



DX APM - SaaS - Spanish - Spain

Table of Contents

Requisitos de red de DX SaaS.....	8
Novedades de DX APM.....	9
24.9.1.....	9
24.4.1.....	9
24.3.2.....	10
23.12.1.....	10
2023.9.1.....	11
2023.7.1.....	12
2023.5.1.....	13
23.1.....	14
22.8.....	16
22.6.....	16
22.3.....	17
22.1.....	20
Notas de la versión de 2021.....	24
21.11.....	24
21.6.....	32
21.4.....	36
21.1.....	40
Notas de la versión de 2020.....	43
20.11.....	43
20.9.....	49
20.6.....	53
20.4.....	57
20.1.....	64
Notas de la versión de 2019.....	69
Noviembre de 2019.....	69
Octubre de 2019.....	71
Agosto de 2019.....	71
Procedimientos iniciales.....	73
Soporte y compatibilidad.....	73
Arquitectura de DX APM.....	73
Recursos de vídeo de DX APM.....	74
Convenciones de nombre de archivo y directorio.....	76
Personalizaciones.....	77
Artículos de la base de conocimiento.....	77

Glosario.....	80
Reconocimientos de software de terceros para SaaS.....	101
Implementación de los agentes.....	102
Configuración del entorno de monitorización.....	103
Roles y privilegios admitidos.....	104
Generación de un token de seguridad.....	108
Creación de notificaciones de alerta.....	109
Configuración de notificaciones de correo electrónico para las alertas.....	113
Configuración de universos.....	114
Configuración de la Vista de experiencia.....	118
Cómo adaptar la monitorización de su entorno con reglas de atributo.....	123
Importación de reglas de atributos en bloque.....	127
Ajuste de la monitorización con alertas.....	129
Gestión de datos de métricas mediante módulos de gestión.....	133
Creación y trabajo con módulos de gestión.....	134
Configuración de agrupaciones de métrica en Team Center.....	139
Creación y configuración de alertas sencillas en Team Center.....	146
Creación y configuración de alertas de resumen.....	153
Creación y edición de calculadoras.....	156
Configuración del Análisis diferencial.....	160
Configuración de extensiones de JavaScript.....	162
Recomendaciones de tamaño para el Monitor de Docker.....	172
Descarga de herramientas adicionales.....	172
Herramienta de importación de agentes.....	173
Conexión con Workstation.....	175
Cloud Proxy.....	178
Métricas de compatibilidad de Cloud Proxy.....	188
Configuración de Workstation.....	191
Reglas de supresión de seguimiento para ocultar datos confidenciales.....	193
Configuración de APM Command Center.....	194
Visualización del estado del agente.....	194
Visualización de los informes del agente.....	196
Configuración de aplicaciones para la incorporación.....	197
Gestión de paquetes del agente.....	198
Configuración de conjuntos.....	200
Búsqueda utilizando el lenguaje de consulta de ACC (AQL).....	201
Uso.....	204
Incorporación de aplicaciones para la monitorización.....	205
Monitorización del rendimiento utilizando la Vista de experiencia.....	207

Investigación de problemas mediante el Bloc de notas de análisis.....	212
Visualización del estado del agente y gestión de las tarjetas de agente.....	217
Monitorización de los valores de métrica del agente con la Vista de métrica.....	220
Incrustación de cuadros de mandos de DX en la Vista de métricas.....	225
Uso de la escala de tiempo y del resaltado.....	228
Uso de la escala de tiempo y visualización de eventos de cambio.....	229
Utilización de atributos en DX APM.....	233
Organización de los componentes utilizando perspectivas.....	235
Visualización de las relaciones de los componentes en el mapa.....	238
Capas del mapa.....	242
Identificación de las áreas de interés mediante filtros.....	246
Monitorización del estado general del entorno con el cuadro de mandos.....	248
Monitorización de los problemas y las anomalías de la Evaluación de errores asistida.....	251
Evaluación de errores asistida y analistas.....	252
Investigación del rendimiento de las transacciones con errores.....	257
Utilización del seguimiento de la transacción entre procesos para solucionar problemas.....	259
Inicio de una nueva sesión de seguimiento de la transacción.....	261
Examen de los componentes individuales y de los datos de seguimiento.....	262
Diagnóstico de problemas de carga del recurso.....	268
Diagnóstico de problemas de rendimiento del sistema.....	272
Detección y análisis de errores y detenciones.....	273
Análisis de las instantáneas de error y detenidas.....	277
Recopilación y análisis de los seguimientos de la transacción.....	281
Análisis de los seguimientos y colaboración en el análisis de problemas.....	294
Monitorización de los eventos y del rendimiento del explorador.....	294
Acceso y presentación de la estación de trabajo.....	303
Descripción general de Workstation.....	305
Evaluación de errores con Workstation.....	309
Ficha Explorador de métrica.....	312
Uso de Transaction Tracer.....	327
Monitorización con Workstation.....	346
Diagnóstico del problema con la ficha Explorador de métrica.....	346
Lectura y comprensión de las notificaciones.....	349
Comprensión del rendimiento nominal.....	349
Uso de Workstation.....	351
Navegación por los cuadros de mandos de la Consola.....	351
Datos históricos y en directo en la Consola de Workstation.....	357
Métricas de DX APM.....	360
Métricas de BlamePoint.....	363
Métricas de JMX.....	370

Métricas de la transacción.....	372
Sostenibilidad del agente.....	382
Métricas relacionadas con la memoria.....	387
Métricas de compatibilidad del clúster.....	392
Métricas de compatibilidad de la evaluación de errores asistida.....	401
Métricas de compatibilidad principales.....	402
Monitorización del rendimiento de CA APM utilizando métricas de compatibilidad.....	404
Istio Support.....	415
Cuadros de mandos de DX.....	428
Solución de problemas.....	430
Resolución de problemas del agente.....	430
El agente se inicia, pero no está visible.....	430
El agente no detecta automáticamente un back-end conocido.....	433
El agente que monitoriza un front-end no detecta automáticamente el back-end.....	433
Excepción ClassNotFoundException por parte del agente al cargar las extensiones dinámicas.....	434
El agente del explorador y los seguimientos de las transacciones del agente .NET no están correlacionados.....	434
El valor de la dirección URL ConfigurationServer no se puede rellenar.....	434
¿Se está decorando el encabezado de la cookie de respuesta del agente del explorador para .NET?.....	435
Bloqueos del agente de Java.....	435
Error de desbordamiento de la pila del agente de Java.....	436
Error de visualización de las métricas de .NET tras la activación de la inserción automática de fragmentos de código del Agente del explorador para .NET.....	437
Ninguna detección automática del back-end debido a un error inesperado al cargar la extensión.....	437
Pico en los recuentos de la métrica.....	437
No se puede instrumentar una aplicación con DX APM.....	438
La agrupación de direcciones URL no funciona.....	438
Cloud Foundry Java Buildpack no puede encontrar la versión solicitada del Agente de Java.....	438
Solución de problemas del cuadro de diálogo de descarga del agente.....	439
Solución de problemas de DX APM.....	440
No se muestra la métrica del componente.....	440
La variación del análisis diferencial no aparece en los nodos.....	440
No hay datos de métrica en la Vista de la experiencia.....	440
Datos enviados por los agentes incompletos o ausentes en el mapa.....	441
Error de visualización de la información del agente en el mapa.....	442
El mapa muestra solo 50.000 nodos.....	442
El selector de atributos de la tarjeta de experiencia no muestra los atributos relacionados con Docker.....	442
La propagación de atributos entre capas no funciona.....	443
Dónde buscar las incidencias potenciales relacionadas con las asignaciones.....	443
Solución de problemas de las transacciones.....	443
Un método que nunca se cierra se identifica como método padre.....	443

Solución de problemas de Workstation.....	444
Se ha producido un error en Workstation al recopilar un volcado de subprocesos nuevo.....	444
Cambios del tipo de operación en las calculadoras del módulo de gestión.....	445
Los cuadros de mandos tienen paneles vacíos.....	445
No hay resultados para la consulta de eventos históricos.....	445
Solución de los problemas del tiempo de espera automático de la sesión en Workstation.....	446
El tiempo de espera de Workstation se agota al iniciar sesión en Enterprise Manager.....	446
Referencia de API.....	447
API de APM Command Center.....	447
Mensajes de error de API.....	452
Recurso del agente.....	454
Recurso agentUpdateTask.....	457
Recurso diagnosticReport.....	458
Recurso diagnosticReportTask.....	459
Recurso del controlador.....	460
Mensajes de error.....	462
Propiedades que permiten la búsqueda.....	467
Búsqueda mediante el lenguaje de consulta de Command Center.....	469
Recurso agentFileOperationTask.....	474
Recurso de archivo.....	475
Recurso del paquete.....	476
Recurso bundle.....	478
Recurso agentPackageTask.....	479
API de hipermedia de DX APM.....	480
Autorización y autenticación de la API.....	482
Acceso a los recursos.....	482
Búsqueda y filtrado de recursos.....	487
Creación y actualización de recursos.....	491
Encabezados HTTP comunes.....	492
Mensajes y códigos de error.....	493
La API de REST de DX APM.....	495
API de la aplicación.....	499
Regla de atributo.....	503
Gráfica.....	507
Vértice del gráfico.....	510
Gráfico incremental.....	516
Id del vértice del gráfico.....	519
Gráfico Vertexstatus incremental.....	520
Recurso raíz.....	522
Universo.....	523

Vértice.....	525
ID del vértice.....	528
Ejemplo de Java de la API de REST para obtener actualizaciones incrementales.....	529
API de REST de SQL.....	537
API de REST de Team Center.....	555
API de REST de consulta de métrica.....	567
Uso de direcciones URL públicas cortas en DX APM.....	581
Compatibilidad internacional.....	583
Funciones de accesibilidad del producto.....	584
Datos de uso (telemetría).....	587
Aviso Legal de Documentación.....	591

Requisitos de red de DX SaaS

La infraestructura de DX SaaS se ha actualizado para aumentar la confiabilidad con el tiempo de inactividad mínimo para las ventanas de mantenimiento. Esta optimización requiere que se implementen las actualizaciones de la configuración de red obligatorias en las políticas de firewall para evitar cualquier interrupción de seguridad relacionada con la red. Se verá afectada tanto la comunicación entrante (por ejemplo, webhook) como la saliente (por ejemplo, agentes, registros, alarmas, RESTMon). Las direcciones IP del nuevo hardware se deben permitir en la implementación cuando se activa el nuevo hardware. Si no se permite la comunicación con las nuevas direcciones IP, la capacidad de ingesta de datos de monitorización se puede ver afectada y, dada la naturaleza de algunas tecnologías de monitorización, esto puede afectar al rendimiento del sistema monitorizado.

Póngase en contacto con el administrador de redes para asegurarse de que se permiten las siguientes direcciones IP para los centros de datos respectivos que se están utilizando actualmente:

NOTE

Las direcciones IP existentes deben seguir estando permitidas simultáneamente hasta nuevo aviso que indique que esas direcciones ya no están en uso.

Centro de datos de EE. UU. (<https://axa.dxi-na1.saas.broadcom.com>)

- Entrante:
 - 34.145.151.0/24
- Saliente:
 - 34.96.90.96/28
 - 34.150.194.136/29

Centro de datos de Europa (<https://axa.dxi-eu1.saas.broadcom.com>)

- Entrante:
 - 34.141.238.0/24
- Saliente:
 - 34.117.194.112/28
 - 34.141.162.16/29

Novedades de DX APM

Obtenga información acerca de las nuevas funciones, mejoras, problemas conocidos y correcciones de defectos relacionados con cada versión de DX APM.

- [24.9.1](#)
- [24.4.1](#)
- [24.3.2](#)
- [23.12.1](#)
- [2023.9.1](#)
- [2023.7.1](#)
- [2023.5.1](#)
- [23.1](#)
- [22.8](#)
- [22.6](#)
- [22.3](#)
- [22.1](#)
- [Notas de la versión de 2021](#)
- [Notas de la versión de 2020](#)
- [Notas de la versión de 2019](#)

24.9.1

A continuación se muestra la nueva función y mejora de DX APM.

Ventana de mantenimiento en la interfaz de usuario de APM

Si una página está en mantenimiento, se muestra el icono Mantenimiento. El icono Mantenimiento estará visible durante un período máximo de 7 días de antelación para cualquier mantenimiento próximo. Para obtener más información, consulte [Gestión de datos de métricas mediante módulos de gestión](#).

24.4.1

Esta versión solo trata los defectos del cliente junto con varios defectos internos.

NOTE

Dado que se trata de una versión de parche, la interfaz de usuario del producto seguirá reflejando la versión de lanzamiento como 24.3.2.

A continuación se muestra la lista de defectos del cliente que se han corregido:

Defecto	Descripción
DE593238	El Agente de Windows de APMIA está conectado y las métricas aparecen en APM, pero el valor de la métrica <code>ConnectionState</code> es 5.
DE597525	Gráfico de vista previa de alertas: cuando el usuario hace clic en el botón X de la opción Última hora y la opción Últimos 8 minutos da un mensaje de error en la interfaz de usuario.

24.3.2

A continuación, se muestran las nuevas funciones y mejoras de DX APM.

- [Calculadora de conectividad del agente](#)
- [Resumen de recuentos del agente](#)
- [Interfaz de usuario mejorada del módulo de gestión](#)
- [Creación de una copia del módulo de gestión](#)
- [Inicio de una sesión de seguimiento de transacciones en la Vista de métricas](#)
- [API de la aplicación para la incorporación de aplicaciones](#)

Calculadora de conectividad del agente

La calculadora de conectividad del agente copia el estado de conectividad del agente en una ubicación fija. Está desactivada de forma predeterminada y la debe activar el administrador. Para obtener más información, consulte [Calculadora de conectividad del agente](#).

Resumen de recuentos del agente

La calculadora también genera un pequeño resumen de los recuentos de agentes para cada ConnectionState en Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Agents|Agent States. Para obtener más información, consulte [Calculadora de conectividad del agente](#).

Interfaz de usuario mejorada del módulo de gestión

Ahora se puede actualizar el módulo de gestión con una interfaz de usuario mejorada. Para obtener más información, consulte [Actualización de un módulo de gestión](#).

Creación de una copia del módulo de gestión

Ahora se puede crear una copia de un módulo de gestión utilizando el botón Guardar como nuevo en la página Editar módulo de gestión. Para obtener más información, consulte [Copia de un módulo de gestión](#).

Inicio de una sesión de seguimiento de transacciones en la Vista de métricas

Ahora se puede iniciar una sesión de seguimiento de transacciones en la página Vista de métricas especificando los valores en el cuadro de diálogo Sesión de seguimiento de transacciones. Para obtener más información, consulte [Inicio de una sesión de seguimiento de transacciones](#).

API de la aplicación para la incorporación de aplicaciones

La API de la aplicación se documenta con OpenAPI versión 3. El documento de OpenAPI se puede descargar desde una instalación de APM. Se puede usar para generar clientes para varios idiomas o con algunos clientes HTTP/REST interactivos. Para obtener más información, consulte [API de la aplicación](#).

23.12.1

A continuación, se muestran las nuevas funciones y mejoras de DX APM.

Dirección URL directa a la vista del grupo de métricas

La página de detalles Alarmas de DX Operational Intelligence y el correo electrónico de notificación de alarmas ahora se configuran con el vínculo Vista de métrica de APM. Este vínculo proporcionará una vista completa del período de tiempo en el que se activó la alerta junto con el estado de otras alertas dentro del mismo grupo de métricas. También

mejorará la visibilidad y facilitará la investigación, ya que proporciona una comprensión más amplia del comportamiento de las métricas de contexto durante el período observado. Para obtener más información, consulte [Detalles de todas las alarmas](#).

Volcado de subprocesos en el Explorador de métrica

Si se selecciona un nodo de agente en el árbol del Explorador de métrica, ahora se muestra la ficha **Volcados de subprocesos**. Esta ficha permite recopilar volcados de subprocesos de Java (volcados de subprocesos) y mostrar los datos de los volcados de subprocesos actuales e históricos. Un volcado de subprocesos proporciona información acerca de todos los subprocesos que están en ejecución en una máquina virtual Java en un momento dado. Para obtener más información, consulte [Visualización de la métrica de un agente en la Vista de métrica global](#).

Limitación del tiempo de ejecución del script en calculadoras de JavaScript

Las calculadoras de JavaScript que procesan los datos de métricas entrantes pueden tardar tiempo y afectar al rendimiento de Enterprise Manager donde se ejecuta la extensión de Javascript. Para proteger contra la sobrecarga de Enterprise Manager, especifique el tiempo de espera del script en el origen de la extensión. Para obtener más información, consulte [Configuración de extensiones de JavaScript](#).

NOTE

Ahora se pueden eliminar las calculadoras de script de Java sin volver a iniciar Enterprise Manager. También se puede establecer el tiempo de espera para limitar el tiempo de ejecución de la calculadora de Javascript.

Subpropiedades para la incorporación de aplicaciones

Es posible ahora seleccionar **ADD PROFILE** y establecer varias configuraciones de la subpropiedad del agente. Por ejemplo, un agente puede monitorizar varias bases de datos de modo que se puedan agregar varios conjuntos de propiedades de conexión de la base de datos. Para obtener más información, consulte [Creación de aplicaciones](#).

Creación de variables en la configuración de la incrustación del cuadro de mandos

Ahora se pueden crear variables directamente en la configuración de la incrustación del cuadro de mandos. Para obtener más información, consulte [Incrustación de cuadros de mandos de DX en la Vista de métricas](#).

Métricas de compatibilidad de Cloud Proxy

Se agregan nuevas métricas de compatibilidad a Cloud Proxy. Se pueden utilizar estas métricas para identificar información más detallada sobre la conexión de Cloud Proxy como, por ejemplo, la conexión de red o el uso de la memoria, entre otros. Por ejemplo, se pueden usar para investigar cualquier problema de red.

Para obtener más ayuda, consulte [Métricas de compatibilidad de Cloud Proxy](#).

Nuevo estilo de la interfaz de usuario

La interfaz de usuario completa de APM SaaS se ha actualizado para utilizar el color, la fuente y el estilo de iconos utilizado por la plataforma DX principal. Los tamaños de fuente se han aumentado en algunas áreas, lo que puede reducir el espacio utilizable de la pantalla pero aumenta el contraste y la legibilidad en algunos monitores. Si se cambia el zoom del exploradora al 90 % se permitirá restaurar el espacio utilizable de la pantalla sin reducir la legibilidad en algunos monitores.

2023.9.1

A continuación, se muestran las nuevas funciones y mejoras de DX APM.

- [Exportación e importación de módulos de gestión](#)
- [Filtrado de referencia de objetos en los módulos de gestión](#)
- [ACC: Interfaz de usuario unificada](#)
- [Problemas conocidos](#)

Exportación e importación de módulos de gestión

Ahora es posible exportar los módulos de gestión con el formato de archivo .jar, así como importar un módulo de gestión existente como archivo .jar. Para obtener más información, consulte [Creación y trabajo con módulos de gestión](#).

Filtrado de referencia de objetos en los módulos de gestión

Ahora se puede hacer clic en el valor de cualquier objeto en la tabla Referencias de objetos de la página Módulo de gestión. Redirecciona a la vista filtrada de la referencia del objeto seleccionado y al módulo de gestión específico desde el que se ha hecho clic. Para obtener más información, consulte [Creación y trabajo con módulos de gestión](#).

ACC: Interfaz de usuario unificada

Se ha rediseñado la interfaz de usuario de ACC para unificarla con la interfaz de usuario de Application Performance Management.

Problemas conocidos

DE559435: La combinación de alertas como Todo no funciona correctamente

Síntoma: Cuando la combinación de alertas se establece en Todo y se configura el correo electrónico de alerta, en este caso, incluso cuando una métrica infringe el umbral de varias métricas configuradas, el estado de la alerta cambia a crítico y se envía el correo de alerta. Además, el estado de alerta cambia a normal y el correo electrónico se envía de nuevo.

2023.7.1

A continuación, se muestran las nuevas funciones y mejoras de DX APM.

- [Recuento de métricas en directo en el árbol de métrica](#)
- [Panel de ACC para ajustar el cambio de tamaño de la ventana del explorador](#)
- [Dirección URL directa al grupo de métricas de la alarma](#)
- [Creación de cuadros de mandos usando atributos capturados](#)
- [Universos de DX Operational Intelligence se completan con universos de APM](#)
- [Cuadros de mandos listos para su uso](#)
- [Optimización del rendimiento de la red y de la CPU en Cloud Proxy](#)

Recuento de métricas en directo en el árbol de métrica

Si se selecciona un agente o una subcarpeta en el árbol de métrica y se encuentran en el modo en directo, seleccione la casilla de verificación **Live Metric Only** (Solo métrica en directo) para ver el número de métricas en directo solamente, es decir, las métricas sobre las que está informando el agente ahora mismo. Para obtener más información, consulte [Visualización de la métrica de un agente en la Vista de métrica global](#).

Panel de ACC para ajustar el cambio de tamaño de la ventana del explorador

En ACC, ahora se puede ajustar el panel de la ventana para ver todas las configuraciones de los paquetes con muchas actualizaciones.

Dirección URL directa al grupo de métricas de la alarma

Los detalles de la alarma en DX Operational Intelligence proporcionan un archivo JSON sin formato en el campo Atributos de alarma desde el que se puede extraer el valor del vínculo Grupo de métricas en APM. Este vínculo apunta directamente al grupo de métricas configurado en APM que ha provocado la alarma o evento. Para obtener más información, consulte [Detalles de todas las alarmas](#).

Creación de cuadros de mandos usando atributos capturados

Ahora se pueden crear cuadros de mandos en cuadros de mandos de DX utilizando los atributos capturados del Analizador de la carga empresarial.

En los cuadros de mandos de DX, cree el cuadro de mandos utilizando la siguiente información:

- Fuente de datos: **AIOps_Metadata**
- Índice principal: **ao_aum_captured_data_2.0**
- Agrupar por: Introduzca el atributo capturado con el formato siguiente: **rr_data@<atributo_capturado>**

Para obtener más información, consulte la documentación de los [cuadros de mandos de DX](#).

Universos de DX Operational Intelligence se completan con universos de APM

La lista desplegable **Todos mis universos** ahora también rellena los universos de DX Operational Intelligence (a excepción del universo Todos los accesos). Estos universos se marcan con una etiqueta de OI con su nombre en la lista desplegable.

Cuadros de mandos listos para su uso

Esta versión incluye los siguientes cuadros de mandos de APM listos para su uso en los cuadros de mandos de DX. Estos cuadros de mandos están disponibles en la carpeta APM-MetricView.

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

Se deben ver estos cuadros de mandos en la Vista de métrica de APM. Vaya a la carpeta en el árbol y seleccione que se muestre el cuadro de mandos como una ficha. Haga clic en la ficha para ver los datos en el cuadro de mandos. Para obtener más información, consulte [APM-MetricView](#).

Optimización del rendimiento de la red y de la CPU en Cloud Proxy

Ahora se puede utilizar `apm.server.compressionLevel` en el archivo `application.yml` para configurar el nivel de compresión para la comunicación de WebSocket entre Cloud Proxy y Gateway. Para obtener más información, consulte [Cloud Proxy](#).

2023.5.1

A continuación, se muestran las nuevas funciones y mejoras de DX APM.

- [Mejoras en la incorporación de aplicaciones](#)
- [Mejoras o cambios en los cuadros de mandos incrustados](#)
- [Capacidad de búsqueda mejorada en el árbol de métrica](#)
- [Documentación de Cloud Proxy](#)
- [Defectos conocidos](#)

Mejoras en la incorporación de aplicaciones

Mientras se utiliza sin problemas la incorporación de aplicaciones para incorporar las aplicaciones en DX APM y para configurar los paquetes de agente, ahora se pueden configurar las opciones relacionadas con el sistema operativo seleccionado. Para obtener más información, consulte [Incorporación de aplicaciones para la monitorización](#).

Mejoras o cambios en los cuadros de mandos incrustados

A partir de esta versión, los siguientes cuadros de mandos de DX se incrustan listos para su uso:

- Cuadro de mandos de Blamepoint
- Cuadro de mandos de FrontendOverview

Estos cuadros de mandos se han configurado previamente. En la Vista de métricas, estos cuadros de mandos aparecen como fichas si se selecciona cualquier métrica que coincida con la condición.

Antes de esta versión, se debían importar e incrustar estos cuadros de mandos manualmente en la Vista de métricas. Para obtener más información, consulte [Incrustación de cuadros de mandos de DX en la Vista de métricas](#).

Capacidad de búsqueda mejorada en el árbol de métrica

Los usuarios ahora pueden marcar elementos como favoritos dentro del árbol. En el árbol de métrica se incorporará un botón llamado Solo mostrar favoritos. Este botón permite a los usuarios filtrar y mostrar solamente los objetos marcados como favoritos. Para obtener más información, consulte [Búsqueda de métricas en el Árbol de métrica](#).

Además, la barra de búsqueda detecta automáticamente cuando la entrada tiene el formato de expresión regular y realiza una búsqueda en consecuencia.

NOTE

La opción para utilizar expresiones regulares se ha eliminado.

Documentación de Cloud Proxy

La documentación de Cloud Proxy ahora está disponible en la documentación de APM SaaS. Consulte [Cloud Proxy](#).

La información de la versión de las mejoras anteriores de Cloud Proxy seguirá formando parte de la [Documentación de los Agentes de APM](#).

Defectos conocidos

A continuación se muestra el defecto conocido para esta versión:

DE559435: La combinación de alertas como Todo no funciona correctamente

Síntoma: Durante la configuración de las alertas, cuando se establece el valor **Combinación** como **Todo** y si solo un valor de métrica coincide con el límite del umbral, se crea una alerta y el estado de la alerta se convierte en Crítico y más tarde cambia a Normal. Debido a este comportamiento, si se configuran las notificaciones por correo electrónico, se envían varios correos electrónicos de alerta: primero para el estado de peligro o precaución y luego cuando el estado se pone verde.

23.1

Obtenga información acerca de las nuevas mejoras y funciones de DX APM.

- [Nuevas funciones](#)

- [Incorporación de agentes simplificada](#)
- [Especificador de métricas sin diferencia entre mayúsculas y minúsculas](#)
- [Supresión de los datos privados](#)
- [Compatibilidad eliminada para el idioma japonés](#)
- [Incrustación de cuadros de mandos de DX en la Vista de métricas](#)
- [Notificación desactivada por métrica individual y opciones de la notificación de la alerta de activación](#)

Nuevas funciones

Obtenga información acerca de las nuevas mejoras y funciones de DX APM SaaS.

Incorporación de agentes simplificada

Se puede utilizar la incorporación de aplicaciones para incorporar las aplicaciones en DX APM sin problemas y configurar fácilmente los paquetes de agente para el entorno. El asistente para la incorporación de aplicaciones le guía a través de la selección de las opciones de monitorización y crea nuevos paquetes de agente. La incorporación de aplicaciones contiene los conceptos siguientes:

- **Aplicación:** Permite monitorizar la aplicación, que consta de uno o más niveles.
- **Nivel:** Denota un nivel de aplicación determinado para monitorizarlo. El nivel hace referencia a uno o más paquetes de agente creados según la selección de un usuario.

NOTE

Todavía se puede utilizar ADD (cuadro de diálogo de descarga del agente) y ACC para agregar aplicaciones y configurar los paquetes del agente en el entorno.

Para obtener más información, consulte [Incorporación de aplicaciones para la monitorización](#).

Especificador de métricas sin diferencia entre mayúsculas y minúsculas

Ahora se puede especificar el valor del especificador de métrica de manera que no diferencia entre mayúsculas y minúsculas al especificar el valor del especificador de métrica entre (?i) y (?-i). Por ejemplo:

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

Consulte [Configuración de agrupaciones de métrica en Team Center](#).

Supresión de los datos privados

Ahora se pueden definir reglas de supresión de seguimiento para identificar los datos confidenciales de los usuarios y reemplazarlos por texto configurado previamente como, por ejemplo, "SUPPRESSED BY APM". Para obtener más información, consulte [Reglas de supresión de seguimiento para ocultar datos confidenciales](#).

Compatibilidad eliminada para el idioma japonés

La interfaz de usuario y la documentación de DX APM ya no se localizan en japonés. Consulte [Compatibilidad internacional](#).

Incrustación de cuadros de mandos de DX en la Vista de métricas

Ahora se pueden incrustar cuadros de mandos de DX en la Vista de métricas. Se puede incrustar lo siguiente:

- **Cuadros de mandos de métricas de front-end y Blamepoint:** Los cuadros de mandos de DX proporcionan archivos JSON para estos cuadros de mandos que se pueden importar. Después de importarlos, estarán disponibles en la Vista de métricas.
- **Cuadros de mandos de DX personalizados:** Cree un cuadro de mandos personalizado en los cuadros de mandos de DX y, a continuación, asigne el cuadro de mandos a través del mosaico **Cuadros de mandos de DX** en la página **Configuración** de DX APM. Una vez incrustado, el cuadro de mandos se muestra en la página Vista de métricas.

Para obtener más información, consulte [Incrustación de cuadros de mandos de DX en la Vista de métricas](#).

Notificación desactivada por métrica individual y opciones de la notificación de la alerta de activación

APM notifica cada cambio de estado de alerta al servicio de Alertas y, por lo tanto, los botones Notificar por métrica individual y Notificación de la alerta de activación son redundantes. Por lo tanto, las opciones Notificar por métrica individual y Notificación de la alerta de activación se eliminan de la página Crear/Editar alerta. Para obtener más información, consulte [Creación y configuración de alertas sencillas en Team Center](#).

Es posible administrar todas las notificaciones de alerta y configurar los detalles de la notificación de la alerta de activación en la sección Políticas del Panel de inicio. Consulte [Creación de una política](#).

22.8

Cambios en la documentación

A partir de esta versión, la información relacionada con los agentes se desacopla de la documentación de DX APM SaaS. La información relacionada con los agentes que anteriormente estaba disponible en la sección Implementación de agentes ahora está disponible en <https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/dx-apm-agents/SaaS.html>. La sección Implementación de agentes ahora tendrá un vínculo que redirige a la documentación de los agentes de DX APM.

NOTE

No funcionará ningún marcador de la información relacionada con cualquier agente que se haya creado desde el sitio de DX APM SaaS anterior. Se recomienda crear nuevos marcadores para la información relacionada con los agente en el sitio de documentación de los [Agentes de DX APM](#). La búsqueda de información relacionada con los agentes utilizando Google mostrará algunos de los vínculos antiguos que no funcionarán. Google tardará tiempo en indexar correctamente la nueva documentación de los Agentes de DX APM SaaS y DX APM. Se recomienda utilizar la funcionalidad de búsqueda en el sitio de documentación hasta que Google indexe correctamente el contenido.

Cifrado de contraseña en el archivo de configuración de Workstation

Durante la configuración de Workstation, ahora puede utilizar **transport.http.proxy.username** y **transport.http.proxy.password** para especificar los valores de autenticación, donde **transport.http.proxy.password** debe cifrarse. Para obtener más información, consulte [Configuración de Workstation con autenticación](#).

Reglas de supresión de seguimiento

Ahora se pueden definir reglas de supresión de seguimiento para identificar los datos confidenciales de los usuarios y reemplazarlos por texto configurado previamente como, por ejemplo, "SUPPRESSED BY APM". Para obtener más información, consulte [Reglas de supresión de seguimiento para ocultar datos confidenciales](#).

22.6

Mejoras en el Agente de la infraestructura

Monitorización de SNMP

SNMPMonitor es una extensión del Agente de la infraestructura de APM que permite monitorizar dispositivos conectados a la red a través del Protocolo simple de administración de red estándar del sector. Es una extensión genérica que puede monitorizar cualquier dispositivo o agente activados para SNMP. Para obtener más información, consulte [Monitorización de SNMP](#).

Servicio de Azure CDN

El monitor de Azure Content Delivery Network permite monitorizar la capacidad de respuesta de Azure CDN al usar aplicaciones, como software de juegos, actualizaciones de firmware, IoT, aplicaciones móviles, plataformas de streaming y sitios web. Para obtener más información, consulte [Servicio de Azure CDN](#).

Monitorización mejorada de Kafka

Se ha agregado la siguiente compatibilidad con la monitorización de Kafka:

- **Compatibilidad con la autenticación SASL/PLAIN del bróker de Kafka:** Se ha agregado la compatibilidad con la autenticación SASL/PLAIN del bróker de Kafka. Se puede activar esta propiedad para las conexiones de cliente proporcionando el nombre de usuario y la contraseña.
- **Función multicliente del Agente de monitorización universal (UMA):** Se ha agregado la compatibilidad para la instalación de equipos multiclientes del Agente de monitorización universal. Use esta función para monitorizar los espacios de nombres.

Para obtener más información, consulte [UMA para el monitor de Kafka](#) y [Monitorización de Kafka](#).

Mejoras en IBM MQ

El Agente de la infraestructura de IBM MQ se ha mejorado para proporcionar una mejor escalabilidad y filtrado. También se ha eliminado el Agente de PCF en desuso. A continuación, se muestra la lista de otras mejoras.

- Tipos de cola agregados en las métricas para obtener una mejor comprensión
- Configuración actualizada de las expresiones regulares

Para obtener más información, consulte [Monitorización de IBM WebSphere MQ](#).

Mejoras en el Agente de .NET/.NET Core

Compatibilidad con .NET 6.0

Se ha agregado la compatibilidad para .Net 6.0 a partir de esta versión para monitorizar el rendimiento de las aplicaciones de .NET 6.

Compatibilidad con WebSocket y Secure WebSocket para .NET agregada

Se ha agregado la compatibilidad con WebSocket y Secure WebSocket para la conexión del Agente de .NET con Cloud Proxy.

Mejoras en el Agente de Node.js

Los nombres de propiedad de las sondas están estandarizados para permitir la implementación fácil del Agente de monitorización universal.

Más información: [Configuraciones del Agente de Node.js](#)

Mejoras en el Agente de monitorización universal

- Se ha agregado la compatibilidad para la monitorización y la generación de informes de eventos del clúster.
Más información: [Configuración de la monitorización de eventos del clúster de UMA - Kubernetes](#) y [Configuración de la monitorización de eventos del clúster de UMA - OpenShift](#)
- Se ha mejorado la monitorización de Prometheus con el Agente de monitorización universal.
Más información: [Ingesta de datos de Prometheus](#)
- Se ha agregado el panel Eventos a los cuadros de mandos de DX del Agente de monitorización universal.
Más información: [Documentación de cuadros de mandos del Agente de monitorización universal](#)

22.3

En esta sección se enumeran las funciones nuevas, modificadas y en desuso en DX Application Performance Management (DX APM) 22.3.

Compatibilidad con K8s 1.22 y OSE 4.9

DX Application Performance Management ahora es compatible con la versión 1.22 de Kubernetes y la versión 4.9 de OpenShift.

Mejoras en el Agente de Nodejs

El agente Nodejs contiene las siguientes mejoras:

Compatibilidad con Redis para NodeJs

DX Application Performance Management es compatible con la instrumentación de llamadas de Redis con la sonda Node.js a partir de esta versión. El compatibilidad con Redis para Node.js permite visualizar el ciclo de vida completo de la transacción, desde el front-end al back-end, de manera estructurada y monitorizar las operaciones CRUD en los puntos finales. La sonda facilita el aislamiento y la evaluación de las incidencias de la aplicación, base de datos o infraestructura con mayor rapidez. Para obtener más información, consulte Redis.

Compatibilidad del framework Async con el agente de la sonda NodeJs

DX Application Performance Management ahora es compatible con el framework Async para el Agente de la sonda NodeJs. Este framework permite correlacionar las llamadas asincrónicas de front-end a back-end asociadas en el nodo Fragments. Para obtener más información, consulte GraphQL

Compatibilidad con la correlación del Agente del explorador de Nodejs

A partir de esta versión, se puede visualizar la correlación de extremo a extremo del entorno desde el explorador hasta la aplicación Nodejs (módulo express js), ver los seguimientos correlacionados y asignarlos para evaluar las incidencias con mayor rapidez. Para obtener más información, consulte Compatibilidad del Agente del explorador en Node.js.

Mejoras en el Agente de .NET

El Agente de .NET contiene las siguientes mejoras:

Compatibilidad para detectar y monitorizar automáticamente detenciones con transacciones de .NET asincrónicas

DX Application Performance Management ahora detecta y monitoriza automáticamente las detenciones con las aplicaciones .NET asincrónicas para evaluar errores y diagnosticar incidencias de rendimiento de la aplicación.

Correlación de seguimiento de extremo a extremo mejorada para aplicaciones .NET asincrónicas

Se ha mejorado la visibilidad del seguimiento de extremo a extremo para las transacciones asincrónicas. Esta función ayuda a solucionar las incidencias de transacción.

Mejoras en el Agente de la infraestructura de APM

El Agente de la infraestructura de APM contiene las siguientes mejoras:

Compatibilidad con Oracle Multitenant en la extensión de monitor de la base de datos de Oracle de APMIA

DX Application Performance Management ahora es compatible con Oracle Multitenant en la extensión de monitor de la base de datos de Oracle. Esta función monitoriza el rendimiento de las bases de datos de Oracle activadas con la opción multicliente. Para obtener más información, consulte Monitorización de la base de datos de Oracle.

vCenter Application Insight Modules (VCAIM)

vCenter Application Insight Modules (VCAIM) proporciona capacidades para monitorizar los sistemas que están bajo control de VMware vCenter Server. VCAIM se puede ejecutar en cualquier sistema Windows donde SystemEDGE esté instalado. VCAIM se comunica con vCenter Server para monitorizar todos los ESX Servers que gestiona el VMware vCenter Server asociado.

Para obtener más información, consulte [vCenter Application Insight Modules](#).

Monitorización de Azure Databricks

La monitorización de Azure Databricks ayuda a supervisar el clúster independiente de Spark y los clústeres de Azure Databricks. Facilita la monitorización de los trabajos, etapas y tareas de una aplicación. Comprueba la memoria y el rendimiento de los ejecutores. La monitorización de Azure Databricks se puede utilizar para la solución de problemas de rendimiento y la caracterización de la carga de trabajo.

Para obtener más información, consulte [Implementación de la monitorización de Spark en Azure Databricks](#).

Monitorización de Azure Active Directory

La monitorización de Azure Active Directory ayuda a supervisar Azure Active Directory mediante registros de auditoría. Los detalles del registro incluyen diversas métricas, tales como Groups Addition Count y Users Addition Count, entre otras. También monitoriza diferentes atributos, como Azure Subscription ID y Azure Tenant ID, entre otros.

Para obtener más información, consulte [Monitorización de Azure Active Directory](#).

Mejora en el APM Command Center

El APM Command Center contiene la siguiente mejora:

Se ha agregado el vínculo de integración del webhook

La integración de terceros permite integrar ACC con la infraestructura (por ejemplo, artifactory) y entregar el paquete de ACC mediante dicha infraestructura. El servidor de configuración de ACC proporciona un vínculo de integración del webhook que activa una aplicación que, a su vez, descarga el paquete y lo importa en la infraestructura. Para obtener más información, consulte [Configuración y descarga de un paquete del agente](#).

Nuevos cuadros de mandos listos para su uso

Los cuadros de mandos de DX incluyen estos nuevos cuadros de mandos:

Cuadros de mandos de Pivotal Cloud Foundry (PCF)

Los cuadros de mandos de PCF son una nueva categoría en los cuadros de mandos de DX APM. Esta categoría incluye los siguientes cuadros de mandos, disponibles en la carpeta General:

- Información de la aplicación de PCF
- Información de VM de PCF (BOSH)
- Información de celda de PCF
- Información del espacio de organización de PCF
- Descripción general de PCF

Para obtener más información, consulte la sección [Cuadros de mandos de PCF](#).

Cuadros de mandos de UMA y mejoras en la visualización

Los cuadros de mandos del UMA se han mejorado para incluir el rendimiento de las aplicaciones correlacionadas. Los cuadros de mandos correlacionados ayudan a determinar rápidamente el impacto de los contenedores en el rendimiento de la aplicación. Para ver la lista de mejoras, consulte [Mejoras del cuadro de mandos](#).

Defectos corregidos

Las siguientes incidencias están reparadas en esta versión:

Defecto DE539968: Se produce un error en `introscope.agent.acc.controller.configurationServer.url` al recuperar los detalles correctos de Cloud Proxy

Solución: La dirección URL de Cloud Proxy del asistente de configuración del paquete `introscope.agent.acc.controller.configurationServer.url` (dirección URL de configserver) y `agentManager.url` (dirección URL de EM) ya no se sincronizan de forma visible en la interfaz de usuario de ACC. Se tiene en cuenta cualquier valor proporcionado y los valores predeterminados están disponibles en el paquete descargado.

NOTE

No se puede obtener el valor de la propiedad `introscope.agent.acc.controller.configurationServer.url` cuando se proporciona una única dirección URL de Isengard (`host:puerto`) para la dirección URL de Cloud Proxy. En ese caso, la propiedad se deja en blanco.

Defecto DE526430: después de actualizar a la versión 2022.1.0.25, los usuarios existentes no se muestran en la página Usuarios y permisos.

Síntoma: he actualizado Enterprise Manager a 2022.1.0.25 y los usuarios existentes no están disponibles en la página Usuarios y permisos.

Solución: inicie sesión en Enterprise Manager después de actualizar y consulte los usuarios existentes.

Defecto DE52234: las perspectivas no cambian al valor predeterminado cuando se cambia entre capas en la página Vista de mapa

Síntoma: he creado tres perspectivas para cada capa de la página Mapa y las he establecido como las perspectivas predeterminadas para cada capa. Al cambiar de una perspectiva a otra en la página Mapa, la perspectiva no cambia.

Defecto DE526577: herramienta de importación de agentes importada a una compilación anterior del agente de la versión 10.7

Síntoma: he importado un agente conectado válido de la versión 10.7 con la herramienta de importación de agentes y he verificado que la página ACC muestra el paquete importado de la compilación anterior.

Solución: como solución alternativa, utilice la versión `<bundle-version>` de la herramienta de importación de agentes.

Defecto DE525374: se muestran paquetes incorrectos al cambiar el paquete para el Agente de la infraestructura en la IU de ACC

Síntoma: mientras cambiaba los paquetes para el Agente de la infraestructura en la IU de ACC y al hacer clic en el vínculo aparece la lista de paquetes que no se pueden aplicar desde la IU de ACC.

22.1

En esta sección se enumeran las funciones nuevas, modificadas y en desuso en DX Application Performance Management (DX APM) 22.1.

Mejoras en el Agente de Java

Compatibilidad con las métricas de monitorización de la plataforma OOB a través de JMX

Compatibilidad adicional con las métricas de monitorización de la plataforma OOB a través de JMX.

Mejoras en el Agente de Nodejs

Compatibilidad de la correlación de la base de datos de Oracle para el Agente Nodejs

Compatibilidad adicional con OracleDB como base de datos de back-end para las aplicaciones de Nodejs. La compatibilidad mejorada de la base de datos de back-end ayuda a detectar componentes descendentes, con la

consiguiente mejora de la topología, los análisis de servicios y los análisis de causa raíz. Para obtener más información, consulte Agente Nodejs.

Compatibilidad del Agente del explorador en Nodejs

La compatibilidad con el Agente del explorador en las aplicaciones de Nodejs correlaciona eventos basados en el navegador y aplicaciones de Nodejs, y calcula el rendimiento del explorador cuando las solicitudes de aplicaciones de Nodejs se procesan en él. HTTP es el módulo principal que procesa las solicitudes de los navegadores en Nodejs. En lo que respecta a la comunicación basada en el explorador, todos los módulos de front-end interactúan con este módulo. Para obtener más información, consulte Compatibilidad del Agente del explorador en Node.js.

Mejoras en el Agente de PHP

Compatibilidad con la correlación del Agente de PHP y el Agente del explorador

A partir de esta versión, se puede visualizar la correlación de extremo a extremo del entorno desde el explorador hasta la aplicación de PHP. También se pueden visualizar los seguimientos correlacionados y asignarlos para evaluar las incidencias con mayor rapidez. Para obtener más información, consulte Inyección del fragmento de código del Agente del explorador utilizando el Agente de PHP.

Mejoras en el Agente de la infraestructura

Compatibilidad con la ingesta de seguimientos de AWS X-Ray para AWS Lambda en DX Application Performance Management

- La monitorización de AWS X-Ray ayuda a monitorizar las aplicaciones que se ejecutan en la nube de AWS. Esta función ayuda a monitorizar el estado y el rendimiento de la infraestructura de AWS.
- La compatibilidad con la creación y el uso de varios perfiles o cuentas ahora se ha introducido para la monitorización de AWS.

Para obtener más información, consulte AWS X-Ray

Entrega de la extensión de monitorización de la infraestructura para IBM App Connect Enterprise v12

A partir de esta versión, DX Application Performance Management admite la monitorización de IBM App Connect Enterprise v11 en adelante (IBM ACE), sucesora de IBM Integration Bus v10 (IIB). La adición de IBM App Connect Enterprise v11 ha enriquecido las plataformas de middleware compatibles en DX Application Performance Management. Mediante el Agente de monitorización de IIB, los usuarios de APM ahora pueden monitorizar la disponibilidad, el estado y el rendimiento de IBM ACE. Para obtener más información, consulte Monitorización de IIB.

Mejoras en el Agente de monitorización universal

Mejora en la monitorización de k8s

La mejora de la monitorización de k8s proporciona información sobre el rendimiento de otras redes y clústeres. Se agregan las siguientes métricas en los datos de rendimiento del pod:

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

Para obtener más información, consulte Datos de las métricas del pod.

Mejoras del UMA

Accesos y privilegios de seguridad para la implementación del UMA

Se pueden agregar los privilegios de seguridad a la implementación del UMA a partir de esta versión.

Solución de problemas mejorada del UMA

Herramientas y mejoras del UMA para gestionar mejor sus implementaciones.

Compatibilidad con las últimas versiones del contenedor de AKS/EKS/GKE

A partir de esta versión, el UMA es compatible con las versiones más recientes de los siguientes contenedores para gestionar el rendimiento de los entornos de contenedor.

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

Compatibilidad con el archivo tools.jar de JDK personalizado en Java Autoattach

Se agregó compatibilidad con el archivo tool.jar de JDK personalizado del UMA para Kubernetes y el UMA para OpenShift. Esta funcionalidad permite adjuntar a todas las máquinas virtuales Java para AutoAttach. Para obtener más información, consulte Instalación y configuración de UMA para Kubernetes e Instalación y configuración de UMA para OpenShift.

Compatibilidad con Red Hat OpenJDK para AutoAttach

A partir de esta versión, el UMA ya es compatible con Red Hat OpenJDK para AutoAttach, lo que permite monitorizar el rendimiento de las aplicaciones en contenedores basadas en la máquina virtual Java de Red Hat.

UMA para mejoras en el diseño de AutoAttach de NodeJS

El UMA es compatible con la detección automatizada de aplicaciones de Nodejs en lista blanca a partir de esta versión. DE FORMA PREDETERMINADA, el monitor del contenedor de aplicaciones del UMA (pod del conjunto de daemons) se ejecuta en modo de lista blanca, de forma que detecta automáticamente y adjunta las aplicaciones de Nodejs en lista blanca.

Certificación de los comandos pm2 y Forever Start para AutoAttach del UMA de NodeJs

UMA es compatible con la monitorización y AutoAttach de las aplicaciones de Nodejs utilizando los comandos de pm2 y Forever Start en el entorno de Kubernetes a partir de esta versión.

Integración de DX Application Performance Management - Mainframe

Compatibilidad con Sysview DB2

A partir de esta versión, DX Application Performance Management ahora mejora la visibilidad de las métricas de Mainframe mediante la compatibilidad con la monitorización del rendimiento de la base de datos de IBM DB2. Ahora, los administradores pueden monitorizar los KPI de la base de datos de IBM DB2 e identificar y evaluar los errores de manera fluida. Para obtener más información, consulte Integración de DX APM Mainframe.

Paquete Kafka con la extensión Mainframe

DX Application Performance Management es compatible con la extensión del bróker de Kafka que gestiona las instancias del bróker de Kafka y Zookeeper y su integración a partir de esta versión.

Esta extensión también se integra con Mainframe para activar la ingesta de registros SMF publicados de un productor de Kafka, como ZAB, a una velocidad elevada en la extensión de IA de Mainframe, con lo que se evita la latencia de red.

Para obtener más información, consulte Extensión del bróker de Kafka.

Mosaico de extensiones de JavaScript agregado en la página Configuración

A partir de esta versión, se agrega un nuevo mosaico de la **extensión de JavaScript** en la sección **Ajustes generales**. Esta función permite acceder a la gestión de las extensiones de JavaScript que pueden procesar las métricas entrantes antes de que se almacenen en DX Application Performance Management. Dentro de una extensión de JavaScript se pueden realizar cálculos, modificar rutas de métrica, modificar nombres de métricas, copiar datos de la métrica en otras nuevas y llevar a cabo operaciones generales de JavaScript en las métricas entrantes. Para obtener más información, consulte Configuración de extensiones de JavaScript.

Cambio de documentación

A partir de esta versión, el nuevo **Cuadros de mandos de DX - Sitio de documentación de SaaS** ya está disponible como sitio independiente. Para obtener más información, consulte *Cuadros de mandos de DX de SaaS*

Problemas conocidos

Defecto DE526430: después de actualizar a la versión 2022.1.0.25, los usuarios existentes no se muestran en la página Usuarios y permisos.

Síntoma: he actualizado Enterprise Manager a 2022.1.0.25 y los usuarios existentes no están disponibles en la página Usuarios y permisos.

Solución: inicie sesión en Enterprise Manager después de actualizar y consulte los usuarios existentes.

Defecto DE52234: las perspectivas no cambian al valor predeterminado cuando se cambia entre capas en la página Vista de mapa

Síntoma: he creado tres perspectivas para cada capa de la página Mapa y las he establecido como las perspectivas predeterminadas para cada capa. Al cambiar de una perspectiva a otra en la página Mapa, la perspectiva no cambia.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE522903: la Vista de métricas produce un error en el explorador y la consola del depurador

Síntoma: he iniciado una sesión de seguimiento de transacciones para un agente a través de la aplicación WebView. En la página Vista de métricas, he accedido a la ficha Seguimientos/Error y a los nodos de métricas de las transacciones generadas de un agente y veo que aparece un error en la página del explorador y en la consola del depurador.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE526577: herramienta de importación de agentes importada a una compilación anterior del agente de la versión 10.7

Síntoma: he importado un agente conectado válido de la versión 10.7 con la herramienta de importación de agentes y he verificado que la página ACC muestra el paquete importado de la compilación anterior.

Solución: como solución alternativa, utilice la versión `<bundle-version>` de la herramienta de importación de agentes.

Defecto DE525374: se muestran paquetes incorrectos al cambiar el paquete para el Agente de la infraestructura en la IU de ACC

Síntoma: mientras cambiaba los paquetes para el Agente de la infraestructura en la IU de ACC y al hacer clic en el vínculo aparece la lista de paquetes que no se pueden aplicar desde la IU de ACC.

Solución: no existe ninguna solución alternativa para esta incidencia.

Defectos corregidos

Las siguientes incidencias se han corregido en esta versión:

Defecto DE521544: no se muestra la lista desplegable de atributos Agregar tarjeta de experiencia

Síntoma: he iniciado sesión en mi cliente y he navegado hasta DX Application Performance Management. He configurado mi Agente de Java de Tomcat y, a continuación, he trabajado con mi aplicación para generar algunas transacciones. En la **Vista de experiencia**, he seleccionado **Agregar nuevo +**. En la página **Agregar tarjeta de experiencia** de la lista desplegable Seleccionar un **universo**, seleccione **Your applications (Sus aplicaciones)**. En la opción **Utilizar todo el universo o aplicar un filtro**, seleccione **Seleccionar agente de la capa de la aplicación**. En la sección **Agrupar por**, cuando he seleccionado la lista desplegable **Atributo**, la lista estaba vacía. La lista no muestra ningún atributo de capa. Esta incidencia solo se produce con agentes de DX Application Performance Management 21.11.

Solución: Seleccione la casilla de verificación **Incluir nodo de experiencia** en la página **Agregar tarjeta de experiencia**. Se puede ver la lista desplegable **Atributos**, pero solo para la capa **Aplicación**, no para las otras capas.

Defecto DE520944: APM Command Center muestra incorrectamente un mensaje de error después de los cambios de configuración del paquete

Síntoma: He utilizado el cuadro de diálogo Descarga del agente para descargar un Agente de la infraestructura. He navegado hasta APM Command Center para configurar el Agente de la infraestructura y he seleccionado **paquetes > Configuración**. He editado mi paquete y configurado una mezcla de propiedades activas e inactivas. Algunas propiedades requieren que se reinicie la aplicación gestionada y otras no. Cuando he hecho clic en **Cambiar**, ha aparecido este mensaje:

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

Cuando he aplicado la nueva versión del paquete al agente, se ha mostrado este mensaje de error para todos los cambios de configuración del Agente de la infraestructura en frío y en caliente:

`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.`

Sin embargo, el paquete se continúa mostrando en la lista de versiones y he podido aplicar el nuevo paquete a mi agente en ejecución.

Solución: Se pueden omitir estos mensajes. Toda la funcionalidad relacionada con el paquete funciona correctamente. Las listas de paquetes muestran las versiones correctas y no hay problemas al aplicar los nuevos paquetes a los agentes en ejecución.

Notas de la versión de 2021

Esta sección contiene las Notas de la versión de las versiones de 2021.

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

21.11

Estas son las funciones nuevas, modificadas y en desuso en DX Application Performance Management (DX APM) 21.11.

Mejoras en la monitorización de Cloud

Aquí se muestran las mejoras que se relacionan con la monitorización en la nube en esta versión.

Monitorización de Google Cloud

Monitorización de Google Cloud Platform Firewall Insights

Ahora se puede monitorizar el estado y el rendimiento de Firewall Insights, que proporciona información sobre el uso y los problemas de configuración del cortafuegos. La monitorización de Firewall Insights admite la correlación entre los elementos de la nube privada virtual (VPC), como el proyecto, la región, la zona y las subredes. Esta correlación proporciona métricas que ofrecen una experiencia de monitorización holística. Se puede comprender y optimizar mejor la configuración del cortafuegos con seguridad. También se pueden revisar informes sobre el uso del cortafuegos y el impacto de diversas reglas de cortafuegos en la red de la nube privada virtual. **Más información:** Monitorización de Google Cloud Platform Firewall Insights

Amazon Web Services (AWS)

Monitorización de la nube privada virtual de AWS

Use la monitorización de la nube privada virtual de AWS para visualizar la nube privada virtual de AWS Cloud Platform y cómo se conectan los componentes de la nube privada virtual. Examine las métricas para monitorizar el estado y el rendimiento de la nube privada virtual. Esta extensión ayuda a comprender el contexto de las aplicaciones que están conectadas a la nube privada virtual, lo que proporciona una correlación de aplicación a infraestructura a red. Monitoree y analice los indicadores clave de rendimiento de la nube privada virtual de AWS Cloud Platform. Estos indicadores incluyen datos entrantes desde el origen, datos salientes del destino, número de conexiones activas y adjudicación del puerto de error. **Más información:** Servicio AWS Virtual Private Cloud

Monitorización de AWS Transit Gateway

AWS Transit Gateway es un servicio que permite conectar las nubes privadas virtuales de AWS Cloud Platform y sus redes locales a una puerta de enlace. La monitorización de AWS Transit Gateway proporciona datos sobre el estado y el rendimiento de AWS Transit Gateway. Esta extensión también correlaciona la instancia de AWS Transit Gateway con otros componentes de la nube privada virtual. La monitorización de la puerta de enlace de tránsito permite visualizar y solucionar problemas con datos exactos de las métricas en las actividades de red y los orígenes de tráfico. Estas métricas ayudan a optimizar las adjudicaciones de ancho de banda, garantizar la correcta planificación de la capacidad, solucionar las incidencias y monitorizar el consumo de ancho de banda. **Más información:** Servicio AWS Transit Gateway

Monitorización de Amazon FSx para Windows File Server

Amazon FSx permite iniciar, ejecutar y administrar sistemas de archivos comerciales y de código abierto en la nube de AWS. La monitorización de Amazon FSx para Windows File Server detecta automáticamente este servicio y realiza una operación de sincronización de forma periódica. Se pueden elegir las matrices para que DX APM monitorice mediante el filtrado básico y avanzado. Se pueden usar los atributos específicos del servicio de la monitorización de Amazon FSx para Windows File Server, como el tipo de ipAddress de ipAddress, el ID de VPC y el nombre de host de DNS. **Más información:** Servicio AWS FSx para Windows File Server

Agente de Java

Monitorización del rendimiento de los front-ends de la experiencia del Agente de Java

El Agente de Java ahora realiza un seguimiento del rendimiento de los front-ends de la experiencia en las transacciones. Esta capacidad permite utilizar la función Evaluación de errores asistida para determinar la causa raíz de los problemas de rendimiento de la aplicación. El Agente de Java localiza los cuellos de botella del rendimiento correlacionando las

anomalías de las aplicaciones de la pila de software con el rendimiento deficiente e inaceptable de la experiencia. **Más información:** Front-ends de la experiencia del Agente de Java

Monitorización de Kafka mejorada para utilizar SSL

La extensión del Agente de Java de monitorización de Kafka permite monitorizar Kafka utilizando el protocolo de seguridad Secure Socket Layer (SSL). **Más información:** Monitorización de Kafka

Monitorización de Azure Java App Services

El Agente de Java para Microsoft Azure App Services permite a las empresas ejecutar aplicaciones de Java en Microsoft Azure para identificar y solucionar problemas de rendimiento. El Agente de Java para Microsoft Azure App Services integra métricas de rendimiento en DX APM para el análisis inteligente, las alertas y la visibilidad en un único cuadro de mandos. Se puede implementar esta extensión del sitio cuando se implementa un contenedor de Tomcat en Azure. Después de implementar el Agente de Java para Microsoft Azure App Services, se pueden configurar las propiedades del agente mediante la configuración del sitio de Azure.

Agente de la infraestructura

Nueva integración de DX APM-Mainframe

Ahora se puede monitorizar el rendimiento del entorno de mainframe de SYSVIEW utilizando la nueva integración de DX APM-Mainframe. Esta integración basada en el Agente de la infraestructura de DX APM incluye cuadros de mandos de Grafana DX listos para su uso, métricas de SYSVIEW y APM entre empresas (CE APM) listas para su uso y alertas para las métricas de SYSVIEW. **Más información:** Integración de DX APM - Mainframe

Nuevos recopiladores de datos de SystemEDGE

El nuevo recopilador de datos de SystemEDGE desacopla SystemEDGE Core de la monitorización del host del Agente de la infraestructura. Sin embargo, DX APM continúa admitiendo todos los casos de uso de la monitorización basados en SystemEDGE heredados y personalizados después de actualizar al Agente de la infraestructura de APM SaaS 21.11. El recopilador de datos de SystemEDGE permite continuar utilizando las bibliotecas principales de SystemEDGE. En el futuro, las bibliotecas de SystemEDGE solo estarán disponibles utilizando los recopiladores de datos de SystemEDGE del Agente de la infraestructura. Los recopiladores de datos de SystemEDGE admiten SNMPv3, lo que proporciona privacidad y autenticación mejoradas de SNMPv.

DX APM proporciona dos recopiladores de datos de SystemEDGE: el recopilador de datos independiente de SystemEDGE y el recopilador de datos de SystemEDGE para Linux. El recopilador de datos independiente de SystemEDGE es compatible con AIX, Linux y Windows. El recopilador de datos de SystemEDGE para Linux permite continuar utilizando la monitorización del host y emplear las ventajas de utilizar un recopilador de datos de SystemEDGE.

Más información: Recopilador de datos de SystemEDGE para Linux

Ejecución de varias instancias del Agente de la infraestructura en el mismo equipo

Ahora se pueden ejecutar varias instancias del Agente de la infraestructura en un equipo para propagar la carga para ayudar a gestionar la monitorización de muchos conjuntos. Se puede configurar el nombre del servicio y los puertos cuando se instala el Agente de la infraestructura para eliminar los conflictos de varios agentes instalados en el mismo equipo. **Más información:** Descarga e instalación del Agente de la infraestructura en AIX, Linux y Solaris

Equilibrio de carga del Agente de la infraestructura para entornos Node.js

Ahora se puede equilibrar la carga de varias instancias del Agente de la infraestructura para lograr una alta disponibilidad en entornos de nube y contenedores complejos de Node.js. El Agente de monitorización universal (UMA) proporciona la comunicación HTTP entre la sonda Node.js y el Agente del recopilador HTTP del Agente de monitorización universal. Esta funcionalidad permite configurar el equilibrio de carga de HTTP para gestionar las instancias del Agente de la infraestructura. El equilibrador de carga proporciona una distribución automatizada del tráfico desde el Agente de Node.js

hacia varias instancias del Agente del recopilador de HTTP. Esta distribución evita la sobrecarga en cualquier instancia del Agente de Node.js. **Más información:** Agente de monitorización universal para el recopilador de HTTP

Mejoras en la monitorización del registro

La monitorización del registro ahora lee los archivos de registro recién generados después de la configuración sin tener que reiniciar la aplicación gestionada. Se pueden configurar los nombres del archivo de registro usando expresiones regulares (regex) para obtener una mejor coincidencia de nombres. La monitorización del registro ahora puede leer dinámicamente los archivos de registro que se crean diariamente o incluso más frecuentemente. DX APM ahora puede leer errores de los archivos de registro y crear las métricas Errors per Interval y Error Snapshots. Team Center muestra seguimientos de transacciones de error cuando se selecciona un vértice de agente del monitor de registro. **Más información:** Monitorización del registro

Mejoras en la seguridad del Agente de la infraestructura

El Agente de la infraestructura ahora es compatible con las últimas plataformas y protocolos de seguridad estándares del sector. Algunos ejemplos son el cifrado de extremo a extremo de AES-256, el hash SHA-256, SNMPv3 (siempre que corresponda), la actualización a VS 2017 y todas las contraseñas que se almacenan en los archivos de configuración se cifran dondequiera que se apliquen. **Más información:** Recopilador de datos independiente de SystemEDGE, Monitorización del host en Linux

La monitorización de MongoDB ahora es compatible con SSL

La monitorización de MongoDB ahora se ha mejorado para utilizar SSL para obtener comunicaciones más seguras entre el cliente de MongoDB y el Agente de la infraestructura. **Más información:** Instalación y configuración de la monitorización de MongoDB.

Agente de .NET/.NET Core

Monitorización mejorada del Agente del explorador

La monitorización del Agente del explorador para las aplicaciones de .NET ahora incluye la decoración de la respuesta basada en encabezados HTTP de forma predeterminada. No es necesario realizar más configuraciones de rastreadores manuales para lograr la correlación del seguimiento de transacciones del Agente del explorador y la correlación desde las sesiones de DX AXA a DX APM. **Más información:** *Artículos de DX APM:* Configuración del Agente del explorador para .NET/.NET Core, Configuración de la inserción automática de fragmentos de código del Agente del explorador para .NET/.NET Core, Configuración de la decoración de la respuesta del Agente del explorador para .NET/.NET Core. *Artículos de CA Experience Collector:* Instalación del Agente de .NET y configuración del Agente del explorador, Configuración del Agente del explorador para .NET, Propiedades del Agente del explorador para .NET.

Agente de monitorización universal (UMA)

Cuadros de mandos de DX del Agente de monitorización universal

El Agente de monitorización universal ahora proporciona cuadros de mandos de Grafana DX listos para su uso para presentar los datos de rendimiento de los entornos de Kubernetes. Estos cuadros de mandos complementan los cuadros de mandos de la capa de la infraestructura de Team Center. Los cuadros de mandos del Agente de monitorización universal son compatibles con todos los entornos de contenedores, incluido Kubernetes, OpenShift y Docker (ECS). **Más información:** Agente de monitorización universal, [Cuadros de mandos del Agente de monitorización universal \(UMA\)](#)

Monitorización del rendimiento del clúster de Kafka del Agente de monitorización universal

Ahora se puede monitorizar el rendimiento del clúster de Kafka utilizando el Agente de monitorización universal. El Agente de monitorización universal detecta automáticamente los pods de ZooKeeper y los pods de Kafka Broker

utilizando anotaciones y las configuraciones de la extensión de monitorización de Kafka. Se puede configurar SSL para Kafka Broker y JMX a través de SSL.

Mejoras en la monitorización de Kubernetes

El Agente de monitorización universal ahora proporciona información más detallada sobre la monitorización de Kubernetes, que proporciona aún más datos de rendimiento de la red y del rendimiento del clúster. Ahora se puede ejecutar la monitorización de Kubernetes en la versión más reciente de Kubernetes. La monitorización de Kubernetes ahora incluye la compatibilidad con volúmenes persistentes, lo que proporciona las nuevas métricas **%CPU/Memory utilization** y **%Disk Utilization by Pods**. Monitorice Kubernetes StatefulSets utilizando las nuevas métricas **%CPU/Memory Utilization** y **%Disk Utilization by Pods**. Las nuevas métricas también se muestran en los cuadros de mandos de DX del Agente de monitorización universal.

Compatibilidad con la función multicliente del Agente de monitorización universal

Ahora se puede utilizar el Agente de monitorización universal en un entorno multicliente. **Más información:** Implementación del Agente de monitorización universal en un entorno multicliente

Gestión de agentes de monitorización universales utilizando APM Command Center

Ahora se pueden crear e implementar paquetes del Agente de monitorización universal en APM Command Center. **Más información:** Implementación de paquetes del Agente de monitorización universal utilizando APM Command Center

Mejoras en la interfaz de usuario

Visualización de roles del universo en Team Center

Cuando se usa la autenticación del inicio de sesión único (SSO), los roles que se pueden reproducir pueden variar para cada sesión dependiendo del protocolo de identidades externo concedido y proporcionado en la respuesta de SAML. En el panel **Launchpad > Configuración > Usuarios**, se pueden ver los roles del universo específicos y los roles de cliente (usuario, usuario avanzado, administrador de clientes). Ahora también se puede ver el rol del perfil actual en la parte superior derecha de la ventana. **Más información:** En el artículo Configuración de universos, consulte la sección **Configuración de la seguridad de universos**.

Nuevo icono de Team Center para acceder a la página Gestión de calculadoras de Javascript

Como administrador de clientes, ahora se puede hacer clic en un icono nuevo para acceder a la pantalla **Gestión de calculadoras de JavaScript**. Se puede establecer la seguridad de la vista de JavaScript en esa pantalla. **Más información:** Roles y privilegios admitidos

El cuadro de diálogo Descarga del agente es compatible con las propiedades de varios niveles

El cuadro de diálogo Descarga del agente ahora permite establecer propiedades que utilizan configuraciones de varios niveles. Por ejemplo, la configuración del monitor de registro utiliza un número variable de matchitems, pathPatterns y matchpatterns. Con esta nueva funcionalidad, se pueden agregar subpropiedades bajo subpropiedades al realizar configuraciones en el cuadro de diálogo Descarga del agente.

Otras funciones

Visibilidad de la base de datos de MongoDB y Redis para la monitorización de aplicaciones del Agente de Python

El Agente de Python de DX APM ahora proporciona una mejor visibilidad de la base de datos de back-end para las aplicaciones de Python. Ahora se pueden monitorizar las bases de datos de MongoDB y Redis para ayudar a detectar componentes descendentes, mejorando la topología junto con los análisis de servicios y los análisis de causa raíz.

Team Center muestra las métricas de rendimiento para las llamadas de back-end y los seguimientos de transacciones correlacionados. **Más información:** Compatibilidad con MongoDB, Compatibilidad con Redis.

Mejora del complemento Jenkins de DX APM

Ahora se dispone de la flexibilidad necesaria para configurar el complemento Jenkins de DX APM en el modo principal o secundario en función de la configuración de Jenkins. **Más información:** Configuración del complemento Jenkins de DX APM

Funcionalidades y plataformas admitidas recientemente

Compatibilidad de APM para SiteMinder (CA APM para CA SSO) con AIX 7

Ahora se puede monitorizar el rendimiento del inicio de sesión único de APM que se ejecuta en AIX 7. Ahora curl está incluido con el Agente web de APM para SSO para AIX, que también es compatible con AIX 7 de 64 bits. **Más información:** En el artículo [APM para SiteMinder 13.3.0](#), consulte la sección **Instalación y configuración en el Agente web (AIX)**.

Compatibilidad y certificación de la plataforma y entorno del Agente de la infraestructura

El Agente de la infraestructura ahora es compatible con las últimas plataformas y protocolos de seguridad estándares del sector. Todas las funcionalidades del Agente de la infraestructura están certificadas para funcionar en estas plataformas y entornos: Windows 10, Windows 2019, Windows CORE 2019, RHEL 8.x, CentOS 8.x, SLES 15.x, OpenSuse 15 y Ubuntu 20.04. SystemEDGE del Agente de la infraestructura es compatible con RHEL 8.x y Windows 2019 Server. La monitorización del host del Agente de la infraestructura es compatible con Windows 2019. **Más información:** Monitorización del host en Windows, Matriz de compatibilidad para el Agente de la infraestructura, Solución de problemas de la monitorización del host

CA APM 10.7 EPAgent compatible con DX APM SaaS

DX APM permite seguir utilizando los scripts de Perl de CA APM 10.7x EPAgent en DX APM SaaS. Para ello, se debe migrar CA APM 10.7 EPAgent a DX APM SaaS. **Más información:** En el artículo [Cloud Proxy](#), consulte la sección **Migración de agentes individuales a DX APM utilizando Cloud Proxy**.

Problemas conocidos

Defecto DE521796: Vértices duplicados de transacciones comerciales en el mapa

Síntoma: He descargado el Agente de Java de Tomcat de DX APM 21.11 con la extensión del Agente del explorador de DX APM 21.11. He navegado por DX APM y he consultado el mapa en Team Center. Para algunos vértices, el vértice de la transacción comercial del Agente del explorador y las transacciones comerciales del Agente de Java se asocian con el vértice del front-end. Esta incidencia solo se produce con agentes de DX APM 21.11.

Solución: Asegúrese de que las tres propiedades siguientes estén establecidas en **false**:

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

Cuando no hay ninguna transacción comercial definida externamente, esta propiedad activa al Agente de Java para crear una transacción comercial predeterminada. El Agente de Java identifica el primer front-end monitorizado.

