superior a 2 segundos são rastreadas.

Consulte também: tempo lógico, componente Blame suspeito, Rastreador de transações

Rastreador de transações

O *Rastreador de transações* monitora a atividade de transações individuais, à medida que elas fluem por estes limites:

- De uma única JVM (Java Virtual Machine - Máquina Virtual Java)
- Da plataforma virtual CLR (Common Language Runtime), no caso do .NET.

O Rastreador de transações reduz o tempo que é necessário para identificar componentes com problemas em uma transação. O rastreador permite rastrear a atividade da transação no nível de componente.

tempo de transferência

No App Synthetic Monitor, o *tempo de transferência* é o período que se leva para concluir os dados de resposta HTTP.

volume de transações

O *volume de transações* é a soma de tamanhos de todas as transações para um período especificado.

triagem

A *triagem* é o processo de:

1. Coletar informações relevantes a um problema.
2. Decidir a gravidade do problema.
3. Atribuir o problema à pessoa que pode corrigi-lo mais rapidamente. A pessoa que trata dessa fase de análise do problema pode ser chamado de responsável pela triagem.

universo

Um *universo* é um grupo significativo de componentes que é ajustado para as necessidades de um usuário ou grupo específico na interface do usuário.

USL (Upper Specification Limit - Limite de Especificação Superior)

O *limite de especificação superior*, ou USL, é um valor numérico que define o valor mais alto aceitável para a característica. Por exemplo, um USL pode ser a taxa de transferência da transação mais alta aceitável.

Conjunto de regras de correspondência de URL

O conjunto de regras de correspondência de URL é o URL a ser monitorado.

banco de dados de variação

O *banco de dados de variação* do DX APM armazena os estados de perfil de desvio e previsão mais recentes para métricas avaliadas pela Análise diferencial. Esses perfis servem como entrada para o mecanismo de regras internas.O mecanismo então produz intensidade de variação para métricas que são exibidas no mapa Análise diferencial no WebView.

Consulte também: banco de dados do APM, métricas heurísticas, banco de dados SmartStor, banco de dados Eventos de transação

WebView

O *WebView* apresenta os painéis personalizáveis e exibições em árvore do Investigador em uma interface de navegador. O WebView permite que informações essenciais sejam exibidas sem o auxílio da Estação de trabalho. Consulte também: Web Start da Estação de trabalho

Estação de trabalho

A *Estação de trabalho* permite controlar o DX APM e acessar as métricas de desempenho. Na Estação de trabalho, é possível executar essas ações e muito mais:

- Definir alertas para métricas individuais ou grupos de métricas lógicos.
- Exibir métricas de desempenho.
- Personalizar exibições para seu próprio ambiente exclusivo.

Consulte também: Web Start da Estação de trabalho

Web Start da Estação de trabalho

O *Workstation Web Start* usa o Java Web Start para iniciar a Estação de trabalho.

Como administrador, você pode criar e configurar alertas e ações no Team Center para monitorar o desempenho. O Team Center oferece os seguintes alertas:

- Alerta simples
- Alertas de resumo

Para obter mais informações sobre como criar, atualizar, excluir e configurar um alerta simples, consulte Criar e configurar alertas simples no Team Center.

Confirmações de software de terceiros - SaaS

Esta seção contém contratos de licença de softwares de terceiros para aplicativos que são adicionados/incluídos como parte da release atual do DX APM.Clique aqui para fazer download dos TPSRs.

Implementando agentes

Saiba como implementar um ou mais agentes, dependendo dos ambientes que você monitora.

O *agente* é um componente de coleta de dados. Esse componente coleta informações de desempenho detalhadas sobre aplicativos e o ambiente de computação, conforme as transações são executadas. Um aplicativo web que relata métricas a um agente é designado como instrumentado.Depois que o aplicativo web é instrumentado, o agente coleta os dados e os relata ao Gerenciador corporativo. O Gerenciador corporativo processa e armazena os dados para geração de relatórios em tempo real e históricos. Você pode exibir e trabalhar com os dados coletados para criar alertas ou executar uma ação de resposta. Você pode modificar o monitoramento padrão para atingir o equilíbrio de visibilidade e desempenho que é necessário. Uma *extensão do agente* é um código de programa que estende a funcionalidade básica do agente.

Para obter mais informações sobre o Agente, consulte Agentes do DX APM.

Use os seguintes links para acessar a documentação de alguns dos principais agentes:

- Agente do Java
- Agente do .NET/.NET Core
- Infrastructure Agent
- Business Payload Analyzer
- Agente do Node.js

Configurar o ambiente de monitoramento

O ambiente de monitoramento permite identificar, medir e avaliar o desempenho de um aplicativo. É possível executar as seguintes tarefas para configurar o ambiente de monitoramento de modo que ele atenda às suas necessidades.

Criar configurações favoritas

É possível marcar os blocos na página **Configurações** como favoritos. Clique no ícone **marcador** no bloco para adicionar a configuração como favorita no painel de navegação à esquerda.Para remover a configuração como favorita, clique no ícone **Remover** da configuração no painel de navegação à esquerda.

Configurações disponíveis

As seguintes configurações estão disponíveis na página **Configurações**:

Se desejar...	Leia estas informações...
Definir as configurações gerais	• Configurar e fazer download de um pacote de agente para o DX APM • Organizar componentes usando perspectivas • Configurar universos • Definir a forma de monitoramento do ambiente com regras de atributo • Segurança • Notificações • Downloads – Fazer download da Estação de trabalho – Fazer download do Cloud Proxy – Ferramenta de importação do agente **Observação:** é possível acessar a ferramenta de importação do agente somente como administrador principal. • Regras de supressão de rastreamento para ocultar dados confidenciais
Configurar as definições do módulo de gerenciamento	• Criar e trabalhar com módulos de gerenciamento • Configurar agrupamentos de métricas no Team Center • Criar e configurar alertas simples no Team Center • Criar e editar calculadoras
Configurar integrações	• Business Payload Analyzer • Configurar o WebView (apenas DX APM no local) • APM Command Center (acesso somente ao administrador) **Observação:** o WebView está disponível somente no DX APM no local, mas não está ativado por padrão. No entanto, é possível ativar o WebView para inquilinos específicos durante a criação do inquilino. Você também pode ativar o WebView posteriormente para qualquer inquilino já criado. Para obter mais informações sobre como ativar o WebView, consulte Serviços de inquilino. Acessar o WebView e o APM Command Center abre uma nova guia.
Definir outras configurações	Ative o download de agentes no Team Center a partir da Configuração avançada.

Configurações de ambiente adicionais

Além das configurações disponíveis na página **Configurações**, é possível executar as tarefas a seguir para configurar o ambiente.

- Criar notificações para alertas
- Configurar notificações por email para alertas
- Configurar a Exibição da experiência
- Ajustar o monitoramento com alertas
- Configurar a estação de trabalho
- Recomendações de dimensionamento do monitor do Docker

O ambiente de monitoramento permite identificar, medir e avaliar o desempenho de um aplicativo.

Para obter mais informações sobre as tarefas que podem ser executadas para configurar o ambiente de monitoramento de modo a atender às suas necessidades, consulte Configurar o ambiente de monitoramento.

Funções e privilégios suportados

Na plataforma do DX, as seguintes funções são suportadas.

- **Administrador de inquilinos**
- **Usuário avançado**
- **Usuário**

No DX APM, as mesmas funções são mapeadas da seguinte maneira:

- Administrador de inquilinos → **Administrador do APM**
- Usuário avançado → **Usuário do APM**
- Usuário → **Usuário do APM**

Funções e privilégios do DX APM

As exibições no Team Center e em outras UIs têm diferentes níveis de acesso para cada função.

- Exibição da experiência (EV)
- Exibição do agente (AV)
- Perspectiva
- Atributos personalizados
- Universos
- Regras
- Agentes
- Segurança
- Alertas
- Notificação
- Módulos de gerenciamento
- Agrupamentos e calculadoras de métricas
- Calculadoras de JavaScript
- Downloads
- AXA na caixa de diálogo de download do agente
- Página Configurações

Exibição da experiência (EV)

Ação	Administração	Usuário	Usuário avançado
Modificar posição	Sim	Sim	Sim
Adicionar nova Exibição da experiência	Sim	Sim	Sim
Tornar a global a Exibição da experiência	Sim	Não	Não
Editar a Exibição da experiência	Sim	Sim	Sim
Excluir a Exibição da experiência	Sim	Sim	Sim
Editar a Exibição da experiência global	Sim	Não	Não
Excluir a Exibição da experiência global	Sim	Não	Não

Exibição do agente (AV)

Ação	Administração	Usuário	Usuário avançado
Adicionar nova Exibição do agente	Sim	Sim	Sim
Tornar global a Exibição do agente	Sim	Não	Não
Editar a Exibição do agente	Sim	Sim	Sim
Excluir a Exibição do agente	Sim	Sim	Sim
Editar a Exibição do agente global	Sim	Não	Não
Excluir a Exibição do agente global	Sim	Não	Não

Perspectiva

Ação	Administração	Usuário	Usuário avançado
Criar perspectiva	Sim	Sim	Sim
Editar perspectiva	Sim	Sim	Sim
Tomar a perspectiva global	Sim	Não	Não
Tornar a perspectiva o padrão	Sim	Não	Não
Excluir perspectiva	Sim	Sim	Sim
Personalizar perspectiva	Não	Sim	Sim

Atributos personalizados

Ação	Administração	Usuário	Usuário avançado
Criar	Sim	Não	Sim
Excluir	Sim	Não	Sim
Modificar	Sim	Não	Sim

Universos

Ação	Administração	Usuário	Usuário avançado
Criar universo	Sim	Não	Não
Renomear universo	Sim	Não	Não
Editar lista de usuários	Sim	Não	Não
Excluir universo	Sim	Não	Não

Regras

Ação	Administração	Usuário	Usuário avançado
Criar regras	Sim	Não	Não
Excluir regras	Sim	Não	Não
Criar regras corporativas	Sim	Não	Não
Excluir regras corporativas	Sim	Não	Não
Duplicar	Sim	Não	Não
Fazer upload das regras	Sim	Não	Não

Agentes

Ação	Administração	Usuário	Usuário avançado
Fazer download de agente	Sim	Não (O administrador pode controlar em **Configurações**)	Sim
Rastrear todos os agentes.	Sim	Não	Sim
Rastrear agente individual	Sim	Não	Sim
Mostrar detalhes de conexão do agente	Sim	Sim, mas (botão **Gerar token** depende da visibilidade da caixa de diálogo de download do agente)	Sim

Segurança

Ação	Administração	Usuário	Usuário avançado
Criar token de API	Sim	Sim	Sim
Gerar token do agente	Sim	Sim - se a caixa de diálogo de download do agente estiver visível (pode ser controlável pelo administrador em **Configurações**)	Sim
Criar token de sistema	Sim	Não	Não

Ação	Administração	Usuário	Usuário avançado
Invalidar token	Sim	Próprio	Próprio
Renomear	Sim	Próprio	Próprio
Definir expiração	Sim	Próprio	Próprio

Alertas

Ação	Administração	Usuário	Usuário avançado
Alerta de leitura	Sim	Sim	Sim
Criar alerta	Sim	Não	Não*
Excluir alerta	Sim	Não	Não*
Ativar/desativar alerta	Sim	Não	Não*
Editar alerta	Sim	Não	Sim

Notificação

Ação	Administração	Usuário	Usuário avançado
Ler	Sim	Sim	Sim
Criar notificação	Sim	Não	Não

Módulos de gerenciamento

Ação	Administração	Usuário	Usuário avançado
Ler	Sim	Sim	Sim
Criar	Sim	Não*	Não*
Modificar	Sim	Não*	Não*
Excluir	Sim	Não*	Não*

Agrupamentos e calculadoras de métricas

Ação	Administração	Usuário	Usuário avançado
Ler	Sim	Sim	Sim
Criar	Sim	Não*	Não*
Excluir	Sim	Não*	Não*
Modificar	Sim	Não*	Não*

Calculadoras de JavaScript

Ação	Administração	Usuário	Usuário avançado
Ler	Sim	Sim	Sim
Criar	Sim	Não	Não

Ação	Administração	Usuário	Usuário avançado
Modificar	Sim	Não	Não
Excluir	Sim	Não	Não

Downloads

Ação	Administração	Usuário	Usuário avançado
Acessar página de download	Sim	Sim	Sim

AXA na caixa de diálogo de download do agente

Ação	Administração	Usuário	Usuário avançado
Criar aplicativo AXA (na caixa de diálogo de download do agente)	Sim	Não	Sim

Página Configurações

Ação	Administração	Usuário	Usuário avançado
Acesso ao Command Center (bloco ACC)	Sim	Não	Sim

* Esse privilégio é o padrão. Os usuários e grupos podem receber privilégios usando o módulo de segurança Universo.

Mais informações: Configurar universos.

A plataforma do DX oferece suporte às seguintes funções:

- Administrador de inquilinos
- Usuário avançado
- Usuário

Para obter mais informações sobre as funções do DX APM e seus privilégios, consulte Funções e privilégios suportados.

Gerar token de segurança

Os tokens de segurança são usados para autenticar solicitações e autorizar a concessão para os agentes. Usando a configuração **Segurança**, você pode gerar os tokens offline que nunca expiram. Esses tokens são usados para acessar as APIs públicas. Você também pode gerar tokens para autorizar agentes ou inquilinos.

> **IMPORTANT**
> A geração de tokens de segurança é uma tarefa apenas de administrador. Você deve ser um administrador principal para gerar o token de segurança. Se você for um inquilino, entre em contato com a equipe de operações de SaaS da Broadcom para obter um token de segurança.

Gerar um token

Siga estas etapas:

1. Efetue logon no Team Center e clique em **Configurações**, bloco **Segurança**.
2. Clique em **Gerar outro token**.
   A caixa de diálogo **Novo token de segurança da API** é exibida.

3. Defina os seguintes detalhes:
   – **Rótulo** (nome): nome do token de segurança.
   – Selecione o tipo de token de segurança:
     - **Agente:** token para autorizar um agente.

       NOTE
       As informações de expiração de um token de agente são definidas dentro do token. Portanto, não será possível alterar a expiração do token após a criação.
     - **API pública:** token para acessar uma API pública. Você pode definir uma data de validade para os tokens da API pública ou pode definir o token para nunca expirar.
     - **Token do inquilino**: token para conceder acesso a um inquilino.

       NOTE
       As informações de expiração de um token de inquilino são definidas dentro do token. Portanto, não será possível alterar a expiração do token após a criação.
4. Clique em **Gerar token**.
   O sistema gera um novo token.

   WARNING

   Por motivos de segurança, você vê um token apenas uma vez. Armazene o token em um local seguro antes de fechar essa janela da caixa de diálogo. Não divulgue o token para indivíduos não autorizados.

   O token agora é exibido entre os outros tokens na guia **Segurança**.

Gerenciar tokens

Para cada token, é possível executar as seguintes ações:

- **Renomear**: se você deseja alterar o nome do token
- **Revogar**: se você deseja revogar a autorização para as APIs ou os agentes
- **Cancelar revogação**: para restaurar a autorização para as APIs ou os agentes
- **Definir expiração**: para APIs públicas, se você tiver definido o token para nunca expirar, usando a opção **Definir expiração**, será possível escolher uma data e hora de expiração do token, isto é, quando o token não pode ser usado para autorizar as APIs públicas.

Os tokens de segurança são usados para autenticar solicitações e autorizar a concessão para os agentes. Usando a configuração Segurança, você pode gerar os tokens offline que nunca expiram. Esses tokens são usados para acessar as APIs públicas. Você também pode gerar tokens para autorizar agentes ou inquilinos.

Para obter mais informações sobre tokens de segurança, consulte Gerar token de segurança.

Criar notificações para alertas

O DX APM permite criar notificações para alertas. As notificações podem retransmitir automaticamente alertas do Application Performance Management tratando desde serviços internos, como listas de distribuição, até serviços externos, por meio da API REST, ou PagerDuty, uma plataforma de resolução de incidentes.

Para obter mais informações sobre como configurar notificações por email, consulte Configurar notificações por email para alertas.

O vídeo a seguir mostra a terminologia, o fluxo de trabalho e exemplos para a criação de notificações para alertas.

PagerDuty

O PagerDuty realize a análise do incidente e envia notificações diretamente aos administradores de TI designados para resolução. Use a integração do PagerDuty para monitorar o sistema em busca de eventos críticos por meio de um

caminho definido, responder rapidamente e manter o sistema em funcionamento com mínimo tempo de inatividade. Para obter mais informações sobre os recursos do PagerDuty, acesse https://www.pagerduty.com.

Para trabalhar com eficiência nos dois sistemas, siga estas regras:

- Um alerta no DX APM dispara um incidente no PagerDuty. O PagerDuty então transmite o incidente como um ticket para um destinatário designado.
- Um alerta que é limpo no DX APM resolve o incidente no PagerDuty. Resolver um incidente no PagerDuty não limpa o alerta no Application Performance Management.

Fluxo de trabalho do incidente

Quando um alerta é gerado e corresponde às definições de configuração do serviço, o DX APM dispara um incidente automaticamente. Os incidentes no PagerDuty contêm as seguintes informações de um alerta para identificar o componente afetado:

- `alertStartTime`
- `alertState`
- `alertName`
- `alertId`
- `vertexId`
- `vertexAttributes` (por exemplo, tipo, nome*)*

O PagerDuty manipula os incidentes de acordo com as configurações de usuário e políticas configuradas.

> **NOTE**
>
> Um alerta limpo no DX APM resolve automaticamente um incidente no PagerDuty. O atraso da notificação é o tempo que o DX APM aguarda antes de disparar um incidente no PagerDuty. O atraso da notificação é útil para reduzir incidentes que são disparados por alertas transitórios.

Criar e modificar uma notificação do PagerDuty

Você deve ter uma conta do PagerDuty para criar uma notificação do PagerDuty. A conta do PagerDuty permite que você configure o comportamento da notificação e receba um Token do usuário da API e uma Chave de integração exclusivos para uso com o DX APM.

Siga estas etapas:

1. Efetue logon no PagerDuty ou crie uma conta.
2. Copie o Token do usuário da API e a Chave de integração do PagerDuty.
3. No DX APM, clique em **Notificações**.
4. Clique em **Create a PagerDuty Notification**.
5. Crie um nome de notificação.
6. Cole o Token do usuário da API e a Chave de integração do PagerDuty.
7. Selecione a gravidade da notificação.
8. Clique em **Salvar**.
9. (Opcional) Selecione a notificação que você deseja alterar e clique em **Editar**.
10. (Opcional) Selecione a notificação que deseja excluir e clique em **Excluir**.

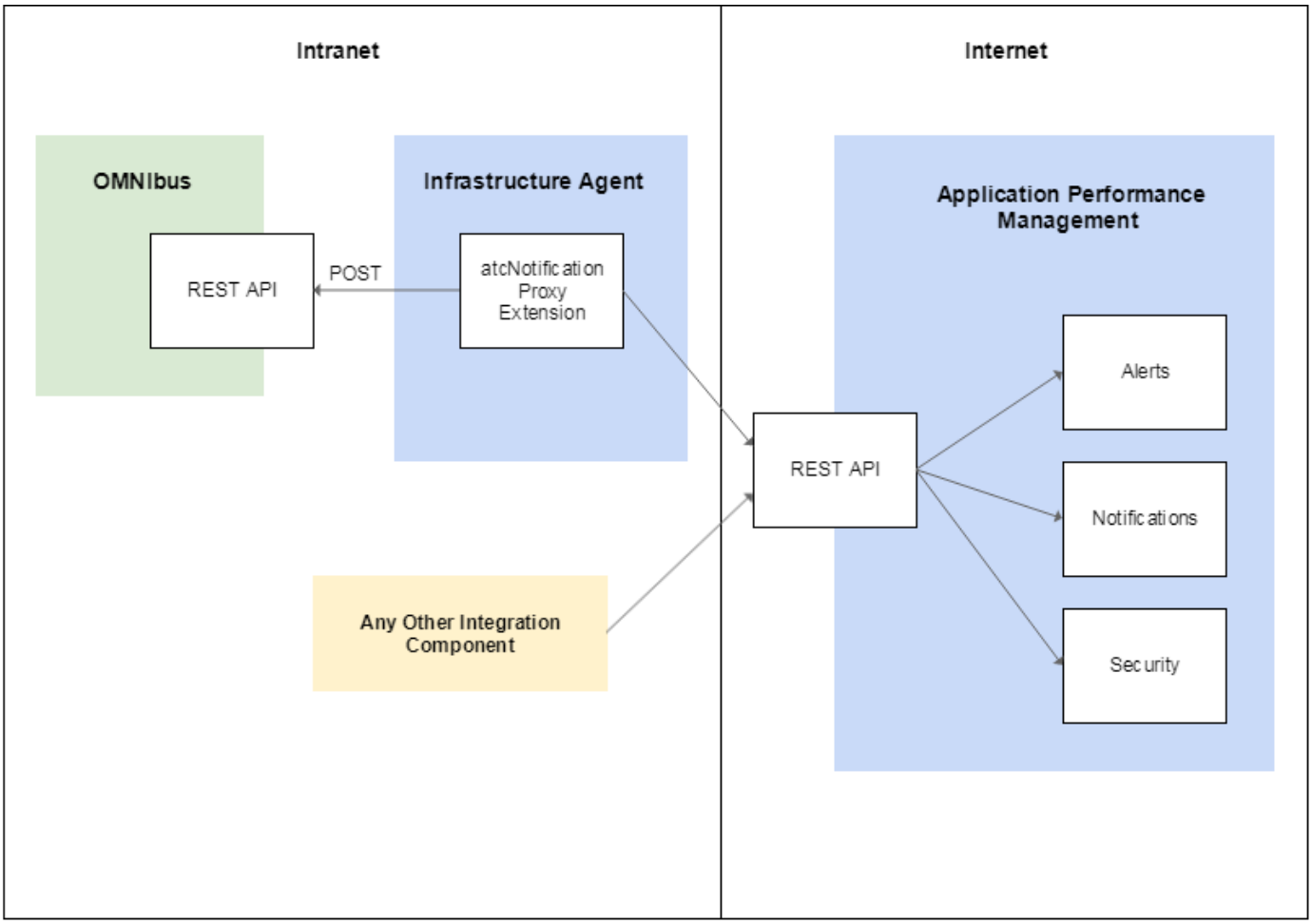
Você criou e modificou uma Notificação do PagerDuty conforme a necessidade.

Notificações da API REST

O DX APM permite que você receba notificações sobre alterações de alerta por meio da API REST. A API REST é a interface de atração que permite que as integrações sejam executadas por trás de firewalls corporativos. Use a API para

integrar as notificações a componentes de terceiros, como vários painéis. O seguinte diagrama mostra a API REST na infraestrutura do Application Performance Management:

Figure 1: Notificação da API REST



Criar e modificar uma notificação da API REST

Siga estas etapas:

1. No DX APM, clique em **Notificações**.
2. Clique em **Create a REST API Notification**.
3. Crie um nome de notificação.
4. Crie um token de proxy exclusivo ou clique em **Gerar token**.
5. Clique em **Salvar**.
6. (Opcional) Selecione a notificação que você deseja alterar e clique em **Editar**.
7. (Opcional) Selecione a notificação que deseja excluir e clique em **Excluir**.

Você criou e modificou uma Notificação da API REST conforme a necessidade.

Integrar as notificações da API REST

Acesse a API REST para integrar as Notificações da API REST a componentes de terceiros.

Siga estas etapas:

1. Gere um token de segurança nas **Configurações** do DX APM. Salve o token de segurança em um local para uso posterior. Para obter mais informações sobre como gerar um token de segurança, consulte Autenticação e autorização da API.
2. Vá para **Notificações** e copie o token do proxy da Notificação da API REST que você deseja integrar.Salve o token do proxy em um local para uso posterior

   NOTE

   Você pode usar o mesmo token de proxy para várias notificações no DX APM. A API REST retorna as notificações de alerta de todas essas configurações de notificação. A chamada à API REST rotula o token do proxy como `proxyKey` . O `proxyKey` identifica o cliente da API REST.
3. Defina o valor da última versão para 0 a fim de receber um status contrário a OK (Cuidado ou Risco) para todos os alertas ativos.
4. Copie o número do host no URL do DX APM. Salve o número do hosts em um local para uso posterior.
5. Cole o número do host, o token de segurança, o token do proxy e a última versão no seguinte comando POST para chamar a API REST:

```
POST
Host: https://<YOUR HOST NUMBER>.apm.cloud.ca.com/apm/appmap/private/graph/
recentstatuschanges
```

Resposta:

A API REST envia um objeto JSON como a resposta. A resposta contém alterações de alerta para todas as notificações com o mesmo valor de token do proxy que ocorreram após a última chamada. A resposta também retorna o campo de versão para a chamada a seguir.

Na resposta, cada notificação contém os seguintes campos:

- – **status** – a gravidade do alerta (OK, CUIDADO, RISCO)
  – **alertName** – nome do alerta
  – **time** – a ocorrência da alteração de status em milissegundos desde o Unix epoch
  – **vertex** – o vértice alertado incluindo todos os atributos de vértice

Exemplo de uma resposta:


```
{
  "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
}
```


Status e códigos de erro HTTP da autenticação

Se a autenticação da solicitação falhar, o servidor de recursos retornará um código de erro HTTP e o cabeçalho de resposta com detalhes do erro.

- 401 Não autorizado – o token de segurança (enviado no cabeçalho HTTP) não é válido para o URL fornecido.
- 403 Proibido – o token do proxy não corresponde a nenhuma configuração de notificação.

Para obter mais informações, consulte as definições de código do status HTTP.

O DX APM permite criar notificações para alertas. As notificações podem retransmitir automaticamente alertas do Application Performance Management tratando desde serviços internos, como listas de distribuição, até serviços externos, por meio da API REST, ou PagerDuty, uma plataforma de resolução de incidentes.

Para obter mais informações sobre as notificações, consulte Criar notificações para alertas.

Configurar notificações por email para alertas

Você pode associar um alerta no DX APM com listas de distribuição de email predefinidas. Usuários, como administradores de TI, que são adicionados às listas de distribuição, são notificados quando o valor da métrica viola os limites de cuidado e risco.

> **NOTE**
>
> Os limites de cuidado e risco do DX APM são denominados limites graves e críticos (respectivamente) no DX SaaS.

Criar uma lista de endereços

1. Efetue logon no DX SaaS como administrador de inquilinos.
2. Selecione **Notificações** (ícone de sino) no painel de navegação à esquerda.
3. Clique na seta no final da linha **Mailing Lists**.
4. Clique em **+ New**.
5. Especifique o nome da lista de distribuição e adicione endereços de email.
6. Salve a lista de distribuição.

Associe uma lista de distribuição a um alerta

Associe uma lista de distribuição a um alerta no DX APM.

> **WARNING**
>
> Alterações nas listas de distribuição, como adicionar ou excluir um novo endereço, só aparecem no painel Alertas depois de 10 minutos. Se a nova lista de distribuição não for exibida em um alerta, verifique o alerta novamente após 10 minutos.

Siga estas etapas:

1. No DX APM, clique no ícone **Alertas**, no painel esquerdo. O painel Alertas é aberto.
2. Selecione o alerta que deseja editar. O menu suspenso Alerta é aberto.
3. Clique no menu suspenso **Notificações**. Uma lista de todas as listas de distribuição disponíveis é exibida.
4. Selecione as listas de distribuição que receberão notificações sobre o alerta em questão.

   > **NOTE**
   >
   > Desmarque as listas de distribuição inválidas que aparecem em vermelho. As listas de distribuição inválidas agora estão excluídas.

5. Clique em **OK** e **Salvar alerta**.

Configurar universos

Universos

Os universos permitem que o administrador refine o número e os tipos de componentes em grupos de autorização fáceis de usar. Esse grupo refinado é um universo. Por motivos de segurança, não há nenhuma atribuição padrão para todos os usuários. Para exibir o DX APM, cada usuário deve estar alocado em um universo. Se não houver um universo associado à ID do usuário, o usuário será avisado. Como administrador, crie universos para os usuários. Use o universo padrão, chamado **Todos os componentes**, ou crie um universo personalizado.

O administrador executa as seguintes tarefas para configurar os universos:

- Cria um universo para as necessidades de usuários ou grupos de usuários.
- Aplica um filtro para selecionar os dados do componente do conjunto de dados.
- (Opcional) Cria vários universos para gerar uma série de espaços gerenciáveis. Os usuários podem alternar facilmente entre os espaços para facilitar a navegação no ambiente.
- (Opcional) Garante que o acesso de um usuário específico seja restrito, conforme exigido pelos requisitos de segurança da empresa.

  > **NOTE**
  >
  > Crie um universo com base em domínios. Crie um filtro **Origens da métrica** e use a mesma expressão regular da definição do domínio. Criar um filtro para os componentes do mapa com base no atributo **agentDomain**, selecione o domínio necessário e selecione **Salvar**.

Como administrador do APM, atribua pelo menos um universo a cada usuário para que eles possam acessar o conteúdo.

Um universo consiste em:

- Um nome – um identificador exclusivo
- Uma descrição - texto opcional para descrever o universo
- Filtros:
  - Filtro de origem da métrica - aplicável em uma exibição de métricas e em gráficos de métricas na exibição do mapa.
  - Filtro de componentes de mapa - aplicável em todas as exibições com base em mapa, como exibição de mapa, exibição de painel, exibição de experiência e exibição do agente.
  - Filtro do módulo de gerenciamento – aplicável ao exibir o conteúdo do módulo de gerenciamento. Por exemplo, alertas no mapa ou painel. Além disso, definições de configuração de calculadoras, origens de métricas e alertas.
- Uma lista de usuários – os usuários com acesso a esse universo

Universos predefinidos

Alguns universos são criados por padrão:

- O universo **Todos os componentes** é criado automaticamente e contém todos os componentes do mapa, a origem da métrica e os módulos de gerenciamento.
- O universo **Empresa** inclui todos os componentes do ambiente. Este universo integrado não pode ser excluído ou definido e é atribuído somente a administradores. A finalidade desse universo é fornecer aos administradores acesso a todos os dados. Esse universo nem é mesmo listado na página de **configuração** dos universos.

  NOTE

  - Os usuários podem ser atribuídos a mais de um universo. Nesse caso, **All My Universes** está disponível na exibição **Experiência** e na exibição **Agentes**. **All My Universes** mostra os dados dos universos de todos os usuários juntos.
  - A lista suspensa **All My Universes** também preenche os universos do DX Operational Intelligence (exceto o universo All Access). Esses universos são marcados com um identificador OI com seu nome na lista suspensa. Não é possível editar os universos do DX Operational Intelligence no APM.

Dois casos de uso diferentes estão disponíveis para a criação de universos:

- **Criar um universo para navegação** - crie universos para navegação de modo a fornecer aos usuários uma série de ambientes filtrados pré-configurados. Os usuários podem alternar rapidamente entre os ambientes para exibir diferentes áreas de um ambiente complexo.
- **Criar um universo para segurança** - crie universos para segurança de modo a restringir os componentes do ambiente que um determinado usuário pode exibir. É recomendável que você baseie o conteúdo de um universo de segurança nos caminhos de transação. Crie atributos personalizados nos limites que permitam aos analistas identificar a continuação do caminho. Se o ambiente usar domínios, o atributo agentDomain será preenchido por padrão. Use o atributo agentDomain como uma condição de filtro para criar um universo que corresponda às restrições de permissão do domínio especificado.

Criar um universo

Ao definir um novo universo, você pode conceder diferentes direitos a usuários e grupos de usuários. Os direitos para acessar o universo, selecionar origens da métrica, mapear componentes e gerenciar módulos.

Siga estas etapas:

1. Avalie o conteúdo que deseja definir nesse universo.
2. Selecione **Universos** no painel esquerdo e, em seguida, selecione **Novo universo**.
   Um painel de caixa de diálogo será exibido.

NOTE
As definições adicionadas a uma guia serão propagadas para a parte individual correspondente do aplicativo. Por exemplo, as definições adicionadas aos componentes do mapa são aplicadas ao mapa. As definições adicionadas às origens da métrica são aplicadas ao navegador de métricas. Outras partes do aplicativo não são afetadas.

3. Atribua um nome ao novo universo.
4. (Opcional) Adicione uma descrição para o universo.
5. Na exibição **Acesso**, você concede direitos de acesso diferentes a esse universo para usuários e/ou grupos de usuários.
   a. Selecione o direito que você deseja conceder:
      - **Ler:** permite que os usuários vejam os componentes selecionados no universo.
      - **Editar:** permite que os usuários modifiquem os componentes que selecionam no universo e adicionem atributos ou regras aos componentes do mapa. Editar também inclui os direitos de Ler.
      - **Gerenciar:** permite que os usuários modifiquem os direitos de acesso para o universo. Os administradores usam o direito Gerenciar para delegar a atribuição de direitos de acesso a outros usuários. Gerenciar também inclui os direitos de Ler e Editar.
   b. Na lista suspensa, selecione o usuário ou o grupo de usuários para o qual você deseja conceder o direito.
   c. Clique em **Adicionar usuário** ou **Adicionar grupo** para adicionar o usuário ou grupo de usuários selecionado ao universo.
   d. (Opcional) Selecione um direito diferente e um usuário ou grupo de usuários e adicione-os à lista.
6. Na exibição **Origens da métrica**,
   – A opção **Filtrar a exibição de métricas por componentes do mapa** filtra árvores de métricas no Navegador de métricas por mapa. Valor padrão: **true** (o filtro é aplicado por padrão). Marque a caixa de seleção para desativar o filtro.
   – Selecionar **Todas as origens de métricas**, incluindo componentes futuros. Se você selecionar essa opção, o universo conterá todas as origens de mapas (agentes) e nada será filtrado.
   – Personalize as origens de métricas selecionando um subconjunto de agentes individuais e/ou adicionando uma expressão regular. As expressões regulares baseiam-se em hostname|processname|agentname. Exemplos de expressões:
      - myhost\|.* - seleciona todos os agentes em execução no host "myhost". O caractere de pipe é usado como escape com uma barra invertida, pois ele é um caractere de controle regex.
      - usnye.* - seleciona agentes de todos os hosts com o prefixo "usnye".
      - .*\|.*\|dmn13t.* - seleciona todos os agentes com o prefixo "dmn13t".

      NOTE
      Clique em **Recarregar** na caixa de diálogo, na parte inferior da página, para ver uma visualização da subárvore dos agentes selecionados.

   WARNING
   As origens das métricas dos universos criados antes da versão 20.11 devem ser reconfiguradas.
7. Na exibição **Componentes de mapeamento**, selecione uma destas ações:
   – Mapear todos os componentes (incluindo componentes futuros). Se você selecionar essa opção, o universo conterá todos os componentes de mapa e nada será filtrado.
   – Use o filtro **Origens da métrica**. Se você selecionar essa opção, o universo conterá todos os componentes do mapa gerados pelos agentes selecionados pelo filtro **Origens de métricas**.
   – Personalize o filtro. Defina um filtro de mapa para selecionar os componentes de mapa necessários. Esse filtro é o mesmo da exibição **Mapa**.

   NOTE
   Para obter mais informações sobre o nó da experiência, consulte Monitorar o desempenho usando a Exibição da experiência.
8. Na exibição **Módulos de gerenciamento**, selecione uma das seguintes opções:

  - Todos os itens (incluindo itens futuros).
  - Um ou mais itens da lista.
9. A exibição **Informações** é gerada depois de salvar o universo. Essa exibição contém uma visão geral das definições do universo. A visão geral inclui o número de componentes em várias partes do aplicativo (por exemplo, exibição de métrica e mapeamento).
10. Selecione **Salvar**.

    NOTE
    Como administrador, você também pode criar um universo diretamente pelo mapeamento no universo Empresa. Defina os filtros de mapeamento e selecione **Salvar como universo**, no canto superior direito, para salvar como um universo os nós de mapeamento atuais filtrados.

Modificar um universo

Siga estas etapas:

1. Selecione **Universos** no painel esquerdo.
2. Identifique o universo que deseja modificar e selecione **Editar**.
3. Siga as etapas descritas na seção Criar um universo.

Excluir um universo

Siga estas etapas:

1. Selecione **Universos** no painel esquerdo.
2. Identifique o universo que deseja remover e selecione **Excluir**.
3. Confirme a exclusão.

Configurar a segurança do universo

Em cada universo, os usuários recebem privilégios individuais para editar alertas, calculadoras e grupos de métricas. A função Usuário avançado, os usuários e os grupos de usuários devem receber permissão para ver ou criar alertas, calculadoras ou grupos de métricas para um módulo de gerenciamento. O Usuário avançado está apto a iniciar manualmente as sessões de rastreamento de transação. O administrador de inquilinos tem todos os privilégios. Os privilégios entram em vigor somente na exibição do universo especificado. Veja a seguir os privilégios por tipo de permissão:

NOTE
Por padrão, um usuário/usuário avançado sem permissão para qualquer universo não poderá ver agentes/métricas na Exibição da métrica. Um usuário com permissão de leitura para um universo pode ver as métricas do agente configuradas no universo na Exibição da métrica.

- **ler:** permite que o Usuário avançado, o usuário ou o grupo de usuários atribuído visualizem os alertas, as calculadoras e os grupos de métricas do módulo de gerenciamento.
- **gravar:** permite que o Usuário avançado, o usuário ou o grupo de usuários atribuído visualizem e modifiquem os alertas, as calculadoras e os grupos de métricas do módulo de gerenciamento.
- **gerenciar:** permite que o Usuário avançado, o usuário ou o grupo de usuários atribuído visualizem e modifiquem os alertas, as calculadoras, os grupos de métricas e os usuários do módulo de gerenciamento. Os usuários com o privilégio **gerenciar** também podem adicionar módulos de gerenciamento ao universo.

O administrador de inquilinos deve conceder explicitamente o caminho da origem da métrica ao universo. Esse caminho permite que os usuários com acesso ao universo visualizem as métricas de alarme e calculadora na Árvore de métricas.

O administrador tem o privilégio de escolher as entidades às quais os usuários terão acesso. Isso inclui métricas, vértices e módulos de gerenciamento.

- Com a permissão de **leitura**, o usuário só pode exibir as entidades, mas não pode alterá-las.
- Com acesso de **gravação**, o usuário pode alterar as entidades. Por exemplo, ele pode alterar o conteúdo do módulo de gerenciamento ou adicionar atributos personalizados aos vértices.
- O acesso de **gerenciamento** dá ao usuário o privilégio de alterar a lista de acesso no universo.

Recomendamos enfaticamente essas configurações para garantir que os usuários tenham o acesso correto às configurações dos módulos de gerenciamento:

- Não atribua usuários a um universo com uma configuração de **escopo de módulo de gerenciamento** definida como **Todos os itens**.
- Adicione explicitamente **módulos de gerenciamento** como parte do escopo a todos os universos*, com exceção do* universo Enterprise. Enterprise um universo especial disponível somente para o administrador de inquilinos.

Mais informações: Funções e privilégios suportados

Os universos permitem que o administrador refine o número e os tipos de componente em grupos de autorização fáceis de usar chamados de universos. Para exibir o DX APM, cada usuário deve estar alocado em um universo. Como administrador, você deve criar universos para os usuários. Use o universo padrão, denominado Todos os componentes, ou crie um universo personalizado.

Para obter mais informações sobre como gerenciar e configurar universos, consulte Configurar universos.

Configurar a Exibição da experiência

Como administrador, configure os Cartões de experiência em Exibição da experiência. Configure os cartões para que os analistas possam exibir facilmente os componentes mais importantes de negócios que afetam a experiência do usuário final.

Exibição da experiência

Os administradores podem realizar as seguintes tarefas:

- Configurar o universo
- Adicionar um novo Cartão de experiência
- Editar um Cartão de experiência
- Compartilhar um Cartão de experiência

Cartões de exibição da experiência

Saiba como criar um Cartão de experiência na Exibição da experiência. Configure os Cartões de experiência para que os analistas tenham o respectivo Universo dividido em grupos significativos.

Configurar o universo

Antes de configurar a Exibição da experiência para um usuário, atribua pelo menos um universo ao usuário.

NOTE

Todos os meus universos estão disponíveis na exibição da **Experiência** apenas para os administradores. Para outros usuários, a exibição Todos os meus universos está disponível na exibição **Agentes**, se mais de um universo estiver atribuído.

Mais informações:

- Configurar universos
- KB000113376: usuários com Acesso de leitura no Team Center não podem ver a exibição Todos os meus universos

Adicionar novo Cartão de experiência

Pronto para uso, para um Gerenciador corporativo, o sistema cria dois Cartões de experiência para cada universo existente. Os Cartões de experiência para aplicativos têm dois níveis de detalhamento com os atributos `Application` e `Name` . Os Cartões de experiência para Serviços têm dois níveis de detalhamento com os atributos `Business service` e `Name` . Como administrador, crie, atualize ou exclua qualquer número de Cartões de experiência personalizados para analistas.

> **NOTE**
> Se você adicionar um novo universo ou se conectar a um novo provedor, os Cartões experiência não serão criados automaticamente.A criação automática dos Cartões de experiência é apenas parte de uma instalação ou atualização.

Siga estas etapas:

1. Abra a Exibição da experiência e verifique se você está na exibição de nível superior.
2. Selecione o botão + para adicionar um Cartão de experiência.
3. Selecione um universo.
4. Use o universo inteiro ou aplique um filtro.
5. Selecione os atributos. Os Cartões de experiência são agrupados por atributos. Os níveis de detalhamento do Cartão de experiência correspondem ao número de atributos que você seleciona.

   > **TIP**
   >
   > É recomendável usar de três a quatro níveis de atributos. Ou agrupar por atributo para monitorar um grupo específico de componentes. Por exemplo, Proprietário = Joe.
6. Selecione um tipo de gráfico padrão:
   a. Histograma
   b. Tempo médio de resposta
   c. Volume de transações
7. Dê um nome ao cartão
8. Selecione a caixa **Tornar público este cartão de experiência**.
9. Selecione **Salvar**.

O administrador agora pode ver os Cartões de experiência na Exibição da experiência.

> **WARNING**
>
> Uma mensagem de erro é exibida quando você tenta exibir mais de 500 transações comerciais no modo dinâmico ou mais de 50 no modo histórico. Por questões de desempenho, a Exibição da experiência limita o número de transações comerciais exibidas. Para obter mais informações, consulte Não há dados de métrica na Exibição da experiência.

Editar Cartão de experiência existente

No nível superior da Exibição da experiência, você pode editar os Cartões de experiência, tanto os cartões padrão quanto os definidos pelo usuário.

Siga estas etapas:

1. Selecione o ícone de expansão, no canto inferior direito do cartão.
2. Selecione **Editar cartão**.
3. Altere as configurações do cartão, conforme a necessidade.
4. Selecione **Salvar**.

Excluir Cartão de experiência

No nível superior da Exibição da experiência, você pode excluir Cartões de experiência, tanto os cartões padrão quanto os definidos pelo usuário.

Siga estas etapas:

1. Selecione o ícone de expansão, no canto inferior direito do cartão.
2. Selecione **Editar cartão**.
3. Selecione **Excluir cartão**.O cartão é removido de todos os usuários que têm acesso.

Compartilhar Cartão de experiência

É possível compartilhar um Cartão de experiência com um usuário em um universo existente.

Siga estas etapas:

1. Verifique se o usuário tem acesso ao universo.
2. Selecione o ícone de expansão, no canto inferior direito do cartão.
3. Selecione **Editar cartão**.
4. Selecione **Tornar público este cartão de experiência**.
5. Selecione **Salvar**.
   O cartão aparece na sua lista de cartões.
6. Envie o link do Cartão de experiência para o usuário.

   NOTE

   É possível compartilhar um Cartão de experiência privado com um usuário do mesmo universo. O usuário poderá exibir temporariamente o cartão privado.

Propagador

A Exibição da experiência permite que você organize experiências (nós de experiência) em cartões que se baseiam em atributos. Para expandir a seleção de atributos para agrupamento de experiências, use o Propagador. O Propagador copia atributos dos componentes adjacentes que estão diretamente conectados a uma experiência. Esses atributos são propagados até a experiência que se baseia em regras. Se vários componentes estiverem conectados a uma única experiência e o mesmo atributo for definido várias vezes, o atributo será propagado somente se todas as ocorrências desse atributo tiverem o mesmo valor.O Propagador também pode coletar e enviar atributos de outras camadas do mapa. Por exemplo, com a propagação entre camadas, é possível organizar as suas experiências com base nos atributos de host ou docker da Camada de infraestrutura.

Definir configurações do Propagador

Defina os atributos que deseja propagar para as suas experiências usando a sintaxe RegEx nos nomes de atributo. Identifique a origem do atributo e configure a propagação entre camadas.

Siga estas etapas:

1. Defina e identifique os atributos que você deseja propagar. As origens de atributo disponíveis são as seguintes:
   - **GATHERED**
     Inclui atributos que o agente definiu no monitoramento do componente.
   - **CUSTOM**
     Contém atributos que você criou manualmente na UI ou definiu na API REST.
   - **DECORATED**
     Agrupa atributos que você criou usando regras de atributo.

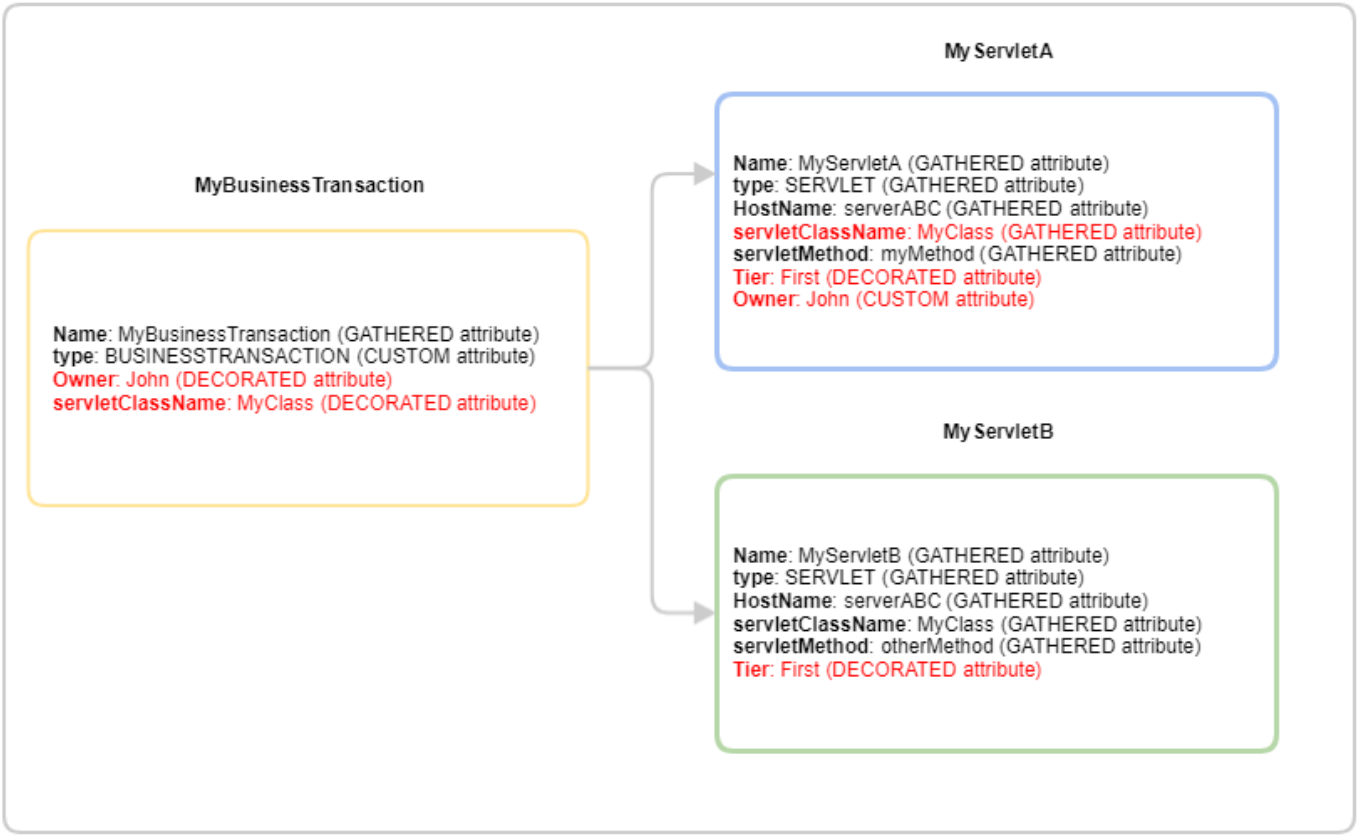
NOTE

Os atributos que são propagados para experiências sempre são decorados. Esses atributos podem ser substituídos pelas regras de atributo, pela API REST ou pelas alterações manuais na UI.

2. Use uma lista branca para propagar determinados atributos ou use uma lista negra para bloquear os atributos. Defina essas regras de propagação global editando as seguintes propriedades encontradas no arquivo `IntroscopeEnterpriseManager.properties`:
   - **introscope.apmserver.atc.propagator.blacklist**
     Especifica os atributos na lista negra.
     Padrão:
     ```
     introscope.apmserver.atc.propagator.blacklist=CUSTOM\..*;DECORATED\..*;Name;Hostname;Agent;AgentDomain
     ```
     A listas negra padrão não propaga os seguintes atributos:
     - Atributos personalizados ou decorados
     - `Nome`
     - `HostName`,
     - `Agent`
     - `AgentDomain`
   - **introscope.apmserver.atc.propagator.whitelist**
     Especifica os atributos na lista branca.
     Padrão:
     ```
     introscope.apmserver.atc.propagator.whitelist=.*Owner
     ```
     A lista branca padrão propaga o atributo `Owner`.

   Exemplo: o exemplo a seguir mostra a propagação dos atributos `Owner` e `servletClassName` para uma experiência do servlet conectado.

Figure 2: propagator



Resultados:

- Tier não é propagado porque a lista negra desativa a propagação de atributos personalizados.
- HostName não é propagado porque ele também está na lista negra.
- servletMethod não é propagado porque os servlets têm valores diferentes.
- Owner é propagado porque não entra em conflito com MyServletB.
- servletClassName é propagado porque ambos os servlets têm os mesmos valores.

3. Para configurar a propagação de atributos entre camadas, abra o arquivo `IntroscopeEnterpriseManager.properties` no diretório `<pasta_principal_EM>/config` . Especifique as camadas de mapeamento na propriedade `introscope.apmserver.atc.propagator.crosslayer` :
Padrão: <em branco> O valor padrão é uma sequência de caracteres vazia, o que significa que a propagação entre camadas está desativada.

   NOTE

   Para ativar a propagação de várias camadas do mapeamento, separe cada camada com uma vírgula.

Exemplo: no seguinte exemplo, o propagador é configurado para extrair atributos da Camada de infraestrutura:

```
introscope.apmserver.atc.propagator.crosslayer=INFRASTRUCTURE
```

NOTE

Mais informações:

- Definir a forma de monitoramento do ambiente com regras de atributo

Limite de dados

O limite de dados do modo histórico é de 50 experiências. O limite de dados do modo dinâmico é de 500 experiências. As experiências são pontos de entrada do aplicativo ou transações comerciais. Se você selecionar um intervalo de tempo no modo histórico dentro das últimas 24 horas, será aplicado o limite de dados para o modo dinâmico (500 experiências). As últimas 24 horas são cobertas pelos dados em cache.

Os administradores configuram os Cartões de experiência na Exibição da experiência para que os analistas possam exibir facilmente os componentes mais críticos para os negócios e que afetam a experiência do usuário final.

Para obter mais informações sobre como configurar os Cartões de experiência, consulte Configurar a Exibição da experiência.

Definir a forma de monitoramento do ambiente com regras de atributo

Atributos são rótulos que são aplicados aos componentes. Cada atributo tem um nome e um valor (por exemplo, color=red). Os atributos facilitam a diferenciação dos componentes e identificam seus relacionamentos com outros componentes.Use atributos em suas as perspectivas, realçando e filtrando para organizar e exibir partes do ambiente do aplicativo monitorado. O DX APM permite atribuir um número ilimitado de atributos a componentes.

Tipos de atributo

O DX APM oferece os seguintes tipos de atributo:

- **Atributos básicos**
  Atributos básicos são automaticamente relatados e atribuídos a cada componente a partir do agente associado.Por exemplo, um componente de banco de dados pode ter os seguintes atributos básicos:
  - `databasename`
  - `inferredBackendNode`
  - `Nome`
  - `provedor`
  - `Agrupamento de origem`
  - `Type`
- **Atributos personalizados**
  Designe atributos personalizados a componentes individuais e, em seguida, adicione-os a perspectivas, grupos e filtros. Por exemplo, use o atributo `owner` para atribuir o componente a um determinado analista. Para exibir os componentes atribuídos a este analista, adicione o atributo `owner` a um filtro e especifique o valor do filtro.
- **Atributos decorados**
  É possível definir regras de atributo que designam automaticamente os novos valores a atributos existentes. Tais atributos recém-derivados denominam-se atributos decorados.

Definir atributos personalizados

Defina um atributo personalizado para um componente individual ou grupo de componentes.

> **NOTE**
>
> É recomendável que você associe os atributos personalizados a todos os componentes do ambiente. Recomendamos que sejam atribuídos valores a `Owner` e `Location` para todos os componentes.

Siga estas etapas:

1. No **Mapa**, selecione um componente ou grupo.

TIP

Você pode adicionar um atributo personalizado a um componente que represente um grupo. O nome do atributo e o valor serão adicionados a todos os componentes desse grupo. Um prompt perguntará se você deseja adicionar o atributo ao grupo ou se deseja criar uma regra de atributo.

2. Vá para a seção **Atributos personalizados** do painel **Exibição de componentes** e selecione valores para os seguintes atributos personalizados padrão:
   - `location`
   - `owner`
   - `region`
   - `tier`
3. (Opcional) Para criar um atributo, selecione **<nome do novo atributo>** e digite o nome do atributo.Selecione **<nome do novo atributo>** e atribua um valor ao atributo.

   NOTE

   O DX APM reconhece se um valor de atributo é um endereço de email ou um URL. Um ícone de link ou envelope aparece ao lado do atributo no painel **Exibição de componentes**. Selecione o ícone para abrir os links em uma nova guia do navegador ou abrir uma página de email do Outlook.
4. Adicione o novo atributo aos filtros e às perspectivas.

O novo atributo e o valor serão exibidos na seção **Atributos personalizados** do painel **Exibição de componentes**.

Definir atributos entre camadas

Os atributos atribuídos aos componentes de uma camada específica ficam visíveis em outras camadas no DX APM. Por exemplo, os atributos que são designados aos componentes da Camada de infraestrutura são incluídos na lista suspensa que é usada para filtrar o Mapa na Camada do aplicativo. Essa funcionalidade entre camadas oferece aos analistas as exibições de dados que mostram as relações entre os componentes do aplicativo e seus componentes de infraestrutura conectados. Essa exibição de dados combinados também funciona como uma visão geral que pode ajudar a definir e organizar as funções de suporte em toda a organização. Os administradores podem designar atributos a componentes da Camada de infraestrutura na seção **Atributos personalizados** do painel **Exibição de componentes** ou definindo uma regra de atributo.

Exemplos

Exemplo 1: usar atributos entre camadas para auxiliar na triagem da infraestrutura

O atributo `Owner = Joe Smith` é designado a todos os componentes de infraestrutura que Joe suporta. Então, esse atributo será usado para criar a perspectiva `Joe Smith` . Os analistas usam essa perspectiva e outras perspectivas `Owner` para identificar quem oferece suporte à infraestrutura para os aplicativos que requerem triagem. Com essas exibições de dados, os analistas também serão capazes de oferecer suporte à infraestrutura com informações importantes que podem resultar em uma triagem mais rápida.

Exemplo 2: uso de atributos entre camadas para definir funções de suporte

Se os componentes do host em seu ambiente seguem uma convenção de nomenclatura, você pode criar uma regra de atributo para definir funções de suporte para os componentes do aplicativo. A regra de atributo a seguir designa Joe Smith a todos os componentes do host localizados em Nova York.Uma perspectiva é, em seguida, criada com base nesse atributo, que permite que o analista Joe Smith exiba seus componentes de aplicativos designados e todos os componentes de infraestrutura conectados.

Nome do atributo personalizado	Valor recém-atribuído	Nome de atributo existente	Operador de condição/ correspondente	Valor da condição
Proprietário	Joe Smith	Hostname	Contém	NY

Os seguintes links fornecem mais informações sobre as camadas e como usar os atributos no DX APM:

NOTE

Mais informações:

- Camadas do mapa
- Identificar áreas problemáticas usando filtros
- Organizar componentes usando perspectivas

Definir atributos decorados usando regras de atributo

Use regras de atributo para automatizar o processo de adição de atributos personalizados. Uma regra usa os atributos básicos e personalizados que já foram associados a um componente. Se o atributo atender à condição especificada na regra, um nome de atributo personalizado será criado (ou atualizado) e receberá o valor especificado. Por exemplo, uma regra de atributo declara que, se o atributo de nome do host de um componente terminar com o sufixo .cz, o atributo personalizado com o nome Suporte local será criado e que seu valor será República Tcheca. Todos os componentes que atenderem aos critérios de uma regra assumirão o valor do atributo personalizado. As regras associam o atributo personalizado no ambiente atual. Elas também associam esse atributo a qualquer componente que atenda aos critérios no futuro.

- **Regras de atributo local**
  Como usuário, você pode criar regras de atributo local que se apliquem aos componentes dentro do universo. A regra aplica o novo valor de atributo a todos os componentes que atenderem aos critérios e que estiverem dentro do universo atual. Esses atributos personalizados são exclusivos para o universo. Somente os usuários que tiverem acesso a esse universo e os administradores poderão vê-los.
- **Regras de atributo global**
  A regra de atributo global aplica os valores do atributo personalizado a todos os componentes que atendem aos critérios da regra no ambiente corporativo. Somente os administradores podem criar regras de atributo global. As regras de atributo global têm precedência sobre as regras de atributo local. **Exemplo:** crie um atributo local para definir um valor de atributo de localização como Long Island. Se uma regra de atributo global estiver definida para atribuir o valor do atributo de localização como Nova Iorque, o valor mostrará Nova Iorque para todos os usuários.

Definir regras de atributo global

Defina regras de atributo para designar atributos aos componentes automaticamente. As regras de atributo global aplicam os atributos personalizados a todos os componentes atuais e futuros que atendam à condição da definição da regra. As regras de atributo global se aplicam a todos os componentes no ambiente corporativo, independentemente do universo. Qualquer usuário que tenha o componente atribuído ao seu universo verá o atributo personalizado. Um usuário não poderá criar uma regra de atributo local que substitua o valor de uma regra de atributo global.

Siga estas etapas:

1. Selecione a guia **Atributos**.
2. Clique em **<nova regra de atributo>**, na coluna **Nome do atributo personalizado**, e preencha o nome e o valor para a nova regra.
3. Clique fora da linha.
   A regra será salva.

Usar o operando RegEx com as regras de atributo

Use o operando Contém RegEx nesses casos:

- Operandos como `Começa com` ou `Contém` não são suficientes para criar a regra de atributo necessária.
- É necessário um novo valor de atributo que tenha como base o valor original.

Uma expressão RegEx que seja usada em um valor de atributo existente poderá ser usada para criar várias regras de atributo personalizadas.

Siga estas etapas:

1. Selecione a guia **Atributos**.
2. Clique em **<regra do novo atributo>**.
3. Associe um nome de atributo personalizado.
4. Associe um valor do grupo RegEx ao **Valor recém-atribuído**.
5. Selecione o **Nome de atributo existente** necessário.
6. Selecione um valor de **Operador de condição/correspondente**: `Contém RegEx` ou `Não contém RegEx`.
7. Especifique a RegEx no **Valor da condição** e pressione **Enter**.

NOTE

A opção **Diferencia maiúsculas de minúsculas** não pode ser selecionada. A diferenciação de maiúsculas e minúsculas é decidida com base em um operando da RegEx.

A regra de atributo será salva e o número de componentes com o novo atributo será exibido em **Número de componentes afetados**.

- Exemplo: o nome do host na rede segue a regra `<código do país com 2 letras><cidade><ID numérica>.fornecedor.com` Você pode usar o operando da RegEx para criar regras de atributo que gerem atributos separados de País e Cidade a partir do nome do host. A sintaxe `"(..)([a-z]*)[0-9]*\.fornecedor\.com"` descreve essa RegEx. É possível criar regras de atributo para extrair os valores de País e Cidade criando essas regras de atributo.

Nome do atributo personalizado	Valor recém-atribuído	Nome de atributo existente	Operador de condição/ correspondente	Diferencia maiúsculas de minúsculas	Valor da condição
País	$1	hostname	ContainsRegEx		(..)([a-z]*)[0-9]*\.vendor\.com
Cidade	$2	hostname	ContainsRegEx		(..)([a-z]*)[0-9]*\.vendor\.com

- Exemplo: dois valores de nome de host em um ambiente: uklondon1234.vendor.com e usdallas1234.vendor.com $1 retorna valores uk e us, e $2 retorna os valores london e dallas. Você também pode criar um link de documentação, como no exemplo a seguir. Selecione qualquer elemento do mapa para ver um link da documentação.

Nome do atributo personalizado	Valor recém-atribuído	Nome de atributo existente	Operador de condição/ correspondente	Diferencia maiúsculas de minúsculas	Valor da condição
País	$1	hostname	ContainsRegEx		(..)([a-z]*)[0-9]*\.vendor\.com
Cidade	$2	hostname	ContainsRegEx		(..)([a-z]*)[0-9]*\.vendor\.com
URL da documentação	https://wiki.vendor.com/searchForServerDoc.cgi?host=$1	hostname	ContainsRegEx		(.*)\.vendor\.com

NOTE

Para obter a sintaxe completa de RegEx, consulte a documentação do Java RegEx. Como alternativa, procure o testador do Online Java RegEx na internet.

Importar regras de atributo em massa

O DX APM permite fornecer descrições exclusivas para os componentes, sejam eles hosts, aplicativos ou até mesmo componentes de aplicativos. Forneça essas descrições, ou atributos personalizados, ao ambiente para que você possa tirar o máximo proveito do Mapa e da Exibição da experiência. Por exemplo, forneça o atributo Proprietário a cada um dos aplicativos no ambiente. Quando você exibir um Mapa dos proprietários, os aplicativos que eles gerenciam estarão aninhados na exibição. Definir o mesmo atributo Proprietário permite que você tenha um bloco que resume o desempenho de todos os aplicativos por proprietário. Você pode detalhar no bloco para ver os aplicativos individuais que pertencem especificamente àquele proprietário.

Para facilitar a aplicação desses atributos, você pode usar um mecanismo de carregamento de regras em massa. Como administrador, você pode criar um conjunto de regras de atributo externamente em um arquivo de valores separados por vírgulas (CSV). Assim, você pode importar o arquivo para criar diversas regras de atributo. Essa funcionalidade permite usar um arquivo do tipo CSV que contenha várias regras de atributo e carregá-lo de uma vez em um curto limite de tempo.

No arquivo, especifique o nome do atributo personalizado, uma vírgula e o valor que você deseja que seja usado. Então, use outra vírgula e especifique o atributo que deseja usar para corresponder à regra. Use mais uma vírgula e, em seguida, o valor esperado do atributo correspondente.

Em outras palavras:

```
WHEN   Hostname equals my-tradeserviceTHEN  Owner equals Ralph
```

Pode ser escrito no arquivo CSV como:

```
Owner,Ralph,Hostname,my-tradeservice
```

Use a seguinte convenção de formato no arquivo CSV:

O nome do atributo personalizado que você deseja adicionar. O atributo pode ser qualquer um dos atributos decorados.	O valor do atributo personalizado que você deseja adicionar.	O nome do atributo de filtro para correspondência. Esses são os atributos básicos.	O valor do atributo de filtro que você deseja corresponder.

Esse arquivo pode conter apenas quatro colunas. O valor do atributo de correspondência na coluna três deve ser um nome de atributo válido.

Siga estas etapas:

1. Em um editor, crie um arquivo CSV usando a convenção de formato, por exemplo:
   ```
   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. Salve e nomeie o arquivo usando a seguinte convenção: `filename.csv` . Por exemplo, no Windows, use o recurso "Salvar como" e salve como o tipo .csv. Feche o arquivo.
3. No DX APM, passe o mouse sobre o painel esquerdo e clique em **Atributos**.
4. Clique em **Fazer upload do arquivo de regras de atributo**.
   A caixa de diálogo Fazer upload do arquivo csv de regras de atributo será exibida.
5. Leia as instruções da caixa de diálogo e selecione mais universos para aplicar as regras, se desejado. Se nenhum universo for selecionado, as regras de atributo serão aplicadas apenas ao universo selecionado no momento.
6. Clique em **Procurar** e selecione o arquivo CSV a ser importado. Você pode repetir essa etapa para selecionar outro arquivo para upload.
7. Clique em **Fazer upload**.
   Uma mensagem é exibida e informa o status de upload do arquivo.

8. Clique em **Concluído**.
   As regras de atributo são exibidas na lista ATTRIBUTE RULES.

Configurar regras para atualização de atributos

Quando desejar atualizar os atributos de vários componentes (por exemplo, para especificar o proprietário de muitos aplicativos ou hosts), fazer upload das regras em um arquivo CSV pode ser mais conveniente do que criá-las na interface do usuário. Você não precisa especificar apenas os atributos existentes. É possível criar atributos adequados às suas finalidades para a criação de blocos de Perspectivas e Exibição da experiência. Depois de fazer upload das regras, você poderá encontrá-las no mapa.

Exemplo:

Como as regras funcionam

Neste exemplo, você deseja atribuir o atributo Proprietário com o valor Eric a dois nomes de host: vermelho e azul. Você também deseja atribuir o atributo Proprietário com valor Susan ao nome de host verde.

```
@ruleset, owners-by-hostOwner,Eric,hostname,redOwner,Eric,hostname,blueOwner,Susan,hostname,green
```

`@ruleset, <nome>` coloca essas três regras no escopo `owners-by-host` . A interface de usuário exibe o identificador ao qual cada uma dessas regras pertence. Cada regra especificada pertence a um grupo com um identificador `@ruleset` exclusivo. Quando `@ruleset` não for especificado, as regras pertencerão implicitamente a um grupo global. Sempre use identificadores de regra, caso contrário, você poderá ser surpreendido por alterações no escopo global e excluir acidentalmente as regras de outros escopos.

Exemplo:

Editar ou excluir uma regra

É possível editar as regras na interface do usuário. Também é possível editar as regras com um arquivo CSV, mas tome cuidado. Neste exemplo, o nome do host roxo especifica Eric como proprietário, mas as outras duas regras especificadas no exemplo anterior foram excluídas.

```
@ruleset, owners-by-hostOwner,Eric,hostname,purple
```

Se especificar um identificador `@ruleset` no arquivo CSV, você excluirá todas as regras que não forem especificadas novamente. Esse comportamento se aplica a todas as regras, e não apenas às regras com alterações. Portanto, o arquivo CSV a seguir excluirá todas as regras do escopo proprietários por host:

```
@ruleset, owners-by-host@ruleset, owners-by-appOwner,Foo,Application,Bar
```

> **WARNING**
>
> Devido a esse comportamento da regra, é recomendável que você mantenha uma cópia mestra do seu arquivo CSV e só faça alterações nela.

Mais informações:

- Organizar componentes usando perspectivas
- Configurar a Exibição da experiência

Usar políticas de decoração para filtrar regras de atributo

Atributos decorados são aqueles criados ou atualizados automaticamente como resultado das regras de atributo. Uma política de decoração permite que você decida quais regras de atributo serão aplicadas ao mapa do Team Center. Em um intervalo fixo, o DX APMatualiza todos os nós aplicáveis que atendem às regras da política de decoração. As políticas de decoração ajudam a organizar e exibir os nós no ambiente do aplicativo monitorado no Team Center.

A seguintes opções permitem filtrar por vários tipos de políticas de decoração:

- Tudo - exibe todas as regras de atributo que você criou.
- Csv Created Rules - exibe as regras de atributo do arquivo CSV.
- Manually Created Rules - exibe todas as regras de atributo que foram criadas manualmente na guia Attribute Rules.

Siga estas etapas:

a. No DX APM, passe o mouse sobre o painel esquerdo e clique em **Atributos**.
b. Clique em **Attribute Rule:<option>** e selecione uma política.
   A lista de regras de atributo é atualizada para mostrar as regras que pertencem à política.

Mais informações: Definir a forma de monitoramento do ambiente com regras de atributo

Ajustar o monitoramento com alertas

Como administrador do APM, você pode criar, editar e excluir os alertas. Defina limites de desempenho para as métricas para que os analistas identifiquem quando um componente específico estiver sobrecarregado. Crie alertas e defina limites para sinalizar os problemas antes que a experiência do cliente seja afetada.

Criar um alerta

Como administrador, você pode criar alertas para monitorar possíveis problemas no ambiente de maneira eficiente.

Siga estas etapas:

1. No painel esquerdo, passe o mouse sobre o ícone de sino e clique em **Alertas**.
2. Clique em **Criar outro alerta**.
3. Digite os valores para **Nome do alerta** e **Descrição**.
4. Mantenha o botão de alternância **Ativo**.
5. Digite os valores de **Especificador de agente** e **Especificador de métrica**.
   Especificador de agente especifica uma expressão regular que filtra a entrada para a métrica e especifica os dados até e inclusive o nome do agente. Essa expressão determina a quais agentes os dados agrupados são limitados. Por exemplo, a expressão (.*)\|WPS2-0[1,2] procura por qualquer agente em todos os domínios que sejam denominados WPS2-01 ou WPS2-02. A expressão do agente é importante quando diversas JVMs geram relatórios para o mesmo Gerenciador corporativo, mas têm finalidades diferentes. Por exemplo, sites diferentes na mesma empresa. Nesse caso, use uma expressão regular para limitar os agentes que seu agrupamento de métricas filtra.
   Especificador de métrica especifica uma expressão regular que especifica a métrica e o recurso. Um recurso é uma cadeia de pastas que leva à métrica. Por exemplo, a expressão LDAP\|([^|:]*)\|(.*):Response Time\(ms\) procura todos os recursos na pasta do recurso LDAP. A expressão procurará apenas a métrica Tempo de resposta (ms) nesses recursos.
6. (Opcional) Clique em **+** ao lado do campo Especificador de métrica para adicionar mais campos para os valores **Especificador de agente** e **Especificador de métrica**.
7. Digite os valores de **Limite de risco** e **Limite de cuidado**.
8. Clique em **Criar alerta**.

Você criou um alerta.

Criar um alerta na Exibição da métrica

Você pode criar alertas na página Exibição da métrica.

Siga estas etapas:

1. Pesquise a Árvore da métrica para selecionar uma métrica, por exemplo, **Erros por intervalo**.
2. Clique com o botão direito na métrica.
3. Clique em Novo alerta simples da métrica Erros por intervalo.
   Você será encaminhado para a página **Alertas**. Os valores de **Especificador de agente** e **Especificador de métrica** serão preenchidos automaticamente.
4. Digite os valores para **Nome do alerta** e **Descrição**.
5. Digite os valores de **Limite de risco** e **Limite de cuidado**.

6. Clique em **Criar alerta**.

Você criou um alerta.

Criar um alerta com as opções avançadas

Siga estas etapas:

1. No painel esquerdo, passe o mouse sobre o ícone de sino e clique em **Alertas**.
2. Clique em **Criar outro alerta**.
3. Digite os valores para **Nome do alerta** e **Descrição**.
4. Mantenha o botão de alternância **Ativo**.
5. Digite os valores de **Especificador de agente** e **Especificador de métrica**.
6. (Opcional) Clique em **+** ao lado do campo Especificador de métrica para adicionar mais campos para os valores de Especificador de agente e Especificador de métrica.
7. Clique em **Mostrar opções avançadas**.
8. Na lista suspensa **Combinação**, selecione qualquer uma das seguintes opções:
   – **Qualquer:** se qualquer métrica que faça parte do agrupamento de métricas de alerta violar o limite, o alerta será disparado.
   – **Tudo:** se todas as métricas que fizerem parte do agrupamento de métricas de alerta violarem o limite, o alerta será disparado.
9. Selecione uma opção na lista suspensa **Operador de comparação**:
   – Menor que
   – Maior que
   – Igual a
   – Não é igual a
10. Digite os valores para os limites **Risco** e **Cuidado**:
   – Limite - especifica um valor que dispara um alerta de risco ou de cuidado.
   – Períodos acima do limite - especifica o número máximo de períodos que o limite pode exceder antes que um alerta seja disparado.
   – Períodos observados - especifica o número total de períodos que estão sendo monitorados para cada iteração do alerta.
11. Clique em **Criar alerta**.

Você criou um alerta com as opções avançadas.

Definir os limites de risco e cuidado

Como administrador, você pode definir os valores de limite de risco e cuidado dos alertas. Um alerta usa as informações de desempenho e as compara com os valores de limite. O alerta exibe *um* dos seguintes estados:

- **Verde** - nenhuma das métricas que o alerta compara está violando os limites de risco ou cuidado, como a configuração do alerta especifica.
- **Amarelo** – um alerta relata um estado de cuidado. Uma tentativa de usar o aplicativo ou o componente provavelmente produzirá resultados insatisfatórios.
- **Vermelho** - um alerta relata o estado de risco, um problema que exige atenção imediata.
- **Cinza** - o alerta não está relatando nenhum dado. As métricas cujas correspondências do alerta simples não estão relatando nada (por exemplo, quando os agentes estão desconectados).
- **N/D** - o alerta não está relatando nenhum dado.Um alerta simples não está ativo ou não corresponde a nenhuma métrica.

Siga estas etapas:

1. No painel esquerdo, passe o mouse sobre o ícone de sino e clique em **Alertas**.
   A página Alertas será exibida e relacionará as métricas a seguir:
   – **Application Errors** - o número de alertas que foram disparados quando o limite de erros do aplicativo for excedido.
   – **Backend Errors** - um alerta que é disparado quando é excedido o limite de erros de back-end não relacionados ao SQL ou ao serviço web.
   – **Status da conexão** - um alerta que é disparado quando há um problema no DockerMonitor Agent ao estabelecer conexão com a configuração do Docker.
   – **CPU Utilization** - um alerta que é disparado quando o limite de utilização da CPU é excedido.
   – **Frontend Errors** - um alerta que é disparado quando é excedido o limite de erros do grupo de URLs de front-end.
   – **Frontend Response Time** - um alerta que é disparado quando é excedido o limite dos tempos de resposta do grupo de URLs de front-end.
   – **Fronted Stalls** - um alerta que é disparado quando é excedido o limite de paralisações do grupo de URLs de front-end. Uma paralisação é uma solicitação de front-end que não foi concluída dentro de um tempo específico (por padrão, 30 segundos). As paralisações indicam um segmento travado devido a algum loop infinito, bloqueio ou restrição de recursos.
   – **Memória heap usada (%)** - um alerta que é disparado quando é excedido o limite do percentual de memória heap usada.
   – **Response Time Variance Intensity** - um alerta que é disparado quando o limite de intensidade de variação de tempo de resposta é excedido.
     A intensidade da variação é uma medida de estabilidade de 10 a 40:
     - 10 - estável
     - De 11 a 25 - relativamente estável
     - De 25 a 30 - moderadamente instável
     - De 30 a 40 - gravemente instável
   – **WebService Client Errors** - um alerta que é disparado quando é excedido o limite de erros no cliente do serviço web (SOAP ou REST). - um alerta que é disparado quando é excedido o limite de erros no cliente do serviço web (SOAP ou REST).
   – **WebService Server Errors** - um alerta que é disparado quando é excedido o limite de erros no servidor do serviço web.
2. Expanda o alerta que você deseja configurar.
3. No campo Limite de risco, digite o valor que dispara um alerta de Risco.
4. No campo Cuidado, digite o valor que dispara um alerta de Cuidado.
   As unidades correspondem ao valor usado no agrupamento de métricas. Por exemplo, se você criar um alerta simples para Tempo médio de resposta, o valor será em milissegundos.
5. Clique em **Salvar alerta**.

   TIP

   Dica: evite configurar os limites de uma maneira que possa gerar alertas com muita frequência. Você deseja ser alertado, mas não tem resultados decisivos.

Ativar ou desativar alertas

Você pode especificar quais alertas deseja usar para o monitoramento. A página Alertas mostra uma lista dos alertas disponíveis de maneira concisa.

Siga estas etapas:

1. No painel esquerdo, passe o mouse sobre o ícone de sino e clique em **Alertas**.

A página Alertas será exibida e relacionará os alertas.
2. Localize o alerta que deseja ativar ou desativar.
3. (Opcional) Clique no nome de uma coluna para classificar de acordo com o valor do cabeçalho.
4. Clique em uma linha para expandir Detalhes de alerta.
5. Defina o botão de alternância como **Ativo** ou **Inativo**.
6. Clique em **Salvar**.

O alerta está ativo ou inativo.

Excluir um alerta

Como administrador, você pode excluir um alerta que não seja mais necessário.

Siga estas etapas:

1. No painel esquerdo, passe o mouse sobre o ícone de sino e clique em **Alertas**.
2. Expanda o alerta que você deseja excluir.
3. Clique em **Excluir**.

Você excluiu um alerta.

Entender as expressões regulares

As expressões regulares definem as métricas a serem incluídas na definição do alerta. Uma expressão regular (RegEx do Perl) é uma sequência de caracteres de texto que descreve um padrão de pesquisa.

Especificador de agente

Um especificador de agente define os agentes dos quais o alerta recupera os dados. Por exemplo, um especificador de agente aplica o alerta apenas aos agentes de todos os domínios denominados WPS2-01 ou WPS2-02. Um especificador de agente é útil quando diversas JVMs geram relatórios para o mesmo Gerenciador corporativo, mas têm finalidades diferentes. Como, por exemplo, executar sites diferentes na mesma empresa. Nesse caso, limite os agentes aos quais o agrupamento de métricas será aplicado usando as expressões regulares para criar um filtro.

Os especificadores de agente usam as seguintes partes:
1. Nome do host que executa o processo a ser monitorado
2. Nome do processo específico em uma instância do aplicativo ou do aplicativo Java gerenciado do qual você deseja coletar dados
3. Agente responsável pela coleta de dados

Especificador de métrica

Um especificador de métrica define as métricas a serem incluídas no alerta. O especificador de métrica filtra todos os dados que os agentes entregam, conforme sua expressão de agente. Os especificadores de métrica requerem uma atenção mais cuidadosa do que os especificadores de agente porque o número de métricas filtradas excede o número de agentes.

Os especificadores de métrica usam as seguintes partes:
1. Recursos que conduzem à métrica
2. Nome da métrica

Gerenciar dados de métrica usando módulos de gerenciamento

Você pode usar os Módulos de gerenciamento para gerenciar e organizar os dados de métrica para monitoramento. Os Módulos de gerenciamento são conjuntos de objetos e configurações.

Módulos de gerenciamento

Os Módulos de gerenciamento de cada domínio contêm elementos. Os elementos são objetos que contêm e organizam dados de métrica com a lógica de monitoramento para apresentação no Team Center. Os elementos são:

- Agrupamentos de métricas
- Alertas (que incluem Alertas simples)
- Módulos de gerenciamento
- Calculadoras

Um Módulo de gerenciamento padrão é incluído no SuperDomain quando você instala o Introscope. Esse Módulo de gerenciamento padrão contém painéis pré-configurados que incluem a lógica de monitoramento de desempenho comumente usada. Crie outros Módulos de gerenciamento para outros domínios criados.

Um Módulo de gerenciamento útil é o Módulo de gerenciamento de Infraestrutura do APM, que contém a definição de alertas e outros objetos que abrangem as principais métricas de integridade do APM.

NOTE
Para ver os alertas na Central de equipe, certifique-se de que as métricas sejam mapeadas para nós e que a configuração Propagar para a Central de equipe esteja ativada. Vá para Team Center, Gerenciamento. A caixa de seleção Propagar para o Team Center está na definição do alerta.

NOTE
Um ícone de Manutenção na página Módulos de gerenciamento, na guia Manutenção, mostra que a página está em manutenção. O ícone Manutenção ficará visível por um período máximo de 7 dias antes de qualquer manutenção futura.

O ícone de manutenção será exibido com base na seguinte ordem de prioridade:

1. Ativo com a hora de término mais recente
2. Ativo com a menor hora de término
3. Programado com a hora de início mais próxima
4. Restante da programação

Permissões, aplicação de domínio e edição de elementos

Os agentes são particionados em domínios. Os usuários recebem acesso a determinados domínios e só podem criar elementos e Módulos de gerenciamento que fazem referência a dados em domínios aos quais os usuários pertencem. Para criar ou editar elementos, você deve ter as permissões apropriadas. Para executar a maioria das alterações nos elementos, é necessário ter permissão de gravação no domínio em que o elemento está. Algumas funções exigem uma permissão específica. Tenha em mente que, ao criar ou modificar um elemento, os elementos nos domínios individuais só poderão fazer referência a outros elementos no mesmo domínio. Os elementos no SuperDomain podem fazer referência a elementos em qualquer domínio.

Se você for um usuário avançado, poderá executar operações CRUD em alertas, módulos de gerenciamento, calculadoras e agrupamentos de métricas.

Personalizar módulos de gerenciamento

Use os módulos de gerenciamento padrão e de Infraestrutura do APM com novas implantações do APM. Os módulos podem ser personalizados para atender aos requisitos de monitoramento de sua organização. A personalização é especialmente válida para as implantações que estão sendo atualizadas a partir de versões mais antigas ou implantações grandes do APM. Os Módulos de gerenciamento mencionados anteriormente e os seus próprios Módulos de gerenciamento devem ser personalizados antes de passarem para o ambiente de produção. Você pode aplicar as seguintes configurações de personalização:

- Ativar ou desativar alertas
- Definir os limites de alerta apropriados
- Ajustar períodos em um limite
- Ativar ou desativar a caixa de seleção **Propagar para o Team Center**

O módulo de gerenciamento do sistema para a página inicial do Team Center contém os alertas e agrupamentos de métricas necessários para o status de integridade de chamadas de back-end, CPU, memória e camada de aplicativo. Os administradores do APM não devem ajustar este módulo de gerenciamento.

NOTE

Mais informações:

- Ativar ou desativar alertas e ações

Este vídeo explica como trabalhar com módulos de gerenciamento no APM Team Center:

Você pode usar os Módulos de gerenciamento para gerenciar e organizar os dados de métrica para monitoramento. Os Módulos de gerenciamento são conjuntos de objetos e configurações. Este tópico aborda as seguintes seções:

- Módulos de gerenciamento
- Permissões, aplicação de domínio e edição de elementos
- Personalizar módulos de gerenciamento

Para gerenciar e organizar os dados de métrica para monitoramento, consulte Gerenciar dados de métrica usando módulos de gerenciamento.

Criar e trabalhar com módulos de gerenciamento

Os módulos de gerenciamento organizam elementos para que você possa localizá-los, copiá-los e editá-los convenientemente. Os módulos de gerenciamento são armazenados como arquivos *.jar* no diretório *<pasta_principal_EM>*/config/modules. Os módulos de gerenciamento também podem existir nos domínios do subdiretório abaixo do diretório *<pasta_principal_do_EM>*/config/modules. Um usuário pode definir esses domínios e o módulo de gerenciamento .jar abaixo deles.

Você pode definir um módulo de gerenciamento como editável/não editável ou ativo/inativo. Quando um módulo não for editável, os elementos dentro dele também não poderão ser editados. Quando um módulo de gerenciamento está inativo, os elementos dentro dele também estão inativos.

Elementos no editor do módulo de gerenciamento

Esta tabela descreve os elementos do módulo de gerenciamento:

Elemento	Descrição
Módulo de gerenciamento	Um recipiente que contém elementos.
Alertas	Notificações de possíveis problemas em seu aplicativo, geradas pela comparação de valores de métrica em relação aos valores de limite definidos pelo usuário e pela geração de um status.
Calculadoras	Uma calculadora soma ou calcula a média de dados da métrica para gerar métricas personalizadas.
Agrupamentos de métricas	Objetos que especificam quais métricas devem ser levadas em consideração; usados como blocos de construção para elementos como alertas.

Pesquisar elementos do módulo de gerenciamento

Você pode pesquisar qualquer elemento do módulo de gerenciamento usando expressões regulares da sintaxe Lucene.

Observação: para obter mais informações,confira Consultar eventos armazenados.

Siga estas etapas:

1. No editor do módulo de gerenciamento, selecione um domínio ou um nó do módulo de gerenciamento.
2. Clique na guia **Pesquisar**.
3. Digite uma expressão regular, usando a sintaxe Lucene, no painel Filtrar.
   Observação: caracteres especiais devem ser representados entre caracteres de escape. Iniciar a sequência de caracteres de pesquisa com um asterisco (*) ou ponto de interrogação (?) provoca um erro. Esses caracteres não são permitidos no início de uma expressão Lucene.
   À medida que você digita no painel **Filtrar**, as correspondências são exibidas a cada tecla pressionada. As correspondências são exibidas em uma tabela na guia **Pesquisar**. Essas informações são exibidas para cada elemento correspondente à pesquisa:
   a. Nome do elemento
   b. Módulo de gerenciamento ao qual o elemento pertence
   c. Domínio ao qual o módulo de gerenciamento pertence

Nomeando módulos de gerenciamento e elementos

As regras a seguir se aplicam à nomenclatura de módulos de gerenciamento e elementos:

- Os módulos de gerenciamento dentro do mesmo domínio devem ter nomes exclusivos.
  Nomes de módulo de gerenciamento não exclusivos são permitidos em domínios separados.
- Os mesmos tipos de elemento do módulo de gerenciamento dentro de um único módulo de gerenciamento devem ter nomes exclusivos.
  Por exemplo, você pode ter um alerta e uma calculadora, ambos denominados **Bytes em uso**, mas não é possível ter dois alertas denominados **Bytes em uso**.
- Os nomes de elemento do módulo de gerenciamento não exclusivos podem existir quando estiverem em módulos de gerenciamento separados.
  Por exemplo, você pode ter dois alertas, ambos denominados **Alerta de servlet A**. Um alerta está no módulo de gerenciamento de amostra e o outro alerta está em um módulo que você criou chamado **Módulo de teste**.

Para facilitar a nomeação, você pode usar a opção **Forçar exclusividade** para criar e nomear um módulo de gerenciamento ou elemento:

- Quando a opção **Forçar exclusividade** estiver ativada e você digitar um nome que já existe, o DX APM adicionará um número ao nome para torná-lo exclusivo.
  O número acrescido aparece depois que o modelo de relatório é criado, quando você o exibe no **Editor do módulo de gerenciamento**.
- Quando a opção **Forçar exclusividade** estiver desativada e já existir um nome de modelo de relatório idêntico, o DX APM exibirá uma mensagem de erro e não criará o relatório.

Criar um módulo de gerenciamento

Para criar um módulo de gerenciamento, execute as tarefas a seguir.

Siga estas etapas:

1. No Team Center, selecione **Módulos de gerenciamento** e clique em **Criar módulo de gerenciamento**.
2. Na página Criar módulo de gerenciamento, digite os seguintes detalhes:
   a. No campo **Nome do módulo de gerenciamento**, digite um nome para o módulo de gerenciamento (o nome é exibido na árvore Editor do módulo de gerenciamento).

   b. Digite os detalhes no campo **Expressão do agente**. Para obter mais informações, consulte Definir expressões do agente para um módulo de gerenciamento.
   c. No campo **Descrição**, digite a descrição necessária que ajuda a identificar o módulo de gerenciamento que você cria.
   d. Clique em **Salvar**.
      O módulo de gerenciamento foi criado com êxito.
3. Clique em **OK**
   O módulo de gerenciamento é exibido na árvore **Editor do módulo de gerenciamento**. Os módulos estão ativos e podem ser editados no momento da criação.

Atualizar um módulo de gerenciamento

Para atualizar um módulo de gerenciamento, execute as tarefas a seguir.

Siga estas etapas:

1. Em **Configurações**, clique em **Módulos de gerenciamento**.
2. Os Módulos de gerenciamento disponíveis para o usuário são exibidos. Também é possível pesquisar um Módulo de gerenciamento específico usando o filtro.
3. Clique no nome do Módulo de gerenciamento necessário. A página **Edit Management Module** correspondente será exibida.
4. Na página **Edit Management Module**, atualize os seguintes detalhes:
   a. Clique no botão de alternância para marcar o Módulo de gerenciamento como ativo ou inativo.
   b. No campo **Nome do módulo de gerenciamento**, edite o nome do Módulo de gerenciamento (o nome é exibido na árvore Editor do módulo de gerenciamento).
   c. No campo **Descrição**, atualize a descrição necessária que ajuda a identificar o módulo de gerenciamento que você cria.
   d. No campo **Nome do arquivo JAR**, atualize o nome do arquivo `.jar` para o módulo de gerenciamento usando caracteres alfanuméricos sem espaços (para conformidade com todos os sistemas operacionais).
   e. Atualize os detalhes no campo **Expressão do agente**. Para obter mais informações, consulte Definir expressões do agente para um módulo de gerenciamento.
   f. A tabela **Visualização** exibe uma lista de todos os agentes conectados e seu estado (Conectado ou Desconectado).
   g. O usuário pode alternar para outras configurações relacionadas a esse módulo de gerenciamento, como agrupamentos de métricas, alertas, alertas de resumo, calculadoras e análise diferencial, a serem atualizadas.
   h. Clique em **Salvar**.
      O módulo de gerenciamento foi atualizado com êxito.
   i. Na caixa de diálogo de confirmação, clique em **OK**.
      O Módulo de gerenciamento atualizado será exibido na página **Módulos de gerenciamento**.

Tornar um módulo de gerenciamento ativo ou inativo

Se o módulo de gerenciamento ficar inativo, tudo o que ele contém também ficará inativo.

Siga estas etapas:

1. Selecione o módulo de gerenciamento na árvore Editor do módulo de gerenciamento.
2. No painel de configurações do módulo de gerenciamento, marque ou desmarque a caixa de seleção **Ativo**.
3. Clique em **Aplicar**.

Copiar um Módulo de gerenciamento

Para copiar um Módulo de gerenciamento, execute as tarefas a seguir.

1. Em **Configurações**, clique em **Módulos de gerenciamento**.
2. Os Módulos de gerenciamento disponíveis para o usuário são exibidos. Também é possível pesquisar um Módulo de gerenciamento específico usando o filtro.
3. Clique no nome do Módulo de gerenciamento necessário. A página **Edit Management Module** correspondente será exibida.
4. Na página **Edit Management Module**, clique em **Save as New**.
5. Na caixa **Criar módulo de gerenciamento** exibida, atualize os detalhes a seguir, se for necessário.
   Você também pode ignorar esta etapa e clicar em **Salvar** na caixa Criar módulo de gerenciamento para criar uma cópia do Módulo de gerenciamento.

   NOTE
   Criar uma cópia do Módulo de gerenciamento existente copiará as configurações apenas da guia Propriedades. Talvez seja necessário criar outras configurações.

   a. Clique no botão de alternância para marcar o Módulo de gerenciamento como ativo ou inativo.
   b. No campo **Nome do módulo de gerenciamento**, edite o nome do Módulo de gerenciamento (o nome é exibido na árvore Editor do módulo de gerenciamento).
   c. Atualize os detalhes no campo **Expressão do agente**. Para obter mais informações, consulte Definir expressões do agente para um módulo de gerenciamento.
   d. No campo **Descrição**, atualize a descrição necessária que ajuda a identificar o módulo de gerenciamento que você cria.
   e. Clique em **Salvar**.
      O módulo de gerenciamento foi criado com êxito.
   f. Na caixa de diálogo de confirmação, clique em **OK**.
      O Módulo de gerenciamento será exibido na página **Módulos de gerenciamento**.

Excluir um módulo de gerenciamento

A exclusão de um módulo de gerenciamento exclui todos os elementos nele.

Siga estas etapas:

1. No Team Center, selecione **Módulos de gerenciamento**.
2. No campo **Pesquisar**, digite o <*nome_do_módulo_de_gerenciamento*> que você deseja atualizar.
   O campo Pesquisar preenche o <*nome_do_módulo_de_gerenciamento*> desejado.
3. Antes de excluir o módulo de gerenciamento, desative-o. No painel de configurações do módulo de gerenciamento, marque ou desmarque a caixa de seleção **Ativo**.
4. Clique em **Aplicar**.
5. No painel do lado esquerdo, clique em **<nome_do_módulo_de_gerenciamento>**.
   A página *Módulo de gerenciamento do* <*nome_do_módulo_de_gerenciamento*> correspondente é exibida.
6. Clique no **ícone Excluir**.
7. Clique em **Sim**.

Exportar um módulo de gerenciamento

Você pode exportar um módulo de gerenciamento existente no formato de arquivo *.jar*.

Siga estas etapas:

1. No Team Center, selecione **Módulos de gerenciamento** e selecione **Exportar**.
   Todos os módulos de gerenciamento serão listados com caixas de seleção anexadas.

2. Selecione os módulos de gerenciamento para exportar e clique em **Exportar**.
   Os módulos de gerenciamento são baixados e exportados para um diretório local com o arquivo denominado modules.zip.
3. Você pode extrair o arquivo modules.zip.
   Todos os módulos de gerenciamento estão disponíveis como arquivos .jar individuais.

Importar um módulo de gerenciamento

Você pode importar um módulo de gerenciamento existente no formato de arquivo *.jar*.

Siga estas etapas:

1. No Team Center, selecione **Módulos de gerenciamento** e selecione **Importar**.
   Uma caixa de diálogo será aberta.
2. Selecione **Choose File** e especifique o arquivo *.jar*.
3. Clique em **Importar** para importar o arquivo.
   O módulo de gerenciamento é exibido na árvore Editor do módulo de gerenciamento. Os módulos estão ativos e podem ser editados no momento da criação.

Definir expressões do agente para um módulo de gerenciamento

Os agrupamentos de métricas (e suas expressões de métrica e agente) filtram dados que correspondem aos critérios de métrica e agente. Todos os agrupamentos de métricas em um módulo de gerenciamento podem compartilhar um único conjunto de expressões do agente. No nível de agrupamento de métricas, você pode especificar se deseja usar a expressão do agente compartilhada ou as expressões do agente do agrupamento de métricas.

O uso de expressões do agente do módulo de gerenciamento simplifica a configuração da lógica de monitoramento. É possível alterar as expressões de métrica e agente do módulo de gerenciamento e fazer com que este as aplique a todos os agrupamentos de métricas que ele contém. Se a implantação for alterada (o nome da máquina, por exemplo), você poderá alterar o módulo de gerenciamento e a alteração se aplicará a todos os itens do módulo. Ou, é possível copiar um módulo de gerenciamento configurado e alterar a expressão do agente para monitorar um agente diferente.

> **NOTE**
> É recomendável usar expressões do agente do módulo de gerenciamento ou expressões do agente do agrupamento de métricas, mas não uma combinação de ambos dentro de um único módulo de gerenciamento. Você também poderá usar somente expressões do agente do agrupamento de métricas se desejar monitorar um conjunto específico de métricas de um conjunto específico de agentes.

Siga estas etapas:

1. No Team Center, selecione **Módulos de gerenciamento**.
2. No campo **Pesquisar**, digite o <*nome_do_módulo_de_gerenciamento*> que você deseja atualizar.
   O campo Pesquisar preenche o <*nome_do_módulo_de_gerenciamento*> desejado.
3. No painel do lado esquerdo, clique em **<nome_do_módulo_de_gerenciamento>**.
   A página *Módulo de gerenciamento do* <*nome_do_módulo_de_gerenciamento*> correspondente é exibida. É exibido um campo Expressões do agente em branco.
4. Você pode fornecer informações de Expressões do agente de duas maneiras:
   – Digite as informações em uma expressão regular.
   – Abra outra janela do Investigador, selecione um agente ou uma métrica e arraste as informações para o campo Expressões do agente. Uma linha é exibida ao redor do campo Expressões do agente.
5. Clique em **Aplicar**.

> **NOTE**
> As Expressões do agente definidas aqui não são automaticamente aplicadas aos agrupamentos de métricas. Use as expressões do agente do módulo de gerenciamento em vez das expressões do agente do agrupamento

de métricas. Para obter informações sobre esse processo, consulte Configurar agrupamentos de métricas no Team Center.

Configurar a segurança do módulo de gerenciamento

Em cada universo, os usuários recebem privilégios individuais por módulo de gerenciamento para editar alertas, calculadoras e grupos de métricas. A função Usuário avançado, os usuários e os grupos de usuários devem receber permissão para ver ou criar alertas, calculadoras ou grupos de métricas para um módulo de gerenciamento.

Siga as instruções em Configurar universos para definir a segurança do módulo de gerenciamento.

Configurar agrupamentos de métricas no Team Center

É possível configurar agrupamentos de métricas no Team Center. Os agrupamentos de métricas são exibidos como uma parte da lista de pastas, que representam os módulos de gerenciamento. Cada pasta contém uma lista de agrupamentos de métricas correspondentes.

Especificando expressões para agrupamentos de métricas

Os agrupamentos de métricas são objetos do módulo de gerenciamento que salvam as seguintes informações:

- A *expressão do agente* -- uma expressão regular em Perl 5 que filtra entradas na métrica especificando os dados até, e inclusive, o nome do agente.
- A *expressão da métrica* – uma expressão regular em Perl 5 que especifica o recurso (a cadeia de pastas que leva à métrica) e a métrica.
- O Módulo de gerenciamento ao qual o agrupamento de métricas pertence.

Veja este exemplo no módulo de gerenciamento de suportabilidade. O agrupamento de métricas de uso do disco (MB) usa estas expressões:

- **Expressão do agente do agrupamento de métricas:**
  ```
  (.*)\|Custom Metric Process \(Virtual\)\|(.*)
  ```
- **Expressão da métrica:**
  ```
  Enterprise Manager\|Data Store\|(.*)Disk Usage \(mb\)
  ```

Para preencher esses campos, você pode digitar as informações usando a linguagem de expressões regulares do Perl 5 ou selecionar e arrastar métricas e agentes do Investigador para os campos. Para fornecer um valor do especificador de métrica sem diferenciação de maiúsculas e minúsculas, especifique o especificador de métrica entre (?i) e (?-i). Por exemplo,

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

As expressões do agente podem ser definidas por módulo de gerenciamento. Essas expressões do agente podem ser aplicadas a agrupamentos de métricas em um módulo de gerenciamento.

Por padrão, cada agrupamento de métrica usa suas próprias expressões de agente para correspondência dos agentes. Se, em vez disso você desejar usar as expressões do agente no módulo de gerenciamento, selecione essa opção no painel de configurações do agrupamento de métricas. Se você selecionar essa opção, os agentes correspondentes mudarão automaticamente se as expressões do agente do módulo de gerenciamento forem alteradas.

Estrutura do nome da métrica

Um nome de métrica totalmente qualificado é semelhante a esta sintaxe:

```
Domain|Hostname|Process|AgentName|Resource:Metric
```

Por exemplo, um nome de métrica totalmente qualificado de uma métrica em um recurso é semelhante a este exemplo:

```
Acme|c1737019-a|AcmeUSA|AcmeWest|GC Heap:Bytes In Use
```

Se uma métrica estiver localizada em dois recursos, o nome se parecerá com este exemplo:

```
Acme|c1737019-a|AcmeUSA|AcmeWest|Servlets|FileServlet:Responses Per Second
```

Se houver camadas de recursos mais profundas, os recursos serão separados pelo caractere de barra vertical (|).

Consulte Usando variáveis para obter mais informações sobre como os nomes das métricas são construídos.

> **NOTE**
> Os usuários que não estão no SuperDomain veem o nome da métrica sem informações do domínio na seguinte sintaxe: *Hostname*|*Process*|*AgentName*|*Resource:Metric*. Por exemplo: c1737019|AcmeUSA|AcmeWest|GC Heap:Bytes In Use

Criar um agrupamento de métricas no menu Elementos

Você pode criar um agrupamento de métricas no menu Elementos.

Siga estas etapas:

1. No Team Center, selecione **Agrupamentos de métricas**.
   A página Agrupamentos de métricas exibe uma lista das métricas que são agrupadas com base nos módulos de gerenciamento.
2. Na página Agrupamentos de métricas, selecione **Criar agrupamento de métricas**.
3. Na página Criar agrupamento de métricas, informe os seguintes detalhes:
   a. No campo **Nome do agrupamento de métricas**, digite um nome de agrupamento de métrica exclusivo (o nome é exibido na árvore Editor do módulo de gerenciamento).
   b. Selecione na lista suspensa um **módulo de gerenciamento** para conter o agrupamento de métricas. Também é possível selecionar **Criar módulo de gerenciamento** para criar um módulo de gerenciamento em uma caixa de diálogo separada.
   c. No campo **Descrição**, digite a descrição necessária que ajuda a identificar o agrupamento de métricas que você criar.
   d. Selecione as expressões do agente necessárias a serem usadas:
      - Selecione **Usar expressões de agente do módulo de gerenciamento** para usar as expressões do agente definidas para o módulo de gerenciamento.
      - Selecione **Usar expressões de agente do agrupamento de métricas** para usar as expressões do agente definidas para esse agrupamento de métricas.
   e. Digite as informações específicas do agente e da métrica nos campos **Expressões de agente do módulo** e **Expressões da métrica**.
   f. Selecione **Criar**.
      O agrupamento de métricas foi criado com êxito.

      > **NOTE**
      > Quando criado, o agrupamento de métricas fica ativo, não podendo ser desativado.

Personalizar agrupamentos de métricas

É possível personalizar as expressões regulares no agrupamento de métricas editando os campos Expressões de agente do agrupamento de métricas e Expressões da métrica a fim de especificar as métricas a serem correspondidas.

Regras para editar os agrupamentos de métricas

- Separe os níveis sucessivos da Árvore do investigador com símbolos de barra invertida. (A barra invertida funciona como um caractere de escape.)
- Em Expressões de agente do agrupamento de métricas: Host\|Process\|AgentName, use **([^\|:]*)** para representar um segmento de recurso.
- Em **Servlets\|([^\|:]*):Average Response Time \(ms\)**, é necessário um caractere de escape (barra invertida) para separadores e parênteses **\|** e **\(** e **\)**.
- Em **Servlets\|Servlet1:Average Response Time \(ms\)** para correspondência de vários itens com uma expressão, é possível incluir listas de itens entre parênteses usando caracteres de barra vertical.
- Em **Servlets\|Servlet(1|14|18):Average Response Time \(ms\)**, se não houver pastas de recurso entre o Nome do agente e a métrica, insira apenas o nome da métrica. Caso contrário, separe as pastas de recurso com símbolos de barra invertida e preceda o nome da métrica com dois-pontos (:).
- Em Expressões da métrica: **resource\|subresource:Metric**
- Em Expressões da métrica: **resource:Metric**
- Em Expressões da métrica: **Metric**
- Por exemplo, em Expressões da métrica, você especifica o tempo médio de consulta JDBC para um servlet chamado OptionReport como **Servlets\|OptionReport\|JDBC:Average Query Time**.
- Use **(.*)** como representação de "qualquer".
- Por exemplo, **Cherubim\|PhoneHome\|(.*)** seguido por **Sockets:Output Bandwidth** especificaria a largura de banda de saída para todos os soquetes de qualquer instância do processo PhoneHome em execução no host Cherubim.
- Uma entrada **File System:(.*)** no campo Expressões da métrica significa que os dados a serem exibidos são as métricas de entrada e saída do arquivo encontradas no Investigador em Sistema de arquivos. Em contrapartida, **File System:File Input Rate** exibe apenas a taxa de entrada do arquivo.
- Use **(.*)\|(.*)\|(.*)** no campo Agente para fazer com que o agrupamento de métricas exiba dados de qualquer servidor, qualquer processo e qualquer agente. Você também pode especificar qualquer um dos segmentos ou todos eles para corresponder aos agentes com um determinado host, processo ou nome de agente.
- Use uma previsão negativa na expressão regular do agrupamento de métricas para excluir uma ramificação da árvore de métricas. Por exemplo, **Agents\|(.*)\|(.*)\|(?!ima_q01)([^\-:]*):ConnectionStatus** exclui "ConnectionStatus" de ima_q01, enquanto ainda exibe "ConnectionStatus" de outros agentes.

Siga estas etapas:

1. No Team Center, selecione **Agrupamentos de métricas**.
   A página Agrupamentos de métricas exibe uma lista das métricas que são agrupadas com base nos módulos de gerenciamento.
2. Expanda o agrupamento de métricas que você deseja atualizar.
3. Selecione o *Nome_do_agrupamento_de_métricas* que você deseja atualizar.
   A página **Editar agrupamento de métricas: <Nome_do_agrupamento_de_métricas>** é exibida.
4. Edite a definição seguindo as regras para editar os agrupamentos de métricas.
5. Se necessário, selecione **sinal de adição (+)** para especificar mais métricas para o agrupamento de métricas.
6. Selecione **Aplicar**.

Excluir um agrupamento de métricas do menu Elementos

É possível excluir um agrupamento de métricas do menu Elementos.

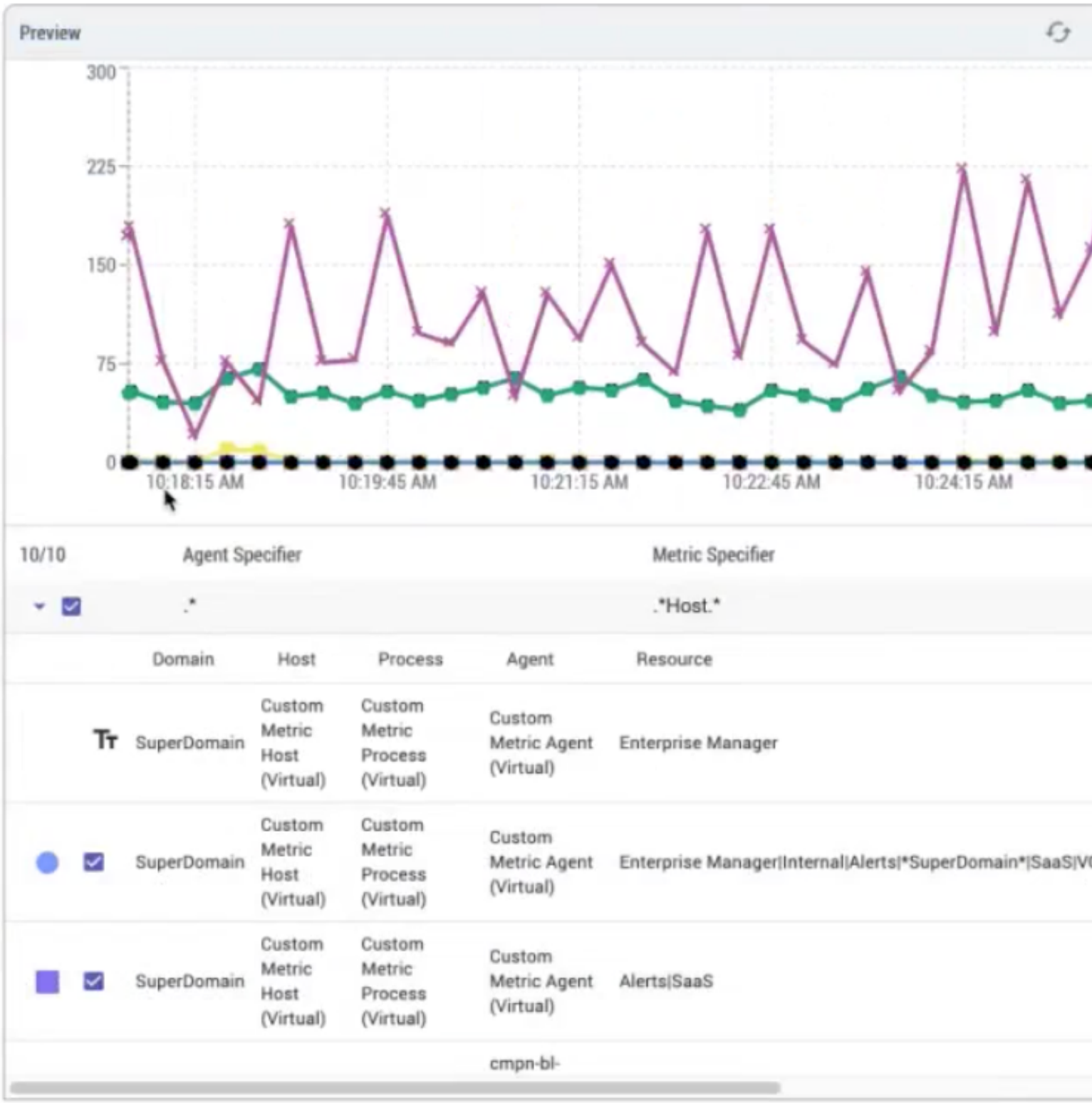
Siga estas etapas:

1. No Team Center, selecione **Agrupamentos de métricas**.
   A página Agrupamentos de métricas exibe uma lista das métricas que são agrupadas com base nos módulos de gerenciamento.
2. Expanda o agrupamento de métricas que você deseja atualizar.

3. Selecione o *Nome_do_agrupamento_de_métricas* que você deseja atualizar.
   A página **Editar agrupamento de métricas: <Nome_do_agrupamento_de_métricas>** é exibida.
4. Selecione o ícone Excluir ( )
5. Selecione **Sim**

Visualização do agrupamento de métricas

A visualização da exibição da métrica mostra o modo de visualização dos grupos de métricas configurados. Você pode exibir dados de métrica relevantes plotados no gráfico. A janela Visualização mostra o gráfico de dados de métricas com base no **Especificador de agente** e no **Especificador de métrica** fornecidos no campo **Expressões**.

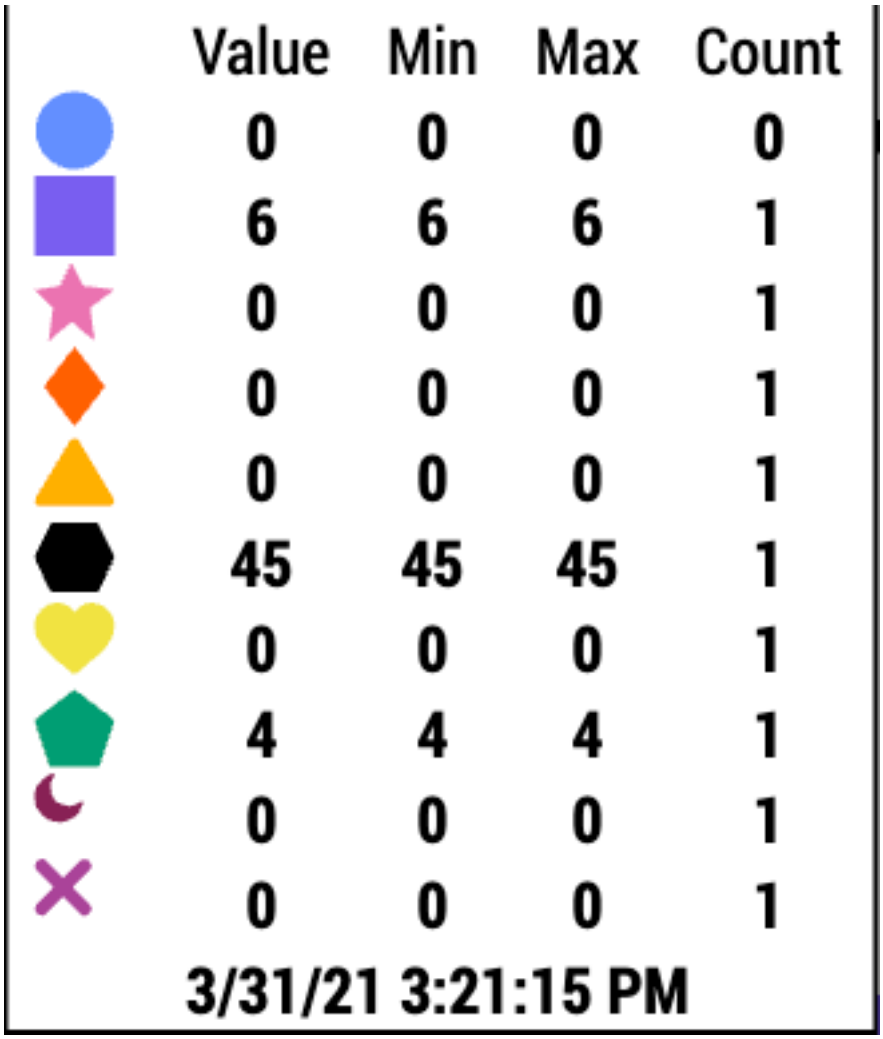


Na janela Visualização, é possível exibir e executar as seguintes tarefas:

- Especifique o **Especificador de métrica** e o **Especificador de agente** no campo **Expressões**, e o ícone de **Atualizar**

  será realçado. Clique no ícone Atualizar para exibir as métricas mais recentes com base nas expressões.
- A tabela Visualização mostra a contagem do total de métricas, o especificador de agente, o especificador de métrica e o número de métricas a serem exibidas no gráfico.
- Você pode selecionar apenas dez métricas para exibir no gráfico.
- É possível personalizar as colunas a serem exibidas na tabela. Clique em

  e selecione as colunas necessárias na lista.
- Há dez cores e formas diferentes para distinguir as métricas representadas no gráfico. À medida que você seleciona uma métrica na lista, uma cor e uma forma são atribuídas automaticamente a uma métrica.



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

- Clique no ícone de tela cheia

  para exibir a janela Visualização no modo de tela cheia.
- No gráfico da visualização, o eixo X representa os valores da métrica e o eixo Y representa o intervalo de tempo.

É possível configurar agrupamentos de métricas no Team Center. Os agrupamentos de métricas são exibidos como uma parte da lista de pastas, que representam os módulos de gerenciamento. Cada pasta contém uma lista de agrupamentos de métricas correspondentes.

Para obter mais informações sobre os itens a seguir, consulte Configurar agrupamentos de métricas no Team Center

- Especificando expressões para agrupamentos de métricas
- Estrutura do nome da métrica
- Criar um agrupamento de métricas no menu Elementos
- Personalizar agrupamentos de métricas
- Excluir um agrupamento de métricas do menu Elementos
- Visualização do agrupamento de métricas

Criar e configurar alertas simples no Team Center

Como administrador, você pode criar e configurar alertas e ações no Team Center para monitorar o desempenho.

> **NOTE**
> Não use o método padrão de criação de alertas do APM para métricas ingeridas diretamente no NASS (isso inclui as métricas de suportabilidade do Cloud Proxy do APM e qualquer métrica que não seja do APM). Em vez disso, use a configuração de alerta com base em métricas do DX OI.

> **NOTE**
> Um ícone de Manutenção na página Alertas, na guia Manutenção, mostra que a página está em manutenção. O ícone Manutenção ficará visível por um período máximo de 7 dias antes de qualquer manutenção futura.
>
> O ícone de manutenção será exibido com base na seguinte ordem de prioridade:
>
> 1. Ativo com a hora de término mais recente
> 2. Ativo com a menor hora de término
> 3. Programado com a hora de início mais próxima
> 4. Restante da programação

O Team Center oferece os seguintes alertas:

Alerta simples

Usa informações de status geradas por uma comparação e compara essas informações com valores de limite definidos pelo usuário. A saída de um alerta simples é um status. Os alertas simples podem usar atrasos na ação de Risco e Cuidado de modo a determinar quando iniciar ações especificadas. Um alerta simples pode produzir um dos seguintes estados:

- **Sem relato de dados**
  Ocorre se o alerta simples estiver inativo, não corresponder a nenhuma métrica, ou se as métricas correspondentes não estiverem gerando relatórios.
- **Verde (OK)**
- **Amarelo (Cuidado)**
- **Vermelho (Risco)**

O alerta simples é o alerta básico no Introscope.Alertas simples podem produzir a entrada para um alerta de resumo. Esse alerta é exibido sob o nó Alertas na Árvore do investigador.

Alertas de resumo

Agrega o status de vários alertas simples e outros alertas de resumo.Esse alerta é exibido sob o nó Alertas na Árvore do investigador.

> **NOTE**
> **Mais informações**: Criar e configurar alertas de resumo

Criar um alerta simples no menu Elementos

Siga estas etapas:

1. No Team Center, selecione **Alertas** e **Criar alerta**.
   A página Alertas exibe uma lista de alertas que são agrupados por Agrupamento de métricas.
2. Na página Alertas, selecione **Criar alerta**.
3. Na página Criar alerta, informe os seguintes detalhes:
   a. No campo **Nome do alerta**, digite um nome para o alerta simples
      O nome é exibido na árvore Editor do módulo de gerenciamento.

TIP

Use nomes informativos para alertas. É recomendável usar uma convenção de nomenclatura que ajude o destinatário do alerta a identificar a origem do alerta.

b. Na lista suspensa **Canais de notificação**, selecione o canal desejado a ser aplicado ao alerta simples que você criar.
c. Na lista suspensa **Módulo de gerenciamento**, selecione o módulo desejado a ser aplicado ao alerta simples que você criar.Também é possível selecionar **Criar módulo de gerenciamento** para criar um módulo de gerenciamento em uma caixa de diálogo separada.
d. No campo **Descrição**, digite a descrição necessária que ajuda a identificar o alerta simples que você criar.
e. No campo **Agrupamento de métricas**, selecione o agrupamento de métricas desejado a ser aplicado ao alerta simples que você criar. Você também pode selecionar **Criar agrupamento de métricas** para criar um **Agrupamento de métricas** em uma caixa de diálogo separada.
f. No campo **Resolução**, especifique a resolução do período em horas, minutos ou segundos. Um alerta usa dados de entrada de um agrupamento de métricas selecionado. Para a resolução de tempo, o alerta coleta informações e resume um valor para esse período. O valor resultante depende do tipo de dados na métrica. Por exemplo, se a métrica for uma taxa, o valor resumido será a taxa média durante esse período. Ou, se a métrica for um contador, será gerado o valor mais recente do contador. Os valores de resolução de tempo devem ser em incrementos de 15 segundos.
g. Na lista suspensa **Operador de comparação**, selecione um valor na lista suspensa para a condição que dispara o alerta simples. O operador de comparação, com os valores de limite de cuidado e risco, define a condição que dispara o alerta simples. O operador de comparação está relacionado aos valores de limite de cuidado e risco. Por exemplo, se você deseja ser notificado quando o tempo médio de resposta do servlet for maior que 5000, use o operador "maior que". O operador de comparação também afeta os valores de limite de cuidado e risco. Se o operador de comparação for definido como maior que, o valor do limite de risco deverá ser maior que o valor do limite de cuidado. Por outro lado, se o operador de comparação for definido como menor que, o valor do limite de risco deverá ser menor do que o valor do limite de cuidado.
h. No campo **Combinação**, especifique se um alerta é disparado quando uma métrica excede um limite (qualquer) ou todas as métricas excedem um limite (todos). O campo Combinação é ignorado quando a caixa de seleção Notificar por métrica individual é marcada.
i. Na seção **Limites**, selecione **Salvar**.
   O módulo de gerenciamento foi criado com êxito.

4. Selecione **OK**

O alerta simples que você criou é realçado na árvore Editor do módulo de gerenciamento e suas configurações são exibidas no painel configurações.

Para obter mais informações sobre como ativar as notificações de alerta, consulte Criar notificações para alertas. Para obter mais informações sobre a documentação da política para configurar notificações de alerta adicionais no Operational Intelligence, consulte Criar política.

Atualizar um alerta simples no menu Elementos

Siga estas etapas:

1. No Team Center, selecione **Alertas**. A página Alertas é exibida com os alertas agrupados pelo Agrupamento de métricas.
2. Vá até o Agrupamento de métricas do alerta que você deseja atualizar.
3. Selecione o <*nome_do_alerta*> que deseja atualizar.
4. Na página **Editar alerta: <nome_do_alerta>**, atualize os seguintes detalhes:
   a. No campo **Nome do alerta**, atualize o nome do alerta simples
      O nome é exibido na árvore Editor do módulo de gerenciamento.

TIP

Use nomes informativos para alertas. É recomendável usar uma convenção de nomenclatura que ajude o destinatário do alerta a identificar a origem do alerta.

b. Na lista suspensa **Canais de notificação**, selecione o canal desejado a ser aplicado ao alerta simples.
c. Na lista suspensa **Módulo de gerenciamento**, selecione o módulo desejado a ser aplicado ao alerta simples.Também é possível selecionar **Criar módulo de gerenciamento** para criar um módulo de gerenciamento em uma caixa de diálogo separada.
d. No campo **Descrição**, atualize a descrição necessária que ajuda a identificar o alerta simples.
e. No campo **Agrupamento de métricas**, selecione o agrupamento de métricas desejado a ser aplicado ao alerta simples. Você também pode selecionar **Criar agrupamento de métricas** para criar um **Agrupamento de métricas** em uma caixa de diálogo separada.
f. Na lista suspensa **Operador de comparação**, selecione um valor na lista suspensa para a condição que dispara o alerta simples. O operador de comparação, com os valores de limite de cuidado e risco, define a condição que dispara o alerta simples. O operador de comparação está relacionado aos valores de limite de cuidado e risco. Por exemplo, se você deseja ser notificado quando o tempo médio de resposta do servlet for maior que 5000, use o operador "maior que". O operador de comparação também afeta os valores de limite de cuidado e risco. Se o operador de comparação for definido como maior que, o valor do limite de risco deverá ser maior que o valor do limite de cuidado. Por outro lado, se o operador de comparação for definido como menor que, o valor do limite de risco deverá ser menor do que o valor do limite de cuidado.
g. Na seção **Limites**, selecione **Salvar**.
O módulo de gerenciamento foi criado com êxito.

5. Selecione **OK**

O alerta simples que você criou é realçado na árvore Editor do módulo de gerenciamento e suas configurações são exibidas no painel configurações.

Copiar um alerta simples

Para copiar um alerta simples, execute as tarefas a seguir.

1. Em **Configurações**, clique em **Alertas**.
2. Os Módulos de gerenciamento disponíveis para o usuário são exibidos. Também é possível pesquisar um Módulo de gerenciamento específico usando o filtro.
3. Clique no nome do Módulo de gerenciamento necessário e no Nome do alerta.
4. Na página **Editar alerta**, clique em **Save as New**.
5. Na caixa **Criar outro alerta** exibida, atualize os detalhes a seguir, se necessário.
Você também pode ignorar essa etapa e clicar em **Salvar** na caixa Criar outro alerta para criar uma cópia do alerta.
   a. Clique no botão de alternância para marcar o Alerta como ativo ou inativo.
   b. No campo **Nome do alerta**, digite um nome para o alerta simples (o nome é exibido na árvore Editor do Módulo de gerenciamento).
   c. Na lista suspensa **Canais de notificação**, selecione o canal desejado a ser aplicado ao alerta simples que você criar.
   d. Na lista suspensa **Módulo de gerenciamento**, selecione o módulo desejado a ser aplicado ao alerta simples que você criar. Também é possível selecionar Criar módulo de gerenciamento para criar um módulo de gerenciamento em uma caixa de diálogo separada.
   e. No campo **Descrição**, digite a descrição necessária que ajuda a identificar o alerta simples que você criar.
   f. No campo **Agrupamento de métricas**, selecione o agrupamento de métricas desejado a ser aplicado ao alerta simples que você criar. Você também pode selecionar Criar agrupamento de métricas para criar um Agrupamento de métricas em uma caixa de diálogo separada.
   g. No campo **Resolução**, especifique a resolução do período em horas, minutos ou segundos. Um alerta usa dados de entrada de um agrupamento de métricas selecionado. Para a resolução de tempo, o alerta coleta informações

e resume um valor para esse período. O valor resultante depende do tipo de dados na métrica. Por exemplo, se a métrica for uma taxa, o valor resumido será a taxa média durante esse período. Ou, se a métrica for um contador, será gerado o valor mais recente do contador. Os valores de resolução de tempo devem ser em incrementos de 15 segundos.

h. Na lista suspensa **Operador de comparação**, selecione um valor na lista suspensa para a condição que dispara o alerta simples. O operador de comparação, com os valores de limite de cuidado e risco, define a condição que dispara o alerta simples. O operador de comparação está relacionado aos valores de limite de cuidado e risco. Por exemplo, se você deseja ser notificado quando o tempo médio de resposta do servlet for maior que 5000, use o operador "maior que". O operador de comparação também afeta os valores de limite de cuidado e risco. Se o operador de comparação for definido como maior que, o valor do limite de risco deverá ser maior que o valor do limite de cuidado. Por outro lado, se o operador de comparação for definido como menor que, o valor do limite de risco deverá ser menor do que o valor do limite de cuidado.

i. No campo **Combinação**, especifique se um alerta é disparado quando uma métrica excede um limite (qualquer) ou todas as métricas excedem um limite (todos). O campo Combinação é ignorado quando a caixa de seleção Notificar por métrica individual é marcada.

j. Especifique os valores em **Limite de risco** e **Limite de cuidado**.

k. Clique em **Create**.
O alerta foi criado com êxito.

l. Na caixa de diálogo de confirmação, clique em **OK**.
O alerta é exibido na página **Módulos de gerenciamento**.

Excluir um alerta simples no menu Elementos

Siga estas etapas:

1. No Team Center, selecione **Alertas**.
A página Alertas é exibida com os alertas agrupados pelo Agrupamento de métricas.
2. Vá até o Agrupamento de métricas do alerta que você deseja excluir.
3. Selecione o <*nome_do_alerta*> que deseja excluir.
A página **Editar alerta: <nome_do_alerta>** é exibida.
4. Na página **Editar alerta: <nome_do_alerta>**, selecione o ícone Excluir ( ).
5. Selecione **Sim**
6. Selecione **OK**

O alerta simples foi excluído com êxito.

Definir as configurações do alerta simples

Depois de criar um alerta simples, defina as condições do disparador.

Siga estas etapas:

1. Localize o alerta simples que você criou na árvore Editor do módulo de gerenciamento, sob o módulo de gerenciamento correspondente. Selecione o alerta simples para exibir suas configurações.
2. No painel de configurações, marque a caixa de seleção **Ativo** para ativar o alerta simples. Marque a caixa de seleção **Propagar para o Team Center** para ver os alertas no Team Center.
3. Use o operador de comparação e as ações de risco e cuidado para definir a condição que dispara o alerta simples. Por exemplo, se você deseja ser notificado quando o tempo médio de resposta do servlet for maior que 5000, use o operador *maior que*.

NOTE

O operador de comparação também afeta os valores de limite de cuidado e risco. Se o operador de comparação for definido como *maior que*, o valor do limite de risco deverá ser maior que o valor do limite de cuidado. Por outro lado, se o operador de comparação for definido como *menor que*, o valor do limite de risco deverá ser menor do que o valor do limite de cuidado.

4. Em ações de Risco ou Cuidado, selecione **Adicionar**.
   a. Selecione uma ação e selecione **Escolher**.
   b. Adicione outra ação, se apropriado.
   c. No painel de configurações do alerta simples, selecione **Aplicar**.
5. No campo Limite, informe um valor que dispare um alerta de Risco ou de Cuidado.
   As unidades nos valores de limite de risco correspondem ao valor usado no agrupamento de métricas. Por exemplo, para criar um alerta simples do Tempo médio de resposta do servlet, use milissegundos.
6. Defina o índice de períodos excessivos que dispara o alerta. Defina essa condição nos campos **Períodos acima do limite** e **Períodos observados**.
   Exemplo: você digitou 8 e 10. O alerta de risco irá disparar somente se a métrica exceder o limite de risco em 8 ou 10 períodos observados.

   TIP

   - Use a propriedade *Pelo menos N dos últimos M períodos* a fim de definir alertas para problemas reais. Essa propriedade define o número de instâncias que são necessárias para que o limite de risco dispare um alerta. Por exemplo, em ambientes de produção, os indicadores chave de desempenho podem ter picos por um curto período. Uma CPU pode ter picos por um período 15 segundos e retornar ao estado normal nos próximos 15 segundos. Esse comportamento de desempenho não requer um alerta e pode ser descartado usando uma condição.
   - É recomendável notificar os destinatários do alerta antes de alterar os limites de alerta existentes. Diminuir o limite de um alerta ativo pode fazer com que o alerta seja enviado.

   NOTE
   Os alertas serão disparados somente no final do **período observado** e não assim que os períodos acima do limite forem atingidos.
7. Defina um atraso na ação em horas, minutos e segundos.
   Os atrasos na ação de risco ou cuidado determinam quando uma ação de alerta simples é disparada.

   NOTE

   Os atrasos na ação de risco ou cuidado não estão disponíveis na opção de alerta Resolução.
8. Selecione **Aplicar**.
   O alerta simples está concluído e aparece na árvore sob o módulo de gerenciamento correspondente. Exemplo: configurar um alerta para desconexão do agente

   NOTE

   Quando você cria um alerta simples a partir de uma métrica, um agrupamento de métricas é criado automaticamente. Esse agrupamento de métricas é exibido no mesmo módulo de gerenciamento.

Configurar um alerta para desconexão do agente

Se um agente for desconectado do Enterprise Manager, você não conseguirá mais coletar nem monitorar os dados desse agente. É possível configurar um alerta para disparar uma notificação que avisará você se ocorrer uma desconexão.

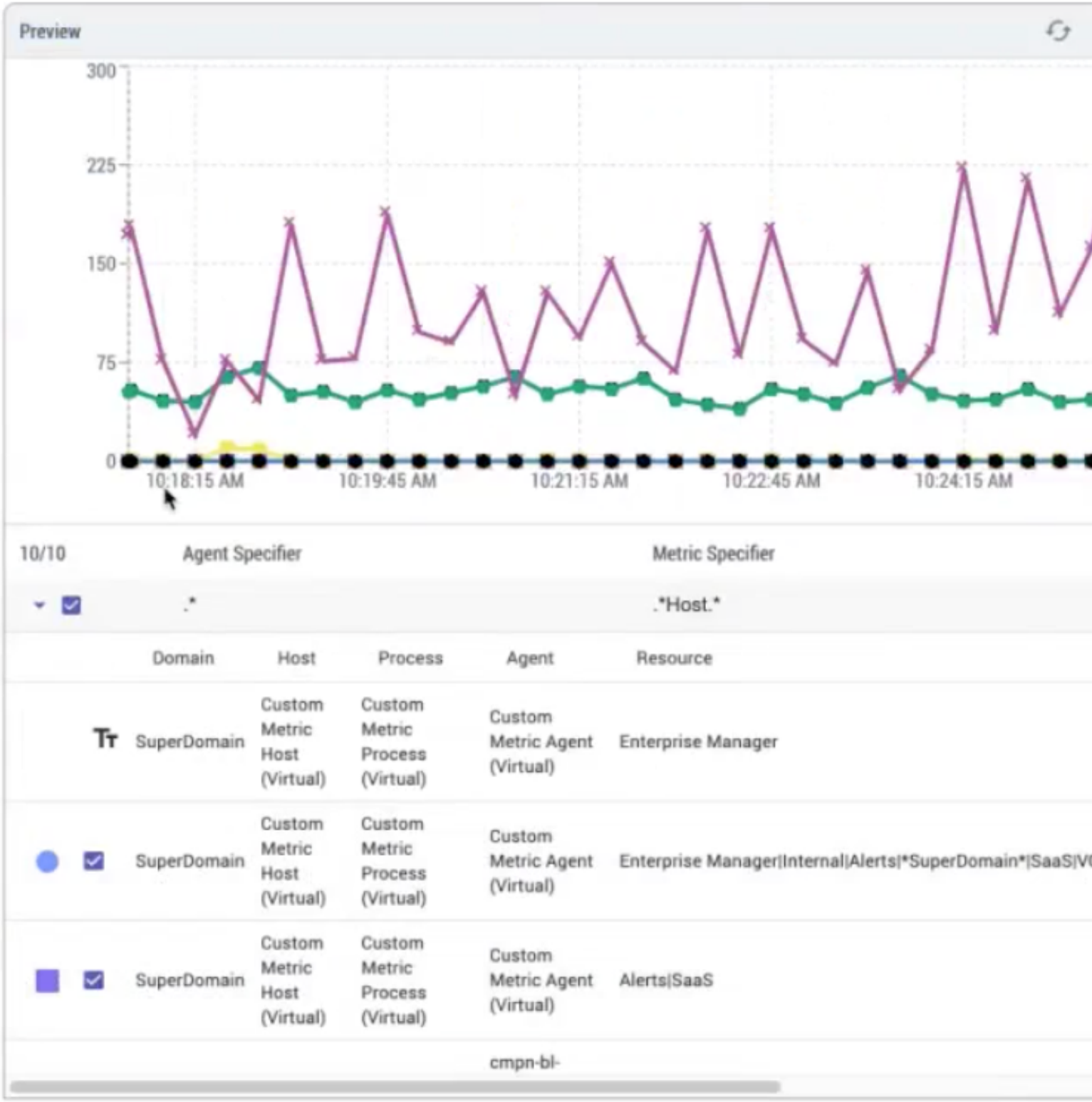
Siga estas etapas:

1. No Team Center, selecione **Agrupamentos de métricas**.
2. Na página Agrupamentos de métricas, selecione **Novo agrupamento de métricas**.

3. Essa métrica tem os seguintes valores:
   – 3 = desconectado, indica que o agente foi desconectado manualmente.
   – 2 = conectado, lento ou sem dados
   – 1 = conectado
   – 0 = não montado, indica que o agente foi desconectado do Enterprise Manager após um determinado período. Esse período pode ser configurado.
4. Digite um nome para o novo alerta e selecione **OK**.
5. Defina o operador de comparação como **Menor que**.
6. Defina o limite de risco e o limite de cuidado.
7. Defina a confidencialidade do limite para o alerta. **Exemplos**:
   – Muito confidencial (Risco = 2, Cuidado = 2, Pelo menos *1* dos últimos *10* períodos)
   – Menos confidencial (Risco = 3, Cuidado = 2, Pelo menos *3* dos últimos *10* períodos)
8. Selecione **Ativo**.
9. Selecione **Aplicar**.

Visualização de alertas

A visualização de alertas exibe o modo de visualização dos grupos de métricas configurados. Você pode exibir dados de métrica relevantes plotados no gráfico. A janela de visualização mostra o gráfico de dados de métricas com base no campo **Agrupamento de métricas**.



Na janela Visualização, é possível exibir e executar as seguintes tarefas:

- Forneça o filtro para o campo Agrupamento de métricas, e o ícone de **Atualizar**

  será realçado. Clique no ícone Atualizar para exibir as métricas mais recentes com base nas expressões.
- A tabela Visualização mostra a contagem do total de métricas, o especificador de agente, o especificador de métrica e o número de métricas a serem exibidas no gráfico.
- Você pode selecionar apenas dez métricas para exibir no gráfico.
- É possível personalizar as colunas a serem exibidas na tabela. Clique em

  e selecione as colunas necessárias na lista.
- Há dez cores e formas diferentes para distinguir as métricas representadas no gráfico. À medida que você seleciona uma métrica na lista, uma cor e uma forma são atribuídas automaticamente a uma métrica.

	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			

- Clique no ícone de tela cheia

  para exibir a janela Visualização no modo de tela cheia.
- No gráfico da visualização, o eixo X representa os valores da métrica e o eixo Y representa o intervalo de tempo.

Como administrador, você pode criar e configurar alertas e ações no Team Center para monitorar o desempenho. O Team Center oferece os seguintes alertas:

- Alerta simples
- Alertas de resumo

Para obter mais informações sobre como criar, atualizar, excluir e configurar um alerta simples, consulte Criar e configurar alertas simples no Team Center.

Criar e configurar alertas de resumo

Um alerta de resumo fornece uma maneira de mostrar o status de vários alertas simples subjacentes com um status geral. Você pode criar e configurar alertas de resumo no Team Center, no Workstation ou no WebView. Você pode modificar o nome e os alertas simples subjacentes em todos os ambientes. Há diferenças entre notificações e ações:

- **Team Center:** suporte para atribuir o Canal de notificação - opção preferida
- **Workstation:** suporte para criar e atribuir ações de rastreamento de transação
- **WebView:** suporte somente para atribuir ações de rastreamento de transação

Esta seção contém as seguintes informações:

- Alertas de resumo
- Criar um alerta de resumo
- Configurar um alerta de resumo
- Atrasos na ação de risco e cuidado

NOTE
Um ícone de Manutenção na página Alertas de resumo mostra que a página está em manutenção. O ícone Manutenção ficará visível por um período máximo de 7 dias antes de qualquer manutenção futura.

O ícone de manutenção será exibido com base na seguinte ordem de prioridade:

1. Ativo com a hora de término mais recente
2. Ativo com a menor hora de término
3. Programado com a hora de início mais próxima
4. Restante da programação

Alertas de resumo

Os alertas de resumo não têm limites explícitos de risco ou cuidado, ou expressões de comparação, como com os alertas simples. Um alerta simples tem um dos quatro estados: não relatando, verde, amarelo e vermelho.

Ícone de estado	Definição	Valor numérico
Diamante ou triângulo amarelo	Cuidado	2
Octógono ou quadrado vermelho	Risco	3
Disco verde	Normal	1
Disco cinza	Não relatando	0

O estado de alerta de resumo é o pior estado entre os alertas simples que ele contém. O alerta de resumo pode ser definido para Qualquer alerta ou Todos os alertas. A opção Qualquer alerta usa o estado máximo de todos os alertas. A opção Todos os alertas usa o estado mínimo de todos os alertas com um estado superior a 0 (Não relatando). Exemplo: você tem um alerta de resumo que consiste nos seguintes alertas:

- Alerta: A; Estado: 0
- Alerta: B; Estado: 1
- Alerta: C; Estado: 1
- Alerta: D; Estado: 2
- Alerta: E; Estado: 3

Nessa situação, a opção Qualquer alerta é 3, e a opção Todos os alertas é 1.

Criar um alerta de resumo

Para o Team Center, faça o seguinte:

1. Vá para **Configurações**, selecione **Alertas**, **Alertas de resumo**.
2. Clique em **Criar alerta de resumo**.
3. Defina as configurações do alerta de resumo.

Para o Workstation ou o WebView, faça o seguinte:

1. Na janela do editor do Módulo de gerenciamento, selecione Elementos, Novo alerta, Novo alerta de resumo.
2. Conclua as seguintes opções:
   - **Nome:** especifica um nome para o elemento. Para identificar a origem de um elemento, use um nome descritivo.

NOTE
Os alertas simples e de resumo são exibidos juntos sob o nó Alertas, portanto, especifique um nome para distinguir os alertas de resumo dos alertas simples.

- **Forçar exclusividade:** acrescenta um número ao nome quando o mesmo nome existe no módulo de gerenciamento.
- **Módulo de gerenciamento:** especifica um módulo de gerenciamento para conter o elemento.

3. Clique em OK. O alerta de resumo que você criou será realçado na árvore do editor do Módulo de gerenciamento e será exibido no painel de configurações.
4. Defina as configurações do alerta de resumo.

Configurar um alerta de resumo

Em todos os ambientes, é possível:

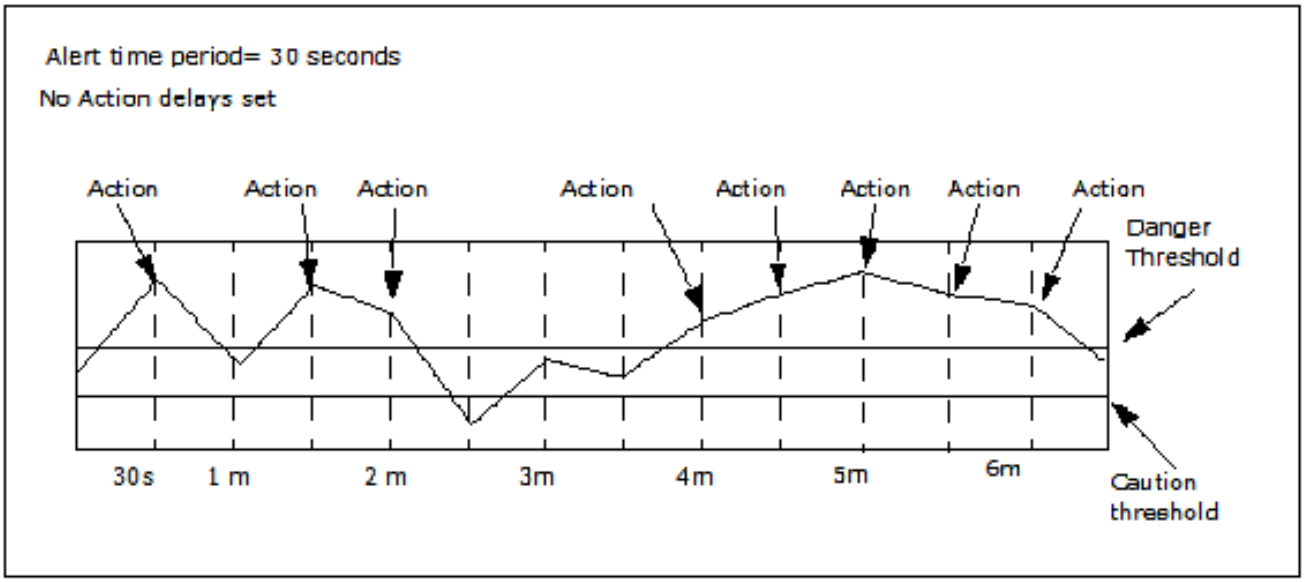
1. Editar os campos conforme apropriado. Por exemplo, você pode executar as seguintes ações:
   - Editar o nome e selecionar um módulo de gerenciamento.
   - Ativar ou desativar o objeto usando a caixa de seleção Ativo.
2. Atribuir alertas ao alerta de resumo. Para o Team Center, use o botão **Adicionar alertas**. Para o Workstation ou o WebView, selecione um ou mais alertas e use as setas para movê-los da lista Disponível para a lista Incluído.
3. Selecionar uma combinação para Qualquer alerta ou Todos os alertas.

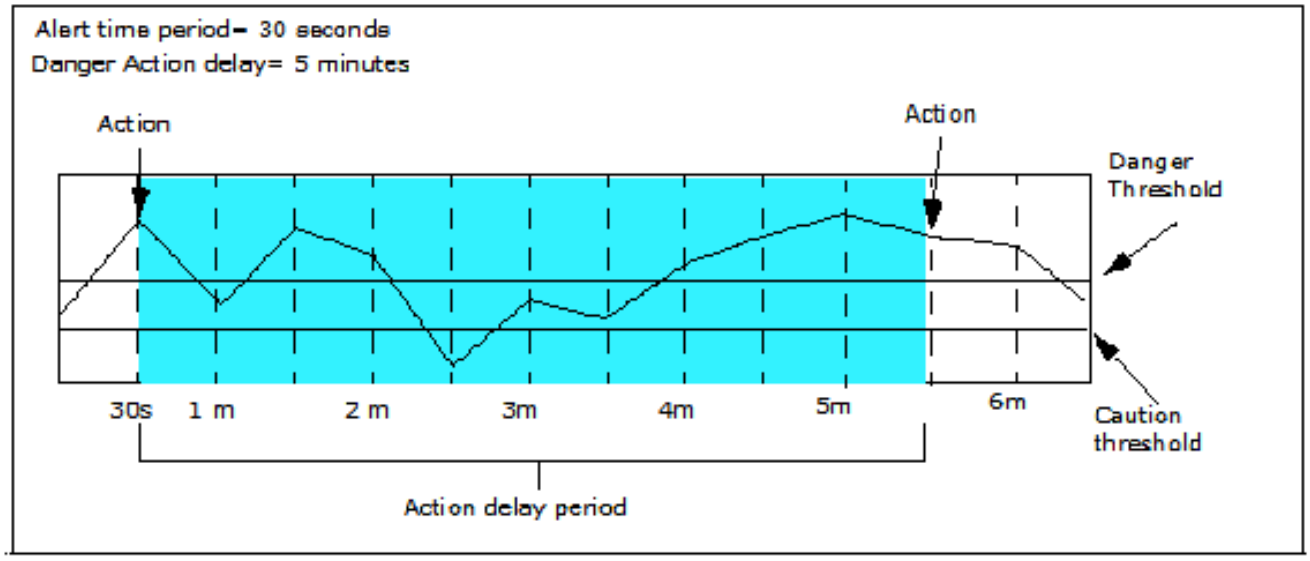
No Team Center, você pode atribuir um Canal de notificação. No Workstation ou no WebView, é possível atribuir uma ação rastreamento de transação e definir um atraso na ação.

Atrasos na ação de risco e cuidado

(Somente no WebView e no Workstation para ações de Rastreamento de transação)

Os atrasos na ação de risco e cuidado determinam as condições nas quais os status de risco ou cuidado são relatados pelo resultado de uma comparação na ação. Esses atrasos na ação evitam inundações de notificações de alerta.
Um atraso age como um botão de pausa intermitente para notificações de alerta. Você pode definir um atraso entre a primeira notificação de alerta e as notificações subsequentes.





Em um cenário em que o período de alerta seja definido como 30 segundos. Se as informações gerarem um status de alerta de Risco e você tiver definido uma ação para ele, a ação será disparada. Sem um atraso definido, se o status de Risco continuar, você será notificado sempre que o limite de Risco for excedido. Por exemplo, você é notificado oito vezes por um curto período. Geralmente, os problemas não são resolvidos em um período tão curto como 30 segundos. Portanto, atrase as ações subsequentes com um atraso na ação. Ou seja, com o mesmo período de alerta de 30 segundos, se definir um atraso de ação de cinco minutos para o status de Risco, você receberá a primeira notificação de alerta na marca de 30 segundos. No entanto, se o status de Risco ocorrer novamente durante o período de apagão de cinco minutos e o limite de Risco ainda for excedido quando o período de apagão terminar, você não será notificado sobre uma segunda ação até cinco minutos após a primeira notificação.

Criar e editar calculadoras

As calculadoras usam os valores de um agrupamento de métricas como entrada e calculam a média ou somam os valores. As calculadoras geram o valor resultante como uma métrica personalizada na Árvore do investigador. As métricas geradas pela calculadora são exibidas em um processo virtual denominado Custom Metric Process. O processo de métrica personalizada é executado em um host virtual chamado de host de métrica personalizada.

Sobre as calculadoras

As calculadoras podem calcular a média ou somar os valores de um agrupamento de métricas e, em seguida, gerar métricas personalizadas na Árvore do investigador. As métricas da calculadora são executadas em um processo virtual conhecido como processo de métrica personalizada. Esse processo é executado em um host virtual, o host de métrica personalizada.

As métricas de suportabilidade coletam dados usando calculadoras. Para relatar dados corretamente, qualquer calculadora com base em MOM requer dados de, pelo menos, um coletor. Sem os dados do coletor, o MOM não pode calcular nem exibir métricas.

Exemplo
Em um MOM, você deseja ver a métrica `(.*)\|Custom Metric Process \(Virtual\)\|Custom Metric Agent \(Virtual\)Enterprise Manager\|Configuration:Number of Metric Groupings`. Você espera um valor de métrica maior que 0.

Quando o MOM não tem nenhum coletor conectado, a métrica `Number of Metric Groupings` relata 0.

Quando o MOM possui pelo menos um coletor conectado, a métrica `Number of Metric Groupings` relata o valor correto.

Calculadora de JavaScript

Uma calculadora de JavaScript executa cálculos complexos, como desvio padrão e médias não ponderadas. Veja mais vantagens a seguir:

- Maior controle sobre a frequência de cálculo das métricas
- Gerenciamento de caminhos da métrica calculada de modo a parecer que um agente está relatando a métrica
- Armazenamento de cálculos anteriores e geração de métricas agregadas por um período especificado usando variáveis globais
- Avaliação de métricas de sequência de caracteres ou geração de uma métrica de sequência de caracteres calculada

Calculadora do módulo de gerenciamento

A calculadora do módulo de gerenciamento executa cálculos simples em métricas, como soma, média, e valores mínimo e máximo.

A calculadora do módulo de gerenciamento requer menos recursos do que as calculadoras de JavaScript. Veja mais vantagens a seguir:

- Requer menos recursos do sistema do que a calculadora de JavaScript
- É possível criar e manter as calculadoras. Não é necessário acesso aos diretórios de instalação para criar ou gerenciar a calculadora do módulo de gerenciamento.

Criar uma calculadora

Você pode criar uma calculadora para um grupo de métricas.

Siga estas etapas:

1. No Team Center, selecione **Calculadoras**.
   A página Calculadoras exibe uma lista de calculadoras que são agrupadas com base nos módulos de gerenciamento.
2. Selecione **Criar calculadora**.
   A página Criar calculadora é exibida.
3. Para editar uma calculadora, selecione a calculadora que deseja atualizar.
   A página Editar calculadora: <*nome_da_calculadora*> é exibida.
4. Na lista suspensa **Módulo de gerenciamento**, selecione o módulo desejado a ser aplicado à calculadora simples que você criar. Também é possível selecionar **Criar módulo de gerenciamento** para criar um módulo de gerenciamento em uma caixa de diálogo separada.
5. No campo **Descrição**, digite a descrição necessária que ajuda a identificar a calculadora simples que você criar.
6. No campo **Agrupamento de métricas**, selecione o agrupamento de métricas desejado a ser aplicado à calculadora simples que você criar. Você também pode selecionar **Criar agrupamento de métricas** para criar um Agrupamento de métricas em uma caixa de diálogo separada.

   NOTE

   - Quando a calculadora é criada, um agrupamento de métricas é automaticamente criado com o mesmo nome que a calculadora. No entanto, o agrupamento de métricas deve ser personalizado para que possa fornecer dados à calculadora.
   - Selecione um agrupamento de métricas que forneça valores inteiros. As calculadoras não podem aceitar valores não inteiros como entrada. Tipos mistos produzem resultados inesperados.

   NOTE

   Mais informações: Configurar o agrupamento de métricas no Team Center

Calculadoras e médias ponderadas

As calculadoras do Introscope podem produzir métricas com base em médias. Os cálculos têm como base as médias ponderadas, não as médias simples. As médias ponderadas são úteis no monitoramento do desempenho do seu aplicativo em um ambiente agrupado. Nessa situação, você pode ver o tempo de resposta preciso entre vários servidores que, provavelmente, têm níveis de carga diferentes.

Exemplo:

Você tem uma calculadora gerando uma métrica a partir do tempo médio de resposta para cinco servlets. Uma média simples adicionaria o tempo de resposta de um período definido e dividiria por cinco. Uma média ponderada daria mais importância aos servlets chamados com mais frequência, o que proporciona uma média mais precisa.

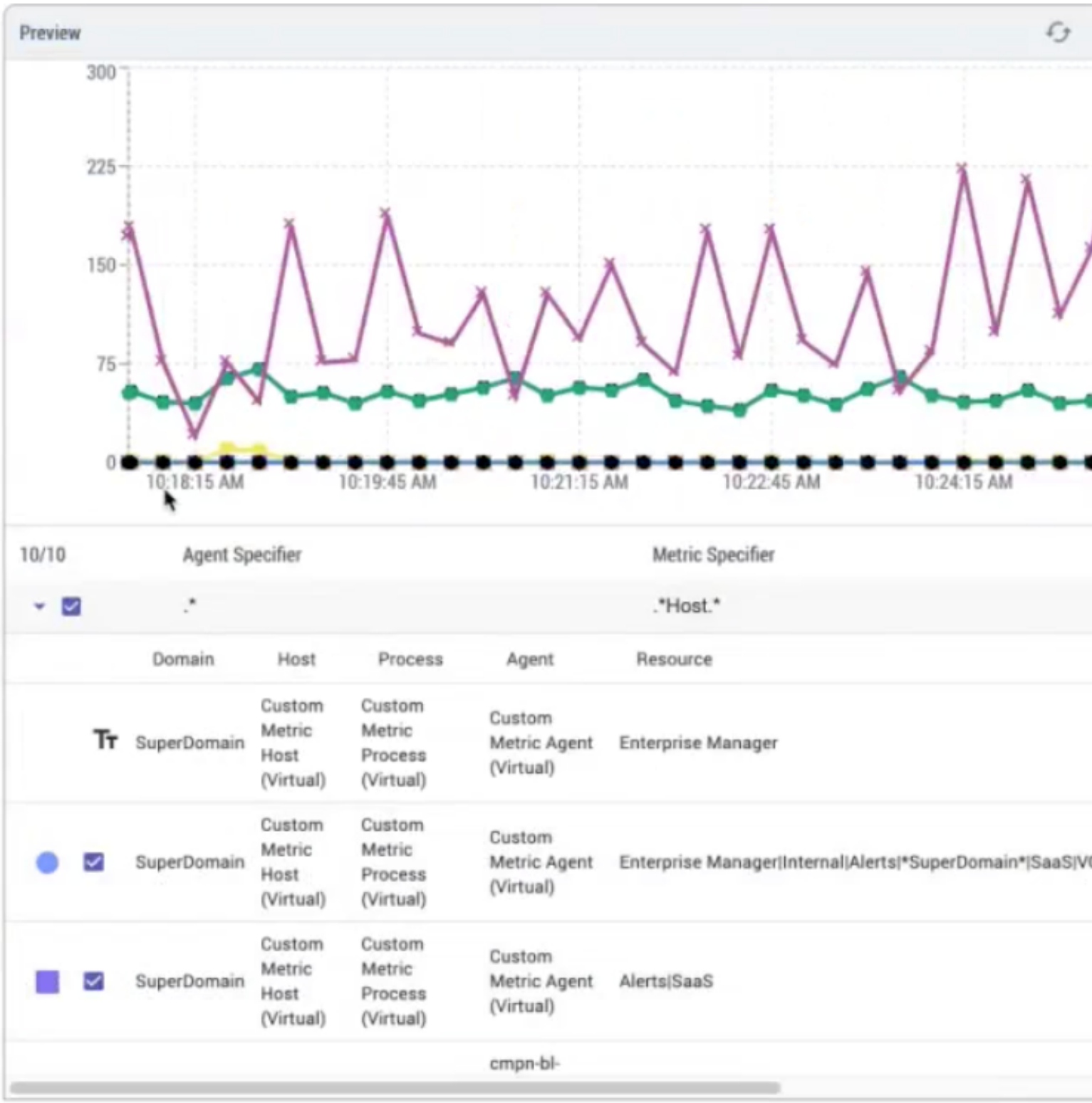
Alterando os tipos de operação em calculadoras do módulo de gerenciamento

Quando você editar uma calculadora em um módulo de gerenciamento, altere o tipo de operação para redefinir o significado da métrica de saída da calculadora. Por exemplo, de MÍN. para MÁX.Se você mantiver o mesmo nome da métrica de saída da calculadora, exibir essa métrica justapõe os valores antigos no histórico (calculados, por exemplo, pelo MÍN.) sobre os novos valores (por exemplo, o MÁX.). A exibição da métrica de saída não fornece qualquer indicação de onde ocorreu a alteração no processamento. Se os usuários ficarem confusos, renomeie a métrica de saída da calculadora quando for alterar o tipo de operação.

> **NOTE**
>
> **Mais informações:** Alterar os tipos de operação nas calculadoras do módulo de gerenciamento

Visualização de calculadoras

A visualização de calculadoras exibe o modo de visualização dos grupos de métricas configurados. Você pode exibir dados de métrica relevantes plotados no gráfico. A janela de visualização mostra o gráfico de dados de métricas com base no campo **Agrupamento de métricas**.



Na janela Visualização, é possível exibir e executar as seguintes tarefas:

- Forneça o filtro para o campo Agrupamento de métricas, e o ícone de **Atualizar**

  será realçado. Clique no ícone Atualizar para exibir as métricas mais recentes com base nas expressões.
- A tabela Visualização mostra a contagem do total de métricas, o especificador de agente, o especificador de métrica e o número de métricas a serem exibidas no gráfico.
- Você pode selecionar apenas dez métricas para exibir no gráfico.
- É possível personalizar as colunas a serem exibidas na tabela. Clique em e selecione as colunas necessárias na lista.
- Há dez cores e formas diferentes para distinguir as métricas representadas no gráfico. À medida que você seleciona uma métrica na lista, uma cor e uma forma são atribuídas automaticamente a uma métrica.

	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			

- Clique no ícone de tela cheia

  para exibir a janela Visualização no modo de tela cheia.
- No gráfico da visualização, o eixo X representa os valores da métrica e o eixo Y representa o intervalo de tempo.

As calculadoras usam os valores de um agrupamento de métricas como entrada e calculam a média ou somam os valores. As calculadoras geram o valor resultante como uma métrica personalizada na Árvore do investigador. As métricas geradas pela calculadora são exibidas em um processo virtual denominado Custom Metric Process.

Para obter mais informações sobre calculadoras, como criar uma calculadora e alterar tipos de operação, consulte Criar e editar calculadoras.

Configurar a análise diferencial

A análise diferencial fica ativa por padrão. Contudo, como administrador, defina as configurações padrão ou crie e configure elementos da análise diferencial. Como responsável pela triagem de aplicativos, você monitora o desempenho usando as informações no mapa ou gráfico da análise diferencial.

Verificar os pré-requisitos da análise diferencial

Antes de implementar a análise diferencial, verifique se a implementação do CA APM inclui o seguinte:

- Um Enterprise Manager
- Agentes configurados para front-ends de aplicativo, back-ends, transações comerciais ou todos.
- Para a instalação do CA CEM, você instalou um TIM (Transaction Impact Monitor).
- Você pode ter um ou mais TIMs em um ambiente do CA CEM.

Criar um controle diferencial

Os controles diferenciais são elementos que detectam instabilidade nas métricas correspondentes. Os limites de cuidado e risco controlam a intensidade da variação, que é uma medida da estabilidade da métrica. Esse comportamento diferencia os controles diferenciais dos alertas tradicionais que combinam o estado nas cores verde, amarelo e vermelho e implicam que existam problemas. Os controles diferenciais permitem determinar quanta instabilidade deve ser registrada para inserir zonas de intensidade de variação de cuidado e risco. As opções avançadas fornecem ainda mais controle sobre as intensidades de variação da análise diferencial. Em geral, os usuários da análise diferencial podem aplicar limites baixos e visualizar o feed completo de mudanças de estabilidade ou usar limites altos e limitar a saída a uma pequena quantidade de mudanças mais extremas (que mais provavelmente indicariam um problema).

É recomendável começar com os limites padrão e alterar as configurações de limite de alerta padrão para indicar as intensidades com as quais você gostaria de obter uma notificação.

O mapa da análise diferencial só será exibido para uma métrica se houver um controle diferencial. Crie um elemento de controle diferencial em um módulo de gerenciamento que corresponda à sua métrica. Os módulos de gerenciamento podem existir para cada domínio ou em todos os domínios, contendo elementos que organizam dados de métrica para apresentação.

Siga estas etapas:

1. No Team Center, selecione **Análise diferencial**.
   A página Análise diferencial exibe uma lista de controles de análise diferencial agrupados com base nos módulos de gerenciamento.
2. Na página Análise diferencial, selecione **Criar controle da análise diferencial**.
   O painel Criar controle da análise diferencial será exibido.
3. Especifique as opções a seguir e clique em **Criar**.
   - **Ativo:** por padrão, um Controle da análise diferencial está ativo. Contudo, configure a ativação ou a desativação.
   - **Nome:** especifique um nome para o elemento Controle da análise diferencial.
   - **Módulo de gerenciamento:** especifique um módulo de gerenciamento ao qual este elemento de Controle da análise diferencial pertence.
   - **Descrição:** opcional. Forneça uma breve descrição do elemento Controle da análise diferencial.
   - **Agrupamento de métricas:** execute um destes procedimentos para selecionar o agrupamento de métricas:
     - Selecione a lista suspensa **Mostrar filtros** e selecione todos os Módulos de gerenciamento dos quais você deseja selecionar o agrupamento de métricas e, em seguida, selecione o agrupamento de métricas necessário na lista. Se necessário, clique em **Abrir** para editar o agrupamento de métricas selecionado.
     - Selecione o agrupamento de métricas necessário na lista de todos os agrupamentos de métricas disponíveis. Se necessário, clique em **Abrir** para editar o agrupamento de métricas selecionado.
     - Selecione o ícone suspenso na lista de agrupamentos de métricas disponíveis e clique em **Criar agrupamento de métricas**, que está disponível na parte inferior da lista.
       A página Criar agrupamento de métricas será exibida para criar um agrupamento de métricas. Para obter mais informações, consulte Configurar agrupamentos de métricas no Team Center.
   - **Limites:** defina as opções de limite para os alertas de **Risco** e **Cuidado**. Esse valor dispara um alerta de risco ou de cuidado.
   - **Janela de avaliação:**
     - **Duração:** especifica o número de células anteriores de 15 segundos que influenciam na importância de uma janela. A importância total da janela determina as regiões de cuidado ou risco. Cada célula da janela contém a

maior importância de todas as regras divididas naqueles 15 segundos, menos qualquer degradação. A célula mais antiga expira e é descartada à medida que novas células são adicionadas. Padrão: 20

- **Degradar:** especifica a taxa na qual as regras violadas se degradam com a célula ao longo do tempo. À medida que novas células são adicionadas, a degradação reduz o efeito das importâncias adicionadas anteriormente na janela. A mais nova tem sempre importância total. Dependendo do valor da degradação, somente partes das importâncias antigas são consideradas para o cálculo final. Dessa forma, cada célula da janela tem uma porcentagem de redução após o nível de degradação. Com base nesse valor de porcentagem de redução, as importâncias são reduzidas em cada nova instância adicionada à janela.

  100 representa a degradação mais rápida, as violações de regra caem de valor rapidamente à medida que expiram. Da mais nova para a mais velha, as células têm reduções progressivas de 0 a 100 na degradação de suas importâncias. Por exemplo, as células mais antigas têm uma redução completa de importância. Essa configuração reduz a probabilidade de notificação de cuidado e risco, especialmente quando um período de instabilidade passa rapidamente.

  0 representa a maior sensibilidade (sem degradação) e as violações mantêm seu valor completo por toda a janela. A mais antiga tem o mesmo valor de quando era a mais recente. Usando essa configuração, um curto período de instabilidade pode manter o pico em um estado de cuidado ou risco até que ele saia completamente da janela. O valor padrão é 20. Violações de regras recentes valem moderadamente mais do que violações de regras mais antigas.

– **Aplicativo da regra:** especifica uma regra para acionar picos:
  - **Regra 1: +3σ** Qualquer ponto de dados único fica fora do limite de 3Σ da linha central.
  - **Regra 2: +2σ (2/3)** Dois de três pontos consecutivos ultrapassam o limite de 2Σ.
  - **Regra 3: +1σ (4/5)** Quatro em cada cinco pontos consecutivos ultrapassam o limite de 1Σ.
  - **Regra 4: Δ f(x) ≥ 0 (10/10)** Dez em cada dez pontos consecutivos estão aumentando ou diminuindo.

Os controles diferenciais são elementos que detectam instabilidade nas métricas correspondentes. Os controles diferenciais permitem determinar quanta instabilidade deve ser registrada para inserir zonas de intensidade de variação de cuidado e risco. As opções avançadas fornecem ainda mais controle sobre as intensidades de variação da análise diferencial.

Em geral, os usuários da análise diferencial podem aplicar limites baixos e visualizar o feed completo de mudanças de estabilidade ou usar limites altos e limitar a saída a uma pequena quantidade de mudanças mais extremas (que mais provavelmente indicariam um problema). A análise diferencial fica ativa por padrão.

Para obter mais informações sobre os pré-requisitos e como criar um controle diferencial, consulte Configurar a análise diferencial.

Configurar as extensões do JavaScript

Uma extensão do JavaScript permite que você crie uma nova extensão e edite uma extensão existente. Essa extensão lê métricas de entrada e produz métricas de saída de acordo com os cálculos especificados em um arquivo de texto JavaScript criado pelo usuário. As novas métricas calculadas podem ser exibidas na Árvore do investigador sob o Agente personalizado virtual. As métricas também podem ser exibidas em qualquer nó da Árvore do investigador, de acordo com a métrica de saída especificada no script de calculadora. Uma métrica calculada pode ser encerrada, mas a calculadora que a produz não sabe sobre o estado de encerramento. O mecanismo JavaScript do Enterprise Manager permite que você implemente dinamicamente calculadoras JavaScript em um Enterprise Manager em execução.

- Acessar extensões do JavaScript
- Gravando calculadoras JavaScript
- Executando calculadoras JavaScript no MOM
- Tipos de dado de métrica

Acessar extensões do JavaScript

Siga estas etapas:

1. Na UI do DX Application Performance Management, clique em **Configurações**.
2. Clique no bloco **Extensões de JavaScript** em **configurações gerais**.
3. Para criar uma nova extensão, clique em **Criar outra extensão**.
4. Selecione um arquivo de extensão e faça upload dele.

   NOTE
   Também é possível editar a extensão existente, fazer download e excluir a extensão.
5. Para ativar ou desativar o status, desative a opção de alternância na coluna **Status**.

A extensão de JavaScript é criada.

Gravando calculadoras JavaScript

Os nomes de arquivo de calculadora JavaScript devem terminar com uma extensão `.js` .

As calculadoras JavaScript especificam métricas de entrada e produzem uma ou mais métricas de saída.

> **NOTE**
> Cada erro em uma calculadora de JavaScript é registrado no log do EM. Erros que ocorrem frequentemente podem encher o log do EM. Teste as calculadoras antes de implantá-las no ambiente de produção.

A função execute( )

Cada calculadora deve ter uma função execute() que utiliza dois argumentos. Além disso, as funções auxiliares estão disponíveis para ajudar a criar métricas a serem enviadas ao Enterprise Manager.A função execute() é chamada a cada 15 segundos pelo mecanismo de script.

Observe o seguinte para a função execute():

- A invocação da função execute() ocorre a cada 15 segundos, mesmo sem métricas que correspondam às expressões regulares retornadas (veja mais tarde). Isso permite que a calculadora, por exemplo, relate uma métrica para indicar que algumas métricas não estão relatando para criar um alerta.
- A invocação a cada 15 segundos é o melhor esforço possível, e não é garantido que sejam exatamente 15 segundos.
- A invocação no segundo 0, 15, 30 e 45 é o melhor esforço possível, mas não é garantido.
- As métricas recebem a marca de data e hora do EM quando são recebidas no retorno de execute().
- Para a estabilidade do EM, a duração da invocação de execute() não deve exceder 7,5 segundos. Exceder 15 segundos provavelmente causará instabilidade no EM e lacunas nas métricas, pois a coleta de métricas dos EMs ficará atrasada. Exceder os 15 segundos de maneira consistente pode causar a falha do EM.
- A única métrica de suportabilidade que alertaria você sobre as calculadoras que estão causando instabilidade é Calculator Harvest Time do Enterprise Manager, que deve exceder 7,5 segundos apenas ocasionalmente e quase nunca exceder 15 segundos.

A sintaxe da função execute() é:

```
function execute(metricData,javascriptResultSetHelper)
```

Em que:

- metricData - é uma matriz de dados de métrica fornecida para a função quando ela é chamada a cada 15 segundos antes dos intervalos de execute().

  NOTE
  A passagem de muitas métricas para uma calculadora deve ser evitada, pois o tempo para criar a matriz MetricData e, especialmente, a memória usada para isso, podem proibir a conclusão em tempo hábil do ciclo de coleta de 15 segundos do Enterprise Manager e causar instabilidade. O limite depende

da configuração do EM. Use Calculator Harvest Time como um indicador de instabilidade, conforme mencionado acima.

```
{ 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

- Ignore as entradas de dados em que data.dataIsAbsent==true.
- Quando nenhuma métrica corresponde às expressões regulares do agente e da métrica, data.length é 0.
- A ordem das métricas dentro da matriz metricData não é definida e pode variar entre as invocações.

- javascriptResultSetHelper - é um objeto que coleta os novos dados de métrica produzidos pelo script e os envia de volta para o EM Esse objeto fornece a função addMetric em duas versões sobrecarregadas:

```
JavascriptResultSetHelper:
  {
    addMetric(fullMetricName, value, type, frequency)



    addMetric(fullMetricName, count, value, min, max, type, frequency)
  }
```

  - kDefaultFrequency - é usado como entrada para o argumento de frequência da função auxiliar addMetric()
  - kIntegerConstant - mapeia para o tipo de métrica constante de número inteiro
  - kIntegerFluctuatingCounter - mapeia para o tipo de métrica do contador de número inteiro flutuante
  - kIntegerConstant - mapeia para o tipo de métrica constante longo
  - kLongFluctuatingCounter - mapeia para o tipo de métrica do contador de longo flutuante
  - kLongTimestamp - mapeia para o tipo de métrica de marca de data e hora longa
  - kLongTimestampConstant - mapeia para o tipo de métrica de constante de marca de data e hora longa
  - kIntegerPercentage - mapeia para o tipo de métrica de percentual de inteiro
  - kIntegerDuration - mapeia para o tipo de métrica de duração do número inteiro
  - kLongDuration - mapeia para o tipo de métrica de duração longa \
  - kLongIntervalCounter - mapeia para o tipo de métrica do contador de intervalo longo
  - kStringIndividualEvents - mapeia para o tipo de métrica de sequência de caracteres
  - addMetric(metricName, count, value, min, max, metricType, frequency) - oferece suporte à configuração de contagem/valor/mín./máx. de um valor de métrica, que é necessária para os tipos de métrica de contagem de intervalo e taxa, em que o "valor" da métrica se baseia em sua "contagem"
  - `getCustomMetricAgentMetric(agentMetric)` - ajuda a criar um nome de métrica totalmente qualificado usando a métrica do agente fornecida e preenchendo o restante com base no nome do agente de métrica personalizado do SuperDomain

NOTE

- Uma métrica só pode ser enviada uma vez. Se métricas duplicadas (apenas por nome) forem enviadas, ocorrerá um erro de métrica atrasada, inválida ou duplicada, que é registrado no log do EM.
- Se a calculadora se destinar a agregar valores de métrica, ela deverá agregar internamente para enviar uma única métrica que seja o valor agregado.
- Se um valor inválido for passado para qualquer valor, ocorrerá um erro (com a mensagem de erro do JavaScript registrada no log do EM).
- A versão anterior, curta e sobrecarregada, define implicitamente count=1.
- Esta última versão, longa e sobrecarregada, é necessária quando você deseja enviar uma métrica com uma contagem maior que 1, o que geralmente é necessário para os tipos de métrica PerIntervalCounter e IntRate (pois estes têm value==count, ou seja, a contagem é tomada como o valor).
- A função execute() deve retornar o objeto javascriptResultSetHelper recebido para enviar as métricas adicionadas pelas chamadas addMetric ao ciclo de coleta dos EMs. Isso porque as chamadas addMetric adicionam métricas a campos ocultos do objeto javascriptResultSetHelper.
- As métricas ocultas no objeto javascriptResultSetHelper só são enviadas ao EM após a conclusão da função execute().

Especificação de métricas de entrada

O script de calculadora pode especificar as métricas de entrada que ele recebe de uma das duas maneiras:

- A maneira de especificar métricas de entrada é com um par de métodos que são chamados pelo EM na implantação da calculadora:
  - função `getAgentRegex()` , que deve retornar uma sequência de caracteres que contém uma expressão regular para corresponder a agentes e
  - função `getMetricRegex()` , que deve retornar uma sequência de caracteres que contém uma expressão regular para corresponder às métricas.

```
function getAgentRegex()
  { return "SuperDomain\\|beta.*\\|Infrastructure Agent\\|EPAgent" }



function getMetricRegex()
  { return "BetaSummary:Rejections" }
```

NOTE

- As expressões regulares no JavaScript têm dois formatos: formato de sequência de caracteres, delimitado por aspas:
  - “(.*)\\|(.*)\\|(.*)”
  - Dentro das sequências de caracteres da expressão regular, os caracteres especiais da expressão regular, que são escritos de forma literal, devem ser representados entre dois caracteres de escape (\\) para aderir ao padrão de escape de barra invertida do Javascript dentro das sequências de caracteres. Portanto, no JavaScript, as barras invertidas (\\) dentro de uma sequência de caracteres significam que a primeira barra invertida está fazendo a função de escape para a segunda, mantendo a segunda barra no lugar.
  - Fora das sequências de caracteres das expressões regulares, não é necessário usar as barras de escape nos caracteres especiais das expressões regulares.
- A expressão regular do agente pode especificar todos os quatro segmentos de um caminho de origem:
  - Domínio | host | processo | agente
  - Os domínios incluem todos os domínios e não apenas o superdomínio
- Não há requisitos de formato para as expressões regulares usadas. Por exemplo, uma expressão regular de agente:

  - “.*”
- incluirá os mesmos agentes que:
  - “.*\|.*\|.*\|.*”
  - “(.*)\|(.*)\|(.*)\|(.*)”
- Se você se preocupar com a eficiência da expressão regular, evite o rastreamento inverso usando correspondências lentas (como em .*?) e grupos de caracteres (como [^\\|]):
  - "SuperDomain\\|beta.*?\\|Infrastructure Agent\\|EPAgent"
  - "SuperDomain\\|beta[^\\|]*\\|Infrastructure Agent\\|EPAgent"

- Como alternativa, você pode usar a função de método `getMetricSpecifier()` , que deve retornar um especificador de métrica completo, ou seja, as expressões regulares do agente e da métrica combinadas.

NOTE
As expressões regulares criadas como sequências de caracteres em functiongetAgentRegex(), função getMetricRegex() e função getMetricSpecifier() devem usar o escape de caracteres, diferentemente de outras expressões regulares usadas no Introscope, por exemplo, em agrupamentos de métricas ou na exibição Pesquisar. Todos os caracteres de escape do Java que são retornados dessas funções JavaScript também devem ser representados entre caracteres de escape no JavaScript. Por exemplo, '\|' deve ser representado entre caracteres de escape como '\\|' no JavaScript.

Log de variáveis globais

Todas as funções de calculadora JavaScript têm acesso a um log de variáveis globais, que é do tipo `IModuleFeedbackChannel` . Por exemplo:

```
function execute(metricData,javascriptResultSetHelper) {
log.info("message");
log.error("message");
log.debug("message");
}
```

NOTE
Se desejar usar os recursos avançados do JavaScript ou estiver preocupado com a conformidade com o ECMA, o mecanismo de script incorpora a biblioteca JavaScript do Mozilla Rhino, versão 1.6_R1.

Criando dados de métrica de saída

A criação de dados de métrica de saída exige:

- **Nome da métrica -** consistindo no agente mais o caminho completo para o nó apropriado na árvore da métrica.
  - Você pode criar um nome de agente com base nos dados de entrada. Os novos dados calculados aparecem com os dados de métrica que o agente relata.
    ou
  - Você pode especificar um novo nome de métrica de calculadora para mostrar os dados de métrica calculados em seu próprio nó na árvore da métrica.
- **Valor dos dados -** calculado pelo script.
- **Tipo de dado do resultado -** especificado por um valor constante da classe com.wily.introscope.spec.metric.MetricTypes.
- Frequência de relatórios - a frequência com que os novos dados de métrica são relatados para o Enterprise Manager, que pode ser obtida a partir dos dados de entrada, ou especificada explicitamente. É possível alterar a frequência para um múltiplo da frequência padrão do Enterprise Manager (15 segundos).

Veja a seguir um valor calculado típico de um script:

```
javascriptResultSetHelper.addMetric(metricName,
 heapUsedValue,Packages.com.wily.introscope.spec.metric.MetricTypes.kIntegerFluctuatingCounter,frequency)
```

NOTE
Especifique expressões regulares com cuidado, pois elas podem corresponder a qualquer métrica que você produz. Por exemplo, uma expressão regular de "EJB.*Time.*" pode inserir um novo valor em EJB. A expressão regular insere um novo valor em "EJB" quando você tem um regex no "EJB.*Time.*". Você pode alterar sua expressão regular para fazer isso ou remover dados de métrica das suas próprias métricas.

Adicionar uma calculadora JavaScript

Para instalar uma nova calculadora JavaScript, faça upload do arquivo de texto JavaScript no EM usando a página Extensões de JavaScript mencionada na seção *Acessar extensões do JavaScript*.

Limitando o tempo de execução do script

O processamento dos dados de métricas de entrada executado pela calculadora pode levar tempo e afetar o desempenho do Enterprise Manager onde a extensão do Javascript é executada. Para proteger o Enterprise Manager contra sobrecarga, especifique o tempo limite do script na origem da extensão. Por exemplo, ao usar uma expressão regular muito genérica para métricas de entrada.

Quando uma função getTimeout() estiver presente na origem do script, o valor retornado será usado como tempo limite do script. Se a função de tempo limite não estiver no script, será usado o tempo limite da extensão padrão do Javascript do Enterprise Manager.

Função `getTimeout()`

Use a função getTimeout() para especificar o tempo limite de execução do script em milissegundos.

Exemplo

Para usar o tempo limite de execução do script como 50ms:

```
function getTimeout() {
   return 50;
}
```

Executando calculadoras JavaScript no MOM

Você pode executar uma calculadora JavaScript no MOM para produzir métricas para o agente de métrica personalizada do MOM. A calculadora não pode produzir métricas para os agentes que estão conectados a um coletor, mas pode ver as métricas de entrada dos agentes nos coletores.

NOTE

Mais informações: Sobre calculadoras.

Se uma calculadora for adicionada, modificada ou excluída em um ambiente agrupado, o MOM propagará automaticamente a alteração para todos os coletores. Essa propagação não ocorre quando as atualizações automáticas de coletores são desativadas.

A função runOnMOM

Uma calculadora JavaScript que não deve ser executada no MOM deve implementar uma função `runOnMOM` que retorna falso, como no exemplo a seguir:

```
// return false if the script should not run on the MOM
// default is true.
```

```
function runOnMOM()
{
   return false;
}
```

Se a função `runOnMOM` retornar `true` ou não for implementada, a calculadora JavaScript também será executada no MOM.

Por padrão, as calculadoras que retornarem false para essa função serão propagadas automaticamente para implantação em todos os coletores.

Para o APM 10.8, esse padrão pode ser substituído por `introscope.enterprisemanager.javascript.hotdeploy.collectors.enable= false`

Isso permite a implantação de diferentes conjuntos de calculadoras limitados em todos os coletores, quando usados com uma correspondência coordenada com a configuração de conexões permitidas de agentes para coletores no arquivo loadbalancing.xml para obter o efeito desejado de limitar execuções da calculadora, conforme a colocação da métrica.

Para o DX APM SaaS, esse controle não é possível, pois o balanceamento de carga é controlado de forma diferente e é agrupado internamente.

Reduzindo o número de erros de criação de métricas registradas

Quando uma calculadora é executada no MOM e cria uma métrica para um agente existente nos coletores, há um registro de uso único do evento no nível de AVISO.
Exemplo

```
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]
```

Os eventos subsequentes são registrados somente no nível de DEPURAÇÃO.

Desativar a atualização automática de coletores

Os ambientes agrupados são definidos automaticamente para propagar uma calculadora JavaScript adicionada, modificada ou excluída a todos os coletores. Se não desejar que as calculadoras sejam propagadas, entre em contato com o Suporte da Broadcom para desativar esse recurso.

Exemplo para criar uma calculadora de amostra

Este exemplo cria uma calculadora simples que recebe uma métrica que é uma contagem acumulada de rejeições (desde que o agente é iniciado) e produz o valor delta por intervalo de 15 segundos.

As primeiras quatro funções de contrato devem ser semelhantes a esta:

```
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; }
```

Ela deve ser executada nos coletores, pois deve produzir uma métrica com um caminho como o nome original e da métrica com o delta acrescentado “:Rejections Delta”. A função execute() é implementada conforme mostrado:

```
'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

- A variável savedValues está em uma variável global e é salva nas invocações de execução.
- A função dataIsAbsent() é usada para processamento de circuito curto posterior de uma entrada metricData quando é verdadeira, continuando com a próxima iteração.
- A metricAttribute é dividida nos dois pontos delimitadores para obter valores separados para o caminho da métrica e o nome da métrica. Isso é necessário porque, para um caminho de métrica vazio, nenhum delimitador de barra vertical deve ser usado na criação da métrica completa (ou você acabaria com "|:", o que é inválido).

Tipos de dado de métrica

O CA APM monitora o desempenho de aplicativos medindo o desempenho em vários pontos dos subsistemas e componentes do aplicativo. Os probes inseridos no código de bytes do componente do aplicativo relatam dados aos agentes, que, por sua vez, relatam os dados ao Introscope Enterprise Manager. Além disso, outros subsistemas, como JMX e PMI, relatam dados coletados por agentes. O Enterprise Manager compila esses dados em métricas e as exibe

no Workstation ou no WebView. Também é possível exportar as métricas para um banco de dados externo. Para obter informações adicionais, consulte as Métricas do APM.

Nas Calculadoras de JavaScript, todos os tipos de dado de métrica são mencionados acrescentando-se previamente o seguinte à frente do tipo de dado da métrica: `Packages.com.wily.introscope.spec.metric.MetricTypes` . Por exemplo, para usar `kIntegerFluctuatingCounter` , o nome completo seria `Packages.com.wily.introscope.spec.metric.MetricTypes.kIntegerFluctuatingCounter` .

Os tipos de dado de métrica são suportados pelo Agente do PHP, pelo Agente do Java, pelo Agente do .NET e pelo Agente do Node.js.

PerIntervalCounter:

kLongIntervalCounter - Um valor numérico de 64 bits que representa um valor de métrica por intervalo. Quando agregada em vários períodos, a soma é usada como o valor agregado. A contagem é o número de conclusões (ou seja, respostas ou erros) durante o intervalo e será igual ao valor.

Métricas de exemplo: respostas por intervalo, erros por intervalo

IntCounter/LongCounter:

kIntegerFluctuatingCounter/kLongFluctuatingCounter - Um valor numérico de 32/64 bits que flutua, mas permanece no último valor conhecido até que novos dados estejam disponíveis. Quando agregado em vários períodos, o valor mais alto é usado como o valor agregado. A contagem é o número total de incrementos e decrementos para o valor que ocorreu durante o intervalo.

Métricas de exemplo: contagem de paralisações, invocação simultânea (IntCounter); Bytes em uso (LongCounter)

IntAverage/LongAverage:

kIntegerDuration/kLongDuration - Um valor numérico de 32/64 bits que representa a duração. Quando agregada em vários períodos, a média ponderada é usada como o valor agregado. A contagem é o número de conclusões (por exemplo, respostas) durante o intervalo, que é usado como o denominador para calcular o valor (por exemplo, média).

Métrica de exemplo: Tempo médio de resposta (ms)

IntRate:

kIntegerRate - Um valor numérico de 32 bits que representa um contador por segundo. Para um intervalo de 15 segundos, o restante (14 ou menos) será truncado. Quando agregada em vários períodos, a média ponderada é usada como o valor agregado.

Métrica de exemplo: consultas por segundo

Marca de data e hora:

kLongTimestamp - Um valor de marca de data e hora que pode ser atualizado. O valor é inserido como o número de milissegundos desde Unix Epoch Time, 1º de janeiro de 1970 00:00:00 UTC. Não persistiu para o SmartStor.

StringEvent:

kStringIndividualEvents - Um valor de sequência de caracteres que pode ser atualizado. Não persistiu para o SmartStor.

Métrica de exemplo: Vazando no momento

IntConstant/LongConstant:

kIntegerConstant/kLongConstant - Um valor numérico de 32/64 bits que é inicializado, mas não é alterado.

Métrica de exemplo: ProcessID

IntPercentage:

kIntegerPercentage - Uma porcentagem do inteiro (sem decimal). Quando agregada em vários períodos, a média é usada como o valor agregado.

Métrica de exemplo: % de utilização (processo)

LongTimeStampConstant:

kLongTimestampConstant - Um valor de marca de data e hora que é inicializado, mas não é alterado. O valor é inserido como o número de milissegundos desde Unix Epoch Time, 1º de janeiro de 1970 00:00:00 UTC. Não persistiu para o SmartStor.

Métrica de exemplo: Hora da inicialização

StringConstant:

kStringConstant – Um valor de sequência de caracteres que é inicializado, mas não é alterado. Não persistiu para o SmartStor.

Métrica de exemplo: Máquina Virtual

Uma extensão do JavaScript permite que você crie uma nova extensão e edite uma extensão existente. Essa extensão lê métricas de entrada e produz métricas de saída de acordo com os cálculos especificados em um arquivo de texto JavaScript criado pelo usuário. As novas métricas calculadas podem ser exibidas na Árvore do investigador sob o Agente personalizado virtual. As métricas também podem ser exibidas em qualquer nó da Árvore do investigador, de acordo com a métrica de saída especificada no script de calculadora.

Para obter mais informações sobre como acessar e configurar extensões JavaScript, consulte Configurar as extensões do JavaScript.

Recomendações de dimensionamento do monitor do Docker

Para otimizar o desempenho do seu ambiente monitorado do Docker, você pode usar as seguintes recomendações de dimensionamento como referência. Estas recomendações são meramente indicativas, não podemos garantir que os exemplos sejam ideais para seu ambiente.

Recomendações de dimensionamento e métricas úteis

- **Alocação de recursos mínima recomendada para um recipiente do monitor do Docker**:
  - **Memória**: 650 MB
  - **CPU**: 0.3 para 25 recipientes. Consulte a tabela na parte inferior para obter uma diretriz quanto à alocação de recursos da CPU
- **Configuração recomendada para o intervalo de sondagem**: docker.interval.seconds=90

Normalmente, a utilização da CPU por um recipiente do monitor do Docker não é muito alta. Contudo, se a métrica **Percentual de utilização da CPU (mCore)** mostrar uma utilização da CPU acima de 80% por mais de uma hora, recomendamos aumentar a alocação de recursos da CPU. É recomendável aumentar a alocação em 0.2 a cada vez.

A métrica **CPU Throttling** é outro indicador que mostra que o monitor do Docker precisa aumentar a alocação de recursos da CPU.

Alocação de recursos mínima

Número de recipientes	Restrições da CPU	Memória (MB)
25	0.3	650
50	0.5	650
75	0.7	700
100	0.9	700

Fazer download de ferramentas adicionais

A opção **Downloads** permite fazer download e configurar ferramentas adicionais no ambiente de monitoramento. As seguintes ferramentas estão disponíveis para download em **Configurações**, bloco **Downloads**:

- **Estação de trabalho**: faça download da ferramenta Estação de trabalho para executar tarefas administrativas e acessar métricas de desempenho
- **Cloud Proxy**: faça download e configure o Cloud Proxy para Windows ou Linux. Você pode configurar o Cloud Proxy para enviar e receber dados coletados pelo agente diretamente para o gateway da nuvem.
- **Ferramenta Importação de agentes**: faça download da ferramenta Importação de agentes para criar um pacote do APM Command Center para agentes de versões anteriores do APM.

- Configurar a estação de trabalho
- Conectar a estação de trabalho
- Cloud Proxy
- Ferramenta Importação de agentes

A opção Downloads permite fazer download e configurar ferramentas adicionais no ambiente de monitoramento. Workstation, Cloud Proxy e Ferramenta Importação de agentes são as ferramentas disponíveis para download no bloco Configurações, Downloads.

Para obter mais informações sobre Downloads e as ferramentas disponíveis para download, consulte Fazer download de ferramentas adicionais.

Ferramenta Importação de agentes

A ferramenta Importação de agentes é um utilitário de linha de comando que permite migrar os agentes Java do CA APM 10.7 criados como um arquivo zip para os agentes Java mais recentes do DX APM.No processo de migração, para cada agente, um novo pacote do APM Command Center é criado com as alterações de configuração preservadas da versão mais antiga. As alterações que são preservadas incluem as alterações nos valores de propriedade e opções de alternância. O pacote resultante pode ser usado para implantar o agente como um substituto do agente antigo. A configuração do novo pacote já foi alterada para estabelecer conexão com a instância da nova geração do DX APM.

> **NOTE**
> Use essa ferramenta somente para pacotes do agente do Java 10.7 que não sejam programas de instalação. Essa ferramenta oferece suporte ao Windows e ao Linux.

Este artigo contém os seguintes tópicos:

Pré-requisitos

Open JDK 11.x ou Oracle JDK 11.x

Processo de migração

Quando você executa o utilitário, ele identifica arquivos e parâmetros usados pelo agente selecionado e cria um pacote do APM Command Center que inclui componentes que contêm os arquivos e a configuração correspondentes. Todas as atualizações manuais dos valores de propriedade ou das opções de alternância serão aplicadas em novos componentes se os valores forem diferentes dos valores padrão no arquivo de configuração do agente original.

O utilitário criará um novo componente personalizado se forem encontrados arquivos, opções de alternância ou parâmetros de configuração não identificados. Esse componente é incluído no pacote criado.

Após a migração, a configuração dos agentes pode ser gerenciada no APM Command Center.

> **NOTE**
> Para que um agente fique visível no APM Command Center, inclua o componente Controlador de agente na extensão do agente Java ou no Infrastructure Agent. O Controlador de agente deve ser implantado no mesmo host.

O utilitário é configurado para usar uma conexão direta com o componente Gateway de nuvem do DX APM. É possível reconfigurar o utilitário para usar o Cloud Proxy local, alterando a propriedade no arquivo de configuração **application.properties** ou usando o parâmetro de linha de comando.

Executar o utilitário Ferramenta Importação de agentes

Ao executar o utilitário Ferramenta Importação de agentes, é necessário definir apenas o caminho do sistema de arquivos para o diretório do agente no parâmetro de linha de comando. Outras opções de linha de comando estão disponíveis para modificação da forma como o utilitário é executado ou para seleção da configuração apropriada do agente.

Siga estas etapas:

1. Vá para DX APM Team Center, **Configurações**, **Downloads**.
2. Na seção **Ferramenta Importação de agentes**, clique em **Fazer download**.
   O seguinte arquivo é baixado: *apmservices.agentimport-<versão>.zip*
3. Extraia o conteúdo do arquivo zip.
   É possível ver o seguinte conteúdo:
   a. pasta **lib**
   b. arquivo **application.properties**
   c. arquivo de script do Windows **import-agent.cmd**
   d. arquivo de script do Linux **import-agent.sh**
4. (Opcional) Atualize as propriedades necessárias no arquivo **application.properties**.

   > **IMPORTANT**
   > Como o diretório do agente pode conter vários perfis de agente, é necessário especificar explicitamente o caminho correto. Por padrão, o *IntroscopeAgent.profile* é usado como o arquivo principal de configuração do agente. No entanto, se desejar usar outro arquivo de perfil, por exemplo, *noredef variant*, é possível usar o parâmetro de linha de comando *--profile*.
   > **NOTE**
   > O utilitário usa o token de segurança específico para o inquilino atual gerado quando ele foi baixado. Para usar outro token, gere um token de API pública no Team Center. Para obter mais informações sobre como gerar o token de segurança, consulte Gerar token de segurança. Depois que o token for gerado, substitua o valor no arquivo **application.properties** ou você pode especificá-lo como um parâmetro de linha de comando.
5. Com base no sistema operacional, execute o script de inicialização da ferramenta de linha de comando com o caminho para o diretório do agente que contém os agentes Java do CA APM 10.7.
   Por exemplo: `import-agent /opt/weblogic/wily`

NOTE
No Linux, atualize a permissão de arquivo e torne-a executável usando o comando `chmod +x import-agent.sh` .

O utilitário identifica o ambiente do agente, como o sistema operacional, a versão, o processo e todas as alterações de configuração, além de criar um pacote correspondente na instância do servidor de configuração do APM Command Center.

NOTE
O utilitário cria um pacote usando os componentes da versão mais recente disponível no APM Command Center.

Parâmetros de linha de comando

Ao extrair os arquivos do utilitário, você obtém scripts para os sistemas operacionais Linux e Windows:

- **Linux**: *import-agent.sh*
- **Windows**: *import-agent.cmd*

NOTE
No Linux, atualize a permissão de arquivo e torne-a executável usando o comando `chmod +x import-agent.sh` .

Quando você executa o script, o único parâmetro obrigatório é o caminho para o diretório de agentes do CA APM 10.7. Por exemplo, `/opt/weblogic/wily`

Opções adicionais de linha de comando

- `-a,--agentJar <arg>` - usa o caminho do arquivo jar do agente relacionado à raiz. Por padrão, o nome do arquivo é **Agent.jar**.
- `-f,--force <arg>` - ignora os erros e continua com a execução do comando. Isso desativa a otimização do pacote.
- `-n,--name <arg>` - nome que é prefixado para o pacote criado e o componente personalizado. Por padrão, o nome do pacote está no seguinte formato: *Imported agent - <plataforma> <processo>*
- `-p,--profile <arg>` - caminho do arquivo do perfil relacionado à raiz. Por padrão, o caminho do perfil é: *core/config/IntroscopeAgent.profile*
- `-t,--token <arg>` - valor do token de segurança da API pública
- `-u,--url <arg>` - URL base do proxy ou do gateway da nuvem

Os valores de URL e token são definidos no arquivo de configuração **application.properties**. No entanto, é possível substituir os valores usando os parâmetros de linha de comando, se necessário.Para obter mais informações sobre como gerar o token de segurança, consulte Gerar token de segurança.

NOTE
Se você estiver usando a JVM da IBM, substitua o valor padrão do arquivo jar do agente pelo arquivo *AgentNoRedefNoRetrans.jar*, pois ele é usado para conectar-se à JVM usando o parâmetro `--agentJar` .

Geração de logs

O utilitário fornece um log detalhado para rastrear como ele identifica componentes individuais e a configuração de propriedades. Ele também registra qualquer solicitação REST ao APM Command Center.

Para ativar o log de depuração, ative ou remova o comentário da seguinte propriedade no arquivo de configuração **application.properties**: `logging.level.com=DEBUG`

A ferramenta Importação de agentes é um utilitário de linha de comando que permite migrar os agentes Java do CA APM 10.7 criados como um arquivo zip para os agentes Java mais recentes do DX APM. No processo de migração, para cada

agente, um novo pacote do APM Command Center é criado com as alterações de configuração preservadas da versão mais antiga.

Para obter mais informações sobre os itens a seguir, consulte Ferramenta Importação de agentes.

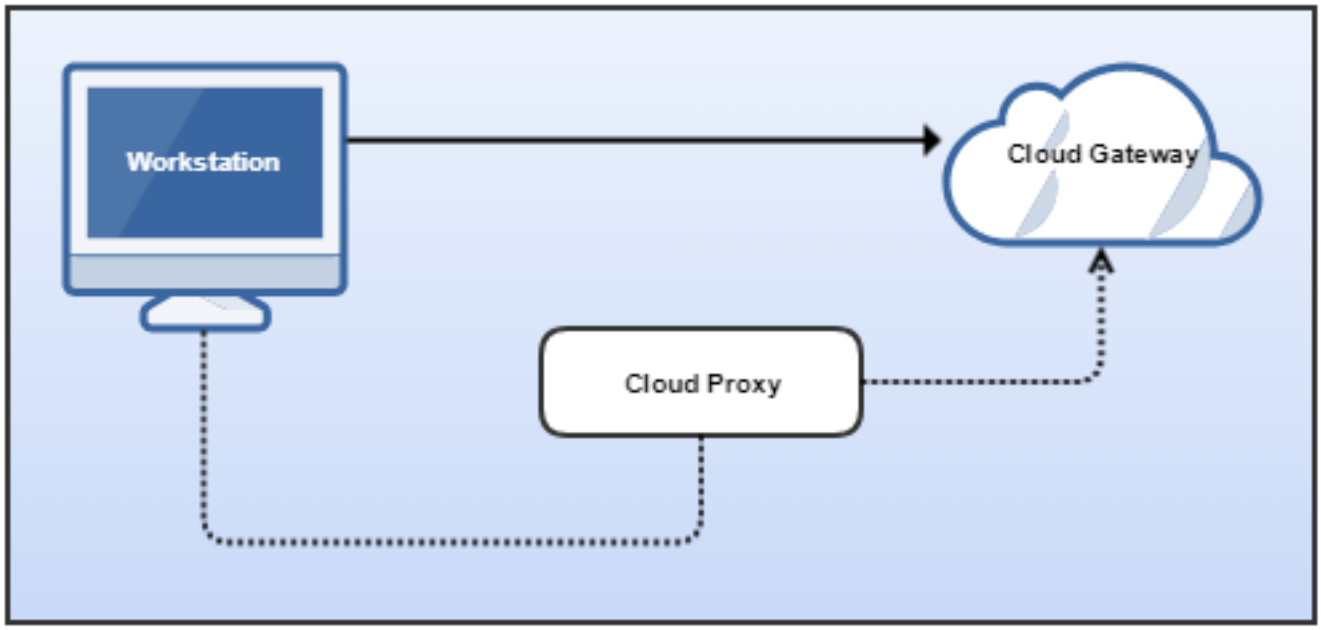
- Processo de migração
- Executar o utilitário Ferramenta Importação de agentes
- Parâmetros de linha de comando
- Geração de logs

Conectar o Workstation

O Workstation está disponível para download pela seção **Downloads**, no painel esquerdo. Por padrão, o Workstation está configurado para se comunicar diretamente com o gateway da nuvem.As organizações que requerem um único canal de comunicação entre o datacenter e o Cloud Gateway podem conectar o Workstation ao Cloud Proxy.

O seguinte diagrama demonstra estas duas opções:

Figure 3: ConnectWorkstation



Conectar a estação de trabalho ao gateway da nuvem

Pré-requisito:

Para executar o Workstation no Linux, certifique-se de que o Oracle ou o OpenJDK 11.x esteja instalado no computador.

> **NOTE**
> O protocolo **Isengard** não é suportado para o Cloud Gateway.

Siga estas etapas:

1. Em **Configurações**, **Downloads**, **Download the Workstation**. Descompacte o arquivo.
2. Inicie a estação de trabalho a partir da linha de comando:
   - `(Windows) start.bat`
   - `(Linux) start.sh`

A caixa de diálogo de conexão CA Introscope Workstation é exibida.

3. Insira sua **Senha**.
4. Selecione **Conectar**.
   O painel Workstation será exibido.

Você conectou o Workstation ao gateway da nuvem.

Conectar o Workstation ao Cloud Proxy

Pré-requisitos:

- Para executar o Workstation no Linux, certifique-se de que o Oracle 11.x ou o OpenJDK 11.x esteja instalado no computador.
- Para executar o Cloud Proxy, certifique-se de ter uma versão suportada do Java instalada no computador: OpenJDK 11.x ou Oracle JDK 11.x.

Siga estas etapas:

1. Configure o Cloud Proxy e verifique se ele está em execução.
   Para obter mais informações sobre como configurar o Cloud Proxy, consulte Configurar o Cloud Proxy.
2. Em **Configurações**, **Downloads**, **Download the Workstation**. Descompacte o arquivo.
3. Inicie a estação de trabalho a partir da linha de comando:
   - `(Windows) start.bat`
   - `(Linux) start.sh`

   A caixa de diálogo de conexão do DX APM Introscope Workstation é exibida.
4. Insira o URL do proxy como o valor do campo **URL da nuvem**. Defina o URL do proxy no seguinte formato:
   Por exemplo, `ws://<<cloudproxyhost>>:8081`

   TIP

   É recomendável usar um dos seguintes protocolos (com a opção de configuração correspondente e os valores padrão) para o Cloud Proxy a fim de se conectar à estação de trabalho:

   - **apm.server.httpPort**
     - WS 8081
   - **apm.server.secureHttpPort**
     - WSS 8444

   NOTE

   - O URL de destino do proxy é pré-configurado quando o recurso de download do Cloud Proxy é executado na GUI.
   - Use os protocolos Isengard e HTTP para estabelecer conexão com os agentes.
5. Insira sua **Senha**.
6. Selecione **Conectar**.
   O painel Workstation será exibido.

Você conectou o Workstation ao Cloud Proxy.

Reiniciar o Workstation

Ao terminar de usar o Workstation, você pode optar por efetuar logoff ou fechar o Workstation. O logoff do Workstation encerra a sessão atual, mas não a fecha. É possível efetuar logon novamente pela caixa de diálogo de conexão exibida por padrão quando se efetua logoff. Sair do Workstation o desconecta e interrompe o processo do Workstation. o Workstation salva o número de janelas abertas do investigador e do console, para que a mesma configuração seja exibida quando você efetuar logon novamente.

Siga estas etapas:

1. Abra o diretório em que a estação de trabalho foi extraída.
2. Inicie a estação de trabalho a partir da linha de comando:
   - `(Windows) start.bat`
   - `(Linux) start.sh`

   A caixa de diálogo de conexão do DX APM Introscope Workstation é exibida.
3. Preencha os campos obrigatórios.
4. Selecione **Conectar**.

Você reiniciou o Workstation.

NOTE

Mais informações:

- Visão geral da Estação de trabalho

O Workstation está disponível para download pela seção **Downloads**, no painel esquerdo. Por padrão, a estação de trabalho está configurada para se comunicar diretamente com o gateway da nuvem. As organizações que requerem um único canal de comunicação entre o datacenter e o Cloud Gateway podem conectar o Workstation ao Cloud Proxy.

Para obter mais informações, consulte Conectar o Workstation.

Cloud Proxy

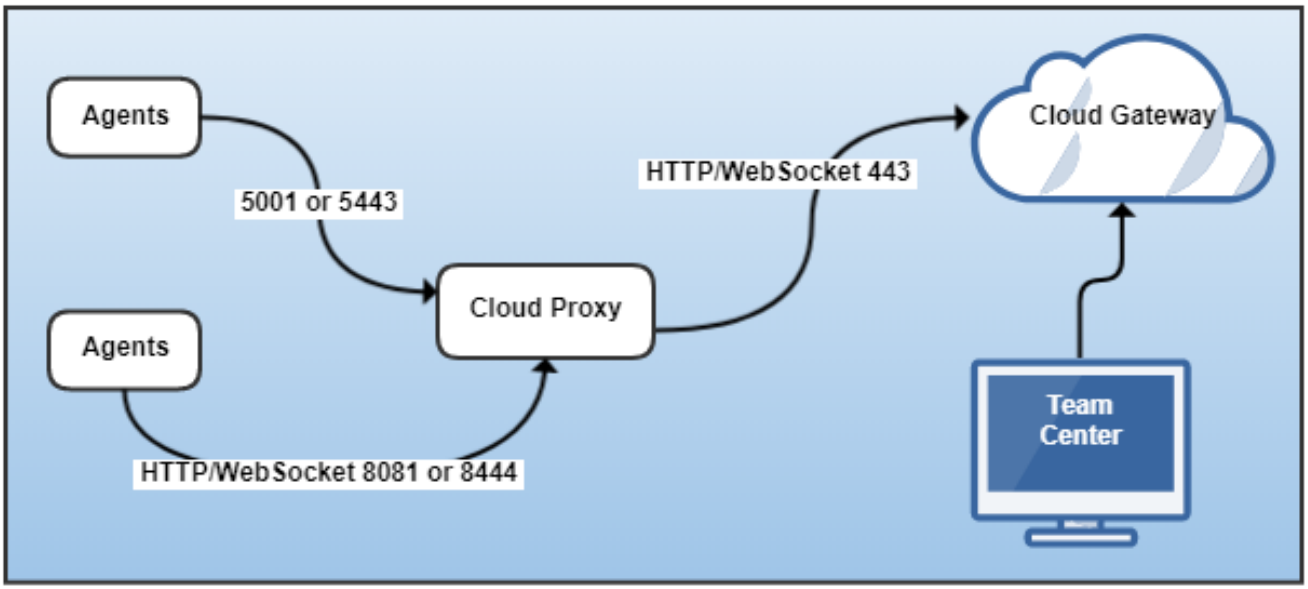
Como administrador, baixe e configure o Cloud Proxy para migrar todos os agentes atualmente conectados ao CA APM versão 9.6 e superior para o DX APM. Sua organização pode exigir comunicação de saída por proxy HTTP ou usar a comunicação a partir de um nó específico para configurar o firewall. Você pode usar o Cloud Proxy para realizar essas configurações. Você pode configurar o Cloud Proxy como independente ou executá-lo dentro de um recipiente do Docker.

NOTE

- Também é possível usar o Cloud Proxy para conectar a estação de trabalho. Para obter mais informações, consulte "Conectar a estação de trabalho" na documentação do APM.
- Não use o método padrão de criação de alertas do APM para métricas ingeridas diretamente no NASS (isso inclui as métricas de suportabilidade do Cloud Proxy do APM e qualquer métrica que não seja do APM). Em vez disso, use a configuração de alerta com base em métricas do DX OI.

Este diagrama mostra as portas disponíveis para o Cloud Proxy:

Figure 4: Cloud Proxy para gateway



Este artigo contém os seguintes tópicos:

- Configurar o Cloud Proxy
  - Configuração do serviço do Linux
  - Configuração do serviço do Windows
  - Configuração da HA (High Availability - Alta Disponibilidade)
- Conectar novos agentes ao Cloud Proxy
- Migrar agentes individuais para o DX APM usando o Cloud Proxy
- Geração de logs do Cloud Proxy
- Otimizar o desempenho da rede e da CPU
- Solução de problemas
- Métricas de integridade de conexão do Cloud Proxy
- Métricas de suportabilidade do Cloud Proxy

Configurar o Cloud Proxy

Apenas uma configuração inicial é necessária para o Cloud Proxy. Se você estiver migrando para de uma versão local do DX APM para o DX APM SaaS, a seguinte configuração executará a migração de todos os agentes atualmente conectados.

Pré-requisitos:

- Certifique-se de ter uma versão suportada do Java instalada no computador: OpenJDK 11.x ou Oracle JDK 11.x.
- Verifique se você tem uma versão do sistema operacional compatível instalada no computador: RHEL 7.6 e superior, CentOS 7.9 e superior ou Windows Server 2016 e superior.
- Para 4.000 agentes por Cloud Proxy, o tamanho recomendado é de 4 GB de memória heap. Portanto, se você quiser ter 10.000 agentes, é recomendável ter três Cloud Proxies.
- Aloque 6GBi de memória do sistema operacional para cerca de 4.000 agentes.

NOTE
6 GBi é uma recomendação de dimensionamento padrão, quando a JVM usa 4 GBi de memória heap.

- Certifique-se de que haja espaço em disco suficiente para armazenar os logs.
- No sistema operacional host, defina o valor do `número máximo de descritores de arquivos abertos` para um **processo** como 16384 ou superior.
- Para conectar 10k agentes por CloudProxy, a recomendação de dimensionamento padrão é 8GBi quando a JVM usar 6GBi da memória heap.
  No sistema operacional host, defina o máximo de descritores de arquivo aberto para um processo como 61440 ou superior.
- Para conectar 15k agentes por CloudProxy, a recomendação de dimensionamento padrão é 12GBi quando a JVM usar 8GBi da memória heap.
  No sistema operacional host, defina o máximo de descritores de arquivo aberto para um processo como 92160 ou superior.

Configuração do serviço do Linux

Siga estas etapas:

1. Na UI do ATC, clique no ícone Configurações
   ( ).
2. Em **Downloads**, faça download do Cloud Proxy no computador em que o MOM do Enterprise Manager estiver sendo executado. Extraia o arquivo.
   O token e o URL de destino do proxy são pré-configurados quando o recurso Download Cloud Proxy é executado na UI do ATC.

   NOTE

   Se necessário, você poderá substituir o token. Na UI do ATC, sob **Segurança**, selecione **Gerar outro token**. Verifique se o tipo de token é **Agente** e defina uma expiração apropriada, pois a expiração de um token do tipo **Agente** não poderá ser modificada posteriormente. Em seguida, na pasta de configuração, arquivo `application.yml` , insira a nova ID do token na propriedade `apm.server.token` .
3. (Opcional) No arquivo `application.yml` na pasta de configuração, essas propriedades estão definidas como padrão. Configure as propriedades para substituir as portas TCP padrão.
   - **`apm.server.port`**
     Padrão: 5001
   - **`apm.server.httpPort`**
     Padrão: 8081
   - **`apm.server.securePort`**
     Padrão: 5443
   - **`apm.server.secureHttpPort`**
     Padrão: 8444

NOTE

- Você pode configurar o Cloud Proxy com portas personalizadas, mas o próprio Enterprise Manager adiciona métricas de host e porta do Enterprise Manager. Portanto, não é possível defini-las a partir de nenhum agente.
- Internamente, o Cloud Proxy usa Isengard, e o servidor Isengard hospeda o apm.server.port. Portanto, a apm.server.port deve estar aberta para que os protocolos http/https possam ser encerrados no Cloud Proxy.
- Para Isengard, o ulimit deve ser definido para duas vezes o número de cada agente conectado. Por exemplo, para oferecer suporte a 8000 agentes, o valor recomendado seria 16000.
- Para conexões HTTP/HTTPS, o ulimit deve ser quatro vezes o número de agentes.

4. (Opcional) Para usar seu próprio certificado de segurança, acesse o arquivo `application.yml` na pasta de configuração. Configure estas propriedades:
   - **`apm.server.useSelfSignedCert`**
     Defina o valor como falso.
   - **`apm.server.keyCertChainFile`**
     Insira um caminho para um arquivo de certificado X.509 usando o formato PEM.
   - **`apm.server.keyFile`**
     Insira um caminho para um arquivo de chave privada PKCS#8 usando o formato PEM. O DX APM oferece suporte apenas ao formato PKCS#8.

     NOTE

     O Cloud Proxy usa um certificado autoassinado gerado por padrão. É altamente recomendável gerar um certificado confiável devidamente assinado. Os certificados autoassinados não devem ser usados em implantações de produção.
5. (Opcional) Para configurar um proxy HTTP para a comunicação entre o Cloud Proxy e o Cloud Gateway:
   a. Acesse o arquivo `application.yml` na pasta de configuração. Configure estas propriedades:
      - **`apm.server.httpProxy.host`**
        Insira o nome do host para o proxy HTTP.
      - **`apm.server.httpProxy.port`**
        Insira o número da porta do proxy HTTP.
   b. Se o proxy HTTP exigir autenticação, forneça um nome de usuário e uma senha válidos:
      - **`apm.server.httpProxy.username`**
        Insira um nome de usuário para acessar o proxy HTTP.
      - **`apm.server.httpProxy.password`**
        Insira uma senha para acessar o proxy HTTP.
6. (Opcional) Para impor a comunicação do TLS 1.3 entre o Cloud Proxy e o DX APM SaaS, configure o valor do parâmetro `apm.server.secureClientProtocol` para “TLSv1.3”.
7. Encerre o MOM do Gerenciador corporativo e todos os coletores.
8. Na linha de comando, insira o comando `apmservices.cloudproxy.sh start` para iniciar o Cloud Proxy.
   O script inicia o processo apmservices.cloudproxy em segundo plano.

   NOTE

   Para uso em produção, é altamente recomendável conectar o script ao sistema de gerenciamento de daemon da plataforma de destino. Por exemplo: init daemon, systemd ou upstart.
9. Verifique estes logs no diretório de logs para garantir que o Cloud Proxy tenha sido iniciado com êxito:
   - `logs/cloudproxy.log`
   - `logs/apmservices.cloudproxy.wrapper.log`

Você iniciou o Cloud Proxy para Linux. Se você tiver migrado os agentes com o Cloud Proxy, agora será possível exibir os agentes em **Configurações**, **Agentes** no Team Center.

> **NOTE**
> Estes argumentos estão disponíveis para uso com `apmservices.cloudproxy.sh:`

Argumento	F
start	Inicia o serviço em segundo plano
run	Inicia o serviço em primeiro plano
stop	Interrompe o serviço quando ele está em execução.
restart	Interrompe o serviço quando ele está em execução e inicia o serviço novan
status	Imprime o status em execução e interrompido do serviço
logs	Segue o log em `logs/cloudproxy.log`
version	Imprime a versão do serviço
install	Instala e inicia *apmservices-cloudproxy* como o serviço *systemd*.
uninstall	Interrompe e inicia o serviço *apmservices-cloudproxy systemd*.

Configuração do serviço do Windows

Siga estas etapas:

1. Em **Configurações**, **Downloads**, faça download do Cloud Proxy no computador em que o MOM do Enterprise Manager estiver sendo executado. Descompacte o arquivo.
   O token e o URL de destino do proxy são pré-configurados quando o recurso Download Cloud Proxy é executado na UI do ATC.

   > **NOTE**
   >
   > Se necessário, você poderá substituir o token. Na UI do ATC, sob **Segurança**, selecione **Gerar outro token**. Verifique se o tipo de token é **Agente** e defina uma expiração apropriada, pois a expiração de um token do tipo **Agente** não poderá ser modificada posteriormente. Em seguida, na pasta de configuração, arquivo `application.yml` , insira a nova ID do token na propriedade `apm.server.token` .
2. (Opcional) No arquivo `application.yml` na pasta de configuração, essas propriedades estão definidas como padrão. Configure as propriedades para sobrepor as portas TCP padrão.
   - **`apm.server.port`**
     Padrão: 5001
   - **`apm.server.httpPort`**
     Padrão: 8081
   - **`apm.server.securePort`**
     Padrão: 5443
   - **`apm.server.secureHttpPort`**
     Padrão: 8444

NOTE

- Você pode configurar o Cloud Proxy com portas personalizadas, mas o próprio Enterprise Manager adiciona métricas de host e porta do Enterprise Manager. Portanto, não é possível defini-las a partir de nenhum agente.
- Internamente, o Cloud Proxy usa Isengard, e o servidor Isengard hospeda o apm.server.port. Portanto, a apm.server.port deve estar aberta para que os protocolos http/https possam ser encerrados no Cloud Proxy.
- Para Isengard, o ulimit deve ser definido para duas vezes o número de cada agente conectado. Por exemplo, para oferecer suporte a 8000 agentes, o valor recomendado seria 16000.
- Para conexões HTTP/HTTPS, o ulimit deve ser quatro vezes o número de agentes.

3. (Opcional) Para usar seu próprio certificado de segurança, acesse o arquivo `application.yml` na pasta de configuração. Configure estas propriedades:
   - **`apm.server.useSelfSignedCert`**
     Defina o valor como falso.
   - **`apm.server.keyCertChainFile`**
     Insira um caminho para um arquivo de certificado X.509 usando o formato PEM.
   - **`apm.server.keyFile`**
     Insira um caminho para um arquivo de chave privada PKCS#8 usando o formato PEM. O DX APM oferece suporte apenas ao formato PKCS#8.

     NOTE

     O Cloud Proxy usa um certificado autoassinado gerado por padrão. É altamente recomendável gerar um certificado confiável devidamente assinado. Os certificados autoassinados não devem ser usados em implementações de produção.
4. (Opcional) Para configurar um proxy HTTP para a comunicação entre o Cloud Proxy e o Cloud Gateway:
   a. Acesse o arquivo `application.yml` na pasta de configuração. Configure estas propriedades:
      - **`apm.server.httpProxy.host`**
        Insira o nome do host para o proxy HTTP.
      - **`apm.server.httpProxy.port`**
        Insira o número da porta do proxy HTTP.
   b. Se o proxy HTTP exigir autenticação, forneça um nome de usuário e uma senha válidos:
      - **`apm.server.httpProxy.username`**
        Insira um nome de usuário para acessar o proxy HTTP.
      - **`apm.server.httpProxy.password`**
        Insira uma senha para acessar o proxy HTTP.
5. (Opcional) Para impor a comunicação do TLS 1.3 entre o Cloud Proxy e o DX APM SaaS, configure o valor do parâmetro `apm.server.secureClientProtocol` para “TLSv1.3”.
6. Encerre o MOM do Gerenciador corporativo e todos os coletores.
7. Encerre o MOM do Gerenciador corporativo e todos os coletores.
8. Instale o serviço do Windows. Execute a linha de comando como administrador e digite `apmservices.cloudproxy.exe install`
9. Inicie o Cloud Proxy. Execute a linha de comando como administrador e digite `apmservices.cloudproxy.exe start`
10. Verifique estes logs no diretório de logs para garantir que o Cloud Proxy tenha sido iniciado com êxito:
    - `logs/cloudproxy.log`
    - `logs/apmservices.cloudproxy.wrapper.log`

Você iniciou o Cloud Proxy para Windows. Se você tiver migrado os agentes com o Cloud Proxy, agora será possível exibir os agentes em **Configurações**, **Agentes** no Team Center.

Configuração do agente para Cloud Proxy

Se você estiver usando o certificado autoassinado, após gerá-lo, execute as seguintes etapas para que o agente se conecte ao EM:

Vá até a pasta em que você fez download do agente. Por exemplo, o introscopeAgent.profile para Tomcat pode ser encontrado em <wily\releases\2022.3\core\config>. Da mesma forma, para um Infrastructure Agent, o introscopeAgent.profile será <apmia\core\config>.

Copie o arquivo **.jks** do sistema Cloud Proxy para o sistema do agente. No **IntroscopeAgent.profile** no sistema do agente, forneça o caminho em que o arquivo **.jks** é copiado.

Por exemplo, *agentManager.trustStore.1=C:\\linux_cp_certs\\trust.jks.*

Forneça a senha na propriedade agentManager.trustStorePassword.1 do IntroscopeAgent.pofile.

Por exemplo, *agentManager.trustStorePassword.1=changeit.*

Configuração da HA (High Availability - Alta Disponibilidade)

O Cloud Proxy é um serviço independente em execução em um ambiente de sistema operacional do host do cliente. O gerenciador de serviços do sistema operacional ou um aplicativo de terceiros é necessário para garantir a disponibilidade da instância. O Cloud Proxy fornece um probe de atividade por meio de terminais HTTP e HTTPs em */supportability/health*. Um balanceador de carga pode ser colocado na frente dos Cloud Proxies do DX APM para atingir alta disponibilidade. O balanceador de carga garante que as reconexões do agente sejam roteadas para uma instância disponível. O balanceador de carga também equilibra o número de conexões entre as instâncias.

Requisitos para diferentes protocolos de transporte de agente para uma solução de balanceamento de carga de terceiros:

1. **Agentes que se conectam via transporte de protocolo HTTP/HTTPs** - o balanceador de carga deve garantir que as solicitações HTTP do agente sejam balanceadas para a instância do Cloud Proxy com base no cookie de sessão HTTP JSESSIONID. A instância do Cloud Proxy mantém um canal WebSocket para o gateway do APM associado à sessão HTTP do agente.
2. **Agentes que se conectam por meio do transporte de protocolo WebSocket** - O transporte WebSocket de agente cria uma conexão estável de soquete de TCP. A solução de terceiros deve oferecer suporte ao protocolo WebSocket.
3. **Agentes que se conectam por meio do protocolo Isengard** - O protocolo Isengard é transferido diretamente por meio de uma conexão de soquete de TCP. Um balanceador de carga de rede ou uma técnica semelhante pode ser usada para garantir a tolerância a falhas para uma instância disponível do Cloud Proxy.

Conectar novos agentes ao Cloud Proxy

Use o Cloud Proxy para direcionar os dados diretos que os agentes coletam no Cloud Gateway por meio de um único canal.

Siga estas etapas:

1. Configure o Cloud Proxy e verifique se ele está em execução.
   Para obter mais informações sobre como configurar o Cloud Proxy, consulte Configurar o Cloud Proxy.

   NOTE

   - Você não precisará configurar o Cloud Proxy toda vez que conectar um novo agente. É necessária apenas uma configuração inicial do Cloud Proxy.
   - Se a conexão do agente com o Cloud Proxy for por meio de ws/wss, certifique-se de que o agente também forneça a propriedade **agentManager.credential**.
2. Baixe e implante o agente.

Para obter mais informações sobre como fazer download do agente, consulte Configurar e fazer download de um pacote de agente.

a. Use o script de inicialização do agente para definir a propriedade do agente `agentManager.url.1` ou digite `-D` e um destes protocolos:
   - **WebSocket**
     `-DagentManager.url.1=ws://proxyhost:8081`
   - **WebSocket Secure**
     `-DagentManager.url.1=wss://proxyhost:8444`
b. Se o agente tiver uma extensão de controlador, especifique a propriedade de controlador `introscope.agent.acc.controller.configurationServer.url` ou digite `-D` e um destes protocolos:
   - **HTTP**
     `-Dintroscope.agent.acc.controller.configurationServer.url=http://proxyhost:8081`
   - **HTTPS**
     `-Dintroscope.agent.acc.controller.configurationServer.url=https://proxyhost:8444`
c. Inicie o agente do Java.
   O agente agora está conectado ao Cloud Proxy.

É possível exibir os agentes conectados clicando em **Configurações**, **Agentes**.

Migrar agentes individuais para o DX APM usando o Cloud Proxy

> **IMPORTANT**
> Execute este procedimento se desejar migrar agentes que estejam em execução no APM 10.7 e versões anteriores. Para o DX APM 11 e versões posteriores, o cluster executa automaticamente o balanceamento de carga.

Você pode configurar os detalhes do Cloud Proxy no arquivo *loadbalancing.xml* na sua instalação local do DX APM e permitir que agentes individuais migrem para o DX APM.

Adicione essa configuração para conectar agentes individuais ao DX APM por meio do Cloud Proxy.

```
<agent-collector name="SendToProxy">
    <agent-specifier>.*\|.*\|.*</agent-specifier>
    <include>
        <collector host="<cloud-proxy-host>" port="5001"/>
    </include>
</agent-collector>
```

> **NOTE**
> Para obter mais informações, consulte "Configurar loadbalancing.xml para agentes permitidos e não permitidos pelo Enterprise Manager" na documentação do APM.

Geração de logs do Cloud Proxy

Os logs do Cloud Proxy estão disponíveis no diretório de logs neste local: `logs/cloudproxy.log` .No entanto, é possível ativar mais configurações de log para exibir informações de log mais detalhadas.

> **IMPORTANT**
>
> Depois de atualizar os detalhes do registro em log, você deverá reiniciar o processo do Cloud Proxy.

Ativar o nível de geração de logs de DEBUG ou TRACE

> **IMPORTANT**
> O nível do registro em log TRACE fornece rastreamentos de transação a partir dos despejos de segmento de todos os pacotes que passam pela transmissão, tokens de informações de segurança confidenciais ou credenciais que são transferidas. Ative o registro em log no nível do TRACE somente quando exigido pelo Suporte da Broadcom ou quando uma solução de problemas aprofundada for necessária. Desative o registro em log no nível do TRACE após concluir os testes.

Opção 1: adicionar uma configuração de JVM

Nível de geração de logs DEBUG

Abra *apmservices.cloudproxy.bat/sh* e adicione a configuração de JVM:

```
-Dlogging.level.com.ca.apm.cloudproxy=DEBUG
```

Nível de geração de logs TRACE

Normalmente, o nível de log DEBUG fornece detalhes suficientes ao registrar em log a maioria das exceções de conexão. No entanto, quando você alterna para o nível de log TRACE, é preciso adicionar uma configuração de JVM extra: *SocketProxyWS* para diagnosticar os pacotes de conexão.

Abra *apmservices.cloudproxy.bat/sh* e adicione a configuração de JVM:

```
-Dlogging.level.com.ca.apm.cloudproxy=TRACE -Dlogging.level.SocketProxyWS=TRACE
```

Estas são as opções de rastreamento de nível baixo que podem ser usadas para depurar quaisquer problemas de entrada:

`-Dlogging.level.CloudProxyIsengard=TRACE` - rastreia a comunicação de entrada para todas as portas de comunicação internas do DX APM.

`-Dlogging.level.CloudProxyHTTP=TRACE` - rastreia toda a comunicação de entrada das portas HTTP.

Para depuração específica, use estas opções:

`-Dlogging.level.HTTPBinaryTunnel=TRACE` - Rastreia os dados do protocolo binário HTTP na entrada. Use a opção para depurar problemas com agentes que se conectam ao proxy usando o protocolo binário HTTP.

`-Dlogging.level.HTTPSoapTunnel=TRACE` - Rastreia os dados do protocolo Soap HTTP na entrada. Use a opção para depurar problemas com agentes que se conectam ao proxy usando o protocolo HTTP Soap (agentes legados).

`-Dlogging.level.WSTunnel=TRACE` - rastreia o protocolo WebSocket na entrada. Use a opção para depurar problemas com conexões WS.

`-Dlogging.level.AccHttpProxy=TRACE` - rastreia a comunicação do proxy HTTP do APM Command Center na entrada.

Opção 2: **adicionar uma propriedade oculta**

Abra o arquivo *./config/application.yml* e, em seguida, adicione a propriedade oculta:

```
logging.level.com.ca.apm.cloudproxy: DEBUG
```

OR

Abra o arquivo *./config/application.yml* e, em seguida, adicione a propriedade oculta:

```
logging.level.com.ca.apm.cloudproxy: TRACE
```

Atualizar o histórico e o tamanho do arquivo de log

Abra os arquivos *./config/application.yml* e adicione estas propriedades:

`logging.file.max-history: <número-de-dias>`

Por padrão, os arquivos de log são alternados quando atingem 10 MB. Os arquivos de log alternados serão retidos por 7 dias, a menos que você atualize o valor dessa configuração.

Exemplo: `logging.file.max-history: 14`

Neste exemplo, os arquivos de log são retidos por 14 dias.

`logging.file.total-size-cap:<size-in-bytes-including-units>`

Em que `logging.file.total-size-cap` se refere aos backups de log a serem armazenados, e é representado em termos do tamanho do arquivo (MB, GB).

Defina o tamanho total do arquivo de log. Quando o tamanho do arquivo exceder o limite, os backups serão excluídos. As unidades suportadas são: byte, kilobyte, megabyte, gigabyte e terabyte.

Exemplo: `logging.file.total-size-cap: 1GB`

Neste exemplo, quando o tamanho total do arquivo de log excede 1 GB, os backups são excluídos.

> **IMPORTANT**
> Por padrão, o tamanho máximo do arquivo de log é definido como 10 MB. Se desejar atualizar esse valor, você poderá usar esta propriedade:
> `logging.file.max-size`

Otimizar o desempenho da rede e da CPU

Use `apm.server.compressionLevel` no arquivo application.yml para configurar o nível de compactação para a comunicação do WebSocket entre o Cloud Proxy e o Gateway. Você pode definir qualquer valor de 0 a 9. Isso equilibra a quantidade de dados e o uso da CPU. Por exemplo,

```
apm.server.compressionLevel: 1
```

Estes são os valores aplicáveis:

- 6: valor padrão
- 1: para atingir a velocidade de rede constante do Cloud Proxy, mas isso pode aumentar ligeiramente o tráfego na rede.
- 9: use para obter a melhor compactação
- 0: sem compactação. É recomendável não usar esse valor, pois aumenta a quantidade de dados, e a melhoria da CPU é mínima.

> **NOTE**
> Reinicie o Cloud Proxy após cada alteração de configuração.

Diferenciar Cloud Proxies

Use `apm.server.proxyAgentNamePrefix` no arquivo `application.yml` para adicionar um prefixo ao nome do host do agente. Pode ser usado para distinguir mais Cloud Proxies. Esse recurso está disponível somente para a comunicação ws/wss com o Cloud Gateway definido por meio de `apm.server.proxyTarget` .

Solução de problemas

Sintoma:

A inicialização do Cloud Proxy apresenta falha e a seguinte mensagem de erro é exibida:

```
No provider succeeded to generate a self-signed certificate.
```

Solução:

A geração de certificado autoassinado não é suportada em ambientes de tempo de execução IBM J9. Os certificados devem ser gerados separadamente e fornecidos ao Cloud Proxy com as propriedades de configuração descritas anteriormente.

Sintoma:

O agente não é capaz de estabelecer conexão com o Cloud Gateway.

Solução:

Use o nome do host do Cloud Gateway fornecido ao definir as regras de saída do firewall. O uso de um endereço IP poderá causar uma interrupção inesperada da conexão se o endereço IP for alterado.

Sintoma:

O agente não pode se conectar ao DX APM e esta mensagem é exibida no arquivo de log `logs/cloudproxy.log` do Cloud Proxy:

```
java.net.SocketException: Too many open files
```

Solução:

No sistema operacional host, defina o valor do `número máximo de descritores de arquivos abertos` para um **processo** como 16384 ou superior. Consulte a documentação do sistema operacional para obter informações sobre como aumentar o limite de recursos do sistema por processo.

Sintoma:

O Cloud Proxy não consegue encaminhar a conexão do agente ou da estação de trabalho, e esta mensagem de erro é exibida:

```
sun.security.validator. ValidatorException: PKIX path building failed: sun.security.provider. certpath.
 SunCertPathBuilderException: unable to find valid certification path to requested target
```

Solução:

Os serviços do DX APM foram implantados com um certificado autoassinado ou inválido. Para permitir que o Cloud Proxy se conecte a esses sistemas, defina a configuração **apm.server.proxyInsecure** como *true* no arquivo *config/application.yml*, conforme mostrado no exemplo.

Exemplo: `apm.server.proxyInsecure: true`

> **NOTE**
> Confiar em certificados inválidos representa um sério risco à segurança. Use somente em casos justificados e desative imediatamente após um certificado válido ser implantado no balanceador de carga de front-end do DX APM Gateway.

Métricas de integridade do Cloud Proxy

Você pode monitorar a integridade de um Cloud Proxy usando as métricas de conexão. Para gerar as métricas, defina um valor de token de agente válido para o parâmetro de configuração `apm.server.token` . Esta seção também contém os detalhes relacionados às métricas de sustentabilidade relatadas pelo Cloud Proxy.

Configure um nome para as métricas do Cloud Proxy usando o parâmetro de configuração `apm.server.id` . Esse nome é exibido na árvore da métrica. Se você não configurar o valor para `apm.server.id` , o Cloud Proxy detectará o nome do host do computador (endereço IP) e o exibirá na árvore da métrica.

> **NOTE**
> Não use as métricas de sustentabilidade do Cloud Proxy para configurar alertas. Em vez disso, você pode usar a interface do usuário do DX Operational Intelligence SaaS para configurar os alertas. Consulte Configuração do alerta com base em métricas.

A tabela a seguir lista alguns nomes de métrica importantes para um Cloud Proxy.

Nome da métrica	Descrição
SuperDomain|apmservices|CloudProxy|PROXY_ID|Agents|Active Connections Count	O número de agentes conectados por meio do Cloud Proxy.
SuperDomain|apmservices|CloudProxy|PROXY_ID|Configuration| Agent HostName Prefix	O prefixo de HostName do agente. É exibido apenas quando o prefixo é configurado para um nome de host do agente.
SuperDomain|apmservices|CloudProxy|PROXY_ID|Beans	Você pode usar as propriedades do bean para uma investigação aprofundada.
SuperDomain|apmservices|CloudProxy|PROXY_ID|Resources	Exibe a utilização de recursos para o Cloud Proxy e o host.
SuperDomain|apmservices|CloudProxy|PROXY_ID|Resources| System|Uptime (ms)	Você pode usar isso para investigar a reinicialização do agente.

Como administrador, baixe e configure o Cloud Proxy para migrar todos os agentes atualmente conectados ao CA APM versão 9.6 e superior para o DX Application Performance Management. Sua organização pode exigir comunicação de saída por proxy HTTP ou usar a comunicação a partir de um nó específico para configurar o firewall. Você pode usar o Cloud Proxy para realizar essas configurações. Você pode configurar o Cloud Proxy como independente ou executá-lo dentro de um recipiente do Docker.

Para obter mais informações sobre como configurar, migrar, registrar em log e solucionar problemas específicos do Cloud Proxy, consulte Cloud Proxy.

Métricas de suportabilidade do Cloud Proxy

Esta página descreve as métricas de suportabilidade do Cloud Proxy.

> **NOTE**
> Veja a seguir os prefixos das métricas: "apmservices | CloudProxy | PROXY_HOSTNAME" ou "apmservices | CloudProxy | PROXY_ID".

Agentes

Nome da métrica	
Active Connections Count	Contagem de agentes conectados.
Closed per Interval	Contagem de conexões fechadas por intervalo.
Connections failed per Interval	A conexão não foi estabelecida.
Connections reset by peer per Interval	Indica que o servidor remoto ou o cliente fechou a conexão inesperadamente, balanceador de carga.
Connections timed out per Interval	A conexão não foi estabelecida no tempo especificado.
I/O exceptions per Interval	A contagem de exceções de E/S por intervalo.
Other exceptions per Interval	A contagem de outros problemas não especificados.
Writes failed per Interval	A contagem de operações de gravação com falha por intervalo.

Beans | SupportabilityManagerPoller

Métricas BlamePoint

Nome da métrica	
Tempo médio de resposta (ms)	A métrica Tempo médio de resposta calcula a média dos tempos de resposta leva para ser concluída.
Tempo médio de resposta (µs)	
Concurrent Invocations	As invocações são solicitações tratadas pelo aplicativo e suas várias partes.
Erros por intervalo	Os erros são o número de exceções que a JVM relata.
Respostas por intervalo	Reflete o número de invocações concluídas nesse intervalo. Essa métrica é u contagem simples de solicitações que são concluídas durante um intervalo.
Contagem de paralisações	As solicitações paralisadas são as não concluídas dentro de um limite de tem paralisada quando sua execução excede o limite de paralisação.
Total de métricas	Contagem de métricas relatadas pelo Cloud Proxy.

Recursos | Pool do buffer

A opção Recursos | Pool do buffer fornece métricas de monitoramento para os buffers diretos alocados fora da memória heap.

Nome da métrica	
Buffer Count	Contagem de buffers nos pools de buffer do Java (buffers diretos, entre outro
Buffer Total Capacity	A capacidade total de todos os buffers.
Buffer Memory Used	A quantidade total de memória usada por todos os buffers.

Recursos | CPU

Nome da métrica	
CPU Used (%)	A soma do uso total da CPU em % para núcleos individuais. Pode ser mais
CPU Used (ms)	A soma do uso total da CPU por núcleos individuais em ms por intervalo.
Kernel CPU (%)	A soma do uso da CPU em % gasto no kernel (tempo do sistema).
Kernel CPU (ms)	A soma do uso da CPU gasto no kernel (tempo do sistema) em ms por inter
User CPU (%)	A soma do uso da CPU em % gasto no espaço do usuário.

Recursos | Host | CPU

Nome da métrica	
CPU Used (%)	A soma do uso total da CPU em % para núcleos individuais. Pode ser mais
CPU Used (ms)	A soma do uso total da CPU por núcleos individuais em ms por intervalo.
Idle CPU (%)	Por quanto tempo a CPU não ficou ocupada.
Idle CPU (ms)	
Kernel CPU (%)	A soma do uso da CPU em % gasto no kernel (tempo do sistema).
Kernel CPU (ms)	A soma do uso da CPU gasto no kernel (tempo do sistema) em ms por inter

Nome da métrica	
Wait CPU (%)	A soma do uso da CPU em % gasto no espaço do usuário.
Wait CPU (ms)	A quantidade de tempo que a CPU aguarda para, por exemplo, que as oper solicitações de E/S pendentes, embora isso talvez não afete a integridade c

Recursos | Host | Memória

Essas métricas são usadas para monitorar a memória do host.

Nome da métrica	
Memory Available (byte)	A quantidade de memória disponível para alocação para um novo process
Memory Total (byte)	Total de memória física no host.
Memory Usage (%)	A memória usada atualmente por processos em execução.

Recursos | Memória

As métricas de Recursos | Memória monitoram a memória que é usada pelo processo da JVM.

Nome da métrica	
GC Count	O número de coletas de lixo da JVM executadas por intervalo.
GC Time (ms)	A duração acumulada de pausas para coleta de lixo por intervalo. Se o te será significativamente afetado.
Memory Heap Committed	A quantidade de memória garantida para estar disponível para uso pela J
Memory Heap Max	A quantidade máxima de memória que pode ser usada para o gerenciam APM_HEAP_XMXMAX em Dimensionamento de armazenamento de dad
Memory Heap Used	A quantidade real de memória usada pela memória heap.
Memory Resident (byte)	A quantidade de memória ocupada pelo processo.
Memory Virtual (byte)	O tamanho da memória virtual do processo.
Memory No Heap Committed	A memória máxima garantida para estar disponível para que a JVM arma
Memory No Heap Max	A memória máxima da JVM usada para armazenar classes carregadas, c
Memory No Heap Used	A memória real da JVM usada para armazenar classes carregadas, códig

Recursos | Armazenamento

Nome da métrica	
Disk Read (byte)	Bytes lidos no disco por intervalo.
Disk Write (byte)	Bytes gravados no disco por intervalo.

Recursos | Sistema

Nome da métrica	
Harvest Cycle Duration (ms)	A duração do período de coleta das métricas de suportabilidade.
Uptime (ms)	O número de milissegundos desde o início da instância.

Configurar a estação de trabalho

Como administrador, você pode configurar as seguintes opções de estação de trabalho:

Executar a estação de trabalho no modo detalhado

Execute a estação de trabalho no modo detalhado para criar mensagens detalhadas de log, que são úteis para depuração ou solução de problemas.

Siga estas etapas:

1. Abra o arquivo IntroscopeWorkstation.properties em *<pasta_principal_da_estação_de_trabalho>*/config.
2. Na propriedade *log4j.logger.Workstation*, substitua *"INFO"* pela seguinte instrução:
   ```
   VERBOSE#com.wily.util.feedback.Log4JSeverityLevel
   ```
3. Salve as alterações.

Redirecionar a saída da estação de trabalho para um arquivo

Defina o arquivo IntroscopeWorkstation.properties para redirecionar as mensagens detalhadas de saída para um arquivo de log.

Siga estas etapas:

1. Abra o arquivo IntroscopeWorkstation.properties no diretório *<pasta_principal_da_estação_de_trabalho>*/config.
2. Na propriedade *log4j.logger.Workstation*, substitua *"console"* por *"logfile".* Por exemplo, esta configuração da propriedade faz com que a estação de trabalho registre mensagens detalhadas em um arquivo de log:
   ```
   log4j.logger.Workstation=VERBOSE#com.wily.util.feedback.Log4JSeverityLevel,logfile
   ```
3. (Opcional) Altere o nome e o local do arquivo de log da estação de trabalho usando a propriedade *log4j.appender.logfile.File.*

Configurar a estação de trabalho para fornecer dados de logon

É possível modificar o arquivo Introscope_Workstation.lax para fornecer dados de logon e ignorar a tela de logon.

Siga estas etapas:

1. Abra o arquivo *<pasta_principal_do_EM>/*Introscope_Workstation.lax.
2. Na propriedade *lax.command.line.args*, adicione os comandos de *-login* para cada comando de logon ao qual um valor deve ser fornecido. Por exemplo, para autenticação local, essa propriedade é semelhante à seguinte instrução:
   ```
   lax.command.line.args=$CMD_LINE_ARGUMENTS$ -loginimmediate
   -loginhost foos -loginport 4503 -loginresponse sanderson,45tst87
   ```

   WARNING
   Não exclua o valor padrão *$CMD_LINE_ARGUMENTS$* da configuração.

Você efetuou logon na estação de trabalho e um console é aberto.Se o logon apresentar falha, a estação de trabalho não é iniciada, e uma mensagem de erro é registrada no log.

Ativar expiração de sessão na estação de trabalho

A expiração automática de sessão adiciona um nível extra de segurança, pois desconecta usuários inativos. Modifique o arquivo IntroscopeEnterpriseManager.properties para ativar a expiração automática de sessão.

Siga estas etapas:

1. Abra o arquivo *<pasta_principal_do_EM>/config/*IntroscopeEnterpriseManager.properties.

2. Adicione a propriedade *introscope.apmserver.ui.inactivityLogoutTimeout* e defina o valor (em minutos) como um número inteiro maior que 0 para ativar a expiração de sessão. Por exemplo, a seguinte instrução permite a expiração após 60 minutos:

```
introscope.apmserver.ui.inactivityLogoutTimeout=60
```

NOTE
A expiração de sessão vem desativada por padrão (valor=0).

Configurar a estação de trabalho para relatórios em idiomas asiáticos

Adicione os componentes abaixo à instalação da sua estação de trabalho para gerar relatórios do Introscope em idiomas que usam conjuntos de caracteres multibyte, como chinês e japonês.

Gerar relatórios em idiomas asiáticos nos formatos RTF e HTML

(Windows) Instale o Suporte a idioma complementar para idiomas do leste asiático. Para obter mais informações sobre o suporte a idiomas, consulte https://msdn.microsoft.com/en-us/goglobal/default.

Gerar relatórios em idiomas asiáticos nos formatos PDF

Siga estas etapas:

1. Faça download do pacote de fontes asiáticas do Acrobat Reader em http://www.adobe.com/support/downloads/product.jsp?platform=windows&product=10
2. Instale o pacote de fontes asiáticas do Acrobat Reader.

Configurar a estação de trabalho para usar o proxy HTTP com autenticação

Use transport.http.proxy.username e transport.http.proxy.password para especificar os valores de autenticação em que transport.http.proxy.password deve ser criptografado. Para criptografar a senha, faça o seguinte.

Siga estas etapas:

1. Abra o arquivo IntroscopeWorkstation.properties em *<pasta_principal_da_estação_de_trabalho>*/config.
2. Na propriedade *transport.http.proxy.password*, forneça a senha criptografada.
   Você pode executar o seguinte comando para criptografar a senha:
   ```
   java -cp plugins\com.wily.core_<VERSION>.jar com.wily.util.properties.PropertiesUtils encrypt <PASSWORD>
   ```
   Em que <VERSION> é a versão instalada do APM na estação de trabalho e <PASSWORD> é a senha não criptografada.
3. Salve as alterações.

Como administrador, você pode configurar as seguintes opções de estação de trabalho:

- Executar a estação de trabalho no modo detalhado
- Redirecionar a saída da estação de trabalho para um arquivo
- Configurar a estação de trabalho para fornecer dados de logon
- Ativar expiração de sessão na estação de trabalho
- Configurar a estação de trabalho para relatórios em idiomas asiáticos
- Configurar a estação de trabalho para usar o proxy HTTP com autenticação

Para obter mais informações sobre cada opção configurável da estação de trabalho, consulte Configurar a estação de trabalho.

Regras de supressão de rastreamento para ocultar dados confidenciais

Os agentes em execução em ambientes de usuários enviam vários tipos de dados, incluindo dados de rastreamento. Esses dados de rastreamento podem conter informações confidenciais/pessoais/confidenciais que o usuário precisa mascarar. É possível definir regras de supressão de rastreamento para identificar esses dados dos usuários e substituí-los por um texto pré-configurado, como SUPRIMIDO PELO APM. Para cada inquilino, é possível adicionar várias regras para todos os atributos para os quais você deseja suprimir o valor do rastreamento.

Os agentes em execução em ambientes de usuários enviam vários tipos de dados, incluindo dados de rastreamento. Esses dados de rastreamento podem conter informações confidenciais/pessoais/confidenciais que o usuário precisa mascarar. É possível definir regras de supressão de rastreamento para identificar esses dados dos usuários e substituí-los por um texto pré-configurado, como SUPRIMIDO PELO APM.

Para configurar uma regra de supressão de dados de rastreamento, consulte Regras de supressão de rastreamento para ocultar dados confidenciais.

Configurar uma regra de supressão de dados de rastreamento

1. Efetue logon no Team Center e clique em **Configurações**, bloco **Segurança**.
2. Clique em **Trace Suppression Rule**.

   A janela **Trace Suppression Rule** será exibida. Esta janela exibe todas as regras configuradas no momento.
3. Clique no botão **Trace Suppression Rule**.

   A caixa de diálogo **Edit Trace Suppression** será exibida.
4. Especifique o seguinte:
   - **Nome**: digite um nome para a regra de supressão de rastreamento.
   - **Descrição**: forneça uma descrição relevante da regra a ser configurada.
   - **Configurar**
     - **Propriedades suprimidas**: digite o atributo para o qual será ocultado o valor de rastreamento no APM. Por exemplo, `FullUrl` . Você pode usar o ícone de adição para adicionar vários atributos.
     - **Expressão regular**: se desejar selecionar vários agentes com nomes semelhantes, use * como um caractere curinga com as mesmas iniciais dos agentes. Por exemplo, para selecionar todos os agentes com nomes que começam com tas-uk, digite `tas-uk.*` . Todos os agentes que atenderem aos critérios serão exibidos na lista **Visualização**.
     - **Agentes individuais**: selecione todos os agentes nessa lista para os quais você deseja suprimir o valor de rastreamento. Todos os agentes selecionados são exibidos na lista **Visualização**.

     Por exemplo, a opção **Propriedades suprimidas** está definida como `FullUrl` e `tas-uk.*` está configurada na **Expressão regular**.Nos dados de rastreamento de todos os agentes cujo nome comece com tas-uk.*, sempre que o valor do atributo FullUrl for exibido, ele será exibido como SUPRIMIDO PELO APM.
5. Para salvar a regra, selecione **Salvar**.

   A regra nova será exibida na lista de regras da janela **Trace Suppression Rule**.

Configurar o APM Command Center

Com o APM Command Center, é possível:

- Exibir as propriedades do agente armazenadas localmente selecionando um agente na lista. Cada agente é verificado, e suas propriedades são atualizadas em intervalos de 24 horas (sinal de monitoramento). Consulte Exibir status do agente.
- Obtenha informações mais detalhadas sobre um determinado agente gerando um relatório. Os relatórios de diagnóstico fornecem detalhes completos sobre um agente. Você pode percorrer as propriedades detalhadas do agente ou fazer o download de um arquivo ZIP que contenha todos os detalhes, incluindo os arquivos de log e de configuração. Você pode usar esse arquivo ZIP ao se referir a esse agente específico. Consulte Exibir relatórios do agente.
- Exibe os aplicativos criados no DX Application Performance Management. Você pode usar esses aplicativos para integrar os aplicativos no DX APM de maneira ininterrupta e para configurar facilmente os pacotes de agentes para o seu ambiente. Consulte Configurar os aplicativos para integração.
- Permite que você crie e implemente pacotes de agente do APM Command Center em servidores de aplicativos. Pacotes de agente são um conjunto implantável de arquivos de configuração e binários do agente em formato ZIP ou TAR. Cada pacote engloba vários componentes. Um *componente* é uma parte compacta da funcionalidade do agente. Consulte Gerenciar pacotes de agentes.
- Os componentes são subconjuntos da funcionalidade de monitoramento de agente. Requisitos de compatibilidade, dependências e inter-relacionamentos são definidos para cada componente e determinam suas possíveis combinações. Para alterar a configuração do agente, modifique as propriedades do componente em um pacote de agentes existente. Consulte Configurar componentes.

API RESTful

Para a interação automatizada com o DX APM Command Center, é possível usar a API RESTful. Consulte API do APM Command Center para obter detalhes.

Exibir status do agente

A página Agentes lista todos os agentes do ambiente. Usando o botão de download, é possível baixar a lista de agentes no formato CSV. O ícone correspondente ao nome do agente fornece o status atual do agente.

- Ativo : o agente responde dentro do intervalo do sinal de monitoramento de 24 horas do agente do controlador.
- Ativo : a configuração do agente foi modificada recentemente, e o agente deve ser reiniciado para que as alterações entrem em vigor.
- Inativo : os agentes da versão 10.2 e versões posteriores se comunicam com o Controlador de agente a cada 60 segundos. Se um agente parar de relatar, ele será marcado como Inativo.
- Fora : o agente não respondeu por mais de 24 horas. Se esse não for o comportamento esperado, verifique se o agente está em execução.

  NOTE

  - Um agente inativo é removido da lista após sete dias.
  - Os dados não são dinâmicos. O aplicativo mostra os dados que eram válidos no momento do último contato regular com o agente. Para versões anteriores dos agentes, os dados ser de até 24 horas atrás.
  - Você pode pesquisar um agente específico usando a barra de pesquisa. Para obter mais informações, consulte Pesquisar um agente

Informações do agente

A seleção de um agente na lista fornece as seguintes informações sobre ele:

- Informações do agente
- Ambiente
- Configuração
- Relatórios de diagnóstico

Ambiente

As informações sobre o ambiente incluem o seguinte:

- JVM
- Versão da JVM
- Servidor de aplicativos
- Versão do servidor de aplicativos
- Tipo de sistema operacional
- Versão do sistema operacional

Configuração

As informações de configuração incluem o seguinte:

- Nome
- Última modificação
- Versão do pacote

Você também pode editar a configuração, editar um pacote ou revelar a configuração do pacote, se disponível.

Para editar a configuração de um agente, selecione o agente e, em seguida, selecione o botão **Editar** no cartão **Configuração**. (ADICIONAR UM LINK À SEÇÃO)

Relatórios de diagnóstico

Você pode gerar o relatório de diagnóstico para um agente selecionando o botão **Gerar** no cartão Relatórios de diagnóstico. Depois que o relatório for gerado, você poderá exibi-lo ou baixá-lo na página Relatórios.

Pesquisar agentes

Para encontrar agentes, use a barra de pesquisa na parte superior da página ACC. Você pode pesquisar pela propriedade do agente, como nome, status, sistema operacional ou outro. Você também pode executar uma pesquisa global na Página inicial.

Para pesquisar agentes usando a AQL (ACC Query Language), consulte Pesquisar usando a AQL (ACC Query Language).

Veja a seguir exemplos de pesquisas de agente:

- appServerName:Tomcat
- Pesquise uma frase usando aspas duplas e caracteres curinga.
  ```
  *"Windows Server 2016"*
  ```
- Use os operadores E (padrão), OU e NÂO.
  ```
  logLevel:info OR logLevel:debug
  ```
- Pesquise os agentes do Tomcat, mas somente aqueles que não tiverem "linux" no nome do servidor:

```
processName:Tomcat NOT serverName:linux
```

- Pesquise os agentes cujos valores de campo estejam entre os limites inferior e superior especificados. Use datas exatas ou um período para um intervalo de tempo, como semanas (w), dias (d), horas (h), minutos (m) e segundos (s).

```
lastContact:[-5w TO NOW]
```

- Use parênteses para agrupar operadores lógicos

```
(osName:windows OR osName:Linux) AND logLevel:info
```

- Coloque as pesquisas de RegEx entre barras "/".

  TIP
  Você pode copiar e colar expressões de pesquisa do agente a partir de métricas do WebView.

```
/ACCServer.*01\|Tomcat\|.*Agent/
```

Salvando a pesquisa

Na barra de pesquisa, use a opção **Salvar como novo conjunto** para salvar um padrão de pesquisa que você usa com frequência. Também é possível usar a pesquisa salva em uma consulta.

Exemplo: usando a coleta em uma consulta

```
collection:"Tomcat Agents" AND reportName:Linux
```

Propriedades de pesquisa do agente

A propriedade padrão para pesquisa do agente é "spaName". Ela contém o nome do servidor, o nome do processo e o nome do agente separados pelo caractere "|".

Para pesquisar várias propriedades, use a propriedade "all", que inclui as seguintes propriedades do agente:

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.

Exibir relatórios do agente

Todos os relatórios gerados para os agentes são exibidos na página Relatórios como uma lista. Você pode selecionar um relatório para exibir os detalhes dos relatórios. Por padrão, os relatórios ficam disponíveis por 40 dias.

Você também pode selecionar um relatório e clicar no botão Fazer download para fazer o download como um arquivo ZIP. Um arquivo ZIP contém o relatório completo no formato HTML com todas as informações que você pode exibir na descrição do relatório. O arquivo ZIP inclui também todos os arquivos de configuração e de log. O nome do arquivo ZIP contém o nome do relatório e uma marca de data e hora para facilitar a identificação.

Você pode usar a barra de pesquisa na parte superior da página para pesquisar um relatório. Você pode pesquisar qualquer propriedade do relatório. Você também pode executar uma pesquisa global na Página inicial.

Pesquisar relatórios

Você pode usar a barra de pesquisa na parte superior da página para pesquisar um relatório. Você pode pesquisar qualquer propriedade do relatório. Você também pode executar uma pesquisa global na Página inicial.

Para pesquisar relatórios usando a AQL (ACC Query Language), consulte Pesquisar usando a AQL (ACC Query Language).

Veja a seguir exemplos de pesquisas de relatório:

- Pesquise por nome de relatório. Use aspas para incluir espaço.

```
reportName:"ACCDemoWin01|Tomcat|Tomcat Agent-3"
```

- Você pode usar os operadores E (padrão), OU e NÃO.

  ```
  logLevel:info OR logLevel:debug
  ```

- Pesquise os relatórios dos agentes do Tomcat, mas somente aqueles que não tiverem "linux" no nome do servidor.

  ```
  processName:Tomcat NOT serverName:linux
  ```

- Pesquise de acordo com o último contato (de 5 semanas atrás até agora):

  ```
  lastContact:[-5w TO NOW]
  ```

- Use parênteses para agrupar operadores lógicos

  ```
  (osName:windows OR osName:Linux) AND logLevel:info
  ```

  Coloque as pesquisas de RegEx entre barras "/".

  > **TIP**
  > Você pode copiar e colar expressões de pesquisa do agente a partir de métricas do WebView.

  ```
  /ACCServer.*01\|Tomcat\|.*Agent/
  ```

Salvando a pesquisa

Na barra de pesquisa, use a opção **Salvar como novo conjunto** para salvar um padrão de pesquisa que você usa com frequência. Também é possível usar a pesquisa salva em uma consulta.

Exemplo: usando a coleta em uma consulta

```
collection:"Tomcat Agents" AND reportName:Linux
```

Propriedades de pesquisa do agente

A propriedade padrão para pesquisa do agente é "spaName". Ela contém o nome do servidor, o nome do processo e o nome do agente separados pelo caractere "|".

Para pesquisar várias propriedades, use a propriedade "all", que inclui as seguintes propriedades do agente:

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.

Configurar os aplicativos para integração

A página Aplicativos exibe todos os aplicativos criados no DX Application Performance Management. Use esses aplicativos para integrar os aplicativos no DX APM de maneira ininterrupta e para configurar facilmente os pacotes de agentes para o seu ambiente.

A Integração de aplicativo contém os seguintes conceitos:

- **Aplicativo:** permite monitorar o aplicativo, que consiste em uma ou mais camadas.
- **Camada:** denota uma camada específica do aplicativo a ser monitorada. A camada faz referência a um ou mais pacotes de agentes criados com base na seleção de um usuário.

Para criar um aplicativo para integração, consulte Criar aplicativos.

Pesquisar aplicativos

Você pode usar a barra de pesquisa na parte superior da página para pesquisar um aplicativo usando apenas o campo de nome. Como o campo de nome é a opção de pesquisa padrão, você pode ignorar a anexação de "nome:" no campo de pesquisa.

Para pesquisar aplicativos usando a AQL (ACC Query Language), consulte Pesquisar usando a AQL (ACC Query Language).

Veja a seguir exemplos de pesquisas de aplicativo:

- Para pesquisar um aplicativo com o nome de Site

  ```
  name:website
  ```

  Ou

  ```
  website
  ```

- Você pode usar os operadores E (padrão), OU e NÃO.

  ```
  name:website AND NOT name:testing
  ```

  Ou

  ```
  website AND NOT name:testing
  ```

Gerenciar pacotes de agentes

Um pacote é uma imagem do agente que pode ser implantada, juntamente com as instruções de instalação, no formato ZIP ou TAR. O pacote é criado a partir de componentes que representam uma parte da funcionalidade do agente. O Command Center também fornece pacotes de inicialização do Java. O pacote de inicialização permite alternar entre diferentes versões do agente com o mínimo esforço. Para transferir definições de pacote entre inquilinos diferentes, use a funcionalidade de exportação/importação.

Na guia Pacote, uma lista de pacotes disponíveis é exibida. Um ícone ao lado do nome do pacote indica que uma atualização está disponível. Selecione esse pacote e clique em Atualizar para atualizar o pacote.

Você pode fazer o seguinte usando a página Pacotes:

- Criar um pacote de agentes
- Usar um componente de um pacote
- Implantar os pacotes de agentes
- Integração de terceiros
- Gerenciar pacotes e componentes de agentes usando o APM Command Center

A página Pacote exibe as seguintes informações sobre um pacote.

Package

O cartão Pacote exibe informações gerais sobre o pacote, como nome, descrição e total de agentes.

O **Total de agentes** mostra quantos agentes usam esse pacote. Você pode acessar a guia **Agentes** e ver os agentes que usam esse pacote.

Versão do pacote

O cartão **Versões** exibe o número de agentes que usam cada versão do pacote. Você pode ver quando o pacote foi modificado pela última vez, o nome do pacote, a versão do pacote e do agente e se o pacote foi arquivado. Essa visão geral ajuda a garantir que todos os agentes usem a versão mais recente.

> **NOTE**
> Você não pode fazer download de um pacote arquivado. Você também não pode fazer nenhuma alteração de configuração no pacote arquivado. Quando você cria outra versão do pacote, ela se baseia na versão atual (não arquivada).

Versões

O cartão de versão exibe as informações sobre cada atualização do pacote e o usuário que o atualizou.

Quando um pacote é criado, seu número de versão inicial é 1. Após edições subsequentes, a Versão do agente permanecerá 1 até que um usuário baixe o pacote ou aplique-o ao agente. A próxima edição alterará o número da versão para 2.

Componentes

O cartão Componentes exibe todos os componentes incluídos no pacote selecionado.

Se um componente personalizado for atualizado para uma versão mais recente, um botão de atualização aparecerá na coluna Versão do painel Componentes personalizados. Se uma atualização do componente personalizado falhar e a mensagem de erro informar que um componente não tem uma versão mais recente, você poderá atualizar o componente manualmente. Clique em **Editar**, vá para a exibição **Selecionar componentes** e substitua a versão do componente por uma versão mais recente, se disponível.

Pesquisar pacotes

Você pode usar a barra de pesquisa na parte superior da página para pesquisar um pacote. Você pode pesquisar qualquer propriedade do pacote. Você também pode executar uma pesquisa global na Página inicial.

Para pesquisar pacotes usando a AQL (ACC Query Language), consulte Pesquisar usando a AQL (ACC Query Language).

Veja a seguir exemplos de pesquisas de pacote:

- Pesquise pelo nome do pacote. Use aspas para incluir espaço.

  ```
  packageName:tomcatLinux
  ```

- Você pode usar os operadores E (padrão), OU e NÃO.

  ```
  logLevel:info OR logLevel:debug
  ```

- Pesquise os relatórios dos agentes do Tomcat, mas somente aqueles que não tiverem "linux" no nome do servidor.

  ```
  processName:Tomcat NOT serverName:linux
  ```

- Pesquise de acordo com o último contato (de 5 semanas atrás até agora):

  ```
  lastContact:[-5w TO NOW]
  ```

- Use parênteses para agrupar operadores lógicos

  ```
  (osName:windows OR osName:Linux) AND logLevel:info
  ```

  Coloque as pesquisas de RegEx entre barras "/".

  > **TIP**
  > Você pode copiar e colar expressões de pesquisa do agente a partir de métricas do WebView.

  ```
  /ACCServer.*01\|Tomcat\|.*Agent/
  ```

Salvando a pesquisa

Na barra de pesquisa, use a opção **Salvar como novo conjunto** para salvar um padrão de pesquisa que você usa com frequência. Também é possível usar a pesquisa salva em uma consulta.

Exemplo: usando a coleta em uma consulta

```
collection:"Tomcat Agents" AND reportName:Linux
```

Propriedades de pesquisa de pacotes

A propriedade padrão para pesquisa de relatório é packageName. Para pesquisar várias propriedades, use a propriedade "all", que abrange as seguintes propriedades do relatório:

bundles, comment, emHost, facets, packageName.

Configurar componentes

Um componente é um bloco de construção do qual os agentes são criados. O componente representa uma parte compacta da funcionalidade do agente, por exemplo, serviços web do SOAP, servlet ou JSP.

Os componentes podem ser implantados dinamicamente ou podem exigir uma reinicialização do processo monitorado. Os componentes dinâmicos podem ser implantados dinamicamente. Você pode implantar o pacote em um agente em execução sem a necessidade de reiniciar o agente. Para implantar o pacote, adicione, remova ou atualize um componente dinâmico em um pacote de agentes. Os componentes dinâmicos são marcados com o ícone Componente dinâmico. Os componentes que podem ser aplicados a um agente em execução, mas que exigem uma reinicialização do processo monitorado, são marcados com o ícone Requer reinicialização.

Para exibir a lista de componentes que estão disponíveis com o APM Command Center por padrão, consulte a Lista de componentes.

Você também pode criar um componente personalizado. Para obter mais informações, consulte Adicionar componentes personalizados. Não é possível editar componentes na página Componentes. Use a página Pacotes para editar as propriedades do componente.

Pesquisar componentes

Você pode usar a barra de pesquisa na parte superior da página para pesquisar um componente. Você pode pesquisar qualquer propriedade do componente. Você também pode executar uma pesquisa global na Página inicial.

Para pesquisar componentes usando a AQL (ACC Query Language), consulte Pesquisar usando a AQL (ACC Query Language).

Veja a seguir exemplos de pesquisas de componente:

- Pesquise pelo nome do componente. Use aspas para incluir espaço.

  ```
  bundleName:"ACCDemoWin01|Tomcat|Tomcat Agent-3"
  ```

- Você pode usar os operadores E (padrão), OU e NÃO.

  ```
  logLevel:info OR logLevel:debug
  ```

- Pesquise o componente dos agentes do Tomcat, mas somente aqueles que não tiverem "linux" no nome do servidor.

  ```
  processName:Tomcat NOT serverName:linux
  ```

- Pesquise de acordo com o último contato (de 5 semanas atrás até agora):

  ```
  lastContact:[-5w TO NOW]
  ```

- Use parênteses para agrupar operadores lógicos

  ```
  (osName:windows OR osName:Linux) AND logLevel:info
  ```

  Coloque as pesquisas de RegEx entre barras "/".

  > **TIP**
  > Você pode copiar e colar expressões de pesquisa do agente a partir de métricas do WebView.

  ```
  /ACCServer.*01\|Tomcat\|.*Agent/
  ```

Salvando a pesquisa

Na barra de pesquisa, use a opção **Salvar como novo conjunto** para salvar um padrão de pesquisa que você usa com frequência. Também é possível usar a pesquisa salva em uma consulta.

Exemplo: usando a coleta em uma consulta

```
collection:"Tomcat Agents" AND reportName:Linux
```

Propriedades de pesquisa do componente

A propriedade padrão para a pesquisa de componentes é "name".Para pesquisar várias propriedades, use a propriedade "all", que abrange as seguintes propriedades do componente:

category, dependencies, description, enhances, facets, name, osName, version.

Pesquisar usando a AQL (ACC Query Language)

Especifique uma consulta personalizada na barra de pesquisa, na parte superior da página do ACC, que filtra os itens mostrados em uma exibição. A consulta personalizada usa a AQL (ACC Query Language) do ACC, que substitui a linguagem Lucene que era usada anteriormente. Para saber mais sobre as diferenças entre o Lucene e a AQL, consulte a documentação Propriedades pesquisáveis.

Criar consultas simples

Digite uma palavra na barra de pesquisa para filtrar todos os resultados correspondentes com base na consulta da palavra. A pesquisa é executada em uma propriedade padrão, normalmente, um nome. Para pesquisar uma propriedade específica, digite a consulta neste formato:

```
propertyName:search_query_word
```

Observe que `propertyName` diferencia maiúsculas de minúsculas. À medida que você digita, a barra de pesquisa mostra as propriedades disponíveis. Use a propriedade "all" para executar a pesquisa em várias propriedades.

Exemplo: pesquisa simples

```
osName:windows
```

Criar consultas de combinação

Digite várias consultas na barra de pesquisa separadas por espaços ou digite várias subconsultas usando os seguintes operadores: E, OU e NÃO.

Os operadores diferenciam maiúsculas de minúsculas, e é possível usar parênteses para agrupar operadores. AND é o operador padrão para consultas separadas por espaços.

Exemplo: consulta de combinação com o operador E

Os exemplos de consulta abaixo filtram os resultados em que todas as palavras são encontradas.

```
word1 AND word2 AND word3
word1 AND word2 word3
word1 word2 word3
```

Exemplo: consulta de combinação com o operador OU

Este exemplo filtra os resultados em que qualquer uma das palavras é encontrada.

```
word1 OR word2 OR word3
```

Exemplo: consulta de combinação com o operador NÃO

Este exemplo filtra os resultados que não contêm a palavra "myquery".

```
NOT myquery
```

Há símbolos alternativos que podem ser usados em vez de operadores nomeados:

Operator	Alternativa
AND	&&
OR	||
NOT	!

Exemplo: consulta de combinação com parênteses

O exemplo agrupa os operadores e filtra os resultados.

```
(word1 AND word2) OR word3
word1 AND (word2 OR word3)
```

Outras consultas de pesquisa

É possível usar sequências de caracteres, caracteres curinga, números, regex e consultas de intervalo como padrões de pesquisa para filtrar os resultados.

Usando sequências de caracteres e caracteres curinga

Digite uma sequência de palavras ou caracteres entre aspas (" ") para filtrar os resultados da pesquisa. Os resultados são uma correspondência exata da sequência de caracteres de pesquisa. Você pode usar os seguintes tipos de caracteres curinga: * para corresponder a qualquer subsequência de caracteres e ? para corresponder a um caractere. O uso de um caractere especial em uma sequência de caracteres é tratado como um caractere comum.

Exemplo: consulta de sequência de caracteres

A consulta abaixo filtra todos os resultados que são uma correspondência exata da sequência de caracteres.

```
"abc xyz"
```

Exemplo: consulta de caractere curinga

A consulta abaixo filtra todos os resultados que contêm a sequência de caracteres de pesquisa.

```
*"abc xyz"*
```

Exemplo: consulta de combinação de sequência de caracteres e caractere curinga

A consulta abaixo mostra um padrão de pesquisa usando caracteres curinga, sequência de caracteres e uma única palavra.

```
word*"quoted string"?
```

Consulta de intervalo

Uma consulta de intervalo pode ser um intervalo de números, versões ou datas.

Exemplo: consulta de intervalo

A consulta abaixo filtra os resultados no intervalo de 0 a 5 na propriedade numérica: prop.