- **Valores:** true, false
- **Valor predeterminado:** true
- **Ejemplo:** introscope.agent.first.frontend.biz.enabled=true
- **Nota:** No es necesario reiniciar la aplicación monitorizada.

- **introscope.agent.crossprocess.biz.enabled**

Esta propiedad permite al Agente de Java reenviar las transacciones comerciales a través de los procesos a los agentes descendentes. Esta propiedad permite a DX APM crear métricas de transacciones comerciales entre procesos para los agentes descendentes.

- **Valores:** true, false
- **Valor predeterminado:** true
- **Ejemplo:** introscope.agent.crossprocess.biz.enabled=true
- **Nota:** No es necesario reiniciar la aplicación monitorizada.

- **introscope.agent.backend.biz.enabled**

Esta propiedad permite al Agente de Java recopilar métricas de transacciones comerciales para los componentes de back-end.

- **Valores:** true, false
- **Valor predeterminado:** true
- **Ejemplo:** introscope.agent.backend.biz.enabled=true
- **Nota:** No es necesario reiniciar la aplicación monitorizada.

Defecto DE521742: Anomalías no convertidas en problemas

Síntoma: He deseado monitorizar las aplicaciones utilizando agentes de DX APM 21.11 sin que se activara el Agente del explorador. Me he dado cuenta de que las anomalías no se están convirtiendo en problemas, incluso cuando los nodos front-end tienen alertas activas. Las alertas activas tienen un estado de peligro o precaución. El Agente de DX APM 21.11 ha creado nuevos vértices de transacciones comerciales. Estos vértices informan sobre las métricas de BlamePoint. Las métricas de BlamePoint se muestran en el nuevo vértice de transacciones comerciales, que coincide con las métricas que genera el agente para el front-end.

Me he dado cuenta de que las anomalías solo se han convertido en problemas cuando los nuevos vértices de transacciones comerciales tenían alertas activas. Veo las métricas en el nodo Front-end, pero no hay métricas de transacciones comerciales para las nuevas transacciones comerciales. Las métricas que faltan son todas las métricas que no son de BlamePoint. Además, las alertas de front-end predeterminadas no están presentes en el nuevo vértice de transacciones comerciales. Esta incidencia solo se produce con agentes de DX APM 21.11.

Solución: Cree las alertas de front-end cambiando la agrupación de métricas para las alertas predeterminadas. Incluya una nueva expresión regular de las métricas del nodo Segmento del negocio o cree alertas personalizadas en las métricas de BlamePoint de la transacción comercial. El agente informa sobre estas métricas en el nodo **Segmento del negocio** del nodo del agente. No se dispone de ninguna solución alternativa para crear alertas personalizadas que se generan en las métricas no relacionadas con BlamePoint del nodo front-end.

Defecto DE521611: Error de vínculo de la definición de alerta cuando el nombre de la alerta contiene el signo más

Síntoma: He creado una alerta y el nombre contiene el signo más (+). El nombre es similar a este nombre: **cpu+Processor1**. He abierto la página **Configuración > Alertas > Editar alertas** para probar la alerta. He abierto DX Operational Intelligence y he navegado hasta la página **Todas las alarmas** para probar la definición de la alerta. He seleccionado la alerta **cpu+Procesador1**. En la sección **Descripción general**, en **Atributos personalizados**, haga clic en el vínculo **Definición de alerta de APM > Definición de alerta**. Sin embargo, no se ha abierto la página **Alerta**. Y en DX APM, en la página **Editar alertas**, se muestra un mensaje parecido a este mensaje de error: **Error al recuperar la alerta**. Se produce el mismo problema cuando un nombre del módulo de gestión contiene el signo más.

Solución: No incluya el signo más en las alertas y los módulos de gestión de DX APM.

Defecto DE521571: Excepción al descargar el conjunto de APM Command Center al agente en ejecución

Síntoma: Al intentar descargar un conjunto de APM Command Center en el Agente de Java en ejecución, el agente lanzaba excepciones similares a este mensaje:

```
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
```

Nota: Este problema solo se produce con ciertas versiones de JDK como, por ejemplo, Java 1.8u25.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE521544: No se muestra la lista desplegable de atributos Agregar tarjeta de experiencia

Síntoma: He iniciado sesión en mi cliente y he navegado hasta DX APM. He configurado mi Agente de Java de Tomcat y, a continuación, he trabajado con mi aplicación para generar algunas transacciones. En la **Vista de experiencia**, he seleccionado **Agregar nuevo +**. En la página **Agregar tarjeta de experiencia** de la lista desplegable **Seleccionar un universo**, seleccione **Your applications** (Sus aplicaciones). En la opción **Utilizar todo el universo o aplicar un filtro**, seleccione **Seleccionar agente de la capa de la aplicación**. En la sección **Agrupar por**, cuando he seleccionado la lista desplegable **Atributo**, la lista estaba vacía. La lista no muestra ningún atributo de capa. Esta incidencia solo se produce con agentes de DX APM 21.11.

Solución: Seleccione la casilla de verificación **Incluir nodo de experiencia** en la página **Agregar tarjeta de experiencia**. Se puede ver la lista desplegable **Atributos**, pero solo para la capa **Aplicación**, no para las otras capas.

Defecto DE520944: APM Command Center muestra incorrectamente un mensaje de error después de los cambios de configuración del paquete

Síntoma: He utilizado el cuadro de diálogo Descarga del agente para descargar un Agente de la infraestructura. He navegado hasta APM Command Center para configurar el Agente de la infraestructura y he seleccionado **paquetes > Configuración**. He editado mi paquete y he configurado una mezcla de propiedades en frío y en caliente. Algunas propiedades requieren un reinicio de la aplicación gestionada y otras no. Cuando he hecho clic en **Cambiar**, ha aparecido este mensaje:

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

Cuando he aplicado la nueva versión del paquete al agente, se ha mostrado este mensaje de error para todos los cambios de configuración del Agente de la infraestructura en frío y en caliente:

```
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.
```

Sin embargo, el paquete se continúa mostrando en la lista de versiones y he podido aplicar el nuevo paquete a mi agente en ejecución.

Solución: Se pueden omitir estos mensajes. Toda la funcionalidad relacionada con el paquete funciona correctamente. Las listas de paquetes muestran las versiones correctas y no hay problemas al aplicar los nuevos paquetes a los agentes en ejecución.

Defecto DE520499: Mensaje de error de datos del conjunto de seguimientos de transacciones en la Consola del explorador y en las notificaciones

Síntoma: He iniciado sesión en mi cliente y he navegado hasta DX APM. Me he conectado a mi Agente de Java de Tomcat y he trabajado con mi aplicación para generar algunas transacciones. En la **Vista de métrica**, he seleccionado un nombre de agente y he hecho clic en la ficha **Seguimientos**. He cambiado el tiempo de **En directo** a varios tiempos históricos como, por ejemplo, 24 o 6 horas mientras mantenía abierta la ficha **Seguimientos**. Después de unos minutos, esta excepción aparecía en la Consola del explorador y en las notificaciones del explorador:

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

Este mensaje también se muestra en el pie de página del explorador y en la Consola del depurador en la **Vista de mapa** cuando seleccioné un vértice.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE519466: El valor cero de la métrica Average Response Time del Agente de MongoDB de Python es incorrecto

Síntoma: Cuando el Agente de Python monitoriza las operaciones de lectura de MongoDB, el valor de la métrica **Average Response Time (ms)** es cero cuando el valor debe ser mayor de cero.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE496868: Actualización - AGREGAR configuraciones guardadas: El paquete no está disponible después de la actualización

Síntoma: He iniciado sesión en DX APM y he navegado hasta el cuadro de diálogo Descarga del agente en Team Center. Anteriormente había creado y guardado paquetes con configuraciones de propiedades. He hecho clic en **Configuración, Agente, Descargar agente**. Al hacer clic en **Configuraciones de paquetes guardados**, solo están disponibles los paquetes existentes para el Agente de la infraestructura. Los paquetes guardados para el resto de los agentes muestran este mensaje de error: **El paquete no está disponible**. Los ejemplos de agentes son Tomcat en los agentes de Windows, Linux y Java. La columna **Acciones** para estos agentes no muestra ningún icono. Por lo tanto, no he podido editar ni descargar estos paquetes que no son del Agente de la infraestructura.

Solución: No existe ninguna solución alternativa para esta incidencia.

21.6

Estas son las funciones nuevas, modificadas y rechazadas en DX APM 21.6.

Mejoras en la monitorización de Cloud

Aquí se muestran las mejoras que se relacionan con la monitorización en la nube en esta versión.

Monitorización de Google Cloud

Servicio de VPN de GCP Cloud

El servicio de red privada virtual (VPN) de GCP Cloud permite monitorizar el estado y el rendimiento de la VPN de Google Cloud Platform Cloud. Esta funcionalidad le ayuda a garantizar que su infraestructura de la nube siempre esté disponible y que cumpla con los acuerdos de nivel de servicio del tiempo de actividad de su cliente.

La VPN de Google establece conexiones seguras entre sus redes locales, las oficinas remotas, los dispositivos cliente y la red global de Google. Esta funcionalidad permite a su organización realizar la transición del alojamiento en la VPN a la nube, lo que mejora el acceso a los recursos basados en la nube. **Más información:** Servicio de Google VPN

Amazon Web Services (AWS)

Servicio de migración de la base de datos de AWS (DMS)

Ahora monitorice el estado y el rendimiento del servicio de migración de la base de datos de AWS, que le permite migrar sin problemas varios componentes a sus datos en AWS Cloud. Estos componentes incluyen bases de datos relacionales, almacenes de datos, bases de datos que no son de SQL y otros tipos de almacenes de datos. Puede usar el servicio de migración de la base de datos de AWS para migrar los datos entre instancias locales (mediante una configuración de AWS Cloud) o entre combinaciones de configuraciones en la nube y locales. Este servicio le permite realizar migraciones únicas y replicar los cambios en curso para mantener los orígenes y los destinos sincronizados. **Más información:** Servicio de migración de la base de datos de AWS

Agente de Java

Registro mejorado de propiedades del Agente de Java

Ahora se pueden examinar los registros del Agente de Java para determinar el conjunto exacto de propiedades de configuración en uso y el origen de los valores de propiedad.

Compatibilidad con Java 13 y Java 14

El Agente de Java ahora es compatible con las versiones de Java 13 y 14.

Compatibilidad con JBoss EAP 7.3

El Agente de Java ahora es compatible con la versión 7.3 de JBoss EAP.

Cambio predeterminado del filtrado automático del seguimiento de transacciones

El filtrado automático del seguimiento de transacciones ya no incluye las transacciones más rápidas y lentas en la configuración predeterminada. Esta configuración puede causar una sobrecarga de recursos superior a la normal para ciertas aplicaciones. Este es el valor predeterminado de la propiedad actual en el archivo `introscopeagent.profile`:

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

Consulte Configuración del filtro de seguimiento de transacciones para activar el filtrado para las transacciones más rápidas y lentas.

Más información: Configuración de las opciones del seguimiento automático de transacciones

Agente de la infraestructura

Monitorización de la base de datos de IBM DB2

Ahora se puede monitorizar el rendimiento de la base de datos de IBM DB2 en el entorno en directo. La monitorización de la base de datos de IBM DB2 le proporciona visibilidad de los KPI de la base de datos. Esta información le permite aislar los problemas de los componentes de la aplicación y ayuda a solucionar rápidamente los problemas en el entorno en directo.

La extensión de monitorización de la base de datos de IBM DB2 es un sistema de gestión de bases de datos relacionales listo para las empresas. Se ha diseñado esta extensión para ofrecer resistencia, rendimiento y efectividad rentable para las cargas de trabajo transaccionales. **Más información:** Monitorización de la base de datos de IBM DB2

Extensión de IBM DataPower

La extensión de IBM DataPower es una única puerta de enlace de varios canales que se diseña para proporcionar seguridad, control e integración. Se ha optimizado esta extensión para acceder a una gama completa de cargas de trabajo de dispositivos móviles, web, interfaz de programación de aplicaciones (API), arquitectura orientada a servicios (SOA), B2B y cargas de trabajo en la nube. La extensión de IBM DataPower permite monitorizar los datos de rendimiento esenciales sobre la puerta de enlace de DataPower. Se pueden identificar de forma proactiva los problemas de rendimiento en el entorno y correlacionar rápidamente los dispositivos de DataPower con las aplicaciones de back-end.

Más información: Extensión de IBM DataPower

Monitorización de vRealize Operations

Se puede monitorizar, solucionar problemas y gestionar el estado y la capacidad del entorno virtual mediante la aplicación de la automatización basada en políticas. La monitorización de vRealize Operations ofrece una gestión inteligente de las operaciones con visibilidad de la aplicación al almacenamiento a través de las infraestructuras físicas,

virtuales y de la nube. Esta extensión recopila datos de rendimiento de cada objeto en todos los niveles del entorno virtual. La extensión analiza los datos para proporcionar información en tiempo real sobre los problemas de rendimiento. **Más información:** Extensión de vRealize Operations

Mejoras en la monitorización de IBM Integration Bus (IIB)

Ahora se puede establecer la conexión de la monitorización de IIB mediante el modo local o remoto durante la configuración. Los requisitos de seguridad establecidos para monitorizar un objeto MQ se han optimizado para proporcionar una monitorización más segura. **Más información:** Instalación y configuración de la extensión de monitorización de IIB, Métricas de monitorización de IIB

Métricas de observabilidad de RESTmon

El Agente de la infraestructura se ha mejorado ahora para admitir las métricas de observabilidad de RESTmon. Se pueden utilizar estas métricas para monitorizar el rendimiento de las implementaciones de monitorización en la nube. Esta compatibilidad proporciona métricas acerca de diversas plataformas. Se proporcionan métricas relacionadas con el punto final de Amazon Web Services, métricas relacionadas con la monitorización de Google Cloud Platform y métricas relacionadas con Azure, entre otras. **Más información:** Métricas de observabilidad de RESTmon

Extensión de monitorización de SiteMinder

DX Application Performance Management (APM) para CA Single Sign-On (CA SSO) es un paquete especial de DX APM para monitorizar CA SiteMinder. La nueva extensión de monitorización de SiteMinder de DX APM incluye este paquete. CA APM para CA SSO recopila periódicamente las métricas de CA SSO y envía las métricas al Agente de la infraestructura de DX APM. La extensión de monitorización de SiteMinder incluye varios cuadros de mandos de DX que proporcionan información sobre el rendimiento de los servidores proxy y los agentes web. **Más información:** Extensión de monitorización de SiteMinder.

Extensión de monitorización de Elastic

La extensión de monitorización de Elastic permite monitorizar el rendimiento del clúster, los nodos y los índices de Elastic Search para identificar problemas en el entorno en directo. Ahora se pueden filtrar métricas y realizar configuraciones de grupo mediante la extensión del Agente de la infraestructura de Elastic Search. **Más información:** Extensión de monitorización de Elastic

Compatibilidad con la monitorización de la base de datos de Oracle para Oracle 19C

La extensión del Agente de la infraestructura de la monitorización de la base de datos de Oracle ahora es compatible con la versión 19C de la base de datos de Oracle. **Más información:** Monitorización de la base de datos de Oracle

Agente de .NET/.NET Core

Mejoras en la instrumentación inteligente

La instrumentación inteligente de .NET/.NET Core detecta automáticamente los front-end y back-end de .NET/.NET Core. Después de la detección, los rastreadores de front-end y back-end se han agregado a un archivo PBD que vuelve a cargar el Agente de .NET. De forma predeterminada, los nuevos rastreadores están desactivados. Sin embargo, se pueden configurar los rastreadores. También se pueden iniciar sesiones de detección mediante una sesión de seguimiento de transacciones. La instrumentación inteligente de .NET/.NET Core también incluye una activación de CPU configurable que inicia una sesión de detección cuando la CPU del usuario excede un umbral. **Más información:** Configuración de la instrumentación inteligente de .NET/.NET Core.

Compatibilidad con .NET 5

El Agente de .NET/.NET Core ahora es compatible con la versión 5 de .NET.

Agente de monitorización universal (UMA)

Paquete y descarga de UMA mediante APM Command Center

Ahora se puede crear un paquete de UMA con capacidades de monitorización específicas de UMA en APM Command Center. **Más información:** Implementación de paquetes de UMA mediante APM Command Center.

Monitorización del uso del disco del pod

Ahora se puede monitorizar el uso del disco de los pods que están configurados con volúmenes persistentes. **Más información:** Datos de rendimiento del pod

Nomenclatura de agentes automática de UMA en entornos del contenedor

UMA ahora puede determinar un nombre de host apropiado del agente para los agentes que se ejecutan en entornos de contenedor. Esta capacidad incluye la nomenclatura automática del Agente de Java en .NET/.NET Core, UMA AutoAttach en Kubernetes, ECS, OpenShift, etc. **Más información:** Instalación y configuración de UMA para Kubernetes.

Compatibilidad con la función multicliente de UMA

Ahora se puede utilizar UMA en un entorno multicliente.

Funcionalidad AutoAttach de UMA para el Agente de la sonda Node.js

Ahora se pueden monitorizar todas las aplicaciones y la infraestructura que se ejecutan en el entorno de Kubernetes con un único agente. La funcionalidad AutoAttach con casi sin intervención o configuración mínima facilita la incorporación y la detección. La funcionalidad AutoAttach ofrece una solución única para gestionar y monitorizar aplicaciones nativas de la nube listas para su uso en la nube híbrida. **Más información:** AutoAttach del Agente de Node.js

Incidencia conocida

Defecto DE504064: Error de la máquina virtual Java de Windows con EXCEPTION_ACCESS_VIOLATION

Síntoma: En determinadas circunstancias, la máquina virtual Java puede realizar un volcado de memoria. Este problema se produce cuando DX APM monitoriza aplicaciones asíncronas.

Solución: Como solución alternativa, tome *una* de estas medidas:

- Actualice al último parche de la máquina virtual Java.
Normalmente, la actualización soluciona este problema.
- Cree o actualice un paquete que contenga el conjunto NoRedef apropiado para su entorno.
El conjunto NoRedef contiene el archivo `AgentNoRedefNoRetrans.jar`, que desactiva la redefinición y la retransformación de las clases para evitar posibles problemas de rendimiento.
Se puede elegir entre estos conjuntos NoRedef:
 - Java Agent NoRedef
 - JBoss NoRedef
 - Sockets NoRedef
 - Tomcat NoRedef
 - WebLogic NoRedef
 - WebSphere NoRedef

Más información: Información de AgentRedef en la configuración de WebSphere Application Server, Implementación de paquetes del agente mediante APM Command Center

21.4

Estas son las funciones nuevas, modificadas y rechazadas en DX APM 21.4.

Mejoras en la monitorización de Cloud

Aquí se muestran las mejoras que se relacionan con la monitorización en la nube en esta versión.

Monitorización de Google Cloud

Servicio Google Cloud Billing

El servicio Google Cloud Billing proporciona métricas sobre el coste de Google Cloud Platform (GCP), con los datos generados diariamente (opción configurable). Este servicio proporciona la información necesaria para hacer un presupuesto del coste de GCP. **Más información:** Servicio Google Cloud Billing

Monitorización de GCP con entrada sin clave

Este servicio permite monitorizar los servicios de Google Cloud sin configurar los tokens de seguridad. En su lugar, el servicio de entrada sin clave utiliza Google Kubernetes Engine (GKE) Workload Identity para proporcionar los permisos correctos. **Más información:** Monitorización de Google Cloud con entrada sin clave

Amazon Web Services (AWS)

Mejora en el servicio de monitorización de AWS EMR

El servicio de monitorización de AWS EMR ahora es compatible con dos métricas nuevas. Estas métricas proporcionan el estado de las aplicaciones que se ejecutan en el clúster AWS EMR:

- **State:** Muestra el estado del clúster EMR.
- **Status Code:** Especifica el motivo del error del clúster (esta métrica solo está disponible para los clústeres finalizados).

Más información: Servicio de monitorización de AWS EMR

Mejora en el servicio de monitorización de AWS Glue

Se ha agregado un nuevo mensaje de error de métrica a este servicio. Esta métrica muestra el mensaje de error real para el trabajo de Glue. **Más información:** Servicio AWS Glue

Servicios de cuotas y uso del servicio de Azure

El nuevo servicio de cuotas y uso del servicio de Azure ayuda a consultar el uso actual y el límite del servicio de los recursos de Azure. Es posible ver el uso y las cuotas para estos proveedores:

- Compute
- Almacenamiento
- Network
- Azure VMware Solution by CloudSimple

Más información: Cuotas y uso del servicio de Azure

Agente de Java

Filtrado automático del seguimiento de transacciones

DX APM monitoriza cada transacción del entorno. Por diseño, DX APM recopila los seguimientos de transacciones para incidencias de rendimiento, errores y detenciones. El filtrado automático del seguimiento de transacciones permite examinar las transacciones potencialmente problemáticas sin tener que ejecutar explícitamente los seguimientos de transacciones. DX APM ahora agrega más configuración para los seguimientos de filtrado automático como, por ejemplo, las N transacciones más lentas, más rápidas, etc. **Más información:** Configuración de las opciones del seguimiento automático de transacciones

Nomenclatura del Agente de Java con contenedor

DX APM ahora determina automáticamente un nombre de host apropiado del agente para los Agentes de Java en los entornos de contenedor. DX APM proporciona la nomenclatura para el Agente de Java tanto para las implementaciones nativas de Kubernetes del Agente de monitorización universal (UMA) como para las implementaciones estándares del Agente de Java que no son del UMA. **Más información:** Nomenclatura del Agente de Java, Instalación y configuración de UMA para Kubernetes. Consulte la sección sobre la solución de propiedades dinámicas de UMA.

Nuevo modo de inicio del Agente de Java

Ahora se puede evitar el retraso de la hora de inicio del Agente de Java configurando la propiedad del sistema `-Dcom.wily.introscope.agent.startup.mode=neo` para iniciar el Agente de Java en modo Neo. Se puede retrasar el inicio del Agente de Java configurando la propiedad del sistema `-Dcom.wily.introscope.agent.startup.delay`. **Más información:** Configuración del modo de inicio

Agente de la infraestructura

Compatibilidad de los seguimientos de la monitorización de la base de datos de SQL Server

Ahora se pueden ver los seguimientos de transacciones de la base de datos de SQL Server en la **Vista de mapa** seleccionando el nodo correspondiente de la base de datos de SQL Server y haciendo clic en la ficha **Base de datos**. Los seguimientos de transacciones de la base de datos de SQL Server están formados por eventos que tienen diversos indicadores de rendimiento para monitorizar y mantener la base de datos de SQL Server. **Más información:** Seguimientos de la base de datos de SQL Server

Nuevas métricas de utilización de la CPU o memoria dinámica

La monitorización de JMX remoto ahora proporciona métricas sobre la memoria dinámica que se utiliza para la adjudicación de objetos. Estas métricas se activan de forma predeterminada y aparecen en el Árbol de métricas: `<infra-agent>|<jmx-metric-root-node>|JVM|Memory|Heap`. La monitorización de JMX remoto ahora también proporciona métricas sobre la memoria gestionada por JVM que se utiliza para almacenar clases y metadatos cargados, así como para el procesamiento interno. Estas métricas se activan de forma predeterminada y aparecen en el Árbol de métricas: `<infra-agent>|<jmx-metric-root-node>|JVM|Memory|Non Heap`. También se pueden ver estas nuevas métricas como métricas estándares de JMX. **Más información:** Monitorización de JMX remoto, Métricas de JMX.

Mejora en la monitorización de F5 LTM

La monitorización de F5 LTM ahora permite, con una única implementación del agente, la monitorización de varias instancias de F5. Para cada instancia de F5, se debe configurar un perfil de F5. **Más información:** Monitorización de F5 LTM

Compatibilidad con la autenticación de capa segura en la monitorización de Redis

La extensión de monitorización de Redis ahora es compatible con la monitorización de Redis a través de SSL. Utilice estas propiedades para activar SSL en la monitorización de Redis:

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

Más información: Configuración de la extensión de monitorización de Redis

Mejora en la monitorización del host

Monitoree el rendimiento de los procesos dedicados del host definiendo argumentos de proceso en la configuración de la monitorización. **Más información:** Propiedades de la monitorización del host

Compatibilidad con RHEL 8.2 para la monitorización del host, SysEDGE

RHEL 8.2 ahora está certificado para la monitorización del host y SysEDGE. **Más información:** Matriz de compatibilidad para el Agente de la infraestructura

Compatibilidad con NGINX 1.19.x

DX APM ahora es compatible con la versión 1.19.0 de NGINX. **Más información:** Monitorización de NGINX

Mejora en la monitorización de vCenter

Ahora se puede monitorizar la nueva métrica **Resource Pool** junto con las otras métricas de vCenter en el entorno de vCenter. **Más información:** Monitorización de vCenter

Agente de .NET/.NET Core

Detección automática de back-ends

El Agente de .NET/.NET Core ahora detecta back-ends de forma automática sin necesidad de instrumentación manual o personalizada. **Más información:** Instrumentación inteligente del Agente de .NET/.NET Core

Agente de monitorización universal (UMA)

Compatibilidad con ECS y Docker Swarm

El Agente de monitorización universal ahora detecta y monitoriza automáticamente los contenedores y la infraestructura de nodos de AWS ECS y Docker Swarm. **Más información:** UMA para AWS ECS, UMA para Docker Swarm.

Monitorización mejorada de Kubernetes

El Agente de monitorización universal ahora proporciona información más profunda de la monitorización de Kubernetes al proporcionar estas nuevas métricas y capacidades de monitorización del rendimiento de la red y del clúster:

- Métricas de red: bytes in, bytes out, bytes sent y bytes received
- Monitoriza el rendimiento de etcd y del servidor de la API
- Monitoriza el rendimiento de las configuraciones de implementación
- Límites de la CPU y de la memoria por proyecto

Funciones de IU

Vista previa de la agrupación de métricas

La vista previa de la Vista de métricas muestra el modo de vista previa de los grupos de métricas configurados. Se pueden ver los datos de las métricas relevantes que se trazan en la gráfica. La ventana Vista previa muestra la gráfica de datos de las métricas en función del **Especificador de agente** y el **Especificador de métrica** proporcionados en el campo **Expresiones**. Más información: Configuración de agrupaciones de métrica en Team Center

Vista previa Alertas

La vista previa de las alertas muestra el modo de vista previa de los grupos de métricas configurados. Se pueden ver los datos de las métricas relevantes que se trazan en la gráfica. La ventana de la vista previa muestra la gráfica de datos de las métricas en función del campo **Agrupación de métrica**. **Más información:** Creación y configuración de alertas sencillas en Team Center

Vista previa Calculadoras

La vista previa Calculadoras muestra el modo de vista previa de los grupos de métricas configurados. Se pueden ver los datos de las métricas relevantes que se trazan en la gráfica. La ventana de la vista previa muestra la gráfica de datos de las métricas en función del campo **Agrupación de métrica**. **Más información:** Creación y edición de calculadoras

Granularidad aumentada de la seguridad de los universos

Ahora, en cada universo, a los usuarios se les asignan derechos individuales por módulo de gestión para editar alertas, calculadoras y grupos de métricas. Anteriormente, solo los usuarios asignados como el usuario avanzado o el administrador de clientes podían modificar las alertas, las calculadoras y los grupo de métricas del módulo de gestión. Ahora el rol del usuario avanzado, los usuarios y los grupos de usuarios deben tener permiso para ver o crear alertas, calculadoras o grupos de métricas en un módulo de gestión. El usuario avanzado continúa iniciando manualmente las sesiones de seguimiento de transacciones. **Más información:** Configuración de universos.

Otras funciones

Aumento de la seguridad para el cuadro de diálogo Descarga del agente, APM Command Center y Cloud Proxy

Los agentes de DX APM descargados y los controladores de ACC ahora son más seguros. Estas son las mejoras:

- La validación del certificado TLS de APM Command Center (ACC) se ha mejorado para las comunicaciones de controlador de ACC y el agente. Ahora DX APM valida el certificado y el nombre de host para los agentes nuevos y actualizados y los controladores de ACC que utilizan la conexión TLS.
- La validación del certificado TLS ahora está activada para todos los agentes que se descargan del cuadro de diálogo Descarga del agente.
- Ahora se pueden especificar almacenes de confianza personalizados para la validación de TLS por parte del cliente y de forma global.
- Se pueden actualizar los agentes y los controladores de ACC existentes con un nuevo almacén de confianza personalizado.
- Cloud Proxy ahora está configurado para usar el almacén de confianza predeterminado de Java para la validación del certificado.

Incidencia conocida

Defecto DE502703: La propiedad `introscope.agent.dotnet.monitorAppPools` no funciona

Síntoma: He quitado las marcas de comentario y configurado la propiedad `introscope.agent.dotnet.monitorAppPools` en el archivo `introscopeagent.profile` de .NET/.NET Core.

Por ejemplo, `introscope.agent.dotnet.monitorAppPools="DefaultAppPool"` .Después de reiniciar el servidor web de IIS, la propiedad no ha surtido efecto.

Solución: Para CA APM 10.7 y versiones anteriores, el valor configurado se ha colocado entre comillas. Para DX APM SaaS y la instancia local de DX APM, el valor debe configurarse *sin* comillas. Por ejemplo, `introscope.agent.dotnet.monitorAppPools=DefaultAppPool` .

Defecto DE499817: No se muestran datos en el mapa, el cuadro de mandos o el Bloc de notas de análisis

Síntoma: Seleccione la opción de perspectiva vacía (un cuadro gris claro) de la lista de perspectivas. Cuando aparece esa perspectiva, no se muestra ningún dato en el mapa, el cuadro de mandos y el **Bloc de notas de análisis de la Vista de experiencia**.

Solución: Seleccione una perspectiva válida de la lista de perspectivas y, a continuación, actualice la página.

21.1

Estas son las funciones nuevas, modificadas y rechazadas en DX APM 21.1.

Estas son las funciones nuevas, modificadas y rechazadas en DX APM 21.1.

Mejoras en la monitorización de Cloud

En esta versión hemos realizado varias mejoras relacionadas con la supervisión de Cloud, incluidas las siguientes:

Nueva capa de red

DX APM aporta una nueva capa de red que correlaciona los componentes de la aplicación, los elementos de la infraestructura y la topología de red. Esta correlación permite identificar si el cuello de botella del rendimiento se encuentra en una aplicación, en la infraestructura o en la red. El mapa de DX APM ahora incluye una **capa de red**. Esta capa de red contiene información de los Agentes de la infraestructura y sus extensiones para Cloud. Además, muestra los elementos Cloud, como la nube privada virtual (VPC), los enrutadores, las interconexiones, las subredes y otros elementos de VPC de Cloud. **Más información:** Capas del mapa

Monitorización de Google Cloud

Active estos servicios Cloud para consultar los componentes y las conexiones en la capa de red:

- **Servicio de nube privada virtual de Google**

La nube privada virtual de Google (VPC) proporciona funcionalidad de red a las instancias de la máquina virtual (VM) de Compute Engine, a los contenedores de Google Kubernetes Engine (GKE) y al entorno flexible de App Engine. El servicio de nube privada virtual de Google permite monitorizar el estado y el rendimiento de la red. **Más información:** Nube privada virtual de Google Cloud

- **Servicio Google Cloud Routers**

Google Cloud Router es un servicio que funciona a través de las conexiones de Cloud Interconnect o la VPN de Cloud. Cloud Router facilita un enrutamiento dinámico usando el Border Gateway Protocol (BGP) para las redes de la nube privada virtual (VPC) de Google Cloud. Con este servicio puede supervisar el estado y el rendimiento de los enrutadores Cloud en Google Cloud Platform. **Más información:** Google Cloud Routers

- **Servicio Google Cloud Interconnect**

El servicio Google Cloud Interconnect permite monitorizar el estado y el rendimiento de Google Cloud Interconnect en Google Cloud Platform. **Más información:** Google Cloud Interconnect

Mejora del servicio Google Compute Engine

Google Compute Engine ahora es compatible con las **métricas Mirroring** y las **métricas Nat**. **Más información:** Servicio Google Compute Engine.

Amazon Web Services

Autenticación basada en roles de AWS sin credenciales

La autenticación basada en roles de Amazon Web Services (AWS) monitoriza las cuentas de AWS sin ninguna credencial. Para utilizar la autenticación basada en roles, cree una política y un rol en las cuentas de AWS para monitorizar el Agente de AWS. **Más información:** Autenticación basada en roles de AWS sin credenciales

Agente de Java

Extensión del bus de servicio de Oracle 12C

La extensión del bus de servicio de Oracle 12C (OSB12) monitoriza los detalles de las transacciones OSB, las métricas de rendimiento y la información detallada del estado documentando información completa sobre los flujos de solicitudes de extremo a extremo. La extensión muestra todos los componentes OSB de un flujo. **Más información:** Extensión del bus de servicio de Oracle 12C

Agente de la infraestructura

Monitorización de vCenter certificada para VMware vSphere, versión 7

La extensión de monitorización de vCenter ahora es compatible con la versión 7.0 de VMware vSphere. **Más información:** Monitorización de vCenter

Agente de monitorización universal

Compatibilidad del Agente de monitorización universal con el perfil de WebSphere Liberty

El Agente de monitorización universal ahora detecta e instrumenta automáticamente los contenedores de WebSphere Liberty. **Más información:** WebSphere Liberty

Funciones de IU

En esta sección se enumeran las funciones nuevas y mejoradas de la interfaz de usuario.

Filtrado de mapas sin diferencia entre mayúsculas y minúsculas

El valor de filtrado de direcciones URL compuesto para consultar las vistas **Mapa** y **Aislamiento** ya no distingue entre mayúsculas y minúsculas. Por ejemplo, si se realiza una consulta del nombre del host **GOOgle.Com**, DX APM también consulta los valores **google.com**.

Árboles de métrica filtrados por mapa

La nueva opción **Filtrar la Vista de métrica por los componentes del mapa** en el editor **Universe** filtra los árboles de métrica en el Explorador de métrica por mapa. **Más información:** Configuración de Universes

Descarga de App Synthetic Monitor desde el cuadro de diálogo de descarga del agente

Ahora se puede descargar el grupo App Synthetic Monitor (ASM) desde el cuadro de diálogo **Seleccionar agente para la descarga** del Agente de la infraestructura.

Mejoras en el cuadro de diálogo Seleccionar agente para la descarga

El cuadro de diálogo **Seleccionar agente para la descarga** del sitio del cuadro de diálogo de descarga del agente presenta un nuevo diseño para distinguir mejor entre los agentes entregados por el Agente de la infraestructura y las extensiones disponibles.

APM Command Center

IU de APM Command Center compatible con WCAG 2.0 AA

Ahora se pueden utilizar tecnologías de asistencia para recorrer la IU de APM Command Center. APM Command Center ahora cumple con los criterios de WCAG 2.0 AA.

Otras funciones

Calculadoras JavaScript persistentes

Las calculadoras JavaScript ahora son compatibles con el cálculo continuo de métricas a través de reinicios y actualizaciones de DX APM sin ninguna interacción manual. Las calculadoras ahora se almacenan en una unidad persistente.

Cuadros de mandos de DX: compatibilidad adicional con las funciones de agregación de NASS API

El lenguaje de consulta NassQL agiliza la realización de consultas y el procesamiento de datos de métricas en el servidor. El lenguaje de consulta NassQL es similar al lenguaje SQL conocido de las bases de datos relacionales. Se pueden consultar los datos de la métrica mediante distintas funciones. Es posible usar la función FROM y los datos del grupo con las funciones WINDOW y GROUP. También se pueden llevar a cabo agregaciones y asignaciones mediante funciones. **Más información:** [Referencia de consultas sobre agregaciones de métricas](#).

Incidencia conocida

Defecto DE492513: No se puede aplicar un nuevo paquete a los agentes en APM Command Center

Síntoma: He creado en APM Command Center un paquete para un agente y he realizado algunas configuraciones durante la creación. Seguidamente, he actualizado el paquete. Al aplicar el paquete a mis agentes, no aparecía ninguno de ellos. Por lo tanto, no pude aplicar la versión actualizada del paquete a mis agentes conectados.

Solución: Use esta solución alternativa para instalar el agente con el paquete actualizado.

Siga estos pasos:

1. En APM Command Center, haga clic en **Paquetes**, en el panel de navegación izquierdo.
2. Seleccione la versión actualizada del agente en la lista **Paquetes**.
En el panel central se mostrará la información del agente.
3. En la sección **Versión del paquete**, busque la fila **Descargar paquete**.
4. Haga clic en **Descargar archivo de archivado del paquete**.
DX APM descarga el paquete en el equipo.
5. Desinstale el agente anterior.
6. Instale el agente con la última versión del paquete.

Notas de la versión de 2020

Esta sección contiene las Notas de la versión de 2020.

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

20.11

Estas son las funciones nuevas, modificadas y rechazadas en DX APM 20.11.

Mejoras en la monitorización de Java

El Agente de Java incluye las siguientes modificaciones:

Monitorización de Spring Cloud Gateway

La extensión de Spring Cloud Gateway es una puerta de enlace de API que proporciona una forma simple y eficaz para dirigir las API. **Más información:** Extensión de Spring Cloud Gateway.

Extensión del portal de WebSphere

La extensión del portal de WebSphere permite crear y gestionar portales web. Se puede utilizar esta extensión para crear un portal, que es una recopilación de portlets. A cada portlet se le asigna un espacio específico en el portal. Se pueden crear los portlets recuperando datos de diversas fuentes y mostrar datos sobre los portlets en la **Vista de métricas**. **Más información:** Extensión del portal de WebSphere.

Compatibilidad con la versión 8.x de MySQL

El Agente de SQL para Java ahora monitoriza el rendimiento de las llamadas del back-end de la base de datos para la versión 8.x de MySQL.

Versión 4.2 de PostgreSQL EDB

El Agente de SQL para Java ahora monitoriza el rendimiento de las llamadas del back-end de la base de datos para la versión 4.2 de PostgreSQL EDB.

Agente de Java mejorado para la monitorización de WebSphere Application Server

Ahora se puede utilizar el archivo Agent.jar como el archivo JAR para WebSphere Application Server (WAS) para las versiones 8 y posteriores. Ya no es necesario configurar el archivo AgentNoRedefNoRetrans.jar. **Más información:** WebSphere Application Server.

Más seguridad del Agente de Java

Ahora se puede utilizar la propiedad `agentManager.tls.validateHostname` para aumentar la DX APM seguridad evitando posibles ataques de tipo "man-in-the-middle". **Más información:** Propiedades del Agente de Java.

Mejoras en el seguimiento de transacciones del Agente de Java

Ahora se pueden utilizar estas dos propiedades para recopilar y decorar los seguimientos automáticos de transacciones de prioridad del Agente de Java. Los seguimientos automáticos de prioridad son seguimientos de transacciones que activan otras capacidades esenciales, como la detección de topología.

- `introscope.agent.deep.automatic.trace.priority.clamp`
Esta propiedad fija el número de seguimientos automáticos de transacciones de prioridad que el agente recopila en el intervalo de 1 minuto.
- `introscope.agent.deep.automatic.trace.detailed.reason`
Esta propiedad permite que los seguimientos automáticos de la transacción se decoren con el motivo detallado por el que se ha activado el agente para recopilar el seguimiento. De lo contrario, los seguimientos se decoran con un motivo resumido.

Más información: Propiedades del Agente de Java.

Mejoras en la monitorización del Agente de .NET

El Agente de .NET incluye las siguientes modificaciones:

Instrumentación inteligente de .NET/.NET Core

La instrumentación inteligente de .NET/.NET Core detecta e instrumenta front-ends de .NET/.NET Core sin ninguna configuración necesaria. La instrumentación inteligente de .NET/.NET Core está activada de forma predeterminada y se activa cuando se inicia un seguimiento de la transacción. Se pueden configurar propiedades para controlar el registro de pilas de subprocesos específicas y la ubicación de archivos .pdb generados. Después de detectar un nuevo front-end, el Agente de .NET/.NET Core agrega más configuración a `detected-frontends.pdb`. **Más información:** Configuración de la instrumentación inteligente de .NET/.NET Core.

Análisis mejorado de causa raíz del rendimiento de la CPU de .NET/.NET Core

El Agente de .NET/.NET Core informa sobre dos métricas nuevas que proporcionan más información sobre el rendimiento de la CPU acerca de los métodos de .NET. Estas métricas pueden ayudarle a determinar si un cuello de botella del rendimiento se debe a la ejecución del código del método o al tiempo de E/S.

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

Más información: Diagnóstico de problemas de rendimiento del sistema.

Métricas de fragmento asincrónico y seguimientos de transacciones de fragmento asincrónico para ASP.NET y ASP.NET Core

En este momento, el Agente de .NET/.NET Core monitoriza las solicitudes asincrónicas en las aplicaciones de ASP.NET y ASP.NET Core. En el Explorador de métrica se muestran las métricas de los front-end en los nodos **Fragments** y **Called Fragments**. El agente también recopila seguimientos de transacciones de fragmentos. **Más información:** Fragmentos asincrónicos de .NET/.NET Core.

Automatic Attribute Decoration para .NET/.NET Core

Automatic Attribute Decoration se incluye en el Agente de .NET/.NET Core para permitir agregar atributos personalizados del entorno del agente a los vértices de Team Center. Con Automatic Attribute Decoration se puede controlar y rellenar automáticamente todos los atributos de los vértices que gestione el agente en el entorno. El mapa muestra los vértices, lo que permite identificar el canal de comunicación entre varios vértices en su entorno. Los atributos agregados permiten identificar y aislar más fácilmente un vértice problemático, lo que permite mitigar los problemas y resolver incidencias de manera más rápida. **Más información:** Automatic Attribute Decoration (Agente de .NET/.NET Core).

Mejoras en la monitorización de Cloud

La monitorización de Cloud incluye las siguientes modificaciones:

Monitorización de Google Cloud

Monitorización de Cloud Bigtable

Google Cloud Bigtable le ayuda a almacenar una gran cantidad de datos de clave única con baja latencia. La monitorización de Cloud Bigtable incluye un nodo estático denominado **multi-region** del tipo **GCP Region**. Este nodo estático permite conectar las instancias de GCP Bigtable a las regiones aplicables. **Más información:** Google Cloud Bigtable.

Monitorización de Google MemoryStore para Memcached

GCP MemoryStore para Memcached es un servicio de Memcached altamente escalable y completamente gestionado para Google Cloud. Se puede monitorizar GCP MemoryStore para Memcached mediante las métricas de estado, los atributos y las métricas de la nube. Para este agente, se puede monitorizar el grupo de métrica a nivel de nodo. **Más información:** Monitorización de Google MemoryStore para Memcached.

Amazon Web Services

Monitorización de AWS SageMaker

AWS SageMaker le permite formar, generar y alojar un modelo en un punto final disponible. Se puede monitorizar el rendimiento de SageMaker mediante la extensión de monitorización de AWS. **Más información:** AWS SageMaker.

Monitorización de AWS Athena

El servicio Amazon Athena es un servicio de consulta interactiva que facilita el análisis de los datos en Amazon S3 con la instrucción SQL estándar. Se pueden monitorizar las métricas de Cloud Watch y de la API de servicio. También se pueden monitorizar las métricas derivadas. La monitorización de AWS Athena es compatible con el grupo de trabajo, lo que ayuda a separar usuarios, equipos, aplicaciones o cargas de trabajo. **Más información:** Servicio AWS Athena.

Monitorización de AWS Step Functions

AWS Step Functions es un servicio de orquestación sin servidor. Este servicio permite combinar funciones de AWS Lambda y otros servicios de AWS para crear aplicaciones comerciales críticas a través de un flujo de trabajo visual. Active este servicio para ver las métricas de Step Functions. **Más información:** AWS Step Functions.

Compatibilidad con la detección basada en etiquetas de los servicios de AWS

El filtrado basado en etiquetas permite monitorizar únicamente instancias con etiquetas específicas para los siguientes servicios de monitorización de AWS:

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

Más información: Filtrado basado en etiquetas del inventario de AWS.

Mejoras en la monitorización de la infraestructura

El Agente de la infraestructura incluye las siguientes modificaciones:

Monitorización de Cassandra

La monitorización de Cassandra es una extensión del Agente de la infraestructura que recopila y muestra las métricas de clúster de la base de datos de Apache Cassandra. **Más información:** Monitorización de Cassandra.

Monitorización de Vault

La monitorización de Vault es una extensión del Agente de la infraestructura que permite monitorizar el rendimiento del servidor de Vault de diferentes bibliotecas y subsistemas. Esta extensión recopila diversas métricas como el tiempo de ejecución, el núcleo, la auditoría, el almacenamiento del back-end, la gestión de solicitudes y el motor secreto. **Más información:** Monitorización de Vault.

Compatibilidad con la extensión de seguimiento de IBM Integration Bus (IIB) 10

La extensión de IIB 10 ayuda a monitorizar el rendimiento de los flujos de mensajes de IBM Integration Bus, lo que genera seguimientos de transacciones y métricas. Se pueden utilizar ccpprobe y userexits, que IIB proporciona, para interactuar con los flujos de mensajes sin modificar la aplicación existente. **Más información:** Extensión de seguimiento de IBM Integration Bus (IIB) 10.

Monitorización mejorada de Cloud Foundry

La extensión del Agente de la infraestructura de monitorización de Cloud Foundry informa sobre nuevas métricas para que pueda gestionar mejor el rendimiento de la plataforma Pivotal Cloud Foundry. Por ejemplo, la monitorización de Cloud Foundry ahora proporciona métricas de Auctioneer y BBS LockHeld y métricas de User Account and Authentication (UAA), entre otras. **Más información:** Métricas de la monitorización de Cloud Foundry.

Monitorización del host mejorada para Windows

La extensión de monitorización del host para el Agente de la infraestructura de Windows ahora incluye todas las métricas de rendimiento y estado de SysEdge. **Más información:** Monitorización del host para Windows

Automatic Attribute Decoration para el Agente de la infraestructura

Automatic Attribute Decoration es una extensión del Agente de la infraestructura que permite agregar atributos personalizados del entorno del agente a los vértices de Team Center. Con Automatic Attribute Decoration se puede controlar y rellenar automáticamente todos los atributos de los vértices que gestione el agente en el entorno. El mapa muestra los vértices, lo que permite identificar el canal de comunicación entre varios vértices en su entorno. Los atributos agregados permiten identificar y aislar más fácilmente un vértice problemático, lo que permite mitigar los problemas y resolver incidencias de manera más rápida. **Más información:** Automatic Attribute Decoration para el Agente de la infraestructura.

Compatibilidad con la autenticación de Windows para la monitorización del servidor web de IIS

Ahora se puede configurar la monitorización del servidor web de IIS mediante la autenticación de Windows. **Más información:** Configuración de la monitorización del servidor web mediante la autenticación de Windows.

Configuración del acceso seguro para la monitorización de F5 LTM

La extensión del Agente de la infraestructura de monitorización de F5 LTM incluye la nueva propiedad `introscope.agent.f5.tokenAuth` para ejecutar la autenticación basada en tokens. **Más información:** Configuración de la monitorización de F5 LTM.

Acceso del Agente de la infraestructura del usuario no root

Los usuarios no root ahora pueden instalar, iniciar y detener el Agente de la infraestructura. Algunos comandos del Agente de la infraestructura han cambiado. Esta tabla enumera los comandos anteriores y actualizados:

Comando anterior	Comando actualizado
force_start	console_start
force_stop	console_stop Este comando también se agrega para el Agente de la infraestructura basado en UNIX.
apmia-ca-installer.sh/apmia-ca-installer.bat	APMIACtrl.sh/APMIACtrl.bat

Funciones de UMA

En esta sección se enumeran las funciones nuevas y mejoradas del Agente de monitorización universal.

UMA para la extensión de la sonda Python

El Agente de monitorización universal para Kubernetes ahora detecta e instrumenta automáticamente las aplicaciones de Python sin necesidad de realizar cambios manuales en la imagen de la aplicación. **Más información:** UMA para la extensión de la sonda Python.

UMA para la extensión de la sonda NGINX

El Agente de monitorización universal para Kubernetes ahora detecta e instrumenta automáticamente las aplicaciones de NGINX sin necesidad de realizar cambios manuales en la imagen de la aplicación. **Más información:** UMA para la extensión de la sonda NGINX.

Soporte de Zipkin

DX APM ahora recopila datos de elemento span sobre las aplicaciones de las que Zipkin, un sistema de seguimiento distribuido, hace un seguimiento. El soporte de Zipkin informa y muestra las métricas de rendimiento de la aplicación, los errores y los seguimientos de transacciones. El soporte de Zipkin es una extensión del Agente de la infraestructura que proporciona datos sobre los front-ends de HTTP, los back-ends de HTTP y los back-ends de la base de datos. **Más información:** Soporte de Zipkin.

Funciones del Agente de Node.js

En esta sección se enumeran las funciones nuevas y mejoradas del Agente de Node.js.

Monitorización del rendimiento del tiempo de ejecución de Node.js en implementaciones en contenedores

Ahora se puede instalar Node.js como un agente independiente sin Python. **Más información:** Instalación del Agente de la sonda Node.js para CA Digital Experience Insights.

Compatibilidad de MS SQL con el Agente de Node.js

El Agente de Node.js ahora es compatible con las llamadas de la base de datos de las versiones 2016 y 2017 de Microsoft SQL Server. **Más información:** Matriz de compatibilidad para el Agente de Node.js.

Funciones del Agente de PHP

DX APM ahora es compatible con la versión 7.4 de PHP. **Más información:** Matriz de compatibilidad para el Agente de PHP.

Funciones de IU

En esta sección se enumeran las funciones nuevas y mejoradas de la interfaz de usuario.

Mejoras en la creación y incorporación de universos

En la nueva vista **Universos**, los administradores pueden conceder distintos derechos a usuarios y grupos de usuarios. Los derechos incluyen el acceso al universo y el filtrado de las fuentes de métrica. El filtrado se puede basar en dominios (acceso a agentes) con atributos y expresiones regulares, componentes del mapa y módulos de administración.

Además, el comportamiento de los universos ha cambiado, lo que afecta al filtrado de las fuentes de métrica. Debido al cambio, se deben volver a configurar las fuentes de las métricas del universo para que se aplique correctamente el filtrado de agentes en el Explorador de métrica. Por ejemplo, supongamos que el entorno tiene diez agentes activos. Antes de las mejoras de los universos 20.11, había cuatro agentes enumerados en el universo X y se muestran en el Explorador de métrica. Después de los cambios del universo 20.11, el universo X contiene diez agentes que se muestran en el Explorador de métrica. Se deben actualizar explícitamente las fuentes de las métricas del universo para que vuelvan a aparecer cuatro agentes en el universo X y que se muestren en el Explorador de métrica.

Más información: Configuración de universos.

Agentes desconectados

Ahora es posible acceder a los datos de los agentes desconectados. **Más información:** Monitorización de los valores de métrica del agente con la Vista de métrica.

Clasificación de atributos en la ventana Perspectiva

Ahora se pueden arrastrar y soltar atributos en la ventana **Perspectiva** para ordenar o cambiar los atributos en la jerarquía. El orden de atributos define el orden en que se aplican los filtros y, por lo tanto, la agrupación de vértices. **Más información:** Organización de los componentes utilizando perspectivas.

Colores de estado para los agentes

Los agentes desconectados ahora se muestran en gris. **Más información:** Monitorización de los valores de métrica del agente con la Vista de métrica.

Otras funciones

Exportación de métricas en la Vista de métrica

Ahora se pueden exportar las métricas en la **Vista de métrica** para, por ejemplo, combinar distintos tipos de datos y crear gráficos en Excel. **Más información:** Monitorización de los valores de métrica del agente con la Vista de métrica.

Problemas conocidos

En esta sección se enumeran los problemas conocidos de la versión actual.

Síntoma: Inicio sesión en el cliente con un cliente activado por SAML en Chrome. Al cerrar sesión, se vuelve a iniciar sesión.

Solución: Esta incidencia se debe a que se mantiene el mismo cliente. Este comportamiento es habitual para las aplicaciones que tienen el inicio de sesión único activado, como DX SaaS. Otras aplicaciones son MS Office 365, Box, SharePoint y Google. La solución es borrar la memoria caché al cerrar la sesión para clientes.

Defecto DE481045: No se puede cerrar la sesión del cliente de DX SaaS SAML

Síntoma: Inicio sesión en el cliente con un cliente activado por SAML en Chrome. Al cerrar sesión, se vuelve a iniciar sesión.

Solución: Esta incidencia se debe a que se mantiene el mismo cliente. Este comportamiento es habitual para las aplicaciones que tienen el inicio de sesión único activado, como DX SaaS. Otras aplicaciones son MS Office 365, Box, SharePoint y Google. La solución es borrar la memoria caché al cerrar la sesión para clientes.

Estas son las soluciones alternativas:

Inicie una nueva sesión sin cerrar la sesión.

- Abra una ventana del explorador de incógnito e inicie una nueva sesión.
- Abra un explorador diferente, como FireFox, e inicie una nueva sesión.

Cierre la sesión e inicie sesión de nuevo para iniciar una nueva sesión.

- Cierre la sesión y, a continuación, haga clic en **Iniciar sesión con otro cliente** en unos segundos.
- Cierre sesión manualmente en un cliente eliminando la cookie **CA_CLOUD_Management**. A continuación, inicie sesión en otro cliente.
- Cierre el explorador y espere hasta que se agote el tiempo de espera. A continuación, inicie sesión en otro cliente.

Defecto DE481045: Dificultad para cambiar entre varios clientes de DX SaaS SAML

Síntoma: Puedo acceder a varios clientes de SAML; sin embargo, no puedo cambiar fácilmente entre ellos.

Solución: Su problema aparente de cambio es el efecto secundario de una incidencia de cierre de sesión de DX SaaS. DX SaaS no puede cerrar la sesión de varios clientes a los que se accede con el mismo explorador. Esta incidencia solo se produce al usar SAML.

Use las mismas soluciones alternativas que para la incidencia anterior.

Defecto DE486199: Comportamiento incorrecto al crear un universo o guardar el filtro del mapa como un universo

Síntomas:

- Cuando se crea un nuevo universo, estos comportamientos no deseados se producen en la página **Crear universo**:
 - A veces, los nombres y las descripciones de los campos se rellenan automáticamente con los datos de un universo existente. Al hacer clic en **Guardar**, la página se guarda con las opciones predeterminadas (ver a continuación).
 - La opción predeterminada del botón de opción **Módulos de gestión de Todos los elementos** cambia a **Elementos seleccionados** cuando relleno los campos **Nombre*** y **Descripción**. Al hacer clic en **Guardar**, la página se guarda con las opciones predeterminadas (ver a continuación).
- Al guardar el filtro del mapa como un universo, se producen estos comportamientos no deseados:
 - El botón de opción **Filtro del módulo de gestión** está situado al lado de **Elementos seleccionados** en lugar de **Todos los elementos**. Al hacer clic en **Guardar**, la página se guarda con las opciones predeterminadas (ver a continuación).
 - Al guardar el filtro del mapa como un universo, la configuración **Incluir nodo de experiencia** no se aplica al universo creado recientemente.

Estas son las opciones predeterminadas para guardar un nuevo universo:

- Cuando se crea el universo haciendo clic en el botón **Nuevo universo**, se selecciona la opción **Todos los elementos** en cada ficha.
- Cuando se crea el universo haciendo clic en **Guardar como universo** de la página **Mapa**, se rellena un filtro en la ficha **Componentes** del **mapa**. Otras fichas tienen la opción **Todos los elementos** seleccionada.

Solución: Estas incidencias no tienen una solución alternativa.

20.9

Estas son las funciones nuevas, modificadas y rechazadas en DX APM 20.9

Mejoras en la monitorización de Java

El Agente de Java incluye las siguientes modificaciones:

Compatibilidad rediseñada con JMX del Agente de Java

La extensión mejorada de JMX del Agente de Java se empaqueta e implementa como nueva extensión del agente compatible con las métricas Spring Boot y Micrometer. Se pueden configurar nuevas propiedades de JMX mediante APM Command Center o en el archivo `bundle.properties` de la carpeta `extensions/deploy`. La extensión mejorada es compatible con Java 7 y versiones posteriores. Para Java 6, continúe utilizando las propiedades de JMX en `IntroscopeAgent.profile`.

Definiciones mejoradas del grupo de direcciones URL de front-end

El Agente de Java ahora normaliza automáticamente los segmentos dinámicos de las direcciones URL para obtener definiciones de direcciones URL de front-end más significativas y útiles.

Detección automática de nombres de aplicaciones Spring-Boot

Ahora se puede configurar la extensión de monitorización del Agente de Java Spring Boot para detectar automáticamente el nombre de la aplicación Spring Boot.

El Agente de SQL es compatible con Oracle 19.x

El Agente de SQL para Java ahora admite la monitorización de bases de datos Oracle, versión 19.x. **Más información:** Configuración de la monitorización de SQL para Java.

Compatibilidad con Webflux, versiones 2.1.x y 2.2.x, de Spring Boot del Agente de Java

DX APM ahora es compatible con las versiones 2.1.x y 2.2.x de Webflux de Spring Boot. **Más información:** Monitorización de la aplicación Spring Boot Reactive.

Compatibilidad con Jetty Framework 8.x

El Agente de Java ahora es compatible con Jetty Framework 8.x.

Mejoras en la monitorización del Agente de .NET

El Agente de .NET incluye las siguientes modificaciones:

Mejora de la visibilidad más exhaustiva del rendimiento de las aplicaciones de .NET Core

DX APM agrega automáticamente mayor visibilidad a las aplicaciones de .NET Core que se ejecutan en Linux sin necesidad de disponer de una instrumentación manual o personalizada.

Mejoras en la monitorización de Cloud

La monitorización de Cloud incluye las siguientes modificaciones:

Google Cloud Platform

Compatibilidad con el servicio Google Cloud BigQuery

El servicio Google Cloud BigQuery permite visualizar el rendimiento de las consultas de BigQuery. **Más información:** Servicio Google Cloud BigQuery.

- Compatibilidad con el servicio Google Dataproc

La extensión de monitorización de Google Cloud Platform recopila métricas para el servicio Dataproc. **Más información:** Google Dataproc.

- Compatibilidad con el servicio Google Cloud Load Balancing

La extensión de monitorización de Google Cloud Platform recopila métricas para el servicio Load Balancing. **Más información:** Consulte la sección Servicio Google Cloud Load Balancing.

- Compatibilidad con el servicio Google Cloud Autoscaler

Google Cloud Autoscaling permite gestionar un aumento del tráfico y reducir los costes cuando la necesidad de recursos es inferior. **Más información:** Google Cloud Autoscaler.

Amazon Web Services

- Detección automática basada en roles para organizaciones de AWS

Compatibilidad con la detección automática basada en roles para las organizaciones de Amazon Web Services. **Más información:** Configuración de la monitorización de organizaciones de AWS

Amazon Web Services (AWS) ya es compatible con los siguientes servicios:

- Compatibilidad con el servicio AWS Elastic Map Reduce (EMR)

El servicio de monitorización AWS EMR agiliza la ejecución de casos de uso en clústeres efímeros y de un único propósito que se escalan automáticamente para satisfacer la demanda o en clústeres altamente disponibles de larga duración por medio del nuevo modo de implementación multimaestro. **Más información:** Servicio de monitorización de AWS EMR.

- Compatibilidad con el servicio AWS Glue

El servicio AWS Glue detecta datos y almacena los metadatos asociados (por ejemplo, el esquema y la definición de tabla) en el Catálogo de datos de AWS Glue. **Más información:** Servicio AWS Glue.

Mejoras en la monitorización de la infraestructura

El Agente de la infraestructura incluye las siguientes modificaciones:

Extensión de monitorización del host remoto

La extensión del Agente de la infraestructura de monitorización del host remoto permite recuperar datos de rendimiento de un sistema que no disponga de un agente. La monitorización del host remoto recopila datos de rendimiento del sistema enviando comandos CLI de manera remota. La extensión recopila métricas sobre el uso de la CPU, el disco, el uso de la memoria y la carga junto con los procesos con un aumento mínimo en la utilización de los recursos del sistema monitorizado. **Más información:** Monitorización del host remoto.

Monitorización de Logstash

La extensión de monitorización del Agente de la infraestructura de Logstash permite monitorizar y recopilar métricas de distintos complementos Logstash. **Más información:** Extensión de monitorización de Logstash.

Compatibilidad con NGINX 1.18.x

DX APM ahora es compatible con la versión 1.18.0 de NGINX. **Más información:** Monitorización de NGINX.

Monitorización del host

Compatibilidad de las métricas Core con la monitorización del host

Las métricas Core anteriores de CPU, disco y memoria, procesos y red de SysEdge se han transferido a la monitorización del host del Agente de la infraestructura en Linux. **Más información:** Métricas de monitorización del host.

Monitorización de la base de datos

Monitorización de bases de datos SAP HANA

La extensión de monitorización de la base de datos SAP-HANA recopila métricas que monitorizan el estado y el rendimiento de las bases de datos SAP HANA. **Más información:** Monitorización de SAP HANA.

Mejoras en la monitorización de Python

El Agente de Python incluye las siguientes modificaciones:

Llamadas asincrónicas compatibles con el Agente de Python

El Agente de Python ya es compatible con todos los marcos de Python que utilizan módulos de instrumentación asincrónica.

Compatibilidad del Agente de Python con Rasa Framework y Rasa SDK

Rasa es un framework de código abierto que se utiliza principalmente para crear asistentes contextuales, es decir, aplicaciones de bot de chat. El Agente de Python ya es compatible con las aplicaciones de monitorización basadas en Rasa Framework. **Más información:** Consulte la sección Rasa Framework.

Mejoras en el Agente de monitorización universal

Compatibilidad agregada del Agente de monitorización universal para la extensión Node.js

Se pueden conectar las aplicaciones de sonda al Agente del recopilador de datos UMA, que se ejecuta como parte del conjunto de daemons UMA, configurando la variable de entorno **COLLECTOR_AGENT_HOST** con un nombre de nodo específico. **Más información:** Consulte la sección Agente de monitorización universal para la extensión Node.js.

Middleware de mensajería, ESB y Web Services Enhancements

Compatibilidad con Apache Camel

La extensión Apache Camel permite monitorizar todas las aplicaciones que utilizan Apache Camel como motor de enrutamiento. Las aplicaciones se pueden implementar en las aplicaciones JBoss Fuse, Tomcat o Spring Boot. **Más información:** Apache Camel.

Mejora del Agente de API Gateway

Compatibilidad con la agregación de métricas de servicio

La agregación de métricas de servicio agrega métricas en varios niveles para los servicios solicitados. Se pueden consultar las métricas en el nivel de la puerta de enlace, nivel de clúster y nivel de EM en los agentes. **Más información:** Consulte la sección Agregación de métricas de servicio en el Agente de CA API Gateway.

Mejoras en el APM Command Center

Sustitución del idioma de consultas Lucene

Se ha reemplazado la búsqueda del idioma de consultas Apache Lucene en APM Command Center por un idioma de consulta interno de DX APM.

Problemas conocidos

En esta sección se enumeran los problemas conocidos de la versión actual.

Defecto DE479068: el Árbol de métricas sigue rotando

Síntoma: En la **Vista de métrica**, se carga la gráfica de métricas al ocultar agentes desconectados, pero no el Árbol de métrica.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE478641: en la alerta de peligro generada por métrica no aparece el icono de peligro

Síntoma: En la **Vista de métrica**, una alerta de peligro generada por una métrica no se muestra como un icono. No obstante, si se cambia entre dos vistas de métricas cualesquiera, aparecerá el icono de alerta de peligro.

Defecto DE477342: Los campos Evaluación de errores asistida no aparecen en la Vista de aislamiento

Síntoma: Si un agente posee atributos personalizados y se activa una alerta, los campos Evaluación de errores asistida no aparecen en la **Vista de aislamiento** de la alerta.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE477272: En el panel derecho de la Vista de experiencia no aparecen problemas ni anomalías

Síntoma: En la **Vista de experiencia**, los problemas y las anomalías se muestran en la tarjeta de experiencia. Sin embargo, al seleccionar un problema o anomalía, el panel derecho de la **Vista de experiencia** no muestra los detalles.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE476351: existe un error con los vínculos de la documentación de instalación del paquete de APM Command Center

Síntoma: Esta incidencia se produce al seleccionar un paquete existente en APM Command Center y hacer clic en el vínculo **aquí** de las instrucciones de instalación. Se muestra una página techdocs.broadcom.com en blanco o el portal de Tech Docs en lugar de la página con las instrucciones de instalación prevista.

Solución: Vaya directamente al [sitio de documentación SaaS de DX APM](#).

Defecto DE449130: No se puede iniciar sesión mediante la cuenta de SAML

Síntoma: Los usuarios no pueden iniciar sesión al utilizar los detalles de la cuenta de SAML.

Solución: Genere un token público e inicie sesión con el token.

20.6

Estas son las funciones nuevas, modificadas y en desuso en DX APM 20.6.

Funciones del agente

En esta sección se enumeran las funciones nuevas y mejoradas relacionadas con el agente.

Monitorización de RabbitMQ

RabbitMQ es un agente de mensajes multiplataforma que proporciona una forma de intercambiar datos entre diferentes aplicaciones.

La extensión de RabbitMQ monitoriza el rendimiento de los nodos, los intercambios de mensajes, las colas y las conexiones de los clústeres y los sistemas autónomos en la infraestructura de RabbitMQ. En un clúster de RabbitMQ, la extensión detecta automáticamente los nodos del clúster que se van a monitorizar. La extensión establece una aplicación en la correlación de infraestructura que permite depurar las incidencias causadas por el servidor de RabbitMQ en una aplicación. En la Vista de mapa, la capa de la infraestructura muestra la asignación entre el clúster y los nodos. También hemos introducido GIF animados como forma de ilustración. Para obtener más información, consulte Monitorización de RabbitMQ.

Soporte de Mule ESB 4.x

Mule ESB 4.x le permite identificar los flujos de comunicación y su correlación en todas las comunicaciones, incluida la comunicación asíncrona. Ahora también se pueden identificar los componentes de modelado específicos de Mule ESB. En el mapa aparece un nuevo icono de Mule en los vértices de Mule. También hemos introducido GIF animados como forma de ilustración. Para obtener más información sobre Mule ESB 4.x, consulte Mule ESB 4.x.

Monitorización de PostgreSQL

La monitorización de PostgreSQL DX APM permite monitorizar el rendimiento y la disponibilidad del entorno de la base de datos de PostgreSQL. Se puede configurar y utilizar esta extensión del Agente de la infraestructura para recopilar estas métricas de rendimiento relacionadas con el servidor de PostgreSQL: utilización de recursos, transacciones, rendimiento e interbloqueos, entre otros. La extensión de PostgreSQL también permite a los usuarios correlacionar la aplicación con el rendimiento de la base de datos en lo que respecta al rendimiento real de la base de datos. Para obtener más información, consulte Monitorización de PostgreSQL.

Compatibilidad de la correlación del monitor de infraestructura de WebLogic

La extensión del monitor de infraestructura de WebLogic ahora es compatible con la correlación entre aplicación e infraestructura. Para obtener más información, consulte Atributos del monitor de infraestructura de WebLogic.

Nuevas métricas de monitorización de vCenter

La monitorización de vCenter DX APM ahora proporciona métricas para las entidades siguientes en el entorno de vCenter: vCenter, Centro de datos, Clúster, Almacén de datos, Agrupaciones de recursos, NIC virtuales y físicas, Conmutadores virtuales, Discos, Sensores, ESX y Máquina virtual. Para obtener más información, consulte Monitorización de vCenter.

La monitorización de AWS es compatible con más servicios

La monitorización de Amazon Web Services (AWS) DX APM ahora es compatible con estos nuevos tipos de servicios: Elastic Load Balancing, Elastic Cache, Auto Scaling, Kinesis Data Streams, Billing, API Gateway, CloudTrail, Functions, Logic App, Redshift, Cloudwatch Logs, Cloudfront, Cloudwatch Events y Fargate. DX APM proporciona soporte de monitorización de AWS basado en roles para el ID externo, lo que le permite evitar ataques delegados confusos en su entorno de AWS. Para obtener más información, consulte Monitorización de Amazon Web Services.

El Agente de monitorización universal es compatible con .NET Core

El Agente de monitorización universal para Kubernetes (UMA) ahora detecta e instrumenta automáticamente las aplicaciones de .NET Core sin necesidad de realizar cambios manuales en la imagen de la aplicación. UMA es compatible con la versión 3.1 y posteriores de NET Core.

Compatibilidad con el Agente del explorador de .NET Core

Ahora se puede configurar la inserción automática de fragmentos de código del Agente del explorador para el Agente de .NET Core. Para obtener más información, consulte [Configuración del Agente del explorador para .NET](#).

Visualización de los datos de UMA para Kubernetes en el Árbol de métricas y en el Mapa

El Agente de monitorización universal para Kubernetes (UMA) tiene datos de métricas, atributos y topología de Kubernetes más detallados que se pueden ver en el Árbol de métricas y en el Mapa.

DX APM recopila y muestra los datos de back-end de OpenTracing Jaeger

DX APM ahora recopila seguimientos del back-end de OpenTracing Jaeger e informa de los datos como métricas de DX APM y seguimientos de transacciones.

Uso de las anotaciones para anular las configuraciones de AutoAttach de UMA

Ahora se pueden utilizar las anotaciones para sobrescribir las configuraciones de la extensión de asociación automática de UMA. A continuación aparecen algunos ejemplos:

- Se pueden sobrescribir las comprobaciones del filtro de la extensión de AutoAttach para la memoria y las JVM.
- Se puede utilizar la anotación para transferir cualquier configuración del Agente de Java como, por ejemplo, la adición de propiedades.
- Se puede activar el Agente del explorador por espacio de nombres y, por lo tanto, se agrega una anotación adecuada. La extensión de AutoAttach utiliza la nueva anotación como una configuración y transfiere las propiedades para activar el Agente del explorador sin necesitar llevar a cabo un reinicio o reimplementación.

El Agente de OpenTracing facilita la correlación

La extensión del Agente de OpenTracing del Agente de la infraestructura ahora se correlaciona entre los seguimientos de las transacciones de DX APM y los intervalos de Jaeger.

El Agente de .NET /.NET Core utiliza la comunicación de WebSocket

El Agente de .NET /.NET Core está configurado para enviar automáticamente información mediante el protocolo de WebSocket. Este protocolo combina la eficacia de la comunicación del socket binario con la compatibilidad de servidores proxy de red HTTP y cortafuegos. Cualquier versión compatible con .NET Core y .NET Framework 4.5 y versiones superiores es compatible con la comunicación de WebSocket.

Creación de nombres de aplicaciones y atributos personalizados de .NET /.NET Core

Ahora se pueden configurar las propiedades `.NET/.NET IntroscopeAgent.profile` para mostrar esta información:

- Atributos personalizados en la ficha **Agente** de la **Vista de componentes** del Mapa
- Nombres de aplicación personalizados en la ficha **Front-end genérico** de la **Vista de componentes** del Mapa
- Los nombres personalizados de aplicaciones que aparecen en el panel de **Detalles de componentes** de Transaction Tracer

Compatibilidad del Agente de .NET Core con el SO Alpine

Ahora, el Agente de .NET Core puede monitorizar el rendimiento de las aplicaciones que se ejecutan en el sistema operativo Alpine Linux.

Funciones de IU

En esta sección se enumeran las funciones nuevas y mejoradas de la interfaz de usuario.

Frases de búsqueda

Ahora, a medida que se escribe la frase de búsqueda, se puede seleccionar una frase de búsqueda anterior que aparece en el menú desplegable de autocompletado. Para obtener más información, consulte [Búsqueda de métricas en el Árbol de métrica](#).

Visualización de agentes desconectados en la escala de tiempo

Los agentes desconectados aparecen en gris en la escala de tiempo.

Cuadros de mandos de DX App Synthetic Monitor

Los nuevos cuadros de mandos de DX App Synthetic Monitor (ASM) listos para su uso proporcionan una descripción general del rendimiento de su entorno web. Se pueden establecer varios monitores en DX ASM para medir el rendimiento de la página. Estos cuadros de mandos están ahora disponibles en DX SaaS:

- **Métricas clave de todos los monitores:** Este cuadro de mandos muestra las métricas clave que todos los monitores recopilan.
- **Métricas clave de un único monitor:** Este cuadro de mandos muestra las métricas clave que un único monitor recopila.

Para obtener más información sobre los cuadros de mandos listos para su uso, consulte [Cuadros de mandos de DX](#).

Otras funciones y mejoras

En esta sección se enumeran las demás funciones mejoradas.

Mejoras en el almacenamiento de topología

Como administrador, ahora se pueden crear particiones de almacenamiento de topología y volver a equilibrar los clientes en las instancias de almacenamiento de topología.

Problemas conocidos

En esta sección se enumeran los problemas conocidos de la versión actual.

Defecto DE466013: Alerta de APM. Se ha ignorado la elección de alerta para las notificaciones de activación

Válido para: DX APM SaaS 20.6

Síntoma: Este problema ocurre después de seleccionar una notificación de alerta de activación al crear una nueva alerta. DX APM no aplica la activación correctamente cuando se modifica el nivel de alerta. Por ejemplo, se crea una alerta y se selecciona la opción de recibir una notificación **cuando aumenta la severidad**.

Si la severidad de la alerta cambia de **Crítica** a **Grave** a **Aceptable**, DX APM no debe enviar una notificación de alerta por correo electrónico. Sin embargo, el canal de notificación se activa y envía por error una notificación de correo electrónico cuando se reduce la severidad de la alerta.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE449130: No se puede iniciar sesión mediante la cuenta de SAML

Válido para: DX APM 20.1, 20.4, 20.6

Síntoma: Los usuarios no pueden iniciar sesión al utilizar los detalles de la cuenta de SAML.

Solución: Genere un token público e inicie sesión con el token.

DE467134: A DX Operational Intelligence le falta la ficha de métricas afectadas en la página de análisis de alarmas

Válido para: DX APM 20.6, CA APM 10.7x

Síntoma: Estos problemas se producen cuando CA APM 10.7x local se configura para enviar alarmas al SaaS de DX Operational Intelligence. Se pueden ver las alertas de CA 10.7x local en la página **Análisis de alarmas** de DX Operational Intelligence. Sin embargo, falta la ficha **Métrica afectada** en todas las alertas de CA 10.7x local. Esta incidencia no se produce cuando DX APM SaaS envía alertas.

Solución: Seleccione las métricas en la página **Análisis de rendimiento**.

20.4

Estas son las funciones nuevas, modificadas y rechazadas en DX APM 20.4

Funciones del agente

En esta sección se enumeran las funciones nuevas y mejoradas relacionadas con el agente.

Monitorización de Undertow

Ahora se puede utilizar la monitorización de Undertow de DX APM para monitorizar el rendimiento de las aplicaciones que implementan los identificadores HTTP de Undertow. Esta extensión de agente de Java se activa cuando se utiliza Undertow y DX APM no muestra ningún front-end de Undertow.

Cuando las aplicaciones utilizan la API de servlet, no es necesario utilizar la monitorización de Undertow, incluso cuando se tiene un servidor subyacente de Undertow. No necesita la extensión en este caso porque el Agente de Java realiza un seguimiento de los servlets de forma predeterminada.

Para implementar la monitorización de Undertow, incluya el conjunto **Undertow (sin servlets)** al crear o editar un paquete en APM Command Center.

Monitorización de la malla de servicios de Istio

DX APM ahora realiza la monitorización de pila completa de las implementaciones de la malla de servicios de Istio. La monitorización de la malla de servicios de Istio proporciona la siguiente información y funcionalidad:

- Datos sobre el estado y el rendimiento de los componentes del plano de control de Istio como, por ejemplo, Mixer, Pilot y Gateway
- Datos de rendimiento del plano de datos que incluyen el proxy de envío
- Datos sobre el estado y el rendimiento de los servicios
- Detección automática de la topología de la malla de servicios, incluida la intercomunicación entre los microservicios y el rendimiento de la infraestructura de contenedores.

Monitorización de etcd

Ahora se puede monitorizar el rendimiento de la implementación de etcd. DX APM utiliza el Agente de monitorización universal configurado para importar los datos de Prometheus para informar de las métricas de etcd sobre el estado de los clústeres de Kubernetes o OpenShift.

Monitorización mejorada de Kubernetes y OpenShift

DX APM ahora incluye informes mejorados sobre el rendimiento de la topología de Kubernetes. El mapa incluye los nodos de los componentes de Kubernetes, incluidos los clústeres y los espacios de nombres. La monitorización de Kubernetes y OpenShift incluye métricas para que pueda evaluar mejor la capacidad del clúster. Las métricas adicionales le ayudan a determinar si el clúster de Kubernetes y los diferentes espacios de nombres y proyectos están por encima o por debajo del aprovisionamiento.

Monitorización de MongoDB

La monitorización de MongoDB DX APM permite monitorizar el rendimiento y la disponibilidad del entorno de MongoDB. La extensión del Agente de la infraestructura de MongoDB proporciona visibilidad en tiempo real de los recursos de la base de datos y ayuda a correlacionar las métricas de rendimiento de la aplicación, la infraestructura y la base de datos en una interfaz unificada.

Monitorización de Google Cloud Platform

La monitorización de Google Cloud Platform (GCP) DX APM monitoriza de forma remota el estado y el rendimiento de la infraestructura y los servicios de GCP. La monitorización de GCP es una extensión del Agente de la infraestructura que utiliza las API de Google Stackdriver para conectarse y detectar los recursos de GCP que se deben monitorizar. La monitorización de GCP es compatible con los siguientes servicios de GCP: Google Compute Engine, Google Cloud Storage, Google Cloud SQL y Google Cloud Filestore. Para obtener más información, consulte Monitorización de Google Cloud Platform.

Servicio AWS CloudTrail

El servicio CloudTrail DX APM de Amazon Web Services (AWS) le permite realizar tareas de cumplimiento, acciones de gobernanza, auditorías operativas y auditorías de riesgo en su cuenta de AWS. Se pueden realizar tareas de cumplimiento de la cuenta de AWS en función de la autoridad reguladora interna de la organización o de una autoridad reguladora de terceros. Para obtener más información, consulte Monitorización de Amazon Web Services.

Monitorización de AWS

La monitorización de AWS DX APM ahora es compatible con estos nuevos tipos de servicios: Elastic Load Balancing, Elastic Cache, Auto Scaling, Kinesis Data Streams, Billing, API Gateway, CloudTrail, Functions, Logic App, Redshift y Fargate. Para obtener más información, consulte Monitorización de Amazon Web Services.

Monitorización de Azure

La monitorización de Azure DX APM ahora es compatible con estos nuevos tipos de servicio: Azure Kubernetes Service, Cost Management, Load Balancer, Azure SQL, Azure Cosmos DB, Event Hub y Service Bus. Para obtener más información, consulte la sección sobre la monitorización de Azure.

Monitorización de la base de datos de SQL Server

La monitorización de la base de datos de SQL Server DX APM permite monitorizar el rendimiento y la disponibilidad del entorno de la base de datos de SQL Server. Esta extensión del Agente de la infraestructura se puede configurar y utilizar para recopilar las métricas de rendimiento de SQL Server que están relacionadas con las conexiones, el administrador de búferes, las estadísticas de índice, etc. La monitorización de SQL Server también proporciona métricas de clúster. Para obtener más información, consulte Monitorización de la base de datos de SQL Server.

Monitorización de Redis

Con la monitorización de Redis DX APM se puede monitorizar una única instancia de un servidor de Redis y varios clústeres.

Los dos componentes principales de un clúster de Redis son el nodo principal y el nodo subordinado. Los datos escritos en el nodo principal también se guardan en el nodo subordinado. La extensión del Agente de la infraestructura de la monitorización de Redis monitoriza tanto el nodo principal como el nodo subordinado. Cuando un nodo subordinado asciende a nodo principal, la monitorización de Redis detecta los cambios y refleja los cambios en la interfaz de usuario. Para obtener más información, consulte Extensión de monitorización de Redis.

Extensión de monitorización de ForgeRock

La extensión del Agente de Java de ForgeRock DX APM está disponible como parte de todos los Agentes de Java. La extensión monitoriza la plataforma de identidad de ForgeRock, que incluye los componentes de gestión de acceso y de la puerta de enlace de identidades. Para obtener más información, consulte Extensión de monitorización de ForgeRock.

Monitorización de GraphQL

DX APM ahora monitoriza el rendimiento de GraphQL, versión 14.x y superior, en Node.js. Se pueden consultar métricas basadas en las rutas de framework de GraphQL de Node.js y la información relacionada.

Mecanismo de conexión mejorado entre la monitorización de IBM WebSphere MQ y el servidor de MQ

DX APM ahora incluye una conexión de modo de enlaces entre la extensión del Agente de la infraestructura de monitorización de IBM WebSphere MQ y el servidor de MQ que reside en el mismo equipo. En este modo, DX APM no requiere ningún host, puerto ni detalles del canal para establecer una conexión con el servidor de MQ. Para obtener más información, consulte Configuración de la conexión del modo de enlaces.

DX APM también ha mejorado el proceso de autenticación de usuarios para conectar la monitorización de IBM WebSphere MQ y el servidor de MQ en el modo cliente-servidor. Ahora se puede ejecutar el script `RunMQCommands` y proporcionar los detalles de autenticación, lo que permite que cualquier usuario de Agente de la infraestructura acceda al servidor de MQ. Para obtener más información, consulte Configuración de la conexión cliente-servidor.

Compatibilidad con Amazon Linux

El Agente de la infraestructura es ahora compatible con estas versiones de Amazon Linux:

- Amazon Linux 2 AMI
- Amazon Linux AMI

Monitorización de la infraestructura de WebLogic

La monitorización de la infraestructura de WebLogic DX APM proporciona capacidades de monitorización de JMX para el servidor de WebLogic, incluidos todos los nodos de clúster. Para obtener más información, consulte Monitorización de la infraestructura de WebLogic.

Analizador de la carga empresarial

Cuando se descarga el Agente de BT Listener, se configuran automáticamente las propiedades siguientes:

- **btListener.output.channel.tenantId**: Esta propiedad se configura con el ID de cliente.
- **btListener.output.channel.url**: Esta propiedad se configura con la dirección URL de DXC.

Muestreo aleatorio dinámico

DX APM da un paso más hacia el muestreo inteligente completo. Se puede configurar el Agente de Java para recopilar dinámicamente los seguimientos de transacciones aleatorios en un período determinado para detectar diferentes tipos de transacciones. Se puede configurar el Agente de Java para recopilar los primeros N seguimientos de transacciones en un período determinado, un número específico de seguimientos de transacciones aleatorios de muestra en un período determinado, o ambos.

Compatibilidad con .NET Core 3.1

Ahora el Agente de .NET Core recopila datos sobre aplicaciones de .NET Core 3.1. Para obtener más información, consulte Agente de .NET/.NET Core y Microsoft .NET Core.

Funciones de IU

En esta sección se enumeran las funciones nuevas y mejoradas relacionadas con la interfaz de usuario.

Cuadros de mandos de la base de datos de Oracle DX APM

Se pueden consultar varios cuadros de mandos relacionados con el rendimiento de la base de datos de Oracle. Los cuadros de mandos de Oracle muestran las métricas relacionadas con el rendimiento de la base de datos y otras actividades de los usuarios que le ayudan a solucionar los problemas de la base de datos. Para obtener más información, consulte Cuadros de mandos de la base de datos de Oracle .

Rol de usuario avanzado en Team Center

Hemos incluido un rol de usuario avanzado que puede realizar operaciones CRUD en alertas, módulos de gestión, calculadoras y agrupaciones de métrica. Para obtener más información, consulte Permisos, aplicación de dominios y edición de elementos.

Visualización de las métricas de los agentes desconectados

Si se mueve la escala de tiempo hasta un intervalo de tiempo pasado y se visualiza un agente conectado en ese momento, se podrán ver las métricas correspondientes en la Vista contextual de mapa.

Importación de agentes existentes a APM Command Center

Ahora se puede importar un agente existente de CA APM 10.7 a APM Command Center mediante la utilidad de la herramienta de importación de agentes. Para obtener más información, consulte Herramienta de importación de agentes.

Columnas definidas por el usuario en los resultados de la búsqueda de métricas

Ahora se pueden mostrar u ocultar columnas para personalizar los resultados de la búsqueda de métricas. Para obtener más información, consulte Búsqueda de métricas en el Árbol de métrica.

Cambio de eventos en el modo en directo

En el modo de escala de tiempo **en directo**, se pueden ver los eventos de cambio relacionados con el estado, la topología y los atributos de un nodo. Para obtener más información, consulte Uso de la escala de tiempo y visualización de eventos de cambio.

Compatibilidad de proxy con el controlador del agente

Como administrador, se pueden configurar los detalles del proxy al configurar el conjunto del controlador del agente en APM Command Center. Para configurar el proxy, active y defina las propiedades siguientes en la página Configuración del controlador del 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

Si no se define ningún valor para la configuración, se tomará de `agentManager.httpProxy.username` en el paquete `em-connection`.

Para obtener más información sobre la configuración de las propiedades del conjunto, consulte Configuración de propiedades del conjunto e instrucciones de instalación en APM Command Center .

Integraciones

En esta sección se enumeran las nuevas y mejoradas integraciones de productos.

DX App Synthetic Monitor e integración con DX APM

Ahora se puede configurar la integración de DX App Synthetic Monitor (ASM) con DX APM en APM Command Center. La integración se ejecuta como parte del Agente de la infraestructura. Para obtener más información, consulte Configuración de DX App Synthetic Monitor para DX APM.

Configure los siguientes requisitos previos antes de utilizar las mejoras:

- `asm.metrics.logs=true` (para los pasos JMeter y Webdriver)
- `asm.metrics.download.full=true` (para los pasos JMeter y Webdriver)
- `asm.metrics.har.requests=true` (solo para los pasos de Webdriver)

También puede utilizar estas mejoras:

- Visualización de los pasos detallados de JMeter
Ahora, cuando el monitor de script ejecuta el script JMeter, se pueden ver los resultados de los pasos de JMeter en la Vista de métrica. Para ver los resultados del paso JMeter, establezca el valor `asm.reportJTLSubtree` como `true`.
- Visualización de los pasos detallados de Webdriver
Ahora, cuando el monitor de script ejecuta el script Webdriver, se pueden ver los resultados de los pasos de Webdriver en la Vista de métrica. Para ver los resultados de los pasos Webdriver, establezca el valor `asm.metrics.har.wdm` como `true`.
- Métrica de comprobación del último resultado
La nueva **Métrica de comprobación del último resultado** muestra el último estado de la comprobación del monitor. Estos son los estados que muestra la métrica:
 - 0: sin errores
 - 1: error
 - 2: modo de mantenimiento

Otras funciones

En esta sección se enumeran las demás funciones mejoradas.

Mejoras del Sistema de automatización de pruebas (TAS)

Se pueden utilizar estas mejoras del TAS:

- **TAS API v2:** Ahora se pueden ejecutar comandos para suprimir una parte del almacenamiento de topología de forma sincrónica o asincrónica.
- **Autenticación de usuarios activada para TAS/NASS:** El usuario que ha iniciado sesión con derechos de administrador de clientes o de administrador principal está autorizado para realizar llamadas a los puntos finales de TAS/NASS (almacenamiento de métricas).

Problemas conocidos

En esta sección se enumeran todos los problemas conocidos de la versión actual.

Defecto DE459955: incidencia del nombre de la base de datos RDS de Amazon Web Services

Válido para: DX APM SaaS 20.4

Síntoma: Se produce un problema de DX APM cuando no se asigna un nombre a una base de datos mientras se crea la instancia de AWS RDS. La incidencia hace que la correlación de la capa de la aplicación con la capa de la infraestructura no funcione en la instancia de la base de datos en el Agente de la infraestructura.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE457462: vínculo de configuración del Agente de PHP inactivo en el diálogo de descarga del agente

Válido para: DX APM SaaS 20.4

Síntoma: En la página del diálogo de descarga del agente para el Agente de la infraestructura de DX APM, el vínculo que se ha proporcionado para acceder a los detalles de la configuración completa del Agente de PHP está inactivo y muestra el error 404.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE457423: Instrucciones incorrectas en el diálogo de descarga del agente para la monitorización de WebLogic del Agente de la infraestructura

Válido para: DX APM SaaS 20.4

Síntoma: En la página del diálogo de descarga del agente para la descarga del Agente de la infraestructura, la página de instrucciones de instalación del monitor de WebLogic contiene un error de contenido. En la sección **Monitor de infraestructura de WebLogic DX APM**, las instrucciones para copiar los archivos JAR no son correctas.

Solución: Utilice estas instrucciones para copiar correctamente los archivos JAR.

Siga estos pasos:

1. Vaya al directorio `<WL_HOME>/lib`.
`WL_HOME` es el directorio en el que está instalado WebLogic Server.
2. Copie el archivo `wlthint3client.jar`.
3. Pegue el archivo `wlthint3client.jar` en el directorio `<APMIA_Home>/lib/`.

Defecto DE456625: Los cambios realizados en el archivo Config.json se han perdido tras instalar la sonda Node.js

Válido para: DX APM SaaS 20.4, NodeJS Probe versión 1.10.83

Síntoma: Después de instalar la sonda más reciente de la aplicación Node.js, todos los cambios realizados en el archivo `config.json` se pierden.

Solución: Antes de instalar la sonda más reciente de la aplicación Node.js, realice las tareas siguientes.

Siga estos pasos:

1. Busque el archivo `config.json` desplazándose a la siguiente ubicación del sistema en el que se ha instalado la aplicación Node.js:
`<Node.js_Installation_Folder>\node-modules\ca-apm-probe\`
2. Realice una copia de seguridad del archivo `config.json`.
3. Instale la sonda Node.js más reciente. Para ello, ejecute el siguiente comando en el sistema en el que se ha instalado la aplicación Node.js:
`npm i ca-apm-probe`
4. Vaya a la siguiente ubicación del sistema en el que se ha instalado la aplicación Node.js:
`<Node.js_Installation_Folder>\node-modules\ca-apm-probe\`
5. Introduzca las nuevas propiedades del archivo `config.json` más reciente en la copia de seguridad del archivo `config.json` (consulte **Paso 2**).
6. Inicie la aplicación Node.js.

Defecto DE456154: problema al correlacionar los back-ends con los front-ends para la aplicación Node.js

Válido para: DX APM SaaS 20.4, NodeJS Probe versión 1.10.83

Síntoma: Cuando los front-ends de la aplicación Node.js llaman de forma asíncrona a más de un back-end, la correlación no funciona en la Vista de métrica ni en el mapa. Sin embargo, la correlación de back-ends con front-ends funciona según lo previsto en los seguimientos de transacciones.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE456144: los valores de configuración de la decoración del atributo no se han cargado en el inicio del Node.js

Válido para: DX APM SaaS 20.4, NodeJS Probe versión 1.10.83

Síntoma: Cuando se inicia la aplicación Node.js, los valores de configuración del archivo `config.json` para Automatic Attribute Decoration de Node.js no se cargan en la sonda Node.js.

Solución: Realice las tareas siguientes para cargar los valores de configuración de Automatic Attribute Decoration.

Siga estos pasos:

1. Confirme que el Agente de la infraestructura esté instalado.

2. Instale NodeJS `ca-apm-probe` e inicie la aplicación Node.js con NodeJS Probe.
3. Asegúrese de configurar la clave de API pública en el archivo `introscopeAgent.profile` del Agente de la infraestructura. Para configurarla, actualice la propiedad siguiente en el archivo `introscopeAgent.profile` tras acceder a la ubicación de la carpeta, `\apmia\core\config\`:
`attribute.decoration.apm.access.token`
4. Abra el archivo `config.json`. Para ello, vaya a la siguiente ubicación en el sistema en el que ha instalado la aplicación Node.js y NodeJS `ca-apm-probe`:
`<Node.js_Installation_Folder>\node-modules\ca-apm-probe\`
5. Actualice el archivo `config.json`.

NOTE

Nota: Asegúrese de que edita el archivo `config.json` con algunos cambios (como, por ejemplo, la inserción de un espacio).

6. Guarde el archivo `config.json`.

Defecto DE454550: el nodo de back-end de MongoDB se muestra como un back-end genérico en el mapa

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

Síntoma: El nodo back-end de MongoDB debería mostrarse como una base de datos inferida con Node.js en el mapa. Sin embargo, el nodo back-end de MongoDB se muestra como un back-end genérico.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE450621: error en el comando de ejecución de Python Django

Válido para: DX APM 20.4, Python 3.x

Síntoma: El siguiente comando de ejecución no funciona en el sistema en el que se ha instalado la aplicación Python Django:

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

Solución: Utilice el siguiente comando de ejecución en el sistema en el que se ha instalado la aplicación Python Django:

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

Defecto DE450599: Se muestra un Agente desconocido de Python Django en la Vista de métrica

Válido para: DX APM 20.4, Python 3.x

Síntoma: Cuando se inicia el Agente de la infraestructura de DX APM, se muestra un agente desconocido en la Vista de métrica.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE450618: error de visualización de las métricas de las direcciones URL de Python Django

Válido para: DX APM 20.4, Python 3.x

Síntoma: Cuando se conecta la aplicación Python Django al Agente de la infraestructura y se explora la aplicación Python Django. Cada métrica de la dirección URL (punto final) de la aplicación Python Django se muestra dos veces en la Vista de métrica.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE449130: No se puede iniciar sesión mediante la cuenta de SAML

Válido para: DX APM 20.1, 20.4

Síntoma: El usuario no puede iniciar sesión con los datos de la cuenta de SAML.

Solución: Genere un token público e inicie sesión con el token.

Defecto DE438579: La correlación de la monitorización del host con el nodo de integración de IIB no funciona**Válido para:** DX APM SaaS 20.4**Síntoma:** La correlación de la monitorización del host con el nodo de **integración** de IBM Integration Bus (IIB) no funciona cuando se activa la capacidad de monitorización del host de la infraestructura de IIB.**Solución:** No existe ninguna solución alternativa para esta incidencia.**Defecto DE405769: La correlación de Mule ESB 3.x con el proxy no funciona****Válido para:** DX APM SaaS 20.4, Mule ESB 3.x**Síntoma:** Una aplicación anidada utiliza la correlación de la aplicación Mule ESB 3.x con el proxy. La correlación no funciona en el mapa ni en los seguimientos de transacciones.**Solución:** No existe ninguna solución alternativa para esta incidencia.

20.1

Estas son las funciones nuevas, modificadas y rechazadas en DX APM 20.1.

Funciones del agente

Complemento del servidor web de Nginx

El analizador de la carga empresarial incluye ahora un complemento para el servidor web de Nginx. Para obtener más información sobre la instalación y la configuración, consulte la sección Instalación y configuración del complemento del servidor web de Nginx.

Ahora se puede implementar toda la funcionalidad del Agente de monitorización universal para Kubernetes mediante un operador de servicio de Kubernetes.

Utilice el operador de servicio Kubernetes para implementar el Agente de monitorización universal para Kubernetes

Ahora se puede implementar toda la funcionalidad del Agente de monitorización universal para Kubernetes mediante un operador de servicio de Kubernetes.

Soporte de OpenTracing

DX APM ahora ofrece soporte de monitorización para las aplicaciones de OpenTracing. El soporte de OpenTracing informa sobre las métricas de rendimiento de la aplicación y los seguimientos de transacciones que se recopilan de las aplicaciones que se instrumentan con Jaeger. DX APM proporciona compatibilidad con OpenTracing como extensión de un Agente de la infraestructura. Para obtener más información, consulte Soporte de OpenTracing.

Instalación del Agente de la infraestructura en AIX

Ahora se puede descargar e instalar el Agente de la infraestructura en la plataforma AIX. Para obtener más información, consulte Instalación del Agente de la infraestructura en DX APM.

Compatibilidad con Python 3.x

El Agente de Python ahora es compatible con Python 3.x y admite la correlación tanto entrante como saliente. Ahora se puede ver la correlación de flujos entrantes en la aplicación Python con flujos salientes de la aplicación Python.

Correlación compatible

- **Correlación entrante:** si hay alguna llamada procedente del flujo entrante (Java o Python) a la aplicación Python, los agentes correspondientes instrumentan los dos flujos.
- **Correlación saliente:** si hay alguna llamada procedente de la aplicación de Python al subdirectorio (Java o Python), los agentes correspondientes instrumentan los dos flujos.

Correlación saliente mediante el módulo de solicitud

El módulo **Solicitudes** es el estándar para realizar solicitudes HTTP en Python. Si alguna aplicación de Python invoca el módulo de solicitud en la sonda Python, se notifica a la sonda y se muestran los seguimientos correspondientes.

Correlación saliente mediante el módulo Urllib

Urllib.request es el módulo que permite recuperar direcciones URL (localizadores uniformes de recursos) en Python. El módulo urllib.request define funciones y clases que ayudan a abrir direcciones URL (principalmente HTTP) en Python. Si alguna aplicación Python invoca este módulo en la sonda Python, se notifica a la sonda y se muestran los seguimientos correspondientes.

Compatibilidad con aplicaciones Python en contenedores de Docker

Ahora se puede utilizar el Agente de Python para monitorizar la estructura de Django y las aplicaciones de Python con estructura Flask.

Servicio AWS CloudTrail

El servicio AWS CloudTrail le permite realizar el cumplimiento, la gobernanza, la auditoría operativa y la auditoría de riesgos de su cuenta de AWS. Puede realizar el cumplimiento de su cuenta de AWS de dos maneras distintas. Se puede obtener el cumplimiento en función de la autoridad reguladora interna de la organización o de una autoridad reguladora de terceros.

Monitorización de IIB Infra

Se puede utilizar la monitorización del bus de integración de IBM (IIB) para monitorizar el estado y la disponibilidad de IIB y los flujos de mensajes correspondientes. Como requisito previo, debe utilizar uno de los siguientes componentes: MQTT, que está integrado en IIB o IBM MQ. La extensión de monitorización de IIB se conecta con uno de los componentes para recopilar las métricas de las estadísticas de IIB. Para obtener más información, consulte Monitorización de IIB.

Monitorización de la base de datos de SQL Server

La monitorización de la base de datos de SQL Server permite monitorizar el rendimiento y la disponibilidad del entorno de la base de datos de SQL Server. Configure y utilice esta extensión para recopilar las métricas de rendimiento de SQL Server que están relacionadas con las conexiones, el administrador de búferes, las estadísticas de índice, etc. Para obtener más información, consulte Monitorización de la base de datos de SQL Server.

Monitorización de la base de datos de MySQL

La monitorización de la base de datos de MySQL permite monitorizar el rendimiento y la disponibilidad del entorno de la base de datos de MySQL. Esta extensión proporciona visibilidad en tiempo real de los recursos críticos de la base de datos. Estos recursos incluyen los bytes enviados y recibidos; conexiones intentadas, anuladas o erróneas; información de InnoDB; operaciones de la base de datos; utilización de recursos y más. Para obtener más información, consulte Monitorización de la base de datos de MySQL.

Soporte de seguimiento de transacciones para la base de datos de Oracle, Oracle RAC y Oracle EBS

DX APM admite la recopilación de seguimientos de la base de datos basada en eventos para las siguientes extensiones de base de datos: base de datos Oracle, Oracle Real Application Clusters (RAC) y Oracle E-Business Suite (EBS).

Las extensiones de base de datos proporcionan seguimientos de base de datos basados en el servicio de base de datos específico. Los seguimientos de la base de datos proporcionan información sobre los indicadores de rendimiento. Los seguimientos también muestran detalles y estadísticas de la recuperación, la espera, el análisis de SQL y la utilización de recursos mientras que la base de datos correspondiente ejecuta las transacciones de la base de datos para una transacción empresarial concreta.

Compatibilidad con la estructura Koa.js para Node.js

El Agente de Node.js es compatible con Koa.js, la estructura web de próxima generación de Node.js.

Soporte de monitorización de NGINX

La extensión del Agente de monitorización de NGINX permite monitorizar la versión de los servicios alojados de NGINX. Se puede utilizar esta extensión junto con otras extensiones existentes para monitorizar el control de la infraestructura de NGINX y el rendimiento de los servicios alojados en la versión de los servicios alojados de NGINX. Para obtener más información, consulte Monitorización de NGINX.

Compatibilidad mejorada con las aplicaciones principales de .NET

DX APM ahora es compatible con la monitorización de transacciones básicas de .NET asíncronas.

Métricas de desplazamiento de consumidores y retraso de la monitorización de Kafka

Ahora, la monitorización de Kafka informa sobre el rendimiento de los desplazamientos de los grupos de consumidores de Kafka. La monitorización de Kafka utiliza las métricas **Desplazamiento actual** y **Retraso** para cada grupo de consumidores cuando la aplicación de Kafka experimenta un rendimiento lento. Estas métricas pueden ayudarle a determinar si el rendimiento lento de Kafka se debe a que los consumidores no leen los mensajes lo suficientemente rápido, lo que genera mensajes sin leer.

Compatibilidad mejorada con Java 11

El Agente de Java ahora monitoriza las aplicaciones de Java 11 sin necesidad de pasar argumentos de línea de comandos adicionales al comando `-javaagent`.

Mejoras en la monitorización de correlación de registros

La monitorización de la correlación de registros ahora es compatible con log4j2. Ahora se puede definir el parámetro `com.ca.apm.log.correlation.mdc.insert.before` con `%m%n` y `%msg` al mismo tiempo. Se pueden definir también varios patrones para el parámetro `com.ca.apm.log.correlation.mdc.insert.before`.

Compatibilidad con aplicaciones Akka y Play

DX APM incluye una extensión de Agente de Java que informa sobre la estructura de rendimiento de Play y Akka. Esta extensión informa de las métricas de rendimiento de Akka, front-end, back-end, correlación y controlador de reproducción.

Monitorización de Prometheus

El Agente de la infraestructura incluye ahora la monitorización de Prometheus, que permite a DX APM ingerir de manera remota las métricas de Prometheus. Se pueden configurar las propiedades del archivo de configuración para recopilar métricas directamente desde un back-end de Prometheus. Por ejemplo, se puede configurar el tipo de métrica, la consulta de métrica, etc. Se puede configurar también la monitorización de Prometheus para recopilar métricas de un exportador de Prometheus.

Monitorización de JMX remoto

El Agente de la infraestructura incluye una nueva extensión de monitorización de JMX remoto. Esta extensión permite monitorizar de forma remota el rendimiento de las aplicaciones Java en JMX sin necesidad de ningún instrumental de aplicaciones directo. Las métricas de rendimiento de JMX se correlacionan con otras métricas de rendimiento, como el rendimiento de las aplicaciones y la infraestructura. Para obtener más información, consulte Monitorización de JMX remoto.

Monitorización de Couchbase

El Agente de la infraestructura incluye una nueva extensión de monitorización de Couchbase. Esta extensión permite monitorizar el rendimiento de Couchbase, incluida la monitorización de un clúster. Para obtener más información, consulte Monitorización de Couchbase.

Modos de monitorización del Agente de Java

El Agente de Java tiene un nuevo modo de monitorización que se puede establecer como **Ninguno**. El modo Ninguno es el modo mínimo del agente, ya que cierra la mayor parte de la funcionalidad y las métricas. Se puede cambiar el modo en tiempo de ejecución sin que sea necesario reiniciar el servidor de aplicaciones.

Mejora de la visibilidad del rendimiento de las aplicaciones .NET

El Agente de NET ahora recopila automáticamente los seguimientos de pila. Los seguimientos de pila contienen toda la pila de llamadas a métodos de aplicación .NET. Los seguimientos de pila se muestran como instantáneas en los seguimientos de transacciones.

Compatibilidad de la aplicación PHP en el contenedor del Docker

El Agente de PHP ahora es compatible con la monitorización de PHP CLI. Se puede utilizar el Agente de PHP para monitorizar los scripts de PHP que se ejecutan desde otro script de PHP.

Compatibilidad de la aplicación Node.js en los contenedores de Docker

El Agente de Node.js permite monitorizar la aplicación Node.js junto con las bases de datos que se conectan a la aplicación Node.js. Por ejemplo, las bases de datos de PostgreSQL, MongoDB y MySQL.

Funciones de IU

API para la descarga del agente disponible desde APM Command Center

Ahora se puede utilizar la API de APM Command Center para descargar los paquetes más recientes desde APM Command Center y personalizar el comportamiento de la descarga definiendo las propiedades obligatorias. Por ejemplo, durante la descarga se puede personalizar la carga y establecer determinadas propiedades como ocultas. Para obtener más información, consulte API de APM Command Center.

Agente de Java para microservicios en APM Command Center

Ahora se puede crear y descargar el Agente de Java para los microservicios desde APM Command Center. Para obtener más información, consulte Implementación de paquetes del agente mediante APM Command Center.

Filtro de la Vista de métrica mediante atributos

En la Vista de métricas, se pueden definir ahora los filtros para los agentes en función de sus atributos.

Mejora de las calculadoras

Ahora se pueden crear calculadoras que capturan los valores de una agrupación de métrica como entrada y promedio, o suma de los valores. Las calculadoras envían el valor resultante como una métrica personalizada en el Explorador de métricas. Las métricas generadas por la calculadora aparecen en un proceso virtual denominado **Proceso de métrica personalizada**. El proceso de métrica personalizada se ejecuta en un host virtual que se denomina **Host de métrica personalizada**. Para obtener más información, consulte Creación y edición de calculadoras.

Ejecución de consultas mediante la API de REST

Ahora se pueden utilizar las siguientes API de REST para consultar las métricas y los datos relacionados:

- API de REST de consulta de métrica

La API de consulta de métricas consulta las métricas para diferentes intervalos de tiempo, frecuencias y métricas. Al igual que otras API de REST de APM, la interfaz de la API de REST de consulta de métrica utiliza la autenticación basada en token. Para obtener más información, consulte la sección API de REST de consulta de métrica.

- API de REST de Team Center

La API de REST de Team Center proporciona diversas funciones de consulta de datos, tanto de métricas como de nivel de cuadro de mandos. Al igual que otras API de REST de DX APM, la interfaz de la API de REST de Team Center utiliza la autenticación basada en token. Para obtener más información, consulte API de REST de Team Center.

Importación y exportación de definiciones de paquetes de agentes desde APM Command Center

Ahora se pueden importar y exportar definiciones de paquetes de agente de un cliente a otro. Para obtener más información, consulte Implementación de paquetes del agente mediante APM Command Center.

Funciones y compatibilidad en desuso

DX APM ya no es compatible con las siguientes funciones y funcionalidades:

- Workstation de línea de comandos
- Python 2.7
- ChangeDetector
- Instrumentación dinámica
- Enterprise Team Center
- Capacidad de montaje/desmontaje del agente.

Los agentes están siempre disponibles en DX APM, por lo tanto ya no es necesario montar y desmontar agentes.

- La propiedad del sistema `-DagentProfile` del Agente de Java ya no es compatible.

Problemas conocidos

Defecto DE449471: La dirección URL de la vista de aislamiento del Agente de la infraestructura no se abre

Válido para: DX APM 20.1

Síntoma: La vista de **aislamiento** no se genera para el Agente de la infraestructura. Esta situación se produce cuando se accede desde **Cuadros de mandos**, **Agente**, **Agregar filtro**, se selecciona el nombre de host del Agente de la infraestructura en la lista desplegable y, a continuación, se selecciona **Capa de la aplicación**.

Solución: En función de la definición de alerta, defina manualmente el filtro correcto en el mapa.

Defecto DE449130: No se puede iniciar sesión mediante la cuenta de SAML

Válido para: DX APM 20.1

Síntoma: El usuario no puede iniciar sesión con los datos de la cuenta de SAML.

Solución: Genere un [token público](#) e inicie sesión con el token.

Defecto DE440008: Al seleccionar un seguimiento el panel de seguimiento de las transacciones vuelve al principio

Válido para: DX APM 20.1

Síntoma: Este problema ocurre cuando hay muchos seguimientos en el panel de seguimiento de transacciones del Visor de seguimiento de transacciones. Tras desplazarse por el panel y seleccionar un seguimiento, el panel de seguimientos de transacciones vuelve al principio.

Solución: Desplácese hacia abajo en el panel de seguimiento de transacciones y busque el seguimiento con un borde.

Defecto DE450933: Error de monitorización de OpenShift

Síntoma: Quiero descargar la monitorización de OpenShift desde el cuadro de diálogo de descarga de APM SaaS APM. Hago clic en **OpenShift** en la **categoría Nube nativa**. Al seguir las instrucciones y ejecutar el comando `oc create -f caagent-openshiftmonitor.yml`, aparece un error.

¿Cómo puedo resolver el problema?

Solución: En el archivo `caagent-openshiftmonitor.yml`, elimine la propiedad `- name: dev & readOnly: true`. Ejecute este comando:

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

Defecto DE432585: Los valores de la métrica estadística de los recursos de monitorización del bus de integración de IBM se muestran como acumulativos

Síntoma: Los valores de métrica de la monitorización del bus de integración de IBM (monitorización del IIB) para las estadísticas de recursos se muestran como **Acumulativos** en lugar de **Por intervalo**.

Solución: No existe ninguna solución alternativa para esta incidencia.

Defecto DE448777: Estadísticas de recursos y flujo de mensajes de monitorización del bus de integración de IBM sin notificar

Síntoma: Al reiniciar el QM suscrito, el flujo de mensajes del bus de integración de IBM (IIB) y las estadísticas de recursos no se registran en DX APM.

Solución: Reinicie el Agente de la infraestructura de DX APM.

Defecto DE448618: El complemento de Jenkins falla en el entorno DX SaaS

Síntoma: El complemento de Jenkins, `em.url`, no funciona en DX SaaS después de actualizar a DX APM.

Solución: Al actualizar el entorno DX SaaS, se debe actualizar el valor de EM URL en el archivo `performance-comparador.properties`.

Siga estos pasos:

1. Inicie sesión en DX SaaS.
2. Haga clic en **Abrir** en el cuadro **DX APM**. Aparecerá la página de inicio de DX APM. La página de inicio muestra la dirección URL utilizada para acceder a DX APM en el explorador web.
3. Vaya a `<Jenkins Workspace>\<jenkins-job name>\properties\`.
4. Abra el archivo `performance-comparator.properties`.
5. Actualice el valor de la propiedad `em.url` con el EM URL más reciente.

Notas de la versión de 2019

Esta sección contiene las Notas de la versión de 2019.

- [Noviembre de 2019](#)
- [Octubre de 2019](#)
- [Agosto de 2019](#)

Noviembre de 2019

Novedades del 26 de noviembre de 2019

Métricas del Agente de la infraestructura para RedHat

Ahora puede ver las métricas del servidor RedHat sobre la CPU, los discos, el sistema de archivos, la memoria, la red, los procesadores, la paginación, el SWAP, el rendimiento del sistema, etc. *Monitorización reactiva de Spring Boot*

Esta nueva extensión del Agente de Java monitoriza las aplicaciones reactivas de Spring Boot. La extensión instrumenta específicamente los servidores HTTP asíncronos Netty, los clientes HTTP asíncronos Netty y las estructuras centrales del Springboot Reactor para proporcionar una correlación entre subprocesos y un seguimiento de componentes asíncronos. Para obtener más información, consulte *Monitorización reactiva de aplicaciones de Spring Boot*.

Monitorización de Oracle RAC

La extensión Oracle RAC permite monitorizar el rendimiento y la disponibilidad de su entorno Oracle Real Application Clusters (Oracle RAC). Se puede utilizar la extensión de Oracle RAC para localizar si algún servicio de una base de datos de clúster tiene problemas de disponibilidad. La extensión Oracle RAC proporciona visibilidad en tiempo real de los recursos críticos de la base de datos como, por ejemplo, interbloqueos, exploraciones completas de tablas, archivos de registro de rehacer, segmentos de reversión, etcétera.

Se puede configurar la extensión Oracle RAC para recopilar las métricas de rendimiento de Oracle RAC con el fin de ayudarle a monitorizar el entorno de Oracle RAC. Puede obtener una rentabilización inmediata en cuadros de mandos preconfigurados y en alertas que se activan por el rendimiento que le informan proactivamente sobre posibles infracciones del acuerdo de nivel de servicio antes de que los usuarios finales se vean afectados. Para obtener más información, consulte *Monitorización de Oracle RAC*.

Monitorización de Oracle EBS

La extensión Oracle E-Business Suite (EBS) permite monitorizar el rendimiento y la disponibilidad de los siguientes componentes de Oracle EBS: los gestores simultáneos, los programas simultáneos y el gestor de resolución de conflictos. Se puede utilizar la extensión Oracle EBS para revisar las tareas simultáneas, los gestores simultáneos tanto en el nivel de clúster como en el nivel de nodo individual. Para obtener más información, consulte Monitorización de Oracle EBS.

Monitorización de IIB

Se puede utilizar la monitorización del bus de integración de IBM (IIB) para monitorizar el estado y la disponibilidad de las aplicaciones conectadas al IIB y los flujos de mensajes correspondientes. Como requisito previo, IBM MQ debe ejecutarse para que la extensión de monitorización del IIB se pueda conectar con IBM MQ y recopilar las métricas de las estadísticas del IIB. Para obtener más información, consulte Monitorización de IIB.

Extensión OkHttp

El Agente de Java ahora es compatible con la monitorización de OkHttp. OkHttp representa un cliente HTTP eficaz que es compatible con el protocolo HTTP/2. Este protocolo carga datos de forma eficaz y ahorra ancho de banda. Para obtener más información, consulte Extensión OkHttp.

Métrica de monitorización del host

Además de las métricas de monitorización del host existentes compatibles con DX APM, se agregan las nuevas métricas de monitorización del host para Solaris y RedHat. Para obtener más información, consulte Monitorización del host.

Soporte de monitorización de NGINX

La extensión del Agente de monitorización de NGINX permite monitorizar las siguientes versiones del servidor NGINX: NGINX-Plus y NGINX Community. Se puede utilizar la extensión para monitorizar la monitorización de la infraestructura de NGINX. Para obtener más información, consulte Monitorización de NGINX.

Carga de instrumentación dinámica del Agente de NET

El Agente de .NET ahora puede cargar de forma dinámica la instrumentación sin que sea necesario reiniciar la aplicación. A continuación aparecen algunos ejemplos:

- Se puede instrumentar un método específico que no coincida con la definición de una sonda existente. En concreto, se pueden instrumentar métodos de MVC asíncronos sin necesidad de reiniciar.
- DX APM puede volver a evaluar los métodos y modificar la instrumentación cuando realice estas acciones:
 - Coloque un archivo .pbd nuevo en la carpeta **hotdeploy**
 - Cambie o elimine un archivo .pbd existente.

Servicios de AWS y Azure

- La nueva extensión de Amazon Web Services (AWS) es compatible con los siguientes tipos de servicios nuevos: informática, almacenamiento, mensajería, base de datos, análisis y servicios móviles. Para obtener más información, consulte Monitorización de Amazon Web Services.
- La nueva extensión de los servicios de Azure admite los siguientes tipos de servicios nuevos: informática, almacenamiento y análisis. Para obtener más información, consulte la sección sobre la monitorización de Azure.

Problema conocido del Agente de la infraestructura

Defecto DE437143: No hay métricas de monitorización del host

Válido para: DX APM 10.7 Service Pack 1 (SP1-3), DX APM, 11.1.3, Kubernetes y Host Monitor

Síntoma:

No se muestra ninguna métrica en el nodo **SystemEdge** en la **Vista de métrica**. Este problema se produce en las siguientes circunstancias:

- Host Monitor se vuelve a instalar mediante el Agente de monitorización universal.
- El proceso de CA SystemEdge no se ha finalizado, incluso cuando Kubernetes destruye el pod correspondiente.

Solución:**Siga estos pasos:**

1. Inicie sesión en el nodo **SystemEdge** en el que no aparece ninguna métrica de Host Monitor.
2. Utilice este comando para finalizar el proceso SystemEDGE si se está ejecutando: `ps -ef | grep "SystemEDGE" | grep -v grep.`
3. Vuelva a implementar el Agente de monitorización universal.

Octubre de 2019

Novedades del 10 de octubre de 2019*Fichas adicionales del Explorador de métrica*

Estas nuevas fichas muestran los seguimientos y los errores relacionados con una transacción comercial.

- Ficha **Seguimientos**: en esta ficha se enumeran las transacciones comerciales y los detalles de los componentes y seguimientos asociados.
- Ficha **Errores**: en esta ficha se enumeran las transacciones comerciales que contienen errores.

Problema conocido del Agente de la infraestructura

Defecto DE437143: No hay métricas de monitorización del host

Válido para: DX APM 10.7 Service Pack 1 (SP1-3), DX APM, 11.1.3, Kubernetes y Host Monitor

Síntoma:

No se muestra ninguna métrica en el nodo **SystemEdge** en la **Vista de métrica**. Este problema se produce en las siguientes circunstancias:

- Host Monitor se vuelve a instalar mediante el Agente de monitorización universal.
- El proceso de CA SystemEdge no se ha finalizado, incluso cuando Kubernetes destruye el pod correspondiente.

Solución:**Siga estos pasos:**

1. Inicie sesión en el nodo **SystemEdge** en el que no aparece ninguna métrica de Host Monitor.
2. Utilice este comando para finalizar el proceso SystemEDGE si se está ejecutando: `ps -ef | grep "SystemEDGE" | grep -v grep.`
3. Vuelva a implementar el Agente de monitorización universal.

Agosto de 2019

Novedades del 31 de agosto de 2019*Compatibilidad con AdoptOpenJDK*

CA Technologies, una empresa Broadcom, está avanzando hacia la incorporación de más tecnologías de código abierto en sus productos. Como parte de esta estrategia, varios productos han empezado a utilizar implementaciones de código abierto de Java. Para alinearse con esta dirección corporativa, DX APM ha incorporado AdoptOpenJDK (11), en sustitución de Oracle JDK.

Problema conocido del Agente de la infraestructura

Defecto DE437143: No hay métricas de monitorización del host

Válido para: DX APM 10.7 Service Pack 1 (SP1-3), DX APM, 11.1.3, Kubernetes y Host Monitor

Síntoma:

No se muestra ninguna métrica en el nodo **SystemEdge** en la **Vista de métrica**. Este problema se produce en las siguientes circunstancias:

- Host Monitor se vuelve a instalar mediante el Agente de monitorización universal.
- El proceso de CA SystemEdge no se ha finalizado, incluso cuando Kubernetes destruye el pod correspondiente.

Solución:**Siga estos pasos:**

1. Inicie sesión en el nodo **SystemEdge** en el que no aparece ninguna métrica de Host Monitor.
2. Utilice este comando para finalizar el proceso SystemEDGE si se está ejecutando: `ps -ef | grep "SystemEDGE" | grep -v grep .`
3. Vuelva a implementar el Agente de monitorización universal.

Novedades del 3 de agosto de 2019*Analizador de la carga empresarial*

El Analizador de la carga empresarial es un sistema de monitorización de la experiencia del usuario final que le permite extraer los servicios para obtener información sin tener que volver a crear las aplicaciones. El Analizador de la carga empresarial proporciona un sofisticado mecanismo de generación de informes y recopilación de datos para realizar un seguimiento de los flujos de trabajo de los servicios en el centro de datos. El Analizador de carga empresarial examina la aplicación monitorizada y recopila las transacciones y métricas empresariales para calcular las métricas de rendimiento. Estas métricas proporcionan información acerca de la experiencia de usuario. La recopilación de datos es automática y no es necesaria ninguna personalización de las aplicaciones. Sin embargo, el administrador de aplicaciones puede configurar el sistema a través de la interfaz de usuario para realizar cualquier monitorización personalizada. Las siguientes funciones clave están disponibles en esta versión del Analizador de la carga empresarial:

- Compatibilidad con la captura de cargas desde IIS (.NET) y los servidores web de Apache Tomcat.
- Compatibilidad inmediata con la captura de URL, encabezados HTTP y formularios HTML.
- Se ha programado el modo de detección periódica para actualizar el modelo de ciencia de datos de la frecuencia de resultados de campo y valor.
- Detección y resaltado automáticos basados en el aprendizaje automático de los valores de datos más importantes, que se definen como parámetros de identificación.
- Identificación de la segmentación de usuarios y de las denominaciones de las transacciones comerciales dinámicas (BT). Es decir, etiquetas demográficas como el valor de la cesta de la compra, el balance de la cuenta y el ID de usuario.
- Capacidad de ajustar la categorización de la ciencia de datos de los campos de carga útil capturados en una interfaz gráfica fácil de utilizar.
- Soporte de administrador para el cambio de nombre y la captura parcial de campos complejos, como cookies.
- Integración de topología de DX APM.
 - El Analizador de la carga empresarial ha detectado que las transacciones comerciales aparecen como elementos de usuario final en la asignación de la aplicación.
 - El Analizador de la carga empresarial ha detectado que las transacciones comerciales aparecen en los seguimientos del Visor de transacciones comerciales de Team Center.
 - La información demográfica del usuario del Analizador de la carga empresarial se comunica como parámetros de seguimiento en el Visor de transacciones comerciales de Team Center.
 - El Analizador de la carga empresarial ha detectado que las transacciones comerciales notifican las métricas de estado y rendimiento en el visor de métrica de Team Center.

Procedimientos iniciales

Realice los primeros pasos con DX APM:

Si desea...	Realice lo siguiente...	Lea esto...
Obtener información sobre Application Performance Management a través de vídeos.	Vaya a los canales de YouTube de CA Technologies y CA Educate en las listas de reproducción de APM.	Recursos de vídeo para los analistas
Mejorar el conocimiento y la productividad de Application Performance Management.	Realice un curso de aprendizaje de CA Education, siga una ruta de aprendizaje o realice una formación.	Formación y educación de DX APM
Familiarizarse con los términos de Application Performance Management.	Busque los términos y lea sus definiciones en el glosario.	Glosario

NOTE

Para descargar y configurar Cloud Proxy, consulte la documentación de [Cloud Proxy](#).

Soporte y compatibilidad

La página del producto DX APM en el sitio web de [Soporte de CA o Broadcom](#) proporciona el software y la documentación para todas las versiones.

Para obtener información sobre el sistema, información sobre el entorno operativo y las versiones compatibles, póngase en contacto con Soporte de Broadcom.

Arquitectura de DX APM

Un entorno de pruebas de DX APM se basa en los siguientes componentes de la arquitectura:

- **Cliente:** un grupo de usuarios que comparten el acceso con privilegios específicos a la instancia de software.
- **Servicio:** Un modelo de entrega de software en el que el software tiene una licencia de suscripción. El software está alojado de forma centralizada.
- **Pod de OpenShift:** uno o varios contenedores que se implementan conjuntamente en un host. Un pod es la unidad más pequeña que se define, implementa y gestiona.
- **Contenedor:** un único contenedor de DX APM que reúne Enterprise Manager, Demo Application y el controlador de carga.

Un contenedor se asigna a pods de OpenShift específicos y estos se ejecutan en unos nodos de OpenShift determinados. Por lo tanto, en el entorno de pruebas, la cardinalidad de Cliente - Servicios - Pod - Contenedor es: 1 - 1 - 1 - 1. Broadcom mantiene un conjunto pod inicializado para acelerar el proceso de incorporación de clientes. Tras la correcta introducción, se asigna un pod que ya está en ejecución y se asigna al cliente y la agrupación obtiene un nuevo pod. Estos pods agrupados estarán inactivos hasta que se les asigne un cliente.

La arquitectura incluye los siguientes elementos clave:

- **Redes**
La comunicación de datos y de consulta de cliente se efectúa mediante HTTPS (443). Todos los datos del cliente y el tráfico de consultas se multiplexa en una única conexión, por lo tanto, el tráfico de todo el sistema se dirige a *.apm.cloud.ca.com. Este sitio aloja un enrutador OpenShift. El enrutador OpenShift utiliza el segmento menos significativo de la dirección de destino, que lleva un identificador de cliente único en el punto final del servicio demux.

Utilice una lista de elementos permitidos para el sistema de nombres de dominio (DNS) público *.apm.cloud.ca.com y no dependa de las direcciones IP porque cambian con frecuencia.

- **Almacenamiento de configuración y datos del cliente**

DX APM almacena distintos tipos de datos de monitorización y estructuras de configuración. Todos estos tipos se externalizan para que los contenedores no tengan ningún estado para facilitar las actualizaciones. Desde un punto de vista estructural, se almacenan dos tipos de datos: los relacionales y los basados en archivos. Los datos relacionales se almacenan en instancias de Google Cloud Platform.

- **Gestión de servicios - Motor de aprovisionamiento**

OpenShift es el motor de aprovisionamiento. Este microservicio de Java recibe los eventos de gestión y el ciclo de vida de los clientes ascendentes (controlados por GIS) y realiza las llamadas de API OpenShift necesarias. Durante la incorporación, el motor de aprovisionamiento (PE) prepara la estructura de carpetas del sistema de archivos de red y el esquema de servicio de base de datos relacional para el cliente. El motor de aprovisionamiento crece y pasa a ser más rico a medida que se añaden nuevas funcionalidades, como las copias de seguridad y la migración, a la nube de DX APM.

Recursos de vídeo de DX APM

DX APM dispone de una amplia selección de recursos de vídeo para complementar la documentación y hacer una demostración de las funciones de DX APM.

Los vínculos que aparecen a continuación se conectan al [canal de YouTube de CA Technologies](#) en las listas de reproducción de DX APM. Cuando se hace clic en el vínculo, se abre una ficha nueva y se establece la conexión con el vídeo del sitio de YouTube. Para ver vídeos incrustados a pantalla completa, haga clic en Reproducir y, a continuación, haga clic en el logotipo de YouTube situado en la barra de herramientas, en la parte inferior de la pantalla. Se abre una ficha nueva con el vídeo de YouTube directamente.

Si su empresa ha bloqueado YouTube, póngase en contacto con el administrador.

DX APM se utiliza para monitorizar el rendimiento de la aplicación. Puede identificar las áreas del entorno que están sometidas a una carga y evaluar los problemas potenciales antes de que afecten a la experiencia del cliente. También se puede utilizar DX APM para realizar un seguimiento de los problemas existentes en la resolución.

DX APM: Cómo identificar la causa raíz de una incidencia de la aplicación

9 min 46 s

Omar muestra cómo navegar por la interfaz de usuario de DX APM para determinar rápidamente el origen de los problemas de rendimiento.

DX APM: Procedimientos iniciales utilizando el Agente de monitorización universal de

23 min 53 s

Rob le presenta las funciones básicas del Agente de monitorización universal (UMA) de .

DX APM: Procedimientos iniciales del análisis de embudo

33 min 42 s

Harish muestra cómo el análisis de embudo puede ayudarle a monitorizar el flujo de negocio.

DX APM: Comprensión y uso del Mapa y del Árbol de métrica

12 min 34 s

Le mostraremos cómo navegar por las capas del mapa para ver las relaciones entre los componentes. Obtenga información acerca de los atributos y explore el Árbol de métrica.

DX APM Arquitectura de referencia: comprensión del enfoque de implementación de DX APM

21 min 05 s

Henrik trata la implementación; la alta disponibilidad, los servicios, la conectividad y el flujo de datos de DX APM.

DX APM Team Center: cómo utilizar los atributos

1 h 11 min 39 s

Andreas le presenta el mapa y los atributos mediante la explicación del vocabulario, la navegación y las prácticas recomendadas.

DX APM: Comprensión de la Vista de experiencia, la evaluación de errores asistida y el Bloc de notas de la experiencia

13 min 11 s

Se describe el uso de la Vista de experiencia y de las tarjetas de experiencia, la evaluación de errores asistida y el Bloc de notas de la experiencia.

DX APM Análisis de alarmas: comprensión y corrección

28 min 33 s

Jan explica información detallada sobre las alarmas, el filtrado y la reducción de ruidos, los tipos de alarmas y sus algoritmos, y la corrección de alarmas.

DX APM: Cómo crear servicios

47 min 14 s

Se presentan los servicios de DX APM, el asistente de creación de servicios, cómo crear el primer servicio y el análisis de servicios.

Cómo implementar el Agente de monitorización universal

8 min 33 s

Le enseñaremos cómo instalar el Agente de monitorización universal, que instrumenta y monitoriza automáticamente el clúster de Kubernetes.

DX APM: Cómo evaluar un inicio de sesión lento

17 min 40 s

Utilizamos una aplicación de demostración que se ejecuta en un entorno de Kubernetes implementado en la nube de AWS para guiarle a través del producto App Experience Analytics. Analizamos la experiencia del usuario final para una aplicación monitorizada. Por ejemplo, el usuario final se bloquea durante la última semana o se producen inicios de sesión lentos en las últimas 24 horas.

DX APM: Obtención de la visibilidad App-to-Infra

9 min 59 s

Omar explora los niveles del mapa, los nodos y las capas, mostrando la captura de métricas mediante etiquetas y la correlación de métricas.

DX APM: Demostración de la gestión de clústeres

10 min 33 s

Dominik presenta los servicios de gestión de clústeres, la implementación de servicios, los servicios de cliente, la creación de clientes, los tókenes y la monitorización del rendimiento utilizando métricas.

App Synthetic Monitor: cómo simular las transacciones comerciales críticas y los trayectos de los usuarios

10 min 07 s

Dominik introduce DX App Synthetic Monitor y muestra cómo crear monitores y scripts sintéticos para replicar la experiencia del usuario final.

DX APM: Trabajo con módulos de gestión en Team Center

5 min 02 s

Le presentamos los módulos de gestión, que permiten a los administradores organizar y gestionar fácilmente los datos de las métricas.

Convenciones de nombre de archivo y directorio

La documentación de DX APM utiliza las siguientes convenciones en los nombres de archivo y en las rutas de directorio:

Convención	La convención hace referencia a
<Agent_Home >	El directorio de nivel superior en el que está instalado el Agente de Introscope. De forma predeterminada, este directorio se llama wily.
<APM_Db_Home>	El directorio de nivel superior en el que está instalado el servidor de aplicaciones. Este directorio suele ser el mismo que el de <Agent_Home>.
<AppServer_Home>	El directorio principal del servidor de aplicaciones.
<EM_Home>	El directorio de nivel superior en el que está instalado Enterprise Manager.
<Installation_Directory>	El directorio de instalación de un componente de DX APM u otra aplicación cuando no se instala en el directorio predeterminado o típico.
<ProductName_Home>	El directorio de instalación de un producto o tipo de aplicación de terceros. Por ejemplo, se puede hacer referencia al directorio principal de WebSphere Application Server como <WAS_Home >.
<Workstation_Home>	El directorio de nivel superior en el que está instalada la estación de trabajo. Este directorio suele ser el mismo que el de <EM_Home >.

<File_Name><version><Operating System or other identifier>.<FileType>	Un nombre de archivo que incluye información de identificación específica. Por ejemplo, si extrae archivos de un paquete TAR para <product_name> 10.7.0 en un sistema operativo UNIX, descargue <product_name> 107.0=.0unix.tar . El nombre de archivo aparece en esta documentación como: <product_name><10.7.0>.unix.tar
Separador de ruta de barra diagonal (/)	El separador de ruta que se utiliza en los nombres de directorio para su entorno operativo. Los entornos y ejemplos de UNIX de esta documentación utilizan la barra diagonal. Utilice el separador adecuado para su sistema operativo.
Variables de entorno de símbolo de dólar (\$)	La notación de variable de entorno que se utiliza en el sistema operativo. Los entornos y ejemplos de UNIX de esta documentación utilizan el símbolo de dólar (\$). Utilice el carácter que sea adecuado para su sistema operativo.

Personalizaciones

DX APM es altamente personalizable; sin embargo, el soporte de Broadcom no es compatible con las personalizaciones que se realizan en las configuraciones listas para su uso. Por ejemplo, puede personalizar la instrumentación del agente, incluida la implementación de archivos PBD personalizadas. Puede crear calculadoras de JavaScript personalizadas, así como scripts de shell y de EPAgent para las extensiones del agente. Cuando se piense que las personalizaciones están causando un problema en el producto, se podrá solicitar que se eliminen o desactiven. A continuación, se tendrá en cuenta ofrecer más ayuda. Para obtener ayuda con una personalización nueva o existente de DX APM, póngase en contacto con su arquitecto de soluciones de cliente.

Artículos de la base de conocimiento

Para consultar la lista completa de artículos de la base de conocimiento para DX Application Performance Management, haga clic [aquí](#).

Use los filtros de búsqueda avanzada para delimitar sus criterios de búsqueda.

1. Seleccione Artículos de conocimiento en la lista de opciones disponibles en **Fuentes**.

Sources	
<input type="checkbox"/> TechDocs	1139422
<input type="checkbox"/> Solutions	503672
<input type="checkbox"/> Community Threads	328165
<input type="checkbox"/> Problems	236777
<input type="checkbox"/> Knowledge Articles	140221
<input type="checkbox"/> Product News	9361

2. Seleccione Application Performance Management en las opciones de **Producto**.

⋮ **Product** ▼

X

<input type="checkbox"/>	ACF2	1550349
<input type="checkbox"/>	CA Automic	1014573
<input type="checkbox"/>	Identity Management Suite	1012945
<input type="checkbox"/>	Application Performance Management	1011866
<input type="checkbox"/>	CA 7 Workload Automation	526756
<input type="checkbox"/>	APCDOC Automated Job Document...	522603
<input type="checkbox"/>	APCDDS Automated Report Balancing	520265
<input type="checkbox"/>	CA Configuration Automation	513009
<input type="checkbox"/>	CA Service Management - Asset Port...	508258

3. Seleccione el idioma requerido.
4. Seleccione la duración requerida de las opciones de **Fecha actualizada**.

Updated Date

☐ All Time 507268
 ☐ Past Year 4090
 ☒ Past Month 390
 ☐ Past Week 77
 ☐ Past Day 25

5. Se muestran los artículos de conocimiento pertinentes para los criterios de filtro especificados.

Glosario

En este glosario se definen los términos clave de DX APM.

NOTE

Todos los términos se aplican a DX APM local y solo algunos se aplican a DX APM.

Agente .NET

El *Agente de .NET* recopila las métricas sobre aplicaciones de Microsoft .NET.

Consulte también: Common Language Runtime (CLR), .NET Framework

.NET Framework

Microsoft *.NET Framework* es un entorno de desarrollo y ejecución que permite que diferentes lenguajes de programación y bibliotecas trabajen juntos. .NET Framework se basa en un entorno de tiempo de ejecución que se conoce como Common Language Runtime (CLR). CLR utiliza lenguajes de programación como C#.

Consulte también: Common Language Runtime (CLR), Agente de .NET

agent

El *agente* recopila las métricas del entorno y de las aplicaciones y las retransmite a Enterprise Manager. Estas aplicaciones pueden ser de cualquier tipo: Java, .NET, PHP o aplicaciones web. Se dice que se está instrumentado una aplicación que informa a un agente sobre la métrica.

Consulte también: instrumentado, Agente de Java, Agente de .NET, Agente de PHP

topología de red del agente con Enterprise Manager

La topología de red del agente con Enterprise Manager es la estructura de red del entorno de DX APM. Esta topología especifica a qué agentes o grupos de agentes se puede conectar:

- Enterprise Manager independientes específicos.
- Recopiladores
- Grupos de recopiladores

equilibrio de carga del agente

El *equilibrio de carga del agente* equilibra la carga de la métrica entre los recopiladores en un entorno agrupado en clúster. Los agentes específicos, que se asignan a MOM, ecualizan el recuento de métrica entre los recopiladores. Los agentes específicos indican a otros agentes que envíen sus datos de métrica al recopilador con menos carga en el clúster.

Consulte también: agente, recopilador, Manager of Managers (MOM)

alerta

Una *alerta* es un conjunto guardado de valores de umbral para "Precaución" y "Riesgo", con otras propiedades correspondientes. Una alerta es uno de los objetos básicos en un módulo de gestión, que guarda las recopilaciones de estos objetos para su reutilización. Normalmente una alerta tiene acciones asociadas, pero las acciones son en sí mismas objetos separados del módulo de gestión.

Se debe distinguir entre la alerta en sí (por ejemplo, el nombre de la alerta que se asocia con los valores del umbral guardado) y lo siguiente:

- El *indicador de alerta*, que es una visualización gráfica del estado de la alerta.
- La *notificación de alerta*, que es una de las acciones posibles que se puede asociar con una alerta.

almacenamiento de Amazon EBS

Amazon EBS (Elastic Block Store) es un volumen de almacenamiento a nivel del bloque que persiste independientemente de la duración de una instancia de EC2. Se recomienda utilizar este tipo de almacenamiento en la instancia para ayudarle a detener y reiniciar la instancia en otro momento.

Amazon Machine Image

Amazon Machine Image (AMI) es una imagen cifrada del equipo, similar a una plantilla, de la unidad raíz de un equipo. La AMI contiene el sistema operativo y puede incluir software y las capas de la aplicación, como ejemplos de las capas de servidores de la base de datos, middleware y servidores web. La AMI se almacena en Amazon Elastic Block Store o Amazon Simple Storage Service.

base de datos de APM

La *base de datos de APM* es una base de datos relacional que almacena datos.

Consulte también: base de datos de SmartStor, base de datos de eventos de la transacción

Application Performance Management (APM)

El producto *DX APM*. DX APM proporciona una estrategia de gestión del rendimiento de las aplicaciones que permite conocer la experiencia del usuario final y medir los acuerdos de nivel de servicio (SLA). Todas las transacciones se pueden asignar a la infraestructura de punto final a punto final. También se puede realizar un mapa de evaluación de errores y el pertinente diagnóstico de la causa raíz de incidentes en una solución completa e integrada.

compatibilidad de aplicaciones

DX APM mide la *compatibilidad de aplicaciones* midiendo el rendimiento de diversos componentes de la aplicación. La métrica proporciona información sobre JVM/CLR, aplicaciones web y sistemas back-end.

DX APM proporciona métricas de compatibilidad para que pueda responder a preguntas sobre el estado de las aplicaciones. La compatibilidad de aplicaciones también se conoce como el estado de la aplicación.

App Synthetic Monitor (ASM)

DX APM App Synthetic Monitor (ASM) es un producto que crea transacciones sintéticas para complementar la monitorización de transacciones en DX APM. ASM ofrece un preaviso de los problemas de disponibilidad de la aplicación.

attribute

Los *atributos* son etiquetas que se aplican a los nodos para diferenciar los componentes e identificar sus relaciones con otros componentes.

reglas de atributo

Las *reglas de atributo* son reglas que automatizan el proceso de adición de atributos personalizados. Solo los administradores pueden crear reglas de atributo.

seguimiento automático de la transacción

Cuando se activa la instrumentación inteligente, los rastreadores de sobrecarga baja altamente optimizados recopilan un *seguimiento automático de la transacción* en condiciones específicas de activación. Un error puede ser un factor de activación. Otro ejemplo de factor de activación lo encontramos al implementar el rastreador `ComponentTimeAutoTraceTriggerTracer` y superar el tiempo de respuesta de un componente. Los seguimientos automáticos de la transacción muestran los componentes con una gran visibilidad y tienen características que difieren de los seguimientos de la transacción no automáticos como, por ejemplo, los seguimientos manuales y de muestra.

AutoProbe

DX APM *AutoProbe* automatiza el proceso de instrumentación de la aplicación agregando de forma dinámica sondas a la aplicación en el tiempo de inicio. Las sondas de DX APM proporcionan los datos de origen para las métricas de DX APM.

Consulte también: instrumentado, ProbeBuilder

Promoción automática

Si se activa la *Promoción automática*, todos los cambios realizados en la configuración del Analizador de la carga empresarial se aplicarán automáticamente.

back-end

Un *back-end* es un sistema externo del que depende una aplicación web para una parte de su procesamiento. Por ejemplo, un back-end puede ser una base de datos, un servidor de correo, un sistema de procesamiento de transacciones o un sistema de mensajería. DX APM identifica automáticamente las bases de datos, los sistemas JMS y los puntos finales de HTTP.

Para otros sistemas externos, DX APM analiza la actividad del socket de la aplicación para detectar y monitorizar los back-ends sin tener que llevar a cabo una configuración manual. Esta capacidad se llama detección *automática de back-ends*.

La métrica de back-end se muestra bajo el nodo Back-ends en el árbol del Explorador de la métrica.

Consulte también: front-end, punto de entrada

tiempo de back-end

El *tiempo de back-end* es la medida de tiempo que el componente de Blame sospechoso (por ejemplo, un componente de la base de datos) del sistema de back-end tarda en completarse, en función de la generación de informes de DX APM. El tiempo de back-end se mide desde el componente de Java que invoca el back-end. Por lo tanto, el tiempo incluye tanto el tiempo de procesamiento del back-end como cualquier otro tiempo de red que se ha tardado en comunicarse con el back-end.