```
prop:[0 TO 5]
```

A consulta a seguir mostra um padrão de pesquisa com intervalo exclusivo e estrela, indicando que não há limite máximo na propriedade numérica:

```
prop prop:{10 TO *]
```

Usando

O DX APM permite usar vários métodos para monitorar os status dos aplicativos comerciais e investigar e solucionar problemas.

Se desejar...	Fazer isso...	Leia isso...
Compreender a geografia do seu ambiente de aplicativos	Vá para a **Exibição da experiência** e exiba o seu ambiente de aplicativos no nível mais alto de seu universo. Detalhe até transações específicas para encontrar falhas.	Monitorar o desempenho usando a Exibição da experiência
Exibir uma visão geral dos valores de métrica de agente	Vá para a **Exibição da métrica** e navegue pela **Árvore de métricas** em um host do servidor de aplicativos. Detalhe a árvore e clique no nó do agente que deseja investigar.	Monitorar valores de métrica do agente com a Exibição da métrica
Exibir a integridade geral do ambiente	Vá para **Painel** e aplique a Exibição do agente e a Exibição da experiência. Um bloco no Painel representa um grupo de todos os componentes que compartilham um nome e valor de atributo. Os blocos mostram os status de alerta mais significativos de qualquer um dos componentes do grupo.	Monitorar a integridade geral do ambiente com o painel
Monitorar problemas e anomalias	Use a triagem assistida para monitorar problemas e anomalias. A triagem assistida identifica as experiências afetadas e nomeia a evidência como um problema. As anomalias são como problemas, mas sem impacto para o usuário. A triagem assistida analisa os dados do agente dos ambientes monitorados e identifica os componentes comuns de um problema para que você não fique sobrecarregado com problemas.	Triagem assistida e analistas
Investigar problemas	Use o Bloco de notas de análise e investigue os problemas que a triagem assistida identificou.	Investigar problemas usando o Bloco de notas de análise
Investigar o baixo desempenho das transações	Use o Visualizador do rastreamento de transação para entender o desempenho da transação e resolver o desempenho ineficaz, identificando quando, onde e por que o desempenho está diminuindo.	Investigar o baixo desempenho das transações
Monitorar a integridade e o desempenho dos agentes	Vá para a **Exibição de agentes** e monitore os agentes que estão disponíveis em seu ambiente. Os cartões de agente da exibição mostram detalhes de um agente ou de um grupo de agentes. Se os agentes forem agrupados em um cartão, as informações de métrica também serão agrupadas.	Exibir status do agente e gerenciar cartões de agente

Integração de aplicativos para monitoramento

Use a integração de aplicativos para integrar os aplicativos no DX APM de maneira ininterrupta e para configurar os pacotes de agentes facilmente para o seu ambiente. O assistente de integração de aplicativos guia você para a seleção das opções de monitoramento e cria pacotes de agentes. A integração de aplicativos contém os seguintes conceitos:

- **Aplicativo:** permite monitorar o aplicativo, que consiste em uma ou mais camadas.
- **Camada:** denota uma camada específica do aplicativo a ser monitorada. A camada faz referência a um ou mais pacotes de agentes criados com base na seleção de um usuário.

Na configuração de camada, cada etapa contém uma ou mais opções que fazem o mapeamento para recursos concretos de monitoramento (por exemplo, monitoramento do banco de dados APMIA e Oracle, sistema operacional Linux). Para integrar aplicativos, configure o seguinte:

1. **Detalhes do aplicativo -** Defina o nome e a descrição de um aplicativo a ser monitorado.
2. **Configuração da camada -** Defina as opções de monitoramento de camadas.
3. **Etapa de download -** Defina os artefatos (pacotes de agentes) para download criados a partir das opções de monitoramento.

Criar aplicativos

Crie aplicativos selecionando as opções de monitoramento e novos agentes de criação para integrar os aplicativos no DX APM. É possível adicionar várias camadas ao aplicativo. Também é possível editar, duplicar ou remover o aplicativo.

1. Na UI do DX APM, selecione **Configurações**.
2. Clique no bloco **Aplicativos**.
3. Se estiver usando os **Aplicativos** pela primeira vez, clique em **Começar** para criar um aplicativo. Caso contrário, crie um aplicativo clicando em

.
4. Forneça os seguintes detalhes para o seu aplicativo:
   a) **Nome do aplicativo:** dê um nome ao seu aplicativo. Você pode alterá-lo a qualquer momento.
   b) **Descrição:** forneça uma descrição do seu aplicativo.
5. Clique **em Adicionar camadas de aplicativo**.
6. Crie uma camada para o seu aplicativo com os seguintes detalhes:
   a) **Nome da camada:** adicione um nome e uma descrição para a camada de aplicativo.
   b) **Sistema operacional:** selecione o sistema operacional necessário no qual o aplicativo é executado. As opções subsequentes mudam de acordo com o sistema operacional selecionado.
   c) **Pilha de tecnologia (opcional):** selecione a pilha de tecnologia em que o aplicativo é executado. Você pode selecionar mais de uma pilha de tecnologia.
   d) **Tipo de recipiente (opcional):** selecione o tipo de recipiente para o seu aplicativo. O tipo de recipiente muda de acordo com o sistema operacional.
   e) **Banco de dados (opcional):** você pode selecionar um ou mais bancos de dados nos quais seu aplicativo é executado. Você pode adicionar vários perfis para os bancos de dados que suportam várias conexões e fornecer configurações de conexão separadas. Marque/desmarque a caixa de seleção **Instantâneos** para ativar/desativar os instantâneos dos rastreamento de banco de dados.
   f) **Servidor web:** selecione um ou mais servidores web em que seu aplicativo é executado. É possível adicionar vários perfis a um servidor web selecionado e definir suas configurações separadamente.
   g) **Sistema de troca de mensagens:** selecione um sistema de troca de mensagens que o aplicativo usa para comunicação. De acordo com a sua seleção, forneça os detalhes do sistema de troca de mensagens. Você

pode adicionar vários perfis aos sistemas de troca de mensagens que suportam várias conexões e definir suas configurações separadamente.

h) **Monitoramento:** selecione as opções de monitoramento para monitorar o desempenho do aplicativo. De acordo com a sua seleção, forneça os detalhes do sistema de monitoramento. Você pode adicionar vários perfis aos sistemas de monitoramento que suportam várias conexões de monitoramento e definir suas configurações separadamente.

i) **Adicional:** opções adicionais são exibidas com base no sistema operacional selecionado. Selecione os recursos necessários e forneça detalhes adicionais com base na sua seleção. Você pode adicionar várias opções para os recursos que suportam várias conexões e configurar seus detalhes separadamente.

j) **Opções:** com base no sistema operacional selecionado, atualize as opções.

k) **Resumo da camada:** verifique as configurações da camada e clique em **Adicionar camada agora**.

A Camada será criada. Você pode editar, duplicar ou remover a camada. Você pode criar e adicionar várias camadas para o aplicativo.

7. Clique em **Criar aplicativo**.
8. Clique em **Concluído**.

O aplicativo é criado com as camadas necessárias. Você pode fazer o download de um aplicativo ou copiar o link para download. Você também pode fazer o download das instruções de instalação ou exibi-las.

Fazer download de aplicativos

Usando a lista suspensa **Fazer download** correspondente a um aplicativo, você pode fazer o download de um aplicativo ou copiar o link do download. Você também pode fazer o download ou exibir as instruções de instalação. O pacote baixado contém o seguinte:

- Uma pasta para cada camada. Cada pasta contém os pacotes de agentes conforme configurado para cada camada.
- **Completed.txt:** se este arquivo não estiver disponível na pasta baixada, significa que o download do pacote não foi feito com êxito.
- **Info.txt:** este arquivo contém um resumo de todos os pacotes dentro das pastas da camada.

Monitorar o desempenho usando a Exibição da experiência

O DX APM permite compreender a geografia do seu ambiente de aplicativos, o que é vital para o monitoramento e a resolução de problemas de maneira eficaz.O Application Performance Management fornece uma visão geral do ambiente de aplicativos. A Exibição da experiência mostra os aplicativos monitorados do ponto de vista da experiência.

As seguintes funções usam a Exibição da experiência:

- Os administradores veem o estado de integridade do ambiente.
- Os analistas de um nível um monitoram os problemas e avisos no ambiente com a Exibição da experiência.
- Os analistas experientes investiguem e resolvem os problemas com o Bloco de notas de análise, o Painel e o Mapa.

Entender o front-end como uma experiência

A experiência é o componente mais à esquerda da transação, o primeiro componente monitorado de toda a transação. O nó da experiência é o primeiro componente de front-end monitorado e contém um atributo chamado Experience. O nó da experiência é o início do caminho da transação. Uma experiência pode ser, por exemplo, um servlet ou um front-end genérico.

Exibição da experiência

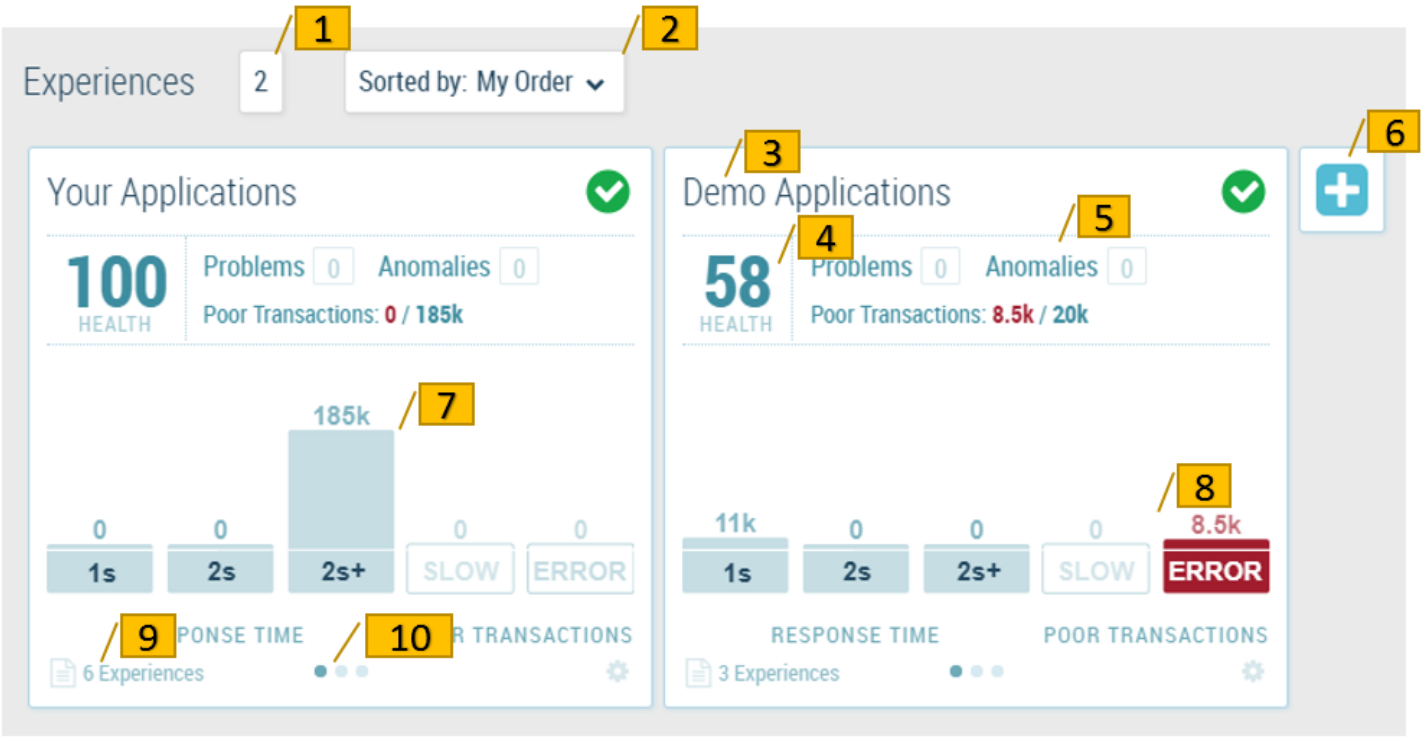
A Exibição da experiência permite:

- Filtrar as partes não problemáticas do ambiente para que seja possível se concentrar nos problemas.
- Detalhar até níveis inferiores da Exibição da experiência para ver seções do ambiente com mais detalhes. Os Cartões de experiência mostram o status de todos os componentes pelos quais você é responsável. As informações do cartão mostram as experiências sobrecarregadas. A triagem assistida identifica as áreas mais prováveis dos problemas e exibe o número de problemas e anomalias.

Tipos de transação na Exibição da experiência:

- Transações íntegras - valores da métrica *Respostas por intervalo* quando o nó da experiência não tem nenhum alerta no estado de cuidado ou risco
- Transações paralisadas - valores da métrica *Paralisações* do nó experiência
- Transações com erro - valores da métrica *Erros por intervalo* do nó experiência
- Transações lentas - valores da métrica *Respostas por intervalo* quando o nó da experiência tem um alerta no estado de cuidado ou risco na métrica Tempo médio de resposta ou na métrica Análise Diferencial
- Transações com alertas - valor da métrica *Respostas por intervalo* quando o nó da experiência não tem alertas no estado de cuidado ou risco em uma métrica diferente de Transações lentas

Use o gráfico a seguir e as legendas correspondentes para compreender os vários recursos da Exibição da experiência.



A legenda a seguir identifica cada item do mapa por número e fornece mais informações:

Número	Nome	Mais informações
1	O número de experiências	
2	Classificar por	Classifica os cartões por nome ou pedido.

3	Cartão de experiência	Os Cartões de experiência mostram informações resumidas e identificam o problema e sua origem. Os cartões são definidos com base em um universo. O número máximo é um universo dentro de um cartão.
4	INTEGRIDADE	A pontuação de INTEGRIDADE mostra a pontuação de integridade geral do ambiente. O número mostra um percentual de transações íntegras dentre o número total de transações. A pontuação mostra o volume de transações íntegras e incorretas. O volume de transações incorretas é a soma de todas as transações não íntegras (lentas, com erros, com alertas, paralisadas).
5	Problemas e anomalias	Mostra o número de problemas e anomalias. Um problema indica uma situação em que um ou mais componentes nas transações relacionadas dispararam alertas. Eventos como paralisações, erros e outras evidências afetaram negativamente as transações. Uma anomalia indica uma situação em que um ou mais componentes nas transações relacionadas dispararam alertas. Eventos como paralisações e erros foram observados, mas afetaram o desempenho da transação.
6	Adicionar cartão de experiência	Clique no sinal de mais para nomear e configurar um novo cartão de experiência. **Observação**: para obter mais informações sobre a adição de um cartão, consulte Exibir status do agente e gerenciar cartões de agente
7	TEMPO DE RESPOSTA	O histograma de TEMPO DE RESPOSTA mostra o tempo de resposta médio por segundo para transações íntegras, concluídas em: • 1s inferior a 1 segundo • 2s de 1 a 2 segundos • 2s+ mais de 2 segundos
8	TRANSAÇÕES INCORRETAS	O histograma TRANSAÇÕES INCORRETAS mostra o número de transações incorretas que ocorreram durante o período. • LENTO mostra o número de transações paralisadas e lentas. Essas transações contam com alertas para Análise diferencial ou Tempo médio de resposta. • ERRO mostra o número de erros por intervalo para o aplicativo.

9	Abrir o Bloco de notas de análise	O Bloco de notas de análise exibe as transações comerciais para um cartão de experiência específico. A contagem de transações comerciais é visível ao lado do ícone do Bloco de notas de análise. **Observação**: por padrão, não será possível abrir o Bloco de notas de análise se o Cartão de experiência contiver mais de 20 transações comerciais.
10	Alternar gráficos	Os gráficos referem-se ao seguinte: Tempo de resposta agregado, Tempo médio de resposta, Volume da transação.

Monitorar o desempenho usando a Exibição da experiência

A Exibição da experiência permite monitorar o desempenho do ambiente desde o nível mais alto do universo. É possível detalhar até transações específicas para encontrar falhas.

Siga estas etapas:

1. Clique em um **Cartão de experiência**.
   Serão exibidos os dados agregados dos grupos de transações comerciais relacionados que estiverem disponíveis no seu universo. Os cartões poderão ser adicionados, configurados e reordenados.
2. Clique no **gráfico** para percorrer os gráficos de métricas.
3. Exiba a **Pontuação de integridade**.
   A Pontuação de integridade mostra a pontuação de integridade geral do ambiente. O número mostra um percentual de transações íntegras dentre o número total de transações. Por exemplo, a pontuação de integridade do ambiente monitorado é 85. Essa pontuação significa que 85% das transações que você monitora estão íntegras. Os 15% restantes são transações incorretas. As transações incorretas são a soma das transações lentas e com falhas.
4. Expanda um **cartão**.Mais detalhes serão exibidos no painel de triagem assistida. O painel de triagem assistida é um item destacável à direita e mostra onde estão ocorrendo os problemas e anomalias. O mecanismo de triagem assistida identifica os componentes comuns de um problema para que você não fique sobrecarregado com problemas. O painel de triagem assistida estará visível na Exibição da experiência, exceto na página de nível superior.
5. Expandir a **história**. Mais detalhes serão exibidos. O painel também mostra os nós suspeitos, destacados pelo mecanismo de triagem assistida como outros possíveis fatores que contribuem para a situação.
6. Expanda os **problemas e as anomalias**.
   Mais detalhes serão exibidos.
7. Clique no **título** do gráfico e vá para o próximo nível do agrupamento.
8. Clique no ícone do **bloco de notas**.
   O Bloco de notas de análise do grupo de componentes será exibido.

   NOTE

   Por padrão, não será possível abrir o Bloco de notas de análise se o Cartão de experiência contiver mais de 20 transações comerciais.

Criando uma triagem usando a Exibição da experiência

Entenda como o painel de triagem assistida relata problemas e anomalias sobre eventos do sistema.

NOTE

Mais informações:

Monitorar problemas e anomalias da triagem assistida

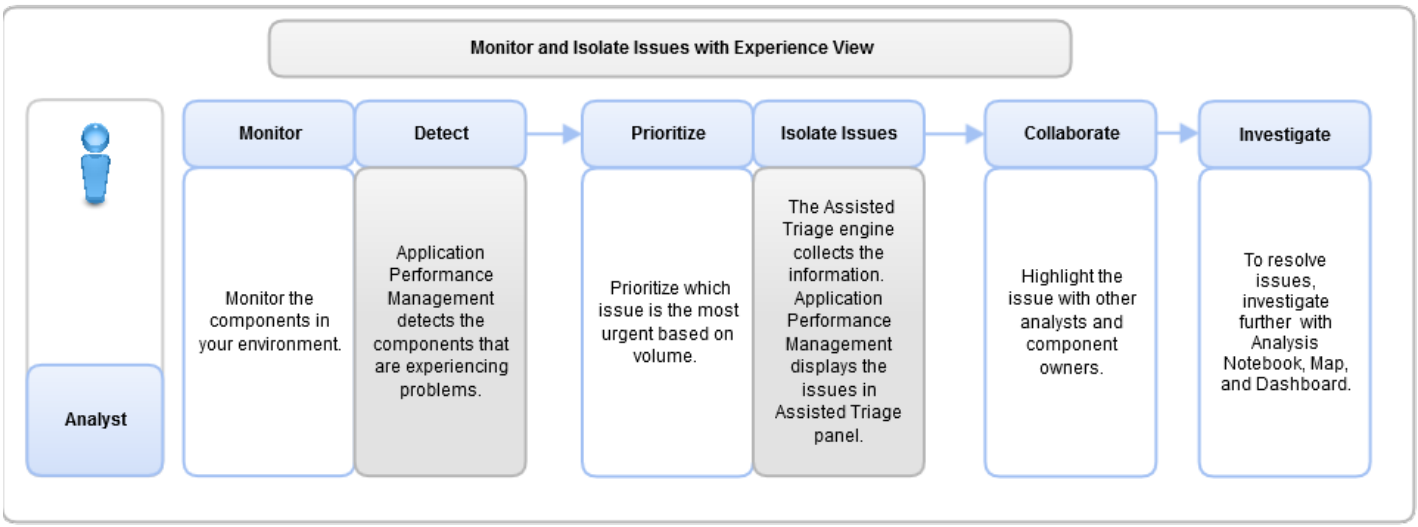
Exemplo: monitorar e isolar problemas usando a Exibição da experiência

A Exibição da experiência permite ver o status de todos os componentes na área do ambiente sob sua responsabilidade. É possível ver as experiências sobrecarregadas e detalhar para identificar os componentes críticos. A triagem assistida ajuda a identificar as áreas problemáticas mais prováveis.

Este exemplo mostra um fluxo de trabalho para um analista. Como analista, você está ciente de um problema no ambiente. Identifique a causa raiz do problema e direcione os recursos para solucioná-lo. O objetivo de diagnosticar problemas é identificar o paciente zero. Paciente zero é o componente do aplicativo que encontra os problemas primeiro e que afeta outros componentes e a experiência do cliente.

O diagrama a seguir mostra o fluxo de trabalho para monitorar um ambiente e isolar os problemas:

Figure 5: Homepage_workflow



1. Monitore os componentes em seu ambiente.
2. Clique em um **Cartão de experiência** para detalhar e ver informações mais detalhadas nos níveis inferiores da Exibição da experiência.
   O Application Performance Management detecta os componentes que estão com problemas e as transações lentas ou com falhas. A combinação de transações lentas e com falhas é exibida como o número total de experiências de cliente incorretas. As experiências são priorizadas com base no volume de transações e no volume de experiências de cliente incorretas.
3. Priorize o problema mais urgente com base no volume. Examine as experiências que estão apresentando os maiores problemas de integridade. Correlacione as experiências com os problemas identificados no painel de triagem assistida. Priorize os problemas a serem resolvidos com base no valor de negócio.
   O mecanismo de triagem assistida coleta as informações e exibe os problemas no painel de triagem assistida. O mecanismo de triagem assistida identifica as transações que compartilham componentes de baixo desempenho. Os componentes relacionados sobrecarregados são identificados juntos como um problema no painel de triagem assistida.
4. Consulte analistas mais experientes ou uma pessoa responsável pelo problema.Use as informações no painel para identificar os proprietários dos componentes com problemas. Compartilhe o URL com a pessoa para que ela possa ter a mesma visualização.
5. Investigue o problema mais a fundo no Bloco de notas de análise, no Mapa e no Painel.

O DX Application Performance Management fornece uma visão geral e permite compreender a geografia do seu ambiente de aplicativos, o que é vital para o monitoramento e a solução de problemas efetivos. A Exibição da experiência mostra os aplicativos monitorados do ponto de vista da experiência.

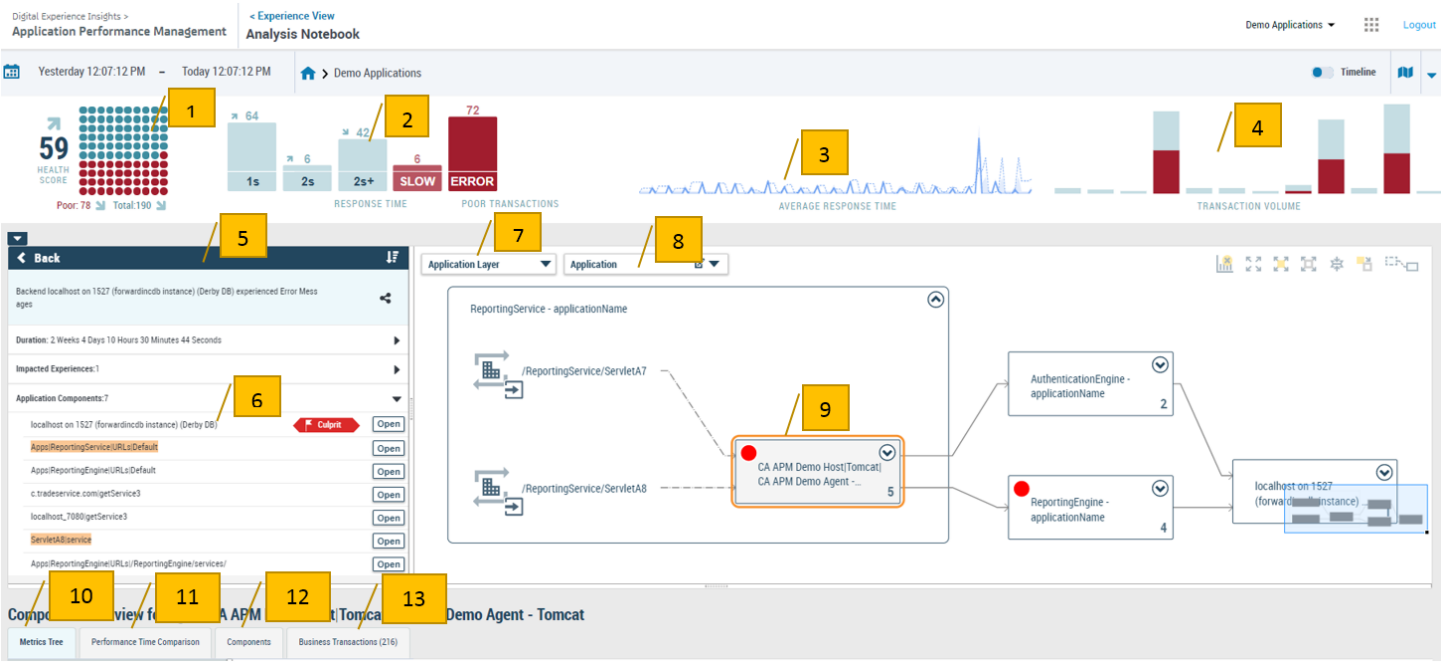
Para monitorar o desempenho do aplicativo usando a Exibição da experiência, consulte Monitorar o desempenho usando a Exibição da experiência.

Investigar problemas usando o Bloco de notas de análise

O DX APM permite que os analistas executem tarefas específicas para sua função. Use o bloco de notas de análise para investigar problemas.

Bloco de notas de análise

Use o gráfico a seguir e as legendas correspondentes para compreender os vários recursos do bloco de notas de análise.

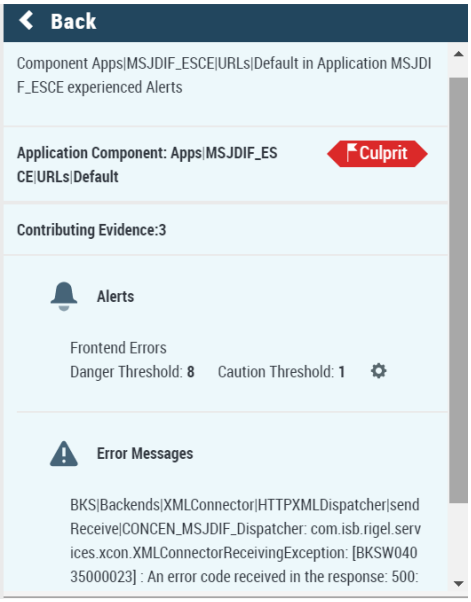


A legenda a seguir identifica cada item por número e fornece mais informações:

Número	Nome	Mais informações
1	PONTUAÇÃO DE INTEGRIDADE	A Pontuação de integridade mostra a pontuação de integridade geral do ambiente. O número mostra um percentual de transações íntegras dentre o número total de transações. A pontuação mostra o volume de transações íntegras e incorretas. O volume de transações incorretas é a soma de todas as transações não íntegras (lentas, com erros, com alertas, paralisadas).

2	Histograma do tempo de resposta agregado	O histograma mostra o tempo médio de resposta por segundo de transações íntegras e incorretas. • **1s** Número de transações íntegras que foram concluídas em menos de 1 segundo. • **2s** Número de transações íntegras que foram concluídas entre 1 e 2 segundos. • **2s+** Número de transações íntegras que foram concluídas em mais de 2 segundos. • **Lento** Número de transações paralisadas e lentas. Transações que violaram o limite do alerta Tempo médio de resposta. • **Erro** Valores da métrica Erros por intervalo para o nó da experiência. O vermelho indica o número de transações com alertas que foram concluídas.
3	Dados de série temporal - gráfico de tempo médio de resposta	Os dados da Série temporal fornecem a visão geral das métricas ou de um determinado intervalo de datas problemático. Você não está limitado apenas à orientação de eventos. Passe o mouse sobre um pico no comportamento da métrica no gráfico para selecionar e ampliar um intervalo de datas problemático. As métricas de respostas por intervalo e erros por intervalo são coletadas a cada 15 segundos. Gráfico Tempo médio de resposta • A linha azul indica o tempo médio de resposta real. • A linha pontilhada indica uma previsão do tempo médio de resposta. • As áreas sombreadas indicam um desvio.Se o valor de previsão estiver fora do intervalo do desvio, significa que algo incomum está acontecendo.

4	Dados de série temporal - histograma de volume de transações	Os dados da Série temporal fornecem a visão geral das métricas ou de um determinado intervalo de datas problemático. Você não está limitado apenas à orientação de eventos. Passe o mouse sobre um pico no comportamento da métrica no gráfico para selecionar e ampliar um intervalo de datas problemático. As métricas Respostas por intervalo e Erros por intervalo são coletadas a cada 15 segundos. Histograma Volume da transação • Divide o intervalo de datas em 12 seções e compara o volume de transações dentro do intervalo de datas selecionado.
5	Painel de triagem assistida	O painel de triagem assistida relaciona os problemas e as anomalias do componente selecionado.

6	Status do componente/responsável	**Círculo vermelho** - O componente está presente em ao menos um problema ou anomalia listada no painel de triagem assistida. Todos os componentes em uma história são tratados como representantes. **Círculo vermelho concêntrico** - O componente é o responsável por ao menos um problema ou anomalia listada no painel de triagem assistida. Todos os representantes têm evidências, mas um responsável é um representante especial. O responsável identifica a causa raiz do problema ou da anomalia no devido aplicativo ou na devida transação. Esse componente pode ser a origem da degradação de desempenho no seu ambiente de aplicativos. **Abrir** - Clique em **Abrir** para exibir os detalhes da evidência da anomalia. Além disso, para os Alertas, é possível exibir os valores de limite e também editar as configurações do alerta. Clique no ícone de configurações de um alerta para ir até elas e personalizar mais os alertas. 
7	Camada	As camadas do mapa sobrepõem diferentes tipos de componente do ambiente no mapa.
8	Filtro	Um filtro é uma lista de atributos e valores obrigatórios que permite exibir componentes específicos no mapa.

9	Nós do componente e conexões	As linhas de conexão entre os nós representam os seguintes status: **Linha cinza** - Nenhum alerta é definido no componente de back-end. **Linha vermelha** - existe pelo menos um alerta vermelho no componente de back-end. O tracejado cinza indica que não existe componente de back-end na conexão.
10	Árvore de métricas	Métricas do componente selecionado em uma estrutura de árvore pesquisável.
11	Comparação de tempo do desempenho	Métricas do componente selecionado em uma tabela.
12	Componentes	Atributos que estão conectados ao componente selecionado.
13	Transações comerciais	Transações comerciais do componente selecionado.

Investigar problemas usando o Bloco de notas de análise

O bloco de notas de análise permite aprofundar a investigação dos problemas individuais.

Siga estas etapas:

1. Ao identificar uma experiência com problemas aparentes, abra o **bloco de notas de análise**.
   O bloco de notas de análise mostra as transações afetadas no formato de mapeamento.
2. Use o mapeamento **Linha de tempo** para exibir eventos e alertas.
3. Agrupe o mapeamento de uma perspectiva predefinida ou crie sua própria perspectiva.
4. Localize os componentes que estiverem marcados como problemas ou anomalias.
   -Um círculo vermelho indica que o componente está presente em ao menos um problema ou anomalia.
   - Um círculo vermelho concêntrico indica que o componente é o responsável por ao menos um problema ou anomalia
5. Passe o mouse sobre um **componente** e clique no ícone.
   O **gráfico de componente** mostra o máximo de 20 nós. Use **gráficos de componentes** para comparar mais métricas dinâmicas ou históricas entre nós arbitrários. O **gráfico de componente** contém mais informações de métricas do que o disponibilizado para cada componente do mapeamento.
   – Histograma do tempo de resposta agregado
   – Minigráfico de média
   – Gráfico Volume da transação
6. Clique em um **componente** no fluxo de relacionamento.
   – A guia **Árvore da métrica** mostra um subconjunto contextual de métricas para o componente selecionado. Para obter mais informações sobre como usar a Árvore de métricas, consulte Monitorar valores de métrica do agente com a Exibição da métrica.
   – A guia **Comparação de tempo do desempenho** exibe um comparador do minigráfico de métricas. A coluna à direita exibe as métricas da hora atual. A coluna mais à esquerda exibe métricas do mesmo horário, mas e um período anterior. É possível definir a hora da comparação nas listas suspensas.
   Os dados da métrica são exibidos no visualizador de métricas lado a lado, com métricas de comparação de um período anterior.
   – A guia **Componentes** contém detalhes de atributo do componente selecionado.
   – A guia **Transações comerciais** lista as transações.
7. Selecione o período para a comparação de métricas usando a lista suspensa.
   O mecanismo de triagem assistida analisa os dados do agente do ambiente monitorado. O mecanismo identifica as conexões e os padrões entre os alertas individuais que indicam um problema em desenvolvimento.O painel de

triagem assistida mostra os problemas e as anomalias detectados. Problemas e anomalias consistem em situações. As situações são agrupadas de acordo com o nome do aplicativo responsável e são classificadas em ordem cronológica e tamanho.
Uma anomalia indica uma situação em que um ou mais componentes nas transações relacionadas dispararam alertas de cuidado.
Um problema indica uma situação em que um ou mais componentes nas transações relacionadas dispararam alertas de aviso.

8. Clique em um **problema** ou em uma **anomalia**.
   Os detalhes sobre o problema ou a anomalia serão exibidos.O componente afetado será realçado no mapeamento.

Exibir status do agente e gerenciar cartões de agente

Use a Exibição de agentes para monitorar a integridade e o desempenho dos agentes disponíveis em seu ambiente. A página Exibição de agentes é uma visão geral com todas as informações importantes do agente em um único local. Na exibição, os Cartões de agente mostram detalhes de um agente ou um grupo de agentes. Se mais agentes forem agrupados em um cartão, as informações de métrica também serão agrupadas. Você pode executar as seguintes ações com o Agente ou Cartão de agente:

Exibir status do agente

A Exibição de agentes permite determinar o status da conectividade do agente, quaisquer problemas com sobrecarga ou quando o agente não coleta métricas. É possível exibir informações no modo dinâmico ou selecionar um intervalo de datas históricas.

Siga estas etapas:

1. Clique em **Exibição de agentes** no painel esquerdo.
   Um Cartão de agente mostra detalhes de um agente ou um grupo de agentes. Se mais agentes forem agrupados em um cartão, as informações de métrica também serão agrupadas.A Exibição de agentes mostra todos os agentes do ambiente e as seguintes métricas:
   - **CPU**
     Mostra a porcentagem da CPU que está sendo usada.
   - **Memória heap**
     Mostra a porcentagem de memória que está sendo usada.
     No gráfico de linhas de CPU e Memória heap, passe o mouse sobre um pico no comportamento de métrica no gráfico. Selecione e amplie um intervalo de datas com problemas.
   - **Data e hora de GC**
     Mostra a porcentagem do intervalo de datas que é gasta no coletor de lixo do intervalo de datas atualmente selecionado.
   - **Métricas coletadas**
     Mostra o número de métricas coletadas por agentes.
     Se o cartão contiver apenas informações de um agente, detalhes mais granulares de atributo, como nome do host ou tempo de atividade, serão mostrados. Se houver mais agentes em um cartão, você poderá ver Contagem de aplicativos, Contagem de agentes e Contagem do coletor.
2. (Opcional) Clique no título do cartão para mostrar uma perspectiva da qual você deseja agrupar os agentes, por exemplo: Tipo.A perspectiva padrão é Nome.
   As perspectivas disponíveis se baseiam em nomes de atributo para que os agentes sejam agrupados de acordo com os respectivos atributos.
3. (Opcional) Clique em **Exibição de isolamento**.
   Uma nova guia abre o mapeamento na **Camada de infraestrutura do APM**. O mapa mostra os componentes que compartilham o valor do atributo como um grupo expandido. Uma perspectiva temporária remove níveis mais

elevados do agrupamento. A Exibição de isolamento aplica um filtro de caminho de transação para que o mapa mostre todas as transações concluídas que passam pelos componentes.

4. Abra um Cartão de agente e selecione uma das seguintes opções na lista suspensa **Classificado por**:
   - **Pontuação de integridade**
     Mostra a integridade geral dos agentes. Vários alertas nos agentes estão monitorando métricas, como a CPU ou a conectividade do agente. A porcentagem da pontuação de integridade conta os alertas das últimas 24 horas. Se qualquer um dos alertas monitorados é disparado nas últimas 24 horas, a porcentagem de pontuação de integridade é desativada. Por exemplo, a Pontuação de integridade de 100% significa que nenhum alerta foi disparado nas últimas 24 horas. A Pontuação de integridade de 50% significa que, nas últimas 24 horas, alguns alertas foram mostrados pelo total de 12 horas.
   - **Conexão**
     Mostra quantos agentes estão disponíveis em seu ambiente e quantos agentes estão desconectados.
   - **CPU mais alta**
     Mostra os cartões com uso mais alto de CPU primeiro.
   - **Memória mais alta**
     Mostra cartões com uso mais alto de memória primeiro.
5. (Opcional) Clique em **View as List**.
   Uma lista é uma alternativa aos Cartões de agente e mostra mais dados em uma página, de maneira concisa. Clique em um nome de coluna pela qual classificar. Clique em uma linha para expandir os dados do agente.

Adiciona um Cartão de agente

Os Cartões de agente permitem dividir agentes em grupos significativos com base nos respectivos atributos. Por padrão, você tem um Cartão de agente com todos os agentes. Como administrador, é possível adicionar novos Cartões de agente.

Siga estas etapas:

1. Na página inicial de Exibição de agentes, clique no sinal de mais próximo aos Cartões de agente existentes.
   Uma nova janela **ADICIONAR CARTÃO DE AGENTE** é aberta.
2. Nomeie o cartão e siga as instruções da janela.
   - **Selecionar universo**
     Na maioria dos ambientes corporativos, o número total de componentes é muito grande para que possa ser visualizado de modo eficiente. Os universos permitem que o administrador refinem o número e os tipos de componente em grupos significativos. Esse grupo refinado é um Universo. Por motivos de segurança, não há nenhuma atribuição padrão para todos os usuários. Você deve ser alocado para um Universo para exibir informações.
   - **Aplicar um filtro**
     Use o Universo inteiro ou aplique um filtro.
   - **Incluir o nó da experiência**
     A experiência é o primeiro componente de front-end monitorado e o início do caminho da transação. Um nó de experiência contém um atributo extra chamado Experience. Se você marcar Incluir o nó da experiência, os resultados filtrados incluirão o nó que mostra onde a transação foi iniciada.
   - **Agrupar por**
     Selecione os atributos que você deseja detalhar em mais níveis do Cartão de agente.
   - **Tipo de gráfico padrão**
     CPU/memória heap
     Número de métricas coletadas/data e hora de GC
     Resumo de atributos
3. Se desejar tornar o cartão público, selecione **Tornar público este cartão de agente**.

NOTE
Se essa opção não for selecionada, o cartão será privado e somente você poderá vê-lo. Se você selecionar essa opção, o cartão será público e todos os usuários que tiverem acesso ao universo relevante poderão ver o cartão.

4. Clique em **Salvar**.

Você adicionou um Cartão de agente.

Editar um Cartão de agente

Você pode editar cartões de agente, por exemplo, se desejar selecionar diferentes atributos como níveis de detalhamento.

Siga estas etapas:

1. Na página inicial de Exibição de agentes, selecione o cartão que deseja editar.
2. Clique no botão de configurações do cartão.
3. Clique em **Editar cartão**.
   Uma nova janela **Editar cartão de agente** é exibida.
4. Edite o cartão.
5. Clique em **Salvar**.

Você editou um Cartão de agente.

Excluir um Cartão de agente

Você pode excluir os cartões de agente que não deseja mais usar.

Siga estas etapas:

1. Na página inicial de Exibição de agentes, selecione o cartão que deseja editar.
2. Clique no botão de configurações do cartão.
3. Clique em **Editar cartão**.
   Uma nova janela **Editar cartão de agente** é exibida.
4. Clique em **Excluir cartão**.
5. Na janela pop-up de confirmação da exclusão, clique em **Excluir**.

Você excluiu um Cartão de agente.

Compartilhar um Cartão de agente

Como administrador, você pode compartilhar um Cartão de agente com um usuário dentro de um universo existente.

Siga estas etapas:

1. Verifique se o usuário tem acesso ao universo.
2. No Cartão de agente, selecione **Tornar público este cartão de agente**.
   O cartão aparece na sua lista de cartões.
3. Envie o link do Cartão de agente para o usuário.

NOTE
É possível compartilhar um Cartão de agente privado com um usuário do mesmo universo. O usuário poderá exibir temporariamente o cartão privado.

A página Exibição de agentes é uma visão geral de todas as informações importantes do agente e permite que o usuário monitore a integridade e o desempenho dos agentes que estão disponíveis no ambiente. Você pode executar as ações a seguir com o Agente ou Cartão de agente.

- Exibir status do agente
- Adiciona um Cartão de agente
- Editar um Cartão de agente
- Excluir um Cartão de agente
- Compartilhar um Cartão de agente

Para obter mais informações sobre como executar qualquer uma dessas ações, consulte Exibir status do agente e gerenciar cartões de agente.

Monitorar valores de métrica do agente com a Exibição da métrica

Como administrador do APM, use a Exibição da métrica para obter uma visão geral clara dos valores de métrica do agente. Investigue agentes para ver os valores de métrica para um determinado intervalo de datas.

Visão geral

O DX APM oferece duas exibições de métricas:

- **Global Metric View:** contém todas as métricas de todos os agentes conectados à Infraestrutura do APM durante o intervalo selecionado.
- **Contextual Metric View:** mostra um subconjunto de métricas que são relevantes para os componentes selecionados no mapeamento.

Ambas as Exibições de métrica contêm uma Árvore de métricas que lista métricas e outras informações no formato de árvore. No DX SaaS, as métricas são organizadas em uma hierarquia `Host|Processo|Agente` . O DX APM local organiza as métricas em uma hierarquia `Domínio|Host|Processo|Agente` .

Entender a Árvore de métricas

O nível mais alto na árvore representa os hosts do servidor de aplicativos (DX SaaS) ou Domínios (DX APM ou local).O próximo nível representa processos, seguidos por agentes que são instalados em hosts individuais do servidor de aplicativos.A exibição em árvore de agentes, recursos e métricas é atualizada a cada 60 segundos para mostrar os dados atuais das métricas.

A Árvore de métricas mostra dois tipos de host:

- **Custom Metric Host (Virtual)** - esse nó representa um host virtual que contém métricas que um agente específico não relatou. Por exemplo, métricas agregadas são exibidos nesse nó. Esse nó não corresponde a um computador host físico.
- **Hosts** - esse nó representa um computador que hospeda um agente. Cada nó do host contém um nó do processo para a instância do aplicativo monitorado. Os nós do processo por sua vez contêm nós do agente. Os nós que correspondem aos recursos do sistema e aplicativo e contêm métricas são armazenados nos nós do agente. Os recursos do aplicativo em nós do agente diferem de acordo com o tipo de agente (Java ou .NET). O nó de alto nível representa os seguintes componentes:
  - Componentes do seu aplicativo J2EE ou .NET, como servlets, EJBs ou página ASP
  - Nós do sistema, incluindo o host que executa o servidor de aplicativos e o computador host que executa o DX APM.

A Árvore de métricas mostra dois tipos de métrica:

- **Métrica de sequência de caracteres** - o valor da métrica é uma sequência de caracteres. O Gráfico da métrica mostra apenas o valor atual no final do intervalo de datas.
- **Métrica numérica** - o Gráfico da métrica mostra os valores de métrica, que incluem os valores mínimo e máximo, o desvio e o histórico de status do alerta associado.

Exibir uma métrica do agente na Global Metric View

Exiba dados dinâmicos ou selecione um intervalo de datas para exibir dados históricos.Compare, correlacione e visualize os valores de métricas de um determinado intervalo de datas.

Siga estas etapas:

1. No DX APM, clique na **Exibição da métrica** no painel esquerdo para abrir a Global Metric View.
   A Árvore de métricas é aberta.
2. Selecione um host de servidor de aplicativos.
3. Detalhe ainda mais a árvore e clique no nó do agente que deseja investigar.

   NOTE
   Os agentes desconectados são exibidos em cinza. Se um agente não enviar uma métrica por algum tempo, a métrica se tornará inativa e também será exibida em cinza.
4. Clique em uma pasta na Árvore de métricas para exibir a **Visão geral da métrica**.
   A **Visão geral das métricas** consiste nas seguintes guias:
   - **Gráficos da métrica**
     Mostra os valores de métrica dos nós selecionados na Árvore da métrica.
   - **Contagem de métricas**
     Mostra informações resumidas das métricas que estão nas subpastas individuais da pasta selecionada.
     1. Clique em uma métrica no gráfico de pizza ou na tabela para abrir a subpasta relevante.
     2. Marque a caixa de seleção **Somente métricas dinâmicas** para ver o número de métricas dinâmicas, ou seja, as métricas que o agente está relatando agora.
   - **Rastreamentos**
     Mostra a lista de todas as transações comerciais associadas
     1. Clique em uma Transação comercial na lista para exibir os rastreamentos correspondentes e os respectivos detalhes.
   - **Errors**
     Mostra uma lista de todas as transações comerciais que contêm erros.
     1. Clique em uma transação comercial para exibir os detalhes do erro.
   - **Despejos de segmento**
     A seleção de um nó do agente na árvore do navegador de métricas exibe os **Despejos de segmento**.Essa guia permite coletar despejos de segmento Java (despejos de segmento) e exibir dados de despejo de segmento atuais e históricos. Um despejo de segmento fornece informações sobre todos os segmentos em execução dentro de uma JVM em determinado momento. Para cada segmento, um despejo de segmento fornece o nome e a ID do segmento, estado e um rastreamento de pilha, que lista todos os métodos chamados. A guia Despejos de segmento inclui o seguinte:
     - O cabeçalho exibe a hora do despejo de segmento.
     - O painel de pesquisa permite procurar uma sequência de caracteres específica em todas as informações de despejo de segmento. Os resultados são exibidos na tabela de informações do segmento.
     - A lista suspensa de estado dos segmentos filtra a tabela de informações do segmento pelo estado do segmento.Quando você seleciona um estado, a tabela de informações do segmento é atualizada.
     - A tabela de informações do segmento exibe uma lista de todos os segmentos. Cada segmento fornece a ID, o nome e o estado do segmento, além do último método chamado pelo segmento logo pouco antes do despejo de segmento.
     - A tabela de rastreamento de pilha de segmentos exibe todos os métodos na ordem chamada.
     - O gráfico de pizza % de segmentos por estado exibe os segmentos nestes estados: bloqueado(a), bloqueado, em execução ou aguardando.

NOTE
Exiba a métrica `<Nome do agente> | Threads | Deadlock Count` na árvore do navegador de métricas, se você estiver fazendo a triagem de problemas do agente. Essa métrica indica se há segmentos bloqueados afetando o agente. A configuração do Introscope é necessária para ativar a métrica Deadlock Count. Para obter mais informações, consulte o Agente do Java.

Você pode fazer o seguinte na guia Despejos de segmento:

- **Coletar novo**: para coletar um despejo de segmento.
- **Salvar como texto**: para salvar o despejo de segmento atual em um arquivo de texto.
- **Carregar anterior**: para carregar um único despejo de segmento coletado anteriormente para ver a marca de data e hora e os dados associados.

Nenhum dado de despejo de segmento é exibido até que um despejo de segmento seja coletado ou depois que um Gerenciador corporativo é reiniciado. Para desmarcar um segmento na tabela, mantenha pressionada a tecla Ctrl e clique na linha novamente.

5. (Opcional) Clique na lupa para encontrar métricas específicas na Árvore de métricas.
   a. Selecione **Todos os lugares** para fazer uma pesquisa global ou selecione a opção de pasta para uma pesquisa local.
6. (Opcional) Para ocultar as métricas que não relatam dados atuais ao agente, clique com o botão direito do mouse no nó do agente e clique em **Hide grayed out metrics**.
   A métrica não é exibida na Árvore de métricas.

   NOTE
   A Árvore de métricas mostra a métrica novamente depois que o agente começa a receber dados atuais da métrica.
7. Clique em uma **métrica**, por exemplo, **Tempo médio de resposta (ms)** para exibir seus valores no Gráfico da métrica.
   Se existir um alerta na métrica, o Gráfico da métrica mostrará o histórico de status do alerta em faixas codificadas por cor, que indicam o status do alerta em um determinado momento:
   – **Verde** - OK
   – **Amarelo** - Aviso
   – **Vermelho** - Risco
   – **Nenhuma cor** - não existem alertas para a métrica selecionada.

   NOTE

   O histórico de status do alerta é exibido nos Gráficos da métrica por até 7 dias. Se você estender o intervalo de tempo para além de 7 dias, as informações sobre o status do alerta não aparecerão.
8. (Opcional) Desmarque a opção **Show Differential Analysis** para ocultar a faixa de desvio.

   NOTE

   Se a métrica oferecer suporte à Análise diferencial, uma faixa destacará o desvio automaticamente na tendência da métrica
9. (Opcional) Clique em **Mostrar exibição mínima/máxima**.
   Os valores mínimo e máximo são mostrados no gráfico.
10. (Opcional) Selecione várias métricas na Árvore de métricas para comparação no Gráfico da métrica.
    a. Clique no nome da métrica fora da caixa de seleção para fazer uma nova seleção.
    b. Clique em **Combinar** para exibir os dados da métrica em um gráfico.
    c. Clique em **Limpar seleção** para selecionar outro conjunto de métricas.

    NOTE

    Você pode selecionar até 10 métricas para comparação nos Gráficos da métrica.
11. Use a **Linha de tempo** para selecionar um intervalo de datas específico.

12. Arraste o cursor sobre o gráfico para ampliar um limite de tempo mais curto.

    NOTE
    A **Linha do tempo** mostra intervalos de no mínimo 8 minutos e no máximo 1 ano.
13. Selecione um período de resolução na lista suspensa **Resolução** (15 minutos, 30 minutos, 1 hora, 2 horas, 6 horas ou 12 horas) para ver os valores do período.Os valores de intervalo de tempo possíveis são 15 segundos, 30 segundos, 1 minuto, 2 minutos, 5 minutos, 15 minutos, 30 minutos, 1 hora, 2 horas, 6 horas, 12 horas, 1 dia, 7 dias, 14 dias.

    NOTE

    Os valores de intervalo de datas na lista suspensa **Resolução** são exibidos com base no intervalo de datas selecionado na **Linha do tempo**.
14. (Opcional) Compartilhe o URL com seus colegas para que eles possam ver a mesma exibição da métrica específica na árvore.

Personalizar os gráficos de métricas

É possível usar as seguintes opções para personalizar o gráfico.

- Selecione um período de resolução na lista suspensa **Resolution** (*15 segundos*, *30 segundos*, *1 minuto*, *2 minutos*) para ver os valores do período.
- Clique em **Combine** e selecione **All** para exibir os dados da métrica em um gráfico ou selecione **By Name** para exibir os gráficos de métricas categorizados pelo nome da métrica. Essa opção é ativada quando você seleciona mais de uma métrica na **Árvore de métricas**.
- Use o botão de **reticências** para exibir e configurar as seguintes opções:
  - **Min/Max Display**: selecione a opção para exibir os valores mínimo e máximo no gráfico.
  - **Combine**: selecione mais de uma métrica na árvore de métricas e selecione uma opção em Combine para exibir todas as métricas em um gráfico.
  - **Time Range Comparison**: compare os dados nos gráficos usando um intervalo de tempo predefinido ou selecione um intervalo de tempo personalizado.
  - **Axis Breaks**: selecione a opção para exibir os dados do intervalo mínimo ao máximo, em vez da exibição padrão que mostra os dados de 0 ao máximo.Quando você seleciona a opção Axis Breaks, não é possível exibir os dados em um intervalo de tempo. Portanto, a opção Time Range Comparison é removida da lista suspensa. Além disso, a opção Axis Breaks é exibida apenas quando você não combina os gráficos de métricas.
  - **Download**: selecione uma ou mais métricas na árvore de métricas e clique na opção Download para fazer download dos detalhes da métrica em um formato de arquivo CSV.

Abrir a Contextual Metric View

Abra a Contextual Metric View no Mapa ou Bloco de notas de análise para exibir um subconjunto de métricas para um nó específico no mapa.

Para abrir a Contextual Metric View no mapa, siga estas etapas:

1. No DX APM, clique em **Mapeamento** no painel esquerdo.
2. No mapa, selecione um nó do qual deseja ver as métricas do agente.

   NOTE
   Se você selecionar mais de um nó, a Árvore de métricas mostrará uma união de métricas relevantes para os nós selecionados.
3. Clique no painel **Navegador de métricas** para abrir a Árvore de métricas.

Para abrir a Contextual Metric View no Bloco de notas de análise, siga estas etapas:

1. No DX APM, clique em **Exibição da experiência** no painel esquerdo.

2. Encontre um **Cartão de experiência** para o qual deseja exibir métricas e clique em **Abrir um bloco de notas de análise**.
   O Bloco de notas de análise é exibido.
3. **Abra** um problema ou anomalia para ver a **Exibição do mapa** correspondente.

   NOTE

   Se o Bloco de notas de análise exibir apenas um problema ou uma anomalia, a **Exibição do mapeamento** correspondente será mostrada por padrão.
4. No mapa, selecione um nó do qual deseja ver as métricas do agente.

   NOTE
   Se você selecionar mais de um nó, a Árvore de métricas mostrará uma união de métricas relevantes para os nós selecionados.
5. Clique no painel **Árvore de métricas** para abrir a Árvore de métricas.

Pesquisar métricas na Árvore de métricas

Na **Árvore da métrica**, é possível pesquisar métricas específicas ou usar expressões regulares do agente para filtrar as métricas necessárias. Além disso, a barra de pesquisa oferece suporte à funcionalidade de pesquisa de texto completo. A barra de pesquisa agora detecta automaticamente se uma entrada está no formato de expressão regular e executa uma pesquisa de expressão regular de acordo com isso.

NOTE
A opção para utilizar expressões regulares tornou-se obsoleta.

Siga estas etapas:

1. No DX APM, clique na **Exibição da métrica** no painel esquerdo para abrir a Global Metric View.
   A **Árvore de métricas** é aberta.
2. Digite o nome da métrica na caixa de texto da pesquisa que você deseja filtrar. A barra de pesquisa detecta se uma entrada está no formato de expressão regular e executa uma pesquisa de acordo com isso.

   NOTE
   Você também poderá selecionar uma frase de pesquisa anterior que apareça na lista suspensa de preenchimento automático ao digitar a frase de pesquisa.
3. As métricas que corresponderem aos critérios de pesquisa serão listadas no painel direito.

   NOTE
   Clique no menu de três pontos à direita da página resultados da pesquisa para mostrar ou ocultar colunas na exibição de resultados da pesquisa.

Além disso, você pode marcar itens na árvore da métrica como favoritos. Essa funcionalidade se estende às métricas de gráfico.

Siga estas etapas:

1. Para marcar um item como favorito, passe o cursor do mouse sobre o item na árvore da métrica.
   Uma estrela será exibida do lado direito do item.
2. Clique no ícone de estrela para marcá-lo como um favorito.
3. Selecionar **Show favorites only** fará com que sejam exibidos apenas os itens que estão marcados como favoritos.

O DX Application Performance Management oferece duas exibições de métrica, a exibição global de métricas e a exibição contextual de métricas.

A Exibição da métrica fornece uma visão geral clara dos valores de métrica do agente. Também ajuda a investigar os agentes para ver os valores de métrica para um determinado intervalo de tempo.

Para obter mais informações sobre como a Exibição da métrica, consulte Monitorar valores de métrica do agente com a Exibição da métrica.

Incorporar painéis do DX na exibição da métrica

Você pode criar painéis personalizados nos Painéis do DX usando as métricas do APM e incorporar esses painéis na página Exibição da métrica. Na Exibição da métrica, o painel incorporado aparecerá como uma guia se você selecionar qualquer métrica que corresponda à condição.

> **NOTE**
> Por padrão, os painéis Blamepoint e Frontend Overview são incorporados na Exibição da métrica. Esses painéis são pré-configurados e estão prontos para uso.

Em linhas gerais,

1. Crie um painel. Crie o painel, marque o painel e adicione as variáveis nos painéis do DX.
2. Mapeie o painel. Mapeie o painel criado anteriormente e o local das métricas no DX APM usando o bloco **Painéis do DX** na página **Configurações** do DX APM.
3. Exiba o painel no DX APM.

Criar um painel personalizado nos painéis do DX

Crie o painel usando a origem de dados **AIOps_Metrics**. No Criador de consultas, adicione as variáveis **$Agent** e **$Attribute**.

Siga estas etapas:

1. Efetue logon nos painéis do DX.
2. Clique em **Criação > Painel** no painel de navegação à esquerda.
   a. Clique em **Add an empty panel**.
   b. Digite o **Título do painel**.
   c. Selecione a visualização.
   d. Crie a consulta:
      a. Selecione a origem de dados **AIOps_Metrics**.
      b. Ative o **Criador de consultas avançado**.
      c. Na seção **Source Name Specifier**,
         a. Selecione o Especificador como **EXACT**. Você também pode especificar o padrão REGEX.
         b. Digite o Nome como **$Agent**.

            > **NOTE**
            > Você pode inserir essa variável como **$Agent** ou pode adicioná-la com valores. Por exemplo, você pode digitar **$Agent:SuperDomain\|apm\-rh7\-197\|Infrastructure\|Agent**.

      d. Na seção **Attribute Name Specifier**,
         a. Selecione o Especificador como **EXACT**. Você também pode especificar o padrão REGEX.
         b. Insira o **Padrão** como **$Attribute**.

            > **NOTE**
            > Você pode inserir essa variável como **$Attribute** ou pode adicioná-la com valores. Por exemplo, você pode inserir **$Attribute: Tempo médio de resposta**.

      > **NOTE**
      > Além de **$Agent** e **da $Attribute**, você também pode usar uma variável personalizada com qualquer nome.
3. Salve o painel na pasta **APM-MetricView**. Como alternativa, você pode usar a **Pasta personalizada** para especificar uma pasta diferente para salvar o painel.
4. Marque o painel.
   a. Clique no ícone **Configurações** do painel.
   b. Adicione o identificador na página **Configurações gerais**.

NOTE
Certifique-se de que o identificador seja exclusivo.

5. Adicione a variável **$Agent**:
   a. Abra a página **Configurações gerais**.
   b. Clique em **Variáveis** no painel de navegação à esquerda.
   c. Forneça as seguintes informações:
      a. **Nome:** digite um nome para a variável.
      b. **Tipo:** selecione o Tipo como **Personalizar**.
      c. **Values Separated by Comma:** digite o valor para um agente.
   d. Clique em **Atualizar**.
6. Adicione a variável **$Attribute**:
   a. Abra a página **Configurações gerais**.
   b. Clique em **Variáveis** no painel de navegação à esquerda.
   c. Forneça as seguintes informações:
      a. **Nome:** digite um nome para a variável.
      b. **Tipo:** selecione o Tipo como **Personalizar**.
      c. **Values Separated by Comma:** digite o valor para qualquer atributo.

         NOTE
         Se você tiver usado parâmetros personalizados, deverá adicionar também as variáveis correspondentes.
7. Clique em **Atualizar**.

Mapear o painel

Depois de criar o painel, a próxima etapa será mapeá-lo usando o bloco **Painéis do DX** na página **Configurações** do **DX APM**.

Siga estas etapas:

1. Efetue logon no DX Application Performance Management.
2. Clique em **Configurações** no painel de navegação à esquerda.
3. Clique em **Painéis do DX** em **Configurações gerais**.
4. Clique em **Novo painel do DX**.
5. Forneça as seguintes informações:
   - **Ativo:** ative o painel.
   - **Nome da guia:** digite um nome para a guia do painel que ficará visível na Exibição da métrica.
   - **Pasta da árvore de métricas:**
     - **Expressão da pasta:** digite a expressão regular da pasta de métricas.

       NOTE
       Para o caminho completo, vá para a **Exibição da métrica**. Clique com o botão direito do mouse na pasta em que essa métrica está disponível e selecione **Copiar o caminho completo como RegExp**.
     - **Métricas filho:** digite a métrica que a pasta de métricas deve conter.
   - **Integração dos painéis do DX:**
     - **Nome do identificador:** digite o identificador do painel a ser mapeado.
     - **Parâmetros:** selecione os parâmetros necessários:
       - **De:** indica a hora de início atual.
       - **Até:** indica a hora de término atual.
       - **Agente:** indica o caminho do agente selecionado.
       - **Atributo:** indica o caminho do atributo selecionado.
   - **Opções avançadas:**

- **Pasta personalizada:** se você tiver salvado o painel em outra pasta, especifique o nome aqui. Para a pasta APM-MetricView, é possível deixar esse campo em branco.
- **Parâmetros personalizados:** se desejar usar os parâmetros personalizados, configure os valores dos seguintes itens:
  - **Nome do parâmetro:** o nome do parâmetro personalizado.
  - **Expressão regular:** a expressão regular que é usada para executar uma pesquisa para uma correspondência no caminho da pasta selecionada. Ela pode usar os grupos de captura (usando parênteses: ()) ou grupos de captura nomeados (usando esta sintaxe: (?<nome>pattern)).
  - **Valor:** especifique o grupo que deve ser usado utilizando o sinal $ Exemplos: $1, $2, $name.
  - **Valor padrão:** o valor padrão que será usado se nenhum valor for correspondido no caminho da pasta selecionada usando a expressão regular.

6. Clique em **Salvar**.
   O mapeamento foi concluído. Esta página exibe as seguintes informações para cada um dos mapeamentos:

- Nome da guia
- Condição
- Nome do identificador
- Active
- Ações (Exibir, Editar, Excluir)

Exibir o painel na exibição da métrica

Depois de mapear o painel no DX APM, o painel incorporado será exibido como uma guia se você selecionar qualquer métrica que corresponda à condição.

Siga estas etapas:

1. Efetue logon no DX APM.
2. Abra o bloco **Painéis do DX** na página **Configurações**.
3. Observe o caminho mencionado na coluna **Condição** para o caminho do painel.
4. Clique em **Exibição da métrica** no painel de navegação à esquerda.
5. Vá até o local e selecione a pasta de métricas.
   O painel será exibido como uma das guias.

Você pode criar painéis personalizados nos Painéis do DX usando as métricas do APM e incorporar esses painéis na página Exibição da métrica. Na Exibição da métrica, o painel incorporado aparecerá como uma guia se você selecionar qualquer métrica que corresponda à condição.

Para criar, mapear e exibir um painel personalizado na exibição de métricas, consulte Incorporar painéis do DX na exibição da métrica.

Usar a linha de tempo e o realce

A Linha de tempo permite a movimentação do modo dinâmico para o passado, para que seja possível ver quais eventos de status ocorreram historicamente. Os realces permitem identificar os componentes do mapa que compartilham um ou mais atributos.

Usar a linha de tempo

A Linha de tempo ajuda a investigar onde um problema começou. Use o controle deslizante da linha de tempo para ver o status dos componentes selecionados em períodos no passado. Alterne os eventos para ver eventos de mudança no intervalo de datas selecionado.

Siga estas etapas:

1. Clique em **Linha de tempo**.
   A linha de tempo será exibida. Por padrão, a linha de tempo está no modo dinâmico e mostra o resumo de alertas agregados dos últimos 8 minutos. O intervalo de datas é bloqueado e é atualizado a cada 30 segundos.
2. Para ativar o modo de **histórico**, selecione **DINÂMICO** e, em seguida, desative **Live Updates**. Selecione **Aplicar**.
   A seção azul-claro da linha de tempo mostra o período ativo. O mapa exibe o status e o ambiente no final do intervalo de datas. As barras de status nos nós mostram os resultados agregados desse período.
3. Altere o período arrastando e deslizando o período ativo na linha de tempo.
4. Altere a escala da linha de tempo usando a roda do mouse ou toques.
5. Selecione uma hora específica clicando na parte superior da linha de tempo.

   NOTE
   Clicar na parte superior da linha do tempo irá alterar a hora de término, mas manterá o intervalo de datas.

   Os eventos de status serão exibidos como ícones na linha de tempo. A exibição do Bloco de notas filtra eventos com base no problema ou na anomalia selecionados.Os resumos de alerta exibem os resultados agregados do período até a hora selecionada.

   TIP

   Em qualquer etapa, use os seletores de hora **START TIME** ou **END TIME** para selecionar uma hora específica.
6. Clique em um **nó** para ver os eventos desse nó no limite de tempo selecionado.
7. Selecione **Status**, **Em topologia** ou **Atributo** para incluir esses eventos de alteração na linha de tempo.

   NOTE

   A seleção do evento de mudança é redefinida ao abrir o Bloco de notas de análise.

   a. Clique em um **ícone de evento** ou no **ícone do grupo de eventos** para ver os detalhes do evento de mudança.
      Certifique-se de que o nó correto esteja selecionado no mapa.
      Os nós que não são afetados pelas alterações selecionadas aparecem esmaecidos no mapa.
   b. Clique em um **nó**.
   c. Clique no **ícone do evento de mudança**.
      Os detalhes do evento ou uma lista cronológica dos eventos do grupo serão exibidos no painel direito.

      NOTE

      A linha do tempo detecta automaticamente os novos componentes que são carregados no APM. Selecione **Status**, **Em topologia** ou **Atributo** para exibir eventos de mudança para novos componentes na linha do tempo.
8. Amplie e reduza a linha de tempo para alterar a escala.
   a. Arraste os controles deslizantes de início e término para definir o intervalo de datas necessário.
   b. Arraste o intervalo de datas ativo para períodos anteriores ou posteriores.
   c. Arraste a linha de tempo inativa (cinza) para mover o intervalo visível.
      Se o intervalo de datas ativo não estiver visível, clique no valor do tempo. O marcador de término do intervalo de datas ativo será movido para a hora selecionada. Defina datas e horas específicas usando os seletores de horas à esquerda.
9. Clique em um **evento individual** para ver os nós afetados no mapa. Os nós que não são afetados ficam esmaecidos. As barras de estado do nó mostram o estado agregado do período selecionado. O mapa mostra o ambiente do período selecionado.

Use o realce

Use o realce para identificar os componentes do mapa que compartilham um ou mais atributos. Uma lista mostra os atributos disponíveis para o realce com base nos atributos dos componentes da exibição atual do mapa.

Siga estas etapas:

1. Clique no ícone **Mapeamento** e, em seguida, clique em **Realçar**.
   Uma barra Realçar será expandida.
2. Clique no ícone de **adição** e selecione o atributo que deseja realçar.
3. (Opcional) Clique no atributo selecionado para classificar ou filtrar ainda mais.
   O mapa mostra o ambiente, incluindo todos os filtros aplicados. O mapa é exibido sob a perspectiva escolhida. O valor do atributo selecionado será exibido em amarelo.

A Linha de tempo ajuda a investigar onde um problema começou. Use o controle deslizante da linha de tempo para ver o status dos componentes selecionados em períodos no passado.

Os realces permitem identificar os componentes do mapa que compartilham um ou mais atributos.

Para obter mais informações sobre a Linha de tempo e o Realçamento, consulte Usar a linha de tempo e o realçamento.

Usar a linha do tempo e exibir eventos de mudança

A linha do tempo permite exibir os eventos de mudança que estão ocorrendo no momento e aqueles que ocorreram historicamente. A Linha de tempo ajuda a investigar onde um problema começou.

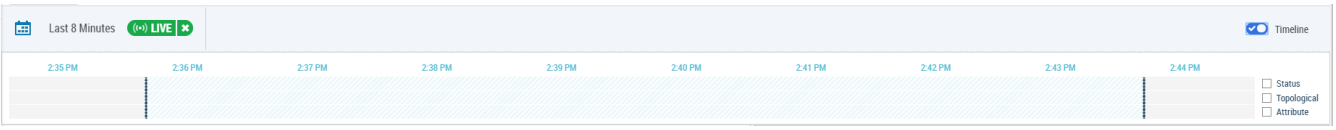
É possível exibir a linha do tempo nas seguintes exibições:

- Exibição da experiência
- Exibição de agentes
- Mapa
- Painéis
- Exibição da métrica

Este artigo contém os seguintes tópicos:

Ações disponíveis na linha do tempo

Quando você ativa a **Linha do tempo** em uma exibição, ela é exibida e a seção azul-clara na linha do tempo mostra o período ativo. A linha do tempo é atualizada a cada 30 segundos.



Você pode executar as seguintes ações na linha do tempo:

Mover a linha do tempo

Clique em qualquer lugar na área cinza da linha do tempo e arraste-a para exibir o tempo no passado, no presente ou no futuro.

Alterar o período ativo

Você pode selecionar a área azul-clara e arrastá-la para ajustar o período ativo. O período ativo está sempre entre a hora atual e a última hora.

Ajustar a escala

Para ajustar a escala ativa, selecione e mova as barras horizontais no final do período ativo. Você pode selecionar uma hora específica clicando na parte superior da linha do tempo ou em um valor de hora.Clicar em um valor de hora ou na parte superior da linha do tempo irá alterar a hora de término, mas irá manter o intervalo de datas.

Exibir nós e eventos afetados

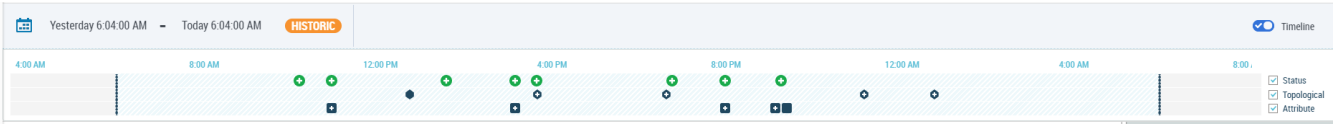
É possível exibir os nós e eventos afetados usando a linha do tempo, o **Mapeamento** ou a **Exibição de componentes**.

> **NOTE**
> A seção de eventos da **Exibição de componentes** será mostrada somente quando você marcar a caixa de seleção do(s) evento(s) na linha do tempo.

- **Ao usar a linha do tempo**
  Quando você selecionar um evento na linha do tempo, o nó no qual o evento ocorreu será realçado no **Mapeamento** ou **Painel** e os nós restantes serão exibidos esmaecidos.
  Se o painel **Exibição de componentes** estiver visível, o(s) evento(s) que você selecionar na linha do tempo será(ão) exibido(s) no destaque amarelo da seção de eventos do painel.
- **Ao usar o mapeamento**
  Quando você selecionar um ou vários nós no **Mapeamento**, os eventos correspondentes serão exibidos na respectiva seção *somente* quando o painel **Exibição de componentes** estiver visível.
- **Ao usar o painel Exibição de componentes**
  Para executar qualquer ação no painel **Exibição de componentes**, certifique-se de que ele esteja visível.
  Para o(s) nó(s) que você selecionar no **Mapeamento**, o painel exibirá todos os eventos relacionados na respectiva seção.A seleção de um evento na linha do tempo fará com que os eventos correspondentes sejam realçados em amarelo na seção de eventos do painel.Da mesma forma, quando você selecionar um evento na seção de eventos no painel, o nó correspondente será centralizado e realçado no **Mapeamento**.

Exibir eventos de mudança na linha do tempo

Nas exibições **Mapeamento**, **Painéis** e bloco de notas, é possível selecionar e exibir os seguintes eventos de mudança: **Status**, **Em topologia** ou **Atributo** na linha do tempo. A exibição do Bloco de notas filtra eventos com base no problema ou na anomalia selecionados.A linha do tempo detecta automaticamente os novos componentes que são carregados no DX APM.Os eventos de mudança estão disponíveis quando a linha do tempo está exibindo dados dinâmicos ou históricos.Os eventos de mudança selecionados aparecem como ícones na linha do tempo.



> **NOTE**
> A seleção do evento de mudança é redefinida ao abrir o Bloco de notas de análise.

Na exibição **Mapeamento**, os detalhes dos eventos estão disponíveis na **Exibição de componentes**.

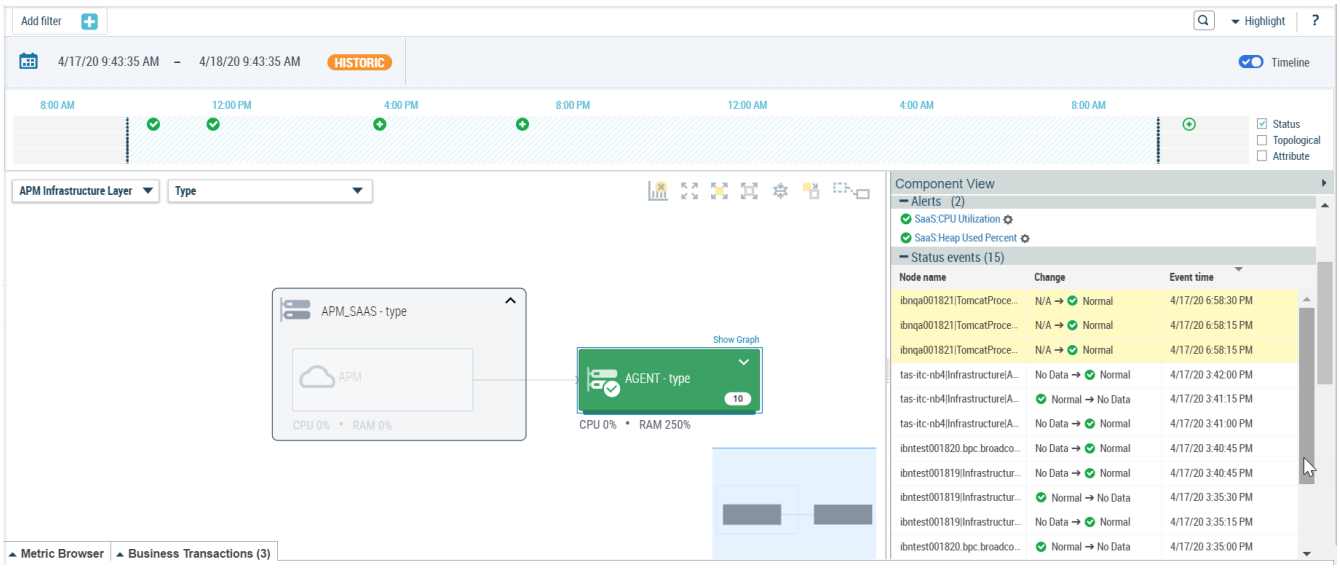
Eventos de mudança de status

Na exibição **Mapeamento** ou **Painéis**, selecione um nó e, em seguida, marque a caixa de seleção **Status** na linha do tempo para exibir os eventos de mudança de status.

Na imagem abaixo, é possível ver que um nó está selecionado no **Mapeamento** e que a caixa de seleção **Status** está marcada na linha do tempo. Como resultado, é possível exibir os eventos de mudança de status como ícones na linha do tempo, o que representa a hora em que a mudança de status ocorreu para o nó selecionado.

Quando você selecionar um nó no **Mapeamento**, todos os eventos relacionados serão exibidos na seção de eventos do painel **Exibição de componentes**, mas *somente* se ele estiver visível. Você pode exibir detalhes do status, como quando o nó foi alterado de normal para um estado em que ele não estava recebendo dados. Além disso, a seleção de

qualquer evento na linha do tempo fará com que esses eventos sejam realçados em amarelo na seção de eventos do painel.

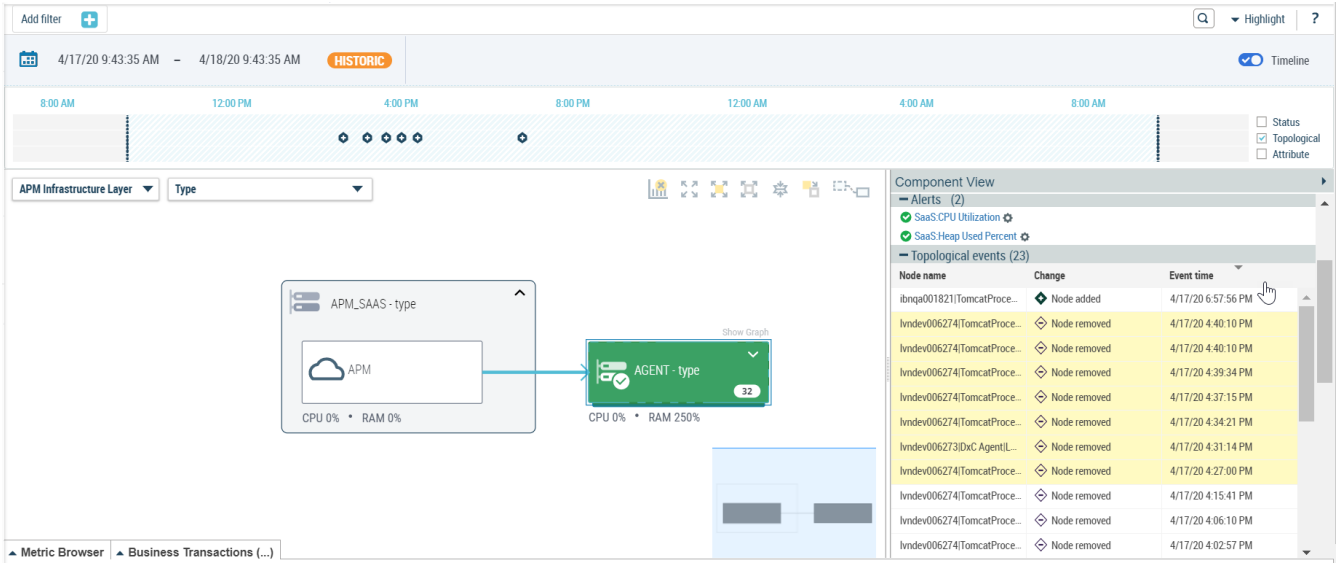


Eventos de mudança topológicos

Na exibição **Mapeamento** ou **Painéis**, selecione um nó e, em seguida, marque a caixa de seleção **Em topologia** na linha do tempo para exibir os eventos de mudança de topologia.Você pode exibir detalhes, como quando o nó foi removido ou adicionado à topologia.

Na imagem abaixo, é possível ver que um nó está selecionado no **Mapeamento** e que a caixa de seleção **Em topologia** está marcada na linha do tempo. Como resultado, é possível exibir os eventos de mudança de topologia como ícones na linha do tempo, o que representa quando a mudança na topologia ocorreu para o nó selecionado.

Quando você selecionar um nó no **Mapeamento**, todos os eventos relacionados serão exibidos na seção de eventos do painel **Exibição de componentes**, mas *somente* se ele estiver visível.Todos os eventos de mudança de topologia que tiverem ocorrido no nó serão listados na seção **Eventos topológicos** da **Exibição de componentes**.Além disso, a seleção de qualquer evento na linha do tempo fará com que esses eventos sejam realçados em amarelo na seção de eventos do painel.

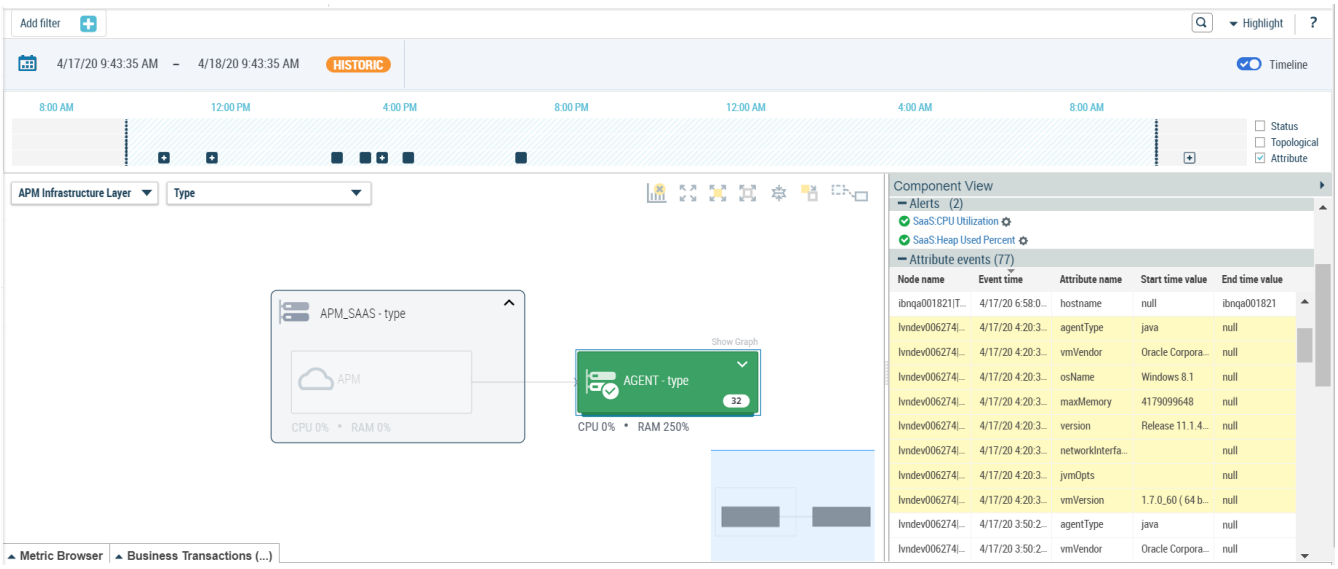


Eventos de mudança de atributo

Na exibição **Mapeamento** ou **Painéis**, selecione um nó e, em seguida, marque a caixa de seleção **Atributo** na linha do tempo para exibir os eventos de mudança de atributo.Você pode exibir detalhes, como quando o atributo foi adicionado, o nome e o valor no início e no fim.

Na imagem abaixo, é possível ver que um nó está selecionado no **Mapeamento** e que a caixa de seleção **Atributo** está marcada na linha do tempo. Como resultado, é possível exibir os eventos de mudança de atributo como ícones na linha do tempo, o que representa quando o atributo foi criado para o nó selecionado.

Quando você selecionar um nó no **Mapeamento**, todos os eventos relacionados serão exibidos na seção de eventos do painel **Exibição de componentes**, mas *somente* se ele estiver visível.Todos os eventos de mudança de atributo que tiverem ocorrido no nó serão listados na seção **Eventos do atributo** da **Exibição de componentes**.Além disso, a seleção de qualquer evento na linha do tempo fará com que esses eventos sejam realçados em amarelo na seção de eventos do painel.Para adicionar um atributo personalizado, você deve estar no modo dinâmico.



A linha do tempo permite exibir os eventos de mudança que estão ocorrendo no momento e aqueles que ocorreram historicamente, e também ajuda a investigar onde o problema começou. A linha do tempo pode ser vista nas seguintes exibições: Exibição da experiência, Exibição de agentes, Mapa, Painéis e Exibição da métrica.

Para obter mais informações sobre as ações disponíveis e exibir eventos de mudança na linha do tempo, consulte Usar a linha do tempo e exibir eventos de mudança.

Usar os atributos no DX APM

Os atributos são marcas ou rótulos que os agentes coletam dos componentes em seu ambiente de aplicativos.Use esses atributos para exibir o mapa de diferentes perspectivas, filtrar os componentes e realçá-los. Os atributos facilitam a diferenciação dos componentes e identificam seus relacionamentos com outros componentes.Cada atributo tem um nome e um valor.

O DX APM coleta os atributos básicos para cada componente. Os administradores podem criar atributos personalizados definindo regras de atributo. Para obter mais informações sobre a criação de atributos personalizados, consulte Definir a forma de monitoramento do ambiente com regras de atributo.

NOTE

Todos os atributos se aplicam ao DX APM, e apenas alguns atributos se aplicam ao DX APM local.

Visão geral

Todos os componentes no mapeamento contêm um conjunto de atributos. O DX APM distingue os seguintes tipos de atributo:

- Os **atributos comuns** são agrupados automaticamente pelo DX APM e existem para a maioria dos componentes.
- Os **atributos personalizados** permitem definir e coletar informações adicionais usando regras de atributo.
- Os **atributos de agente** fornecem informações sobre componentes específicos que os agentes instalados monitoram.
- Os **atributos de extensão** fornecem informações adicionais que as extensões de agente coletam.

Os atributos disponíveis para uso em filtros e perspectivas são exibidos na lista suspensa de atributos.

> **NOTE**
>
> **Mais informações:**
>
> - Organizar componentes usando perspectivas
> - Identificar áreas problemáticas usando filtros
> - Monitorar a integridade geral do ambiente com o painel

Atributos comuns

O DX APM reúne os seguintes atributos comuns:

- `name`
  Define o nome do componente. Esse atributo é derivado de um ou mais atributos.
- `type`
  (Vértice)
  Indica o tipo do componente do vértice.
- **`Source cluster`** Define o agrupamento do APM ao qual o componente se reporta.
- `agent`
  Define o identificador do agente (`hostname|process|agentName`). Esse atributo mostra a origem do vértice.
- `hostname`
  Define o nome do host ou do recipiente em que o componente é executado.
- `agentDomain`
  Define o domínio do agente.
- `processedBy`
  Indica o nome da classe que processou e criou esse componente. Esse atributo geralmente é originado de um rastreamento de transações.
- `applicationName`
  Define o nome do aplicativo. Localize `applicationName` na descrição da implantação do aplicativo web ou verifique o caminho da métrica `Front-ends|Apps|<nome_do_aplicativo>` do agente.
- `containerId`
  (Docker) Indica a ID do recipiente do Docker. A `containerID` fica visível na Camada de aplicativo.

  > **NOTE**
  >
  > Essa ID estará presente apenas se o agente do Java, Node JS, PHP ou Python for executado no recipiente.
- `remotePort`
  Indica a porta remota que o componente chama.
- `backendNode`
  Será mostrado como `true` se o vértice for um componente de back-end em um aplicativo.
- `remoteName`

Indica o nome do host remoto que o componente chama.

- `localAddress`
  Define o endereço IP local do componente.
- `serviceId`
  Identifica o serviço de negócios definido no CEM.
- `Experience`
  Indica o nome da experiência, conforme mostrado na exibição da experiência, por exemplo, "Apps|ActivityService|URLs|/api/v1/ em serv17.ca.com (GENERICFRONTEND)". Esse atributo existirá apenas se o valor do atributo `IsExperience` for `true` . Para obter mais informações sobre as experiências, consulte Monitorar o desempenho usando a Exibição da experiência.
- `IsExperience`
  Indica que o vértice é uma experiência ou o componente mais à esquerda do mapeamento. Para obter mais informações sobre as experiências, consulte Monitorar o desempenho usando a Exibição da experiência.
- `remoteAddress`
  Indica o endereço IP remoto que o componente chama.
- `inferredBackendNode`
  Será mostrado como true se esse vértice tiver sido inferido de uma ou mais conexões com este componente de back-end.
- `provider`
  Indica o provedor do banco de dados ou o fornecedor, por exemplo, "Postgres DB", "Oracle DB" ou "Derby DB".
- **`port`**
  Indica a porta de escuta do banco de dados ou do EM (Enterprise Manager - Gerenciador Corporativo).

Atributos personalizados

Os administradores podem criar atributos personalizados nos componentes para que os usuários possam exibir as perspectivas e filtrar o mapa de acordo com os componentes que compartilham um nome de atributo. Você pode adicionar um atributo personalizado a um componente individual ou a uma regra de atributo. Os atributos personalizados permitem aos usuários identificar e relacionar componentes específicos com facilidade. Os analistas exibem as perspectivas e filtram o mapa de acordo com os componentes que compartilham o nome do atributo.O Application Performance Management permite filtrar por qualquer valor de atributo. Os atributos designados aos componentes de uma camada específica do DX APM também são visíveis em outras camadas.

NOTE

Mais informações:

- Definir a forma de monitoramento do ambiente com regras de atributo
- Camadas do mapa

Atributos de agente

Os agentes Java e Node.js coletam apenas os atributos comuns.

Atributos de extensão

As extensões do Infrastructure Agent coletam atributos para componentes específicos da infraestrutura. Consulte os links abaixo para obter uma lista completa dos atributos de extensão disponíveis.

NOTE

Mais informações:

- Amazon Web Services
- Atributos do Azure
- Atributos do Docker
- Configurar atributos personalizados do Docker
- Atributos e métricas do F5 LTM
- Atributos de monitoramento de host
- Atributos do Kubernetes
- Atributos do OpenShift

Os atributos são marcas ou rótulos que os agentes coletam dos componentes em seu ambiente de aplicativos. Use esses atributos para exibir o mapa de diferentes perspectivas, filtrar os componentes e realçá-los. Os atributos facilitam a diferenciação dos componentes e identificam seus relacionamentos com outros componentes. Cada atributo tem um nome e um valor.

Para obter mais informações sobre os atributos, consulte Usar atributos no DX APM.

Organizar componentes usando perspectivas

As perspectivas permitem agrupar componentes no **Mapeamento** e no **Painel** sem removê-los do conjunto de dados. É possível criar perspectivas pessoais que sejam exclusivas para os seus universos.Selecione um ou mais atributos compartilhados para agrupar os componentes. Os administradores do DX APM podem criar e editar mais perspectivas públicas, que estão disponíveis para todos os usuários.As perspectivas OOTB (Out-of-the-box - Prontas para Uso) exibem os componentes de aplicativos e de infraestrutura das pilhas de tecnologia e dos serviços de hospedagem no ambiente de aplicativos.

Visão geral

A lista suspensa Perspectivas está localizada no **Mapeamento** e no **Painel**. O quadro exibe a perspectiva atual que está aplicada. Expanda a lista suspensa para ver as perspectivas definidas.

- As perspectivas pessoais são exibidos acima da linha.
- As perspectivas públicas, que o administrador define, são exibidas abaixo da linha.
- As perspectivas prontas para uso, que mostram os relacionamentos entre os componentes existentes nas camadas, são exibidas abaixo da linha. As seguintes perspectivas são definidas como prontas para uso:

Camada do mapa	**Perspectiva pronta para uso**							
Camada do aplicativo	Type	Padrão	Hostname	Usuário final, aplicativo	Localização	Proprietário	Jenkins	Infraestrutura de aplicativos
Camada de infraestrutura do APM	Type							
Camada de infraestrutura	Type	Padrão						
Camada de rede	Type							

A última perspectiva da lista suspensa é sempre `Nenhuma perspectiva` , que mostra todos os componentes separadamente. Combine uma perspectiva com os filtros para remover componentes indesejados do **Mapeamento** e do **Painel**.

NOTE

A perspectiva padrão na Camada do aplicativo não compartilha os mesmos atributos com a perspectiva padrão na Camada de infraestrutura.

Usar perspectivas OOTB

Use as perspectivas OOTB para exibir componentes de aplicativo e seus componentes de infraestrutura associados.

Siga estas etapas:

1. Vá para o **Mapeamento** ou **Painel**.
2. Exiba componentes de infraestrutura e aplicativo.
   Para exibir os componentes de infraestrutura de um componente específico do aplicativo:
   a. Selecione **Camada do aplicativo** na lista suspensa superior.
   b. Selecione a lista suspensa **Perspectivas** e selecione **Infraestrutura do aplicativo**.

      NOTE

      Se seu ambiente de aplicativos usar recipientes do Docker, selecione essa perspectiva para ver os recipientes, hosts e instâncias de servidor associados do Docker.
   c. Selecione um componente de aplicativo no **Mapeamento** ou **Painel** para exibir os componentes de infraestrutura relacionados.
3. Exiba mais informações sobre os componentes na **Exibição de componentes**, que é exibida ao lado do **Mapeamento**.

Você usou uma perspectiva pronta para uso para exibir os relacionamentos entre os componentes existentes em camadas.

Criar uma perspectiva pessoal

As perspectivas permitem agrupar os componentes do mapa de acordo com a um atributo específico. Os componentes que compartilham um valor desse atributo aparecem no Mapeamento em grupos discretos. Por exemplo, a perspectiva `Localização` tem três grupos:

- Todos os componentes com o valor `London`
- Todos os componentes com o valor `Prague`
- Todos os componentes com o valor `New York`

Usuários individuais criam e personalizam grupos de perspectivas pessoais.

Siga estas etapas:

1. Selecione **Perspectivas** no painel esquerdo.
2. Selecione **Criar perspectiva**.
3. Dê um nome à perspectiva.
4. Selecione cada **camada aplicável** em que deseja que a perspectiva fique visível.
5. (Opcional) Em **Visibilidade**, ative as opções necessárias:
   – Selecione a caixa **Pública** para ativar os direitos de visibilidade para outros usuários.
   – Selecione a caixa **Agrupamento automático** para reorganizar os vértices do mapa em grupos padrão.
6. Na **Hierarquia do agrupamento**, selecione ao menos um atributo.
   Clique em **Adicionar atributo** para aplicar atributos adicionais para agrupar os vértices. Observe que cada atributo pode ser adicionado apenas uma vez.
   Se você ativou a opção **Agrupamento automático**, o agrupamento padrão será aplicado primeiro aos vértices, seguido dos atributos selecionados na seção **Hierarquia de agrupamento**. Os atributos na seção **Hierarquia**

de agrupamento são aplicados na ordem de cima para baixo. Se você excluir qualquer atributo, a lista será reorganizada e os atributos serão aplicados na nova ordem de cima para baixo.

Clique no botão referente a um atributo e arraste e solte para classificar ou reorganizar os atributos na hierarquia. A ordem dos atributos é importante, pois define a ordem em que os filtros serão aplicados e, consequentemente, o agrupamento de vértices.

NOTE

Os atributos são listados sob a camada correspondente. É possível selecionar atributos a partir de camadas que não foram selecionadas como as **Camadas aplicáveis** para uma determinada perspectiva.

7. (Opcional) Crie um grupo de perspectivas de vários níveis. Selecione outros atributos.
8. Selecione **Salvar**.

A perspectiva é exibida na lista suspensa **Perspectivas** no **Mapa** quando uma camada correspondente é selecionada.

Personalizar uma perspectiva pública

O administrador cria grupos de perspectivas públicas. Esses grupos estão disponíveis para todos os usuários do APM. É possível personalizar uma perspectiva pública.

Siga estas etapas:

1. Selecione **Perspectivas** no painel esquerdo.
2. Identifique a perspectiva pública que você deseja personalizar e selecione **Editar**.
   Uma janela pop-up é exibida.
3. (Opcional) Altere o nome da perspectiva.
4. (Opcional) Selecione uma camada diferente ou adicione outras camadas onde deseja que a perspectiva fique visível. Para obter mais informações, consulte Camadas do mapeamento.
5. Na **Hierarquia do agrupamento**, selecione ao menos um atributo.
6. (Opcional) Crie um grupo de perspectivas de vários níveis. Selecione outros atributos.
7. (Opcional) Selecione **+** para adicionar mais atributos ao grupo de perspectivas.
8. Selecione **Salvar**.

Você personalizou uma perspectiva pública. A perspectiva que você criou é pessoal. Você pode editar ou excluir a perspectiva pessoal. A perspectiva é exibida na lista suspensa **Perspectivas** do **Mapeamento**.

Editar uma perspectiva pessoal

Siga estas etapas:

1. Selecione **Perspectivas** no painel esquerdo.
2. Selecione a perspectiva pessoal e selecione **Editar**.
   Uma janela pop-up é exibida.
3. (Opcional) Altere o nome da perspectiva.
4. (Opcional) Selecione uma camada diferente ou adicione outras camadas onde deseja que a perspectiva fique visível. Para obter mais informações, consulte Camadas do mapeamento.
5. Na **Hierarquia do agrupamento**, selecione ao menos um atributo.
6. (Opcional) Crie um grupo de perspectivas de vários níveis. Selecione outros atributos.
7. (Opcional) Selecione **+** para adicionar mais atributos ao grupo de perspectivas.
8. Selecione **Salvar**.

Você editou a perspectiva pessoal.

Excluir uma perspectiva pessoal

Siga estas etapas:

1. Selecione **Perspectivas** no painel esquerdo.
2. Identifique a perspectiva pessoal e selecione **Excluir**.
3. Uma janela pop-up de confirmação será exibida. Selecione **Sim**.

Você excluiu a perspectiva pessoal.

As perspectivas permitem agrupar componentes no Mapeamento e no Painel sem removê-los do conjunto de dados. É possível criar perspectivas pessoais que sejam exclusivas para os seus universos. Selecione um ou mais atributos compartilhados para agrupar os componentes. Os administradores do DX APM podem criar e editar mais perspectivas públicas, que estão disponíveis para todos os usuários.

Para obter mais informações sobre perspectivas, consulte Organizar componentes usando perspectivas.

Exibir relacionamentos entre os componentes do mapa

O mapa usa componentes como nós, alertas, painel de detalhes e a visão geral de desempenho. Os grupos de componentes mostram as informações de status agregadas para todos os componentes desse grupo. O mapa mostra os relacionamentos entre componentes individuais dentro do ambiente. O Paciente zero é o primeiro componente de uma série de dependências que indica problemas de desempenho. Esse componente parece ser a origem da degradação do desempenho em seu ambiente de aplicativos.

Mapa

O mapa mostra o status do alerta, o nome e o tipo de ícone para cada componente. O DX APM coleta as informações do Enterprise Manager e as exibe em cada nó.

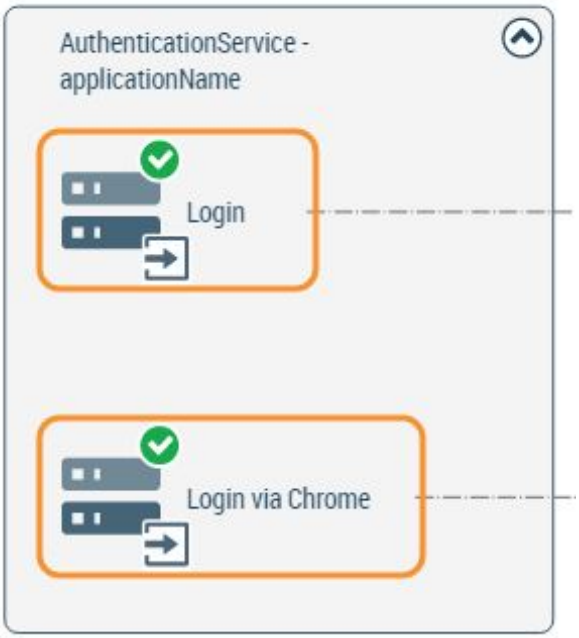
Várias opções permitem restringir o foco no mapa, por exemplo, você pode:

- Selecionar diferentes perspectivas para exibir o mapa.
- Usar filtros para focar em componentes específicos.
- Usar a Exibição de componentes para ver alertas, métricas e atributos de cada nó no mapa. Selecione as guias para exibir informações de outras camadas do mapa.
- Usar a linha do tempo para comparar informações atuais e históricas. A linha do tempo apresenta marcadores que mostram quando as mudanças no alerta, na topologia e no atributo ocorreram e você pode inspecionar essas alterações. As informações são calculadas pelo período especificado na linha do tempo. No modo dinâmico, o período de agregação é de 8 minutos.

O DX APM oferece suporte ao Permalink, que contém todos os detalhes da página quando você exibe o URL. É possível enviar o URL da página para qualquer outro usuário. Esse usuário vê a mesma exibição. Você também pode marcar esses URLs para retornar à mesma exibição em uma sessão posterior.

Front-end como uma experiência

O nó da experiência é o primeiro componente de front-end monitorado e contém um atributo chamado Experience. O nó Experience é o início do caminho da transação. O Experiencie pode, por exemplo, ser um servlet ou um front-end genérico. O Mapa mostra um nó de experiência com um ícone de seta. O exemplo mostra um nó de experiência *Logon* e um nó de experiência *Logon via Chrome*.



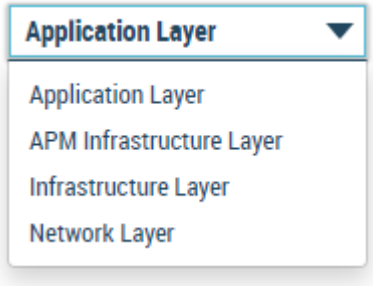
NOTE
Nem todo front-end é uma experiência. A maioria dos nós de front-end aparece no meio de uma transação e, portanto, não são experiências.

Entender o mapa

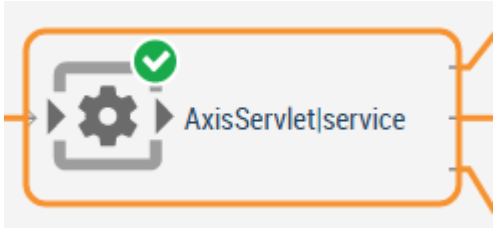
Use o exemplo de fluxo de trabalho a seguir para saber mais sobre o mapa. O mapa é atualizado para mostrar a nova topologia a cada 5 minutos por padrão. Esse recurso é configurável. Os componentes novos são mostrados com uma borda azul e os componentes removidos são mostrados com uma borda pontilhada azul.

Siga estas etapas:

1. Selecione a **Camada de aplicativo** para ver os componentes do Mapeamento.Os componentes correspondem aos cartões de Experiência e Exibição da experiência.

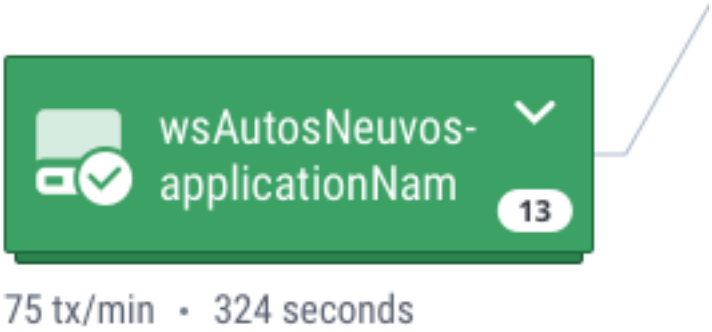


2. Procure os nós e coloque o ponteiro do mouse sobre um nó para ver mais informações.
   O nó é uma representação dos componentes de software diretamente monitorados ou agregados e de transações comerciais no contexto topológico. O mapa oferece suporte a até 50.000 nós. Se o número de nós a serem mostrados no mapa for grande o suficiente para causar problemas de desempenho, o mapa agrupará os nós automaticamente. Os grupos não representam qualquer perspectiva ou atributo específico. Por padrão, o agrupamento automático ocorrerá quando o número de nós a serem mostrados for acima de 150. Adicione filtros ou defina perspectivas para reduzir o número de nós do mapa a ser mostrado.O gráfico de status mostra o último status no final do intervalo selecionado que é relatado para esse componente ou grupo.



Para saber qual tipo de dispositivo um nó representa, coloque o ponteiro do mouse sobre o ícone próximo ao nome do dispositivo.

No exemplo a seguir, um grupo de nós compartilha o atributo `applicationName` .



- O número 13 indica que o grupo inclui 13 nós.
- 75 tx/min indica respostas por intervalo
- 324 segundo indica o tempo médio de resposta

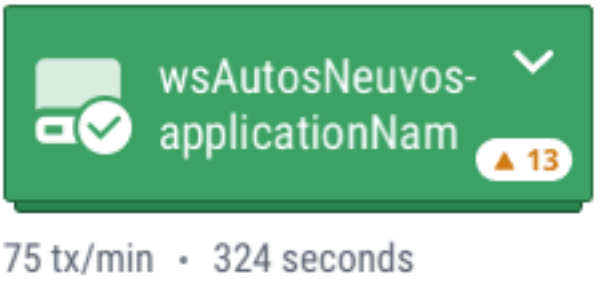
3. Identifique as conexões:
   As conexões do mapa podem conter componentes de back-end.
   O APM reconhece as seguintes conexões:
   - **Linha sólida** - existe um componente de back-end na conexão. Selecione a conexão para ver as propriedades do componente de back-end na Exibição de componentes.
   - **Linha cinza tracejada** - não existe componente de back-end na conexão. A conexão não é clicável.
   - (Somente a Camada de infraestrutura) **Linha cinza pontilhada** - a linha entre dois nós significa que o primeiro nó contém o segundo nó.
   - (Somente a Camada de infraestrutura) **Linha cinza** - a linha entre dois dockers significa que o primeiro docker está relacionado ao segundo docker.

   A cor da linha cheia indica o status do alerta do componente de back-end:
   - **Linha cinza** - Nenhum alerta é definido no componente de back-end.
   - **Linha verde** - todos os alertas no componente de back-end são verdes.
   - **Linha amarela** - existe pelo menos um alerta amarelo e nenhum alerta vermelho no componente de back-end.
   - **Linha vermelha** - existe pelo menos um alerta vermelho no componente de back-end.
   - **Linha laranja** - A linha significa um rastreamento de transação.
4. Agrupe componentes na camada selecionada para encontrar problemas de desempenho para os componentes de infraestrutura compartilhada (componentes entre camadas).

A cor do ícone do grupo indica o status do alerta do componente entre camadas:

- **Ícone cinza** - existe pelo menos um alerta verde para o componente entre camadas que agrupa componentes da camada selecionada.
- **Ícone vermelho** - existe pelo menos um alerta vermelho para o componente entre camadas que agrupa componentes da camada selecionada.
- **Ícone amarelo** - existe pelo menos um alerta amarelo para o componente entre camadas que agrupa componentes da camada selecionada.

No exemplo a seguir, os grupos de agentes compartilham um host. O número 13 indica um componente do host e 12 componentes do agente. O triângulo laranja representa um aplicativo em um estado de cuidado:



5. Coloque o ponteiro do mouse sobre um componente para ver o rastreamento de transação.
   O rastreamento de transação mostra todos os componentes que uma transação vincula ao fluxo ativo e inativo. Coloque o ponteiro do mouse sobre um nó de experiência para ver o caminho completo da transação destacado.
6. Alterne entre as camadas do Mapa.
   - Selecione **Camada de infraestrutura do APM** para ver Gerenciadores corporativos e Agentes no Mapeamento. A exibição corresponde à Exibição de agentes. Use essa exibição se desejar ver, por exemplo, quais Gerenciadores corporativos estão em execução e quais agentes estão conectados. Ao detalhar de um cartão de Agente para a Exibição de isolamento, o Mapa mostrará a camada de infraestrutura do APM.
   - Selecione **Camada de infraestrutura** para ver a infraestrutura de rede do seu ambiente, incluindo Monitores de Docker.

     NOTE
     Para obter mais informações sobre as camadas do mapa, consulte Camadas do mapa.
7. Selecione **Navegador de métricas** para abrir a Exibição da métrica.

Investigar transações comerciais

A Exibição de mapa ajuda a encontrar componentes a serem monitorados. Na guia Transações comerciais, é possível exibir detalhes e resumos do rastreamento de transação relacionado. Essas informações ajudam a entender o desempenho da transação e a resolver o desempenho ineficaz, identificando quando, onde e por que o desempenho está diminuindo.

Siga estas etapas:

1. Selecione os nós individuais ou grupos de nós até o máximo de 1.000 nós.
2. Selecione a guia **Transações comerciais**.
   Uma lista de resumo mostra os rastreamentos correspondentes ao componente no intervalo selecionado na linha do tempo. Os rastreamentos mostram os tempos de duração. Os rastreamentos são codificados por cor para indicar qualquer problema associado a uma transação, por exemplo, vermelho indica um erro. É possível identificar os métodos problemáticos observando a duração do rastreamento. Rastreamentos inesperadamente longos são causas prováveis de transações lentas.

     NOTE
     A lista é atualizada automaticamente quando você usa o modo Dinâmico.

3. Investigar o baixo desempenho das transações.

NOTE

Mais informações:

- Organizar componentes usando perspectivas
- Identificar áreas problemáticas usando filtros
- Monitorar o desempenho usando a Exibição da experiência

O mapa usa componentes como nós, alertas, painel de detalhes e a visão geral do desempenho para mostrar os relacionamentos entre componentes individuais dentro do ambiente. Os grupos de componentes mostram as informações de status agregadas para todos os componentes desse grupo.

Para obter mais informações sobre o mapa e sua relação com os componentes, consulte Exibir relacionamentos entre componentes no mapa.

Camadas do mapeamento

Como administrador, você pode navegar rapidamente pelas camadas do mapa a fim de identificar a causa raiz dos problemas de desempenho. Alterne entre as camadas no mapeamento para exibir os problemas de desempenho causados por componentes do aplicativo, componentes da infraestrutura ou componentes do DX APM. Aplique mais filtros para exibir tipos específicos de componente dentro das camadas. Refine o número e os tipos de componente em grupos fáceis de usar (universos).

Visão geral

As camadas do mapa sobrepõem diferentes tipos de componente do ambiente no mapa. O mapa mostra componentes e conexões de componentes que estão dentro da camada selecionada. As conexões entre componentes das diferentes camadas são chamadas de conexões entre camadas. Os componentes que têm conexões entre camadas com componentes dentro da camada selecionada são exibidos na **Exibição de componentes** à direita. Por exemplo, quando você seleciona um componente de servlet no mapa, a **Exibição de componentes** mostra as propriedades do servlet com as propriedades do agente que monitora o servlet.As conexões entre camadas também podem ser exibidas no mapa usando os filtros de atributo entre camadas. Para obter mais informações, consulte Definir a forma de monitoramento do ambiente com regras de atributo.

NOTE

O DX APM adiciona automaticamente conexões entre camadas entre os agentes e os componentes de aplicativo que os agentes monitoram.

Usar camadas do mapa

Alterne entre as camadas do mapa para exibir componentes de uma camada específica. Selecione um componente no mapa e veja as conexões entre camadas na **Exibição de componentes**.

Siga estas etapas:

1. Selecione uma camada do mapa na lista suspensa. Escolha dentre as seguintes camadas:
   - **Camada do aplicativo**
     Mostra os componentes de aplicativo que os agentes do APM monitoram. Essa camada corresponde aos componentes do mapa das versões anteriores do APM.
   - **Camada de infraestrutura do APM**
     Mostra os componentes do APM, como agentes e coletores.
   - **Camada de infraestrutura**

Mostra hosts, instâncias do docker e outros componentes físicos. Essa camada contém informações dos Infrastructure Agents e suas extensões. A camada de infraestrutura também coleta informações de integrações, por exemplo, do CA UIM (Unified Infrastructure Management).

NOTE

O DX APM local permite integrar componentes de outros sistemas à camada de infraestrutura usando a API REST. O CA UIM usa essa API REST para se integrar ao DX APM local de modo que o DX APM local mostre componentes de hardware.

– **Camada de rede**
Mostra os elementos de rede da nuvem, como VPC (Virtual Private Cloud - Nuvem Privada Virtual), roteadores, interconexões, sub-redes e outros elementos de VPCs da nuvem. Essa camada contém informações dos Infrastructure Agents e suas extensões de nuvem.

NOTE
Para ver os serviços de monitoramento das extensões de nuvem do GCP na camada de rede, configure os serviços do GCP, como o Google Virtual Private Cloud, o Google Cloud Interconnect e o Google Cloud Router. Para obter mais informações, consulte Configurar a extensão do Google Cloud Platform.

2. Selecione um componente no mapa para abrir a **Exibição de componentes**.
3. Alterne entre as guias na **Exibição de componentes** para ver as propriedades do componente selecionado e dos componentes conectados de outras camadas.

Aplicar filtros nas camadas do mapa

Um filtro é uma lista de atributos e valores obrigatórios que permite exibir componentes específicos no mapa. Aplique um filtro para exibir todos os componentes da camada de filtragem que correspondem aos atributos de filtro. Se você alternar entre as camadas, os componentes que têm conexões entre camadas com os componentes filtrados permanecerão visíveis no mapa.

Para aplicar um filtro no mapa, selecione um atributo de filtro da lista de atributos.

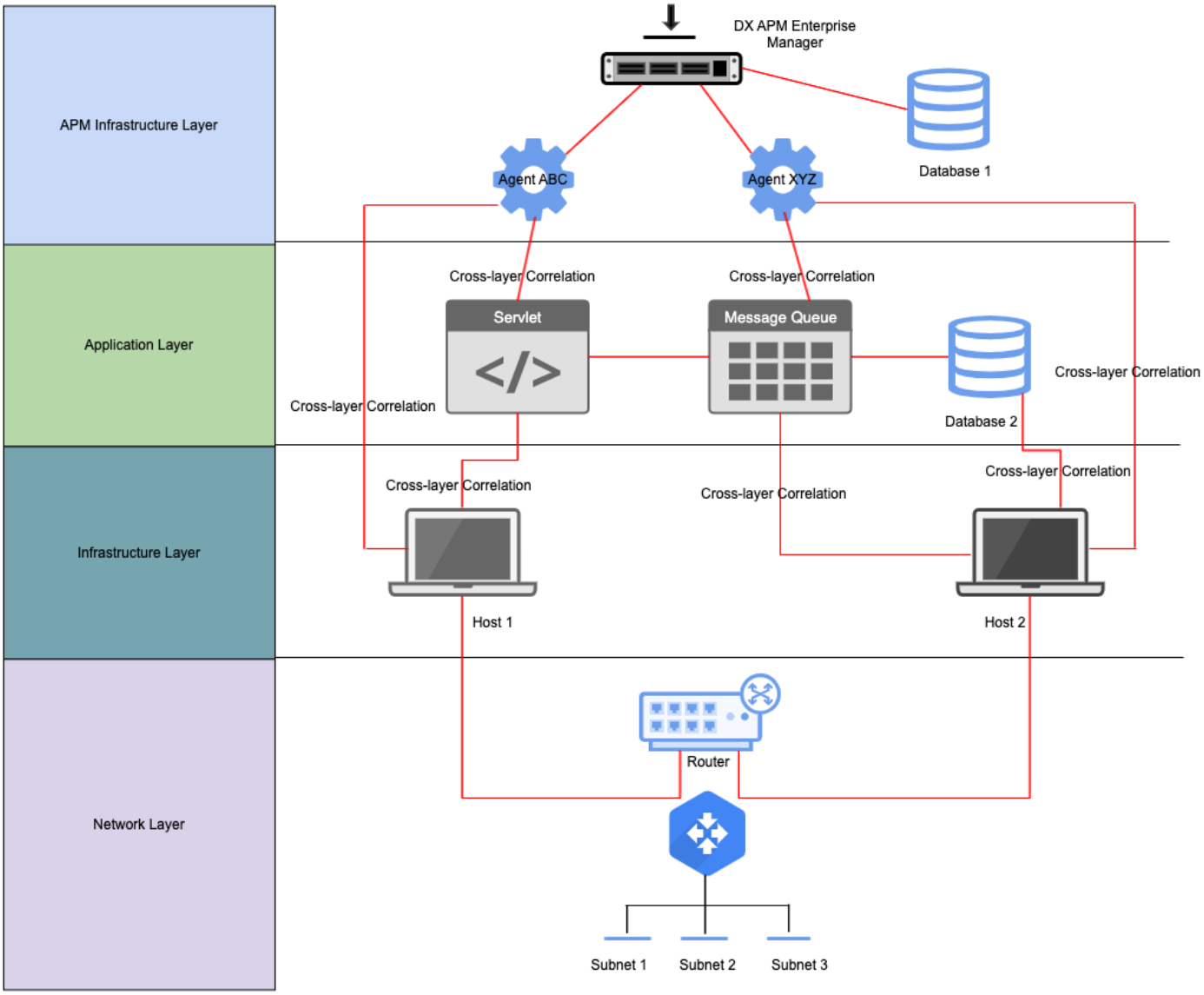
NOTE

Os atributos são listados sob a camada correspondente. É possível selecionar atributos de mais de uma camada.

Exemplo:

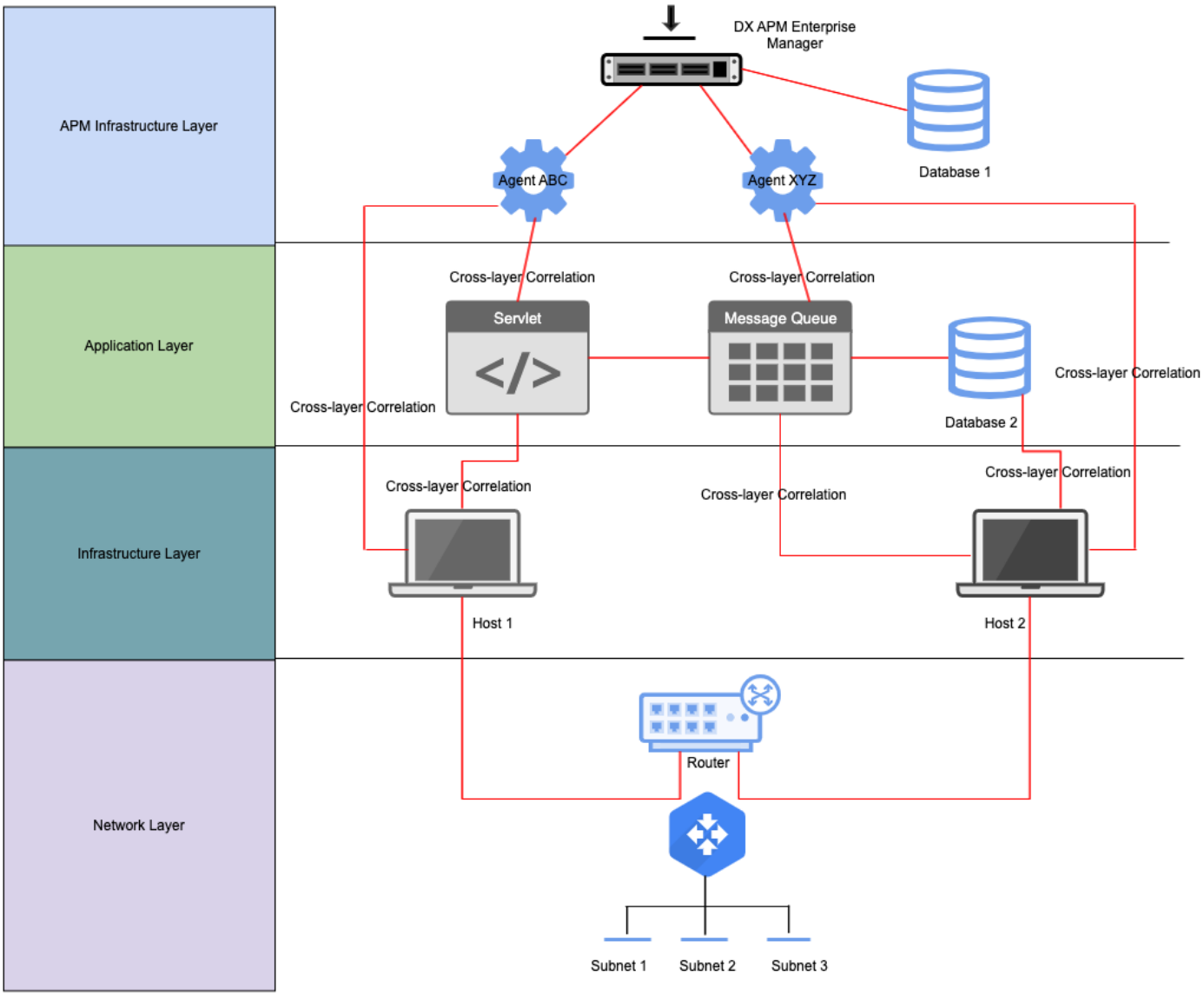
O seguinte diagrama mostra um mapa não filtrado que contém várias conexões entre camadas:

Figure 6: camada do mapeamento 1



Ação:
Na Camada de infraestrutura do APM, é possível definir o filtro para retornar agentes com 'ABC' e 'XYZ' nos nomes.

Resultado: o diagrama a seguir mostra os resultados filtrados para cada camada do mapeamento:



NOTE

A Camada de infraestrutura do APM não mostrará coletores nem bancos de dados do EM quando a camada de filtragem for a Camada do aplicativo. Os coletores e bancos de dados do EM não têm conexões entre camadas com componentes de aplicativo. Somente os componentes do tipo agente têm conexões entre camadas com a Camada do aplicativo.

Aplicar universos nas camadas do mapa

Após definir um filtro para selecionar componentes específicos, é possível salvar o filtro como um universo. Autorize os usuários a acessar todos os componentes no universo, incluindo componentes que têm conexões entre camadas com os componentes selecionados. Para obter mais informações sobre a configuração de universos, consulte Configurar universos.

Os exemplos a seguir mostram possíveis usos de filtros nas camadas do mapa.

Exemplo 1: capturar transações completas que passam por um domínio específico

Esse universo contém transações monitoradas completas que passam por um domínio selecionado, incluindo nós de transação comercial e componentes de back-end inferidos. Esse universo também contém todos os agentes que estão monitorando os componentes de aplicativo.
Siga estas etapas:

1. Selecione a **Camada do aplicativo** como a camada de filtragem.
2. Selecione **Adicionar filtro** e **SEGUIR O CAMINHO DE TRANSAÇÃO**.
3. Selecione **agentDomain** na lista de atributos.
4. Insira o nome do **agentDomain** no **Filtro** para encontrar transações para esse domínio.

Exemplo 2: conceder acesso administrativo a todos os coletores do EM, bancos de dados do EM e agentes de um domínio específico

Esse universo contém os componentes obrigatórios da Camada de infraestrutura do APM, bem como os componentes de aplicativo que os agentes monitoram no domínio especificado. Os resultados não mostram transações comerciais ou de back-end inferidas, pois essas transações não são monitoradas pelos agentes.
Siga estas etapas:

1. Selecione a **Camada de infraestrutura do APM** como a camada de filtragem.
2. Selecione **Adicionar filtro** e **atributo agentDomain**.
3. Insira o nome do **agentDomain** no **Filtro.**
4. Selecione **+** para adicionar um novo item de filtro e **Adicionar novo grupo de filtros**.
5. Selecione **Type** na lista de atributos.
6. Selecione todos os valores de atributo, exceto **AGENT**, por exemplo, **EM_COLLECTOR**, **EM_DATABASE**, entre outros.

O mapa mostra componentes e conexões de componentes que estão dentro da camada selecionada. As camadas do mapa permitem identificar a causa raiz dos problemas de desempenho. Você pode alternar entre as camadas no mapeamento para exibir os problemas de desempenho causados por componentes do aplicativo, componentes da infraestrutura ou componentes do DX APM.

Para obter mais informações sobre as camadas do mapa, consulte Camadas do mapa.

Identificar áreas problemáticas usando filtros

Os filtros permitem reduzir sua pesquisa de componentes por nome e valor de atributo. Os filtros removem as informações do conjunto de dados que o painel e o mapa exibem. Use os filtros para identificar áreas problemáticas durante o monitoramento do seu ambiente. Filtre para remover grupos de componentes não afetados a fim de simplificar o painel e o mapa para fazer a triagem e o monitoramento. Os filtros são cumulativos da esquerda para a direita. É possível filtrar os resultados de um filtro com outro. É possível criar camadas de filtros para detalhar até áreas específicas de um ambiente. Os filtros são persistentes entre o painel e o mapa.

O Application Performance Management tem os seguintes recursos de filtro:

- Filtrar seguindo um caminho de transação
- Filtrar componentes por qualquer atributo
- Aplicar vários grupos de filtros
- Incluir o nó de experiência no resultado do filtro
- Arrastar e soltar filtros individuais entre grupos de filtros

Grupos de filtros e filtros de atributo

Um grupo de filtros define o conjunto de nomes e valores de atributos que são exibidos no mapa e no painel. Todos os outros componentes são removidos do conjunto de dados. Dentro de um único grupo de filtros, cada condição de filtro adicional limita o conjunto de nós resultante exibido.Um filtro de atributo remove todos os componentes do conjunto de

dados que não têm os nomes e valores de atributo na condição do filtro. Um filtro de caminho de transação remove todos os componentes do conjunto de dados que não têm valores de caminho de transação na condição do filtro.

- Os filtros dentro de um único grupo de filtros são combinados com um operador E. Cada condição de filtro pode ser um filtro de atributo ou um filtro de caminho de transação. Adicione um grupo de filtros para incluir um segundo conjunto de dados filtrados no mapa e no painel.
- Diferentes grupos de filtros são combinados com um operador OU. O mapa exibe todos os nós que satisfazem os critérios do grupo de filtros 1 e todos os nós que satisfazem os critérios do grupo de filtros 2.

Você pode arrastar e soltar as condições do filtro para editar os grupos de filtros. Se você arrastar e soltar um filtro de caminho de transação entre grupos de filtros, ele passará a ser um filtro de atributo. Não é possível mover filtros de caminho de transação entre grupos de filtros. Você pode editar o filtro e marcar a caixa de seleção **Seguir o caminho de transação** para ativar o rastreamento das transações.

Você pode alterar a ordem dos filtros usando o recurso de arrastar e soltar. É possível alterar a ordem dos filtros movendo-os entre os grupos de filtros, e para dentro e para fora dos filtros de caminho de transação. A única limitação é que não é possível mover o filtro de caminho de transação como um todo. Se você mover a última condição do filtro para fora do quadro de filtros de caminho de transação, o quadro desaparecerá.

NOTE

Mais informações:

- Definir a forma de monitoramento do ambiente com regras de atributo

Definir um filtro de caminho de transação

O Application Performance Management gera dados de mapa por meio da amostragem dos rastreamentos de transação. Existe um registro de cada caminho de transação que passa por qualquer componente.

NOTE
Identificar todas as transações em ambientes grandes pode fazer com que seja gerado um grande número de vértices, o que pode afetar o desempenho. Para evitar explosões de dados em ambientes grandes, esse recurso poderá ser desativado.

Um filtro de caminho de transação identifica todos os componentes em todos os caminhos de transação com os valores de atributo especificados nos critérios do filtro.Por exemplo, digamos que você deseje ver no mapa todas as transações que passem por qualquer componente cujo atributo de localização seja Paris. Se você definir um filtro de transação para a localização Paris, o mapa exibirá todos os componentes das transações que passarem pelos nós Paris.

NOTE

Os caminhos de transação são obtidos do nó da experiência, o que é o primeiro componente de front-end monitorado e é o início do caminho da transação. Um nó de experiência contém um atributo extra chamado Experience. Se uma transação for desviada em qualquer etapa, os filtros de caminho de transação identificarão todos os componentes dessa transação. Os filtros de caminho de transação também identificarão ramificações desviadas, independentemente de onde o atributo especificado esteja dentro da transação.

Siga estas etapas:

1. Selecione **Adicionar filtro**, adicione os critérios do filtro e selecione **Seguir o caminho de transação**.
2. (Opcional) Marque a caixa de seleção **Incluir o nó da experiência**. Esse nó é o primeiro componente de front-end monitorado e é o início do caminho da transação. O atributo de experiência nos filtros contém o nó da experiência, incluindo todos os outros nós no caminho da transação. Se você selecionar **Incluir o nó da experiência**, adicionará todos os nós de experiência que usarem os nós filtrados.

TIP

É possível remover manualmente nós específicos. Atribua um atributo personalizado ao nó e depois descarte esse atributo.

Defina um filtro de caminho de transação.

Criar um grupo de filtros

Siga estas etapas:

1. Selecione o ícone do sinal de mais ao lado de um filtro.
   Uma lista suspensa de nomes de atributo será exibida.
2. (Opcional) Selecione **Seguir o caminho de transação**.
3. Selecione um nome de atributo pelo qual filtrar.

   NOTE

   Os atributos são listados sob a camada correspondente.
4. Selecione o ícone do sinal de mais. Selecione **Adicionar novo grupo de filtros** e, em seguida, selecione um nome de atributo para filtrar.
5. Selecione a lista suspensa de condições de filtro e desmarque os valores de atributo a serem removidos pelo filtro. Os ícones de status ao lado dos valores de filtro indicam o status da integridade dos componentes associados somente no modo dinâmico.
6. (Opcional) Adicione mais critérios de filtro. Selecione o ícone de adição dentro do quadro azul e adicione mais nomes de atributos à condição do filtro de caminho da transação.

Você criou um grupo de filtros.

TIP

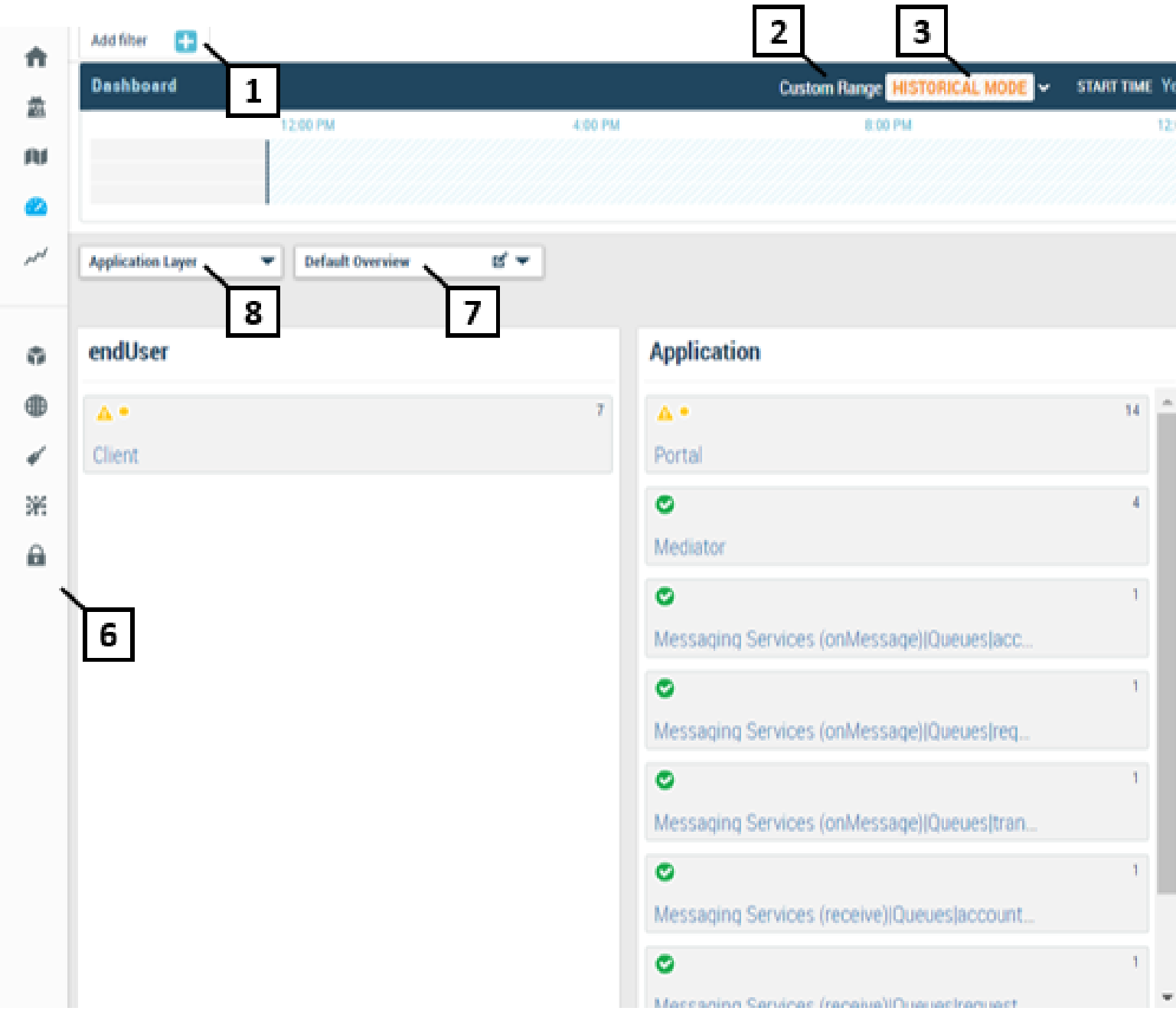
Se você optar por editar o grupo de filtros mais tarde, salve o URL primeiro. Você pode usar o URL para retornar às configurações anteriores do grupo de filtros.

Monitorar a integridade geral do ambiente com o painel

O DX APM fornece uma visão geral de um ambiente de aplicativo. O Painel mostra a integridade geral do ambiente. Um bloco representa um grupo de todos os componentes que compartilham um nome e valor de atributo. Os blocos mostram o status do alerta e a análise diferencial mais significativa de qualquer um dos componentes do grupo.

Visão geral

Os blocos do Painel são organizados em colunas. Cada coluna representa um atributo da perspectiva selecionada. O nome do atributo está no cabeçalho da coluna. Cada bloco em uma coluna mostra o status de todos os componentes que têm um valor de atributo específico.



A legenda a seguir identifica cada item do mapa por número e fornece mais informações:

Número	Nome	Mais informações
1	Filtro	
2	Intervalo de datas	Clique para selecionar um intervalo de datas atual ou personalizado.
3	Modo de linha de tempo (Histórico ou Dinâmico)	

4	Expandir ou recolher a linha de tempo	Selecione **Status**, **Em topologia** ou **Atributo** para exibir esses eventos de mudança na linha do tempo. **Observação:** por padrão, a Linha de tempo é carregada sem uma seleção de eventos de mudança.
5	Link da Ajuda online	
6	Painel de navegação	
7	Perspectivas	Uma perspectiva agrupa os componentes de modo lógico e se baseia em seus atributos compartilhados.
8	Camadas	As camadas mostram componentes que correspondem às exibições do Application Performance Management, por exemplo, Exibição de agentes e Exibição da experiência.
9	Status do alerta	Os alertas mostram o status de qualquer um dos componentes do grupo. A intensidade do alerta no Painel reflete a intensidade do status do alerta. O status do alerta se baseia em informações adicionais provenientes de alertas. Os fatores incluem por quanto tempo o nó é afetado e em quanto as métricas associadas excedem os limites. A escala tem cinco graus que vão de baixo a alto.Quando não há grau, significa que não há dados suficientes para chegar a uma conclusão.
10	Bloco	Os blocos no painel representam grupos de componentes que compartilham um nome e valor de atributo. O bloco exibe os resultados do status do alerta e da análise diferencial mais significativa para qualquer componente do grupo. O valor do atributo é o cabeçalho do bloco. Esse cabeçalho é um link clicável. Clique nesse link para ver esse grupo no mapa.
11	Número de blocos neste grupo	

Exibir camadas no painel

As camadas permitem aplicar as exibições padrão do Application Performance Management ao painel, por exemplo, Exibição de agentes e Exibição da experiência. Alterne entre as seguintes camadas no painel:

- **Camada do aplicativo**
  Mostra os componentes no mapa. Os componentes correspondem aos Cartões de experiência na Exibição da experiência.
- **Camada de infraestrutura do APM**
  Mostra os Gerenciadores corporativos e Agentes no painel.Essa camada corresponde à Exibição de agentes.
- **Camada de infraestrutura**
  Mostra a infraestrutura de rede do seu ambiente, incluindo Monitores de Docker.

Exibir perspectivas no painel

Uma perspectiva é uma maneira de agrupar componentes nas exibições do Application Performance Management que se baseia nos respectivos atributos compartilhados. As perspectivas permitem agrupar componentes no painel sem removê-los do conjunto de dados. Para obter mais informações sobre perspectivas, consulte Organizar componentes usando perspectivas.

O DX Application Performance Management fornece uma visão geral do ambiente de aplicativos. O Painel mostra a integridade geral do ambiente. Um bloco representa um grupo de todos os componentes que compartilham um nome e valor de atributo. Os blocos mostram o status do alerta e a análise diferencial mais significativa de qualquer um dos componentes do grupo.

Para obter mais informações sobre o painel, consulte Monitorar a integridade geral do ambiente com o painel.

Monitorar problemas e anomalias da triagem assistida

As informações sobre eventos interessantes são exibidas como problemas e anomalias (históricos) na Exibição da experiência ou no Bloco de notas de análise. Experiência é um componente do ambiente em que uma transação é iniciada. A triagem assistida reúne evidências para detectar problemas em potencial ou que estejam surgindo no ambiente. A coleta de evidências pode ser feita em um estágio inicial, quando a evidência ainda não aponta para nenhuma experiência afetada. A essa evidência dá-se o nome de *anomalia*. Quando a triagem assistida tem informações suficientes para identificar as experiências afetadas, a evidência recebe o nome de *problema*. As anomalias são como problemas, mas sem impacto para o usuário.

A Exibição da experiência ou o Bloco de notas de análise fornecem locais convenientes para monitorar todo o sistema. No seu aplicativo, muitos eventos diferentes ocorrem continuamente, mas muitos deles talvez não sejam do seu interesse. A triagem assistida ajuda a identificar e priorizar os problemas relatando eventos significativos do sistema do aplicativo. Esses eventos significativos são exibidos como históricos com títulos na Exibição da experiência ou no Bloco de notas de análise e explicam os seguintes aspectos:

- Qual é o provável problema
- Quem é afetado pelo problema
- Quem pode ser afetado pelo problema (potencial)
- Quais componentes estão envolvidos no problema
- Que tipos de eventos ocorreram nos componentes envolvidos no problema
- Quando esse problema começou e quando terminou

Como em uma página de jornal real, você ver as manchetes periodicamente ao longo do dia. O nível de interesse em relação a uma experiência está diretamente alinhado com o escopo das suas responsabilidades como analista. Por exemplo, um ou mais dos seguintes casos podem indicar que um problema ou anomalia precisa de atenção:

- O escopo do impacto no cliente é grave. Muitas vezes, a triagem assistida avalia o impacto usando as informações sobre quem é afetado.
- O escopo do impacto no cliente não foi especificado ou a experiência não está clara. Por exemplo, se a informação sobre o local indicar um aplicativo ou transação chave, talvez seja necessário investigar melhor.

Siga estas etapas:

1. Clique no botão **Exibição da experiência**.
   A Exibição da experiência mostra os cartões de experiência individuais.Cada cartão mostra um resumo. Este resumo representa o que aconteceu e explica o motivo. Os itens em vermelho indicam áreas problemáticas, como transações com falhas.
2. Navegue pela página e clique no ícone **Abrir um bloco de notas de análise** em um cartão de seu interesse.Os problemas e as anomalias aparecem no painel de triagem assistida. O mecanismo de triagem assistida identifica as transações que compartilham componentes de baixo desempenho.

NOTE
Ao detalhar em um Cartão de experiência de uma exibição para a outra, as histórias da Triagem assistida podem se alterar de problemas para anomalias. Uma transação comercial pode mostrar um problema e nenhuma anomalia. Ao detalhar de um Cartão de experiência ainda mais, um novo cartão pode não exibir nenhum problema e uma anomalia.

Isso ocorre porque uma história da Triagem assistida pode ser um problema para uma das transações comerciais e uma anomalia para outra. Uma das transações comerciais que tenha um problema oculta as outras transações de comerciais para mostrá-las como anomalias. Ao tentar fazer o detalhamento de uma única transação comercial, as anomalias que foram ocultadas na exibição anterior agora estarão visíveis.

3. Procure o painel e leia os detalhes sobre o problema ou a anomalia de interesse.Clique no botão **Abrir** de um problema ou uma anomalia.
   O Relationship Flow mostra os caminhos de transação das experiências selecionadas. Este mapa fornece o contexto sobre o evento ocorrido, especialmente onde ele ocorreu. O APM mostra *somente* o subconjunto de todo o mapeamento do aplicativo em que se encontra o problema ou a anomalia. Por exemplo, os detalhes podem dizer quanto tempo o problema durou e quais componentes foram afetados. O Responsável aparece no painel Triagem assistida e no mapeamento.

   TIP

   Use a lista suspensa **Perspectiva** e crie ou selecione uma perspectiva. Você pode usar as perspectivas para agrupar os componentes de acordo com seus atributos compartilhados.
   O mapa Relationship Flow reduz a visualização.
4. No painel Triagem assistida, expanda **Duração**, **Experiências afetadas** ou **Componentes do aplicativo** e investigue a causa raiz do problema. Clique em **Abrir** para ver a evidência de contribuição.
5. Continue a investigação usando as diversas opções do Bloco de notas de análise.

Triagem assistida e analistas

A triagem assistida é um mecanismo e um gerador de histórico. A triagem assistida identifica os eventos mais significativos que ocorreram nos sistemas ocupados e fornece informações contextualizadas (históricos) sobre esses eventos. Esses históricos são exibidos como problemas e anomalias com títulos. A natureza confiável e inteligente dos históricos gerados pela triagem assistida o mantém totalmente informado sobre o estado do seu domínio de monitoramento.

Como a triagem assistida funciona

A triagem assistida cria problemas e anomalias sobre os eventos do sistema. A triagem assistida reage aos seguintes tipos de eventos:

- Paralisações
- Erros
- Alertas
- Tempos de resposta instáveis

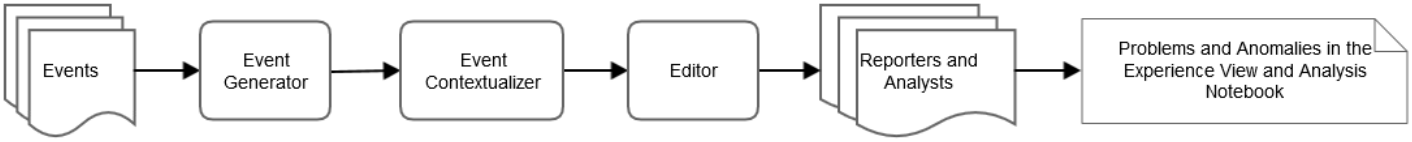
Os problemas e as anomalias explicam os aspectos de um ou mais eventos. Por exemplo, os aspectos incluem:

- O que resume o evento, inclusive quaisquer causas suspeitas (o motivo). Essa informação é exibida como um título de um problema ou anomalia na Exibição da experiência e no Bloco de notas de análise.
- Onde se localiza a ocorrência de um evento. Em geral, é uma informação como o nome do host e do agente. A informação de local pode ter mais detalhes, quando disponíveis.
- Quem identifica as transações que são afetadas ou podem ser afetadas. Esse aspecto também determina o número de transações afetadas.
- O aspecto Quando registra a ocorrência de um evento. Normalmente, o início e o término de um evento de paralisação, um evento de erro ou uma instabilidade.
- O motivo explica a ocorrência de um evento. Por exemplo, a instrução a seguir explica um problema de índice de chamadas alto:

```
Potential high call ratio from ViewOrders|service to 138.0.0.1_7080|getService 2 in the order of 214980
```

O diagrama a seguir e as etapas correspondentes descrevem como a triagem assistida funciona:

Figure 7: Arquitetura de triagem assistida



1. Os eventos do sistema APM ocorrem como intensidade de variação, erros, paralisações, alertas do APM e assim por diante. Um evento contém uma possível suspeita do que está causando o problema.
2. Um gerador de eventos reúne dados de eventos de diferentes origens e envia esses dados ao processador de eventos.
3. O contextualizador de eventos recebe os eventos dos geradores em um agrupamento, processa-os e reúne todos os eventos relacionados em um contexto. As informações de contexto incluem o possível impacto sobre o componente mais à esquerda e todas as transações que passam pelo componente.
   O contextualizador passa essas informações de contexto para o editor.
4. O editor rastreia diferentes contextos e atribui um gerador de relatórios por contexto de evento específico para análise adicional.
5. Os geradores de relatórios conhecem os diferentes tipos de analistas que estão disponíveis no sistema e percorrem o contexto de cada analista. Os analistas analisam o contexto para detectar os tipos de eventos, padrões e o possível impacto, e cada analista cria uma instrução.Os analistas trabalham juntos para registrar a evidência ou criar históricos a partir das instruções e, em seguida, armazenam os dados no banco de dados do APM. Os históricos são eliminados do banco de dados quando têm mais de 62 dias.
6. Os históricos são exibidos como problemas ou anomalias na Exibição da experiência e no Bloco de notas de análise.

> **NOTE**
> O Enterprise Manager gera e coleta métricas sobre os componentes da triagem assistida. Essas métricas de suportabilidade são úteis para avaliar a integridade do Gerenciador corporativo.

Analistas

Os analistas são como médicos especialistas que sabem como diagnosticar classes específicas de doenças. A triagem assistida usa os principais tipos de analistas a seguir. Cada tipo de analista inclui outros analistas específicos.

Os *analistas de eventos* procuram determinados tipos de eventos e criam instruções de evento que servem como evidência. Exemplos de analistas de eventos incluem:

- Um analista de Análise Diferencial verifica a intensidade da variação
- Um analista de erros verifica os eventos de erro nos contextos
- Um analista de eventos de recurso monitora os eventos de alerta nos recursos do sistema

Os *analistas de padrões* procuram determinados padrões no contexto e criam instruções de padrão. Essas instruções são uma parte do resumo de um histórico. Exemplos de analistas de padrões incluem:

- Um analista padrão determina o componente mais profundo em um contexto (de acordo com o mapa de relacionamento). O analista padrão também é conhecido como o identificador de zona.
- Um analista de índice de chamadas alto procura o componente mais profundo em determinado contexto (de acordo com o mapa de relacionamento). Este analista vê se o componente chama algum nó do tipo back-end um número de vezes incomum.

As instruções dos analistas formam um resumo de histórico.

Exemplo de histórico: analista de padrão (identificador de zona)

Este exemplo explica o histórico de um analista padrão (ou identificador de zona). Este analista sempre entrará em ação se outros analistas específicos encontrarem padrões. O analista padrão identifica uma provável zona. A zona pode ser um front-end, um back-end ou um componente interno entre eles. Por exemplo, uma instrução do analista padrão se parece com esse título:

```
Problem isolated to {type} {component}
```

{tipo} pode ser um front-end, uma transação comercial, um componente interno ou um back-end.

{componente} é o nome do componente envolvido na zona.

Por exemplo, considere os seguintes componentes do sistema:

- Front-end F
- Back-end B
- Componente interno M

Todos esses componentes estão relacionados por terem uma transação comercial: F->M->B.

A sequência de eventos a seguir ocorre no fluxo da transação:

1. Ocorrem eventos que estão relacionado apenas ao Front-end F.
   O histórico do analista padrão relata um evento que está isolado no Front-end F.
2. Ocorre um evento no componente interno M.
   O analista padrão relaciona esses dois eventos porque eles estão no mesmo fluxo de transação. O analista declara: o problema foi isolado no componente interno M
3. Ocorre um evento no Back-end B.
   O analista padrão combina todos os três eventos e estados: o problema foi isolado no back-end B

Procure nas anomalias ou nos problemas da Exibição da experiência e do Bloco de notas um título que inclua um tipo e um componente, por exemplo:

```
Problem isolated to internal component AxisServlet|service
```

Este título descreve um histórico do analista padrão. Por exemplo, os detalhes devem descrever um problema na zona entre as transações de front-end e back-end para o aplicativo ACME.

Exemplo de histórico: índice de chamadas alto

Este exemplo explica como a triagem assistida relata um histórico de índice de chamadas alto. Um índice de chamadas alto ocorre quando um componente do cliente emite muitas transações próprias, sobrepondo a transação sobrejacente inicial. Ou seja, quando o índice do chamador para o receptor da chamada resulta em um número pequeno para o chamador e um número alto para o receptor, por exemplo, 1:20. Este número mostra que uma chamada feita para o chamador resulta em 20 chamadas para o receptor. O analista de padrão relata o histórico de índice de chamadas alto para nós/componentes de back-end, como bancos de dados ou de clientes de serviços web.

Os seguintes sintomas podem indicar um problema de índice de chamadas alto:

- A latência está alta em uma posição anterior a um componente na pilha de chamadas, mas a latência do componente em si está baixa, o que indica um uso do índice de chamadas alto por parte do componente ou anterior ao componente.
- Transações de latência longa com padrões de código de barras: o componente A chama o componente B inúmeras vezes em um curto intervalo. Este comportamento geralmente resulta na latência normal para B, mas latência alta para A.

Pesquise as anomalias ou os problemas na Exibição da experiência e no Bloco de notas para identificar um título Índice de chamadas alto. Por exemplo, as anomalias e os problemas mostram o seguinte título:

```
Potential high call ratio from {culprit.name} to {calledComp.name} in the order of {ratio}
```

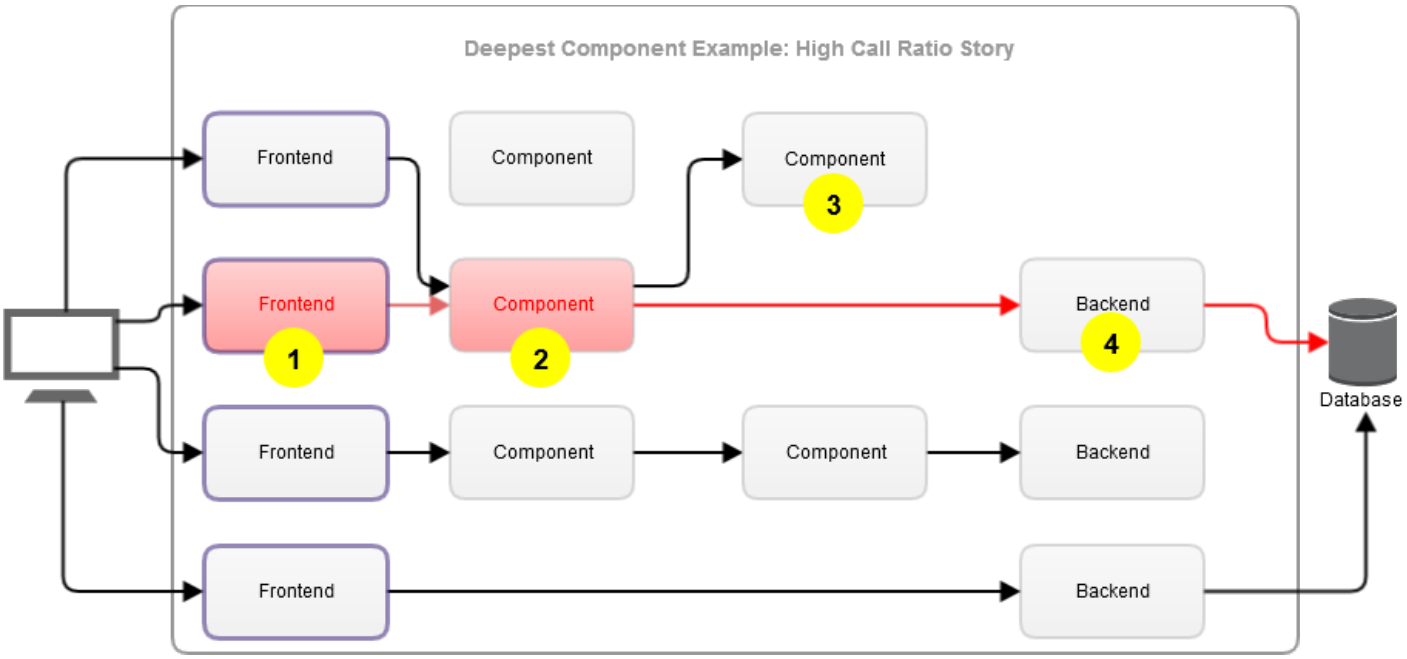
Este título descreve um histórico de índice de chamadas alto. Por exemplo, os detalhes devem descrever um problema de latência para uma conexão de cliente com o banco de dados em Nova Iorque.

Exemplo: como um analista determina o componente mais profundo em um histórico de índice de chamadas alto

O exemplo a seguir mostra como um analista de padrões pesquisa o componente mais profundo em um histórico de índice de chamadas alto:

1. A Análise diferencial dispara um alerta -- uma transação se tornou lenta e agora faz parte de um histórico.
2. Ocorreu um evento no caminho de chamada proveniente da transação. O analista pesquisa o componente mais profundo no contexto.
3. Um componente é terminal. O componente não chama um back-end, então, o analista o ignora.
4. Um componente chama um back-end. Usando dados históricos, o analista compara os números de Respostas por intervalo no componente de chamada com o número de Respostas por intervalo para as chamadas de back-end. Se o índice for alto (por exemplo, > 1:50), significa que a transação tem um índice de chamadas alto anormal que poderia prejudicar o desempenho do aplicativo.
   Outros componentes também podem ter um índice de chamadas alto ao banco de dados. O analista não irá diagnosticar o índice alto até que existam componentes no caminho de chamada provenientes do front-end. O analista não está preocupado com o aplicativo inteiro, mas sim em detectar um histórico identificado.

Figure 8: Exemplo do componente mais profundo: histórico de índice de chamadas alto



Suporte do analista aos eventos de recurso

A triagem assistida usa um analista de eventos de recurso para monitorar os alertas sobre eventos de recurso, como CPU, memória, e assim por diante, como segue:

1. Um aplicativo apresenta problemas e, ou devido a, problemas de recursos do sistema.
2. Os eventos de recursos são listados como suspeitos de um determinado problema ou anomalia.
3. Um componente de infraestrutura/recurso é identificado como o possível responsável na infraestrutura.

Os analistas de recursos ajudam os agentes do DX APM e o DX APM Infrastructure Agent. A triagem assistida fornece o contexto para as informações de infraestrutura que são relatadas pelo Infrastructure Agent em relação a um aplicativo. Os alertas disparados nos componentes da infraestrutura são incorporados nas histórias de triagem assistida (evidências). Por exemplo:

1. Uma CPU está em alta execução em um servidor, possivelmente tornando o aplicativo mais lento.
2. O Infrastructure Agent relata o problema.
3. A triagem assistida associa esse problema de recurso ao aplicativo afetado e ao componente da infraestrutura.
4. O componente da infraestrutura é listado como o possível responsável na infraestrutura.

NOTE

As seguintes etapas de pré-requisitos se aplicam ao analista de eventos de recurso:

1. Certifique-se de que o monitoramento DX APM Infrastructure Agent esteja ativado e de que os alertas sejam mapeados para componentes da infraestrutura.
2. Na exibição do mapeamento, selecione **Camada do aplicativo** para ver os componentes do aplicativo.
3. Clique em um componente de aplicativo no mapeamento.
   Deve haver valores de correlação, incluindo o componente de infraestrutura correspondente.

Mais informações:

Camadas do mapa

Infrastructure Agent

Investigar o baixo desempenho das transações

Dados de métrica, como o tempo médio de resposta de um componente importante, podem informá-lo sobre a experiência dos clientes que usam esse componente. No entanto, esses dados não ajudam a entender os casos em que o desempenho é excepcionalmente lento.Quando as transações estão lentas, o rastreamento de transação pode atuar como uma espécie de raio-x: mostrando detalhes que não são visíveis na superfície e permitindo que você detecte, com mais detalhes, em que ponto a transação gastou tempo. O Application Performance Management (originalmente conhecido como Wily Introscope) foi pioneiro na abordagem de rastreamento de transação para obter uma visão aprofundada de transações individuais. O rastreamento de transação monitora a atividade de cada transação à medida que ela passa pelos aplicativos monitorados pelo agente.Enquanto os dados de métrica informam quando há um afunilamento no tráfego, os rastreamentos de transação podem informar sobre a experiência de um único carro: onde ele se atrasou, por quanto tempo e até mesmo por qual motivo. Os rastreamentos de transação são armazenados, então, é possível visualizar seus detalhes horas ou dias depois que as transações ocorreram pela primeira vez.

Localizar os rastreamentos de transações lentas ou com falhas

Como analista, a **Exibição da experiência** o ajuda a encontrar rastreamentos de transação úteis para investigar. Na guia **Transações comerciais**, é possível exibir resumos e detalhes do rastreamento de transação. Essas informações ajudam a entender o desempenho da transação e a resolver o desempenho ineficaz, identificando quando, onde e por que o desempenho está diminuindo.

Siga estas etapas:

1. No painel esquerdo, clique em **Exibição da experiência**.
   A Exibição da experiência mostra os cartões de experiência individuais. Cada cartão mostra um resumo. Os itens em vermelho indicam transações lentas ou com falhas.

   NOTE
   Para obter mais informações sobre a Exibição da experiência, consulte Monitorar o desempenho usando a Exibição da experiência.

   TIP

   Também é possível iniciar a investigação no Mapa. No painel esquerdo, clique no **Mapeamento** e ignore a próxima etapa.
2. Procure os cartões e clique no ícone **Bloco de notas** de um cartão que seja do seu interesse.
   O Bloco de notas de análise mostra os detalhes sobre a experiência.
3. No painel **PROBLEMAS**, clique em **Abrir** em um problema de interesse.
   -Um círculo vermelho indica que o componente está presente em ao menos um problema ou anomalia.Todos os componentes em uma história são tratados como representantes.
   - Um círculo vermelho concêntrico indica que o componente é o responsável por ao menos um problema ou anomalia. Todos os representantes têm evidências, mas um responsável é um representante especial. O responsável identifica a causa raiz do problema ou da anomalia no devido aplicativo ou na devida transação.
   Esse componente pode ser a origem da degradação de desempenho no seu ambiente de aplicativos.
   O Relationship Flow mostra os caminhos de transação das experiências selecionadas. Este mapa fornece o contexto sobre o evento ocorrido.
4. Clique nos nós individuais ou grupos de nós até o máximo de 1.000 nós. Selecione **Camada do aplicativo** ou **Camada de infraestrutura do APM** no mapeamento para ver todos os rastreamentos que são coletados por host, agente ou aplicativo.
   Um gráfico **Visão geral do componente** é exibido e mostra as transações íntegras e incorretas.
   Clique aqui para obter ajuda para o gráfico de componente...

O gráfico de componente mostra o máximo de 20 nós. Use gráficos de componentes para comparar métricas dinâmicas ou históricas entre nós arbitrários. O gráfico de componente contém mais informações de métricas do que o disponibilizado para cada componentes do mapa. Use as opções de alternância (pontos) na parte inferior do gráfico para exibir as informações a seguir.

- Histograma TEMPO DE RESPOSTA: o histograma mostra o tempo médio de resposta agregado por segundo de transações íntegras e incorretas. O histograma permite comparar dados e identificar tendências com facilidade, por exemplo, quando o número de rastreamentos aumenta ou diminui.
- Minigráfico TEMPO MÉDIO DE RESPOSTA: o minigráfico mostra a forma geral da variação ao longo do tempo das métricas de diagnóstico de qualquer componente. O minigráfico mostra informações para o período ativo que é selecionado na linha de tempo. Passe o mouse sobre qualquer ponto no minigráfico para ver um valor numérico.
- Gráfico VOLUME DA TRANSAÇÃO: o gráfico de barras ajuda a determinar rapidamente o nível do volume de transações. As barras também facilitam a identificação das tendências em relação ao volume.

O componente é realçado no painel **AFFECTED APPLICATION COMPONENTS**.

5. Clique na guia **Transações comerciais**.
   Uma lista de resumo mostra os rastreamentos correspondentes ao componente no intervalo selecionado na linha do tempo. Os rastreamentos de componentes inferidos serão listados mesmo que essas transações não sejam monitoradas pelos agentes. Por exemplo, os componentes inferidos podem ser back-ends, serviços web ou soquetes. Os rastreamentos mostram os tempos de duração e são codificadas por cores. Cada cor indica uma característica associada a uma transação, por exemplo, vermelho indica um erro. É possível identificar os métodos problemáticos observando a duração do rastreamento. Rastreamentos inesperadamente longos são causas prováveis de transações lentas.

   NOTE
   A lista é atualizada automaticamente quando você usa o modo Dinâmico.

   A lista mostra as seguintes informações de rastreamento de, no máximo, 2.000 rasteamentos.

   URL — o URL que foi chamado para iniciar essa transação ou o caminho para o componente que iniciou a transação

   Nome - o nome do componente de alto nível, por exemplo: Default

   Marca de data e hora — A hora de início, no relógio do sistema do computador host do agente, da invocação do componente selecionado

   Duração - o tempo de execução em milissegundos do componente selecionado

   Tipo de rastreamento — o tipo de rastreamento: Outros, Erro ou Instantâneo.

   ID de usuário - a ID do usuário conectado que está executando a transação

   Essas informações ajudam a compreender a sequência de chamadas de um período e avaliar o desempenho.

   Observação: nem todas as informações sobre componentes de visibilidade profunda estão disponíveis.
6. Execute uma ou mais ações:
   - Clique no **botão pop-out** para abrir o visualizador em uma caixa de diálogo de exibição cheia. Pressione a tecla **Esc** para fechar a caixa de diálogo.
   - Selecione uma opção na lista suspensa **Tipo de rastreamento** para categorizar os rastreamentos por características. Um rastreamento pode ter mais de uma característica:

     Outros: retorna todos os outros rastreamentos de transação que não forem rastreamentos com erros ou paralisações. Laranja-claro

     indica que a Análise diferencial acionou um alerta; uma transação apresenta variação não controlada.

     Erro: retorna os rastreamentos de transação com uma característica de erro. Um erro é uma exceção relatada pelos códigos de erro da JVM ou do HTTP. Por exemplo, erros incluem um status de erro do HTTP, uma exceção do SQL ou uma exceção do Java. Quando o Tipo de rastreamento for Normal, mas um erro tiver disparado um rastreamento de transação automático, o componente será exibido como um erro e será contabilizado no total de erros.

Também serão retornados rastreamentos de transações com uma mensagem de erro de `transação paralisada`. Uma paralisação é uma transação ou um componente de uma transação que não foi concluído dentro do limite de tempo especificado.

Instantâneo: retorna todas as transações com instantâneos.

- Clique em um **cabeçalho de coluna**.

  A lista classificará os rastreamentos pelo tipo da coluna, por exemplo, pela `ID de usuário`. O tipo de rastreamento não é classificável clicando-se no cabeçalho da coluna.

  Observação: a ID de usuário é a identificação do usuário conectado que está executando a transação (se este campo estiver configurado e se a ID estiver disponível).

7. Examinar componentes individuais e dados de rastreamento. É possível analisar a sequência de chamada e o código para determinar a causa de um problema.

Mais informações:

Usar o rastreamento de transação entre processos para resolver problemas

Iniciar uma sessão de rastreamento de transações

Examinar componentes individuais e dados de rastreamento

Diagnosticar problemas de carregamento do recurso

Diagnosticar problemas de desempenho do sistema

Detectar e analisar erros e paralisações

Analisar instantâneos de erro e paralisação

Analisar rastreamentos e colaborar na análise de problemas

Usar o rastreamento de transação entre processos para resolver problemas

Muitas vezes, as transações percorrem várias instâncias de JVMs, CLRs ou Node.js**,** ou serviços de aplicativo, dependendo do ambiente. O processamento passa de qualquer combinação de instâncias de JVM, CLR ou Node.js, ou servidor de aplicativos, para outra. A coleta do caminho da transação completa requer rastreamento de chamadas síncronas e assíncronas entre os limites da instância de JVM, CLR ou Node.js. Ser capaz de rastrear transações entre várias plataformas também pode exigir a execução de um agente suportado. O *rastreamento de transação entre processos* coleta o caminho da transação completa entre várias plataformas.Esse recurso permite que você veja detalhes quando os métodos de chamada das transações em várias JVMs ou CLRs são executados em servidores diferentes.

> **NOTE**
> O rastreamento de transação entre processos é suportado na execução manual, em amostras e outros rastreamentos de transação que usam a filtragem de agente. As transações entre processos nos rastreamentos automáticos de transação são suportadas apenas para aplicativos Java.

Correlação de transações

Os aplicativos distribuídos são complexos. As transações de único usuário geralmente abrangem vários segmentos que são executados em CLRs ou JVMs de agente separados.Frequentemente, uma transação única inclui chamadas síncronas e assíncronas.O agente também deve considerar as chamadas de transações individuais para apresentar o caminho da transação completa como uma unidade lógica.

Normalmente, as transações consistem em várias chamadas e respostas que são passadas de um processo para outro. Muitas vezes, diferentes processos em uma transação fazem chamadas para diferentes servidores físicos ou lógicos. Os processos também podem ser distribuídos para serem executados em diferentes componentes ou sistemas back-end.A montagem de uma transação completa requer um agente para identificar todos os processos incluídos e a ordem de chamada. O agente também exige informações sobre segmentos e chamadas síncronas e assíncronas.

O rastreamento de um caminho de transação completa que inclui chamadas entre processos exige que o agente se conecte aos processos de modo lógico. O agente usa um *identificador de correlação* (ID de correlação), que correlaciona ou cria uma exibição conectada dos processos.O agente faz a conexão inserindo o identificador de correlação na transação.O identificador de correlação pode ser passado de um processo para outro. Essa vinculação de processo permite que o agente identifique os front-ends e back-ends que fazem parte da mesma transação. Nos **Detalhes do componente** do Visualizador do rastreamento de transação, a ID de correlação é o valor da propriedade Realizar processamento cruzado dos dados.

A montagem de uma transação completa também exige que um agente determine quando um processo em uma transação chama outro.Você pode ver a ordem na qual front-ends e back-ends chamam uns aos outros em uma transação. Em transações síncronas, a ordem pode ajudar a identificar as relações entre chamador e receptor. Em transações assíncronas, a ordem pode ajudar a identificar um fluxo de trabalho em vários processos para segmentos de transação complexos de cliente e servidor. A combinação do identificador de correlação e da ordem de sequência de chamadas fornece um *rastreamento de transação correlacionado* ou *rastreamento correlacionado*.

O rastreamento de transação entre processos também oferece suporte à correlação entre segmentos dentro do mesmo processo.

O agente gerencia automaticamente o conjunto de dados do identificador de correlação e fornece os dados ao Gerenciador corporativo. O Gerenciador corporativo constrói a representação gráfica das transações selecionadas exibidas pelo Visualizador do rastreamento de transação.

Usar o rastreamento de transação para resolver problemas

O processo a seguir descreve como você pode examinar transações no Visualizador do rastreamento de transação, o que ajuda a encontrar a causa raiz de um problema.

1. Quando o Visualizador do rastreamento de transação exibe uma pilha gráfica, isso significa que o agente rastreou processos relacionados em um evento de rastreamento selecionado. Os processos que são rastreados de diferentes agentes aparecem em diferentes áreas sombreadas.
2. Você pode examinar os componentes vinculados para ver as transações entre processos ou entre JVMs. Por exemplo, é possível ver se uma determinada transação saiu de um processo e depois entrou em um processo diferente.
3. Também é possível obter informações sobre as chamadas que podem ser a origem de transações lentas e paralisadas.

Exemplo de rastreamento de transação entre processos

Este exemplo descreve como o rastreamento de transação entre processos pode ajudar você a identificar e avaliar problemas de maneira rápida e eficaz.

1. Você está analisando um rastreamento de transação em busca de uma transação com problemas e nota um tempo de execução de 6 segundos (6000 ms).
2. Na pilha gráfica, você vê chamadas de um método por parte do cliente, `dataservice.yourcompany.net/invoke`, para um método por parte do servidor, `thirdparty.mycompany.net/invoke`.
3. Você observa que o serviço web do lado do servidor está fazendo muitas chamadas a um serviço web de terceiros. O serviço web de terceiros não é instrumentado, de modo que o seu tempo de processamento não é explicitamente exibido no rastreamento.
4. A pilha gráfica mostra que o back-end do serviço web de terceiros está atendendo a solicitações repetidas em rápida sucessão.Esse comportamento indica que a lógica de programação, como um loop aninhado, provavelmente está causando chamadas repetidas no serviço lado do servidor. Você determinou que a operação de invocação do lado do servidor é responsável por grande parte do tempo de execução geral da transação.
5. Com essas informações, você entra em contato com o proprietário do aplicativo do serviço web do lado do servidor.
6. O proprietário solicita uma investigação sobre a lógica do aplicativo que chama o back-end do serviço web de terceiros.

Iniciar uma sessão de rastreamento de transação

Para executar uma sessão de rastreamento de transação manualmente, especifique os agentes cujas transações você deseja rastrear e o período da captura de dados. Depois que a sessão de rastreamento de transação é iniciada, as transações que correspondem aos critérios de filtro aparecem no Visualizador do rastreamento de transação. Os eventos de transação incluem erros e rastreamentos de transação.

Depois que um rastreamento é iniciado por um período, a sessão é interrompida no final do período especificado.

> **NOTE**
> Você só pode iniciar uma sessão de rastreamento para um agente especificado em um determinado período. Se você reiniciar uma sessão de rastreamento ativa, uma notificação o lembrará que a sessão de rastreamento de transação está ativa para o agente e mostrará o tempo restante na sessão ativa. É possível iniciar um novo rastreamento para o mesmo agente depois que uma sessão de rastreamento ativa termina.
>
> Por exemplo, "A sessão de rastreamento de transação está atualmente ativa para este agente - Tempo restante: menos de um minuto".

É possível iniciar a sessão de rastreamento de transação na página Agentes ou na página Exibição da métrica.

Para iniciar a sessão de rastreamento de transação na página **Agentes**, siga estas etapas:

1. No painel esquerdo, em **Configurações**, clique em **Agentes**.
   A página de agentes é exibida e lista os agentes.
2. (Opcional) Clique na seta de **Aplicativos**.
   Todos os aplicativos que o agente monitora são listados.
3. Selecione um ou mais agentes para o qual rastrear transações:
   – Para rastrear todos os agentes, clique em **Rastrear todos os agentes**. Essa opção rastreia agentes suportados que estão conectados no momento e qualquer um que se conecte durante a sessão de rastreamento.
   – Para rastrear agentes selecionados, clique em **Rastrear agente** para um agente.
   A caixa de diálogo Sessão de rastreamento de transação é exibida.
4. Especifique valores para o rastreamento de transação nos campos da caixa de diálogo ou aceite os padrões e clique em **Iniciar**:
   – Especifique a **Duração mínima da transação** em milissegundos para o rastreamento de transação. O padrão é 1000 milissegundos. O valor mínimo é 1 milissegundo.
   – Especifique a **Duração da sessão de rastreamento** em minutos. O padrão é 1 minuto com uma duração máxima de 5 minutos para uma única sessão de rastreamento.
   Um painel exibe o status da sessão.
5. (Opcional) Feche a caixa de diálogo depois que um rastreamento for iniciado com êxito. A sessão de rastreamento continuará sendo executada em segundo plano.

Para iniciar a sessão de rastreamento de transação na página **Exibição da métrica**, siga estas etapas:

1. No painel esquerdo, clique em **Exibição da métrica**.
2. Na guia **Árvore de métricas**, procure o agente cujas transações você deseja rastrear.
3. Clique com o botão direito do mouse no agente e clique na opção "Rastrear agente: <Nome>".A caixa de diálogo Sessão de rastreamento de transação será exibida.
4. Especifique os valores para o rastreamento de transação na caixa de diálogo.
   – Especifique a **Duração mínima da transação** em milissegundos para o rastreamento de transação. O padrão é 1000 milissegundos. O valor mínimo é 1 milissegundo.
   – Especifique a **Duração da sessão de rastreamento** em minutos. O padrão é 1 minuto com uma duração máxima de 5 minutos para uma única sessão de rastreamento.
5. Clique em **Iniciar**. A mensagem de confirmação "Sessão de rastreamento de transação iniciada." será exibida.
6. Clique em **Cancelar** para fechar a caixa de diálogo e retornar à página **Exibição da métrica**.

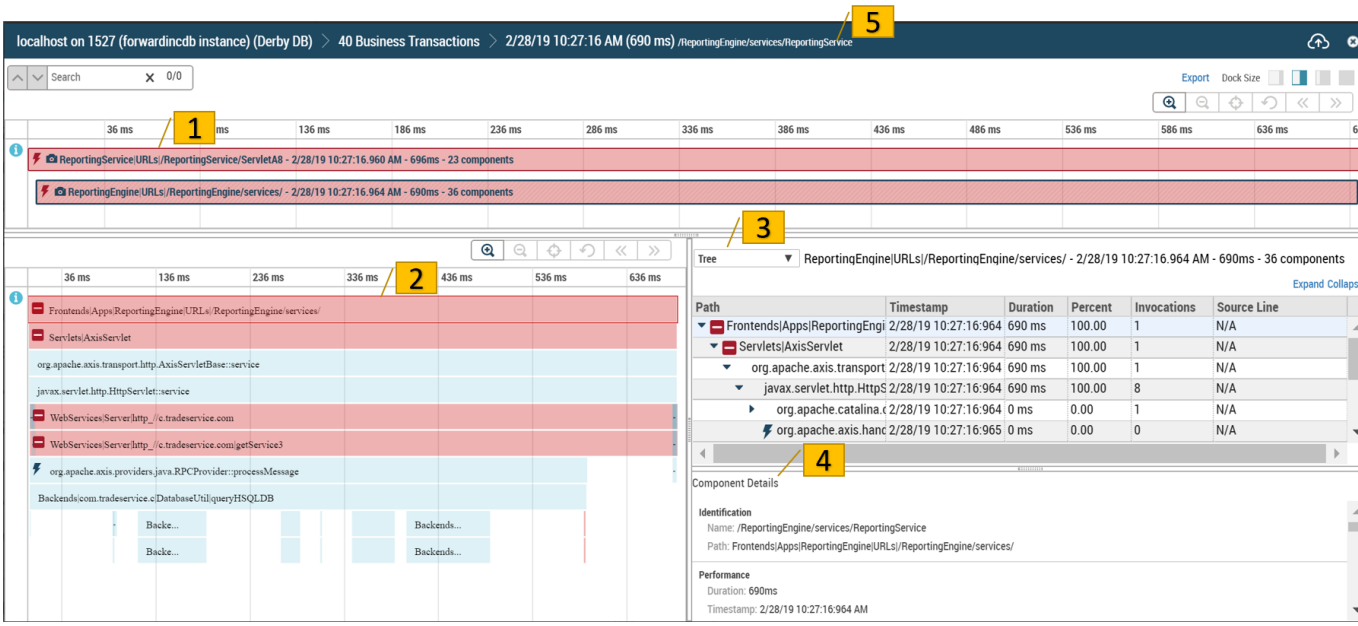
Examinar componentes individuais e dados de rastreamento

Você pode examinar informações detalhadas sobre os dados de rastreamento para encontrar o motivo pelo qual as transações estão lentas ou danificadas. O Visualizador do rastreamento de transação exibe várias representações dos dados para ajudar a identificar os componentes que estão com baixo desempenho.

Siga estas etapas:

1. No mapa ou no Bloco de notas de análise, vá para a guia **Transações comerciais**.
2. Clique na guia **Transações comerciais**.
3. Clique em uma linha da lista Rastreamento de transação.
   O Visualizador do rastreamento de transação exibe quatro painéis para mostrar informações sobre o rastreamento de transação e os componentes.
   – Os **Rastreamentos de transação** são exibidos no painel superior.
   – Os detalhes do **Rastreamento de transação** são exibidos no painel inferior esquerdo.
   – O painel inferior direito é dividido em dois subpainéis:
     - As **Informações sobre a transação** relacionadas ao rastreamento de transação selecionado são exibidas no subpainel superior direito.
     - Os **Detalhes do componente** são exibidos no subpainel inferior direito.

   Use o gráfico e as legendas correspondentes a seguir para compreender os vários recursos do Visualizador do rastreamento de



transação.

A legenda a seguir identifica cada item por número e fornece mais informações:

Número	Nome	Mais informações
1	Rastreamentos de transação	Examine cada rastreamento de transação. Se houver mais de um, as informações sobre o rastreamento de transação selecionado serão exibidas em outros painéis.

2	Painel de detalhes do rastreamento de transação	Este painel mostra a pilha gráfica, que é a ordem das transações dos componentes de cima para baixo. Você pode se referir à pilha gráfica como "bolo de casamento", pois a representação pode se parecer com um bolo de casamento de cabeça para baixo.
3	Painel Informações sobre a transação	Este painel mostra informações sobre o rastreamento de transação selecionado. Observe que o caminho à direita da lista suspensa é o caminho do rastreamento de transação selecionado no painel Rastreamento de transação. Você pode escolher estas exibições na lista suspensa: **Árvore**, **Resumo**, **Data e hora do navegador**, **Propriedades do sistema** e **Instantâneo**.
4	Detalhes do componente	Este painel fornece informações sobre o componente selecionado na pilha gráfica. Quando você não tiver selecionado um componente, as informações serão sobre o componente do topo da pilha gráfica.
5	Navegação estrutural	O caminho localizado acima do Visualizador do rastreamento de transação.

A pilha gráfica e os dados de rastreamento de transação mostram informações que ajudam na avaliação do desempenho, por exemplo:

Relações de chamada entre componentes	As linhas dos componentes são exibidas de cima para baixo na ordem de chamada. **Observação:** chamada e componente são sinônimos. Ao selecionar um componente, você está selecionando uma chamada na transação. Uma chamada pode fazer chamadas filho, o que forma a pilha ou a profundidade: 1 linha = 1 ou mais chamadas = 1 ou mais componentes que podem fazer chamadas ou invocações filho A Exibição em árvore mostra uma correspondência de um-para-um dos dados: 1 linha = 1 chamada = 1 componente A visualização do resumo mostra dados agregados, não uma correspondência de um-para-um: 1 linha = caminho O caminho é o rótulo da chamada e o nível na pilha. Por exemplo, um "logon" de chamada foi feito 5 vezes no mesmo nível de pilha. Você vê 5 componentes na mesma linha. Na Exibição em árvore, você vê 5 linhas. A contagem da exibição Resumo é 5, e a coluna Duração Total mostra a soma dos tempos de todas as 5 chamadas.
Erros e instantâneos	O quadrado vermelho com o ícone de sinal de menos branco indica um componente com um erro. O ícone de câmera identifica uma transação com um instantâneo de paralisação ou erro relacionado. **Observação:** para obter mais informações, consulte Analisar instantâneos de paralisação e erros.
Pontos de entrada	Os pontos de entrada geralmente são exibidos como o primeiro componente de uma transação. Se a transação for uma transação comercial, a transação comercial será exibida como o primeiro componente seguido pelo ponto de entrada.
Sequência de transações	A colocação dos componentes da esquerda para a direita indica a sequência. O tempo relativo em milissegundos é exibido no topo da transação. Se o tempo de rastreamento for extenso o suficiente, ele será mostrado em segundos, horas e dias.

Dados de transação entre processos e entre JVMs	Um identificador exclusivo, a ID de correlação, transações de front-end e back-end rastreados por links.A sequência se baseia na ordem em que os front-ends chamam os back-ends em uma transação. A ID de correlação ajuda você a perceber quais chamadas podem ser a origem de uma transação lenta ou paralisada. Nos **Detalhes do componente** do Visualizador do rastreamento de transação, a ID de correlação é o valor da propriedade Realizar processamento cruzado dos dados. Várias pilhas gráficas no visualizador mostram processos relacionados para o evento de rastreamento selecionado.Os processos que são rastreados de diferentes agentes aparecem em diferentes áreas sombreadas. Examine os componentes vinculados em um rastreamento de transação para exibir transações entre processos ou entre JVMs. Por exemplo, veja se uma determinada transação saiu de um processo e, em seguida, entrou em outro processo. Também é possível perceber quais chamadas podem ser a origem de transações lentas e paralisadas. **Observação:** para obter mais informações sobre a correlação de transações, consulte Usar o rastreamento de transação entre processos para resolver problemas.
Componentes de visibilidade profunda	Um ícone de raio indica um componente de visibilidade profunda. Esse tipo de componente é um método ou componente que é detectado automaticamente sem o uso das Diretivas do ProbeBuilder. O Application Performance Management analisa métodos para a sua complexidade a fim de determinar as chamadas e os componentes a serem instrumentados e exibe como componentes de visibilidade profunda.
Visibilidade de lacuna do tempo de execução	Com visibilidade de lacuna do tempo de execução, os agentes instrumentam e monitoram automaticamente aplicativos com base no desempenho do tempo de execução. **Observação:** para obter mais informações, consulte Configurar a instrumentação inteligente.

4. (Opcional) Execute uma ou mais ações:
   – Digite uma sequência de caracteres de texto para filtragem de rastreamentos no campo Pesquisar.A pesquisa faz a correspondência com informações de todos rastreamentos de transação e componentes. Os resultados são mostrados em todas as exibições e em qualquer uma das propriedades dos **Detalhes do componente**. A pesquisa também retorna correspondências parciais. Por exemplo, os critérios de pesquisa são para `node1` . A exibição **Resumo** mostra os rastreamentos para `node1` , `node124` e `node1_323` .

     A pilha gráfica e as exibições mostram todos os componentes relacionados. Os componentes que correspondem à pesquisa são destacados em amarelo na pilha. Onde aplicável nas exibições, o texto correspondente tem um fundo amarelo.
   – Passe o mouse sobre o **ícone de informações** (o ponto azul com um i).

     Uma dica de ferramenta mostra o nome do agente totalmente qualificado. O ícone de informações e a linha correspondente representam cada agente individual.
5. Examine os rastreamentos de transação de cima para baixo para determinar quais rasteamentos o agente capturou.

NOTE

Se um número excessivo de rastreamentos tiver sido coletado, você será informado que o Visualizador do rastreamento de transação não poderá processá-los. (Por exemplo, no Internet Explorer, um pop-up explica que o arquivo JSON é muito grande para que se possa fazer upload.)

- Passe o mouse sobre um rastreamento ou componente para exibir a dica de ferramenta que mostra o resumo das informações sobre o rastreamento de transação. Quando apenas uma parte do componente é mostrada, a dica de ferramenta é útil.
- Use as funções de navegação para ajustar a exibição.
  Clique aqui para obter ajuda de navegação...

  Ampliar (Shift + Igual) muda a escala para mostrar mais detalhes.

  Reduzir (Shift + Menos) muda a escala para mostrar menos detalhes.

  Redefinir (Shift + R) retorna os dados do visualizador ao seu estado original.

  Centralizar (Shift + C) centraliza os dados do visualizador.

  Aplicar panorâmica para a esquerda (Shift + Esquerda) move o foco para a esquerda.

  Aplicar panorâmica para a direita (Shift + Direita) move o foco para a direita.

  A opção Select Next (seta para baixo) seleciona a próxima linha.

  A opção Select Previous (seta para cima) seleciona a linha anterior.

  Use os divisores que separam os painéis para exibir mais de um painel de interesse. Clique duas vezes em um separador para minimizar ou maximizar a parte superior e inferior dos painéis esquerdos.

  Clique na opção **Tamanho do encaixe** para aumentar ou diminuir o tamanho dos painéis direito e esquerdo relacionados entre si.

  Observe que uma seleção em qualquer representação é feita automaticamente nas outras representações quando há informações associadas e vice-versa. Por exemplo, clique em uma linha na pilha gráfica. A pilha gráfica, o item Informações sobre a transação, os **Detalhes do componente** e as exibições relacionadas mostram informações que correspondem a essa linha.

6. Clique no rastreamento de uma transação do seu interesse.
   É possível selecionar apenas um rastreamento de transação por vez.
7. Examine os componentes da pilha gráfica de cima para baixo para entender a sequência de chamada em um período. Um tempo de transação de componente incomumente longo pode indicar a causa raiz do problema.Observe que o nome e o primeiro número da linha do arquivo de origem do Java do método instrumentado do Java são exibidos entre parênteses.
   As linhas vermelhas indicam uma condição de erro. As linhas azul-claras indicam que não há problemas. As linhas laranja-claras indicam que a análise diferencial disparou um alerta. As linhas laranjas mais escuras indicam uma paralisação. As linhas amarelas indicam um resultado de pesquisa
   As transações que duram 0 milissegundo aparecem como um ponto no plano de fundo azul-claro.
8. Clique em um componente de interesse.
   No painel inferior direito, os painéis **Informações sobre a transação** e **Detalhe do componente** exibem informações detalhadas em seus respectivos subpainéis.
9. No subpainel superior, selecione uma opção na lista suspensa **SELECT A VIEW** para exibir várias representações dos dados. O comportamento da seleção varia de acordo com a exibição. Por exemplo, a exibição **Árvore** lista os caminhos do rastreamento de transação, ao passo que **Data e hora do navegador** mostra os dados de páginas permanentes e os recursos associados a páginas temporárias. Portanto, as informações que você pode selecionar para essas exibições são diferentes.
   Árvore
   A exibição **Árvore** lista os caminhos de rastreamento em ordem hierárquica de chamada. Cada caminho inclui os nomes de classes e métodos de uma chamada. É possível exibir as alterações que ocorreram entre um ponto inicial e um ponto final de um rastreamento. Os dados Caminho, Marca de data e hora, Duração, Percentual e Número de itens chamados são exibidos em colunas que podem ser classificadas. (A Linha de fonte não é classificável.) Alguns rastreamentos de um componente podem não ter informações sobre a linha de fonte. Nesse caso, N/D (não aplicável) será exibido na coluna Linha de fonte. Ajuste a quantidade de informações exibida ao

expandir ou recolher os caminhos.Os ícones coloridos indicam o tipo de rastreamento.Por exemplo, laranja-claro

indica que a análise diferencial disparou um alerta; uma transação apresenta variação não controlada. A exibição **Árvore** permite percorrer a análise de dados e navegar até componentes específicos para identificar problemas de desempenho. Os valores dos dados ajudam a entender como um valor inicial é afetado por uma série de valores intermediários.

Resumo

A exibição **Resumo** mostra os dados nas cores que indicam o tipo de rastreamento. (O sombreado dos valores de índice de chamada mais altos é mais profundo porque as chamadas são processadas uma em cima da outra.) Esse resumo visual permite que você identifique as áreas com problema rapidamente. Após a identificação de um problema, você poderá usar a exibição **Árvore** para investigar os detalhes desse tipo de chamada.

Os dados da coluna mostram os totais de cada linha. Por exemplo: um componente é chamado 100 vezes na linha de nível 4 de uma transação. A contagem de linhas de nível 4 é 100. Cada chamada dura 2 milissegundos, portanto, a duração total é de 200 milissegundos (100 x 2). O valor da duração total na navegação estrutural pode ser diferente do valor de duração total no **Resumo**. Essa diferença pode ocorrer porque o valor da navegação estrutural inclui todos os rastreamentos correlacionados de um back-end e o valor da exibição **Resumo**, não.

Data e hora do navegador

Data e hora do navegador mostra dados de páginas permanentes e seus recursos, bem como de recursos que estão associados a páginas temporárias. (Os dados de uma página temporária em si não são exibidos.)

> **NOTE**
> Para obter mais informações sobre Data e hora do navegador, consulte Diagnosticar problemas de carregamento de recursos.

Propriedades do sistema

As propriedades do sistema fornecem dados de monitoramento do tempo de CPU e de contenção de segmentos para rastreamentos de transações no método do servlet.

> **NOTE**
> Para obter mais informações sobre Propriedades do sistema, consulte Diagnosticar problemas de desempenho do sistema.

Instantâneo

O instantâneo fornece informações sobre os instantâneos de paralisação do erro.

> **NOTE**
> Para obter mais informações sobre instantâneos de paralisação e erro, consulte Analisar instantâneos de paralisação e erro.

10. Examine o painel **Detalhes do componente**.
    Clique aqui para obter os detalhes do componente...

    > **NOTE**
    >
    > Nem todas as informações sobre os componentes de uma visibilidade profunda estão disponíveis.

    Nome - o nome do componente, por exemplo: Default

    Caminho - o nome completo do recurso do componente, por exemplo: `Frontends|Apps|AuthenticationService|URLs|Default`
    Duração - o tempo de execução em milissegundos do componente selecionado
    Marca de data e hora (relativa) - a hora de início (com base no relógio do sistema) da invocação do componente raiz
    Percentual da duração - a porcentagem de tempo total da transação

    Propriedades do sistema - os dados de tempo permitem diagnosticar problemas de desempenho nos segmentos do método. As caixas coloridas identificam as várias propriedades do sistema. Um gráfico de barras representa os valores de dados para essas propriedades do sistema. Quando os valores são 0 ms, o gráfico mostra uma linha preta. Cada propriedade do sistema e seu valor são listados abaixo do gráfico.
    Propriedades -- uma lista das propriedades opcionais do componente, incluindo a seguinte propriedade:

- Linha de fonte - apenas agente do Java - o nome e o número da primeira linha do arquivo de origem do método instrumentado do Java. O agente do Java não coleta os números de linha do código que chama o método instrumentado do Java. Os despejos de pilha de segmento de exceção padrão em depuradores e despejos centrais normalmente exibem esses números de linha.

  TIP

  Clique em **Expandir** para expandir a árvore inteira. Clique em **Recolher** para recolher a árvore inteira. Clique na seta para a direita ao lado de um componente para mostrar um único subcomponente.

  Redimensione qualquer coluna para mostrar mais ou menos informações.

  Passe o mouse sobre um **nome de coluna** ou um **segmento do gráfico de propriedades do sistema** para ver uma dica de ferramenta com informações sobre o item.

11. Determine a causa raiz do problema de desempenho do aplicativo. Use as informações de identificação para reunir detalhes específicos sobre o problema. De modo geral, você procura os componentes de execução mais longa e profunda no rastreamento. Por exemplo:
    - Uma única chamada a um banco de dados
    - Uma grande quantidade de chamadas rápidas que juntas resultam em alta latência

Entre em contato com a equipe de operações para solicitar uma revisão de código do aplicativo. A equipe determina se existe um problema de código ou de dependência de aplicativo.

NOTE

Mais informações: Analisar rastreamentos e colaborar na análise de problemas.

Diagnosticar problemas de carregamento do recurso

Para diagnosticar problemas de desempenho em uma página da web, você deve examinar a data a e hora dos recursos que seu HTML e JavaScript estão baixando. A exibição **Data e hora do navegador** no Visualizador do rastreamento de transação ajuda a visualizar os recursos que foram baixados em resposta a solicitações HTTP associadas a um rastreamento. Data e hora do navegador representa dados que são gerados de modo cumulativo e sequencial em um rastreamento de transação. Você pode examinar as informações detalhadas sobre os dados do rastreamento. Os dados aparecem para páginas permanentes e seus recursos, bem como para recursos que estão associados a páginas temporárias. (Os dados de uma página temporária em si não são exibidos.) Os recursos são exibidos em cinza por padrão e cada fase tem a sua própria cor. Essa representação em cascata ajuda a entender como os diferentes fatores contribuem para um rastreamento de transação. Essa exibição funciona de maneira semelhante a uma exibição em cascata nas ferramentas do desenvolvedor do navegador.

NOTE

Mais informações: Examinar componentes individuais e dados de rastreamento.

Siga estas etapas:

1. Na guia **Transações comerciais**, clique em um rastreamento de transação de interesse.
   Os componentes da transação individual são exibidos em uma pilha gráfica (bolo de casamento), no painel **Transaction Trace Detail**.
2. Examine os componentes na pilha gráfica, de cima para baixo, para entender a sequência de chamada em um período. Um tempo de transação de componente incomumente longo pode indicar a causa raiz do problema.
3. Clique em um componente de interesse.
4. No painel **Informações sobre a transação**, selecione **Data e hora do navegador**, na lista suspensa **SELECT A VIEW**.
5. Examine as informações exibidas na exibição para diagnosticar problemas de carregamento de recurso:

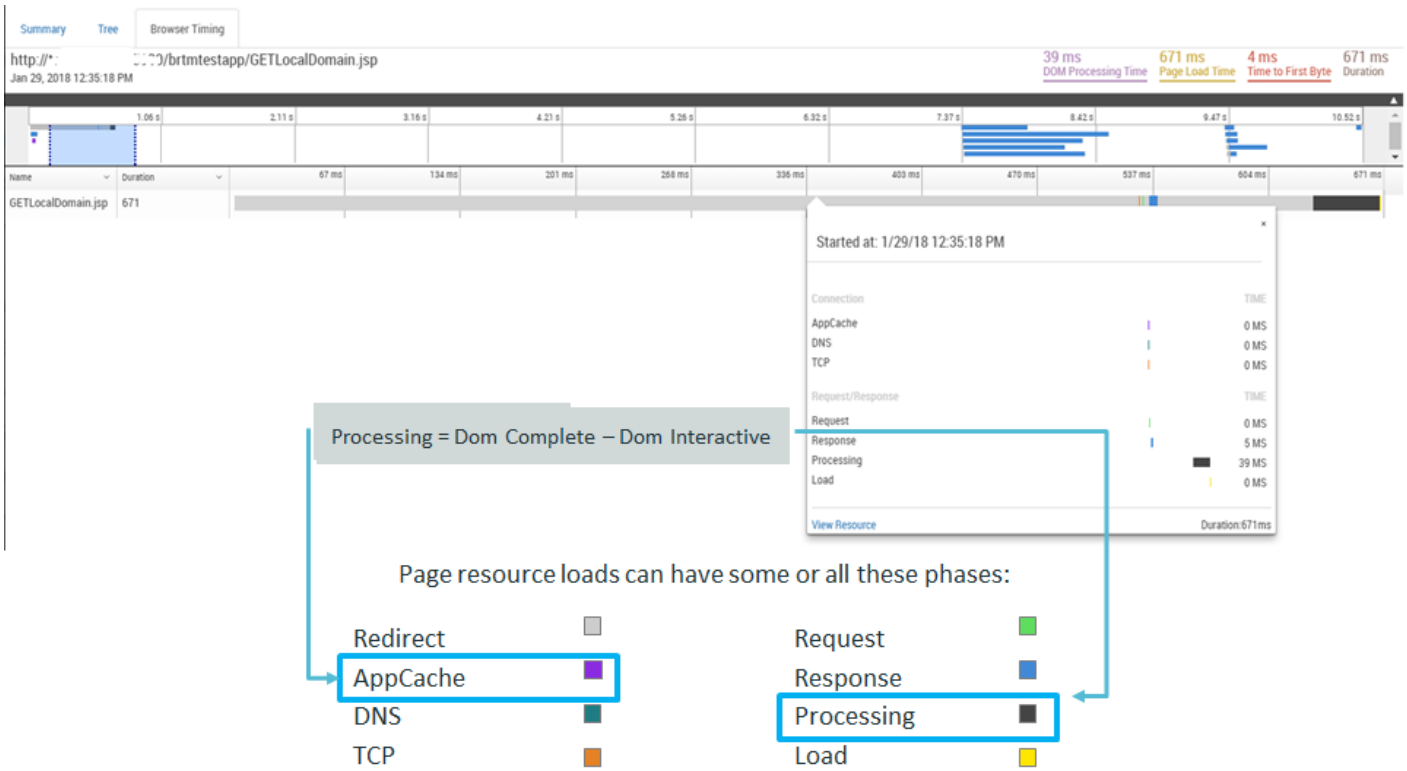
A exibição **Data e hora do navegador** consiste em três partes:

- Uma área de resumo que contém informações sobre o componente no rastreamento que disparou o download do recurso.
- Uma linha de tempo que permite restringir o intervalo de datas para focar em recursos específicos. O intervalo da linha de tempo permite exibir todos os recursos no contexto e restringir o período exibido na grade. É possível alterar o intervalo arrastando os marcadores no final ou arrastando a linha inteira do meio.
- Uma grade que mostra uma linha de detalhes de cada recurso.

A grade inclui os seguintes tipos de linha:

- Linhas de carregamento da página
  Quando o rastreamento selecionado representa um carregamento de página permanente, a página em si é representada na grade. (Um carregamento de página temporária simplesmente atualiza a página existente usando JavaScript). A última coluna na grade mostra o intervalo de datas selecionado, dividido em 10 períodos iguais. Uma barra cinza representa a duração total do carregamento da página e as faixas coloridas representam várias "fases" no carregamento da página. As durações das fases não podem totalizar a duração geral do carregamento da página, pois a duração geral inclui a duração de Data e hora do navegador. A duração de Data e hora do navegador inclui datas e horas relacionadas à rede e alternância de contexto do navegador. Para exibir o detalhamento de data e hora de um rastreamento, passe o mouse sobre a fase.
  Os carregamentos de recurso da página podem ter algumas ou todas as seguintes fases:
- – Redirecionamento
  – AppCache
  – DNS
  – TCP
  – Solicitação
  – Resposta
  – Processamento
  – Carregamento

  O Agente do navegador relata diretamente a maioria das fases, mas duas fases são calculadas como mostrado no seguinte gráfico:
- AppCache: DNS (Pesquisa do domínio) – Buscar
- Processamento: Conclusão do dom – Dom interativo



- Linhas de carregamento de recurso
  As fases do recurso não são exibidas na pilha (bolo de casamento), de modo que não é possível ver os dados brutos das fases. Cada recurso que a página baixa tem uma linha na grade Data e hora do navegador. Tal como as informações de carregamento de página, é possível ver mais detalhes de cada recurso passando o mouse sobre o respectivo gráfico na grade.
  Os carregamentos de recurso podem ter algumas ou todas as seguintes fases:
  – AppCache
  – DNS
  – TCP
  – Solicitação
  – Resposta
  – Tempo de execução de retorno de chamada
  Os recursos que a página baixa são exibidos da mesma maneira que os carregamentos de página, mas as fases são ligeiramente diferentes. O Agente do navegador relata todas as fases, exceto AppCache. AppCache é calculada como DNS – Buscar. O seguinte gráfico mostra as fases de carregamento de recurso:

Summary Tree Browser Timing

http:// :5080/brtmtestapp/GETLocalDomain.jsp
Jan 29, 2018 12:35:18 PM

Name	Duration
GETLocalDomain.jsp	671
framework.pack.js.s...	56
hexa.png	24
sample.txt	526
sample.txt	1160
sample.txt	950
sample.txt	805
sample.txt	959
sample1.txt	76
sample1.txt	98
sample1.txt	97
sample1.txt	322
sample1.txt	78
sample.txt	46

Resource loads can have some o

AppCache = DNS - Fetch

Redirect
AppCache
DNS
TCP

Reque
Respo
Callba

Os valores de rastreamento de recurso podem não corresponder aos valores de data e hora para os mesmos rastreamentos na guia Firefox Network. Além disso, a exibição **Data e hora do navegador** não mostra alguns recursos que são exibidos na guia Rede. Os valores incompatíveis ocorrem para todos os recursos, pois o valor de data e hora da guia Firefox Network é o início da solicitação ao fim da resposta. Contudo, a duração de Data e hora do navegador inclui datas e horas relacionadas à rede e alternância de contexto do navegador. Os recursos que estiverem ausentes na exibição Data e hora do navegador são filtrados por padrão (não configurável). Esses recursos incluem solicitações pelo cliente para a configuração de perfil e o envio das respostas da métrica. Data e hora do navegador não relata métricas de página para recursos obrigatórios para o Agente do navegador. O valor da duração total pode não corresponder em todos os navegadores, pois o tempo de execução do retorno de chamada é adicionado para ajustar o valor da duração.

NOTE
A data e a hora podem ser arredondadas para mais ou para menos em um milissegundo.

Diagnosticar problemas de desempenho do sistema

A exibição Propriedades do sistema do Visualizador do rastreamento de transação fornecem dados de monitoramento do tempo de CPU e de contenção de segmentos dos rastreamentos de transações nos métodos da API do Servlet.

NOTE

Mais informações: Examinar componentes individuais e dados de rastreamento.

Geralmente, os métodos são executados quando o usuário clica em um link, envia um formulário ou executa outro tipo de ação em um site.As propriedades do sistema podem ajudá-lo a compreender a origem da lentidão, do travamento de servidor ou do uso excepcionalmente alto da CPU, por exemplo:

- O DX APM exibe as métricas de paralisação, mas nenhuma transação é exibida na execução de um rastreamento de transação. Essa situação pode ocorrer porque as transações não estão sendo concluídas e o Gerenciador corporativo está recebendo informações incompletas sobre o travamento do servidor do agente.
- O uso da CPU para um aplicativo é baixo, mas há tempos de resposta demorados. Essa situação pode indicar que todos os segmentos em uma operação estão bloqueados ou em espera.
- Um método está demorando muito tempo para carregar; um segmento pode estar usando uma grande quantidade dos recursos da CPU.

Os dados de tempo permitem diagnosticar problemas de desempenho nos segmentos do método.

Siga estas etapas:

1. Na guia **Transações comerciais**, clique em um rastreamento de transação de interesse.
   Os componentes da transação individual são exibidos em uma pilha gráfica no painel **Detalhes da transação**.
2. No painel **Informações sobre a transação**, selecione **Propriedades do sistema**, na lista suspensa **SELECT A VIEW**.
3. Examine as informações na grade. Os valores de dados são mostrados como a duração, em milissegundos, e como a porcentagem do tempo total gasto em cada método ou segmento. Procure valores elevados para saber quais segmentos usam alta capacidade de processamento, estão aguardando ou estão bloqueados.

   TIP

   Quando você clica em uma linha na grade, o rastreamento correspondente é realçado na pilha gráfica e vice-versa.

   Métricas do agente do Java

   Tempo total de CPU - o tempo total da CPU para o segmento atual, qualquer segmento ou nenhum segmento. O valor é o total de tempo do sistema da CPU mais o tempo do usuário da CPU.

   Tempo da CPU do usuário - o tempo que o processador gastou executando o código do programa ou o código em bibliotecas para uma transação quando a JVM oferece suporte à mediação do tempo de CPU.

Tempo da CPU do sistema - o tempo gasto executando código no kernel do sistema operacional em uma transação de aplicativo monitorado quando a JVM oferece suporte à medição de tempo de CPU.

Tempo de espera - o tempo decorrido aproximado em que um segmento de transação esteve no estado WAITING ou TIMED_WAITING quando a JVM oferece suporte ao monitoramento de contenção de segmento.

Bloqueado - o tempo decorrido aproximado em que um segmento esteve no estado BLOCKED quando a JVM oferece suporte ao monitoramento de contenção de segmento.

Outros - o tempo decorrido aproximado que não seja a soma do tempo da CPU, do tempo bloqueado e do tempo de espera

Memória alocada - o número aproximado de bytes alocados para a memória heap do segmento de transação quando a JVM oferece suporte à medição da alocação de memória do segmento.

Caminho - o nome do recurso completo do segmento.

Métricas do agente do .NET/.NET Core

Tempo da CPU do usuário - o tempo que o processador gastou executando o código do programa ou o código em bibliotecas para uma transação quando o CLR do .NET/.NET Core oferece suporte à mediação do tempo de CPU.

Tempo da CPU do sistema - o tempo gasto executando código no kernel do sistema operacional em uma transação de aplicativo monitorado quando o CLR do .NET/.NET Core oferece suporte à medição de tempo de CPU.

4. Encontre detalhes sobre **Propriedades do sistema** nos **Detalhes do componente**. Os valores de tempo estão em milissegundos. Estas propriedades se aplicam ao tempo do sistema:
   Tempo bloqueado (ms) - o tempo decorrido aproximado em que um segmento esteve no estado BLOCKED quando a JVM oferece suporte ao monitoramento de contenção de segmento.
   Tempo da CPU do sistema (ms) - o tempo gasto executando código no kernel do sistema operacional em uma transação de aplicativo monitorado quando a JVM oferece suporte à medição de tempo de CPU.
   Tempo de CPU (ms) - o tempo total da CPU para o segmento atual, qualquer segmento ou nenhum segmento. O valor é o total de tempo do sistema da CPU mais o tempo do usuário da CPU.
   Tempo da CPU do usuário - o tempo que o processador gastou executando o código do programa ou o código em bibliotecas para uma transação quando a JVM oferece suporte à mediação do tempo de CPU.
   Outro tempo (ms) - o tempo decorrido aproximado que não seja a soma do tempo da CPU, do tempo bloqueado e do tempo de espera.
   Tempo de espera (ms) - o tempo decorrido aproximado em que um segmento de transação esteve no estado WAITING ou TIMED_WAITING quando a JVM oferece suporte ao monitoramento de contenção de segmento.

Detectar e analisar erros e paralisações

Uma *paralisação* é uma transação ou um componente de uma transação que não foi concluído dentro do limite de tempo especificado.Depois de determinar o local de uma transação ou de um componente paralisado, você pode:

Como analisar erros e paralisações

Quando usar esse cenário

Você usa esse cenário quando tem um problema de desempenho de aplicativo, conforme exibido no painel DX Application Performance Management ou quando relatado em uma notificação.

Pré-requisito

Isole o local do problema antes de iniciar.

Os agentes coletam dados sobre transações e os enviam ao Enterprise Manager para processamento e exibição. Esses dados incluem informações sobre erros e paralisações de aplicativo.

Erro
Um erro é uma exceção relatada pelos códigos de erro da JVM ou do HTTP. Por exemplo:

- um status de erro HTTP – por exemplo, 404, Page Not Found

- uma exceção SQL
- uma exceção Java

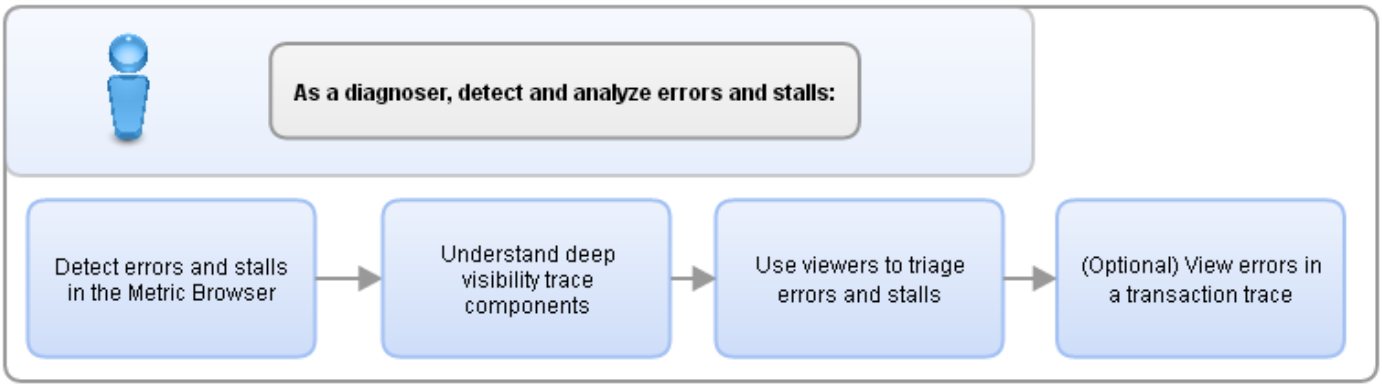
Paralisação
Uma paralisação é uma transação ou um componente de uma transação que não foi concluído dentro do limite de tempo especificado.

Você pode executar estas tarefas:

- Detectar e fazer triagem da causa de paralisações e erros graves conforme eles ocorrem e monitor os eventos relacionados.
- Determinar a frequência e a natureza dos erros.
- Determinar a causa raiz de um problema.

O diagrama a seguir descreve como analisar erros e paralisações a fim de identificar a causa raiz do problema de desempenho de um aplicativo.

Figure 9: 9.8 Detectar e analisar erros e paralisações



Siga estas etapas:

1. Detecte erros e paralisações na Exibição da métrica.
2. Entenda os componentes de rastreamento de ampla visibilidade.
3. Use visualizadores para classificar erros e paralisações.
4. (Opcional) Exiba erros no rastreamento de transação.

Detectar erros e paralisações na Exibição da métrica

Você pode detectar e classificar a causa de erros e paralisações graves à medida que eles ocorrem. É possível monitorar os agentes e componentes conferindo as informações detalhadas na guia **Exibição da métrica**.

O DX Application Performance Management atualiza a exibição do erro e as informações de paralisação a cada 15 segundos.

Siga estas etapas:

1. Vá para o Team Center.
2. Na **Exibição da métrica**, procure o agente ou componente que deseja monitorar e selecione a guia **Erros** na parte inferior da página.
   A guia **Erros** exibe dados relatados por um agente sobre um CLR da JVM ou do .NET. Se algum erro ou paralisação estiver sendo relatado para o agente ou componente, uma lista de erros e paralisações será exibida.

  – Descrição da guia Erro selecionada.
3. Selecione a guia **Rastreamentos**.
   Descrição da guia Rastreamentos selecionada.
4. Clique em Marca de data e hora para classificar. À medida que novos erros e paralisações ocorrem, eles aparecem na ordem classificada.

Componentes de rastreamento de ampla visibilidade

Quando a instrumentação inteligente está ativada, os agentes detectam e coletam automaticamente informações detalhadas sobre componentes de transação no nível do método. Os agentes detectam e instrumentam automaticamente os componentes de ampla visibilidade sem usar as PBDs (ProbeBuilder Directives - Diretivas do ProbeBuilder). Os componentes de ampla visibilidade que você exibe em transações paralisadas contêm somente nome da classe, nome do método e duração. Dependendo de seus requisitos e do ambiente, é possível configurar a profundidade e o escopo da ampla visibilidade de rastreamento. Por exemplo, defina se o agente irá detectar e instrumentar automaticamente uma quantidade baixa, média ou alta de código do aplicativo. Para obter mais informações, consulte Configurar a instrumentação inteligente.

> **NOTE**
> A instrumentação inteligente está disponível somente para agentes do Java, não para agentes do .NET.

Detectar erros na Exibição da métrica

Os agentes coletam dados sobre transações e os enviam ao Enterprise Manager para processamento e exibição em um visualizador de dados. Esses dados incluem informações sobre erros de aplicativo. Você pode detectar e classificar a causa dos erros à medida que eles ocorrem. É possível monitorar os agentes e componentes conferindo as informações detalhadas na guia **Exibição da métrica**.

O DX Application Performance Management atualiza a exibição das informações de erro a cada 15 segundos.

Siga estas etapas:

1. Vá para o Team Center.
2. Na **Exibição da métrica**, vá para o agente ou componente que deseja monitorar.
3. Procure a métrica Erros por intervalo. Se o valor:
   = 0, não há erros atuais.
   > 0 pular para a Etapa 4: selecione a guia Rastreamentos.
4. Selecione a guia **Rastreamentos**.
5. Clique em um cabeçalho de coluna para classificar as linhas pelo conteúdo da coluna. À medida que novos rastreamentos ocorrem, eles aparecem na ordem de classificação. Os erros na lista de rastreamentos aparecem em vermelho.
6. Exiba o erro no rastreamento de transação que o Introscope coletou automaticamente.
   Se os rastreamentos automáticos de transação não forem exibidos, consulte Rastreamentos de transação coletados automaticamente.
7. Selecione a guia **Erros**.
   A guia Erros exibe dados relatados de um CLR da JVM ou do .NET por um agente. Se algum erro estiver sendo relatado para o agente ou componente, uma lista de erros será exibida. Clique em um cabeçalho de coluna para classificar as linhas pelo conteúdo da coluna. À medida que novos erros ocorrem, eles aparecem na ordem de classificação.
8. Selecione um instantâneo do erro para obter mais informações sobre ele, incluindo o caminho de chamada e os parâmetros. Use os visualizadores de eventos dinâmicos e históricos para fazer a triagem dos problemas.

Exibir erros em um rastreamento de transação

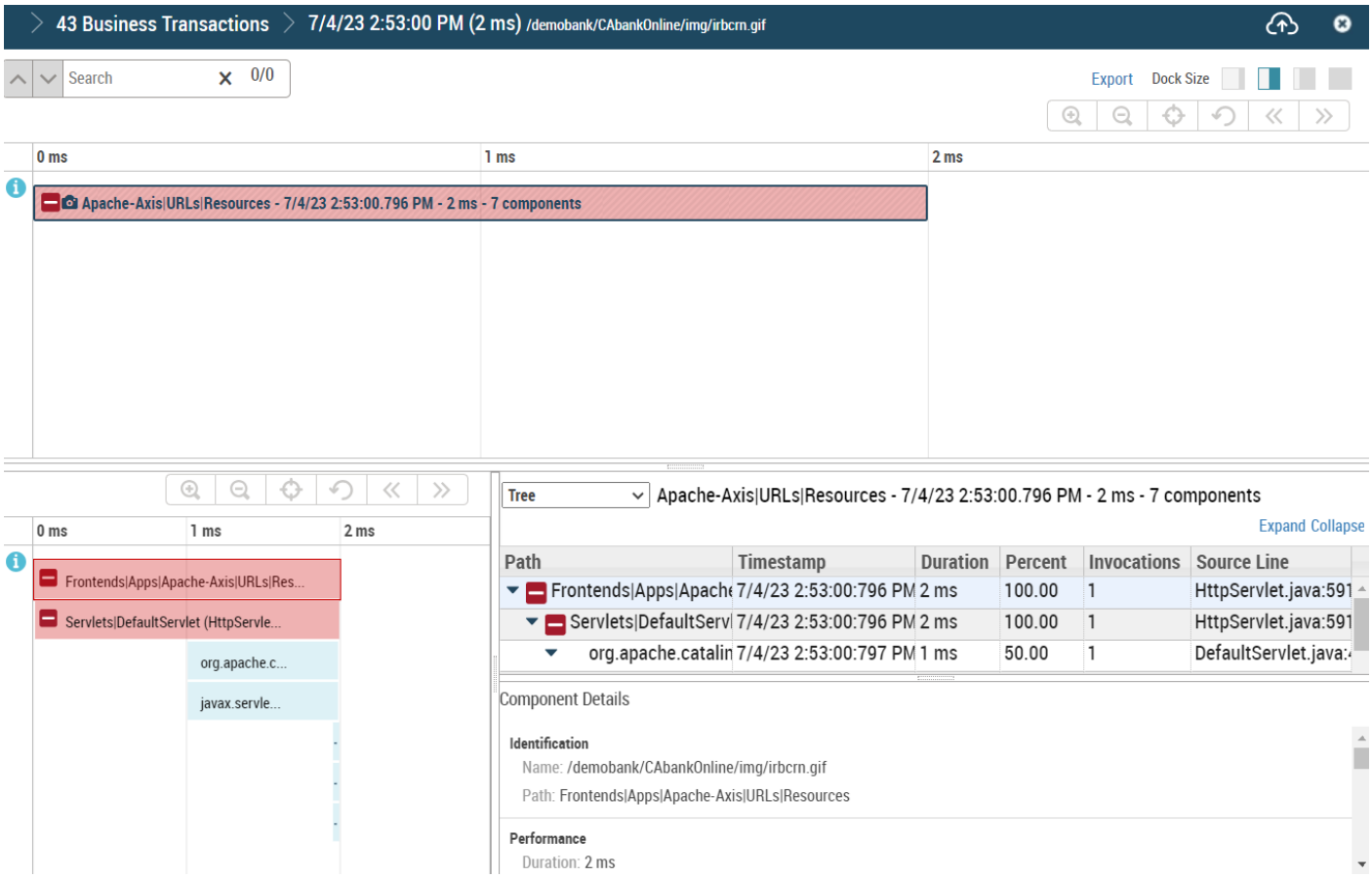
Você pode ver as informações do erro, incluindo componentes de ampla visibilidade, em um rastreamento de transação.

Você pode usar dois métodos para coletar os rastreamentos de transação para ver informações do erro:

- Execute um rastreamento de transação manualmente.
- Quando a instrumentação inteligente está ativada, o Introscope coleta automaticamente um rastreamento de transação quando um erro ocorre.
  Quando um erro dispara um rastreamento de transação automático, esses detalhes do componente exibem:
  - O componente que gerou a exceção inclui as propriedades do componente.
  - O primeiro componente no rastreamento de transação exibe a propriedade Critérios dos disparador de rastreamento automático como Erro.

Siga estas etapas:

1. Vá para o Team Center.
2. Clique na **Exibição da métrica**.
3. Selecione um aplicativo na árvore de métricas.
4. Clique na guia **Error View** no painel inferior.
   Observação: no modo Dinâmico, a guia Rastreamentos lista os eventos de rastreamento de transação dos últimos 20 minutos. Os eventos de rastreamento de transação com mais de 20 minutos não são exibidos no modo dinâmico.
5. Selecione um dos erros listados para exibir informações detalhadas.
   Uma tela exibe a descrição completa do erro selecionado.



6. Determine a causa raiz do problema de desempenho do aplicativo.
   Use as informações de identificação nas guias disponíveis para reunir detalhes específicos sobre o problema. Exiba estes campos: marca de data e hora, duração, descrição, ID de usuário (se nenhum estiver associado ao problema), mensagem de erro, tempo da chamada e caminho.
   É possível:

– Classifique as colunas para encontrar as chamadas ou os métodos com o tempo de resposta mais longo ou com mais erros.
– Use a guia Pesquisar para filtrar os resultados.
– Use as mensagens de erro e outras informações para entender mais sobre o problema.

Depois de identificar os componentes aparentemente causadores do problema, a equipe de operações poderá solicitar uma alteração no código do aplicativo para resolver o problema.

Analisar instantâneos de erro e paralisação

Os agentes detectam e coletam automaticamente informações detalhadas sobre componentes de transação para o nível de método.Esses dados incluem informações sobre erros e paralisações de aplicativo:

- **Erro**
  Determinados eventos em um aplicativo causam erros de transação, por exemplo:
  - um status de erro HTTP, por exemplo: 404 Not Found
  - uma exceção em um método
  - uma exceção no código não instrumentado, por exemplo, em um componente de rastreamento profundo.
  - uma implementação do rastreador de erros personalizado na lógica do Framework ou Communication
- **Paralisação**
  Uma paralisação é uma transação ou um componente de uma transação que não foi concluído dentro do limite de tempo especificado.

Um *instantâneo* mostra os caminhos de rastreamento de transações para um erro ou uma paralisação, bem como os detalhes sobre o que estava acontecendo quando o evento ocorreu.

Uma transação pode incluir erros e paralisações que disparam instantâneos associados. Por exemplo, uma transação tem 100 chamadas. A chamada 3 começa a ser executada lentamente e dispara um instantâneo de paralisação. Depois de algumas chamadas, chegamos à chamada 6, que apresenta um erro problemático, o qual dispara um instantâneo de erro. A chamada 81 encontra um erro diferente, o qual dispara outro instantâneo de erro.

No Visualizador do rastreamento de transação, a exibição **Árvore** mostra todas as chamadas de cada caminho possível em uma transação. A exibição do **Instantâneo** mostra um caminho por meio de uma transação. Este é o caminho de chamada direta de uma paralisação ou um erro específicos. Portanto, na exibição **Árvore**, você normalmente vê várias camadas de chamadas, enquanto na exibição Instantâneo, os instantâneos de paralisação e erro estão em apenas uma camada.

NOTE

Mais informações: Examinar componentes individuais e dados de rastreamento.

Examinar os instantâneos para investigar erros e paralisações

Um instantâneo o ajuda a executar estas tarefas:

- Detectar e fazer triagem da causa de paralisações e erros graves conforme eles ocorrem e monitor os eventos relacionados.
- Determinar a frequência e a natureza dos erros.
- Determinar a causa raiz de um problema.

Siga estas etapas:

1. Na guia **Transação comercial**, selecione **Instantâneo** na lista suspensa **Tipo de rastreamento**.
2. Selecione o rastreamento que deseja investigar.
   Os componentes da transação individual são exibidos em uma pilha gráfica (bolo de casamento), em **Detalhes da transação**.

Uma linha vermelha e uma caixa vermelha com um ícone branco de sinal de menos identificam um rastreamento com um erro.

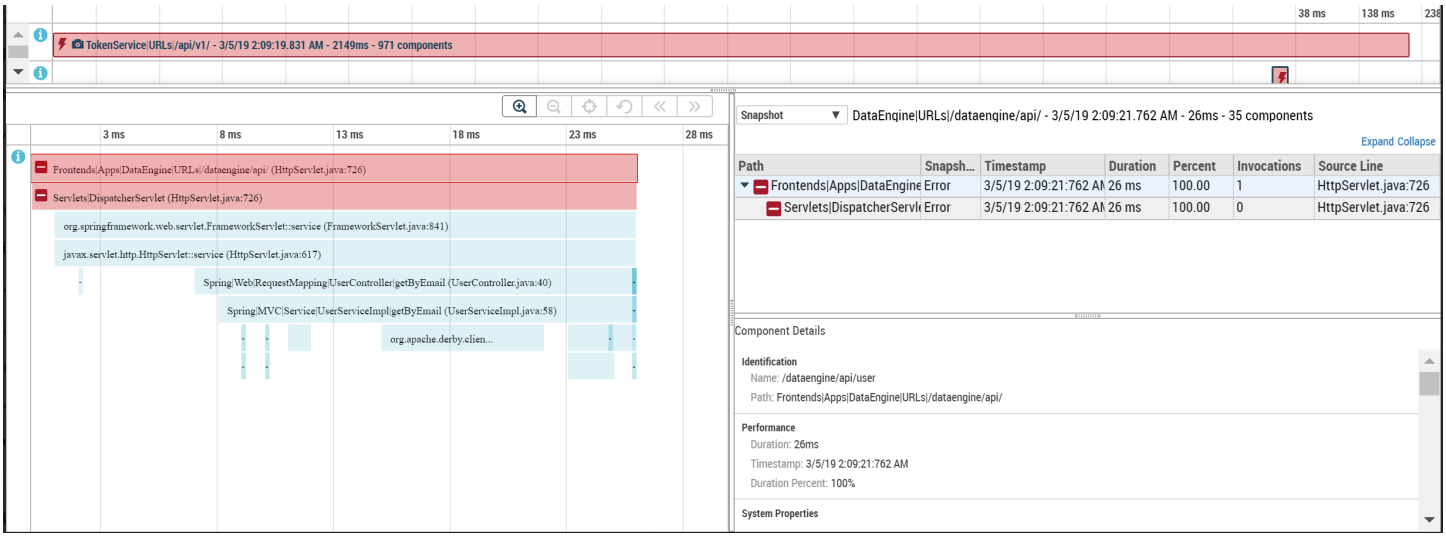
3. Na pilha gráfica, observe as características do instantâneo usando estes identificadores:
   Um ícone de câmera
   identifica uma transação normal com um ou mais instantâneos relacionados.
   Um prefixo **Instantâneo do erro** antes do nome do componente identifica uma única transação com um instantâneo, mas sem caminhos de rastreamento relacionados a um erro ou uma paralisação. Uma transação pode não ter rastreamentos relacionados nestes casos:
   - Você está usando um agente que não está atualizado para a release atual.
   - Um problema na transação ocorre antes de as informações de correlação serem extraídas da carga de solicitação. Nesse caso, as informações de rastreamento não são incluídas no evento.
   - O agente não relata todos os rastreamentos porque depende da amostragem. Por padrão, os agentes pegam uma amostra do comportamento da transação rastreando periodicamente cada URL exclusivo normalizado em um aplicativo. Um evento de erro que não tem rastreamento de transação pode ocorrer devido à implementação da detecção de erro (rastreador do agente) ou porque um limite para rastreamentos foi atingido no Gerenciador corporativo ou no agente.
4. No painel **Rastreamento de transação**, selecione um rastreamento de interesse.
5. No painel **Informações sobre a transação**, selecione o **Instantâneo** na lista suspensa.
   As listas de exibição **Instantâneo** rastreia caminhos em ordem hierárquica de chamada. Considere um rastreamento na grade como uma árvore com diferentes ramificações de folhas. Um instantâneo é um caminho por um conjunto de ramificações até uma folha. Você pode ter vários instantâneos, e cada um é representado como uma "raiz" na grade. Um instantâneo ajuda a detectar erros ou paralisações que ocorreram em várias ramificações. A árvore expandida é chamada de instantâneo e mostra onde o problema ocorreu no caminho de chamada.A árvore permite percorrer a análise de dados e navegar até componentes específicos para identificar problemas de desempenho. Os valores dos dados ajudam a entender como um valor inicial é afetado por uma série de valores intermediários. O valor em **Tipo de instantâneo** mostra Erro ou Paralisação.

   TIP

   Quando você clica em uma linha na grade, o rastreamento correspondente é realçado na pilha gráfica e vice-versa.
6. Examine o instantâneo para encontrar a causa raiz do problema.
7. Identifique os componentes aparentemente culpados pelo problema. A equipe de operações pode solicitar uma alteração no código do aplicativo para resolver o problema.

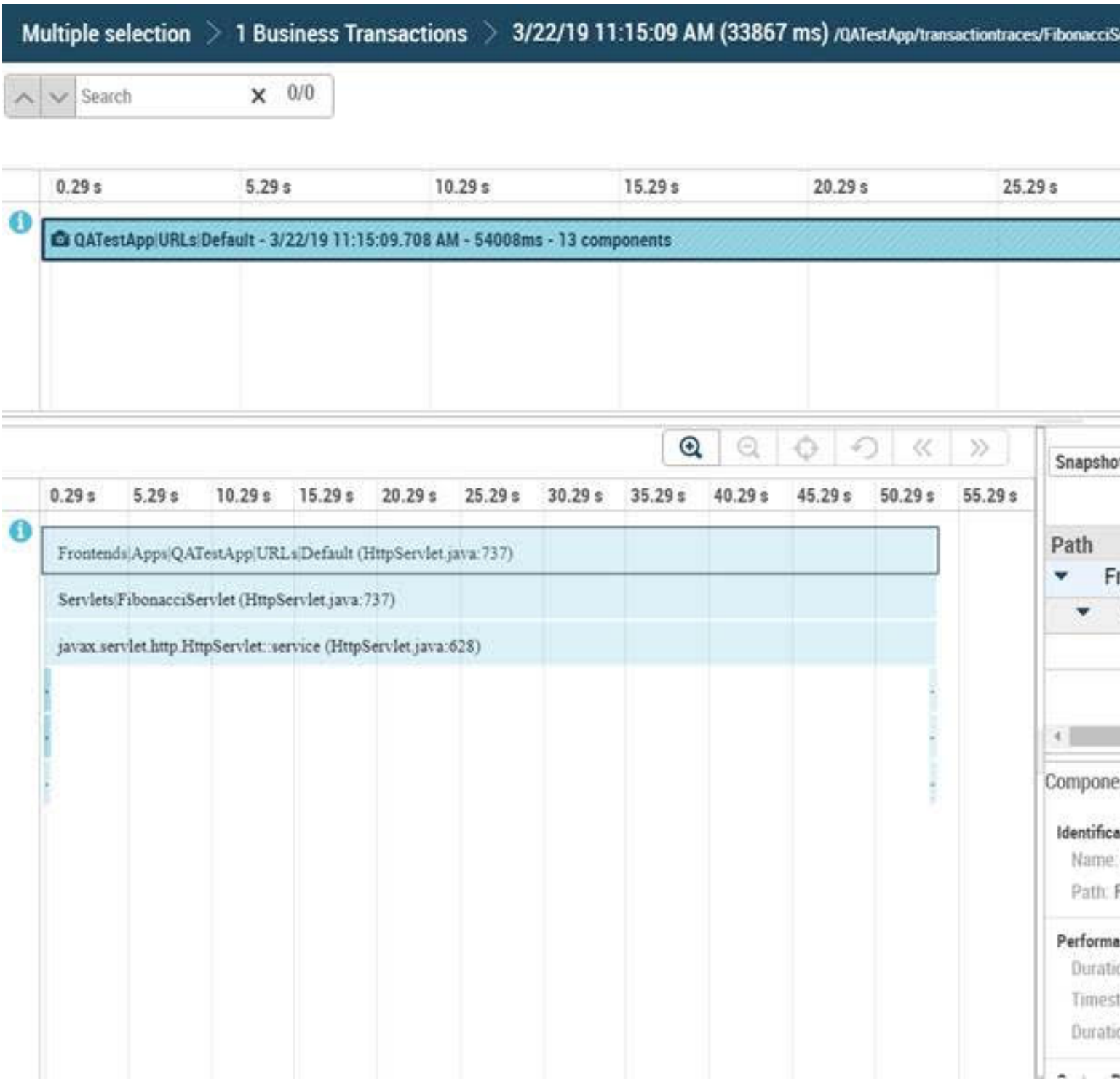
Exemplo: transação com um instantâneo de erro relacionado

O gráfico a seguir mostra uma transação com um instantâneo de erro relacionado.Observe o ícone de câmera à esquerda do rastreamento de transação e o valor **Erro** na coluna **Instantâneo.**



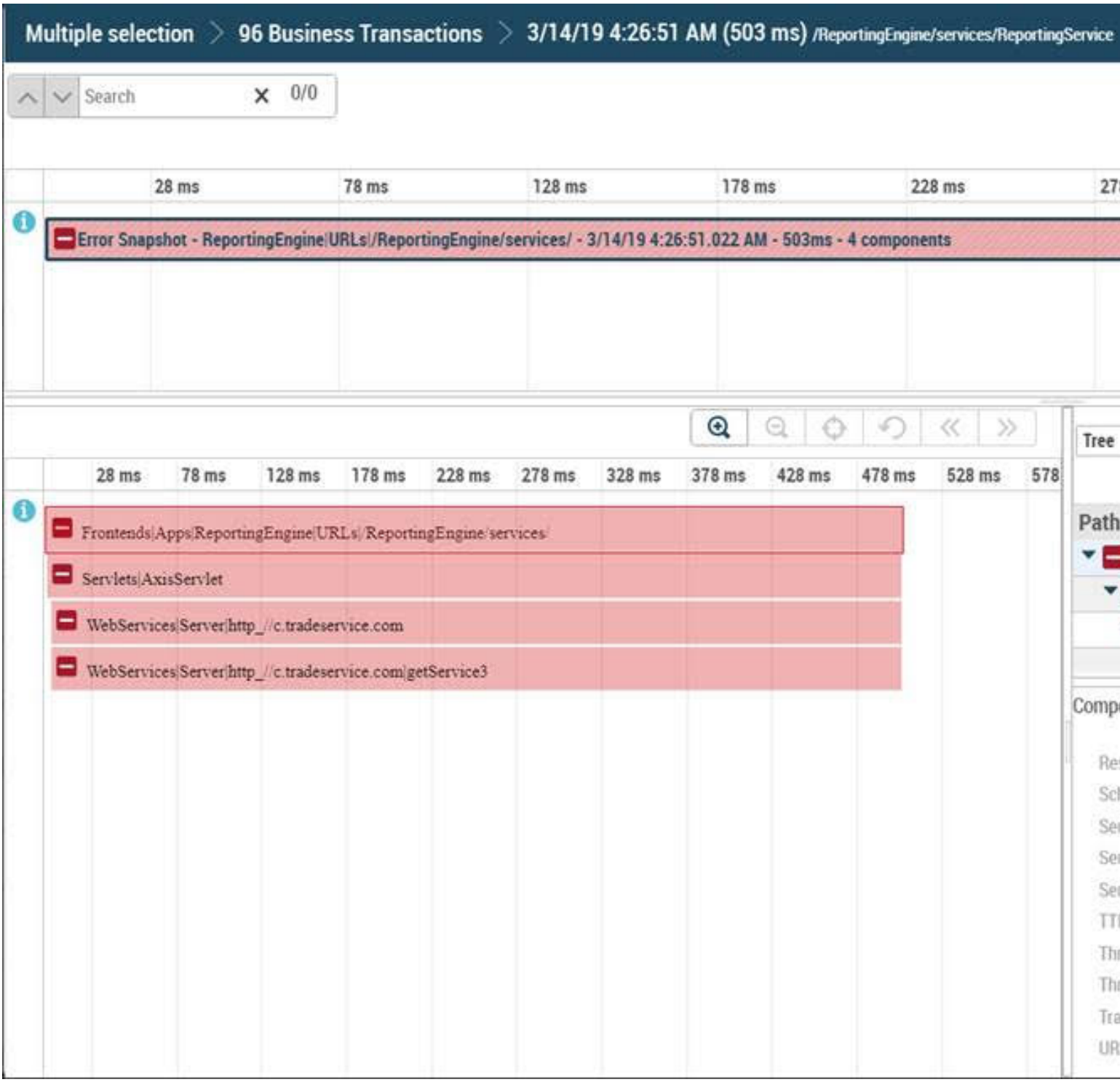
Exemplo: transação com um instantâneo de paralisação relacionado

O gráfico a seguir mostra uma transação normal com um instantâneo da paralisação relacionada. Observe o ícone de câmera e o valor **Paralisação** na coluna **Instantâneo**.



Exemplo: única transação com um instantâneo, mas sem rastreamentos relacionados a erros ou paralisações

O gráfico a seguir mostra uma única transação com um instantâneo, mas sem caminhos de rastreamento relacionados a um erro ou uma paralisação.Observe o prefixo do **Instantâneo do erro**, mas sem nenhum ícone de câmera.



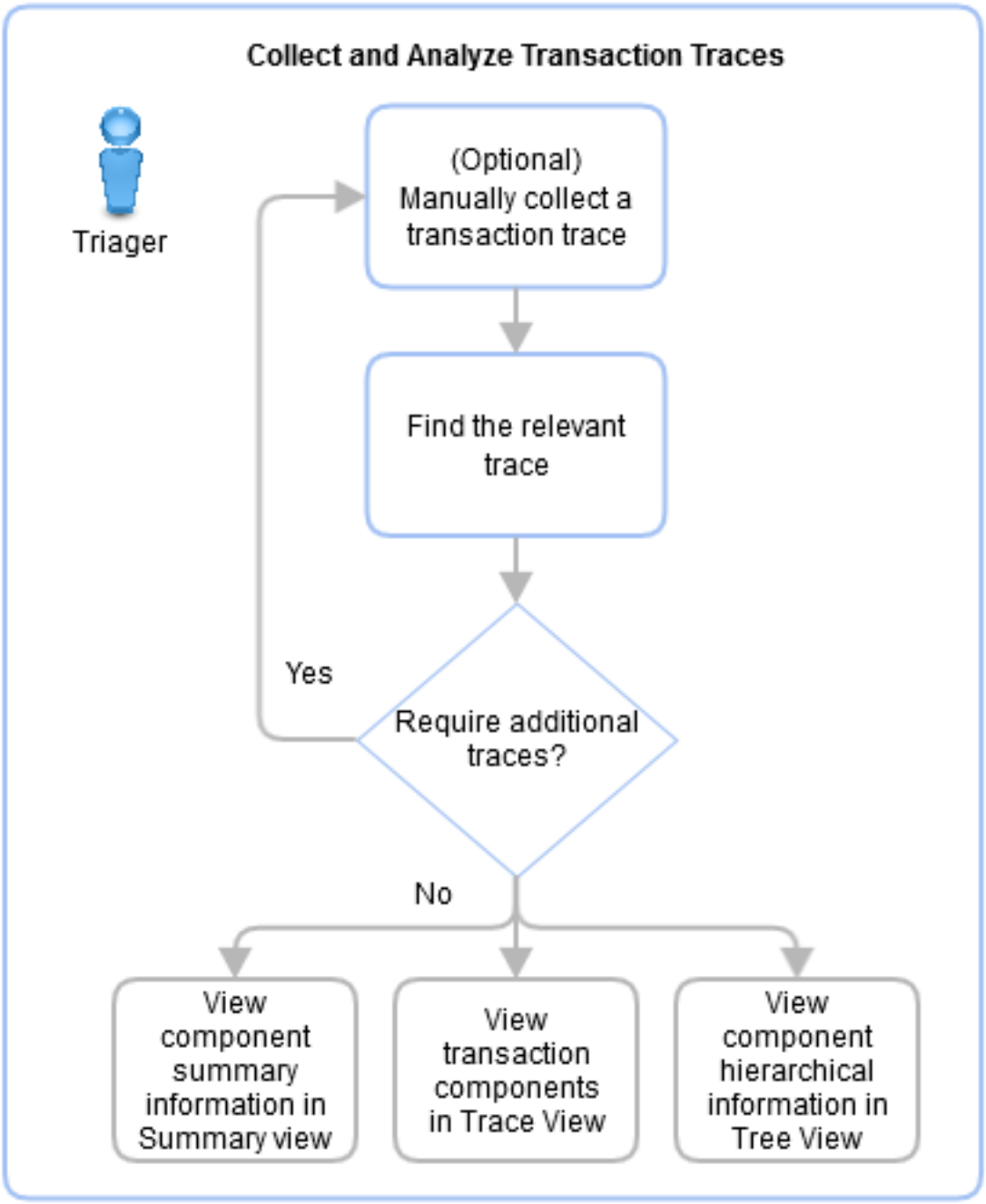
Coletar e analisar rastreamentos de transações

Como diagnosticador, responsável pela triagem ou administrador, você exibe informações detalhadas sobre componentes de rastreamento de transação, como métodos. Essas informações ajudam a identificar a causa raiz dos problemas de desempenho do aplicativo.Com o Rastreador de transações, é possível examinar os rastreamentos

de transações coletados automática ou manualmente. As informações são exibidas porque os componentes são instrumentados usando PBDs ou a instrumentação inteligente está ativada.

Este diagrama mostra como identificar a causa dos problemas de desempenho do aplicativo ao exibir informações detalhadas sobre os componentes da transação.

Figure 10: Como coletar e analisar rastreamentos de transações



Visão geral do rastreamento de transação

O Rastreador de transações monitora a atividade de transações individuais à medida que elas fluem pelos limites de agentes suportados. Os agentes oferecem suporte ao monitoramento de aplicativos Java, .NET e Node.js.O rastreamento de transação entre processos monitora chamadas de transação entre diferentes instâncias de JVM (Java Virtual Machine – Máquina virtual Java), CLR (Common Language Runtime) e Node.js. O monitoramento pode ocorrer em computadores locais ou remotos. Exibir os detalhes da transação entre processos ajuda você a investigar o problema entre os processos de transação.

Veja a seguir como coletar rastreamentos de transação:

- O Introscope coleta automaticamente os rastreamentos de transação.
  - Quando a instrumentação inteligente está ativada, o Introscope coleta automaticamente um rastreamento de transação em várias situações.
    Observação: a instrumentação inteligente está disponível somente para Java, PHP e Node.js, não para agentes .NET.
  - O Introscope coleta regularmente uma amostra do rastreamento de transação.
- Coletar manualmente um rastreamento de transação

Depois que uma sessão de rastreamento de transação é iniciada, as transações que correspondem aos critérios de filtro aparecem na estação de trabalho ou no WebView. É possível exibir as informações de rastreamento na guia Rastreador de transações, incluindo eventos de transação, como rastreamentos de transação e erros.

Rastreamentos de transação coletados automaticamente

Quando a instrumentação inteligente está ativada, o Introscope coleta automaticamente um rastreamento de transação quando estas ações ocorrem:

- Análise diferencial detecta instabilidade do aplicativo
  Observação: os rastreamentos automáticos de transação da análise diferencial exigem a versão 10.0 ou superior do agente.
- Ocorre um erro
- O rastreador `ComponentTimeAutoTraceTriggerTracer` está implantado e o tempo de resposta do componente é excedido
- Uma API dispara um rastreamento automático de transação que se baseia em critérios personalizados.
  Mais informações: entre em contato com o CA APM Implementation Services.

Altamente otimizados, os rastreadores de baixa sobrecarga coletam rastreamentos automáticos de transação. Os rastreamentos automáticos geram muito menos sobrecarga no desempenho do que a execução e a amostragem manuais, entre outros rastreamentos de transação. Esses outros tipos de rastreamentos de transação usam a filtragem do agente, que adiciona sobrecarga.

Os rastreamentos automáticos de transação apresentam estas características:

- São suportados para agentes Java, PHP e Node.js. O agente .NET não é suportado.
- Todos os componentes instrumentados pelo PBD têm uma métrica associada na Árvore do investigador. Os componentes de ampla visibilidade não têm uma métrica associada.
- Os componentes de visibilidade profunda contêm somente nome da classe, nome do método e duração. Para front-ends e back-ends (por exemplo, servlets, serviços web, chamadas SQL), o nome é formatado com base na configuração do PBD.
- Incluem rastreamentos de transação entre processos
  Observação: as transações entre processos nos rastreamentos automáticos de transação são suportadas apenas para aplicativos Java.
- Os rastreamentos automáticos de transação não exibem todas as propriedades detalhadas do componente que os outros tipos de rastreamento de transação exibem.
- As seguintes propriedades são exibidas em ComponentProperties:

  - O Tipo de rastreamento é Normal.
  - Se um erro disparou o rastreamento de transação, o componente que gerou a exceção incluirá as propriedades do componente.
  - O primeiro componente do rastreamento de transação exibe a propriedade `Auto Trace Trigger`.

Se os rastreamentos automáticos de transação não forem exibidos, pode ser por um destes motivos:

- A instrumentação inteligente não está ativada.
- O número de rastreamentos automáticos de transação por valor limite do intervalo (`agent.deep.automatic.trace.clamp property`) foi excedido.

  NOTE

  Mais informações: Sustentabilidade do Agente

  Durante a execução manual de um rastreamento, se algum filtro manual corresponder a um rastreamento automático, o Introscope coletará somente o rastreamento manual.

Transações entre processos nos rastreamentos automáticos de transação

Exibir transações entre processos em rastreamentos automáticos de transação ajuda você a avaliar transações entre camadas. É possível determinar a camada que é o gargalo de uma transação com problemas.

> **NOTE**
> As transações entre processos nos rastreamentos automáticos de transação são suportadas apenas para aplicativos Java.

Agentes de upstream e downstream

Os agentes que monitoram transações podem ser de upstream, downstream ou de upstream e downstream em relação a outros agentes que monitoram a mesma transação. Os agentes de upstream podem fazer chamadas entre processos para agentes de downstream. As chamadas de transação podem percorrer mais de dois processos.Portanto, os agentes que monitoram processos entre a primeira e a última chamada da transação são posicionados como upstream e downstream em relação a outros agentes. Veja um exemplo:

1. Você está analisando um rastreamento de transação em busca de uma transação com problemas e nota um tempo de execução de 6 segundos (6000 ms).
2. Na **Exibição de rastreamento**, você vê chamadas de um método do lado do cliente, `dataservice.yourcompany.net/invoke`, para um método do lado do servidor,`thirdparty.mycompany.net/invoke` .
3. Você observa que o método do servidor está fazendo uma grande quantidade de chamadas para produtos de terceiros

   `3PP site data`

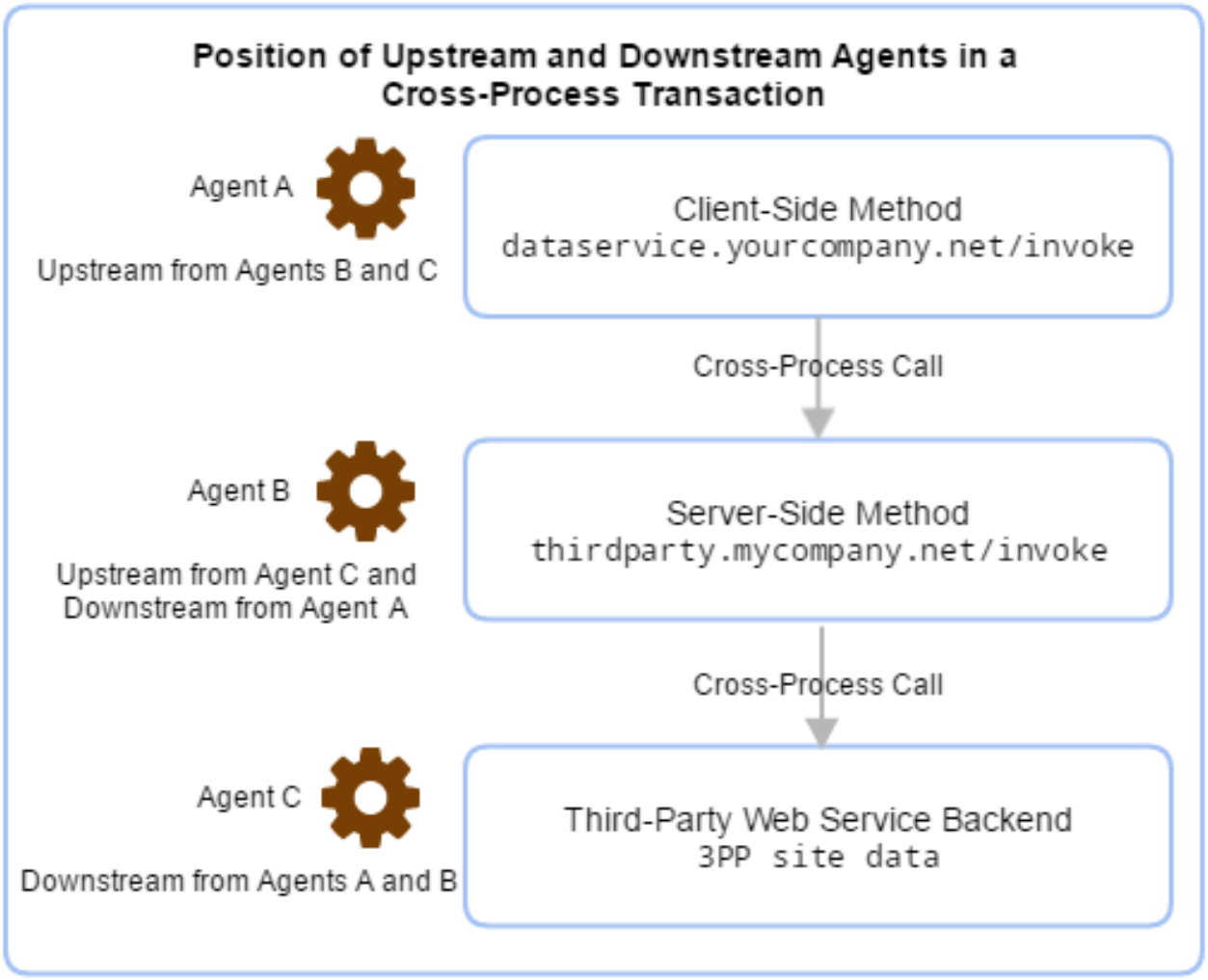
   o serviço web, que é instrumentado.
4. A **Exibição de rastreamento** mostra que o

   `3PP site data`

   back-end do serviço web está atendendo a solicitações repetidas em rápida sucessão. Esse comportamento indica que a lógica de programação, como um loop aninhado, provavelmente está causando chamadas repetidas no serviço do servidor. Você determinou que a operação de invocação do lado do servidor é responsável por grande parte do tempo de execução geral da transação.

Esta imagem gráfica mostra as posições do agente no exemplo de transação entre processos.

Figure 11: Diagrama de agentes de upstream e downstream



Os agentes relatam problemas quando eles os encontram e, às vezes, os agentes iniciam rastreamentos de transação. Antes das chamadas entre processos incluídas do rastreamento automático de transação, somente os agentes de upstream podiam relatar problemas e coletar rastreamentos de transação.

Visibilidade antes do rastreamento entre processos em rastreamentos automáticos de transação

Um agente perto do início de uma transação não sabe se a transação tem um problema de downstream. No fim da transação, um agente de downstream relata qualquer problema de downstream para o agente de upstream mais próximo. Tudo o que os agentes de upstream sabem é que a transação não será finalizada até que um agente de downstream relate a conclusão. Na conclusão da transação, o agente de upstream mais próximo do início da transação relata ao Gerenciador corporativo que encontrou problemas como rastreamentos de transação. Antes do monitoramento de chamadas entre processos incluído no rastreamento automático de transação, os agentes de downstream que detectavam problemas nunca enviavam rastreamentos de transação ao Gerenciador corporativo. Se problemas detectados pelos agentes de downstream não pudessem ser relatados até o agente de upstream superior, esses problemas não eram relatados.Essa situação resultou em uma significativa falta de visibilidade dos problemas de aplicativos.

Visibilidade de ponta a ponta com rastreamento entre processos em rastreamentos automáticos de transação

Com o rastreamento entre processos suportado, os agentes Java podem usar armazenamento em cache inteligente para enviar rastreamentos automáticos de transação para transações entre processos problemáticas de downstream. Esse recurso fornece visibilidade de ponta a ponta para transações de Java.

Agentes de upstream e downstream que detectam transações com problemas podem disparar rastreamentos automáticos de transação.Eles também podem enviar informações do rastreamento de transação ao Gerenciador corporativo.Os agentes que disparam rastreamentos automáticos decidem no fim da transação se enviam um rastreamento ao Gerenciador corporativo.Esse momento de decisão é especialmente útil para análise diferencial, quando os limites da linha de base do Gerenciador corporativo disparam rastreamentos automáticos de transação.

As transações podem usar um protocolo suportado, por exemplo, HTTP ou SOAP, para invocar um serviço dentro do mesmo processo. Nessa situação, os agentes que fazem chamadas entre processos podem ser posicionados como upstream e downstream em relação a outros agentes.Quando um agente de upstream coleta um rastreamento automático de transação, todos os agentes de downstream participantes também coletam rastreamentos automáticos de transação.O rastreamento de transação entre processos coleta somente os rastreamentos importantes para você na triagem de problemas para análise de causa raiz.

Quando um agente de upstream dispara um rastreamento,

```
Component Details Auto Tracing Triggered
```

a propriedade exibe o tipo de disparador. Por exemplo, um erro.Quando um agente de downstream dispara um conjunto de rastreamentos automáticos,