Consulte también: back-end, componente de Blame sospechoso

línea de referencia

La *línea de referencia* es un conjunto inicial de datos que se utilizan como una comparación o control. DX APM emplea algoritmos de línea de referencia para monitorizar las aplicaciones web.

DX APM determina el color del indicador de alerta en la ficha **Descripción general** evaluando las métricas actuales con respecto a una línea de referencia para dichas métricas. Con un nodo del agente seleccionado en el árbol centrado en el agente, el nodo Heurística muestra los valores de métrica relacionados con estos indicadores.

Para una métrica determinada, el algoritmo de línea de referencia de DX APM determina el siguiente valor esperado y la desviación esperada de ese valor. Cuando la desviación real supera (2x) o supera significativamente (4x) la desviación esperada, la línea de referencia indica una infracción grave o moderada. La heurística asociada se pone en amarillo o rojo.

Internamente, la línea de referencia evalúa la pendiente de la serie temporal y determina el valor esperado de la pendiente. Los datos recientes tienen un peso mayor que los datos más antiguos.

Consulte también: métrica heurística, especificación

Blame

DX APM *Blame* es la tecnología que se utiliza para instrumentar una aplicación. DX APM realiza el seguimiento de las interacciones de los componentes y del uso de los recursos marcando los front-ends y los back-ends de la aplicación. DX APM también proporciona las métricas necesarias para las investigaciones de los problemas.

Consulte también: back-end, front-end, instrumentado, Transaction Tracer

BT Listener

Business Transaction Listener (BT Listener) es un componente del Analizador de la carga empresarial que filtra y redirige solamente los datos interesados solicitados por BT Diviner. Se implementa BT Listener entre el complemento y BT Diviner. BT Listener es compatible con Windows y Linux.

aplicación del negocio

Una *aplicación del negocio* es un programa de software que automatiza un servicio empresarial. DX APM monitoriza las transacciones web, que son el producto de las aplicaciones web. Una aplicación del negocio forma parte de la jerarquía de transacciones.

servicio empresarial

En SOA Performance Management, un servicio empresarial realiza solicitudes salientes a sistemas de back-end para el bus de servicios de la empresa.

componente de la transacción comercial

Un *componente de la transacción comercial* representa un par de solicitud/respuesta HTTP que se ha instrumentado y monitorizado para realizar un seguimiento del estado de una transacción comercial. Los componentes de la transacción comercial son el origen de la métrica de estado del mapa.

El componente de la transacción comercial es el único componente de identificación de la transacción.

Un componente de la transacción comercial es similar a estos dos componentes:

- Transacción (porque es la única transacción de identificación de la transacción comercial).
- Componente de la transacción (porque es el único componente de identificación en una transacción).

Consulte también: transacción, componente de la transacción, jerarquía de transacciones

atributos capturados

En el Analizador de la carga empresarial se pueden definir los atributos que se deseen capturar en todas las transacciones cuando estén disponibles como *atributos capturados*. Se puede aplicar una tendencia a los atributos capturados con valores numéricos a lo largo del tiempo como KPI en el Explorador de métrica o en los cuadros de mandos.

Consulte: Introducción a los atributos del Analizador de la carga empresarial

Regla de captura

En el Analizador de la carga empresarial, la *regla de captura* define los atributos que se capturarán en cada transacción cuando estén disponibles.

fijación

Una *fijación* es un límite configurable del número de valores de métrica que se devuelve para una función específica. Se utiliza en la fijación del seguimiento de la transacción y en la fijación de la métrica para varios componentes de DX APM como, por ejemplo, los agentes y Enterprise Manager.

Consulte también: fijación de la métrica, Transaction Tracer

recopilador

Un *recopilador* es un Enterprise Manager que se utiliza en un entorno de clúster. Manager of Managers (MOM) gestiona los recopiladores en entornos en clúster.

Consulte también: Enterprise Manager (EM), Manager of Managers (MOM)

Common Language Runtime (CLR)

Common Language Runtime (CLR) es la implementación de Microsoft de Common Language Infrastructure (CLI). La finalidad de la CLI es proporcionar una plataforma independiente del idioma para la ejecución y el desarrollo de aplicaciones.

CLR de .NET es casi idéntico a la máquina virtual Java de la plataforma Java.

Consulte también: Agente de .NET, .NET Framework

configurar

En DX APM, *configurar* tiene una definición específica. *Configurar* consiste en establecer o cambiar los valores o las entradas en las propiedades, scripts, PBD, PBL, etc. El soporte de Broadcom es compatible con las configuraciones que se describen en la documentación de DX APM.

Consulte también: personalizar

Console, Workstation

La *consola* es la vista predeterminada cuando se inicia la estación de trabajo. La consola contiene cuadros de mandos que muestran datos de rendimiento en vistas gráficas.

Consulte también: cuadro de mandos, Workstation, Workstation

contenedor

Un *contenedor* hace referencia a un entorno de tiempo de ejecución de Java para los enterprise beans. Un contenedor que se ejecuta en un servidor EJB (Enterprise JavaBeans) gestiona los ciclos de vida de los objetos de enterprise bean, coordina las transacciones distribuidas e implementa la seguridad de los objetos.

Consulte también: transacción

personalizar

En DX APM, *personalizar* tiene una definición específica. *Personalizar* es programar una nueva forma de monitorización, generación de scripts, procesamiento, formato de un complemento y mucho más.

DX APM es altamente personalizable; sin embargo, el soporte de Broadcom no es compatible con las personalizaciones que se realizan en las configuraciones listas para su uso. Por ejemplo, puede personalizar la instrumentación del agente, incluida la implementación de archivos PBD personalizadas. Puede crear calculadoras de JavaScript personalizadas, así como scripts de shell y de EPAgent para las extensiones del agente. Cuando se piense que las personalizaciones están causando un problema en el producto, se podrá solicitar que se eliminen o desactiven. A continuación, se tendrá en cuenta ofrecer más ayuda. Para obtener ayuda con una personalización nueva o existente de DX APM, póngase en contacto con su arquitecto de soluciones de cliente.

Consulte también: configurar

cuadro de mandos

Un *cuadro de mandos* combina y presenta las métricas de la aplicación en vistas para monitorizar el entorno general de la aplicación. Los cuadros de mandos ofrecen información detallada sobre el rendimiento que se necesita para la evaluación rápida de problemas, el diagnóstico y la solución para las aplicaciones en producción. En Team Center, el cuadro de mandos muestra el estado general del entorno.

Consulte también: métrica

métrica inactiva

Una *métrica inactiva* no tiene nuevos datos notificados durante un período de tiempo determinado. Se puede configurar la cantidad de tiempo.

Consulte también: métrica en directo, métrica

componente de visibilidad exhaustiva

Un *componente de visibilidad exhaustiva* es un método o componente que el agente detecta y muestra automáticamente sin tener que utilizar las directivas de ProbeBuilder (PBD). Cuando se activa la instrumentación inteligente, el agente analiza los métodos para comprobar su complejidad y así poder determinar las llamadas y los componentes que se deben instrumentar y mostrar como componentes de visibilidad exhaustiva.

Análisis diferencial

El *Análisis diferencial* es un enfoque para identificar automáticamente los cambios importantes que se producen en el rendimiento de las aplicaciones. Las líneas de referencia heredadas predicen lo que es normal. El Análisis diferencial busca una varianza sin control en el Tiempo medio de respuesta de las aplicaciones del front-end y de la métrica de transacciones comerciales. La varianza sin control aparece como picos en un flujo de datos estable, lo que no es enteramente diferente a cómo un sismógrafo detecta los terremotos.

programación de detección

Una *programación de detección* determina qué se debe detectar en la carga de la aplicación del Analizador de la carga empresarial.

atributos ignorados

En el Analizador de la carga empresarial, los atributos que BT Listener detecta en la carga útil de la aplicación en función de la regla de detección se clasifican como atributos ignorados.

Consulte: Introducción a los atributos del Analizador de la carga empresarial

domain

Un *dominio* de DX APM es una manera de particionar los agentes y la lógica de gestión para definir qué usuarios pueden ver qué tipo de información.

red de doble pila

En una *red de doble pila*, se admiten aplicaciones y servicios de IPv4 e IPv6. Esto requiere hosts y enrutadores para implementar protocolos IPv4 e IPv6.

El enfoque de doble pila es una forma común para introducir IPv6 en una arquitectura de IPv4 existente. Este enfoque permite a las redes admitir IPv4 e IPv6 durante el período de transición, lo que permite que los servicios y aplicaciones de IPv6 se vuelvan disponibles más rápidamente.

DX APM

DX APM es una solución de gestión del rendimiento de las aplicaciones del negocio que permite realizar lo siguiente:

- Monitorizar aplicaciones complejas en entornos de producción las 24 horas al día, los 7 días a la semana.
- Detectar problemas antes de que afecten a los clientes.
- Solucionar estos problemas rápida y colaborativamente.

Consulte también: agente, Enterprise Manager, métrica

propiedad dinámica

Una *propiedad* dinámica en los archivos de configuración de DX APM (por ejemplo, el archivo `IntroscopeAgent.profile`) se implementa en cuanto se guarda el archivo de configuración. No es necesario reiniciar la aplicación o los servidores de aplicaciones para que se aplique el cambio.

activar aplicación

Los datos de una aplicación se envían al Analizador de la carga empresarial solamente cuando la aplicación está activada. Para activar una aplicación, configure la programación de detección que determina qué se debe detectar en la carga útil de la aplicación.

Consulte: Introducción a los atributos del Analizador de la carga empresarial

extensión

Una *extensión* de DX APM es el código de programa (archivo JAR) que amplía la funcionalidad básica de Enterprise Manager o de un agente.

Consulte también: Enterprise Manager, agente

Enterprise Manager

Enterprise Manager almacena y agrega la métrica de rendimiento de la aplicación como, por ejemplo, el tiempo de respuesta, el ancho de banda o la asignación de memoria. Varios agentes, dispersos por la empresa, recopilan y transmiten la métrica medioambiental y de la aplicación, y van informando sobre la misma a Enterprise Manager.

Consulte también: recopilador, Manager of Managers (MOM)

punto de entrada

Cuando se activan la instrumentación inteligente y la detección automática del punto de entrada, DX APM monitoriza automáticamente los subprocesos que se invocan en las transacciones de llamada de socket del cliente. Los *puntos de entrada* son los puntos de inicio de la transacción. Los puntos de entrada se muestran en el árbol centrado en el agente y en los seguimientos de la transacción.

Consulte también: instrumentación inteligente, back-end automático

Environmental Performance Agent (EPAgent, EPA)

Environmental Performance Agent (EPA, EPAgent) es una versión modificada del agente que ayuda a integrar datos de la métrica de orígenes genéricos y no basados en Java en DX APM. EPA utiliza scripts sencillos que permiten al agente monitorizar prácticamente cualquier tipo de subsistema de la aplicación que tiene un impacto en el rendimiento. Por ejemplo, servidores de directorios, sistemas operativos, middleware de mensajería y servidores de transacciones.

Consulte también: agente, complementos con estado, complementos sin estado

instantánea de error

ErrorDetector genera una *instantánea de error*, que muestra información detallada sobre lo que estaba pasando cuando se ha producido un error. Los datos de la instantánea de error se almacenan en la base de datos de eventos de la transacción.

Consulte también: ErrorDetector

ErrorDetector

ErrorDetector permite al personal de soporte de la aplicación detectar y diagnosticar la causa de los errores graves, que pueden impedir que los usuarios finalicen las transacciones web.

Los errores "graves" predefinidos que se basan en información que se incluye en las especificaciones de PHP, J2EE y .NET incluyen estos errores:

- Errores HTTP (por ejemplo, 404 y 500)
- Errores de instrucción SQL
- Errores de conectividad de la red (errores de tiempo de espera excedido)
- Errores del back-end (por ejemplo, no se puede enviar un mensaje a través de JMS o no se puede escribir un mensaje en la cola de mensajes)

Consulte también: instantánea error

evento

Un *evento* de DX APM es cualquier acción para la que los agentes capturan valores de métrica. Por ejemplo, seguimientos de la transacción, errores y detenciones.

Consulte también: ErrorDetector, métrica, detención, seguimiento de la transacción

extensión

Las *extensiones* son las aplicaciones de DX APM que amplían las capacidades de monitorización de los datos. Las extensiones se integran fácilmente con los componentes predeterminados de DX APM, lo que aporta una mayor visibilidad de su entorno y aplicaciones monitorizadas.

Algunas extensiones requieren un reinicio de la aplicación y otras, no. Puede activar las extensiones que se suministran con DX APM.

Federal Information Processing Standards (FIPS)

Federal Information Processing Standards (FIPS) son estándares anunciados públicamente. El Gobierno Federal de los EE.UU. ha desarrollado estos estándares para que los puedan utilizar todas las agencias gubernamentales no militares y todos los contratistas del gobierno. Muchos estándares FIPS son versiones modificadas de los estándares que se utilizan en el sector más amplio de la industria del software.

La publicación de FIPS 140-2, "Security Requirements for Cryptographic Modules", especifica el estándar de seguridad para las bibliotecas criptográficas. Esta publicación especifica los algoritmos que los productos de software deben utilizar para el cifrado. El cifrado afecta el almacenamiento y la verificación de las contraseñas. También afecta a la comunicación de toda la información confidencial entre los componentes de un producto y entre diferentes productos.

front-end

Un *front-end* es el componente de una aplicación que primero gestiona una transacción entrante. En las aplicaciones J2EE más habituales, este componente es un JSP o un servlet. En algunos casos de Java, puede ser un EJB o algún otro componente. DX APM identifica automáticamente los servlets y los JSP como front-ends, pero no lo hace con cualquier otro componente. Para marcar un componente como un front-end de forma explícita, utilice el rastreador `FrontendMarker`.

Consulte también: back-end

pila gráfica

En un seguimiento de la transacción, la *pila gráfica* es la representación del orden de las transacciones de los componentes, de arriba a abajo. Nos referiremos a la pila gráfica como gráfico de tarta debido a que la representación puede parecer una tarta al revés. Puede ver la pila gráfica en el Visor de seguimiento de transacciones.

Consulte también: seguimiento de la transacción, Transaction Tracer

GUID

El *GUID* (identificador único global) es una clave única que produce `ServletHeaderDecorator`. La clave identifica una transacción en la aplicación monitorizada del negocio. El GUID es la información clave que correlaciona algunas transacciones.

Los GUID pueden crearse de varias formas. Por lo general, los GUID son una combinación de configuraciones únicas que se basan en una hora específica. Por ejemplo, un GUID puede ser una combinación de una dirección IP, una dirección MAC de red, la fecha y la hora.

Consulte también: dirección MAC, `ServletHeaderDecorator`

latido

El *latido* es el intervalo de tiempo cuando se comprueba la métrica, normalmente en segundos.

métrica heurística

Las *métricas heurísticas* de DX APM se utiliza para evaluar y generar informes de estado. Son números enteros, pero los números enteros son símbolos de estado y no miden nada. El valor de una métrica heurística se determina evaluando la métrica actual con respecto a una línea de referencia para esta métrica.

Se pueden definir alertas en términos de métrica heurística en lugar de umbrales fijos. La definición de alertas utilizando las métricas heurísticas que determina los valores normales de los indicadores clave de rendimiento (los KPI) cambia el trabajo del administrador de APM a DX APM.

Consulte también: línea de referencia, métrica

propiedad oculta

Una *propiedad oculta* es una propiedad en un archivo de configuración. La propiedad solo está disponible para su uso cuando se agrega la propiedad al archivo de configuración. Por ejemplo, un archivo de configuración es el archivo `IntroscopeAgent.profile` o el archivo `IntroscopeEnterpriseManager.properties`.

HTTPHeaderDecorator

HTTPHeaderDecorator de DX APM es una extensión de agente que aumenta los encabezados de respuesta HTTP para los Agentes de .NET.

Consulte también: GUID, ServletHeaderDecorator, Transaction Tracer

atributos de identificación

Los atributos que se desean incluir en la regla de denominación de la transacción comercial se pueden establecer como atributos de identificación. La regla de denominación nombra a una transacción comercial de forma exclusiva y ayuda a identificar una transacción comercial en DX APM.

Consulte: Introducción a los atributos del Analizador de la carga empresarial

componente de identificación

El *componente de identificación* es el primer componente de la transacción en el conjunto de componentes de la transacción. El componente de identificación identifica de forma exclusiva el inicio de una transacción. Un componente de identificación no debe ser un componente de otra transacción.

NOTE

Una redirección puede aparecer como el primer componente de un registro de la transacción, pero no es el componente de identificación.

Consulte también: jerarquía de transacciones

transacción de identificación

La *transacción de identificación* es la primera transacción en un conjunto de transacciones comerciales. La transacción de identificación identifica de forma exclusiva el inicio de una transacción comercial. Una transacción de identificación no debe ser una transacción de ninguna otra transacción comercial.

Consulte también: jerarquía de transacciones

tipo de instancia

Tipo de instancia es una especificación que define la memoria, la CPU, la capacidad de almacenamiento y el coste por hora de una instancia de Amazon Web Services (AWS). Los tipos de instancia pueden diseñarse para aplicaciones estándares o para aplicaciones intensivas con el uso de la CPU y de la memoria.

instrumentado

El código de la aplicación se ha *instrumentado* cuando ProbeBuilder inserta las sondas en el código de bytes para enviar la métrica al agente.

Consulte también: agente, AutoProbe, aplicación gestionada, ProbeBuilder

Investigator, Workstation

Workstation *Investigator* permite ver el estado de las aplicaciones y del sistema para buscar en los datos de la métrica mediante una estructura de árbol. Puede tener más de una ventana de Investigator abierta a la vez.

Consulte también: consola, Workstation; Workstation

Agente de Java

El *Agente de Java* recopila métricas en entornos de Java.

puerto de escucha

Se utiliza un *puerto de escucha* para simplificar la administración de la asociación entre una fábrica de conexión, el destino y el bean controlado por el mensaje implementado.

métrica en directo

Una *métrica en directo* informa activamente sobre los datos de un agente específico.

Consulte también: métrica inactiva, métrica

tiempo de lógica

El *tiempo de lógica* es la medida de tiempo que el código de programa del componente de Blame sospechoso tarda en completarse. Este tiempo se basa en la generación de informes de DX APM.

Consulte también: componente de Blame sospechoso

dirección MAC

La *dirección MAC* (dirección Media Access Control) es una dirección de hardware que identifica cada nodo de una red de forma exclusiva.

La dirección MAC puede ser útil durante el proceso de resolución de problemas. Por ejemplo, cuando los servidores web se encuentran detrás de un equilibrador de carga que oculta la verdadera identidad del servidor web en el nivel de IP. Por ejemplo, en entornos de equilibrio de carga de Resonate, todos los servidores web parecen tener la misma dirección IP. Sin embargo, la dirección MAC que se envía en la respuesta puede identificar los servidores de forma exclusiva.

aplicación gestionada

Cuando se está ejecutando una aplicación instrumentada, se llama *aplicación gestionada*.

Consulte también: instrumentado

módulo de gestión

Un *módulo de gestión* contiene un conjunto de información sobre la configuración de la monitorización. Los módulos de gestión se muestran para cada dominio y contienen elementos. Los elementos son objetos que contienen y organizan los datos con lógica de monitorización como alertas, acciones y cuadros de mandos.

Consulte también: cuadro de mandos, WebView, Workstation

Manager of Managers (MOM)

Manager of Managers (MOM) almacena métricas tal y como las recopilan varios Enterprise Manager. La agrupación en clústeres de Enterprise Manager permite a un Enterprise Manager (el MOM) gestionar a otros Enterprise Manager. Cada uno de los Enterprise Manager gestionados, llamados recopiladores, recopila la métrica del agente y, a su vez, transmite la métrica al MOM.

Consulte también: recopilador, Enterprise Manager (EM)

mapa

En Team Center, el *mapa* muestra las relaciones entre los componentes individuales dentro del entorno.

valor de la mediana

El *valor de la mediana* es un valor único que representa una distribución de datos. Se prefiere el valor de la mediana que el valor medio como una representación de un único número de una distribución cuando la distribución no es una distribución normal (curva de campana).

fijación de la métrica

Una *fijación de la métrica* es un límite o fijación en el número de métricas en el agente y en Enterprise Manager. Una fijación de la métrica ayuda a evitar picos en el número de métricas notificadas (expansiones de la métrica) en Enterprise Manager.

Consulte también: agente, fijación, métrica

expansión de la métrica

Se produce una *expansión de la métrica* cuando aparezcan nuevas métricas en grandes cantidades en unos pocos minutos. Las definiciones de métrica mal configuradas pueden hacer que los metadatos de la métrica cambien con los cambios del valor de la métrica, con lo que aparecerán como nueva métrica. Por ejemplo, las cadenas de variables en una métrica de SQL. Las propiedades de conexión del agente mal configuradas para un conjunto de nuevos agentes pueden provocar miles de nuevas métricas para sobrecargar Enterprise Manager. Estas situaciones pueden reducir el rendimiento.

Consulte también: pérdida de métrica, agente, fijación, métrica

agrupación de métricas

Las *agrupaciones de métricas* son objetos del módulo de gestión que guardan esta información:

- La *expresión del agente*: Una expresión regular en Perl 5 que filtra la entrada para la métrica especificando los datos hasta e incluyendo el nombre del agente.
- La *expresión de la métrica*: Una expresión regular en Perl 5 que especifica el recurso (la cadena de carpetas que llevan a la métrica) y la métrica.
- El módulo de gestión al que pertenece la agrupación de métricas.

pérdida de métrica

Una *pérdida de métrica* se produce cuando una configuración incorrecta de DX APM da lugar a agentes que informan sobre métricas durante un tiempo limitado. Este problema da lugar a una acumulación gradual de metadatos de métrica sin los datos de métrica asociados.

Consulte también: expansión de la métrica, agente, fijación, métrica, DX APM

limitador de la métrica

Un *limitador de la métrica* detiene un agente cuando los resultados de la métrica pasan a ser excesivos.

Consulte también: agente, fijación, métrica

métrica, DX APM

Una *métrica de DX APM* es una medida del rendimiento de la aplicación. Estos son los tipos de métrica:

- Ancho de banda: archivo y actividad de socket a nivel de JVM y CLR
- Concurrencia: número de invocaciones de método que se inician pero que todavía no han finalizado
- Recuento: número de invocaciones de método hasta la fecha
- Excepción: captura las excepciones
- Memoria: memoria que se adjudica a la JVM o CLR en uso, relacionada con la recolección de elementos no utilizados
- Tasa: número de ejecuciones de método por segundo o intervalo de tiempo
- Tiempo de respuesta: tiempo medio de ejecución de método en milisegundos
- Métodos detenidos: número de métodos que se han iniciado pero cuyas horas de invocación han excedido un umbral.
- Registros del sistema: monitoriza la salida del sistema y la salida de errores del sistema.
- Subprocesos: número de subprocesos instrumentados

Consulte también: fijación de la métrica, expansión de la métrica, limitador de la métrica

puerto duplicado

Un *puerto duplicado* es una función de software de los conmutadores y enrutadores de la red.

Consulte también: toma de red

conmutación por error de MOM

La *conmutación por error de MOM* se produce cuando MOM Enterprise Manager se desconecta o bloquea debido a un error de hardware o red. La conmutación por error se produce cuando se ha configurado un segundo MOM Enterprise Manager para reemplazar el primer MOM Enterprise Manager.

Consulte también: recopilador, Enterprise Manager (EM), Manager of Managers (MOM)

monitor

Los agentes *monitorizan* el rendimiento web de final a final, los componentes de Java y sus dependencias, los componentes de CLR y sus dependencias, las conexiones a sistemas de back-end, los niveles de recursos (incluido el software de terceros) y los recursos del servidor de aplicaciones.

Consulte también: agente, sincronización de todos los monitores

regla de denominación

Una regla de denominación también se puede definir como una cadena de atributos de identificación. La regla de denominación nombra a una transacción comercial de forma exclusiva y ayuda a identificar una transacción comercial en DX APM.

toma de red

Una *toma de red* es un dispositivo de hardware que accede directamente a la infraestructura de cableado. Este dispositivo crea copias de paquetes y los reenvía a uno o más destinos.

Consulte también: puerto duplicado

nodo

Un *nodo* es el lugar donde se recopila y se muestra información específica de la métrica en la vista de árbol del Explorador de métrica. Por ejemplo, Introscope Investigator muestra el nodo de back-ends o el nodo de uso de la CPU. Cuando se expande el nodo, se pueda ver y buscar información más detallada de la métrica. En Team Center, un nodo representa las transacciones comerciales y los componentes agregados o monitorizados directamente en un contexto topológico.

Consulte también: Investigator, Workstation, métrica, Workstation

acuerdo de nivel operativo (OLA)

Un *acuerdo de nivel operativo (OLA)* es un contrato entre una organización de TI y los grupos de soporte internos. Los términos del contrato dependen de las necesidades de las partes involucradas. Los acuerdos de nivel operativo se utilizan para gestionar los compromisos de servicio por los grupos de TI para el cumplimiento.

oportunidad

Una *oportunidad* es cualquier área dentro de un producto, proceso, servicio u otro sistema donde se puede producir un defecto. Por lo general, los productos más complejos significan más oportunidades para los defectos.

Consulte también: defecto, especificación

respuesta parcial

Una *respuesta parcial* significa que no se ha observado una respuesta completa para un componente concreto dentro del período de tiempo configurable esperado (el valor predeterminado es de 60 segundos).

Consulte también: respuesta que falta

paciente cero

El *paciente cero* es el primer componente en una serie de dependencias que indica cuáles son los problemas de rendimiento. Este componente parece ser el origen de la degradación del rendimiento en su entorno de aplicaciones. Es probable que el paciente cero sea la causa raíz del problema.

valor de percentil

El *valor de percentil* de una distribución es un número donde un porcentaje de la distribución es menor o igual a ese valor de percentil. Por ejemplo, el percentil 25 (también llamado cuartil inferior) es donde el 25 por ciento de los valores de los datos se encuentren por debajo del mismo.

A continuación, se muestra otro ejemplo. Para una gráfica del tiempo de respuesta, el número que se encuentra en el percentil 95 significa que el 95 por ciento de las transacciones realizadas durante ese período de tiempo tiene un tiempo de respuesta a ese nivel o menos.

perspectiva

Una *perspectiva* agrupa lógicamente los componentes en la interfaz de usuario. Los grupos se basan en sus atributos compartidos.

Agente de PHP

El *Agente de PHP* recopila métricas en aplicaciones de PHP.

complemento

El *complemento* es uno de los componentes del Analizador de la carga empresarial. El Analizador de la carga empresarial incluye complementos para los siguientes servidores web:

- Servidor web de Apache (Windows y Linux)
- Servidor web de IIS
- Servidor web de Nginx

regla de privacidad

Una regla de privacidad le permite enmascarar los valores de los campos que no desea que aparezcan en la interfaz de usuario o que se almacenen en la base de datos. Por ejemplo, puede ocultar los últimos cuatro dígitos del número de tarjeta de crédito utilizado para las transacciones o usar el hash SHA-256 unidireccional en la descripción médica de un paciente. Para obtener más información, consulte la sección Menú Acciones.

sonda

Una *sonda* mide elementos específicos de información sobre una aplicación sin cambiar la lógica del negocio de la aplicación. Un agente está instalado en el mismo equipo que la aplicación web instrumentada.

Consulte también: agente, instrumentado, ProbeBuilder

ProbeBuilder

ProbeBuilder lleva a cabo el proceso de instrumentación, en el que los rastreadores identifican las métricas que recopila un agente de las aplicaciones y de las máquinas virtuales en tiempo de ejecución. Los rastreadores se definen en archivos de directivas de ProbeBuilder (PBD).

Consulte también: agente, AutoProbe, directiva de ProbeBuilder (PBD)

directiva de ProbeBuilder (PBD)

Los archivos de *directiva de ProbeBuilder (PBD)* indican a ProbeBuilder cómo agregar sondas a componentes de PHP, .NET o Java para instrumentar la aplicación. Ejemplos de sondas son los temporizadores y los contadores. Los archivos de directivas de ProbeBuilder controlan la métrica específica que los agentes notifican a Enterprise Manager.

También se pueden crear directivas personalizadas para realizar un seguimiento de las clases y métodos únicos para aplicaciones específicas.

Consulte también: AutoProbe, Enterprise Manager (EM), ProbeBuilder, listas de ProbeBuilder (PBL)

listas de ProbeBuilder (PBL)

Un archivo de *listas de ProbeBuilder (PBL)* contiene una lista de varios archivos de directivas de ProbeBuilder. Varios archivos PBL pueden hacer referencia a los mismos archivos PBD.

Consulte también: AutoProbe, ProbeBuilder, directiva de ProbeBuilder (PBD)

ProbeBuilding dinámico

ProbeBuilding dinámico es útil para realizar correcciones en los archivos PBD o para cambiar niveles de recopilación de datos durante la evaluación de errores sin interrumpir el servicio de la aplicación.

tiempo de procesamiento

En App Synthetic Monitor, el *tiempo de procesamiento* es el período que transcurre después de enviar la solicitud HTTP y el monitor espera los primeros bytes del resultado.

ServletHeaderDecorator

ServletHeaderDecorator de DX APM aumenta los encabezados de respuesta HTTP de los servlets para los Agentes de Java.

El GUID se utiliza como el identificador de la transacción. *ServletHeaderDecorator* es una extensión del agente.

Consulte también: GUID, Transaction Tracer

SiteMinder

SiteMinder de DX APM es una aplicación que proporciona funciones de seguridad como el inicio de sesión único y el control centralizado del acceso del usuario a aplicaciones web.

instrumentación inteligente

La *instrumentación inteligente* es un método que utiliza DX APM para instrumentar aplicaciones. Este método utiliza rastreadores de baja sobrecarga y altamente optimizados. Los rastreadores permiten a los agentes detectar e instrumentar automáticamente más métodos para proporcionar una visibilidad exhaustiva a los componentes sin tener que utilizar las directivas de ProbeBuilder (PBD). La instrumentación inteligente también proporciona el seguimiento automático de la transacción.

Consulte también: seguimiento automático de la transacción, componentes de visibilidad exhaustiva

base de datos SmartStor

La *base de datos SmartStor* es una base de datos no relacional que registra todos los datos de rendimiento de las aplicaciones (métricas de agente) en todo momento. Esta base de datos permite a los usuarios analizar los datos históricos para identificar las causas raíz de la indisponibilidad de las aplicaciones o para realizar el análisis de capacidad sin necesidad de tener una base de datos externa.

SmartStor se activa de forma predeterminada durante la instalación de DX APM. Los datos de SmartStor se establecen para que sean antiguos con el tiempo para que el almacén de datos no se haga demasiado grande. Existen varios archivos de datos y crecen en número a medida que se generan más datos.

Consulte también: base de datos de APM, base de datos de eventos de la transacción

especificación

Una *especificación* es un requisito para una transacción o un componente de una transacción. Si una transacción o un componente no cumple con el requisito que se establece en la especificación relacionada, se define como un defecto. Por ejemplo, un defecto de tiempo lento puede definirse como el tiempo de cualquier transacción que sea mayor a 5 segundos.

Consulte también: defecto, límite de especificación superior

detención

Una *detención* de DX APM suele hacer referencia a los métodos que se han iniciado, pero que con los tiempos de invocación han superado un umbral.

Consulte también: métrica

burbuja de inicio

Una *burbuja de inicio* es el período de tiempo temporal cuando hay una demanda elevada de recursos que puede afectar a algo más que la generación de informes de la métrica de DX APM. Durante la burbuja de inicio, es posible que la aplicación instrumentada deje de responder.

Es posible que otros componentes se vean afectados al compartir el uso de los recursos con la aplicación instrumentada o por estar en el mismo entorno. La burbuja de inicio puede comprobarse con el Agente de .NET en el momento de inicio.

Consulte también: Agente de .NET

complementos con estado

Los *complementos con estado* deben ser scripts de larga ejecución (por ejemplo, daemons). Los complementos con estado se inician cuando se inicia Environment Performance Agent (EPAgent) y se ejecutan para siempre, alimentando datos a DX APM a través del canal de salida estándar del complemento. Cuando finaliza un complemento con estados, EPA lo reinicia.

Consulte también: Environmental Performance Agent (EPAgent, EPA), complementos sin estado

complementos sin estado

Los *complementos sin estado* están diseñados para ejecutarse según una programación repetitiva y se configuran con la frecuencia (especificada como el retraso entre ejecuciones) en la que se deben ejecutar. Se espera que los complementos sin estado sean scripts de corta duración que simplemente recopilan algunos datos, los envían a Environment Performance Agent (EPA) a través del canal de salida estándar y finalizan. El EPA no realiza ninguna comprobación de errores especial para garantizar que se está ejecutando una única instancia del complemento sin estado, por lo que los desarrolladores de complementos deben diseñar sus complementos sin estado para ejecutarse y completarse en un tiempo mínimo razonable.

Consulte también: Environmental Performance Agent (EPAgent, EPA), complementos con estado

SuperDomain

El nodo *SuperDomain* contiene métrica para todos los agentes que notifican al Enterprise Manager al que está conectada la Workstation e incluye todos los agentes y dominios definidos por el usuario. Este nodo solo es visible para los usuarios con acceso de SuperDomain. Las métricas se organizan en la jerarquía Host|Proceso|Agente.

métrica de compatibilidad

Las *métricas de compatibilidad* de DX APM ayuda a dar soporte al correcto funcionamiento de Enterprise Manager. Enterprise Manager genera y recopila métrica sobre sí mismo que es útil para evaluar su estado y para determinar lo bien que lo hace teniendo en cuenta su carga de trabajo.

componente de back-end de Blame sospechoso

El *componente de back-end de Blame sospechoso* es la parte más específica de la hora del back-end que se identifica como la causa del retardo en una transacción lenta. En DX APM, el componente de back-end de Blame sospechoso aparece como el componente de back-end más amplio, pero no necesariamente el más bajo, en la gráfica.

NOTE

Es el componente de back-end *más lento y más bajo*, pero no el componente de back-end *más bajo y más lento* en las gráficas de DX APM.

El componente de back-end de Blame sospechoso se identifica tomando el componente de back-end más bajo que tarda más de ¼ del tiempo total del back-end para completarse.

componente de Blame sospechoso

El *componente de Blame sospechoso* es la parte más específica de la lógica (o código de programa) que se identifica como la causa del retardo en una transacción lenta. En DX APM, el componente de Blame sospechoso aparece como el componente más amplio, pero no necesariamente el más bajo, en la gráfica.

NOTE

Es el componente *más lento y más bajo*, pero no el componente *más bajo y más lento* en las gráficas de DX APM.

El componente de Blame sospechoso se identifica tomando el componente (no back-end) más bajo que tarda más de ¼ del tiempo total de la transacción para completarse.

métrica de sostenibilidad

Una *métrica de sostenibilidad* proporciona información sobre el estado interno del agente en lugar de proporcionar el estado interno de la aplicación que el agente está monitorizando. Estos datos pueden ayudarle a investigar el comportamiento del agente.

Team Center

Team Center es una interfaz de usuario que proporciona una descripción general de un entorno de aplicación.

tiempo hasta la primera respuesta

El *tiempo hasta la primera respuesta* es el tiempo transcurrido desde el *último* paquete de la solicitud hasta el primer paquete de la respuesta para el componente.

El tiempo hasta la primera respuesta varía en función del tipo de defecto del que se está realizando un seguimiento:

- Defecto de componente, el tiempo hasta la primera respuesta para ese componente
- Defecto de transacción, el tiempo hasta la primera respuesta para el componente de identificación de la transacción
- Defecto de la transacción comercial, el tiempo hasta la primera respuesta para identificar el componente de la transacción de identificación

NOTE

Esta configuración se puede cambiar para el *primer* paquete de la solicitud para el primer paquete de la respuesta. Si necesita esta configuración para determinar la latencia de red entrante, póngase en contacto con el soporte de Broadcom.

El cambiar esta configuración solo afecta a los nuevos datos. (Los valores de datos existentes se basan en la configuración del tiempo hasta la primera respuesta que se encontraba en el momento en que se recopilaban los datos).

escala de tiempo

En la interfaz de usuario, la *escala de tiempo* permite ir del modo en directo al pasado para ver qué eventos de estado han ocurrido. La escala de tiempo permite investigar donde se ha iniciado un problema.

transacción

Una *transacción* de DX APM es la invocación y el procesamiento de un servicio. Es un ciclo de procesamiento completo, donde el contexto de la aplicación define la finalización:

- En el contexto de una aplicación web, es la invocación y el procesamiento de una dirección URL enviada desde un explorador web.
- En el contexto de un servicio web, es la invocación y el procesamiento de un mensaje SOAP desde un cliente de servicios web.

DX APM puede capturar las transacciones e incluir detalles acerca de la solicitud que se realiza en el servicio, así como los detalles relacionados con el procesamiento del servicio, como llamadas a una base de datos SQL.

Una transacción normalmente consta de un componente HTML, seguido por ninguno o más subcomponentes (por ejemplo, una hoja de estilo CSS, archivos de JavaScript JS e imágenes GIF y JPG). Para cada transacción, hay un componente de la transacción de identificación.

Una única acción del usuario puede resultar en una o más transacciones que se encapsulan en una transacción comercial.

Consulte también: jerarquía de transacciones

base de datos de eventos de la transacción

La *base de datos de eventos de la transacción* contiene datos detallados de la transacción. Estos datos incluyen seguimientos de la transacción, detenciones y datos que se recopilan de los eventos activados como, por ejemplo, instantáneas de error.

La base de datos de eventos de la transacción normalmente reside en el directorio de seguimientos y abarca varios archivos. Se crea un archivo al día y se almacenan los datos durante el número de días especificado.

Consulte también: base de datos de APM, base de datos de SmartStor, transacción, Transaction Tracer

jerarquía de transacciones

Las métricas y la información de DX APM se organizan en una *jerarquía de transacciones*. Esta jerarquía es una forma de traducir los servicios empresariales y las transacciones comerciales en los elementos HTTP técnicos que crean la experiencia del cliente.

La jerarquía de transacciones de DX APM es la siguiente:

Una aplicación del negocio es un programa de software que automatiza un servicio empresarial. Cada una de las transacciones (utilizando el servicio empresarial, la transacción comercial y, por último, la transacción) se asocia con una aplicación del negocio.

Ejemplo: Siebel

Ejemplo: Avitek

Un servicio empresarial es un grupo arbitrario de transacciones comerciales.

Ejemplo: Avitek Financial (incluye compra, venta y consulta)

Ejemplo: Siebel Call Center (incluye el inicio de sesión, además de otras transacciones comerciales de Siebel)

Una transacción comercial es un conjunto de transacciones que representa una acción del usuario.

Ejemplo: Conjunto relacionado con la compra (puede incluir varias transacciones relacionadas con la compra)

Ejemplo: Conjunto relacionado con la venta (puede incluir varias transacciones relacionadas con la venta)

Una transacción es un conjunto de componentes de la transacción que generalmente representa una solicitud al servidor de aplicaciones.

Ejemplo: Compra (la transacción real de compra)

Ejemplo: Consulta del precio de compra (una consulta relacionada con la compra)

Se utiliza un componente de la transacción comercial en DX APM como alternativa al conjunto completo de las transacciones y componentes de la transacción que pertenecen a una transacción comercial. El componente de la transacción comercial se corresponde con el componente de la transacción de identificación de la transacción de identificación, cuyo nombre tiene.

Ejemplo: Envío de la compra (el elemento de identificación para la transacción y la transacción de identificación para la transacción comercial)

Un componente de la transacción es un elemento de bajo nivel que representa un par de solicitud/respuesta HTTP.

Ejemplo: Envío de compra (el elemento de identificación de la transacción que puede ser JavaScript)

Ejemplo: main.css (un elemento de no identificación pero importante para la transacción)

Un parámetro de la transacción es el elemento de nivel más bajo en la jerarquía; un par de nombre/valor HTTP.

Ejemplo: Ruta de dirección URL=/dir/file.html (el elemento de identificación del componente)

Ejemplo: Cookie=JSESSIONID

parámetro de la transacción

Un *parámetro de la transacción* es un par nombre/valor HTTP, que consta de un tipo, un nombre y un patrón. Los ejemplos incluyen la dirección URL, consulta, post y cookie (por ejemplo: URL Host=www.company.com).

Consulte también: jerarquía de transacciones

El *tamaño de la transacción* es el tamaño, en bytes, del tráfico HTTP observado para una transacción. El tamaño incluye el encabezado HTTP y tanto las solicitudes como las respuestas HTTP. El tamaño no incluye los encabezados de Ethernet, IP y TCP.

seguimiento de la transacción

Un *seguimiento de la transacción* es la salida de Transaction Tracer. El seguimiento contiene una lista de componentes que se ejecutan durante una transacción y sus períodos de duración asociados.

Consulte también: Transaction Tracer

duración del seguimiento de la transacción

La *duración del seguimiento de la transacción* es el tiempo de ejecución de la *sesión de seguimiento de la transacción*.

La duración máxima de la sesión de seguimiento de la transacción es un límite de tiempo. El valor predeterminado es de 30 minutos.

Consulte también: Transaction Tracer

umbral de tiempo del seguimiento de la transacción

El *umbral de tiempo del seguimiento de la transacción* es el límite del tiempo de ejecución de la *transacción*. Cuando se está ejecutando un seguimiento de la transacción, se realiza un seguimiento de todas las transacciones que no se completan en el umbral.

El umbral de tiempo del seguimiento de la transacción es un porcentaje, que se basa en la especificación del defecto de tiempo lento. Por ejemplo, la especificación del defecto de tiempo lento se establece en 8 segundos y se establece el umbral de tiempo del seguimiento de la transacción en 25 por ciento. Se realiza un seguimiento de todas las transacciones con un componente de Blame sospechoso (tiempo de lógica) superior a 2 segundos.

Consulte también: tiempo de lógica, componente de Blame sospechoso, Transaction Tracer

Transaction Tracer

Transaction Tracer monitoriza la actividad de las transacciones individuales a medida que fluyen a través de estos límites:

- De una sola máquina virtual Java (JVM)
- La plataforma virtual Common Language Runtime (CLR), en el caso de .NET.

Transaction Tracer reduce el tiempo necesario para identificar los componentes con problemas en una transacción. El rastreador permite realizar un seguimiento de la actividad de la transacción a nivel del componente.

tiempo de transferencia

En App Synthetic Monitor, el *tiempo de transferencia* es el período necesario para completar los datos de respuesta HTTP.

volumen de la transacción

El *volumen de la transacción* es la suma de tamaños de todas las transacciones durante un período de tiempo especificado.

evaluación de errores

La *evaluación de errores* es el proceso de:

1. Recopilar información relevante para un problema.
2. Decidir la gravedad del problema.
3. Asignar el problema a la persona que podrá corregirlo más rápidamente. La persona que gestiona esta fase del análisis de problemas puede llamarse evaluador de errores.

universo

Un *universo* es un grupo significativo de componentes que se adapta a las necesidades de un usuario o grupo concreto en la interfaz de usuario.

límite de especificación superior (USL)

El *límite de especificación superior*, o USL, es un valor numérico que define el valor más alto aceptable para la característica. Por ejemplo, un USL puede ser el rendimiento de la transacción más alto aceptable.

Conjunto de reglas de coincidencia de dirección URL

El conjunto de reglas de coincidencia de URL es la dirección URL que se debe monitorizar.

base de datos de la varianza

La *base de datos de la varianza* de DX APM almacena los estados de perfil de la predicción y desviación más recientes para las métricas que evalúa el análisis diferencial. Estos perfiles sirven como entrada para el motor de reglas interno. El motor, a continuación, genera la intensidad de la varianza para la métrica que se muestra en el mapa del análisis diferencial en WebView.

Consulte también: base de datos de APM, métrica heurística, base de datos de SmartStor, base de datos de eventos de la transacción

WebView

WebView presenta las vistas de árbol de Investigator y los cuadros de mandos personalizables en una interfaz del explorador. *WebView* permite que la información vital se pueda visualizar sin la ayuda de Workstation. Consulte también: Workstation Web Start

Workstation

Workstation permite controlar DX APM y acceder a las métricas de rendimiento. En la estación de trabajo puede realizar las siguientes acciones, entre otras:

- Establecer alertas para métricas individuales o para grupos de métricas lógicas.
- Ver métrica de rendimiento.
- Personalizar las vistas para su propio entorno único.

Consulte también: *Workstation Web Start*

Workstation Web Start

Workstation Web Start utiliza Java Web Start para iniciar Workstation.

Como administrador, se pueden crear y configurar alertas y acciones en Team Center para monitorizar el rendimiento. Team Center ofrece las siguientes alertas:

- Alerta sencilla
- Alertas de resumen

Para obtener más información sobre cómo crear, actualizar, suprimir y configurar una alerta sencilla, consulte [Creación y configuración de alertas sencillas en Team Center](#).

Reconocimientos de software de terceros para SaaS

Esta sección contiene los acuerdos de licencia de software de terceros para aplicaciones que se agregan o incluyen como parte de la versión actual de DX APM. Haga clic [aquí](#) para descargar los TPSR.

Implementación de los agentes

Obtenga más información sobre cómo implementar uno o más agentes en función de los entornos que monitoriza.

El *agente* es un componente de recopilación de datos. El componente recopila información de rendimiento detallada sobre las aplicaciones y el entorno informático mientras se ejecutan las transacciones. Se dice que se está instrumentado una aplicación web que informa a un agente sobre la métrica. Una vez instrumentada la aplicación web, el agente recopila los datos e informará a Enterprise Manager. A continuación, Enterprise Manager procesa y almacena los datos para los informes históricos y en tiempo real. A partir de este momento, se puede consultar y trabajar con los datos recopilados para crear alertas o tomar medidas de capacidad de respuesta. Se puede modificar la monitorización predeterminada para lograr el equilibrio necesario entre visibilidad y rendimiento. Una *extensión de agente* es el código del programa que amplía las funciones básicas del agente.

Para obtener más información sobre el agente, consulte [Agentes de DX APM](#).

Utilice los siguientes vínculos para acceder a la documentación de algunos de los agentes clave:

- [Agente de Java](#)
- [Agente de .NET/.NET Core](#)
- [Agente de la infraestructura](#)
- [Analizador de la carga empresarial](#)
- [Agente de Node.js](#)

Configuración del entorno de monitorización

El entorno de monitorización permite identificar, medir y evaluar el rendimiento de una aplicación. Puede realizar tareas para configurar el entorno de monitorización para satisfacer sus necesidades.

Creación de valores de configuración favoritos

Se pueden marcar los mosaicos como favoritos en la página **Configuración**. Haga clic en el icono de **anclar** en el mosaico para agregar el valor de configuración como favorito en el panel de navegación de la izquierda. Para eliminar la configuración de los favoritos, haga clic en el icono **Eliminar** de la configuración en el panel de navegación de la izquierda.

Configuraciones disponibles

En la página **Configuración** se encuentran disponibles las configuraciones siguientes:

Si desea...	Lea esta información...
Configuración de valores de configuración generales	<ul style="list-style-type: none"> • Configuración y descarga de un paquete del agente para DX APM • Organización de los componentes utilizando perspectivas • Configuración de universos • Cómo adaptar la monitorización de su entorno con reglas de atributo • Seguridad • Notificaciones • Descargas <ul style="list-style-type: none"> — Descarga de estación de trabajo — Descarga de Cloud Proxy — Herramienta de importación de agentes <p>Nota: Solo se puede acceder a la herramienta de importación de agentes como administrador principal.</p> <ul style="list-style-type: none"> • Reglas de supresión de seguimiento para ocultar datos confidenciales
Configuración de los valores de configuración del módulo de gestión	<ul style="list-style-type: none"> • Creación y trabajo con módulos de gestión • Configuración de agrupaciones de métrica en Team Center • Creación y configuración de alertas sencillas en Team Center • Creación y edición de calculadoras
Configuración de integraciones	<ul style="list-style-type: none"> • Analizador de la carga empresarial • Configuración de WebView (solo en la instancia local de DX APM) • APM Command Center (acceso de solo administrador) <p>Nota: WebView solo está disponible en la instancia local de DX APM. En DX APM local, WebView no está activado de forma predeterminada. Sin embargo, se puede activar WebView para clientes específicos durante la creación de clientes. También se puede activar WebView más tarde para cualquier cliente creado anteriormente. Para obtener más información sobre la activación de WebView, consulte Servicios de clientes. Al acceder a WebView y APM Command Center, se abre una nueva ficha.</p>
Configuración de otros valores	Active la descarga de agentes desde la configuración avanzada de Team Center.

Configuraciones de entorno adicionales

Aparte de las configuraciones disponibles en la página **Configuración**, se pueden realizar las siguientes tareas para configurar el entorno.

- [Creación de notificaciones de alerta](#)
- [Configuración de notificaciones de correo electrónico para las alertas](#)
- [Configuración de la Vista de experiencia](#)
- [Ajuste de la monitorización con alertas](#)
- [Configuración de Workstation](#)
- [Recomendaciones de tamaño para el Monitor de Docker](#)

El entorno de monitorización permite identificar, medir y evaluar el rendimiento de una aplicación.

Para obtener más información sobre las tareas que se pueden realizar para configurar el entorno de monitorización para cubrir sus necesidades, consulte [Configuración del entorno de monitorización](#).

Roles y privilegios admitidos

En la plataforma DX, se admiten los roles siguientes.

- **Administrador de clientes**
- **Usuario avanzado**
- **Usuario**

En DX APM, los mismos roles se correlacionan de la siguiente manera:

- Administrador de clientes → **Administrador de APM**
- Usuario avanzado → **Usuario de APM**
- Usuario → **Usuario de APM**

Roles y privilegios de DX APM

Las vistas en Team Center y otras interfaces de usuario tienen distintos niveles de acceso para cada rol.

- [Vista de experiencia \(EV\)](#)
- [Vista de agente \(AV\)](#)
- [Perspectiva](#)
- [Atributos personalizados](#)
- [Universos](#)
- [Reglas](#)
- [Agentes](#)
- [Seguridad](#)
- [Alertas](#)
- [Notificación](#)
- [Módulos de gestión](#)
- [Agrupación de métricas y calculadoras](#)
- [Calculadoras de JavaScript](#)
- [Descargas](#)
- [AXA en el cuadro de diálogo de descarga del agente](#)
- [Página Configuración](#)

Vista de experiencia (EV)

Acción	Administrador	Usuario	Usuario avanzado
Modificar posición	Sí	Sí	Sí
Agregar nueva EV	Sí	Sí	Sí
Convertir en EV global	Sí	No	No
Editar EV	Sí	Sí	Sí
Suprimir EV	Sí	Sí	Sí
Editar EV global	Sí	No	No
Suprimir EV global	Sí	No	No

Vista de agente (AV)

Acción	Administrador	Usuario	Usuario avanzado
Agregar nueva AV	Sí	Sí	Sí
Convertir en AV global	Sí	No	No
Editar AV	Sí	Sí	Sí
Suprimir AV	Sí	Sí	Sí
Editar AV. global	Sí	No	No
Eliminar AV global	Sí	No	No

Perspectiva

Acción	Administrador	Usuario	Usuario avanzado
Crear perspectiva	Sí	Sí	Sí
Editar perspectiva	Sí	Sí	Sí
Convertir en perspectiva global	Sí	No	No
Convertir en perspectiva predeterminada	Sí	No	No
Suprimir perspectiva	Sí	Sí	Sí
Personalizar perspectiva	No	Sí	Sí

Atributos personalizados

Acción	Administrador	Usuario	Usuario avanzado
Crear	Sí	No	Sí
Suprimir	Sí	No	Sí
Modificar	Sí	No	Sí

Universos

Acción	Administrador	Usuario	Usuario avanzado
Crear universo	Sí	No	No
Renombrar universo	Sí	No	No
Editar lista de usuarios	Sí	No	No
Suprimir universo	Sí	No	No

Reglas

Acción	Administrador	Usuario	Usuario avanzado
Crear reglas	Sí	No	No
Suprimir reglas	Sí	No	No
Crear reglas de empresa	Sí	No	No
Suprimir de reglas de empresa	Sí	No	No
Duplicado	Sí	No	No
Cargar reglas	Sí	No	No

Agentes

Acción	Administrador	Usuario	Usuario avanzado
Descargar agente	Sí	No (El administrador puede controlar en Configuración)	Sí
Realiza un seguimiento de todos los agentes.	Sí	No	Sí
Realizar un seguimiento de un agente individual	Sí	No	Sí
Mostrar detalles de la conexión del agente	Sí	Sí, pero (el botón Generar token depende de la visibilidad del cuadro de diálogo de descarga del agente)	Sí

Seguridad

Acción	Administrador	Usuario	Usuario avanzado
Crear token de la API	Sí	Sí	Sí
Generar token del agente	Sí	Sí, si el cuadro de diálogo de descarga del agente es visible (se puede controlar mediante el administrador en Configuración)	Sí
Crear token del sistema	Sí	No	No

Acción	Administrador	Usuario	Usuario avanzado
Invaldar token	Sí	Propio	Propio
Renombrar	Sí	Propio	Propio
Establecer caducidad	Sí	Propio	Propio

Alertas

Acción	Administrador	Usuario	Usuario avanzado
Leer alerta	Sí	Sí	Sí
Crear alerta	Sí	No	No*
Suprimir alerta	Sí	No	No*
Activar o desactivar alerta	Sí	No	No*
Editar alerta	Sí	No	Sí

Notificación

Acción	Administrador	Usuario	Usuario avanzado
Lectura	Sí	Sí	Sí
Crear notificación	Sí	No	No

Módulos de gestión

Acción	Administrador	Usuario	Usuario avanzado
Lectura	Sí	Sí	Sí
Crear	Sí	No*	No*
Modificar	Sí	No*	No*
Suprimir	Sí	No*	No*

Agrupación de métricas y calculadoras

Acción	Administrador	Usuario	Usuario avanzado
Lectura	Sí	Sí	Sí
Crear	Sí	No*	No*
Suprimir	Sí	No*	No*
Modificar	Sí	No*	No*

Calculadoras de JavaScript

Acción	Administrador	Usuario	Usuario avanzado
Lectura	Sí	Sí	Sí
Crear	Sí	No	No

Acción	Administrador	Usuario	Usuario avanzado
Modificar	Sí	No	No
Suprimir	Sí	No	No

Descargas

Acción	Administrador	Usuario	Usuario avanzado
Acceder a la página Descarga	Sí	Sí	Sí

AXA en el cuadro de diálogo de descarga del agente

Acción	Administrador	Usuario	Usuario avanzado
Crear la aplicación AXA (en el cuadro de diálogo de descarga del agente)	Sí	No	Sí

Página Configuración

Acción	Administrador	Usuario	Usuario avanzado
Acceso a Command Center (mosaico de ACC)	Sí	No	Sí

* Este privilegio es la opción predeterminada. A los usuarios y grupos se les pueden conceder privilegios mediante el módulo de seguridad del universo.

Más información: [Configuración de universos](#).

La plataforma DX es compatible con los roles siguientes:

- Administrador de clientes
- Usuario avanzado
- Usuario

Para obtener más información sobre los roles de DX APM y sus privilegios, consulte [Roles y privilegios admitidos](#).

Generación de un token de seguridad

Los tokens de seguridad se utilizan para autenticar solicitudes y autorizar la concesión a los agentes. Mediante la configuración de **seguridad**, se pueden generar tokens sin conexión que nunca caducan. Estos tokens se utilizan para acceder a las API públicas. También se pueden generar tokens para autorizar a agentes o clientes.

IMPORTANT

La generación de tokens de seguridad es una tarea de solo administrador. Debe ser un administrador principal para generar el token de seguridad. Si es un cliente, póngase en contacto con el equipo de operaciones de Broadcom SaaS para obtener un token de seguridad.

Generación de un token

Siga estos pasos:

1. Inicie sesión en Team Center y haga clic en el mosaico **Configuración, Seguridad**.
2. Haga clic en **Generar un token nuevo**.

Aparecerá el cuadro de diálogo **Nuevo token de seguridad de la API**.

3. Defina los detalles siguientes:

- **Etiqueta** (nombre): Nombre del token de seguridad.
- Seleccione el tipo de token de seguridad:
 - **Agente:** Token para autorizar un agente.

NOTE

La información de caducidad del token de un agente se define dentro del token. Por lo tanto, no se puede cambiar la caducidad del token después crearlo.

- **API pública:** Token para acceder a una API pública. Se puede establecer una fecha de caducidad para los tokens de la API pública o se puede establecer que el token no caduque nunca.
- **Token de cliente:** Token para conceder acceso a un cliente.

NOTE

La información de caducidad del token de un cliente se define dentro del token. Por lo tanto, no se puede cambiar la caducidad del token después crearlo.

4. Haga clic en **Generar token**.

El sistema genera un nuevo token.

WARNING

Por razones de seguridad, solo verá un token una vez. Guarde el token en un lugar seguro antes de cerrar este cuadro de diálogo. No revele nunca el token a personal no autorizado.

El token ahora aparece entre los otros tokens en la ficha **Seguridad**.

Gestión de tokens

Para cada token, se pueden realizar las siguientes acciones:

- **Renombrar:** Si desea cambiar el nombre del token
- **Revocar:** Si se desea revocar la autorización para las API o los agentes
- **Cancelar la revocación:** para restaurar la autorización de las API o los agentes
- **Establecer caducidad:** En el caso de las API públicas, si se ha establecido que el token no caduque nunca, utilizando la opción **Establecer caducidad** se puede elegir una fecha y hora en la que caduque el token, es decir, cuando no se pueda utilizar el token para autorizar a las API públicas.

Los tokens de seguridad se utilizan para autenticar solicitudes y autorizar la concesión a los agentes. Mediante la configuración de seguridad, se pueden generar tokens sin conexión que nunca caducan. Estos tokens se utilizan para acceder a las API públicas. También se pueden generar tokens para autorizar a agentes o clientes.

Para obtener más información sobre los tokens de seguridad, consulte [Generación de un token de seguridad](#).

Creación de notificaciones de alerta

DX APM permite crear notificaciones para alertas. Las notificaciones pueden retransmitir automáticamente alertas de Application Performance Management a través de servicios internos como por ejemplo listas de distribución, a servicios externos a través de la API de REST o de PagerDuty, una plataforma de resolución de incidentes.

Para obtener más información sobre la configuración de notificaciones de correo electrónico, consulte [Configuración de notificaciones de correo electrónico para las alertas](#).

El video siguiente muestra la terminología, el flujo de trabajo y los ejemplos necesarios para crear las notificaciones para las alertas.

PagerDuty

PagerDuty realiza un análisis de los incidentes y envía las notificaciones directamente a los administradores de TI designados para su resolución. Utilice la integración de PagerDuty para monitorizar el sistema para eventos críticos a través de una ruta definida, responder con rapidez y mantener el sistema operativo con el tiempo de inactividad mínimo. Para obtener más información sobre las capacidades de PagerDuty, vaya a <https://www.pagerduty.com>.

Para que funcione eficazmente en los dos sistemas, siga las reglas siguientes:

- Una alerta en DX APM activa un incidente en PagerDuty. A continuación, PagerDuty transmite el incidente como un ticket a un destinatario designado.
- Una alerta que se desactiva en DX APM resuelve el incidente en PagerDuty. La resolución de un incidente en PagerDuty no desactiva la alerta de Application Performance Management.

Flujo de trabajo de un incidente

Cuando se genera una alerta y coincide con los valores de configuración del servicio, DX APM activa automáticamente un incidente. Los incidentes en PagerDuty contienen la siguiente información para que una alerta pueda identificar el componente afectado:

- `alertStartTime`
- `alertState`
- `alertName`
- `alertId`
- `vertexId`
- `vertexAttributes` (por ejemplo, tipo, nombre)

A continuación, PagerDuty gestiona los incidentes según las políticas configuradas y los valores de configuración del usuario.

NOTE

Una alerta desactivada en DX APM resuelve automáticamente un incidente en PagerDuty. El retraso de notificación es un período de tiempo que DX APM espera antes de activar un incidente en PagerDuty. El retraso en la notificación es útil para reducir el número de incidentes que se activan por alertas transitorias.

Creación y modificación de una notificación de PagerDuty

Se debe disponer de una cuenta de PagerDuty para crear una notificación de PagerDuty. La cuenta de PagerDuty permite configurar el comportamiento de las notificaciones y recibir un token de usuario de la API único y la clave de integración para utilizarlos con DX APM.

Siga estos pasos:

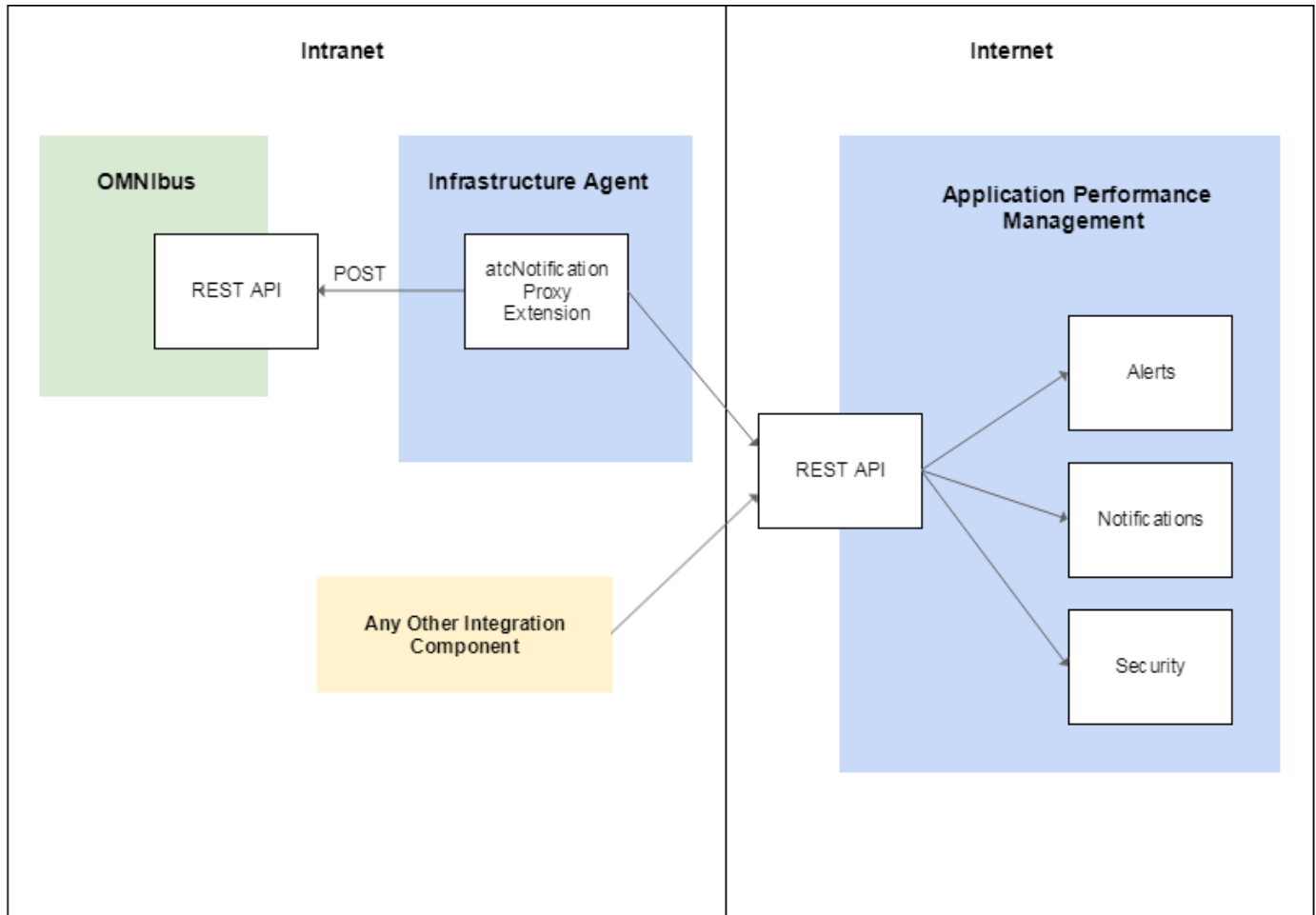
1. Inicie sesión en [PagerDuty](#) o cree una cuenta.
2. Copie el token de usuario de la API y la clave de integración de PagerDuty.
3. En DX APM, haga clic en **Notificaciones**.
4. Haga clic en **Create a PagerDuty Notification (Crear una notificación de PagerDuty)**.
5. Cree un nombre para la notificación.
6. Pegue el token de usuario de la API y la clave de integración de PagerDuty.
7. Seleccione la severidad para la notificación.
8. Haga clic en **Guardar**.
9. (Opcional) Seleccione la notificación que desee cambiar y haga clic en **Editar**.
10. (Opcional) Seleccione la notificación que desee suprimir y haga clic en **Suprimir**.

Se ha creado y modificado una notificación de PagerDuty en función de sus necesidades.

Notificaciones de la API de REST

DX APM permite recibir notificaciones acerca de cambios en alertas a través de la API de REST. La API de REST es la interfaz de extracción que permite a las integraciones que se ejecuten tras los cortafuegos corporativos. Utilice la API para integrar las notificaciones con componentes de terceros, como varios cuadros de mandos. El siguiente diagrama muestra la API de REST de la infraestructura de Application Performance Management:

Figure 1: Notificación de la API de REST



Creación y modificación de una notificación de la API de REST

Siga estos pasos:

1. En DX APM, haga clic en **Notificaciones**.
2. Haga clic en **Create a REST API Notification (Crear una notificación de la API de REST)**.
3. Cree un nombre para la notificación.
4. Cree un token de proxy único o haga clic en **Generar token**.
5. Haga clic en **Guardar**.
6. (Opcional) Seleccione la notificación que desee cambiar y haga clic en **Editar**.
7. (Opcional) Seleccione la notificación que desee suprimir y haga clic en **Suprimir**.

Se ha creado y modificado una notificación de la API de REST en función de sus necesidades.

Integración de las notificaciones de la API de REST

Acceda a la API de REST para integrar las notificaciones de la API de REST con componentes de terceros.

Siga estos pasos:

1. Genere un token de seguridad **Configuración** de DX APM. Guarde el token de seguridad para utilizarlo más adelante. Para obtener más información sobre cómo generar un token de seguridad, consulte [Autorización y autenticación de la API](#).
2. Vaya a **Notificaciones** y copie el token del proxy de la notificación de la API de REST que vaya a integrar. Guarde el token del proxy para utilizarlo más adelante.

NOTE

Se puede utilizar el mismo token del proxy para varias notificaciones en DX APM. La API de REST devuelve las notificaciones de alerta desde todas estas configuraciones de notificación. La llamada de la API de REST etiqueta el token del proxy como `proxyKey`. `proxyKey` identifica al cliente de la API de REST.

3. Establezca el último valor de versión en 0 para recibir estados de mal funcionamiento (precaución o peligro) para todas las alertas activas.
4. Copie el número de host de la dirección URL de DX APM. Guarde el número de host para utilizarlo más adelante.
5. Pegue el número de host, el token de seguridad, el token del proxy y la última versión en el siguiente comando POST para llamar a la API de REST:

POST

Host: `https://<YOUR HOST NUMBER>.apm.cloud.ca.com/apm/appmap/private/graph/recentstatuschanges`

Respuesta:

La API de REST envía un objeto JSON como respuesta. La respuesta contiene los cambios de alerta para todas las notificaciones con el mismo valor de token del proxy que se hayan producido después de la última llamada. La respuesta devuelve también el campo versión de la siguiente llamada.

En la respuesta, cada notificación contiene los campos siguientes:

- **status:** Indica la severidad de la alerta (correcto, precaución, o peligro).
- **alertName:** Define el nombre de la alerta.
- **time:** Indica el cambio de estado en milisegundos desde la [época de Unix](#).
- **vertex:** Define el vértice de la alerta, incluidos los atributos del vértice.

Ejemplo de respuesta:

```
{
  "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
}

```

Códigos de error y estados HTTP de la autenticación

Si se produce un error de autenticación de una solicitud, el servidor de recursos devuelve un código de error HTTP y un encabezado de respuesta con los detalles del error.

- 401 - No autorizado: El token de seguridad (enviado en un encabezado HTTP) no es válido para la dirección URL proporcionada.
- 403 - Prohibido: El token del proxy no coincide con ninguna configuración de notificación.

Para obtener más información, consulte [Definiciones de código de estado HTTP](#).

DX APM permite crear notificaciones para alertas. Las notificaciones pueden retransmitir automáticamente alertas de Application Performance Management a través de servicios internos como por ejemplo listas de distribución, a servicios externos a través de la API de REST o de PagerDuty, una plataforma de resolución de incidentes.

Para obtener más información sobre notificaciones, consulte [Creación de notificaciones de alerta](#).

Configuración de notificaciones de correo electrónico para las alertas

Se puede asociar una alerta en DX APM con listas de distribución de correo electrónico predefinidas. Se notifica a los usuarios que se han agregado a las listas de distribución, por ejemplo, los administradores de TI, cuando el valor de la métrica supera los umbrales de precaución o de peligro.

NOTE

Los umbrales de precaución y peligro de DX APM se denominan umbrales graves y críticos (respectivamente) en DX SaaS.

Crear una lista de correo

1. Inicie sesión en DX SaaS como administrador de clientes.
2. Seleccione **Notificaciones** (icono de la campana) en el panel de navegación izquierdo.
3. Haga clic en la flecha al final de la fila de **listas de distribución**.
4. Haga clic en **+ Nuevo**.
5. Especifique el nombre de la lista de distribución y agregue direcciones de correo electrónico.
6. Guarde la lista de distribución.

Asociación de una lista de distribución con una alerta

Se asocia una lista de distribución con una alerta en DX APM.

WARNING

Los cambios en las listas de distribución, como la adición o eliminación de una nueva dirección, no aparecen en el panel Alertas hasta después de 10 minutos. Si no aparece la nueva lista de distribución en una alerta, compruebe la alerta de nuevo después de 10 minutos.

Siga estos pasos:

1. En DX APM, haga clic en el icono **Alertas** en el panel izquierdo. Se abre el panel Alertas.
2. Seleccione la alerta que desea editar. Se abre la lista desplegable Alerta.
3. Haga clic en el menú desplegable **Notificaciones**. Aparecerá una lista de todas las listas de distribución disponibles.
4. Seleccione las listas de distribución donde desea que se reciban notificaciones acerca de esta alerta.

NOTE

Anule la selección de las listas de distribución no válidas que aparecen en rojo. Las listas de distribución no válidas son listas que se han suprimido.

5. Haga clic en **Aceptar** y **Guardar alerta**.

Configuración de universos

Universos

Los universos permiten al administrador ajustar el número y los tipos de componentes en grupos de autorización fáciles de usar. Este grupo que se ha ajustado es un universo. Por razones de seguridad, no hay ninguna asignación predeterminada para todos los usuarios. Para ver DX APM, cada usuario se debe asignar a un universo. Si no hay ningún universo asociado con el ID de usuario, se enviará una advertencia al usuario. Como administrador, cree universos para los usuarios. Utilice el universo predeterminado denominado **Todos los componentes** o cree un universo personalizado.

El administrador realiza las tareas siguientes para configurar los universos:

- Crea un universo según las necesidades de los usuarios o de los grupos de usuarios.
- Aplica un filtro para seleccionar los datos del componente del conjunto de datos.
- (Opcional) Crea numerosos universos para crear una serie de espacios fáciles de gestionar. Los usuarios pueden cambiar fácilmente entre los espacios para facilitar la navegación del entorno.
- (Opcional) Garantiza que se restringe el acceso a usuarios específicos según sea necesario por requisitos de seguridad de la empresa.

NOTE

Cree un universo basado en dominios. Cree un filtro **Fuentes de la métrica** y utilice las mismas expresiones regulares de la definición del dominio. Cree un filtro para los componentes del mapa que se base en el atributo **agentDomain**, seleccione el dominio que desee y haga clic en **Guardar**.

Como administrador de APM, asigne al menos un universo a cada usuario para que puedan acceder al contenido.

Un universo está formado por:

- Un nombre: un identificador único
- Una descripción: texto opcional para describir el universo
- Filtros:
 - Filtro de fuentes de métricas: aplicable en una Vista de métrica y en los Gráficos de métrica de la Vista de mapa.
 - Filtro de componentes del mapa: aplicable en todas las vistas basadas en el mapa, es decir, la Vista de mapa, la Vista de cuadro de mandos, la Vista de experiencia y la Vista de agente.
 - Filtro del módulo de gestión: aplicable cuando se visualiza el contenido del módulo de gestión. Por ejemplo, alertas en el mapa o el cuadro de mandos. Además, se pueden configurar definiciones de calculadoras, fuentes de las métricas y alertas.
- Una lista de usuarios: los usuarios con acceso a este universo

Universos predefinidos

Algunos universos se crean de forma predeterminada:

- El universo **Todos los componentes** se crea automáticamente y contiene todos los componentes en el mapa, la fuente de la métrica y los módulos de gestión.
- El universo **Empresa** incluye todos los componentes del entorno. Este universo integrado no se puede suprimir ni definir y solo se asigna a los administradores. La finalidad de este universo es proporcionar a los administradores acceso a todos los datos. Este universo ni siquiera aparece en la página de **configuración** de los universos.

NOTE

- Los usuarios pueden estar asignados a más de un universo. En este caso, **Todos mis universos** está disponible en la **Vista de experiencia** y en la **Vista de agente**. **Todos mis universos** muestra datos de los universos de todos los usuarios en conjunto.
- La lista desplegable **Todos mis universos** también rellena los universos de DX Operational Intelligence (a excepción del universo Todos los accesos). Estos universos se marcan con una etiqueta de OI con su nombre en la lista desplegable. No se pueden editar los universos de DX Operational Intelligence en APM.

Existen dos casos de uso diferentes disponibles para la creación de universos:

- **Creación de un universo para la navegación:** cree universos para la navegación para proporcionar a los usuarios una serie de entornos filtrados configurados previamente. Los usuarios pueden alternar de forma rápida entre los entornos para poder ver diferentes áreas de un entorno complejo.
- **Creación de un universo para la seguridad:** cree universos para la seguridad para limitar los componentes del entorno que un usuario individual puede ver. Se recomienda basar el contenido de un universo de seguridad en rutas de la transacción. Cree atributos personalizados en los límites que permiten a los analistas identificar la continuación de la ruta. Si el entorno utiliza dominios, el atributo agentDomain se rellena de forma predeterminada. Utilice el atributo agentDomain como condición de filtro para crear un universo que coincida con las restricciones de permisos del dominio especificado.

Creación de un universo

Al definir un nuevo universo, se pueden conceder distintos derechos a los usuarios y a los grupos de usuarios. Los derechos para acceder al universo, seleccionar fuentes de las métricas, asignar componentes y gestionar módulos.

Siga estos pasos:

1. Tenga en cuenta el contenido que desea definir en este universo.
2. Seleccione **Universos** en el panel izquierdo y, a continuación, seleccione **Nuevo universo**.

Se abre un panel de diálogo.

NOTE

Las definiciones agregadas a una ficha se propagan a la parte individual correspondiente de la aplicación. Por ejemplo, las definiciones agregadas a los componentes del mapa se aplican al mapa. Las definiciones agregadas a las fuentes de las métricas se aplican al Explorador de métrica. Otras partes de la aplicación no se ven afectadas.

3. Asigne un nombre al nuevo universo.
4. (Opcional) Agregue una descripción para el universo.
5. En la vista **Acceso**, se conceden distintos derechos de acceso a este universo a los usuarios o grupos de usuarios.
 - a. Seleccione el derecho que desea conceder:
 - **Lectura:** permite a los usuarios ver los componentes que están seleccionados en el universo.
 - **Edición:** permite a los usuarios modificar los componentes que han seleccionado en el universo y agregar atributos o reglas a los componentes del mapa. También incluye derechos de lectura.
 - **Gestión:** permite a los usuarios modificar los derechos de acceso al universo. Los administradores utilizan el derecho de gestión para delegar la asignación de derechos de acceso a otros usuarios. También incluye derechos de lectura y edición.
 - b. Seleccione el usuario o grupo de usuarios al que desea conceder el derecho de la lista desplegable.
 - c. Haga clic en **Agregar usuario** o **Agregar grupo** para agregar el usuario o grupo de usuarios seleccionado al universo.
 - d. (Opcional) Seleccione otro derecho y usuario o grupo de usuarios, y agréguelos a la lista.
6. En la vista **Fuentes de la métrica**:
 - La nueva opción **Filtrar la Vista de métrica por los componentes del mapa** filtra los árboles de métrica en el explorador de métrica por mapa. Valor predeterminado: **true** (el filtro se aplica de forma predeterminada). Seleccione la casilla de verificación para desactivar el filtro.
 - Seleccione **Todas las fuentes de la métrica**, incluidos los componentes futuros. Si selecciona esta opción, el universo contiene todas las fuentes del mapa (agentes) y no se filtra nada.
 - Personalice las fuentes de la métrica seleccionando un subconjunto de agentes individuales o agregando una expresión regular. Las expresiones regulares se basan en `hostname|processname|agentname`. Ejemplos de expresiones:
 - `myhost\.*`: selecciona todos los agentes que se ejecutan en el host "myhost". El carácter de barra vertical se escapa con una barra diagonal inversa, ya que es un carácter de control de expresión regular.
 - `usnye.*`: selecciona los agentes de todo el host con el prefijo "usnye".
 - `.*\.*\dmn13t.*`: selecciona todos los agentes con el prefijo "dmn13t".

NOTE

Haga clic en **Volver a cargar** en el cuadro de diálogo de la parte inferior de la página para ver una vista previa del subárbol para los agentes seleccionados.

WARNING

Se deben volver a configurar las fuentes de las métricas de los universos creados antes de la versión 20.11.

7. En la vista **Componentes del mapa**, seleccione una de estas acciones:
 - Asignar todos los componentes (incluidos los futuros componentes). Si selecciona esta opción, el universo contiene todos los componentes del mapa y no se filtrará nada.
 - Utilice el filtro **Fuentes de las métricas**. Si selecciona esta opción, el universo contiene todos los componentes del mapa generados por los agentes seleccionados por el filtro **Fuentes de las métricas**.
 - Personalice el filtro. Defina un filtro del mapa para seleccionar los componentes del mapa necesarios. Este filtro es el mismo que el que está en la vista **Mapa**.

NOTE

Para obtener más información sobre el nodo de experiencia, consulte [Monitorización del rendimiento utilizando la Vista de experiencia](#).

8. En la vista **Módulos de gestión**, seleccione una de las siguientes opciones:
 - Todos los elementos (incluidos los elementos futuros).
 - Uno o más elementos de la lista.
9. La vista **Información** se genera después de guardar el universo. Esta vista contiene una descripción general de las definiciones de universo. La descripción general incluye el número de componentes en las diversas partes de la aplicación (por ejemplo, el mapa y la vista de métricas).
10. Seleccione **Guardar**.

NOTE

Como administrador, se puede crear un universo directamente desde el mapa en el universo "Enterprise". Defina los filtros de mapa y seleccione **Guardar como universo** en la esquina superior derecha para guardar los nodos de mapa filtrados actualmente como un universo.

Modificación de un universo**Siga estos pasos:**

1. En el panel izquierdo, seleccione **Universos**.
2. Identifique el universo que desee modificar y seleccione **Editar**.
3. Siga los pasos que se describen en la sección [Crear universo](#).

Supresión de un universo**Siga estos pasos:**

1. En el panel izquierdo, seleccione **Universos**.
2. Identifique el universo que desee eliminar y seleccione **Suprimir**.
3. Confirme la supresión.

Configuración de la seguridad del universo

En cada universo, a los usuarios se les asignan privilegios individuales para editar alertas, calculadoras y grupos de métricas. El rol del usuario avanzado, los usuarios y los grupos de usuarios deben tener permiso para ver o crear alertas, calculadoras o grupos de métricas para un módulo de gestión. El usuario avanzado puede iniciar manualmente las sesiones de seguimiento de transacciones. El administrador de clientes tiene todos los privilegios. Los privilegios tienen efecto solamente cuando se visualiza el universo especificado. Estos son los privilegios por tipo de permiso:

NOTE

De forma predeterminada, un usuario o usuario avanzado sin permiso en ningún universo no puede ver ningún agente o métrica en la Vista de métrica. Un usuario con permiso de lectura para un universo puede ver las métricas de agente configuradas del universo en la Vista de métrica.

- **lectura:** Permite al usuario, usuario o grupo de usuarios asignados ver las alertas, las calculadoras y los grupos de métrica del módulo de gestión.
- **escritura:** Permite al usuario, usuario o grupo de usuarios asignados ver y modificar las alertas, las calculadoras y los grupos de métrica del módulo de gestión.
- **gestión:** Permite al usuario, usuario o grupo de usuarios asignados ver y modificar las alertas, las calculadoras, los grupos de métrica y los usuarios del módulo de gestión. Los usuarios con el privilegio **gestión** también pueden agregar módulos de gestión al universo.

El administrador de clientes debe conceder explícitamente la ruta de la Fuente de las métricas al universo. Esta ruta permite a los usuarios con acceso al universo ver las métricas de la calculadora y de la alarma en el Árbol de métrica.

El administrador tiene el privilegio de elegir las entidades a las que los usuarios tendrán acceso. Esto incluye métricas, vértices y módulos de gestión.

- Con el permiso de **lectura**, el usuario solo puede ver las entidades, pero no puede cambiarlas.
- Con el acceso de **escritura**, el usuario puede cambiar las entidades. Por ejemplo, puede cambiar el contenido del módulo de gestión o agregar atributos personalizados a los vértices.
- El acceso de **gestión** proporciona al usuario el privilegio para cambiar la lista de acceso en el universo.

Se recomienda encarecidamente esta configuración para asegurarse de que los usuarios tengan el acceso correcto a la configuración de módulos de gestión:

- No asigne usuarios a un universo con una configuración del **Ámbito del módulo de gestión** de **Todos los elementos**.
- Agregue explícitamente **Módulos de gestión** como parte del ámbito de todos los universos *excepto* de Enterprise Universe. Enterprise Universe es un universo especial que solo está disponible para el administrador de clientes.

Más información: [Roles y privilegios admitidos](#)

Los universos permiten al administrador ajustar el número y los tipos de componentes en grupos de autorización fáciles de usar llamados universo. Para ver DX APM, cada usuario se debe asignar a un universo. Como administrador, es necesario crear universos para los usuarios. Utilice el universo predeterminado, denominado Todos los componentes, o cree un universo personalizado.

Para obtener más información sobre cómo gestionar y configurar universos, consulte [Configuración de universos](#).

Configuración de la Vista de experiencia

Como administrador, configure las tarjetas de experiencia en la Vista de experiencia. Configure las tarjetas para que los analistas puedan ver fácilmente el mayor número de componentes esenciales del negocio que afectan a la experiencia del usuario final.

Vista de experiencia

Los administradores pueden realizar las siguientes tareas:

- Configuración del universo
- Adición de una nueva tarjeta de experiencia
- Edición de una tarjeta de experiencia
- Uso compartido de una tarjeta de experiencia

Tarjetas de la Vista de experiencia

Obtenga más información sobre cómo crear una tarjeta de experiencia en la Vista de experiencia. Configure las tarjetas de experiencia para que los analistas tengan su universo dividido en grupos significativos.

Configuración del universo

Antes de poder configurar la Vista de experiencia de un usuario, asigne al menos un universo al usuario.

NOTE

Todos mis universos solo está disponible en la Vista de **experiencia** para los administradores. Para otros usuarios, la vista Todos mis universos está disponible en la Vista de **agente** si se ha asignado más de un universo.

Más información:

- [Configuración de universos](#)
- [KB000113376: Users with Read Access in team center can't see All My Universes View](#)

Adición de una nueva tarjeta de experiencia

De forma predeterminada, para Enterprise Manager, el sistema crea dos tarjetas de experiencia para cada universo existente. Las tarjetas de experiencia para las aplicaciones tienen dos niveles de detalles con los atributos *Aplicación* y *Nombre*. Las tarjetas de experiencia para Servicios tienen dos niveles desplegables con los atributos *Servicio de negocio* y *Nombre*. Como administrador, cree, actualice o suprima cualquier número de tarjetas de experiencia personalizadas para los analistas.

NOTE

Si se agrega un nuevo universo o si se conecta un nuevo proveedor, las tarjetas de experiencia no se crearán automáticamente. La creación automática de las tarjetas de experiencia es solo una parte de la instalación o actualización.

Siga estos pasos:

1. Abra la Vista de experiencia y asegúrese de que se encuentra en la vista de nivel superior.
2. Seleccione el botón + para agregar una nueva tarjeta de experiencia.
3. Seleccione un universo.
4. Utilice el universo completo o aplique un filtro.
5. Seleccione los atributos. Las tarjetas de experiencia se agrupan por atributos. Los niveles de detalles de la tarjeta de experiencia se corresponden con el número de atributos seleccionados.

TIP

Se recomienda utilizar de tres a cuatro niveles de atributos. O bien agrupar por un atributo para monitorizar un grupo específico de componentes. Por ejemplo, propietario = Joe.

6. Seleccione un tipo de gráfico predeterminado:
 - a. Histograma
 - b. Tiempo medio de respuesta
 - c. Volumen de la transacción
7. Nombre de la tarjeta
8. Seleccione la casilla **Hacer que esta tarjeta de experiencia sea pública**.
9. Seleccione **Guardar**.

El administrador puede ver ahora las tarjetas de experiencia en la Vista de experiencia.

WARNING

El mensaje de error se muestra al intentar mostrar más de 500 transacciones comerciales en modo en directo o más de 50 transacciones comerciales en modo histórico. La Vista de la experiencia limita el número de transacciones comerciales mostradas por motivos de rendimiento. Para obtener más información, consulte [No hay datos de métrica en la Vista de la experiencia](#).

Edición de una tarjeta de experiencia existente

En el nivel superior de la Vista de experiencia, se pueden editar las tarjetas de experiencia, tanto las predeterminadas como las definidas por el usuario.

Siga estos pasos:

1. Seleccione el icono Expandir de la esquina inferior derecha de la tarjeta.
2. Seleccione **Editar tarjeta**.
3. Cambie la configuración de la tarjeta según sea necesario.

4. Seleccione **Guardar**.

Supresión de una tarjeta de experiencia

En el nivel superior de la Vista de experiencia, se pueden suprimir las tarjetas de experiencia, tanto las predeterminadas como las definidas por el usuario.

Siga estos pasos:

1. Seleccione el icono Expandir de la esquina inferior derecha de la tarjeta.
2. Seleccione **Editar tarjeta**.
3. Seleccione **Suprimir tarjeta**. La tarjeta se ha eliminado para todos los usuarios que tienen acceso.

Uso compartido de una tarjeta de experiencia

Se puede compartir una tarjeta de experiencia con un usuario dentro de un universo existente.

Siga estos pasos:

1. Compruebe que el usuario tiene acceso al universo.
2. Seleccione el icono Expandir de la esquina inferior derecha de la tarjeta.
3. Seleccione **Editar tarjeta**.
4. Seleccione la casilla **Hacer que esta tarjeta de experiencia sea pública**.
5. Seleccione **Guardar**.
Aparecerá la tarjeta en la lista de tarjetas.
6. Envíe el vínculo de la tarjeta de experiencia al usuario.

NOTE

Se puede compartir una tarjeta de experiencia privada con un usuario del mismo universo. El usuario puede ver temporalmente la tarjeta privada.

Propagator

La Vista de experiencia permite organizar las experiencias (nodos de experiencias) en tarjetas que se basan en los atributos. Para expandir la selección de los atributos para agrupar las experiencias, utilice el componente Propagator. Propagator copia atributos desde los componentes contiguos que están conectados directamente a una experiencia. Estos atributos se propagan hasta la experiencia en función de las reglas. Si varios componentes están conectados a una única experiencia y el mismo atributo se define varias veces, el atributo se propaga solo si todas las repeticiones de ese atributo tienen el mismo valor. Propagator también puede recopilar y enviar los atributos desde otras capas del mapa. Por ejemplo, con esta propagación entre capas, se pueden organizar las experiencias en función a los atributos de Docker y host de la capa de infraestructura.

Configuración de Propagator

Defina los atributos que desea propagar a las experiencias utilizando la sintaxis de expresiones regulares en los nombres de atributo. Identifique la fuente del atributo y configure la propagación entre capas.

Siga estos pasos:

1. Defina e identifique los atributos que desea propagar. Los orígenes de los atributos disponibles son los siguientes:
 - **GATHERED**
Incluye atributos que el agente define cuando se monitoriza el componente.
 - **CUSTOM**
Contiene atributos que se crean manualmente en la interfaz de usuario o que se definen en la API de REST.
 - **DECORATED**

Agrupar los atributos que se han creado utilizando las reglas de atributo.

NOTE

Los atributos que se propagan a las experiencias siempre están decorados. Estos atributos se pueden sobrescribir utilizando reglas de atributo, la API de REST o los cambios manuales en la interfaz de usuario.

2. Utilice una lista de elementos permitidos para propagar ciertos atributos o utilice una lista de elementos no permitidos para bloquear atributos. Defina estas reglas de propagación globales editando las siguientes propiedades que se encuentran en el archivo `IntroscopeEnterpriseManager.properties`:

– **introscope.apmserver.atc.propagator.blacklist**

Especifica los atributos incluidos en la lista de elementos no permitidos.

Valor predeterminado:

```
introscope.apmserver.atc.propagator.blacklist=CUSTOM\.*;DECORATED\.*;Name;Hostname;Agent;AgentDomain
```

La lista predeterminada de elementos no permitidos no propaga los atributos siguientes:

- Atributos personalizados o decorados
- Name
- HostName ,
- Agent
- AgentDomain

– **introscope.apmserver.atc.propagator.whitelist**

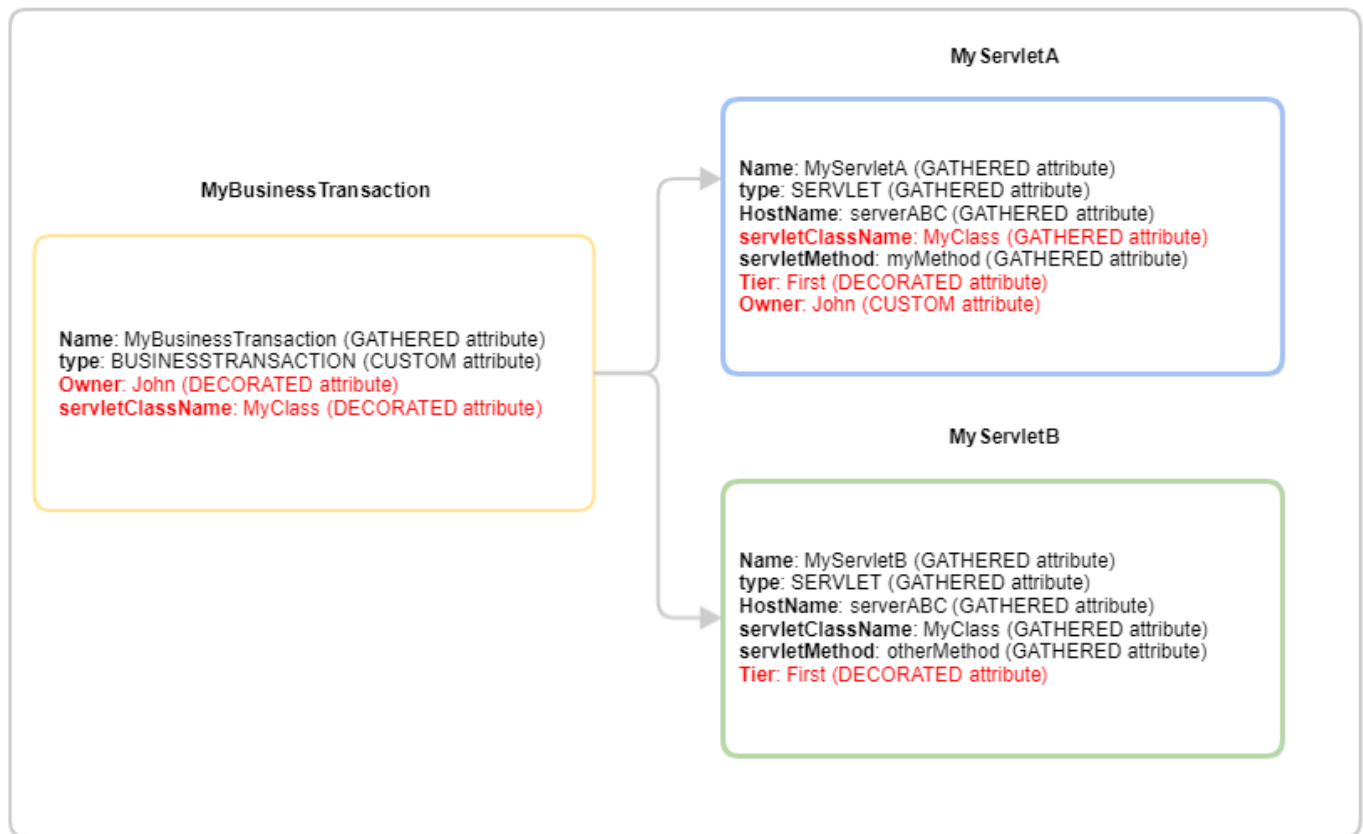
Especifica los atributos incluidos en la lista de elementos permitidos.

Valor predeterminado:

```
introscope.apmserver.atc.propagator.whitelist=.*Owner
```

La lista predeterminada de elementos permitidos propaga el atributo `Propietario`.

Ejemplo: En el ejemplo siguiente se muestra la propagación de los atributos `Propietario` y `servletClassName` a una experiencia desde el servlet conectado.

Figure 2: propagator**Resultados:**

- Nivel no se propaga debido a que la lista de elementos no permitidos desactiva la propagación de atributos personalizados.
 - HostName no se propaga debido a que también se ha restringido.
 - No se propaga servletMethod porque los servlets tienen valores diferentes.
 - Propietario se propaga debido a que no está en conflicto con MyServletB.
 - servletClassName se propaga porque ambos servlets tienen los mismos valores.
3. Para configurar la propagación de atributos entre capas, abra el archivo `IntroscopeEnterpriseManager.properties` desde el directorio `<EM_Home>/config`. Especifique las capas de mapa en la propiedad `introscope.apmserver.atc.propagator.crosslayer`:
- Valor predeterminado:** `<blank>` El valor predeterminado es una cadena vacía, lo que significa que la propagación entre capas está desactivada.

NOTE

Para activar la propagación de varias capas de mapa, separe cada capa con una coma.

Ejemplo: En el ejemplo siguiente, se ha configurado el componente Propagator para extraer los atributos de la capa de la infraestructura:

```
introscope.apmserver.atc.propagator.crosslayer=INFRASTRUCTURE
```

NOTE

Más información:

- [Cómo adaptar la monitorización de su entorno con reglas de atributo](#)

Fijación de datos

La fijación de datos en modo histórico es de 50 experiencias. La fijación de datos de modo activo es de 500 experiencias. Las experiencias son las transacciones comerciales o los puntos de entrada de la aplicación. Si se selecciona un intervalo de tiempo en modo histórico en las últimas 24 horas, se aplica la fijación de datos de modo activo (500 experiencias). Las últimas 24 horas se tratan en los datos almacenados en caché.

Los administradores configuran las tarjetas de experiencia en la Vista de experiencia de modo que los analistas puedan ver fácilmente los componentes más importantes del negocio que afectan a la experiencia del usuario final.

Para obtener más información sobre la configuración de las tarjetas de experiencia, consulte [Configuración de la Vista de experiencia](#).

Cómo adaptar la monitorización de su entorno con reglas de atributo

Los atributos son etiquetas que se aplican a los componentes. Cada atributo tiene un nombre y un valor (por ejemplo, color=rojo). Los atributos facilitan la distinción de los componentes e identifican sus relaciones con otros componentes. Utilice los atributos en sus perspectivas, el resaltado y el filtrado para organizar y mostrar partes del entorno de la aplicación monitorizada. DX APM permite asignar un número ilimitado de atributos a los componentes.

Tipos de atributo

DX APM ofrece los siguientes tipos de atributo:

- **Atributos básicos**

Los atributos básicos son notificados y asignados automáticamente a cada componente del agente asociado. Por ejemplo, un componente de base de datos puede tener los siguientes atributos básicos:

- `dbname`
- `inferredBackendNode`
- `Name`
- `provider`
- `Source cluster`
- `Type`

- **Atributos personalizados**

Asigne atributos personalizados a componentes individuales para, a continuación, agregarlos a las perspectivas, los grupos y los filtros. Por ejemplo, utilice el atributo `owner` para asignar el componente a un analista concreto. Para ver los componentes que están asignados a este analista, agregue el atributo `owner` a un filtro y especifique el valor del filtro.

- **Atributos representativos**

Se pueden definir reglas de atributo para que asignen automáticamente nuevos valores a atributos existentes. Estos nuevos atributos derivados se denominan atributos representativos.

Definición de los atributos personalizados

Defina un atributo personalizado para un componente individual o grupo de componentes.

NOTE

Se recomienda asignar los atributos personalizados a todos los componentes del entorno. Se recomienda asignar valores para `Owner` y `Location` a todos los componentes.

Siga los pasos siguientes:

1. En **Mapa**, seleccione un componente o grupo.

TIP

Se puede agregar un atributo personalizado a un componente que representa un grupo. El nombre del atributo y el valor se agregan a todos los componentes de ese grupo. En un mensaje se solicita si desea agregar el atributo al grupo o crear una regla de atributo.

2. Vaya a la sección **Atributos personalizados** del panel **Vista del componente** y seleccione los valores para los atributos personalizados predeterminados siguientes:

- location
- owner
- region
- tier

3. (Opcional) Para crear un nuevo atributo, seleccione **<nuevo nombre de atributo>** y escriba el nombre del atributo. Seleccione **<nuevo valor de atributo>** y asigne un valor al atributo.

NOTE

DX APM reconoce si un valor de atributo es una dirección de correo electrónico o una dirección URL. Aparecerá un icono de vínculo o de sobre al lado del atributo en el panel **Vista del componente**. Seleccione el icono para abrir los vínculos en una ficha nueva del explorador o abra una página de correo electrónico de Outlook.

4. Agregue el nuevo atributo a los filtros y las perspectivas.

El nuevo atributo y el valor aparecen en la sección **Atributos personalizados** del panel **Vista del componente**.

Definición de los atributos entre capas

Los atributos que se asignan a los componentes de una capa específica están visibles en otras capas de DX APM. Por ejemplo, los atributos que se asignan a los componentes de la capa de la infraestructura se incluyen en la lista desplegable que se utiliza para filtrar el mapa en la capa de la aplicación. Esta funcionalidad entre capas ofrece a los analistas vistas de datos que muestran las relaciones entre los componentes de la aplicación y sus componentes de la infraestructura conectados. Esta vista de datos combinados también sirve como una descripción general que ayuda a definir y organizar los roles de soporte de una organización. Los administradores pueden asignar atributos a los componentes de la capa de la infraestructura desde la sección **Atributos personalizados** del panel **Vista del componente** o mediante la definición de una regla de atributo.

Ejemplos**Ejemplo 1: Uso de atributos entre capas para ayudar en la evaluación de errores de la infraestructura**

El atributo `Owner = Joe Smith` se asigna a todos los componentes de la infraestructura a los que Joe proporciona soporte. A continuación, este atributo se utiliza para crear la perspectiva `Joe Smith`. Los analistas utilizan esta perspectiva y otras perspectivas `Owner` para identificar quién proporciona soporte a la infraestructura para las aplicaciones que requieren una evaluación de errores. Con estas vistas de datos, los analistas también pueden proporcionar soporte de infraestructura con información clave que puede dar lugar a una evaluación de errores más rápida.

Ejemplo 2: Uso de atributos entre capas para definir los roles de soporte

Si los componentes de host del entorno siguen una convención de nomenclatura, se puede crear una regla de atributo para definir los roles de soporte para los componentes de la aplicación. La siguiente regla de atributo asigna a Joe Smith a todos los componentes de host que se encuentran en Nueva York. A continuación, se crea una perspectiva basada en

este atributo, lo que permite al analista Joe Smith visualizar todos los componentes de la aplicación que tiene asignados y todos los componentes de la infraestructura conectados.

Nombre del atributo personalizado	Valor recién asignado	Nombre del atributo existente	Condición/operador de coincidencia	Valor de la condición
Propietario	Joe Smith	Hostname	Contiene	NY

Los vínculos siguientes proporcionan más información sobre las capas y cómo utilizar atributos en DX APM:

NOTE

Más información:

- [Capas del mapa](#)
- [Identificación de las áreas de interés mediante filtros](#)
- [Organización de los componentes utilizando perspectivas](#)

Definición de los atributos representativos mediante reglas de atributo

Utilice reglas para automatizar el proceso de adición de atributos personalizados. Una regla utiliza los atributos básicos y los atributos personalizados que ya se han atribuido a un componente. Si el atributo cumple la condición especificada en la regla, se crea (o actualiza) un nombre de atributo personalizado y se le asigna el valor especificado. Por ejemplo, una regla de atributo indica que si el atributo de nombre de host de un componente termina con el sufijo .cz, se creará el atributo personalizado con el nombre Ubicación de soporte y su valor será República Checa. A todos los componentes que cumplen los criterios de una regla se les atribuye el valor del atributo personalizado. A todos los componentes que cumplen los criterios de una regla se les atribuye el valor del atributo personalizado. Las reglas asignan el atributo personalizado en el entorno actual. Las reglas también asignan ese atributo a cualquier componente que coincida con los criterios futuros.

• Reglas de atributo locales

Como usuario, puede crear reglas de atributo locales que se aplican a los componentes dentro del universo. La regla aplica el nuevo valor de atributo a todos los componentes que cumplan los criterios y se encuentren dentro del universo actual. Estos atributos personalizados son exclusivos para el universo. Solo los usuarios con acceso a este universo y el administrador pueden verlos.

• Reglas de atributo global

La regla de atributo global aplica valores de atributo personalizados a todos los componentes que cumplen los criterios de regla en el entorno empresarial. Solo el administrador puede crear reglas de atributos globales. Las reglas de atributo globales tienen prioridad sobre las reglas de atributo locales. **Ejemplo:** Creación de un atributo local para establecer un valor de atributo local de ubicación en Long Island. Si se establece una regla de atributo global para asignar el valor del atributo de ubicación a Nueva York, el valor muestra Nueva York para todos los usuarios.

Definición de reglas de atributo globales

Defina reglas de atributo para asignar automáticamente atributos a los componentes. Las reglas de atributo global aplican atributos personalizados a todos los componentes actuales y futuros que cumplen la condición de la definición de reglas. Las reglas de atributo global se aplican a todos los componentes en el entorno empresarial independientemente del universo. Cualquier usuario que tiene el componente que se asigna a su universo ve el atributo personalizado. Un usuario no puede crear una regla de atributo local que sobrescribe un valor de regla de atributo global.

Siga los pasos siguientes:

1. Seleccione la ficha **Atributos**.
2. Haga clic en **<nueva regla de atributo>** en la columna **Nombre del atributo personalizado** y complete el nombre y el valor para la nueva regla.
3. Haga clic en el exterior de la fila.

La regla se ha guardado.

Uso de operando de expresiones regulares con reglas de atributo

Utilice el operando Contains RegEx en estos casos:

- Los operandos como `Starts with` o `Contains` no son suficientes para crear la regla de atributo que necesita.
- Es necesario un nuevo valor de atributo en función del valor original.

Una expresión regular que se utiliza en un valor de atributo existente puede utilizarse para crear varias reglas de atributo personalizado.

Siga estos pasos:

1. Seleccione la ficha **Atributos**.
2. Haga clic en **<nueva regla de atributo>**.
3. Asigne un nombre de atributo personalizado.
4. Asigne un valor de grupo de expresiones regulares en el **Valor recién asignado**.
5. Seleccione el **Nombre de atributo existente**.
6. Seleccione un valor para **Condición/operador de coincidencia**: `Contains RegEx` o `Doesn't contain RegEx`.
7. Introduzca la expresión regular en el **Valor de la condición** y pulse la tecla **Intro**.

NOTE

No se puede seleccionar **Distingue entre mayúsculas y minúsculas**. El uso de mayúsculas y minúsculas depende del operando de expresiones regulares.

La regla del atributo se guarda y se muestra el número de componentes con el nuevo atributo en **Componentes afectados**.

- Ejemplo: El nombre de host de la red sigue la regla `<código país de 2 letras><ciudad><ID numérico>.vendor.com`. Se puede utilizar el operando de expresión regular para crear reglas de atributo para crear atributos individuales de país y ciudad a partir del nombre de host. La sintaxis `"([a-z]*[0-9]*\.vendor\.com)"` describe esta expresión regular. Se pueden crear reglas de atributo para extraer los valores País y Ciudad mediante la creación de estas reglas de atributo.

Nombre del atributo personalizado	Valor recién asignado	Nombre del atributo existente	Condición/operador de coincidencia	Uso de mayúsculas y minúsculas	Valor de la condición
País	\$1	hostname	ContainsRegEx		<code>([a-z]*[0-9]*\.vendor\.com)</code>
Ciudad	\$2	hostname	ContainsRegEx		<code>([a-z]*[0-9]*\.vendor\.com)</code>

- Ejemplo: Dos valores de nombre de host en un entorno: `uklondon1234.vendor.com` y `usdallas1234.vendor.com`. \$1 devuelve los valores de uk y us, \$2 devuelve los valores de london y dallas. También se puede crear un vínculo a la documentación, como en el ejemplo siguiente. Seleccione cualquier elemento del mapa para visualizar un vínculo a la documentación.

Nombre del atributo personalizado	Valor recién asignado	Nombre del atributo existente	Condición/operador de coincidencia	Uso de mayúsculas y minúsculas	Valor de la condición
País	\$1	hostname	ContainsRegEx		<code>([a-z]*[0-9]*\.vendor\.com)</code>
Ciudad	\$2	hostname	ContainsRegEx		<code>([a-z]*[0-9]*\.vendor\.com)</code>

URL de documentación	https://wiki.vendor.com/searchForServerDoc.cgi?host=\$1	hostname	ContainsRegEx		(.*)\.vendor\.com
----------------------	---	----------	---------------	--	-------------------

NOTE

Para la sintaxis completa de la expresión regular, consulte la documentación de [Java RegEx](#).
Opcionalmente, busque en Internet un evaluador de Expresión regular de Java en línea.

Importación de reglas de atributos en bloque

DX APM permite ofrecer descripciones únicas para los componentes, ya estén en hosts, aplicaciones o incluso en componentes de la aplicación. Proporcione estas descripciones - o atributos personalizados - a su entorno para que pueda aprovechar las vistas de experiencia y del mapa. Por ejemplo, proporcione un atributo de propietario a cada una de las aplicaciones en su entorno. Cuando se ve un mapa de los propietarios, las aplicaciones que gestionan se anidan dentro de este. La configuración de ese mismo atributo de propietario permite disponer de un mosaico que resuma el rendimiento de todas las aplicaciones por propietario. A continuación, puede profundizar en el mosaico para ver las aplicaciones individuales que pertenecen específicamente a ese propietario.

Para aplicar estos atributos más fácilmente, puede utilizar un mecanismo de carga de regla masiva. Como administrador, puede crear un conjunto de reglas de atributo externamente en un archivo de valores separados por comas (CSV). A continuación, puede importar el archivo para crear numerosas reglas de atributo. Esta funcionalidad le permite utilizar un archivo del tipo CSV que contiene varias reglas de atributo y cargarlas todas al mismo tiempo en un corto período de tiempo.

En el archivo, especifique el nombre del atributo personalizado, una coma y el valor que desee tomar. A continuación, utilice otra coma y especifique el atributo que desee utilizar para que coincida con la regla. Utilice una coma más y, a continuación, el valor esperado del atributo coincidente.

En otras palabras:

```
WHEN Hostname equals my-tradeservice THEN Owner equals Ralph
```

Se puede escribir en un archivo CSV como:

```
Owner,Ralph,Hostname,my-tradeservice
```

Utilice la siguiente convención de formato en el archivo CSV:

El nombre del atributo personalizado que desee agregar. El atributo puede ser cualquiera de los atributos representativos.	El valor del atributo personalizado que desee agregar.	El nombre del atributo del filtro con el que se desea coincidir. Estos atributos son los atributos básicos.	El valor del atributo de filtro con el que se desea coincidir.
--	--	---	--

Este archivo puede incluir solo cuatro columnas. El valor del atributo coincidente en la tercera columna debe ser un nombre de atributo válido.

Siga estos pasos:

1. En un editor, cree un archivo CSV mediante la convención de formato, por ejemplo:

```
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. Guarde y nombre el archivo con la convención siguiente: `filename.csv`. Por ejemplo, en Windows, utilice la función "Guardar como" y guarde el archivo como tipo CSV. Cierre el archivo.
3. En DX APM, pase el ratón sobre el panel izquierdo y haga clic en **Atributos**.
4. Haga clic en **Cargar archivo de la regla de atributo**.

Aparecerá el cuadro de diálogo Cargar archivo CSV de la regla de atributo.

5. Lea las instrucciones del cuadro de diálogo y, si lo desea, seleccione más universos a los que aplicar las reglas. Si no se selecciona ningún universo, las reglas del atributo se aplican solo al universo seleccionado actual.
6. Haga clic en **Explorar** y seleccione el archivo CSV para importar. Puede repetir este paso para seleccionar otro archivo para cargar.
7. Haga clic en **Cargar**.
Aparece un mensaje, en el que se informa del estado de la carga del archivo.
8. Haga clic en **Finalizado**.
Las reglas de atributo aparecen en la lista de reglas de atributo.

Configuración de reglas para la actualización de atributos

Cuando desea actualizar los atributos de numerosos componentes (por ejemplo, para especificar el propietario de muchas aplicaciones o hosts), puede ser más conveniente cargar reglas CSV que crearlas en la interfaz de usuario. No es necesario especificar solo los atributos existentes. Se pueden crear atributos que se adecuen mejor a sus objetivos en relación con la creación de los mosaicos Vista de la experiencia y Perspectivas. Después de cargar las reglas, se pueden encontrar en el mapa.

Ejemplo:

Cómo funcionan las reglas

En este ejemplo, desea asignar el propietario del atributo con el valor Eric a dos nombres de host: rojo y azul. También desea asignar el propietario del atributo con el valor Susan al nombre de host verde.

```
@ruleset, owners-by-hostOwner, Eric, hostname, redOwner, Eric, hostname, blueOwner, Susan, hostname, green
```

@ruleset, <name> coloca estas tres reglas en el ámbito owners-by-host . La interfaz de usuario muestra el identificador al que pertenece cada una de estas reglas. Cada regla especificada pertenece a un grupo con un identificador único @ruleset . Cuando no se especifica @ruleset , las reglas pertenecen de forma implícita a un grupo global. Siempre debería utilizar identificadores de regla, o quizá se sorprenda por los cambios realizados en el ámbito global y suprima reglas accidentalmente en otros ámbitos.

Ejemplo:

Edición o supresión de una regla

Puede editar las reglas en la interfaz de usuario. También puede editar las reglas con CSV, pero debe ir con cuidado.

En este ejemplo, el nombre de host púrpura especifica a Eric como su propietario, pero se suprimen las otras dos reglas especificadas en el ejemplo anterior.

```
@ruleset, owners-by-hostOwner, Eric, hostname, purple
```

Si especifica un identificador @ruleset en el archivo CSV, suprimirá las reglas que no se han especificado de nuevo. Este comportamiento se aplica a todas las reglas y no solo a las reglas con los cambios. Por lo tanto, el archivo CSV siguiente suprime todas las reglas en el ámbito owners-by-host:

```
@ruleset, owners-by-host@ruleset, owners-by-appOwner, Foo, Application, Bar
```

WARNING

Debido a este comportamiento de la regla, se recomienda guardar una copia master del archivo CSV y realizar los cambios solo en este.

Más información:

- [Organización de los componentes utilizando perspectivas](#)
- [Configuración de la Vista de experiencia](#)

Uso de políticas de decoración para filtrar las reglas de atributo

Los atributos representativos son aquellos que se crean o actualizan automáticamente como resultado de reglas de atributo. Una política de decoración le permite decidir qué reglas de atributo se aplican al mapa de Team Center.

En un intervalo fijo, DX APM actualiza todos los nodos correspondientes que cumplan las reglas de la política de decoración. Las políticas de decoración le ayudarán a organizar y mostrar los nodos en el entorno de la aplicación monitorizada en Team Center.

Las siguientes opciones permiten filtrar por distintos tipos de políticas de decoración:

- Todos: muestra todas las reglas de atributo que se han creado.
- Reglas creadas mediante CSV: muestra las reglas de atributo de CSV.
- Reglas creadas manualmente: muestra todas las reglas de atributo que se crean manualmente en la ficha Reglas de atributo.

Siga estos pasos:

- a. En DX APM, pase el ratón sobre el panel izquierdo y haga clic en **Atributos**.
- b. Haga clic en **Regla de atributo:<option>** y selecciona una política.

La lista de reglas de atributo se actualizará para mostrar las reglas que pertenecen a la política.

Más información: [Cómo adaptar la monitorización de su entorno con reglas de atributo](#)

Ajuste de la monitorización con alertas

Como administrador de APM, puede crear, editar y suprimir alertas. Puede establecer umbrales de rendimiento para las métricas para que los analistas puedan identificar cuándo un componente específico está cargándose. Cree alertas y establezca umbrales para indicar problemas antes de que se vea afectada la experiencia del cliente.

Creación de una nueva alerta

Como administrador, puede crear alertas para monitorizar posibles problemas en el entorno de modo eficaz.

Siga estos pasos:

1. En el panel izquierdo, pase el ratón por encima del icono de la campana y haga clic en **Alertas**.
2. Haga clic en **Crear una nueva alerta**.
3. Introduzca los valores **Nombre de alerta** y **Descripción**.
4. Mantenga el botón de alternar **Activo**.
5. Introduzca los valores para **Especificador de agente** y **Especificador de métrica**.

El **Especificador de agente** especifica una expresión regular que filtra la entrada a la métrica y especifica los datos que incluyen el nombre del agente. Esta expresión determina a qué agentes se limitan los datos agrupados. Por ejemplo, la expresión `(.*)\WPS2-0[1,2]` busca cualquier agente en todos los dominios que se denominan WPS2-01 o WPS2-02. La expresión del agente es importante cuando varias JVM notifican al mismo Enterprise Manager pero tienen distintas finalidades. Por ejemplo, sitios web distintos en la misma compañía. En este caso, se utiliza una expresión regular para limitar qué agentes filtra la agrupación de métricas.

El **Especificador de métrica** especifica una expresión regular que especifica la métrica y el recurso. Un recurso es una cadena de carpetas que conducen a la métrica. Por ejemplo, la expresión `LDAP\[([^\:]*)\](.*)Response Time\(\ms\)` busca todos los recursos en la carpeta de recursos LDAP. La expresión solo busca la métrica del tiempo de respuesta (en milisegundos) en esos recursos.

6. (Opcional) Haga clic en **+** junto al campo Especificador de métrica para agregar más campos a los valores **Especificador de agente** y **Especificador de métrica**.
7. Introduzca los valores **Umbral de peligro** y **Umbral de precaución**.
8. Haga clic en **Crear alerta**.

Se ha creado una alerta.

Creación de una nueva alerta desde la vista de la métrica

Puede crear alertas desde la página Vista de la métrica.

Siga estos pasos:

1. Explore el árbol de la métrica para seleccionar una métrica, por ejemplo, **Errores por intervalo**.
2. Haga clic con el botón secundario del ratón en la métrica.
3. Haga clic en Nueva alerta sencilla de la métrica, Errores por intervalo.
Se le dirigirá a la página **Alertas**. Los valores **Especificador de agente** y **Especificador de métrica** se rellenan automáticamente.
4. Introduzca los valores **Nombre de alerta** y **Descripción**.
5. Introduzca los valores **Umbral de peligro** y **Umbral de precaución**.
6. Haga clic en **Crear alerta**.

Se ha creado una alerta.

Creación de una nueva alerta con opciones avanzadas**Siga estos pasos:**

1. En el panel izquierdo, pase el ratón por encima del icono de la campana y haga clic en **Alertas**.
2. Haga clic en **Crear una nueva alerta**.
3. Introduzca los valores **Nombre de alerta** y **Descripción**.
4. Mantenga el botón de alternar **Activo**.
5. Introduzca los valores para **Especificador de agente** y **Especificador de métrica**.
6. (Opcional) Haga clic en + junto al campo Especificador de métrica para agregar más campos a los valores Especificador de agente y Especificador de métrica.
7. Haga clic en **Mostrar opciones avanzadas**.
8. En la lista desplegable **Combinación**, seleccione una de las siguientes opciones:
 - **Cualquier**: Si alguna métrica que forma parte de la agrupación de métricas de alertas infringe el umbral, se activa la alerta.
 - **Todo**: Si todas las métricas que forman parte de la agrupación de métricas de alertas infringen el umbral, se activa la alerta.
9. Seleccione una opción de la lista desplegable **Operador de comparación**:
 - Inferior a
 - Superior a
 - Igual a
 - No igual a
10. Introduzca los valores para los umbrales **Peligro** y **Precaución**.
 - Umbral: especifica un valor que activa una alerta de peligro o una alerta de precaución.
 - Períodos por encima del umbral: especifica el número máximo de períodos que puede exceder el umbral antes de que se active una alerta.
 - Períodos observados: especifica el número total de períodos que se están monitorizando por cada iteración de alerta.
11. Haga clic en **Crear alerta**.

Se ha creado una alerta con las opciones avanzadas.

Establecimiento de umbrales de peligro y precaución

Como administrador, puede establecer valores del umbral de peligro y de precaución para las alertas. Una alerta recopila información de rendimiento y la compara con los valores del umbral. La alerta muestra *uno* de los siguientes estados:

- **Verde:** ninguna de las métricas que coinciden con la alerta infringen los umbrales de precaución o peligro, tal y como especifica la configuración de la alerta.
- **Amarillo:** una alerta informa sobre un estado de precaución. Un intento de utilizar la aplicación o el componente es probable que produzca resultados no satisfactorios.
- **Rojo:** una alerta informa sobre un estado de peligro, un problema que requiere atención inmediata.
- **Gris:** una alerta no está informando de los datos. No se notifican las métricas que coinciden con la alerta simple (por ejemplo, cuando los agentes están desconectados).
- **N/D:** una alerta no está informando de los datos. Una alerta simple que no está activa o no coincide con ninguna otra métrica.

Siga estos pasos:

1. En el panel izquierdo, pase el ratón por encima del icono de la campana y haga clic en **Alertas**.
Se abre la página Alertas y muestra las métricas siguientes:
 - **Errores de la aplicación:** el número de alertas que se activan cuando se supera el umbral de errores de la aplicación.
 - **Errores de back-end:** una alerta que se activa cuando se supera el umbral de errores de back-end que no son SQL ni de servicios web.
 - **Estado de conexión:** una alerta que se inicia cuando hay un problema en el agente DockerMonitor al conectarse con la configuración del Docker.
 - **Utilización de la CPU:** una alerta que se inicia cuando se supera el umbral para el uso de la CPU.
 - **Errores de front-end:** una alerta que se activa cuando se supera el umbral de errores del grupo de URL de front-end.
 - **Tiempo de respuesta de front-end:** una alerta que se inicia cuando se supera el umbral para los tiempos de respuesta del grupo de URL de front-end.
 - **Detenciones de front-end:** una alerta que se activa cuando se supera el umbral de detenciones del grupo de URL de front-end. Una detención es una solicitud de front-end no se ha completado en un momento específico (30 segundos de forma predeterminada). Las detenciones indican un bloqueo de un subproceso, debido a un bucle infinito, a un interbloqueo o a recursos limitados.
 - **Porcentaje de memoria dinámica utilizada:** una alerta que se inicia cuando se supera el umbral para el porcentaje de memoria dinámica que se utiliza.
 - **Intensidad de variación del tiempo respuesta:** una alerta que se inicia cuando se supera el umbral de intensidad de variación del tiempo de respuesta.
La intensidad de la variación es una medida de la estabilidad de 10 a 40:
 - 10: estable
 - 11 a 25: relativamente estable
 - 25 a 30: moderadamente inestable
 - 30 a 40: gravemente inestable
 - **Errores de cliente del servicio web:** una alerta que se inicia cuando se supera el umbral de errores del cliente del servicio web (SOAP o REST).
 - **Errores del servidor del servicio web:** una alerta que se inicia cuando se supera el umbral de errores del servidor de servicio web.
2. Expanda la alerta que desea configurar.
3. En el campo Umbral de peligro, introduzca el valor que activa una alerta de peligro.
4. En el campo Precaución, introduzca el valor que activa una alerta de precaución.
Las unidades se corresponden con el valor que se utiliza en la agrupación de la métrica. Por ejemplo, si crea una alerta simple para el tiempo de respuesta medio, el valor es en milisegundos.
5. Haga clic en **Guardar alerta**.

TIP

Sugerencia: Evite establecer los umbrales de manera que se puedan generar alertas demasiado frecuentes. Desea ser avisado pero no tener resultados abrumadores.

Activación o desactivación de alertas

Puede especificar qué alertas desea utilizar para la monitorización. La página Alertas muestra una lista de alertas disponibles de forma concisa.

Siga estos pasos:

1. En el panel izquierdo, pase el ratón por encima del icono de la campana y haga clic en **Alertas**.
Se abre la página Alertas y muestra las alertas.
2. Busque la alerta que desee activar o desactivar.
3. (Opcional) Haga clic en un nombre de columna para ordenar por el valor del encabezado.
4. Haga clic en una línea para expandir los detalles de la alerta.
5. Establezca el botón de alternar en **Activo** o **Inactivo**.
6. Haga clic en **Guardar**.

La alerta se ha activado o desactivado.

Supresión de una alerta

Como administrador, puede suprimir una alerta que ya no necesite.

Siga estos pasos:

1. En el panel izquierdo, pase el ratón por encima del icono de la campana y haga clic en **Alertas**.
2. Expanda la alerta que desee suprimir.
3. Haga clic en **Suprimir**.

Se ha suprimido la alerta.

Cómo entender las expresiones regulares

Las expresiones regulares definen las métricas que se incluirán en la definición de la alerta. Una expresión regular (Perl RegEx) es una cadena de texto que describe un patrón de búsqueda.

Especificador de agente

Un especificador de agente define los agentes desde los que la alerta recupera los datos. Por ejemplo, un especificador de agente aplica las alertas solamente en los agentes de todos los dominios que se denominan WPS2-01 o WPS2-02. Un especificador de agente es útil cuando varias JVM notifican al mismo Enterprise Manager pero tienen distintas finalidades. También para ejecutar sitios web distintos en la misma compañía. En este caso, se limitan los agentes que se aplican a la agrupación de métricas mediante el uso de expresiones regulares para crear dicho filtro.

Los especificadores de agente utilizan las siguientes partes:

1. Nombre del host que ejecuta el proceso para monitorizar
2. Nombre del proceso concreto en una aplicación o instancia de la aplicación de Java gestionada desde las que se desean recopilar los datos
3. Agente responsable de recopilar los datos

Especificador de métrica

Un especificador de métrica define la métrica que se incluirá en la alerta. El especificador de métrica filtra todos los datos que entregan los agentes según su expresión de agente. Los especificadores de métrica requieren una consideración

más detenida que los especificadores de agente debido a que el número de métricas filtradas supera el número de agentes.

Los especificadores de métrica utilizan las siguientes partes:

1. Recursos que conducen a la métrica
2. Nombre de la métrica

Gestión de datos de métricas mediante módulos de gestión

Se pueden utilizar módulos de gestión para gestionar y organizar los datos de la métrica para la monitorización. Los módulos de gestión son recopilaciones de objetos y valores de configuración.

Módulos de gestión

Existen módulos de gestión para cada dominio y contienen elementos. Los elementos son objetos que contienen y organizan datos de métrica con la lógica de monitorización para su presentación en el Team Center. Los elementos son:

- Agrupaciones de métrica
- Alertas (que incluyen Alertas sencillas)
- Módulos de gestión
- Calculadoras

Al instalar Introscope, se incluye un módulo de gestión predeterminado en el superdominio. Este módulo de gestión predeterminado contiene cuadros de mandos configurados previamente que incluyen la lógica de monitorización del rendimiento que se utiliza comúnmente. Cree otros módulos de gestión para otros dominios creados.

Un módulo de gestión útil es el módulo de gestión de la infraestructura de APM, que contiene la definición de alertas y otros objetos que cubren las métricas de estado de APM principales.

NOTE

Para ver alertas en Team Center, asegúrese de que las métricas se asignan a los nodos y de que está activada la configuración Propagar a Team Center. Vaya a Team Center, Gestión. La casilla de verificación Propagar a Team Center se encuentra en la definición de la alerta.

NOTE

Un icono Mantenimiento en la página Módulos de gestión en la ficha Mantenimiento muestra que la página está en mantenimiento. El icono Mantenimiento estará visible durante un período máximo de 7 días de antelación para cualquier mantenimiento próximo.

Aparecerá el icono Mantenimiento en función del siguiente orden de prioridad:

1. Activo con la última hora de finalización
2. Activo con la hora de finalización más corta
3. Programado con la hora de inicio más próxima
4. Resto de la programación

Permisos, aplicación de dominios y edición de elementos

Los agentes se dividen en dominios. A los usuarios se les concede acceso a determinados dominios y solo se pueden crear elementos y módulos de gestión que hagan referencia a los datos de los dominios a los que pertenecen los usuarios. Para crear o editar elementos, debe disponer de los permisos adecuados. Para realizar la mayor parte de los cambios en los elementos, es necesario disponer de permiso de escritura en el dominio en el que se encuentra el elemento. Algunas funciones requieren un permiso específico. Tenga en cuenta al crear o modificar un elemento, que los elementos de los dominios individuales solo pueden hacer referencia a otros elementos del mismo dominio. Los elementos del superdominio pueden hacer referencia a los elementos de cualquier dominio.

Si es el usuario avanzado, puede realizar las operaciones CRUD en alertas, módulos de gestión, calculadoras y agrupaciones de métrica.

Personalización de los módulos de gestión

Utilice los módulos de gestión de la infraestructura de APM y predeterminados con nuevas implementaciones de APM. Los módulos se pueden personalizar para cumplir los requisitos de monitorización de la organización. La personalización es especialmente válida para las implementaciones que se actualizan desde versiones anteriores o implementaciones de APM a gran escala. Los módulos de gestión mencionados anteriormente y sus propios módulos de gestión deben personalizarse antes de pasar a producción. Se pueden aplicar los siguientes valores de configuración de personalización:

- Activación o desactivación de alertas
- Establecimiento de los umbrales de alerta adecuados
- Ajuste de los períodos por encima de un umbral
- Activación o desactivación de la casilla de verificación **Propagar a Team Center**

El módulo de gestión del sistema para la página principal del Team Center contiene alertas y agrupaciones de métricas necesarias para las llamadas de back-end, CPU, memoria y el estado a nivel aplicación. No se espera que los administradores de APM ajusten este módulo de gestión.

NOTE

Más información:

- [Activación o desactivación de alertas y acciones](#)

Este vídeo explica cómo trabajar con los módulos de gestión en APM Team Center:

Se pueden utilizar módulos de gestión para gestionar y organizar los datos de la métrica para la monitorización. Los módulos de gestión son recopilaciones de objetos y valores de configuración. Este tema trata sobre las siguientes secciones:

- Módulos de gestión
- Permisos, aplicación de dominios y edición de elementos
- Personalización de los módulos de gestión

Para gestionar y organizar los datos de métricas para la monitorización, consulte [Gestión de datos de métricas mediante módulos de gestión](#).

Creación y trabajo con módulos de gestión

Los módulos de gestión organizan elementos para que pueda buscarlos, copiarlos y editarlos adecuadamente. Los módulos de gestión se almacenan como archivos *.jar* en el directorio `<EM_home>/config/modules`. Los módulos de gestión pueden además existir en dominios de subdirectorios en el directorio `<EM_home>/config/modules`. Un usuario puede definir esos dominios y el archivo JAR del módulo de gestión debajo de ellos.

Se puede definir un módulo de gestión como editable o no editable, así como activo o inactivo. Cuando un módulo no es editable, tampoco se podrán editar los elementos que contiene. Cuando un módulo de gestión está inactivo, los elementos que contiene también estarán inactivos.

Elementos del Editor de módulo de gestión

En esta tabla se describen los elementos del módulo de gestión:

Elemento	Descripción
módulo de gestión	Un contenedor que contiene elementos.

Alertas	Notificaciones de posibles problemas en la aplicación, generadas mediante la comparación de valores de métrica con los valores de umbral definidos por el usuario y produciendo un estado.
Calculadoras	Una calculadora suma o calcula el promedio de los datos de la métrica para generar métricas personalizadas.
Agrupaciones de métrica	Objetos que especifican las métricas en las que se debe actuar; se utilizan como bloques de creación para elementos como alertas.

Búsqueda de elementos del módulo de gestión

Se puede buscar cualquier elemento del módulo de gestión mediante expresiones regulares de la sintaxis de Lucene.

Nota: Para obtener más información, consulte [Consulta de eventos almacenados](#).

Siga estos pasos:

1. En el editor de módulo de gestión, seleccione un dominio o un nodo de módulo de gestión.
2. Haga clic en la ficha **Buscar**.
3. Introduzca una expresión regular, utilizando la sintaxis de Lucene, en el panel Filtro.
Nota: Los caracteres especiales se deben escapar. Si inicia la cadena de búsqueda con el asterisco (*) o signo de interrogación (?), se produce un error. Estos caracteres no están permitidos al principio de una expresión de Lucene. A medida que se escribe en el panel **Filtro**, aparecen coincidencias con cada pulsación de teclas. Las coincidencias aparecen en una tabla en la ficha **Buscar**. Esta información se muestra para cada elemento que coincide con la búsqueda:
 - a. Nombre del elemento
 - b. Módulo de gestión al que pertenece el elemento
 - c. Dominio al que pertenece el módulo de gestión

Módulos y elementos de gestión de nombres

Las reglas siguientes se aplican a los módulos y elementos de gestión de nombres:

- Los módulos de gestión que estén en el mismo dominio deben tener nombres únicos.
Los nombres de módulos de gestión que no sean únicos se permiten en dominios independientes.
- Los mismos tipos de elementos de módulo de gestión que estén en un mismo módulo de gestión deben tener nombres únicos.
Por ejemplo, se puede tener una alerta y una calculadora, ambas denominadas **Bytes en uso**, pero no se pueden tener dos alertas denominadas **Bytes en uso**.
- Los nombres de elementos de módulo de gestión que no sean únicos pueden existir cuando se encuentran en módulos de gestión independientes.
Por ejemplo, se puede tener dos alertas, ambas denominadas **Alerta de servlet A**. Una alerta está en el módulo de gestión de muestras y la otra alerta se encuentra en un módulo creado por el usuario llamado **Módulo de prueba**.

Para facilitar la asignación de nombres, se puede utilizar la opción **Imponer unicidad** para crear y nombrar un módulo o elemento de gestión:

- Cuando la opción **Imponer unicidad** está activada y se introduce un nombre que no es único, DX APM agrega un número al nombre para que sea único.
El número añadido aparece después de crear la plantilla de informe, cuando se consulta en el **Editor del módulo de gestión**.
- Cuando la opción **Imponer unicidad** está desactivada y existe un nombre de plantilla de informe idéntico, DX APM muestra un mensaje de error y no crea el informe.

Creación de un módulo de gestión

Para crear un módulo de gestión, realice las siguientes tareas:

Siga estos pasos:

1. En Team Center, seleccione **Módulos de gestión** y haga clic en **Crear módulo de gestión**.
2. En la página Crear nuevo módulo de gestión, introduzca los detalles siguientes:
 - a. En el campo **Nombre del módulo de gestión**, introduzca un nombre para el módulo de gestión (el nombre aparece en el árbol del Editor del módulo de gestión).
 - b. Introduzca los detalles en el campo **Expresión del agente**. Para obtener más información, consulte [Definición de expresiones de agente para un módulo de gestión](#).
 - c. En el campo **Descripción**, introduzca la descripción necesaria que ayuda a identificar el módulo de gestión que se crea.
 - d. Haga clic en **Guardar**.
El módulo de gestión se ha creado correctamente.
3. Haga clic en **Aceptar**.
El módulo de gestión aparece en el árbol del **Editor del módulo de gestión**. Los módulos están activos y se pueden editar en el momento en el que se crean.

Actualización de un módulo de gestión

Para actualizar un módulo de gestión, realice las siguientes tareas:

Siga estos pasos:

1. En **Configuración**, haga clic en **Módulos de gestión**.
2. Se muestran los módulos de gestión disponibles para el usuario. También se puede buscar un módulo de gestión específico utilizando el filtro.
3. Haga clic en el nombre del módulo de gestión necesario. Se muestra la página **Editar módulo de gestión** correspondiente.
4. En la página **Editar módulo de gestión**, actualice los siguientes detalles:
 - a. Haga clic en el botón de alternar para marcar el módulo de gestión como activo o inactivo.
 - b. En el campo **Nombre del módulo de gestión** edite el nombre del módulo de gestión (el nombre aparece en el árbol del Editor del módulo de gestión).
 - c. En el campo **Descripción**, actualice la descripción necesaria que ayuda a identificar el módulo de gestión que se crea.
 - d. En el campo **Nombre del archivo jar**, actualice el nombre del archivo `.jar` para el módulo de gestión utilizando caracteres alfanuméricos sin espacios (para que funcione en todos los sistemas operativos).
 - e. Actualice los detalles en el campo **Expresión del agente**. Para obtener más información, consulte [Definición de expresiones de agente para un módulo de gestión](#).
 - f. La tabla **Vista previa** muestra una lista de todos los agentes conectados y su estado (Conectado o Desconectado).
 - g. El usuario puede cambiar a otros valores de configuración relacionados con este módulo de gestión como, por ejemplo, Agrupaciones de métrica, Alertas, Alertas de resumen, Calculadoras y Análisis diferencial, para actualizarlos.
 - h. Haga clic en **Guardar**.
El módulo de gestión se ha actualizado correctamente.
 - i. En el cuadro de diálogo de confirmación, haga clic en **Aceptar**.
El módulo de gestión actualizado aparece en la página **Módulos de gestión**.

Establecer un módulo de gestión como activo o inactivo

Si el módulo de gestión se desactiva, todo lo que contiene también se desactiva.

Siga estos pasos:

1. Seleccione el módulo de gestión en el árbol del Editor del módulo de gestión.
2. En el panel de configuración del módulo de gestión, marque o desmarque la casilla de verificación **Activo**.
3. Haga clic en **Aplicar**.

Copia de un módulo de gestión

Para copiar un módulo de gestión, realice las siguientes tareas:

1. En **Configuración**, haga clic en **Módulos de gestión**.
2. Se muestran los módulos de gestión disponibles para el usuario. También se puede buscar un módulo de gestión específico utilizando el filtro.
3. Haga clic en el nombre del módulo de gestión necesario. Se muestra la página **Editar módulo de gestión** correspondiente.
4. En la página **Editar módulo de gestión**, haga clic en **Guardar como nuevo**.
5. En el cuadro **Crear nuevo módulo de gestión**, actualice los siguientes detalles, si es necesario.
También puede omitir este paso y hacer clic en **Guardar** en el cuadro Crear nuevo módulo de gestión para crear una copia de la alerta.

NOTE

Al crear una copia del módulo de gestión existente, solo se copiarán los valores de configuración de la ficha Propiedades. Es posible que tenga que crear otros valores de configuración, si es necesario.

- a. Haga clic en el botón de alternar para marcar el módulo de gestión como activo o inactivo.
- b. En el campo **Nombre del módulo de gestión** edite el nombre del módulo de gestión (el nombre aparece en el árbol del Editor del módulo de gestión).
- c. Actualice los detalles en el campo **Expresión del agente**. Para obtener más información, consulte [Definición de expresiones de agente para un módulo de gestión](#).
- d. En el campo **Descripción**, actualice la descripción necesaria que ayuda a identificar el módulo de gestión que se crea.
- e. Haga clic en **Guardar**.
El módulo de gestión se ha creado correctamente.
- f. En el cuadro de diálogo de confirmación, haga clic en **Aceptar**.
El módulo de gestión aparece en la página **Módulos de gestión**.

Supresión de un módulo de gestión

Al suprimir un módulo de gestión, se suprimen todos los elementos que contenga.

Siga estos pasos:

1. En Team Center, seleccione **Módulos de gestión**.
2. En el campo **Búsqueda**, introduzca *<Management_Module_Name>* que desea actualizar.
El campo Búsqueda se rellena con *<Management_Module_Name>* que desea.
3. Antes de suprimir el módulo de gestión, desactívelo. En el panel de configuración del módulo de gestión, marque o desmarque la casilla de verificación **Activo**.
4. Haga clic en **Aplicar**.
5. En el panel izquierdo, haga clic en *<Management_Module_Name>*.
Aparecerá la página *<Management_Module_Name> Management Module* correspondiente.
6. Haga clic en el icono **Suprimir**.

7. Haga clic en **Sí**.

Exportación de un módulo de gestión

Se puede exportar un módulo de gestión existente en formato de archivo *.jar*.

Siga estos pasos:

1. En Team Center, seleccione **Módulos de gestión** y, a continuación, seleccione **Exportar**.
Todos los módulos de gestión se detallan con casillas de selección añadidas.
2. Seleccione los módulos de gestión para exportarlos y haga clic en **Exportar**.
Los módulos de gestión exportados se descargan a un directorio local con el nombre *modules.zip*.
3. Se puede extraer el archivo *modules.zip*.
Todos los módulos de gestión están disponibles como archivos *.jar* individuales.

Importación de un módulo de gestión

Se puede importar un módulo de gestión existente en formato de archivo *.jar*.

Siga estos pasos:

1. En Team Center, seleccione **Módulos de gestión** y, a continuación, seleccione **Importar**.
Se abre un diálogo.
2. Seleccione **Elegir archivo** y especifique el archivo *.jar*.
3. Haga clic en **Importar** para importar el archivo.
El módulo de gestión aparece en el árbol del Editor del módulo de gestión. Los módulos están activos y se pueden editar en el momento en el que se crean.

Definición de expresiones de agente para un módulo de gestión

Las agrupaciones de métrica (y sus expresiones de agente y métrica) filtran los datos que coinciden con los criterios de métrica y de agente. Todas las agrupaciones de métrica en un módulo de gestión pueden compartir un único conjunto de expresiones de agente. A continuación, se puede especificar en el nivel de agrupación de métrica si se debe utilizar la expresión de agente compartida o las expresiones de agente de agrupación de métrica.

El uso de expresiones de agente del módulo de gestión simplifica la configuración de la lógica de monitorización. Se pueden cambiar las expresiones de agente y métrica del módulo de gestión y aplicarlas a todas las agrupaciones de métrica que contiene. Si la implementación cambia (por ejemplo, el nombre del equipo), se puede cambiar el módulo de gestión y el cambio se aplica a todo lo que hay en el módulo. También se puede copiar un módulo de gestión configurado y cambiar la expresión del agente para monitorizar un agente diferente.

NOTE

Se recomienda utilizar expresiones de agente de módulo de gestión o expresiones de agente de agrupación de métrica, pero no una mezcla de ambas en un único módulo de gestión. También se pueden utilizar solamente expresiones de agente de agrupación de métrica si se desea monitorizar un conjunto específico de métricas de un conjunto específico de agentes.

Siga estos pasos:

1. En Team Center, seleccione **Módulos de gestión**.
2. En el campo **Búsqueda**, introduzca *<Management_Module_Name>* que desea actualizar.
El campo Búsqueda se rellena con *<Management_Module_Name>* que desea.
3. En el panel izquierdo, haga clic en **<Management_Module_Name>**.
Aparecerá la página *<Management_Module_Name> Management Module* correspondiente. Aparecerá un campo de expresiones de agente en blanco.
4. Se puede proporcionar información de expresiones de agente de una de las dos maneras siguientes:

Las expresiones de agente que se definen aquí no se aplican automáticamente a las agrupaciones de métrica. Utilice las expresiones de agente del módulo de gestión en lugar de las expresiones de agente de agrupación de métrica. Para obtener más información sobre este proceso, consulte [Configuración de agrupaciones de métrica en Team Center](#).

En cada universo, a los usuarios se les asignan privilegios individuales por módulo de gestión para editar alertas, calculadoras y grupos de métricas. El rol del usuario avanzado, los usuarios y los grupos de usuarios deben tener permiso para ver o crear alertas, calculadoras o grupos de métricas para un módulo de gestión.

Configuración de agrupaciones de métrica en Team Center

Las agrupaciones de métrica son objetos del módulo de gestión que guardan la siguiente información:

- Consulte este ejemplo en el módulo de gestión de la compatibilidad. La agrupación de métrica de uso de disco (MB) utiliza estas expresiones:

- ```
(.*)\\Custom Metric Process \\\(Virtual\\)\\ (.*)
```

- Enterprise Manager\|Data Store\|(.\*)Disk Usage \ (mb\|

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

139



en el panel de valores de agrupación de métrica. Si se selecciona esta opción, los agentes coincidentes cambiarán automáticamente si cambian las expresiones del Agente del módulo de gestión.

### **Estructura del nombre de la métrica**

Un nombre completo de métrica tiene la siguiente sintaxis:

```
Domain|Hostname|Process|AgentName|Resource:Metric
```

Por ejemplo, un nombre completo de métrica de una métrica en un recurso tiene el aspecto siguiente:

```
Acme|c1737019-a|AcmeUSA|AcmeWest|GC Heap:Bytes In Use
```

Si una métrica se encuentra dentro de dos recursos, el nombre se parece a este ejemplo:

```
Acme|c1737019-a|AcmeUSA|AcmeWest|Servlets|FileServlet:Responses Per Second
```

Si hay capas de recursos más profundas, los recursos están separados por el carácter de barra vertical (|).

Consulte [Uso de variables](#) para obtener más información sobre cómo se crean los nombres de métrica.

#### **NOTE**

Los usuarios en dominios que no sean el superdominio verán el nombre de la métrica sin la información del dominio en la siguiente sintaxis: *Hostname|Process|AgentName|Resource:Metric*. Por ejemplo: c1737019|AcmeUSA|AcmeWest|GC Heap:Bytes In Use

### **Creación de una agrupación de métrica en el menú Elementos**

Se puede crear una agrupación de métrica en el menú Elementos.

**Siga estos pasos:**

1. En Team Center, seleccione **Agrupaciones de métrica**.  
La página Agrupaciones de métrica muestra una lista de métricas que se agrupan en función de los módulos de gestión.
  2. En la página Agrupaciones de métrica, seleccione **Crear agrupación de métrica**.
  3. En la página Crear agrupación de métrica, introduzca los detalles siguientes:
    - a. En el campo **Nombre de agrupación de métrica**, introduzca un nombre de agrupación de métrica único (el nombre aparece en el árbol del Editor del módulo de gestión).
    - b. Seleccione un **módulo de gestión** para que contenga la agrupación de métrica de la lista desplegable. También puede seleccionar **Crear módulo de gestión** para crear un módulo de gestión en un cuadro de diálogo independiente.
    - c. En el campo **Descripción**, introduzca la descripción necesaria que ayuda a identificar la agrupación de métrica que se ha creado.
    - d. Seleccione las expresiones del agente necesarias que se vayan a utilizar:
      - Seleccione **Uso de expresiones del Agente del módulo de gestión** para utilizar las expresiones de agente que se han definido para el módulo de gestión.
      - Seleccione **Uso de expresiones del Agente de la agrupación de métrica** para utilizar expresiones de agente definidas para esta agrupación de métrica.
    - e. Introduzca información específica del agente y de la métrica en los campos **Expresión del Agente del módulo** y **Expresión de la métrica**.
    - f. Seleccione **Crear**
- La agrupación de métrica se ha creado correctamente.

#### **NOTE**

La agrupación de métrica está activa cuando se crea y no se puede desactivar.



## Personalización de las agrupaciones de métrica

Se pueden personalizar las expresiones regulares en la agrupación de métrica mediante la edición de los campos Expresiones del Agente de la agrupación de métrica y Expresiones de métrica para especificar las métricas que con las que deben coincidir.

### Reglas para editar las agrupaciones de métrica

- Separe los niveles sucesivos del árbol de Investigator con símbolos de barra diagonal inversa. (La barra diagonal inversa actúa como un carácter de escape).
- En Expresiones del Agente de la agrupación de métrica : Host\|Process\|AgentName, utilice **([^\|:]\*)** para representar un segmento de recursos.
- En **Servlets\([^\|:]\*)Average Response Time \(\ms\)**, es necesario un carácter de escape (barra diagonal inversa) para separadores y paréntesis \| y \( y \).
- En **Servlets\Servlet1Average Response Time \(\ms\)**, para que coincidan varios elementos con una expresión, puede incluir listas de elementos entre paréntesis usando caracteres de barra vertical.
- En **Servlets\Servlet(1|14|18)Average Response Time \(\ms\)**, si no hay ninguna carpeta de recursos entre el nombre de agente y la métrica, introduzca solamente el nombre de la métrica. De lo contrario, separe las carpetas de recursos con símbolos de barra diagonal inversa y anteponga el nombre de la métrica con dos puntos (:).
- In Expresiones de métrica: **resource\|subresource:Metric**
- In Expresiones de métrica: **resource:Metric**
- In Expresiones de métrica: **Metric**
- Por ejemplo, en Expresiones de métrica se especifica el tiempo medio de consulta de JDBC para un servlet llamado OptionReport como **Servlets\OptionReport\JDBC:Average Query Time**.
- Utilice **(.\*)** para representar "cualquiera".
- Por ejemplo, **Cherubim\PhoneHome\(.\*)** seguido de **Sockets:Output Bandwidth** especificará el ancho de banda de salida para todos los sockets de cualquier instancia del proceso PhoneHome que se ejecute en el host Cherubim.
- Una entrada de **File System:(.\*)** en el campo Expresiones de métrica significa que los datos que se van a mostrar son las métricas de entrada y salida de archivo que se encuentran en Investigator, en Sistema de archivos. Por el contrario, **File System:File Input Rate** muestra solo la tasa de entrada del archivo.
- Utilice **(.\*)\(.\*)\(.\*)** en el campo Agente para que la agrupación de métrica muestre los datos de cualquier servidor, proceso y agente. También se puede especificar cualquiera de los segmentos o todos ellos para que se ajusten a los agentes con un nombre de agente, proceso o host determinado.
- Utilice la lectura negativa en la expresión regular de la agrupación de métrica para excluir una rama del árbol de métrica. Por ejemplo, **Agents\(.\*)\(.\*)\(!ima\_q01)([^\|:]\*)ConnectionStatus** excluye "ConnectionStatus" de ima\_q01, pero sigue mostrando "ConnectionStatus" de otros agentes.


### Siga estos pasos:

1. En Team Center, seleccione **Agrupaciones de métrica**.  
La página Agrupaciones de métrica muestra una lista de métricas que se agrupan en función de los módulos de gestión.
2. Expanda la agrupación de métrica que desee actualizar.
3. Seleccione el *Metric\_Grouping\_Name* que desea actualizar.  
Aparecerá la página **Edit Metric Grouping: <Metric\_Grouping\_Name>**.
4. Edite la definición siguiendo las [Reglas para editar las agrupaciones de métrica](#).
5. Si es necesario, seleccione **el signo más ( + )** para especificar más métricas para la agrupación de métrica.
6. Seleccione **Aplicar**.

### Supresión de una agrupación de métrica en el menú Elementos

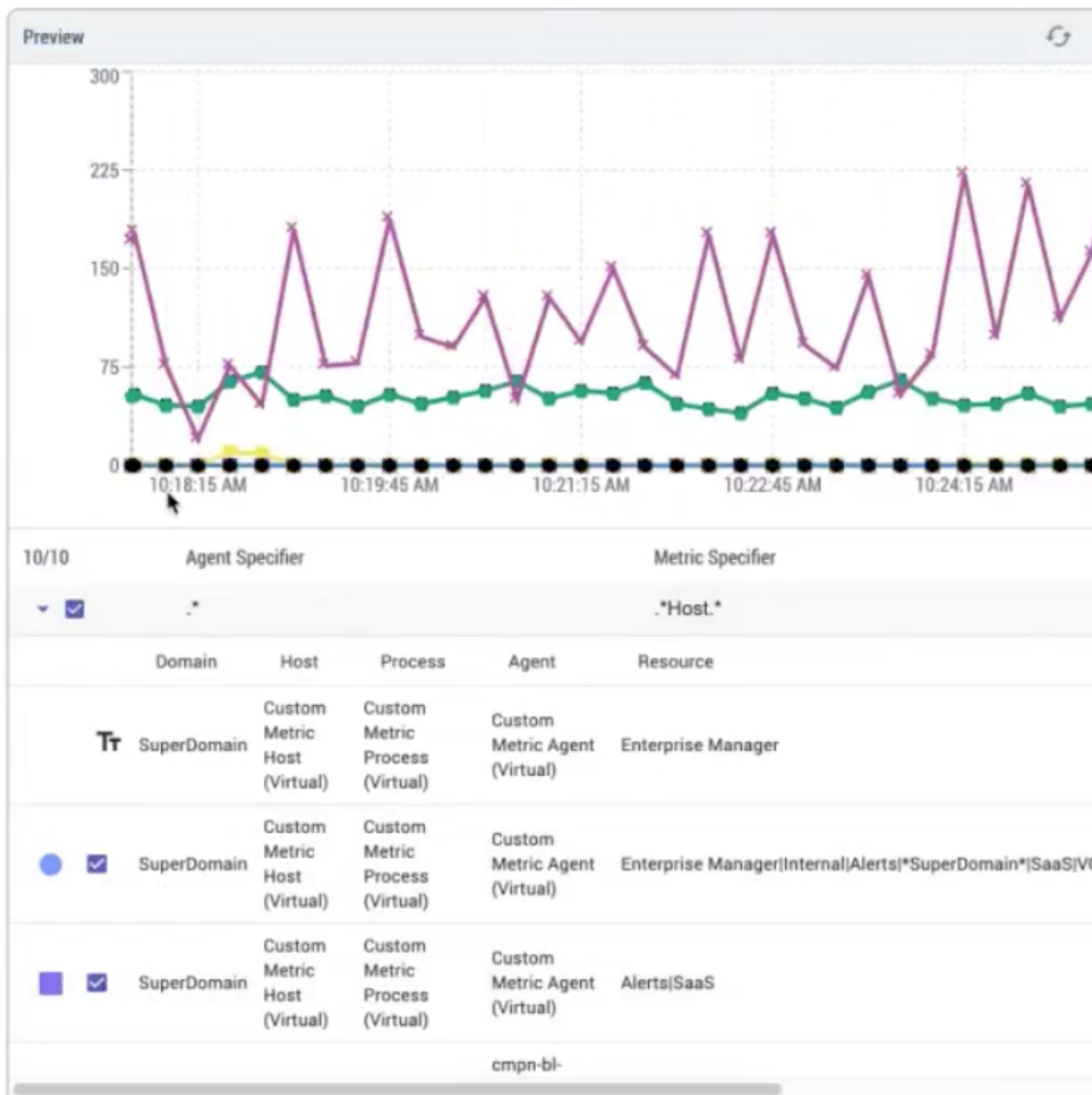
Se puede suprimir una agrupación de métrica en el menú Elementos.

**Siga estos pasos:**

1. En Team Center, seleccione **Agrupaciones de métrica**.  
La página Agrupaciones de métrica muestra una lista de métricas que se agrupan en función de los módulos de gestión.
2. Expanda la agrupación de métrica que desee actualizar.
3. Seleccione el *Metric\_Grouping\_Name* que desea actualizar.  
Aparecerá la página **Edit Metric Grouping: <Metric\_Grouping\_Name>**.
4.  
Seleccione el icono Suprimir (  )
5. Seleccione **Sí**

**Vista previa para la agrupación de métricas**

La vista previa de la Vista de métricas muestra el modo de vista previa de los grupos de métricas configurados. Se pueden ver los datos de las métricas relevantes trazados en la gráfica. La ventana Vista previa muestra la gráfica de datos de las métricas en función del **Especificador de agente** y el **Especificador de métrica** proporcionados en el campo **Expresiones**.



En la ventana Vista previa, se puede ver y realizar las siguientes tareas:

- Especifique el **Especificador de métrica** y el **Especificador de agente** en el campo **Expresiones** y se resaltará el icono **Actualizar**













Haga clic en el icono Actualizar para ver las últimas métricas en función de las expresiones.

- La tabla de la vista previa muestra el recuento de las métricas totales, el especificador de agente, el especificador de métrica y el número de métricas para ver en el gráfico.
- Se pueden seleccionar solamente diez métricas para ver en el gráfico.
- Se pueden personalizar las columnas que se mostrarán en la tabla. Haga clic en



y seleccione las columnas necesarias de la lista.

- Existen diez colores y formas diferentes para distinguir las métricas representadas en la gráfica. Al seleccionar una métrica de la lista, se asignan automáticamente un color y una forma a una 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     |
| <b>3/31/21 3:21:15 PM</b>                                                           |       |     |     |       |

- Haga clic en el icono de pantalla completa



para ver la ventana Vista previa en el modo de pantalla completa.

- En la gráfica de vista previa, el eje X representa los valores de las métricas y el eje Y representa el intervalo de tiempo.

Se pueden configurar agrupaciones de métrica en Team Center. Las agrupaciones de métrica se muestran como parte de la lista de carpetas, que representan los módulos de gestión. Cada carpeta contiene una lista de las agrupaciones de métrica correspondientes.

Para obtener más información sobre lo siguiente, consulte [Configuración de agrupaciones de métricas en Team Center](#).

- Especificación de expresiones para las agrupaciones de métrica
- Estructura del nombre de la métrica
- Creación de una agrupación de métrica en el menú Elementos
- Personalización de las agrupaciones de métrica
- Supresión de una agrupación de métrica en el menú Elementos
- Vista previa para la agrupación de métricas

## Creación y configuración de alertas sencillas en Team Center

Como administrador, se pueden crear y configurar alertas y acciones en Team Center para monitorizar el rendimiento.

### NOTE

No utilice el método estándar de creación de alertas de APM para las métricas ingeridas directamente en NASS (esto incluye las métricas de compatibilidad de APM Cloud Proxy y cualquier métrica que no sea de APM). En su lugar, utilice la [Configuración de alertas basadas en métricas](#) de DX OI.

### NOTE

Un icono Mantenimiento en la página Alertas en la ficha Mantenimiento muestra que la página está en mantenimiento. El icono Mantenimiento estará visible durante un período máximo de 7 días de antelación para cualquier mantenimiento próximo.

Aparecerá el icono Mantenimiento en función del siguiente orden de prioridad:

1. Activo con la última hora de finalización
2. Activo con la hora de finalización más corta
3. Programado con la hora de inicio más próxima
4. Resto de la programación

Team Center ofrece las siguientes alertas:

### Alerta sencilla

Utiliza la información de estado que produce una comparación y compara esta información con los valores del umbral definido por el usuario. El resultado de una alerta sencilla es un estado. Las alertas sencillas pueden utilizar los retrasos de acciones de peligro y precaución para determinar cuándo se deben iniciar las acciones especificadas. Una alerta sencilla puede producir uno de los estados siguientes:

- **No hay datos notificados**

Se produce si la alerta sencilla está inactiva, no coincide con ninguna métrica o las métricas coincidentes no se notifican.

- **Verde (Correcto)**
- **Amarillo (Precaución)**
- **Rojo (Peligro)**

La alerta sencilla es la alerta básica de Introscope. Las alertas sencillas pueden generar la entrada para una alerta de resumen. Esta alerta aparece en el nodo Alertas del árbol de Investigator.

### Alertas de resumen

Agrega el estado de varias alertas sencillas y otras alertas de resumen. Esta alerta aparece en el nodo Alertas del árbol de Investigator.

### NOTE

Más información: [Creación y configuración de alertas de resumen](#)

### Creación de una alerta sencilla desde el menú Elementos

Siga estos pasos:

1. En Team Center, seleccione **Alertas y Crear alerta**.  
La página Alertas muestra una lista de alertas que se agrupan por agrupación de métrica.
2. En la página Alertas, seleccione **Crear alerta**.
3. En la página Crear alerta, introduzca los detalles siguientes:
  - a. En el campo **Nombre de la alerta**, introduzca un nombre para la alerta sencilla.  
El nombre aparece en el árbol del Editor del módulo de gestión.

**TIP**

Utilice nombres informativos para las alertas. Se recomienda utilizar una convención de nomenclatura que ayude al destinatario de las alertas a identificar el origen de la alerta.

- b. En la lista desplegable **Canales de notificación**, seleccione el canal que desee aplicar a la alerta sencilla que se crea.
  - c. En el menú desplegable **Módulo de gestión**, seleccione el módulo deseado que se aplicará a la alerta sencilla que se crea. También puede seleccionar **Crear módulo de gestión** para crear un módulo de gestión en un cuadro de diálogo independiente.
  - d. En el campo **Descripción**, introduzca la descripción necesaria que ayuda a identificar la alerta sencilla que se crea.
  - e. En el campo **Agrupación de métrica**, seleccione la agrupación de métrica deseada que se aplicará a la alerta sencilla que se crea. También se puede seleccionar **Creación de una agrupación de métrica** para crear una **agrupación de métrica** en un cuadro de diálogo independiente.
  - f. En el campo **Resolución**, especifique la resolución del período de tiempo en horas, minutos o segundos. Una alerta utiliza datos de entrada de una agrupación de métricas seleccionadas. Para la resolución del tiempo, la alerta recopila información y resume un valor para ese período de tiempo. El valor resultante depende del tipo de datos en la métrica. Por ejemplo, si la métrica es un índice, el valor resumido es el promedio durante ese período de tiempo. O si la métrica es un contador, genera el valor más reciente del contador. Los valores del tiempo de resolución deben ser en incrementos de 15 segundos.
  - g. En el menú desplegable **Operador de comparación**, seleccione un valor de la lista desplegable para la condición que activa la alerta sencilla. El Operador de comparación, con valores del umbral de riesgo y de precaución, define la condición que activa la alerta sencilla. El Operador de comparación se refiere a los valores del umbral de peligro y de precaución. Por ejemplo, si desea que se le notifique cuando un tiempo de respuesta medio de un servlet sea superior a 5000, utilice el operador "mayor que". El Operador de comparación también afecta a los valores de los umbrales de precaución y peligro. Si el Operador de comparación se establece en mayor que, el valor del umbral de peligro debe ser mayor que el valor de umbral de precaución. Por el contrario, si el Operador de comparación se establece en menor que, el valor del umbral de peligro debe ser menor que el valor de umbral de precaución.
  - h. En el campo **Combinación**, especifica si se ha activado una alerta cuando una métrica supera un umbral (cualquiera) o cuando todas las métricas superan un umbral (todos). El campo Combinación se ignora cuando se selecciona la casilla de verificación Notificar por métrica individual.
  - i. En la sección **Umbrales**, seleccione **Guardar**.  
El módulo de gestión se ha creado correctamente.
4. Seleccione **Aceptar**.

La alerta sencilla que se ha creado se resalta en el árbol del Editor del módulo de gestión y su configuración aparece en el panel de configuración.

Para obtener más información sobre cómo activar notificaciones de alertas, consulte [Creación de notificaciones de alerta](#). Para obtener más información sobre la documentación de políticas para configurar notificaciones de alerta adicionales en Operational Intelligence, consulte [Creación de una política](#).

### **Actualización de una alerta sencilla desde el menú Elementos**

#### **Siga estos pasos:**

1. En Team Center, seleccione **Alertas**. Aparece la página Alertas con las alertas que se agrupan por agrupación de métrica.
2. Vaya a la agrupación de métrica de la alerta que se desea actualizar.
3. Seleccione **<Alert\_Name>** que desea actualizar.
4. En la página **Edit Alert: <Alert\_Name>** actualice los siguientes detalles:
  - a. En el campo **Nombre de la alerta**, actualice el nombre de la alerta sencilla.

El nombre aparece en el árbol del Editor del módulo de gestión.

### TIP

Utilice nombres informativos para las alertas. Se recomienda utilizar una convención de nomenclatura que ayude al destinatario de las alertas a identificar el origen de la alerta.

- b. En la lista desplegable **Canales de notificación**, seleccione el canal que desee aplicar a la alerta sencilla.
  - c. En el menú desplegable **Módulo de gestión**, seleccione el módulo deseado que se aplicará a la alerta sencilla. También puede seleccionar **Crear módulo de gestión** para crear un módulo de gestión en un cuadro de diálogo independiente.
  - d. En el campo **Descripción**, actualice la descripción necesaria que ayuda a identificar la alerta sencilla.
  - e. En el campo **Agrupación de métrica**, seleccione la agrupación de métrica deseada que se aplicará a la alerta sencilla. También se puede seleccionar **Creación de una agrupación de métrica** para crear una **agrupación de métrica** en un cuadro de diálogo independiente.
  - f. En el menú desplegable **Operador de comparación**, seleccione un valor de la lista desplegable para la condición que activa la alerta sencilla. El Operador de comparación, con valores del umbral de riesgo y de precaución, define la condición que activa la alerta sencilla. El Operador de comparación se refiere a los valores del umbral de peligro y de precaución. Por ejemplo, si desea que se le notifique cuando un tiempo de respuesta medio de un servlet sea superior a 5000, utilice el operador "mayor que". El Operador de comparación también afecta a los valores de los umbrales de precaución y peligro. Si el Operador de comparación se establece en mayor que, el valor del umbral de peligro debe ser mayor que el valor de umbral de precaución. Por el contrario, si el Operador de comparación se establece en menor que, el valor del umbral de peligro debe ser menor que el valor de umbral de precaución.
  - g. En la sección **Umbrales**, seleccione **Guardar**.  
El módulo de gestión se ha creado correctamente.
5. Seleccione **Aceptar**.

La alerta sencilla que se ha creado se resalta en el árbol del Editor del módulo de gestión y su configuración aparece en el panel de configuración.

### Copia de una alerta sencilla

Para copiar una alerta sencilla, realice las siguientes tareas.


1. En **Configuración**, haga clic en **Alertas**.
2. Se muestran los módulos de gestión disponibles para el usuario. También se puede buscar un módulo de gestión específico utilizando el filtro.
3. Haga clic en el nombre del módulo de gestión necesario y en el nombre de la alerta.
4. En la página **Editar alerta**, haga clic en **Guardar como nuevo**.
5. En el cuadro **Crear nueva alerta**, actualice los siguientes detalles, si es necesario.  
También puede omitir este paso y hacer clic en **Guardar** en el cuadro Crear nueva alerta para crear una copia de la alerta.
  - a. Haga clic en el botón de alternar para marcar la alerta como activa o inactiva.
  - b. En el campo **Nombre de la alerta**, introduzca un nombre para la alerta sencilla (el nombre aparece en el árbol del Editor del módulo de gestión).
  - c. En la lista desplegable **Canales de notificación**, seleccione el canal que desee aplicar a la alerta sencilla que se crea.
  - d. En el menú desplegable **Módulo de gestión**, seleccione el módulo deseado que se aplicará a la alerta sencilla que se crea. También puede seleccionar **Crear módulo de gestión** para crear un módulo de gestión en un cuadro de diálogo independiente.
  - e. En el campo **Descripción**, introduzca la descripción necesaria que ayuda a identificar la alerta sencilla que se crea.



- f. En el campo **Agrupación de métrica**, seleccione la agrupación de métrica deseada que se aplicará a la alerta sencilla que se crea. También se puede seleccionar Creación de una agrupación de métrica para crear una agrupación de métrica en un cuadro de diálogo independiente.
- g. En el campo **Resolución**, especifique la resolución del período de tiempo en horas, minutos o segundos. Una alerta utiliza datos de entrada de una agrupación de métricas seleccionadas. Para la resolución del tiempo, la alerta recopila información y resume un valor para ese período de tiempo. El valor resultante depende del tipo de datos en la métrica. Por ejemplo, si la métrica es un índice, el valor resumido es el promedio durante ese período de tiempo. O si la métrica es un contador, genera el valor más reciente del contador. Los valores del tiempo de resolución deben ser en incrementos de 15 segundos.
- h. En el menú desplegable **Operador de comparación**, seleccione un valor de la lista desplegable para la condición que activa la alerta sencilla. El Operador de comparación, con valores del umbral de riesgo y de precaución, define la condición que activa la alerta sencilla. El Operador de comparación se refiere a los valores del umbral de peligro y de precaución. Por ejemplo, si desea que se le notifique cuando un tiempo de respuesta medio de un servlet sea superior a 5000, utilice el operador "mayor que". El Operador de comparación también afecta a los valores de los umbrales de precaución y peligro. Si el Operador de comparación se establece en mayor que, el valor del umbral de peligro debe ser mayor que el valor de umbral de precaución. Por el contrario, si el Operador de comparación se establece en menor que, el valor del umbral de peligro debe ser menor que el valor de umbral de precaución.
- i. En el campo **Combinación**, especifica si se ha activado una alerta cuando una métrica supera un umbral (cualquiera) o cuando todas las métricas superan un umbral (todos). El campo Combinación se ignora cuando se selecciona la casilla de verificación Notificar por métrica individual.
- j. Especifique los valores en **Umbrales de peligro** y **Umbrales de precaución**.
- k. Haga clic en **Create**.  
La alerta se ha creado correctamente.
- l. En el cuadro de diálogo de confirmación, haga clic en **Aceptar**.  
La alerta aparece en la página **Módulos de gestión**.

### Supresión de una alerta sencilla desde el menú Elementos

#### **Siga estos pasos:**

1. En Team Center, seleccione **Alertas**.  
Aparece la página Alertas con las alertas que se agrupan por agrupación de métrica.
2. Vaya a la agrupación de métrica de la alerta que se desea suprimir.
3. Seleccione **<Alert\_Name>** que desea suprimir.  
Aparece la página **Edit Alert: <Alert\_Name>**.
4.  
En la página **Edit Alert: <Alert\_Name>** seleccione el icono Suprimir (  ).
5. Seleccione **Sí**
6. Seleccione **Aceptar**.

La alerta sencilla se ha suprimido correctamente.

### Configuración de los valores de configuración de una alerta sencilla

Después de crear una alerta sencilla, se definen las condiciones de activación.

#### **Siga estos pasos:**

1. Busque la alerta sencilla creada en el árbol del Editor de módulos de gestión, en el módulo de gestión correspondiente. Seleccione la alerta sencilla para mostrar sus valores de configuración.
2. En el panel de configuración, seleccione la casilla de verificación **Activa** para activar la alerta sencilla. Seleccione la casilla de verificación **Propagar a Team Center** para ver las alertas en Team Center.

3. Utilice el Operador de comparación, con las acciones de riesgo y de precaución, para definir la condición que activa la alerta sencilla.

Por ejemplo, si desea que se le notifique cuando un tiempo de respuesta medio de un servlet sea superior a 5000, utilice el operador *mayor que*.

#### NOTE

El Operador de comparación también afecta a los valores de los umbrales de precaución y peligro. Si el Operador de comparación se establece en *mayor que*, el valor del umbral de peligro debe ser mayor que el valor de umbral de precaución. Por el contrario, si el Operador de comparación se establece en *menor que*, el valor del umbral de peligro debe ser menor que el valor de umbral de precaución.

4. En Acciones de peligro o Acciones de precaución, seleccione **Agregar**.
  - a. Seleccione una acción y seleccione **Elegir**.
  - b. Agregue otra acción si es necesario.
  - c. En el panel Configuración de alerta sencilla, seleccione **Aplicar**.
5. En el campo Umbral, introduzca un valor que activa una alerta de peligro o una alerta de precaución. Las unidades de los valores del umbral de peligro se corresponden con el valor utilizado en la agrupación de la métrica. Por ejemplo, si crea una alerta sencilla para el tiempo medio de respuesta del servlet, utilice milisegundos.
6. Defina la proporción de períodos excesivos que activan la alerta. Establezca esta condición en los campos **Períodos por encima del umbral** y **Períodos observados**.

**Ejemplo:** Ha introducido 8 y 10. La alerta de peligro solo se activa cuando la métrica supera el umbral de peligro en 8 de los 10 períodos observados.

#### TIP

- Utilice la propiedad *Al menos N de los últimos M períodos* para definir alertas de problemas reales. Esta propiedad define el número de instancias necesarias para que el umbral de peligro active una alerta. Por ejemplo, en los entornos de producción, los indicadores clave de rendimiento pueden tener un pico durante un corto período de tiempo. Una CPU puede llegar al pico en un período de 15 segundos y, a continuación, volver a la normalidad en el siguiente período de 15 segundos. Este comportamiento de rendimiento no requiere una alerta y se puede descartar mediante una condición.
- Se recomienda notificar a los destinatarios de alerta antes de cambiar los umbrales de alerta existentes. Reducir el umbral de una alerta activa puede provocar que se envíe la alerta.

#### NOTE

Las alertas se activarán solo al final del **Período observado** y no tan pronto como se alcance el valor de la opción Períodos por encima del umbral.

7. Establezca un retraso de acción en horas, minutos y segundos.  
Los retrasos de acción de peligro o precaución determinan cuándo se activa una acción de alerta sencilla.

#### NOTE

Los retrasos de acción de peligro o precaución no están disponibles en la opción Alerta de resolución.

8. Seleccione **Aplicar**.  
La alerta sencilla se completa y aparece en el árbol del módulo de gestión correspondiente. Ejemplo: Configuración de una alerta para la desconexión del agente

#### NOTE

Cuando se crea una alerta sencilla a partir de una métrica, se crea automáticamente una agrupación de métrica. Esta agrupación de métrica aparece en el mismo módulo de gestión.

### Configuración de una alerta para la desconexión del agente

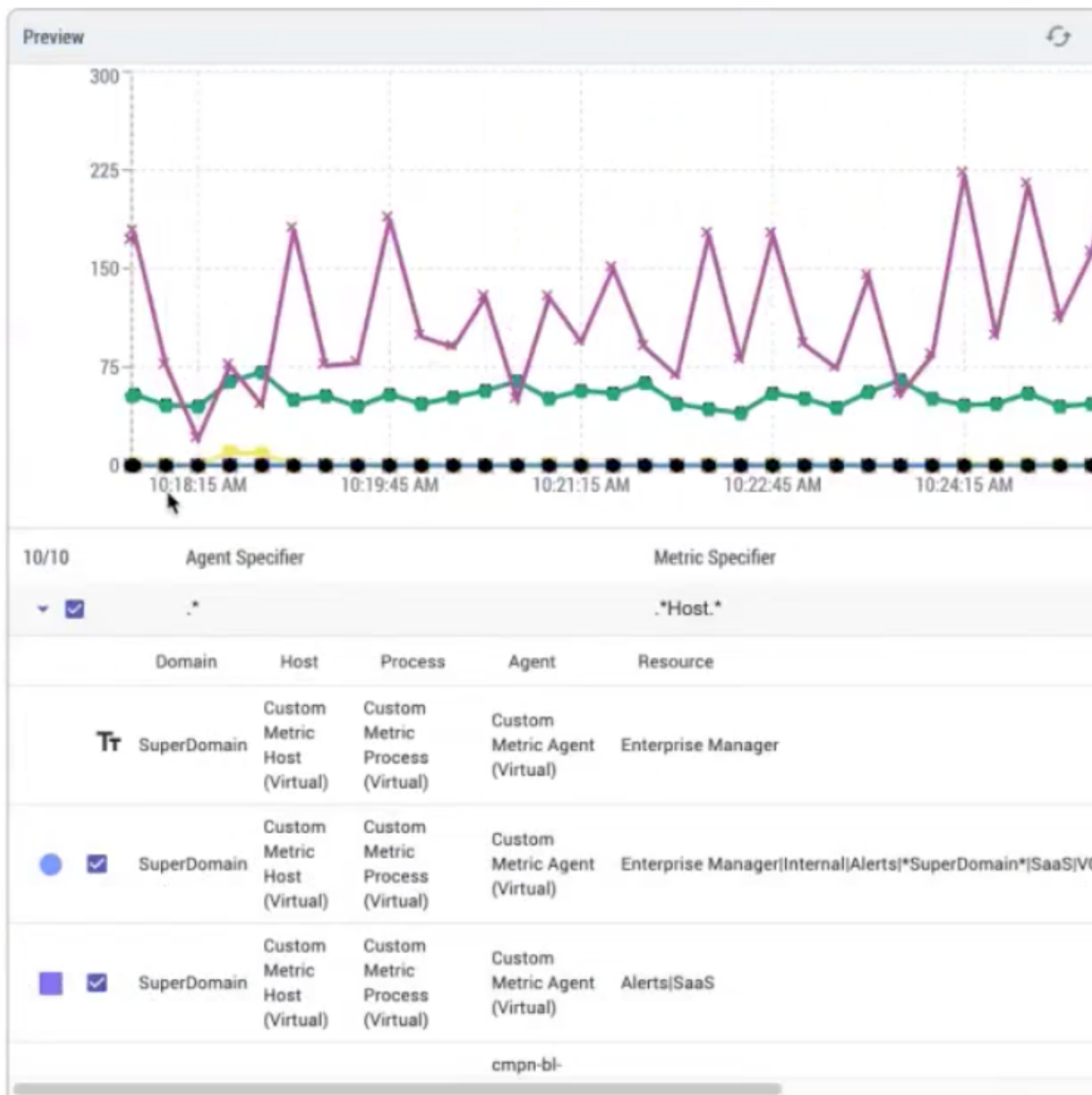
Si un agente se desconecta de Enterprise Manager, ya no podrá recopilar o monitorizar los datos de ese agente. Puede configurar una alerta para activar una notificación que le avise si se produce una desconexión.

**Siga estos pasos:**

1. En Team Center, seleccione **Agrupaciones de métrica**.
2. En la página Agrupaciones de métrica, seleccione **Nueva agrupación de métrica**.
3. Esta métrica tiene los valores siguientes:
  - 3 = desconectado. Indica que el agente se ha desconectado de forma manual.
  - 2 = conectado, ritmo lento o sin datos
  - 1 = conectado
  - 0 = desmontado. Indica que el agente se ha desconectado de Enterprise Manager después de un período de tiempo determinado. Este período se puede configurar.
4. Escriba un nombre para la nueva alerta y, a continuación, seleccione **Aceptar**.
5. Establezca el Operador de comparación como **Menor que**.
6. Establezca el umbral de peligro y el umbral de precaución.
7. Establezca la sensibilidad del umbral de la alerta. **Ejemplos:**
  - Muy sensible (Peligro=2, Precaución=2, Al menos 1 de los últimos 10 períodos)
  - Menos sensible (Peligro=3, Precaución=2, Al menos 3 de los últimos 10 períodos)
8. Seleccione **Activo**.
9. Seleccione **Aplicar**.

**Vista previa para las alertas**

La vista previa de las alertas muestra el modo de vista previa de los grupos de métricas configurados. Se pueden ver los datos de las métricas relevantes trazados en la gráfica. La ventana de la vista previa muestra la gráfica de datos de las métricas en función del campo **Agrupación de métrica**.



En la ventana Vista previa, se puede ver y realizar las siguientes tareas:

- Proporcione el filtro para el campo Agrupación de métrica y se resaltará el icono **Actualizar**













Haga clic en el icono Actualizar para ver las últimas métricas en función de las expresiones.

- La tabla de la vista previa muestra el recuento de las métricas totales, el especificador de agente, el especificador de métrica y el número de métricas para ver en el gráfico.
- Se pueden seleccionar solamente diez métricas para ver en el gráfico.
- Se pueden personalizar las columnas que se mostrarán en la tabla. Haga clic en



y seleccione las columnas necesarias de la lista.

- Existen diez colores y formas diferentes para distinguir las métricas representadas en la gráfica. Al seleccionar una métrica de la lista, se asignan automáticamente un color y una forma a una 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

- Haga clic en el icono de pantalla completa



para ver la ventana Vista previa en el modo de pantalla completa.

- En la gráfica de vista previa, el eje X representa los valores de las métricas y el eje Y representa el intervalo de tiempo.

Como administrador, se pueden crear y configurar alertas y acciones en Team Center para monitorizar el rendimiento. Team Center ofrece las siguientes alertas:

- Alerta sencilla
- Alertas de resumen

Para obtener más información sobre cómo crear, actualizar, suprimir y configurar una alerta sencilla, consulte [Creación y configuración de alertas sencillas en Team Center](#).

## Creación y configuración de alertas de resumen

Una alerta de resumen proporciona una manera de mostrar el estado de varias alertas sencillas subyacentes con un estado general. Se pueden crear y configurar alertas de resumen en Team Center, Workstation o WebView. Es posible modificar el nombre y las alertas sencillas subyacentes en todos los entornos. Hay diferencias en las notificaciones y las acciones:

- **Team Center:** Compatibilidad para la asignación del canal de notificación: método preferido
- **Workstation:** Compatibilidad para crear y asignar acciones del seguimiento de transacciones
- **Webview:** Compatibilidad solo para la asignación de acciones del seguimiento de transacciones

Esta sección contiene la siguiente información:

- [Alertas de resumen](#)
- [Creación de una alerta de resumen](#)
- [Configuración de una alerta de resumen](#)
- [Retrasos en las acciones de peligro y precaución](#)

#### NOTE

Un icono Mantenimiento en la página Alertas de resumen muestra que la página está en mantenimiento. El icono Mantenimiento estará visible durante un período máximo de 7 días de antelación para cualquier mantenimiento próximo.

Aparecerá el icono Mantenimiento en función del siguiente orden de prioridad:

1. Activo con la última hora de finalización
2. Activo con la hora de finalización más corta
3. Programado con la hora de inicio más próxima
4. Resto de la programación

### Alertas de resumen

Las alertas de resumen no tienen umbrales de peligro ni precaución explícitos, así como tampoco expresiones de comparación, como sí los tienen las alertas sencillas. Una alerta sencilla tiene uno de cuatro estados: sin generar informes, verde, amarillo y rojo.

| Icono de estado               | Definición           | Valor numérico |
|-------------------------------|----------------------|----------------|
| Diamante o triángulo amarillo | Precaución           | 2              |
| Octágono o cuadrado rojo      | Peligro              | 3              |
| Disco verde                   | Normal               | 1              |
| Disco gris                    | Sin generar informes | 0              |

El estado de alerta de resumen es el peor estado entre las alertas sencillas que contiene. La alerta de resumen se puede definir para Cualquier alerta o Todas las alertas. La opción Cualquier alerta usa el estado máximo de todas las alertas. La opción Todas las alertas usa el estado mínimo de todas las alertas con un estado superior a 0 (sin generar informes). Ejemplo: Hay una alerta de resumen que incluye las siguientes alertas:

- Alerta: A; Estado: 0
- Alerta: B; Estado: 1
- Alerta: C; Estado: 1
- Alerta: D; Estado: 2
- Alerta: E; Estado: 3

En esta situación, la opción Cualquier alerta toma el estado 3 y la opción Todas las alertas, el estado 1.

### Creación de una alerta de resumen

Para Team Center, realice las siguientes acciones:

1. Vaya a **Configuración**, seleccione **Alertas, Alertas de resumen**.
2. Haga clic en **Crear alerta de resumen**.

3. Establezca la configuración de la alerta de resumen.

Para Workstation o Webview, realice las siguientes acciones:

1. En la ventana Editor del módulo de gestión, seleccione Elementos, Nueva alerta, Nueva alerta de resumen.
2. Complete las siguientes opciones:

- **Nombre:** Especifica el nombre del elemento. Para identificar la fuente de un elemento, utilice un nombre descriptivo.

#### **NOTE**

Las alertas sencillas y de resumen aparecen juntas en el nodo Alertas. Por lo tanto, especifique un nombre para distinguir las alertas de resumen de las alertas sencillas.

- **Imponer unicidad:** Añade un número al nombre cuando existe el mismo nombre en el módulo de gestión.
  - **Módulo de gestión:** Especifica un módulo de gestión para contener el elemento.
3. Haga clic en Aceptar. La alerta de resumen que se ha creado se resalta en el árbol del Editor del módulo de gestión y aparece en el panel de configuración.
  4. Establezca la configuración de la alerta de resumen.

### **Configuración de una alerta de resumen**

En todos los entornos, se puede hacer lo siguiente:

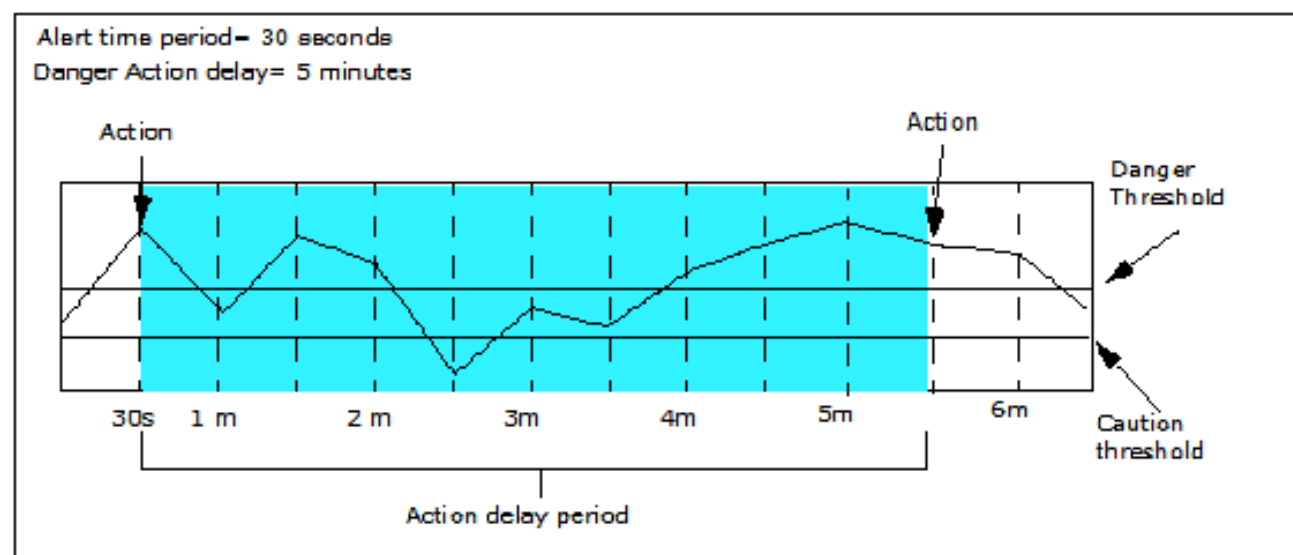
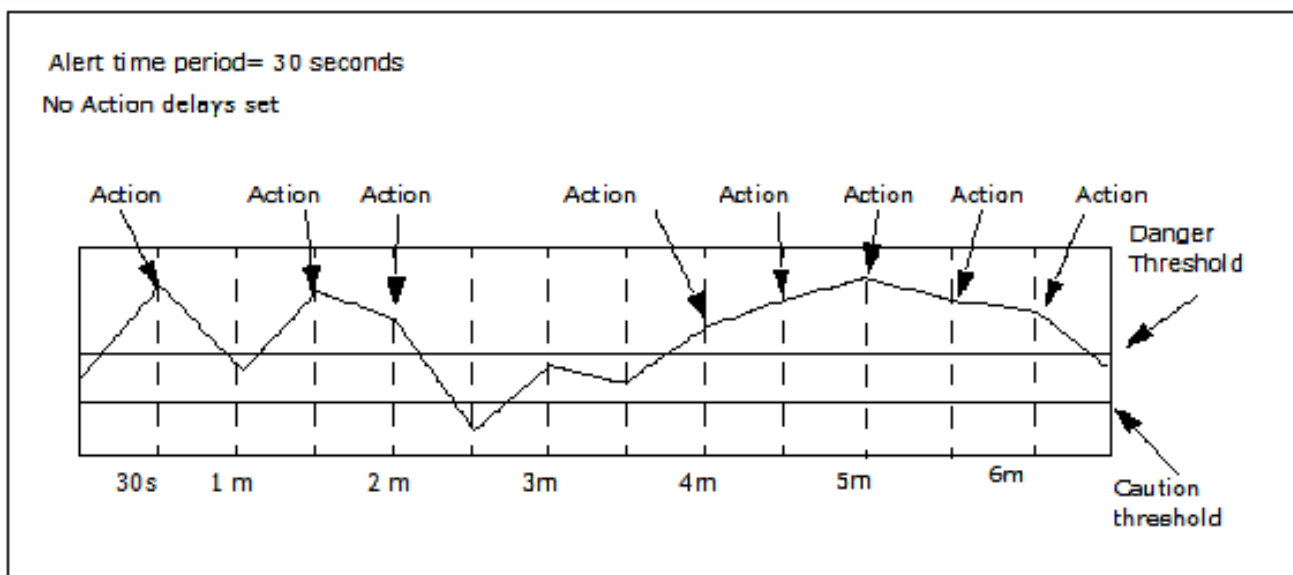
1. Edite los campos según sea necesario. Por ejemplo, se pueden realizar las siguientes acciones:
  - Edite el nombre y seleccione un módulo de gestión.
  - Active o desactive el objeto mediante la casilla de selección Activo.
2. Asigne las alertas a la alerta de resumen. Para Team Center, utilice el botón **Agregar alertas**. Para Workstation o Webview, seleccione una o más alertas y utilice las flechas para moverlas de la lista Disponibles a la lista Incluidos.
3. Seleccione una combinación para Cualquier alerta o Todas las alertas.

En Team Center, se puede asignar un canal de notificación. En Workstation o Webview, se puede asignar una acción del seguimiento de transacciones y se puede establecer un retraso de la acción.

### **Retrasos en las acciones de peligro y precaución**

(Solo Webview y Workstation para las acciones del seguimiento de transacciones)

Los retrasos en la acción de peligro y precaución determinan las condiciones en las cuales los estados de peligro o precaución se notifican mediante un resultado de comparación en una acción. Estos retrasos de la acción evitan inundaciones de notificaciones de alerta. Un retraso actúa como un botón para posponer las notificaciones de alerta. Es posible configurar un retraso entre la primera notificación de alerta y las notificaciones subsiguientes.



En una situación donde el período de alerta se configura en 30 segundos. Si la información genera un estado de alerta de peligro y se ha definido una acción para él, se activa la acción. Sin un retraso establecido, si el estado de peligro continúa, se le notificará cada vez que se excede el umbral de peligro. Por ejemplo, se le notifica ocho veces durante un período corto. Los problemas, por lo general, no se solucionan en un período tan corto como 30 segundos. Por lo tanto, retrase las acciones subsiguientes con un retraso de la acción. Es decir, con el mismo período de alerta de 30 segundos, si se configura un retraso de acción de cinco minutos para el estado de peligro, se recibirá la primera notificación de alerta en la marca de 30 segundos. Sin embargo, si el estado de peligro ocurre de nuevo durante ese período de tiempo sin disponibilidad de la acción de cinco minutos y el umbral de peligro aún se excede cuando finaliza el período sin disponibilidad, no se le notificará una segunda acción hasta cinco minutos después de la primera notificación.

## Creación y edición de calculadoras

Las calculadoras admiten los valores de una agrupación de métrica, como la entrada, el promedio o la suma de los valores. Las calculadoras envían el valor resultante como una métrica personalizada en el árbol de Investigator. Las



métricas generadas por la calculadora aparecen en un proceso virtual denominado Proceso de métrica personalizada. El proceso de métrica personalizada se ejecuta en un host virtual que se denomina Host de métrica personalizada.

### **Acerca de las calculadoras**

Las calculadoras pueden calcular el promedio o sumar los valores de una agrupación de métrica y, a continuación, generar métricas personalizadas en el árbol de Investigator. Métricas de la calculadora que se ejecutan en un proceso virtual, denominado proceso de métrica personalizada. Este proceso se ejecuta en un host virtual, el host de métrica personalizada.

Las métricas de compatibilidad recopilan datos a través de las calculadoras. Para notificar los datos correctamente, cualquier calculadora basada en MOM requiere datos de al menos un recopilador. Sin los datos del recopilador, MOM no puede calcular ni mostrar las métricas.

#### **Ejemplo**

En una MOM, se desea ver la métrica `(.*)\\Custom Metric Process \\(Virtual\\)\\Custom Metric Agent \\(Virtual\\)Enterprise Manager\\Configuration:Number of Metric Groupings`. Se espera un valor de métrica mayor que 0.

Cuando MOM no tiene ningún recopilador conectado, la métrica `Número de agrupaciones de métrica` notifica 0.

Cuando MOM tiene al menos un recopilador conectado, la métrica `Número de agrupaciones de métrica` notifica el valor correcto.

### **Calculadora de JavaScript**

Una calculadora de JavaScript realiza cálculos complejos, como la desviación estándar y los medios no ponderados. Aquí se presentan más ventajas:

- Mayor control sobre la frecuencia de cálculo de las métricas
- La gestión de rutas de la métrica calculada para que parezca que agente informa de la métrica
- Almacenar cálculos anteriores y generar métricas agregadas durante un período de tiempo especificado mediante variables globales
- Evaluar métricas de cadena o producir una métrica de cadena calculada

### **Calculadora del módulo de gestión**

La calculadora del módulo de gestión realiza cálculos simples en métricas como Suma, Promedio, Mín. y Máx.

La calculadora del módulo de gestión requiere menos recursos que las calculadoras de JavaScript. Aquí se presentan más ventajas:

- Requiere menos recursos del sistema que la calculadora de JavaScript
- Se pueden crear y mantener las calculadoras. No es necesario acceder a los directorios de instalación para crear o gestionar la calculadora del módulo de gestión.

### **Creación de una calculadora**

Se puede crear una calculadora para un grupo de métricas.

#### **Siga estos pasos:**

1. En Team Center, seleccione **Calculadoras**.  
La página Calculadoras muestra una lista de calculadoras que se agrupan en función de los módulos de gestión.
2. Seleccione **Crear calculadora**.  
Aparecerá la página Crear calculadora.
3. Para editar una calculadora, seleccione la calculadora que desea actualizar.

Aparecerá la página Editar calculadora: <Calculator\_Name>.

4. En el menú desplegable **Módulo de gestión**, seleccione el módulo deseado que se aplicará a la calculadora sencilla que se crea. También puede seleccionar **Crear módulo de gestión** para crear un módulo de gestión en un cuadro de diálogo independiente.
5. En el campo **Descripción**, introduzca la descripción necesaria que ayuda a identificar la calculadora sencilla que se crea.
6. En el campo **Agrupación de métrica**, seleccione la agrupación de métrica deseada que se aplicará a la calculadora sencilla que se crea. También se puede seleccionar **Creación de una agrupación de métrica** para crear una agrupación de métrica en un cuadro de diálogo independiente.

#### NOTE

- Cuando se crea la calculadora, se crea automáticamente una agrupación de métrica con el mismo nombre que la calculadora. Sin embargo, la agrupación de métrica debe personalizarse antes de que pueda proporcionar datos a la calculadora.
- Seleccione una agrupación de métrica que proporcione valores enteros. Las calculadoras no pueden aceptar valores que no sean enteros como entrada. Los tipos mixtos producen resultados inesperados.

#### NOTE

**Más información:** [Configuración de agrupaciones de métrica en Team Center](#)

### Calculadoras y medias ponderadas

Las calculadoras de Introscope pueden generar métricas que se basan en promedios. Los cálculos se basan en las medias ponderadas, no en las medias directas. Las medias ponderadas resultan útiles para monitorizar el rendimiento de la aplicación en un entorno de clúster. En esta situación, se puede ver un tiempo de respuesta preciso entre varios servidores que probablemente tengan diferentes niveles de carga.

#### Ejemplo:

Se dispone de una calculadora que genera una métrica a partir del tiempo medio de respuesta para cinco servlets. Una media directa sumaría el tiempo de respuesta para un período de tiempo determinado y lo dividiría por cinco. Una media ponderada daría más peso a los servlets a los que se llama más a menudo, proporcionando un promedio más preciso.

### Cambios de los tipos de operación en las calculadoras del módulo de gestión

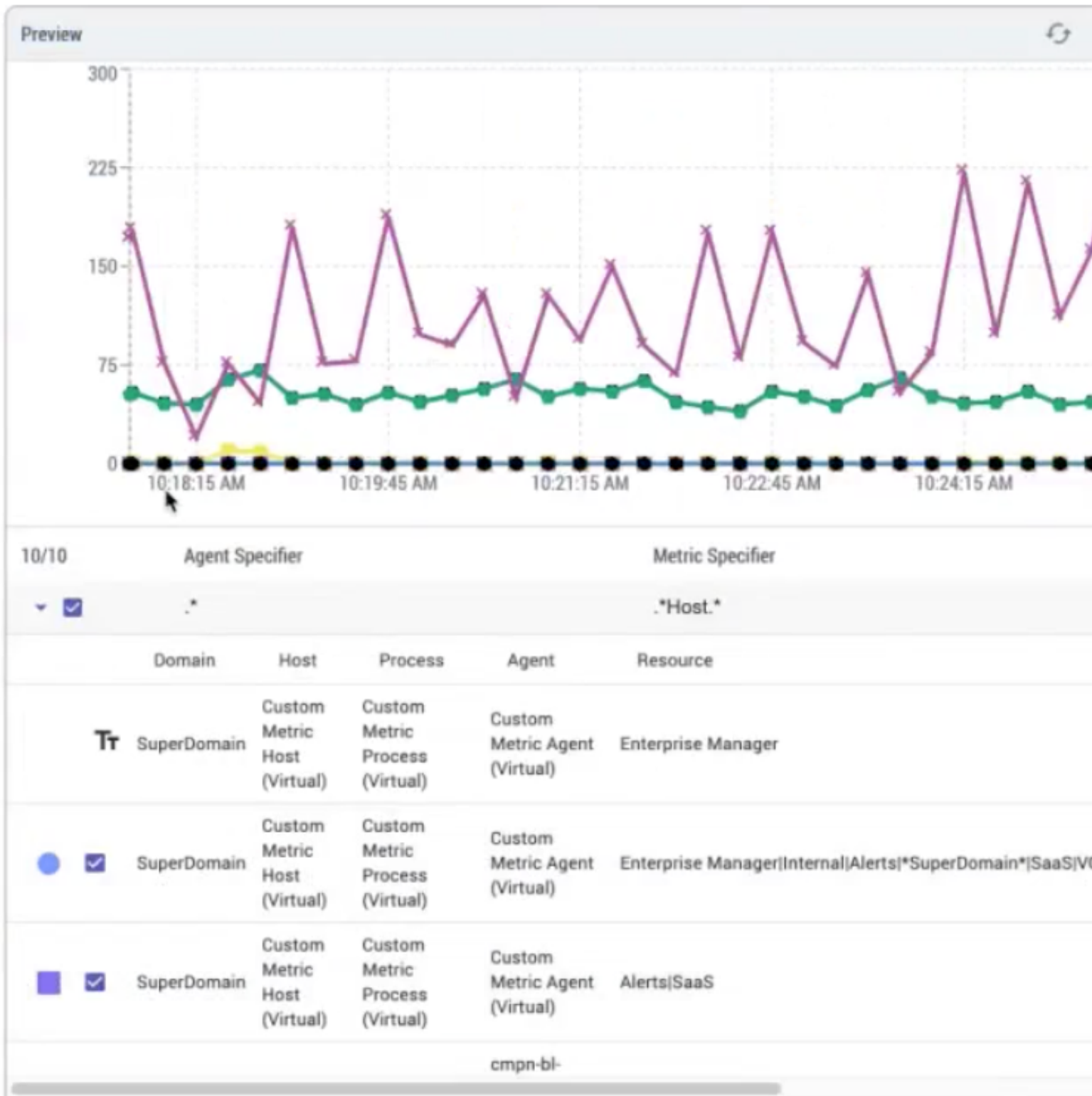
Cuando se edita una calculadora en un módulo de gestión, al cambiar el tipo de operación, se redefine el significado de la métrica de salida de la calculadora. Por ejemplo, de MÍN a MÁX. Si se mantiene el mismo nombre de la métrica de salida de la calculadora, la visualización de esta métrica yuxtapone los valores anteriores en el historial (calculado, por ejemplo, por el MÍN) con los nuevos valores (por ejemplo, el MÁX). La visualización de la métrica de salida no ofrece ninguna indicación sobre el lugar en el que se produjo la alteración del procesamiento. Si los usuarios se pueden confundir, cambie el nombre de la métrica de salida de la calculadora al cambiar el tipo de operación.

#### NOTE

**Más información:** [Cambios del tipo de operación en las calculadoras del módulo de gestión](#)

Vista previa para las calculadoras

La vista previa Calculadoras muestra el modo de vista previa de los grupos de métricas configurados. Se pueden ver los datos de las métricas relevantes trazados en la gráfica. La ventana de la vista previa muestra la gráfica de datos de las métricas en función del campo **Agrupación de métrica**.



En la ventana Vista previa, se puede ver y realizar las siguientes tareas:


- Proporcione el filtro para el campo Agrupación de métrica y se resaltará el icono **Actualizar**













Haga clic en el icono Actualizar para ver las últimas métricas en función de las expresiones.

- La tabla de la vista previa muestra el recuento de las métricas totales, el especificador de agente, el especificador de métrica y el número de métricas para ver en el gráfico.
- Se pueden seleccionar solamente diez métricas para ver en el gráfico.
- 



Se pueden personalizar las columnas que se mostrarán en la tabla. Haga clic en  y seleccione las columnas necesarias de la lista.

- Existen diez colores y formas diferentes para distinguir las métricas representadas en la gráfica. Al seleccionar una métrica de la lista, se asignan automáticamente un color y una forma a una 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                                                                  |       |     |     |       |

- Haga clic en el icono de pantalla completa



para ver la ventana Vista previa en el modo de pantalla completa.

- En la gráfica de vista previa, el eje X representa los valores de las métricas y el eje Y representa el intervalo de tiempo.

Las calculadoras admiten los valores de una agrupación de métrica, como la entrada, el promedio o la suma de los valores. Las calculadoras envían el valor resultante como una métrica personalizada en el árbol de Investigador. Las métricas generadas por la calculadora aparecen en un proceso virtual denominado Proceso de métrica personalizada.

Para obtener más información sobre las calculadoras, sobre cómo crear una calculadora y sobre cómo cambiar los tipos de operación, consulte [Creación y edición de calculadoras](#).

## Configuración del Análisis diferencial

El Análisis diferencial está activo de forma predeterminada. Sin embargo, como administrador, se puede establecer la configuración predeterminada o crear y configurar elementos del Análisis diferencial. Como evaluador de errores de las aplicaciones, se puede monitorizar el rendimiento utilizando la información que aparece en el mapa o gráfico del Análisis diferencial.

### Verificación de los requisitos previos del Análisis diferencial

Antes de implementar el Análisis diferencial, verifique que la implementación de CA APM incluya lo siguiente:

- Una instancia de Enterprise Manager
- Agentes configurados para los front-end, los back-end, las transacciones comerciales o todos.
- Para la instalación de CA CEM, se ha instalado una instancia de Transaction Impact Monitor (TIM).
- Se pueden tener una o más instancias de TIM en un entorno de CA CEM.

### **Creación de un control diferencial**

Los controles diferenciales son elementos que detectan inestabilidad en las métricas de coincidencia. Los umbrales de precaución y peligro controlan la intensidad de la varianza, que es una medida de la estabilidad de la métrica. Este comportamiento hace que los controles diferenciales sean diferentes a las alertas tradicionales que combinan un estado de verde, amarillo y rojo e implican que existen problemas. Los controles diferenciales permiten determinar cuánta inestabilidad se debe registrar para introducir zonas de intensidad de la varianza de peligro y precaución. Las opciones avanzadas proporcionan aún más control sobre la intensidad de la varianza del Análisis diferencial. En general, los usuarios del Análisis diferencial pueden aplicar umbrales bajos y ver la fuente completa de los cambios de estabilidad o utilizar umbrales altos y limitar la salida a un goteo de solo los cambios más extremos (por lo que es más probable que indiquen que existe un problema).

Se recomienda comenzar con los umbrales predeterminados y cambie la configuración predeterminada del umbral de alerta para indicar las intensidades con las que se desea recibir una notificación.

El mapa del Análisis diferencial aparece solamente para una métrica si existe un control diferencial. Se crea un elemento del control diferencial en un módulo de gestión que coincida con la métrica. Los módulos de gestión pueden existir para cada dominio o en todos los dominios y contienen elementos que organizan los datos de las métricas para su presentación.

Siga estos pasos:

1. En Team Center, seleccione **Análisis diferencial**.

La página Análisis diferencial muestra una lista de controles del Análisis diferencial agrupados en función de los módulos de gestión.

2. En la página Análisis diferencial, seleccione **Crear el control del Análisis diferencial**.

Se muestra la página Crear el control del Análisis diferencial.

3. Especifique las siguientes opciones y haga clic en **Crear**.

- **Activo:** Un control del Análisis diferencial está activo de forma predeterminada. Sin embargo, se configura si está activo o inactivo.
- **Nombre:** Especifique un nombre para el elemento Control del Análisis diferencial.
- **Módulo de gestión:** Especifique un módulo de gestión al que pertenece este elemento Control del Análisis diferencial.
- **Descripción:** Opcional. Proporcione una descripción breve del elemento Control del Análisis diferencial.
- **Agrupación de métricas:** Realice una de las siguientes acciones para seleccionar la agrupación de métricas:
  - Seleccione la lista desplegable **Mostrar filtros**, seleccione todos los módulos de gestión de los que desee seleccionar la agrupación de métricas y, a continuación, seleccione la agrupación de métricas necesaria de la lista. Si es necesario, haga clic en **Abrir** para editar la agrupación de métrica seleccionada.
  - Seleccione la agrupación de métricas necesaria de la lista de todas las agrupaciones de métricas disponibles. Si es necesario, haga clic en **Abrir** para editar la agrupación de métrica seleccionada.
  - Seleccione el icono desplegable de la lista de agrupaciones de métricas disponibles y, a continuación, haga clic en **Crear agrupación de métricas**, que está disponible en la parte inferior de la lista.

La página Crear agrupación de métricas aparece para crear una nueva agrupación de métricas. Para obtener más información, consulte Configuración de agrupaciones de métricas en Team Center.
- **Umbrales:** Establezca las opciones del umbral para las alertas de **Peligro** y de **Precaución**. Este valor activa una alerta de peligro o una alerta de precaución.
- **Ventana de evaluación:**

- **Longitud:** Especifica el número de celdas anteriores de 15 segundos que influyen en el peso de una ventana. El peso total de la ventana determina las regiones de precaución o peligro. Cada celda de la ventana contiene el mayor peso de todas las reglas rotas durante esos 15 segundos, menos cualquier disminución. Las celdas más antiguas dejan de aparecer y se van descartando a medida que se agregan nuevas celdas. Valor predeterminado: 20
- **Disminución:** Especifica la velocidad a la que las reglas infringidas disminuyen con su celda a lo largo del tiempo. A medida que se agregan celdas nuevas, la disminución reduce el efecto de los pesos agregados anteriormente en la ventana. El más nuevo siempre tiene el peso completo. En función del valor de la disminución, solo se tienen en cuenta algunas partes de los pesos antiguos para el cálculo final. Por lo tanto, cada celda de la ventana tiene un porcentaje de reducción después del nivel de disminución. En función de este valor del porcentaje de reducción, se reducen los pesos en cada nueva instancia agregada a la ventana. 100 representa la disminución más rápida, las infracciones de reglas se reducen rápidamente a medida que se van haciendo más antiguas. De la más nueva a la más antigua, las celdas tienen reducciones progresivas de la disminución de 0 a 100 en su peso. Por ejemplo, las celdas más antiguas tienen una reducción completa de su peso. Esta configuración reduce la probabilidad de recibir una notificación de precaución y peligro, especialmente cuando un período de inestabilidad pasa rápidamente. 0 representa la sensibilidad más alta (sin disminución) y las infracciones mantienen su valor completo durante toda la ventana. La más antigua tiene el mismo valor que tenía cuando era la más nueva. Mediante esta configuración, un período corto de inestabilidad puede mantener el pico en un estado de precaución o peligro hasta que esté completamente fuera de la ventana. El valor predeterminado es 20. Las infracciones recientes de reglas valen moderadamente más que las más antiguas.
- **Aplicación de reglas:** Especifica una regla para activar los picos:
  - **Regla 1:  $+3\sigma$**  Cualquier punto de datos único se encuentra fuera del límite  $3\sigma$  de la línea central.
  - **Regla 2:  $+2\sigma$  (2/3)** Dos de los tres puntos consecutivos se encuentran por encima del límite  $2\sigma$ .
  - **Regla 3:  $+1\sigma$  (4/5)** Cuatro de los cinco puntos consecutivos se encuentran por encima del límite  $1\sigma$ .
  - **Regla 4:  $\Delta f(x) \geq 0$  (10/10)** Diez de los diez puntos consecutivos aumentan o disminuyen.

Los controles diferenciales son elementos que detectan inestabilidad en las métricas de coincidencia. Los controles diferenciales permiten determinar cuánta inestabilidad se debe registrar para introducir zonas de intensidad de la varianza de peligro y precaución. Las opciones avanzadas proporcionan aún más control sobre la intensidad de la varianza del Análisis diferencial.

En general, los usuarios del Análisis diferencial pueden aplicar umbrales bajos y ver la fuente completa de los cambios de estabilidad o utilizar umbrales altos y limitar la salida a un goteo de solo los cambios más extremos (por lo que es más probable que indiquen que existe un problema). El Análisis diferencial está activo de forma predeterminada.

Para obtener más información sobre los requisitos previos y sobre cómo crear un control diferencial, consulte [Configuración del Análisis diferencial](#).

## Configuración de extensiones de JavaScript

Una extensión de JavaScript permite crear una nueva extensión y editar una existente. Esta extensión lee las métricas de entrada y genera métricas de salida según los cálculos especificados en un archivo de texto de JavaScript creado por el usuario. Las nuevas métricas calculadas pueden aparecer en el árbol de Investigator, en el Agente personalizado virtual. Las métricas también pueden aparecer en cualquier nodo del árbol de Investigator, según la métrica de salida que se especifique en el script de la calculadora. Se puede apagar una métrica calculada, pero la calculadora que la produce no conoce el estado de apagado. El motor de JavaScript de Enterprise Manager permite implementar en caliente calculadoras de JavaScript en un Enterprise Manager en ejecución.

- [Acceso a extensiones de JavaScript](#)
- [Escritura de calculadoras de JavaScript](#)
- [Ejecución de calculadoras de JavaScript en MOM](#)
- [Tipos de datos de la métrica](#)

## **Acceso a extensiones de JavaScript**

### **Siga estos pasos:**

1. En la IU de DX Application Performance Management, haga clic en **Configuración**.
2. Haga clic en el mosaico **Extensiones de JavaScript** **Ajustes generales**.
3. Para crear una nueva extensión, haga clic en **Crear nueva extensión**.
4. Seleccione un archivo de extensión y cárguelo.

#### **NOTE**

También se puede editar, descargar y eliminar la extensión existente.

5. Para activar o desactivar el estado, deshabilite el conmutador en la columna **Estado**.

Se crea la extensión de JavaScript.

## **Escritura de calculadoras de JavaScript**

Los nombres de archivo de la calculadora de JavaScript deben terminar con una extensión `.js`.

Las calculadoras de JavaScript especifican las métricas de entrada y producen una o más métricas de salida.

#### **NOTE**

Cada error dentro de una calculadora de JavaScript se registra en el registro de EM. Los errores que se producen con frecuencia pueden inundar el registro de EM. Pruebe sus calculadoras antes de implementarlas en la producción.

## **Función execute()**

Cada calculadora debe tener una función `execute()` que tome dos argumentos. Además, las funciones de ayuda están disponibles para facilitar la generación de métricas y su devolución a Enterprise Manager. El motor de generación de scripts llama cada 15 segundos a la función `execute()`.

Tenga en cuenta lo siguiente para la función `execute()`:

- La invocación de la función `execute()` se produce cada 15 segundos, incluso cuando no haya métricas que coincidan con las expresiones regulares devueltas (consulte más adelante). Esto permite que la calculadora, por ejemplo, informe sobre una métrica para indicar que algunas métricas no informan sobre cómo crear una alerta.
- La invocación cada 15 segundos se realiza en el mejor esfuerzo posible y no se garantiza que sea exactamente de 15 segundos.
- La invocación en el segundo 0, 15, 30 y 45 es el mejor esfuerzo posible, pero no está garantizado.
- Las métricas tienen una marca de tiempo proporcionada por EM cuando se recibe en el retorno de `execute()`.
- Para la estabilidad de EM, la duración de una invocación de `execute()` no debe exceder los 7,5 segundos. Más de 15 segundos probablemente provocará inestabilidad de EM y huecos de métrica al retrasarse la recopilación de métricas de EM. Si se exceden los 15 segundos, es posible que se bloquee EM.
- La métrica de compatibilidad que alertaría sobre las calculadoras que causan inestabilidad es Calculator Harvest Time de Enterprise Manager, que solo debe exceder muy de vez en cuando los 7,5 segundos y casi no debe exceder los 15 segundos.

La sintaxis de la función `execute()` es la siguiente:

```
function execute(metricData, javascriptResultSetHelper)
```

Donde

- `metricData`: es una matriz de datos de métrica que se facilitan a la función cuando se llama cada 15 segundos antes de los intervalos de `execute()`.

**NOTE**

Se debe evitar que se pasen muchas métricas a una calculadora, ya que el tiempo que se necesita para generar la matriz de MetricData y, especialmente, la memoria utilizada pueden prohibir la finalización oportuna del ciclo de recolección de 15 segundos de Enterprise Manager y causar inestabilidad. El límite depende de la configuración de EM. Utilice Calculator Harvest Time como indicador de inestabilidad, tal y como se ha mencionado anteriormente.

```
{ 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**

- Omita las entradas de datos donde data.dataIsAbsent==true.
  - Cuando ninguna métrica coincide con las expresiones regulares del agente y de la métrica, data.length es 0.
  - El orden de las métricas dentro de la matriz metricData no está definido y puede variar entre invocaciones.
- javascriptResultSetHelper: es un objeto que recopila los datos de la nueva métrica generados por el script y los envía a EM. Este objeto proporciona la función addMetric en dos versiones sobrecargadas:

```
JavaScriptResultSetHelper:
{
 addMetric(fullMetricName, value, type, frequency)

 addMetric(fullMetricName, count, value, min, max, type, frequency)
}
```



- `kDefaultFrequency`: se utiliza como entrada en el argumento `frequency` de la función de ayuda `addMetric()`.
- `kIntegerConstant`: asigna al tipo de métrica de constante de número entero
- `kIntegerFluctuatingCounter`: asigna al tipo de métrica de contador fluctuante de número entero
- `kIntegerConstant`: asigna al tipo de métrica de constante larga
- `kIntegerFluctuatingCounter`: asigna al tipo de métrica de contador fluctuante largo
- `kLongTimestamp`: asigna al tipo de métrica de marca de tiempo larga
- `kLongTimestampConstant`: asigna al tipo de métrica de constante de marca de tiempo larga
- `kIntegerPercentage`: asigna al tipo de métrica de porcentaje de número entero
- `kIntegerDuration`: asigna al tipo de métrica de duración de número entero
- `kLongDuration`: asigna al tipo de métrica de duración larga \
- `kLongIntervalCounter`: asigna al tipo de métrica de contador de intervalos largos
- `kStringIndividualEvents`: asigna al tipo de métrica de la cadena
- `addMetric(metricName, count, value, min, max, metricType, frequency)`: admite la configuración del recuento/valor/ mín./máx. de un valor de métrica necesario para los tipos de métrica de recuento de tasas e intervalos, donde el "valor" de la métrica se basa en su "recuento"
- `getCustomMetricAgentMetric (agentMetric)` : permite crear un nombre de métrica completamente válido mediante la métrica del agente proporcionada rellenoando el resto en función del nombre del Agente de métrica personalizada de SuperDomain.