```
Component Details Auto Tracing Triggered
```

a propriedade é

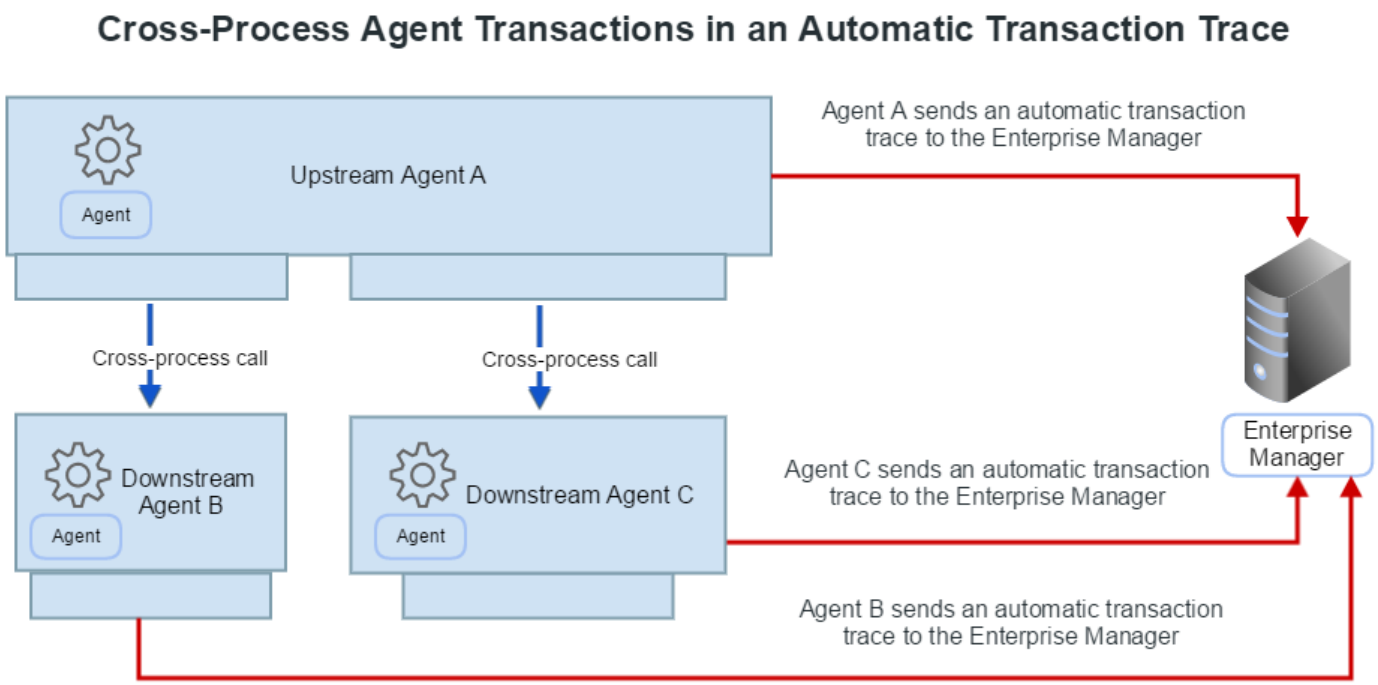
```
Cross Process Trigger
```

.

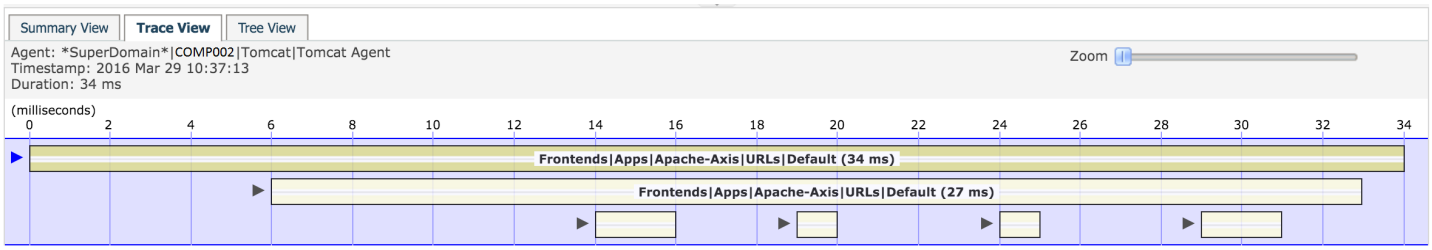
Exemplo: correlação de rastreamento de transação entre processos do agente em rastreamentos automáticos de transação

Um agente que é upstream em relação a outros agentes detecta um problema. O agente de upstream dispara um conjunto de rastreamento automático de transação e avisa os agentes de downstream para fazerem o mesmo. Todos os agentes enviam sues rastreamentos automáticos de transação ao Gerenciador corporativo. Juntos, os agentes criam uma transação entre processos correlacionada, conforme mostrado no diagrama a seguir.

Figure 12: as transações de processo cruzado acionam o rastreamento automático do agente



Os rastreamentos automáticos de transação também oferecem suporte à correlação entre segmentos dentro do mesmo processo. As chamadas de segmento podem percorrer mais de uma transação. Uma transação em um processo pode passar por segmentos diferentes. No gráfico a seguir, você pode ver quatro segmentos entre processos na linha inferior de um rastreamento automático de transação.

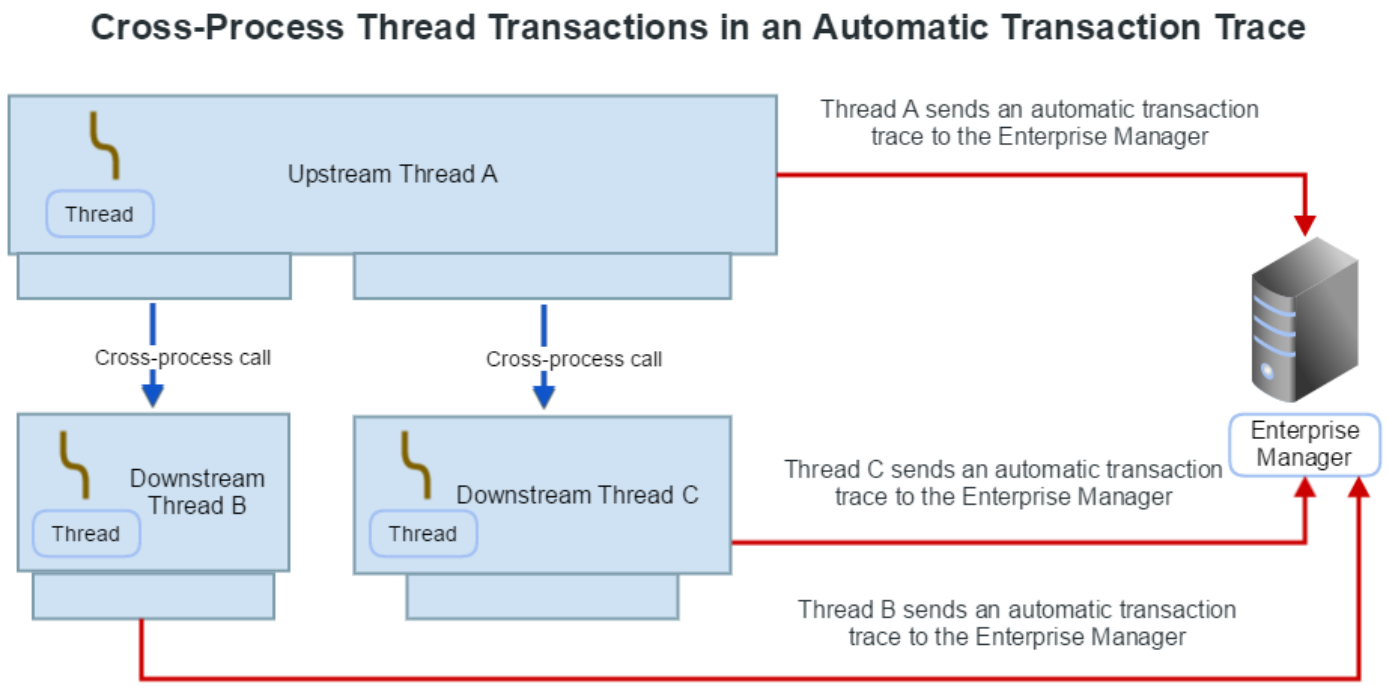


Os segmentos de upstream podem disparar rastreamentos automáticos de transação a qualquer momento, antes ou depois que os segmentos de downstream são invocados.Os detalhes da transação dependem de o segmento ser upstream ou downstream do segmento de disparo inicial na transação.

Exemplo: correlação de rastreamento de transação entre processos do segmento em rastreamentos automáticos de transação

Um segmento de upstream detecta um problema. O segmento de upstream dispara um conjunto de rastreamento automático de transação e avisa os segmentos de downstream para fazerem o mesmo. Todos os segmentos enviam sues rastreamentos automáticos de transação ao Gerenciador corporativo. Juntos, os segmentos criam uma transação entre processos correlacionada.

Figure 13: Rastreamento automático 2 de transação entre processos



Coletar automaticamente um rastreamento de transação com base na instabilidade do aplicativo

A análise diferencial controla a estabilidade dos aplicativos. Por padrão, a análise diferencial procura variação não controlada nas métricas Tempo médio de resposta da transação comercial e do front-end.O mapa da análise diferencial é uma exploração visual da estabilidade e da capacidade de resposta de muitos aplicativos. Cada faixa no mapa corresponde a uma única métrica. Em um período tranquilo e estável, a faixa apresenta um sombreado claro. Quando a estabilidade diminui, o sombreado da faixa escurece progressivamente de acordo com a gravidade da instabilidade. Desse modo, uma única faixa permite que você veja a estabilidade de um único aplicativo ou transação comercial ao longo do tempo. O mapa coloca as faixas mais instáveis no topo.

Quando um aplicativo se torna ligeiramente instável, a análise diferencial notifica o agente, que é preparado para coletar rastreamentos automáticos de transação relacionados. Normalmente, o agente coleta rastreamentos de transação até que o aplicativo se torne estável. No entanto, o agente pode decidir não coletar um rastreamento de transação quando o período de instabilidade for breve. Exiba esses rastreamentos de transação para obter informações detalhadas específicas à mudança de estabilidade e obter insights sobre a causa raiz.

> **NOTE**
>
> Os rastreamentos automáticos de transação da análise diferencial exigem a versão 10.0 ou superior do agente.

Siga estas etapas:

1. No APM Team Center, clique em **WebView**.
   O WebView do APM é exibido.
2. Clique no **Investigador**.
   Uma árvore mostra uma exibição hierárquica do seu sistema.
3. Na árvore, selecione o agente para o qual deseja obter informações de desempenho, por exemplo:
   `SuperDomain | Host | Process | Agent | Frontends | Apps | App Name`
4. Clique na guia **Análise diferencial**.

O mapa mostra uma representação gráfica de dados de desempenho e os últimos 8 minutos de dados. As 100 principais métricas problemáticas são exibidas na ordem da instabilidade decrescente. Os dados são atualizados quando você consulta, altera o período ou seleciona um nó diferente.

5. Clique em uma faixa de interesse no mapa.
   O gráfico de análise diferencial é exibido. Este gráfico ajuda a entender a estabilidade da métrica pela linha do tempo que a faixa representa. O gráfico mostra o status do componente monitorado, de modo que é possível detectar rapidamente o desempenho normal e anormal:
   Uma linha representa um valor de métrica real.
   As regiões sombreadas correspondem às bandas de desvio padrão 1, 2 e 3. Quanto mais escura a banda, maior o desvio do valor previsto. Qualquer métrica em branco é melhor do que a prevista. Todas as métricas que aparecem acima da área branca inferior excederam o valor previsto. Por exemplo, se a métrica exceder a banda superior, ela está excedendo em 3 vezes o desvio padrão.
6. Passe o mouse sobre a linha.
   As dicas de ferramenta exibem os valores da métrica.
7. Clique no hiperlink da métrica de interesse, por exemplo, Tempo médio de resposta.
8. No navegador de métricas, clique no nó da pasta diretamente acima da métrica e clique na guia **Rastreamentos**.
   É possível exibir os rastreamentos automáticos de transação gerados pela instabilidade.
9. (Opcional) Clique em outros nós para ver os rastreamentos de transações gerados pela análise diferencial.
   Por exemplo, clique no nó **Frontends** e, em seguida, na guia **Rastreamentos** para ver rastreamentos automáticos para todos os seus aplicativos de front-end.

Você pode configurar a análise diferencial para pontos de entrada e outras métricas de aplicativo.

Disparar os rastreamentos de transação automáticos quando o tempo de resposta do componente for excedido

Você pode implantar um PBD para disparar um rastreamento de transação automaticamente quando o tempo de resposta do componente for excedido. Crie uma entrada PBD com um rastreador para coletar esse rastreamento automático.Por exemplo, para coletar um rastreamento quando o tempo de resposta de um servlet específico exceder 10 segundos. Use a opção do rastreador `ComponentTimeAutoTraceTriggerTracer` para configurar este recurso.

> **NOTE**
>
> **Mais informações:** Configurar opções do rastreamento de transação

Coletar manualmente um rastreamento de transação

Para executar uma sessão de rastreamento de transação manualmente, especifique os agentes cujas transações você deseja rastrear e o período da captura de dados. Especifique filtros para limitar o rastreamento a transações que excederam o limite de tempo de execução, corresponderam os valores de parâmetro ou que contêm erros.Depois que a sessão de rastreamento de transação é iniciada, as transações que correspondem aos critérios de filtro aparecem na tabela de transação. Os eventos de transação incluem erros e rastreamentos de transação.

Você deve ter a permissão`run_tracer` para executar uma nova sessão de rastreamento de transação.

Siga estas etapas:

1. No APM Team Center, clique em **WebView**.
   O WebView do APM é exibido.
2. Clique em **Ferramentas**, **Rastreador de transações**.
3. Clique em **Iniciar a sessão de rastreamento**.
4. Na área Rastrear transações:
   - Especifique a duração mínima para o rastreamento de transação. Selecione milissegundos ou segundos na lista suspensa. O padrão é 5000 milissegundos.
   - (Opcional) Especifique uma das seguintes condições de filtro para o rastreamento de transação:
     - **É igual a**

O valor do parâmetro que correspondente às sequências de caracteres que são rastreadas.
- **Não é igual a**
  O valor do parâmetro que não corresponde à sequência de caracteres especificada que é rastreada. As transações que não incluem o parâmetro ao qual o filtro se aplica também são rastreadas.
- **Contém**O valor do parâmetro que contém a sequência de caracteres especificada que é rastreada.
- **Começa com**O valor do parâmetro que começa com a sequência de caracteres especificada que é rastreada.
- **Termina com**
  O valor do parâmetro que termina com a sequência de caracteres especificada que é rastreada.
- **Existe**
  As transações que incluem o parâmetro ao qual o filtro se aplica são rastreadas, independentemente do valor do parâmetro.
- **Não existe**
  As transações que não incluem o parâmetro ao qual o filtro se aplica são rastreadas.

5. Informe a duração da sessão de rastreamento.
6. Na área **Rastrear agentes**, selecione um ou mais agentes para os quais rastrear transações:
   – Para rastrear todos os agentes, clique em **Rastrear todos os agentes suportados**. Essa opção rastreia agentes suportados que estão conectados no momento e qualquer um que se conecte durante a sessão de rastreamento.
   – Para rastrear agentes selecionados, clique em **Trace selected Agents (Rastrear agentes selecionados)** e selecione os agentes na lista (**CTRL + clique** para selecionar vários agentes).
7. Clique em **OK** para iniciar a sessão de rastreamento de transação.
   Depois que a sessão é iniciada, a barra de status no painel inferior exibe as seguintes informações:
   – Número de transações rastreadas e uma breve descrição da configuração do rastreamento.
   – Tempo restante da sessão.
   No modo Dinâmico, a guia **Rastreamentos** lista os eventos de rastreamento de transação dos últimos 20 minutos. Os eventos de rastreamento de transação com mais de 20 minutos não são exibidos no modo dinâmico. São listados até 500 eventos de rastreamento de transação.

Interromper, reiniciar ou alternar as sessões de rastreamento de transação

Você pode gerenciar a sessão de rastreamento na guia **Rastreador de transações** da seguinte maneira:

- Clique em **Interromper rastreamento** para encerrar a sessão.
- Clique em **Reiniciar o rastreamento** para continuar rastreando transações nos agentes de destino usando as mesmas condições. É possível reiniciar uma sessão de rastreamento de transação:
  – Depois que uma sessão tiver expirado.
  – Para reiniciar uma sessão que foi interrompida.
  – Para reiniciar uma sessão em andamento.
- Clique em **Ativar/desativar rastreamento** para selecionar uma sessão de rastreamento diferente a ser executada.

Encontrar o rastreamento relevante

Examine um único rastreamento para coletar informações sobre o problema do aplicativo.

Siga estas etapas:

1. Analise as informações de atividade do rastreamento para a sessão de rastreamento na tabela de transações. Selecione uma linha da tabela para exibir mais detalhes.
2. Execute nova sessão, ou interrompa, reinicie ou alterne as sessões de rastreamento, conforme a necessidade.
3. Examine as guias **Exibição do resumo**, **Exibição de rastreamento** e **Exibição em árvore** no painel inferior. As informações podem ajudar você a diagnosticar e fazer a triagem dos problemas de aplicativo e de desempenho.

Compreender os pontos de entrada

A detecção automática do ponto de entrada permite monitorar e fazer a triagem rapidamente de aplicativos Java sem a configuração manual das diretivas do ProbeBuilder.

Quando a instrumentação inteligente e a detecção do ponto de entrada estão ativadas, o Introscope monitora os segmentos que estão envolvidos nas transações de chamada de soquete do cliente. A instrumentação inteligente e a detecção do ponto de entrada são configuradas como ativadas por padrão. *Os pontos de entrada* são os pontos de início da transação.Um mecanismo de regras no agente identifica candidatos ao ponto de entrada.O agente instrumenta e monitora o candidato ao ponto de entrada mais antigo no segmento de transações. Qualquer ponto de entrada que um agente detecta e persiste é ativado para monitoramento por todos os agentes que compartilham o diretório de instalação. No entanto, quando vários agentes compartilham a instrumentação, o relatório de métricas depende das JVMs do servidor de aplicativos que executam o mesmo código ou as mesmas classes de estrutura.

Veja a seguir alguns exemplos de transações nas quais a detecção do ponto de entrada fornece visibilidade automaticamente:

- Pilhas e estruturas tecnológicas que a instrumentação do Introscope ainda não monitora
- Chamadas à API personalizadas ou patenteadas
- Segmentos em segundo plano que consomem recursos críticos e podem afetar o desempenho geral do aplicativo

> **NOTE**
>
> A detecção do ponto de entrada não oferece suporte ao UDP (User Datagram Protocol - Protocolo de Datagrama de Usuário).

O agente salva os pontos de entrada no arquivo `AutoPersist.pbd` , que é mantido no diretório <*pasta_principal_do_agente*>\core\config\hotdeploy.

> **WARNING**
> O usuário do sistema que executar o servidor de aplicativos precisará ter acesso de leitura/gravação ao diretório /hotdeploy.Essas permissões permitem que o agente grave dados no
> `AutoPersist.pbd`
> .

Pontos de entrada são diferentes de front-ends. O agente do Java detecta automaticamente pontos de entrada que estão perto do início de um caminho de chamada de transação. Os front-ends são definidos manualmente nos PBDs e podem estar em qualquer lugar do caminho de chamada de transação.

> **WARNING**
> Não faça alterações manuais em
> `AutoPersist.pbd`
> . No entanto, você pode copiar pontos de entrada detectados e usá-los em outro PBD.

As métricas dos pontos de entrada são exibidos na árvore centrada no agente, no subnó Automatic Entry Points sob o nó do agente.

> **NOTE**
>
> : certifique-se de que a propriedade `introscope.autoprobe.dynamicinstrument.enabled` em`IntroscopeAgent.profile` esteja definida como true. Essa configuração permite que o agente relate métricas de ponto de entrada sem exigir a reinicialização do aplicativo.

O Introscope relata as cinco métricas de diagnóstico padrão para cada ponto de entrada.Os pontos de entrada são exibidos no rastreamento de transação, mas não no mapa. Os nomes dos pontos de entrada são formatados como `ponto de entrada <nome da classe _ nome do método>` . O Introscope relata métricas de suportabilidade de detecção do ponto de entrada.

Você pode configurar a coleta de pontos de entrada. Por exemplo, uma propriedade de configuração limita o número de pontos de entrada que `AutoPersist.pbd` pode persistir.

NOTE

Mais informações: Criar PBDs para converter pontos de entrada em front-ends

Compreender back-ends automáticos

Quando a detecção de *back-end automático* está ativada, o agente detecta e monitora automaticamente os back-ends de aplicativo sem configuração manual.

Um mecanismo de detecção no agente identifica candidatos ao back-end automático. Qualquer back-end automático que um agente detecta e persiste é ativado para monitoramento por todos os agentes que compartilham o diretório de instalação.

Veja a seguir alguns exemplos de tipos de back-end que a detecção de back-end automático pode encontrar e monitorar:

- Pilhas e estruturas tecnológicas de back-end que o agente ainda não monitora. Entre os exemplos estão os back-ends NoSQL, como MongoDB e Cassandra.
- Back-ends personalizados ou patenteados

O agente salva os back-ends automáticos no arquivo `AutoPersist.pbd` , que é mantido no diretório *<pasta_principal_do_agente>\core\config\hotdeploy*.

WARNING

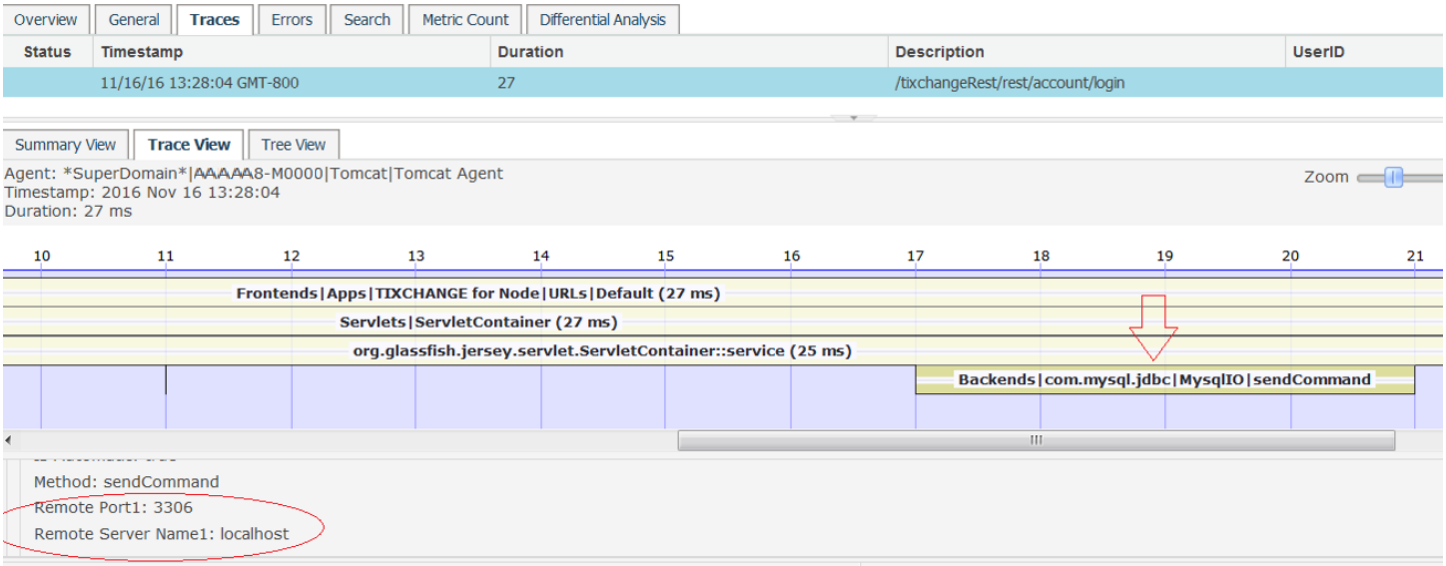
- O usuário do sistema que executar o servidor de aplicativos precisará ter acesso de leitura/gravação ao diretório /hotdeploy.Essas permissões permitem que o agente grave dados no arquivo AutoPersist.pbd.
- Não faça alterações manuais em AutoPersist.pbd. No entanto, você pode copiar back-ends automáticos detectados e usá-los em outro PBD.

Você pode configurar a detecção automática de back-end. Por exemplo, uma propriedade de configuração limita o número de back-ends automáticos que AutoPersist.pbd pode persistir.

Na **Exibição de rastreamento**, os parâmetros `porta remota` e `nome do servidor remoto` são exibidos nos **Detalhes do componente**.

Observe o caminho da chamada de back-end e os parâmetros neste rastreamento de transação:

- O componente do rastreamento de transação para o caminho da chamada de back-end é: Backends|com.mysql.jdbc|MysqlIO|sendCommand.
- O parâmetro de porta remota é `3306` e o parâmetro do host do servidor remoto é `Name1: localhost` .



Entender os componentes de ampla visibilidade

Quando a instrumentação inteligente está ativada, os agentes detectam e coletam automaticamente informações detalhadas sobre componentes de transação para o nível de método.Os agentes detectam e instrumentam automaticamente os componentes de ampla visibilidade sem o uso de PBDs (ProbeBuilder Directives - Diretivas do ProbeBuilder). O Introscope analisa métodos para a sua complexidade a fim de determinar as chamadas e os componentes a serem instrumentados e exibidos como componentes de ampla visibilidade.

Observação: a instrumentação inteligente está disponível somente para agentes Java, não para agentes .NET.

Fatos sobre os componentes de ampla visibilidade que você deve conhecer:

- Um ícone de raio indica um componente de visibilidade profunda. O rótulo Componente de rastreamento profundo também é exibido na dica de ferramenta quando você passa o mouse sobre o componente em questão.
- Os componentes de ampla visibilidade não incluem links para métricas. Não são exibidos dados de métrica na Árvore do investigador nem no Mapa.
- Contêm apenas o nome da classe, o nome do método e a duração.
- As seguintes propriedades são exibidas nos detalhes do componente:
  - Nível da instrumentação
    O nível da instrumentação inteligente em que uma transação foi detectada.
  - Pontuação do nível de método
    O nível da instrumentação inteligente está relacionado à pontuação que o algoritmo de pontuação do Introscope atribui a um método de componente de ampla visibilidade. O Introscope pode exibir métodos de componente de ampla visibilidade tendo pontuações variadas em um rastreamento de transação, um erro ou uma paralisação. Por exemplo, uma transação detectada usando nível médio pode exibir métodos com pontuações de nível de método médio e baixo.

Use essas propriedades para entender a ampla visibilidade da instrumentação inteligente de um rastreamento de transação e métodos em um rastreamento. Por exemplo, é possível comparar os vários métodos que a instrumentação inteligente detecta em dois níveis diferentes de instrumentação. Você pode observar o nível de instrumentação inteligente em que o Introscope pontuou métodos específicos. É possível ajustar a solução de monitoramento para a visibilidade de monitoramento desejada equilibrando a sobrecarga e a visibilidade.

Os componentes instrumentados padrão e os componentes da ampla visibilidade podem aparecer por meio de uma sessão de rastreamento de transação.

Dependendo de seus requisitos e do ambiente, é possível configurar a profundidade da visibilidade da instrumentação inteligente.

Analisar rastreamentos e colaborar na análise de problemas

Você pode exportar o arquivo JSON (JavaScript Object Notation) para um ou mais rastreamentos de transação. Use um editor simples e pesquise no arquivo para encontrar um componente ou parâmetros dentro de um componente. Compartilhe o arquivo por email ou em uma unidade de rede compartilhada para permitir que os usuários colaborem na análise de problemas. Outro usuário pode carregar o arquivo exportado para exibir as mesmas informações. Essa perspectiva compartilhada o ajuda a colaborar para identificar rapidamente se um componente está disponível ou o componente está com problemas de desempenho. Por exemplo, você pode examinar se os usuários podem efetuar logon, fazer reservas ou exibir os dados. É possível ver os tempos de resposta dos usuários e as causas dos problemas quando eles ocorrerem.

Para exportar ou carregar o rastreamento JSON, trabalhe na guia **Transações comerciais**. Para abrir a guia, use o Bloco de notas de análise e clique em um problema de interesse.

Exportar o JSON de rastreamento

Exporte os dados de rastreamento como JSON para analisar ou compartilhar.

Siga estas etapas:

1. Clique na guia **Transações comerciais**.
2. Clique em um segmento ou componente da transação de seu interesse e clique em **Fazer upload**.
   O nome do arquivo baixado aparece na parte inferior da página.
3. (Opcional) Abra o arquivo e analise os dados:
   – Use um editor como o JSON Editor Online.
   – Arraste o arquivo para o Chrome.

   NOTE

   As informações de exibição do **instantâneo** não estão disponíveis no JSON exportado.

Fazer upload do JSON de rastreamento

Faça upload dos dados de rastreamento como JSON para exibir uma perspectiva compartilhada.

Siga estas etapas:

1. Clique na guia **Transações comerciais**.
   Uma lista mostra os rastreamentos correspondentes ao componente.
2. Clique no ícone **Rastreamento de upload JSON** para carregar os dados da lista ou clique em um segmento da transação de seu interesse e clique no ícone **Rastreamento de upload JSON**.
3. Procure e selecione o arquivo <*nome*>.json e clique em **Abrir**.

   NOTE
   O tamanho máximo permitido para o arquivo JSON é 52.4288 MB. A pilha gráfica Detalhes da transação reflete os dados JSON carregados.

Monitorar o desempenho e os eventos do navegador

O agente do navegador permite monitorar as métricas e os erros de desempenho no carregamento de páginas web. É possível identificar a degradação de desempenho do navegador, da rede ou do servidor de aplicativos.

Como um proprietário do aplicativo, siga estas etapas de alto nível:

1. Use os procedimentos normais para monitorar o desempenho:

   NOTE

   Monitorar o desempenho usando a Exibição da experiência

   Investigar o baixo desempenho das transações

   Diagnosticar problemas de carregamento do recurso
2. Leia e use essas informações adicionais específicas do agente do navegador:

Monitorar o desempenho do aplicativo com o agente do navegador

É possível monitorar o tempo de resposta do navegador para o seu aplicativo gerenciado e ver os seus aplicativos da perspectiva dos serviços de negócios e de suas dependências. Um mapa é gerado automaticamente a partir do desempenho e da análise de métricas, erros e eventos.

NOTE
Apenas as métricas de carregamento de páginas são exibidas no mapeamento. As métricas de estruturas fundamentais, como o AJAX, não aparecem no mapa.

Siga estas etapas:

1. No painel esquerdo, clique em **Exibição da experiência**.
   A Exibição da experiência mostra os cartões de experiência individuais. Cada cartão mostra um resumo. Os itens em vermelho indicam transações lentas ou com falhas.
2. Procure os cartões e clique no ícone **Bloco de notas** de um cartão que seja do seu interesse.
   O Bloco de notas de análise mostra os detalhes sobre a experiência. O Relationship Flow mostra os caminhos de transação das experiências selecionadas. Este mapa fornece o contexto sobre o evento ocorrido.
3. (Opcional) Selecione **Tipo** na lista suspensa **Perspectiva**.
4. Analise o mapa e identifique o primeiro componente (o componente mais à esquerda) em uma série de dependências que indica problemas de desempenho. Esse componente pode ser a origem da degradação de desempenho no seu ambiente de aplicativos.
5. Clique em um **componente** de seu interesse no mapeamento.
   A guia Métricas mostra as métricas de BlamePoint e W3C.
6. (Opcional) Na guia **Métricas**, clique no **nome de uma métrica** do seu interesse, por exemplo, Resultados de página por intervalo.
   A Árvore de métricas será exibida e mostrará a métrica específica.
7. Use essas informações para investigar os problemas de desempenho.

Analisar as métricas do agente do navegador

Aplicativos com baixo desempenho podem afetar a experiência do usuário final. É possível exibir dados dinâmicos na Árvore de métricas para ajudar a analisar e resolver problemas de desempenho.A exibição em árvore de agentes, recursos e métricas é atualizada a cada 15 segundos para mostrar os dados atuais das métricas.

Todas as métricas do agente do navegador são exibidas no seguinte caminho:

- Nó **Agente DxC, Segmento comercial**. As descrições de caminho das métricas nas seções a seguir mostram os caminhos do **Agente DxC**.

  NOTE
  Todos os valores de métricas do agente do navegador são arredondados para baixo. Adicione links à seção Calculations do agente do navegador ou adicione-os individualmente a cada subtópico abaixo dos cálculos específicos.

Métricas de carregamento de página

O agente do navegador relata os tempos de resposta e os eventos do navegador para páginas web. Quando disponível, o agente do navegador relata seus tempos de resposta do navegador. Alguns navegadores têm limitações:

- Para uma página inicial, não há descarregamento de página anterior associado.
- Se um carregamento de página aguardar a entrada do usuário, esse tempo será incluído na métrica Tempo médio de carregamento da página (ms).

A tabela a seguir descreve como as métricas de carregamento da página são calculadas para os navegadores. A coluna Metric Calculation indica o cálculo matemático usado pelo agente do navegador para obter uma determinada métrica. Por exemplo, o Tempo médio de processamento da página (ms) é obtido subtraindo-se duas horas de evento do navegador: loadEventEnd e domComplete.

Métrica	Descrição	Cálculo da métrica
Tempo médio de processamento da página (ms)	O tempo para processar o conteúdo após o DOM (Document Object Model - Modelo de Objeto do Documento) ter sido processado.	Hora de loadEventEnd - hora de domComplete
Tempo médio de estabelecimento de conexão (ms)	O tempo para o navegador estabelecer a conexão TCP com o servidor.	Hora de connectEnd - hora de connectStart
Tempo médio de pesquisa do domínio (ms)	O tempo para o navegador concluir a pesquisa de serviço de nome para o domínio da página web atual.	Hora de domainLookupEnd - hora de domainLookupStart
Tempo médio de processamento do DOM (ms)	O tempo desde o início da navegação até o momento em que o navegador processa o DOM. **Observação**: essa hora não é quando todos os objetos no DOM são recuperados e carregados.	Hora de domComplete - hora de domLoading
Tempo médio de carregamento da página (ms)	O tempo desde o início da navegação até o momento em que o navegador carrega todos os componentes e a página é concluída.	Hora de loadEventEnd - hora de navigationStart
Tempo médio de descarregamento da página anterior (ms)	O tempo para descarregar a página exibida anteriormente. Se não houver nenhuma página para descarregar (por exemplo, quando uma sessão do navegador é iniciada), nenhum valor estará disponível.	Hora de unloadEventEnd - hora de unloadEventStart
Tempo médio até o primeiro byte (ms)	O tempo para o navegador receber o primeiro byte de resposta dos caches do servidor ou do aplicativo.	Hora de responseStart - hora de requestStart
Tempo médio até o último byte (ms)	O tempo para o navegador receber o último byte de resposta dos caches do servidor ou do aplicativo.	Hora de responseEnd - hora de requestStart
Erros do JavaScript por intervalo	O número de ocorrências de erro do JavaScript na página web monitorada dentro de um determinado intervalo.	Não aplicável
Resultados de página por intervalo	O número de ocorrências em que a página web monitorada foi solicitada dentro de um determinado intervalo.	Não aplicável
Tempo médio de paralisação da página	O tempo que a solicitação de página aguardou até que pudesse ser enviada.	(Hora de connectStart - hora de domainLookupEnd) + (hora de requestStart - hora de connectEnd)

O agente do navegador usa limites onde as métricas do navegador não podem ser criadas e relatadas. Os limites para as métricas assíncronas, de carregamento de página e de função do JavaScript têm determinados limites padrão que são configuráveis. A data e a hora do navegador devem estar de acordo com os limites para que as métricas sejam criadas.

As métricas de navegador não podem ser criadas na Árvore de métricas porque não são relatadas. Nesse caso, as métricas não são exibidas no Mapa. Por exemplo, se a métrica Tempo médio até o primeiro byte (ms) não for exibida na Árvore de métricas, ela não será exibida no Mapa.

O agente do navegador relata os tempos de resposta e os eventos do navegador para páginas web. Quando disponível, o agente do navegador usa a API Navigation Timing do W3C para relatar os tempos de resposta do navegador. A API Navigation Timing do W3C é uma interface que os navegadores modernos implementam. Alguns desses navegadores têm limitações:

- Para uma página inicial, não há descarregamento de página anterior associado.
- Se um carregamento de página aguardar a entrada do usuário, esse tempo será incluído na métrica Tempo médio de carregamento da página (ms).

Quando uma transação comercial não é iniciada para a página de nível superior, as métricas são exibidas em:

- Segmento comercial | <host_do_URL_da_página>/<porta_do_URL_da_página> | <caminho_do_URL_da_página>

Quando uma transação comercial é iniciada para a página de nível superior, as métricas são exibidas em:

- Segmento comercial | <serviço_comercial> | <transação_comercial> | <componente_da_transação_comercial> | Navegador

> **NOTE**
> Quando ocorrerem erros, o agente do navegador incrementará a métrica Erros de página por intervalo no caminho de métrica da página. Esta métrica reflete o número total de erros do JavaScript e do AJAX na página.

Métricas de carregamento de página temporária

Os aplicativos de página única fazem uma única solicitação de página para recuperar todo o conteúdo da página no seu carregamento inicial. Dessa forma, os aplicativos podem, de maneira dinâmica, obter recursos do servidor e atualizar a interface como resultado das interações do usuário. Muitos aplicativos de página única usam as APIs History do HTML5 e as propriedades de hash do local do URI para indicar a navegação lógica do usuário na mesma página única. Esse tipo de navegação lógica do usuário, que dispara a alteração de rota sem o recarregamento completo da página, é chamado de navegação de página temporária. O agente do navegador monitora o tempo de carregamento das páginas temporárias e relata a métrica Tempo médio de carregamento da página (ms). O agente do navegador também monitora o número de ocorrências em que a página temporária monitorada foi visitada dentro de um determinado intervalo. O agente do navegador relata esse número como a métrica Resultados de página por intervalo. Essas informações fornecem uma visão mais abrangente da experiência do usuário final em relação aos aplicativos de página única.

As métricas a seguir estão disponíveis para os aplicativos de página única e para a navegação de página temporária. Esses cálculos de métricas usam as variáveis:

- TSPE = hora em que a navegação temporária é iniciada (alteração de rota sem o carregamento da página)
- TSPS = hora em que a página temporária conclui o carregamento

Métrica	Descrição	Cálculo da métrica
Tempo médio de carregamento da página (ms)	O tempo médio desde quando a navegação flexível ocorre (alteração de rota sem o carregamento da página) até quando a página temporária conclui o carregamento.	TSPE - TSPS
Resultados de página por intervalo	O número de ocorrências em que a página temporária monitorada foi visitada dentro de um determinado intervalo.	Não aplicável

Quando ocorre uma navegação de página temporária, as métricas Tempo médio de carregamento da página (ms) e Resultados de página por intervalo são exibidas abaixo do nó Soft Page Hash da página de nível superior:

- Segmento comercial | <host_do_URL_da_página>/<porta_do_URL_da_página> | <caminho_do_URL_da_página> | <caminho_da_página> | <hash_da_página_temporária>

Quando uma transação comercial é iniciada para a página de nível superior, as métricas da página temporária são exibidas em:

- Segmento comercial | <serviço_comercial> | <transação_comercial> | <componente_da_transação_comercial> | Navegador | <hash_da_página_temporária>

Métricas do AJAX

Para aplicativos web, o agente do navegador pode fornecer tempos de resposta do navegador para páginas web dinâmicas em estruturas fundamentais, como o AJAX (Asynchronous JavaScript and XML).

O agente do navegador não suporta:

- Retornos de chamada aninhados do AJAX
- Solicitações síncronas do AJAX
- Funções de retorno de chamada, como `XMLHttpRequest.onerror` e `XMLHttpRequest.ontimeout` . (Os tempos de execução do retorno de chamada são suportados para `XMLHttpRequest.onreadystatechange` e `XMLHttpRequest.onload` .)
  Ícone

  NOTE
  Para obter mais informações sobre o suporte, consulte a Matriz de compatibilidade do produto.

As métricas a seguir estão disponíveis para as estruturas que usam o AJAX. Esses cálculos de métricas usam as variáveis:

- TSE = hora em que o envio de chamadas do AJAX é encerrado
- TFB = hora em que o navegador recebe o primeiro byte de resposta do servidor
- TLB = hora em que o navegador recebe o último byte de resposta do servidor
- TCS = hora em que a execução do retorno de chamada do AJAX começa
- TCE = hora em que a execução do retorno de chamada do AJAX termina

Métrica	Descrição	Cálculo da métrica
Tempo médio de execução de retorno de chamada (ms)	O tempo médio para `XMLHttpRequest.onreadystatechange` ou `XMLHttpRequest.onload` as funções de retorno de chamada processarem a resposta do servidor.	TCE - TCS
Contagem de invocações por intervalo	O número total de vezes que a solicitação do AJAX foi feita em um determinado intervalo.	Não aplicável
Tempo médio até o primeiro byte (ms)	O tempo médio desde o momento em que a solicitação do AJAX é emitida para um recurso HTTP até o recebimento do primeiro byte de resposta do servidor.	TFB - TSE
Tempo médio de carregamento do recurso (ms)	O tempo médio desde o momento em que a solicitação do AJAX é emitida para um recurso HTTP até que o retorno de chamada do AJAX (a função responsável por receber e processar os dados do servidor) seja concluído.	TCE - TSE
Tempo médio de resposta de download (ms)	O tempo médio entre o recebimento do primeiro byte e do último byte de resposta do servidor.	TLB - TFB

NOTE
Para as chamadas do AJAX, as métricas Tempo médio de resposta de download (ms) e Tempo médio de execução de retorno de chamada (ms) são relatadas de forma independente. Essas métricas podem não ser relatadas devido às limitações de determinadas estruturas do AJAX, especialmente as chamadas do AJAX por meio do jQuery 1.x.

- O agente do navegador pode não relatar o Tempo médio de execução de retorno de chamada (ms) para a chamada inicial do AJAX.
- O agente do navegador pode não relatar o Tempo médio de resposta de download (ms) e o Tempo médio até o primeiro byte (ms).

Uma chamada do AJAX pode ocorrer na página de nível superior ou na página temporária. As métricas do AJAX estão categorizadas em solicitações síncronas e assíncronas:

Métricas síncronas do AJAX

Quando uma transação comercial não é iniciada para a página de nível superior, as métricas do AJAX são exibidas abaixo do nó Recursos da página.

- Segmento comercial | <host/porta> | <caminho_da_página> | Recursos | Chamada do AJAX | Síncrona | <host_do_URL_do_AJAX>/<porta_do_URL_do_AJAX> | <caminho_do_URL_do_AJAX>
- Segmento comercial | <host/porta> | <caminho_da_página> | <hash_da_página_temporária> | Recursos | Chamada do AJAX | Síncrona | <host_do_URL_do_AJAX>/<porta_do_URL_do_AJAX> | <caminho_do_URL_do_AJAX>

Quando uma transação comercial é iniciada para a página de nível superior, as métricas do AJAX são exibidas em:

- Segmento comercial | <serviço_comercial> | <transação_comercial> | <componente_da_transação_comercial> | Navegador | Recursos | Chamada do AJAX | Síncrona | <host_do_URL_do_AJAX>/<porta_do_URL_do_AJAX> | <caminho_do_URL_do_AJAX>
- Segmento comercial | <serviço_comercial> | <transação_comercial> | <componente_da_transação_comercial> | Navegador | <hash_da_página_temporária> | Recursos | Chamada do AJAX | Síncrona | <host_do_URL_do_AJAX>/<porta_do_URL_do_AJAX> | <caminho_do_URL_do_AJAX>

Quando uma transação comercial for iniciada para a chamada do AJAX, ele terá prioridade sobre a transação comercial que for iniciada para a página de nível superior. As métricas do AJAX são exibidas em:

- Segmento comercial | <AJAX_do_serviço_comercial> | <AJAX_da_transação_comercial> | <AJAX_do_componente_da_transação_comercial> | Navegador | Recursos | Chamada do AJAX | Síncrona | <host_do_URL_do_AJAX>/<porta_do_URL_do_AJAX> | <caminho_do_URL_do_AJAX>

Métricas assíncronas do AJAX

Quando uma transação comercial não é iniciada para a página de nível superior, as métricas do AJAX são exibidas abaixo do nó Recursos da página.

- Segmento comercial | <host/porta> | <caminho_da_página> | Recursos | Chamada do AJAX | Assíncrona | <host_do_URL_do_AJAX>/<porta_do_URL_do_AJAX> | <caminho_do_URL_do_AJAX>
- Segmento comercial | <host/porta> | <caminho_da_página> | <hash_da_página_temporária> | Recursos | Chamada do AJAX | Assíncrona | <host_do_URL_do_AJAX>/<porta_do_URL_do_AJAX> | <caminho_do_URL_do_AJAX>

Quando uma transação comercial é iniciada para a página de nível superior, as métricas do AJAX são exibidas em:

- Segmento comercial | <serviço_comercial> | <transação_comercial> | <componente_da_transação_comercial> | Navegador | Recursos | Chamada do AJAX | Assíncrona | <host_do_URL_do_AJAX>/<porta_do_URL_do_AJAX> | <caminho_do_URL_do_AJAX>
- Segmento comercial | <serviço_comercial> | <transação_comercial> | <componente_da_transação_comercial> | Navegador | <hash_da_página_temporária> | Recursos | Chamada do AJAX | Assíncrona | <host_do_URL_do_AJAX>/<porta_do_URL_do_AJAX> | <caminho_do_URL_do_AJAX>

Quando uma transação comercial for iniciada para a chamada do AJAX, ele terá prioridade sobre a transação comercial que for iniciada para a página de nível superior. As métricas do AJAX são exibidas em:

- Segmento comercial | <AJAX_do_serviço_comercial> | <AJAX_da_transação_comercial> | <AJAX_do_componente_da_transação_comercial> | Navegador | Recursos | Chamada do AJAX | Assíncrona | <host_do_URL_do_AJAX>/<porta_do_URL_do_AJAX> | <caminho_do_URL_do_AJAX>

  NOTE
  Quando uma chamada do AJAX tiver um erro, o agente do navegador incrementará a métrica Erros de recurso por intervalo no caminho de métrica do AJAX.

Métricas do recurso web

O agente do navegador relata as métricas de todos os recursos web da página, como imagens, CSS e JavaScript. As páginas web são criadas a partir do conteúdo que não pode ser exibido no download inicial da página em si. Esse conteúdo pode estar na forma de imagens, som ou outras mídias. Por exemplo, um aplicativo web pode usar serviços de entrega de conteúdo para hospedar imagens e também incluir anúncios incorporados. Esses itens de suporte que a página baixa e aos quais faz referência são denominados recursos. Como analista, você deve entender se o baixo desempenho de um aplicativo se deve ao próprio aplicativo ou aos recursos web, que podem ser fornecidos por terceiros.

As métricas de recursos web para todos os outros recursos da página são exibidas em Recursos, no nó HTML da página:

- Segmento comercial | <host_do_URL_da_página>/<porta_do_URL_da_página> | <caminho_do_URL_da_página> | <caminho_da_página> | Recursos | HTML | <host_do_URL_do_recurso>/<porta_do_URL_do_recurso> | <caminho_do_URL_do_recurso>
- Segmento comercial | <host_do_URL_da_página>/<porta_do_URL_da_página> | <caminho_do_URL_da_página> | <hash_da_página_temporária> | Recursos | HTML | <host_do_URL_do_recurso>/<porta_do_URL_do_recurso> | <caminho_do_URL_do_recurso>

Quando uma transação comercial é iniciada para a página, as métricas de recursos web são exibidas em:

- Segmento comercial | <serviço_comercial> | <transação_comercial> | <componente_da_transação_comercial> | Navegador | Recursos | HTML | <host_do_URL_do_recurso>/<porta_do_URL_do_recurso> | <caminho_do_URL_do_recurso>
- Segmento comercial | <serviço_comercial> | <transação_comercial> | <componente_da_transação_comercial> | Navegador | <hash_da_página_temporária> | Recursos | HTML | <host_do_URL_do_recurso>/<porta_do_URL_do_recurso> | <caminho_do_URL_do_recurso>

Siga estas etapas:

1. No painel esquerdo, clique em **Métricas**.
   A Árvore de métricas lista as métricas e outras informações em formato de árvore. Os nós de alto nível imediatamente abaixo dos nós de domínio representam os agentes instalados nos hosts do servidor de aplicativos individuais ou equivalente. Um nó é o local em que informações específicas da métrica são reunidas e exibidas na exibição em árvore centralizada no agente. Ao expandir um nó, você poderá exibir e pesquisar informações mais detalhadas da métrica.
2. Expanda o nó **Agente DxC, Segmento comercial**.
   A exibição em árvore de agentes, recursos e métricas é atualizada a cada 15 segundos para mostrar os dados atuais das métricas.
3. Exiba as métricas do navegador navegando nos nós.
4. (Opcional) Compartilhe o URL com seus colegas para que eles possam ver a mesma exibição da métrica específica na árvore.

Analisar erros

Os aplicativos web usam o JavaScript para ações como:

- Aceitar informações do usuário
- Fornecer efeitos de transição
- Processar e até mesmo apresentar dados complexos

Uma seção não funcional de uma página web provavelmente se deve a um erro no JavaScript ou no AJAX. O monitoramento de erros no JavaScript e no AJAX do agente do navegador fornece visibilidade dessas situações problemáticas.

Erros do JavaScript

O tratamento de erros do JavaScript pode ser local, com blocos try e catch, e global, com manipuladores de eventos. O agente do navegador usa um manipulador de erros global para capturar todos os erros do JavaScript não detectados na janela do navegador atual. O agente do navegador pode:

- Relatar o número de erros do JavaScript na métrica Erros de página por intervalo. Essa métrica é exibida sob o caminho da métrica da página no contexto apropriado da transação comercial ou do URL.
- Coletar informações sobre erros no JavaScript nativo e personalizado dentro da janela do navegador, como o número da linha e da coluna, a marca de data e hora e o rastreamento de pilha do erro.
- Gerar instantâneos por erro com os detalhes do erro.

Erros do AJAX

Os códigos de status do AJAX podem indicar um problema com os terminais do AJAX. O agente do navegador relata todas as chamadas do AJAX com os seguintes códigos de status do HTTP de resposta como erros do AJAX:

- Erro do cliente 4XX
- Erro de servidor 5XX

O agente do navegador também captura informações sobre uma resposta de erro para ajudá-lo a entender os problemas de cada uma das chamadas do AJAX. O agente do navegador pode:

- Relatar o número total de erros do AJAX na página por meio da métrica Erros de página por intervalo. Essa métrica é exibida sob o caminho da métrica da página no contexto apropriado da transação comercial ou do URL.
- Relatar os Erros de recurso por intervalo no caminho da métrica do AJAX no contexto apropriado da transação comercial ou do URL.
- Capturar informações sobre uma resposta de erro:
  - O código de status da resposta, por exemplo: 404
  - O texto de status da resposta, por exemplo: Não encontrado
  - Quaisquer mensagens de erro personalizadas do jQuery, por exemplo, uma mensagem de erro do analisador do JSON e o rastreamento de pilha

Analisar erros no instantâneo do erro

O agente do navegador cria um instantâneo por erro individual do JavaScript ou do AJAX. Cada erro que ocorre em uma página web monitorada em um intervalo contém as seguintes informações:

- Nome do navegador
- Versão do navegador
- URL da página web em que ocorreu o erro
- Descrição do erro conforme relatado pelo navegador
- Número da linha do erro conforme relatado pelo navegador
- Número da coluna do erro conforme relatado pelo navegador
- Nome do arquivo de origem conforme relatado pelo navegador

Exiba o instantâneo do erro para ver mais informações sobre o erro, incluindo o caminho de chamada e os parâmetros. A cada 15 segundos, um instantâneo de erro individual mostra os erros do JavaScript ou do AJAX no intervalo.

Siga estas etapas:

1. Clique na guia **Transações comerciais**.
   Uma lista de resumo mostra os rastreamentos correspondentes ao componente. Os segmentos mostram os tempos de duração. Os segmentos são codificadas por cor para indicar qualquer problema associado a uma transação, por exemplo, vermelho indica um erro.
2. Clique no rastreamento de uma transação do seu interesse.
   Os componentes da transação individual são exibidos em uma pilha gráfica (bolo de casamento).
3. Clique em um segmento comercial vermelho do seu interesse, por exemplo, para um erro do JavaScript:
   `Segmento comercial | <caminho_da_página> ou <transação comercial>/jserrors/error_SyntaxError.jsp (0 ms)`
4. Exiba **Component Details** e exiba os detalhes do erro.

   NOTE
   Nem todos os navegadores podem fornecer um rastreamento de pilha. Por exemplo, o Internet Explorer 10, o Microsoft Edge e o Safari 9.x não fornecem rastreamento de pilha.
5. Identifique os componentes que parecem causar o problema e siga o processo de resolução de problemas de sua organização.

Acessar e compreender a estação de trabalho

A estação de trabalho está disponível no DX APM. Saber mais sobre como acessar a estação de trabalho, onde encontrar as funções que foram movidas e quais funções não estão disponíveis.

- Acessar a estação de trabalho
- Compreender a estação de trabalho

Acessar a estação de trabalho

É possível fazer download da estação de trabalho a partir da interface do usuário. Para obter mais informações sobre como fazer download e conectar a estação de trabalho, consulte Conectar a estação de trabalho.

Compreender a estação de trabalho

A tabela a seguir explica quais funções não estão disponíveis na estação de trabalho. Use a coluna Mais informações para saber como é possível executar tarefas semelhantes na interface do usuário.

Table 1:

Função (Localização)	Descrição		Removido na estação de trabalho	Disponível na interface do usuário	Mais informações
Mapeamento de triagem de aplicativos (Investigador da estação de trabalho)	Apresenta a exibição gráfica de um aplicativo gerenciado, mostrando os erros e a integridade do aplicativo		Sim	Sim	• Exibir relacionamentos entre os componentes do mapa • Monitorar o desempenho usando a Exibição da experiência
Preferências do usuário > Guia Investigador (Estação de trabalho, todas as exibições)	Permite ativar ou desativar o recurso de atualização automática para a exibição do mapeamento de triagem do aplicativo		Sim	Sim	• Usar a linha de tempo e o realce
Mapeamento de dependência do SOA (Investigador da estação de trabalho, Navegador de métricas, Folhas de agente)	Fornece uma representação visual dos serviços que você implantou no ambiente de SOA e ajuda a monitorar e compreender como vários componentes se relacionam entre si		Sim	Não	N/D

Função (Localização)	Descrição		Removido na estação de trabalho	Disponível na interface do usuário	Mais informações
Mapeamento do local (Investigador da estação de trabalho, Navegador de métricas, Host e Folhas de agente)	Permite visualizar a configuração e monitorar o desempenho de sua infraestrutura.		Sim	Sim	• Exibir relacionamentos entre os componentes do mapa • Camadas do mapa
Encerrar o Enterprise Manager (Estação de trabalho, Editor do módulo de gerenciamento, Gerente)	Permite interromper o Enterprise Manager e o desconecta da estação de trabalho		Sim	Não	N/D
Publicar MIB (Estação de trabalho, Editor do módulo de gerenciamento, Gerente)	Permite capturar os dados de métrica armazenados nas coleções SNMP		Sim	Não	N/D
Nova ação (Estação de trabalho, Editor do módulo de gerenciamento, Elementos)	Permite criar: • Nova ação de notificação do console • Nova ação de notificação de SNMP • Nova ação de envio de email SMTP • Nova ação de comando do shell • Nova ação de alerta SNMP		Sim		• Criar e configurar ações de notificação no Team Center
Nova sessão de rastreamento de transação (Estação de trabalho, todas as exibições)	Rastreia a atividade das transações dentro de um aplicativo de produção		Sim	Sim	• Iniciar uma sessão de rastreamento de transações • Exibir relacionamentos entre os componentes do mapa
Novo visualizador de erros dinâmico (Estação de trabalho, todas as exibições)	Permite investigar erros em todos os agentes monitorados por um Enterprise Manager no modo *dinâmico*		Sim	Sim	• Investigar problemas usando o Bloco de notas de análise

Função (Localização)	Descrição		Removido na estação de trabalho	Disponível na interface do usuário	Mais informações
Consultar eventos históricos (Estação de trabalho, todas as exibições)	Permite investigar erros em todos os agentes monitorados pelo Enterprise Manager no modo *histórico*		Sim	Sim	• Investigar problemas usando o Bloco de notas de análise
console de status do APM (Estação de trabalho, todas as exibições)	É possível exibir status e eventos importantes para um Enterprise Manager independente ou agrupado		Sim	Não	N/D

Visão geral da Estação de trabalho

A estação de trabalho fornece o Investigador e o Console para exibição da integridade e dos dados do aplicativo.

O DX APM, por meio do ProbeBuilder, adiciona probes do agente a um aplicativo Java, PHP ou .NET. Usar o AutoProbe automatiza esse processo, com o ProbeBuilder adicionando probes dinamicamente quando o aplicativo é iniciado. Os arquivos PBD (ProbeBuilder Directive - Diretiva do ProbeBuilder) informam o ProbeBuilder como adicionar probes, como temporizadores e contadores, a componentes de Java, PHP ou .NET. Os probes instrumentam o aplicativo web.

Os probes medem partes de informações específicas sobre um aplicativo sem alterar a lógica comercial do aplicativo. Um agente é instalado no mesmo computador que o aplicativo instrumentado. Depois que os probes tiverem sido instalados no código de bytes, o aplicativo Java será apontado como um *aplicativo instrumentado*. Quando o aplicativo Java com probes estiver em execução, ele será chamado de aplicativo gerenciado.

O DX APM também detecta e instrumenta automaticamente componentes adicionais sem que as diretivas do ProbeBuilder estejam sendo definidas.

Enquanto um aplicativo gerenciado é executado, os probes retransmitem os dados coletados ao agente. O agente coleta e resume os dados e os envia ao Gerenciador corporativo.

Os dados coletados pelo Gerenciador corporativo podem ser acessados por meio de uma ou mais Estações de trabalho. É possível usar a estação de trabalho para exibir dados de desempenho. Você também pode configurar o Gerenciador corporativo para executar tarefas como coleta de informações para análise posterior e criação de alertas.

Enquanto um aplicativo gerenciado é executado, os agentes coletam dados de desempenho em tempo real e enviam as informações ao Enterprise Manager. A estação de trabalho permite executar estas tarefas:

- Configurar o Gerenciador corporativo
- Organizar métricas
- Exibir as informações que você escolhe em um formato conveniente

Monitorar o desempenho com ferramentas da estação de trabalho

As ferramentas da estação de trabalho ajudam você com as seguintes tarefas para monitorar melhor o desempenho do aplicativo:

- Filtrar e exibir métricas de desempenho para vários elementos do sistema em que seu aplicativo é executado.
- Detalhar para descobrir a causa raiz dos problemas de desempenho do sistema.
- Criar exibições gráficas de métricas.

Acessar diferentes exibições dos dados de métrica

Use a estação de trabalho para exibir dados de métrica em diferentes formulários. Os usuários autorizados podem executar funções administrativas e de configuração. A estação de trabalho apresenta informações nestas janelas:

- **Console**
  Mostra dados em painéis que contêm visualizadores de dados.
- **Investigador**
  Apresenta exibições em árvore de agentes, aplicativos, recursos e métricas.
- **Editor do módulo de gerenciamento**
  Apresenta uma exibição em árvore dos Módulos de gerenciamento, permitindo que você crie e edite Módulos de gerenciamento.
- **Editor de painéis**
  Permite que os usuários com permissão de *gravação* de um domínio (ou SuperDomain) criem e editem visualizadores de dados e outros objetos de painel, como imagens, formas, linhas e texto importados.
- **Visualizadores de dados**
  A apresentação visual de dados com base no tipo.

Conectar a estação de trabalho

A estação de trabalho está disponível para download pela seção **Downloads**, no painel esquerdo. Por padrão, a estação de trabalho está configurada para se comunicar diretamente com o gateway da nuvem. No entanto, as organizações que exigem comunicação por um único canal entre o data center e o gateway da nuvem podem conectar a estação de trabalho ao Cloud Proxy.

Sobre o console da estação de trabalho

O console é a exibição padrão quando você inicia a estação de trabalho e contém os painéis que mostram os dados de desempenho em exibições gráficas. Os painéis são ferramentas básicas para exibição de dados de gerenciamento no DX APM.

O Módulo de gerenciamento padrão fornece um conjunto de painéis de amostra. Os usuários autorizados podem criar painéis personalizados usando o Editor de painéis.

Você pode ter mais de uma janela do console aberta simultaneamente.

Para abrir uma nova janela do console:

- Selecione Estação de trabalho > Novo Console.

Sobre o Investigador da estação de trabalho

Use o Investigador para exibir métricas sobre aplicativos e seus chamados back-ends de diferentes maneiras.Você pode ter mais de uma janela do investigador aberta simultaneamente.

Para abrir uma nova janela do Investigador:

- Selecione Estação de trabalho > Novo investigador.

O Investigador é aberto, mostrando dados do seu aplicativo Java ou .NET.

Também é possível abrir uma janela do Investigador pelo console, clicando duas vezes em alguns elementos do painel, dependendo de como o elemento foi criado.

A guia Navegador de métricas

A guia Navegador de métricas mostra uma exibição centrada no agente dos seus aplicativos monitorados. Use-a para executar as seguintes tarefas:

- Exibir aplicativos e métricas organizados em uma hierarquia de árvore.
- Monitorar métricas detalhadas de cada camada de tecnologia.
- Use o rastreamento de transações para triagem de anomalias no desempenho do aplicativo.

Sobre o Editor do módulo de gerenciamento

Use o Editor do módulo de gerenciamento para criar ou editar um módulo de gerenciamento, que contém um conjunto de informações de configuração de monitoramento do DX APM. Os Módulos de gerenciamento são listados para cada domínio.

Observação: se você tiver uma licença completa do DX APM, será possível criar, editar ou excluir informações no Editor do módulo de gerenciamento. Na ausência de uma licença completa, você só poderá exibir informações aqui.

A árvore do Editor do módulo de gerenciamento lista os Módulos de gerenciamento implantados no Gerenciador corporativo pelo domínio.

O lado direito do Editor do módulo de gerenciamento apresenta as definições da configuração atual para o elemento que está selecionado na árvore.

Um usuário autorizado pode modificar elementos no Editor do módulo de gerenciamento.

Sobre o Editor de painéis

O Editor de painéis fornece ferramentas para criação e disposição de visualizadores de dados, formas, linhas, caixas de texto e conectores. Os usuários com permissões apropriadas podem criar e editar painéis e objetos de painel como imagens, formas, linhas e texto importados.

Sobre visualizadores de dados

Os visualizadores de dados no painel visualizador da guia Navegador de métricas ou em um painel exibem dados de um aplicativo ativado para DX APM em um formato visual. Os visualizadores de dados podem exibir dados de uma métrica, um recurso ou um elemento, como um alerta.

Observação: o valor de data e hora em visualizadores de dados é a hora do relógio no computador que está hospedando o Gerenciador corporativo. No entanto, o valor de tempo é ajustado para o fuso horário em que a estação de trabalho está em execução.

Tipos de visualizador de dados

Os tipos de dados tem um tipo de visualizador de dados padrão e visualizadores alternativos.

Tipo de dado	Tipo de visualizador de dados padrão	Também pode ser exibido como
Métrica	Gráfico	Medidor de discagem, Gráfico de barras, Equalizador gráfico, Visualizador de sequência de caracteres, Visualizador de texto
Agrupamento de métricas	Gráfico	Gráfico de barras, Visualizador de sequência de caracteres
Alerta	Indicador de alerta	Gráfico, Gráfico de barras ou Visualizador de sequência de caracteres
Calculadora	Gráfico	Medidor de discagem, Gráfico de barras, Equalizador gráfico, Visualizador de sequência de caracteres

Dependendo do tipo de métrica ou do elemento, a estação de trabalho pode exibir os dados em um visualizador de dados com os tipos de exibição mostrados aqui.

Gráfico

Os gráficos plotam valores ao longo do tempo. Nas exibições em tempo real, o gráfico exibe dinamicamente o período mais recente que se encaixa no gráfico.

Se o gráfico exibir um alerta, os limites de cuidado e risco aparecem como linhas amarela e vermelha, respectivamente.

Você pode alterar a escala dos gráficos ao exibir dados dinâmicos para ver dados em uma exibição mais clara.

Gráfico de barras

Gráficos de barras exibem valores de dados atuais como barras horizontais. O gráfico de barras é a exibição padrão para as N principais exibições filtradas.

Se um gráfico de barras estiver mostrando um alerta, as barras serão verdes, amarelas ou vermelhas para corresponder ao status do alerta.

O gráfico de barras está disponível apenas para exibição de dados dinâmicos.

Equalizador gráfico

Os Equalizadores gráficos mostram o valor atual dos dados, bem como níveis altos recentes.

Visualizador de sequência de caracteres

Os visualizadores de sequência de caracteres exibem um valor como uma linha de texto. Eles permitem que alguns valores sejam exibidos em um espaço relativamente pequeno. Você também pode usar um visualizador de sequência de caracteres para valores simples que não são alterados, como Hora da inicialização ou Endereço IP.

Observação: com métricas dinâmicas de agentes conectados, a maior parte dos dados é válida apenas a fração de tempo de 15 segundos mais recente. Portanto, quando um agente é desconectado, as métricas de sequência de caracteres não mostram valores. No entanto, algumas métricas constantes, como o horário de início original do agente, permanecem válidas, quer o agente esteja ou não esteja conectado no momento.

Visualizador de texto

Os visualizadores de texto mostram o texto de dados quando novos valores são acrescentados a, por exemplo, um log do sistema ou de exceções.

Sobre alertas e indicadores de alerta

Os indicadores de alerta mostram se uma métrica ultrapassou um limite:

- Disco verde = status normal
- Diamante amarelo = cuidado, o limite foi ultrapassado
- Octógono vermelho = risco, o limite foi ultrapassado
- Disco cinza = o alerta não tem dados.

Os indicadores de alerta podem aparecer como acima, como uma matriz de três indicadores na qual o indicador ativo informa o status. Com mais frequência, eles aparecem como um indicador único que muda de cor e forma quando seu status muda.

Os indicadores de alerta podem aparecer em vários locais e modos:

- em painéis
- na guia Visão geral
- como linhas de limite em um gráfico
- como cores nas células da tabela, em que a funcionalidade é suportada
- no lugar de nós de árvore

Entendendo a diferença entre *alertas* e *indicadores de alerta*

É importante compreender exatamente o que é um alerta. Certifique-se de saber a diferença entre:

- o **alerta** em si, a definição que inclui atributos salvos como:
  - valores limitados
  - o agrupamento de métricas ao qual ele é vinculado
  - o Módulo de gerenciamento ao qual ele pertence
- o **indicador de alerta**, que é uma exibição gráfica do status do alerta

Fazer triagem com a estação de trabalho

O Investigador da estação de trabalho fornece uma exibição centrada no agente que permite examinar métricas e identificar possíveis causas de problemas no seu ambiente.

Recursos gerais do Investigador

Dicas de navegação

Para abrir um Investigador:

- Selecione **Estação de trabalho** > **Novo investigador**.

Para navegar para frente e para trás:

- Os botões de seta Avançar e Voltar estão localizados no canto superior direito. Use esses botões para avançar e retroceder entre itens da árvore hierárquica exibidos anteriormente.
- Faça seleções nas listas suspensas ao lado dos botões Avançar ou Voltar no canto superior direito do Investigador.

Painéis do investigador

O Investigador contém dois painéis:

- Uma hierarquia de árvore em um painel restrito no lado esquerdo
- Um painel visualizador grande no lado direito
  - O conteúdo do painel visualizador varia de acordo com o tipo de item selecionado na árvore hierárquica.
  - Uma ou mais guias compõem o painel visualizador.Cada guia mostra uma exibição diferente.

Os gráficos de métrica são a maneira mais comum de exibir métricas, mas não a única. Para métricas, uma exibição dos dados da métrica é mostrada. Cada tipo de métrica tem uma exibição padrão no painel visualizador.

Dicas de ferramenta

As dicas de ferramenta identificam os caminhos e valores nas árvores hierárquicas e em painéis visualizadores. Acesse as dicas de ferramenta na guia Navegador de métricas passando o mouse sobre o nome da métrica em uma área de legenda do visualizador de dados.

Você poderá ver vários tipos de informação na dica de ferramenta, dependendo do elemento da UI sobre o qual o cursor estiver. Essas informações podem incluir os seguintes dados:

- Nome da métrica totalmente qualificada, seu valor e seus valores mínimo e máximo
- Uma contagem de quantos pontos de dados foram relatados na fração de tempo selecionada
- Uma marca de data e hora do valor de dados mais próximo do cursor, ou uma nota de comparação
- Por exemplo, "Valor muito alto", quando o valor da métrica excede um limite definido.

NOTE

As dicas de ferramenta não estão mais disponíveis nos nós.

Exibição centrada no agente

Um agente é uma parte do software que é instalada em um host em que um aplicativo está implantado. O agente coleta métricas de aplicativo e ambientais e as retransmite ao Gerenciador corporativo.A guia Navegador de métricas permite navegar em uma lista abrangente de métricas que um único agente está relatando. Cada aplicativo cujos dados um agente está relatando aparece em uma árvore hierárquica sob um nó chamado **Front-ends**.

A exibição centrada em agente contém as seguintes seções:

- A *árvore centrada no agente* à esquerda fornece informações sobre cada host e aplicativo que o Gerenciador corporativo gerencia. As métricas que aparecem na árvore centrada no agente são uma função destes fatores:
  - Recursos que seus aplicativos usam
  - Dados que os agentes do Introscope foram configurados para relatar.
- O *painel visualizador* à direita apresenta detalhes, muitas vezes gráficos, para o recurso ou a métrica na árvore. É possível selecionar guias Exibir para abrir diferentes exibições de dados. As guias disponíveis variam de acordo com o item selecionado na árvore. Em algumas exibições, na seção inferior do painel visualizador, você pode ter opções para controlar os dados exibidos no visualizador.
- Uma tabela na parte inferior do painel visualizador, que exibe dados em formato tabular. Os dados exibidos na tabela variam de acordo com as seleções feitas no painel visualizador ou na árvore.

Limite da métrica do agente

Um ícone de agente exibindo uma faixa vermelha indica um agente com limitação de métrica. Um agente é limitado quando o número de métricas que ele produz é maior que o número de métricas que o Gerenciador corporativo pode processar. Depois que as métricas do agente são limitadas, não sabemos quais métricas não estão sendo relatadas. As métricas podem ser limitadas no final do agente ou no final do Gerenciador corporativo. Para um limite de métrica com base no agente, você vê mensagens nos logs indicando que o limite foi aplicado e nenhum valor novo de métrica foi reportado. Para um limite de métrica com base no Gerenciador corporativo, todas as métricas que foram relatadas antes do limite ser aplicado continuam relatando valores, mas nenhum novo tipo de métrica aparece. A métrica de suportabilidade de um agente limitado relata um valor 1. Um agente que está limitado indica que muita instrumentação está ativada. Ajuste o nível de instrumentação na configuração do agente.

Um agente limitado também pode indicar uma explosão de métricas. Nessa situação, os componentes dentro dos agentes relatam métricas constantemente variadas.Para obter mais informações sobre explosões de métricas, consulte Explosões de métricas.

Nó Super Domain

O nó **SuperDomain** contém métricas para todos os agentes que se reportam ao Enterprise Manager ao qual a estação de trabalho está conectada. As métricas são organizadas em uma hierarquia `Host|Processo|Agente` .

Os nós logo abaixo do nó **SuperDomain** são hosts virtuais e físicos.

- **Custom Metric Host (Virtual)** Este nó não corresponde a um computador host físico. O nó é um host virtual que contém métricas diferentes daquelas relatadas por agentes individuais específicos. Por exemplo, as métricas

personalizadas são exibidas sob o nó Custom Metric Host. As métricas personalizadas podem ser de calculadoras que você configurou ou de agentes agregados configurados.
- **Hosts** Um nó para cada computador que hospeda um agente. Cada nó do host contém um nó do processo para a instância do aplicativo que está sendo monitorado. O nó do processo contém um nó de agente. O nó de agente contém nós que correspondem aos recursos do sistema e aplicativo, que contêm métricas.
  Observação: os recursos de aplicativo que aparecem no nó de agente variam com base no tipo de agente, seja Java, seja .NET.

O SuperDomain inclui todos os domínios e agentes definidos pelo usuário. O administrador do Gerenciador corporativo pode configurar o Gerenciador corporativo para mostrar domínios filho com permissões separadas.

As métricas que a árvore centrada no agente exibe são uma função destes dois fatores:

- Diretivas ProbeBuilder usadas para instrumentar o aplicativo
- Atividade em tempo de execução do aplicativo em si

Uma métrica aparece na árvore apenas quando o agente começa a relatá-la. A métrica permanece visível na árvore, mesmo que o agente deixe de relatá-la.

Quando as métricas têm diferentes tipos de métrica, no Investigador, as métricas podem ter o mesmo nome e podem aparecer duas vezes. Como ocorre com todas as métricas, as métricas inativas nessa situação aparecem esmaecidas.

Ferramentas para monitorar a integridade do Gerenciador corporativo

Métricas de suportabilidade

As métricas de suportabilidade fornecem informações sobre o estado do Gerenciador corporativo e do computador no qual ele está em execução. Você pode exibi-las no caminho `SuperDomain|Custom Metric Host|Custom Metric Agent|Enterprise Manager`.

Nó de domínio

O administrador do DX APM pode organizar os agentes que se reportam ao Enterprise Manager em domínios. Nesse caso, o nó de domínio da árvore centrada no agente contém subnós para cada domínio. Cada nó de domínio está estruturado na mesma hierarquia `Host|Processo|Agente` que o SuperDomain. Cada nó de domínio também pode conter um Custom Metric Agent para métricas personalizadas.

Como as permissões de usuário afetam o que você pode exibir

O administrador do DX APM atribui permissões para os domínios e componentes que os usuários da estação de trabalho podem ver. As permissões são disponibilizadas apenas quando um administrador as configurou usando o Enterprise Enablement Manager.

O conteúdo da guia **Navegador de métricas** se baseia nas permissões de domínio do usuário:

- Os usuários com a permissão `SuperDomain` (pelo menos permissão de leitura) veem todos os domínios para esse Enterprise Manager na árvore centrada no agente.
- Os usuários com permissões para vários domínios veem informações do domínio para os ambientes na árvore centrada no agente.
- Os usuários com permissões para apenas um domínio não veem informações de domínio na árvore centrada no agente. Os usuários veem apenas as pastas para métricas e módulos de gerenciamento.

Guia Navegador de métricas

A guia Navegador de métricas lista métricas e outras informações em formato de árvore. Os nós de alto nível imediatamente abaixo dos nós de domínio representam os agentes instalados nos hosts do servidor de aplicativos individuais ou equivalente.

Entre os vários componentes que representam os nós de alto nível estão:

- Componentes do seu aplicativo J2EE, PHP ou .NET, como servlets, EJBs ou página ASP
- Nós do sistema, incluindo o host que executa o servidor de aplicativos e o computador host que executa o DX APM.
- Eventos, defeitos e outras ocorrências diferenciadas

Você pode exibir dados dinâmicos no Investigador ou selecionar um intervalo temporal para exibir dados históricos. A exibição de dados padrão é Dinâmica.

Métricas na guia Navegador de métricas

As métricas padrão que a estação de trabalho exibe na guia Navegador de métricas varia de acordo com o nó que você seleciona na árvore hierárquica.

Métricas padrão

Para componentes de aplicativo monitorados de front-end e back-end, bem como para muitos outros componentes de aplicativo, o Introscope exibe cinco métricas padrão, às vezes, chamadas de Métricas de diagnóstico:

- Tempo médio de resposta (ms) – uma medida da velocidade de resposta do aplicativo.
- Invocações simultâneas – o número de solicitações que são tratadas em um determinado momento.
- Erros por intervalo – o número de erros que ocorrem durante um período especificado.
- Respostas por intervalo — o número de solicitações que são concluídas durante um período especificado.
- Contagem de paralisações – o número de paralisações (ou solicitações não concluídas) que não foram concluídas antes de um limite de tempo especificado.

Além das cinco métricas padrão e, às vezes, no lugar delas, o Introscope coleta e exibe outras métricas relevantes para o nó.

Front-ends e back-ends

Por padrão, o Introscope define um front-end como um arquivo .war ou .jsp que primeiro trata de uma transação de entrada para um aplicativo. Em um aplicativo .NET, o equivalente seria uma página ASP.

Um *back-end* é um sistema externo do qual um aplicativo web depende para alguma parte de seu processamento. Normalmente, é um banco de dados, mas pode ser qualquer sistema externo, como servidor de email, um sistema de processamento de transações (como IBM CICS ou BEA Tuxedo) ou um sistema de troca de mensagens (como MQSeries). O Introscope identifica automaticamente os bancos de dados como sistemas de back-end pelo seu nome. Para outros sistemas externos, o Introscope analisa a atividade do soquete do aplicativo e nomeia o back-end com base no endereço IP e na porta pelos quais o aplicativo está se comunicando.

Exibir métricas para back-ends

O nó Backends da árvore do navegador de métricas contém um nó para cada back-end, incluindo aqueles detectados automaticamente pelo Introscope ou marcados explicitamente como um back-end durante o ProbeBuilding.

Geralmente, os back-ends são um banco de dados, mas podem ser um sistema externo, como um servidor de email, um sistema de processamento de transações (como IBM CICS ou BEA Tuxedo) ou um sistema de troca de mensagens (como MQSeries).

Métricas de back-end do banco de dados

Quando o sistema de back-end for um banco de dados, essas métricas refletirão a atividade e o desempenho do back-end em todos os aplicativos que ele atende:

- Tempo médio de resposta (ms)
- Concurrent Invocations
- Erros por intervalo
- Contagem de conexões – o número de conexões com o banco de dados durante um determinado intervalo.
- Respostas por intervalo
- Contagem de paralisações

Formato da nomenclatura do back-end do banco de dados

Esta seção explica a convenção de nomenclatura do Introscope para back-ends do banco de dados.

Oracle

O nome do back-end é uma concatenação da sequência de caracteres da SID do Oracle, do host e da porta do banco de dados delimitados por um hífen, mais a sequência de caracteres *(Oracle DB)*.

Por exemplo:

```
PRODORCL3 sfoprod6.globex.com-1521 (Oracle DB)
```

DB/2

O nome do back-end é uma concatenação da sequência de caracteres DBName e da sequência de caracteres *(DB/2 DB)*.

Por exemplo:

```
Inventory4 (DB/2 DB)
```

Microsoft SQL Server

O nome do back-end pode ser uma concatenação do nome do banco de dados, do nome da instância, do host e da porta do banco de dados delimitados por um hífen, mais a sequência de caracteres *(MS SQL Server DB)*, dependendo da configuração do driver do banco de dados.

Se o driver tiver um nome de banco de dados e um nome de instância, o nome do back-end no Investigador será parecido com este:

```
PRODORCL3 (instance Mx22) on prod6.globex.com-1521 (MS SQL Server DB)
```

Se o driver não tiver nome de banco de dados, o nome do back-end no Investigador será parecido com este:

```
SQLServer on prod6.globex.com-1521 (MS SQL Server DB)
```

Se o driver tiver um nome de banco de dados e nenhum nome de instância, o nome do back-end no Investigador será parecido com este:

```
PRODORCL3 on prod6.globex.com-1521 (MS SQL Server DB)
```

Se o driver tiver um nome de instância e nenhum nome de banco de dados, o nome do back-end no Investigador será parecido com este:

```
(instance Mx22) on prod6.globex.com-1521 (MS SQL Server DB)
```

Padrões e retornos

Nos casos em que o driver do banco de dados não oferecer suporte à consulta ao nome do banco de dados, o nome será padronizado para o URL do JDBC, sendo o caractere de dois-pontos (:) substituído pelo caractere de porcentagem (%). Em alguns casos, até mesmo esse valor de retorno não será disponibilizado, de modo que o nome do banco de dados será padronizado para o nome da classe do driver do banco de dados. O comportamento exato varia de acordo com o fornecedor e a versão do driver do banco de dados.

Outras métricas de back-end

Cada sistema de back-end também pode ser configurado para relatar as seguintes métricas:

- Confirmações
- Reversões
- SQL

Métricas de alerta na árvore centrada no agente

Cada cor de alerta tem um valor de métrica:

- Cinza – 0, não há dados disponíveis
- Verde – 1, OK
- Amarelo – 2, Cuidado
- Vermelho – 3, Risco

A tabela a seguir mostra como são os valores de alerta da unidade de métricas na guia Visão geral.

Tipo de métrica	O que um indicador amarelo significa	O que um indicador vermelho significa
Usuário	Erros de front-end estão anormais Tempo de resposta do front-end está anormal Contagem de paralisações do front-end está anormal	Erros do front-end estão *bastante* anormais Contagem de paralisações do front-end está *bastante* anormal
VM	Agregação da utilização da CPU está anormal e acima de 30% Utilização do pool de conexões JDBC está anormal	Agregação da utilização da CPU está *bastante* anormal e acima de 50% Utilização do pool de conexões JDBC está *bastante* anormal
Resumo de back-end	Tempo de resposta do back-end está anormal Contagem de erros do back-end está anormal Paralisações do back-end estão anormais	Contagem de erros do back-end está *bastante* anormal Paralisações do back-end estão *bastante* anormais

É possível exibir as métricas de alerta selecionando as métricas User, VM e Backends|*BackendName*, abaixo do nó Heuristics no Investigador.

As métricas subjacentes que orientam as métricas de alerta são exibidas nas pastas User, VM e Backends|*BackendName* na árvore.

Administrando conexões de agente da estação de trabalho

Você pode emitir comandos diretamente da estação de trabalho para desmontar, ou desativar agentes ou métricas individuais.

Quando um agente é implantando em um servidor de aplicativos, ele inicia automaticamente quando o servidor de aplicativos é iniciado, e aparece na árvore Navegador de métricas abaixo do Gerenciador corporativo para o qual ele relata os dados de métrica. Quando o agente é exibido na árvore, diz-se que ele está *montado*.

Quando um servidor de aplicativos é desativado, o agente para de relatar dados ao Gerenciador corporativo. Diz-se que esse agente está *desconectado* e será exibido na árvore Navegador de métricas em cinza e esmaecido, em vez de colorido.

Um agente desconectado continua aparecendo montado na árvore Navegador de métricas e você ainda consegue navegar pelas métricas que ele relatou antes que ele seja desconectado. Se desejar removê-lo da árvore Navegador de métricas, você deverá *desmontar* o agente.

Para desmontar um agente:

1. Clique com o botão direito em um agente desconectado.
2. Escolha Desmontar <*Nome_do_agente*>.
   O Agente desaparecerá da árvore Navegador de métricas.

Se desejar exibir os dados históricos armazenados no banco de dados SmartStor de um agente que foi desmontado, você poderá remontar o agente para que ele apareça novamente na árvore Navegador de métricas.

Para remontar um agente desconectado:

1. Escolha Gerenciador > Montar agente.
   A caixa de diálogo Seletor de agentes é exibida.
2. Na lista, selecione um agente para remontar.
3. Clique em OK.

A árvore Navegador de métricas exibe os agentes desconectados e você pode navegar pelos dados armazenados no banco de dados SmartStor.

Caso queira que o Gerenciador corporativo pare de armazenar dados de um agente que ainda esteja em execução, você poderá interromper a coleta de dados sem interromper o servidor de aplicativos, selecionando o comando Encerrar.
Observação: o comando Encerrar não finaliza de fato o agente; ele encerra a conexão entre um agente em execução e o Gerenciador corporativo.

Para encerrar a conexão com um agente em execução:

1. Clique com o botão direito em um agente conectado.
2. Escolha Encerrar "<*Nome_do_agente*>".

O agente continuará em execução no servidor de aplicativos desde que este esteja em execução, mas o Gerenciador corporativo não estará mais conectado a ele nem armazenará mais dados de métrica para ele.

É possível ativar a conexão com um agente depois de tê-la encerrado.

Para ativar a conexão com um agente encerrado:

1. Clique com o botão direito em um agente encerrado.
2. Escolha Ativar todos os componentes do agente.

A conexão entre o agente e o Gerenciador corporativo será reaberta e o agente começará a relatar dados ao Gerenciador corporativo. Observe que você terá que aguardar de 30 a 45 segundos para que os dados comecem a aparecer na estação de trabalho.
Observação: o comando Ativar todos os componentes do agente funcionará somente se você tiver encerrado anteriormente a conexão do agente por meio da estação de trabalho usando o comando Encerar "<*Nome_do_agente*>".

Exibições na guia Navegador de métricas

Com a guia do navegador de métricas selecionada no painel esquerdo do Investigador, as exibições que aparecem no painel direito variam de acordo com o recurso ou a métrica selecionado(a) na árvore da guia do navegador de métricas. Dependendo do tipo de nó selecionado, você verá as guias para uma ou mais destas exibições:

- Guia Geral
- Guias Visão geral
- Guia Pesquisar
- Guia Rastreamentos
- Guia Erros
- Guia Contagem de métricas
- Guia Despejos de segmento

Guia Geral

Quando você seleciona uma métrica, a guia Geral mostra uma exibição gráfica dela – seja para dados dinâmicos, seja para um período histórico selecionado. Consulte Exibindo dados históricos na guia Navegador de métricas para ver uma explicação de como selecionar intervalos de dados históricos a serem exibidos.

Para alguns nós na árvore, a guia Geral mostra o caminho para esse objeto de nó na hierarquia do Investigador. Por exemplo, quando o nó Frontends é selecionado, a guia Geral é exibida neste caminho:

```
*SuperDomain*|HostName|ProcessName|AgentName|Frontends
```

Para alguns outros nós na árvore, a guia Geral mostra a exibição 10 mais lentos do nó selecionado. Por exemplo, quando o nó EJB é selecionado, a guia Geral mostra os tempos de resposta dos dez principais componentes chamados do nó EJB selecionado.

Dez métricas mais lentas ou piores

Quando você seleciona determinados recursos no Investigador, a guia Geral do painel Visualizador mostra as dez métricas mais lentas/piores para o recurso selecionado. Os recursos Java incluem servlets, JSP, EJBs e JDBC; para recursos .NET, os recursos incluem ASP.NET, ADO.NET e componentes atendidos.

Essas métricas são exibidas em um gráfico de barras no painel Visualizador do Investigador.

Também é possível exibir os tempos de resposta dos dez principais componentes chamados de um servlet, EJB, ou JSP para Java selecionado, ou ASP.NET, ADO.NET e componentes atendidos para .NET.

Caso você veja menos de dez barras no gráfico, isso significa que há menos de dez componentes monitorados sob esse recurso. Se as métricas não contiverem dados, é possível que nomes de métrica sejam exibidos no painel Visualizador, mas nenhuma barra de dados.

Guias Visão geral

O Investigador resume as informações em uma guia Visão geral para:

- o Aplicativo geral – consulte Visão geral do aplicativo
- a integridade do EM — consulte Visão geral do EM.
- dados das páginas ASP.NET — consulte Visão geral do ASP.NET.
- dados de EJBs — consulte Visão geral do EJB.
- dados de front-ends do aplicativo – consulte Visões gerais do front-end.
- dados dos sistemas de back-end do aplicativo – consulte Visão geral do back-end.
- a memória heap da GC (Garbage Collection - Coleta de Lixo) – consulte Visão geral da memória heap da GC.
- contagens de instâncias das classes Java instanciadas na JVM — consulte Contagens de instâncias.
- dados de JavaNIO — consulte Visão geral do JavaNIO.
- dados de componentes da JTA — consulte Visão geral da JTA.
- dados de servlets — consulte Visão geral do servlet.
- conexões de soquete — consulte Visão geral do soquete.
- dados de struts — consulte Visão geral de struts.
- dados em segmentos em execução – consulte Visão geral de segmentos.
- dados de componentes XML – consulte Visão geral de XML.

NOTE

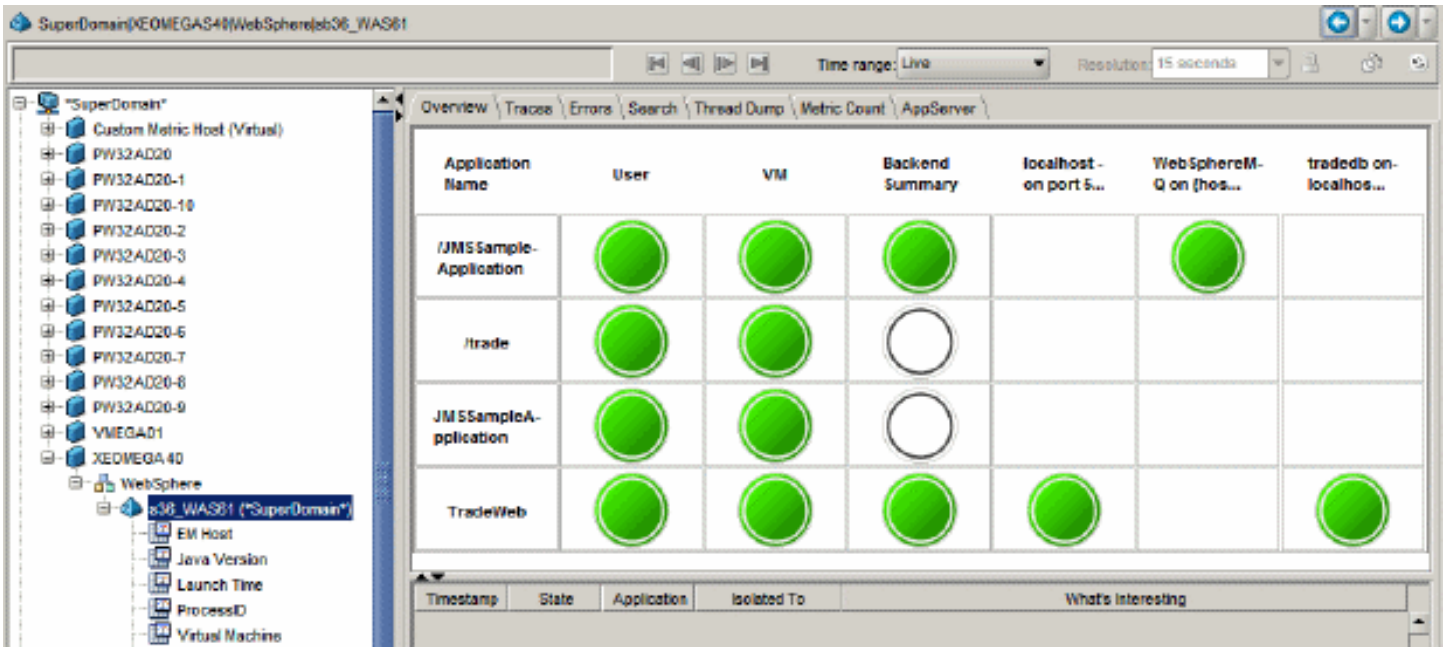
As guias Visão geral exibem o valor da métrica atual quando exibidas no **Modo dinâmico**. Quando exibidas no **Modo histórico**, as guias Visão geral mostram valores de métrica agregados (valores médios ou somados, dependendo do tipo de métrica) para o intervalo de datas selecionado.

Visão geral do aplicativo

A Visão geral do aplicativo é disponibilizada quando você seleciona um agente na árvore centrada no agente e ativa o monitoramento e a triagem do aplicativo. Ela mostra indicadores gerais de integridade, bem como um log de eventos relacionados e informações históricas de métrica.

A Visão geral mostra uma linha de indicadores para cada aplicativo gerenciado pelo agente selecionado no momento. O Introscope apresenta esses dados para cada aplicativo que detecta — quando um servlet é executado, o Introscope faz uma chamada a *getServletContextName()* da interface *ServletContext* para determinar o nome do aplicativo. Depois que o aplicativo é iniciado, a guia Visão geral é atualizada automaticamente para exibir uma linha de indicadores para ele.

A ilustração abaixo mostra a guia Visão geral de um agente em um servidor de aplicativos WebSphere chamado *s36_WAS61:*



Essa ilustração mostra quatro aplicativos — um em cada linha da tabela - gerenciados por esse agente. Para esse aplicativo, é possível exibir alertas mostrando o estado de:

Usuário: indica o quão satisfatória as interações dos usuários finais com o aplicativo podem ser. Satisfação é uma função de tempo de resposta, esperas, paralisações e erros.

- Verde — interações normais, satisfatórias do usuário com o aplicativo.
- Amarelo – uma tentativa de usar o aplicativo que provavelmente terá resultados insatisfatórios; por exemplo, demora no tempo de resposta ou erros.
- Vermelho – indica um grave problema de disponibilidade e que uma tentativa de usar o aplicativo provavelmente falhará.

VM: indica a integridade e a disponibilidade dos recursos de servidor, como pools de recursos e CPU.

- Verde — integridade normal dos recursos de servidor.
- Amarelo – limitações ou interrupções de recurso
- Vermelho – limitações ou interrupções graves.

Resumo de back-end: indica as piores integridade e disponibilidade em todos os back-ends acessados pelo aplicativo. Por exemplo, se um dos três back-ends tiver uma limitação ou interrupção grave de recurso, o indicador Todos os back-ends estará vermelho. A finalidade do indicador Todos os back-ends é permitir que o usuário, com rolagem mínima, avalie rapidamente se algum dos back-ends tem problemas que exigem investigação.

- Verde — integridade e disponibilidade normais do back-end em todos os back-ends avaliados pelo aplicativo.
- Amarelo – pelo menos um dos back-ends acessados pelo aplicativo está recebendo erros ou enfrentando paralisações, ou os tempos de resposta estão muito longos.
- Vermelho – pelo menos um dos back-ends acessados pelo aplicativo está enfrentando limitações ou interrupções graves de recurso.

Back-ends: todos os indicadores à direita do indicador Resumo de back-end correspondem aos back-ends individuais.

- Verde — integridade e disponibilidade do back-end normais.
- Amarelo – erros ou paralisações de back-end, ou tempos de resposta muito longos.
- Vermelho – limitações ou interrupções graves de recurso do back-end.

Os indicadores são atualizados a cada 15 segundos. As linhas são classificadas primeiro por cor (linhas com indicadores vermelhos precedem as linhas com amarelos, que precedem as linhas com verdes) para reduzir a necessidade de rolagem na identificação de possíveis problemas. Em uma categoria de cor, as linhas são colocadas em ordem alfabética por nome do aplicativo.

Usando alertas para detalhar mais os dados

É possível clicar duas vezes em um alerta na guia Visão geral para exibir os dados subjacentes dessa camada de aplicativos. Por exemplo, se você clicar duas vezes no alerta Usuário, a estação de trabalho exibirá o nó de URLs para esse agente.

Métricas da visão geral do aplicativo no modo histórico

Em um intervalo histórico, uma cor de alerta reflete o valor de pior caso da heurística em qualquer ponto no intervalo histórico. Por exemplo, se em algum momento durante um intervalo histórico, a heurística Usuário para um agente foi amarela, mas nunca vermelha, a guia Visão geral desse intervalo histórico será amarela.

Métricas da visão geral do aplicativo para um agente virtual

Para Agentes virtuais, as heurísticas são avaliadas com base nas métricas de Agente virtual. Por esse motivo, a guia Visão geral de um Agente virtual pode indicar um valor diferente do valor para os agentes físicos no Agente virtual.

Por exemplo, a guia Visão geral do Agente virtual pode exibir um alerta de usuário verde, mesmo que a guia Visão geral de um dos agentes nesse Agente virtual mostre um alerta de usuário amarelo.

As métricas heurísticas serão geradas apenas se as métricas que são analisadas existirem. Assim, se o Agente virtual for configurado para não incluir métricas PMI do WebSphere, CPU ou JMX, por exemplo, não haverá pasta de VM e o alerta de VM permanecerá cinza.

Visão geral do EM

Você pode exibir várias métricas no próprio Gerenciador corporativo selecionando o nó EM em Custom Metric Agent.

Visão geral do ASP.NET

Em ambientes onde o Introscope está monitorando um aplicativo .NET, um nó ASP.NET na árvore centrada no agente permite monitorar as métricas para componentes do aplicativo.

Visão geral do EJB

A visão geral do EJB (Enterprise Java Beans) mostra estatísticas de beans de entidade, sessão e orientados a mensagens.

Visões gerais do front-end

As visões gerais dos nós Frontend mostram métricas de aplicativo em gráficos, além de estatísticas relacionadas a transações no aplicativo:

Os programas que o Investigador exibe no nó Frontends representam os componentes de um aplicativo que trata primeiramente de uma transação de entrada.

Visão geral do back-end

As visões gerais dos nós Backend mostram exibições gráficas de métricas de banco de dados e uma exibição de tabela do SQL abaixo do nó.

Visão geral da memória heap da GC

A visão geral da memória heap da GC (Garbage Collection - Coleta de Lixo) mostra o uso da memória heap.

Guia Visão geral do GC Monitor

Clicar no nó GC Monitor na árvore Navegador de métricas faz com que a guia Visão geral do GC Monitor seja exibida no painel do visualizador. A guia Visão geral exibe três painéis:

- Topo: um indicador de alerta na métrica Percentual de memória heap do Java em uso para a JVM.
- Central: uma exibição tabular dos coletores de lixo na JVM
- Parte inferior: uma exibição tabular de pools de memória na JVM

OBSERVAÇÃO: o indicador de alerta no painel superior da guia Visão geral, bem como o sombreamento colorido que aparece na tabela nos painéis central e parte inferior, baseiam-se nos limites de cuidado e risco predefinidos. Os usuários não podem redefinir esses limites.

Quando você seleciona qualquer um dos nós individuais Garbage Collector ou Memory Pools, os gráficos exibem as mesmas métricas mostradas na guia Visão geral.

Para obter mais informações:

- Entenda como usar as métricas do GC Monitor para ajustar a alocação de memória da JVM

Ativar/desativar GC Monitor

As métricas do GC Monitor são ativadas por padrão.

Para desativar as métricas do GC Monitor:

1. Abra o arquivo *IntroscopeAgent.profile*.
2. Edite o valor da propriedade introscope.agent.gcmonitor.enable de true para false.
3. Salve e feche o arquivo.
   OBSERVAÇÃO: essa é uma propriedade que pode ser configurada dinamicamente; as alterações não exigem reinicialização do Gerenciador corporativo.

Para obter mais informações sobre como editar o arquivo IntroscopeAgent.profile, consulte Agente do Java.

Contagens de instância

A guia Contagens de instâncias mostra as classes instanciadas na JVM.

Visão geral do JavaNIO

A visão geral do NIO mostra as tabelas de datagramas e canais, incluindo métricas de cliente e servidor. Com o nó JavaNIO selecionado, a guia Visão geral exibe informações gerais sobre o nó selecionado, incluindo todas as portas com atividade do NIO.

Visão geral de Channels do NIO

A guia Visão geral do nó Channels exibe informações de servidor e cliente para datagramas e soquetes.

Visão geral de Sockets do NIO

A guia Visão geral do nó Sockets exibe gráficos para dados de largura de banda de entrada e saída, bem como dados de leitores e gravadores simultâneos, além de informações de cliente e servidor para soquetes.

Visão geral de Datagrams do NIO

A guia Visão geral do nó Datagrams exibe gráficos para dados de largura de banda de entrada e saída, bem como dados de leitores e gravadores simultâneos, além de informações de cliente e servidor para datagramas.

Visão geral da JTA

A guia Visão geral da JTA exibe dados sobre componentes da JTA.

Visão geral do servlet

A Visão geral do servlet mostra uma tabela de servlets no nó. Quando você seleciona um servlet, o Investigador mostra suas estatísticas em um gráfico.

Selecione um servlet individual para ver sua guia Visão geral resumida.

Visão geral do soquete

A Visão geral do soquete (não deve ser confundido com a visão geral de Sockets do NIO) mostra tabelas para soquetes de cliente e servidor, além de informações de soquete para cada porta. Com o nó Socket selecionado na árvore centrada no agente, o painel do visualizador no lado direito exibe todas as portas com soquetes ativos. Selecionar uma porta na tabela Servidor, no topo do painel do visualizador, exibe as portas de cliente desse servidor na tabela Cliente na parte inferior. A seleção de uma porta na árvore centrada no agente exibe gráficos de métrica sobre eventos e carga.

Visão geral de struts

A guia Visão geral de struts mostra os componentes de struts, com uma exibição do tempo médio de resposta para todos os componentes.

A seleção de um dos nós do componente mostra uma visão geral das métricas para esse nó.

Visão geral de segmentos

A Visão geral de segmentos mostra todos os segmentos ativos que estão sendo processados por um agente.

Visão geral de XML

A guia Visão geral para o nó XML exibe métricas dos componentes do XML.

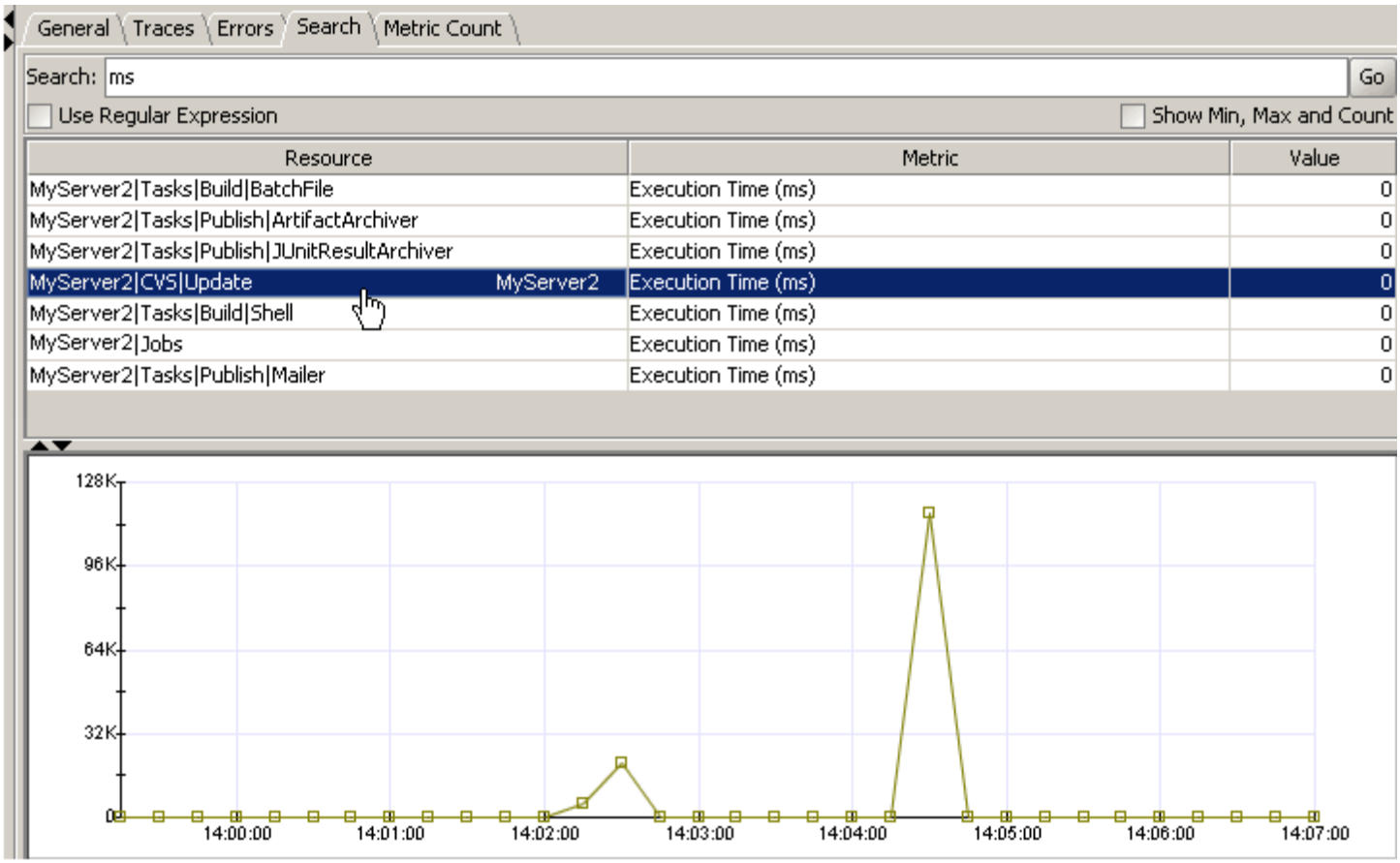
Outras guias

Além das guias Visão geral, existem as guias Pesquisar, Rastreamentos, Erros e Contagem de métricas.

Guia Pesquisar

A guia Pesquisar é disponibilizada quando você seleciona um nó na árvore centrada no agente que contém as métricas. Ela permite localizar rapidamente as métricas.

A ilustração abaixo mostra como a guia Pesquisar aparece no painel do visualizador.



Pontos a serem observados:

- O nó selecionado na árvore centrada no agente define o escopo de uma pesquisa. Por exemplo, se você selecionar Frontends na árvore, a pesquisa buscará apenas os recursos sob esse nó.
- É possível inserir uma sequência de caracteres ou uma expressão regular no campo Pesquisar.
- Se você inserir uma expressão regular, marque a caixa Usar expressão regular.
  Observação: expressões regulares não podem ser filtradas por agente, de modo que não é possível pesquisar por nome de agente, nome do host nem nome do processo.

O painel direito lista os recursos com as métricas que correspondem ao argumento da pesquisa, e o valor de cada um. Para exibir as colunas Mín., Máx. e Contagem, clique em Mostrar mínimo, máximo e contagem.

Se você clicar em uma métrica na lista, uma exibição aparecerá na parte inferior do painel direito.

Se você clicar em outro nó que contenha métricas, o argumento de pesquisa usado na pesquisa anterior permanecerá ativo e será aplicado ao nó selecionado recentemente.

Para obter informações sobre como usar a Pesquisa, consulte Usando a pesquisa.

Guia Rastreamentos

A guia Rastreamentos, disponível quando um recurso ou componente é selecionado na árvore centrada no agente, é semelhante ao Rastreador de transações (consulte Usando o Rastreador de transações). A guia Rastreamentos lista os eventos registrados do Rastreamento de transação para o recurso ou componente selecionado.

Observação: o intervalo de datas para rastreamentos no modo dinâmico é de 20 minutos. Os rastreamentos com mais de 20 minutos não são exibidos no modo dinâmico; eles vencerão (não serão mostrados) quando passarem de 20 minutos.

Definindo a unidade de duração

Por padrão, a guia Rastreamentos mostra a duração das transações e os componentes da transação em milissegundos (ms), milésimos de segundo.

Você pode alterar essa unidade para:

- segundos
- milissegundos (ms)

Para alterar a unidade da coluna Duração na guia Rastreamentos:

1. Clique com o botão direito no cabeçalho da coluna Duração (ms).
2. No menu suspenso, selecione uma das opções:
   - segundos
   - milissegundos (padrão)
   - microssegundos

A guia Rastreamentos exibe a nova unidade no cabeçalho da coluna e processa a duração usando a nova unidade em todas as exibições da transação (incluindo no Visualizador do rastreamento de transação – consulte Usando o Visualizador do rastreamento de transação).

Guia Erros

A guia Erros, disponível quando um recurso ou componente é selecionado na árvore centrada no agente, lista erros e detalhes do erro para o item selecionado. A guia Erros permite que a equipe de suporte detecte e diagnostique a causa dos erros graves à medida que eles ocorrem, determine a frequência e a natureza dos erros, o que pode impedir que os usuários finais concluam transações na web, e forneça informações específicas sobre a causa raiz aos desenvolvedores. **Observação:** a opção ErrorDetector deve estar ativada para que você veja a guia Erros. Para obter informações sobre como ativar o ErrorDetector, consulte ErrorDetector.

A metade superior da guia Erros lista a hora, a descrição e o tipo de cada erro. A metade inferior da guia mostra informações detalhadas para cada componente envolvido no erro selecionado na lista acima.

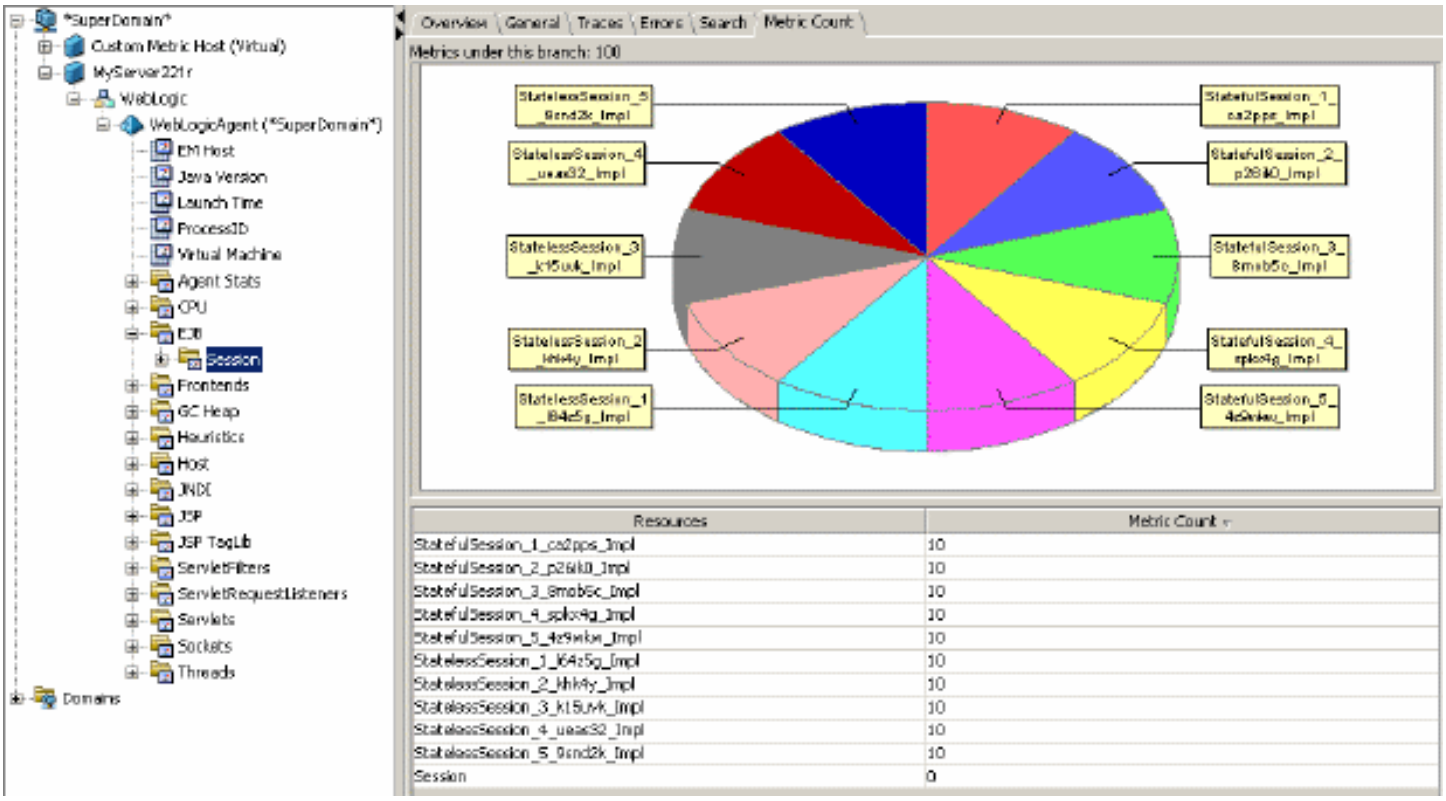
Guia Contagem de métricas

Muitos dos nós na árvore centrada no agente têm uma guia Contagem de métricas, que exibe um gráfico de pizza com a distribuição das métricas do nó.

A ilustração abaixo mostra o gráfico de pizza, com uma exibição de tabela dos mesmos dados abaixo dela.

O gráfico de pizza exibe no máximo 50 fatias. Quando há mais de 50 recursos no nó selecionado:

- O gráfico exibe os recursos relatando os 50 valores mais altos.
- Além das fatias que representam os 50 valores mais altos, uma fatia adicional será rotulada "Todas as outras métricas" para mostrar a proporção de métricas com dados fora dos 50 principais relatados.
- A barra de status mostra a mensagem "Exibindo os 50 principais recursos. Os demais recursos estão agrupados em "Todas as outras métricas"."



Passar o mouse sobre uma área do gráfico de pizza exibe uma dica de ferramenta com a contagem e a porcentagem.

Rótulos longos serão truncados, mas quando você selecionar uma fatia do gráfico, o nome totalmente qualificado do recurso será exibido na tabela abaixo do gráfico.

A guia Contagem de métricas exibe todas as contagens de métricas para o período do intervalo de tempo selecionado, incluindo as métricas dos agentes desconectados no mesmo período.

Há um intervalo de 30 minutos para que as métricas dos agentes desconectados ainda apareçam na contagem de métricas. Se o intervalo de tempo selecionado for inferior a 30 minutos, as métricas dos agentes desconectados desaparecerão após 30 minutos. Se o intervalo de tempo selecionado for maior, as métricas desconectadas estarão presentes para o intervalo de tempo integral.

Exibição da guia Recursos

A guia Recursos mostra gráficos das métricas Resource. A guia Recursos pode ser vista na árvore Navegador de métricas quando o agente é selecionado.

Observação:

- Embora os gráficos para todas as métricas Resource apareçam na exibição da guia Recursos, os gráficos não exibirão dados quando as classes da métrica estiverem indisponíveis para o agente.
- A fonte original da métrica que aparece nos gráficos Segmentos em uso e Conexões do JDBC em uso variará conforme o agente, dependendo do tipo de agente (WebLogic, Tomcat, .NET, ou outros) e do seu mapeamento, especificados no arquivo ResourceMetricMap.properties.

Na árvore Navegador de métricas, eles aparecem sob o nó do agente, da seguinte maneira:

Figure 14: Nome do agente

Guia Despejos de segmento

Cada nó do agente na árvore Navegador de métricas tem uma guia Despejos de segmento. Essa guia permite coletar despejos de segmento Java (despejos de segmento) e exibir dados de despejo de segmento atuais e históricos.
Um despejo de segmento fornece informações sobre todos os segmentos em execução dentro de uma JVM em determinado momento. Para cada segmento, um despejo de segmento fornece o nome e a ID do segmento, estado e um rastreamento de pilha, que lista todos os métodos chamados.

A guia Despejos de segmento inclui estas partes:

- O cabeçalho exibe a hora do despejo de segmento.
- A barra de resumo do despejo de segmento exibe o número total de segmentos e o número de segmentos que estão aguardando, bloqueados e em execução.
- O painel de pesquisa permite procurar uma sequência de caracteres específica em todas as informações de despejo de segmento. Os resultados são exibidos na tabela de informações do segmento.
- A lista suspensa de estado dos segmentos filtra a tabela de informações do segmento pelo estado do segmento. Quando você seleciona um estado, a tabela de informações do segmento é atualizada.
- A tabela de informações do segmento exibe uma lista de todos os segmentos. Para cada segmento, ela fornece a ID, o nome e o estado do segmento, além do último método chamado pelo segmento logo pouco antes do despejo de segmento.
- A tabela de rastreamento de pilha de segmentos exibe todos os métodos na ordem chamada.
- O gráfico de pizza % de segmentos por estado exibe os segmentos nestes estados: bloqueado(a), bloqueado, em execução ou aguardando.
  - Passar o mouse sobre uma área exibe uma dica de ferramenta com o número e a porcentagem de segmentos em cada estado.

A guia Despejos de segmento pode ser exibida na árvore Navegador de métricas quando você selecionou um nó de agente.

Observação: se você estiver fazendo a triagem dos problemas de agente, exiba a métrica <Nome do agente>|Segmentos|Contagem de bloqueios na árvore Navegador de métricas. Essa métrica indica se há segmentos bloqueados afetando o agente. A configuração do Introscope é necessária para ativar a métrica Deadlock Count. Para obter mais informações, consulte o Agente do Java

Você pode clicar no:

- Botão Coletar novo para coletar um despejo de segmento.
- Botão Salvar como texto para salvar o despejo de segmento atual em um arquivo de texto.
- Botão Carregar anterior para carregar um único despejo de segmento coletado anteriormente e para ver a marca de data e hora e os dados associados.

Nenhum dado de despejo de segmento é exibido até que um despejo de segmento seja coletado ou depois que um Gerenciador corporativo é reiniciado.

A guia Despejos de segmento está disponível no modo dinâmico; nenhum dado de despejo de segmento histórico é exibido no modo histórico.

Usar dicas de ferramenta para exibir valores e nomes de métrica em um visualizador de dados

Em um Visualizador de dados, você pode passar o cursor sobre um ponto em um gráfico para abrir uma dica de ferramenta.

Para abrir uma dica de ferramenta:

- Passe o mouse sobre qualquer elemento na árvore de métricas da estação de trabalho ou em um Visualizador de dados, como um ponto em um gráfico.

Um ponto de dados específico no gráfico mostra:

- Nome da métrica
- Valor exato da métrica
- Valores mínimo/máximo para a métrica durante o período representado pelo ponto de dados. Em vez de arredondar para um valor usando K para milhar ou M para milhão, as dicas de ferramenta mostram valores exatos.
  Isso é discutido no tópico abaixo, Como o intervalo de datas afeta pontos de dados.
- A contagem de intervalos de 15 segundos, representada pelo ponto de dados.
- A data e hora para o ponto de dados no gráfico.

Pressionar F2 enquanto uma dica de ferramenta está ativa permite que você clique no texto de um hiperlink. Ao fazer isso, uma janela do Investigador é aberta com a árvore expandida para a métrica mostrada na dica de ferramenta.

Como o intervalo de datas afeta pontos de dados

Cada ponto de dados em um gráfico representa uma divisão igual do tempo coberto pelo gráfico. Se o intervalo de datas for definido como Dinâmico (como na ilustração acima), cada ponto de dados representará um intervalo de 15 segundos.

Se o intervalo de datas for definido para outro valor, o intervalo representado por cada ponto de dados será diferente. Se o intervalo de datas for definido para duas horas, por exemplo:

- Cada ponto de dados representa um intervalo de dois minutos ou oito intervalos de 15 segundos.
- Como existem oito intervalos de 15 segundos em dois minutos, a contagem de cada ponto de dados é 8.

A guia Navegador de métricas lista métricas e outras informações em formato de árvore. Os nós de alto nível imediatamente abaixo dos nós de domínio representam os agentes instalados nos hosts do servidor de aplicativos individuais ou equivalente.

Para obter mais informações sobre as métricas, consulte Guia Navegador de métricas.

Usar o Rastreador de transações

Os usuários da estação de trabalho com permissões apropriadas usam o rastreador de transações para rastrear a atividade de transações dentro de um aplicativo de produção. As transações são rastreadas conforme elas fluem por uma Máquina virtual Java ou um CLR (Common Language Runtime) em um ambiente do .NET.

O rastreador de transações permite a captura de transações que atendem a determinados critérios. O rastreador de transações examina as chamadas que são feitas em todo o sistema para essa transação. A interface gráfica do usuário permite fazer a triagem dos problemas de desempenho e das falhas de aplicativo com facilidade.

As duas maneiras de coletar os rastreamentos de transação são estes métodos:

- Usar o rastreador de transações.

Para executar uma sessão de rastreamento de transação, especifique os agentes cujas transações você deseja rastrear e o período da captura de dados. Você pode especificar opções de filtro para limitar o rastreamento às transações. É possível filtrar por transações que excedem o tempo de execução do limite, correspondem aos valores de parâmetro ou que contenham erros.
Depois que a sessão de rastreamento de transação é iniciada, as transações que correspondem aos critérios de filtro aparecem na tabela de transações. Os eventos de transação incluem erros e rastreamentos de transação.

- O agente coleta automaticamente um os rastreamentos de transação.

Quando a instrumentação inteligente está ativada, o agente coleta automaticamente um rastreamento de transação em várias situações.

O rastreador de transações pode rastrear transações síncronas que ultrapassem os limites em ambientes de servidor de aplicativos homogêneos que oferecem suporte a este recurso:

- WebLogic Server 8.0 e posterior
- WebSphere 6.x

Em outros ambientes, as transações podem ser rastreadas dentro dos limites de uma única VM (Virtual Machine - Máquina Virtual) ou um CLR.

Você pode exibir os resultados de uma consulta de rastreamento de transação entre processos na guia Exibição de rastreamento do Visualizador do rastreamento de transação.

O DX APM salva os dados da sessão de rastreamento de transação no banco de dados Eventos de transação por um período especificado. Os dados expiram periodicamente para reduzir a sobrecarga.

Você pode configurar o agente para capturar os dados do rastreamento de transação com base nos valores das variáveis do servlet ou do ASP.NET. As variáveis incluem cabeçalhos de solicitação HTTP, parâmetros de solicitação, atributos de sessão, ID da sessão, nome de usuário, URLs e sequências de caracteres da Consulta de URL. Além disso, por padrão, os agentes fazem amostras das transações.

> **NOTE**
> O estado Encerrar da métrica não afeta os dados do rastreamento de transação. Quando um agente gerenciado é encerrado, ele não relata dados de rastreamento de transação. Um agente pode ser encerrado durante uma sessão de rastreamento de transação. Nessa situação, o agente relata os dados que foram coletados antes da solicitação de encerramento.

Amostragem do rastreamento de transação

Por padrão, os agentes fazem amostras do comportamento da transação rastreando cada URL exclusivo normalizado em um aplicativo a cada hora. Você pode exibir e analisar rastreamentos testados de um intervalo de datas histórico selecionado:

- Na estação de trabalho
- Na guia **Rastreamentos** do Navegador de métricas

Também é possível configurar amostragem de rastreamento de transação mesmo se nenhum grupo de URLs estiver configurado. Especifique o número de transações a serem amostradas durante um intervalo de datas. O valor padrão é uma transação a cada 2 minutos.

A amostragem do rastreamento de transação é ativada por padrão. Você pode desativar o comportamento, alterar o período de amostragem ou cancelar a aleatoriedade do tempo de amostragem, conforme apropriado.

NOTE

Mais informações: Configurar opções do rastreamento de transação (agente do Java) ou Opções do Rastreador de transações (agente do .NET).

Sobrecarga do rastreamento de transação

Uma sessão de rastreamento de transação afeta a sobrecarga desde a hora de início até que todas as transações do processo sejam concluídas no fim da sessão. Você pode especificar o limite de execução no nível de milissegundos, mas, fazendo isso, a carga no sistema aumenta.

Esses recursos do Rastreador de transações reduzem a probabilidade de que as sessões de rastreamento imponham sobrecarga inaceitável:

- **Tempo limite da sessão de rastreamento de transação -** uma sessão de rastreamento de transação expira após um período definido pelo usuário para que o usuário administrador não possa deixar acidentalmente o Rastreador de transações ativado e afete negativamente o desempenho de um período prolongado. No final do tempo limite, o agente interrompe o rastreamento de novas transações e conclui o rastreamento das transações em andamento.
- **Lógica anti-inundação –** para impedir a sobrecarga excessiva, a lógica anti-inundação do agente limita o número de transações que são rastreadas no intervalo de 15 segundos para 200. Depois que esse limite é excedido, o agente registra no log que o limite anti-inundação foi excedido. O agente não relata dados de rastreamento de transação para o Gerenciador corporativo até que o período de 15 segundos expire. Depois que o período de 15 segundos expirar, a lógica anti-inundação resume o relatório.

Rastreamentos de transação coletados automaticamente

Quando a instrumentação inteligente está ativada, o agente coleta automaticamente um rastreamento de transação quando:

- Ocorre um erro
- A Análise diferencial detecta instabilidade no aplicativo e o limite do rastreamento automático por intervalo não é excedido.
  Observação: o rastreamento automático de transação com base na análise diferencial precisa do agente 10.0, no mínimo.
- O rastreador `ComponentTimeAutoTraceTriggerTracer` está implantado e o tempo de resposta do componente é excedido
- Uma API dispara rastreamentos de transação automáticos com base em critérios personalizados. Para obter mais informações, entre em contato com o DX APM Implementation Services.

Altamente otimizados, os rastreadores de baixa sobrecarga coletam rastreamentos de transação automáticos. Os rastreamentos automáticos geram muito menos sobrecarga no desempenho do que a execução e a amostragem manuais, entre outros rastreamentos de transação. Esses outros tipos de rastreamentos de transação usam a filtragem do agente, que adiciona sobrecarga. Os rastreamentos de transação automáticos não exibem todas as propriedades detalhadas do componente que os outros tipos de rastreamento de transação exibem.

Os rastreamentos automáticos de transação apresentam estas características:

- Todos os componentes instrumentados pelo PBD têm uma métrica associada na árvore do navegador de métricas. Os componentes de ampla visibilidade não têm uma métrica associada.
- Os componentes de visibilidade profunda contêm somente nome da classe, nome do método e duração. Para front-ends e back-ends (por exemplo, servlets, serviços web, chamadas SQL), o nome é formatado com base na configuração do PBD.
- As seguintes propriedades são exibidas nos detalhes do componente:

  - O **Tipo de rastreamento** é **Normal**.
  - Se um erro disparou o rastreamento de transação, o componente que gerou a exceção incluirá as propriedades do componente.
  - O primeiro componente do rastreamento de transação exibe a propriedade `Auto Trace Trigger`.
- Suporte ao rastreamento de transação entre processos.

  NOTE

  Mais informações:

  - A seção Configurar a instrumentação inteligente aborda a configuração de transações entre processos nos rastreamentos de transação automáticos.

Se os rastreamentos automáticos de transação não forem exibidos, pode ser por um destes motivos:

- A instrumentação inteligente não está ativada.

  NOTE
  A instrumentação inteligente está disponível somente para agentes do Java, não para agentes do .NET.
- Um agente do modo herdado está monitorando a JVM.O modo herdado não oferece suporte aos recursos da instrumentação inteligente.
- O número de rastreamentos de transação automáticos por valor limite do intervalo (`agent.deep.automatic.trace.clamp` propriedade) foi excedido. Exiba a métrica de suportabilidade `Deep Tracing|Auto Tracing: Clamped: Clamped Traces`

  NOTE

  Mais informações:

  - Configurar a instrumentação inteligente
  - Propriedades da instrumentação inteligente

Quando você executar manualmente um rastreamento de transação e algum filtro manual corresponder a um rastreamento automático, o agente coletará somente o rastreamento manual.

Rastreamentos automáticos de transação quando o tempo de resposta do componente é excedido

Você pode implantar um PBD para disparar um rastreamento de transação automaticamente quando o tempo de resposta do componente for excedido. Crie uma entrada PBD com um rastreador para coletar esse rastreamento automático. Por exemplo, para coletar um rastreamento quando o tempo de resposta de um servlet específico exceder 10 segundos. Use a opção do rastreador `ComponentTimeAutoTraceTriggerTracer` para configurar este recurso.

NOTE

Mais informações: Configurar opções do rastreamento de transação

Quando `ComponentTimeAutoTraceTriggerTracer` dispara um rastreamento de transação, o primeiro componente no rastreamento inclui a propriedades dos detalhes do componente `Auto Trace Trigger Criteria`. A propriedade exibe **O valor do limite de <*nome do componente*> para o tempo de resposta excedeu <*valor*>**.

Componentes de ampla visibilidade

Quando a instrumentação inteligente está ativada, os agentes detectam e coletam automaticamente informações detalhadas sobre componentes de transação para o nível de método.Os agentes detectam e instrumentam automaticamente os componentes de ampla visibilidade sem o uso de PBDs (ProbeBuilder Directives - Diretivas do ProbeBuilder).O agente analisa métodos para a sua complexidade a fim de determinar as chamadas e os componentes a serem instrumentados e exibidos como componentes de visibilidade profunda.

NOTE
A instrumentação inteligente está disponível somente para agentes do Java, não para agentes do .NET.

Fatos sobre os componentes de ampla visibilidade que você deve conhecer:

- Os componentes de ampla visibilidade não incluem links para métricas. Nenhum dado de métrica é exibido na árvore do navegador de métricas.
- Contêm apenas o nome da classe, o nome do método e a duração.
- As seguintes propriedades de detalhes do componente são exibidas na **Exibição de rastreamento**:
  - A propriedade chamada `Is Unmonitored` indica um componente de visibilidade profunda.
  - Nível de instrumentação: o nível da instrumentação inteligente em que uma transação foi detectada.
  - Nível de pontuação do método: o nível da instrumentação inteligente está relacionado à pontuação que o algoritmo de pontuação do DX APM atribui a um método de componente de visibilidade profunda. O DX APM pode exibir métodos de componente de visibilidade profunda tendo pontuações variadas em um rastreamento de transação, um erro ou uma paralisação. Por exemplo, uma transação detectada usando nível médio pode exibir métodos com níveis de pontuação de método médio e baixo.
    Use as propriedades Nível de instrumentação e Nível de pontuação do método para entender a ampla visibilidade da instrumentação inteligente de um rastreamento de transação. Você também pode compreender a amplitude da visibilidade dos métodos em um rastreamento. Por exemplo, é possível comparar os vários métodos que a instrumentação inteligente detecta em dois níveis diferentes de instrumentação. Você pode observar o nível de instrumentação inteligente em que o DX APM pontua alguns métodos específicos. É possível ajustar a solução de monitoramento para a visibilidade de monitoramento desejada equilibrando a sobrecarga e a visibilidade.
- O ícone de raio que identifica os componentes de visibilidade profunda não é exibido na estação de trabalho.

Dependendo de seus requisitos e do ambiente, é possível configurar a profundidade da instrumentação inteligente. Por exemplo, defina se o agente irá detectar e instrumentar automaticamente uma quantidade baixa, média ou alta de código do aplicativo.

Pontos de entrada

A detecção automática do ponto de entrada permite monitorar e fazer a triagem rapidamente de aplicativos Java sem a configuração manual das diretivas do ProbeBuilder.

Quando a instrumentação inteligente e a detecção do ponto de entrada estão ativadas, o agente monitora os segmentos que estão envolvidos nas transações de chamada de soquete do cliente. A instrumentação inteligente e a detecção do ponto de entrada são configuradas como ativadas por padrão. *Os pontos de entrada* são os pontos de início da transação.Um mecanismo de regras no agente identifica candidatos ao ponto de entrada.O agente instrumenta e monitora o candidato ao ponto de entrada mais antigo no segmento de transações. Qualquer ponto de entrada que um agente detecta e persiste é ativado para monitoramento por todos os agentes que compartilham o diretório de instalação. No entanto, o relatório de métricas do ponto de entrada exige as mesmas classes de estrutura ou código para existir em outras JVMs do servidor de aplicativos.

Veja a seguir alguns exemplos de transações nas quais a detecção do ponto de entrada fornece visibilidade automaticamente:

- Pilhas e estruturas tecnológicas que a instrumentação do DX APM ainda não monitora
- Chamadas à API personalizadas ou patenteadas
- Segmentos em segundo plano que consomem recursos críticos e podem afetar o desempenho geral do aplicativo

NOTE

A detecção do ponto de entrada não oferece suporte ao UDP (User Datagram Protocol - Protocolo de Datagrama de Usuário).

O agente salva os pontos de entrada no arquivo `AutoPersist.pbd` , que é mantido no diretório <*pasta_principal_do_agente*>\core\config\hotdeploy.

WARNING
O usuário do sistema que executar o servidor de aplicativos precisará ter acesso de leitura/gravação ao diretório /hotdeploy.Essas permissões permitem que o agente grave dados no arquivo AutoPersist.pbd.

Pontos de entrada são diferentes de front-ends. O agente do Java detecta automaticamente pontos de entrada que estão perto do início de um caminho de chamada de transação. Os front-ends são definidos manualmente nos PBDs e podem estar em qualquer lugar do caminho de chamada de transação.

WARNING
Não faça alterações manuais em AutoPersist.pbd. No entanto, você pode copiar pontos de entrada detectados e usá-los em outro PBD.

As métricas dos pontos de entrada são exibidos na árvore centrada no agente, no subnó **Automatic Entry Points** sob o nó do agente.

NOTE
Certifique-se de que a propriedade `introscope.autoprobe.dynamicinstrument.enabled` no arquivo `IntroscopeAgent.profile` esteja definida como `true` . Essa configuração permite que o agente relate métricas de ponto de entrada sem exigir a reinicialização do aplicativo.

O agente relata as cinco métricas BlamePoint padrão para cada ponto de entrada.Os pontos de entrada são exibidos nos rastreamentos de transação. Os nomes do ponto de entrada são formatados como `ponto de entrada <nome da classe _ nome do método>` .O agente relata métricas de suportabilidade do ponto de entrada.

Você pode configurar a coleta de pontos de entrada. Por exemplo, uma propriedade de configuração limita o número de pontos de entrada que AutoPersist.pbd pode persistir.

NOTE

Mais informações: Criar PBDs para converter pontos de entrada em front-ends

Back-ends automáticos

Quando a detecção de *back-end automático* está ativada, o agente detecta e monitora automaticamente os back-ends de aplicativo sem configuração manual.

Um mecanismo de detecção no agente identifica candidatos ao back-end automático. Qualquer back-end automático que um agente detecta e persiste é ativado para monitoramento por todos os agentes que compartilham o diretório de instalação.

Veja a seguir alguns exemplos de tipos de back-end que a detecção de back-end automático pode encontrar e monitorar:

- Pilhas e estruturas tecnológicas de back-end que o agente ainda não monitora. Entre os exemplos estão os back-ends NoSQL, como MongoDB e Cassandra.
- Back-ends personalizados ou patenteados

O agente salva os back-ends automáticos no arquivo `AutoPersist.pbd` , que é mantido no diretório `<pasta_principal_do_agente>\core\config\hotdeploy` .

WARNING

- O usuário do sistema que executar o servidor de aplicativos precisará ter acesso de leitura/gravação ao diretório `/hotdeploy` . Essas permissões permitem que o agente grave dados no arquivo `AutoPersist.pbd` .
- Não faça alterações manuais em `AutoPersist.pbd` . No entanto, você pode copiar back-ends automáticos detectados e usá-los em outro PBD.

Você pode configurar a detecção automática de back-end. Por exemplo, uma propriedade de configuração limita o número de back-ends automáticos que AutoPersist.pbd pode persistir.

Na **Exibição de rastreamento**, os parâmetros `porta remota` e `nome do servidor remoto` são exibidos nos **Detalhes do componente**.

Iniciar, interromper e reiniciar um rastreamento de transação

Índice

Para executar uma sessão de rastreamento de transação, especifique os agentes cujas transações deseja rastrear e por quanto tempo capturar os dados. Você pode especificar opções de filtro para limitar o rastreamento às transações que:

- excederem o limite de tempo de execução definido
- corresponderem a valores de parâmetro como ID de usuário, informações de cabeçalhos de solicitação, etc.
- tiverem erros, se o ErrorDetector estiver ativado

Quando a sessão de rastreamento de transação é iniciado, o Introscope captura os dados de rastreamento especificados no perfil do agente para cada transação. As transações que correspondem aos critérios do filtro são exibidas na janela do Visualizador do rastreamento de transação e são salvos no banco de dados Eventos de transação.

Iniciando uma sessão de rastreamento de transação

Para iniciar uma sessão de rastreamento de transação:

1. Selecione Estação de trabalho > Nova sessão de rastreamento de transação.
   A janela Nova sessão de rastreamento de transação é aberta.
2. Na seção Rastrear transações da janela, especifique a duração mínima das transações a serem rastreadas.
   Selecione milissegundos ou segundos na lista suspensa.
   Observação: durações em subsegundos podem ter um impacto negativo no desempenho.
3. Para especificar um filtro de transações, marque a caixa de seleção à esquerda do menu suspenso esmaecido onde se lê ID de usuário, na seção *Rastrear transações* e selecione um tipo na lista:
   - ID de usuário -- insira um operador e um valor de parâmetro.
   - ID da sessão - insira um operador e um valor de parâmetro.
   - URL ou Consulta de URL -- insira um operador e um valor de parâmetro.
   - Cabeçalho da solicitação -- insira um nome de tipo de dado, uma condição e um valor.
   - Parâmetro de solicitação -- insira um nome de tipo de dado, um operador e um valor de parâmetro.
   - Atributo da sessão -- insira um nome de tipo de dado, um operador e um valor de parâmetro.
     Observação: os dados só estarão disponíveis para uso em filtros se o agente estiver configurado para capturá-los.

   As condições do filtro são as seguintes:
   - é igual a -- são rastreadas as transações em que o valor do parâmetro corresponde à sequência de caracteres especificada.
   - não é igual a -- são rastreadas as transações em que o valor do parâmetro não corresponde à sequência de caracteres especificada.
     Observação: também são rastreadas as transações que não incluem o parâmetro ao qual o filtro se aplica.
   - contém -- são rastreadas as transações em que o valor do parâmetro contém a sequência de caracteres especificada.
   - não contém -- são rastreadas as transações em que o valor do parâmetro não contém a sequência de caracteres especificada.

Observação: também são rastreadas as transações que não incluem o parâmetro ao qual o filtro se aplica.
  - começa com -- são rastreadas as transações em que o valor do parâmetro começa com a sequência de caracteres especificada.
  - termina com -- são rastreadas as transações em que o valor do parâmetro termina com a sequência de caracteres especificada.
  - existe -- são rastreadas as transações que incluem o parâmetro ao qual o filtro se aplica, independentemente do valor do parâmetro.
  - não existe -- são rastreadas as transações que não incluem o parâmetro ao qual o filtro se aplica.
4. Especifique a duração da sessão de rastreamento em minutos.
5. Na seção Rastrear agentes, selecione um ou mais agentes para os quais rastrear transações:
  - Para rastrear todos os agentes que suportam o rastreamento de transação, selecione Rastrear todos os agentes suportados. Essa opção rastreia agentes suportados que estão conectados no momento e qualquer um que se conecte durante a sessão de rastreamento.
  - Para rastrear agentes selecionados, selecione Rastrear o(s) agente(s) selecionado(s) e selecione os agentes na lista (CTRL + clique para selecionar vários agentes).
6. Selecione OK para iniciar a sessão Rastreamento de transação.
   Os resultados do rastreamento de transação são exibidos no Visualizador do rastreamento de transação.
   No modo Dinâmico, são exibidos os eventos de rastreamento de transação dos últimos 20 minutos. Os eventos de rastreamento de transação com mais de 20 minutos não são exibidos no modo dinâmico. São exibidos até 500 eventos de rastreamento de transação.

Interrompendo uma sessão de rastreamento de transação

Para interromper uma sessão de rastreamento de transação:

- Clique em Interromper ou
- Selecione Rastreamento > Interromper a sessão de rastreamento.

Reiniciando uma sessão de rastreamento de transação

Reiniciar a sessão Rastreamento de transação redefine o tempo limite para o período definido pelo usuário e prossegue com o rastreamento de transações nos agentes de destino que usam os mesmos critérios de limite.

É possível reiniciar uma sessão de rastreamento de transação:

- depois que uma sessão tiver expirado.
- para reiniciar uma sessão interrompida.
- para reiniciar uma sessão em andamento.

Para reiniciar uma sessão de rastreamento de transação:

- Clique em Reiniciar ou
- Selecione Rastreamento > Reiniciar a sessão de rastreamento.

Usando o Visualizador do rastreamento de transação

O Visualizador do rastreamento de transação mostra informações de rastreamento para transações que atendem aos critérios especificados para a sessão de rastreamento.

A tabela no painel superior do Visualizador do rastreamento de transação lista transações que foram rastreadas durante a sessão. Você pode classificar as linhas pela coluna clicando no cabeçalho da coluna. Novas transações são inseridas na tabela na ordem classificada.

Esta tabela lista as colunas na tabela de transações:

Campo	Descrição
Type	O tipo de informação na linha de rastreamento: Rastreamento de transação (T) Erro (E) Amostra (R) Uma transação que a amostragem aleatória escolhe. Paralisada (S) Uma transação paralisada Os dados do erro aparecerão somente se ErrorDetector estiver ativado. Asterisco Se um asterisco for exibido após o símbolo de tipo, alguns dos componentes da transação foram truncados ou limitados. Somente as transações dos tipos T e E podem ser limitadas. Os tipos listados aqui se aplicam às transações disponíveis no modo Dinâmico. Ao consultar transações históricas, outros tipos de transação são disponibilizados.
Domínio	Domínio para o qual o agente rastreado é mapeado.
Host	Host em que o agente rastreado está em execução.
Processo	Nome do processo do agente
Agent	Nome do agente
Marca de data e hora	Hora de início, no relógio do sistema do computador do agente, da invocação do componente raiz.
Duração	Tempo de execução do relógio de parede do componente raiz
Descrição	O URL que foi invocado para iniciar essa transação ou o caminho do Introscope para o componente que iniciou a transação.
ID de usuário	A ID do usuário conectado que está executando a transação (se estiver configurada e disponível).

A janela Rastreador de transações inclui três guias:

- Exibição do resumo
- Exibição de rastreamento
- Exibição em árvore

Exibição do resumo

Na primeira vez que você seleciona uma transação na tabela de transações, a Exibição do resumo é aberta. Quando você seleciona uma transação que já foi aberta antes, ela é aberta na exibição selecionada mais recentemente.

Estas informações são exibidas para a transação selecionada no momento em cada guia:

- O nome totalmente qualificado do agente
- Hora de início, no relógio do sistema do computador do agente, da invocação do componente raiz.
- Tempo de execução do componente raiz em milissegundos

A Exibição do resumo mostra as métricas para os componentes da transação selecionada. As métricas incluem o caminho, o número de chamadas, a duração da chamada em milissegundos, bem como os tempos mínimo, médio e máximo das chamadas. Clique duas vezes em uma das métricas listadas na exibição de tabela para abri-la na Árvore de navegação.

Na parte inferior da janela Rastreamento, a barra de status de Rastreamento de transação mostra:

- Número de transações que foram coletadas na sessão.
- Critérios de filtro para a sessão de Rastreamento de transação.
- Tempo restante antes que a sessão atual atinja o tempo limite.

> **NOTE**
>
> Para componentes de transação correlacionados, as guias Exibição do resumo e Exibição em árvore exibem somente o escopo da primeira JVM. A guia Exibição de rastreamento mostra todo o escopo dos componentes de transação relacionados. Esteja ciente dessa limitação ao alternar da Exibição de rastreamento para outras exibições de guia.

Exibição de rastreamento

A Exibição de rastreamento mostra uma transação selecionada em uma exibição de pilha gráfica dos componentes que compõem a transação. Quando você seleciona um dos componentes, é possível ver detalhes do componente no painel inferior do visualizador.

A Exibição de rastreamento mostra:

- Cada componente da transação como uma barra
- A porcentagem do tempo total de execução da transação para cada componente
- Relações de chamada entre componentes
  As barras dos componentes são exibidas de cima para baixo na ordem de chamada.
- Sequência de transações ao longo do tempo
  A colocação dos componentes da esquerda para a direita indica a sequência. O tempo relativo do relógio de parede em milissegundos é exibido no topo do instantâneo da transação.
- Componentes de ampla visibilidade, que o Introscope detecta e instrumenta automaticamente usando a instrumentação inteligente sem o uso de PBDs.

  > **NOTE**
  >
  > A instrumentação inteligente está disponível somente para agentes do Java, não para agentes do .NET.
- Erros dentro das transações (Detectar e analisar erros e paralisações). Se o ErrorDetector estiver ativado.
  As fatias vermelhas no Instantâneo da transação representam erros nas transações.

  > **NOTE**
  >
  > O intervalo de datas padrão para rastreamentos no modo dinâmico é de 20 minutos. Os rastreamentos com mais de 20 minutos não são exibidos no modo dinâmico. Os rastreamentos vencem (não serão mostrados) quando passam de 20 minutos.

Na Exibição de rastreamento, é possível executar estas ações:

- Passar o ponteiro do mouse sobre um componente para abrir uma dica de ferramenta.
- Clicar com o botão direito do mouse em um componente para abrir a Árvore de métricas e exibir as métricas do componente.
- Selecione um componente na Exibição de rastreamento para abrir o painel Transaction Component Details.

Detalhes do componente da transação

Os detalhes do componente da Exibição do rastreamento mostram estas informações:

- **Tipo**: componente de alto nível (por exemplo, EJB, Servlet, JSP no Java e ASPX no .NET)
- **Nome**: o nome do componente.
- **Caminho**: o nome completo do recurso do componente.
- **Duração**: o tempo de execução do componente selecionado. A unidade padrão é milissegundos.
- **Marca de data e hora (relativa)**: a hora de início, no relógio do sistema do computador host do agente, da invocação do componente selecionado.
- **% do tempo total da transação**: percentual do tempo total da transação que o componente selecionado leva.
- **Propriedades**: todas as propriedades opcionais relatadas pelo componente (por exemplo, URL, Consulta de URL, SQL Dinâmico) ou definidas para coleta no perfil do agente (ID de usuário, Cabeçalho da solicitação, `RequestParameter` ou Atributo da sessão). É possível selecionar o texto de qualquer campo nos detalhes da propriedade e copiá-lo usando CTRL+C.

Propriedade	Descrição
ID de usuário (Servlet, JSP, ASPX)	ID do usuário que está invocando a solicitação do servlet HTTP.
URL (Servlet, JSP, ASPX)	URL passado ao servlet ou JSP, não incluindo a sequência de caracteres de consulta (texto após o delimitador '?' no URL)
Consulta de URL (Servlet, JSP, ASPX)	Parte do URL que especifica os parâmetros de consulta na solicitação HTTP (texto após delimitador '?' no URL)
ID da sessão (Servlet, JSP, ASPX)	A ID da sessão HTTP associada à solicitação do servlet, se houver.
SQL dinâmico (instruções dinâmicas do JDBC ou ADO.NET, quando o Agente para SQL está instalado).	Instrução SQL dinâmica generalizada, uma vez que ela será vista no formulário agregado do Agente para SQL.
SQL resgatável (instruções resgatáveis do JDBC ou ADO.NET, quando o Agente para SQL está instalado).	SQL resgatável (com o '?' ainda presente).
SQL preparado (instruções preparadas do JDBC ou ADO.NET, quando o Agente para SQL está instalado).	SQL preparado (com o '?' ainda presente).
Método (rastreadores com diagnóstico; com exceção de instruções de servlets, JSPs e JDBC para Java, ASPX e ADO.NET para .NET)	Nome do método rastreado
Não é monitorado	A instrumentação inteligente detecta o nome do componente rastreado. Nenhuma métrica é coletada para esse componente.
Rastreamento truncado	O rastreamento de transação é truncado no último método do rastreamento. Geralmente, o truncamento se deve às chamadas recursivas profundas.

Critérios do disparador de rastreamento automático	O disparador do Introscope para coletar um rastreamento de transação automático. Por exemplo, um erro ou um tempo de resposta de componente excedido quando o rastreador `ComponentTimeAutoTraceTriggerTracer` é implantado. Quando `ComponentTimeAutoTraceTriggerTracer` é o disparador, a propriedade `Auto Trace Trigger Criteria` exibe a mensagem `Response time of <nome do componente> exceeds threshold <valor>`. `Auto Trace Trigger Criteria` exibe os seguintes disparadores quando os agentes coletam transações entre processos nos rastreamentos de transação automáticos: • Quando um agente de upstream dispara uma transação entre processos, `Auto Trace Trigger Criteria` exibe o disparador do Introscope. Por exemplo, `error` ou Response time of <*nome do componente*> exceeds threshold <*valor*>. • Quando um agente downstream dispara uma transação entre processos, a propriedade `Auto Trace Trigger Criteria` exibe o `Cross Process Trigger`.
Nível da instrumentação	O nível da instrumentação inteligente em que uma transação é detectada.
Pontuação do nível de método	O nível da instrumentação inteligente que se correlaciona à pontuação que o algoritmo de pontuação do Introscope atribui a um método de componente de ampla visibilidade. O Introscope pode exibir métodos de componente de ampla visibilidade tendo pontuações variadas em um rastreamento de transação, um erro ou uma paralisação. Por exemplo, uma transação detectada usando nível médio pode exibir métodos com pontuações de nível de método médio e baixo.

Dicas de ferramenta no Visualizador do rastreamento de transação

Você pode passar o seu cursor sobre qualquer um dos componentes individuais, ou camadas, da representação gráfica de uma transação. Uma dica de ferramenta exibe detalhes sobre o componente.

A dica de ferramenta exibe estas informações:

- Caminho
- Duração
- Marca de data e hora (relativo)
- % do tempo total da transação

Exibição em sequência

A guia Exibição em sequência mostra os componentes de transação na ordem em que um processo chama os componentes.

IDs de correlação em transações entre processos

O Introscope Workstation usa um identificador exclusivo, a ID de correlação, para vincular as transações de front-end e back-end rastreadas. A ordem na qual front-ends chamam back-ends em uma transação determina o sequenciação dessa ID.

Você pode usar essa ID de correlação para reconhecer e rastrear o caminho de componentes vinculados em um rastreamento de transação. Essas informações podem fornecer insights sobre quais chamadas podem ser a origem de uma transação lenta ou paralisada.

NOTE

Mais informações: Usar o rastreamento de transação entre processos para resolver problemas

Transações limitadas

Uma propriedade de limite impede que resultados de rastreamento de transação incomuns consumam muitos ciclos. O limite nos componentes de rastreamento de transação é definido em 5000 por padrão. A propriedade `introscope.agent.transactiontrace.componentCountClamp` é especificada no arquivo IntroscopeAgent.profile. Você pode configurar propriedades do agente do Java e do agente do .NET.

Os componentes de rastreamento de transação que excedem os limites de `introscope.agent.transactiontrace.componentCountClamp` são marcados com um asterisco.

Pontos a serem observados:

- A primeira linha de rastreamentos é selecionada.
- O símbolo de Tipo é marcado com um asterisco. O asterisco significa que alguns componentes da transação foram truncados ou limitados.
- Uma dica de ferramenta indica quantos componentes foram truncados. No exemplo acima, 15 dos componentes no rastreamento selecionado excederam o número especificado da propriedade `introscope.agent.transactiontrace.componentCountClamp` .
- Os componentes que não foram truncados aparecem na guia Exibição do resumo na parte inferior do visualizador.
- Cada agente tem um valor heurístico `IsClamped` com 0 = não limitado e 1 = limitado.

Aparência do arquivo XML exportado quando as transações são limitadas

Quando um componente de rastreamento é limitado, o arquivo XML exportado é bem formado e inclui um parâmetro como:

```
<Parameter Value="15" Name="Components Not Shown"/>
```

Para ver uma dica de ferramenta com mais informações sobre um rastreamento:

1. Selecione um dos rastreamentos na tabela.
2. Passe o cursor sobre o rastreamento selecionado.
   A dica de ferramenta exibe o tipo de rastreamento e o número de componentes truncados, ou limitados.

Para classificar os rastreamentos por tipo:

- Clique no cabeçalho da coluna Tipo na tabela.

Procurando transações limitadas

Você pode pesquisar transações limitadas emitindo uma consulta de eventos históricos. Use um exemplo de sequência de caracteres em sua consulta, conforme mostrado neste exemplo:

```
componentsNotShown:[1 TO 9999]
```

Usar uma sequência de caracteres garante que a consulta retorne rastreamentos que tiveram transações limitadas.

NOTE

Como a pesquisa de visualizador de eventos históricos usa a sintaxe Lucene, estas regras de sintaxe se aplicam às consultas de eventos históricos:

- A palavra TO na sequência de caracteres diferencia maiúsculas de minúsculas.
- A sintaxe da pesquisa é lexicográfica, não numérica. Por esse motivo, executar consultas históricas usando `componentNotShown` como um filtro de consulta pode retornar resultados incorretos.
- As sequências de caracteres que começam com `*` (asterisco) ou `?` (ponto de interrogação) não são permitidas.

Exibindo erros com o rastreador de transações

Quando o Detectar e analisar erros e paralisações estiver ativado, você poderá usar o rastreador de transações para identificar e exibir os erros.

Sobre a Exibição em árvore no Rastreador de transações

Exiba os componentes da transação em uma exibição hierárquica de informações. Você pode ir até o componente e identificar problemas de desempenho.

É possível exibir os componentes que são instrumentados usando PBDs e componentes de ampla visibilidade. O Introscope detecta e instrumenta automaticamente os componentes de ampla visibilidade sem usar PBDs.

> **NOTE**
>
> A instrumentação inteligente está disponível somente para agentes do Java, não para agentes do .NET.

Siga estas etapas:

1. No WebView, clique em Ferramentas, Rastreador de transações.
2. Selecione um rastreamento de transação na tabela.
3. Clique na guia Exibição em árvore no painel inferior.
4. Expanda um nó na árvore.
   Cada nó na árvore exibe o componente, o nome, a duração e o percentual da duração total da transação. A cor do ícone de círculo indica a duração:
   – Vermelho: duração do componente > 25% da duração total
   – Amarelo: duração do componente > 9% < 25% da duração total
   – Verde: duração do componente <= 9% da duração total

   Neste elemento gráfico, você pode acompanhar os indicadores circulares vermelhos na árvore. Veja os métodos envolvidos na maior parte do tempo da transação. Por exemplo, o método `AxisServer:` :invoke usou 95% dos 37 ms que a transação levou para ser executada.
   Os componentes de rastreamento que não contribuem com um tempo significativo para a transação são codificados por cor com um ícone verde.
5. Selecione um componente para exibir as seguintes informações na área Detalhes do componente:
   – Tipo, nome e caminho do componente
   – Duração, marca de data e hora e tempo total da transação

> **NOTE**
>
> Para componentes de transação correlacionados, as guias Exibição do resumo e Exibição em árvore exibem somente o escopo da primeira JVM. A guia Exibição de rastreamento mostra todo o escopo

dos componentes de transação relacionados. Esteja ciente dessa limitação ao alternar da Exibição de rastreamento para outras exibições de guia.

Dados agregados de múltiplas transações

No rastreador de transações, você pode selecionar várias transações para ver dados agregados de todos os componentes nos rastreamentos.

Siga estas etapas:

1. Abra uma lista de transações executando um Rastreamento de transação.
2. Selecione várias transações usando CTRL-clique ou SHIFT-clique.
3. Abra a exibição de resumo ou em árvore para ver os dados de transação agregados.
   - O Rastreador de transações mostra os dados agregados na tabela.
     Talvez seja necessário rolar para baixo para ver todos os dados.
   - A Exibição em árvore mostra os dados agregados.
     Na Exibição em árvore, o Rastreador de transações adicionará um nó se as transações selecionadas não compartilharem um nó raiz comum. O nó é chamado de Raiz.

     NOTE

     Mais informações:

     - Imprimir, salvar e exportar informações de rastreamento de transaçãohttps://techdocs.broadcom.com

Consultar eventos armazenados

Os resultados da sessão de Rastreamento de transação são automaticamente armazenados no banco de dados Evento de transação. Os eventos de transação incluem Rastreamentos de transação e erros, inclusive paralisações (se você tiver instalado o Introscope Error Detector.) O banco de dados Evento de transação contém os Rastreamento de transação que foram automaticamente amostrados pelo Introscope. O banco de dados também contém os resultados das sessões de Rastreamentos de transação que você mesmo executa.

O banco de dados Evento de transação oferece suporte a estes tipos de consulta:

- eventos históricos (básicos) – veja Consultando eventos históricos
- eventos semelhantes (para seleção)
- eventos correlacionados (para seleção)
  Observação: certifique-se de executar algumas sessões de Rastreamento de transação antes de usar a consulta histórica, para que haja dados a serem consultados.

Sintaxe da consulta

As seções abaixo descrevem como usar o recurso Consulta histórica para consultar erros armazenados. O recurso de consulta:

- **Não diferencia maiúsculas de minúsculas** – para sequências de caracteres de consulta ou valores para opções de consulta.
- **Oferece suporte ao caractere curinga asterisco (*)** – insira o fragmento de um termo de pesquisa seguido pelo asterisco. (Você não pode iniciar um termo de pesquisa com o caractere de asterisco.) Por exemplo, para procurar

erros associados a um componente cujo nome inclui a sequência de caracteres Compras, use a sequência de caracteres de consulta Compras*.

- **Oferece suporte a operadores booleanos --** Os termos de pesquisa podem usar a lógica Booleana, como "AND", "OR", "NOT" e os agrupamentos "()".
- **Oferece suporte a condições de exclusão** – use "+JDBC-CICS" para procurar transações com JDBC, mas não CICS.
- **Oferece suporte a opções de consulta** – use as opções descritas nas opções de consulta e a sintaxe para limitar os eventos de erro de consulta que ocorreram em um período específico ou que estão associados a determinados usuários ou elementos do ambiente de hospedagem (conforme identificado pelo domínio, o agente, host ou processo).

Consultar eventos históricos

Você pode consultar eventos de transação históricos.

Siga estas etapas:

1. Selecione Estação de trabalho > Eventos históricos de consulta.
   O Visualizador de consultas históricas é aberto.
   O campo Consulta será exibido, em uma lista suspensa, até doze pesquisas anteriores a partir dessa sessão, ou sessões anteriores pelo mesmo usuário da estação de trabalho. Isso permite que você selecione uma de suas pesquisas salvas em vez de redigitá-la.
   Dica: por padrão, o campo se lembrará de até doze pesquisas; você pode designar outro número de pesquisas a serem lembradas pelo campo editando a propriedade introscope.workstation.historical.query.history.limit em *IntroscopeWorkstation.properties*.
2. No campo Consulta, digite uma combinação de:
   – *tipo* da opção de consulta: para incluir todos os eventos de transação que correspondem ao tipo especificado.
   – sequência de caracteres de consulta – para procurar erros que contêm ou correspondem a uma sequência de caracteres. Se você não inserir uma sequência de caracteres de consulta, todos os eventos de erros serão retornados.
   – opções de consulta – para limitar a pesquisa com base nos parâmetros do evento, conforme definido na sintaxe e nas opções de consulta.
   Dica: à medida que você começa a digitar no campo Consulta, as pesquisas exibidas na lista suspensa serão limitadas àquelas que corresponderem ao que você digitou.
3. Use a opção Intervalo de tempo para filtrar sua consulta com base no intervalo, se apropriado – consulte Exibindo dados históricos para obter uma explicação de como usar a opção Intervalo de tempo.
   Se você não selecionar um intervalo de tempo, a consulta usará o padrão Todos e não aplicará um filtro.
4. Clique em Ir.
   As transações que correspondem à consulta são exibidas na janela Consulta histórica – o formato é semelhante ao do Visualizador do rastreamento de transação. Para obter mais informações, consulte Usando o Visualizador do rastreamento de transação.
   Observação: somente 500 eventos podem ser exibidos. Se mais de 500 eventos corresponderem à consulta, serão mostrados os 500 mais antigos.

Sintaxe e opções de consulta

As consultas usam a sintaxe da expressão regular Lucene para localizar e substituir as sequências de caracteres de texto.
Observação: para obter informações sobre a sintaxe Lucene, consulte o site da Lucene (lucene.apache.org) e procure por "sintaxe de consulta".

Campo	Descrição	Exemplo
agente	Limita a pesquisa a eventos relatados por um determinado agente.	agent:ControlledRangeAgent
domínio	Limita a pesquisa a eventos relacionados a componentes de um determinado domínio.	domain:AcmeWest
fullAgent	Limita a pesquisa a eventos relatados por agente(s) específico(s), conforme especificado pelo seu caminho completo: *domain|process|host|agent.*	fullAgent:AcmeWest| Custom Metric Host| ControlledRange Agent
host	Limita a pesquisa a eventos ocorridos em um host específico.	host:Wmiddle01
process	Limita a pesquisa a erros relacionados a componentes de um determinado aplicativo.	process:Custom Metric Host
root	Limita a pesquisa a eventos associados a componentes específicos, conforme especificado pelo caminho da métrica.	root:servlets|accountServlet
type	Especifica o tipo de evento a ser incluído nos resultados da consulta. **errorsnapshot** – limita a pesquisa a eventos de erro. **normal** – retorna eventos de transação que são capturados nos Rastreamentos de transação iniciados pelo usuário. **sampled** – retorna eventos de transação que foram capturados como resultado da amostragem de transação padrão do Introscope.	type:errorsnapshot type:normal type:sampled
url	Limita a pesquisa aos eventos associados ao prefixo de caminho de URL da transação especificada. O prefixo de caminho é a parte do URL após o nome do host. No seguinte URL: *http://burger1.com/bWar/burgerServlet?ViewItem&category=11776&item=55562630&rd=1* ...o prefixo do caminho é: */bWar/burgerServlet*	url:/bWar/burgerServlet
urlParams	Limita a pesquisa aos eventos associados aos parâmetros de URL da transação especificada. Os parâmetros de URL seguem um ponto de interrogação (?) no URL. Neste URL: http://ubuy.com/ws/shoppingServlet?category=734&item=3772&tc=photo a parte do parâmetro de URL é: ?category=734&item=3772&tc=photo **Observação:** urlParams não pode começar com um caractere curinga.	urlParams:category=734*

user	Limita a pesquisa a eventos de transações associados ao nome do usuário especificado.	user:jdoe
duration	Limita a pesquisa pela duração do evento (milissegundos padrão).	
componentsNotShown	Limita a pesquisa a eventos em que um determinado componente não é exibido	
durationencoded	Nenhuma definição fornecida	
time	Limita a pesquisa a eventos antes ou após um período especificado.	time:[yyyyMMddHH] em que y=ano, M=mês, d=data e H=hora do dia
traceID	Limita a pesquisa a eventos com uma ID de rastreamento especificada.	traceID:1340419311156\:3957 **Observação**: um caractere de barra invertida (\) é obrigatório antes do segundo dois-pontos (:).

Se os seguintes caracteres especiais fizerem parte da sua consulta, a sintaxe Lucene permitirá que seja usado o caractere de barra invertida (\) como escape para eles:

```
+ - && || ! ( ) { } [ ] ^ " ~ * ? : \
```

Por exemplo, para procurar (1+1):2, use a consulta:

\(1\+1\)\:2

Observação: os caracteres * (asterisco) e ? (ponto de interrogação) não são suportados no início de uma consulta.

Consulta de eventos semelhantes

No Introscope, é possível consultar eventos que são semelhantes a um evento selecionado. Por exemplo, eventos semelhante podem ser todos que contenham os mesmos componentes (Servlet > EJB > SQL) com tempos de resposta variados. O Introscope irá considerar eventos semelhantes se 60% das sequências de caracteres dentro deles (nomes de componente, nomes de tabelas SQL e assim por diante) se sobrepuserem.
Observação: mesmo que um evento de tipo de transação seja selecionado, transações e erros podem ser retornados nos resultados (erros serão retornados apenas se ErrorDetector estiver instalado).

Siga estas etapas:

1. Com uma janela de resultados de consulta aberta, selecione uma linha da tabela.
2. Selecione Rastreamento > Eventos semelhantes.

O Introscope lista eventos semelhantes na janela Consulta histórica.

Consulta de eventos correlacionados

No Introscope, é possível consultar eventos que estejam correlacionados – aqueles que fazem parte da mesma transação maior. Por exemplo, um evento de tempo de resposta do navegador está correlacionado a um evento de transação de servlet.
Observação: mesmo que um evento de tipo de transação seja selecionado, transações e erros podem ser retornados nos resultados.

Siga estas etapas:

1. Com uma janela de resultados de consulta aberta, selecione uma linha da tabela.
2. Selecione Rastreamento > Eventos correlacionados.

O Introscope lista eventos correlacionados na janela Consulta histórica.

Imprimir, salvar e exportar informações de rastreamento de transação

É possível executar estas atividades com informações de rastreamento de transação:

- Imprimir a janela de rastreamento de transação.
- Salvar dados de rastreamento de transação como um arquivo XML que pode ser aberto posteriormente na janela Rastreamento de transação.
- Exportar dados de rastreamento de transação como um arquivo de texto para análise em um editor de texto.

Imprimir a janela Rastreamento de transação

Siga estas etapas:

1. Selecione Estação de trabalho > janela Imprimir.
   A janela Page Setup é aberta. Os padrões de impressão são tamanho Letter e orientação de retrato.
2. Clique em OK para continuar ou altere as opções e, em seguida, clique em OK.
   A janela Imprimir é exibida.
3. Selecione as opções de impressão e clique em OK.
   Observação: a impressão de um intervalo de páginas não é suportado (tudo é impresso em uma página).

O conteúdo de toda a janela de rastreamento de transação é impresso, ajustado para caber em uma página.

Salvar dados de rastreamento de transação

Salve os dados de rastreamento de transação em um arquivo XML. Posteriormente, é possível abrir o arquivo em uma janela de rastreamento de transação para a reprodução dos dados em questão.

Siga estas etapas:

1. No Visualizador do rastreamento de transação, selecione os Rastreamentos de transação a serem salvos:
   - CTRL + clique para selecionar vários rastreamentos de transação.
   - Editar > Selecionar tudo para selecionar todos os rastreamentos de transação na janela.
2. Clique em Salvar como.
3. Abra o arquivo ou selecione o local em que deseja salvar o arquivo.
4. Se você está salvando o arquivo, digite um nome e clique em Salvar.

Abrindo dados salvos no XML do rastreador de transações

Você pode abrir e exibir os dados salvos no rastreamento de transação em uma nova janela Rastreamento de transação. É possível compartilhar os arquivos salvos por email ou armazená-los em uma unidade de rede compartilhada. O compartilhamento de arquivos permite que os usuários colaborem em análises de problemas.

Ao abrir os dados de rastreamento de transação salvos:

- Não é possível reiniciar a sessão de rastreamento de transação que está sendo exibida.
- Os links de componentes de rastreamento de transação para seus caminhos de métrica não estarão disponíveis se os caminhos de métrica não estiverem online no Gerenciador corporativo ao qual a estação de trabalho está conectada.

Para abrir dados de rastreamento de transação salvos em um arquivo XML:

1. Selecione Estação de trabalho > Eventos históricos de consulta
2. Selecione Rastreamento > Abrir eventos salvos (XML).
3. Selecione o arquivo XML na janela do navegador e clique em Abrir.
   Os dados no arquivo XML são exibidos em uma nova janela de consulta histórica.

Observação: quando você exibir eventos históricos salvos em um arquivo XML, os eventos correlacionados serão exibidos, mas não serão mostrados como correlacionados. Para ver a correlação de eventos históricos em um rastreamento de transação, exiba um rastreamento ativo (verifique como consultar eventos correlacionados).

Agora é possível executar estas ações:

- Exportar um rastreamento de transação como arquivo de texto.
- Selecionar rastreamentos de transação nos dados e salvá-los como um novo arquivo XML.

Exportar um rastreamento de transação em um arquivo de texto

Para exportar rastreamentos de transação em um arquivo de texto:

1. No Visualizador do rastreamento de transação, selecione os Rastreamentos de transação a serem exportados:
   – CTRL + clique para selecionar vários rastreamentos de transação
   – Editar > Selecionar tudo para selecionar todos os rastreamentos de transação na janela.
2. Selecione Rastreamento > Exportar.
3. Selecione um local para salvar o arquivo e o nome do arquivo (o nome padrão é *<tipo de componente raiz>_<nome do componente raiz>.txt*), e clique em OK.

Arquivo XML de rastreamento de transação de exemplo


```
<?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>
```


Monitorar com estação de trabalho

Os usuários avançados do DX APM compreendem que o DX APM é muito útil não apenas para investigar problemas de aplicativos, mais também para monitorar o desempenho do aplicativo nominal. Depois de entender o desempenho nominal do aplicativo, você estará mais bem equipado para compreender sinais de problemas de desempenho e falhas.

Esta seção contém os seguintes tópicos:

- Compreendendo o desempenho nominal
- Ler e compreender as notificações
- Diagnosticar o problema com a guia Navegador de métricas

Diagnosticar o problema com a guia Navegador de métricas

As ferramentas na guia Navegador de métricas ajudam a encontrar e investigar problemas.

Índice

As seguintes ferramentas na guia **Navegador de métricas** ajudam a encontrar mais informações sobre um problema:

- Métricas históricas
- Pesquisa
- Rastreador de transações

Usando métricas históricas e dinâmicas

Por padrão, as exibições são de métricas dinâmicas, com atualização de dados a cada 15 segundos. Os dados que não são exibidos em um gráfico dinâmico são salvos pelo Gerenciador corporativo como dados históricos. Para diagnosticar um problema que pode ter começado alguns minutos ou horas atrás, exiba os dados históricos.

Exibindo dados históricos na guia Navegador de métricas

Para exibir dados históricos, selecione um intervalo de tempo. Usar o intervalo de tempo pode ajudar você a identificar rapidamente a hora em que um problema ocorreu. Por exemplo, você acha que o problema ocorreu na última hora. Defina o intervalo de tempo para uma hora e examine os dados do momento atual para trás. Caso o problema não seja visualizado dentro desse intervalo de hora, você poderá usar os controles para mover para frente ou para trás. Mova-se pelo intervalo até localizar a hora em que o problema ocorreu.

Para exibir dados históricos:

1. Selecione a métrica ou o painel para o qual deseja ver os dados históricos.
2. Selecione no menu suspenso **Intervalo de tempo**, um intervalo de tempo para a exibição histórica.
   Os dados são exibidos para esse intervalo. O intervalo usa a duração que você selecionou e a define a hora de término para a hora atual.
   Observação: o DX APM aplica o intervalo de tempo que você seleciona para exibir dados históricos para outras métricas e painéis na mesma janela. Esse intervalo de tempo se aplica a todas as janelas novas que você abrir.
3. Para selecionar uma resolução que ajuste a granularidade da exibição, aumente ou diminua o número de pontos de dados que são exibidos.

Cada intervalo de tempo predefinido está associado a uma resolução padrão. Em geral, não é necessário alterar a resolução. Altere a resolução para ver um nível maior de detalhes ou mais granularidade de dados.

4. É possível ajustar um intervalo de tempo depois de selecionar o intervalo. Use os controles para rolar em incrementos com base no intervalo de tempo selecionado:
   - Arraste o controle deslizante na barra de tempo para alterar o intervalo de tempo.
   - Clique nas setas para retroceder e avançar no tempo.
     As setas simples movem para trás ou para frente em incrementos de tempo pequenos. As setas duplas movem para trás ou para frente em incrementos que estão próximos à hora do intervalo de tempo selecionado.
   - Clique no ícone **Redefinir** para redefinir a hora de término do intervalo para a hora atual.

Usando o zoom em dados históricos nos gráficos

Ao exibir dados históricos em um gráfico, você pode ampliar os dados.

Para ampliar os dados em um gráfico:

- Execute uma das seguintes ações:
  - Clique o ponteiro do mouse em uma posição no gráfico e arrastre para especificar o intervalo de tempo.
  - Clique com o botão direito do mouse no gráfico e clique em **Aplicar zoom** para ajustar os dados.

Os dados no visualizador são atualizados com base na nova consulta, e o intervalo de tempo no visualizador mostra o novo intervalo.

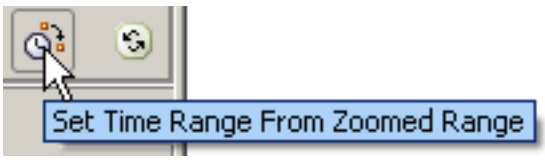
Para reduzir o zoom:

1. Clique com o botão direito no gráfico ampliado.
2. Clique em **Menos zoom** ou **Aplicar o máximo de zoom**.

O intervalo de tempo global na janela e o controle do Intervalo de tempo não são alterados automaticamente quando você amplia os dados. Por exemplo, você amplia um período de 10 minutos em um gráfico com o intervalo de tempo definido como 1 hora. O gráfico mostra o período de 10 minutos, mas o controle permanece em 1 hora. A barra de hora ainda mostra o intervalo de horas.

Para definir o intervalo de tempo global e o controle de Intervalo de tempo para corresponder com a exibição com zoom:

- Clique no botão **Definir intervalo de tempo a partir do intervalo de zoom**:



Usando a pesquisa

A guia Pesquisar (veja a guia Pesquisar) está ativa para cada nó na Árvore do investigador. Usando essa guia, você procura qualquer uma das métricas em um nó específico.

Para encontrar a guia Pesquisar:

1. Selecione um nó na árvore do navegador de métricas.
2. Selecione a guia Pesquisar.

Para usar a pesquisa de texto sem formatação:

1. Digite uma sequência de caracteres no painel de pesquisa.
2. Pressione **Ir** ou **Enter**.

Os resultados da pesquisa são exibidos no formato de tabela. Os resultados mostram todos os recursos cujo nome inclui a sequência de caracteres da pesquisa.

TIP

Selecionar qualquer uma das métricas listadas na tabela exibe um gráfico mostrando uma exibição dinâmica da métrica.

Para exibir resultados incluindo Mín., Máx. e Contagem de cada resultado:

- Selecione **Mostrar mínimo, máximo e contagem**.

TIP

É possível selecionar **Mostrar mínimo, máximo e contagem** após a pesquisa e os resultados são atualizados com as novas colunas.

Usando expressões regulares

O painel Pesquisar aceita qualquer expressão regular que usa a linguagem de expressões regulares Perl 5.

TIP

A linguagem de expressão regular Perl 5 também é usada para definir agrupamentos de métricas.

Para usar expressões regulares na pesquisa:

1. Selecione **Usar expressões regulares**.
2. Digite uma expressão regular no painel Pesquisar.
3. Pressione **Ir** ou **Enter**.
   A guia **Pesquisar** mostra os resultados.

Usando rastreamento de transação

O rastreador de transações é uma poderosa ferramenta para rastrear a atividade das transações à medida que elas passam por um aplicativo. Você executa rastreamentos de transação para monitorar as transações que ocorrem em uma JVM (Java Virtual Machine - Máquina Virtual Java) em um ambiente Java ou em um CLR (Common Language Runtime) em um ambiente .NET.

Consulte Usar o Rastreador de transações.

Ler e compreender as notificações

Notificações de alerta em painéis

A forma mais óbvia é uma notificação visual em um painel de console. A ilustração abaixo mostra um painel com um único gráfico que foi configurado com uma linha amarela mostrando o limite de Cuidado em 3000 ms e o limite de Risco em 4000 ms.

O gráfico mostra:

- O Tempo médio de resposta ultrapassando o limite de Cuidado várias vezes nos últimos minutos.
- O Tempo médio de resposta ultrapassando o limite de Risco uma vez, há cerca de dois minutos.
- De acordo com a medida mais recente, o desempenho do aplicativo está em estado de Cuidado.

Os indicadores no gráfico mostram outra forma de indicar o status de alerta. A maneira como os painéis aparecem depende de como você ou o administrador os configurou.

Quando um painel mostra uma condição Cuidado ou Risco, o indicador de alertas geralmente acumula métricas de várias fontes. Sua tarefa deve ser descobrir quais métricas subjacentes estão causando a condição.

Para alterar uma exibição de alertas:

- Exiba um alerta no painel Investigator Preview e selecione Propriedades > Exibição de alertas.

Mensagens de alerta

As mensagens de alerta são disparadas por uma ação associada a um status de alerta. Esses alertas são exibidos automaticamente. Também é possível exibir mensagens de alerta selecionando Estação de trabalho > Mostrar mensagens de alerta.

Compreendendo o desempenho nominal

Compreender o desempenho normal do aplicativo cria familiaridade com seu sistema, bem como com as ferramentas e os utilitários do DX APM. Essa compreensão fornece um contexto mais amplo para entender quais são os problemas inevitáveis. Quando houver algum problema, você terá os conhecimentos para localizá-lo.

Três nós diferentes na árvore do Navegador de métricas são especialmente úteis para permitir o monitoramento do desempenho do aplicativo. Tais nós (**GC Heap**, **Front-ends** e **Back-ends**) podem ser considerados como os sinais vitais do seu aplicativo.

Monitorar o desempenho com métricas de GC Heap

A coleta de lixo é o processo de liberação da memória consumida por objetos que não estão mais em uso. Depois de liberada, essa memória pode ser usada por outros objetos. As métricas de **GC Heap** (memória heap da coleta de lixo) são uma boa ferramenta para monitorar e compreender o desempenho dos aplicativos.

GC Heap|Bytes In Use

A métrica GC Heap|Bytes In Use informa a quantidade de memória sendo usada atualmente pelos objetos.

GC Heap|Bytes Total

A métrica GC Heap|Bytes Total informa a quantidade total de memória alocada pela JVM.

A falta ou o excesso de memória alocada para a JVM podem levar a problemas de desempenho. Em resumo, você pode usar as seguintes diretrizes:

- Quando há falta de memória alocada, o processo de GC é executado mais vezes, o que leva a problemas de degradação do desempenho por curtos períodos, mas com frequência.
- Quando há excesso de memória alocada, o processo de GC é executado por um tempo relativamente longo e gera degradação no desempenho durante esse período.

Você pode usar essas métricas para ajudar a determinar o tamanho correto da memória heap.

Depois de determinar o tamanho correto, você pode acompanhar as métricas de memória heap de GC ao longo do tempo para compreender o desempenho nominal. A métrica **Bytes em uso** deve mostrar reduções e aumentos periódicos. Com o tempo, as métricas formarão um padrão que se repete e não mostrarão nenhuma evidência de vazamento de memória.

Monitorar o desempenho com métricas do GC Monitor

O GC Monitor fornece um conjunto de métricas sobre o funcionamento interno da JVM, incluindo alocação de memória e taxa de crescimento da memória heap.O GC Monitor ajuda na alocação da memória heap da JVM, verificando se todos os coletores de lixo e seus pools de memória estão alocados de forma adequada. Dessa forma, você pode detectar problemas de GC que estão afetando negativamente o desempenho.

JVMs suportadas

O GC Monitor oferece suporte apenas às seguintes JVMs:

- Sun JVM, versão 1.5.0 e superior, tanto de 32 quanto de 64 bits
- IBM, versão 1.5.0 e superior, tanto de 32 quanto de 64 bits

Para usar as métricas do GC Monitor para ajustar a alocação de memória:

1. Na árvore Navegador de métricas, vá para o nó do agente no host cuja atividade de GC deseja monitorar. Expanda o nó **GC Monitor**.
2. Monitore as métricas e o uso do pool de memória de cada coletor de lixo.
3. Com base nas métricas, realoque o tamanho dos pools de memória para aumentar a eficiência da GC.

Caso precise de diretrizes para ajudá-lo a realocar o tamanho dos pools de memória, consulte a documentação apropriada para a sua JVM.

Monitorar o desempenho com métricas de Front-ends

Você pode usar o nó **Front-ends** de duas maneiras para monitorar o desempenho geral do aplicativo: monitorando as métricas padrão e observando os principais URLs.

Monitorando as métricas padrão de Front-ends

O DX APM exibe as cinco métricas básicas de diagnóstico para cada front-end. Consulte essas métricas na árvore do Navegador de métricas em `Front-ends|Apps|<nome_do_front-end>`.

Bom desempenho

Um aplicativo está funcionando bem quando um grande volume de solicitações estão sendo atendidas (**Respostas por intervalo**), o que corresponde a uma latência baixa (um baixo **Tempo médio de resposta**). Uma boa regra é de aproximadamente um segundo por transação.

Desempenho problemático

Os métodos simultâneos são métodos que começam durante um intervalo e não são finalizados durante o mesmo intervalo. Como você deseja que os métodos sejam concluídos rapidamente, um número excepcionalmente alto de invocações simultâneas é indesejável. Você pode observar picos temporários em invocações simultâneas, mas a métrica deve retornar para zero todas as vezes. Uma métrica que não retorna para zero pode indicar um afunilamento de segmentos, o número de conexões de banco de dados ou algum outro recurso compartilhado.

Reconhecendo as transações com o pior desempenho

Outra boa maneira de monitorar o desempenho é estar ciente de quais transações apresentam desempenho sempre baixo. Você pode configurar um visualizador de dados para exibir as transações mais lentas em um gráfico de barras.

Uma das melhores maneiras de exibir as transações mais lentas é configurar grupos de URLs como base para o agrupamento de suas métricas.

Monitorar o desempenho com métricas de Back-ends

O nó **Back-ends** da árvore do Navegador de métricas mostra as cinco métricas padrão para cada sistema back-end conectado.

Duas métricas diferentes sob o nó **Back-ends** o ajudarão a reconhecer o desempenho nominal.

Frequência de instrução SQL

Manter-se informado sobre quais instruções SQL são mais processadas é uma boa maneira de se familiarizar com o desempenho do aplicativo.

Para verificar a frequência de uma instrução SQL como uma medida de desempenho:

1. Sob o nó **Back-ends**, abra o nó para o aplicativo que deseja monitorar.
2. No aplicativo, abra o nó do aplicativo que você deseja monitorar.

A guia **Visão geral** exibe uma lista de consultas e outras instruções SQL em execução em relação ao recurso de banco de dados.

3. Na seção **Consultas** do painel direito, clique no cabeçalho de coluna **Respostas** para classificar a tabela pelo número de respostas.
4. Observe as consultas SQL mais enviadas.

Padrões de conexão do banco de dados

Fique atento aos padrões de conexão do banco de dados de aplicativos e mantenha-se informado sobre quando o padrão é interrompido.

A maneira como seu aplicativo estabelece e mantém as conexões do banco de dados depende da plataforma.

Usar a estação de trabalho

O console de estação de trabalho exibe informações de métrica nos painéis. Os painéis são janelas pré-configuradas que representam exibições gráficas de métricas de disponibilidade e desempenho atuais ou históricos.

Quando você abre o console, ele mostra dados de disponibilidade e desempenho em tempo real. É possível exibir dados históricos selecionando um intervalo de tempo.

Navegando entre painéis no Console

Índice

Você pode selecionar os painéis Console de várias maneiras diferentes:

- Lista suspensa Painel
- Botões de avanço e retrocesso
- Lista Histórico
- Botão Página inicial
- Hiperlinks

Lista suspensa Painel

Você pode selecionar painéis na lista suspensa na parte superior da página Console. É possível digitar todo o nome do painel, ou parte dele, para restringir as seleções na lista.

Depois de exibir vários painéis, você pode navegar entre eles:

- Usando as setas para avançar e voltar
- Usando a lista suspensa próxima das setas para avançar e voltar.
- Se você tiver definido um painel de página inicial em suas preferências de usuário, será possível abri-lo clicando no botão Página inicial.

Navegar usando hiperlinks

Você pode usar hiperlinks para navegar entre painéis do Introscope e o Investigador:

- Hiperlinks automáticos – o Introscope vincula automaticamente um Visualizador de dados ao agrupamento de métricas no qual ele se baseia. O menu Links do visualizador contém um link para a definição do agrupamento de métricas subjacente no Editor do módulo de gerenciamento. Da mesma forma, os painéis que contêm Visualizadores

de dados com base no mesmo agrupamento de métricas são vinculados automaticamente, e você pode navegar entre eles usando o menu Links.

- Hiperlinks personalizados — você pode definir links personalizados para itens do painel, de modo a vinculá-los a páginas da web ou a outros painéis. Será possível definir links personalizados se você tiver permissão de edição de painel.
  Observação: alguns painéis Console prontos para uso – por exemplo, Capacidade do EM – não contém automaticamente links para dados subjacentes. Edite esses painéis padrão ou crie novos painéis com links.

Para ver uma lista de links de painel disponíveis:

1. Clique com o botão direito do mouse em um objeto do painel.
2. Selecione Propriedades > Links.

Se não houver links disponíveis para um objeto, o menu Links será desativado

Para seguir os links do painel:

1. Passe o cursor sobre um objeto do painel que tenha um hiperlink.
   O ponteiro muda para uma mão.
2. Clique duas vezes no objeto a fim de seguir o link para seu destino padrão.

Criando favoritos do painel

Para simplificar o acesso aos painéis que você usa com frequência, é possível adicioná-los ao menu Favoritos do Console.

Para adicionar um painel aos Favoritos:

1. Vá até o painel.
2. Selecione Favoritos > Adicionar aos favoritos.
   Observação: os links para favoritos não são mantidos quando você renomeia ou exclui um painel favorito. Atualize o link ou exclua o link antigo e crie um novo.

Para excluir um painel de Favoritos:

1. No Console, selecione Favoritos > Organizar favoritos.
2. Selecione um painel.
3. Selecione Excluir.

Para editar a lista de favoritos:

1. No Console, selecione Favoritos > Organizar favoritos.
2. Selecione um painel.
3. Selecione Editar.

Iniciando o Investigador no Console

Se estiver exibindo dados dinâmicos no Console e iniciar o Investigador da estação de trabalho por esse Console, você poderá exibir os dados dinâmicos também no Investigador. No entanto, no Investigador, o valor padrão para o intervalo de datas é de 8 minutos e a resolução é de 15 segundos. Não existe a opção de inserir um intervalo de datas personalizado e a resolução para o modo dinâmico no Investigador.

Se você estiver exibindo dados históricos no Console e iniciar o Investigador da estação de trabalho por esse Console, será possível exibir os dados históricos também no Investigador para o mesmo intervalo de datas e resolução selecionados para os dados históricos no Console.

Iniciando o Console no Investigador

Se estiver exibindo dados dinâmicos no Investigador e iniciar o Console da estação de trabalho nesse Investigador, você poderá exibir dados dinâmicos também no Console. No entanto, no Console, o valor padrão para o intervalo de datas é de 8 minutos e a resolução é de 15 segundos. É possível inserir um intervalo de datas personalizado e a resolução para o modo dinâmico no Console.

Se estiver exibindo dados históricos no Investigador e iniciar o Console da estação de trabalho por esse Investigador, você poderá exibir dados históricos também no Console para o mesmo intervalo de datas e resolução selecionados para os dados históricos no Investigador.

Encontrar mais informações em painéis

Quando desejar saber mais sobre os dados que são apresentados nos painéis, você pode usar atalhos para obter mais informações.

Siga estas etapas:

1. Clique com o botão direito do mouse em um gráfico ou um alerta, selecione Links e vá até o alerta correspondente no Módulo de gerenciamento ou outro painel que esteja associado ao gráfico ou alerta.
2. Clique duas vezes em uma métrica do gráfico que exibe os dados da métrica N principais (por exemplo, 10 ou 25 mais lentos) para exibir os respectivos detalhes no Investigador.

Filtrando por agente com a Lente do console

Use a Lente do console para filtrar dados de métrica para os agentes que estão relatando dados. Em um painel que mostra dados de mais de um agente, é possível usar a Lente do console para exibir dados somente de agentes selecionados.

Quando você aplica a Lente do console, essa filtragem permanece em vigor até que você feche a janela Console, efetue logoff na estação de trabalho ou use o comando Limpar lente.

Aplicando a Lente do console

Para aplicar a Lente do console:

1. Selecione o botão Lente (ou selecione Painel, Lente).
   Se o Console estiver no modo Dinâmico, a caixa de diálogo listará os agentes atualmente conectados. Se você estiver exibindo um intervalo de datas dos dados históricos, a caixa de diálogo listará os agentes conectados para o intervalo histórico selecionado.
2. Na caixa de diálogo Selecionar agente, selecione um único agente ou vários agentes (selecione e arraste ou CTRL/clique) pelos quais filtrar.
   Observação: você pode começar a digitar um nome de agente, nome do host ou nome do processo no campo Pesquisar. Conforme você digita, o agente lista os filtros para correspondência com o que é digitado.
3. Selecione Aplicar ou pressione Enter.
   O painel é atualizado para mostrar apenas os dados do(s) agente(s) selecionado(s). A seta na lente muda de azul-claro para escuro quando uma lente é aplicada.

Widgets não suportados

Alguns widgets do painel não oferecem suporte ao recurso de efeito de lente:

- Gráficos equipados com calculadoras
- Gráficos com base em um Agente Virtual equipado com um alerta simples. Isso inclui um gráfico Os 10 principais agentes conectados no painel Visão geral.

Observação: ao editar um painel para adicionar um novo alerta simples, esteja ciente de que quando uma lente é aplicada ao painel, algum tempo pode decorrer antes que o novo alerta exiba quaisquer dados de status.

Limpando as Lentes do console

Para limpar as Lentes do console:

1. Selecione Lente.
2. Limpe as Lentas clicando no botão Limpar na caixa de diálogo Aplicar lente do console.

Lente do console e exibições da guia em painéis

O efeito que uma Lente do console tem sobre uma exibição do Investigador em um painel depende do tipo de item de árvore ao qual a exibição está associada.

Se o item do Investigador associado à exibição for:	e...	então
um domínio	um único agente for selecionado na lente...	...a associação do item mudará para uma seleção de agente único. Se a exibição não oferecer suporte à seleção de agente, uma mensagem de erro será exibida.
um agente	um único agente for selecionado na lente...	...a associação do item mudará para uma seleção de agente único.
uma métrica	um único agente for selecionado na lente...	...a mesma métrica no agente selecionado se tornará a seleção atual. Se essa métrica não existir, uma mensagem de erro será exibida.
um caminho de métrica	um único agente for selecionado na lente...	...o mesmo caminho de métrica no agente selecionado se tornará a seleção atual. Se esse caminho não existir, uma mensagem de erro será exibida.
outro tipo de item		uma mensagem de erro será exibida.

Se mais de um agente for selecionado, uma mensagem de erro será exibida.

Se o agente com efeito de lente for um Agente virtual, a exibição mostrará dados desse agente se ele oferecer suporte a esse tipo de seleção. É possível determinar quais exibições são suportadas para um determinado tipo de item selecionando um item na árvore e observando as guias de exibição disponíveis.

Um Agente virtual é um grupo de agentes físicos que são configurados para serem um único agente, permitindo que você veja uma exibição agregada das métricas relatadas por vários agentes.

Manipulando o conteúdo de visualizadores de dados

Os visualizadores de dados no painel visualizador do Investigador ou em um painel mostram dados de um aplicativo instrumentado em um formato visual. Os dados são exibidos em um visualizador de dados com base no seu tipo — por exemplo, as métricas aparecem como gráficos e os alertas como indicadores coloridos. Os visualizadores de dados podem exibir dados de uma métrica, um recurso ou um elemento, como um alerta.

Nos visualizadores de dados, é possível:

- Exibir os valores mínimo/máximo de métrica em um gráfico
- Mostrar ou ocultar os dados de métrica em um gráfico
- Alterar a escala dos gráficos
- Mover métricas para frente ou para trás em gráficos
- Exportar dados

Exibindo os valores mínimo/máximo de métrica em um gráfico

Você pode configurar um gráfico para mostrar os valores mínimo e máximo.

Para mostrar os valores mínimo e máximo de métricas e agrupamentos de métricas em um gráfico:

1. Selecione o gráfico no Console para selecioná-lo.
2. Mostre os valores mínimo e máximo de duas maneiras:
   – Clique com o botão direito do mouse no visualizador de dados e selecione Mostrar mínimo e máximo.
   – Selecione o menu Propriedades e selecione Mostrar mínimo e máximo.
   Observação: essa alteração permanece em vigor somente enquanto você exibe o painel atual. Se você abrir um novo Console ou alternar para outro painel, essa configuração será revertida para o padrão, que não mostra os valores mínimo e máximo da métrica. Para mostrar os valores mínimo e máximo da métrica por padrão em um gráfico, ative essa opção ao editar um painel com o Editor de painéis.

Mostrando/ocultando os dados de métrica em um gráfico

Se você estiver exibindo os dados de várias métricas em um gráfico, é possível mostrar ou ocultar dados de métrica individualmente.

Para mostrar ou ocultar uma métrica em um gráfico:

1. Exiba um gráfico no painel, no Console.
2. É possível:
   – Mostre a métrica clicando em sua caixa de seleção.
   – Oculte a métrica desmarcando a caixa de seleção.
   Observação: as opções de mostrar/ocultar métricas não são disponibilizadas quando você exibe elementos gráficos ou gráficos de barras que exibem dados classificados ou filtrados.

Alterando a escala dos gráficos

Você pode alterar a escala dos gráficos ao exibir dados dinâmicos na estação de trabalho, de modo a fornecer uma exibição mais clara. É possível alterar a escala de um gráfico configurando um valor mínimo e máximo para o eixo de dados do gráfico.

O recurso de escala do gráfico está disponível somente para gráficos no modo dinâmico. Ele não está disponível para outros tipos de visualizador, como gráficos de barras, os 10 principais ou visualizador de sequência de caracteres. **Observação:** as alterações de escala que você faz em um gráfico são temporárias – as configurações não são salvas com o painel. Quando você seleciona um novo painel ou fecha a janela Console, o Introscope descarta as configurações e retorna para as opções de escala que foram aplicadas quando o painel foi criado.

Para exibir a escala de um gráfico:

- Clique em um gráfico para selecioná-lo e, em seguida:
- Selecione Visualizador > Opções de escala ou
- Clique com o botão direito do mouse e selecione Opções de escala no menu de contexto.
  A caixa de diálogo Opções de dados é aberta.

Definir os valores padrão mínimo e máximo da escala automática fornece uma exibição mais clara dos gráficos no modo Dinâmico.

Para redimensionar usando os valores mínimo e máximo:

1. Clique em um gráfico para selecioná-lo e, em seguida:
   – Selecione Visualizador > Opções de escala ou
   – Clique com o botão direito do mouse e selecione Opções de escala no menu de contexto.
2. Digite os valores mínimo e máximo para o eixo de dados do gráfico.

3. Selecione OK.
   Por exemplo, se os valores de dados do gráfico estiverem basicamente entre 350 e 550, mas o eixo de valor do gráfico mostrar de 0 a 1000, pode ser útil definir a valor mínimo da escala para 300 e o valor máximo para 600, a fim de oferecer uma exibição melhor dos dados relevantes.

Para forçar os valores mínimo e máximo:

1. Clique em um gráfico para selecioná-lo.
2. Selecione Visualizador > Opções de escala.
3. Selecione o Marcador nos lados Mínimo e Máximo da caixa de diálogo e insira um valor para os pontos mínimo e máximo do acesso aos dados.
4. Selecione OK.

No entanto, configurar valores mínimo e máximo para um gráfico que mostra dados dinâmicos é arriscado, caso haja uma chance de que os dados possam exceder os valores definidos.

Para evitar esse problema, use a opção Escala automática de modo a definir automaticamente o gráfico para alterar sua escala de acordo com os dados que ele exibe.

Para redimensionar usando a Escala automática:

1. Clique em um gráfico para selecioná-lo.
2. Selecione Visualizador > Opções de escala.
3. Selecione Escala automática nos lados Mínimo e Máximo da caixa de diálogo.
4. Selecione OK.

O eixo de dados do gráfico resultante é redefinido com base nos dados do gráfico. Isso frequentemente resulta em altos e baixos mais destacados na exibição do gráfico

Você também pode definir as opções de escalação para Expandir automaticamente. Essa opção usa 0 como a parte inferior do eixo dados, bem como expande e dimensiona automaticamente o eixo de dados para exibir todos os dados do intervalo de datas.

Para redimensionar usando Expandir automaticamente:

1. Clique em um gráfico para selecioná-lo.
2. Selecione Visualizador > Opções de escala.
3. Escolha Expandir automaticamente nos lados Mínimo e Máximo da caixa de diálogo.
4. Selecione OK.

Movendo métricas para frente/trás no gráfico

Quando um gráfico contém várias métricas, é possível que pontos de dados se sobreponham. Você pode usar as opções Trazer para a frente ou Enviar para trás para escolher qual métrica aparecerá no topo da lista de métricas.
Observação: as opções Trazer para a frente/Enviar para trás não são disponibilizadas durante a exibição de gráficos que mostram dados classificados ou filtrados.

Para alterar a ordem de sobreposição das métricas em um gráfico:

1. Abra o Console e exiba um gráfico em um painel.
2. Clique com o botão direito do mouse no rótulo da métrica a ser alterada e escolha uma opção no menu:
   – Trazer para a frente (move a métrica selecionada para o topo das métricas listadas)
   – Enviar para trás (move a métrica selecionada para a base das métricas listadas)
   A métrica é movida para a posição escolhida.

Copiando um visualizador de dados para a área de transferência

Você pode copiar um instantâneo dos dados em um visualizador de dados para a área de transferência como uma imagem mapeada por bits. Em seguida, você cola a imagem em um email ou outro documento, ou qualquer aplicativo que aceite imagens mapeadas por bits. Essa será uma ferramenta útil se, por exemplo, você desejar mostrar dados em um visualizador de dados para um colega, ou talvez usá-los em uma apresentação.

Para copiar um visualizador de dados para a área de transferência:

1. Abra um Console e selecione um visualizador de dados
2. Selecione Visualizador > Copiar como imagem na área de transferência.
   Observação: não é possível copiar vários visualizadores de dados.

Exportando dados de visualizadores de dados

Você pode capturar um instantâneo dos dados atuais em um visualizador de dados e exportá-lo para um arquivo de valores separados por vírgulas (.csv). É possível exportar dados de todos os tipos do visualizador de dados, com exceção de alertas.

Para exportar dados de um visualizador de dados:

1. No Console, selecione um visualizador de dados.
2. Selecione Visualizador > Exportar dados.
3. Na caixa de diálogo Salvar, escolha um local para salvar o arquivo *.csv* e selecione Salvar.

Dados históricos e dinâmicos no console da estação de trabalho

Você pode exibir dados dinâmicos no console ou selecionar um intervalo de tempo para exibir dados históricos. A exibição de dados padrão é Dinâmica.

É possível verificar se a estação de trabalho está no modo Dinâmico examinando a lista suspensa Intervalo de tempo.

Exibir dados dinâmicos de consulta no console da estação de trabalho

Siga estas etapas:

- Clique em Dinâmico para ativá-lo e exibir dados dinâmicos.

O valor padrão para o intervalo de tempo é de 8 minutos e a resolução é de 15 segundos. Não é possível inserir um intervalo de tempo personalizado e a resolução para o modo dinâmico no console.

Observação: clique em Dinâmico para desativá-lo e selecione um intervalo de tempo e uma resolução na lista suspensa para exibir dados históricos. Você também pode inserir um intervalo de tempo personalizado.

Para exibir dados históricos e dados dinâmicos de consulta no console da estação de trabalho:

- Para exibir os dados dinâmicos de consulta para o intervalo de tempo maior que 8 minutos, edite a propriedade introscope.enterprisemanager.workstation.extendedLiveQuery no arquivo IntroscopeEnterpriseManager.properties no diretório <*pasta_principal_do_EM*>\config como se segue:
  introscope.enterprisemanager.workstation.extendedLiveQuery=true
  Quando essa propriedade é definida como true, você pode usar as listas suspensas Intervalo de tempo e Resolução no painel Estação de trabalho no modo Dinâmico. Essas opções permitem inserir intervalo de tempo personalizado e resolução para o modo dinâmico no lugar do intervalo de tempo padrão de 8 minutos e resolução de 15 segundos.
  É possível definir o intervalo de tempo para um período maior que o intervalo de tempo padrão de 8 minutos.
  Observação: o intervalo de tempo máximo para o qual você pode exibir dados dinâmicos é de 30 dias. Se você inserir um intervalo de tempo superior a 30 dias, o Intervalo de tempo será definido para 8 minutos por padrão. O número de pontos de dados que são exibidos no painel é igual a (intervalo de tempo/resolução). Se (intervalo de tempo/resolução) for inferior a 2, a resolução será definida para 15 segundos por padrão.

WARNING
Definir o intervalo de tempo para mais de 8 minutos pode afetar o desempenho do Enterprise Manager devido às operações de E/S de disco necessárias para buscar dados no SmartStor.

Ativar e desativar o modo dinâmico

No console da estação de trabalho, o modo dinâmico é ativado por padrão. Você pode ativar ou desativar o modo dinâmico clicando no botão Dinâmico.

Observação: quando o console estiver no modo dinâmico e a resolução for 15 segundos, a resolução que é mostrada no console (barra de ferramentas) será usada para exibir os dados dinâmicos. Quando o console estiver no modo dinâmico e a resolução for um número maior que 15 segundos, a resolução do widget será usada para exibir os dados dinâmicos.

Exibir dados históricos

Para exibir dados históricos, selecione um intervalo de tempo. Quando você seleciona um intervalo de tempo, o Introscope imediatamente mostra os dados desse intervalo, define a hora de término para a hora atual e baseia a duração na sua seleção de intervalo de tempo.

Para alternar de dados dinâmicos para histórico:

- Clique no botão Dinâmico.

Com o modo dinâmico desativado, você pode:

- Selecionar um intervalo de tempo e uma resolução nas listas suspensas.
- Digitar um intervalo de tempo personalizado
- Exibir dados históricos.

Os controles do intervalo de tempo podem ajudar a identificar a hora em que um problema ocorreu. Por exemplo, você acha que o problema ocorreu na última hora, então defina o intervalo de tempo para uma hora e observe os dados da hora atual para trás. Se o problema não for visto nesse intervalo de hora, use os controles para ir para frente ou para trás, de modo a localizar a hora em que o problema ocorreu.

Para exibir dados históricos:

1. Selecione a métrica ou o painel para o qual deseja ver os dados históricos.
2. Selecione na lista suspensa Intervalo de tempo, um intervalo de tempo para a exibição histórica.
   O Introscope mostra os dados desse intervalo usando o período que você selecionou na lista suspensa Intervalo de tempo e definindo a hora de término para a hora atual.
   Observação: se o intervalo de tempo histórico incluir um ano, um ano de quatro dígitos será obrigatório.
   Por exemplo, suponha que você selecione um intervalo de tempo às 4:06:45, com uma duração de 8 minutos — a hora de término do intervalo, portanto, será definida como 4:06:45 e a hora de início será 3:59:30.
   Observação: quando você usa o controle de intervalo de tempo para exibir dados históricos, o intervalo selecionado é aplicado a outros painéis ou métricas na mesma janela, assim como a qualquer janela nova que é aberta.
3. Agora, você pode selecionar uma resolução para ajustar a granularidade da exibição, aumentando ou diminuindo o número de pontos de dados que são exibidos.
   Cada intervalo de tempo predefinido está associado a uma resolução padrão. Normalmente, você não precisa alterar essa configuração. Alterar a resolução é útil quando você deseja ver um nível maior de detalhes ou de granularidade dos dados do que é mostrado por padrão.
   Aqui, é possível:
   – Selecionar um intervalo de tempo predefinido na lista suspensa, ou
   – Inserir um valor no campo Resolução. Digite valores numéricos, seguidos pela duração – segundos, minutos, horas ou dias. Por exemplo, "90 segundos".
4. Depois de selecionar um intervalo de tempo, você pode ajustá-lo usando os controles de intervalo de tempo.

Alertas no modo histórico não refletem o estado de alerta histórico

Os valores de alerta não são capturados em bancos de dados, de modo que se um painel no modo histórico exibir alertas, esses alertas *não* refletirão o estado histórico. Se os dados dos alertas estiverem sendo relatados no tempo presente, os alertas refletirão valores dinâmicos, não históricos.

Controles do intervalo de tempo

Você pode usar controles do intervalo de tempo para rolar em incrementos que se baseiam no intervalo de tempo selecionado.

Controle deslizante

Arraste o controle deslizante na barra de tempo para alterar o intervalo de tempo.

Setas

Clique nas setas para retroceder e avançar no tempo.

As setas simples retrocedem ou avançam em pequenos incrementos; as setas duplas retrocedem ou avançam em incrementos de tempo que são quase iguais ao tempo do intervalo selecionado.

Ícone de redefinição

Clique no ícone Redefinir para redefinir a hora de término do intervalo para a hora atual.

Ícone de bloqueio

Clicar no ícone Bloquear mantém sua resolução selecionada enquanto você seleciona intervalos de tempo diferentes ampliando os dados.

Definir um intervalo de datas personalizado

Para definir um intervalo de tempo personalizado a fim de exibir dados históricos:

1. Selecione a métrica ou o painel para o qual deseja ver os dados históricos.
2. Selecione um intervalo personalizado na lista suspensa Intervalo de tempo.
   A janela Intervalo personalizado é aberta, mostrando a data atual (Hoje) destacada com um contorno.
3. Selecione datas:
   a. Use os controles de calendário para selecionar as datas e horas de início e término.
   b. Use os controles de menu na parte superior do calendário para selecionar mês e ano, selecione a data no calendário e digite a hora no campo de hora na parte inferior do calendário.
   c. Clique em OK.

   A estação de trabalho mostra os dados para o intervalo personalizado.

Aplicar zoom em dados históricos nos gráficos

Ao exibir dados históricos em um gráfico, você pode ampliar os dados clicando com o ponteiro do mouse em uma posição no gráfico e arrastando para especificar o intervalo de tempo.

O Introscope atualiza os dados no visualizador com base na nova consulta, e o intervalo de tempo no visualizador mostra o novo intervalo.

O intervalo de tempo global na janela e o controle do Intervalo de tempo não são alterados automaticamente quando você amplia os dados. Por exemplo, se você ampliar um período de dez minutos em um gráfico com o Intervalo de tempo definido para 1 hora, o gráfico mostrará o período de dez minutos, mas o controle permanecerá em 1 hora, e a barra de tempo continuará mostrando o intervalo de hora.

É possível substituir as ações de zoom padrão das seguintes maneiras:

- Defina o intervalo de tempo global e o controle do Intervalo de tempo para corresponder à exibição com zoom: selecione Visualizador > Definir intervalo de tempo a partir do intervalo de zoom ou clique no ícone Definir intervalo de tempo a partir do intervalo de zoom.
- Bloqueie a resolução selecionada clicando no ícone Bloquear.
- Mantenha pressionada a tecla shift enquanto aplica o zoom para restringir o efeito de zoom ao eixo de tempo.

Métricas do DX APM

O DX APM exibe dados de desempenho de aplicativos, que são coletados de sistemas remotos e locais, como métricas.

Como o DX APM fornece métricas

O DX APM monitora o desempenho do aplicativo de métodos individuais, conforme vários componentes do aplicativo o executa.

1. Os probes que são inseridos no código de bytes do componente do aplicativo relatam dados aos agentes.
2. Os agentes relatam os dados ao Enterprise Manager. Outros subsistemas, como JMX e PMI, também relatam os dados que os agentes coletam.
3. O Gerenciador corporativo compila esses dados em métricas, o desempenho do aplicativo, conforme medido em vários pontos nos subsistemas do aplicativo.

   NOTE
   O Enterprise Manager registra a hora do desempenho para os eventos do sistema em um arquivo de log de desempenho, <pasta_principal_do_EM>/logs/perflog.txt. Como alternativa às métricas exibidas no Investigador, o arquivo perflog.txt pode conter informações úteis.
4. As métricas são exibidas na interface do usuário.
5. É possível exportar as métricas em um banco de dados externo.

Termos comuns

Para compreender as métricas, saiba como o DX APM usa alguns termos comuns.

Há mais termos disponíveis no Glossário do DX APM.

back-end

Um back-end é um sistema externo, como um banco de dados, um servidor de email, um sistema de processamento de transações (por exemplo, CICS ou Tuxedo) ou um sistema de mensagens (por exemplo, WebSphere MQ).

simultaneidade e invocações simultâneas

Os métodos simultâneos são métodos que começam durante um intervalo e não são finalizados durante o mesmo intervalo. Como você deseja que os métodos sejam concluídos rapidamente, um valor excepcionalmente alto para as invocações simultâneas é indesejável.

erros

Erros gerados pelo aplicativo ou sistema sendo monitorado.

eventos

Um evento é qualquer ação para a qual os agentes capturam dados, além das métricas. Exemplos de evento incluem rastreamentos de transação, erros e paralisações. Os agentes registram eventos em situações específicas, entre elas:

- Rastreamentos de transação
- Paralisações
- Erros - captura a geração e detecção de exceções e rastreia todos os locais em que foram geradas e detectadas exceções.

  NOTE
  Desative a captura de exceções em produção, pois ela pode causar uma degradação significativa no desempenho.

front-end

Um front-end é o componente de um aplicativo que primeiro manipula uma solicitação de entrada. O componente pode ser um Servlet, um JSP, um banco de dados de gerenciamento, um EJB ou algum outro componente.

coleta

Coleta é o processo em que o Introscope reúne os dados dos coletores.

interval

Um intervalo é uma fatia de tempo definida pelo usuário, usado para definir e determinar a média de métricas. No Introscope, esse período é, geralmente, de 7.5 segundos. Alguns dos sistemas monitorados capturam dados em intervalos diferentes.

resposta

A resposta sempre se refere à execução do método. A resposta é medida da seguinte forma:

- contagem - o número de transações concluídas durante o intervalo.
- tempo - o tempo levado para executar um método, em milissegundos.

Responses Per Interval é a métrica padrão de taxa de transferência do Introscope.

tempo de resposta

O tempo de resposta é o período em que executar um método que é medido da seguinte forma:

- tempo médio de resposta (ms) — o tempo médio, em milissegundos, que levou para executar o método durante o intervalo.
- tempo de resposta mínimo e máximo - o tempo de resposta mais baixo e mais alta durante o intervalo.

taxa

A taxa é o número de execuções de método por segundo ou intervalo.

paralisação

Uma paralisação é uma instância em que o tempo de invocação de um método excedeu um limite definido por um administrador.

Tipos de métrica

Os tipos de métrica incluem:

- Métricas de contagem
- Métricas de porcentagem
- Dados de sequência de caracteres

Métricas de contagem

A contagem é um número inteiro. Por exemplo, a contagem pode representar:

- O número de pontos de dados determinados como a média para calcular uma métrica.
- O número de eventos a partir de um determinado ponto no tempo
- O número de segmentos em uso

Exemplos de métricas de contagem são a contagem de erros e de paralisações.

Métricas de porcentagem

As *porcentagens* são usadas para medir o uso de um recurso em relação ao máximo de recursos disponíveis. Exemplos são:

- Utilização da CPU
- O percentual de tempo gasto em coletas de lixo nos últimos 15 minutos

Dados de sequência de caracteres

Além das medidas e do status, o Introscope coleta informações identificam os sistemas e aplicativos monitorados. Exemplos desse tipo de dado são nomes de componentes do sistema, como o nome de um banco de dados, versões do JVM ou um endereço IP.

Métricas BlamePoint

O DX APM usa cinco métricas básicas chamadas *métricas de BlamePoint*. As métricas de BlamePoint fornecem a direção inicial para que os responsáveis pela triagem identifiquem os especialistas em sistema que podem ajudar com um problema.

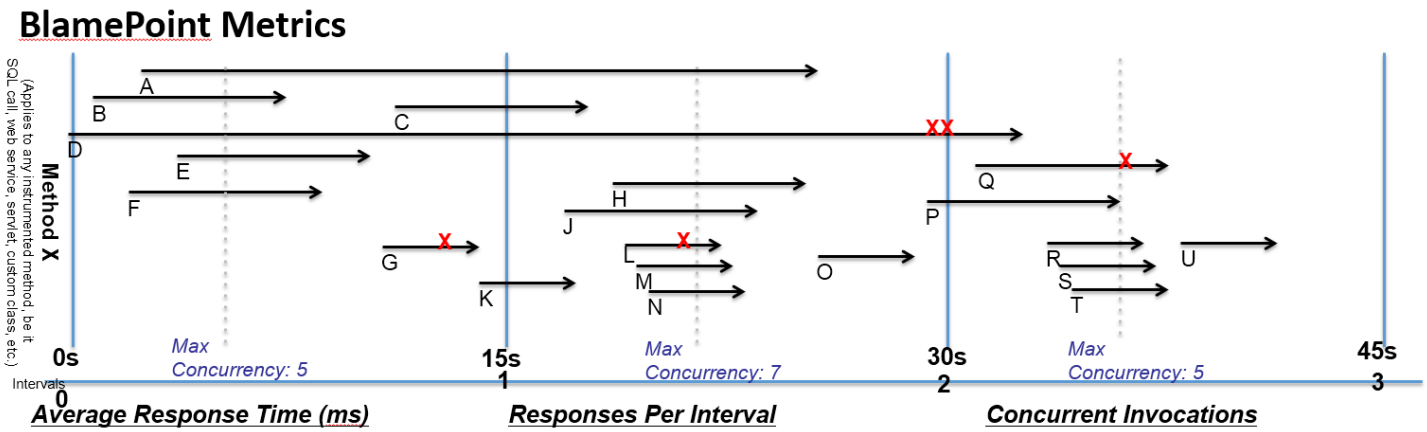
Observação: as métricas de BlamePoint também são conhecidas como métricas padrão.

O APM relata essas métricas sempre que os métodos Java são monitorados, por exemplo:

- Front-ends
- Back-ends
- SQL
- Servlets
- Serviços web (inclusive a métrica de falha SOAP)
- EJB
- JSP
- Todos os métodos/classes Java personalizados

A maioria dos métodos instrumentados relata estas cinco métricas:

A seguinte ilustração mostra como o APM relata as métricas de BlamePoint para métodos Java:

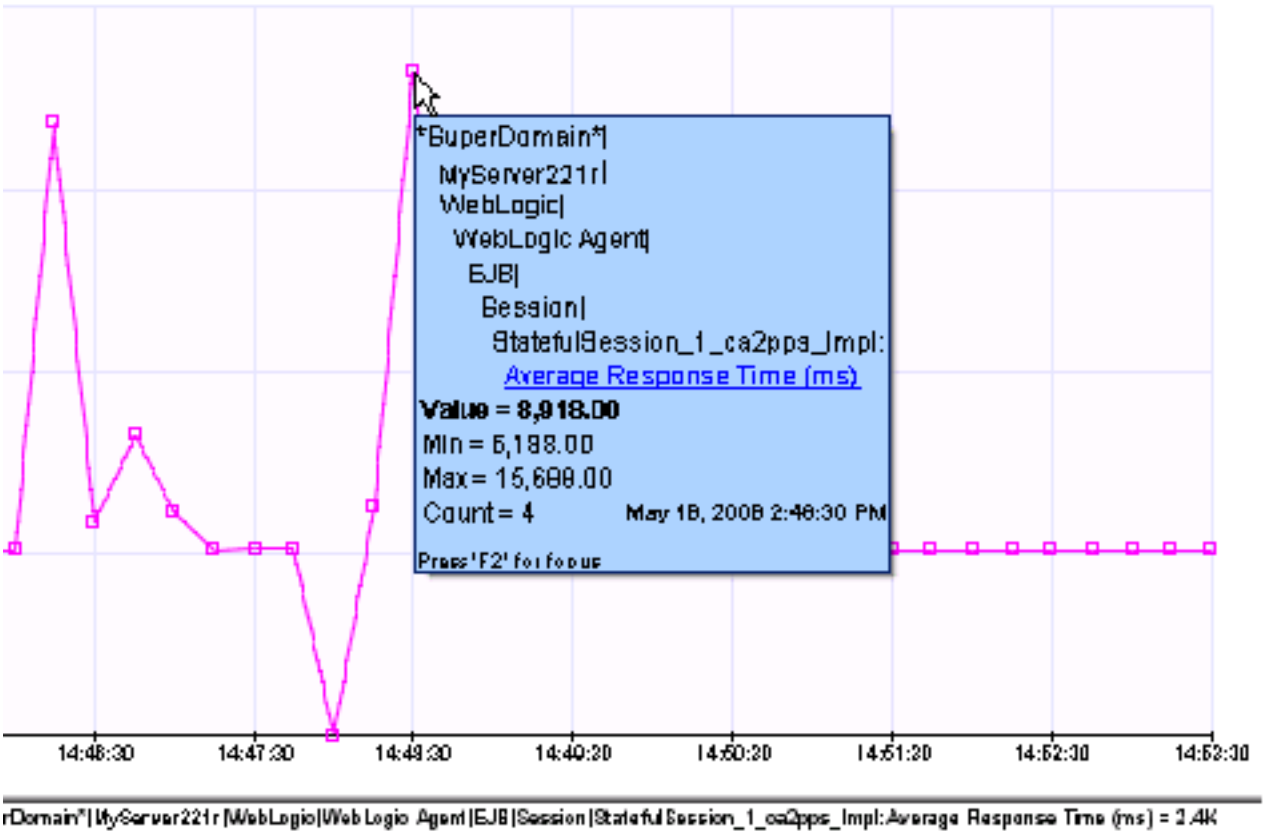


Tempo médio de resposta (ms)

A métrica Tempo médio de resposta calcula a média dos tempos de resposta de todas as solicitações que foram concluídas durante um intervalo.Tempo de resposta é o período que uma solicitação leva para ser concluída. Esse tempo fornece uma medição básica da velocidade de resposta do aplicativo, portanto:

- Tempos de resposta baixos são desejáveis.
- Tempos de resposta altos sugerem um problema.

Observação: a contagem do Tempo médio de resposta é idêntica ao valor das Respostas por intervalo.



A ilustração mostra um gráfico de Tempo médio de resposta para uma sessão EJB, conforme exibido na Estação de trabalho. Pontos a serem observados:

- Passe o mouse sobre um ponto de dados para ver uma dica de ferramenta com mais informações sobre o ponto de dados.
- No exemplo:
  - O valor do ponto de dados, 8919 ms, é o tempo médio de resposta das solicitações que são concluídas durante o intervalo.
  - A contagem, 4, significa que quatro solicitações foram concluídas durante o intervalo selecionado.
- Além do valor e da contagem, cada ponto de dados tem um mínimo e um máximo de dados.
  - Mínimo é o valor único mais baixo das solicitações que são representadas na contagem. Nesse exemplo, a solicitação que levou menos tempo para ser concluída.
  - Máximo é o valor único mais alto das solicitações que são representadas na contagem. Nesse exemplo, a solicitação que levou mais tempo para ser concluída.

Considere as seguintes informações sobre o Tempo médio de resposta:

- **Triagem usando o Tempo médio de resposta**
  Use as tendências do Tempo médio de resposta, que é combinado com alterações em outras métricas, para identificar e diagnosticar problemas.
- **Problemas consistentes**
  Quando acompanhados por uma contagem baixa de Segmento disponível, os Tempos médios de resposta consistentemente altos podem indicar os seguintes problemas:
  - Código ineficiente

- Uso excessivo do sistema externo
- Back-end lento
- Muitas camadas

- **Problemas periódicos**
  Os picos periódicos em um gráfico mostram Tempos médios de resposta altos que depois voltam ao normal.Quando acompanhados por uma Contagem de segmentos disponíveis baixa, os Tempos médios de resposta periodicamente altos podem indicar:
  - Perdas frequentes de GC
  - Afunilamento de back-end relacionado à carga

  Quando acompanhados por uma leitura baixa de Utilização da CPU, os Tempos médios de resposta periodicamente altos podem indicar:
  - Ponto de obstrução interno
- **Problemas progressivos**
  Um aumento constante no Tempo médio de resposta por um longo período, quando acompanhado por uma leitura baixa das Respostas por intervalo, pode indicar uma perda de memória.

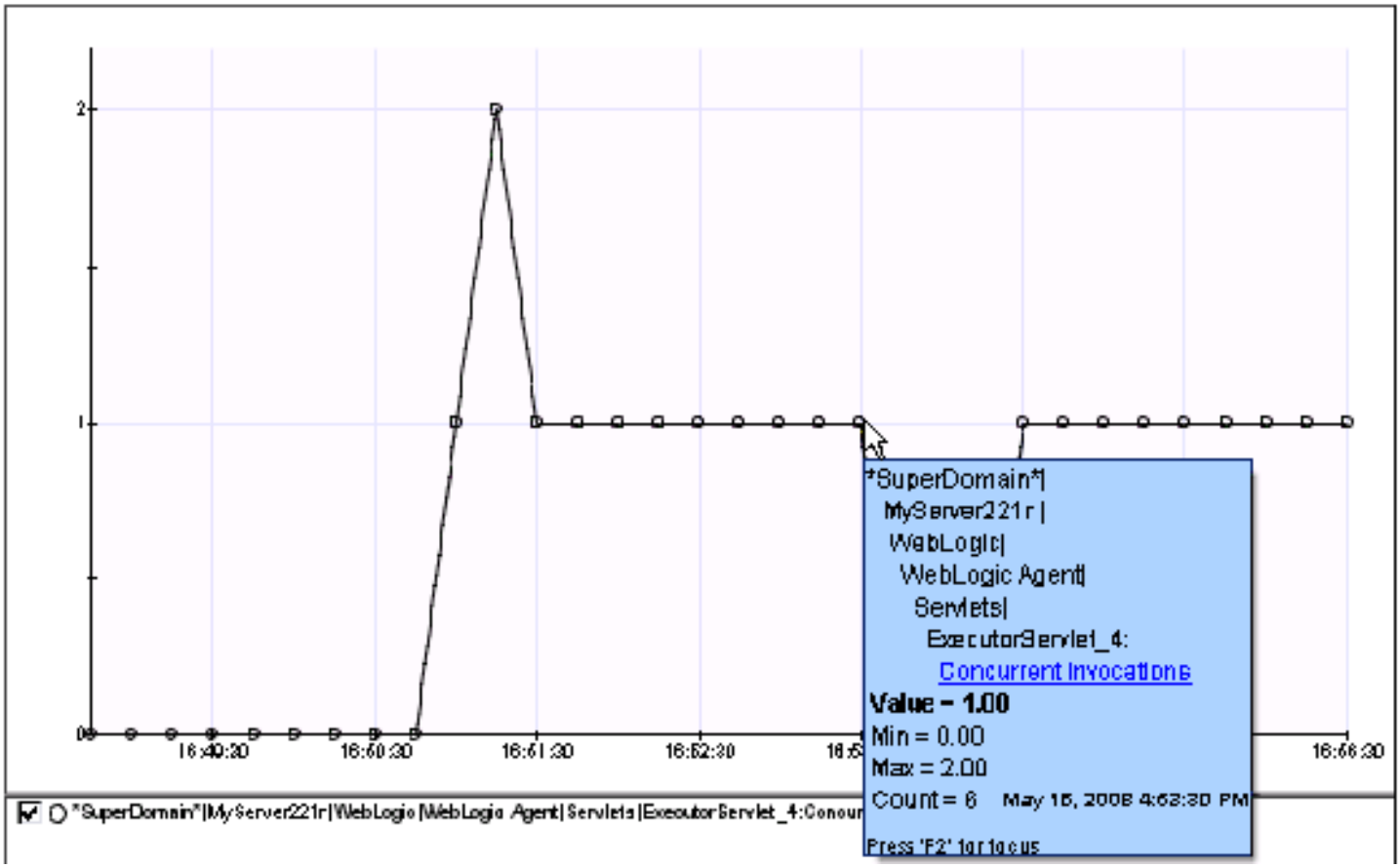
Invocações simultâneas

As invocações são solicitações tratadas pelo aplicativo e suas várias partes. As invocações simultâneas são as solicitações que são tratadas em um determinado momento.

O DX APM calcula a métrica Invocações simultâneas contando o número de solicitações que ainda estavam sendo tratadas no fim de um determinado intervalo.

- É desejável um valor baixo de Invocações simultâneas.
- Um valor alto de Invocações simultâneas sugere um problema.

As invocações simultâneas começam durante um intervalo e não são finalizadas durante o mesmo intervalo. Como você deseja que os métodos sejam concluídos rapidamente, um número excepcionalmente alto de invocações simultâneas é indesejável. Podem ocorrer picos temporários em invocações simultâneas, mas a métrica deve retornar para zero todas as vezes. Uma métrica que não retorna para zero pode indicar um afunilamento de segmentos, o número de conexões de banco de dados ou algum outro recurso compartilhado.



Na ilustração, o valor 1 indica que uma solicitação ainda estava sendo tratada no final do intervalo selecionado.As solicitações que ainda estiverem em andamento no fechamento do intervalo selecionado provavelmente serão concluídas durante os intervalos subsequentes. Essas solicitações que não são concluídas antes dos fins dos limites especificados são chamadas de paralisações (consulte Contagem de paralisações).

Considere as seguintes informações sobre as invocações simultâneas:

- **Triagem usando invocações simultâneas**
  Use as tendências das Invocações simultâneas, que são combinadas com alterações em outras métricas, para identificar e diagnosticar problemas.
- **Problemas consistentes**
  Os valores consistentemente altos de Invocação simultânea podem indicar os seguintes problemas: Uso excessivo do sistema externo, Back-end lento
  Quando acompanhados por uma leitura baixa de Respostas por intervalo, valores consistentemente altos de Invocação simultânea podem indicar:
  - Código ineficiente
  - Muitas camadas
- **Problemas periódicos**
  Valores periodicamente altos de Invocação simultânea são mostrados em um gráfico com picos periódicos que depois retornam ao normal. Esse pico pode indicar um afunilamento de back-end relacionado à carga.
  Quando acompanhados por uma leitura baixa de Conexões disponíveis, os valores periodicamente altos de Invocação simultânea podem indicar vazamentos frequentes do lixo coletado.
  Quando acompanhados por uma leitura baixa de Contagem de segmentos disponíveis, valores periodicamente altos de Invocação simultânea podem indicar um ponto de obstrução interno.
- **Problemas progressivos**

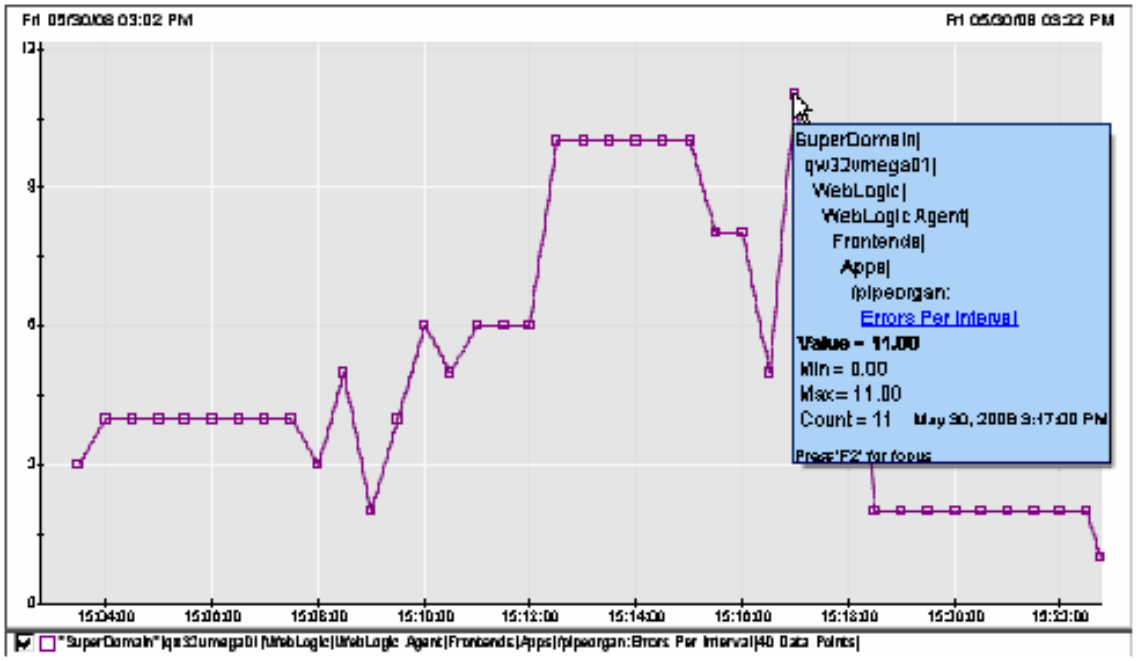
Um aumento constante nas Invocações simultâneas por um longo período, especialmente quando acompanhado por uma leitura baixa de Respostas por intervalo, pode indicar uma perda de segmento.

Erros por intervalo

Os erros são o número de exceções reportadas pelos códigos de erro JVM e HTTP. Os exemplos de erros incluem:

- O status 404 Página não encontrada relatado pelo servidor HTTP
- Uma exceção SQL
- Uma exceção Java

É desejável uma contagem de erros baixa.



A métrica é uma contagem simples de erros que são relatados durante o intervalo. A ilustração mostra um ponto de dados selecionado com um valor de 11, o que significa que 11 erros foram relatados durante essa fração de tempo. Como essa métrica é uma contagem simples, o valor e o valor máximo são sempre iguais.

O caminho da métrica abaixo do gráfico identifica o aplicativo que está relatando a exceção. Para encontrar mais informações sobre os erros que são mostrados em um gráfico, analise os logs do aplicativo.

Em sistemas com o ErrorDetector ativado, os erros também geram instantâneos de erro. Os instantâneos de erro fornecem detalhes sobre o que estava acontecendo quando um erro ocorreu. Essas informações são armazenadas no banco de dados Eventos de transação. Um grande número de erros gera uma grande quantidade de informações documentais. Evitar essas informações é outro motivo para minimizar erros.

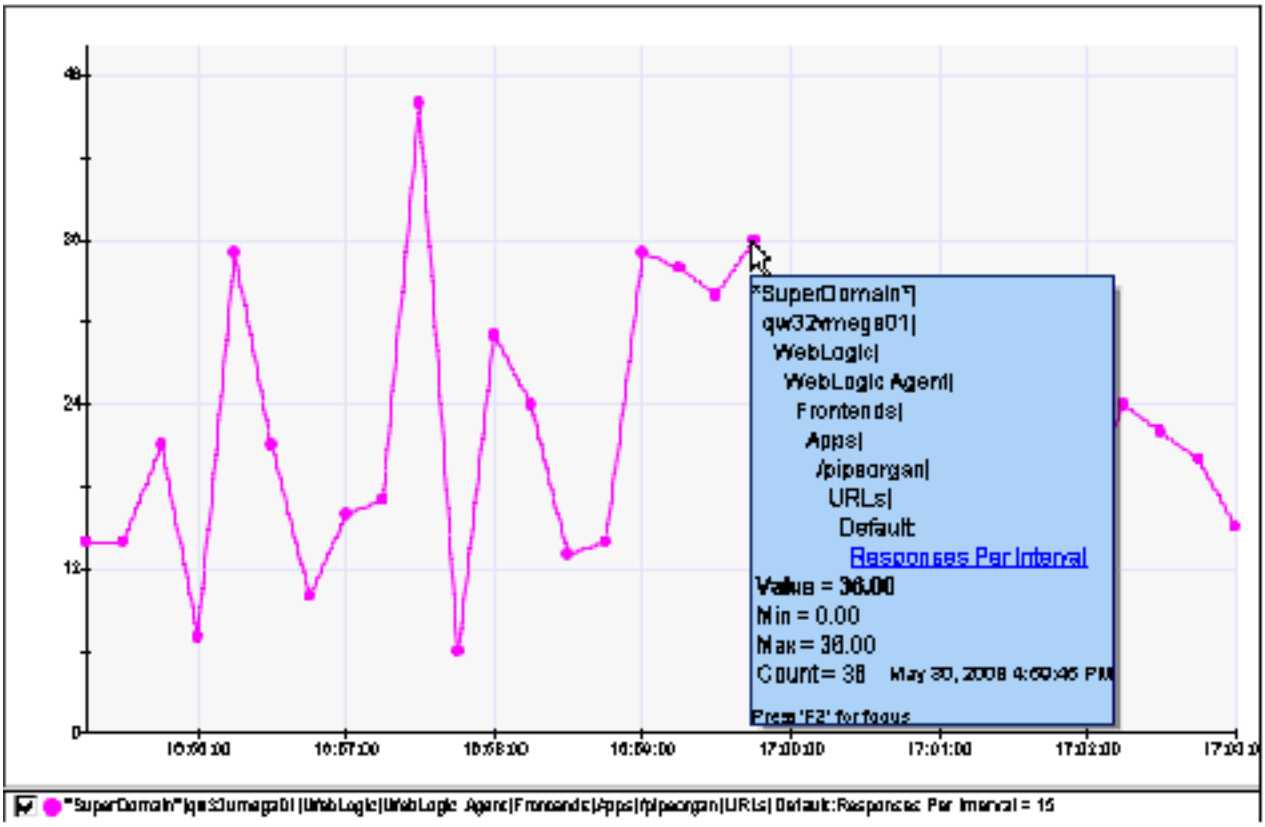
Respostas por intervalo

As Respostas por intervalo refletem o número de invocações concluídas nesse intervalo. Essa métrica é uma medida da taxa de transferência de dados e, portanto, do desempenho do aplicativo.A métrica é uma contagem simples de solicitações que são concluídas durante um intervalo.

- O valor da métrica Respostas por intervalo é sempre o mesmo da contagem para a métrica Tempo médio de resposta.
- As Respostas por intervalo são uma métrica do tipo IntCounter. Essa métrica não é uma média do número de respostas; ela é sempre o valor máximo do número de respostas durante o intervalo.

De modo geral:

- Um número alto é desejável.
- Um número baixo é indesejável.
- Um pico inesperado nas respostas pode indicar uso excessivo do sistema externo, como um ataque de negação de serviço em um site.



Na ilustração, a dica de ferramenta mostra o valor do ponto de dados selecionado. Como essa métrica é uma contagem simples, o valor e o valor máximo da métrica são sempre iguais.

Considere as seguintes informações sobre as Respostas por intervalo:

- **Triagem com Respostas por intervalo**
  Use as tendências de Respostas por intervalo, que são combinadas com alterações em outras métricas, para identificar e diagnosticar problemas.
- **Problemas consistentes**
  Valores consistentemente altos de Respostas por intervalo podem indicar um uso excessivo do sistema externo.

Contagem de paralisações

As solicitações paralisadas são aquelas que não foram concluídas dentro de um limite de tempo especificado. (O limite padrão de paralisação é de 30 segundos.) Quando a execução da solicitação ultrapassa o limite de paralisação, a solicitação é contada como paralisada.

- Uma contagem baixa é desejável.
- Uma contagem alta é indesejável.

As paralisações podem representar qualquer um dos casos a seguir. Pode haver outros motivos para uma paralisação, mas esses casos são mais comuns.

- **Um segmento em um loop infinito**
  Às vezes, os programadores escrevem código no qual um loop que deve ser encerrado, normalmente, não é. Quando um segmento entra em um loop infinito, os componentes que o chamam têm um aumento na respectiva Contagem de paralisações. Os loops infinitos têm a característica adicional de ocupar um núcleo de CPU. Por exemplo, em um sistema silencioso com quatro núcleos, se um segmento entrar em um loop infinito, a utilização total da CPU poderá aumentar em aproximadamente 25%. Se um segundo segmento entrar no loop infinito, a utilização da CPU deverá aumentar para 50%, e assim por diante.
- **Um segmento que aguarda um longo tempo ou um segmento que nunca atingirá o tempo limite**
  Quando um segmento tenta abrir um recurso como um soquete para um sistema remoto, o programador pode especificar que ele seja interrompido após um determinado número de segundos. Se esse período for suficiente, por exemplo, cinco minutos, a Contagem de paralisações irá aumentar e permanecer incrementada pelos cinco minutos. Às vezes, não há tempo limite para tentativas de conexão, casos em que o segmento permanece ocupado e a Contagem de paralisações nunca diminui.
  Em muitos sistemas, há segmentos que são bloqueados dessa maneira por motivos de rotina. Isso porque, às vezes, a Contagem de paralisações pode ser diferente de zero para um componente, mesmo quando o sistema está ocioso. Preste atenção à contagem "natural" de segmentos e discorde apenas com as alterações anormais.
- **Um segmento que é envolvido em uma paralisação ou livelock**
  Os programadores usam bloqueios para garantir que os dados não sejam corrompidos. Às vezes, os bloqueios podem ser obtidos na ordem incorreta, caso em que o programa pode desenvolver o que conhecemos como paralisação. Uma paralisação significa que dois ou mais segmentos estão presos aguardando o avanço um do outro. Os segmentos não podem avançar sem recursos que os outros segmentos já reservaram. As paralisações são falhas de sistemas catastróficas em quase todos os casos. Os despejos de segmento, muitas vezes, são a técnica mais útil para identificar o código desfeito. Um livelock é uma paralisação na qual um ou mais segmentos usam intensivamente a CPU. As paralisações são diferentes dos loops infinitos na medida em que o loop infinito é apenas o resultado de uma condição desfeita para um loop, enquanto a paralisação envolve a semântica de bloqueio, ou código "sincronizado", do aplicativo no qual ele ocorre.

Observação: as informações sobre os eventos de paralisação são armazenadas no banco de dados Eventos de transação.

Considere as seguintes informações sobre a Contagem de paralisações:

- **Medida da contagem de paralisações**
  O Rastreamento de transação pode mostrar várias solicitações que não foram concluídas durante o limite de tempo especificado (paralisações), mas o Investigar exibe um número diferente como a Contagem de paralisações.
  Esse número ocorre porque a Contagem de paralisações é registrada como um valor pontual (em dado momento durante um intervalo) e não como um valor de intervalo (por um período). Pode haver vários valores de paralisação representando transações longas que são concluídas durante um intervalo, mas apenas a contagem disponível durante um único momento é usada como o ponto de dados.
- **Triagem com Contagem de paralisações**
  Use as tendências de Contagem de paralisações, combinadas com alterações em outras métricas, para identificar e diagnosticar problemas.
- **Problemas consistentes**
  Valores consistentemente altos de Contagem de paralisações podem indicar um sistema back-end lento.
- **Problemas periódicos**
  Valores periodicamente altos de Contagem de paralisações podem indicar um afunilamento de back-end relacionado à carga.
- **Problemas progressivos**
  Um aumento constante nos valores de Contagem de paralisações por um longo período, especialmente quando acompanhado por uma contagem baixa de Segmentos disponíveis, pode indicar uma perda de recurso - segmentos.

Métricas JMX

As seguintes métricas estão disponíveis na Árvore do investigador sob o nó JMX no formato: JMX\|(.*)\|(Type=)?<*Nome do MBean*>:<*Nome do atributo*>.

- **ServerRuntime: OpenSocketsCurrentCount**
  O número atual de soquetes abertos no servidor.
- **ServerRuntime: SocketsOpenedTotalCount**
  O número total de soquetes que foram abertos no servidor.
- **ExecuteQueueRuntime: ExecuteThreadCurrentIdleCount**
  O número de segmentos ociosos que são atribuídos à fila.
- **ExecuteQueueRuntime: PendingRequestCurrentCount**
  O número de solicitações aguardando na fila.
- **ExecuteQueueRuntime: ServicedRequestTotalCount**
  O número de solicitações processadas por essa fila.
- **JDBCDataSourceRuntime: ActiveConnectionsCurrentCount**
  O número de conexões JDBC atualmente em uso nessa origem de dados.
- **JDBCDataSourceRuntime: ConnectionsTotalCount**
  O número total de conexões JDBC criadas nessa origem de dados desde a hora em que ela foi implantada.
- **JDBCDataSourceRuntime: LeakedConnectionCount**
  O número de conexões JDBC que vazaram.
- **JDBCDataSourceRuntime: WaitingForConnectionCurrentCount**
  O número de solicitações de conexão aguardando uma conexão JDBC.
- **JDBCDataSourceRuntime: NumAvailable**
  O número de conexões JDBC que estão disponíveis no momento nessa origem de dados.
- **EJBCacheRuntime: ActivationCount**
  O número total de beans desse EJB Home que foram ativados.
- **EJBCacheRuntime: CacheAccessCount**
  O número total de tentativas de acessar um bean desse cache.
- **EJBCacheRuntime: CachedBeansCurrentCount**
  O número atual de beans desse EJB Home que estão no cache do EJB.
- **EJBCacheRuntime: CacheHitCount**
  O número de tentativas de acessar o cache que foram bem-sucedidas.
- **EJBLockingRuntime: TimeoutTotalCount**
  Número total de segmentos que atingiram o tempo limite aguardando um bloqueio em um bean.
- **EJBPoolRuntime: BeansInUseCount**
  O número de instâncias de bean nesse pool que estão sendo usadas no momento.
- **EJBPoolRuntime: IdleBeansCount**
  O número de instâncias de bean nesse pool que estão livres no momento.
- **EJBPoolRuntime: TimeoutTotalCount**
  Número total de segmentos que atingiram o tempo limite aguardando um bean disponível desse pool.
- **EJBPoolRuntime: WaiterCurrentCount**
  Fornece uma contagem do número de segmentos que atualmente estão aguardando uma instância de bean disponível do pool livre.
- **EJBTransactionRuntime: TransactionCommittedTotalCount**
  O número total de transações que foram confirmadas para esse EJB.
- **JMSRuntime: ConnectionsTotalCount**
  O número total de conexões JMS feitas com esse WebLogic Server após a última redefinição.
- **JMSRuntime: JMSServersCurrentCount**

O número total de servidores JMS implantados nessa instância do WebLogic Server.

- **JMSPooledConnectionRuntime: NumAvailable**
  O número de sessões JMS disponíveis no pool que não estão sendo usadas no momento.
- **JMSDestinationRuntime: BytesReceivedCount**
  O número de bytes recebidos nesse destino após a última redefinição.
- **JMSDestinationRuntime: ConsumersTotalCount**
  O número total de consumidores que acessaram esse destino após a última redefinição.
- **JMSDestinationRuntime: MessagesReceivedCount**
  O número de mensagens recebidas nesse destino após a última redefinição.
- **JMSDestinationRuntime: BytesCurrentCount**
  O número atual de bytes armazenados no destino.
- **JMSDestinationRuntime: ConsumersCurrentCount**
  O número atual de consumidores acessando esse destino.
- **JMSDestinationRuntime: MessagesCurrentCount**
  O número atual de mensagens no destino.
- **JMSDurableSubscriberRuntime: MessagesReceivedCount**
  O número de mensagens que esse assinante durável recebe após a última redefinição.
- **JMSDurableSubscriberRuntime: BytesCurrentCount**
  O número de bytes que esse assinante durável recebe.
- **JMSDurableSubscriberRuntime: MessagesCurrentCount**
  O número de mensagens ainda disponível por esse assinante durável.
- **JMSServerRuntime: BytesReceivedCount**
  O número total de bytes que esse servidor JMS recebe após a última redefinição.
- **JMSServerRuntime: BytesCurrentCount**
  O número atual de bytes armazenados nesse servidor JMS.
- **JMSConnectionRuntime: SessionsCurrentCount**
  O número atual de sessões para essa conexão.
- **TransactionNameRuntime: TransactionAbandonedTotalCount**
  O número total de transações que foram abandonadas após a última redefinição.
- **TransactionNameRuntime: TransactionCommittedTotalCount**
  O número total de transações que foram confirmadas após a última redefinição.
- **TransactionNameRuntime: TransactionHeuristicsTotalCount**
  O número total de transações que foram concluídos com um status heurístico após a última redefinição.
- **TransactionNameRuntime: TransactionRolledBackTotalCount**
  O número total de transações que foram revertidas após a última redefinição.
- **TransactionNameRuntime: TransactionRolledBackTimeoutTotalCount**
  O número total de transações que foram revertidas devido a uma experiência de tempo limite após a última redefinição.
- **TransactionNameRuntime: TransactionTotalCount**
  O número total de transações processadas (confirmadas/revertidas/heurística) desde a última redefinição.
- **TransactionResourceRuntime: TransactionCommittedTotalCount**
  O número total de transações que foram confirmadas desde a última redefinição.
- **TransactionResourceRuntime: TransactionHeuristicsTotalCount**
  O número total de transações que foram concluídas com um status heurístico desde a última redefinição.
- **TransactionResourceRuntime: TransactionRolledBackTotalCount**
  O número total de transações que foram revertidas desde a última redefinição.
- **TransactionResourceRuntime: TransactionRolledBackTimeoutTotalCount**
  O número total de transações que foram revertidas devido a uma experiência de tempo limite desde a última redefinição.
- **TransactionResourceRuntime: TransactionTotalCount**

O número total de transações processadas (confirmadas/revertidas/heurística) desde a última redefinição.
- **JTARuntime: TransactionAbandonedTotalCount**
  O número total de transações que foram abandonadas desde a última redefinição.
- **JTARuntime: TransactionCommittedTotalCount**
  O número total de transações que foram confirmadas desde a última redefinição.
- **JTARuntime: TransactionHeuristicsTotalCount**
  O número total de transações que foram concluídas com um status heurístico desde a última redefinição.
- **JTARuntime: TransactionRolledBackTotalCount**
  O número total de transações que foram revertidas desde a última redefinição.
- **JTARuntime: TransactionRolledBackTimeoutTotalCount**
  O número total de transações que foram revertidas devido a uma experiência de tempo limite desde a última redefinição.
- **JTARuntime: TransactionTotalCount**
  O número total de transações processadas (confirmadas/revertidas/heurística) desde a última redefinição.
- **Server: IdleConnectionTimeout**
  O valor atual do tempo limite da Sessão HTTP.

Métricas agregadas JMX

As seguintes métricas estão disponíveis na Árvore do investigador no nó WebLogic, JMX Aggregate:

- **Thread Pool: Waiting Request Count**
  Fornece uma contagem do número total de segmentos que atualmente estão solicitando uma instância disponível do pool livre.
- **JDBC Connection Pool: Waiting Thread Count**
  Fornece uma contagem do número total de segmentos que atualmente estão aguardando uma instância de conexão disponível do pool livre.
- **EJB Pool: Waiting Thread Count**
  Fornece uma contagem do número total de segmentos que atualmente estão aguardando uma instância de bean disponível do pool livre.

Métricas de transação

As métricas de transação medem uma parte específica de uma transação. Dependendo da arquitetura do seu sistema, as seguintes métricas Java podem aparecer no Investigador. A maioria aparece na árvore de métricas.

O agente do Java também relata o contexto do aplicativo Java como atributos de tempo de execução para eixos da Team Center. O conjunto de atributos que o agente do Java reporta são os atributos comuns, que existem para a maioria dos componentes. O DX APM coleta automaticamente os atributos comuns.Você pode criar as suas próprias perspectivas usando os atributos Java.

> **NOTE**
> Algumas dessas métricas, como Banco de dados e XML, aplicam-se também ao agente do NET.

EJB

Onde os EJBs (Enterprise JavaBeans) fizerem parte da arquitetura, eles poderão ser dos seguintes tipos:

- Bean de entidade do EJB
- Bean de sessão do EJB
- Bean orientado a mensagens do EJB

Para cada um desses tipos, as duas métricas seguintes são exibidas:

- Average Method Invocation Time (ms)
- Method Invocations Per Interval

Para cada método ou classe EJB que aparece como nó filho em tipos do EJB, o Gerenciador corporativo relata as cinco métricas BlamePoint:

- Tempo médio de resposta (ms)
- Invocações simultâneas
- Erros por intervalo
- Respostas por intervalo
- Contagem de paralisações

Servlets

O nó Servlets geralmente exibe as cinco métricas básicas BlamePoint para cada servlet invocado pelo aplicativo monitorado:

- Tempo médio de resposta (ms)
- Invocações simultâneas
- Erros por intervalo
- Respostas por intervalo
- Contagem de paralisações

O nó Servlets também exibe estas métricas relacionadas à CPU:

> **NOTE**
> Essas métricas relacionadas à CPU não são suportadas para servlets assíncronos.

- Average Block Time (ms)
  O tempo decorrido aproximado em milissegundos que um segmento esteve no estado BLOCKED quando a JVM oferece suporte ao monitoramento de contenção de segmento.
- Average Bytes Allocated
  O número aproximado de bytes alocados para a memória heap do segmento de transação quando a JVM oferece suporte à medição da alocação de memória do segmento.

  > **NOTE**
  >
  > JVMs da IBM não oferecem suporte a essa métrica.
- Average System CPU Time (ms)
  O tempo gasto executando código no kernel do sistema operacional em uma transação de aplicativo monitorado quando a JVM oferece suporte à medição de tempo de CPU.
- Average User CPU Time (ms)
  Quantidade de tempo que o processador gastou executando o código do programa ou o código em bibliotecas para uma transação quando a JVM oferece suporte à mediação do tempo de CPU.
- Average Wait Time (ms)
  O tempo decorrido aproximado em milissegundos que um segmento de transação esteve no estado WAITING ou TIMED_WAITING quando a JVM oferece suporte ao monitoramento de contenção de segmento.

JSP (JavaServer Pages)

Tempo médio de resposta (ms)

O tempo médio de resposta dos métodos `_jspService()` de todas as JSPs em execução na JVM. O cálculo desse valor é obtido pela média dos tempos de resposta de todas as JSPs individuais.

Respostas por intervalo

O número de invocações concluídas dos métodos `_jspService` de todas as JSPs em execução na JVM nos últimos 15 segundos.

Tempo médio de resposta (ms) pelo nome da classe

Tempo médio de resposta em milissegundos da JSP identificada pelo nome da classe. Para chegar a esse valor, são calculados o tempo e a média de cada invocação do método `_jspService()` .

Respostas por intervalo

O número de invocações concluídas do método `_jspService()` da JSP identificada pelo nome da classe no intervalo mais recente de 15 segundos.

Respostas por segundo

Taxa na qual os métodos `_jspService()` de todas as JSPs em execução na JVM estão sendo concluídos.

Respostas por segundo pelo nome da classe

Taxa na qual as invocações do método `_jspService()` da JSP identificada por um determinado nome de classe estão sendo concluídas.

Métodos paralisados por nome da classe e por nome do método

O número de JSPs que estão demorando mais do que um limite definido para concluir a execução do método `_jspService()` .

Invocações simultâneas

O número de segmentos que estão executando o método `_jspService()` .

Bibliotecas de marcas JSP (JSP TagLib)

As bibliotecas de marcas são conjuntos de marcas personalizadas usadas em páginas JSP para invocar ações personalizadas. A especificação de JSP fornece seis ações padrão. Uma ação personalizada é qualquer ação que não esteja incluída no conjunto de seis ações padrão. Os exemplos de tarefas que as ações personalizadas invocam são controle de formulário, acesso a sistemas externos, como bancos de dados e email, e controle de fluxo.

As seguintes métricas estão disponíveis para bibliotecas de marcas JSP:

- Average Method Invocation Time (ms)
- Method Invocations Per Interval
- Average Method Invocation Time (ms) by class name and method name
- Method Invocations Per Interval by class name
- Method Invocations Per Interval by class name and method name
- Method Invocations Per Second
- Method Invocations Per Second by class name
- Method Invocations Per Second by class name and method name
- Concurrent Method Invocations
- Concurrent Method Invocations by class name
- Concurrent Method Invocations by class name and method name
- Stalled Methods over 30 seconds by class name and method name
- Average Method Invocation Time (ms)

TagLibrary de E/S JSP

- Warning Count
- Exception Count

RMI (Remote Method Invocations - Invocações de método remoto)

As invocações de método remoto são invocações de métodos de objetos Java distribuídos, que são objetos Java que podem existir em mais de um host.

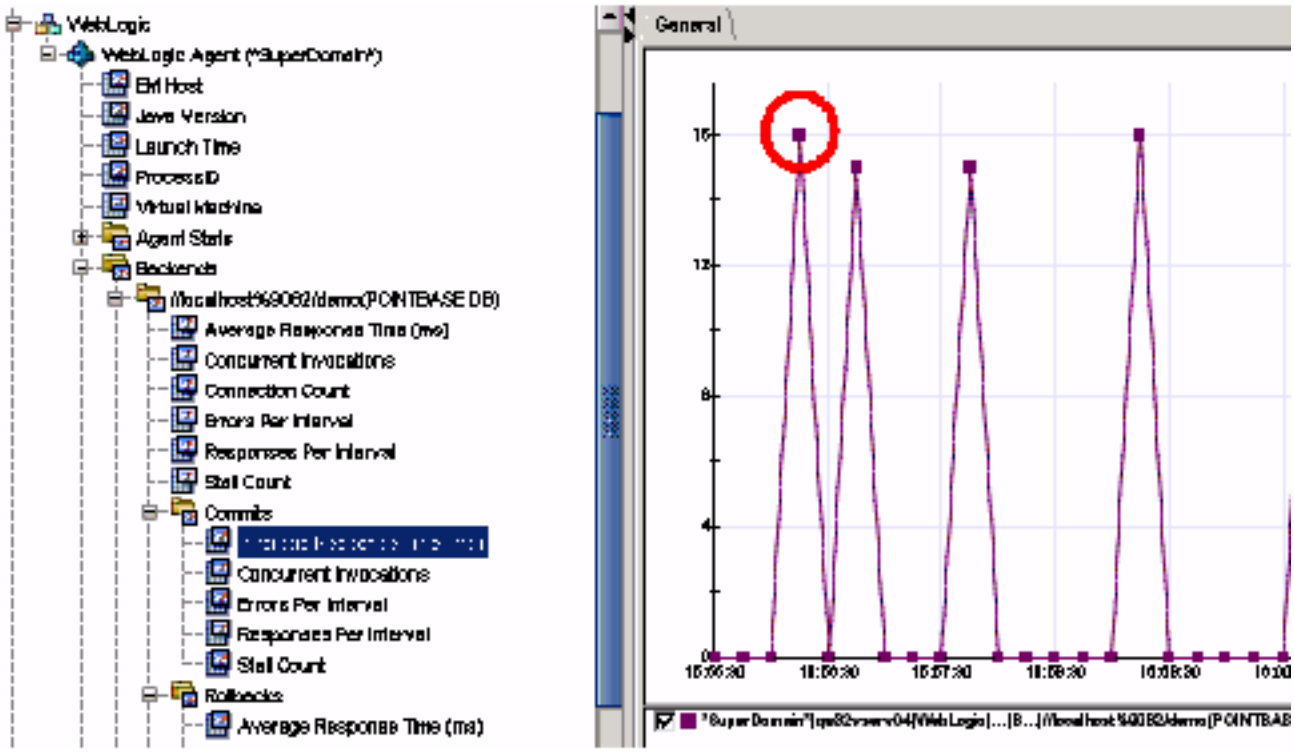
As métricas a seguir estão disponíveis para clientes e servidores RMI.

- Average Method Invocation Time (ms)
- Method Invocations Per Interval
- Average Method Invocation Time (ms) by class name
- Method Invocations Per Interval by class name
- Method Invocations Per Second
- Method Invocations Per Second by class name
- Stalled Methods over 30 seconds
- Concurrent Method Invocations
- Concurrent Method Invocations by class name

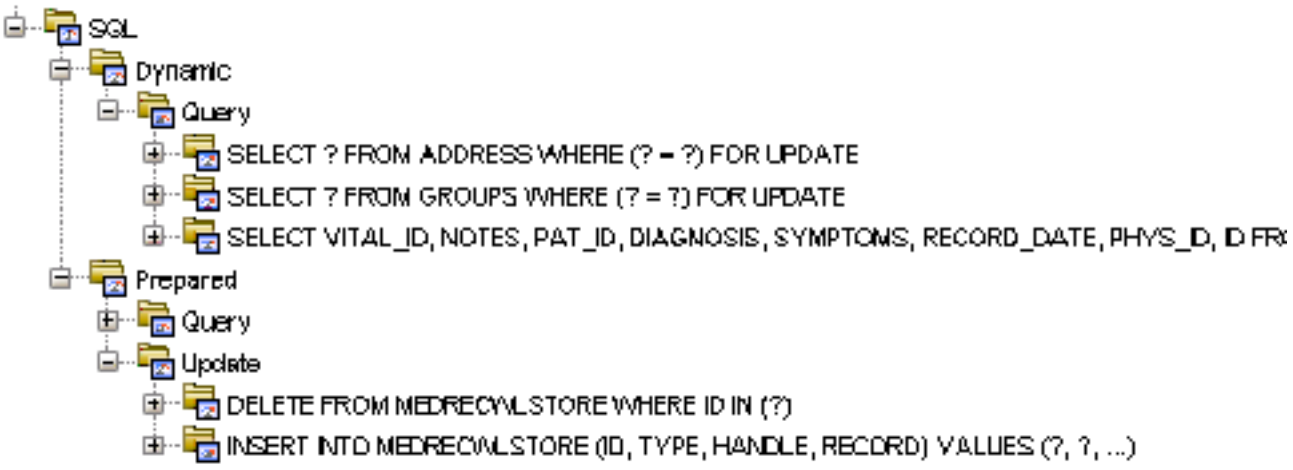
Métricas de banco de dados (SQL)

Cada back-end do banco de dados pode ser configurado para relatar as seguintes métricas:

- Commits: cada transação concluída de consulta e resposta é conhecida como uma *commit*. As cinco métricas padrão são coletadas e exibidas para todas as transações que foram confirmadas em um determinado intervalo. Por exemplo, na captura de tela abaixo, o ponto de dados circulado mostra o tempo médio de resposta para todas as transações de banco de dados confirmadas no intervalo.



- Rollbacks: uma reversão é uma transação concluída de consulta e resposta que não foi bem-sucedida. As cinco métricas padrão são coletadas e exibidas para todas as transações revertidas em um determinado intervalo.
- SQL:



Para cada uma das instruções que o banco de dados processa durante um intervalo, o agente relata estas seis métricas:

- Tempo médio de resposta (ms)
- Invocações simultâneas
- Erros por intervalo
- Contagem de objetos da conexão ativa
- Respostas por intervalo
- Contagem de paralisações

Pontos a serem observados:

- As instruções são separadas por subnó, dependendo de elas estarem no nó Prepared ou Dynamic.
- Cada tipo de instrução SQL, como GRANT, UPDATE, QUERY, REVOKE, DROP, é listado sob um subnó para o tipo de instrução em questão.

Back-ends automáticos

As métricas de back-end automático têm um caminho de métrica ligeiramente diferente das métricas de back-end padrão**.**

Back-ends|<*Pacote Java*>|<*nome da classe* > |<*método* >

Por exemplo: Backends|com.mysql.jdbc|MysqlIO|sendCommand

As métricas de resumo entre diferentes back-ends no mesmo pacote Java aparecem aqui:

Backends|<*Pacote Java*>

Por exemplo: Backends|com.mysql.jdbc

O Introscope relata métricas de suportabilidade de back-end automático.

XML (Extensible Markup Language)

As métricas XML podem ser dos tipos a seguir.

SAX

- SAX:Average Method Invocation Time (ms)
- SAX:Method Invocations Per Interval
- SAX:Average Method Invocation Time (ms) by class name
- SAX:Method Invocations Per Interval by class name
- SAX:Method Invocations Per Second
- SAX:Method Invocations Per Second by class name
- SAX:Stalled Methods over 30 seconds by class name and method name
- SAX:Concurrent Method Invocations
- SAX:Concurrent Method Invocations by class name

XSLT

- XSLT:Average Method Invocation Time (ms)
- XSLT:Method Invocations Per Interval
- XSLT:Average Method Invocation Time (ms) by class name
- XSLT:Method Invocations Per Interval by class name
- XSLT:Method Invocations Per Second
- XSLT:Method Invocations Per Second by class name
- XSLT:Stalled Methods over 30 seconds by class name and method name
- XSLT:Concurrent Method Invocations
- XSLT:Concurrent Method Invocations by class name

JAXM

- JAXM|Listener:Average Method Invocation Time (ms)
- JAXM|Listener:Method Invocations Per Interval
- JAXM|Listener:Average Method Invocation Time (ms) by class name
- JAXM|Listener:Method Invocations Per Interval by class name
- JAXM|Listener:Method Invocations Per Second
- JAXM|Listener:Method Invocations Per Second by class name
- JAXM|Listener: Stalled Methods over 30 seconds by class name and method name
- JAXM|Listener:Concurrent Method Invocations
- JAXM|Listener:Concurrent Method Invocations by class name

Conector J2EE

- Average Method Invocation Time (ms)
- Method Invocations Per Interval
- Average Method Invocation Time (ms) by class name
- Method Invocations Per Interval
- Method Invocations Per Second
- Method Invocations Per Second by class name
- Stalled Method count over 30 seconds by class name and method name
- Concurrent Method Invocations
- Concurrent Method Invocations by class name

JTA (Java Transaction API)

- Average Method Invocation Time (ms)
- Method Invocations Per Interval
- Average Method Invocation Time (ms) by class name
- Method Invocations Per Interval by class name
- Method Invocations Per Second
- Method Invocations Per Second by class name
- Stalled Methods over 30 seconds by class name and method name
- Concurrent Method Invocations

JNDI (Java Naming and Directory Interface)

As métricas JNDI incluem:

- JNDI lookup
- JNDI lookupLink
- JNDI search
- Métricas chamadas pela JNDI

JNDI Lookup

- Lookup:Context Average Method Invocation Time (ms)
- Lookup:Context Method Invocations Per Interval
- Lookup:Context Average Method Invocation Time (ms) by class name
- Lookup:Context Method Invocations Per Interval by class name
- Lookup:Context Method Invocations Per Second
- Lookup:Context Method Invocations Per Second by class name
- Lookup:Context Stalled Methods over 30 seconds by class name and method name
- Lookup:Context Concurrent Method Invocations
- Lookup:Context Concurrent Method Invocations by class name

JNDI lookupLink

- lookupLink:Context Average Method Invocation Time (ms)
- lookupLink:Context Method Invocations Per Interval
- lookupLink:Context Average Method Invocation Time (ms) by class name
- lookupLink:Context Method Invocations Per Interval by class name
- lookupLink:Context Method Invocations Per Second
- lookupLink:Context Method Invocations Per Second by class name
- lookupLink:Context Stalled Methods over 30 seconds by class name and method name
- lookupLink:Context Concurrent Method Invocations
- lookupLink:Context Concurrent Method Invocations by class name

JNDI Search

- Search:Context Average Method Invocation Time (ms)
- Search:Context Method Invocations Per Interval
- Search:Context Average Method Invocation Time (ms) by class name
- Search:Context Method Invocations Per Interval by class name
- Search:Context Method Invocations Per Second
- Search:Context Method Invocations Per Second by class name
- Search:Context Stalled Methods over 30 seconds by class name and method name
- Search:Context Concurrent Method Invocations
- Search:Context Concurrent Method Invocations by class name

Métricas chamadas pela JNDI

- File system I/O

JMS (Java Messaging Service)

O JMS tem quatro subnós:

- message listener
- message consumer
- topic publisher
- queue sender

As seguintes métricas podem aparecer sob qualquer um dos subnós:

- Average Method Invocation Time (ms)
- Method Invocations Per Interval
- Average Method Invocation Time (ms) by class name
- Method Invocations Per Interval by class name
- Method Invocations Per Second
- Method Invocations Per Second by class name
- Stalled Methods over 30 seconds by class name and method name
- Concurrent Method Invocations
- Concurrent Method Invocations by class name

Para APIs síncronas de recebimento do JMS, as seguintes métricas são relatadas sob o nó do investigador Frontends:

- Messages Received Per Interval
- Errors Per Interval
- Estimated Message Processing Time (ms)

Os valores das métricas individuais `{queuename}` e `{topicname}` são agregados respectivamente nos valores dos nós Filas e Tópicos.

Messages Received Per Interval

A métrica Messages Received Per Interval aumenta em um toda vez que o método `receive()` é concluído com êxito com um valor de retorno que não seja nulo.

Erros por intervalo

A métrica Erros por intervalo aumentará em um se algum dos métodos instrumentados retornar uma exceção. Além disso, ErrorDetector gera um instantâneo de erro.

NOTE

Quando o método `receive()` do JMS do IBM WebSphere MQ termina com uma exceção MQRC_NO_MSG_AVAILABLE, o APM não relata alguns resultados. A métrica Erros por intervalo não aumenta, e o ErrorDetector não gera um instantâneo de erro.

Estimated Message Processing Time (ms)

Essa métrica mostra o tempo aproximado entre a conclusão bem-sucedida do método `receive()` com um valor de retorno não nulo e o método `receive()` após o início da invocação. Essa métrica coleta dados quando os métodos estão no mesmo objeto de consumidor e no mesmo segmento. Quando o agente não puder identificar qualquer recebimento subsequente, o rastreador do JMS usará o método pai da chamada de recebimento do JMS para calcular o valor da métrica. Nesse caso, o valor da métrica será o tempo entre o fim do recebimento atual e a conclusão do método pai. Somente depois que o agente identificar o método pai de recebimento do JMS e tiver instrumentado com êxito usando `JMSReceiveParentTracer` , o agente poderá gerar um rastreamento de transação. O rastreamento mostra o valor do tempo de processamento da métrica. Veja a seção a seguir.

Identificação e instrumentação do método pai

O método pai de uma chamada a `JMS Receive` é o método responsável pelo processamento da mensagem que é recebida quando se chama `JMS Receive` . Às vezes, o rastreador não pode encontrar uma chamada de `recebimento` depois do recebimento atual. Nesse caso, identificar o método pai é essencial para fornecer o valor da métrica e o rastreamento de transação.

A identificação do método pai funciona da seguinte maneira:

1. Em um rastreamento de pilha que é coletado no rastreador do `método de recebimento` , as classes podem ser rotuladas com o método `run` ou `call` . As classes rotuladas implementam o método `interfaces` `java.lang.Runnable` ou o método `java.lang.Callable` . As classes que são rotuladas com o método `run` ou `call` são identificadas como métodos pai.Quando houver mais métodos pai no rastreamento de pilha, o método mais próximo da chamada `receive` será marcado como o pai.

   NOTE

   O Introscope ignora diversos componentes ao identificar o método e a classe pai do rastreamento de pilha. O Introscope ignora todas as classes do JDK, métodos e classes lambda dinâmicos, e classes de proxy.
2. Um rastreamento de pilha pode não ter os métodos `run` ou `call` que o agente pode usar para identificar o método pai. Nesse caso, o agente baseia a identificação no valor de índice constante. Por padrão, a classe no índice 7 é identificada como o método pai. Quando a classe no índice 7 for um JDK, uma lambda dinâmica ou uma classe de proxy, o Introscope irá ignorar a classe. O Introscope considera a classe no próximo índice inferior (mais perto da chamada `receive`) e repetições, até marcar uma classe como o pai.
   Você pode encontrar os pais identificados que são armazenados no arquivo JMSParentMethodPersist.pbd no diretório <pasta_principal_do_agente>/core/hotdeploy.

   NOTE

   Mais informações: Um método que nunca sai é identificado como método pai

Java Mail

O email do Java tem dois subnós:

- Java Mail (Send)
- Java Mail (sendMessage)

As seguintes métricas podem aparecer sob os subnós Send ou sendMessage:

- Transport:Average Method Invocation Time (ms)
- Transport:Invocações de método por intervalo
- Transport:Average Method Invocation Time (ms) by class name
- Transport:Method Invocations Per Interval by class name
- Transport:Method Invocations Per Second
- Transport:Method Invocations Per Second by class name
- Transport:Stalled Methods over 30 seconds by class name and method name
- Transport:Concurrent Method Invocations
- Transport:Concurrent Method Invocations by class name

CORBA

- Average Method Invocation Time (ms)
- Method Invocations Per Interval
- Average Method Invocation Time (ms) by class name
- Method Invocations Per Interval by class name
- Method Invocations Per Second
- Stalled methods in any class over 30 seconds
- Concurrent Method Invocations
- Concurrent Method Invocations by class name

Struts

- Average Method Invocation Time (ms)
- Method Invocations Per Interval
- Average Method Invocation Time (ms) by class name and method name
- Method Invocations Per Interval by class name
- Method Invocations Per Second
- Method Invocations Per Second by class name
- Stalled Methods over 30 seconds by class name and method name
- Concurrent Method Invocations
- Concurrent Method Invocations by class name

Sustentabilidade do agente

As métricas de sustentabilidade aparecem sob o nó **Agent Stats**. Essas métricas mostram informações sobre o estado interno do agente, em vez do aplicativo que o agente está monitorando. As métricas de sustentabilidade podem fornecer dados úteis quando você está investigando o comportamento do agente.

Métricas de sustentabilidade de rastreamento profundo

O subnó **Deep Tracing** está localizado sob o subnó **Sustainability**. Deep Tracing exibe as seguintes métricas sobre os recursos do agente que são usados para fornecer visibilidade de rastreamento profundo de transação:

Métricas de sustentabilidade de instrumentação inteligente e visibilidade de rastreamento profundo de transação

Analyzed Methods Count

Número total de métodos que o Introscope analisou para instrumentação inteligente. O número inclui métodos que a instrumentação inteligente instrumenta e não instrumenta.

Average Component Array Size

Tamanho da estrutura de dados da matriz de componentes da instrumentação inteligente interna conforme relatado pelas transações dinâmicas.

Average Component Count Per Transaction

Média do número de componentes de visibilidade profunda e diagnóstico por transação.

Average Deep Component Count Per Transaction

Número médio de componentes de visibilidade profunda por transação.

Classes Processed Per Interval

Número de classes que o ProbeBuilder processou para instrumentação inteligente.

Instrumented Methods Count

Número total de métodos que a instrumentação inteligente está instrumentando no momento.

Max Instrumentable Methods Count

Número máximo de métodos que o Introscope qualifica para instrumentação quando o nível de instrumentação inteligente é definido para alto.

ProbeInfo Collection Size

O tamanho da lista da matriz interna ProbeInfo Collection.

Auto Tracing: Cached Transaction Count Per Interval

Número de transações que são armazenadas em um cache interno por intervalo de 15 segundos.

Auto Tracing: Clamped Traces

Número de rastreamentos de transação automática que foram limitados e não foram enviados ao Gerenciador corporativo nem exibidos na interface do usuário.

Auto Tracing: Downstream GUID Count Per Interval

Número de identificadores de rastreamento downstream adicionados a um cache interno por intervalo de 15 segundos.

Auto Tracing: Sent Traces

Número de rastreamentos de transação automática que são enviados ao Gerenciador corporativo e exibidos na interface do usuário.

Auto Tracing: Trace Cache Hits

Número de rastreamentos de transação automática que são enviados de um agente de downstream por intervalo de 15 segundos.

Auto Tracing: Trace Cache Misses

Número de identificadores de rastreamento que não correspondem a um identificador em um cache interno por intervalo de 15 segundos.

Auto Tracing: Upstream GUID Count Per Interval

Número de identificadores de rastreamento upstream adicionados a um cache interno por intervalo de 15 segundos.

Instrumentation Level: Number Of Candidate Classes For Reinstrumentation

Número total de classes potenciais a serem recarregadas depois que um nível de instrumentação inteligente muda. Esse número não muda quando o Introscope está processando uma alteração no nível. O número será zero quando o processamento terminar.

Instrumentation Level: Current Instrumentation Level

O nível atual da instrumentação inteligente. Valores: 1=low, 2=medium, 3=high.Quando o Introscope processa uma alteração do nível X para Y, o valor da métrica exibe o nível X até que o processamento seja concluído.

Métricas de sustentabilidade de detecção do ponto de entrada

Entry Point Detection: Analyzed Stack Snapshots

Número total de pilhas de segmentos que são analisadas para candidatos de ponto de entrada após início do aplicativo monitorado.

Entry Point Detection: Candidates Discarded

Número total de candidatos de ponto de entrada rastreados que são descartados como inadequados antes de se tornarem pontos de entrada.

Entry Point Detection: Entry Points Discarded

Número de pontos de entrada que o agente descartou como inadequados. Esses pontos de entrada serão ignorados permanentemente.

Entry Point Detection: **Entry Points Discovered**

Número de pontos de entrada que esse agente detectou após início do aplicativo monitorado.

Entry Point Detection: Initial Candidates Current

Número atual de candidatos de ponto de entrada que o agente encontrou, mas o mecanismo de regras ainda não processou.

Entry Point Detection: Initial Candidates Total

Número total de candidatos de ponto de entrada que o agente encontrou após início do aplicativo monitorado.

Entry Point Detection: Stack Snapshot Queue Length

Número atual de instantâneos de pilha de segmentos coletados aguardando análise para candidatos de ponto de entrada.

Entry Point Detection: Total Entry Points

Número total de pontos de entrada em AutoPersist.pbd.

Entry Point Detection: Total Entry Points Discarded

Número total de pontos de entrada proibidos e ignorados que são mantidos em AutoPersist.pbd.

Entry Point Detection: Tracked Candidates Current

Número atual de candidatos de ponto de entrada que o agente está rastreando para desempenho adequado.

Entry Point Detection: Tracked Candidates Total

Número total de candidatos de ponto de entrada que o agente está rastreando após início do aplicativo monitorado.

Entry Point Detection: Tracked Threads

Número atual de segmentos que o agente está rastreando para possível detecção de ponto de entrada.

Métricas de sustentabilidade de detecção automática de back-end

Detecção automática de back-end: instantâneos de pilha analisados

Número total de instantâneos de pilha analisados para candidatos de back-end após início do aplicativo monitorado.

Detecção automática de back-end: back-ends detectados

Número total de back-ends que o agente detectou após início do aplicativo monitorado.

Automatic Backend Detection: Backends Persisted

Número total de back-ends mantidos em AutoPersist.pbd

Métricas de sustentabilidade de extensões

As Métricas de sustentabilidade de extensões estão localizadas no subnó **Extension Bundles**, que está no subnó **Sustainability**. As métricas de extensões fornecem informações sobre as extensões do agente. As métricas fornecem dados de implantação, carregamento e descarregamento da extensão.

Métricas específicas de implantação de extensões

Deployment|Count|All Cycles:Count
O número total de ciclos de implantação que ocorreram depois que o agente foi iniciado. Cada ciclo começa com a aquisição de um bloqueio de implantação e termina com a liberação do bloqueio.

Deployment|Count|Failed Cycles:Count
Número total de ciclos de implantação que falharam depois que o agente foi iniciado. Cada ciclo começa com a aquisição de um bloqueio de implantação e termina com a liberação do bloqueio. Os ciclos de implantação podem falhar por vários motivos. Por exemplo, descompactação do arquivo tar sujeita a erros, exclusão do arquivo tar, cálculo da soma de verificação, etc.

Um valor maior que zero e crescente indica que o implantador de extensão está tendo dificuldades para descompactar uma ou mais extensões.

Deployment|Count|Successful Cycles:Count
Número total de ciclos de implantação bem-sucedidos depois que o agente foi iniciado. Cada ciclo começa com a aquisição de um bloqueio de implantação e termina com a liberação do bloqueio.O ideal é que esse valor seja igual ao valor da métrica All Cycles Count.

Deployment|Current Cycle|Status

Status do segmento `ExtensionDeployer` em execução para implantar e desimplantar extensões do respectivo arquivo .tar no diretório <*Pasta_principal_do_agente*>/extensions/deploy/. Essa métrica tem dois valores: 0 indica que a extensão está implantada e 1 significa que a extensão está em implantação. O ideal é que o valor seja 0, indicando o status implantada.Quando o valor da métrica permanecer em 1 por vários minutos, o segmento `ExtensionDeployer` será bloqueado. Investigue o segmento e reinicie o aplicativo monitorado.

Deployment|Last Cycle|Time (milliseconds)
Tempo gasto em milissegundos para conduzir o ciclo de implantação `ExtensionDeployer` mais recente. Esse valor é o tempo gasto entre a aquisição e a liberação do bloqueio de implantação.

Métricas de carregamento de extensão

Failed: Count
Número total de extensões com falha no carregamento. A falha pode ser em razão de qualquer combinação de PBDs, arquivos JAR ou qualquer outro artefato de extensão opcional com defeito.

Um valor maior que 0 significa falha no carregamento de uma extensão, provavelmente devido a um conflito de PBD.

Loaded: Count
Número total de extensões que foram carregadas com êxito.

Total: Count
Número total de extensões do agente no diretório <*Pasta_principal_do_agente*>/extensions.

Métricas de sustentabilidade de limite JMX

O subnó **JMX Clamp** está localizado sob o subnó **Sustainability**.

Clamp Status

Quando o valor da propriedade introscope.agent.jmx.clamp estiver no limite ou acima dele, o valor será 1. Quando o valor da propriedade estiver abaixo do limite, o valor será 0.

Métricas de visibilidade da lacuna de tempo de execução da instrumentação inteligente

O subnó **Runtime Visibility** está localizado sob o subnó **Sustainability**.

Gaps Found Per Interval

Número de lacunas que a visibilidade da lacuna de tempo de execução encontrou durante o intervalo. O intervalo é determinado pela propriedade introscope.agent.deep.instrumentation.visibility.processor.interval.

Runtime Components Per Transaction

O número médio de componentes de visibilidade da lacuna de tempo de execução por transação de 15 segundos.

Methods Instrumented Per Interval

Número de métodos que a visibilidade da lacuna de tempo de execução instrumentou durante o intervalo. O intervalo é determinado pela propriedade introscope.agent.deep.instrumentation.visibility.processor.interval.

Methods UnInstrumented Per Interval

Número de métodos que a visibilidade da lacuna de tempo de execução não instrumentou durante o intervalo. O intervalo é determinado pela propriedade introscope.agent.deep.instrumentation.visibility.processor.interval.

Total Methods Instrumented

Número de métodos atualmente instrumentados pela visibilidade da lacuna de tempo de execução.

Métricas de sustentabilidade SQL

O subnó **SQL** está localizado no subnó **Sustainability**.

SQL: SQL Statement Count

Número atual de instruções SQL exclusivas para as quais o agente para SQL criou métricas.

Métricas de log de sustentabilidade

As Métricas de log de sustentabilidade estão localizadas no subnó **Configuration**, em **Sustainability**. Essas métricas fornecem contagens de erros e avisos relatados pelo agente no arquivo de log.

AutoProbe Errors Count

Essa métrica tem dois valores: 0 indica que não houve qualquer falha do AutoProbe, 1 indica que foram relatadas falhas do AutoProbe.

Error Count

Número total de erros relatados pelo agente no arquivo **IntroscopeAgent.log** desde que o agente foi iniciado.

Errors Per Interval

Número total de erros relatados pelo agente no arquivo **IntroscopeAgent.log** no intervalo de relatório atual.

Warnings Count

Número total de avisos relatados pelo agente no arquivo **IntroscopeAgent.log** desde que o agente foi iniciado.

Warnings Per Interval

Número total de avisos relatados pelo agente no arquivo **IntroscopeAgent.log** no intervalo de relatório atual.

Métricas do Overhead Manager

As métricas do Overhead Manager estão localizadas sob o subnó **Sustainability**. Essas métricas indicam se o agente está coletando dados de monitoramento no servidor de aplicativos. A propriedade que controla isso é a `introscope.agent.overhead.level` . Para obter mais informações sobre essa propriedade, consulte Propriedades do agente do Java.

Modo Overhead

O valor 1 indica o monitoramento normal do servidor de aplicativos pelo agente. O valor 0 indica que não há nenhum agente monitorando o servidor de aplicativos.

Métricas relacionadas à memória

As métricas relacionadas à memória são relatadas na função GC (Garbage Collection - Coleta de Lixo).

NOTE

- Todas as métricas listadas se aplicam ao DX APM local, e apenas algumas métricas se aplicam ao DX APMSaaS.
- As contagens de instâncias são especiais: por padrão, essas métricas não são relatadas. As contagens de instâncias têm relação com a memória (mas apenas contam o número, não o tamanho) e relatam dados sobre os objetos transacionais.

Coleta de lixo

A coleta de lixo é a recuperação automática de memória voltada aos objetos que não são mais usados por um aplicativo. Quando o processo encontra um objeto não utilizado, a memória é recuperada. Quando o processo encontra um objeto que ainda está ativo, ele é copiado para um pool de memória de geração mais recente. À medida que os pools de memória de gerações mais recentes são preenchidos, a coleta de lixo secundária ocorre. Os objetos ativos são copiados para o segundo pool de memória do espaço restante. Quando esse segundo espaço restante não for mais suficiente para conter todos os objetos, os objetos ativos também serão copiados para os espaços de pool de memória permanentes.

A coleta de lixo pode ocorrer com frequência para que a quantidade de memória recuperada seja maximizada. No entanto, esse comportamento requer muita sobrecarga dedicada ao processo. Por outro lado, a coleta de lixo que não ocorrer com a frequência suficiente deixará muito pouca memória. Quando o processo de GC ocorrer, também precisará de uma sobrecarga significativa para ser executado. Portanto, a coleta de lixo é mais eficiente decorrido o período certo entre as pequenas coletas de lixo. A eficiência equilibra o número de objetos que são limpos com a quantidade de sobrecarga que é necessária para limpá-los.

Em um processo de coleta de lixo eficiente, os pools de memória de gerações mais novas ficam do tamanho certo. Se os pools de memória forem muito pequenos, a coleta de lixo automática ocorrerá com muita frequência. Se os pools de memória forem muito grandes, muitos objetos sem uso se acumularão. Esse acúmulo faz com que o processo de GC menos frequente cause muita sobrecarga ao ser executado. A sobrecarga pode causar um pico no percentual de tempo gasto na coleta de lixo.

- Métricas de memória heap da GC: por padrão, o Introscope relata as métricas de memória heap da GC. Essas métricas usam bytes como unidade de medida.
- Métricas do GC Monitor: essas métricas fornecem informações adicionais sobre o uso de memória. Essas métricas não serão coletadas ou relatadas até que sejam ativadas por um administrador.
- As métricas de sistema de arquivos, UDP e soquetes são medidas da taxa de transferência de dados.

Métricas de memória heap da GC

Essas métricas são ativadas por padrão.

- **GC Heap|Bytes In Use**
  A métrica GC Heap|Bytes In Use informa a quantidade de memória sendo usada atualmente pelos objetos.
- **GC Heap|Bytes Total**
  A métrica GC Heap|Bytes Total informa a quantidade total de memória que a JVM aloca.
  Compare essa métrica com a métrica Current Capacity (bytes), que está disponível quando o DX APMGC Monitor está ativado. A métrica Current Capacity fornece informações sobre a quantidade de memória que é confirmada para todos os segmentos de memória da JVM. A métrica Bytes Total fornece a quantidade de memória que é confirmada para a JVM no total.

Métricas do GC Monitor

As métricas do GC Monitor relatam informações sobre os coletores de lixo e pools de memória, ajudando você a detectar problemas na GC que estejam afetando negativamente o desempenho.

As métricas GC Monitor são exibidas na árvore do navegador de métricas, diretamente abaixo do nó **GC Heap**. As métricas são ativadas por padrão. Algumas das métricas têm limites predefinidos que disparam indicadores de alerta na guia **Visão geral do GC Monitor**.

> **NOTE**
> Para obter mais informações sobre as limitações do GC Monitor e as JVMs suportadas, consulte a matriz de compatibilidade do produto.

Métricas genéricas

As métricas genéricas são:

- **GC Policy**
  Identifica os nomes de lixos da JVM.
- **JVM Type**
  Identifica a JVM sendo monitorada.
- **Percentual de memória heap do Java em uso**
  Identifica o percentual de memória heap disponível que é usada no computador em que o agente está implantado.
  - O Limite de cuidado é 60%.
  - O Limite de risco é 80%.

  Por padrão, a máquina virtual aumenta ou diminui a memória heap a cada coleta. Essa ação mantém a proporção de espaço livre para os objetos ativos em um intervalo específico. O intervalo alvo é definido por meio dos parâmetros da seguinte maneira:
  - `-XX:MinHeapFreeRatio=<mínimo>`
  - `-XX:MaxHeapFreeRatio=<máximo>`

  O tamanho total tem como base `-Xms` e `-Xmx` .
  O tamanho padrão geralmente é muito pequeno.

  > **WARNING**
  > Mantenha a métrica abaixo de 60%. Se a métrica ficar acima dos 80%, ajuste o tamanho da memória heap da JVM. Para conceder memória suficiente e acessível à máquina virtual, ajuste os parâmetros -Xms e -Xmx.

  Os valores padrão do intervalo alvo são o mínimo de 30% mínimo e o máximo de 70%. Frequentemente, aplicativos maiores apresentam problemas com os valores padrão. Um problema pode ser inicialização lenta, o que ocorre quando a memória heap inicial é pequena e precisa ser redimensionada em muitas coletas. A configuração dos parâmetros `-Xms` e `-Xmx` com o mesmo valor aumenta a previsibilidade, removendo a decisão de dimensionamento mais importante da máquina virtual. Por outro lado, a máquina virtual não conseguirá compensar isso se você fizer uma escolha ruim.
  Certifique-se de aumentar a memória à medida que aumentar o número de processadores, porque a alocação pode ser feita em paralelo.

Métricas do coletor de lixo

As métricas do coletor de lixo são:

- **GC Algorithm**
  Exibe o algoritmo da coleta de lixo do gerenciador de memória correspondente.
- **GC Invocation Per Interval**
  Exibe uma métrica de contagem relatando o número de coletas de lixo que ocorreram em cada intervalo de 15 segundos. A métrica é agregada e calculada a partir da Contagem total de invocações de GC por meio do rastreamento da diferença entre o intervalo atual e o mais recente.
  Essa métrica indica a coleta por intervalo que é feita no pool de memória. Se a métrica aumentar ao longo do tempo, significa que há coletas frequentes acontecendo em um pool de memória e que não está do tamanho correto. Aumentar o tamanho do pool de memória ajuda a reduzir as coletas de lixo frequentes.
- **Contagem total de invocações de GC**
  O número total de coletas de lixo que ocorreram desde que a JVM foi iniciada.
  Essa métrica indica o número de coletas desde o momento de inicialização do servidor. A métrica aumenta lentamente em intervalos regulares.
  Os picos na métrica indicam coletas frequentes, o que afeta a taxa de transferência geral do aplicativo. Para reduzir a frequência de coletas de lixo e aumentar a taxa de transferência, aumente o tamanho do pool de memória.
- **GC Time Per Interval (ms)**
  Exibe a quantidade de tempo que a coleta de lixo levou durante o intervalo de 15 segundos. Essa métrica agregada é calculada a partir do tempo total da coleta de lixo por meio do rastreamento da diferença na coleta de lixo entre o intervalo atual e o mais recente.
  O comportamento normal dessa métrica é permanecer constante ou aumentar lentamente à medida que o tempo gasto para fazer a coleta de lixo aumenta.
  Aumentos drásticos indicam lentidão na execução do aplicativo, aumentando os tempos de pausa da coleta de lixo. Para evitar esse problema, configure a memória máxima usando o sinalizador `-Xmx` com um valor ideal. O ajuste adequado faz com que os tempos de pausa da coleta de lixo sejam reduzidos e com que a taxa de transferência da coleta de lixo melhore. Se a memória estiver definida com um valor muito alto, a frequência da coleta de lixo passa a ser menor e a taxa de transferência/eficiência dela melhora. No entanto, o aplicativo terá longos tempos de pausa, pois o sistema tentará manter um espaço de memória heap muito grande. O tamanho ideal de memória heap garante tempos de pausa e de coleta de lixo menores.
- **Memória recuperada por intervalo**
  Calcula e relata a quantidade de memória em bytes recuperada por um coletor de lixo durante o intervalo atual. Quando há várias invocações de um determinado coletor de lixo, essa métrica exibe a soma de todas as invocações na memória do coletor de lixo.
- **Porcentagem de memória heap usada após a invocação da GC**
  Calcula e relata a porcentagem de memória heap que a JVM usou após o evento de coleta de lixo. A métrica exibe um valor de 0 para intervalos sem uma invocação de coleta de lixo. Quando há várias invocações de um determinado coletor de lixo em um intervalo, essa métrica exibe a porcentagem média da memória heap de todas as invocações.
  O DX APM oferece suporte a essa métrica nas versões 1.7 e superiores da Oracle JVM.
- **O percentual de tempo gasto na GC nos últimos 15 minutos**
  Exibe uma métrica agregada calculada por meio de uma calculadora do Gerenciador corporativo. O percentual desse valor é calculado usando a fórmula:
  ```
  (total GC time spent/length of time in ms) * 100
  ```
  Exemplo, intervalo de 15 minutos:
  ```
  45600/(15*60*1000) * 100 = 5 %
  ```
  Um aumento drástico do tempo indica lentidão na execução do aplicativo, aumentando os tempos de pausa da coleta de lixo. Configure a memória máxima usando o sinalizador `-Xmx` com um valor ideal.
  Uma métrica estável que chega ao pico repentinamente indica que uma coleta de lixo isolada levou mais tempo do que o normal. Após esse pico, a métrica de volta ao normal e nenhuma ação é necessária.
- **Total GC Time (ms)**

Exibe o tempo total do processo de coleta de lixo, em milissegundos.
O comportamento normal dessa métrica é aumentar gradualmente.
O aumento drástico do tempo indica lentidão na execução do aplicativo, aumentando os tempos de pausa da coleta de lixo. Para evitar esse problema, configure a memória máxima usando o sinalizador `-Xmx` com um valor ideal. O ajuste adequado faz com que os tempos de pausa da coleta de lixo sejam reduzidos e com que a taxa de transferência da coleta de lixo melhore.

Ativar e usar métricas mais métricas de GC

A coleta de lixo e o gerenciamento de memória podem ter um efeito significativo no desempenho dos aplicativos. As métricas básicas de memória heap da GC estão disponíveis por padrão. É possível ativar métricas opcionais para fornecer mais detalhes sobre o processamento da coleta de lixo e o uso do pool de memória. Essas métricas adicionais são exibidas no nó **GC Monitor** no navegador de métricas quando ativadas. As métricas do GC Monitor relatam informações para ajudar a otimizar a alocação do pool de memória e o processamento da coleta de lixo. Portanto, geralmente você ativa essas métricas para uso específico. Por exemplo, ao desenvolver ou testar aplicativos, ou pesquisar problemas de desempenho de aplicativos. Na maioria dos casos, as métricas não são usadas para o gerenciamento de aplicativos em tempo real em um ambiente de produção e são desativadas por padrão.

Quando a propriedade `introscope.agent.gcmonitor.enable` estiver definida como `true` (padrão), você poderá exibir os detalhes sobre os coletores de lixo e pools de memória da JVM que estiver monitorando.

Métricas do pool de memória

As métricas do pool de memória são as seguintes:

- **Amount of Space Used (bytes)**
  Exibe a quantidade de espaço de memória usado. O valor inclui todos os objetos do pool, incluindo objetos acessíveis e inacessíveis.
  O comportamento normal dessa métrica é aumentar gradualmente. A métrica poderá diminuir quando a coleta de lixo terminar e a memória for recuperada.
  Um pico temporário que depois volta ao normal pode ser um aviso de problemas na memória.
  Em um aumento rápido, a métrica pode atingir o limite máximo de memória, o que produz exceções de falta de memória. Para evitar esse problema, defina o tamanho máximo do pool de memória com um valor mais acessível.
- **Current Capacity (bytes)**
  A quantidade de memória confirmada para esse pool e todos os segmentos de memória da JVM. Essa quantidade de memória é garantida para o uso da JVM.

  > **NOTE**
  > Adicionar todas as métricas de capacidade atual de segmentos de memória individuais quase iguala a métrica Bytes Total (consulte Métricas de memória heap da GC). Se a quantidade de espaço atingir a capacidade atual, poderá causar exceções de memória. Para evitar esse problema, planeje a necessidade de lidar com operações diárias e picos inesperados.
- **Growth Rate**
  A taxa de crescimento média da memória usada, expressa em bytes por segundo. Em um pool de memória, em bytes por segundo ao longo do último minuto. Essa métrica agregada é calculada da seguinte maneira:
  – Localizando-se o último valor do ponto de dados em bytes (lastValue).
  – Localizando-se o primeiro valor do ponto de dados em bytes (firstValue).
  Inclui-se também o espaço no intervalo de 1 minuto mais recente. A taxa é calculada usando esta fórmula:
  ```
  (lastValue - firstValue) / 60
  ```
  Essa métrica aumentará lentamente, permanecerá constante ou falhará, se a memória não utilizada for retornada para o pool.
  Um aumento drástico em 15 minutos ou mais indica que a memória não está sendo reciclada após a coleta de lixo. Esse comportamento indica um possível vazamento de memória. É recomendável investigar melhor.
- **Maximum Capacity (bytes)**

A quantidade máxima de memória (em bytes) usada para o gerenciamento de memória. Não há garantia de que essa quantidade de memória estará disponível para o gerenciamento de memória se ela for maior do que a capacidade atual (quantidade de memória confirmada).
Essa métrica permanece constante ao longo do tempo.

- **Memory Type**
  Tipo da memória, podendo ser:
  – Memória heap
  – Memória diferente de heap
- **Percentage of Maximum Capacity Currently Used**
  Exibe a representação em porcentagem do uso de memória atual (acima do valor máximo). Essa métrica indica o percentual de memória usado ao longo do tempo.
  Essa métrica aumentará lentamente, permanecerá constante ou falhará, se a memória não utilizada for retornada para o pool.
  Se a métrica exceder de 70 a 80%, defina a memória máxima com um valor maior e melhor.

Sistema de arquivos, soquetes e UDP

Como a métrica Respostas por intervalo, as métricas de sistema de arquivos, soquetes e UDP são medidas de taxa de transferência de dados. Elas são medidas em bytes por segundo:

Sistema de arquivos

- File output rate (bytes per second)
- File input rate (bytes per second)

UDP (User Datagram Protocol)

- Output bandwidth (bytes per second)
- Input bandwidth (bytes per second)

Soquetes (total, bem como informações específicas sobre host/porta)

- Output bandwidth (bytes per second)
- Input bandwidth (bytes per second)

Um grande número de métricas relacionadas à porta indica que as métricas de taxa do soquete devem ser desativadas, porque essa situação provavelmente é um problema de explosão de métricas.

Contagens de instância

As métricas de contagem de instâncias medem o número de instâncias de objeto de uma determinada classe na memória heap.

- Contagem aproximada de instâncias por pacote e nome de classe

Métricas de suportabilidade do agrupamento

Um cluster integra os recursos de dois ou mais dispositivos de computação (que podem, de outra forma, funcionar separadamente) para uma finalidade comum. O cluster permite que um Enterprise Manager gerencie outros Enterprise Managers ou atue como um MOM (Manager of Managers). O APM avalia a suportabilidade de aplicativos medindo o desempenho dos diversos componentes do aplicativo e fornece as seguintes métricas:

Os dados a seguir são relatados para o computador que hospeda o Enterprise Manager e para cada computador com métodos instrumentados.

- Host do EM – nome do host do servidor do Enterprise Manager
- Porta do EM – porta do Enterprise Manager à qual o agente está conectado
- Java Version

As métricas de suportabilidade exibem informações sobre o Enterprise Manager, e não do aplicativo que ele está monitorando. Essas métricas são exibidas na árvore do investigador, em:

Custom Metric Host (Virtual)

Custom Metric Process (Virtual)

Custom Metric Agent (Virtual)(SuperDomain)

Abaixo desse nível, as métricas de suportabilidade são organizadas na hierarquia a seguir. As definições de algumas dessas métricas seguem a lista.

Nó do agente

Os agentes têm a seguinte hierarquia:

```
<Host_Name>
   <Process_Name>
    <Agent_Name>
```

<Nome_do_processo> e *<Nome_do_agente>* podem ser configurados em IntroscopeAgent.profile.

Para cada <Agent_Name>, as seguintes métricas estão disponíveis:

- ConnectionStatus, uma destas opções:
  - 3 = desconectado
  - 2 = conectado, lento ou sem dados
  - 1 = conectado
  - 0 = desmontado
- IsClamped, um destes valores:
  - 1 = Limitado
  - 0 = Não limitado

  Observação: para obter mais informações sobre limitação de métrica, consulte Usando o visualizador do rastreamento de transação.
- Contagem de métricas
- Contagem de métricas brutas

Calculadora de conectividade do agente

A calculadora de conectividade do agente copia o status de conectividade do agente em um local fixo. Atualmente, o status é armazenado na pasta Collectors, mas quando o agente se reconecta a um coletor diferente, a métrica continua sendo coletada em uma pasta diferente. A calculadora de conectividade do agente, nesse caso, copia todos os status da pasta Collectors para a pasta MOM, um único local de persistência.

> **NOTE**
> A calculadora de conectividade do agente fica desativada por padrão e deve ser ativada pelo administrador na instância do MOM e reiniciada no MOM por meio da definição da propriedade `introscope.apm.calculator.agentconnectivity.enabled=true`

A calculadora gera as seguintes métricas em `Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|<Nome_do_agente>`:

- Tempo de atividade - Um valor que aumenta regularmente e é útil para ver quando exatamente o agente se conecta. Cai para 0 quando o agente é desconectado.
- Métricas - O número de métricas brutas fornecidas por um agente.
- ConnectionState - A conectividade do agente. Pode ser qualquer um dos seguintes valores inteiros:
  - 4 – Ativo, o agente está conectado e enviando métricas.
  - 5 - Parado, o agente foi encerrado corretamente.
  - 6 – Reconectado, o agente mudou para um coletor diferente.
  - 7 - Interrompido, o agente não foi desconectado normalmente, mas o APM não recebe nenhuma métrica dele.
  - 8 - Expirado, o agente foi encerrado ou interrompido por mais de 24 horas.

A calculadora também gera um pequeno resumo das contagens de agentes para cada `ConnectionState` em `Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Agents|Agent States`.

Métricas do agente

<*Nome_do_agente*> | ErrorSnapshot Events Per Interval

O número total de eventos de instantâneo do erro por agente e por intervalo.

Nó do Enterprise Manager

Sob o nó do Enterprise Manager, as seguintes métricas de suportabilidade estão disponíveis:

- Host
- Nome
- Capacidade geral (%)
- Porta
- CPU
  - EM CPU Used (%)
- Configuração
  - Agent Clusters Metric Load
  - Number of Agent Clusters
  - Number of Map Entity Metric Groupings
  - Number of Metric Groupings
- Conexões

  - Disallowed Agents Clamped – indica se o número máximo de agentes não permitidos, conectados a um determinado MOM, coletor ou Enterprise Manager autônomo foi excedido. Se o valor for 0, o limite não está em vigor. Se o valor for 1, o limite está em vigor.
  - EM Historical Metric Clamped
  - EM Live Metric Clamped
  - Métrica Max Number of Agent Connection Limit Exceeded Per Interval – indica se o número máximo de agentes conectados ao MOM, coletor ou Enterprise Manager autônomo foi excedido. Se o valor for 0, o limite não está em vigor. Se o valor for 1, o limite está em vigor.
  - Metrics From External Agents – mostra a contagem de métricas do EM gerada pelos agentes virtuais do EM.
  - Metrics Queued (%)
  - Number of Agents
  - Number of Applications – o número de aplicativos do agente que estão relatando dados no momento.
  - Number of Disallowed Agents - exibe o número de agentes não permitidos conectados a um determinado MOM, coletor ou Enterprise Manager autônomo. Agentes passivamente conectados não enviam dados de métrica.
  - Number of Events Processed
  - Number of Events Processed Limit Exceeded
  - Number of Metrics Handled – número de métricas de entrada processadas por intervalo de 15 segundos. Esse número varia, mas pode girar em torno do mesmo valor do número de métricas. Um valor menor do que o número de métricas indica que o Enterprise Manager pode estar sobrecarregado e não está processando os dados de entrada com rapidez suficiente.
  - Number of Metrics – exibe a carga total da métrica no Enterprise Manager.
  - Number of Unique Applications
  - Number of Workstations

Nó de repositório de dados

Sob o nó de repositório de dados, as seguintes métricas estão disponíveis:

- SmartStor
  - Metrics Appended To Query Per Interval
  - Metrics Converted From Spool to Query Per Interval
  - SmartStor Disk Usage (mb)
  - MetaData
    - Agent Metric Cache Size
      O número de métricas do agente no 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)

Subnó de integridade

- CPU Capacity (%) - porcentagem de CPUs usadas. Por exemplo, 300% significa que três núcleos da CPU são totalmente utilizados.
- GC Capacity (%)
- Harvest Capacity (%)
- Heap Capacity (%)
- Capacidade dos dados de entrada (%)
- SmartStor Capacity (%)

Subnó interno

As métricas a seguir são exibidas abaixo do subnó Interno:

- Number of Connection Tickets
- Number of Dependent Calculator Input Metrics
  O número total de métricas que são entradas para calculadoras dependentes. As calculadoras dependentes costumam usar como entrada os valores de métrica que outras calculadoras produzem. Essa contagem se refere a todas as métricas fornecidas às calculadoras dependentes, e não apenas às métricas produzidas por outras calculadoras.
- Number of Non-Dependent Calculator Input Metrics
  O número total de métricas que são usadas como entrada para calculadoras não dependentes. As calculadoras não dependentes não usam valores de métrica que outras calculadoras produzem. Por exemplo, as métricas provenientes de agentes.
- 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)
- Alertas
  - *<Nome_do_módulo_de_gerenciamento>*
    - Agent Connection Status
      - Número de métricas avaliadas
  - Total Number of Evaluated Metrics
    O número total de métricas avaliadas para todos os alertas.
- Calculadoras
  - Total Number of Evaluated Metrics
    O número total de métricas avaliadas para todas as calculadoras. Essa métrica é a soma do número de métricas de entrada da calculadora dependente e do número de métricas de entrada da calculadora não dependente. Quando essa contagem chega ao pico, o Enterprise Manager está realizando muitos cálculos em tempo real, o que pode sobrecarregar os recursos da CPU.
  - <nome da calculadora> | Total Number of Evaluated Metrics
    O número total de métricas avaliadas para uma calculadora individual.

    NOTE
    Essa métrica é exibida no investigador somente quando a calculadora é definida.
- GC Heap

  - Coletores
    - *<Nome_do_coletor>*
      - Collection Count Per Interval
      - GC Duration (ms)
  - Pools
- Harvest
  - Alert Action Processing Time (ms)
    Tempo decorrido que o Enterprise Manager leva para processar todas as ações de alerta.
  - Calculator Queries Wait Time (ms)
    Tempo decorrido para o segmento de consultas da calculadora concluir seu trabalho atual, incluindo aguardar a finalização do loop de consulta fora da calculadora. O novo processamento de consulta da calculadora é iniciado depois que todas as entregas fora da calculadora do intervalo anterior são feitas para o cliente.
  - Non Calculator Queries Delivery Time (ms)
    Tempo que o Enterprise Manager levou para executar e entregar consultas fora da calculadora a todos os clientes solicitantes em um intervalo.
    Após a execução de todas as consultas de calculadora, o Enterprise Manager executa consultas fora da calculadora e envia os resultados para todos os clientes que as solicitaram.
  - Non Calculator Queries Excess Time (ms)
    Excesso de tempo de espera para consultas fora da calculadora a serem concluídas além de um intervalo.
    Os clientes enviam solicitações de consulta fora da calculadora ao Enterprise Manager, que envia os resultados de volta. Se esse processo não for concluído dentro de um intervalo, ele será transmitido até ser concluído.
    Essa métrica mostra por quanto tempo além de um intervalo as consultas fora da calculadora são estendidas.
  - Metrics From All Agents
    Número total de métricas exclusivas geradas por todos os agentes conectados que enviaram dados no último intervalo. Essa contagem não inclui métricas históricas. As configurações de limite não afetam essa contagem.
  - Spooling Data File Write Time (ms)
    Tempo que o Enterprise Manager levou para gravar os dados coletados no arquivo spool (.spool) em um intervalo.
  - Spooling Preparation Time (ms)
    Tempo que o Enterprise Manager levou para preparar os dados coletados a serem gravados no arquivo spool (.spool) em um intervalo.
- Management Module Calculators
  - Total Number of Evaluated Metrics
    Número de métricas que são entradas para as calculadoras do módulo de gerenciamento.
- Messaging
  - Active Incoming Threads
  - Active Outgoing Threads
  - Corrupted Messages Per Interval
  - Post Offices
    - *<Nome_do_Post_Office>*
      - Number of Mailboxes
      - Queued Messages
- Grupo de métricas
  - Metric Matches Per Interval
    Número total de métricas que foram avaliadas em todas as consultas no último intervalo.
  - Queued Queries Per Interval
    Número de consultas que, no momento, estão aguardando o processamento no intervalo do ciclo de coleta. O valor geralmente é zero após a inicialização.
- Query

  - Cache Queries Duration (ms)
  - Cache Queries Per Interval
  - SmartStor Queries Duration (ms)
  - SmartStor Queries Per Interval
- Segmentos
  - *<Nome_do_segmento>*
    - Blocked Count
    - Blocked Time (ms)
    - CPU Time (ms)
    - User Time (ms)
    - Wait Count
    - Wait Time (ms)

Subnó de problemas

Módulos de gerenciamento

- Warning Count

Subnó de tarefas

Harvest Duration (ms)

SmartStor Duration (ms)

Métricas de coleta

Capacidade de coleta

A métrica Capacidade de coleta exibe o percentual de tempo necessário para a coleta de dados em um intervalo de 15 segundos. Por exemplo, se a coleta de dados levar 15 segundos, o valor da métrica será 100. O investigador exibe essa métrica no local.

```
Custom Metric Host (Virtual)| Custom Metric Process (Virtual)| Custom Metric Agent (Virtual)(*SuperDomain*)|
 Enterprise Manager | Health | Harvest Capacity (ms)
```

Harvest Duration

A métrica Harvest Duration mostra o tempo, em milissegundos (durante um intervalo de 15 segundos), gasto na coleta de dados. A métrica geralmente é um bom indicador para determinar se o Enterprise Manager está acompanhando a carga de trabalho atual. Você pode encontrar essa métrica no local a seguir na Árvore do investigador.

```
Custom Metric Host (Virtual)| Custom Metric Process (Virtual)| Custom Metric Agent (Virtual)(*SuperDomain*)|
 Enterprise Manager | Tasks | Harvest Duration (ms)
```

Capacidade dos dados de entrada (%)

A capacidade do Enterprise Manager para lidar com os dados de entrada. A métrica é calculada multiplicando-se a capacidade total da métrica por 2. Por exemplo, se 150.000 métricas estiverem na fila aguardando para serem processadas, e o Enterprise Manager tiver uma capacidade para lidar com 300.000 métricas, a capacidade de dados de entrada será 25%.

Você pode encontrar essa métrica no local a seguir no Navegador de métricas.