#### NOTE

- Una métrica solo se puede enviar una vez. Si se envía una métrica duplicada (por nombre solamente), se producirá un error de métrica no válida o duplicada que se registra en el registro de EM.
- Si la calculadora debe agregar valores de métricas, se deben agregar internamente para enviar una única métrica, que sea el valor agregado.
- Si un valor no válido se pasa para cualquier valor, se produce un error (con el mensaje de error de JavaScript registrado en el registro de EM).
- La versión anterior, corta y sobrecargada se establece implícitamente en `count=1`.
- La última versión, larga y sobrecargada, es necesaria cuando se desea enviar una métrica con un recuento mayor de 1, lo que suele ser necesario para los tipos de métricas `PerIntervalCounter` e `IntRate` (ya que tienen `value==count`, es decir, el recuento se toma como el valor).
- La función `execute()` debe devolver el objeto `javascriptResultSetHelper` recibido para enviar las métricas agregadas por las llamadas de `addMetric` en el ciclo de recolección de las instancias de EM. Las llamadas de `addMetric` agregan métricas a los campos ocultos del objeto `javascriptResultSetHelper`.
- Las métricas ocultas en el objeto `javascriptResultSetHelper` solo se envían a EM cuando se completa la función `execute()`.

#### **Especificación de las métricas de entrada**

El script de la calculadora puede especificar las métricas de entrada que reciba de una de dos posibles maneras:

- La forma de especificar las métricas de entrada es con un par de métodos que llama EM en la implementación de la calculadora:
  - La función `getAgentRegex()` que debe devolver una cadena que contiene una expresión regular para que coincida con los agentes y
  - la función `getMetricRegex()` que debe devolver una cadena que contenga una expresión regular para que coincida con las métricas.

```
function getAgentRegex()
{ return "SuperDomain\\|beta.*\\|Infrastructure Agent\\|EPAgent" }
```

```
function getMetricRegex()
```

```
{ return "BetaSummary:Rejections" }
```

### NOTE

- Las expresiones regulares en JavaScript tienen dos formatos: formato de cadena, delimitado por comillas:
  - “(.\*)(.)(.)(.\*)”
  - Dentro de las cadenas de expresión regular, los caracteres especiales de la expresión regular, que se deben tomar literalmente, deben tener caracteres de doble escape \ que se deben adherir a la barra diagonal inversa de Javascript dentro de las cadenas. Por lo tanto, en JavaScript, \ dentro de una cadena significa que la primera barra invertida es el carácter de escape de la segunda dejando esa segunda barra invertida en su lugar.
  - Fuera de las cadenas de expresión regular, no hay necesidad de escapar los caracteres especiales de expresión regular.
- La expresión regular del agente puede especificar los cuatro segmentos de una ruta de origen:
  - Dominio | host | proceso | agente
  - Los dominios incluyen todos los dominios y no solo SuperDomain.
- No hay requisitos de formato para las expresiones regulares usadas. Por ejemplo, una expresión regular del agente de:
  - “.”
- incluirá los mismos agentes que:
  - “.\*\.\*\.\*\.\*”
  - “(.\*)(.)(.)(.\*)”
- Si le importa la eficacia de la expresión regular, evite la vuelta atrás en la expresión regular usando coincidencias perezosas (como en .\*?) y grupos de caracteres (como [^\\]):
  - “SuperDomain\\|beta.\*?\\|Infrastructure Agent\\|EPAgent”
  - “SuperDomain\\|beta[^\\]\*\\|Infrastructure Agent\\|EPAgent”
- De forma alternativa, se puede utilizar la función del método `getMetricSpecifier()` , que debe devolver un especificador de métrica completo, es decir, la expresión regular del agente y la expresión regular de la métrica combinadas.

### NOTE

Las expresiones regulares creadas como cadenas en la función `getAgentRegex()`, en la función `getMetricRegex()` y en la función `getMetricSpecifier()` deben utilizar los caracteres de escape de manera diferente que otras expresiones regulares que se utilicen en Introscope como, por ejemplo, en las agrupaciones de métricas o en la vista de búsqueda. Cualquier carácter de escape de Java que se devuelva desde estas funciones de JavaScript también se debe escapar en JavaScript. Por ejemplo, “\” se debe escapar como “\\” en JavaScript.

## Registro de variables globales

Todas las funciones de la calculadora de JavaScript tienen acceso a un registro de variables globales, que es del tipo `IModuleFeedbackChannel` . Por ejemplo:

```
function execute(metricData,javascriptResultSetHelper) {
log.info("message");
log.error("message");
log.debug("message");
}
```

### NOTE

Si desea usar las funciones avanzadas de JavaScript o está preocupado por el cumplimiento de ECMA, el motor de script integra la versión 1.6\_R1 de la biblioteca de Mozilla Rhino JavaScript.

## Creación de datos de métrica de salida

La creación de datos de métrica de salida requiere lo siguiente:

- **Nombre de la métrica:** compuesto por el agente y la ruta completa al nodo adecuado en el árbol de métrica.
  - Es posible crear un nombre de agente que se base en los datos entrantes. Los nuevos datos calculados aparecen junto con los datos de métrica sobre los que informa el agente.
  - o
  - Se puede especificar un nuevo nombre de métrica de la calculadora para que exponga los datos de métrica calculados en su propio nodo en el árbol de métrica.
- **Valor de datos:** calculado por el script.
- **Tipo de datos de resultado :** especificado por un valor constante de la clase `com.wily.introscope.spec.metric.MetricTypes`.
- Frecuencia de la generación de informes: la frecuencia con la que se informa a Enterprise Manager sobre los nuevos datos de la métrica, que se pueden obtener de los datos entrantes o se pueden especificar explícitamente. Se puede cambiar la frecuencia a un múltiplo de la frecuencia predeterminada de Enterprise Manager (15 segundos).

A continuación, se muestra un valor típico calculado a partir de un script:

```
javascriptResultSetHelper.addMetric(metricName,
 heapUsedValue, Packages.com.wily.introscope.spec.metric.MetricTypes.kIntegerFluctuatingCounter, frequency)
```

### NOTE

Especifique las expresiones regulares con cuidado, ya que pueden coincidir potencialmente con cualquier métrica que se produzca. Por ejemplo, una expresión regular de "EJB.\*Time.\*" podría insertar un nuevo valor en EJB. La expresión regular inserta un nuevo valor en "EJB" cuando se tiene una expresión regular en "EJB.\*Time.\*". Puede cambiar la expresión regular para hacerlo o eliminar los datos de métricas de sus propias métricas.

## Adición de una calculadora de JavaScript

Para instalar una nueva calculadora de JavaScript, cargue el archivo de texto de JavaScript en EM mediante la página Extensiones de JavaScript que se menciona en la sección *Acceso a extensiones de JavaScript*

## Limitación del tiempo de ejecución del script

El procesamiento de la calculadora de los datos de métricas entrantes puede tardar tiempo y afectar al rendimiento de Enterprise Manager donde se ejecuta la extensión de Javascript. Para proteger contra la sobrecarga de Enterprise Manager, especifique el tiempo de espera del script en el origen de la extensión. Por ejemplo, al utilizar expresiones regulares demasiado genéricas para las métricas de entrada.

Cuando una función `getTimeout()` está presente en la fuente del script, el valor que devuelve se utiliza como el tiempo de espera del script. Si la función `timeout` no está en el script, se utiliza el tiempo de espera de la extensión de JavaScript predeterminado de Enterprise Manager.

Función `getTimeout()`

Utilice la función `getTimeout()` para especificar el tiempo de espera de la ejecución del script en milisegundos.

### Ejemplo

Para utilizar el tiempo de espera de la ejecución del script como 50 ms:

```
function getTimeout() {
 return 50;
}
```

## Ejecución de calculadoras de JavaScript en MOM

Se puede ejecutar una calculadora de JavaScript en MOM para generar métricas para el agente de métrica personalizada de MOM. La calculadora no puede generar métricas para los agentes que están conectados a un recopilador, pero puede consultar las métricas de entrada de los agentes en los recopiladores.

### NOTE

Más información: [Acerca de las calculadoras](#)

Si se agrega, modifica o elimina una calculadora en un entorno agrupado en clúster, MOM propaga automáticamente el cambio a todos los recopiladores. Esta propagación no ocurre cuando están desactivadas las actualizaciones automáticas para los recopiladores.

## La función runOnMOM

Una calculadora de JavaScript que no debe ejecutarse en MOM debe implementar una función `runOnMOM` que devuelva el valor `false`, como en el ejemplo siguiente:

```
// return false if the script should not run on the MOM
// default is true.
function runOnMOM()
{
 return false;
}
```

Si la función `runOnMOM` devuelve un valor `true` o no se implementa, la calculadora de JavaScript también se ejecuta en MOM.

Las calculadoras que devuelven `false` para esta función se propagarán automáticamente de forma predeterminada para la implementación en todos los recopiladores.

Para APM 10.8, esta opción predeterminada se puede anular utilizando

```
introscope.enterprisemanager.javascript.hotdeploy.collectors.enable= false.
```

Esto permite la implementación de conjuntos de calculadoras diferentes y limitados en los recopiladores cuando se utilizan con una forma coordinada a la configuración de agentes a recopiladores que permiten conexiones dentro de `loadbalancing.xml` para conseguir el efecto deseado de la limitación de las ejecuciones de la calculadora según la ubicación de la métrica.

Para DX APM SaaS, este control no es posible ya que el equilibrio de carga se controla de forma diferente y se agrupa en clústeres internamente.

## Reducción del número de errores de creación de métrica registrados

Cuando una calculadora se ejecuta en MOM y crea una métrica para un agente existente en los recopiladores, se debe registrar el evento en el nivel WARN una vez.

Ejemplo

```
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-dtl|EPAgentProcess1|EPAgent15|GC Heap:Heap Used (%) 5/15/07 02:32:20 PM PDT
[WARN] [Manager.MetricCalculatorBean]
```

Los siguientes eventos se registran solamente en el nivel DEBUG.

## **Desactivación de la actualización automática de los recopiladores.**

Los entornos agrupados en clúster están definidos, automáticamente, para que propaguen una calculadora de JavaScript agregada, modificada o eliminada a todos los recopiladores. Si no desea que las calculadoras se propaguen, póngase en contacto con el soporte de Broadcom para desactivar esta función.

## **Ejemplo de creación de una calculadora de muestra**

En este ejemplo se crea una calculadora simple que recibe una métrica que es un recuento acumulado de rechazos (desde que se inicia el agente) y produce el valor delta por intervalo de 15 segundos.

Las primeras cuatro funciones de contrato deben tener el siguiente aspecto:

```
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; }
```

Se debe ejecutar en los recopiladores, ya que debe producir una métrica con una ruta de la métrica como el nombre original de la métrica y el nombre de la métrica con la diferencia añadida ":Rejections Delta". Se implementa la función `execute()` tal y como se muestra a continuación:

```
'use strict';
var savedValues= {} // An object for saved metric values
function execute(metricData, javascriptResultSetHelper)
{
 try
 {
 var metricsReceived= 0;
 for (var i = 0; i < metricData.length; i++)
 {
 var data= metricData[i];
 if (data.timeslicedValue.dataIsAbsent())
 continue;
 metricsReceived++;
 var
 metricSource= data.agentName.processURL,
 metricAttribute= data.agentMetric.attributeURL,
 split= metricAttribute.split(":"),
 metricPath= split[0]=="?"?"":split[0], // Leave empty or prepend a segment pipe
 metricName= split[1] + " Delta",
 metricValue= data.timeslicedValue.value;
 metric= metricSource + metricPath + metricName;
 var savedValue= savedValues[metric]
 if (savedValue) // Iff a saved value is present calculate the delta to submit
 {
 var delta= metricValue - savedValue
 JavascriptResultSetHelper.addMetric(
 metric, delta,
 Packages.com.wily.introscope.spec.metric.MetricTypes.LongFluctuatingCounter,
 Packages.com.wily.introscope.spec.metric.Frequency.getFrequencyInSeconds(15))
 metricsSubmitted++;
 }
 savedValues[metric]= metricValue;
 }
 }
}
```

```

 }
 return javascriptResultSetHelper;
}
catch (e)
{ log.error(e); }
}

```

## NOTE

- La variable savedValues se encuentra en una variable global y se guarda en las invocaciones de ejecución.
- La función dataIsAbsent() se utiliza para cortocircuitar el procesamiento de una entrada metricData cuando el valor es true continuando con la siguiente iteración.
- metricAttribute se divide en dos en el carácter de dos puntos delimitado para obtener valores separados para la ruta de la métrica y el nombre de la métrica. Esto es necesario porque para una ruta de métrica vacía, no debe usarse ningún delimitador de barra vertical al crear la métrica completa (o bien terminaría con "|:", que no es válido).

## Tipos de datos de la métrica

CA APM monitoriza el rendimiento de las aplicaciones midiendo el rendimiento en varios puntos de los componentes y los subsistemas de la aplicación. Las sondas insertadas en el código de bytes del componente de la aplicación envían datos a los agentes, que a su vez notifican estos datos a Introscope Enterprise Manager. Además, otros subsistemas, como JMX y PMI, informan sobre los datos recopilados por los agentes. Enterprise Manager recopila estos datos en métricas y las muestra en Workstation o en WebView. Las métricas también se pueden exportar a una base de datos externa. Para obtener más información, consulte las [Métricas de APM](#).

En las calculadoras de JavaScript, se hace referencia a todos los tipos de datos de métrica anteponiendo lo siguiente al principio del tipo de datos de la métrica: `Packages.com.wily.introscope.spec.metric.MetricTypes`. Por ejemplo, para utilizar `kIntegerFluctuatingCounter`, el nombre completo será `Packages.com.wily.introscope.spec.metric.MetricTypes.kIntegerFluctuatingCounter`.

Los tipos de datos de métricas son compatibles con el Agente de PHP, el Agente de Java, el Agente de .NET y el Agente de Node.js.

### PerIntervalCounter:

**kLongIntervalCounter:** valor numérico de 64 bits que representa un valor de métrica por intervalo. Cuando se agrega durante varios períodos de tiempo, se utiliza la suma como el valor agregado. El recuento es el número de finalizaciones (es decir, respuestas o errores) que se han producido durante el intervalo de tiempo y que será igual al valor.

Métricas de ejemplo: Responses Per Interval, Errors Per Interval

### IntCounter/LongCounter:

**kIntegerFluctuatingCounter/kLongFluctuatingCounter:** valor numérico de 32 o 64 bits que fluctúa, pero que permanece en el último valor conocido hasta que se dispone de nuevos datos. Cuando se agrega durante varios períodos de tiempo, se utiliza el valor más alto como el valor agregado. El recuento es el número total de aumentos y disminuciones del valor que se han producido durante ese intervalo de tiempo.

Métricas de ejemplo: Stall Count, Concurrent Invocation (IntCounter); Bytes In Use (LongCounter)

### IntAverage/LongAverage:

**kIntegerDuration/kLongDuration:** valor numérico de 32 o 64 bits que representa la duración del tiempo. Cuando se agrega durante varios períodos de tiempo, el promedio ponderado se utiliza como el valor agregado. El recuento es el

número de finalizaciones (por ejemplo, respuestas) durante el intervalo de tiempo que se utiliza como el denominador para calcular el valor (por ejemplo, el promedio).

Métrica de ejemplo: Average Response Time (ms)

#### **IntRate:**

**kIntegerRate:** valor numérico de 32 bits que representa un contador por segundo. Para un intervalo de 15 segundos, se truncará el resto (14 o menos). Cuando se agrega durante varios períodos de tiempo, el promedio ponderado se utiliza como el valor agregado.

Métrica de ejemplo: Queries Per Second

#### **TimeStamp:**

**kLongTimestamp:** un valor de marca de tiempo que se puede actualizar. El valor se introduce como el número de milisegundos desde Unix Epoch Time, 1 de enero de 1970 00:00:00 UTC. No se persiste en SmartStor.

#### **StringEvent:**

**kStringIndividualEvents:** un valor de cadena que se puede actualizar. No se persiste en SmartStor.

Métrica de ejemplo: Currently Leaking

#### **IntConstant/LongConstant:**

**kIntegerConstant/kLongConstant:** valor numérico de 32 o 64 bits que se inicializa pero que no cambia.

Métrica de ejemplo: ProcessID

#### **IntPercentage:**

**kIntegerPercentage:** un porcentaje entero (sin decimal). Cuando se agrega durante varios períodos de tiempo, se utiliza el promedio como el valor agregado.

Métrica de ejemplo: Utilization % (process)

#### **LongTimeStampConstant:**

**kLongTimestampConstant:** un valor de marca de tiempo que se inicializa, pero que no cambia. El valor se introduce como el número de milisegundos desde Unix Epoch Time, 1 de enero de 1970 00:00:00 UTC. No se persiste en SmartStor.

Métrica de ejemplo: Launch Time

#### **StringConstant:**

**kStringConstant:** valor de cadena que se inicializa, pero que no cambia. No se persiste en SmartStor.

Métrica de ejemplo: Virtual Machine

Una extensión de JavaScript permite crear una nueva extensión y editar una existente. Esta extensión lee las métricas de entrada y genera métricas de salida según los cálculos especificados en un archivo de texto de JavaScript creado por el usuario. Las nuevas métricas calculadas pueden aparecer en el árbol de Investigator, en el Agente personalizado virtual. Las métricas también pueden aparecer en cualquier nodo del árbol de Investigator, según la métrica de salida que se especifique en el script de la calculadora.

Para obtener más información sobre cómo acceder y configurar las extensiones de JavaScript, consulte [Configuración de extensiones de JavaScript](#).

## Recomendaciones de tamaño para el Monitor de Docker

Para optimizar el rendimiento del entorno de Docker monitorizado, puede utilizar las siguientes recomendaciones de tamaño como referencia. Estas recomendaciones son simplemente un indicador y no podemos garantizar que los ejemplos sean óptimos para su entorno.

### Recomendaciones de tamaño y métricas útiles

- **Se recomienda la siguiente adjudicación mínima de recursos para un contenedor del Monitor de Docker:**
  - **Memoria:** 650 MB
  - **CPU:** 0,3 para 25 contenedores. Consulte la tabla que se encuentra en la parte inferior como guía para asignar los recursos de la CPU.
- **Configuración recomendada para el intervalo de sondeo:** `docker.interval.seconds=90`

Por lo general, la utilización de la CPU de un contenedor del Monitor de Docker no es muy elevada. Sin embargo, si la métrica **Porcentaje de utilización de la CPU (mCore)** muestra una utilización de la CPU por encima del 80 por ciento durante más de una hora, se recomienda aumentar la adjudicación de recursos de la CPU. Se recomienda aumentar la adjudicación por 0,2 cada vez.

La métrica **Limitación de la CPU** es otro indicador que muestra que el Monitor de Docker debe aumentar su adjudicación de recursos de la CPU.

### Adjudicación mínima de recursos

| Número de contenedores | Restricciones de la CPU | Memoria (MB) |
|------------------------|-------------------------|--------------|
| 25                     | 0,3                     | 650          |
| 50                     | 0,5                     | 650          |
| 75                     | 0,7                     | 700          |
| 100                    | 0,9                     | 700          |

## Descarga de herramientas adicionales

**Descargas** permite descargar y configurar herramientas adicionales en el entorno de monitorización. Las siguientes herramientas se pueden descargar desde el mosaico **Configuración, Descargas**:

- **Workstation:** Descargue la herramienta Workstation para realizar tareas administrativas y acceder a las métricas de rendimiento.
- **Cloud Proxy:** Descargue y configure Cloud Proxy para Windows o Linux. Se puede configurar Cloud Proxy para enviar y recibir datos recopilados por el agente directamente en Cloud Gateway.
- **Herramienta de importación de agentes:** Descargue la herramienta de importación de agentes para crear un paquete de APM Command Center para agentes de versiones anteriores de APM.
- [Configuración de Workstation](#)
- [Conexión de Workstation](#)
- [Cloud Proxy](#)
- [Herramienta de importación de agentes](#)

Descargas permite descargar y configurar herramientas adicionales en el entorno de monitorización. Workstation, Cloud Proxy y la herramienta de importación de agentes son las herramientas que están disponibles para su descarga en el mosaico Configuración, Descargas.



Para obtener más información sobre las descargas y las herramientas disponibles para descargar, consulte [Descarga de herramientas adicionales](#).

## Herramienta de importación de agentes

La herramienta de importación de agentes es una utilidad de línea de comandos que permite migrar los Agentes Java de CA APM 10.7 creados como archivos zip a los Agentes de Java de DX APM más recientes. En el proceso de migración, se crea un nuevo paquete de APM Command Center para cada agente con los cambios de configuración que se conservan de la versión anterior. Los cambios que se conservan incluyen cambios en los valores de propiedad y alternancia. El paquete resultante se puede utilizar para implementar el agente como sustituto del agente anterior. La configuración del nuevo paquete ya se ha modificado para conectarse a la instancia DX APM de nueva generación.

### NOTE

Utilice esta herramienta solamente para los paquetes del agente sin instalador de Java 10.7. Esta herramienta es compatible con Windows y Linux.

Este artículo incluye los temas siguientes:

### Requisitos previos

Abra JDK 11.x u Oracle JDK 11.x.

### Proceso de migración

Al ejecutar la utilidad, se identifican los archivos y los parámetros utilizados por el agente seleccionado y se crea un paquete de APM Command Center que incluye los conjuntos que contienen los archivos y la configuración correspondientes. Todas las actualizaciones manuales realizadas en los valores de propiedad o alternancia se aplican en los conjuntos nuevos si los valores son diferentes a los valores predeterminados del archivo de configuración del agente original.

La utilidad crea un nuevo conjunto personalizado si se encuentra algún archivo, alternancia o parámetro de configuración no identificado. A continuación, este conjunto se incluye en el paquete creado.

Después de la migración, la configuración de los agentes se puede gestionar desde APM Command Center.

### NOTE

Para que un agente sea visible en APM Command Center, incluya el conjunto de controlador de agente en la extensión del Agente de Java o en el Agente de la infraestructura. El controlador del agente se deberá implementar en el mismo host.

La utilidad se configura para utilizar una conexión directa con el componente de puerta de enlace en la nube de DX APM. Se puede volver a configurar la utilidad para utilizar el Cloud Proxy local. Para ello, se debe cambiar la propiedad en el archivo de configuración [application.properties](#) o utilizar el [parámetro de la línea de comandos](#).

### Ejecución de la utilidad de la herramienta de importación de agentes

Al ejecutar la utilidad de la herramienta de importación de agentes, solo es necesario definir la ruta del sistema de archivos en el directorio del agente en el parámetro de la línea de comandos. Hay opciones adicionales de la línea de comandos disponibles para modificar el modo de ejecución de la utilidad o para seleccionar la configuración adecuada del agente.

#### Siga estos pasos:

1. Vaya a Team Center DX APM, **Configuración, Descargas**.
2. En la sección **Herramienta de importación de agentes**, haga clic en **Descargar**.  
Se descargará el siguiente archivo: *apmservices.agentimport-<version>.zip*
3. Extraiga el contenido del archivo zip.

Este incluirá lo siguiente:

- a. Carpeta **lib**
  - b. Archivo **application.properties**
  - c. Archivo de script de Windows **import-agent.cmd**
  - d. Archivo de script de Linux **import-agent.sh**
4. Opcional: Actualice las propiedades necesarias en el archivo **application.properties**.

#### IMPORTANT

Como el directorio del agente puede contener varios perfiles de agente, debe especificar explícitamente la ruta correcta. De forma predeterminada, *IntroscopeAgent.profile* se utiliza como el archivo de configuración del agente principal. Sin embargo, si se desea utilizar otro archivo de perfil, por ejemplo, *noredef variant*, se puede utilizar el parámetro `--profile` de la línea de comandos.

#### NOTE

La utilidad utiliza el token de seguridad específico del cliente actual que se genera cuando se ha descargado. Para utilizar otro token, genere un token de API pública en Team Center. Para obtener más información sobre cómo generar un token de seguridad, consulte [Generación de un token de seguridad](#). Después de que se genere el token, reemplace el valor en el archivo **application.properties** o especifíquelo como un parámetro de la línea de comandos.

5. En función del sistema operativo, ejecute el script de inicio de la herramienta de línea de comandos con la ruta del directorio del agente que contiene los Agentes de Java de CA APM 10.7.

Por ejemplo: `import-agent /opt/weblogic/wily`

#### NOTE

En Linux, actualice el permiso de archivo y haga que se pueda ejecutar mediante el comando `chmod +x import-agent.sh`.

La utilidad identifica el entorno del agente como, por ejemplo, el sistema operativo, la versión, el proceso y los cambios de configuración, y crea un paquete correspondiente en la instancia del servidor de configuración de APM Command Center.

#### NOTE

La utilidad crea un paquete mediante los conjuntos de la versión más reciente disponible en APM Command Center.

### Parámetros de la línea de comandos

Cuando se extraen los archivos de la utilidad, se obtienen scripts para los sistemas operativos Linux y Windows:

- **Linux:** `import-agent.sh`
- **Windows:** `import-agent.cmd`

#### NOTE

En Linux, actualice el permiso de archivo y haga que se pueda ejecutar mediante el comando `chmod +x import-agent.sh`.

Cuando se ejecuta el script, el único parámetro obligatorio es la ruta al directorio de agentes de CA APM 10.7. Por ejemplo, `/opt/weblogic/wily`.

### Opciones adicionales de la línea de comandos

- `-a, --agentJar <arg>` : obtiene la ruta del archivo jar del agente relacionada con la raíz. De forma predeterminada, el nombre de archivo es **Agent.jar**.
- `-f, --force <arg>` : ignora los errores y continúa con la ejecución del comando. Esto desactiva la optimización de paquetes.
- `-n, --name <arg>` : nombre que tiene el prefijo para el paquete creado y el conjunto personalizado. De forma predeterminada, el nombre del paquete se encuentra en el formato siguiente: *Imported agent - <platform> <process>*.
- `-p, --profile <arg>` : ruta del archivo de perfil relacionada con la raíz. De forma predeterminada, la ruta del perfil es: *core/config/IntroscopeAgent.profile*.
- `-t, --token <arg>` : valor del token de seguridad de la API pública.
- `-u, --url <arg>` : URL base del proxy o de la puerta de enlace en la nube.

Los valores de URL y token se definen en el archivo de configuración **application.properties**. Sin embargo, si es necesario, se pueden sobrescribir los valores mediante los parámetros de la línea de comandos. Para obtener más información sobre cómo generar un token de seguridad, consulte [Generación de un token de seguridad](#).

#### NOTE

Si está utilizando IBM JVM, sobrescriba el valor del archivo jar del agente predeterminado por el archivo *AgentNoRedefNoRetrans.jar*, ya que se utiliza para conectarse a JVM mediante el parámetro `--agentJar`.

### Registro

La utilidad proporciona un registro detallado para realizar un seguimiento de cómo se identifican los conjuntos individuales y la configuración de las propiedades. También registra cualquier solicitud de REST en APM Command Center.

Para activar el registro de depuración, active los comentarios o quite la marca de comentario de la propiedad siguiente en el archivo de configuración **application.properties**: `logging.level.com=DEBUG`.

La herramienta de importación de agentes es una utilidad de línea de comandos que permite migrar los Agentes de Java de CA APM 10.7 creados como archivos ZIP a los Agentes de Java de DX APM más recientes. En el proceso de migración, se crea un nuevo paquete de APM Command Center para cada agente con los cambios de configuración que se conservan de la versión anterior.

Para obtener más información, consulte [Herramienta de importación de agentes](#).

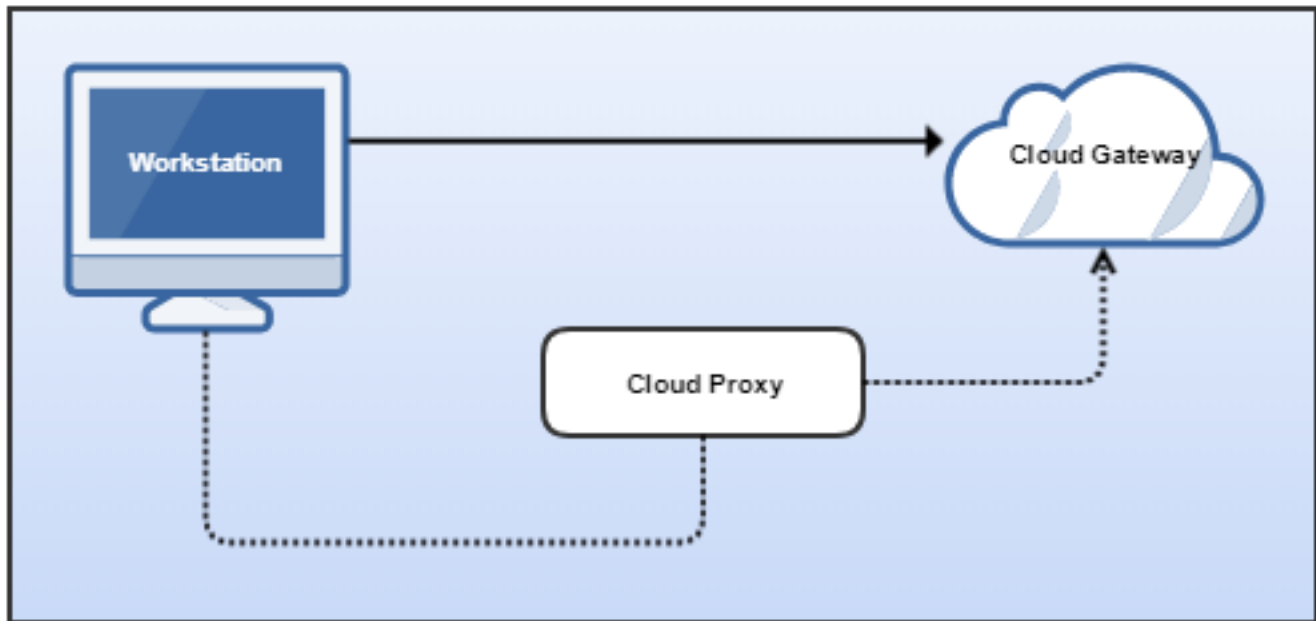
- Proceso de migración
- Ejecución de la utilidad de la herramienta de importación de agentes
- Parámetros de la línea de comandos
- Registro

### Conexión con Workstation

Workstation está disponible para la descarga desde la sección **Descargas** en el panel izquierdo. De forma predeterminada, Workstation está configurada para comunicarse directamente con la puerta de enlace de la nube. Las organizaciones que requieren comunicación de canal única entre el centro de datos y la puerta de enlace de la nube pueden conectar Workstation con Cloud Proxy.

El diagrama siguiente muestra estas dos opciones:

Figure 3: ConnectWorkstation



### Conexión de Workstation con la puerta de enlace de la nube

#### Requisitos previos:

Para ejecutar Workstation en Linux, asegúrese de que Oracle u OpenJDK 11.x está instalado en el equipo.

#### NOTE

El protocolo **Isengard** no se admite para Cloud Gateway.

#### Siga estos pasos:

1. En **Configuración, Descargas, Descargar** Workstation. Descomprima el archivo.
2. Inicie Workstation desde la línea de comandos:
  - (Windows) `start.bat`
  - (Linux) `start.sh`
 Aparecerá el cuadro de diálogo de conexión de CA Introscope Workstation.
3. Introduzca la **contraseña**.
4. Seleccione **Conectar**.  
Aparecerá el cuadro de mandos de Workstation.

Se ha conectado Workstation con la puerta de enlace de la nube.

### Conexión de Workstation con Cloud Proxy

#### Requisitos previos:

- Para ejecutar Workstation en Linux, asegúrese de que Oracle 11.x u OpenJDK 11.x está instalado en el equipo.
- Para ejecutar Cloud Proxy, asegúrese de que dispone de una versión de Java compatible instalada en el equipo: OpenJDK 11.x u Oracle JDK 11.x.

**Siga estos pasos:**

1. Configure Cloud Proxy y asegúrese de que se está ejecutando.  
Para obtener más información sobre la configuración de Cloud Proxy, consulte [Configuración de Cloud Proxy](#).
2. En **Configuración**, **Descargas**, **Descargar** Workstation. Descomprima el archivo.
3. Inicie Workstation desde la línea de comandos:
  - (Windows) `start.bat`
  - (Linux) `start.sh`
 Aparecerá el cuadro de diálogo de conexión de Introscope Workstation DX APM.
4. Introduzca la URL del proxy como el valor de **URL de la nube**. Defina la dirección URL del proxy con el formato siguiente:  
Por ejemplo, `ws://<<cloudproxyhost>>:8081`

**TIP**

Se recomienda utilizar uno de los siguientes protocolos (con la opción de configuración y los valores predeterminados correspondientes) para Cloud Proxy para conectarse a Workstation:

- **apm.server.httpPort**
  - WS 8081
- **apm.server.secureHttpPort**
  - WSS 8444

**NOTE**

- La dirección URL de destino del proxy se preconfigura cuando se ejecuta la función Descarga de Cloud Proxy en la interfaz gráfica de usuario.
- Utilice los protocolos Isengard y HTTP para conectarse a los agentes.

5. Introduzca la **contraseña**.
6. Seleccione **Conectar**.  
Aparecerá el cuadro de mandos de Workstation.

Se ha conectado Workstation con Cloud Proxy.

**Reinicio de Workstation**

Cuando haya terminado de utilizar Workstation, puede cerrar sesión o cerrar Workstation. Al desconectarse de Workstation finaliza la sesión actual, pero no se cierra. Puede iniciar sesión otra vez desde el cuadro de diálogo de conexión que aparece de forma predeterminada al cerrar sesión. Al salir de Workstation se cierra sesión en Workstation y se detiene el proceso de Workstation. Workstation guarda el número de ventanas abiertas de Investigator y de la consola, de manera que aparece la misma configuración cuando se vuelve a iniciar sesión.

**Siga estos pasos:**

1. Abra el directorio en el que se ha extraído la estación de trabajo.
2. Inicie Workstation desde la línea de comandos:
  - (Windows) `start.bat`
  - (Linux) `start.sh`
 Aparecerá el cuadro de diálogo de conexión de Introscope Workstation DX APM.
3. Introduzca los campos obligatorios.
4. Seleccione **Conectar**.

Se ha reiniciado Workstation.

**NOTE****Más información:**

- [Descripción general de Workstation](#)

Workstation está disponible para la descarga desde la sección **Descargas** en el panel izquierdo. De forma predeterminada, Workstation está configurada para comunicarse directamente con la puerta de enlace de la nube. Las organizaciones que requieren comunicación de canal única entre el centro de datos y la puerta de enlace de la nube pueden conectar Workstation con Cloud Proxy.

Para obtener más información sobre Workstation, consulte [Conexión de Workstation](#).

## Cloud Proxy

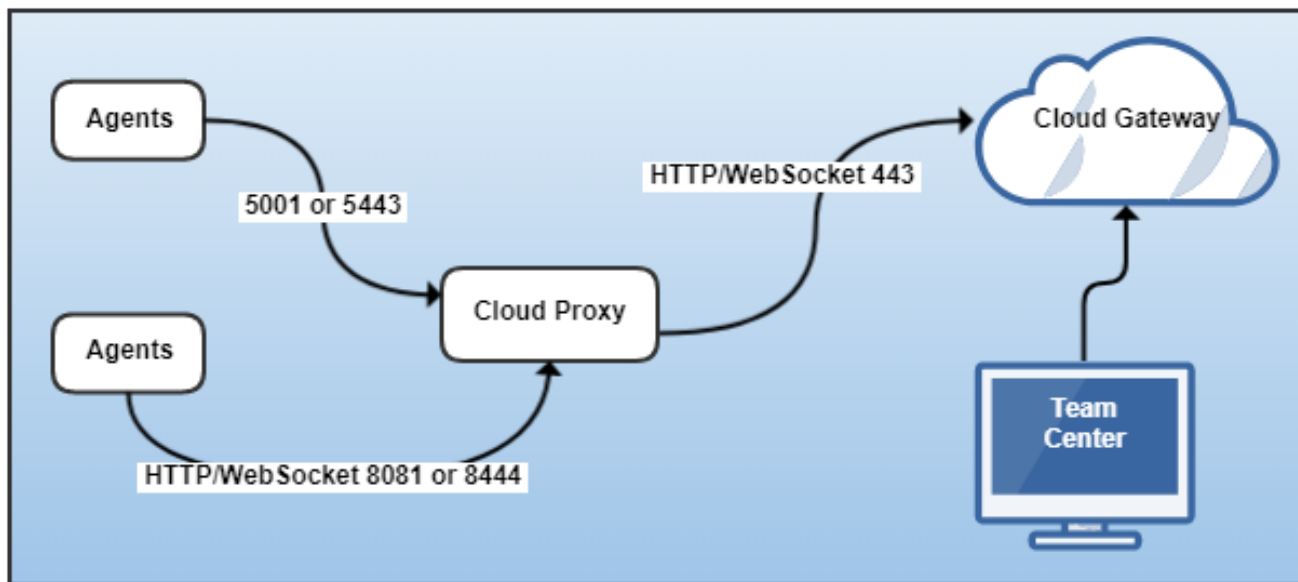
Como administrador, descargue y configure Cloud Proxy para migrar a todos los agentes que están conectados actualmente a CA APM 9.6 y versiones posteriores a DX APM. Su organización puede requerir la comunicación saliente a través de un proxy HTTP o el uso de la comunicación a partir de un nodo específico para configurar el cortafuegos. Se puede utilizar Cloud Proxy para realizar estas configuraciones. Se puede configurar el Cloud Proxy de manera independiente o ejecutarlo dentro de un contenedor de Docker.

### NOTE

- También se puede utilizar Cloud Proxy para conectarse a Workstation. Para obtener más información, consulte "Conexión con Workstation" en la documentación de APM.
- No utilice el método estándar de creación de alertas de APM para las métricas ingeridas directamente en NASS (esto incluye las métricas de compatibilidad de APM Cloud Proxy y cualquier métrica que no sea de APM). En su lugar, utilice la [Configuración de alertas basadas en métricas](#) de DX OI.

Este diagrama muestra los puertos disponibles para Cloud Proxy:

**Figure 4: Cloud Proxy para puerta de enlace**



Este artículo contiene estos temas:

- [Configuración de Cloud Proxy](#)

- Configuración del servicio de Linux
- Configuración del servicio de Windows
- Configuración de alta disponibilidad (HA)
- Conexión de nuevos agentes con Cloud Proxy
- Migración de agentes individuales a DX APM mediante Cloud Proxy
- Registro de Cloud Proxy
- Optimización del rendimiento de la red y de la CPU
- Solución de problemas
- Métricas de estado de conexión de Cloud Proxy
- Métricas de compatibilidad de Cloud Proxy

### **Configuración de Cloud Proxy**

Solamente se necesita realizar una configuración inicial para Cloud Proxy. Si se está migrando a DX APM SaaS desde una versión local de DX APM, la siguiente configuración ejecutará la migración de todos los agentes conectados actualmente.

#### **Requisitos previos:**

- Asegúrese de que dispone de una versión de Java compatible instalada en el equipo: OpenJDK 11.x u Oracle JDK 11.x.
- Asegúrese de que tiene una versión del SO admitida instalada en el equipo: RHEL 7.6 y versiones posteriores, CentOS 7.9 y versiones posteriores, o Windows Server 2016 y versiones posteriores.
- Para 4000 agentes por Cloud Proxy, el tamaño recomendado es de 4 GB de memoria dinámica. Por lo tanto, si desea tener 10000 agentes, se recomienda tener tres instancias de Cloud Proxy.
- Adjudique 6 GBi de memoria del SO para aproximadamente 4000 agentes.

#### **NOTE**

Se recomiendan 6 GBi de tamaño de forma predeterminada cuando la máquina virtual Java utiliza 4 GBi de memoria dinámica.

- Asegúrese de que haya suficiente espacio en disco para almacenar los registros.
- En el sistema operativo host, establezca el valor del número máximo de descriptores de archivo abiertos para un **proceso** en 16384 o superior.
- Para conectar 10000 agentes por Cloud Proxy, la recomendación de tamaño predeterminada es de 8 GBi cuando la máquina virtual Java utiliza 6 GBi de la memoria dinámica.  
En el sistema operativo del host, establezca el número máximo de descriptores de archivo abiertos para un proceso en 61440 o superior.
- Para conectar 15000 agentes por Cloud Proxy, la recomendación de tamaño predeterminada es de 12 GBi cuando la máquina virtual Java utiliza 8 GBi de la memoria dinámica.  
En el sistema operativo del host, establezca el número máximo de descriptores de archivo abiertos para un proceso en 92160 o superior.

### **Configuración del servicio de Linux**

#### **Siga estos pasos:**

1. En la IU de ATC, haga clic en el icono Configuración



- ( ).
2. Seleccione **Descargas** y descargue Cloud Proxy en el equipo donde se esté ejecutando el MOM de Enterprise Manager. Extraiga el archivo.

La dirección URL de destino del proxy y el token se preconfiguran cuando se ejecuta la función Descarga de Cloud Proxy en la IU de ATC.

#### NOTE

Si es necesario, se puede sobrescribir el token. En **Seguridad** en la IU de ATC, seleccione **Generar un nuevo token**. Asegúrese de que el tipo de token sea **Agente** y que se haya establecido una caducidad adecuada, porque la caducidad para un token del tipo **Agente** no puede modificarse más adelante. A continuación, en la carpeta de configuración, introduzca el ID de token nuevo en la propiedad `apm.server.token` del archivo `application.yml`.

3. (Opcional) En el archivo `application.yml` en la carpeta de configuración, estas propiedades se establecerán en el valor predeterminado. Configure las propiedades para sobrescribir los puertos TCP predeterminados.

- `apm.server.port`  
Valor predeterminado: 5001
- `apm.server.httpPort`  
Valor predeterminado: 8081
- `apm.server.securePort`  
Valor predeterminado: 5443
- `apm.server.secureHttpPort`  
Valor predeterminado: 8444

#### NOTE

- Se puede configurar Cloud Proxy con puertos personalizados, pero Enterprise Manager agrega las métricas de host y puerto de Enterprise Manager. Por lo tanto, no se pueden configurar desde ningún agente.
- Internamente, Cloud Proxy utiliza Isengard y el servidor de Isengard aloja `apm.server.port`. Por lo tanto, `apm.server.port` debe estar abierto para que los protocolos http/https puedan finalizar en Cloud Proxy.
- Para Isengard, el valor de `ulimit` debe establecerse con el doble del número de cada agente conectado. Por ejemplo, para admitir 8000 agentes, el valor recomendado es 16000.
- Para las conexiones HTTP/HTTPS, `ulimit` debe ser cuatro veces el número de agentes.

4. (Opcional) Para utilizar un certificado de seguridad propio, acceda al archivo `application.yml` en la carpeta de configuración. Configure estas propiedades:

- `apm.server.useSelfSignedCert`  
Establezca el valor en `false`.
- `apm.server.keyCertChainFile`  
Introduzca una ruta a un archivo de certificado X.509 utilizando el formato PEM.
- `apm.server.keyFile`  
Introduzca una ruta a un archivo de clave privada PKCS#8 utilizando el formato PEM. DX APM solo es compatible con el formato PKCS#8.

#### NOTE

Cloud Proxy utiliza un certificado autofirmado generado de forma predeterminada. Recomendamos encarecidamente generar un certificado de confianza firmado correctamente. Los certificados autofirmados no deben utilizarse en las implementaciones de producción.

5. (Opcional) Para configurar un proxy HTTP para la comunicación entre Cloud Proxy y la puerta de enlace de la nube:
  - a. Acceda al archivo `application.yml` en la carpeta de configuración. Configure estas propiedades:
    - `apm.server.httpProxy.host`  
Introduzca el hostname para el proxy HTTP.
    - `apm.server.httpProxy.port`  
Introduzca el número de puerto del proxy HTTP.
  - b. Si el proxy HTTP requiere autenticación, proporcione un nombre de usuario y una contraseña válidos:



- `apm.server.httpProxy.username`  
Introduzca un nombre de usuario para acceder al proxy HTTP.
  - `apm.server.httpProxy.password`  
Introduzca una contraseña para acceder al proxy HTTP.
- (Opcional) Para aplicar la comunicación de TLS 1.3 entre Cloud Proxy y DX APM SaaS, configure el valor del parámetro `apm.server.secureClientProtocol` a "TLSv1.3".
  - Cierre todos los compiladores y los MOM de Enterprise Manager.
  - En la línea de comandos, introduzca el comando de `apmservices.cloudproxy.sh start` para iniciar Cloud Proxy.  
El script inicia el proceso `apmservices.cloudproxy` en segundo plano.

**NOTE**

Para el uso de producción, se recomienda encarecidamente conectar el script al sistema de gestión de daemon de la plataforma de destino. Por ejemplo: `init daemon`, `systemd` o `upstart`.

- Compruebe estos registros en el directorio de registros para asegurarse de que Cloud Proxy se haya iniciado correctamente:
  - `logs/cloudproxy.log`
  - `logs/apmservices.cloudproxy.wrapper.log`

Se ha iniciado Cloud Proxy para Linux. Si se han migrado los agentes con Cloud Proxy, ahora se pueden ver en **Configuración, Agentes** de Team Center.

**NOTE**

Estos argumentos están disponibles para su uso con `apmservices.cloudproxy.sh`:

| Argumento        | Función                                                                            |
|------------------|------------------------------------------------------------------------------------|
| <b>start</b>     | Inicia el servicio en segundo plano.                                               |
| <b>run</b>       | Inicia el servicio en primer plano.                                                |
| <b>stop</b>      | Detiene el servicio cuando se está ejecutando.                                     |
| <b>restart</b>   | Detiene el servicio cuando se está ejecutando e inicia el servicio de nuevo.       |
| <b>status</b>    | Imprime el estado en ejecución, detenido del servicio.                             |
| <b>logs</b>      | Sigue el registro en los <code>logs/cloudproxy.log</code>                          |
| <b>version</b>   | Imprime la versión del servicio.                                                   |
| <b>install</b>   | Instalación e inicio de <i>apmservices-cloudproxy</i> como servicio <i>systemd</i> |
| <b>uninstall</b> | Detención y desinstalación del servicio <i>apmservices-cloudproxy systemd</i> .    |

**Configuración del servicio de Windows****Siga estos pasos:**

- En **Configuración, Descargas**, descargue Cloud Proxy en el equipo donde se está ejecutando el MOM de Enterprise Manager. Descomprima el archivo.  
La dirección URL de destino del proxy y el token se preconfiguran cuando se ejecuta la función Descarga de Cloud Proxy en la IU de ATC.

**NOTE**

Si es necesario, se puede sobrescribir el token. En **Seguridad** en la IU de ATC, seleccione **Generar un nuevo token**. Asegúrese de que el tipo de token sea **Agente** y que se haya establecido una caducidad adecuada, porque la caducidad para un token del tipo **Agente** no puede modificarse más

adelante. A continuación, en la carpeta de configuración, introduzca el ID de token nuevo en la propiedad `apm.server.token` del archivo `application.yml`.

2. (Opcional) En el archivo `application.yml` en la carpeta de configuración, estas propiedades se establecerán en el valor predeterminado. Configure las propiedades para anular los puertos TCP predeterminados.

- `apm.server.port`  
Valor predeterminado: 5001
- `apm.server.httpPort`  
Valor predeterminado: 8081
- `apm.server.securePort`  
Valor predeterminado: 5443
- `apm.server.secureHttpPort`  
Valor predeterminado: 8444

#### NOTE

- Se puede configurar Cloud Proxy con puertos personalizados, pero Enterprise Manager agrega las métricas de host y puerto de Enterprise Manager. Por lo tanto, no se pueden configurar desde ningún agente.
- Internamente, Cloud Proxy utiliza Isengard y el servidor de Isengard aloja `apm.server.port`. Por lo tanto, `apm.server.port` debe estar abierto para que los protocolos http/https puedan finalizar en Cloud Proxy.
- Para Isengard, el valor de `ulimit` debe establecerse con el doble del número de cada agente conectado. Por ejemplo, para admitir 8000 agentes, el valor recomendado es 16000.
- Para las conexiones HTTP/HTTPS, `ulimit` debe ser cuatro veces el número de agentes.

3. (Opcional) Para utilizar un certificado de seguridad propio, acceda al archivo `application.yml` en la carpeta de configuración. Configure estas propiedades:

- `apm.server.useSelfSignedCert`  
Establezca el valor en `false`.
- `apm.server.keyCertChainFile`  
Introduzca una ruta a un archivo de certificado X.509 utilizando el formato PEM.
- `apm.server.keyFile`  
Introduzca una ruta a un archivo de clave privada PKCS#8 utilizando el formato PEM. DX APM solo es compatible con el formato PKCS#8.

#### NOTE

Cloud Proxy utiliza un certificado autofirmado generado de forma predeterminada. Recomendamos encarecidamente generar un certificado de confianza firmado correctamente. Los certificados autofirmados no deben utilizarse en las implementaciones de producción.

4. (Opcional) Para configurar un proxy HTTP para la comunicación entre Cloud Proxy y la puerta de enlace de la nube:

- a. Acceda al archivo `application.yml` en la carpeta de configuración. Configure estas propiedades:

- `apm.server.httpProxy.host`  
Introduzca el hostname para el proxy HTTP.
- `apm.server.httpProxy.port`  
Introduzca el número de puerto del proxy HTTP.

- b. Si el proxy HTTP requiere autenticación, proporcione un nombre de usuario y una contraseña válidos:

- `apm.server.httpProxy.username`  
Introduzca un nombre de usuario para acceder al proxy HTTP.
- `apm.server.httpProxy.password`  
Introduzca una contraseña para acceder al proxy HTTP.

5. (Opcional) Para aplicar la comunicación de TLS 1.3 entre Cloud Proxy y DX APM SaaS, configure el valor del parámetro `apm.server.secureClientProtocol` a "TLSv1.3".

6. Cierre todos los recopiladores y los MOM de Enterprise Manager.
7. Cierre todos los recopiladores y los MOM de Enterprise Manager.
8. Instale el servicio de Windows. Ejecute la línea de comandos como administrador y especifique  
`apmservices.cloudproxy.exe install`
9. Inicie Cloud Proxy. Ejecute la línea de comandos como administrador y especifique  
`apmservices.cloudproxy.exe start`
10. Compruebe estos registros en el directorio de registros para asegurarse de que Cloud Proxy se haya iniciado correctamente:
  - `logs/cloudproxy.log`
  - `logs/apmservices.cloudproxy.wrapper.log`

Se ha iniciado Cloud Proxy para Windows. Si se han migrado los agentes con Cloud Proxy, ahora se pueden ver en **Configuración, Agentes** de Team Center.

### Configuración del agente para Cloud Proxy

Si está utilizando el certificado autofirmado, después de generar el certificado autofirmado, realice los siguientes pasos para que el agente se conecte a EM:

Vaya a la carpeta donde se haya descargado el agente. Por ejemplo, `introscopeAgent.profile` para Tomcat se puede encontrar en `<wily\releases\2022.3\core\config>`. De forma similar, para un Agente de la infraestructura, `introscopeAgent.profile` se encuentra en `<apmia\core\config>`.

Copie el archivo **.jks** del sistema de Cloud Proxy al sistema de agentes. En **IntroscopeAgent.profile** del sistema de agentes, proporcione la ruta donde se copie el archivo **.jks**.

Por ejemplo, `agentManager.trustStore.1=C:\\linux_cp_certs\\trust.jks`.

Proporcione la contraseña en la propiedad `agentManager.trustStorePassword.1` de `IntroscopeAgent.profile`.

Por ejemplo, `agentManager.trustStorePassword.1=changeit`.

### Configuración de alta disponibilidad (HA)

Cloud Proxy es un servicio independiente que se ejecuta en un entorno de sistema operativo del host del cliente. El gestor de servicios del SO o una aplicación de terceros son necesarios para garantizar la disponibilidad de la instancia. Cloud Proxy proporciona una sonda de ejecución a través de puntos finales HTTP y HTTPS en `/supportability/health`. Se puede colocar un equilibrador de carga delante de Cloud Proxy de DX APM para lograr una alta disponibilidad. El equilibrador de carga garantiza que las reconexiones del agente se enruten a una instancia disponible. El equilibrador de carga también equilibra el número de conexiones entre las instancias.

Requisitos para los diferentes protocolos de transporte de agentes para una solución de equilibrio de carga de terceros:

1. **Agentes que se conectan mediante el transporte de protocolo HTTP/HTTPS:** el equilibrador de carga debe asegurarse de que las solicitudes HTTP de agentes estén equilibradas con la instancia de Cloud Proxy en función de la cookie de la sesión de HTTP `JSESSIONID`. La instancia de Cloud Proxy consigue un canal de WebSocket a la puerta de enlace de APM asociada con la sesión HTTP del agente.
2. **Agentes que se conectan mediante el transporte del protocolo de WebSocket:** el transporte de WebSocket de los agentes crean una conexión de socket TCP estable. La solución de terceros debe ser compatible con el protocolo de WebSocket.
3. **Agentes que se conectan a través del protocolo Isengard:** el protocolo Isengard se transfiere directamente a través de una conexión de socket TCP. Se puede utilizar un equilibrador de carga de red o una técnica similar para garantizar la conmutación por error a una instancia de Cloud Proxy disponible.

### Conexión de nuevos agentes con Cloud Proxy

Utilice Cloud Proxy para dirigir los datos que los agentes recopilan a Cloud Gateway a través de un único canal.

**Siga estos pasos:**

1. Configure Cloud Proxy y asegúrese de que se está ejecutando.

Para obtener más información sobre la configuración de Cloud Proxy, consulte [Configuración de Cloud Proxy](#).

**NOTE**

- No es necesario configurar Cloud Proxy cada vez que se conecta a un nuevo agente. Solo se debe realizar una configuración inicial de Cloud Proxy.
- Si la conexión del agente a Cloud Proxy se realiza a través de ws/wss, asegúrese de que el agente también proporciona la propiedad **agentManager.credential**.

2. Descargue e implemente el agente.

Para obtener más información sobre la descarga y la implementación de agentes, consulte [Configuración y descarga de un paquete del agente](#).

- a. Utilice el script de inicio del agente para establecer la propiedad del agente `agentManager.url.1` o introduzca `-D` y uno de estos protocolos:

- **WebSocket**

```
-DagentManager.url.1=ws://proxyhost:8081
```

- **WebSocket Secure**

```
-DagentManager.url.1=wss://proxyhost:8444
```

- b. Si el agente tiene una extensión de controlador, especifique la propiedad del controlador `introscope.agent.acc.controller.configurationServer.url` o introduzca `-D` y uno de estos protocolos:

- **HTTP**

```
-Dintroscope.agent.acc.controller.configurationServer.url=http://proxyhost:8081
```

- **HTTPS**

```
-Dintroscope.agent.acc.controller.configurationServer.url=https://proxyhost:8444
```

- c. Inicie el agente.

El agente ahora está conectado a Cloud Proxy.

Es posible ver los agentes conectados haciendo clic en **Configuración, Agentes**.

**Migración de agentes individuales a DX APM utilizando Cloud Proxy****IMPORTANT**

Ejecute este procedimiento si desea migrar agentes que se están ejecutando en APM 10.7 y versiones anteriores. Para DX APM 11 y versiones posteriores, el clúster realiza automáticamente el equilibrio de carga.

Se pueden configurar los detalles del Cloud Proxy en el archivo *loadbalancing.xml* de la instalación local de DX APM y permitir a los agentes individuales migrar a DX APM.

Agregue esta configuración para conectar agentes individuales a DX APM a través de Cloud Proxy.

```
<agent-collector name="SendToProxy">
 <agent-specifier>.*\|.*\|.*</agent-specifier>
 <include>
 <collector host="<cloud-proxy-host>" port="5001"/>
 </include>
</agent-collector>
```

**NOTE**

Para obtener más información, consulte "Configuración de loadbalancing.xml para agentes permitidos y no permitidos por Enterprise Manager" en la documentación de APM.

## Registro de Cloud Proxy

Los registros de Cloud Proxy están disponibles en el directorio de registro en esta ubicación: `logs/cloudproxy.log`. Sin embargo, se pueden activar más configuraciones de registro para consultar información de registro más detallada.

### IMPORTANT

Tras actualizar los detalles de registro, debe reiniciar el proceso de Cloud Proxy.

## Activar nivel de registro de DEBUG o TRACE

### IMPORTANT

El nivel de registro de TRACE proporciona seguimientos de transacciones de volcados de subprocesos de todos los paquetes que pasan por cable, los tokens de información confidencial de seguridad o las credenciales transferidas. Active el registro de nivel TRACE solo cuando lo requiera Soporte de Broadcom o cuando sea necesario realizar una solución de problemas en profundidad. Desactive el registro de nivel TRACE después de completar las pruebas.

### Opción 1: adición de una configuración de JVM

#### Nivel de registro DEBUG

Abra `apmservices.cloudproxy.bat/sh` y, a continuación, agregue la configuración de JVM:

```
-Dlogging.level.com.ca.apm.cloudproxy=DEBUG
```

#### Nivel de registro de TRACE

Por lo general, el nivel de registro DEBUG proporciona suficientes detalles registrando la mayoría de las excepciones de conexión. Sin embargo, cuando se cambia al nivel de registro TRACE, se debe agregar una configuración de la máquina virtual Java adicional: `SocketProxyWS` para diagnosticar los paquetes de cableado.

Abra `apmservices.cloudproxy.bat/sh` y, a continuación, agregue la configuración de JVM:

```
-Dlogging.level.com.ca.apm.cloudproxy=TRACE -Dlogging.level.SocketProxyWS=TRACE
```

A continuación se muestran las opciones de seguimiento de bajo nivel que se pueden utilizar para depurar cualquier problema de entrada:

```
-Dlogging.level.CloudProxyIsengard=TRACE : Realiza un seguimiento de la comunicación entrante para todos los puertos de comunicación internos de DX APM.
```

```
-Dlogging.level.CloudProxyHTTP=TRACE : Realiza un seguimiento de la comunicación entrante con todos los puertos HTTP.
```

Para la depuración específica, utilice estas opciones:

```
-Dlogging.level.HTTPBinaryTunnel=TRACE : realiza un seguimiento de los datos del protocolo binario HTTP en la entrada. Utilice la opción para depurar incidencias con los agentes que se conectan al proxy a través del protocolo binario HTTP.
```

```
-Dlogging.level.HTTPSoapTunnel=TRACE : realiza un seguimiento de los datos del protocolo HTTP Soap en la entrada. Utilice la opción para depurar incidencias con los agentes que se conectan al proxy con el protocolo HTTP Soap (agentes heredados).
```

```
-Dlogging.level.WSTunnel=TRACE : Realiza un seguimiento del protocolo de WebSocket en la entrada. Utilice la opción para la depuración de las incidencias con las conexiones de WS.
```

```
-Dlogging.level.AccHttpProxy=TRACE : Realiza un seguimiento de la comunicación del proxy HTTP de APM Command Center en el lado entrante.
```

### Opción 2: adición de una propiedad oculta

Abra el archivo `./config/application.yml` y, a continuación, agregue la propiedad oculta:

```
logging.level.com.ca.apm.cloudproxy: DEBUG
```

OR

Abra el archivo `./config/application.yml` y, a continuación, agregue la propiedad oculta:

```
logging.level.com.ca.apm.cloudproxy: TRACE
```

### **Actualizar el tamaño y el historial de archivos de registro**

Abra los archivos `./config/application.yml` y, a continuación, agregue estas propiedades:

```
logging.file.max-history: <number-of-days>
```

De forma predeterminada, los archivos de registro rotan cuando alcanzan 10 MB. Los archivos de registro rotados se conservan durante 7 días, a menos que se actualice el valor de esta configuración.

**Ejemplo:** `logging.file.max-history: 14`

En este ejemplo, los archivos de registro se conservan durante 14 días.

```
logging.file.total-size-cap:<size-in-bytes-including-units>
```

Donde `logging.file.total-size-cap` hace referencia a las copias de seguridad del registro que se almacenarán y se representa en términos de tamaño de archivo (MB, GB).

Define el tamaño del archivo de archivado de registro total. Cuando el tamaño del archivo de archivado supera el umbral, se suprimen las copias de seguridad. Las unidades compatibles son byte, kilobyte, megabyte, gigabyte y terabyte.

**Ejemplo:** `logging.file.total-size-cap: 1GB`

En este ejemplo, cuando el tamaño total del archivo de archivado del registro supera 1 GB, se suprimen las copias de seguridad.

#### **IMPORTANT**

De forma predeterminada, el tamaño máximo del archivo de registro se configura en 10 MB. Si desea actualizar este valor, puede utilizar esta propiedad:

```
logging.file.max-size
```

### **Optimización del rendimiento de la red y de la CPU**

Utilice `apm.server.compressionLevel` en el archivo `application.yml` para configurar el nivel de compresión para la comunicación de WebSocket entre Cloud Proxy y Gateway. Es posible configurar cualquier valor entre 0 y 9. Equilibra la cantidad de datos y el uso de la CPU. Por ejemplo:

```
apm.server.compressionLevel: 1
```

A continuación se muestran los valores aplicables:

- 6: Valor predeterminado
- 1: Para alcanzar la velocidad de red constante para Cloud Proxy, pero esto puede aumentar levemente el tráfico de red.
- 9: Para obtener la mejor compresión
- 0: Sin compresión Se recomienda no usar este valor porque aumenta la cantidad de datos y la mejora de la CPU es mínima.

#### **NOTE**

Reinicie Cloud Proxy después de cada cambio de configuración.

## **Cómo distinguir entre las instancias de Cloud Proxy**

Utilice `apm.server.proxyAgentNamePrefix` en el archivo `application.yml` para agregar un prefijo al nombre de host del agente. Se puede utilizar para distinguir entre las instancias de Cloud Proxy. Esta función solo está disponible para la comunicación de ws/wss con Cloud Gateway definida mediante `apm.server.proxyTarget`.

## **Solución de problemas**

### **Síntoma:**

Se produce un error al iniciar Cloud Proxy y aparece el mensaje de error siguiente:

```
No provider succeeded to generate a self-signed certificate.
```

### **Solución:**

La generación de certificados autofirmados no es compatible con entornos de tiempo de ejecución de IBM J9. Los certificados se deben generar por separado y se deben proporcionar a Cloud Proxy a través de las propiedades de configuración descritas anteriormente.

### **Síntoma:**

El agente no puede conectarse a la puerta de enlace de la nube.

### **Solución:**

Utilice el nombre de host de puerta de enlace de la nube especificado al definir las reglas de cortafuegos salientes. Si se utiliza una dirección IP, se puede producir una interrupción inesperada de la conexión si cambia la dirección IP.

### **Síntoma:**

El agente no puede conectarse a DX APM y aparece este mensaje en el archivo de registro de Cloud Proxy `logs/cloudproxy.log`:

```
java.net.SocketException: Too many open files
```

### **Solución:**

En el sistema operativo host, establezca el valor del número máximo de descriptores de archivo abiertos para un **proceso** en 16384 o superior. Consulte la documentación del sistema operativo para obtener información sobre cómo aumentar el límite de recursos del sistema por proceso.

### **Síntoma:**

Cloud Proxy no puede reenviar la conexión con el agente o Workstation y aparece este mensaje de error:

```
sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.
SunCertPathBuilderException: unable to find valid certification path to requested target
```

### **Solución:**

Los servicios de DX APM se implementan con un certificado autofirmado o no válido. Para que Cloud Proxy se conecte a dichos sistemas, configure el valor `apm.server.proxyInsecure` como `true` en el archivo `config/application.yml`, tal como se indica en el ejemplo.

**Ejemplo:** `apm.server.proxyInsecure: true`

### **NOTE**

La confianza en certificados no válidos supone un grave riesgo de seguridad. Use solamente en casos justificados y desactive inmediatamente cuando un certificado válido se implemente en el equilibrador de carga de front-end de la puerta de enlace de DX APM.

Métricas de estado de Cloud Proxy

Se puede monitorizar el estado de Cloud Proxy mediante las métricas de conexión. Para generar estas métricas, establezca un valor de token de agente válido para el parámetro de configuración `apm.server.token`. Esta sección también contiene los detalles relacionados con las métricas de sostenibilidad notificadas desde Cloud Proxy.

Configure un nombre para las métricas de Cloud Proxy mediante el parámetro de configuración `apm.server.id`. Este nombre se muestra en el árbol de métrica. Si no configura el valor de `apm.server.id`, Cloud Proxy detecta el nombre de host del equipo (dirección IP) y lo muestra en el árbol de métrica.

#### NOTE

No utilice las métricas de sostenibilidad de Cloud Proxy para configurar las alertas. En su lugar, se puede utilizar la interfaz de usuario de DX Operational Intelligence SaaS para configurar las alertas. Consulte [Configuración de alertas basada en métricas](#).

En la tabla siguiente se enumeran algunos nombres de métricas importantes para Cloud Proxy.

Nombre de la métrica	Descripción
SuperDomain apmservices CloudProxy PROXY_ID Agents Active Connections Count	El número de agentes conectados a través de Cloud Proxy.
SuperDomain apmservices CloudProxy PROXY_ID Configuration Agent HostName Prefix	El prefijo de HostName (nombre del host) del agente. Solo se muestra cuando el prefijo se configura para un nombre de host del agente.
SuperDomain apmservices CloudProxy PROXY_ID Beans	Puede utilizar las propiedades del bean para un estudio detallado.
SuperDomain apmservices CloudProxy PROXY_ID Resources	Muestra el uso de los recursos por parte de Cloud Proxy y host.
SuperDomain apmservices CloudProxy PROXY_ID Resources System Uptime (ms)	Se puede utilizar esto para investigar el reinicio del agente.

Como administrador, descargue y configure Cloud Proxy para migrar a todos los agentes que están conectados actualmente a CA APM 9.6 y versiones posteriores a DX Application Performance Management. Su organización puede requerir la comunicación saliente a través de un proxy HTTP o el uso de la comunicación a partir de un nodo específico para configurar el cortafuegos. Se puede utilizar Cloud Proxy para realizar estas configuraciones. Se puede configurar el Cloud Proxy de manera independiente o ejecutarlo dentro de un contenedor de Docker.

Para obtener más información sobre cómo configurar, migrar, registrar y solucionar problemas específicos de Cloud Proxy, consulte [Cloud Proxy](#).

## Métricas de compatibilidad de Cloud Proxy

En esta página, se describen las métricas de compatibilidad de Cloud Proxy.

#### NOTE

A continuación se muestran los prefijos para las métricas siguientes: "apmservices | CloudProxy | PROXY\_HOSTNAME" or "apmservices | CloudProxy | PROXY\_ID".

### Agentes

Nombre de la métrica	
Active Connections Count	Recuento de agentes conectados.
Closed per Interval	Recuento de conexiones cerradas por intervalo.
Connections failed per Interval	La conexión no se ha establecido.
Connections reset by peer per Interval	Indica que el servidor remoto o el cliente cerró la conexión inesperadamente.



Nombre de la métrica	
Connections timed out per Interval	La conexión no se estableció en el tiempo indicado.
I/O exceptions per Interval	El recuento de excepciones de E/S por intervalo.
Other exceptions per Interval	El recuento de otros problemas sin especificar.
Writes failed per Interval	El recuento de operaciones de escritura con errores por intervalo.

### **Beans | SupportabilityManagerPoller**

#### Métricas de BlamePoint

Nombre de la métrica	
Tiempo medio de respuesta (ms)	La métrica Tiempo medio de respuesta genera un promedio de los tiempos de respuesta es el período de tiempo que tarda una solicitud en completarse.
Tiempo medio de respuesta (ms)	
Invocaciones simultáneas	Las invocaciones son solicitudes que gestionan la aplicación y sus componentes.
Errores por intervalo	Los errores son el número de excepciones sobre los que informa la máquina.
Responses Per Interval	Refleja el número de invocaciones finalizadas en ese intervalo. Esta métrica es para aplicaciones. La métrica es un simple recuento de las solicitudes que se completan.
Recuento de detenciones	Las solicitudes detenidas son las que no se han completado dentro de un umbral de tiempo. Se considera "detenida" cuando su ejecución excede el umbral de detención.
Total Metrics	Recuento de las métricas notificadas por Cloud Proxy.

### **Resources | Buffer Pool**

Resources|Buffer Pool proporciona métricas de monitorización para los búferes directos asignados fuera de la memoria dinámica.

Nombre de la métrica	
Buffer Count	Recuento de búferes en agrupaciones de búferes de Java (búferes directos, búferes indirectos).
Buffer Total Capacity	La capacidad total de todos los búferes.
Buffer Memory Used	La cantidad total de memoria utilizada por todos los búferes.

### **Resources | CPU**

Nombre de la métrica	
CPU Used (%)	La suma del uso total de la CPU en % para núcleos individuales. Puede ser el uso de la CPU en % para todos los núcleos.
CPU Used (ms)	La suma del uso total de la CPU para núcleos individuales en ms por intervalo.
Kernel CPU (%)	La suma del uso de la CPU en % transcurrido en el kernel (tiempo del sistema).
Kernel CPU (ms)	La suma del uso de la CPU transcurrido en el kernel (tiempo del sistema) en ms por intervalo.
User CPU (%)	La suma del uso de la CPU en % transcurrido en el espacio del usuario.