```
Custom Metric Host (Virtual)| Custom Metric Process (Virtual)| Custom Metric Agent (Virtual)(*SuperDomain*)|
 Enterprise Manager | Health | Incoming Data Capcity (%)
```

Métricas do coletor

As métricas a seguir são do Coletor.

- **EM Live Metric Clamped**
  Indica se o número de métricas dinâmicas que são controladas pelo Enterprise Manager é menor ou maior que o limite máximo especificado na propriedade introscope.enterprisemanager.metrics.live.limit para os bloqueios do Enterprise Manager. O valor da métrica será 0 se o número de métricas dinâmicas para o Enterprise Manager for menor do que o limite especificado. O valor da métrica será 1 se o número de métricas dinâmicas para o Enterprise Manager for maior do que o limite especificado.

  NOTE
  Você pode definir o limite de bloqueio para a propriedade introscope.enterprisemanager.metrics.live.limit no arquivo apm-events-thresholds-config.xml. O arquivo apm-events-thresholds-config.xml está localizado no diretório <*diretório_principal_do_EM*>\config.
- **EM Historical Metric Clamped**
  Indica se o número de métricas dinâmicas que são controladas pelo Enterprise Manager é menor ou maior que o limite máximo especificado na propriedade introscope.enterprisemanager.metrics.historical.limit para os bloqueios do Enterprise Manager. O valor da métrica será 0 se o número de métricas dinâmicas para o Enterprise Manager for menor do que o limite especificado. O valor da métrica será 1 se o número de métricas dinâmicas para o Enterprise Manager for maior do que o limite especificado.

  NOTE
  Você pode definir o limite de bloqueio para a propriedade introscope.enterprisemanager.metrics.historical.limit no arquivo apm-events-thresholds-config.xml. O arquivo apm-events-thresholds-config.xml está localizado no diretório <*diretório_principal_do_EM*>\config.
- **Max Number of Agent Connection Limit Exceeded Per Interval**
  O número de vezes que o limite de bloqueio definido na propriedade introscope.enterprisemanager.agent.connection.limit foi excedido para um determinado intervalo.

  NOTE
  Você pode definir o limite de bloqueio para a propriedade introscope.enterprisemanager.agent.connection.limit no arquivo apm-events-thresholds-config.xml. O arquivo apm-events-thresholds-config.xml está localizado no diretório <*diretório_principal_do_EM*>\config.
- **Number of Events Processed**
  Indica o número total de todos os eventos, como rastreamentos de transação e erros, que o Enterprise Manager processa em cada intervalo.
- **Number of Events Processed Limit Exceeded**
  O número de vezes que o limite de bloqueio definido na propriedade introscope.enterprisemanager.events.limit foi excedido para um determinado intervalo.

  NOTE
  Você pode definir o limite de bloqueio para a propriedade introscope.enterprisemanager.events.limit no arquivo apm-events-thresholds-config.xml. O arquivo apm-events-thresholds-config.xml está localizado no diretório <*diretório_principal_do_EM*>\config.

Métricas de consulta

Data Points Retrieved From Disk Per Interval

O número de pontos de dados que são recuperados do SmartStor por intervalo.

Data Points Returned Per Interval

O número de pontos de dados que o Enterprise Manager retornou aos clientes por intervalo.

Metrics Read From Disk Per Interval

Número de métricas que são lidas no SmartStor por intervalo.

Metrics Returned Per Interval

O número de métricas exclusivas que o Enterprise Manager retornou aos clientes.

Queries Exceeding Max Data Points Read From Disk Limit Per Interval

Indica se o número máximo de pontos de dados de métrica especificado na propriedade `introscope.enterprisemanager.query.datapointlimit` que um Enterprise Manager retorna para uma determinada consulta em lote foi excedido. Se o número de pontos de dados de métrica que o Enterprise Manager retorna for menor que o limite especificado, o valor da métrica será 0. Se o número de pontos de dados de métrica que o Enterprise Manager retorna exceder o limite especificado, o valor da métrica será 1.

> **NOTE**
> Defina o limite de bloqueio para a propriedade
> `introscope.enterprisemanager.query.datapointlimit`
> no arquivo
> `IntroscopeEnterpriseManager.properties`
> . Localize o arquivo
> `IntroscopeEnterpriseManager.properties`
> no diretório
> `<EM_Home>\config`
> .

Queries Exceeding Max Data Points Returned Limit Per Interval

Indica se o número máximo de pontos de dados de métrica que são especificados na propriedade `queryintroscope.enterprisemanager.query.returneddatapointlimit` que um Enterprise Manager pode retornar para uma determinada consulta em lote foi excedido. Se o número de pontos de dados de métrica que o Enterprise Manager retornar for menor que o limite especificado, o valor da métrica será 0. Se o número de pontos de dados de métrica que o Enterprise Manager retorna exceder o limite especificado, o valor da métrica será 1.

> **NOTE**
> Defina o limite de bloqueio para a propriedade
> `introscope.enterprisemanager.query.returneddatapointlimit`
> no arquivo
> `IntroscopeEnterpriseManager.properties`
> . A propriedade
> `IntroscopeEnterpriseManager.properties`
> está localizado no diretório
> `<EM_Home>\config`
> .

Converting Spool to Data Metric

A métrica Converting Spool to Data rastreia se a tarefa de conversão de spool em dados está em execução. Você pode encontrar essa métrica no local a seguir na Árvore do investigador:

```
Custom Metric Host (Virtual)| Custom Metric Process (Virtual)| Custom Metric Agent (Virtual)(*SuperDomain*)|
 Enterprise Manager | Data Store | SmartStor | Tasks | Converting Spool to Data
```

Se essa métrica permanecer em 1 por mais de 10 minutos por hora, isso significa que a reorganização do arquivo de spool SmartStor está demorando muito tempo.

Métrica Overall Capacity (%)

A métrica Overall Capacity (%) do Enterprise Manager estima a porcentagem da capacidade do Enterprise Manager que é consumida. Você pode encontrá-la neste local na árvore do investigador:

```
Custom Metric Host (Virtual)| Custom Metric Process (Virtual)| Custom Metric Agent (Virtual)(*SuperDomain*)|
 Enterprise Manager: Overall Capacity (%)
```

Capacidade geral (%) é um valor máximo de Capacidade da CPU (%), Capacidade de coleta (%), Capacidade da memória heap (%), Capacidade do SmartStor (%), Capacidade dos dados de entrada (%) e Capacidade de GC (%).

Métrica SmartStor Capacity (%)

A métrica SmartStor Capacity (%) exibe a porcentagem de tempo necessária para o processo de gravação do SmartStor em um intervalo de 15 segundos, em que 15 segundos é igual a 100%.

Você pode encontrá-la neste local na árvore do investigador:

```
Custom Metric Host (Virtual)| Custom Metric Process (Virtual)| Custom Metric Agent (Virtual)(*SuperDomain*)|
 Enterprise Manager | Health | SmartStor Capacity (%)
```

Métrica Heap Capacity (%)

A métrica Heap Capacity (%) é determinada pela porcentagem de heap que a JVM está usando no momento (com base na métrica GC Heap: In Use Post GC (mb)).

Métrica Number of Agents

Essa métrica exibe o número de agentes conectados no momento. O local da métrica é:

```
Custom Metric Host (Virtual)| Custom Metric Process (Virtual)| Custom Metric Agent (Virtual)(*SuperDomain*)|
 Enterprise Manager | Connections
```

Number of Metrics

Essa métrica exibe a carga total da métrica no Enterprise Manager. O local da métrica é:

```
Custom Metric Host (Virtual)| Custom Metric Process (Virtual)| Custom Metric Agent (Virtual)(*SuperDomain*)|
 Enterprise Manager | Connections
```

Métricas de suportabilidade da triagem assistida

O APM fornece métricas de suportabilidade de triagem assistida medindo o desempenho dos vários componentes do aplicativo de triagem assistida. O Enterprise Manager gera e coleta métricas sobre os componentes da triagem assistida. Essas métricas de suportabilidade são úteis para avaliar a integridade do Gerenciador corporativo.

Observação: para obter informações sobre a triagem assistida, consulte Monitorar problemas e anomalias da triagem assistida.

Monitorar o desempenho do componente de triagem assistida

As métricas de suportabilidade de triagem assistida ajudam a monitorar o desempenho dos vários componentes da triagem assistida.

Outras métricas podem aparecer, por exemplo:

- Métricas de eventos de Análise diferencial que são criados quando a intensidade da variação ultrapassa um determinado valor
- Métricas de eventos de erro que são criados quando a triagem assistida recebe um instantâneo ou um erro de paralisação

Siga estas etapas:

1. No APM Team Center, clique no link **WebView**.
2. Clique na guia **Investigador**.
3. Expanda o nó do domínio do seu interesse.
4. Vá para o nó **Enterprise Manager**, **Triagem assistida**.
5. Expanda um nó do seu interesse, por exemplo: **Event Generator**.
   As métricas de suportabilidade para o gerador de eventos serão exibidas, por exemplo:
   ```
   DA : Average Processing Time (ms)
   ```
   Essa métrica fornece o tempo médio de processamento, em milissegundos, dos eventos da DA (Differential Analysis - Análise Diferencial) que o processador de eventos da triagem assistida recebeu.

Gerador de eventos

A triagem assistida usa geradores de eventos que geram eventos e dependem de diferentes tipos de origens. Por exemplo, uma origem são os alertas do APM que os administradores definem nos módulos de gerenciamento. Exemplos de eventos incluem:

- Eventos de Análise diferencial que são criados quando a intensidade da variação excede um determinado valor
- Eventos de erro e paralisação

O APM fornece as métricas a seguir para monitorar o componente Event Generator. Essas métricas aparecem sob o nó Event Generator no Investigador:

```
Enterprise Manager | Assisted Triage | Event Generator | <Metric>
```

- **DA : Average Processing Time (ms)**
  Fornece o tempo médio de processamento, em milissegundos, dos eventos da DA (Differential Analysis - Análise Diferencial) que o processador de eventos da triagem assistida recebeu.
- **DA : Raw States Received Per Interval**
  Fornece o número de eventos da DA (Differential Analysis - Análise Diferencial) que o processador de eventos da triagem assistida recebeu por intervalo.
- **DA : Events Sent Per Interval**
  Fornece o número de eventos agregados da DA (Differential Analysis - Análise Diferencial) que são enviados de volta ao processador de eventos da DA.
- **Alerta : Average Processing Time (ms)**
  Fornece o tempo médio de processamento, em milissegundos, de todos os eventos de alerta processados pelo gerador de alertas.
- **Alerta : Raw Alert States Received Per Interval**
  Fornece o número de alertas recebidos por intervalo pelo gerador de alertas.
- **Alerta : Events Sent Per Interval**
  Fornece o número de eventos de alerta agregados que são enviados de volta aos processadores de eventos da triagem assistida.

Principais métricas de suportabilidade

As métricas de suportabilidade ajudam a avaliar problemas de desempenho que envolvem o EM (Enterprise Manager). As seguintes cinco métricas de suportabilidade geralmente causam problemas de desempenho em vários ambientes do APM.

Duração do SmartStor (ms)

Nome do caminho da métrica: `SuperDomain | Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) | Enterprise Manager | Tarefas: Duração do SmartStor (ms)`

Descrição: a quantidade de tempo que o EM ou o coletor leva para salvar os dados coletados no disco.

Produto: APM

Componente: Enterprise Manager

Versão: todas as releases suportadas

Impacto: se essa métrica exceder 1 segundo, significa que o EM ou os coletores possivelmente estão enfrentando problemas de desempenho relacionados a E/S. Se a métrica for superior a 3,5 segundos, outras tarefas dentro do EM ou do coletor poderão ser atrasadas.

Configuração: configure um disco separado (Controlador) para os dados do SmartStor editando a propriedade `introscope.enterprisemanager.smartstor.directory` no arquivo `config/IntroscopeEnterpriseManager.properties`.

Faixa: íntegro: <1.000 ms, risco: > 3.500 ms, risco extremo: > 15 s.

Correção: cada banco de dados do SmartStor deve residir em um disco físico separado e dedicado. É altamente recomendável uma unidade SSD com uma velocidade de leitura/gravação de 220 MBPS com tamanho do bloco de 4 KB.

Duração da coleta (ms)

Nome do caminho da métrica: `SuperDomain | Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) | Enterprise Manager | Tarefas: Duração da coleta (ms)`

Descrição: a quantidade de tempo que o EM ou o coletor leva para agregar métricas de intervalos de 15 segundos na preparação para gravá-las no banco de dados do SmartStor.

Produto: APM

Componente: Enterprise Manager

Versão: todas as releases suportadas

Impacto: se essa métrica exceder 1 segundo, significa que o EM em seus MOMs e coletores possivelmente estão com problemas de desempenho. Verifique os valores das métricas `Enterprise Manager | Internal | Calculadoras: Total Number of Evaluated Metrics` e `Enterprise Manager | Internal: Number of [Non] Dependent Calculator Input Metric`. Se os valores forem superiores a 3,5 segundos, outras tarefas dentro do EM ou do coletor poderão ser atrasadas.

Configuração

- Verifique as seguintes contagens de métricas para avaliar se o número de métricas está sobrecarregando o EM:
  - `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`
- Reduza o número de métricas nos alertas e nas calculadoras.

Faixa: íntegro: <1.000 ms, risco: > 3.500 ms, risco extremo: > 15 s.

Correção: reduza os seguintes componentes:

- Métricas em alertas e calculadoras
- Consultas do CLW
- Conexões do Workstation

Duração da GC (ms)

Nome do caminho da métrica: `SuperDomain | Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) | Enterprise Manager | ApplicationTriageMap | Ontology engine:Average Process Time (ms)`

Descrição: a quantidade de tempo que a JVM gasta liberando memória não usada (coleta de lixo) em um intervalo de 15 segundos.

Produto: APM

Componente: Enterprise Manager

Versão: todas as releases suportadas

Impacto: se essa métrica exceder 1 segundo, significa que o EM em seus MOMs e coletores possivelmente estão com problemas de desempenho. Convém aumentar o tamanho da memória heap e alterar as configurações ou os algoritmos da coleta de lixo (GC).

Faixa: íntegro: <1.000 ms, risco: > 3.500 ms.

Correção: entre em contato com o Suporte da CA.

Ontology Engine: Average Process Time (ms)

Nome do caminho da métrica: `SuperDomain | Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) | Enterprise Manager | ApplicationTriageMap | Ontology engine:Average Process Time (ms)`

Descrição: a quantidade de tempo que o EM leva para processar alterações no mapa de topologia em um intervalo de 15 segundos.

Produto: APM

Componente: Enterprise Manager

Versão: todas as releases suportadas

Impacto: se essa métrica exceder 1 segundo, significa que o EM em seus MOMs e coletores possivelmente estão com problemas de desempenho.

Configuração: N/A

Faixa: íntegro: <1.000 ms, risco: > 3.500 ms.

Correção: entre em contato com o Suporte da CA.

Monitoramento do desempenho do CA APM usando métricas de suportabilidade

Monitore o desempenho da implantação do APM com as ferramentas de monitoramento de desempenho do APM. Para monitorar com eficácia seu ambiente de produção, é importante que os EMs (Enterprise Managers) estejam em estado íntegro.

O CA APM fornece as seguintes ferramentas que permitem detectar problemas e impedir que mudanças inesperadas comprometam seu ambiente de monitoramento:

- Métricas de suportabilidade
- Alertas

Monitorar o desempenho usando métricas de suportabilidade do Enterprise Manager

A cada 15 segundos, o Enterprise Manager coleta e registra as métricas de integridade sobre seu próprio ambiente. Você pode exibir essas métricas para solucionar problemas de desempenho do Enterprise Manager examinando estas fontes:

- Árvore do navegador de métricas do Investigador
- Arquivo de log
- Guia Visão geral do Enterprise Manager

Exibir as métricas de suportabilidade na árvore do Navegador de métricas

Para um Enterprise Manager autônomo ou um MOM, as métricas de suportabilidade aparecem na árvore do Navegador de métricas abaixo do nível superior `*SuperDomain*` :

```
Custom Metric Host (Virtual)
   Custom Metric Process (Virtual)
    Custom Metric Agent (Virtual)(SuperDomain)
        Enterprise Manager
```

Em um ambiente agrupado, as métricas de suportabilidade do Coletor têm um caminho de métrica semelhante, mas o nível do agente da métrica personalizada inclui o nome da máquina e a porta do Coletor.

O exemplo a seguir mostra uma Árvore do investigador que tem um MOM e um Coletor:

```
Custom Metric Host (Virtual)
   Custom Metric Process (Virtual)
    Custom Metric Agent (Virtual)(SuperDomain)
        Enterprise Manager
    Custom Metric Agent (Virtual)(Collector1@5001)(SuperDomain)
        Enterprise Manager
```

Exibir as métricas de suportabilidade no arquivo de log

Por padrão, os Enterprise Managers gravam as métricas de suportabilidade em um arquivo de log denominado `perflog.txt` . As métricas de suportabilidade são geradas em intervalos de 15 segundos. O local padrão desse arquivo está no diretório `<pasta_principal_do_EM>/logs` .

Por padrão, o arquivo `perflog.txt` é gerado em um modo compactado. Os valores são separados por vírgulas, com cabeçalhos de coluna. Nesse formato, o arquivo `perflog.txt` pode ser facilmente importado em uma planilha para análise.

Desativar o modo compactado faz com que o Enterprise Manager grave o arquivo `perflog.txt` em um formato mais detalhado, mais adequado para leitura.

Siga estas etapas:

1. Abra o arquivo `IntroscopeEnterpriseManager.properties` .
2. Defina os seguintes valores de configuração:
   - `introscope.enterprisemanager.performance.compressed=false`
   - `log4j.logger.Manager.Performance=DEBUG, performance, logfile`
3. Salve e feche o arquivo `IntroscopeEnterpriseManager.properties` .

Exibir as métricas de suportabilidade na guia Visão geral do Enterprise Manager

Para exibir informações de resumo sobre as métricas de suportabilidade de um Enterprise Manager, selecione a pasta Enterprise Manager na árvore do navegador de métricas. Essas informações incluem uma guia Visão geral, que exibe gráficos que mostram as métricas de suportabilidade mais importantes em uma única exibição. A guia Visão geral do Enterprise Manager é uma ferramenta útil para uma análise rápida da carga e da utilização de recursos do Enterprise Manager.

Executar uma verificação de integridade de desempenho do agrupamento do APM

Como administrador, use o arquivo `perflog.txt` para revelar problemas comuns de integridade que afetam os Coletores em um agrupamento. Uma verificação padrão de integridade do desempenho consiste nas seguintes etapas:

- **Verificar o tamanho da fila de mensagens**
- **Verificar o tamanho máximo da memória heap**
- Analisar o

> **NOTE**
>
> Para obter uma verificação abrangente da integridade do ambiente agrupado, entre em contato com o departamento CA Services.

Verificar o tamanho da fila de mensagens

Siga estas etapas:

1. Abra o arquivo `IntroscopeEnterpriseManagerSupport.log` e pesquise `transport.outgoingMessageQueueSize`.

   > **NOTE**
   >
   > Se o arquivo de log não contiver uma entrada para essa métrica, o tamanho da fila de mensagens padrão será 3.000.

2. Para melhorar a taxa de transferência da fila de mensagens entre o MOM e os coletores, abra os arquivos `IntroscopeEnterpriseManager.properties` do MOM e de todos os coletores:
   a. Aumente a propriedade `transport.outgoingMessageQueueSize` para 6.000.
   b. Defina `transport.override.isengard.high.concurrency.pool.min.size` como 10.
   c. Defina a propriedade
      `transport.override.isengard.high.concurrency.pool.max.size`
      para 10.

   > **WARNING**
   >
   > Aumentar o tamanho da fila de mensagens e do pool em um determinado ponto pode fazer com que o Introscope consuma mais recursos. Não defina `transport.outgoingMessageQueueSize` como mais de 9.000. O tamanho mínimo e máximo do pool não deve exceder 20.

3. Reinicie todos os Enterprise Managers.

Verificar o tamanho máximo da memória heap

Siga estas etapas:

1. Nos parâmetros de inicialização da JVM, verifique se o tamanho da memória heap inicial (`-Xms`) e o tamanho máximo da memória heap (`-Xmx`) correspondem para o MOM e para todos os coletores. Esses valores devem ser os maiores possíveis, considerando a JVM do Java implantada e a RAM disponível. Por exemplo, para um EM que esteja em execução em uma JVM de 32 bits, o limite máximo de memória heap é de 1,5 GB no Windows ou 2 GB no Linux.

NOTE

Se o EM estiver em execução em uma JVM de 64 bits, o tamanho máximo da memória heap será limitado somente pela quantidade de RAM disponível.

2. Para definir o tamanho da memória heap, abra o arquivo `Introscope_Enterprise_Manager.lax` no diretório `<pasta_principal_do_EM>` e edite a propriedade `lax.nl.java.option.additional` .
   Exemplo: neste exemplo,
   `-Xms`
   e
   `-Xmx`
   são ambos definidos como 1024m.

   ```
   lax.nl.java.option.additional=-Xms1024m -Xmx1024m
   ```

3. Reinicie o Enterprise Manager.

Analisar o arquivo `Perflog.xlsx`

Para executar análises adicionais no Microsoft Excel, converta o arquivo `preflog.txt` para o formato `.xlsx` .

Siga estas etapas:

1. Renomeie o arquivo `<pasta_principal_do_EM>/logs/perflog.txt para perflog.csv` .
2. Abra o arquivo `perflog.csv` com o Microsoft Excel e execute as seguintes etapas de formatação:
   a. Selecione a primeira linha que contém os blocos:
      a. Clique com o botão direito do mouse na linha e selecione **Formatar células...**
      b. Selecione **Alinhamento** e selecione **Quebrar texto automaticamente**.
      c. Selecione **OK**.
   b. Exclua todas as linhas acima da linha que contém os blocos.
   c. Selecione **Exibir**, **Congelar Painéis** e selecione **Congelar Linha Superior**
   d. Selecione a primeira linha que contém os blocos, selecione **Dados** e selecione **Filtrar** para adicionar filtros às colunas.
   e. Selecione valores para os filtros e role o conteúdo da janela do filtro.
   f. Clique em **Arquivo**, selecione **Salvar como** e salve o arquivo no formato `.xlsx` .

Analise o arquivo convertido usando filtros nas seguintes colunas de métrica de desempenho:

- **Total JVM Memory (coluna B)**
  Relata o total de memória disponível para a JVM. Se a memória heap inicial (`-Xms`) e a memória heap máxima (`-Xmx`) forem iguais, o valor permanecerá relativamente inalterado ao longo do tempo. Essa integridade é causada pelo fato de o máximo de memória heap ser alocado logo após a inicialização, e não durante a coleta da JVM.
- **Total JVM Free Memory (coluna C)**
  Relata a quantidade de memória livre da JVM disponível em qualquer intervalo. Se a memória livre cair para um número de dois dígitos ou menos no Coletor, aumente o tamanho da memória heap disponível para a JVM. Adicione memória ao servidor, se necessário. Se você já tiver alocado memória suficiente para a JVM, investigue as outras colunas da planilha. Esse problema é incomum em um MOM.
- **Duração da coleta (coluna F)**
  Relata a duração da coleta. Essa métrica indica a quantidade de tempo que o Coletor gasta agregando as métricas de intervalos de 15 segundos antes de salvá-las no banco de dados SmartStor. Por exemplo, se a duração da coleta

frequentemente exceder 3.000 ms (3 segundos), é provável que o Coletor esteja tendo dificuldade para agregar as métricas do intervalo de entrada.

- **Duração do SmartStor (coluna G)** Relata a duração do SmartStor. Essa métrica indica a quantidade de tempo que o Coletor gasta gravando os dados coletados no disco. Valores de endereço que excedem 5.000 ms (5 segundos).

  NOTE

  É recomendável usar um disco separado em um controlador dedicado para armazenar dados do SmartStor. Verifique o local do diretório `/data` do SmartStor para garantir que o banco de dados SmartStor não compartilhe o disco com o Enterprise Manager. Verifique se a propriedade `introscope.enterprisemanager.smartstor.dedicatedcontroller` está definida como `true` no arquivo `IntroscopeEnterpriseManager.properties`.

Métricas de suportabilidade importantes do Enterprise Manager

As métricas de suportabilidade a seguir são úteis para prever tendências, detectar problemas e identificar causas raiz de problemas de capacidade do Enterprise Manager. Cada métrica é descrita com informações sobre como ela pode ser usada.

NOTE

Mais informações:

- Principais métricas de suportabilidade

Duração da coleta

A métrica `Duração da coleta` mostra o tempo, em milissegundos (durante um intervalo de 15 segundos), gasto na coleta de dados. Esta métrica geralmente é um bom indicador para determinar se o Enterprise Manager está acompanhando a carga de trabalho atual.

Como o tempo de execução da calculadora é um componente importante da duração da coleta, a métrica `Duração da coleta` é uma boa aproximação do uso da CPU. O valor ideal da métrica `Duração da coleta` é inferior a 3.500 ms [3,5 segundos]. Um valor superior a 7.500 ms [7,5 segundos] indica que o Enterprise Manager tem capacidade insuficiente de CPU para a carga da métrica e da calculadora.

É possível exibir a métrica nestes locais:

- Árvore do navegador de métricas em `Enterprise Manager | Tarefas`.
- `perflog.txt` em `Performance.Harvest.HarvestDuration`

Duração do SmartStor

A métrica `Duração do SmartStor` mostra o tempo necessário para que as métricas recebidas e geradas durante um intervalo sejam gravadas no banco de dados SmartStor.

A métrica `Duração do SmartStor` é um indicador do desempenho de gravação de E/S de disco do SmartStor. Valores inconsistentes indicam a contenção de recursos relacionados ao disco. Valores consistentemente altos indicam uma largura de banda de gravação em disco inadequada para a carga da métrica que está sendo tratada.

Em condições padrão do Enterprise Manager, o valor médio de `Duração do SmartStor` deve ser inferior a 3.500 ms (3,5 segundos). O valor de `Duração do SmartStor` *deve* ser inferior a 15.000 ms (15 segundos). Um valor de métrica superior a 15 segundos indica um Enterprise Manager sobrecarregado de forma crítica.

É possível exibir a métrica nestes locais:

- Árvore do navegador de métricas em `Enterprise Manager | Tarefas`
- `perflog.txt` em `Performance.SmartStor.Duration`

Número de métricas do coletor

A métrica `Número de métricas do coletor` mostra o número total de métricas que estão sendo rastreadas no momento no agrupamento. Essa métrica é a soma dos valores da métrica de suportabilidade de `Enterprise Manager | Conexões | Número de métricas` de todos os coletores do agrupamento.

É possível exibir a métrica nestes locais:

- Árvore do navegador de métricas em `Enterprise Manager | MOM | Número de métricas do coletor`.
- `perflog.txt` em `Performance.MOM.NumberOfCollectorMetrics`

Métricas do coletor recebidas por intervalo

A métrica `Métricas do coletor recebidas por intervalo` é a soma dos pontos de dados da métrica do Coletor que o MOM recebeu a cada intervalo de 15 segundos. Os pontos de dados são provenientes destas fontes:

- Assinaturas de métrica em nome dos Módulos de gerenciamento, por exemplo, painéis, calculadoras, alertas
- Consultas que os clientes geram, por exemplo, consultas do Workstation e da CLW
- Consultas para métricas que são geradas por alertas e calculadoras integrados

A métrica `Métricas do coletor recebidas por intervalo` é um indicador da carga da consulta do agrupamento e do consumo de largura de banda da rede para a comunicação entre o Coletor e o MOM. Alguma variação é esperada. Picos grandes indicam forte atividade de consulta espontânea. O valor de `Métricas do coletor recebidas por intervalo` aproxima as métricas de número que as calculadoras estão processando.

É possível exibir a métrica nestes locais:

- Árvore do navegador de métricas em `Enterprise Manager | MOM | Métricas do coletor recebidas por intervalo`
- `perflog.txt` em `Performance.MOM.CollectorMetricsReceivedPerInterval`

Alerts: Total Number of Evaluated Metrics

Os alertas são *calculadoras dependentes* porque operam na saída de outras calculadoras. As calculadoras dependentes não podem ser executadas em paralelo às calculadoras que fornecem suas entradas. Por esse motivo, os alertas podem estender a duração da coleta mais do que calculadoras não dependentes. A métrica de suportabilidade Alerts: Total Number of Evaluated Metrics exibe o número de métricas que os alertas processaram durante cada intervalo.

É possível exibir a métrica na árvore do navegador de métricas em `Enterprise Manager | Internal | Alertas`.

Se um aumento na duração da coleta for correlacionado a um aumento nas métricas avaliadas pelos alertas, você poderá aumentar a capacidade do EM otimizando os alertas. Para identificar os alertas que consomem mais recursos, pesquise e classifique por valor todas as métricas cujo nome corresponda à seguinte expressão regular:

```
(.*)Enterprise Manager|Internal|(.*)Alerts(.*)Number of Evaluated Metrics
```

Se o Introscope tiver alertas para avaliar um grande número de métricas (especialmente métricas de vários coletores), considere estas ações:

- Desativar os alertas que fornecem pouco valor.
- Ajustar as expressões regulares nos grupos de métricas alertados para incluir apenas as métricas mínimas necessárias para indicar a condição com alerta.
- Dividir o alertas que avaliam as métricas de vários coletores em vários alertas que avaliem apenas as métricas de um único coletor. Essa ação não reduz necessariamente o número de métricas que o MOM processa, mas melhora o desempenho da consulta em todo o agrupamento.

Capacidade geral (%)

A métrica `Capacidade geral (%)` estima a porcentagem da capacidade do Enterprise Manager que é consumida.

É possível exibir a métrica na árvore do navegador de métricas em `Enterprise Manager |` .

A métrica `Capacidade geral (%)` é calculada, em parte, a partir das seguintes métricas de contribuição, que podem ser exibidas na árvore do navegador de métricas em `Enterprise Manager | Integridade` :

- CPU Capacity (%)
- GC Capacity (%)
- Capacidade de coleta (%)
- Métrica Heap Capacity (%)
- Capacidade dos dados de entrada (%)
- Capacidade do SmartStor (%)

A métrica `Capacidade geral (%)` é mais valiosa em um período longo do que para um período específico de 15 segundos. Como a métrica `Capacidade geral (%)` se baseia em métricas em tempo real, o valor de `Capacidade geral (%)` pode subir um pouco mais de 100%. O pico pode ocorrer, por exemplo, porque o subsistema de E/S do hardware fica sobrecarregado rapidamente. No entanto, o Enterprise Manager tende a se recuperar dessas situações de pico automaticamente quando elas não são duradouras. Em geral, um pico, por exemplo, para 200% não é motivo para preocupação se for temporário. No entanto, em um longo período, a média ideal de `Capacidade geral (%)` é de 75% ou menos.

Durante os períodos em que a métrica `Capacidade geral (%)` sobe para valores altos, pelo menos uma das outras métricas de contribuição provavelmente também mostra um pico. Investigar e compreender a origem do pico secundário pode ajudar a identificar a causa raiz do problema de recurso. Por exemplo, você pode encontrar o problema analisando a métrica Heap Capacity (%), que alimenta a métrica `Capacidade geral (%)` .

Exibir a métrica `Capacidade geral (%)` no modo histórico é útil para uma exibição geral e comparativa do status de capacidade do Enterprise Manager. No entanto, a carga de trabalho do Enterprise Manager é complexa, e vários aspectos da carga de trabalho afetam a métrica `Capacidade geral (%)` de maneiras diferentes e não lineares. Por exemplo, a duração das tarefas de manutenção do SmartStor (spool para conversão e reperiodização de dados) pode ser um indicador importante da capacidade do Enterprise Manager. No entanto, essas tarefas de manutenção não participam diretamente do cálculo de `Capacidade geral (%)` . As tarefas de manutenção do SmartStor causam um aumento na utilização de CPU e memória heap. O aumento da utilização resulta em um aumento no percentual da capacidade. No entanto, a magnitude do aumento não reflete o impacto total dos problemas de manutenção do SmartStor.

A métrica `Capacidade geral (%)` é focada principalmente na maneira como um Enterprise Manager lida com a carga de trabalho de métricas do agente. Essa métrica não avalia diretamente a capacidade em relação aos dados do CA CEM. Por exemplo, a métrica `Capacidade geral (%)` não reflete os serviços do Enterprise Manager sobrecarregados ou os problemas de E/S do banco de dados do APM.

Heap Capacity (%)

A métrica `Heap Capacity (%)` mostra quanto da memória heap alocada está em uso. Essa métrica é normalizada para 75% da memória heap alocada para fornecer um buffer de segurança e evitar falhas. Um valor de métrica de 100 significa que a memória heap alocada é utilizada apenas 75%.

A métrica `Heap Capacity (%)` permite avaliar se a memória heap alocada para um Enterprise Manager é suficiente para a carga. Essa métrica também permite detectar tendências que afetam o uso da memória heap. Às vezes, uso elevado da CPU, a alta duração da coleta ou ambos podem resultar da alta utilização da memória heap.

É possível exibir a métrica na árvore do navegador de métricas em `Enterprise Manager | Integridade` .

Number of Historical Metrics

A métrica `Número de métricas históricas` é o número total de métricas que um Enterprise Manager detectou e manteve no SmartStor. Esse número aumenta à medida que os agentes relatam novas métricas e diminui à medida que

as métricas expiram no SmartStor. A desconexão temporária do agente e o reporte de mais dados para uma métrica existente não alteram esse número.

O número de métricas históricas afeta o desempenho da consulta histórica e a sobrecarga da reperiodização noturna do SmartStor. Um valor crescente pode indicar os seguintes problemas:

- **Vazamento de métricas**
  Um número gradualmente crescente de métricas devido a um ambiente de monitoramento instável com conexões de agente não controladas
- **Explosão de métricas**
  Um número rapidamente crescente de métricas devido ao surgimento de muitos agentes novos ou de métricas do Agente para SQL especificadas incorretamente

É possível exibir a métrica na árvore do navegador de métricas em `Enterprise Manager | Conexões`.

Partial Metrics without Data

A métrica `Partial Metrics without Data` informa o número de métricas do agente que não estão mais sendo relatadas dinamicamente. Essas métricas consomem memória heap e afetam negativamente o desempenho da consulta, contribuindo para a contagem de métricas `Historical Metrics`.

As penalidades de desempenho serão pequenas, a menos que o valor da métrica `Partial Metrics without Data` se torne grande.

Se você tiver problemas com capacidade de resposta da consulta histórica ou com os tempos longos de reperiodização do SmartStor, compare o valor da métrica `Partial Metrics without Data` com o valor da métrica `Partial Metrics with Data`. É possível exibir a métrica `Partial Metrics with Data` na árvore do navegador de métricas em `Enterprise Manager | Data Store | SmartStor | MetaData`. Se o valor da métrica `Partial Metrics without Data` se aproximar do valor da métrica `Partial Metrics with Data`, use as ferramentas SmartStor para remover metadados indesejados das métricas.

É possível exibir a métrica neste local:

- Árvore do navegador de métricas em `Enterprise Manager | Data Store | SmartStor | MetaData`

Number of Traces in Insert Queue

O Enterprise Manager tenta inserir todos os eventos de entrada em uma fila de inserção de Rastreamento de transação. A métrica `Number of Traces in Insert Queue` exibe o número médio de eventos na fila durante o intervalo anterior.

A métrica `Number of Traces in Insert Queue` indica se o Enterprise Manager está acompanhando o processamento do Rastreamento de transação. Se a fila de inserção do Rastreamento de transação estiver cheia quando um novo evento entrar, o evento será descartado. É possível exibir a métrica `Transações: Número de itens descartados por intervalo` para ver o número de Rastreamentos de transação que o Enterprise Manager não pôde controlar durante o intervalo e que foram descartados.

É possível exibir a métrica `Transações: Número de itens descartados por intervalo` nos seguintes locais:

- Árvore do navegador de métricas em `Enterprise Manager | Data Store | Transações`
- `perflog.txt` em `Performance.Transactions.Num.Dropped.Per.Interval`

É possível exibir a métrica `Number of Traces in Insert Queue` nos seguintes locais:

- Árvore do navegador de métricas em `Enterprise Manager | Data Store | Transações`
- `perflog.txt` em `Performance.Transactions.TT.Queue.Size`

Consultas do SmartStor por intervalo

A métrica `Consultas do SmartStor por intervalo` mostra o número de consultas para dados de métrica que foram recebidas durante o intervalo anterior.

O equilíbrio de gravações de métricas que são comparadas às consultas de métrica determina seus requisitos de configuração de disco do SmartStor.

Para avaliar o desempenho do carregamento de consulta da métrica, verifique estas métricas:

- Métrica `Consultas do SmartStor por intervalo`
- Métrica `Duração de consultas do SmartStor (ms)`
  Essa métrica mostra a duração média da consulta durante o intervalo anterior.

Você pode exibir a métrica `Duração de consultas do SmartStor (ms)` e a métrica `Consultas do SmartStor por intervalo` nestes locais:

- Árvore do navegador de métricas em `Enterprise Manager | Internal | Consulta`
- `perflog.txt`

Mais métricas de suportabilidade do Enterprise Manager

Use a lista a seguir de outras métricas úteis de suportabilidade.

- **`CPU usada do EM (%)`**
  Utilização do processador por segmentos do EM (Enterprise Manager) durante o período medido. Em um intervalo de 15 segundos, a utilização é: `<ms do processador usado pelo EM>/(15000 * <# de processadores>)`.
  Localizado na árvore do investigador em `Enterprise Manager|CPU`.

  NOTE

  Esse número não reflete a utilização total do processador durante o intervalo. Essa métrica mede apenas a participação do Enterprise Manager na utilização total do processador.
- **`Número de agentes`**
  O número de agentes conectados no momento.
  Exiba a árvore do navegador de métricas em `Enterprise Manager | Conexões`.
- **`Capacidade de coleta (%)`**
  O percentual de tempo para a coleta de dados em um intervalo de 15.000 ms (15 segundos), em que 100% é o total de 15 segundos. Por exemplo, se a duração da coleta for 15.000 ms, o valor dessa métrica será 100.

  NOTE

  Em um ambiente de monitoramento íntegro, a capacidade de coleta permanece abaixo de 25%.

  Exiba a árvore do navegador de métricas em `Enterprise Manager | Integridade`.
- **`Número de métricas`**
  A carga de métricas em um Enterprise Manager. Quando um agente é desconectado, esse número cai.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Conexões`.
- **`Capacidade do SmartStor (%)`**
  O percentual de tempo que o processo de gravação do SmartStor leva em um intervalo de 15.000 ms (15 segundos), em que 100% é o total de 15 segundos. Por exemplo, se a duração da gravação do SmartStor for 15.000 ms, o valor dessa métrica será 100.

  NOTE

  Em um ambiente de monitoramento íntegro, a capacidade do SmartStor permanece abaixo de 25%.

  Localizado na árvore do navegador de métricas em `Enterprise Manager | Integridade`.
- **`Active Incoming Threads`**
  O número de segmentos que lidam ativamente com mensagens dos clientes.

A métrica Active Incoming Threads fornece informações sobre a simultaneidade da execução de consultas. Várias consultas de métrica simultâneas podem interferir em outras atividades do SmartStor e aumentar a duração do SmartStor.
Localizado na árvore do navegador de métricas em `Enterprise Manager | Messaging`.

- **`Active Outgoing Threads`**
  O número de segmentos que entregam dados ativamente aos clientes.
  Essa métrica é um indicador da simultaneidade de consultas. Um aumento no número de segmentos que trabalham na entrega de dados pode indicar problemas de rede.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Messaging`.
- **`Number of Dependent Calculator Input Metrics`**
  O número total de métricas que são entradas para calculadoras dependentes.
  As calculadoras dependentes operam em valores de métrica que outras calculadoras produzem. As entradas para calculadoras dependentes também podem incluir valores de métrica que são relatados por agentes. Essa contagem se refere a todas as métricas fornecidas às calculadoras dependentes, e não apenas às métricas produzidas por outras calculadoras.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Internal`.
- **`Number of Non Dependent Calculator Input Metrics`**
  O número total de métricas que são entradas para calculadoras não dependentes.
  As calculadoras não dependentes operam em métricas que são relatadas por agentes, e não nas métricas que são a saída de outras calculadoras.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Internal`.
- **`Total Number of Evaluated Metrics (Calculators)`**
  O número total de métricas avaliadas para todas as calculadoras. A soma do número de métricas de entrada da calculadora dependente e do número de métricas de entrada da calculadora não dependente.
  Quando essa contagem chega ao pico, o Enterprise Manager está realizando muitos cálculos em tempo real, o que pode sobrecarregar os recursos da CPU.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Internal | Calculadoras`.
- **`<nome da calculadora> | Total Number of Evaluated Metrics`**
  O número total de métricas avaliadas para uma calculadora individual.
  O valor dessa métrica indica quanto a calculadora associada contribui para a duração da coleta. Concentre-se nas calculadoras que avaliam um grande número de métricas para otimizar a capacidade do Enterprise Manager.

  > **NOTE**
  > Essa métrica é exibida no investigador somente quando a calculadora é definida.

  Localizado na árvore do navegador de métricas em `Enterprise Manager | Internal`.
- **`Alert Action Processing Time (ms)`**
  O tempo decorrido que o Enterprise Manager leva para processar todas as ações de alerta.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Harvest`.
- **`Calculator Queries Wait Time (ms)`**
  O tempo decorrido para o segmento de consultas da calculadora concluir seu trabalho atual, incluindo aguardar a finalização do loop de consulta fora da calculadora.
  O novo processamento de consulta da calculadora é iniciado depois que todas as entregas fora da calculadora do intervalo anterior são feitas para o cliente. Quando essa contagem chega ao pico, o Enterprise Manager está realizando muitos cálculos em tempo real, o que pode sobrecarregar os recursos da CPU.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Harvest`.
- **`Non Calculator Queries Delivery Time (ms)`**
  O tempo que o Enterprise Manager levou para executar e entregar consultas fora da calculadora a todos os clientes solicitantes em um intervalo.
  Após a execução de todas as consultas de calculadora, o Enterprise Manager executa consultas fora da calculadora. Em seguida, o EM envia os resultados a todos os clientes que os solicitaram. Quando essa contagem atinge ao pico,

significa que o Enterprise Manager está enviando muitos resultados de consulta fora da calculadora aos clientes, o que pode sobrecarregar a rede.
Localizado na árvore do navegador de métricas em `Enterprise Manager | Harvest`.

- **`Non Calculator Queries Excess Time (ms)`**
  O excesso de tempo de espera para consultas fora da calculadora a serem concluídas além de um intervalo.
  Os clientes enviam solicitações de consulta fora da calculadora ao Enterprise Manager, que envia os resultados de volta. Se esse processo não for concluído dentro de um intervalo, ele será transmitido até ser concluído.
  Essa métrica mostra por quanto tempo além de um intervalo as consultas fora da calculadora são estendidas.
  Use essa métrica para determinar se consultas fora da calculadora estão sobrecarregando um Enterprise Manager.
  Em geral, o valor dessa métrica é 0 quando o Introscope tem uma carga pequena. Um valor maior que 0 indica que o Enterprise Manager está sobrecarregado e não é possível processar consultas de métricas dentro de um intervalo.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Harvest`.
- **`Metrics From All Agents`**
  Número total de métricas exclusivas geradas por todos os agentes conectados que enviaram dados no último intervalo. Essa contagem não inclui métricas históricas. As configurações de limite não afetam essa contagem.
  Quando o limite de introscope.enterprisemanager.agent.metrics.limit é disparado, o valor dessa métrica informa em quanto o limite foi excedido.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Harvest`.
- **`Spooling Data File Write Time (ms)`**
  O tempo que o Enterprise Manager levou para gravar os dados coletados no arquivo de spool (`.spool`) em um intervalo.
  Use essa métrica para monitorar o ciclo de coleta.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Harvest`.
- **`Spooling Preparation Time (ms)`**
  O tempo que o Enterprise Manager levou para preparar os dados coletados a serem gravados no arquivo de spool (.spool) em um intervalo.
  Use essa métrica para monitorar o ciclo de coleta.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Harvest`.
- **`Total Number of Evaluated Metrics (Management Module Calculators)`**
  O número de métricas que são entradas para as calculadoras do Módulo de gerenciamento.
  Quando esse número atinge o pico, indica que uma consulta ou calculadora com uma consulta corresponde a métricas demais.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Internal | Módulo de gerenciamento | Calculadoras`.
- **`Metric Matches Per Interval`**
  O número total de métricas que foram avaliadas em todas as consultas no último intervalo.
  Essa métrica mostra um valor quando ocorrem estas ações:
  - Novos agentes se conectam ao Enterprise Manager.
  - As expressões regulares são usadas em consultas internas e consultas geradas pelo usuário, incluindo agrupamentos de métricas do Módulo de gerenciamento.
  - Os usuários selecionam as métricas na árvore do navegador de métricas.
  - Os usuários abrem painéis que contêm gráficos.

  Quando o valor dessa métrica é alto, significa que muitas consultas estão ocorrendo em pouco tempo.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Internal | Metric Group`.
- **`Queued Queries Per Interval`**
  Número de consultas que, no momento, estão aguardando o processamento no intervalo do ciclo de coleta. O valor geralmente é zero após a inicialização.
  Localizado na árvore do navegador de métricas em `Enterprise Manager | Internal | Metric Group`

Métricas de suportabilidade do pool de conexões do banco de dados do APM

Os serviços do Enterprise Manager fornecem métricas que descrevem a alocação e o uso dos pools de conexões do banco de dados do APM. Esses pools permitem a troca de dados entre os serviços do Enterprise Manager e o banco de dados do APM. As métricas de suportabilidade do pool de conexões do banco de dados do APM são exibidas no Workstation Investigator em:

```
Custom Metric Agent|Enterprise Manager|Internal|Database|Connection Pools
```

Elas também estão disponíveis no arquivo de log `tessperflog.txt` e têm o prefixo `Internal.Database.Connection Pools.`

As métricas são fornecidas para as origens de dados do APM:

O nome `apmDataSource` identifica a origem de dados do APM.

A lista a seguir descreve as métricas de suportabilidade do pool de conexões do banco de dados do APM:

- **`numBusyConnections`**
  Número de conexões atualmente em uso
- **`numConnections`**
  Número de conexões abertas
- **`numIdleConnections`**
  Número de conexões abertas que não estão em uso
- **`numUnclosedOrphanedConnections`**
  Número de conexões abertas que permaneceram não utilizadas após excederem um limite de tempo.
- **`threadPoolNumTasksPending`**
  Número de tarefas em fila aguardando uma conexão

Monitorar conexões da estação de trabalho usando métricas de suportabilidade

A métrica de suportabilidade `Conexões: Número de estações de trabalho` mostra o número atual de conexões da estação de trabalho. Para os coletores em um ambiente agrupado, o valor dessa métrica é 0.

Consulte a métrica `Conexões: Número de estações de trabalho` aqui na árvore do navegador de métricas:

```
*SuperDomain*|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|
Custom Metric Agent (Virtual)(*SuperDomain*)|Enterprise Manager|
Connections:Number of Workstations
```

> **NOTE**
> A
> `Connections:Number of Workstations`
> métrica não reflete as conexões da Command Line Workstation (CLW) ou do WebView.

Istio Support

O DX APM Istio Support relata métricas e rastreamentos de transação de aplicativos (geralmente microsserviços) instrumentados com os rastreadores em conformidade com o OpenTracing.

O Istio é um service mesh de código aberto e independente de fornecedor que as organizações usam para reduzir a complexidade de seus ambientes de nuvem híbrida e de várias nuvens. O Istio injeta um proxy do sidecar no pod em que um recipiente de aplicativos está em execução. O proxy do sidecar monitora as solicitações de aplicativo de entrada e saída do tráfego de rede (geralmente, microsserviços).

O DX APM estende o importador Prometheus do UMA (Universal Monitoring Agent) para relatar os dados de solicitação de proxy do sidecar do Istio. O Istio Support relata as métricas de integridade do aplicativo e do Istio, além de exibir os rastreamentos de transação e os dados de mapeamento do Team Center.

Versões suportadas do Istio

- Istio 1.4.x

Ativar o back-end do importador Prometheus para suporte ao Istio

Ative o back-end do importador Prometheus no Istio Support antes de instalar o UMA.

Siga estas etapas:

1. Abra o arquivo apropriado para o seu ambiente em um editor de texto:
   - (Operador do UMA) Vá até o diretório `uma-operator` e abra o arquivo `uma_cr.yaml` .
   - (Gráfico Helm) Vá até o diretório `helm-chart/uma` e abra o arquivo `values.yaml` .
   - (Arquivo YAML do UMA) Vá até o arquivo YAML do aplicativo, que é denominado `ca-uma-agent.yaml` .
2. (Operador do UMA/Gráfico Helm) Configure a propriedade `prometheus.backend.enabled` .

   NOTE
   Ignore essa etapa se você usar o arquivo YAML do UMA para instalar o UMA. O arquivo `ca-uma-agent.yaml` ativa o suporte ao back-end do importador Prometheus por padrão.

   a. Localize a propriedade `prometheus.backend.enabled` .
   b. Defina a propriedade `prometheus.backend.enabled` como `true` . O valor padrão é `false` .
3. Defina o URL do back-end do importador Prometheus.
   a. (Operador do UMA/Gráfico Helm) No arquivo apropriado (`uma_cr.yaml` para Operador do UMA/`values.yaml` para gráfico Helm), adicione o URL do back-end do importador Prometheus após **url:**. Veja esta seção do arquivo:

   ```
   container: | prometheus: | backend: | endPoint: | url: <URL>
   ```

   b. (Operador do UMA/Gráfico Helm) Quando o URL do back-end do importador Prometheus estiver protegido, forneça o nome de usuário e a senha.

   No arquivo apropriado (`uma_cr.yaml` para o Operador do UMA/`values.yaml` para o Gráfico Helm), insira as credenciais nas propriedades username: e password: nestas seções do arquivo:

   ```
   container: | prometheus: > backend: | endPoint: | username: | and prometheus: | backend: | endPoint: |
    username:
   container: | prometheus: | backend: > endPoint: | username: | and prometheus: | backend: | endPoint: |
    password:
   ```

   Veja a seguir exemplos de configurações para os arquivos `uma_cr.yaml` e `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
   ```

   (Arquivo YAML do UMA)

   No arquivo YAML do aplicativo, defina a propriedade `Prometheus_server_url` como Prometheus_server_url: "<*URL*>". Certifique-se de incluir um símbolo de aspas duplas `"` antes e depois do URL. Aqui está um exemplo:

   ```
   Prometheus_server_url: “http://10.80.89.157:30007/”
   ```

Instalar o Istio Support usando o UMA

Depois de configurar a conexão com o back-end do Prometheus, instale o UMA usando uma das destas opções:

- Operador do Kubernetes
- Gráfico do Helm
- Arquivo YAML do UMA

Consulte Instalar e configurar o Universal Monitoring Agent para Kubernetes para instalar o UMA.

Métricas do Istio

O UMA implementa o pod **cluster-performance-prometheus** com o importador Prometheus ativado, como mostrado nesta captura de tela de exemplo:

```
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/clusterinfo-866886f49f-mb5tt                    1/1     Running   0          21h
pod/container-monitor-8655dfd798-ffs4q              1/1     Running   0          21h
```

O agente do DX APM Prometheus extrai as métricas do servidor do Prometheus e relata as métricas sob o nó **Istio**. Este é o caminho do navegador de métricas:

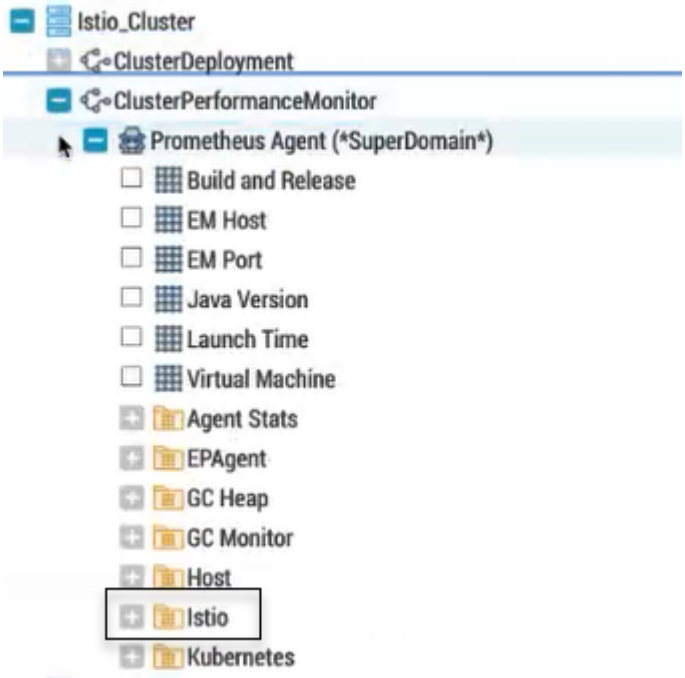
SuperDomain | <*nomeDoCluster*> | ClusterPerformanceMonitor | Prometheus Agent | Istio

Você fornece o nome do cluster na propriedade `clusterName` do arquivo `uma_cr.yaml` (Operador do UMA) ou do arquivo `values.yaml` (Gráfico Helm).

- Exemplo: `DevelopmentCluster`
- Valor padrão: `SandBox`

Nesse caso, o caminho do navegador de métricas seria um SuperDomain | ?DevelopmentCluster? ou ?SandBox? | ClusterPerformanceMonitor | Agente do Prometheus | Istio

Após a instalação do UMA, o DX APM exibe o nó **Istio** abaixo do nó **Prometheus Agent**, conforme mostrado nesta captura de tela:



O Istio Support fornece duas categorias de métrica. A primeira categoria refere-se às métricas de serviços e cargas de trabalho, que fornecem dados de desempenho sobre os aplicativos em execução no service mesh Istio. A segunda categoria refere-se às métricas de integridade específicas do Istio.

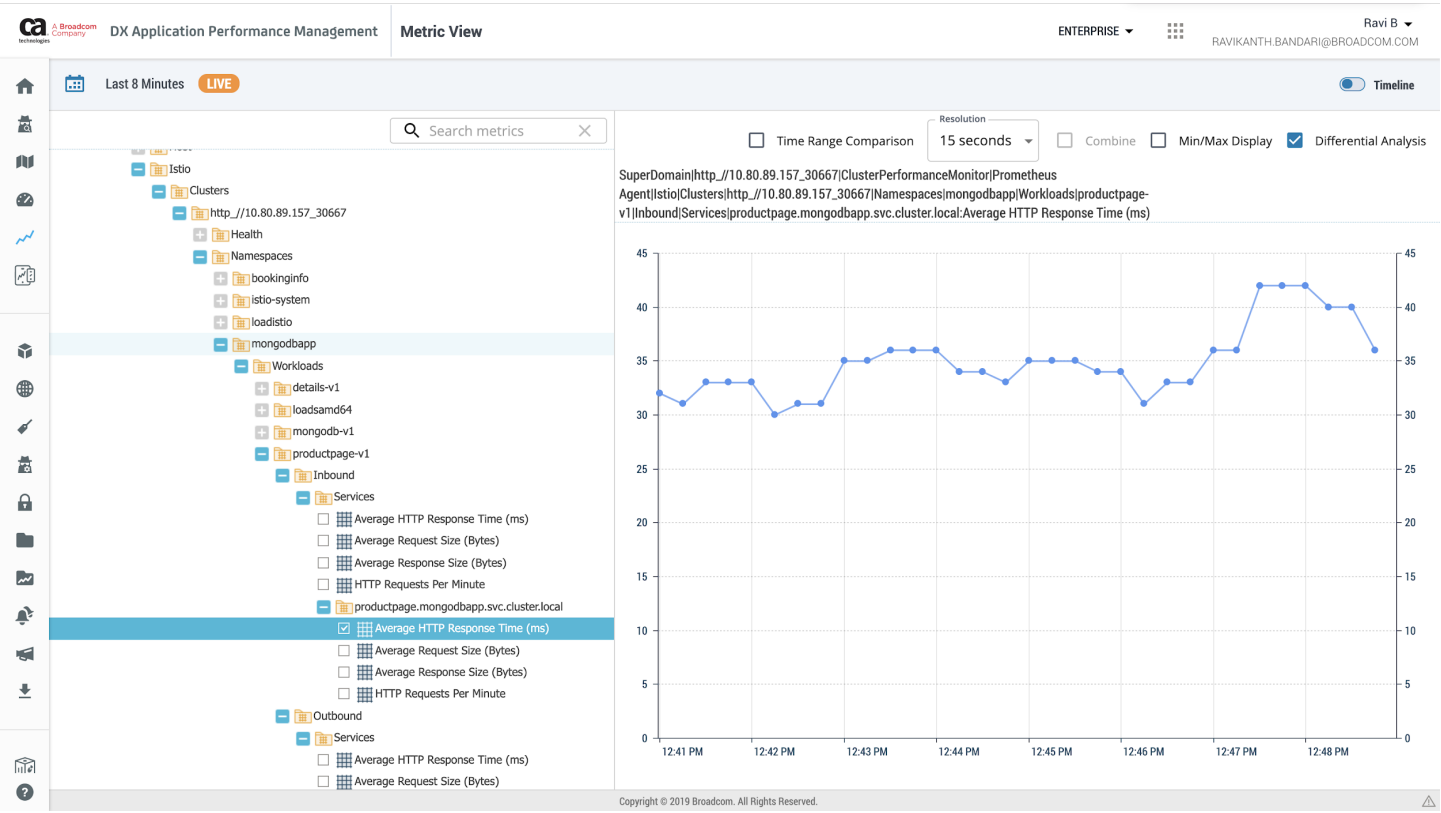
Métricas de carga de trabalho e serviços do Istio Support

No Istio Support, um *serviço* se refere a um serviço Kubernetes ou OpenShift. Uma *carga de trabalho* se refere a uma implementação de Kubernetes ou OpenShift. Os termos *entrada* e *saída* referem-se ao tráfego de rede que entra ou sai de um serviço ou uma carga de trabalho Kubernetes ou OpenShift.

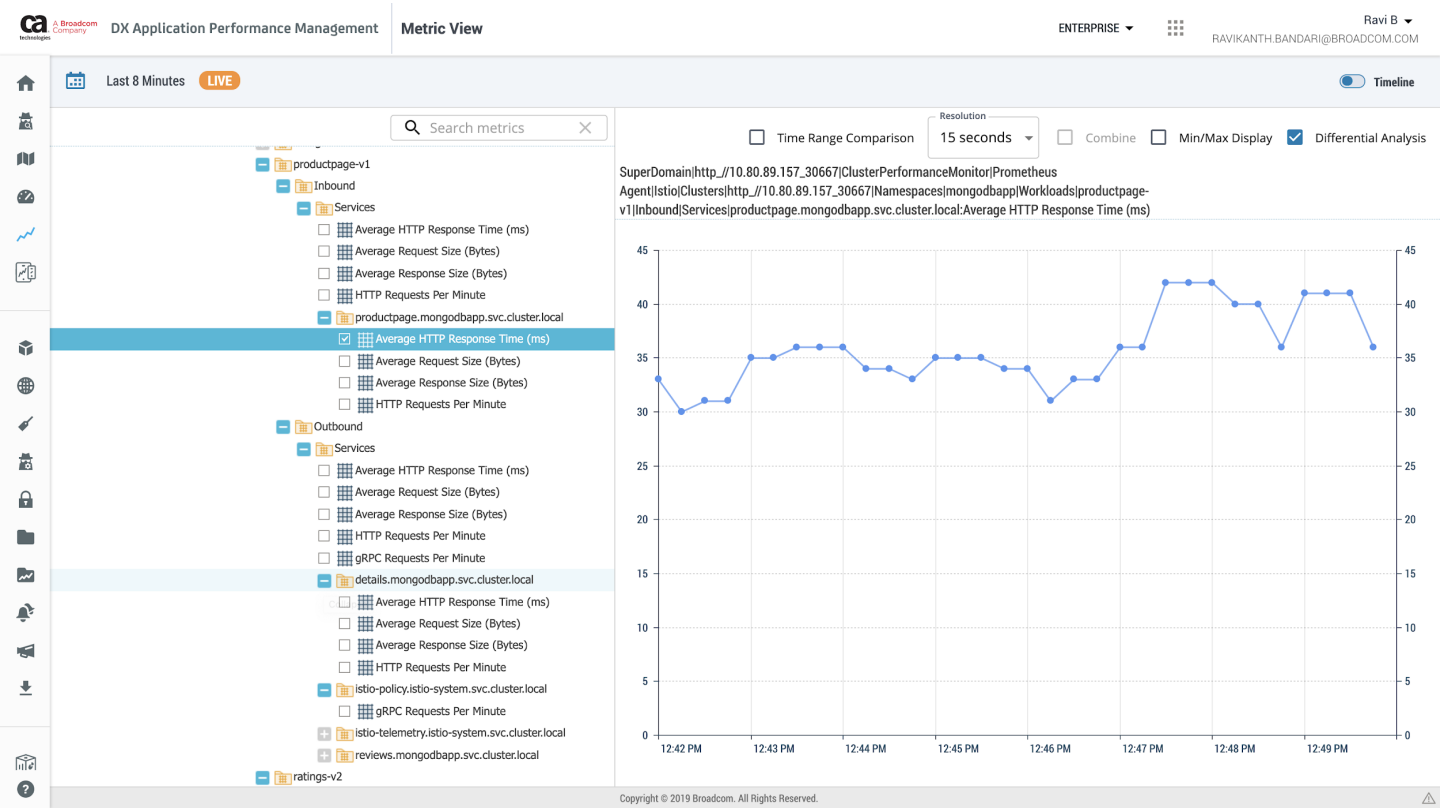
O Istio Support relata essas métricas por serviço ou carga de trabalho. O Istio Support não relata todas as métricas para cada serviço ou carga de trabalho. As métricas que o Istio Support relata dependem do tipo de tráfego que está fluindo pelo serviço ou pela carga de trabalho: HTTP, chamadas de procedimento remoto (gRPC) e TCP (Transmission Control Protocol). Por exemplo, quando os tráfegos HTTP e gRPC estão fluindo por meio de um serviço ou uma carga de trabalho, o Istio Support relata todas as métricas que estão relacionadas ao HTTP e gRPC. Este é o caminho do navegador de métricas para as métricas de serviços e de carga de trabalho:

SuperDomain | <*nomeDoCluster*> | ClusterPerformanceMonitor | Prometheus Agent | Istio | Clusters | <*URL do back-end do importador Prometheus*> | namespaces | <*nome do aplicativo*> | Workloads | <*Nome da carga de trabalho*> | Inbound/Outbound | Services | <*Nome do serviço*> |

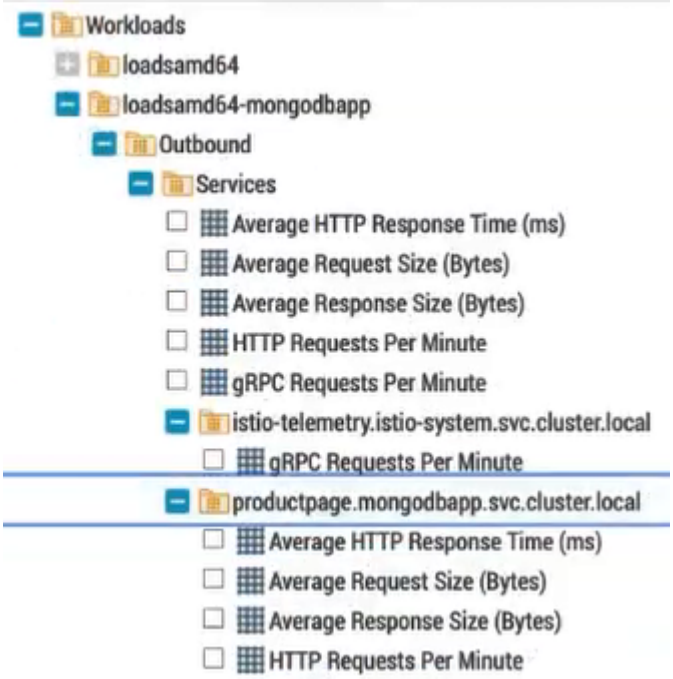
Na primeira das duas próximas capturas de tela, o navegador de métricas exibe as métricas de todos os **serviços** de **entrada** e alguns de **saída** para o aplicativo **mongdbapp**. Em ambas as capturas de tela, o gráfico exibe os dados da métrica **Average Response Time** para o aplicativo **mongdbapp**, a carga de trabalho **productpage-v1** e o serviço de entrada **productpagemongodbapp.svc.cluster.local**. Observe que a carga de trabalho **productpage-v1** também possui serviços de entrada e de saída.



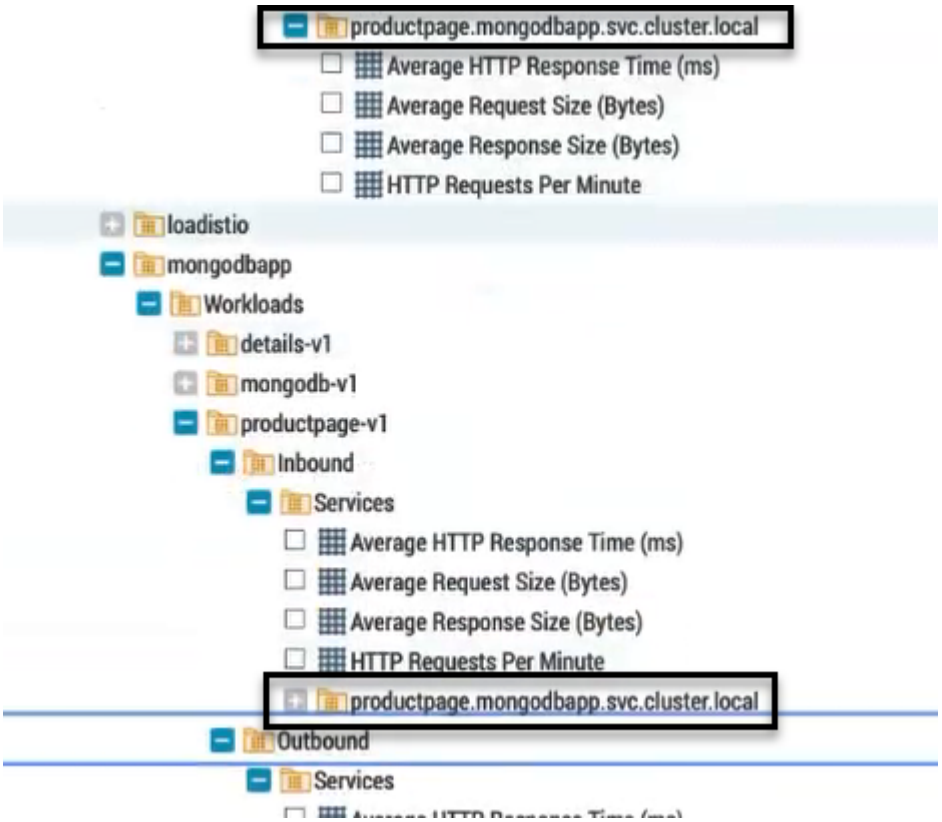
Na primeira das duas próximas capturas de tela, o navegador de métricas exibe as métricas de todos os **serviços** de **entrada** e alguns de **saída** para o aplicativo **mongdbapp**.



Às vezes, uma carga de trabalho tem apenas tráfego de saída. Nesta captura de tela, o navegador de métricas exibe uma carga de trabalho do MongoDB chamada **loadsamd64-mongod**. Essa carga de trabalho tem apenas comunicação de saída, enviando tráfego para dois serviços: telemetria (**istio-telementry.istio-system.sve.cluster.local**) e productpage (**productpage.mongodbapp.svc.cluster.local**).



Na próxima captura de tela, observe que o tráfego de entrada mostra a solicitação proveniente do serviço **productpage.mongodb.svc.cluster.local**.



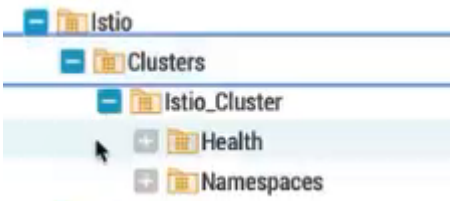
Veja a seguir as métricas de carga de trabalho e serviço do Istio Support:

- 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

Métricas de integridade do Istio Support

As métricas de integridade do Istio Support fornecem informações sobre o desempenho específico do Istio e são exibidas no diretório **Health**. Este é o caminho completo do navegador de métricas:

SuperDomain | <*nomeDoAgrupamento*> | ClusterPerformanceMonitor | Prometheus Agent | Istio | Clusters | Istio Cluster or <*URL de back-end do Importador Prometheus*> | Health



As métricas de integridade são obtidas dos componentes Citadel, Pilot e Gallery do Istio. Esta tabela descreve as métricas de integridade por componente:

Métricas do Citadel

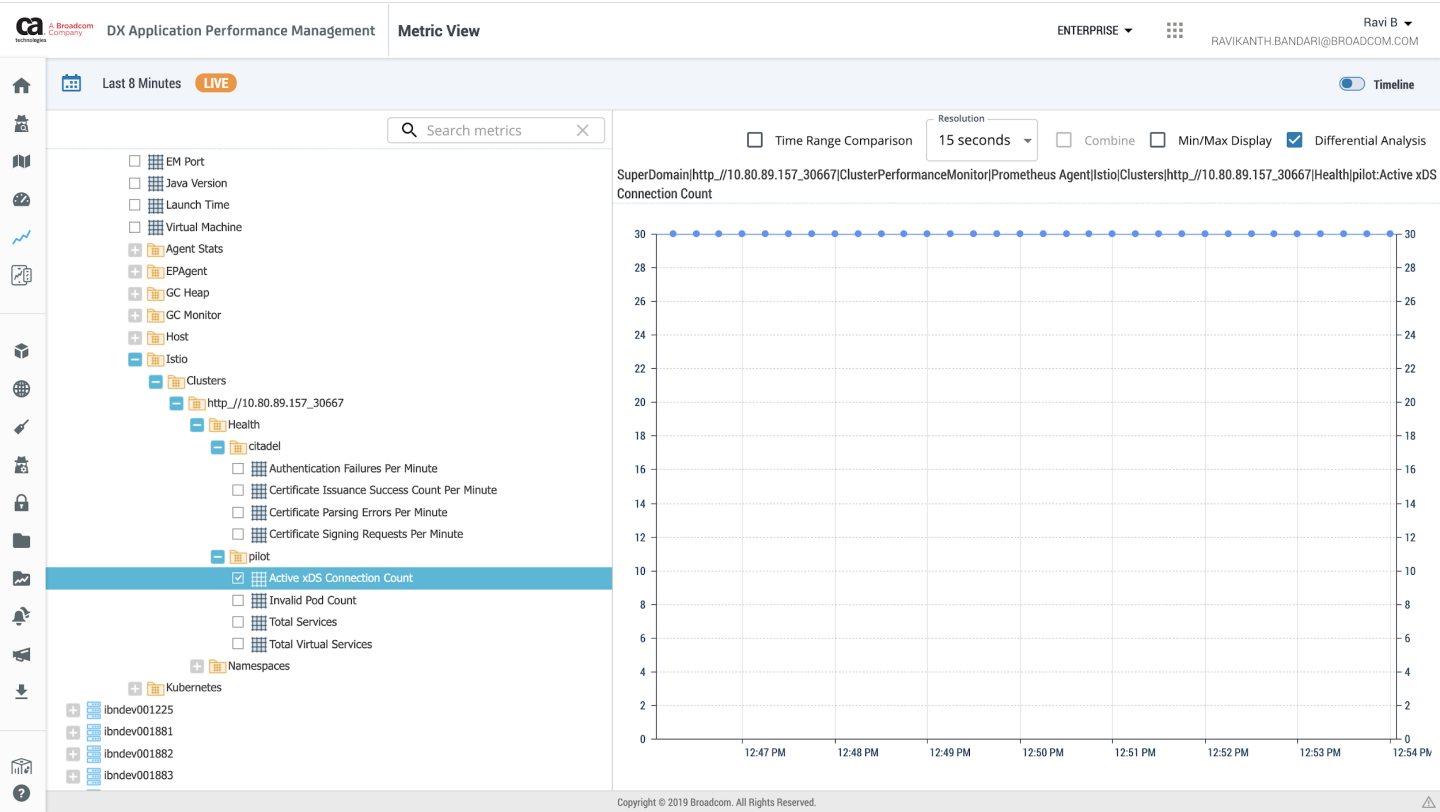
- **Authentication Failures Per Minute**
  Sasanka: http://10.80.89.157:30007/ no exemplo de arquivo é um URL interno da CA?
- **Certificate Issuance Success Count Per Minute**
  O número de emissões de certificados que tiveram êxito por minuto.
- **Certificate Parsing Errors Per Minute**
  O número de erros por minuto que ocorrem durante a análise das CSRs (Certificate Signing Requests - Solicitações de Assinatura de Certificado).
- **Certificate Signing Requests Per Minute**
  O número de CSRs que o servidor do Citadel recebeu por minuto.

Métricas do Pilot

- **Active xDS Connection Count**
  O número de endpoints/proxies envoy conectados a esse piloto usando o protocolo XDS Envoy.
- **Invalid Pod Count**
  O número de proxies que não são selecionados por nenhum serviço. Essa métrica de erro ocorre quando a lista de endpoints de um serviço não é atualizada no piloto.
- **Total Services**
  O número total de serviços sobre os quais o Pilot sabe.
- **Total Virtual Services**
  O número total de serviços virtuais sobre os quais o Pilot sabe.

Métrica do Galley

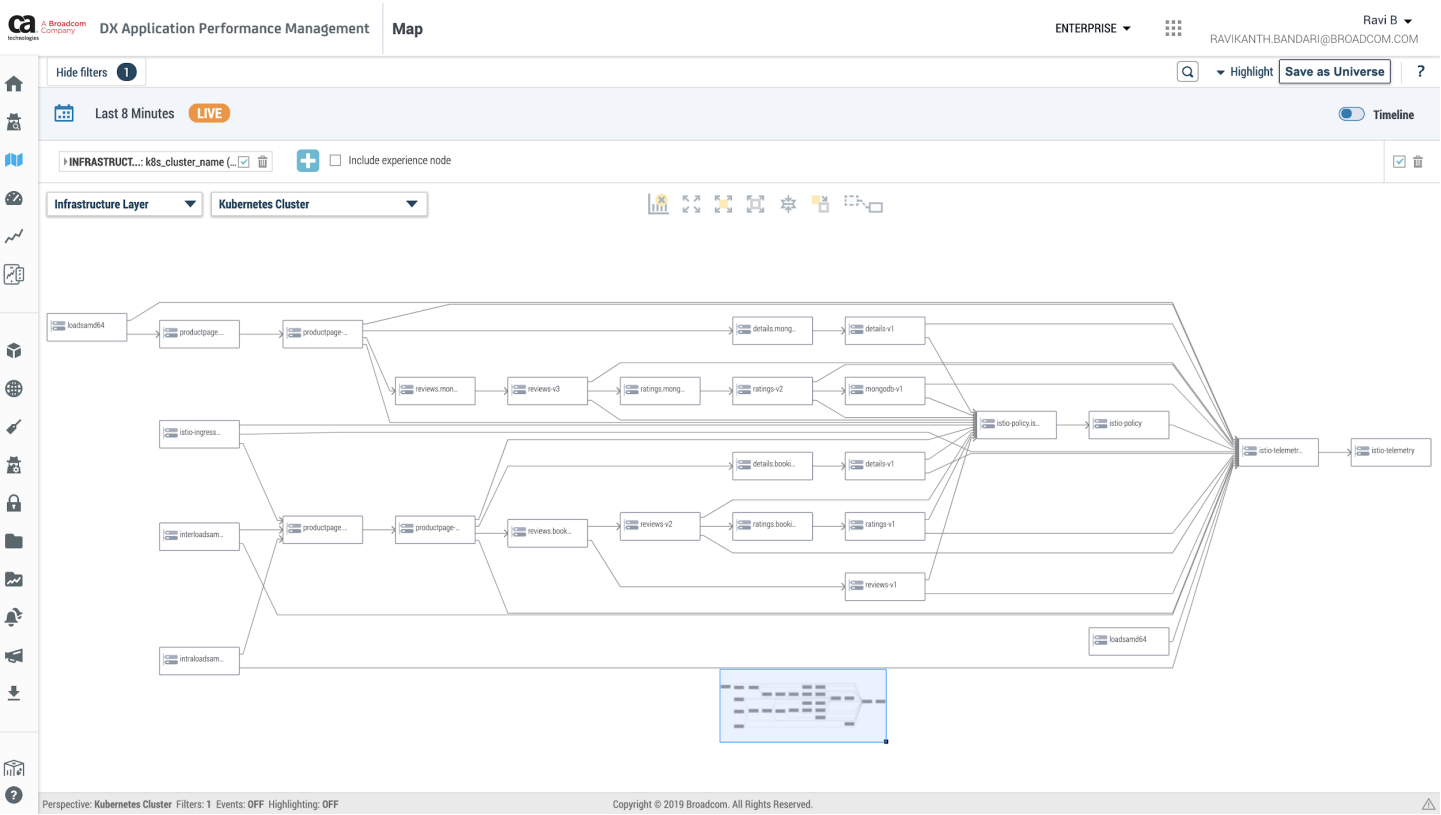
- **Validation Failures Per Minute**
  Número de validações em que o webhook da validação de configuração falhou por minuto.



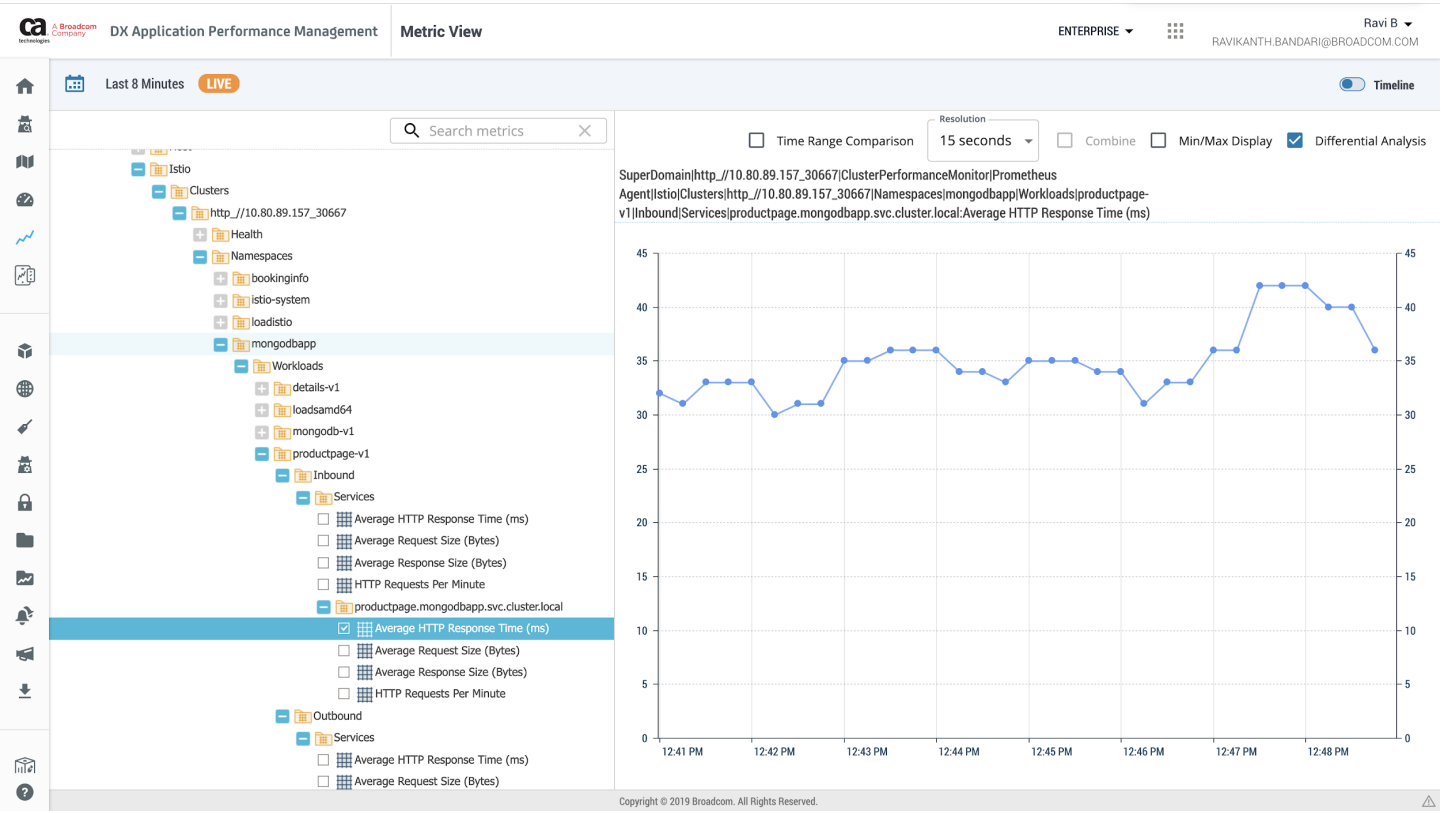
Istio Support exibido no mapa

O Istio Support permite que você visualize a topologia do seu service mesh Istio no mapa, que exibe serviços específicos que se comunicam entre si.

Nesta captura de tela, a camada **Infraestrutura** do mapa exibe oito minutos de fluxo de tráfego de rede do Istio em um cluster Kubernetes.

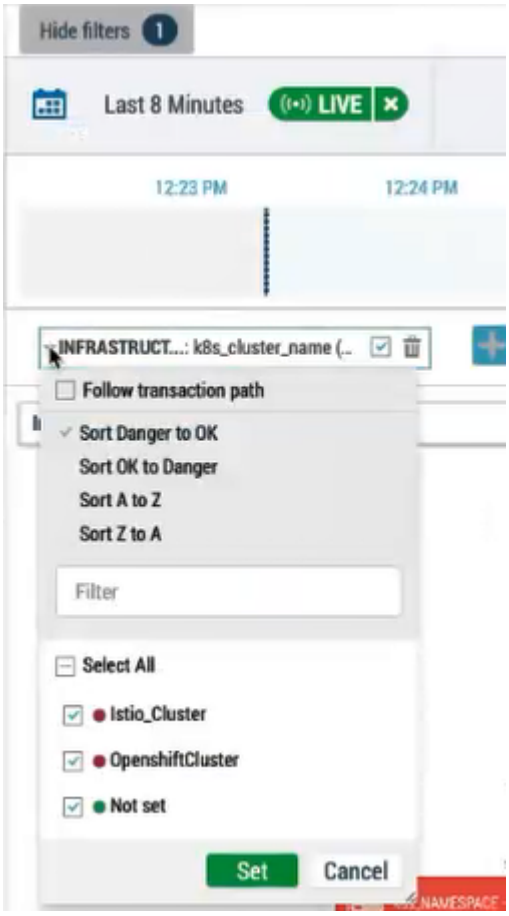


Você também pode ver os mesmos componentes que estão envolvidos no tráfego de rede na árvore do navegador de métricas, como mostrado nesta captura de tela.



Usar filtros para refinar os componentes do Istio Support que são exibidos no mapa

É possível aplicar filtros para que o mapa exiba dados mais específicos para sua investigação atual. Por exemplo, você pode definir um filtro para o nome do cluster. Nesta captura de tela, o usuário selecionou dois nomes de cluster: **Istio_Cluster** e **OpenshiftCluster**.



Siga estas etapas:

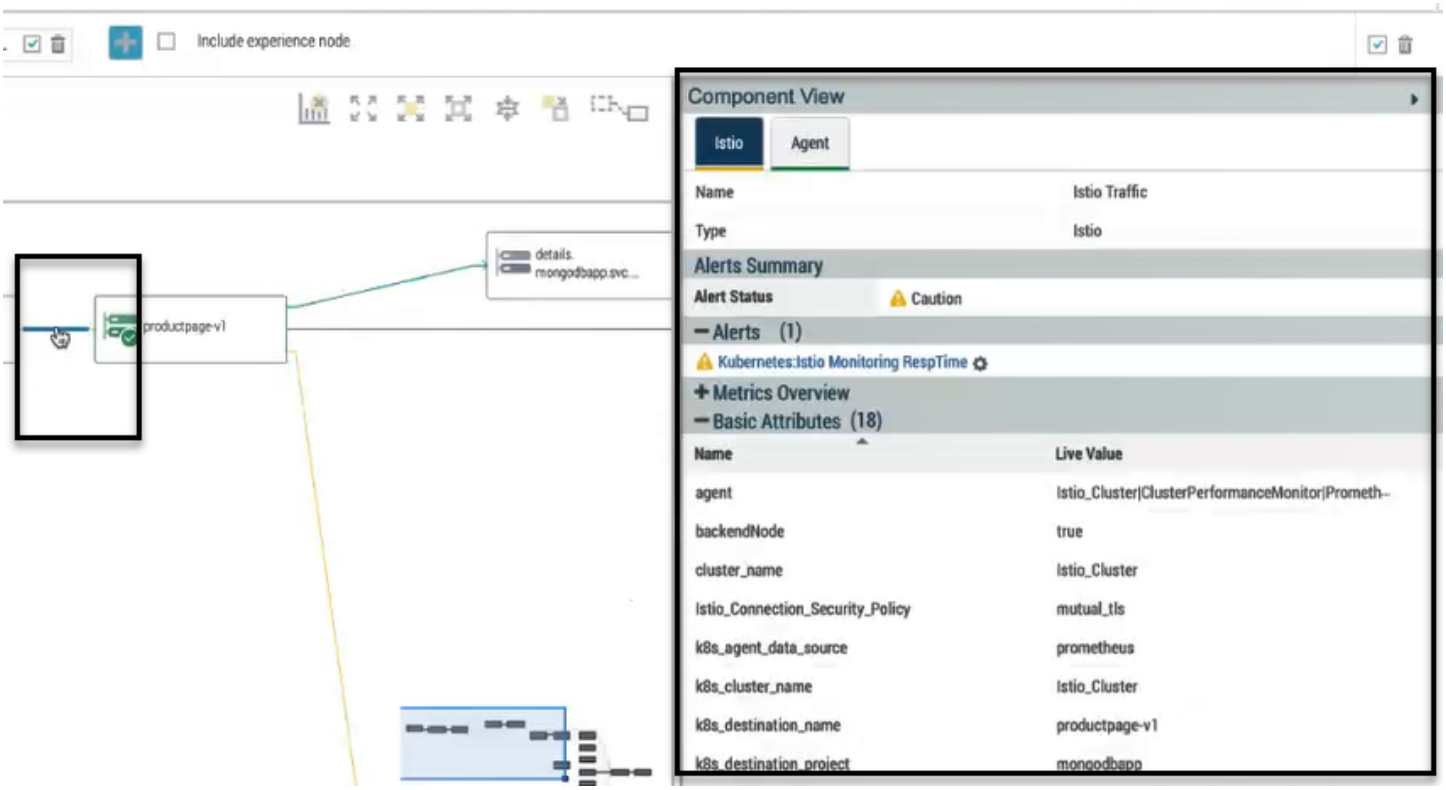
1. Na parte superior esquerda do mapa, clique no lado esquerdo da lista suspensa da camada do mapa **Infraestrutura**.
2. Defina um ou mais filtros.
3. Clique em **Definir**.

O mapa exibe mais ou menos dados de acordo com as configurações de filtro.

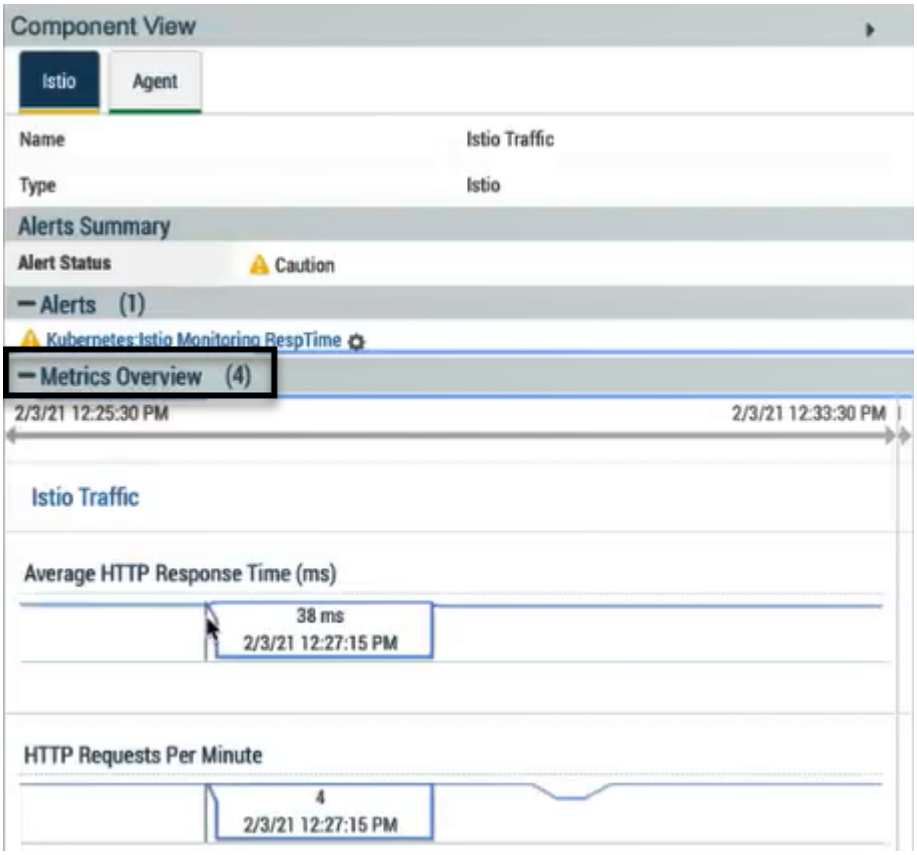
Mais informações: Camadas do mapa

Exibir taxas e latências do tráfego de rede do Istio Support

Clique em uma borda (linha conectando dois componentes) para ver a **exibição de componentes**, na qual é possível exibir as métricas sobre as taxas e latências do tráfego da rede entre os componentes. Na próxima captura de tela, o usuário clicou na linha que mostra o tráfego inserindo a carga de trabalho **productpage-v1**. (Sabemos sobre essa parte do tráfego a partir das capturas de tela anteriores usadas como exemplos). A **exibição de componentes** é aberta, mostrando dados sobre um alerta e 18 **atributos básicos** associados à **visão geral das métricas**.



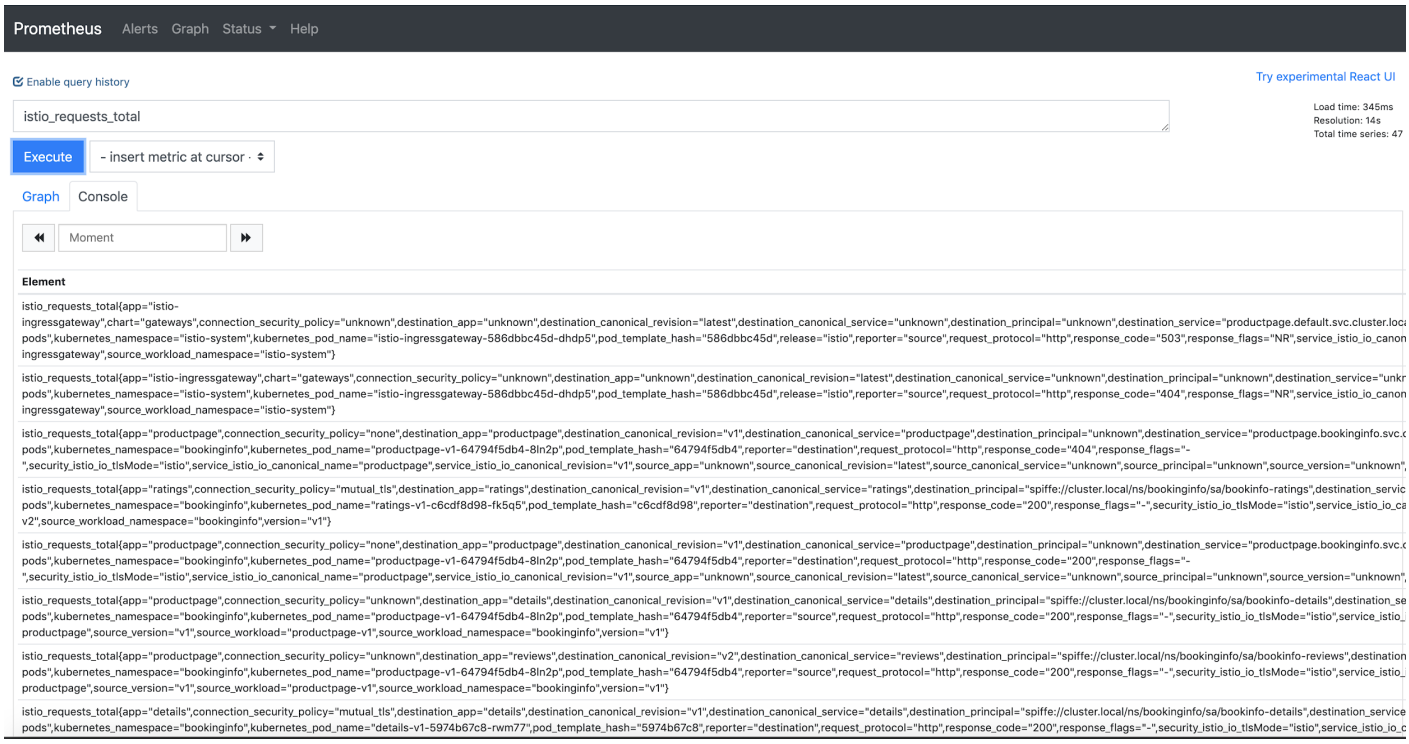
O usuário clicou em uma borda em outro momento para ver a **exibição de componentes**, a fim de exibir as métricas de uma carga de trabalho específica na **visão geral das métricas**. O usuário deseja examinar as métricas **Average HTTP Response Time** e **HTTP Requests Per Minute** por um período específico, como mostrado na próxima captura de tela.



Solução de problemas do Istio Support

Quando você enfrenta ?que tipo de problemas do Istio Support?, execute estas tarefas da solução de problemas:

- Verifique os erros de conexão do servidor do Prometheus no pod **cluster-performance-prometheus**. Se houver erros de conexão, certifique-se de que os detalhes do usuário, da senha e do token do Prometheus estejam corretos.
- Certifique-se de que as métricas do Istio sejam relatadas no Prometheus. Para fazer isso, efetue logon no URL do Prometheus e execute a consulta **istio_requests_total**. O console é preenchido com o QUÊ?:

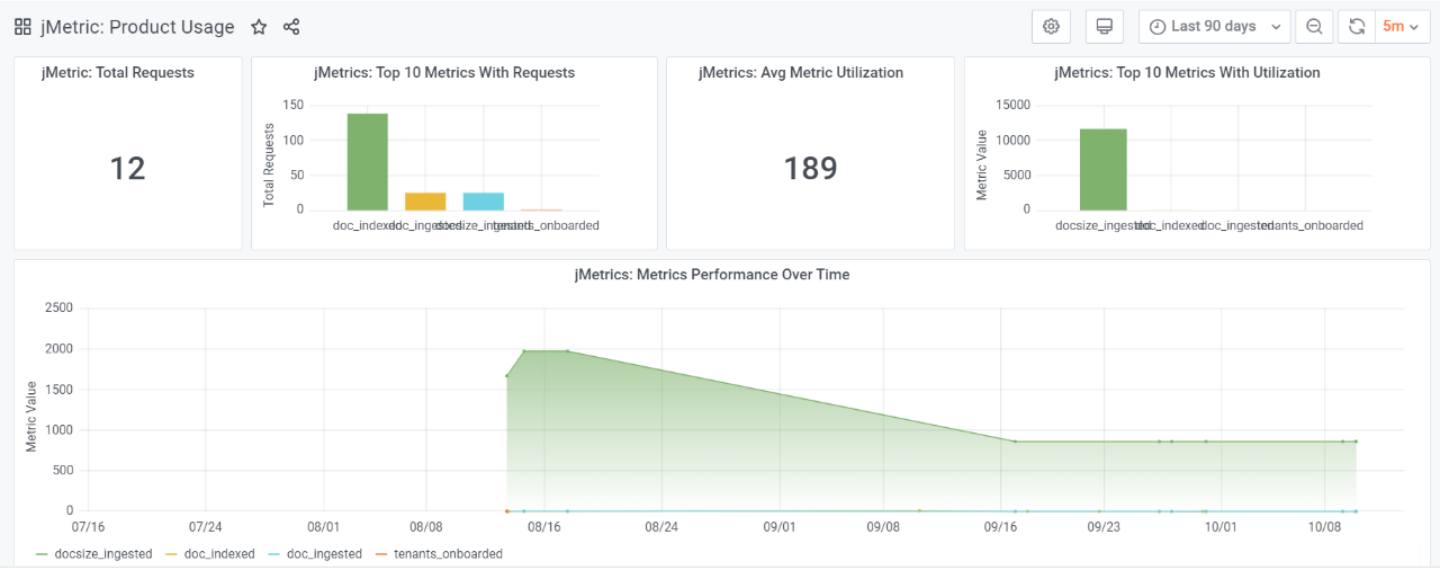


Veja a seguir um exemplo para os arquivos uma_cr.yaml e values.yaml

```
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
```

Painéis DX

Os painéis DX são uma plataforma de visualização projetada para pesquisar, exibir e interagir com os dados armazenados. Usando os painéis DX, é possível criar relatórios de negócios abrangentes para visualizar a análise em tempo real. Cada *painel DX* é um conjunto de painéis que são organizados em um padrão de grade. Cada quadro no painel interage com os dados da fonte de dados e fornece visualização dos dados. Um painel também permite fazer uma busca detalhada nos detalhes.



Os painéis DX incluem os seguintes benefícios:

- Permite que você visualize o inventário, a integridade, os alarmes, as métricas e os logs
- Oferece suporte à multilocação
- Oferece suporte a anotações de gráfico
- Permite que os usuários façam uma busca detalhada em camadas diferentes
- Fornece decomposição e análise do data lake AIOps

> **NOTE**
> As fontes de dados dos painéis DX não são suportadas com uma instância externa do Grafana. No entanto, você pode implementar os painéis DX como uma instância independente e pode se conectar a qualquer uma das fontes de dados. Para obter assistência, entre em contato com o **Suporte da Broadcom**.

Para obter mais informações sobre os painéis DX, consulte a documentação dos painéis DX.

Solução de problemas

A solução de problemas ajuda você a resolver sintomas problemáticos em sua implementação.

Mais informações: Uma abordagem geral da solução de problemas do DX Application Performance Management.

- Solução de problemas do agente
- Solução de problemas do DX APM
- Solução de problemas de transação
- Solução de problemas de estação de trabalho

Solução de problemas do agente

As informações sobre a solução de problemas do agente oferecem as perguntas frequentes ou relaciona os sintomas que o usuário observa para uma ou mais soluções.

Geral

- O agente foi iniciado, mas não está visível
- O agente não detecta automaticamente um back-end conhecido
- O agente que está monitorando um front-end não detecta o back-end automaticamente
- O agente aciona ClassNotFoundException ao carregar extensões dinâmicas
- Solução de problemas da caixa de diálogo de download do agente
- O cabeçalho do cookie de resposta do agente do navegador para .NET está sendo decorado?
- Valor do URL de ConfigurationServer falha ao ser preenchido
- Aumento em contagens de métricas

Agente do Java

- O agrupamento de URLs não está funcionando
- Não é possível instrumentar um aplicativo com o DX APM
- Falhas do agente do Java
- Erro de estouro de pilha do agente do Java
- Sem detecção automática de back-end devido ao erro insperado de carregamento de extensão
- O buildpack do Java no Cloud Foundry não consegue encontrar a versão solicitada do agente Java
- Falha do controlador ACC na geração de relatórios de diagnóstico

Agente do .NET

- Os rastreamentos de transação do agente do navegador e do agente do .NET não são correlacionados
- Sem métricas do .NET depois de ativar a injeção automática de snippet do Agente do navegador para .NET

O agente foi iniciado, mas não está visível

O agente DX APM é iniciado com êxito, mas não está visível no navegador de métricas, no WebView ou no Team Center.

Sintoma:

O agente DX APM é iniciado com êxito, mas não está visível no navegador de métricas, no WebView ou no Team Center.A versão do Enterprise Manager é 10.7.

O agente é:

- um agente do DX APM SaaS com versão 20.x ou superior
- um agente do DX APM no local com a versão 11.x ou superior

Esse sintoma se aplica a qualquer agente. Por exemplo, agente do Java, agente do .NET, extensões de monitoramento do Infrastructure Agent e assim por diante.

O log do Agente inclui uma mensagem de erro semelhante a estes exemplos:

- O log indica que o agente está conectado, mas no modo sem permissão.

```
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.
```

- O log indica que o agente não pode se conectar devido a um cliente incompatível.

```
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.).
```

Solução:

O agente da versão mais alta está tentando se conectar ao CA APM 10.7 Enterprise Manager, mas não pode se conectar devido à incompatibilidade de versão. Atualize o arquivo `IntroscopeAgent.profile` para o agente local do DX APM SaaS ou DX APM, dependendo do seu ambiente. Essa solução se aplica a qualquer tipo de agente. Por exemplo, agente do Java, agente do .NET, extensões do Infrastructure Agent e assim por diante.

Configure todos os agentes, exceto os aplicativos Java no Cloud Foundry

1. Vá para o arquivo `<diretório_principal_do_agente>\releases\<número_da_release>\core\config\IntroscopeAgent.profile` para o agente do DX APM SaaS ou o agente local do DX APM .
2. Abra o arquivo `IntroscopeAgent.profile` em um editor de texto.
3. Adicione a propriedade `introscope.agent.connection.compatibility.version=10.7` .
4. Desabilite a propriedade `agentManager.credential` .

   A configuração `introscope.agent.connection.compatibility.version=10.7` proporciona compatibilidade somente quando a propriedade `agentManager.credential` está comentada ou não está configurada. Aqui estão dois exemplos:

   ```
   #agentManager.credential=<your agent token>
   agentManager.credential=
   ```

   A definição incorreta de `agentManager.credential` resulta em um erro em **FailedToAuthenticateException**.

   > **NOTE**
   > Ao configurar credenciais do agente usando o arquivo IntroscopeAgent.profile ou argumentos da VM, não use aspas duplas (“”) para fornecer um valor vazio para a propriedade agentManager.credential. Por exemplo, `agentManager.credential=` .

5. Remova o protocolo **ws://** ou **wss://** do início da propriedade `agentManager.url` .

   Para usar o agente do DX APM com um CA APM 10.7 Enterprise Manager, você deve remover o protocolo **ws** da propriedade `agentManager.url.1` . Essa alteração na configuração permite que o agente do DX APM use o protocolo TCP padrão do CA APM 10.7 para a comunicação direta de soquete.

   Exemplo de configuração incorreta:

   ```
   agentManager.url.1=ws://apmhost:5001
   ```

   Exemplo de configuração correta:

   ```
   agentManager.url.1=apmhost:5001
   ```

   A falha ao remover o protocolo **ws** da sequência de caracteres da propriedade resulta em um erro semelhante a este:

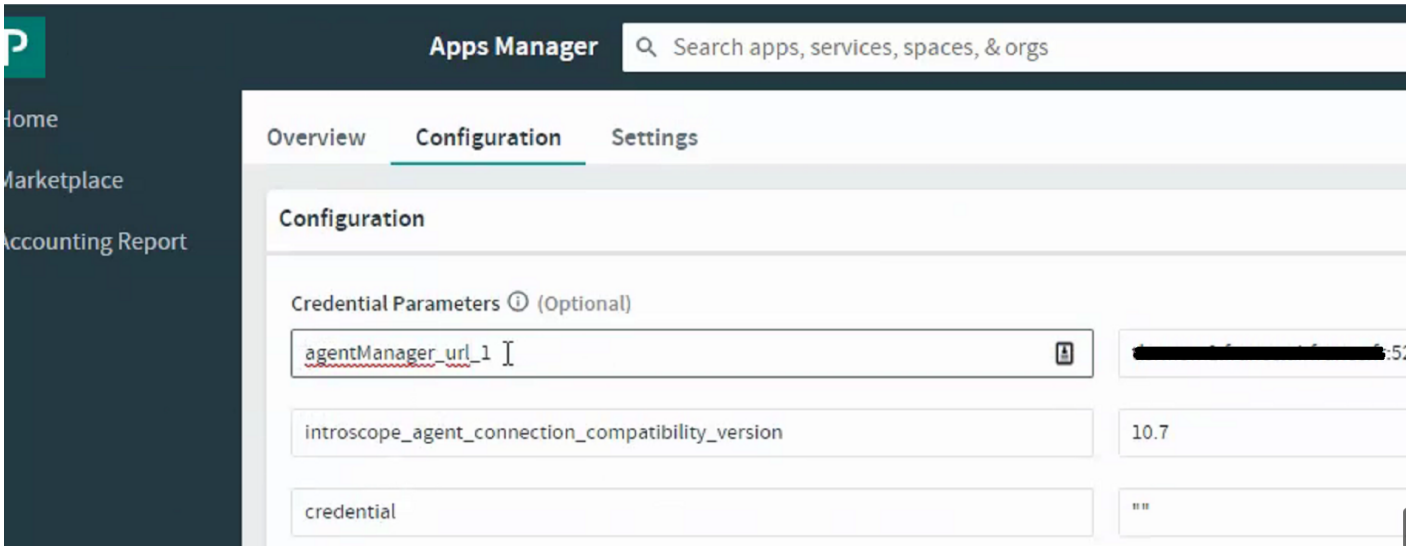
```
9/25/20 08:00:02 PM EDT [WARN] [IntroscopeAgent.ConnectionThread] Failed
 to connect to the Introscope Enterprise Manager at <APM services gateway
 URL>,com.wily.isengard.client.transport.websocket.WebSocketFactory (java.io.IOException:Connection
```

6. Salve o arquivo `IntroscopeAgent.profile` .
7. Reinicie o aplicativo gerenciado.

Aplicativos Java no Cloud Foundry

Quando você estiver monitorando aplicativos Java no Cloud Foundry, configure a compatibilidade usando *uma* das seguintes opções:

- Execute este comando em uma linha de comando do Cloud Foundry:
  ```
  cf cups introscope -p '{"agent_manager_url”:”host:port",
   "introscope_agent_connection_compatibility_version":"10.7", "credential":"”}'
  ```
- Atualize a configuração no Gerenciador de aplicativos do Pivotal Web Services (PWS), conforme mostrado neste gráfico e descrito nas etapas a seguir.



1. Vá para a guia **Configuração**.
2. No campo **Credential Parameters (Optional)**, informe este valor:
   `agentManager_url_1`
3. Certifique-se de que o campo à *direita* do campo **Credential Parameters (Optional)** esteja em branco.
4. No campo *abaixo* do campo **Credential Parameters (Optional)**, informe este valor:
   `introscope_agent_connection_compatibility_version`
5. No campo à *direita* de `introscope_agent_connection_compatibility_version` , informe este valor:
   `10.7`
6. No campo *abaixo* de `introscope_agent_connection_compatibility_version` , informe este valor:
   `credential`
7. No campo à *direita* da `credential` , informe este valor (aspas duplas):
   `""`

> **NOTE**
> Ao configurar as credenciais do agente para aplicativos Java no Cloud Foundry usando a UI do gerenciador de aplicativos do Pivotal Web Services (PWS), use aspas duplas (“”) para fornecer um valor vazio para a propriedade agentManager.credential. Por exemplo, `agentManager.credential=""` .

8. Salve a configuração.
9. Reinicie o aplicativo gerenciado.

O agente não detecta automaticamente um back-end conhecido

Sintoma

Sei que uma transação inclui um back-end não monitorado, mas o agente não detecta automaticamente esse back-end.

O log do agente no nível informativo não contém mensagens sobre a detecção de possíveis back-ends. Espera-se encontrar uma mensagem como neste exemplo:

```
[INFO] [IntroscopeAgent.AutomaticBackendDetection] Backend Candidates: [<my-expected backend1>,<my-expected
 backend2>…]
```

Essas duas métricas de sustentabilidade do agente mostram o valor 0:

- Detecção automática de back-end: instantâneos de pilha analisados
- Detecção automática de back-end: back-ends detectados

Solução

A detecção automática de back-end precisa que primeiro o agente detecte e monitore algum tipo de front-end. Verifique se a transação está monitorando um front-end, um ponto de entrada ou um componente personalizado.

> **NOTE**
>
> Talvez o agente precise de alguns minutos para detectar e instrumentar automaticamente uma transação que inclua back-ends automáticos.

O agente que está monitorando um front-end não detecta o back-end automaticamente

Sintoma

Uma transação que estou investigando inclui um front-end monitorado e um back-end não monitorado. O agente não detecta o back-end.
Aqui estão os valores relevantes da métrica de suportabilidade do agente:

- Sustentabilidade | Detecção automática de back-end: o valor de instantâneos de pilha analisados é > 0.
- Sustentabilidade | Detecção automática de back-end: o valor de back-ends detectados é 0.

Solução

Adicione a instrumentação personalizada para monitorar o back-end.

A detecção automática de back-end talvez não detecte back-ends em casos incomuns. Por exemplo, chamadas de comunicação de soquetes por meio de soquetes de datagrama.

O agente aciona ClassNotFoundException ao carregar extensões dinâmicas

Sintoma

Quando você remove e, em seguida, adiciona extensões dinâmicas ao diretório `<Pasta_principal_do_agente>/extensions/deploy` , o agente aciona o erro `ClassNotFoundException` . O log do agente exibe uma mensagem de erro semelhante a este exemplo:

```
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
```

Solução

1. Descarregue todas as extensões dinâmicas no diretório <`Pasta_principal_do_agente` >/extensions/deploy que estão aguardando para serem carregadas para implantação.
2. Certifique-se de que todas as extensões dinâmicas sejam descarregadas.
3. Recarregue as extensões dinâmicas no diretório `<Pasta_principal_do_agente>/extensions/deploy` .

Os rastreamentos de transação do agente do navegador e do agente do .NET não são correlacionados

Sintoma

Não consigo ver o rastreamento de transação do agente do navegador correlacionado com o rastreamento de transação do agente do .NET.O motivo é que o agente do .NET ignora automaticamente a codificação `gzip` .

Solução

Verifique o tipo de conteúdo de resposta para a propriedade de codificação não suportada:

```
introscope.agent.browseragent.encodings.skip.
```

Valor do URL de ConfigurationServer falha ao ser preenchido

Sintoma

A configuração de configurationServer.url feita para o controlador de agente no ACC fica ausente quando você faz o download do pacote e implementa o pacote nos servidores.

Esse problema ocorre quando nenhum esquema (http(s) ou ws(s)) é adicionado ao URL. A sequência de caracteres de conexão é considerada herdada, usada para a comunicação do Isengard (a porta padrão é 5001). O controlador do ACC se comunica somente por meio da chamada REST por http(s)/ws(s).

Solução

Como solução, você deve ativar http(s)/ws(S) no Cloud Proxy, seguindo *um* dos processos:

- Ative HTTP(s)/ws(s) no Cloud Proxy e use uma conexão por HTTP(s)/ws(s). É possível atualizar o Cloud Proxy no painel de criação do pacote e o URL de conexão é definido para os componentes em-connection e acc-controller.
- Ative HTTP(s)/ws(s) no Cloud Proxy e defina o URL de conexão na propriedade `introscope.agent.acc.controller.configurationServer.url` do componente acc-controller.

O cabeçalho do cookie de resposta do agente do navegador para .NET está sendo decorado?

O cabeçalho do cookie de resposta do agente do navegador para .NET está sendo decorado?

Sintoma:

Não tenho certeza se o cabeçalho do cookie de resposta do agente do navegador para .NET está sendo decorado.

Solução:

Veja se o agente do .NET enviou o cookie de resposta.Pressione a tecla **<F12>** e verifique no navegador.

Falhas do agente do Java

Sintoma

O agente do Java falha, trava ou tem muita sobrecarga ou uso elevado de CPU.

Solução

Problemas no agente podem ser resultado de:

- Configuração não suportada
- Bug na JVM que ocorre devido ao uso feito pelo DX APM do mecanismo de instrumentação da plataforma Java para o monitoramento
- Instrumentação ou explosão de métricas

Para solucionar esses problemas, tente as sugestões a seguir:

- Algo foi atualizado recentemente?
- Alguma instrumentação ou extensão personalizada foi implementada pelo Broadcom Professional Services?
- A configuração é suportada?
- Determine se o problema está relacionado à instrumentação ou a um bug da JVM, da seguinte maneira:
  a. Interrompa o servidor de aplicativos.
  b. Abra o arquivo `IntroscopeAgent.profile` e defina `introscope.autoprobe.enable=false` .
  c. Inicie o servidor de aplicativos.
     Se o problema persistir, significa que ele não está relacionado à instrumentação do DX APM. Tente as seguintes soluções:
     - Tente alternar de `-javaagent` para `-Xbootclasspath` .
     - Atualize para a versão mais recente da JVM ou use uma JVM alternativa.
     - Abra um incidente no suporte do fornecedor da JVM.
- Para ajudar a identificar a causa do problema, reduza temporariamente a quantidade de instrumentação:
  a. Interrompa o servidor de aplicativos.
  b. Abra o arquivo `IntroscopeAgent.profile` e defina `introscope.autoprobe.enable=false` .
- Alguns aplicativos usam um grande número de sequências de caracteres de instruções SQL exclusivas, especialmente quando o SQL é construído dinamicamente. Essa ação resulta em uma explosão de métricas do SQLAgent. Para testar, desative o SQLAgent removendo o arquivo `<pasta_principal_do_agente>/core/ext/SQLAgent.jar` do diretório AGENT. Se essa ação não for possível, defina `introscope.agent.sqlagent.sql.maxlength=120` (o valor padrão é 990).

Nenhum limite em relação ao tamanho das instruções SQL além dos limites impostos pelo próprio banco de dados; maxlength permite truncar o tamanho das instruções SQL. O objetivo dessa ação é evitar uma explosão de métricas do SQL.

- Desative os rastreadores de rede, de sistema de arquivos e das métricas do sistema de arquivo em `toggles.PBD`. Não é recomendável que eles estejam ativos em produção.

```
# TurnOn: SocketTracing
# TurnOn: UDPTracing
# TurnOn: FileSystemTracing
```

- Desative a coleta do JMX. Sondar grandes quantidades de métricas do JMX consome muitos recursos de CPU.
  Se possível, por enquanto, defina `introscope.agent.jmx.enable=false`
  Nunca defina a sequência de caracteres de filtro como nulo, por exemplo:
  `introscope.agent.jmx.name.filter=`
  Sem um filtro definido, um único agente pode produzir dezenas de milhares de métricas do JMX.
- Desative todos os complementos adicionais do agente do Java, como: ErrorDetector, Leakhunter ou outras extensões.
  Leakhunter é uma ferramenta de diagnóstico, não uma ferramenta de monitoramento em tempo integral.
  Recomendação: não ative essa ferramenta em um ambiente de produção.
  As extensões podem gerar muitas métricas que causam muita sobrecarga.
- Desative todos os pbds adicionais personalizados.
  Evite o uso das diretivas: `TraceAllMethodsOfClass` e `TraceComplexMethodsOfClass`.
  Escolha cuidadosamente quais métodos monitorar.

Se o problema persistir, antes de entrar em contato com o Atendimento ao cliente da Broadcom, colete as seguintes informações:

- `<Pasta_principal_do_agente>/logs` em um arquivo zip
- IntroscopeAgent.profile
- Gere uma série de cinco despejos de segmento no servidor de aplicativos com um intervalo de 5 a 10 segundos entre si quando ocorrer a sobrecarga, a perda de memória, o travamento ou o alto consumo de CPU.
- Para problemas de sobrecarga, gere um despejo da memória heap. Para a Sun JVM, adicione a seguinte opção da JVM:

```
XX:+HeapDumpOnOutOfMemoryError
```

  Reinicie o agente.
- Ative o log de GC. Para a Sun JVM, adicione as seguintes opções da JVM:

```
-Xloggc:<File_Name>.log -XX:+PrintGCDetails
```

- Arquivos de log do servidor de aplicativos a serem carregados no Suporte da Broadcom:
  – WebSphere: `System.out`, `system.err.native_stdout`, `native_stderr` e `server.xml`
  – WebLogic: arquivo de log e script de inicialização do servidor de aplicativos
  – Tomcat: arquivo de log e `catalina.sh/bat`
  – JBoss: arquivo de log e `run.bat/sh`
- Despejo completo do núcleo, se aplicável

Erro de estouro de pilha do agente do Java

Válido para: DX APM 8.x, 9.x

Sintoma

Uma translação falha em um aplicativo monitorado e uma mensagem StackOverflowError é registrada no log do servidor de aplicativos.

Solução

O agente adiciona as instruções a um aplicativo em execução. Quando um aplicativo com um caminho profundo de chamadas recursivas atinge o tamanho de pilha próximo ao máximo, as instruções do agente adicionado podem exceder o limite de tamanho da pilha.

1. Aumente o tamanho da pilha da JVM no argumento de inicialização do java -Xss. Por exemplo:
   `-Xss10024k`
2. Reinicie o servidor de aplicativos.

Sem métricas do .NET depois de ativar a injeção automática de snippet do Agente do navegador para .NET

Sintoma:

Não vejo métricas do .NET depois de ativar a injeção automática de trecho do Agente do navegador para .NET.

Solução:

Verifique a origem no navegador. Procure a marca de script do Agente do navegador.

Sem detecção automática de back-end devido ao erro insperado de carregamento de extensão

Sintoma

A detecção automática de back-end não detecta back-ends automáticos. Uma mensagem de erro semelhante a este exemplo aparece no log do agente devido a uma incompatibilidade da versão da JVM:

```
[ERROR] [IntroscopeAgent.Agent] Unexpected error loading extension
java.lang.UnsupportedClassVersionError: com/wily/introscope/agent/intelligent/entrypoint/
tracers/AbstractDetectionHelperTracer : Unsupported major.minor version 51.0
```

Solução

Verifique se a versão da JVM é 1.7 ou superior.

Aumento em contagens de métricas

Sintoma

Os valores de pico são agregados e não são valores separados.

Solução

A API Web Timing relata o tempo de rede como parte do descarregamento de uma página anterior. O Agente do navegador (anteriormente, BRTM) não pode excluir esses valores.

Não é possível instrumentar um aplicativo com o DX APM

Sintoma

Não consigo instrumentar um aplicativo com o DX APM.

Solução

Verifique o seguinte:

- O script de inicialização do servidor de aplicativos ou os arquivos de configuração contêm as duas principais entradas do DX APM:

  ```
  -javaagent and - Dcom.wily.introscope.agentProfile
  =
  ```

- Verifique se há algum arquivo de log em `\wily\logs` . Se houver, verifique o arquivo `Autoprobe.log` . Se o tamanho for 0 ou 1 KB, é provável que você esteja usando um pbd personalizado ou que tenha modificado um dos existentes incorretamente.

Coletar dados antes de entrar em contato com o Suporte da Broadcom

Se você tiver revisado as sugestões anteriores e ainda estiver com problemas, colete os seguintes dados antes de entrar em contato com o Suporte da Broadcom. Essas informações ajudarão o Suporte da Broadcom a orientá-lo de forma eficiente e eficaz.

- `<Pasta_principal_do_agente>\logs` em um arquivo zip
- Arquivo de log do servidor de aplicativos
- O script de inicialização do servidor de aplicativos ou o arquivo de configuração que contém as entradas do DX APM

O agrupamento de URLs não está funcionando

Sintoma

O agrupamento de URLs não está funcionando.

Solução

Verifique a seção Problemas conhecidos das Notas da versão sobre o agrupamento de URLs. Teste o problema usando uma definição de agrupamento de URL simples.

Se o problema persistir, antes de entrar em contato com o Atendimento ao cliente, colete as seguintes informações:

- `<EM_Home>/logs/*` em um arquivo zip; esses arquivos ajudam a determinar se o problema está relacionado com o desempenho.
- Arquivo `IntroscopeAgent.profile`
- Captura de tela dos URLs de exemplo da guia Investigador

O buildpack do Java no Cloud Foundry não consegue encontrar a versão solicitada do agente Java

Sintoma

Ao implantar um aplicativo Java no Cloud Foundry, atualize o manifesto do aplicativo para a versão 10.x executando o seguinte comando:

```
JBP_CONFIG_INTROSCOPE_AGENT: '{ version: 10.x.0_xx}
```

Execute o comando **cf push** para obter o buildpack do Java contendo o agente Java 10.x. A CLI do Cloud Foundry exibe a mensagem **No version resolvable error**, semelhante à mensagem neste exemplo:

```
[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
```

Solução

Você está usando um buildpack do Java offline. Os buildpacks offline vêm com algumas versões do agente do Java, mas nem todas. Se desejar usar uma versão anterior ou posterior do agente Java, faça download e use a versão apropriada do buildpack offline.

Faça download do Java buildpacks offline aqui: https://github.com/cloudfoundry/java-buildpack/releases. Como alternativa, você pode usar o buildpack do Java online.

> **NOTE**
>
> **Mais informações:** implantar e monitorar um aplicativo Java no Cloud Foundry

Solução de problemas da caixa de diálogo de download do agente

Encontre abaixo uma lista de possíveis causas dos problemas de exibição e itens de ação para corrigi-los:

- **As propriedades de configuração não são exibidas**
  - Examine os avisos e erros de conteúdo da caixa de diálogo de download no log do ACC.
  - Analise os erros de configuração em downloadPackageConfig.json.
- **O conteúdo não está localizado**
  - Examine os avisos e erros de conteúdo da caixa de diálogo de download no log do ACC.
  - Examine os arquivos de propriedades para ver se há chaves ausentes ou não localizadas.
- **O formato das instruções de instalação está corrompido**
  - Verifique a sintaxe de conteúdo do markdown no arquivo de propriedades.
  - Certifique-se de que as chaves de instruções de instalação tenham um sufixo do markdown.
- **A lista de aplicativos AXA não está visível na configuração do agente do navegador**
  - **Causa possível:**
    - O AXA não está disponível.
    - A integração com o AXA não está configurada corretamente.
  - **Tente o seguinte:**
    - Verifique a configuração do EM.
    - Verifique se há erros no console do desenvolvedor do navegador.

Solução de problemas do DX APM

As informações sobre a solução de problemas do DX APM oferecem as perguntas frequentes ou relaciona os sintomas que o usuário observa para uma ou mais soluções.

As métricas de componentes não são exibidas

A variação de análise diferencial não aparece nos nós

Não há dados de métrica na Exibição da experiência

Dados enviados pelos agentes no mapa estão incompletos ou ausentes

O mapa não exibe corretamente as informações do agente

O mapa mostra apenas 50.000 nós

Seletor de atributo do Cartão de experiência não mostra os atributos relacionados ao Docker

A propagação de atributo entre camadas não funciona

Onde procurar possíveis problemas relacionados a mapas

As métricas de componentes não são exibidas

Sintoma

As métricas não são exibidas para um componente.

Solução

Nomeie os componentes com, no máximo, 250 caracteres. Se o nome de um componente exceder 250 caracteres, ele será reduzido a 250 caracteres. Como resultado, os nós associados não exibem as métricas e os alertas associados quando o atributo de nome é usado para calcular a métrica, por exemplo, SOCKET, EJBCLIENT, DATABASE, BUSINESSTRANSACTION, GENERICBACKEND, GENERICFRONTEND.

A variação de análise diferencial não aparece nos nós

Sintoma

As métricas de variação da análise diferencial não aparecem nos nós.

Solução

O status da análise diferencial não é associado a uma métrica quando o caminho da métrica excede 1.000 caracteres. As configurações da análise diferencial e a barra Análise diferencial não são visíveis na visão geral do desempenho dessas métricas.

Não há dados de métrica na Exibição da experiência

Sintoma

Não é possível ver os dados na Exibição da experiência. O seguinte erro é exibido no navegador:

```
That's a lot of data. The number of metrics exceeds the display maximum.
```

A mensagem de erro é exibida quando você tenta exibir mais de 500 transações comerciais no modo dinâmico ou mais de 50 no modo histórico. Por questões de desempenho, a Exibição da experiência limita o número de transações comerciais exibidas.

Solução

Há várias maneiras para limitar o número de transações comerciais exibidas.

- Detalhe até outros níveis dos Cartões de experiência. O próximo nível mostrará métricas porque haverá menos transações comerciais.
- Aplique os filtros ao nível superior dos Cartões de experiência.
- Crie Universos com menos transações comerciais.

Dados enviados pelos agentes no mapa estão incompletos ou ausentes

Sintoma

Depois de conectar um novo agente ou implantar um novo aplicativo, a topologia correspondente não aparece no mapa ou apenas dados parciais aparecem instantaneamente. Os dados completos são processados após um ou dois minutos.

Solução

Inicie um rastreamento de transação no agente para agilizar a coleta de dados inicial na **Exibição de mapa**. Ao executar um rastreamento de transação em um agente, você coleta um alto volume de rastreamentos de transação. Essa ação permite que o servidor reconstrua a Exibição de mapa rapidamente. Para executar uma sessão de rastreamento de transação manualmente, especifique os agentes cujas transações você deseja rastrear e o período da captura de dados. Depois que a sessão de rastreamento de transação é iniciada, as transações que correspondem aos critérios de filtro aparecem no Visualizador do rastreamento de transação. Os eventos de transação incluem erros e rastreamentos de transação.

Depois que um rastreamento é iniciado por um período, a sessão é interrompida no final do período especificado. Você só pode iniciar uma sessão de rastreamento para um agente especificado em um determinado período. Se você reiniciar uma sessão de rastreamento ativa, uma notificação lembrará que a sessão de rastreamento de transação está ativa para o agente. A notificação mostra o tempo restante da sessão ativa. É possível iniciar um novo rastreamento para o mesmo agente depois que uma sessão de rastreamento ativa termina.

Siga estas etapas:

1. No painel esquerdo, em CONFIGURAÇÕES, clique em **Agentes**.
   A página de agentes é exibida e lista os agentes.
2. (Opcional) Clique na seta de **Aplicativos**.
   Todos os aplicativos que o agente monitora são listados.
3. Selecione um ou mais agentes para o qual rastrear transações:
   – Para rastrear todos os agentes, clique em **Rastrear todos os agentes**. Essa opção rastreia agentes suportados que estão conectados no momento e qualquer um que se conecte durante a sessão de rastreamento.
   – Para rastrear agentes selecionados, clique em **Rastrear agente** para um agente.
   A caixa de diálogo Sessão de rastreamento de transação é exibida.
4. Especifique valores para o rastreamento de transação nos campos da caixa de diálogo ou aceite os padrões e clique em **Iniciar**:
   – Especifique a **Duração mínima da transação** em **milissegundos** para o rastreamento de transação. O padrão é 1000 milissegundos. O valor mínimo é 1 milissegundo.
   – Especifique a **Duração da sessão de rastreamento** em minutos. O padrão é 1 minuto com uma duração máxima de 5 minutos para uma única sessão de rastreamento.

Um painel exibe o status da sessão.

5. (Opcional) Feche a caixa de diálogo depois que um rastreamento for iniciado com êxito.
   A sessão de rastreamento continuará sendo executada em segundo plano.

   NOTE

   Mais informações:

   Analisar rastreamentos e colaborar na análise de problemas

O mapa não exibe corretamente as informações do agente

Sintoma

O mapa não exibe corretamente as informações do agente.

Solução

Sincronize os relógios do sistema para todos os agentes monitorados pelo DX APM com um caminho transacional específico.

É recomendável sincronizar os relógios do servidor de aplicativos com o protocolo NTP.

O mapa mostra apenas 50.000 nós

Sintoma

O mapa mostra apenas 50.000 nós.

Solução

Para manter o bom desempenho, o DX APM está configurado para exibir mapas com, no máximo, 50.000 nós. Os dados são limitados para não ultrapassarem esse valor.

Siga estas etapas:

1. Clique em Painel.
2. Adicione filtros para reduzir o número de nós exibidos para menos de 50.000.

Seletor de atributo do Cartão de experiência não mostra os atributos relacionados ao Docker

Sintoma

Quando crio ou edito um Cartão de experiência, não vejo atributos relacionados ao Docker na lista suspensa.

Solução

Na **exibição Mapeamento**, marque Experiências para verificar se alguma Experiência contém os atributos que não aparecem na lista suspensa.

NOTE

Mais informações:

- KB000115511 Cartões de experiência e atributos do Docker no APM 10.7
- Configurar a Exibição da experiência

A propagação de atributo entre camadas não funciona

Sintoma

A propagação de atributo da Camada de infraestrutura para Camada do aplicativo não funciona.

Solução

Veja **Exibição de componentes** para verificar se os nós relativos estão conectados e compartilham atributos.

NOTE

Mais informações:

- KB000115511 Cartões de experiência e atributos do Docker no APM 10.7
- Configurar a Exibição da experiência

Onde procurar possíveis problemas relacionados a mapas

Você pode verificar o seguinte para encontrar possíveis problemas relacionados a mapas:

- Abra o console do desenvolvedor e procure por exceções.
- No caso de um "erro interno do servidor 500", procure por "informações adicionais" na resposta do servidor.

Solução de problemas de transação

As informações da solução de problemas de transação fornecem as perguntas frequentes ou relacionam os sintomas que um usuário observa a uma ou mais soluções.

Um método que nunca sai é identificado como método pai

Um método que nunca sai é identificado como método pai

Sintoma

Após a identificação do método pai de uma chamada de recebimento do JMS, conforme descrito em Métricas de transação, um método que nunca sai é identificado como pai.

Solução

Defina o método pai manualmente usando um dos seguintes procedimentos:

- Abra o arquivo `JMSParentMethodPersist.pbd` na pasta **hotdeploy** em um editor de texto e anexe a definição do rastreador do método pai na parte inferior:

```
TraceOneMethodOfClass: <class name> <method> JMSReceiveParentTracer "JMSParentInstrumentation"
```

- Altere o valor de índice da constante (consulte a etapa 2 acima) para o valor que pertence ao método pai correto, como ele é visto no rastreamento de pilha, alterando o valor da propriedade `jms.receive.parent.lookupFallback.maximumDepth` no arquivo de perfil do agente.

Solução de problemas de estação de trabalho

As informações da solução de problemas de estação de trabalho fornecem as perguntas frequentes ou relacionam os sintomas que um usuário observa a uma ou mais soluções. Alguns dos artigos da solução de problemas são:

Erro na estação de trabalho ao coletar o novo despejo de segmento

Alterar os tipos de operação nas calculadoras do Módulo de gerenciamento

Painéis têm painéis vazios

Nenhum resultado de eventos históricos de consulta

Solucionar problemas de tempo limite de sessão automática em estação de trabalho

Expiração da estação de trabalho durante logon no Gerenciador corporativo

Erro na estação de trabalho ao coletar o novo despejo de segmento

Erro na estação de trabalho

Sintoma: Quando o agente do Tomcat é executado com um tamanho de memória heap de 50 MB, o erro **ConnectionExeptionErrorStatus** é exibido na estação de trabalho e os logs do EM mostram o log de erros a seguir.

```
[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
```

Resolução

Aumente a memória heap no servidor de aplicativos (servidor de execução do agente). Esse erro é exibido apenas quando a JVM (servidor de aplicativos) está em execução com pouco espaço de memória heap.

Alterar os tipos de operação nas calculadoras do Módulo de gerenciamento

Sintoma

Quando você edita uma calculadora em um Módulo de gerenciamento, alterar o tipo de operação redefine o significado da métrica de saída para a calculadora. Por exemplo, você alterou o tipo de operação de MIN para MAX e manteve o nome da métrica de saída da calculadora. A métrica de saída mostra os valores antigos no histórico (por exemplo, MIN) com os novos valores (por exemplo, MAX). Não será exibida nenhuma indicação de onde ocorreu a alteração no processamento.

Solução

Renomeie a métrica de saída da calculadora ao alterar o tipo de operação, caso desconfie que esses valores estão causando confusão.

Painéis têm painéis vazios

Sintoma

Os painéis têm painéis vazios.

Solução

Você está vendo painéis vazios porque seu aplicativo não usa essas métricas.

Por padrão, os painéis exibem um conjunto de métricas de desempenho gerais.

Nenhum resultado de eventos históricos de consulta

Sintoma

Nenhum resultado é exibido quando consulto eventos históricos.

Solução

- O problema ocorre quando são usados filtros básicos, como type:sampled? Isso ajuda a confirmar se os dados estão gravados no banco de dados de rastreamentos.
- O problema pode estar relacionado ao índice de rastreamentos corrompidos. Interrompa o Gerenciador corporativo, exclua o diretório \traces\index e execute a ferramenta de reindexação para reindexar o banco de dados de rastreamento.

Coletar dados antes de entrar em contato com o Suporte da Broadcom

Se você tiver revisado as sugestões anteriores e ainda estiver com problemas, colete os seguintes dados antes de entrar em contato com o Suporte da Broadcom. Essas informações ajudarão o Suporte da Broadcom a orientá-lo de forma eficiente e eficaz.

- `<Pasta_principal_do_EM>/logs/*` em um arquivo zip
- `<Pasta_principal_do_agente>/logs/*` e `IntroscopeAgent.profile` em um arquivo zip
- Captura de tela da janela Rastreador de transações e os detalhes da classe que você espera ver

Solucionar problemas de tempo limite de sessão automática em estação de trabalho

Sintomas

O tempo limite da sessão automática é interrompido e mostra ao menos um dos seguintes sintomas:

- As janelas da estação de trabalho não fecham automaticamente após o período de inatividade.
- Nenhuma mensagem de logoff é exibida na janela de logon.

Solução

Somente os administradores do DX SaaS podem modificar o arquivo `<pasta_principal_do_EM>/config/IntroscopeEnterpriseManager.properties` . Entre em contato com o administrador para garantir que a propriedade `introscope.apmserver.ui.inactivityLogoutTimeout` esteja definida com um número inteiro maior que 0 para ativar o tempo limite da sessão.

Solução

Abra o arquivo `IntroscopeWorkstation.log` ou um arquivo de log separado que rastreie os eventos da estação de trabalho. Confirme se as seguintes mensagens estão presentes no arquivo de log:

- **Session timeout configured to <x> minute(s)**
  Indica que as configurações de tempo limite de sessão automática foram definidas corretamente.
- **User activity check: there has been no user action for more than several minutes, therefore logging out.**
  Indica a notificação de tempo limite da sessão.

Expiração da estação de trabalho durante logon no Gerenciador corporativo

Sintoma

A estação de trabalho atinge o tempo limite ao efetuar logon no Gerenciador corporativo.

Solução

O tempo de limite padrão de conexão da estação de trabalho é 60 segundos. A estação de trabalho pode atingir o tempo limite pelos seguintes motivos:

- Latência de rede entre a estação de trabalho e o Gerenciador corporativo
- A estação de trabalho recebe um pull de uma grande quantidade de dados (métricas e módulos de gerenciamento) e 60 segundos não é suficiente, mesmo que a rede esteja em condições normais.

Você pode aumentar o tempo de limite de conexão do cliente adicionando a seguinte propriedade ao arquivo `IntroscopeEnterpriseManager.properties` :

```
introscope.enterprisemanager.workstation.timeout=[value in seconds]
```

Reinicie o EM para que as alterações entrem em vigor.

Referência a APIs

O Application Performance Management é composto pelo seguinte conjunto de APIs de serviços web:

Os seguintes usuários são o público-alvo pretendido dessas APIs:

- Desenvolvedores e administradores do Application Performance Management
- Desenvolvedores, serviços profissionais ou engenheiros de pré-vendas da CA Technologies ou de terceiros
- Cada uma das APIs de serviços web do Application Performance Management fornece aos desenvolvedores e administradores a capacidade de estender suas soluções de gerenciamento de aplicativos. Elas podem recuperar informações relevantes do Application Performance Management e integrar dados a soluções personalizadas ou de terceiros.

API do APM Command Center

Uma visão geral das APIs RESTful implementadas para o APM Command Center. Para cada serviço web disponível, listamos os parâmetros de solicitação e verbos HTTP suportados.

Esta seção fornece uma visão geral das APIs RESTful implementadas para o APM Command Center. Para cada serviço web disponível, serão listados os verbos e parâmetros de solicitação HTTP suportados. É recomendável ler também a seção API de hipermídia do APM para obter informações gerais sobre como a API RESTful é implementada no DX APM.

Fazer download do pacote mais recente no APM Command Center

Usando a API do Command Center, é possível baixar os pacotes mais recentes do APM Command Center e personalizar o comportamento do download definindo as propriedades necessárias. Por exemplo, durante o download, é possível personalizar a atividade e definir determinadas propriedades como ocultas.

O URL para baixar o pacote pode ser obtido neste local: **ACC**, **Packages**, **Package Detail Screen**, **Package URL**

Os terminais para baixar os pacotes foram estendidos para adicionar uma solicitação POST. Por exemplo:

```
POST /acc/apm/acc/downloadpackage/uid/SsApAZq75k3G/version/latest?
format=archive&layout=bootstrap_preferred&packageDownloadSecurityToken=d19a78c5a88bfe750f3a7a4bc
```

Na carga, defina a lista de propriedades json no seguinte formato:

```
{
    "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
}
```

Da mesma forma, é possível definir propriedades adicionais na carga.

Nome da propriedade	Descrição	Exemplo/valor padrão
bundleName	Opcional. Defina o nome do componente.	A lista de componentes dentro do pacote específico com a ID 2 (com UID: SsApAZq75k3G) pode ser obtida pelo terminal: • GET /acc/apm/acc/package/2/bundles
propertyName	Obrigatória. Defina o nome da propriedade.	A lista dos nomes de propriedade do bundleName especificado (isto é, o componente que tem a ID: 91) pode ser obtida pelo terminal: • /acc/apm/acc/package/2/bundles/91/profile
propertyValue	Obrigatória. Defina o valor da propriedade.	None
hidden	Opcional. Defina um valor booleano: **true** ou **false** se desejar que o parâmetro fique oculto durante o download do pacote. Se você definir o valor como **true**, seu valor será comentado no arquivo do pacote de resultados.	Padrão: **false**
allowOnlyExistingProperties	Opcional. Defina um valor booleano: **true** ou **false** Se você definir o valor como **true**, as validações durante o download vão gerar o erro HTTP 400, caso o nome da propriedade especificado no corpo de POST não esteja contido dentro de nenhuma propriedade do componente do pacote. É recomendável definir a propriedade como **true** se desejar substituir somente as propriedades existentes e executar a verificação de validação durante a chamada REST.	Padrão: **false**

Validação e solução de problemas

Quando o terminal conclui a validação com êxito, ele retorna o pacote binário do tipo zip ou tar, com base na plataforma específica, ou seja, Windows ou Unix/Linux. Esse pacote contém os parâmetros substituídos ou novos com o código de resposta 200 OK.

No entanto, se a validação falhar, o código de resposta 400 SOLICITAÇÃO INVÁLIDA será retornado para o usuário com a mensagem de erro detalhada.

O APM Command Center oferece suporte aos seguintes serviços web RESTful públicos:

Os URLs dos recursos estão no seguinte formato:

```
https://<APMtenanthost>/apm/appmap/acc/apm/acc/<nome do recurso>
```

O host de inquilino do APM Command Center contém o nome do Pod do Enterprise Manager dentro do Kubernetes e o nome DNS do roteador do Kubernetes. Por exemplo: 10-778046.KUBERNETES-ROUTER. O primeiro número é o número do inquilino. O segundo número é diferente para cada inquilino. KUBERNETES-ROUTER é o roteador do Kubernetes que está instalado.

A tabela a seguir mostra todos os recursos disponíveis da API do APM Command Center, bem como os parâmetros e verbos HTTP aos quais eles oferecem suporte.

Recurso	Verbos HTTP						Parâmetros				
	GET	HEAD	POST	DELETE	OPTIONS	format	projection	page	size	sort	q
agente Uma lista de agentes gerenciados, incluindo suas propriedades.	Sim	Sim	Não	Não	Sim	JSON, CSV	lista	Sim	Sim	Sim	Sim
agentUpdateSiTask Capacidade de modificar o nível de log de um agente individual.	Sim	Sim	Não	Não	Sim	JSON	Não	Sim	Sim	Sim	Não
diagnosticReport Uma lista de relatórios de diagnóstico, incluindo a capacidade de baixar os relatórios.	Sim	Sim	Não	Não	Sim	JSON, ZIP	lista	Sim	Sim	Sim	Sim

diagnosticReportTask Fornece a capacidade de gerar um novo relatório de diagnóstico para um agente.	Sim	Sim	Sim	Não	Sim	JSON	Não	Sim	Sim	Sim	Não
controller Uma lista de Controladores de agente conectados ao Servidor de configuração.	Sim	Sim	Não	Não	Sim	JSON, CSV	Não	Sim	Sim	Sim	Não
agentFileOperationTask Fornece a capacidade de enviar por push (ou excluir) um arquivo a um diretório em um sistema remoto.	Sim	Sim	Sim	Não	Sim	JSON	Não	Sim	Sim	Sim	Não
file Uma lista de arquivos armazenados no Servidor de configuração.	Sim	Sim	Sim	Sim	Sim	JSON	Não	Sim	Sim	Sim	Não

auditRecord Uma lista de registros de auditoria associados a operações que alteram o ambiente.	Sim	Sim	Não	Não	Sim	JSON	lista	Sim	Sim	Sim	Sim
package Uma lista de pacotes de agentes criados.	Sim	Sim	Sim	Sim	Sim	ZIP, TAR, arquivo	lista	Sim	Sim	Sim	Sim
agentPackageTask Capacidade de enviar por push componentes do agente para o diretório de instalação do agente.	Sim	Sim	Sim	Não	Sim	JSON	Não	Sim	Sim	Sim	Não
bundle Uma lista de pacotes de agentes disponíveis.	Sim	Sim	Sim	Sim	Sim	JSON, arquivo	Não	Sim	Sim	Sim	Sim

Observe que os parâmetros format, projection, page, size, sort, q diferenciam maiúsculas de minúsculas e devem estar em letras minúsculas (por exemplo, Format=csv não funcionará).

Autenticação

Um token de segurança é uma sequência de caracteres de texto gerada aleatoriamente e é basicamente equivalente a uma senha em texto. Esse token fornece à API acesso ao serviço web do Command Center.

Você poderá gerar quantos tokens forem necessários.Você pode alterar a descrição de um token ou excluir um token usando o botão Editar. Os tokens poderão ser revogados apenas se forem excluídos. Qualquer usuário pode excluir qualquer token.

Também é possível ver quando um token foi gerado e quando foi usado pela última vez.

Siga estas etapas:

1. Na UI do DX APM, selecione a guia **Segurança**.
2. Selecione **Gerar outro token**.
3. Selecione **API pública**.
4. (Opcional) Selecione quando o token expira.
5. Selecione **Gerar token**.
6. Copie o token gerado.
   Observação: certifique-se de que o token seja armazenado imediatamente com segurança para uso futuro. Você não poderá exibi-lo novamente na UI do DX APM.
7. Use o token no cabeçalho de autorização da sua solicitação. Consulte Autenticação e autorização da API para obter detalhes.

Mais informações:

- Gerar códigos e mensagens de erro da API
- Mensagens de erro da API do Command Center

Mensagens de erro da API

Esta seção lista mensagens de erro da API retornadas pelo DX APM Command Center. Para obter uma visão geral de todos os códigos e mensagens de erro da API do DX APM Hypermedia, consulte a seção Mensagens e códigos de erro.

EA0100 a EA0599

Os erros no intervalo entre EA0100 e EA0599 são códigos de status HTTP padrão.Para obter informações detalhadas, consulte RFC 7231.

EA1001

Consulta de pesquisa incorreta

Motivo:

Retornado quando uma solicitação de filtro ou pesquisa falha devido a uma consulta que não está em conformidade com a sintaxe Lucene.

EA1002

Pacote atualmente em uso por {0} agentes

Motivo:

Você não tem permissão para excluir pacotes quando agentes estiverem fazendo referência a eles no momento.

EA3100

Atualização do agente em andamento: {id do agente}

Motivo:

Outra tarefa de atualização do agente está em andamento no agente específico.

Solução:

Aguarde até que a tarefa de atualização atual seja concluída.

EA3101

A atualização já está em andamento para o controlador em {nomeDoServidor}

Motivo:

Somente uma ControllerUpgradeTask pode estar em execução em um controlador de agente. Uma tentativa de iniciar uma nova ControllerUpgradeTask enquanto a atual ainda estiver em execução resultará nessa mensagem de erro.

Solução:

Aguarde até que a tarefa de atualização atual seja concluída.

EA3102

O arquivo já sendo atualizado para o agente

Motivo:

Somente uma AgentFileOperationTask pode estar em execução para a mesma combinação de arquivo de destino e agente.

Solução:

Aguarde até que a tarefa de operação atual seja concluída.

EA3103

O controlador não está conectado

Motivo:

Você tentou atualizar um controlador de agente que não está em execução. Uma ControllerUpgradeTask não pode ser iniciada para os controladores de agente que não estão em execução no momento.

Solução:

Inicie o controlador de agente.

EA3104

Atualização automática do controlador não permitida

Motivo:

A atualização automática do controlador de agente não pode ser ativada, pois o envio do pacote do controlador de agente está desativado.

Solução:

Consulte a seção de solução de problemas do processo de atualização para obter instruções.

EA3105

O pacote foi arquivado e não pode ser usado para essa operação

Motivo:

Não é possível usar pacotes arquivados para nenhuma operação. Por exemplo, um pacote arquivado não pode ser baixado.

Solução:

Escolha outro pacote para baixar ou cancele o arquivamento do pacote solicitado e tente novamente.

EA3108

O filtro nomeado {name} é usado por outros filtros: {otherFilters}.

Motivo:

O filtro nomeado não pode ser excluído, pois é usado (referido) por outros filtros.

Recurso do agente

Este serviço web retorna informações sobre agentes registrados com o Command Center (ACC). Verbos suportados: GET, HEAD, OPTIONS. Parâmetros suportados: page, size, sort, q, format, projection

GET

```
GET https://<ACC tenant HOST>/apm/appmap/acc/apm/acc/agent
```

Use a seguinte solicitação para obter informações somente sobre o agente com a ID 2:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent/2
```

HEAD

O método HEAD retorna cabeçalhos com informações sobre o serviço, incluindo, por exemplo, campos de pesquisa permitidos.

```
HEAD https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent/
```

Um exemplo de resposta:

```
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
```

Propriedades do recurso. Estão disponíveis as seguintes propriedades contendo informações sobre o recurso:

Nome da propriedade	Type	Descrição	Versão da API
tenant	número inteiro	ID do inquilino.	1.1
id	número inteiro	ID interna do recurso do agente.	1.0
agentName	sequência de caracteres	O 'name' do agente, conforme fornecido pelo agente quando ele se registra no ACC. Formulários que fazem parte do agente triplo.	1.0
serverName	sequência de caracteres	O servidor no qual reside o agente registrado. Formulários que fazem parte do agente triplo.	1.0
processName	sequência de caracteres	O nome do processo do agente, conforme conhecido pelo agente e o EM. Formulários que fazem parte do agente triplo.	1.0

Nome da propriedade	Type	Descrição	Versão da API
status	enum	Indica se o agente é considerado ativo - pode ser "ativo" ou "ausente". Por padrão,'ATIVO' indica que o agente foi visto nas últimas 24 horas.	1.0
type	enum	O tipo de agente, conforme informado no ACC como parte do registro do agente. Atualmente, é sempre 'JavaAgent'.	1.0
version	sequência de caracteres	A versão do agente, conforme definido no manifesto do agente (por exemplo, 9.7.1).	1.0
compilação	sequência de caracteres	A compilação do agente, conforme informado no manifesto do agente.	1.0
logLevel	enum	O nível de geração de logs atual do agente (FATAL, ERROR, WARN, INFO, VERBOSE, DEBUG, TRACE).	1.0
registrationTimestamp	data	A hora que o agente registrou no ACC, representada em formato UTC.	1.0
registrationUnixTimestamp	data	A hora que o agente registrou no ACC, representada em formato UNIX.	1.0
lastContact	data	A hora em que o agente entrou em contato pela última vez com o ACC, representada em formato UTC.	1.0
emCollectorHost	sequência de caracteres	O nome do coletor EM no qual o agente está conectado, como conhecido pelo agente.	1.0
emCollectorPort	número inteiro	A porta do coletor EM na qual o agente está conectado, como conhecida pelo agente.	1.0
appServerName	sequência de caracteres	O servidor de aplicativos no qual o agente está em execução (quando conhecido)- por exemplo, "Apache Tomcat".	1.0
appServerVersion	sequência de caracteres	A versão do servidor de aplicativos na qual o agente está em execução (quando conhecido).	1.0

Nome da propriedade	Type	Descrição	Versão da API
platformName	sequência de caracteres	A plataforma na qual o agente está em execução (Java Runtime) - por exemplo, "Oracle Corporation".	1.0
platformVersion	sequência de caracteres	A versão da plataforma (Java Runtime) na qual o agente está em execução - por exemplo, 1.7.0.	1.0
platformArch	sequência de caracteres	A arquitetura da plataforma (Java Runtime) na qual o agente está em execução, se for detectável.	1.0
osName	sequência de caracteres	O sistema operacional no qual o agente está em execução (Windows, RedHat,...).	1.0
osVersion	sequência de caracteres	A versão do sistema operacional no qual o agente está em execução.	1.0
osArch	sequência de caracteres	A arquitetura do processador do sistema operacional na qual o agente está em execução, por exemplo, amd64.	1.0
metricCount	número inteiro	O número de métricas que o agente acredita que está coletando.	1.0
registrationErrors	matriz da sequência de caracteres	Erros retornados por plugins ao detectar informações adicionais sobre o agente.	1.0
installPath	sequência de caracteres	O caminho totalmente qualificado no qual o agente está instalado.	1.0
agentProfile	sequência de caracteres	O caminho totalmente qualificado para o perfil do agente.	1.0
platformProperties	mapa	Pares de chave/valor das propriedades do sistema Java conhecidas pelo agente.	1.0
environmentVariables	mapa	Pares de chave/valor das variáveis de ambiente conhecidas pelo processo do agente.	1.0
controllerId	UUID	UUID do controlador do ACC ao qual este agente está conectado.	1.0

Recurso agentUpdateTask

O serviço web agentUpdateTask pode ser usado para atualizar o perfil do agente (atualmente limitado à alteração do nível de log).

O serviço web agentUpdateTask pode ser usado para atualizar o perfil do agente (atualmente limitado à alteração do nível de log).O recurso também pode ser usado para listar todas as solicitações anteriores. Verbos suportados: GET, HEAD, POST, OPTIONS Parâmetros suportados: page, size, sort

acessando recursos**GET**

```
GET https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/agentUpdateTask/
```

POST

Usando o método POST, é possível atualizar o perfil do agente. Este exemplo altera o nível de log do agente com a ID 1 para info:

```
POST https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/agentUpdateTask{ "agent":
 "agent/1", "property" : "log4j.logger.IntroscopeAgent", "value": "INFO"}
```

Propriedades do recurso. Estão disponíveis as seguintes propriedades contendo informações sobre o recurso:

Nome da propriedade	Type	Descrição	Versão da API
tenant	número inteiro	ID do inquilino.	1.1
status	enum	Status da operação (segue a definição de recurso da tarefa).	1.0
creationTimestamp	data	Hora em que o recurso foi criado (em UTC).	1.0
completionTimestamp	data	Hora em que a operação foi concluída (em UTC).	1.0
expectedDuration	número inteiro	Quanto tempo será necessário para a operação em andamento.	1.0
property	sequência de caracteres	A propriedade no perfil que está sendo atualizado.	1.0
value	sequência de caracteres	O valor solicitado.	1.0
currentValue	sequência de caracteres	O valor pelo qual o agente é conhecido por ter.	1.0
pendingValue	sequência de caracteres	O valor que foi gravado pela última vez no perfil.	1.0
agentId	número inteiro	Identificador exclusivo do agente no qual a operação é executada.	1.0
user	sequência de caracteres	O usuário que iniciou a operação.	1.0
updateErrors	Matriz	Matriz de erros retornados durante a operação.	1.0

Recurso diagnosticReport

Este serviço web retorna informações sobre os relatórios de diagnóstico.

Este serviço web retorna informações sobre os relatórios de diagnóstico. Um relatório de diagnóstico contém detalhes completos sobre um agente. Os termos suportados são: GET, HEAD, OPTIONS. Os parâmetros suportados são: page, size, sort, projection, q

GET

```
GET https://<host_do_inquilino_do_ACC>/apm/appmap/acc/apm/acc/diagnosticReport/
```

Propriedades do recurso. Estão disponíveis as seguintes propriedades contendo informações sobre o recurso:

Table 2:

Nome da propriedade	Type	Descrição	Versão da API
tenant	número inteiro	Tenant ID	1.1
id	número inteiro	ID interna do recurso diagnosticReport.	1.0
reportName	sequência de caracteres	Nome de exibição do relatório.	1.0
requestTimestamp	data	Hora em que o relatório foi solicitado (em UTC).	1.0
completionTimestamp	data	Hora em que o relatório foi concluído (em UTC).	1.0
generationDuration	número inteiro	Tempo total necessário para gerar o relatório, em milissegundos.	1.0
status	enum	O status da geração do relatório.	1.0
commandCenterInfo	mapa	Pares de chave/valor que fornecem informações sobre o Servidor de configuração e o Controlador de agente usados para gerar o relatório.	1.0
agentProfile	mapa	Pares de chave/valor que fornecem informações sobre o perfil usado para configurar o agente. Inclui um link para o conteúdo.	1.0
generationErrors	Matriz	Matriz de erros encontrados ao gerar o relatório.	1.0
agentProperties	mapa	Pares de chave/valor que representam as informações sobre o agente em que o relatório foi gerado (copiado do recurso do agente).	1.0

Nome da propriedade	Type	Descrição	Versão da API
environmentVariables	mapa	Pares de chave/valor que representam as variáveis de ambiente conhecidas do agente no momento em que o relatório foi gerado (copiado do recurso do agente).	1.0
platformProperties	mapa	Pares de chave/valor que representam as propriedades da plataforma (Propriedades do sistema Java) conhecidas pelo agente no momento em que o relatório foi gerado (copiado do recurso do agente).	1.0
platformParameters	sequência de caracteres	Linha de comando usada para iniciar o processo no qual o agente está sendo executado.	1.0
extensionDirectory	sequência de caracteres	Caminho totalmente qualificado do diretório de extensões do agente.	1.0
extensionFiles	mapa	Sub-recurso que contém detalhes dos arquivos de extensão em execução no agente, incluindo o nome, a data de modificação, o tamanho e a versão.	1.0
logFiles	mapa	Sub-recurso que contém detalhes dos arquivos de log do agente, incluindo o nome, o caminho, a data de modificação, o tamanho e o link para o conteúdo.	1.0
pbdPblFiles	mapa	Sub-recurso que contém detalhes dos arquivos PBD em execução no agente, incluindo o nome, a data de modificação, o tamanho e o link para o conteúdo.	1.0

Recurso diagnosticReportTask

O serviço web diagnosticReportTask pode ser usado para solicitar um relatório de diagnóstico.

O serviço web diagnosticReportTask pode ser usado para solicitar um relatório de diagnóstico. A criação de um recurso diagnosticReportTask inicia a geração de um relatório. Você pode monitorar o andamento da geração do relatório recuperando (sondando) o recurso diagnosticReportTask criado. O recurso também pode ser usado para listar todas as solicitações anteriores. Verbos suportados: GET, HEAD, POST, OPTIONS Parâmetros suportados: page, size, sort

GET

A seguinte solicitação retorna informações sobre a tarefa de relatório de diagnóstico com a ID 2:

```
GET https://<host_do_inquilino_do_ACC>/apm/appmap/acc/apm/acc/diagnosticReportTask/2/
```

POSTO uso do método POST permite iniciar a geração de um relatório de diagnóstico para um agente especificado. Esse é o exemplo de uma solicitação que cria uma nova tarefa de relatório de diagnóstico para o agente com a 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"}
```

Propriedades do recurso. Estão disponíveis as seguintes propriedades contendo informações sobre o recurso:

Nome da propriedade	Type	Descrição	Versão da API
tenant	número inteiro	ID do inquilino.	1.1
id	número inteiro	Identificador exclusivo para este recurso.	1.0
status	enum	O status da operação (segue a definição de recurso da tarefa).	1.0
creationTimestamp	data	Hora em que o recurso foi criado (em UTC).	1.0
completionTimestamp	data	Hora em que a operação foi concluída (em UTC).	1.0
expectedDuration	número inteiro	Quanto tempo será necessário para a operação em andamento.	1.0
diagReportId	número inteiro	Identificador exclusivo do recurso diagnosticReport criado.	1.0
agentId	número inteiro	Identificador exclusivo do agente no qual a operação é executada.	1.0

Recurso de controlador

Este serviço web retorna informações sobre os Controladores de agente conectados ao Servidor de configuração.

Este serviço web retorna informações sobre os Controladores de agente conectados ao Servidor de configuração. Verbos suportados: GET, HEAD, OPTIONS Parâmetros suportados: page, size, sort

GET

```
GET https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/controller
```

Propriedades do recurso. Estão disponíveis as seguintes propriedades contendo informações sobre o recurso:

Nome da propriedade	Type	Descrição	Versão da API
tenant	número inteiro	ID do inquilino.	1.1
id	UUID	UUID do recurso controlador.	1.0
version	sequência de caracteres	Versão do Controlador de agente, conforme definido em seu manifesto.	1.0

Nome da propriedade	Type	Descrição	Versão da API
messagingApiVersion	número inteiro	Versão máxima da interface de mensagens suportada por este controlador.	1.0
buildNo	sequência de caracteres	Número da compilação do controlador, conforme definido em seu manifesto.	1.0
hostNames	matriz da sequência de caracteres	Matriz de todos os nomes de host conhecidos para esse controlador.	1.0
ipAddresses	matriz da sequência de caracteres	Matriz de todos os endereços IP conhecidos (v4 e v6) para esse controlador.	1.0
osArch	sequência de caracteres	A arquitetura do sistema operacional na qual o controlador está em execução, por exemplo, amd64.	1.0
osName	sequência de caracteres	O nome do sistema operacional no qual o controlador está em execução, por exemplo, "Windows Server 2008 R2".	1.0
osVersion	sequência de caracteres	A versão do sistema operacional em que o controlador está em execução, por exemplo, 6.1.	1.0
registrationTimestamp	data	A data/hora em que o controlador foi registrado no Servidor de configuração no formato UTC.	1.0
registrationUnixTimestamp	data	A data/hora em que o controlador foi registrado no Servidor de configuração no formato Unix.	1.0
pluginRuntimeVersion	número inteiro	A versão máxima do tempo de execução do plugin suportada por este controlador (usado para determinar a compatibilidade do script).	1.0
pluginsUpdatable	Booleano	Indica se o controlador permite que (versões de) plugins novos sejam enviados para ele.	1.0

Mensagens de erro

Esta seção explica as mensagens de erro do DX APM Command Center.

EC1001

Não foi possível salvar o plugin {0}: {1}

O Controlador de agente tem um plugin desatualizado, mas não foi possível salvar o plugin atualizado baixado do servidor do DX APM Command Center.

Motivo:

O host no qual o Controlador de agente está em execução pode ter problemas de espaço em disco ou o Controlador de agente pode estar em execução como um usuário que não tem permissão suficiente para gravar no diretório "plugins".

Solução:

Verifique o espaço em disco disponível no host do Controlador de agente e se o usuário com o qual o Controlador de agente está em execução possui permissões de gravação no diretório "plugin" e nos arquivos contidos nele.

EC1002

O upgrade do Controlador não foi concluído no tempo esperado

Motivo:

A tarefa de upgrade do Controlador de agente foi iniciada, mas o Controlador não foi registrado novamente no servidor dentro do tempo esperado.

Solução:

Se o Controlador ainda não estiver reconectado, revise o arquivo upgrade.log no sistema do controlador para determinar a causa.

EC1003

Falha no upgrade do Controlador de agente, versão inalterada.

Motivo:

A operação de upgrade do Controlador de agente foi iniciada, mas não foi possível concluir o upgrade. A versão original foi restaurada.

As causas comuns são:

- Espaço insuficiente no sistema de arquivos;
- O Controlador não tem permissão para gravar em um diretório acessado durante o processo de upgrade (normalmente, /tmp e o diretório de instalação do Controlador);
- Um dos arquivos está bloqueado por um processo existente. É mais provável que isso aconteça em sistemas operacionais Windows. Certifique-se de que nenhuma janela do Explorer ou prompt de comando esteja usando ou bloqueando o diretório de upgrade do Controlador.

Solução:

Gere um relatório de diagnóstico para um dos agentes neste servidor e revise o arquivo upgrade.log no cartão "Arquivos de log do controlador". Verifique a mensagem de erro e tente resolver o problema.

EC1004

Os seguintes componentes não foram adicionados: {0}

Um pacote foi enviado por push a um agente, mas o agente não pôde adicionar todos os componentes do pacote.

Motivo:

Um pacote que contém novos componentes foi enviado por push a um agente em execução. No entanto, o agente não pôde adicionar todos esses componentes. Aqueles que não foram adicionados estão incluídos na mensagem.

Solução:

Executar um relatório de diagnóstico do agente permite examinar remotamente os arquivos de log do agente. Os logs fornecerão o motivo pelo qual o componente não pôde ser carregado. Por exemplo, o próprio componente pode estar corrompido.

EC1005

Os seguintes componentes não foram removidos: {0}

Um pacote foi enviado por push a um agente, mas o agente não pôde remover todos os componentes necessários do pacote.

Motivo:

Um pacote foi enviado por push a um agente com menos componentes do que o agente está usando atualmente. Esses componentes devem ser removidos do agente em execução. No entanto, o agente não pôde remover todos esses componentes. Aqueles que não foram removidos estão incluídos na mensagem.

Solução:

Executar um relatório de diagnóstico do agente permite examinar remotamente os arquivos de log do agente. Os logs fornecerão o motivo pelo qual o componente não pôde ser removido. Por exemplo, o diretório do componente pode estar em uso.

EP1000

Não foi possível acessar o processo {0}

Não foi possível acessar o processo do servidor de aplicativos.

Motivo:

O processo do servidor de aplicativos não está mais em execução ou o Controlador de agente não tem privilégios suficientes para exibir o processo.

Solução:

Verifique se o processo do servidor de aplicativos está em execução usando a ID de processo fornecida. Se estiver em execução, verifique se o Controlador de agente está em execução com permissão suficiente para exibir esse processo. Por exemplo, se ele está sendo executado como o mesmo usuário ou usando o mesmo "grupo".

EP1001

{0} não existe

O arquivo ou diretório não existe.

Motivo:

Não foi possível localizar o arquivo especificado.

Solução:

Se o arquivo se refere a um arquivo de diretiva do criador de probes, verifique se o arquivo existe e se ele foi nomeado corretamente em qualquer lista de diretivas do criador de probes.

EP1002

Permissão negada para ler {0}

Não foi possível ler o arquivo ou diretório.

Motivo:

O Controlador de agente não tem permissão suficiente para ler o arquivo nomeado.

Solução:

O Controlador de agente deve ser executado com permissões suficientes para ler os arquivos que o agente do APM produz. Por exemplo, o Controlador de agente deve ser executado como o mesmo "usuário" do servidor de aplicativos ou deve usar o mesmo "grupo".

EP1003

Ocorreu um erro de E/S ao ler {0}

Não foi possível ler o arquivo especificado.

Motivo:
O arquivo pode estar "bloqueado" por outro processo ou o Controlador de agente não tem permissão suficiente para ler o arquivo.

Solução:
O Controlador de agente deve ser executado com permissões suficientes para ler os arquivos que o agente do APM produz. Por exemplo, o Controlador de agente deve ser executado como o mesmo "usuário" do servidor de aplicativos ou deve usar o mesmo "grupo".

EP1004

Não há suporte para o sistema operacional {0}

O Controlador de agente não pode determinar os parâmetros da linha de comando para a ID de processo fornecida, pois o sistema operacional atual não tem suporte.

Solução:
Entre em contato com o Suporte da CA para saber para quando está previsto o suporte para esse sistema operacional.

EP1005

Não foi possível determinar o servidor de aplicativos {0}. Detalhes do erro: {1}

Não foi possível determinar o tipo do servidor de aplicativos.

Motivo:
O tipo ou a versão do servidor de aplicativos ainda não tem suporte, ou o Controlador de agente não tem privilégios suficientes para determinar o tipo de servidor. O erro contém mais detalhes da causa.

Solução:
Certifique-se de que o Controlador de agente tenha permissões suficientes para acessar os arquivos do servidor de aplicativos. Por exemplo, o Controlador de agente deve ser executado como o mesmo "usuário" do servidor de aplicativos ou deve usar o mesmo "grupo".

EP1006

Valor da propriedade introscope.autoprobe.directivesFile ausente em {0}.

Motivo:

A propriedade introscope.autoprobe.directivesFile em IntroscopeAgent.profile está indefinida ou vazia.

Solução:

Verifique a validade do arquivo IntroscopeAgent.profile.

EP1007

Permissão negada para gravar em {0}

Motivo:

O Controlador de agente não tem direitos de acesso suficientes para gravar no arquivo nomeado. Esse problema pode ocorrer em várias circunstâncias:

- Ao tentar alterar o nível de registro em log do agente do Introscope.
- Ao tentar atualizar a instalação do Controlador de agente.
- Ao tentar copiar um arquivo para o diretório de instalação do agente do Introscope.

Solução:

Certifique-se de que o Controlador de agente esteja em execução com permissões suficientes para gravar nesse arquivo e diretório. Por exemplo, executando como o mesmo "usuário" ou usando o mesmo "grupo".

EP1010

Não foi possível copiar o arquivo de {0} para {1}. Detalhes do erro: {2}

O URL {0} não pode ser acessado devido a problemas de rede. Veja os detalhes completos do erro {2}.

Motivo:

Você aplicou um novo pacote de agente ou atualizou o Controlador.

Solução:

Certifique-se de que a conexão de rede entre o Controlador e o Servidor do Command Center funcione. Repita a ação.

EP1012

A release {0} já existe

Motivo:

Essa mensagem será retornada se o diretório de release for criado manualmente durante a aplicação do pacote do agente.

Solução:

Reinicie o agente para que ele seja detectado novamente e possa ser registrado corretamente.

EP1013

O agente não é do tipo agente de inicialização

Motivo:

Falha na atualização da inicialização do agente, pois o agente não é um agente de inicialização, mas o Command Center registrou o agente como inicializável.

Solução:

Reinicie o agente para que ele seja detectado novamente e possa ser registrado corretamente.

EP2000

Falha de script com a mensagem {1}

Foi detectado um problema ao tentar recuperar os detalhes de um agente.

Motivo:

Esse problema pode ter muitas causas. Pode haver um erro de sintaxe no script que está sendo executado (ocorre apenas com scripts personalizados). Pode haver problemas ao acessar os arquivos necessários para o script.

Outro motivo pode ser usar uma versão ou implementação do Java sem suporte.

ES1000

Falha na alteração do nível de log

Motivo:

Outro usuário alterou o nível de log para o mesmo agent ao mesmo tempo. O plugin do Controlador de agente já atualizou o IntroscopeAgent.profile com um novo nível de log definido pelo outro usuário, mas a alteração ainda não foi exibida na interface do usuário.

Solução:

Verifique o nível de log atual e aplique a alteração novamente, se necessário.

ES1002

Erro: ocorreu um erro de HTTP {0} ao criar uma requisição de mudança de agente.

Motivo:

Houve falha na requisição de mudança de propriedade, e a tarefa de alteração de propriedade não foi iniciada.

Solução:

Muito provavelmente, esse é um problema de back-end. Verifique o arquivo de log e entre em contato com o administrador do sistema.

EU3106

O pacote {packageName} não existe.

Motivo:

O pacote usado por esse agente não é conhecido pelo DX APM Command Center.

EU3400

O tempo limite {0} foi atingido

Motivo:

A conexão está lenta ou o servidor não está disponível.

Solução:

Se o problema persistir, ou se você estiver acessando o APM Command Center com uma conexão lenta, recomendamos aumentar o tempo limite da solicitação do padrão de 10 segundos (10.000 ms).

Para fazer isso, adicione a seguinte propriedade ao arquivo config/apmccsrv.properties do servidor de configuração e defina o valor dele como 30.000 para aumentar o tempo limite para 30 segundos:

```
com.ca.apm.acc.ui.requestTimeout=30000
```

Reinicie o servidor de configuração para que a alteração entre em vigor.

Propriedades pesquisáveis

Esta seção lista todas as propriedades que podem ser usadas em pesquisas de agentes, relatórios, pacotes ou componentes na interface de usuário do DX APM Command Center.

A tabela a seguir lista as propriedades que podem ser usadas em uma pesquisa. Na primeira coluna, você encontrará a sequência de caracteres de pesquisa que você precisa digitar na caixa de pesquisa (as sequências de caracteres correspondem às chamadas de API reais). A segunda coluna mostra o nome correspondente da propriedade como aparece nos cartões na interface do usuário.

Para obter mais informações sobre a pesquisa usando a linguagem de consulta do Command Center, consulte Pesquisar usando a linguagem de consulta do Command Center.

O seguinte padrão é usado: nome da página - (nome do cartão) - nome do campo.

Sequência de caracteres de pesquisa	Campo correspondente na interface do usuário	Observações
agentCompatibility	Componentes - compatibilidade	Versões do agente com as quais o componente é compatível. A pesquisa de intervalo não é suportada. Digite "10" para obter os componentes compatíveis com todas as versões 10.x.
agentId	Não aplicável	Identificador exclusivo do agente.
agentName	Agentes, relatórios - nome do agente	
agentProfile	Relatórios - diretório do perfil do agente	Caminho do perfil do agente.
agentProfile.name	Relatórios - nome do perfil do agente	Retorna relatórios para agentes com o nome do perfil especificado.
agentVersion	Pacotes - versão do agente	Retorna os pacotes criados para agentes da versão específica.
appServerName	Agentes - servidor de aplicativos	Nome do servidor de aplicativos onde o agente está em execução.
appServerVersion	Agentes - versão do servidor de aplicativos	A versão do servidor de aplicativos onde o agente está em execução.
author	Componentes - autor	Retorna os componentes criados pelo usuário especificado.
compilação	Não aplicável	
categoria	Componentes - categoria	Categoria do componente: core, ambiente, recurso, personalizado.
Collections	Não aplicável	Usa uma sequência de caracteres de pesquisa salva como um conjunto.
comment	Pacotes - comentário	Retorna os pacotes que contêm o comentário especificado.
controllerId	Não aplicável	Retorna os agentes conectados ao controlador de agente especificado.
excluído	Não aplicável	Retorna uma lista de componentess excluídos ou ativos. Use 'true' ou 'false'.

dependencies	Componentes - dependências	Retorna os componentes que dependem das facetas especificadas.
description	Componentes - descrição	Retorna os componentes com a descrição especificada.
dynamic	Pacotes - implantáveis sem reinicialização	Indica se o componente pode ou não ser implantado dinamicamente. Os valores válidos para a pesquisa são 'true' e 'false'.
emCollectorHost	Agentes - Enterprise Manager	Host do coletor do Enterprise Manager
emCollectorPort	Agentes - Enterprise Manager	Porta do coletor do Enterprise Manager
enhances	Componentes - aprimoramentos	Retorna os componentes que aprimoram as facetas especificadas.
environmentVariables.value	Relatórios - variáveis de ambiente	Mapa de variáveis de ambiente (pares de chave e valor). Somente os valores são pesquisáveis.
extensionFiles.name	Relatórios - diretório de extensões	Caminho do diretório de extensões de um agente. Somente o nome do arquivo é pesquisável.
facets	Componentes - facetas	Retorna os componentes que contêm as facetas especificadas.
id	Não aplicável	ID literal do componente, conforme usada na definição do pacote.
installPath	Não aplicável	Retorna os agentes instalados no caminho especificado.
isBootstrapped	Não aplicável	Retorna os agentes que podem ser atualizados por uma atualização de inicialização controlada.
lastContact	Agentes - último contato	
logLevel	Agentes - nível de log	Valores: unknown, info, trace, debug, warn, error
name	Não aplicável	O nome real do pacote, e não o nome de exibição mostrado no campo Nome mostrado na página Componentes.
osArch	Relatórios - propriedades do sistema Java	Arquitetura do sistema operacional. Exemplo: x64
osName	Agentes - tipo de sistema operacional, relatórios - SO, pacotes - tipo de SO	Nome do sistema operacional. Exemplo: Linux. Para componentes, os valores pesquisáveis são 'unix' ou 'windows'.
osVersion	Agentes - versão do SO, relatórios - versão do SO	Versão do sistema operacional.
packageName	Agents - pacote - nome, pacotes - nome	Retorna os pacotes que correspondem à sequência de caracteres de pesquisa e todos os agentes que usam o pacote.
packageVersion	Agentes - pacote - versão do pacote	Retorna todos os agentes que usam a versão do pacote especificado.
pbdPblFiles.name	Relatórios - diretivas do criador de probes	Listagem de arquivos de um agente quando o relatório foi gerado. Contém somente arquivos PBD e PBL e apenas o nome do arquivo é pesquisável.
platformArch	Não aplicável	Arquitetura da plataforma. Exemplo: x86

platformName	Agentes - ambiente - JVM	Plataforma, em que o agente está em execução (Open Java, Oracle Java, .NET 4.0)
platformParameters	Relatórios - propriedades do sistema Java	Sequência de caracteres de parâmetros da plataforma. Use os parâmetros de inicialização da JVM ou um equivalente para o .NET.
platformProperties.value	Relatórios - propriedades do sistema Java	Mapa de propriedades da plataforma (pares de chave e valor). Use as propriedades do sistema JVM ou um equivalente para o .NET. Somente os valores são pesquisáveis.
platformVersion	Agentes - ambiente - versão da JVM	
process	Pacotes - ambiente - processo	Retorna os pacotes criados para o servidor de aplicativos especificado.
processName	Agentes - nome do processo, relatórios - agente - nome do processo	Retorna os agentes (e seus relatórios) que são executados no servidor de aplicativos especificado.
reportName	Relatórios - nome do relatório	
restartRequired	Não aplicável (um ícone ao lado do nome do agente)	Retorna uma lista de agentes que foram modificados recentemente e requer uma reinicialização para que as alterações entrem em vigor.
serverName	Agentes - nome do servidor, relatórios - agente - nome do servidor	Retorna os agentes (e seus relatórios) que são executados no servidor especificado.
specificationVersion	Não aplicável	Versão dos metadados usados no componente.
status	Agentes - status do agente	Status do agente. Valores: active, down, away
type	Não aplicável	Tipo de agente (por exemplo, agente do Java).
version	Agentes - versão do agente, relatórios - versão do agente, pacotes - versão	Retorna os agentes da versão específica ou os relatórios gerados para esses agentes ou componentes da versão específica.

Pesquisar usando a linguagem de consulta do Command Center

Especifique uma consulta personalizada na barra de pesquisa na parte superior da página do Command Center (ACC), que filtra os itens mostrados em uma exibição. A consulta personalizada usa a linguagem de consulta do ACC (AQL), que substitui a linguagem Lucene usada anteriormente. Para saber mais sobre as diferenças entre a Lucene e a AQL, consulte Propriedades pesquisáveis.

Criar consultas simples

Digite uma palavra na barra de pesquisa para filtrar todos os resultados correspondentes com base na consulta da palavra. A pesquisa é executada em uma propriedade padrão, normalmente, um nome.

Para pesquisar uma propriedade específica, digite a consulta neste formato:
propertyName:palavra_consulta_pesquisa

NOTE

O valor de **propertyName** diferencia maiúsculas de minúsculas À medida que você digita, a barra de pesquisa mostra as propriedades disponíveis. Use a propriedade **all** para executar a pesquisa em várias propriedades.

Pesquisa simples - exemplo:

```
osName:windows
```

Propriedades relacionadas a entidades

A tabela a seguir lista as propriedades padrão, as propriedades disponíveis e as propriedades que são pesquisadas ao usar a palavra-chave **all**.

Entidade	Propriedade padrão	Propriedades na palavra-chave 'all'	Propriedades disponíveis
Agent	spaName Essa propriedade executa uma pesquisa no serverName, processName e 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
Diagnostic Report	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

Entidade	Propriedade padrão	Propriedades na palavra-chave 'all'	Propriedades disponíveis
Bundle	name	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

Criar consultas de combinação

Digite várias consultas na barra de pesquisa separadas por espaços ou digite várias subconsultas usando os operadores: AND, OR e NOT.

Os operadores diferenciam maiúsculas de minúsculas, e é possível usar parênteses para agrupar operadores. AND é o operador padrão para consultas separadas por espaços.

Consulta de combinação com operador AND - exemplo

Os exemplos de consulta abaixo filtram os resultados em que todas as palavras são encontradas.

```
word1 AND word2 AND word3
word1 AND word2 word3
word1 word2 word3
```

Consulta de combinação com operador OR - exemplo

Este exemplo filtra os resultados em que qualquer uma das palavras é encontrada.

```
word1 OR word2 OR word3
```

Consulta de combinação com operador NOT - exemplo

Este exemplo filtra os resultados que não contêm a palavra *myquery*.

```
NOT myquery
```

Há símbolos alternativos que podem ser usados em vez de operadores nomeados:

Operator	Alternativa
AND	&&
OR	||
NOT	! ou -

Combinação de consulta com símbolo alternativo - exemplo

Este exemplo filtra os resultados que não contêm a palavra *myquery*.

```
-myquery
```

Consulta de combinação com parênteses - exemplo

O exemplo agrupa os operadores e filtra os resultados.

```
(word1 AND word2) OR word3
word1 AND (word2 OR word3)
```

Outras consultas de pesquisa

É possível usar sequências de caracteres, caracteres curinga, números, regex e consultas de intervalo como padrões de pesquisa para filtrar os resultados.

Usando sequências de caracteres e caracteres curinga

Digite uma sequência de palavras ou caracteres entre aspas (**" "**) ou barra (*/*) para filtrar os resultados da pesquisa.
Os resultados são uma correspondência exata da sequência de caracteres de pesquisa. Usando caracteres curinga, é possível filtrar os resultados que contêm a sequência de caracteres. Você pode usar os seguintes tipos de caracteres curinga: ***** para corresponder a qualquer subsequência de caracteres e **?** para corresponder a um caractere. O uso de um caractere especial em uma sequência de caracteres é tratado como um caractere comum.

Consulta de sequência de caracteres - exemplo

A consulta abaixo filtra todos os resultados que são uma correspondência **exata** da sequência de caracteres.

```
"abc xyz"
```

Consulta com caracteres curinga - exemplo

A consulta abaixo filtra **todos** os resultados que contêm a sequência de caracteres de pesquisa.

```
*"abc xyz"*
```

Consulta de combinação de sequência de caracteres e curinga - exemplo

A consulta abaixo mostra um padrão de pesquisa usando caracteres curinga, sequência de caracteres e uma única palavra.

```
word*"quoted string"?
```

Consulta de intervalo

Uma consulta de intervalo pode ser um intervalo de números, versões ou datas.

A consulta abaixo filtra os resultados no intervalo de **0 a 5** na propriedade numérica: **prop**.

```
prop:[0 TO 5]
```

A consulta a seguir mostra um padrão de pesquisa com intervalo exclusivo e estrela, indicando que não há limite máximo na propriedade numérica: **prop**

```
prop:{10 TO *]
```

Salvando a pesquisa

Na barra de pesquisa, use a opção **Salvar como novo conjunto** para salvar um padrão de pesquisa que você usa com frequência. Também é possível usar a pesquisa salva em uma consulta.

Usando conjunto em uma consulta - exemplo

```
collection:"Tomcat Agents" AND reportName:Linux
```

Expressão regular

A consulta de expressão regular permite pesquisar usando expressão regular. Ele começa e termina com um caractere de barra. É possível usar uma barra invertida para citar o próximo caractere de regexp. É possível incluir uma barra como um caractere dentro de uma consulta.

Exemplo: `name:/^test [3-4][0-9]/`

Recurso agentFileOperationTask

Este serviço web pode ser usado para enviar arquivos (por exemplo, arquivos de configuração do agente) para um diretório de agente em um sistema remoto.

Este serviço web pode ser usado para enviar arquivos (por exemplo, arquivos de configuração do agente) para um diretório de agente em um sistema remoto.Fornece a capacidade de excluir um arquivo de um diretório. Esse recurso também pode ser usado para obter uma lista de operações de cópia de arquivo executadas em relação a um agente.

Verbos suportados: GET, HEAD, POST, DELETE, OPTIONS Parâmetros suportados: Page, size, Sort

> **NOTE**
> Por padrão, os métodos POST e DELETE, bem como o envio de arquivos para o recurso de arquivo da API, estão desativados e resultam na resposta Não permitido. Para ativar essa funcionalidade, edite o arquivo theapmcccsrv.properties.

POST na solicitação a seguir copia o arquivo com a ID 12 para o diretório de configuração do agente com a ID 2 como o arquivo "my-new-app.pbd". Essa solicitação é enviada do servidor em que o agente está em execução.

```
POST https://<ACC tenant host>/apm/appmap/acc/apm/acc/agentFileOperationTask{  "agent" :
 "agent/2",  "file" : "file/12",  "destination" : "core/config/my-new-app.pbd",
 "operation":"COPY"}
```

A solicitação a seguir exclui o arquivo de configuração "my-new-app.pbd".

```
POST https://<ACC tenant host>/apm/appmap/acc/apm/acc/agentFileOperationTask{  "agent" :
 "agent/2",  "destination" : "core/config/my-new-app.pbd",  "operation":"DELETE"}
```

Observe que só é possível registrar arquivos que foram previamente enviados para o recurso de arquivo do servidor de configuração (URL *https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/file)* ou arquivos que fazem parte de um relatório de diagnóstico. Propriedades do recurso Estão disponíveis as seguintes propriedades contendo informações sobre o recurso:

Nome da propriedade	Type	Descrição	Versão da API
tenant	número inteiro	ID do inquilino.	1.1
status	enum	O status da operação (segue a definição de recurso da tarefa).	1.0
creationTimestamp	data	Hora em que o recurso foi criado (em UTC).	1.0
completionTimestamp	data	Hora em que a operação foi concluída (em UTC).	1.0
expectedDuration	número inteiro	Quanto tempo será necessário para a operação em andamento.	1.0
origem	sequência de caracteres	O arquivo que você deseja enviar para o agente, em relação ao diretório fileUploads do Servidor de configuração.	1.0

Nome da propriedade	Type	Descrição	Versão da API
destino	sequência de caracteres	O local do arquivo que você deseja atualizar ou excluir, em relação ao diretório de instalação do agente.	1.0
operação	enum	Operação que deseja executar: "Copiar" ou "Excluir".	1.0
agentId	número inteiro	Identificador exclusivo do agente no qual a operação é executada.	1.0
user	sequência de caracteres	O usuário que iniciou a operação.	1.0
updateErrors	Matriz	Matriz de erros retornados durante a operação.	1.0

Recurso de arquivo

Esse serviço web retorna informações sobre arquivos armazenados no Servidor de configuração.

Esse serviço web retorna informações sobre arquivos armazenados no Servidor de configuração. Os arquivos, em sua maioria, estão relacionados aos relatórios de diagnóstico (arquivos de log, perfis de agente e PBDs), mas esse recurso também é usado como armazenamento para arquivos que são destinados a registros em sistemas remotos. Os arquivos podem ser transferidos por upload para esse recurso usando o método POST.

Verbos suportados: GET, POST, DELETE, OPTIONS

Parâmetros suportados: page, size, sort

GET

```
GET https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/file/
```

POST

Este é um exemplo de upload de arquivo usando curl:

```
curl -k -H "Authorization:Bearer 3f77f1e5-6985-4019-8f49-af1ed04e0119"     -F name=my-new-app.pbd     -F file=@mylocalFile.pbd     https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/file
```

Você obtém uma resposta semelhante a esta:

```
{   "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://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/file/1/content"     }   }}
```

O valor de "id" é um identificador do arquivo que você usa posteriormente na solicitação POST agentFileOperationTask para o campo "arquivo" (por exemplo, "arquivo" : "arquivo/32").

Propriedades do recurso

Estão disponíveis as seguintes propriedades contendo informações sobre o recurso:

Nome da propriedade	Type	Descrição	Versão da API
tenant	número inteiro	ID do inquilino.	1.1
id	número inteiro	Identificador exclusivo para este recurso.	1.1
name	sequência de caracteres	Nome do arquivo.	1.1
size	número inteiro	Tamanho em bytes do arquivo descompactado.	1.1
createdBy	sequência de caracteres	O nome de usuário que fez POST do arquivo; será nulo se fizer parte de um relatório de diagnóstico.	1.1
modified	data	A hora da modificação do arquivo. Defina como 'hora atual' se um usuário tiver feito POST do arquivo.	1.1
file	arquivo com várias partes	Parâmetro de formulário usado em comandos POST para carregar o recurso de arquivo.	1.1

Recurso de pacote

Este serviço web retorna informações sobre os pacotes de agente disponíveis no APM Command Center.

Este serviço web retorna informações sobre os pacotes de agente disponíveis no APM Command Center. Também é possível fazer download desses pacotes no formato ZIP ou TAR. Verbos suportados: GET, HEAD, POST, PATCH, DELETE, OPTIONS

Parâmetros suportados: page, size, sort, q, format, projection

GET

```
GET https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/package
```

Use a seguinte solicitação para obter informações sobre o pacote com a ID 1:

```
GET https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/package/1
```

Para fazer download do pacote, acesse o link disponível na página de detalhes do pacote do Command Center na interface do usuário.

Use a seguinte solicitação para obter a instrução de instalação (no formato do Markdown) do pacote:

```
GET https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/package/1/
installInstructions
```

Use a seguinte solicitação para obter informações sobre os componentes que o pacote contém:

```
GET https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/package/1/bundles
```

Use a seguinte solicitação para obter informações sobre os componentes que são obrigatórios para o pacote:

```
GET https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/package/1/requiredBundles
```

Use a seguinte solicitação para obter informações sobre todos os componentes compatíveis com o pacote, incluindo aqueles que já estão incluídos no pacote:

```
GET https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/package/1/compatibleBundles
```

Use a seguinte solicitação para obter informações sobre todos os pacotes compatíveis com o pacote especificado:

```
GET https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/package/1/compatiblePackages
```

POST A solicitação a seguir cria um pacote de agentes com as propriedades especificadas.

```
POST https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/package{ "name": "WebSphere
 Windows Package", "description": "Example WebSphere Package", "environment": { "osName":
 "windows", "process": "websphere", "agentVersion": "10.2" }}
```

PATCH As solicitações PATCH permitem adicionar ou atualizar uma propriedade do componente no pacote. O exemplo a seguir atualiza as propriedades patched.via.rest.api e introscope.agent.acc.port com os valores fornecidos:

```
PATCH https://<host do inquilino do 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 A seguinte solicitação exclui o pacote de agentes com a ID 2:

```
DELETE https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/package/2
```

Propriedades do recurso

Estão disponíveis as seguintes propriedades contendo informações sobre o recurso:

Nome da propriedade	Type	Descrição	Versão da API
tenant	número inteiro	ID do inquilino.	1.1
id	número inteiro	Identificador exclusivo para este recurso.	1.1
name	sequência de caracteres	Nome do pacote.	1.1
description	sequência de caracteres	Comentário sobre o pacote inserido pelo usuário.	1.1
version	número inteiro	Número da versão deste pacote (incrementado após o download do pacote editado).	1.1
bundles	Sub-recurso	Componentes que o pacote contém.	1.1
emHost	sequência de caracteres	O nome do host ou o endereço IP e a porta das instâncias do Enterprise Manager às quais o agente se conecta.	1.1
latest	Booleano	Indica qual versão do pacote é a atual.	1.1
origin	número inteiro	ID da versão original do pacote.	1.1
draft	Booleano	Indica se o pacote deve estar disponível para uso.	1.1

Recurso do componente

Este serviço Web retorna informações sobre os componentes disponíveis no APM Command Center. Verbos suportados: GET, HEAD, POST, DELETE, OPTIONS. Parâmetros suportados: page, size, sort, q

GET

```
GET https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/bundle
```

POST

Esse é um exemplo de upload do componente usando a curl:

```
curl -k -H "Authorization:Bearer <TOKEN>" -F file=@leakhunter-10.5.tar.gzhttps://<host do
 inquilino do ACC>/apm/appmap/acc/apm/acc/bundle
```

Você obtém uma resposta semelhante a esta:


```
{ "id": 26, "name": "leakhunter", "addedBy": null, "author": "Not Specified",
 "displayName": "Leak Hunter", "description": "Este pacote controla o tamanho da
 maioria das coleções Java padrão.", "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

A solicitação a seguir exclui o componente com a ID 21:

```
DELETE https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/bundle/21
```

Quando um componente é excluído:

- Não ficará mais visível quando um GET do recurso for executado.
- Não será mais listado como um componente disponível quando um novo pacote for criado ou um existente editado.
- Será exibido nos pacotes existentes que o utilizam, mas serão marcados como um componente excluído. Após o componente for removido de um pacote, não será possível adicioná-lo novamente.

Observação: não é possível excluir componentes centrais. Propriedades do recurso.

Estão disponíveis as seguintes propriedades contendo informações sobre o recurso:

Nome da propriedade	Type	Descrição	Versão da API
tenant	número inteiro	ID do inquilino.	1.1
id	número inteiro	Identificador exclusivo do recurso.	1.1
name	sequência de caracteres	Nome interno do componente	1.1
displayName	sequência de caracteres	Nome do componente no formato fácil de usar.	1.1
description	sequência de caracteres	Breve descrição do componente.	1.1
version	sequência de caracteres	Versão do componente.	1.1
agentVersion	sequência de caracteres	Versão do agente do APM para o qual o componente foi criado.	1.1

Nome da propriedade	Type	Descrição	Versão da API
caminho	sequência de caracteres	Caminho para o arquivo morto do componente.	1.1
facets	Matriz	Lista de facetas que identificam o componente.	1.1
dependencies	Matriz	Lista de facetas das quais depende o componente.	1.1
enhances	Matriz	Lista de facetas que o componente aprimora.	1.1
compatibility	Sub-recurso	Define as restrições de compatibilidade do componente como "osName" e "agentVersion".	1.1
specificationVersion	sequência de caracteres	Versão da especificação de metadados do componente.	1.1
type	sequência de caracteres	Tipo do componente. Atualmente, é sempre "java".	1.1
excluído	Booleano	Determina se o componente será excluído (verdadeiro) ou ativo (nulo ou falso).	1.1
categoria	sequência de caracteres	Categoria do componente: core, ambiente, recurso, personalizado.	1.1

Recurso agentPackageTask

O serviço web agentPackageTask pode ser usado para atualizar um pacote do agente com complementos modificados ou novos que podem ser implantados dinamicamente.

O serviço web agentPackageTask pode ser usado para atualizar um pacote do agente com complementos modificados ou novos que podem ser implantados dinamicamente. Esse serviço web fornece um pacote com as modificações feitas no diretório de instalação do agente do APM. Verbos suportados: GET, HEAD, POST, OPTIONS. Parâmetros suportados: page, size, sort

GET

```
GET https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/agentPackageTask/
```

POSTA API REST a seguir inicia uma solicitação de push. Os componentes não podem ser implantados diretamente nos agentes, eles devem ser incluídos em um pacote que é enviado por push ao agente. Especifique a ID do agente que você deseja atualizar e a ID do pacote a ser entregue.

```
POST https://<host do inquilino do ACC>/apm/appmap/acc/apm/acc/agentPackageTask{agent:
 agent/1,package: package/5}
```

Propriedades do recurso. Estão disponíveis as seguintes propriedades contendo informações sobre o recurso:

Nome da propriedade	Type	Descrição	Versão da API
tenant	número inteiro	ID do inquilino.	1.1
agente	número inteiro	Identificador exclusivo do agente no qual a operação é executada.	1.1
package	número inteiro	Identificador exclusivo do pacote implantado para o agente.	1.1
status	enum	O status da solicitação.	1.1
extStatus	sequência de caracteres	Explica o status COM FALHA. De acordo com as diretrizes da API REST, um único estado com falha é obrigatório. Expande a causa dos erros; por exemplo, o controlador não responde, não é possível registrar novamente o agente no devido tempo.	1.1
creationTimestamp	data	Hora em que o recurso foi criado (em UTC).	1.1
completionTimestamp	data	Hora em que a operação foi concluída (em UTC).	1.1
expectedDuration	número inteiro	Quanto tempo será necessário para a operação em andamento.	1.1
user	sequência de caracteres	O usuário que iniciou a operação.	1.1
updateErrors	Matriz	Uma matriz de erros relacionados ao plugin, como problemas de permissões ao copiar componentes para o diretório wily.	1.1
addedBundles	Matriz	A lista de nomes de componentes que estão sendo adicionados (pode estar vazia).	1.1
removedBundles	Matriz	A lista de nomes de componentes que estão sendo removidos (pode estar vazia).	1.1

API de hipermídia do DX APM

O DX APM fornece diversas APIs de hipermídia públicas que podem ser utilizadas pelos usuários. Esta seção aborda os conceitos básicos e os mecanismos comuns compartilhados entre as APIs de hipermídia do DX APM:

A arquitetura de aplicativos REST HATEOAS (Hypermedia as the Engine of Application State - Hipermídia como o Mecanismo de Estado do Aplicativo) permite que um cliente interaja com o DX APM por meio de hipermídia. Para poder

usar a API de hipermídia, você só precisa conhecer o URL base - todos os recursos e ações disponíveis são fornecidos de maneira dinâmica pelo servidor de aplicativos à medida que você trabalha.

As APIs RESTful do DX APM usam HTTP como o protocolo padrão, e HAL (Hypertext Application Language) e JSON para as representações.

Observe que nem todos os recursos descritos nesta especificação são implementados em todas as APIs. Para obter detalhes sobre cada API, consulte API REST do DX APM.

Você pode usar várias ferramentas para interagir com as APIs de hipermídia do DX APM. Por exemplo:

- Extensão Postman do Chrome
- cURL (ferramenta de linha de comando)
- Linguagens de script (Python)

Códigos de Status de resposta

A API retorna códigos de status HTTP junto com a resposta.

Em geral, os códigos de status HTTP são agrupados em algumas categorias diferentes:

- Os códigos **1xx** são informativos
- **2xx** indica sucesso
- **3xx** instrui um redirecionamento
- **4xx** indica erros do cliente (o cliente fez algo errado)
- **5xx** define erros do servidor (o servidor fez algo errado)

A tabela a seguir mostra os códigos de status de sucesso de acordo com o método usado:

Método	Retorno em caso de êxito	Cabeçalho que acompanha	Corpo da resposta
GET	200 OK	varia	varia
POST	201 Criado	Local: aponta para o recurso criado	vazio
POST - assíncrono	202 Aceito	Local: aponta para um recurso que será criado em breve	vazio
POST	200 OK	-	recurso criado
PUT (novo recurso)	201 Criado	Local: aponta para o recurso criado	vazio
PUT (novo recurso)	200 OK	-	recurso criado
PUT (novo recurso) - assíncrono	202 Aceito	Local: aponta para um recurso que será criado em breve	vazio
PUT (recurso existente)	204 Sem conteúdo	-	vazio
PUT (recurso existente) - assíncrono	202 Aceito	Local: aponta para um recurso que será atualizado em breve	vazio
PATCH	204 Sem conteúdo	-	vazio
PATCH - assíncrono	202 Aceito	-	vazio
DELETE	200 OK	-	-
DELETE - assíncrono	202 Aceito	-	-

Autenticação e autorização da API

A autenticação das APIs RESTful do APM se baseia em tokens de portador que podem ser criados na interface do usuário do aplicativo associado. O token fornece à API o acesso aos serviços web do aplicativo.

Os clientes podem criar tokens associados às suas contas. Eles também poderão atualizar, recuperar e excluir (revogar) os tokens de sua propriedade ou aos quais tenham acesso de leitura/gravação, desde que estejam autenticados e autorizados.

Criar tokens de portador

Consulte a documentação da API específica para obter informações sobre como criar um token de portador.

Usando tokens de portador

O cliente deve enviar um token com cada solicitação. A demonstração de um token é suficiente para o servidor de recursos autenticar o cliente e aplicar as regras de autorização à solicitação.

O token de portador é enviado ao servidor de recursos no campo de cabeçalho da solicitação de autorização. Por exemplo:

```
GET /resource HTTP/1.1
Host: server.example.com
Authorization: Bearer f47ac10b-58cc-4378-a567-0e02b2c3d479
```

Status e códigos de erro HTTP da autenticação

Se a autenticação da solicitação falhar por algum motivo, o servidor de recursos retornará um código de erro HTTP relevante e um cabeçalho de resposta com detalhes do erro.

- 401 Não autorizado
- 403 Proibido

Consulte a página HTTP status code definitions (em inglês) para obter mais detalhes.

Acessando recursos

A recuperação de recursos pode ser implementada com solicitações HTTP GET simples. Ao acessar o URL base usando o navegador, você recupera o recurso raiz que informa sobre os recursos e ações disponíveis. É possível solicitar recursos individuais ou conjuntos de recursos, controlar a paginação ou a classificação, filtrar e pesquisar os recursos.

As APIs RESTful do DX APM oferecem suporte ao tipo de mídia Internet HAL e, por padrão, um documento formatado por HAL é retornado. Algumas APIs também podem oferecer suporte a outros formatos, por exemplo, application/xml, text/csv, text/plain, etc.

Recurso raiz

Todas as APIs públicas do DX APM expõem um recurso raiz. O recurso raiz contém (HAL) links para todos os recursos disponíveis e também informações adicionais, como metadados, versões, etc.

O recurso raiz pode ser recuperado acessando o URL base da API.

```
GET https://<host>:<port>/apm/<service>
```

Por exemplo, use a seguinte solicitação para obter o recurso raiz do APM Command Center:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc
```

Este é um recurso raiz recebido como resposta:

```
{
  "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
    },
    .
    .
    .
    }
  }
}
```

O recurso raiz inclui as seguintes informações:

- vendor: Broadcom
- apiVersion: a versão da API
- serverVersion: a versão do aplicativo/componente que expõe a sua lógica de negócios por essa API RESTful.
- serviceProvider: o nome do serviço totalmente qualificado
- _links: uma lista de links para todos os recursos disponíveis

Conjunto de recursos

O cliente pode solicitar recursos individuais ou um conjunto de recursos.Os conjuntos são representados como matrizes (de acordo com o formato JSON) de recursos individuais.

```
GET https://<host>:<port>/apm/<service>/resource
```

Uma matriz de recursos individuais está inserida dentro da propriedade _embedded do recurso:

```
{
    "_links": {
        << list of related links >>
    },
    "_embedded": {
         "<< resource name >>": [
            {
            << resource 1 data >>
            },
            {
            << resource 2 data >>
            },
             .....
         ]
     },
     "_page" : {
         <paging information>
     }
 }
```

Quando um recurso individual é solicitado, a resposta contém apenas o recurso solicitado.

```
GET https://<host>:<port>/apm/<service>/resource/1
```

Um exemplo de resposta:

```
{
    "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"
        }
    }
}
```


Parâmetros de solicitação comum

Ao acessar conjuntos de recursos, o número de recursos pode ser muito grande para uso prático. Portanto, os clientes podem usar as seguintes propriedades como parâmetros de consulta HTTP GET para tornar as solicitações mais específicas:

- page and size
- sort
- projection
- format
- q

Page e Size

Você pode controlar qual página é retornada ou quantos resultados uma página deve conter. Por padrão, os 20 primeiros resultados são retornados.

Use os seguintes parâmetros:

- **page**
  O número da página a ser retornada (o padrão é 0 = a primeira página é retornada).
- **size**
  O tamanho desejável da página.Size=0 significa que todos os recursos são exibidos.

Exemplos:

A seguinte solicitação retorna os primeiros 50 resultados:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?page=0&size=50
```

A seguinte solicitação retorna resultados de 51 a 60:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?page=5&size=10
```

Sort

Os conjuntos podem ser classificados pelas propriedades de recurso específicas. Os clientes podem usar o parâmetro sort para controlar a classificação.

Exemplos:

A seguinte solicitação classifica os agentes pelo nome:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?sort=agentName
```

A seguinte solicitação recupera o primeiro (size=1) recurso do agente da lista classificada por nome do agente em ordem decrescente e caminho de instalação em ordem crescente. Observe que a ordem dos parâmetros é levada em consideração.

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?
sort=name,DESC&sort=installPath,ASC&size=1
```

Projection

As projeções retornam um subconjunto predefinido dos dados.Há dois tipos de projeção disponíveis:

- **Projeções estáticas**
  As projeções estáticas são subconjuntos predefinidos das propriedades disponíveis do recurso. Elas têm um nome documentado e podem ser passadas com o parâmetro HTTP "projection" na solicitação de um conjunto de recursos ou de um recurso específico.
- **Projeções dinâmicas**
  As projeções dinâmicas permitem que o cliente defina explicitamente quais propriedades do recurso devem ser retornadas. Quando os recursos dinâmicos são usados, o parâmetro HTTP "fields" define uma lista dos campos de recurso esperados separados por vírgula.

As projeções, onde disponíveis, são documentadas na documentação de API relevante.

Exemplo:

A seguinte solicitação retorna uma lista de agentes com informações básicas:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?projection=list
```

Um exemplo de resposta:


```
{  "_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

Retorna dados no formato especificado.O parâmetro format tem precedência sobre o cabeçalho HTTP "Accept" que é o mecanismo padrão para solicitar um formato específico (por exemplo, Accept: text/csv; q=1.0).

Exemplo:

A seguinte solicitação retorna informações sobre agentes no formato CSV:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?format=csv
```

Um exemplo de resposta:


```
"id","agentName","serverName","processName","status","type","version","build","logLevel","regis
```

```
"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

Filtragem de conjunto ou pesquisa. Essa opção pode ser usada para passar consultas de pesquisa ou filtro ao servidor de recursos.

Data e hora

Datas e horas são representadas usando o formato ISO 8601.

Recursos de pesquisa e filtragem

Pesquisa é uma funcionalidade que permite a um cliente recuperar informações da API. O resultado geralmente é um documento com vários recursos diferentes.

A Pesquisa usa um recurso explícito (/search) que aceita solicitações GET passando a sequência de caracteres de pesquisa como o valor do parâmetro de consulta HTTP "q" ou solicitações POST enviando a sequência de caracteres de pesquisa com o corpo da solicitação. A resposta contém um documento JSON com os resultados na forma de recursos _embedded.

Filtragem é a capacidade da API de retornar um conjunto filtrado de um recurso específico.

A Filtragem é implementada como parte de cada recurso que oferece suporte à filtragem. Os recursos que oferecem suporte à filtragem anunciam o recurso de filtragem nos links modelados HAL (observe o parâmetro "q" no seguinte exemplo):

```
 {
    "_links": {
        "self": {
            "href": "/agent{?q,page,projection,size,sort}",
            "templated": true
         }
    }
...
...
}
```

Os clientes podem usar os recursos de filtragem de um recurso usando uma solicitação GET (passando a sequência de caracteres de pesquisa como o valor do parâmetro de consulta HTTP "q") ou uma solicitação POST (enviando a sequência de caracteres de pesquisa com o corpo da solicitação).

Exemplo:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=agentName:Tomcat
```

> **NOTE**
> O recurso de pesquisa nem sempre está disponível em uma API, assim como o recurso de filtragem nem sempre é implementado. Os usuários devem ler a documentação das APIs individuais para verificar se os recursos estão disponíveis.

A sintaxe Lucene é suportada para pesquisa e filtragem.Os parágrafos a seguir descrevem a Sintaxe da sequência de caracteres de consulta à qual as APIs RESTful do CA APM podem oferecer suporte.

Termos

Uma consulta pode consistir em um único termo ou uma frase entre aspas duplas. Vários termos podem ser combinados com os operadores Booleanos para formar uma consulta mais complexa.

Campos

Ao executar uma pesquisa, é possível especificar um campo. Você pode pesquisar qualquer campo digitando o nome do campo seguido por dois-pontos e, em seguida, o termo pelo qual está procurando. Use aspas para frases com várias palavras. Se nenhum campo for especificado, todos os campos serão pesquisados.

Exemplo:

A seguinte consulta encontra todos os agentes chamados Apache Tomcat:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=agentName:"Apache Tomcat"
```

Pesquisas com caractere curinga

A pesquisa oferece suporte a pesquisas com um único ou vários caracteres curinga dentro de termos simples (mas não em consultas de frase):

- Para executar uma pesquisa com um único caractere curinga, use o símbolo "?".
- Para executar uma pesquisa com vários caracteres curinga, use o símbolo "*".

Exemplo:

A seguinte consulta encontra todos os agentes em execução em um servidor cujo nome inclui "Linux":

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=serverName:*Linux*
```

Pesquisas de expressão regular

A pesquisa pode oferecer suporte a pesquisas de expressão regular que correspondem a um padrão entre barras "/". A sintaxe pode mudar entre as releases, mas a sintaxe atual suportada é documentada na classe RegExp.

Exemplo:

A consulta a seguir encontra relatórios cujo nome inclui os caracteres indicados. Ambas as sequências de caracteres, "ACCServerWin01|Tomcat|Tomcat Agent" e "ACCServerLinux01|Tomcat|Bobcat Agent", correspondem a essa consulta.

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/diagnosticReport?q=/ACCServer.*01\|
Tomcat\|.*Agent/
```

Pesquisas de faixa

As consultas de faixa permitem corresponder documentos cujos valores de campo estão entre o limite inferior e superior especificado pela consulta de faixa. As consultas de faixa podem ser inclusivas ou exclusivas dos limites superior e inferior. As consultas de faixa inclusivas são indicadas pelos colchetes e as consultas de faixa exclusivas por chaves.A classificação é feita de maneira lexicográfica.

Além das datas exatas, você também pode usar períodos, como semanas (w), dias (d), horas (h), minutos (m) e segundos (s).

Exemplos:

A seguinte consulta encontra todos os agentes cuja marca de data e hora do último contato é entre 1º de abril de 2015 (inclusive) e o presente:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=lastContact:[2015-04-01 TO
NOW]
```

Esta consulta encontra todos os agentes cuja marca de data e hora do último contato é entre 1º de abril e 1º de junho de 2015, mas excluindo esses dias:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=lastContact:{2015-04-01 TO
2015-06-01}
```

Esta consulta encontra agentes cuja marca de data e hora do último contato não é superior a cinco dias:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=lastContact:[-5d TO NOW]
```

A seguinte consulta encontra agentes cuja marca de data e hora do último contato são dois ou mais dias, mas não mais do que cinco semanas:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=lastContact:[-5w TO -2d]
```

Elevando um termo

A sintaxe de pesquisa pode fornecer um nível de importância de documentos correspondentes com base nos termos encontrados. Para elevar um termo, use o acento circunflexo, "^", símbolo com um fator de elevação (um número) no final do termo que está sendo pesquisado. Quanto maior o fator de elevação, mais relevante o termo será.

Operadores booleanos

Os operadores booleanos permitem que termos sejam combinados por meio de operadores lógicos.

- **OR**
  O operador OR é o operador de conjunção padrão. Isso significa que, se não houver qualquer operador booleano entre dois termos, o operador OR será usado. O operador OR vincula dois termos e encontra um documento correspondente se um dos termos existir em um documento. O símbolo || pode ser usado no lugar da palavra OR.
- **AND**
  O operador AND corresponde documentos em que ambos os termos existem em qualquer lugar no texto de um único documento. O símbolo && pode ser usado no lugar da palavra AND.
- **+**

O "+" ou operador necessário requer que o termo após o símbolo "+" exista em algum lugar no campo de um único documento.

- **NOT**
  O operador NOT exclui documentos que contêm o termo após NOT. O símbolo "!" pode ser usado no lugar da palavra NOT.
- **-**
  O "-" ou operador de proibição exclui documentos que contêm o termo após o símbolo "-".

Exemplos:

A seguinte consulta encontra agentes cujo nome é Tomcat e seu nível de registro no log é definido como debug:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=agentName:Tomcat AND
logLevel:debug
```

A seguinte consulta encontra todos os agentes ativos que são executados em um servidor Linux:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=osName:Linux NOT status:away
```

A seguinte consulta procura recursos que devem conter "Linux" e podem conter "server":

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=+Linux server
```

Agrupamento

A sintaxe oferece suporte usando parênteses para agrupar cláusulas e formar subconsultas. Isso poderá ser útil se desejar controlar a lógica booleana de uma consulta.

Exemplo:

A seguinte consulta encontra agentes cujo nome é Tomcat e estão em execução no servidor de aplicativos versão 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
```

Agrupamento de campos

A sintaxe oferece suporte usando parênteses para agrupar várias cláusulas em um único campo.

Exemplo:

A seguinte consulta encontra agentes que são executados em servidores Windows ou Linux:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=osName:(Windows OR Linux)
```

Usando escape para caracteres especiais

A sintaxe oferece suporte ao escape de caracteres especiais: + - && || ! ( ) { } [ ] ^ " ~ * ? : \ /

Para usar escape nesses caracteres, coloque uma barra invertida "\" antes do caractere.

Criando e atualizando recursos

Os recursos são criados por meio de solicitações HTTP POST ou PUT:

- POST é usado quando o cliente não precisa especificar a ID do recurso que é gerado. A API cria a ID e a retorna ao cliente.
- PUT é usado quando a ID é conhecida pelo cliente.

Um recurso pode ser atualizado utilizando-se PUT ou PATCH:

- PUT requer uma representação completa da entidade a ser fornecida, mas os campos opcionais podem ser omitidos, caso em que o servidor de recursos preserva os valores existentes. O campo Tipo de conteúdo define o tipo de mídia de internet da representação.
- PATCH é interpretado pelo servidor de recursos como uma solicitação para aplicar um patch a um recurso existente. O corpo da solicitação deve conter todas as informações necessárias para a alteração.

> **NOTE**
> Nem todos os recursos suportam esses métodos, pois alguns são somente leitura. Consulte a documentação da API específica antes de usar solicitações não seguras (criar, atualizar e excluir).

Roteiro de métodos HTTP

A tabela a seguir pode ajudá-lo a decidir qual verbo HTTP usar para criar, atualizar ou excluir recursos.

Ação	Método HTTP	URL	Corpo da solicitação
Criar um recurso sem especificar a ID	POST	Use o URL do conjunto. Por exemplo, http://host:port/apm/acc/agents	Inclua todas as propriedades não-nulas do recurso na carga. Omitir uma propriedade fará com que seu valor seja definido com o padrão, se for permitido, ou resultará em um erro, se a propriedade não tiver um valor padrão.
Criar um recurso com uma ID específica	PUT	Especifique a ID exata no URL. Por exemplo: http://host:port/apm/acc/agents/14 para criar um agente com a ID 14.	Inclua todas as propriedades não-nulas do recurso na carga. Omitir uma propriedade fará com que seu valor seja definido com o padrão, se for permitido, ou resultará em um erro, se a propriedade não tiver um valor padrão.
Atualizar um recurso com um novo (atualização completa)	PUT	Especifique a ID exata no URL. Por exemplo: http://host:port/apm/acc/agents/14 para criar um agente com a ID 14.	Inclua todas as propriedades não-nulas do recurso na carga. Omitir uma propriedade fará com que seu valor seja definido com o padrão, se for permitido, ou resultará em um erro, se a propriedade não tiver um valor padrão.
Atualizar parcialmente um recurso	PATCH	Especifique a ID exata no URL. Por exemplo: http://host:port/apm/acc/agents/14 para criar um agente com a ID 14.	Inclua apenas as propriedades que deseja atualizar. Omitir uma propriedade fará com que o servidor use o valor atual do recurso.

Excluir um recurso	DELETE	Especifique a ID exata no URL. Por exemplo: http://host:port/apm/acc/agents/14 para excluir um agente com a ID 14.	Não aplicável

Exemplos

Para obter exemplos de uso dos métodos POST, PUT ou PATCH, consulte a documentação das implementações da API específica.

Cabeçalhos HTTP comuns

Cabeçalhos de solicitação

A tabela a seguir lista os cabeçalhos de solicitação HTTP que normalmente são suportados pelas APIs RESTful do DX APM.

Cabeçalho HTTP	Caso de uso/finalidade
Accept-Language	O cliente solicita uma linguagem específica a ser usada ao construir as representações. O campo do cabeçalho de solicitação Accept-Language é semelhante a Accept, mas restringe o conjunto de linguagens naturais que são preferidas como uma resposta à solicitação.
Content-Type	Usado quando o cliente envia o corpo da mensagem com uma solicitação POST/PUT/PATCH. Descreve o tipo de mídia de internet usado para codificar o corpo da solicitação HTTP.
Authorization	Usado quando o cliente deseja autenticar a solicitação. O cliente envia as credenciais com as informações de autenticação.
Accept-Encoding	O cliente solicita que o servidor use a compactação de respostas (se possível).
Host	Cabeçalho obrigatório de acordo com o protocolo HTTP. O campo do cabeçalho de solicitação Host especifica o host da Internet e o número da porta do recurso que está sendo solicitado, conforme obtidos do URI original fornecido pelo usuário ou recurso de referência.
If-None-Match	O cliente usa esse cabeçalho para enviar o valor da marca eletrônica da representação em cache.
If-Match	O cliente desejará processar a operação solicitada (por exemplo, EXCLUIR) somente se a pré-condição da marca eletrônica for correspondida. O cabeçalho contém o valor da resposta da marca eletrônica de uma chamada anterior. O servidor deverá agir se nenhum outro cliente tiver modificado o recurso.
If-Modified-Since	O cliente usa esse cabeçalho para enviar a data da última modificação do recurso em cache.

Cabeçalhos de resposta

A tabela a seguir lista os cabeçalhos de resposta HTTP que podem ser retornados pelo servidor.

Cabeçalho HTTP	Caso de uso/finalidade
Content-Type	Descreve o tipo de mídia de internet usado para codificar o corpo da resposta HTTP.

Content-Encoding	Se estiver presente, o valor indica codificações adicionais de conteúdo que foram aplicadas ao corpo da entidade (por exemplo, compactação gzip).
Cache-Control	O campo de cabeçalho geral Cache-Control é usado para especificar diretivas que devem ser obedecidas por todos os mecanismos de armazenamento em cache ao longo da cadeia de solicitação/resposta.

Mais informações:

Consulte o site do W3C para obter informações detalhadas sobre as definições de campo de cabeçalho.

Mensagens e códigos de erro

Para cada operação com um resultado inesperado, a API retorna um erro que contém:

- código de erro
- mensagem de erro
- marca de data e hora
- um link para a documentação com a descrição completa do erro

Este é um exemplo de mensagem de erro:

```
{   "_links": {   "description": {   "href": "http://wiki.ca.com/.../Errors#ES1001"   }   },   "errorCode":
 "ES1001",   "errorMessage": "Invalid parameter: serverNames",   "timestamp": "2015-04-12T18:51:19+01:00"}
```

Intervalos de código de erro

Os códigos de erro da API começam com EA seguido por quatro dígitos.Os erros se dividem em duas categorias: erros comuns (para todas as APIs) e erros específicos de recurso. Para obter descrições de erros específicos de recurso, consulte a documentação da API relevante.

Intervalo de código de erro	Provedor de recursos
1000 - 1014	Códigos de erro herdados do EPAgent
EA0000 - EA0999	Erros de padrão do setor (códigos de status HTTP)
EA1000 - EA1999	Erros gerais de API do CA APM
EA2000 - EA2999	Erros de API REST do Gerenciador corporativo
EA3000 - EA3999	Erros de API REST da Central de comandos
EA4000 - EA4999	Códigos de erro novos do EPAgent

Erros de padrão do setor

Os erros no intervalo entre EA0100 e EA0599 são códigos de status HTTP padrão. Para obter informações detalhadas, consulte RFC 7231.

Erros gerais de API do CA APM

Código de erro (intervalo)	Descrição	Uso
EA1001	Consulta de pesquisa incorreta	Retornado quando uma solicitação de filtro ou pesquisa falha devido a uma consulta que não está em conformidade com a sintaxe Lucene.

Mensagens e códigos de erro específicos da API

Código de erro	Tipo de erro
403 Proibido	
1000	ACCESS_FORBIDDEN
1001	LOGIN_FAILED
405 Method Not Allowed	
2000	METHOD_NOT_ALLOWED
2001	ATTRIBUTE_CANNOT_BE_DELETED
2002	ATTRIBUTE_CANNOT_BE_UPDATED
400 Bad Request	
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 Not Found	
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 Conflict	

Código de erro	Tipo de erro
5000	CONFLICT
5100	OUTDATED_RESOURCE
5101	OUTDATED_DECORATION_POLICY
5102	OUTDATED_GROUPING
5103	OUTDATED_SETTINGS
5104	UNEXPECTED_NODE_STATE
5105	FOLLOWERS_TOKEN_INVALID
5106	FOLLOWER_UNREACHABLE
5107	MASTER_IS_UNREACHABLE
5200	LAST_RECORD_CANNOT_BE_DELETED
500 Internal Server Error	
6000	INTERNAL_SERVER_ERROR
415 Unsupported Media Type	
7000	UNSUPPORTED_MEDIA_TYPE
503 Service Unavailable	
8000	SERVICE_UNAVAILABLE
8001	ACC_SERVER_UNAVAILABLE

API REST do DX APM

Você pode usar a API REST do DX APM em scripts automatizados para criar, atualizar e excluir atributos de vértice.Para cada serviço web disponível, serão listados os verbos e parâmetros de solicitação HTTP suportados.

NOTE

Mais informações: API de hipermídia do DX APM

O DX APM oferece suporte aos seguintes serviços web RESTful públicos:

- Regra de atributo
- Gráfico
- Vértice do gráfico
- Incremental do gráfico
- ID do vértice de gráfico
- Vertexstatus incremental do gráfico
- Recurso raiz
- Universo
- Vértice
- ID do vértice
- Exemplo da API REST do Java para obter atualizações incrementais

Essa API inclui **novos** recursos que não estavam disponíveis anteriormente. Os recursos root, /vertex/ e /vertex/{id} originais são suportados. É recomendável migrar para a nova interface para tirar proveito dos novos recursos.

Os URLs dos recursos estão nos seguintes formatos:

- DX APMlocal:
  `http://{{hostname}}:8081/{tenantId}/apm/atc/api/`
- DX SaaS:
  `https://{{hostname}}/{tenantId}/apm/atc/api/`

A tabela a seguir mostra todos os recursos disponíveis da API REST do DX APM, bem como verbos e parâmetros HTTP que os recursos suportam.

Recurso	Descrição	Verbos HTTP	Parâmetros	Outros
/{tenantId}/apm/atc/api/vertex (conjunto)	Representa um conjunto de vértices	• GET: Sim • POST: Não • PATCH: Sim • PUT: Não • DELETE: Não	• **/vertex?projection=full** - para recuperar a projeção completa • **/vertex?projection=compact** - para recuperar a projeção compacta	• Amigável ao EPT: Não • Marca de data e hora: Sim • Filtragem: Sim
/{tenantId}/apm/atc/api/vertex/{id}	Representa um agente	• GET: Sim • POST: Não • PATCH: Sim • PUT: Não • DELETE: Não	Não	• Amigável ao EPT: Não • Marca de data e hora: Sim • Filtragem: Não
/{tenantId}/apm/atc/api/	Representa um agente	• GET: Sim • POST: Não • PATCH: Não • PUT: Não • DELETE: Não	Não	• Amigável ao EPT: Sim • Marca de data e hora: Não • Filtragem: Não
/{tenantId}/apm/atc/api/graph/vertex	Representa um conjunto de vértices	• GET: Sim • POST: Não • PATCH: Sim • PUT: Não • DELETE: Não	• /vertex?timestamp=1970-01-01T00:00:01Z - recupera um instantâneo a partir de uma data específica. O padrão é o momento presente. • /vertex?projection=full - para recuperar a projeção completa • /vertex?projection=compact - para recuperar a projeção compacta • /vertex - a carga especifica uma consulta.	• Amigável ao EPT: Sim • Marca de data e hora: Sim • Filtragem: Sim
/{tenantId}/apm/atc/api/graph/vertex/{id}	Representa um único vértice	• GET: Sim • POST: Não • PATCH: Sim • PUT: Não • DELETE: Não	/vertex?timestamp=1970-01-01T00:00:01Z - recupera um instantâneo a partir de uma data específica. O padrão é o momento presente.	• Amigável ao EPT: Sim • Marca de data e hora: Sim • Filtragem: Não

Recurso	Descrição	Verbos HTTP	Parâmetros	Outros
/{tenantId}/apm/atc/api/graph	Representa o gráfico com vértices e bordas	• GET: Sim • POST: Não • PATCH: Não • PUT: Não • DELETE: Não	• GET /{tenantId}/apm/atc/api/graph - retorna vértices, status de vértices e bordas até o momento • Filtragem no formato json, o mesmo para /graph/vertex • /graph?timestamp=1970-01-01T00:00:01Z - recupera um instantâneo a partir de uma data específica. O padrão é o momento presente. Retorna um erro para uma data futura	• Amigável ao EPT: Sim • Marca de data e hora: Sim • Filtragem: Sim
/{tenantId}/apm/atc/api/graph/incremental	Atualizações feitas nos vértices e nas bordas desde a última chamada	• GET: Sim • POST: Não • PATCH: Não • PUT: Não • DELETE: Não	• GET /{tenantId}/apm/atc/api/graph/incremental?sinceVersion=0 - esta chamada inicial retorna os vértices e as bordas até o momento. A resposta inclui lastVersion para obter as atualizações incrementais • GET /{tenantId}/apm/atc/api/graph/incremental?sinceVersion=XXXVersion4 - retorna todas as alterações incrementais desde XXXVersion4. A resposta contém informações sobre vértices e bordas atualizados e excluídos.	• Amigável ao EPT: Sim • Marca de data e hora: Não • Filtragem: Sim

Recurso	Descrição	Verbos HTTP	Parâmetros	Outros
/{tenantId}/apm/atc/api/graph/ vertexstatus/incremental	Instantâneo + atualizações incrementais feitas nos status dos vértices	• GET: Sim • POST: Não • PATCH: Não • PUT: Não • DELETE: Não	• GET /{tenantId}/apm/atc/api/vertexstatus/incremental?sinceVersion=0 - esta chamada inicial retorna os status até o momento. A resposta inclui lastVersion para obter as atualizações incrementais • GET /{tenantId}/apm/atc/api/vertexstatus/incremental?sinceVersion=XXXVersion4 - retorna todas as alterações incrementais desde a versão XXXVersion4. A resposta contém informações sobre os status atualizados.	• Amigável ao EPT: Sim • Marca de data e hora: Não • Filtragem: Não
/{tenantId}/apm/atc/api/apmData/query	Funciona como a interface de consulta propriamente dita. É possível transmitir consultas SQL usando os recursos que a tabela de esquema retornou.	• GET: Não • POST: Sim • PATCH: Não • PUT: Não • DELETE: Não	• 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"} - retorna uma contagem de métricas agrupadas por host de agente.	• Amigável ao EPT: Sim • Marca de data e hora: Sim • Filtragem: Sim
/{tenantId}/apm/atc/api/apmData/schema	Descreve todas as tabelas virtuais conhecidas que a interface pode retornar.	• GET: Sim • POST: Não • PATCH: Não • PUT: Não • DELETE: Não	GET http://<EM_HOST>:8081/{tenantId}/apm/atc/api/apmData/schema - retorna o esquema do banco de dados	• Amigável ao EPT: Sim • Marca de data e hora: Sim • Filtragem: Sim

Observação: os parâmetros diferenciam maiúsculas de minúsculas e devem estar em minúsculas.

Filtragem suportada na sintaxe do Lucene

- Oferece suporte à filtragem na sintaxe Lucene - a descrição completa da sintaxe está disponível em https://lucene.apache.org/core/4_7_0/queryparser/org/apache/lucene/queryparser/classic/package-summary.html

Autenticação

Um token de segurança é uma sequência de caracteres de texto gerada aleatoriamente e é basicamente equivalente a uma senha em texto. Esse token fornece à API acesso ao serviço web do DX APM. Você poderá gerar quantos tokens forem necessários. Você pode definir uma expiração para um token e também revogar um token. Os tokens podem ser revogados a qualquer momento e por qualquer usuário. No entanto, os tokens são permanentes e nunca desaparecem da lista na guia **Segurança**.

Siga estas etapas:

1. Na interface de usuário, selecione **Configurações**, **Segurança**.
2. Selecione o botão **Gerar outro token**.
3. Defina a expiração e adicione um rótulo.
4. Selecione **API pública** para **Tipo**.
5. Selecione **Gerar token**.

   WARNING
   Por motivos de segurança, não é possível exibir um token de mais de uma vez. A única vez que o token é exibido é após clicar em **New Token**.
6. Use o token no cabeçalho de autorização sua solicitação.

   NOTE

   Mais informações:

   - Autenticação e autorização da API
   - Gerar códigos e mensagens de erro da API

Configuração

NOTE
A configuração da API REST do DX APM só está disponível no DX APM local.

API de aplicativo

A API de aplicativo é documentada por meio do OpenAPI versão 3. O documento do OpenAPI pode ser baixado de uma instalação do APM. Ele pode ser usado para gerar clientes para várias linguagens ou com alguns clientes HTTP/REST interativos.

Siga as etapas mencionadas abaixo para acessar o documento do OpenAPI 3 que descreve a API pública do servidor de configuração do APM para a Integração de aplicativos e usá-la para gerar clientes Java usando o openapi-generator.

Siga estas etapas:

1. Faça download do documento do OpenAPI atual.
   a. Efetue logon como um usuário que possa acessar o servidor de configuração do APM.
   b. Abra o URL `https://<HOST>/acc/apm/acc/versioned.api.json` e baixe-o.

      NOTE
      No URL acima, substitua <HOST> pelo nome do host/nome do DNS real.
2. Crie um script para baixar e executar o `openapi-generator` . Esse script é para shell Bash, mas pode ser adaptado para ser executado em outros ambientes. Coloque-o em um novo diretório e forneça um nome, por exemplo, `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
```

```
fi

java -jar "$(set -- openapi-generator-cli*.jar; echo "$1")" generate \
  -i versioned.api.json \
  --api-package com.example.apm.acc.client.api \
  --model-package com.example.apm.acc.client.model \
  --invoker-package com.example.apm.acc.client.invoker \
  --group-id com.example.apm.acc \
  --artifact-id spring-openapi-generator-api-client \
  --artifact-version 0.0.1-SNAPSHOT \
  -g java \
  -p java8=true \
  -c <(echo '{"openApiNullable": false}') \
  --library resttemplate \
  -o spring-openapi-generator-api-client
```

3. Coloque o `versioned.api.json` baixado no mesmo diretório que o script e execute-o. Ele irá baixar o arquivo jar para `openapi-generator` , se ele estiver faltando. Em seguida, execute o gerador com opções adequadas para o código abaixo. A saída estará no subdiretório `spring-openapi-generator-api-client` .
4. Adicione o arquivo `spring-openapi-generator-api-client/src/main/java/com/example/ClientTestTool.java` com o conteúdo abaixo:

```
package com.example;

import com.example.apm.acc.client.api.ApplicationApi;
import com.example.apm.acc.client.invoker.ApiClient;
import com.example.apm.acc.client.model.ApplicationRestDto;
import com.example.apm.acc.client.model.DraftChangeDto;
import com.example.apm.acc.client.model.DraftChangeItemType;
import com.example.apm.acc.client.model.DraftChangeListDto;
import com.example.apm.acc.client.model.OnboardingConfigurationDto;
import com.example.apm.acc.client.model.TierConfigurationItemPropertyValueType;
import com.example.apm.acc.client.model.TierRestDto;
import com.example.apm.acc.client.model.TierRestDtoOverridesInner;
import com.example.apm.acc.client.model.TierUserChoiceItemDto;
import com.example.apm.acc.client.model.TierUserChoiceItemPropertyDto;
import org.springframework.web.client.RestClientException;

import java.util.ArrayList;
import java.util.List;
import java.util.TreeMap;

public class ClientTestTool {
    public static void main(String[] args) throws RestClientException {
        ApiClient defaultClient = new ApiClient();

 defaultClient.setBearerToken("eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NiJ9.eyJzdWIiOiJURU5BTlQxIiwiZHluZXhwIjp0cnVlLCJ0aWQi
xpCNYNHI7Jr5tSys88jNycgTg10m5Ueao-nUHrnfyUBq2aLJ7Vt0ZRrfA");
        defaultClient.setBasePath("https://HOST/acc/apm/acc");// optional, can use the default value if
 server is the same as in json
        ApplicationApi applicationApi = new ApplicationApi(defaultClient);

        System.out.println("Reading configuration");
```

```
        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(TierConfigurationItemPropertyValueType.BOOLEAN);
        optionsValueUseOpenTracingJavaMapValue.add(openTracingJavaEnable);
        optionsValueUseOpenTracingJavaMap.put("open-tracing-java",
optionsValueUseOpenTracingJavaMapValue);
        optionsValueUseOpenTracingJava.setOverrides(optionsValueUseOpenTracingJavaMap);
        optionsValue.add(optionsValueUseOpenTracingJava);
        final TierUserChoiceItemDto optionsValueHttpCollectorIagent = 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(TierConfigurationItemPropertyValueType.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(TierConfigurationItemPropertyValueType.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.addItemsItem(itemsItem);
            System.out.println("Publishing the application.");
            applicationApi.publishApplication(createdApplication.getEntityId(), draftChangeListDto);

            System.out.println("Creation is complete.");
        }
    }
```

NOTE
Este programa Java usará o cliente gerado para criar um aplicativo e adicionar uma camada a ele que descreva o Infrastructure Agent para Linux configurado para monitorar um PostgresDB.

5. Obtenha um token de API na UI do APM ATC. Vá para **Configurações** > **Segurança** > **Gerar outro token**. Selecione o tipo como "API pública".
6. Atualize a chamada para o método `setBearerToken` com o token válido na origem da classe `ClientTestTool` .
7. Compile e execute a classe `ClientTestTool` .
   a. Você pode fazer isso por meio de qualquer IDE que ofereça suporte a Java e Maven.
   b. Você pode fazer isso por meio do Java e do Maven diretamente na linha de comando.
      a. Compile com o comando mvn clean install no diretório `spring-openapi-generator-api-client` .
      b. Execute com `mvn exec:exec -Dexec.executable=java -Dexec.args="-cp %classpath com.example.ClientTestTool"` .
8. O resultado deve ser um novo aplicativo com uma camada que define o monitor de infraestrutura do `PostgresDB` para Linux.

NOTE
Se desejar usar o documento do OpenAPI para gerar um cliente com modelo tipificado com outras linguagens/estruturas de destino, certifique-se de que as propriedades desconhecidas do objeto JSON sejam ignoradas na desserialização e que o cliente esteja enviando corretamente os cabeçalhos Accept e Content-Type, de acordo com o documento OpenAPI, para obter compatibilidade com versões futuras do APM.

Solução de problemas

Sintoma	Solução
Para o APM local, o cliente pode falhar com a exceção `javax.net.ssl.SSLHandshakeException` quando o APM é configurado com um certificado HTTPS autoassinado ou assinado por uma autoridade de certificação não conhecida publicamente.	Você precisa de um truststore com um certificado correspondente ao usado no servidor para conectar o cliente. Por exemplo, dessa forma, um truststore chamado `trust.jks` (no diretório `spring-openapi-generator-api-client`) será usado: `mvn exec:exec -Dexec.executable=java -Dexec.args="-cp %classpath -Djavax.net.ssl.trustStore=trust.jks -Djavax.net.ssl.trustStorePassword=changeit com.example.ClientTestTool"`

Regra de atributo

Diretrizes para Métodos Post e Put use as seguintes diretrizes para criar (POST) e atualizar (PUT) as regras de atributo.

As diretrizes e os métodos a seguir estão disponíveis para este recurso:

- Diretrizes para métodos Post e Put
- Métodos

Diretrizes para métodos Post e Put

Use as diretrizes a seguir para criar (POST) e atualizar (PUT) regras de atributo.

Campos de carga

Os campos obrigatórios para todas as solicitações de carga são os seguintes:

layer	existingName	customName	customValue	operator	operand

Valores de campo

Operator

Os valores permitidos para o campo `operator` são os seguintes:

Observação: os valores que terminam com `_CI` não diferenciam maiúsculas de minúsculas.

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**

Observação: se o valor do `operator` for igual a `IS_EMPTY` ou `IS_NOT_EMPTY` , o `operand` deve ser uma sequência de caracteres vazia:

```
"operator" : "IS_NOT_EMPTY" ,
"operand" :  "" ,
```

Camada

Os valores permitidos para o campo `layer` são os seguintes:

ATC	APM_INFRASTRUCTURE	INFRASTRUCTURE

UniverseId

Se você fornecer um valor nulo para o campo `Universoid` ou não especificar o campo `Universoid` , a regra de atributo será criada no universo Empresa. Se a regra de atributo já existir, a regra de atributo será transferida para o universo Empresa.

Enabled

Se você não especificar o campo `enabled` , o valor será definido como falso por padrão.Esse valor falso desativa a visibilidade da regra de atributo na GUI.

Id and _links

Os campos `id` e `_links` são somente leitura. Se você fornecer valores para esses campos, os valores serão ignorados.

outputclass="bc-h2" id="Methods">Methods

Métodos

GET /{tenantId}/apm/atc/api/attribute/rule

Esse método retorna a lista de regras de atributo para todos os universos aos quais um usuário tem acesso.

```
{
 "_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}

Esse método usa uma ID de regra de atributo para retornar uma única regra de atributo.


```
{
 "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

Esse método cria uma regra de atributo. Veja a seguir um exemplo de carga de solicitação:

```
{
 "existingName": "agent",
 "operator": "IS_NOT_EMPTY",
 "operand": "",
 "customName": "aaaa",
 "customValue": "aaaa",
 "universeId": null,
 "layer": "APM_INFRASTRUCTURE",
 "enabled": false
 }
```

Veja a seguir um exemplo de resposta:

```
{
 "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}

Esse método usa uma ID de regra de atributo para atualizar a regra de atributo que corresponde à ID fornecida. Veja a seguir um exemplo de solicitação:

```
{
 "existingName":"agent",
 "operator":"CONTAINS",
 "operand":"name",
 "customName":"sample",
 "customValue":"2144",
 "universeId":null,
 "layer":"ATC",
 "enabled":true
 }
```

Veja a seguir um exemplo de resposta:

```
{
 "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}

Esse método usa uma ID de regra de atributo para excluir a regra de atributo que corresponde à ID fornecida.

Gráfico

Este recurso retorna um gráfico completo, incluindo vértices, status de vértice e bordas, de acordo com a marca de data e hora e os critérios de filtragem especificados. Você poderá usar seus próprios scripts ou uma biblioteca de terceiros para percorrer o gráfico e extrair as informações necessárias. Por exemplo, vértices crescentes, vértices decrescentes ou o caminho mais curto entre dois vértices.

- Faz a junção dos gráficos em todos os universos aos quais você tem acesso
- Se ETC atender a diversos agrupamentos, o terminal unirá os vértices entre os agrupamentos.
- Permite consultas históricas a partir da marca de data e hora. Atributos, alertas e outros campos têm histórico. A marca de data e hora padrão é o momento presente.

É possível invocar este terminal de duas maneiras:

1. Formulário GET simples, se você não precisar de um filtro
2. GET /{tenantId}/apm/atc/api/graph?timestamp=2016-01-01T00:00:01Z
3. A opção POST será útil se você precisar de um filtro - dessa forma, a condição de filtro será enviada como uma carga POST. Para obter mais informações sobre filtros, consulte Vértice do gráfico.
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"
  }
}}
```

Vértice do gráfico

Este recurso retorna a lista de vértices de acordo com os critérios de filtragem e a projeção especificados.

- Permite consultas históricas a partir da marca de data e hora. Atributos, alertas e outros campos têm histórico. A marca de data e hora padrão é o momento presente.
- Suporta projeções estáticas - compactas e completas. O padrão é compacta.

É possível invocar este terminal de duas maneiras:

1. Formulário GET simples, se você não usar um filtro.
   GET /{tenantId}/apm/atc/api/graph/vertex?timestamp=2016-01-01T00:00:01Z&projection=full
2. A opção POST será útil se você usar um filtro - dessa forma, a condição de filtro será enviada como uma carga 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"
                        }
                ]
            }
        ]}
```

Formato e recursos de filtro

1. Operações suportadas - IN, NOT_IN, MATCHES, NOT_MATCHES
2. IN - correspondência exata

```
// 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 - não é igual.

```
// 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 - correspondência com o caractere curinga usando '*'.Um asterisco (*) no padrão pode fazer a correspondência com zero ou mais caracteres no valor.

```
// 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 - o caractere curinga não corresponde.

```
// 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 ]
                        }
                ]
        }
    ]
}
```

O filtro pode combinar mais de uma condição de filtragem:

```
    {
        "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"]
                                }
                            ]
                        }
                    ]
                },
        ]
    }
```

Como o filtro "attributeName" suporta

- Nomes de atributo de vértice válidos - por exemplo, "agente" ou "nome do host"
- "serviceId" - para filtrar por "Serviço comercial", da mesma forma que está visível na UI
- "transactionId" - para filtrar por "Transação Comercial", da mesma forma que está visível na UI

Projeções

Compacta (padrão)

```
?{
  "_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"
    }
  }
}
```


Completa


```
?{
  "_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

Atualiza os valores de atributo para um vértice escolhido.

- Os nomes de atributo devem ser exclusivos. Os atributos duplicados serão descartados.
- NULL exclui o atributo.
- Se existir um atributo para um determinado vértice, ele será atualizado, caso contrário, o PATCH criará um atributo CUSTOM.
- Os atributos CUSTOM podem ser criados, atualizados ou excluídos. Se PATCH criar um atributo, ele será sempre CUSTOM.
- Os atributos CUSTOM criados pelas regras de atributo podem ser atualizados.
- Os atributos BASIC não podem ser atualizados ou excluídos.

Veja a seguir um exemplo de carga de solicitação:

```
?{ "items" : [
    {
            "id":"Enterprise Team Center:8",
            "attributes": {
                "Attr1":["newValue", "newValue2"],
                 "Attr2": null
        }
    },
    {...},
    {...}
  ]
}
```

Incremental do gráfico

Retorna as atualizações incrementais feitas na estrutura do gráfico.Cada resposta contém a **lastVersion** a ser usada para a próxima chamada.

- Faz a junção dos gráficos em todos os universos aos quais você tem acesso
- A resposta não contém todas as atualizações. Se houver mais de uma atualização do mesmo vértice/borda, somente a última atualização efetivada será relatada.
- Em uma configuração de vários agrupamentos, faça a correlação entre agrupamentos no destinatário - veja o exemplo.

GET /{tenantId}/apm/atc/api/graph/incremental?sinceVersion=0
Essa chamada inicial retornará os vértices e as bordas a partir de agora. A resposta inclui **lastVersion** para obter as atualizações incrementais. Armazene os resultados no cache do destinatário como um instantâneo inicial.

```
{
```

```
    "_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"
      },
      "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/incremental?
sinceVersion=eyJ0eXBlIjoiR1JBUEgiLCJ2ZXJzaW9ucyI6eyJ0YXMtY3otbmVkLmNhLmNvbTo4MDgxIjoxNDczNzUzMzE5NjY2LCJ0YXMtY3otbmMwLm
      }
  },
  "lastVersion":
 "eyJ0eXBlIjoiR1JBUEgiLCJ2ZXJzaW9ucyI6eyJ0YXMtY3otbmVkLmNhLmNvbTo4MDgxIjoxNDczNzUzMzE5NjY2LCJ0YXMtY3otbmMwLmNhLmNvbTo4M
 means reset the cache
```

```
}
```

GET /{tenantId}/apm/atc/api/graph/incremental?sinceVersion=XXXXYYYYZZZZZ
Retorna as alterações incrementais feitas desde a última chamada. A última chamada é identificada pelo campo **lastVersion** da resposta.
A resposta contém informações sobre vértices novos ou modificados, vértices removidos, bordas novas ou modificadas e bordas removidas. Aplique a resposta ao instantâneo. Mantenha-a no cache do destinatário. Veja o exemplo.

```
{
    "_embedded": {
      "vertex": [ //vertex inserts and updates
            {
          "id": "Enterprise Team Center:8",
          "externalId": "ApplicationService:Mediator"
          "startTime":"2015-04-12T09:59:12.221Z" ,
          "attributes": {
                "name1": ["value1","val5"],
                "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": [ //vertex deleted since last call. Only changes are included, i.e. if Vertex appeared
 but then went away then it won't be shown here.
        {
            "id": "Enterprise Team Center:12",
            "endTime" : "2015-04-12T10:22:14.556Z"
        },
        {
            "id": "Enterprise Team Center:14",
            "endTime": "2015-04-12T10:23:14.556Z"
        }
      ],
      "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": [  //Edges deleted since last call. Same as for Vertices.
        {
            "sourceId" : "Enterprise Team Center:10",
            "targetId" : "Enterprise Team Center:11",
              "businessTransactionId" : "Enterprise Team Center:1"
              "endTime": "2015-04-12T10:59:12.221Z"
        },
        {...}
      ]
    },
    "_links": {
      "self": {
        "href": "http://tas-cz-nc6.ca.com:8081/{tenantId}/apm/atc/api/graph/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/incremental?
sinceVersion=eyJ0eXBlIjoiR1JBUEgiLCJ2ZXJzaW9ucyI6eyJ0YXMtY3otbmVkLmNhLmNvbTo4MDgxIjoxNDczNzUzOTU2MDc0LCJ0YXMtY3otbmMwLm
      }
    },
    "lastVersion":
 "eyJ0eXBlIjoiR1JBUEgiLCJ2ZXJzaW9ucyI6eyJ0YXMtY3otbmVkLmNhLmNvbTo4MDgxIjoxNDczNzUzOTU2MDc0LCJ0YXMtY3otbmMwLmNhLmNvbTo4M
 means reset the cache
}
```


ID do vértice de gráfico

Representa um único vértice identificado por 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

Atualiza os valores de atributo para um vértice escolhido.

- Os nomes de atributo devem ser exclusivos. Os atributos duplicados serão descartados.
- NULL exclui o atributo
- Se existir um atributo para um determinado vértice, ele será atualizado, caso contrário, o PATCH criará um atributo CUSTOM.
- Os atributos CUSTOM podem ser criados, atualizados ou excluídos. Se PATCH criar um atributo, ele será sempre CUSTOM.
- Os atributos CUSTOM criados pelas regras de atributo podem ser atualizados.
- Os atributos BASIC não podem ser atualizados ou excluídos.

Veja a seguir um exemplo de carga de solicitação:

```
{
    "attributes": {
        "Attr1": ["newValue3", "newVal3"],
        "Attr2": null
    }
}
```

Vertexstatus incremental do gráfico

Retorna as atualizações incrementais para os status do vértice.Cada resposta contém a **lastVersion** a ser usada para a próxima chamada.

- Faz a junção dos status do vértice em todos os universos aos quais um usuário tem acesso
- A resposta não contém todas as atualizações. Se houver mais de uma atualização do mesmo status, somente a última atualização efetivada será relatada.

GET /{tenantId}/apm/atc/api/graph/vertexstatus/incremental?sinceVersion=0
Essa chamada inicial retornará todos os status a partir de agora. A resposta inclui **lastVersion** para obter as atualizações incrementais. Armazene essa chamada no cache do destinatário como um instantâneo inicial.

```
?{
    "_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=eyJ0eXBlIjoiVkVSVEVYU1RBVFVTIiwidmVyc2lvbnMiOnsidGFzLWN6LW5lZC5jYS5jb206ODA4MSI6MTQ3Mzc1NDMzMDQ1MSwidGFzLW
      }
    },
    "lastVersion":
 "eyJ0eXBlIjoiVkVSVEVYU1RBVFVTIiwidmVyc2lvbnMiOnsidGFzLWN6LW5lZC5jYS5jb206ODA4MSI6MTQ3Mzc1NDMzMDQ1MSwidGFzLWN6LW5jMC5jY
 means reset the cache
}
```

GET /{tenantId}/apm/atc/api/graph/incremental?sinceVersion=XXXXYYYYZZZZZ
Retorna as alterações incrementais feitas desde a última chamada. A última chamada é identificada pelo campo **lastVersion** da resposta.
A resposta contém informações sobre vértices novos ou modificados, vértices removidos, bordas novas ou modificadas e bordas removidas. Aplique esta resposta ao instantâneo. Mantenha-a no cache do destinatário. Veja um exemplo:

```
{
    "_embedded": {
      "status": {
            "alerts": [  //we only have updates here because status does not get deleted, it only goes to
 "UNKNOWN"
                        //only status changes since last call are included - same as we do with Vertices and
 Edges
                    {
                    "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": "UNKNOWN",        // "UNKNOWN" means alert went away
                    "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=eyJ0eXBlIjoiVkVSVEVYU1RBVFVTIiwidmVyc2lvbnMiOnsidGFzLWN6LW5lZC5jYS5jb206ODA4MSI6MTQ3Mzc1NDMzMDQ1MSwidGFzLW
      }
    },
 "lastVersion":
 "eyJ0eXBlIjoiVkVSVEVYU1RBVFVTIiwidmVyc2lvbnMiOnsidGFzLWN6LW5lZC5jYS5jb206ODA4MSI6MTQ3Mzc1NDMzMDQ1MSwidGFzLWN6LW5jMC5jY
 means reset the cache
}
```


NOTE

- Repita as chamadas para obter atualizações incrementais com a frequência que for necessária. Toda vez que você fizer a chamada, todas as alterações serão atendidas sem a definição de limites e sem paginação. Cargas muito grandes serão tratadas com um JSON de resposta por streaming em vez de serem mantidas na memória.
- Você pode obter um novo instantâneo dos dados a qualquer momento. Use **GET /{tenantId}/apm/atc/api/graph/incremental?sinceVersion=0**. Por exemplo, essa chamada poderá ser usada se o aplicativo for reiniciado. Essa chamada lhe dará uma nova lastVersion para obter atualizações incrementais.

Recurso raiz

Retorna a lista de opções disponíveis para a API com informações gerais sobre a API em questão. O recurso pode ser acessado pelo público em geral no SSL sem necessidade de um token de autorização. O recurso raiz atua como um ponto de partida para a execução da API, pois ele vincula todos os caminhos disponíveis que são acessíveis. O link para um recurso pode ser um modelo de URI. Nesse caso, o recurso contém uma propriedade templated:true. Se a propriedade não estiver presente ou seu valor for diferente, o recurso conterá um URI simples.

GET

Exemplo de resposta:


```
{
  "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
      }
    ]
  }
}
```

Propriedades do recurso:

Nome da propriedade	Type	Descrição	Versão da API
serviceProvider	Sequência de caracteres	Descreve o provedor do serviço - com.ca.apm.appmap	1.0.0
serverVersion	Sequência de caracteres	Versão do servidor que fornece a API (versão do APM)	1.0.0
apiVersion	Sequência de caracteres	Versão da API	1.0.0
vendor	Sequência de caracteres	Fornecedor do serviço - Broadcom	1.0.0
_links	Matriz	Lista todas as opções disponíveis para essa API	1.0.0
_links.self	Link HAL	Contém o URL para o recurso raiz em si	1.0.0
_links.doc	Link HAL	Contém o URL para a documentação da API pública	1.0.0
_links.* Por exemplo, vértice.	Link HAL	Apresenta todos os terminais disponíveis para um determinado recurso	1.0.0

Universo

Este recurso retorna as propriedades básicas de universos individuais ou de todos os universos aos quais um usuário tem acesso.

Este recurso retorna as propriedades básicas de universos individuais ou de todos os universos aos quais um usuário tem acesso.

É possível invocar este terminal de duas maneiras:

- **GET /{tenantId}/apm/atc/api/universe**
  Retorna uma lista dos universos aos quais um usuário tem acesso

```
{
"_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 /{tenantId}/apm/atc/api/universe/{id}**
  Retorna as propriedades do universo individual que corresponde à ID do universo fornecida.


```
{
"name": "TestUniverse",
"_links": {
 "parent": {
 "href": "http://localhost/{tenantId}/apm/atc/api/universe"
},
"self":{
 "href": "http://localhost/{tenantId}/apm/atc/api/universe/UN172"
 }
 },
"id": "UN172"
}
```


Vértice

Retorna a lista de vértices de acordo com critérios de filtragem e a projeção especificados

- Permite consultas históricas a partir da marca de data e hora. Atributos, alertas e outros campos têm histórico. A marca de data e hora padrão é o momento presente.
- Suporta projeções estáticas - compactas e completas. O padrão é compacta.

Verbos suportados: GET, PATCH

Parâmetros suportados: projection, timestamp, q

GET

Filtragem suportada do conjunto

Por marca de data e hora para recuperar um instantâneo do conjunto a partir da marca de data e hora. O padrão é o momento presente.

- GET /{tenantId}/apm/atc/api/vertex?timestamp:1970-01-01T00:00:01Z
- Oferece suporte à filtragem na sintaxe Lucene - a descrição completa da sintaxe está disponível em https://lucene.apache.org/core/4_7_0/queryparser/org/apache/lucene/queryparser/classic/package-summary.html

Exemplos de filtragem:

- GET /{tenantId}/apm/atc/api/vertex**?q=city:Paris AND sky:blue** você pode combinar as expressões de filtragem usando operadores lógicos
- GET /{tenantId}/apm/atc/api/vertex**?q=(city:Paris AND sky:blue) OR (city:London AND sky:grey)** expressões lógicas de agrupamento usando chaves
- GET /{tenantId}/apm/atc/api/vertex**?q=sky\ color:deep\ bluespaces** e outros caracteres especiais devem ser separados por barras de escape

/vertex/ suporta as projeções compacta e completa. O padrão é compacta.

Completa


```
?{
    "_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"}
                    }
                }
            ]
    }
}
```


Compacta


```
? {
    "_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

Atualiza os valores de atributo para um vértice escolhido.

- Os nomes de atributo devem ser exclusivos. Os atributos duplicados serão descartados.
- Se existir um atributo para um determinado vértice, ele será atualizado, caso contrário, o PATCH criará um atributo CUSTOM com um nome especificado.
- Os atributos CUSTOM podem ser criados, atualizados ou excluídos. Os atributos criados pelo PATCH serão sempre CUSTOM
- Os atributos DECORATED podem ser atualizados. Se forem atualizados, passarão a ser CUSTOM.
- Os atributos agrupados não podem ser atualizados nem excluídos.

Veja a seguir um exemplo de carga de solicitação:

- Os nomes de atributos fornecidos devem ser exclusivos. PATCH ignora quaisquer atributos duplicados.

```
 [{
    "id":"3",
    "attributes": {
        "Attr1":"newValue",
        "Attr2": null // NULL deletes attribute
        }
},
...]
```

Parâmetros suportados

Nome da propriedade	Type	Descrição
vertex	Matriz	Matriz de vértices - depende da projeção.

ID do vértice

O recurso retorna informações detalhadas para um único vértice.

A estrutura de retorno é as mesma em GET /vertex.

Verbos suportados: todos

Parâmetros suportados: 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>}
       }
```

Parâmetros HTTP adicionais

- timestamp - recupera um instantâneo do recurso a partir da marca de data e hora. O padrão é o momento presente. GET /{tenantId}/apm/atc/api/vertex/123?timestamp=1970-01-01T00:00:01Z

PATCH

Atualiza os valores de atributo para um vértice escolhido.

- Os nomes de atributo devem ser exclusivos. Os atributos duplicados serão descartados.
- Se existir um atributo para um determinado vértice, ele será atualizado, caso contrário, o PATCH criará um atributo CUSTOM com um nome especificado.
- Os atributos CUSTOM podem ser criados, atualizados ou excluídos. Os atributos criados pelo PATCH serão sempre CUSTOM.
- Os atributos DECORATED podem ser atualizados. Se forem atualizados, passarão a ser CUSTOM.
- Os atributos agrupados não podem ser atualizados nem excluídos.

Veja a seguir um exemplo de carga de solicitação:

- Os nomes de atributos fornecidos devem ser exclusivos. PATCH ignora quaisquer atributos duplicados.

```
{
    "attributes": {
        "Attr1":"newValue",
        "Attr2": null // NULL deletes attribute
    }
```

```
}
```

Parâmetros suportados

Nome da propriedade	Type	Descrição
id	Matriz de uma única sequência de caracteres	A ID do vértice
marca de data e hora	Marca de data e hora	*Marca de data e hora do instantâneo fornecido no formato 1970-01-01T00:00:01Z*
attributes	Matriz	Lista de todos os atributos definidos no vértice
attributes.name	Sequência de caracteres	Nome do atributo
attributes.value	Sequência de caracteres	Valor do atributo
attributes.type	Sequência de caracteres	Tipo do atributo. Os tipos de atributos suportados no momento são "CUSTOM","DECORATED" e "GATHERED"

Exemplo da API REST do Java para obter atualizações incrementais

O exemplo a seguir mostra como usar a API REST pública para obter atualizações incrementais.

```
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 do SQL

Use a API REST pública do SQL para extrair dados brutos de métrica do APM e integrá-los às ferramentas personalizadas. Assim como outras APIs REST do APM, a interface da API REST do SQL usa autenticação que se baseia em token. Essa API REST é executada nos seguintes modos do EM (Enterprise Manager - Gerenciador Corporativo):

- Independente
- Coletor
- MOM (Manager of Managers - Gerenciador de Gerenciadores)
- Enterprise Team Center

NOTE

- O recurso API REST do SQL foi introduzido na release 10.7 Service Pack 1 (SP1).
- Esse recurso não fornece todos os recursos SQL, como JOINs e subseleções.

IMPORTANT
Use a API REST pública do SQL *somente* para extrair dados de métricas do APM. Para extrair dados de métricas do APM ou de outros produtos, use a API REST de consulta de métricas.

Estabelecer conexão com a API REST do SQL

Siga estas etapas:

1. Efetue logon no Team Center e clique em **Segurança**.
2. Clique em **Gerar outro token**.
   Uma janela de caixa de diálogo é exibida.
3. Informe o **Rótulo** (nome) e selecione **API pública** para o **Tipo**.
4. Defina a data de expiração ou selecione **Nunca expira**.
5. Clique em **Gerar token**.
   O sistema gera um novo token.

WARNING

Por motivos de segurança, você vê um token apenas uma vez. Armazene o token em um local seguro antes de fechar essa janela da caixa de diálogo. Não divulgue o token para indivíduos não autorizados.

O token agora é exibido entre os outros tokens na guia **Segurança**.

6. Teste a conexão com a amostra de uma consulta, por exemplo:

```
URL
                http://<EM Host>:8081/{tenantId}/apm/atc/api/apmData/schema
                GET
Header
                Accept: application/json
                Authorization: Bearer <Security Token>
```

Você estabeleceu conexão com a API REST.

Métricas de suportabilidade

As métricas de suportabilidade para a API REST do SQL têm o prefixo `Enterprise Manager|Data Store|SQL API` em seus nomes. A seguinte tabela lista as métricas de suportabilidade disponíveis:

Nome da métrica de suportabilidade	Descrição
Tempo médio de resposta (ms)	Tempo médio para processar a consulta de entrada
Bytes Sent Per Interval	Número de bytes enviados como resultado em um intervalo
Respostas por intervalo	Consultas bem-sucedidas em um intervalo
Invocações simultâneas	Número de conexões paralelas com um terminal de consulta
Clamped Connections Per Interval	Número de conexões rejeitadas devido ao limite
Erros por intervalo	Número de consultas com falha em um intervalo

Recursos de API REST

A API REST do SQL contém os seguintes recursos:

`/{tenantId}/apm/atc/api/apmData/schema`

Descreve todas as tabelas virtuais conhecidas que a interface pode retornar.

`/{tenantId}/apm/atc/api/apmData/query`

Funciona como a interface de consulta propriamente dita. É possível transmitir consultas SQL usando os recursos que a tabela de esquema retornou.

Você pode definir consultas usando as funções contagem, mínimo, máximo e média. As funções agregadas a seguir são suportadas apenas na coluna agg_value na tabela metric_data: sum; apm_average; apm_aggregate. A função de agregação resulta no seguinte:

- a função de agregação sum fornece a soma dos valores da coluna agg_values
- apm_aggregate fornece a soma ou a média ponderada com base nas métricas consultadas
- apm_average fornece apenas a média ponderada

Exemplos de consulta

Use os seguintes exemplos para consultar a API:

- Exemplo 1: **Obter contagem de métricas agrupadas pelo host do agente**

Este exemplo usa uma solicitação POST no recurso `/{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"}
```

Exemplo 2: Obter esquema

Este exemplo usa uma solicitação GET no recurso `/{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"
                    ]
                }
            ]
        }
    ]}
```

- **Exemplo 3: Obter dados de métrica com uma cláusula where**

Este exemplo usa uma solicitação POST no recurso `/{tenantId}/apm/atc/api/apmData/query`.

```
{

  "query" : "select <Columns> from metric_data <Where Clause>"

}
```

Resultado:

```
{
  "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 ]

  ]}
```

- **Exemplo 4: Obter dados de métrica com uma função de agregação**

Este exemplo usa uma solicitação POST no recurso `/{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"
}
```

Resultado:

```
{
    "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
        ]
    ]
}
```

Exemplos de consulta de URL

Use os seguintes exemplos para consultar a API no cURL:

- **Exemplo 1: Obter esquema**

```
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
```

- **Exemplo 2: Obter um esquema legível para humanos sem recursos 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
```

- **Exemplo 3: Obter todas as fontes**

```
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;" }'
```

Resultado:

```
{"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"]

]}
```

- **Exemplo 4: Obter todas as métricas de agentes com caracteres específicos na coluna 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%'\" }"
```

Resultado:

```
{"columns":[{"name":"source_name","type":"string"},
{"name":"agent_host","type":"string"},{"name":"agent_process","type":"string"},
{"name":"agent_name","type":"string"},{"name":"domain_name","typ

e":"string"},{"name":"metric_path","type":"string"},
{"name":"metric_attribute","type":"string"},{"name":"attribute_type","type":"long"},
{"name":"first_seen","type":"timestamp"},{"name":"last_see

n","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]

,….
```

- **Exemplo 5: Obter a contagem de métricas agrupadas por agentes**

```
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 \" }"
```

Resultado:

```
{"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]

]}
```

- **Exemplo 6: Obter todos os dados de métrica da última hora**

  NOTE

  Essa consulta retorna um arquivo JSON muito grande. Cuidado na execução.

```
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}\" }"
```

- **Exemplo 7: Obter o valor máximo agrupado pelo caminho da métrica dos dados de métrica de todas as métricas Average (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 \" }"
```

Resultado:

```
{"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]
```

- **Exemplo 8: Obter a utilização média de CPU para agentes**

```
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\" }"
```

Resultado:

```
{"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]

]}
```

- Exemplo 9: **Obter a contagem máxima de métricas para coletores**

```
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\" }"
```

Resultado:

```
{"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 do Team Center

Use a API REST do Team Center para fornecer várias funcionalidades no nível do painel do Team Center e de consulta de dados de métricas.Assim como outras APIs REST do APM, a interface da API REST do Team Center usa a autenticação com base em token. Para obter mais informações sobre como obter o token, consulte Gerar token de segurança.

A API REST do Team Center contém os seguintes recursos:

Recurso	Descrição	Exemplo
/atc/private/apmData/query	Obtém os dados da métrica usando a consulta de sintaxe padrão do SQL na carga.	POST /atc/private/apmData/query

Recurso	Descrição	Exemplo
/atc/private/apmData/schema	Obtém os recursos de esquema do SQL (ou seja, tabelas suportadas, detalhes de colunas) que podem ser usados na consulta SQL REST.	GET /atc/private/apmData/schema

IMPORTANT
Use a API REST pública do SQL *somente* para extrair dados de métricas do APM. Para extrair dados de métricas do APM ou de outros produtos, use a API REST de consulta de métricas.

Recursos da API REST do Team Center

Você pode definir consultas usando as funções contagem, mínimo, máximo e média. As funções agregadas a seguir são suportadas apenas na coluna agg_value na tabela metric_data: sum; apm_average; apm_aggregate.

A função de agregação resulta no seguinte:

- a função de agregação sum fornece a soma dos valores da coluna agg_values
- apm_aggregate fornece a soma ou a média ponderada com base nas métricas consultadas
- apm_average fornece apenas a média ponderada

A API REST do Team Center contém os seguintes recursos:

Recurso 1:

```
/atc/private/apmData/query
```

Obtém os dados da métrica usando a consulta de sintaxe padrão do SQL na carga.

Exemplo: POST /atc/private/apmData/query

Carga:

```
{  "query": <SQLQuery(string)> //sql query string}// Example:{ "query": "select * from metric_data where ts >=
 1572518520000 and ts <= 1572518535000"}
```

Resposta:

```
{
    "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": [
        [
            "",
            "brtlvlts1719sl",
            "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
        ],
        [
            "",
            "brtlvlts1719sl",
            "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
        ]
         ]}
```

Recurso 2:

`/atc/private/apmData/schema`

Obtém os recursos de esquema do SQL (ou seja, tabelas suportadas, detalhes de colunas) que podem ser usados na consulta SQL REST.

Exemplo: GET /atc/private/apmData/schema

Resposta:

```
{
    "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 consulta de métricas

A API REST de consulta de métricas usa a API de consulta de métrica para consultar as métricas de diferentes intervalos de datas, frequências e métricas.Assim como outras APIs REST do APM, a interface da API REST de consulta de métricas usa a autenticação com base em token. Para obter mais informações sobre como obter o token, consulte Gerar token de segurança.

A API contém os seguintes recursos:

Recurso	Descrição	Exemplo
/metrics/queryMetric	Execute uma consulta para obter as métricas e recupere os valores das métrica com base nos critérios de consulta e no intervalo de datas especificados. <QuerySpecifier> pode ser uma combinação de especificadores de consulta.	POST /metrics/queryMetric

IMPORTANT
Você pode usar a API REST de consulta de métricas para gerar dados de métrica do APM e de outros aplicativos. A API REST pública do SQL também pode ser usada para gerar os dados de métricas do APM. Para obter mais informações sobre a geração de dados de métrica do APM usando a API REST pública do SQL, consulte API REST do SQL.

Exemplo: POST /metrics/queryMetric

Carga:

```
{
  "querySpecifier": <QuerySpecifier>,
  "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:
{
  "querySpecifier": {
    "op": "SPEC",
    "sourceNameSpecifier": {
      "op": "EXACT",
      "names": [
        "SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent
 (Virtual)"
      ]
    },
    "attributeNameSpecifier": {
      "op": "REGEX",
      "pattern": "Enterprise Manager:.*"
    }
  },
  "queryRange": {
    "endTime": 1571823645,
    "rangeSize": 120,
    "frequency": 15
  },
  "clampSize": 100
}
```

Resposta:

```
{
  "metrics": [{
    "id": <MetricId(string)>,
    "source": <SourceName(string)>,
    "attribute": <AttributeName(string)>,
    "attributes": <Attributes_Optinal(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]]
            ]
        }
    ]
}
```

Agregações suportadas

A API oferece suporte aos seguintes especificadores agregados:

- MetricSpecifier direto
- MetricSpecifier de compartimento de memória

MetricSpecifier direto

TopK: obtenha os principais elementos com o pior desempenho, sendo que esses elementos no APM seriam, por exemplo, URLs, back-ends, front-ends e assim por diante.

Exemplos:

1. Obter os dois principais URLs com o pior desempenho
2. Obter as duas JVMs que consomem mais memória

Exemplo: POST /metrics/queryMetric

Carga: os dois principais URLs com o pior desempenho de acordo com o Tempo médio de resposta (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
            }
        }
    ]
}
```

Resposta:


```
{
  "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: obtenha os últimos elementos com o pior desempenho, sendo que esses elementos no APM seriam, por exemplo, URLs, back-ends, front-ends e assim por diante.

Carga: os dois últimos URLs com o pior desempenho de acordo com o Tempo médio de resposta (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": "BOTTOMK",
                "limit": "10",
                "includeAggregateTimeSeries": true
            }
        }
    ]
}
```

Resposta:

```
{
  "aggregations": {
  "BOTTOMK": [
  {
  "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
          ]
        ]
      }
    ]
  }
}
```


MetricSpecifier de compartimento de memória

Agrupe X em Y e obtenha os principais N de Y. Por exemplo: obtenha as 10 principais JVMs que atendem o máximo de solicitações, sendo que o máximo de solicitações é a soma das respostas de todos os pontos de entrada.

Exemplo: POST /metrics/queryMetric

Carga: as 2 principais JVMs de acordo com o número de solicitações atendidas (agrupe os front-ends nas JVMs e obtenha os 10 principais das JVMs)

```
{
  "querySpecifier": {
  "op": "SPEC",
  "sourceNameSpecifier": {
  "op": "ALL"
  },
    "attributeNameSpecifier": {
      "op": "AND",
      "specifiers": [
        {
          "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
            }
        }
    ]
}
```

Valores suportados para a operação de compartimento de memória:

Operação (OP)	Valor
BUCKET_ATTRIBUTE	<Nome_do_atributo_personalizado>
BUCKET_SOURCE	• hostname • domínio • Processo • agente
BUCKET_ATTRIBUTE_NAME	• metricpath • metricname

Resposta:

```
{
  "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
          ]
        ]
      }
    ]
  }
}
```


Usar URLs públicos abreviados no DX APM

O DX APM fornece URLs públicos abreviados para evitar o corte de URLs longos e para facilidade de uso. É possível usar esses URLs para conduzir os usuários diretamente a layouts pré-configurados no DX APM. Você pode fornecer URLs abreviados aos usuários para a exibição de métricas e mapas.Além disso, também é possível usar URLs públicos abreviados em alertas e notificações por email.

NOTE

Os usuários não podem acessar esses links sem um nome de usuário e senha do DX APM.

Os parâmetros de URL completo podem mudar com o tempo. É possível usar os seguintes parâmetros para mapear seus URLs públicos.

Para obter informações sobre os parâmetros para as APIs, consulte Referência a APIs.

Roteamentos

A tabela a seguir mostra como o roteamento público é mapeado para o roteamento interno.

Roteamento público	DX APMRoteamento interno do
/public/vertex	/map
/public/alerts	/alert
/public/metrics	/metrics

Parâmetros

Use os seguintes parâmetros públicos para atribuir valores específicos.

Roteamento	Parâmetro público	Obrigatório	Valor	Valor padrão
/public/vertex	id	Sim	ID do vértice	

	endTime	Não	Hora de término em milissegundos	modo dinâmico, se endTime não estiver especificado
	faixa	Não	Intervalo em milissegundos	480000
	layer	Não	[ATC | APM_INFRASTRUCTURE]	ATC
/public/alerts	name	Sim	<<nome do domínio>>:<<módulo de gerenciamento>>:<<nome do alerta>>	
/public/metrics	items	Sim	Uma série de vírgulas delimita os caminhos de métricas	
	endTime	Não	Hora de término em milissegundos	
	faixa	Não	Intervalo em milissegundos	480000

Exemplos

Os exemplos abaixo mostram como mapear os URLs abreviados.

```
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
```

Suporte internacional

Um produto internacionalizado é um produto em inglês que funciona corretamente em versões de idiomas locais do sistema operacional e de produtos de terceiros necessários. Um produto internacionalizado também oferece suporte a dados no idioma local para a entrada e a saída. Produtos internacionalizados também oferecem suporte à possibilidade de especificar convenções no idioma local para data, hora, moeda e formatos de número.

Um produto traduzido é um produto internacionalizado que inclui suporte ao idioma local para a interface de usuário do produto, ajuda online e outras documentações.Um produto traduzido também inclui as configurações padrão no idioma local para data, hora, moeda e formatos de número.Às vezes, um produto traduzido é chamado de produto localizado.

O DX Application Performance Management oferece suporte às opções internacionais a seguir. O produto está totalmente localizado e oferece suporte a configurações regionais de data, hora e formatação de números. A interface do usuário está disponível nos seguintes idiomas:

- Inglês
- Francês
- Português (Brasil)
- Espanhol

A documentação do produto está disponível nos seguintes idiomas:

- Inglês
- Francês
- Português (Brasil)
- Espanhol

Recursos de acessibilidade do produto

Estamos comprometidos em garantir que todos os clientes, independentemente de sua habilidade, possam usar com sucesso nossos produtos e a documentação de suporte para realizar tarefas vitais aos negócios.Esta seção descreve os recursos de acessibilidade do DX Application Performance Management.

Melhorias do produto

O DX APM oferece melhorias de acessibilidade nas seguintes áreas:

- Exibição
- Som
- Teclado
- Mouse

As seguintes informações se aplicam a aplicativos com base em Windows e Macintosh. Os aplicativos Java são executados em vários sistemas operacionais do host, alguns dos quais já têm tecnologias adaptativas disponíveis. Essas tecnologias adaptativas existentes precisam de duas funcionalidades relacionadas à JVM para fornecer acesso a programas escritos em JPL. As tecnologias adaptativas precisam do suporte à acessibilidade do Java, que está disponível na JVM.As tecnologias adaptativas também precisam de uma ponte entre si em seus ambientes nativos. A ponte tem uma ponta na JVM e outra na plataforma nativa. Portanto, a ponte é um pouco diferente para cada plataforma conectada à JVM. A Sun está desenvolvendo os dois lados dessa ponte, JPL e Win32.

Exibição

Para aumentar a visibilidade na tela do computador, é possível ajustar as seguintes opções:

- **Estilo da fonte, cor e tamanho dos itens**

Define a cor e o tamanho da fonte, além de outras combinações visuais.

- **Resolução da tela**

Define a contagem de pixels para ampliar objetos na tela.

- **Largura e taxa de intermitência do cursor**

Define a largura e a taxa de intermitência do cursor para facilitar a localização do cursor ou minimizar sua intermitência.

- **Tamanho dos ícones**

Define o tamanho dos ícones. É possível aumentar os ícones para maior visibilidade, ou diminuí-los para aumentar o espaço na tela.

- **Esquemas de alto contraste**

Define as combinações de cores. É possível selecionar as cores que são mais fáceis de visualizar.

Som

Para usar o som como uma alternativa visual ou para tornar os sons do computador mais fáceis de ouvir ou distinguir, ajuste as seguintes opções:

- **Volume**

Define o volume do computador.

- **Conversão de texto em fala**

Define as opções do computador para ouvir comandos e ler texto em voz alta.

- **Avisos**

Define os avisos visuais.

- **Notificações**

Define as indicações visuais ou de áudio quando os recursos de acessibilidade estão ativados ou desativados.

- **Esquemas**

Associa sons do computador a eventos específicos do sistema.

- **Legendas**

Permite exibir legendas para fala e sons.

Teclado

É possível fazer os seguintes ajustes no teclado:

- **Taxa de repetição**

Define a velocidade com que um caractere se repete quando a tecla é pressionada.

- **Tons**

Define a tons ao pressionar certas teclas.

- **Teclas de aderência**

Define a tela modificadora, como as teclas Shift, Ctrl e Alt ou a tecla com o logotipo Windows, para fazer combinações de teclas de atalho. As teclas de aderência permanecem ativas até que outra tecla seja pressionada.

Mouse

É possível usar as seguintes opções para tornar o mouse mais rápido e fácil de usar:

- **Velocidade do clique**

Define a velocidade do clique do botão do mouse para fazer uma seleção.

- **Bloqueio de clique**

Configura o mouse para realçar ou arrastar itens sem pressionar o botão.

- **Ação inversa**

Define a função inversa que é controlada pelos botões esquerdo e direito do mouse.

- **Taxa de intermitência**

Define a velocidade de intermitência do cursor.

- **Opções do ponteiro**

Permitem definir os comportamentos a seguir:

- – Ocultar o ponteiro enquanto digita
  – Mostrar o local do ponteiro
  – Definir a velocidade com que o ponteiro se move na tela
  – Selecionar o tamanho e a cor do ponteiro para maior visibilidade
  – Mover o ponteiro para um local padrão em uma caixa de diálogo

Atalhos de teclado

O DX APM oferece suporte a esses atalhos de teclado:

- **Ctrl+X** - Recortar
- **Ctrl+C** - Copiar
- **Ctrl+K** - Localizar próximo
- **Ctrl+F** - Localizar e substituir
- **Ctrl+V** - Colar
- **Ctrl+S** - Salvar
- **Ctrl+Shift+S** - Salvar tudo
- **Ctrl+D** - Excluir linha
- **Ctrl+Right** - Próxima palavra
- **Ctrl+Down** - Rolar para a linha de baixo
- **End** - Fim da linha

Atalhos de teclado para os vídeos do produto

A documentação do DX APM inclui tutoriais em vídeo do produto hospedados no YouTube. Ao assistir a esses vídeos do produto, você poderá usar os seguintes atalhos de teclado:

- **Tab** - Rolar para frente nas funções
- **Tab+Shift** - Rolar para trás
- **Enter** - Seleciona a função que está realçada em uma lista
- **Seta para frente** e **seta para trás** - Controlam o volume do vídeo

Dados de uso (Telemetria)

Telemetria é um elemento fundamental do modelo PLA (Portfolio License Agreement - Contrato de Licença de Portfólio) de software corporativo. O requisito inicial do esforço de telemetria é coletar e relatar o uso diário específico do produto para oferecer suporte ao novo modelo de consumo. Se a sua organização for uma cliente da Broadcom sob o PLA de software corporativo, você deverá ativar a telemetria e compartilhar os dados de uso. Este artigo descreve como ativar a telemetria e rotear os dados de uso para o Portal de relatórios de uso. Para obter mais informações, consulte a seção Portal de relatórios de uso.

- Dados coletados por telemetria
- Frequência da coleta de dados
- Configurações do usuário em IntroscopeEnterpriseManager.properties
- Configuração do proxy HTTP
- Como as métricas de licença são calculadas
- Como relatar dados de uso automaticamente
- Como relatar dados de uso manualmente

Dados coletados por telemetria

A telemetria coleta dois tipos de detalhe para cada cliente PLA:

- **Dados do cliente:** esses dados identificam o cliente e o site do cliente por meio da ID do site. Os dados também incluem uma ID de cobrança opcional para identificar a divisão ou o grupo a ser cobrado pela utilização.
- **Dados de uso:** os dados reais de uso com base no consumo são coletados. Você deve ativar o upload dos dados de uso. Para obter mais informações sobre os dados de uso que são coletados, consulte a respectiva documentação do produto.

> **NOTE**
> A telemetria não coleta PII (Personally Identifiable Information - Informações que Identificam Pessoalmente) nem informações confidenciais. Para obter mais informações sobre como as informações são coletadas e usadas, leia nossa declaração de privacidade.

Frequência da coleta de dados

Por padrão, a telemetria coleta e armazena os dados diariamente às 00:00. Se o agendador não estiver ativo às 00:00, os dados serão coletados somente na execução do dia seguinte. Os dados são coletados somente uma vez por dia.

Configurações do usuário em IntroscopeEnterpriseManager.properties

Para fazer upload dos dados, o usuário precisa configurar as propriedades a seguir no arquivo `IntroscopeEnterpriseManager.properties` e, em seguida, definir o valor de `introscope.platelemetry.upload.enabled` (configurável dinamicamente) como true. As propriedades a seguir estão disponíveis para configuração.

Nome da propriedade	Descrição
`introscope.platelemetry.instance.id`	ID gerada internamente para cada instância do produto
`introscope.platelemetry.customer.domain.name`	O nome de domínio do cliente (não um endereço de email)
`introscope.platelemetry.customer.site.id`	A ID do site do cliente
`introscope.platelemetry.customer.provisioned`	Sinalizador para determinar se uma instalação ou atualização está relacionada ao uso incremental como resultado do PLA (padrão: false)

Nome da propriedade	Descrição
`introscope.platelemetry.customer.company.id`	Opcional. Usado para identificar a divisão ou o grupo para se referir ao uso de consumo para relatar à empresa broadcom.com.

Configuração do proxy HTTP

Para obter uma descrição das propriedades padrão do EM para um proxy HTTP, como `transport.http.proxy.host` , `transport.http.proxy.port` , `transport.http.proxy.username` , `transport.http.proxy.password` (valor criptografado), consulte Configurar a estação de trabalho.

Dados coletados

Os seguintes dados são coletados para o DX Application Performance Management:

- Dispositivos

As seguintes tabelas exibem as atividades de telemetria:

Table 3: Atividades de telemetria

Propriedades da atividade de telemetria	Descrição
domain_name	nome do domínio (por exemplo, href="http://customer.com/">customer.com, bank.eu).
site_id	SiteID da empresa que o cliente usa para acessar o site de suporte. Para obter o SiteID no portal de suporte, vá para Minha conta, Perfil, Suporte da CA (guia), Login Site ID.
pla_agreement	Valor booleano em formato numérico (1 == true, 0 == false). Esse valor indica se o cliente está participando do contrato de licença de portfólio da assinatura.
chargeback_id	Valor fornecido pelo cliente para o grupo de identidades ou a área de encargos para seu uso interno, como faturamento para grupos.
product_sku	O valor de SKU específico do produto é fornecido à biblioteca subjacente pelo produto no momento da inicialização.
sku_description	A descrição de SKU do produto é fornecida à biblioteca subjacente pelo produto no momento da inicialização.
product_version	Versão do produto
instance_id	UUID gerado pelo produto na primeira instalação. Várias instalações exigem que os produtos gerem um novo valor de ID de instância a cada vez.
multiple telemetry metrics key_name	Todos os pares de chave/valor contêm um prefixo de namespace para torná-los exclusivos em comparação com os valores acima. A telemetria deve ser o prefixo dessa propriedade. Os pares de chave/valor são adicionados à atividade. Esses pares de chave/valor contêm métricas de uso específicas do produto.
date_collected	A data em que os dados de telemetria foram coletados. O formato de data é 'AAAA-MM-DD' (por exemplo, '2018-02-20')

Variáveis de ambiente

A seguinte tabela lista as variáveis com valores de exemplo que são usadas para telemetria:

Variável	Descrição
APMMANAGER_TELEMETRY_ENVTYPE=onprem	Essa variável é para o tipo de instalação.
APMMANAGER_TELEMETRY_CUSTOMERINFOPROPERTIESFILEPATH=<path to/customer/info/file>	Você informa a localização do arquivo de propriedades das informações do cliente.
APMMANAGER_TELEMETRY_UPLOADENABLED=false	Essa variável é usada para fazer upload dos dados de telemetria.

Como as métricas de licença são calculadas

As métricas do DX Application Performance Management são calculadas para cada agente de aplicativos da seguinte forma:

Aplicativos	Mapeamento
Java	Cada instância em execução de uma JVM (máquina virtual Java) monitorada consome 4 dispositivos.
.NET e .NET CorePS	Cada instância do sistema operacional que executa um aplicativo .NET monitorado ou CLR (Common Language Runtime) consome 4 dispositivos.
PHP	Cada instância em execução do agente do probe PHP consome 2 dispositivos.
Nodejs	Cada processo monitorado do NodeJS consome 0.4 dispositivos.
Python	Cada instância do sistema operacional que executa um aplicativo monitorado do Python consome 4 dispositivos.

Como relatar dados de uso automaticamente

Após instalação bem-sucedida, configure para enviar os dados de telemetria a Broadcom.com.

Siga estas etapas:

1. Copie o conteúdo do arquivo **opt/dxplatelemetry/configcommon/esdplatelemetry_onpreminfo.properties.template** no arquivo **opt/dxplatelemetry/configcommon/esdplatelemetry_onpreminfo.properties**.
2. Edite o arquivo opt/dxplatelemetry/configcommon/esdplatelemetry_onpreminfo.properties e preencha as seguintes chaves com as informações corretas:
   – **dxitenantid:** insira a ID do inquilino para armazenar os dados de telemetria PLA no NASS.

     NOTE

     - Digite a ID do inquilino, e não a ID do coorte.
     - dxitenantid diferencia maiúsculas de minúsculas.

   – **perform_upload:** determina se os cálculos da telemetria PLA serão enviados a Broadcom.com. Digite True para fazer upload dos cálculos de telemetria. Valores: true/false
3. Reinicie o pod PLA Telemetry para concluir a configuração.

Como relatar dados de uso manualmente

Você pode relatar o uso da telemetria manualmente seguindo essas etapas. Você somente deverá relatar o uso manualmente se for um cliente de PLA e se houver um motivo válido para que não seja possível configurar a telemetria para relatar uso automaticamente.

Você pode configurar isso como parte das etapas posteriores à instalação. Para obter as etapas completas, consulte Preencher as informações e configurar a telemetria. Também pode ser necessário configurar o uso da telemetria usando a API do Coletor de Utilização do Produto. Para obter mais informações sobre esse uso dessa API, consulte Coletor de Utilização do Produto.

Aviso legal da documentação

A presente documentação, que inclui os sistemas de ajuda incorporados e os materiais distribuídos eletronicamente (doravante denominados "Documentação"), destina-se apenas a fins informativos e está sujeita a alterações ou remoção por parte da Broadcom a qualquer momento. Esta Documentação contém informações proprietárias da Broadcom e não pode ser copiada, transferida, reproduzida, divulgada, modificada nem duplicada, parcial ou completamente, sem o prévio consentimento por escrito da Broadcom.

Se o Cliente for um usuário licenciado do(s) produto(s) de software referido(s) na Documentação, é permitido que ele imprima ou, de outro modo, disponibilize uma quantidade razoável de cópias da Documentação para uso interno seu e de seus funcionários envolvidos com o software em questão, contanto que todos os avisos de direitos autorais e legendas da Broadcom estejam presentes em cada cópia reproduzida.

O direito à impressão ou, de outro modo, à disponibilidade de cópias da Documentação está limitado ao período em que a licença aplicável ao referido software permanecer em pleno vigor e efeito. Em caso de término da licença, por qualquer motivo, fica o usuário responsável por garantir à Broadcom, por escrito, que todas as cópias, parciais ou integrais, da Documentação sejam devolvidas à Broadcom ou destruídas.

NA MEDIDA EM QUE PERMITIDO PELA LEI APLICÁVEL, A BROADCOM FORNECE ESTA DOCUMENTAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM NENHUM TIPO DE GARANTIA, INCLUINDO, ENTRE OUTRAS, QUAISQUER GARANTIAS IMPLÍCITAS DE COMERCIABILIDADE, ADEQUAÇÃO A UM DETERMINADO FIM OU NÃO VIOLAÇÃO. EM NENHUMA OCASIÃO, A BROADCOM SERÁ RESPONSÁVEL PERANTE O USUÁRIO OU TERCEIROS POR QUAISQUER PERDAS OU DANOS, DIRETOS OU INDIRETOS, RESULTANTES DO USO DA DOCUMENTAÇÃO, INCLUINDO, ENTRE OUTROS, LUCROS CESSANTES, PERDA DE INVESTIMENTO, INTERRUPÇÃO DOS NEGÓCIOS, FUNDO DE COMÉRCIO OU PERDA DE DADOS, MESMO QUE A BROADCOM TENHA SIDO EXPRESSAMENTE ADVERTIDA SOBRE A POSSIBILIDADE DE TAIS PERDAS E DANOS.

O uso de qualquer produto de software mencionado na Documentação é regido pelo contrato de licença aplicável, sendo que tal contrato de licença não é modificado de nenhum modo pelos termos deste aviso.

O fabricante desta Documentação é a Broadcom Inc.

Fornecida com "Direitos Restritos". O uso, a duplicação ou a divulgação pelo governo dos Estados Unidos estão sujeitos às restrições estabelecidas pelas regulamentações FAR, seções 12.212, 52.227-14 e 52.227-19(c)(1) - (2), e DFARS, seção 252.227-7014(b)(3), conforme aplicável, ou sucessoras.

Copyright © 2005-2024 Broadcom. Todos os direitos reservados. O termo "Broadcom" refere-se à Broadcom Inc. e/ou suas subsidiárias. Todas as marcas comerciais, os nomes de marcas, as marcas de serviço e os logotipos aqui mencionados pertencem a suas respectivas empresas.

BROADCOM®
SOFTWARE