**Resources | Host | CPU**

Nombre de la métrica	
CPU Used (%)	La suma del uso total de la CPU en % para núcleos individuales. Puede ser
CPU Used (ms)	La suma del uso total de la CPU para núcleos individuales en ms por intervalo.
Idle CPU (%)	La cantidad de tiempo que la CPU no estuvo ocupada.
Idle CPU (ms)	
Kernel CPU (%)	La suma del uso de la CPU en % transcurrido en el kernel (tiempo del sistema).
Kernel CPU (ms)	La suma del uso de la CPU transcurrido en el kernel (tiempo del sistema) en ms.
Wait CPU (%)	La suma del uso de la CPU en % transcurrido en el espacio del usuario.
Wait CPU (ms)	La cantidad de tiempo que la CPU espera para que, por ejemplo, finalicen las operaciones pendientes, lo que no implica que el sistema tenga un estado incorrecto, pero

**Resources | Host | Memory**

Estas métricas se utilizan para monitorizar la memoria del host.

Nombre de la métrica	
Memory Available (byte)	La cantidad de memoria que está disponible para su asignación a un nuevo proceso.
Memory Total (byte)	Memoria física total en el host.
Memory Usage (%)	La memoria utilizada actualmente por los procesos en ejecución.

**Resources | Memory**

Las métricas de Resources|Memory monitorizan la memoria que utiliza el proceso de la máquina virtual Java.

Nombre de la métrica	
GC Count	El número de recopilaciones de elementos no utilizados de JVM ejecutados.
GC Time (ms)	La duración acumulada de las pausas de GC por intervalo. Si el tiempo acumulado es demasiado largo, el rendimiento del sistema se verá afectado significativamente.
Memory Heap Committed	La cantidad de memoria garantizada que estará disponible para su uso por el proceso.
Memory Heap Max	La cantidad máxima de memoria que se puede utilizar para la gestión de la memoria heap. Las métricas APM_HEAP_XMXPCT, APM_HEAP_XMXMIN y APM_HEAP_XMXMAX enlazadas a esta métrica muestran el porcentaje de memoria heap utilizada.
Memory Heap Used	La cantidad de memoria real utilizada por la memoria dinámica.
Memory Resident (byte)	La cantidad de memoria que está ocupada por el proceso.
Memory Virtual (byte)	El tamaño de la memoria virtual del proceso.
Memory No Heap Committed	La memoria máxima garantizada que está disponible para la máquina virtual.
Memory No Heap Max	La memoria máxima de la máquina virtual Java utilizada para almacenar la memoria no heap.
Memory No Heap Used	La memoria actual de la máquina virtual Java utilizada para almacenar la memoria no heap.

**Resources | Storage**

Nombre de la métrica	
Disk Read (byte)	Bytes leídos del disco por intervalo.
Disk Write (byte)	Bytes escritos en el disco por intervalo.

**Resources | System**

Nombre de la métrica	
Harvest Cycle Duration (ms)	La duración del período de recopilación de las métricas de compatibilidad.
Uptime (ms)	El número de milisegundos desde el inicio de la instancia.

## Configuración de Workstation

Como administrador, puede configurar las siguientes opciones de Workstation:

**Ejecución de Workstation en modo detallado**

Ejecute Workstation en modo detallado para crear mensajes de registro detallados que son útiles para la depuración o la resolución de problemas.

**Siga estos pasos:**

1. Abra el archivo `IntroscopeWorkstation.properties` en `<Directorio_principal_Workstation>/config`.
2. En la propiedad `log4j.logger.Workstation`, sustituya `"INFO"` con la siguiente instrucción:  
`VERBOSE#com.wily.util.feedback.Log4JSeverityLevel`
3. Guarde los cambios.

**Redireccionamiento de la salida de Workstation a un archivo**

Establezca el archivo `IntroscopeWorkstation.properties` para redirigir los mensajes de salida de forma detallada a un archivo de registro.

**Siga estos pasos:**

1. Abra el archivo `IntroscopeWorkstation.properties` en el directorio `<Directorio_principal_Workstation>/config`.
2. En la propiedad `log4j.logger.Workstation`, sustituya `"console"` con `"logfile"`. Por ejemplo, este valor de propiedad hace que Workstation registre mensajes detallados en un archivo de registro:  
`log4j.logger.Workstation=VERBOSE#com.wily.util.feedback.Log4JSeverityLevel,logfile`
3. (Opcional) Cambie el nombre y la ubicación del archivo de registro Workstation mediante la propiedad `log4j.appender.logfile.File`.

**Configuración de Workstation para proporcionar valores de inicio de sesión**

Puede modificar el archivo `Introscope_Workstation.lax` para proporcionar valores de inicio de sesión para omitir la pantalla de inicio de sesión.

**Siga estos pasos:**

1. Abra el archivo `<Dir_principal_EM>/Introscope_Workstation.lax`.

2. En la propiedad *lax.command.line.args*, agregue los comandos *-login* para cada comando de inicio de sesión al que se debe proporcionar un valor. Por ejemplo, para la autenticación local, esta propiedad se parece a la siguiente declaración:

```
lax.command.line.args=$CMD_LINE_ARGUMENTS$ -loginimmediate
-loginhost foos -loginport 4503 -loginresponse sanderson,45tst87
```

### **WARNING**

No suprima el valor predeterminado, *\$CMD\_LINE\_ARGUMENTS\$*, de configuración.

Ha iniciado sesión en Workstation y se abrirá una consola. Si se produce un error de inicio de sesión, Workstation no se inicia y se registra un mensaje de error.

### **Activación del tiempo de espera de la sesión en Workstation**

El tiempo de espera de la sesión automática agrega un nivel adicional de seguridad mediante la desconexión de los usuarios inactivos. Modifique el archivo *IntroscopeEnterpriseManager.properties* para activar el tiempo de espera de la sesión automática.

#### **Siga estos pasos:**

1. Abra el archivo *<Dir\_principal\_EM>/config/IntroscopeEnterpriseManager.properties*.
2. Agregue la propiedad *introscope.apmserver.ui.inactivityLogoutTimeout* y establezca el valor (en minutos) en un número entero mayor que 0 para activar el tiempo de espera de la sesión. Por ejemplo, la siguiente instrucción permite un tiempo de espera después de 60 minutos:

```
introscope.apmserver.ui.inactivityLogoutTimeout=60
```

### **NOTE**

El tiempo de espera de la sesión está desactivado de forma predeterminada (valor = 0).

### **Configuración de Workstation para los informes de idiomas asiáticos**

Agregue los siguientes componentes a la instalación de Workstation para generar informes de Introscope en idiomas que utilizan conjuntos de caracteres de varios bytes como el chino y el japonés.

### **Generación de informes de idiomas asiáticos en formatos HTML y RTF**

(Windows) Instale el soporte idiomático complementario en los idiomas del este asiático. Para obtener más información sobre el soporte idiomático, consulte <https://msdn.microsoft.com/en-us/goglobal/default>.

### **Generación de informes de idiomas asiáticos en formatos PDF**

#### **Siga estos pasos:**

1. Descargue el paquete de fuente asiática de Acrobat Reader desde <http://www.adobe.com/support/downloads/product.jsp?platform=windows&product=10>
2. Instale el paquete de fuente asiática de Acrobat Reader.

### **Configuración de Workstation para utilizar el proxy HTTP con autenticación**

Use *transport.http.proxy.username* y *transport.http.proxy.password* para especificar los valores de autenticación donde *transport.http.proxy.password* debe cifrarse. Para cifrar la contraseña, haga lo siguiente.

#### **Siga estos pasos:**

1. Abra el archivo *IntroscopeWorkstation.properties* en *<Directorio\_principal\_Workstation>/config*.
2. En la propiedad *transport.http.proxy.password*, proporcione la contraseña cifrada.  
Se puede ejecutar el comando siguiente para cifrar la contraseña:

```
java -cp plugins\com.wily.core_<VERSION>.jar com.wily.util.properties.PropertiesUtils encrypt <PASSWORD>
```

Donde <VERSION> es la versión instalada de APM en Workstation y <PASSWORD> es la contraseña sin cifrar.

### 3. Guarde los cambios.

Como administrador, puede configurar las siguientes opciones de Workstation:

- Ejecución de Workstation en modo detallado
- Redireccionamiento de la salida de Workstation a un archivo
- Configuración de Workstation para proporcionar valores de inicio de sesión
- Activación del tiempo de espera de la sesión en Workstation
- Configuración de Workstation para los informes de idiomas asiáticos
- Configuración de Workstation para utilizar el proxy HTTP con autenticación

Para obtener más información sobre cada opción de estación de trabajo configurable, consulte [Configuración de Workstation](#).

## Reglas de supresión de seguimiento para ocultar datos confidenciales

Los agentes que se ejecutan en entornos de usuario envían varios tipos de datos, incluidos los datos de seguimiento. Estos datos de seguimiento pueden contener información confidencial o personal que el usuario necesita enmascarar. Se pueden definir reglas de supresión de seguimiento para identificar estos datos y reemplazarlos por texto configurado previamente como, por ejemplo, "SUPPRESSED BY APM". Para cada cliente, se pueden agregar varias reglas para todos los atributos para los que se desea suprimir el valor de seguimiento.

Los agentes que se ejecutan en entornos de usuario envían varios tipos de datos, incluidos los datos de seguimiento. Estos datos de seguimiento pueden contener información confidencial o personal que el usuario necesita enmascarar. Se pueden definir reglas de supresión de seguimiento para identificar estos datos y reemplazarlos por texto configurado previamente como, por ejemplo, "SUPPRESSED BY APM".

Para configurar una regla de supresión de datos de seguimiento, consulte [Reglas de supresión de seguimiento para ocultar datos confidenciales](#).

## Configuración de una regla de supresión de datos de seguimiento

1. Inicie sesión en Team Center y haga clic en el mosaico **Configuración, Seguridad**.
2. Haga clic en **Regla de supresión de seguimiento**.  
Se muestra la ventana **Regla de supresión de seguimiento**. Esta ventana muestra todas las reglas configuradas actualmente.
3. Haga clic en el botón **Regla de supresión de seguimiento**.  
Aparecerá el cuadro de diálogo **Editar supresión de seguimiento**.
4. Especifique lo siguiente:
  - **Nombre:** Introduzca un nombre para la regla de supresión de seguimiento.
  - **Descripción:** Proporcione una descripción relevante de la regla que se va a configurar.
  - **Configurar**
    - **Propiedades suprimidas:** Introduzca el atributo para el que se va a ocultar el valor de seguimiento en APM. Por ejemplo, `FullUrl`. Se puede utilizar el icono del signo más para agregar más atributos.
    - **Expresión regular:** Si desea seleccionar varios agentes con nombres similares, use \* como carácter comodín junto con las mismas iniciales de los agentes. Por ejemplo, para seleccionar todos los agentes con nombres

que empiezan por `tas-uk`, introduzca `tas-uk.*`. Todos los agentes que cumplen los criterios aparecen en la lista **Vista previa**.

- **Agentes individuales:** Seleccione todos los agentes de esta lista para los que se desea suprimir el valor de seguimiento. Todos los agentes seleccionados aparecen en la lista **Vista previa**.

Por ejemplo, las **Propiedades suprimidas** se establecen en `FullUrl` y `tas-uk.*` se configura en **Expresión regular**. En los datos de seguimiento de todos los agentes para los que el nombre del agente empieza con `tas-uk.*`, siempre que aparezca el valor del atributo `FullUrl`, se mostrará el texto "SUPPRESSED BY APM".

5. Para guardar la regla, seleccione **Guardar**.

La nueva regla aparecerá en la lista de reglas de la ventana **Regla de supresión de seguimiento**.

## Configuración de APM Command Center

Con APM Command Center, se pueden realizar las siguientes acciones:




- Mostrar las propiedades del agente almacenadas localmente seleccionando un agente de la lista. Se comprueba cada agente y sus propiedades se actualizan en intervalos de 24 horas (latido). Consulte [Visualización del estado del agente](#).
- Obtener información más detallada sobre un agente en particular mediante la generación de un informe. Los informes de diagnóstico proporcionan los detalles completos sobre un agente. Es posible desplazarse a través de las propiedades del agente detalladas o descargar un archivo ZIP que contenga todos los detalles, incluidos los archivos de registro y de configuración. Es posible usar este archivo ZIP cuando hace referencia a este agente determinado. Consulte [Visualización de los informes del agente](#).
- Muestra todas las aplicaciones creadas en DX Application Performance Management. Se pueden utilizar estas aplicaciones para incorporarlas sin problemas en DX APM y para configurar fácilmente los paquetes de agente para el entorno. Consulte [Configuración de aplicaciones para la incorporación](#).
- Permite crear e implementar paquetes de agente de APM Command Center en servidores de aplicaciones. Los paquetes del agente son un conjunto de archivos binarios del agente y archivos de configuración en formato ZIP o TAR para implementar. Cada paquete consta de varios conjuntos. Un *conjunto* es una pieza compacta de funcionalidad del agente. Consulte [Gestión de paquetes del agente](#).
- Los conjuntos son subconjuntos de funcionalidades monitorizadas por el agente. Los requisitos de compatibilidad, las dependencias y las relaciones entre ellos se definen para cada conjunto y determinan sus combinaciones posibles. Para cambiar la configuración del agente, modifique las propiedades del conjunto en un paquete existente del agente. Consulte [Configuración de conjuntos](#).

### API de RESTful

Para la interacción automatizada con DX APM Command Center, se puede utilizar la API de RESTful. Consulte [API de APM Command Center](#) para obtener información.


## Visualización del estado del agente

La página Agentes muestra todos los agentes del entorno. Con el botón Descargar, se puede descargar la lista de agentes en formato CSV. El icono correspondiente al nombre del agente proporciona el estado actual del agente.

-  Activo: El agente responde dentro del intervalo de latido de 24 horas del Agente del controlador.
-  Activo: La configuración del agente se ha modificado recientemente y el agente debe reiniciarse para que los cambios surtan efecto.
- Inactivo 

:

Los agentes de la versión 10.2 y versiones posteriores se comunican con el controlador del agente cada 60 segundos. Si un agente deja de informar, se marca como Inactivo.

-  Ausente: El agente no ha respondido durante más de 24 horas. Si este no es el comportamiento esperado, verifique que el agente se esté ejecutando.

#### NOTE

- Un agente inactivo se elimina de la lista transcurridos siete días.
- Los datos no están en directo. La aplicación muestra los datos que eran válidos en el momento del último contacto regular con el agente. Los datos pueden haberse producido hasta 24 horas antes para las versiones anteriores de los agentes.
- Es posible buscar un agente específico usando la barra de búsqueda. Para obtener más información, consulte [Búsqueda de un agente](#).

### Información del agente

La selección de un agente en la lista proporciona la siguiente información sobre el agente:

- Información del agente
- Entorno
- Configuration
- Informes de diagnóstico

### Entorno

La información de entorno incluye lo siguiente:

- JVM
- Versión de la máquina virtual Java
- Servidor de aplicaciones
- Versión del servidor de aplicaciones
- OS Type
- OS Version

### Configuration

La información de configuración incluye lo siguiente:

- Nombre
- Fecha de la última modificación
- Versión del paquete

También se puede editar la configuración, editar un paquete o mostrar la configuración del paquete, si está disponible.

Para editar la configuración de un agente, seleccione el agente y, a continuación, seleccione el botón **Editar** de la tarjeta **Configuración**. (ADD A LINK TO THE SECTION)

### Informes de diagnóstico

Es posible generar el informe de diagnóstico para un agente seleccionando el botón **Generar** en la tarjeta Informes de diagnóstico. Una vez que el informe se genera, se puede ver o descargar de la página Informes.

## Búsqueda de agentes

Para buscar agentes, use la barra de búsqueda que aparece en la parte superior de la página de ACC. Es posible buscar por propiedad del agente como nombre, estado, sistema operativo u otras propiedades. También es posible realizar una búsqueda global en la página principal.

Para buscar los agentes utilizando el lenguaje de consulta de ACC, consulte [Búsqueda utilizando el lenguaje de consulta de ACC \(AQL\)](#).

A continuación se muestran ejemplos de búsquedas de agentes:

- `appServerName:Tomcat`
- Se busca una frase utilizando comillas dobles y caracteres comodín.  
`*"Windows Server 2016"*`
- Se usan los operadores AND (opción predeterminada), OR y NOT.  
`logLevel:info OR logLevel:debug`
- Se buscan agentes de Tomcat, pero solamente los que no tengan "linux" en el nombre del servidor:  
`processName:Tomcat NOT serverName:linux`
- Se buscan agentes cuyos valores de campo están entre el límite especificado inferior y el superior. Se usan fechas exactas o un período para un intervalo de tiempo, como semanas (w), días (d), horas (h), minutos (m) y segundos (s).  
`lastContact:[-5w TO NOW]`
- Se utilizan paréntesis para agrupar los operadores lógicos.  
`(osName:windows OR osName:Linux) AND logLevel:info`
- Se encierran entre barras diagonales "/" las búsquedas que tienen expresiones regulares.

### TIP

Se pueden copiar y pegar las expresiones de búsqueda del agente desde las métricas de WebView.

```
/ACCServer.*01\|Tomcat\|.*Agent/
```

## Guardar la búsqueda

En la barra de búsqueda, utilice la opción **Guardar como nueva recopilación** para guardar un patrón de búsqueda que se utiliza frecuentemente. También se puede utilizar la búsqueda guardada en una consulta.

### Ejemplo: Uso de la recopilación en una consulta

```
collection:"Tomcat Agents" AND reportName:Linux
```

## Propiedades para la búsqueda de agentes

La propiedad predeterminada para la búsqueda de agentes es "spaName". Contiene el nombre del servidor, el nombre del proceso y el nombre del agente separados por el carácter "|".

Para buscar varias propiedades, utilice la propiedad "all", que incluye las siguientes propiedades del 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.

## Visualización de los informes del agente

Todos los informes generados para los agentes aparecen en la página Informes como una lista. Es posible seleccionar un informe para ver los detalles de los informes. De forma predeterminada, los informes están disponibles durante 40 días.

Es posible también seleccionar un informe y hacer clic en el botón Descargar para descargarlo como un archivo ZIP. Un archivo ZIP contiene el informe completo en formato HTML con toda la información que se puede ver en la descripción



del informe. El archivo ZIP además incluye todos los archivos de configuración y de registro. El nombre del archivo ZIP contiene el nombre del informe y una marca de tiempo para su fácil identificación.

Se puede utilizar la barra de búsqueda situada en la parte superior de la página para buscar un informe. Se puede buscar por cualquier propiedad del informe. También es posible realizar una búsqueda global en la página principal.

### **Búsqueda de informes**

Se puede utilizar la barra de búsqueda situada en la parte superior de la página para buscar un informe. Se puede buscar por cualquier propiedad del informe. También es posible realizar una búsqueda global en la página principal.

Para buscar los informes utilizando el lenguaje de consulta de ACC, consulte [Búsqueda utilizando el lenguaje de consulta de ACC \(AQL\)](#).

A continuación se muestran ejemplos de búsquedas de informes:

- Búsqueda por nombre del informe. Use las comillas para incluir un espacio.

```
reportName:"ACCDemoWin01|Tomcat|Tomcat Agent-3"
```

- Se pueden usar los operadores AND (opción predeterminada), OR y NOT.

```
logLevel:info OR logLevel:debug
```

- Se buscan informes de agentes de Tomcat, pero solamente los que no tengan "linux" en el nombre del servidor:

```
processName:Tomcat NOT serverName:linux
```

- Búsqueda por último contacto (desde hace 5 semanas hasta ahora):

```
lastContact:[-5w TO NOW]
```

- Se utilizan paréntesis para agrupar los operadores lógicos.

```
(osName:windows OR osName:Linux) AND logLevel:info
```

Se encierran entre barras diagonales "/" las búsquedas que tienen expresiones regulares.

#### **TIP**

Se pueden copiar y pegar las expresiones de búsqueda del agente desde las métricas de WebView.

```
/ACCServer.*01\|Tomcat\|.*Agent/
```

### **Guardar la búsqueda**

En la barra de búsqueda, utilice la opción **Guardar como nueva recopilación** para guardar un patrón de búsqueda que se utiliza frecuentemente. También se puede utilizar la búsqueda guardada en una consulta.

#### **Ejemplo: Uso de la recopilación en una consulta**

```
collection:"Tomcat Agents" AND reportName:Linux
```

### **Propiedades para la búsqueda de agentes**

La propiedad predeterminada para la búsqueda de agentes es "spaName". Contiene el nombre del servidor, el nombre del proceso y el nombre del agente separados por el carácter "|".

Para buscar varias propiedades, utilice la propiedad "all", que incluye las siguientes propiedades del 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.

## **Configuración de aplicaciones para la incorporación**

La página Aplicaciones muestra todas las aplicaciones creadas en DX Application Performance Management. Utilice estas aplicaciones para incorporarlas sin problemas en DX APM y para configurar fácilmente los paquetes de agente para el entorno.

La incorporación de aplicaciones contiene los conceptos siguientes:

- **Aplicación:** Permite monitorizar la aplicación, que consta de uno o más niveles.
- **Nivel:** Denota un nivel de aplicación determinado para monitorizarlo. El nivel hace referencia a uno o más paquetes de agente creados según la selección de un usuario.

Para crear una nueva aplicación para la incorporación, consulte [Creación de aplicaciones](#).

## **Búsqueda de aplicaciones**

Es posible usar la barra de búsqueda situada en la parte superior de la página para buscar una aplicación usando solamente el campo de nombre. Como el campo de nombre es la opción de búsqueda predeterminada, se puede omitir el añadido de "nombre" en el campo de búsqueda.

Para buscar las aplicaciones utilizando el lenguaje de consulta de ACC, consulte [Búsqueda utilizando el lenguaje de consulta de ACC \(AQL\)](#).

A continuación se muestran ejemplos de búsquedas de aplicaciones:

- Para buscar una aplicación con el nombre Sitio web  

```
name:website
```

☐

```
website
```
- Se pueden usar los operadores AND (opción predeterminada), OR y NOT.  

```
name:website AND NOT name:testing
```

☐

```
website AND NOT name:testing
```

## **Gestión de paquetes del agente**

Un paquete es una imagen del agente que se puede implementar, junto con las instrucciones de instalación y con los formatos ZIP o TAR. El paquete se genera a partir de conjuntos que representan una parte de la funcionalidad del agente. Command Center además proporciona paquetes de arranque de Java. El paquete de arranque permite cambiar entre diferentes versiones del agente con un esfuerzo mínimo. Para transferir definiciones de paquetes entre clientes diferentes, utilice la funcionalidad de exportación e importación.

En la ficha Paquete, aparece una lista de paquetes disponibles. Un icono situado al lado del nombre del paquete indica que una actualización está disponible. Seleccione ese paquete y haga clic en Actualizar para actualizarlo.

Usando la página Paquetes, se puede realizar lo siguiente:

- [Creación de un paquete del agente](#)
- [Uso de un conjunto en un paquete](#)
- [Implementación de los paquetes del agente](#)
- [Integración de terceros](#)
- [Gestión de paquetes y conjuntos del agente utilizando APM Command Center](#)

La página Paquete muestra la siguiente información sobre un paquete.

## **Paquete**

La tarjeta Paquete muestra información general sobre el paquete, como el nombre, la descripción y el total de agentes.

El valor de **Número total de agentes** muestra cuántos agentes usan este paquete. Es posible ir a la ficha **Agentes** y ver los agentes que utilizan este paquete.

## **Versión del paquete**

La tarjeta **Versiones** muestra el número de agentes que utilizan cada versión del paquete. Es posible ver cuándo el paquete se modificó por última vez, el nombre del paquete, el paquete y la versión del agente, así como si el paquete está archivado. Esta descripción general ayuda a garantizar que todos los agentes utilizan la versión más reciente.

### **NOTE**

No es posible descargar un paquete archivado. Además no se puede realizar ningún cambio de configuración al paquete archivado. Cuando se crea una nueva versión del paquete, se basa en la versión actual (no archivada).

## **Versions**

La tarjeta de la versión muestra la información acerca de cada actualización del paquete y el usuario que actualizó el paquete.

Cuando se crea un paquete, su número de versión inicial es 1. Después de las subsiguientes ediciones, la versión del agente sigue siendo 1 hasta que un usuario descarga el paquete o aplica el paquete al agente. La siguiente edición cambia el número de versión a 2.

## **Conjuntos**

La tarjeta Conjuntos muestra todos los conjuntos incluidos en el paquete seleccionado.

Si un conjunto personalizado se actualiza a una versión más reciente, aparece el botón de actualización en la columna Versión del panel Conjuntos personalizados. Si se produce un error en la actualización del conjunto personalizado y el mensaje de error informa que un conjunto no tiene una versión más reciente, se puede actualizar manualmente. Haga clic en **Editar**, vaya a la vista **Seleccionar conjuntos** y reemplace la versión del conjunto con una versión más reciente, si está disponible.

## **Búsqueda de paquetes**

Se puede utilizar la barra de búsqueda situada en la parte superior de la página para buscar un paquete. Se puede buscar por cualquier propiedad del paquete. También es posible realizar una búsqueda global en la página principal.

Para buscar los paquetes utilizando el lenguaje de consulta de ACC, consulte [Búsqueda utilizando el lenguaje de consulta de ACC \(AQL\)](#).

A continuación se muestran ejemplos de búsquedas de paquetes:

- Búsqueda por nombre del paquete. Use las comillas para incluir un espacio.

```
packageName:tomcatLinux
```

- Se pueden usar los operadores AND (opción predeterminada), OR y NOT.

```
logLevel:info OR logLevel:debug
```

- Se buscan informes de agentes de Tomcat, pero solamente los que no tengan "linux" en el nombre del servidor:

```
processName:Tomcat NOT serverName:linux
```

- Búsqueda por último contacto (desde hace 5 semanas hasta ahora):

```
lastContact:[-5w TO NOW]
```

- Se utilizan paréntesis para agrupar los operadores lógicos.

```
(osName:windows OR osName:Linux) AND logLevel:info
```

Se encierran entre barras diagonales "/" las búsquedas que tienen expresiones regulares.

#### TIP

Se pueden copiar y pegar las expresiones de búsqueda del agente desde las métricas de WebView.

```
/ACCServer.*01\|Tomcat\|.*Agent/
```

### Guardar la búsqueda

En la barra de búsqueda, utilice la opción **Guardar como nueva recopilación** para guardar un patrón de búsqueda que se utiliza frecuentemente. También se puede utilizar la búsqueda guardada en una consulta.

#### Ejemplo: Uso de la recopilación en una consulta

```
collection:"Tomcat Agents" AND reportName:Linux
```

### Propiedades para la búsqueda de paquetes

La propiedad predeterminada para la búsqueda de informe es packageName. Para buscar varias propiedades, use la propiedad "all", que cubre las propiedades siguientes del informe:

bundles, comment, emHost, facets, packageName.

## Configuración de conjuntos

Un conjunto es un componente esencial desde el que se crean los agentes. El conjunto representa una parte compacta de la funcionalidad del agente como, por ejemplo, los servicios web SOAP, el servlet o JSP.

Los conjuntos pueden implementarse en caliente o pueden requerir un reinicio del proceso monitorizado. Los conjuntos dinámicos se pueden implementar en caliente. Se puede implementar el paquete en un agente en ejecución sin la necesidad de reiniciar el agente. Para implementar el paquete, agregue, elimine o actualice un conjunto dinámico en un paquete del agente. Los conjuntos dinámicos se marcan con el icono Conjunto dinámico. Los conjuntos que se pueden aplicar a un agente en ejecución pero que requieren un reinicio del proceso monitorizado se marcan con el icono Requiere reinicio.

Para ver la lista de conjuntos que están disponibles con APM Command Center de forma predeterminada, consulte [Lista de conjuntos](#).

También se puede crear un conjunto personalizado. Para obtener más información, consulte [Agregación de conjuntos personalizados](#). No se pueden editar conjuntos en la página Conjuntos. Utilice la página Paquetes para editar las propiedades del conjunto.

### Búsqueda de conjuntos

Se puede utilizar la barra de búsqueda situada en la parte superior de la página para buscar un grupo. Se puede buscar por cualquier propiedad del conjunto. También es posible realizar una búsqueda global en la página principal.

Para buscar los conjuntos utilizando el lenguaje de consulta de ACC, consulte [Búsqueda utilizando el lenguaje de consulta de ACC \(AQL\)](#).

A continuación se muestran ejemplos de búsquedas de conjuntos:

- Búsqueda por nombre de conjunto. Use las comillas para incluir un espacio.

```
bundleName:"ACCDemoWin01|Tomcat|Tomcat Agent-3"
```

- Se pueden usar los operadores AND (opción predeterminada), OR y NOT.

```
logLevel:info OR logLevel:debug
```

- Se buscan conjuntos de agentes de Tomcat, pero solamente los que no tengan "linux" en el nombre del servidor.

```
processName:Tomcat NOT serverName:linux
```

- Búsqueda por último contacto (desde hace 5 semanas hasta ahora):

```
lastContact:[-5w TO NOW]
```

- Se utilizan paréntesis para agrupar los operadores lógicos.

```
(osName:windows OR osName:Linux) AND logLevel:info
```

Se encierran entre barras diagonales "/" las búsquedas que tienen expresiones regulares.

### TIP

Se pueden copiar y pegar las expresiones de búsqueda del agente desde las métricas de WebView.

```
/ACCServer.*01\|Tomcat\|.*Agent/
```

## Guardar la búsqueda

En la barra de búsqueda, utilice la opción **Guardar como nueva recopilación** para guardar un patrón de búsqueda que se utiliza frecuentemente. También se puede utilizar la búsqueda guardada en una consulta.

### Ejemplo: Uso de la recopilación en una consulta

```
collection:"Tomcat Agents" AND reportName:Linux
```

## Propiedades de la búsqueda de conjuntos

La propiedad predeterminada para la búsqueda de conjuntos es "name". Para buscar varias propiedades, utilice la propiedad "all", que incluye las siguientes propiedades del conjunto:

category, dependencies, description, enhances, facets, name, osName, version.

## Búsqueda utilizando el lenguaje de consulta de ACC (AQL)

Especifique una consulta personalizada en la barra de búsqueda situada en la parte superior de la página de ACC que filtra los elementos mostrados en una vista. La consulta personalizada utiliza el lenguaje de consulta de ACC (AQL), que sustituye al idioma Lucene que se utilizaba anteriormente. Para obtener más información sobre las diferencias entre Lucene y AQL, consulte la documentación [Propiedades que permiten la búsqueda](#).

### Creación de consultas simples

Escriba una palabra en la barra de búsqueda para filtrar todos los resultados coincidentes basados en la consulta de palabra. La búsqueda se realiza en una propiedad predeterminada, normalmente, un nombre. Para buscar una propiedad específica, escriba la consulta con este formato:

```
propertyName:search_query_word
```

Tenga en cuenta que `propertyName` distingue entre mayúsculas y minúsculas. Mientras se escribe, la barra de búsqueda muestra las propiedades disponibles. Utilice la propiedad "all" para realizar la búsqueda en varias propiedades.

### Ejemplo: Búsqueda sencilla

```
osName:windows
```

### Crear consultas de combinación

Escriba varias consultas en la barra de búsqueda separadas por espacios o escriba varias subconsultas utilizando los siguientes operadores: AND, OR o NOT.

Los operadores distinguen entre mayúsculas y minúsculas, y se pueden utilizar paréntesis para agruparlos. AND es el operador predeterminado para las consultas separadas por espacios.

#### Ejemplo: Consulta de combinación con el operador AND

Los siguientes ejemplos de consulta filtran los resultados donde se encuentran todas las palabras.

```
word1 AND word2 AND word3
word1 AND word2 word3
word1 word2 word3
```

#### Ejemplo: Consulta de combinación con el operador OR

Este ejemplo filtra los resultados donde se encuentra una de las palabras.

```
word1 OR word2 OR word3
```

#### Ejemplo: Consulta de combinación con el operador NOT

Este ejemplo filtra los resultados que no contienen la palabra "myquery".

```
NOT myquery
```

Existen símbolos alternativos que se pueden utilizar en lugar de los operadores con nombre:

Operator	Alternativo
AND	&&
OR	
NOT	!

#### Ejemplo: Consulta de combinación con paréntesis

El ejemplo agrupa los operadores y filtra los resultados.

```
(word1 AND word2) OR word3
word1 AND (word2 OR word3)
```

### Otras consultas de búsqueda

Se pueden utilizar cadenas, caracteres comodín, números, expresiones regulares y consultas de intervalo como patrones de búsqueda para filtrar los resultados.

#### Uso de cadenas y caracteres comodín

Escriba una cadena de palabras o caracteres entre comillas (" ") para filtrar los resultados de búsqueda. Los resultados son una coincidencia exacta de la cadena de búsqueda. Se pueden utilizar los siguientes tipos de caracteres comodín \* para coincidir con cualquier subcadena y ? para coincidir con un carácter. El uso de un carácter especial dentro de una cadena se trata como un carácter ordinario.

#### Ejemplo: Consulta de cadena

La siguiente consulta filtra todos los resultados que coinciden exactamente con la cadena.

```
"abc xyz"
```

#### Ejemplo: Consulta de caracteres comodín

La siguiente consulta filtra todos los resultados que contienen la cadena de búsqueda.

```
"abc xyz"
```

**Ejemplo: Consulta de combinación de cadena y carácter comodín**

La siguiente consulta muestra un patrón de búsqueda utilizando caracteres comodín, cadenas y una única palabra.

```
word*"quoted string"?
```

**Consulta de intervalo**

Una consulta de intervalo puede ser un intervalo de números, versiones o fechas.

**Ejemplo: Consulta de intervalo**

La siguiente consulta filtra los resultados incluidos en el intervalo del 0 al 5 en la propiedad numérica: prop

```
prop:[0 TO 5]
```

La siguiente consulta muestra un patrón de búsqueda con un intervalo exclusivo y un inicio que no denota ningún límite máximo en la propiedad numérica: prop

```
prop prop:{10 TO *}]
```

## Uso

DX APM permite utilizar varios métodos para monitorizar los estados de las aplicaciones del negocio, así como investigar y solucionar los problemas.

Si desea...	Realice lo siguiente...	Lea esto...
Comprender la ubicación geográfica del entorno de la aplicación	Vaya a la <b>Vista de experiencia</b> y vea el entorno de la aplicación desde el nivel más alto del universo. Explore en profundidad transacciones específicas para buscar errores.	<a href="#">Monitorización del rendimiento utilizando la Vista de experiencia</a>
Cómo ver una descripción general de los valores de métrica del agente	Vaya a la <b>Vista de métrica</b> y desplácese por el <b>Árbol de métrica</b> hasta un host del servidor de aplicaciones. Desplácese por el árbol y haga clic en el nodo del agente que desee investigar.	<a href="#">Monitorización de los valores de métrica del agente con la Vista de métrica</a>
Ver el estado general del entorno	Vaya al <b>Cuadro de mandos</b> y aplique la Vista de agente o la Vista de experiencia. Un mosaico en el cuadro de mandos representa un grupo de todos los componentes que comparten un nombre de atributo y un valor. Los mosaicos muestran los estados de alerta más significativos de cualquiera de los componentes del grupo.	<a href="#">Monitorización del estado general del entorno con el cuadro de mandos</a>
Monitorizar problemas y anomalías	Utilice la Evaluación de errores asistida para monitorizar los problemas y las anomalías. La Evaluación de errores asistida identifica experiencias afectadas e identifica la evidencia como un problema. Las anomalías son como los problemas, pero sin provocar ningún impacto en el usuario. La Evaluación de errores asistida analiza los datos del agente de los entornos monitorizados e identifica los componentes comunes de un problema para que no se vea desbordado por las incidencias.	<a href="#">Evaluación de errores asistida y analistas</a>
Investigar problemas	Utilice el Bloc de notas de análisis e investigue los problemas identificados por la Evaluación de errores asistida.	<a href="#">Investigación de problemas mediante el Bloc de notas de análisis</a>
Investigar el rendimiento de las transacciones con errores	Utilice el Visor de seguimiento de la transacción para comprender el rendimiento de la transacción y solucionar un problema de rendimiento pobre identificando cuándo, dónde y por qué se degrada el rendimiento.	<a href="#">Investigación del rendimiento de las transacciones con errores</a>



Monitorizar el estado y el rendimiento de los agentes	Vaya a la <b>Vista de agentes</b> y monitorice los agentes que están disponibles en el entorno. Las tarjetas de agente muestran los detalles de un agente o de un grupo de agentes. Si se agrupan los agentes en una misma tarjeta, la información de la métrica también se agrupa.	<a href="#">Visualización del estado del agente y gestión de las tarjetas de agente</a>
-------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------

## Incorporación de aplicaciones para la monitorización

Se puede utilizar la incorporación de aplicaciones para incorporar las aplicaciones sin problemas en DX APM y para configurar fácilmente los paquetes de agente para el entorno. El asistente para la incorporación de aplicaciones le guía para seleccionar las opciones de monitorización y crea nuevos paquetes de agente. La incorporación de aplicaciones contiene los conceptos siguientes:

- **Aplicación:** Permite monitorizar la aplicación, que consta de uno o más niveles.
- **Nivel:** Denota un nivel de aplicación determinado para monitorizarlo. El nivel hace referencia a uno o más paquetes de agente creados según la selección de un usuario.


En la configuración del nivel, cada paso contiene una o más opciones que se asignan a las funcionalidades de monitorización concretas (por ejemplo, la monitorización de la base de datos de APMIA y Oracle, el sistema operativo Linux). Para incorporar aplicaciones, configure lo siguiente:

1. **Detalles de la aplicación:** Defina el nombre y la descripción de una aplicación para monitorizarla.
2. **Configuración del nivel:** Defina las opciones de monitorización del nivel.
3. **Paso de descarga:** Defina los artefactos (paquetes del agente) para descargar que se crean a partir de las opciones de monitorización.

## Creación de aplicaciones

Cree aplicaciones seleccionando las opciones de monitorización y creando nuevos agentes para incorporar las aplicaciones en DX APM. Es posible agregar varios niveles a la aplicación. También se puede editar, clonar o eliminar.

1. En la interfaz de usuario de DX APM, seleccione **Configuración**.
2. Haga clic en el mosaico **Aplicaciones**.
3. Si está utilizando **Aplicaciones** por primera vez, haga clic en **Comenzar** para crear una nueva aplicación. De lo

contrario, cree una aplicación haciendo clic en .

4. Proporcione los detalles siguientes para la aplicación:
  - a) **Nombre de la aplicación:** Dé un nombre a la aplicación. Es posible cambiarlo en cualquier momento.
  - b) **Descripción:** Proporcione una descripción de la aplicación.
5. Haga clic en **Agregar niveles de la aplicación**.
6. Cree un nivel para la aplicación con los detalles siguientes:
  - a) **Nombre del nivel:** Agregue un nombre de nivel y una descripción para el nivel de la aplicación.
  - b) **Sistema operativo:** Seleccione el sistema operativo necesario en el cual se ejecuta la aplicación. Las opciones subsiguientes cambian según el sistema operativo seleccionado.
  - c) **Pila de tecnología (opcional):** Seleccione la pila de tecnología en la cual se ejecuta la aplicación. Es posible seleccionar más de una pila de tecnología.
  - d) **Tipo de contenedor (opcional):** Seleccione el tipo de contenedor para la aplicación. El tipo de contenedor cambia según el sistema operativo.
  - e) **Base de datos (opcional):** Es posible seleccionar una o más bases de datos en las cuales se ejecuta la aplicación. Es posible agregar varios perfiles para las bases de datos que admiten varias conexiones y proporcionar una configuración de conexión diferente. Seleccione o anule la selección de la casilla de verificación **Instantáneas** para activar o desactivar las instantáneas de seguimiento de la base de datos.
  - f) **Servidor web:** Seleccione uno o más servidores web en los cuales se ejecuta la aplicación. Es posible agregar varios perfiles para un servidor web seleccionado y configurar sus opciones por separado.
  - g) **Sistema de mensajería:** Seleccione un sistema de mensajería que utiliza la aplicación para la comunicación. En función de la selección, proporcione los detalles del sistema de mensajería. Es posible agregar varios perfiles para los sistemas de mensajería que admiten varias conexiones y configurar sus opciones por separado.
  - h) **Monitorización:** Seleccione las opciones de monitorización para monitorizar el rendimiento de la aplicación. En función de la selección, proporcione los detalles del sistema de monitorización. Es posible agregar varios perfiles para los sistemas de monitorización que admiten varias conexiones de monitorización y configurar sus opciones por separado.
  - i) **Adicional:** Se muestran opciones adicionales basadas en el sistema operativo seleccionado. Seleccione las funciones necesarias y proporcione detalles adicionales basados en su selección. Es posible agregar varias opciones para las funciones que admiten varias conexiones y configurar sus detalles por separado.
  - j) **Opciones:** En función del sistema operativo seleccionado, actualice las opciones.
  - k) **Resumen del nivel:** Revise la configuración del nivel y haga clic en **Agregar nivel ahora**.

Se crea el nivel. También se puede editar, clonar o eliminar. Es posible crear y agregar varios niveles a la aplicación.
7. Haga clic en **Crear aplicación**.
8. Haga clic en **Finalizado**.

La aplicación se crea con los niveles necesarios. Puede descargar una aplicación o copiar el vínculo para descargarla. Es posible también descargar las instrucciones de instalación o verlas en pantalla.

## Descarga de las aplicaciones

Con la lista desplegable **Descargar** correspondiente a una aplicación, se puede descargar una aplicación o copiar el vínculo de descarga. Es posible también descargar o ver las instrucciones de instalación. El paquete descargado contiene lo siguiente:

- Una carpeta para cada nivel. Cada carpeta contiene los paquetes del agente según la configuración para cada nivel.
- **Completed.txt**: Si este archivo no está disponible en la carpeta descargada, el paquete no se ha descargado correctamente.
- **Info.txt**: Este archivo contiene un resumen de todos los paquetes incluidos en las carpetas del nivel.

## Monitorización del rendimiento utilizando la Vista de experiencia

DX APM permite comprender la ubicación geográfica del entorno de aplicaciones, lo que es fundamental para realizar de forma eficaz la monitorización y la solución de problemas. Application Performance Management proporciona una descripción general de un entorno de aplicaciones. La Vista de experiencia muestra las aplicaciones monitorizadas desde el punto de vista de la experiencia.

Los siguientes roles utilizan la Vista de la experiencia:

- Los administradores ven el estado del entorno.
- Los analistas de primer nivel monitorizan problemas y advertencias en el entorno con la Vista de la experiencia.
- Los analistas experimentados investigan y solucionan problemas con el Bloc de notas de análisis, el Cuadro de mandos y el Mapa.

### Funcionamiento del front-end como una experiencia

La experiencia es el componente del extremo izquierdo de la transacción, el primer componente monitorizado de toda la transacción. El nodo de la experiencia es el primer componente del front-end monitorizado y contiene un atributo que se llama Experiencia. El nodo de la experiencia es el principio de la ruta de la transacción. Una experiencia puede ser, por ejemplo, un servlet o un front-end genérico.

### Vista de experiencia

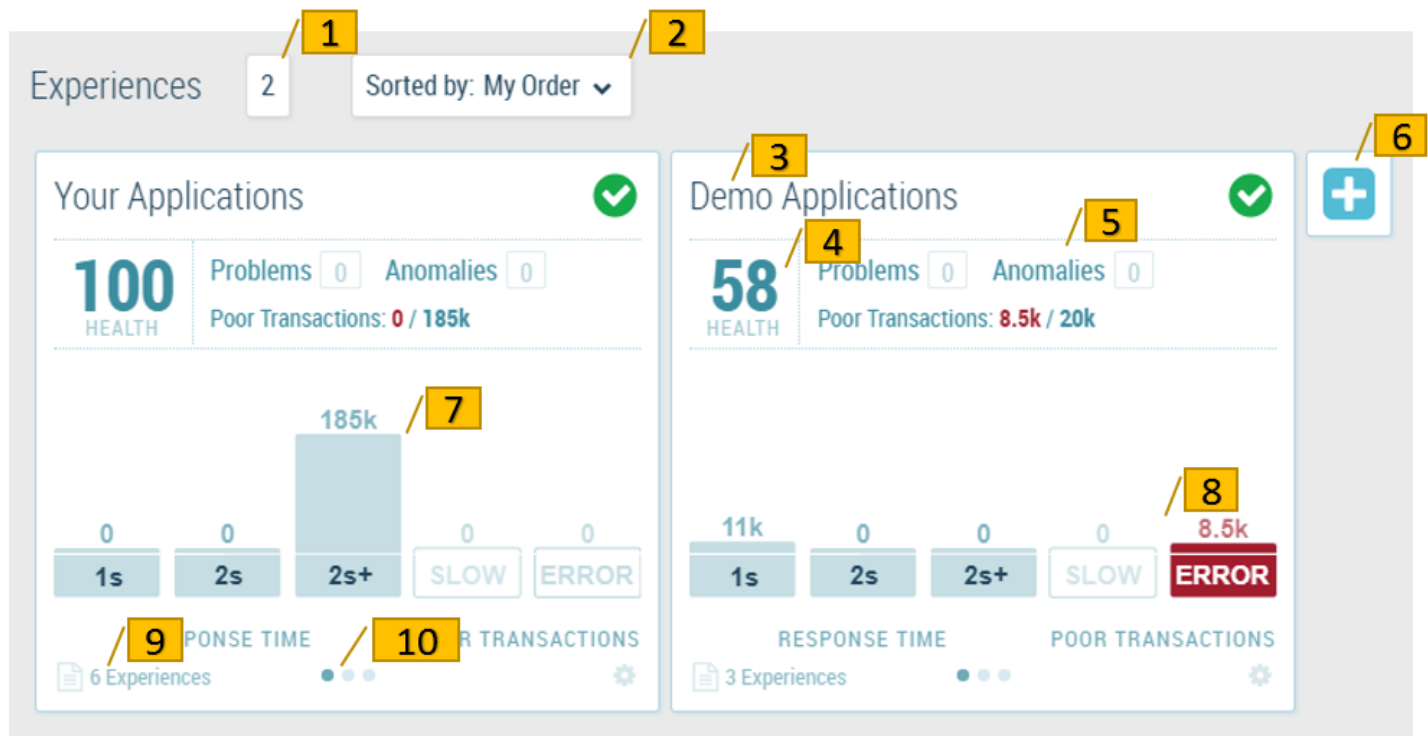
La Vista de la experiencia permite:

- Filtrar las partes que no tienen problemas del entorno a fin de centrarse en las incidencias.
- Desplazarse hasta los niveles más bajos de la Vista de la experiencia para ver las secciones del entorno con más detalle. Las tarjetas de experiencia muestran el estado de todos los componentes de los que es responsable el usuario. La información de la tarjeta muestra las experiencias que se están cargando. La Evaluación de errores asistida identifica las áreas con problemas más probables y muestra el número de problemas y anomalías.

Tipos de transacción en la Vista de experiencia:

- Transacciones sin errores: Los valores de la métrica *Respuestas por intervalo* cuando el nodo de la experiencia no tiene ninguna alerta en el estado de precaución o peligro.
- Transacciones detenidas: Los valores de la métrica *Detenciones* del nodo de la experiencia.
- Transacciones erróneas: Los valores de la métrica *Errores por intervalo* del nodo de la experiencia.
- Transacciones lentas: El valor de la métrica *Respuestas por intervalo* cuando el nodo de la experiencia tiene una alerta en el estado de precaución o peligro en la métrica Tiempo medio de respuesta o en una métrica de análisis diferencial.
- Transacciones con alertas: El valor de la métrica *Respuestas por intervalo* cuando el nodo de la experiencia no tiene ninguna alerta en el estado de precaución o peligro en una métrica que no sean las transacciones lentas.

Utilice el siguiente gráfico y su correspondiente leyenda para conocer las distintas funciones de la Vista de la experiencia.



La siguiente leyenda identifica cada elemento del mapa con un número y proporciona más información:

Número	Name	Más información
1	El número de experiencias	
2	Ordenar por	Ordena las tarjetas por Nombre o por Mi orden.
3	Tarjeta de experiencia	Las tarjetas de experiencia muestran información de resumen e identifican el problema y el origen del problema. Las tarjetas se definen en función de un universo. El número máximo es un universo dentro de una tarjeta.
4	ESTADO	La puntuación del ESTADO muestra la puntuación general del estado del entorno. El número muestra un porcentaje de transacciones sin errores con respecto al número total de transacciones. La puntuación muestra el volumen de transacciones sin errores y de transacciones con errores. El volumen de transacciones con errores es una suma de todas las transacciones que tienen errores (lentas, erróneas, con alerta, detenidas).

5	Problemas y Anomalías	<p>Muestra el número de problemas y anomalías.</p> <p>Un problema indica una situación donde uno o más componentes de transacciones relacionadas han activado alertas. Eventos como detenciones, errores y otras evidencias han afectado negativamente a las transacciones.</p> <p>Una anomalía indica una situación donde uno o más componentes de transacciones relacionadas han activado alertas. Se han observado eventos como detenciones y errores pero no han afectado al rendimiento de la transacción.</p>
6	Adición de una tarjeta de experiencia	<p>Haga clic en el signo más para dar nombre y configurar una nueva tarjeta de experiencia.</p> <p><b>Nota:</b> Para obtener más información sobre cómo agregar una tarjeta, consulte <a href="#">Visualización del estado del agente y gestión de las tarjetas de agente</a></p>
7	TIEMPO DE RESPUESTA	<p>El histograma TIEMPO DE RESPUESTA muestra el tiempo medio de respuesta por segundo para las transacciones sin errores que se han completado en:</p> <ul style="list-style-type: none"> <li>• 1s menos de 1 segundo</li> <li>• 2s entre 1 y 2 segundos</li> <li>• 2s+ más de 2 segundos</li> </ul>
8	TRANSACCIONES CON ERRORES	<p>El histograma TRANSACCIONES CON ERRORES muestra el número de transacciones con errores que se han producido durante el período.</p> <ul style="list-style-type: none"> <li>• LENTA muestra el número de transacciones detenidas y lentas. Estas transacciones tienen alertas para el Análisis diferencial o alertas para el Tiempo medio de respuesta.</li> <li>• ERROR muestra el número de errores por intervalo de la aplicación.</li> </ul>
9	Abre el Bloc de notas de análisis	<p>El Bloc de notas de análisis muestra las transacciones comerciales para una tarjeta de experiencia específica. El recuento de transacciones comerciales es visible al lado del icono Bloc de notas de análisis.</p> <p><b>Nota:</b> De forma predeterminada, no se puede abrir el Bloc de notas de análisis si la tarjeta de experiencia contiene más de 20 transacciones comerciales.</p>
10	Alternar gráficas	<p>Las gráficas son Tiempo de respuesta agregado, Tiempo medio de respuesta y Volumen de la transacción.</p>

## **Monitorización del rendimiento mediante la Vista de la experiencia**

La Vista de la experiencia permite monitorizar el rendimiento del entorno desde el nivel más alto del universo. Se pueden explorar en profundidad transacciones específicas para buscar errores.

### **Siga estos pasos:**

1. Haga clic en una **Tarjeta de experiencia**.  
Aparecen los datos agregados para los grupos de transacciones comerciales relacionados que están disponibles en el universo. Se pueden agregar, configurar y volver a ordenar las tarjetas.
2. Haga clic en el **gráfico** para recorrer los gráficos de los valores de métrica.
3. Vea la **Puntuación del estado**.  
La puntuación del estado muestra la puntuación general del estado del entorno. El número muestra un porcentaje de transacciones sin errores con respecto al número total de transacciones. Por ejemplo, la puntuación del estado del entorno que se está monitorizando es de 85. Esta puntuación significa que el 85 % de las transacciones que se están monitorizando no tienen errores. El 15 % restante son transacciones con errores. Las transacciones con errores son la suma de las transacciones lentas y erróneas.
4. Expanda una **tarjeta**. Aparecen más detalles en el panel Evaluación de errores asistida. El panel Evaluación de errores asistida es un panel que se puede extraer de la derecha y muestra donde se están produciendo los problemas y las anomalías. El motor de la Evaluación de errores asistida identifica los componentes comunes de un problema para que el usuario no se vea desbordado por las incidencias. El panel Evaluación de errores asistida es visible en la Vista de la experiencia excepto en la página de nivel superior.
5. Expande la **historia**. Aparecerán más detalles. El panel también muestra los nodos sospechosos, que el motor de la Evaluación de errores asistida resalta como otros posibles contribuyentes a la situación.
6. Expande **Problemas y Anomalías**.  
Aparecerán más detalles.
7. Haga clic en el **título** del gráfico y explore en profundidad hasta el siguiente nivel de agrupación.
8. Haga clic en el icono del **bloc de notas**.  
Se abrirá el Bloc de notas de análisis para el grupo de componentes.

### **NOTE**

De forma predeterminada, no se puede abrir el Bloc de notas de análisis si la tarjeta de experiencia contiene más de 20 transacciones comerciales.

## **Creación de una evaluación de errores utilizando la Vista de la experiencia**

Comprenda cómo el panel Evaluación de errores asistida informa sobre los problemas y las anomalías en los eventos del sistema.

### **NOTE**

#### **Más información:**

[Monitorización de los problemas y las anomalías de la Evaluación de errores asistida](#)

## **Ejemplo: Monitorización y aislamiento de las incidencias con la Vista de la experiencia**

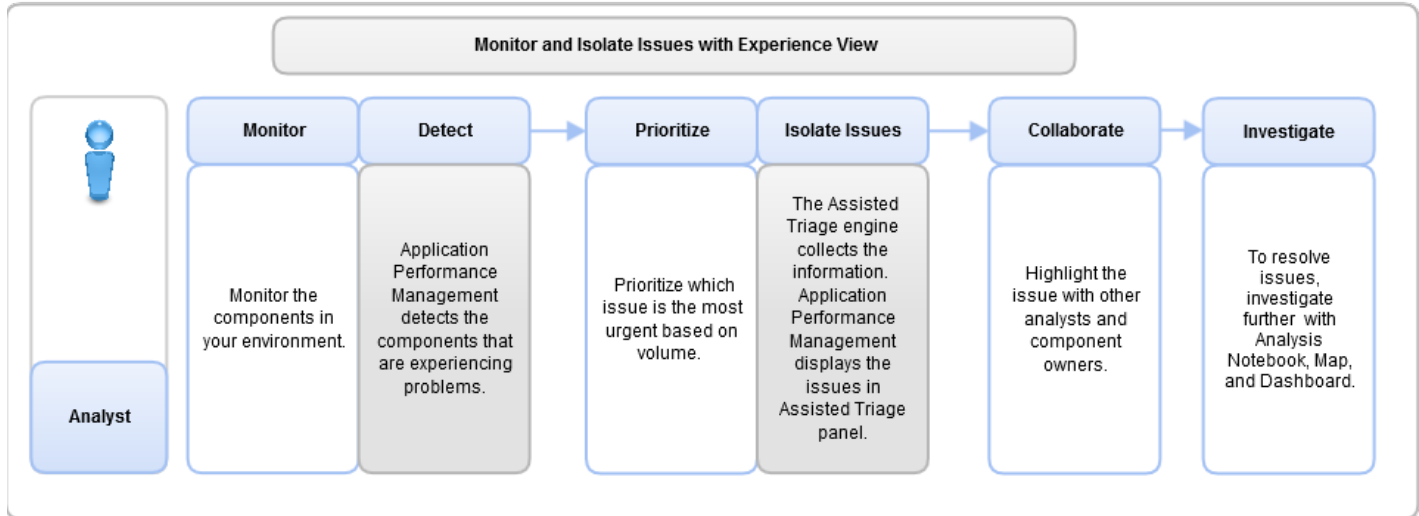
La Vista de la experiencia permite ver el estado de todos los componentes en el área del entorno que es responsabilidad del usuario. Se pueden ver las experiencias bajo condición de carga y se puede explorar en profundidad para identificar los componentes esenciales. La Evaluación de errores asistida le ayuda a identificar las áreas problemáticas más probables.

Este ejemplo muestra un flujo de trabajo para un analista. Como analista, el usuario es consciente de que se ha producido una incidencia en el entorno. Se debe identificar la causa raíz del problema y gestionar los recursos para solucionar los problemas. El objetivo del diagnóstico de incidencias es identificar al paciente cero. El paciente cero es

el componente de la aplicación que se encuentra con problemas en primer lugar y afecta a otros componentes y a la experiencia del cliente.

El siguiente diagrama muestra el flujo de trabajo para monitorizar un entorno y aislar los problemas:

**Figure 5: Homepage\_workflow**



1. Monitorizar los componentes del entorno.
2. Haga clic en una **Tarjeta de experiencia** para explorar en profundidad y ver información más detallada en los niveles inferiores de la Vista de experiencia.  
Application Performance Management detecta los componentes que tienen problemas y detecta las transacciones que se están ejecutando lentamente o en las que se está produciendo un error. La combinación de transacciones erróneas y lentas se muestra como el número total de experiencias del cliente insatisfactorias. Las experiencias se priorizan según el volumen de transacciones y el volumen de experiencias del cliente insatisfactorias.
3. Priorice qué incidencia es más urgente en función del volumen. Mire las experiencias que están experimentando los problemas de estado más graves. Correlacione las experiencias a los problemas identificados en el panel Evaluación de errores asistida. Priorice qué problemas se deben solucionar en función del valor del negocio.  
El motor de la Evaluación de errores asistida recopila la información y muestra las incidencias en el panel Evaluación de errores asistida. El motor de la Evaluación de errores asistida identifica las transacciones que comparten componentes que tienen un mal rendimiento. Los componentes relacionados bajo condición de carga se identifican juntos como un problema en el panel Evaluación de errores asistida.
4. Póngase en contacto con analistas con más experiencia o con una persona responsable para realizar una consulta sobre la incidencia. Utilice la información del panel para identificar los propietarios de los componentes con incidencias. Comparta la dirección URL con la persona para que pueda ver la misma vista.
5. Investigue con más detalle el problema en el Bloc de notas de análisis, el mapa y el cuadro de mandos.

DX Application Performance Management proporciona una vista general y permite comprender la ubicación geográfica del entorno de aplicaciones, lo que es fundamental para realizar de forma eficaz la monitorización y la solución de problemas. La Vista de experiencia muestra las aplicaciones monitorizadas desde el punto de vista de la experiencia.

Para monitorizar el rendimiento de la aplicación mediante la Vista de experiencia, consulte [Monitorización del rendimiento mediante la Vista de experiencia](#).

# Investigación de problemas mediante el Bloc de notas de análisis

DX APM permite a los analistas realizar tareas concretas para su rol. Utilice el Bloc de notas de análisis para investigar los problemas.

## Bloc de notas de análisis

Utilice el siguiente gráfico y su correspondiente leyenda para conocer las distintas funciones del Bloc de notas de análisis.



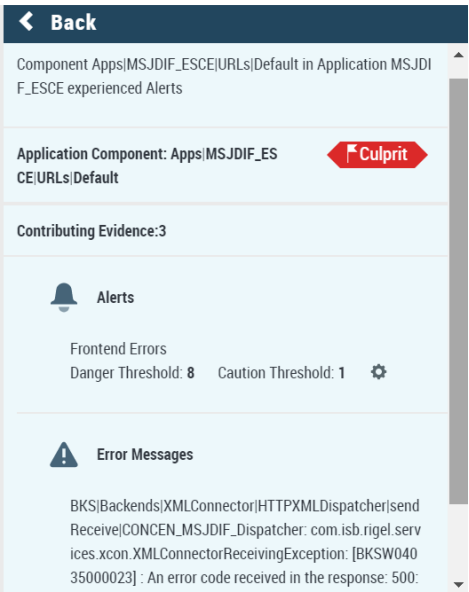
La siguiente leyenda identifica cada elemento con un número y proporciona más información:

Número	Name	Más información
1	PUNTUACIÓN DEL ESTADO	La puntuación del estado muestra la puntuación general del estado del entorno. El número muestra un porcentaje de transacciones sin errores con respecto al número total de transacciones. La puntuación muestra el volumen de transacciones sin errores y de transacciones con errores. El volumen de transacciones con errores es una suma de todas las transacciones que tienen errores (lentas, erróneas, con alerta, detenidas).



2	Histograma del tiempo de respuesta agregado	<p>El histograma muestra el tiempo medio de respuesta por segundo para las transacciones sin errores y con errores.</p> <ul style="list-style-type: none"> <li>• <b>1 s</b> Número de transacciones sin errores que se completan en menos de 1 segundo.</li> <li>• <b>2 s</b> Número de transacciones sin errores que se completan entre 1 y 2 segundos.</li> <li>• <b>más de 2 s</b> Número de transacciones sin errores que se completan en más de 2 segundos.</li> <li>• <b>Lenta</b> Número de transacciones detenidas y lentas. Transacciones que han infringido el umbral de alerta Tiempo medio de respuesta.</li> <li>• <b>Error</b> Valores de la métrica Errores por intervalo para los nodos de experiencia.</li> </ul> <p>El color rojo indica el número de transacciones con alerta que se han completado.</p>
3	Datos de series temporales: Gráfica del tiempo medio de respuesta	<p>Los datos de series temporales proporcionan la descripción general de los valores de métrica o un intervalo de tiempo problemático en concreto. No está limitado a depender únicamente de la orientación proporcionada por los eventos. Pase el ratón sobre un pico del comportamiento de la métrica en la gráfica para seleccionar y acercarse a un intervalo de tiempo problemático. Los valores de la métrica de respuestas por intervalo y de la métrica de errores por intervalo se recopilan cada 15 segundos.</p> <p>Gráfica Tiempo medio de respuesta</p> <ul style="list-style-type: none"> <li>• La línea azul indica el tiempo medio de respuesta real.</li> <li>• La línea de puntos indica una predicción del tiempo medio de respuesta.</li> <li>• Las áreas sombreadas indican una desviación. Si el valor de pronóstico está fuera del intervalo de desviación, ocurre algo inusual.</li> </ul>

4	Datos de series temporales: Histograma Volumen de la transacción	<p>Los datos de series temporales proporcionan la descripción general de los valores de métrica o un intervalo de tiempo problemático en concreto. No está limitado a depender únicamente de la orientación proporcionada por los eventos. Pase el ratón sobre un pico del comportamiento de la métrica en la gráfica para seleccionar y acercarse a un intervalo de tiempo problemático.</p> <p>Los valores de la métrica de respuestas por intervalo y de la métrica de errores por intervalo se recopilan cada 15 segundos.</p> <p>Histograma Volumen de la transacción</p> <ul style="list-style-type: none"> <li>El intervalo de tiempo se divide en 12 secciones y compara el volumen de la transacción dentro del intervalo de tiempo seleccionado.</li> </ul>
5	Panel de evaluación de errores asistida	El panel Evaluación de errores asistida enumera los Problemas y Anomalías para el componente seleccionado.

6	Estado o causante del componente	<p><b>Círculo rojo:</b> El componente es un actor en al menos un problema o anomalía que aparece en el panel Evaluación de errores asistida. Todos los componentes de una historia se tratan como actores.</p> <p><b>Círculo rojo concéntrico:</b> El componente es el causante de al menos un problema o anomalía que aparece en el panel Evaluación de errores asistida. Todos los actores cuentan con evidencias, pero un causante es un actor especial. El causante identifica la causa raíz del problema o de la anomalía en la aplicación o transacción proporcionada. Este componente puede ser el origen de la degradación del rendimiento en su entorno de aplicaciones.</p> <p><b>Abrir:</b> Haga clic en <b>Abrir</b> para ver los detalles de evidencia de la anomalía. Además, en el caso de las alertas, se pueden ver los valores del umbral y editar también los valores de configuración de alertas. Haga clic en el icono de configuración de una alerta para desplazarse a la configuración de alertas y personalizar aún más las alertas.</p> 
7	Layer	Asigne distintos tipos de componentes de superposición de capas del mapa desde el entorno hacia el mapa.
8	Filtro	Un filtro es una lista de atributos y valores obligatorios que permiten visualizar componentes específicos de la asignación.

9	Conexiones y nodos del componente	Las líneas de conexión entre los nodos representan los estados siguientes: <b>Línea gris:</b> No hay ninguna alerta definida en el componente de back-end. <b>Línea roja:</b> Al menos existe una alerta roja en el componente de back-end. La línea discontinua gris indica que no existe ningún componente del back-end en la conexión.
10	Árbol de métrica	Métrica para el componente seleccionado en una estructura de árbol que se puede buscar.
11	Comparación del tiempo de rendimiento	Métrica para el componente seleccionado en una tabla.
12	Componentes	Atributos que están conectados al componente seleccionado.
13	Transacciones comerciales	Transacciones comerciales para el componente seleccionado.

### **Investigación de problemas mediante el Bloc de notas de análisis**

El Bloc de notas de análisis permite investigar más problemas individuales.

#### **Siga estos pasos:**

1. Cuando se identifica una experiencia con problemas aparentes, abra el **Bloc de notas de análisis**.  
El Bloc de notas de análisis muestra las transacciones que se ven afectadas en el formato del mapa.
2. Utilice el mapa de **línea de tiempo** para ver eventos y alertas.
3. Agrupe el mapa con una perspectiva predefinida o cree su propia perspectiva.
4. Busque componentes que se marcan como problemas o anomalías.
  - Un círculo rojo indica que el componente es un actor en al menos un problema o una anomalía.
  - Un círculo rojo concéntrico indica que el componente es el culpable en al menos un problema o una anomalía.
5. Coloque el ratón sobre un **componente** y haga clic en el icono.  
El **gráfico de componentes** muestra un máximo de 20 nodos. Utilice los **gráficos de componentes** para comparar más métricas en directo o históricas entre nodos arbitrarios. El **gráfico de componentes** contiene más información de la métrica de la que está disponible en el mapa para todos los componentes.
  - Histograma del tiempo de respuesta agregado
  - Minigráfico medio
  - Gráfico Volumen de la transacción
6. Haga clic en un **componente** en el flujo de relaciones.
  - La ficha **Árbol de métrica** muestra un subconjunto contextual de métricas para el componente seleccionado. Para obtener más información sobre el uso del Árbol de métrica, consulte [Monitorización de los valores de métrica del agente con la Vista de métrica](#).
  - La ficha **Comparación del tiempo de rendimiento** muestra un comparador de minigráfico de la métrica. La columna derecha muestra la métrica de la hora actual. La columna izquierda muestra la métrica con la misma hora que la de un período anterior. Puede definir la hora de comparación de las listas desplegadas. Los datos de la métrica aparecen en el visor de la métrica junto con las métricas de comparación para un período anterior.
  - La ficha **Componentes** contiene detalles de atributos del componente seleccionado.
  - La ficha **Transacciones comerciales** enumera las transacciones.
7. Seleccione el período de tiempo para la comparación de la métrica mediante la lista desplegable.

El motor de Evaluación de errores asistida analiza los datos del agente desde el entorno monitorizado. El motor identifica las conexiones y los patrones entre las alertas individuales que indican un problema de desarrollo. El panel Evaluación de errores asistida muestra los problemas y las anomalías detectados. Los problemas y las anomalías están formados por situaciones. Las situaciones se agrupan por nombre de la aplicación culpable y se ordenan cronológicamente y por tamaño;

Una anomalía indica una situación donde uno o más componentes de transacciones relacionadas han activado alertas de precaución.

Un problema indica una situación donde uno o más componentes de transacciones relacionadas han activado alertas de advertencia.

8. Haga clic en un **problema** o en una **anomalía**.

Aparecerá información sobre el problema o la anomalía. El componente afectado se resalta en el mapa.

## Visualización del estado del agente y gestión de las tarjetas de agente

Utilice la Vista de agente para monitorizar el estado y el rendimiento de los agentes que están disponibles en el entorno. La página Vista de agente es una descripción general con toda la información importante sobre los agentes en un mismo lugar. En la vista, las tarjetas de agente muestran los detalles de un agente o de un grupo de agentes. Si se agrupan varios agentes en una misma tarjeta, la información de la métrica también se agrupa. Con el agente o la tarjeta de agente, se pueden realizar las acciones siguientes:

### Visualización del estado del agente

La Vista de agente permite determinar el estado de conectividad del agente, los problemas de sobrecarga o si el agente no está recopilando métrica. La información se puede visualizar en el modo en directo o se puede seleccionar un intervalo de tiempo histórico.

#### Siga estos pasos:

1. Haga clic en **Vista de agente** en el panel izquierdo.

Una tarjeta de agente muestra los detalles de un agente o grupo de agentes. Si se agrupan varios agentes en una misma tarjeta, la información de la métrica también se agrupa. La Vista de agente muestra a todos los agentes del entorno y la métrica siguiente:

- **CPU**

Muestra el porcentaje de la CPU que se está utilizando.

- **Memoria dinámica**

Muestra el porcentaje de memoria que se está utilizando.

En el gráfico de líneas de CPU y Memoria dinámica, pase el ratón por encima de un pico en el comportamiento de la métrica de la gráfica. Seleccione y acérquese a un intervalo de tiempo problemático.

- **Tiempo de GC**

Muestra el porcentaje del intervalo de tiempo empleado en el recopilador de elementos no utilizados para el intervalo de tiempo seleccionado actualmente.

- **Métrica recopilada**

Muestra el número de instancias de métrica recopiladas por los agentes.

Si la tarjeta únicamente contiene información para un agente, se muestran detalles de atributo más granulares, como el nombre de host o el tiempo de actividad. Si hay más de un agente en una tarjeta, se muestra el recuento de aplicaciones, el recuento de agentes y el recuento de recopiladores.

2. (Opcional) Haga clic en el título de la tarjeta para mostrar la perspectiva desde la que desea agrupar los agentes; por ejemplo, Tipo. La perspectiva predeterminada es Nombre.

Las perspectivas disponibles se basan en nombres de atributo para que los agentes se agrupen en función de sus atributos.

3. (Opcional) Haga clic en **Vista de aislamiento**.

Una nueva ficha abre el mapa en la **Capa de la infraestructura de APM**. El mapa muestra los componentes que comparten el valor del atributo como un grupo expandido. Una perspectiva temporal elimina los niveles de agrupación superiores. La vista de aislamiento aplica un filtro de ruta de transacción para que el mapa muestre todas las transacciones completadas que pasan por los componentes.

4. Abra una tarjeta de agente y seleccione una de las opciones siguientes de la lista desplegable **Ordenado por**:

- **Puntuación del estado**

Muestra el estado general de los agentes. Varias alertas en agentes están monitorizando la métrica, como la CPU o la conectividad del agente. El porcentaje de la puntuación del estado cuenta las alertas de las últimas 24 horas. Si cualquiera de las alertas monitorizadas se ha activado en las últimas 24 horas, el porcentaje de la puntuación del estado baja. Por ejemplo, una puntuación del estado del 100 % significa que no se ha activado ninguna alerta en las últimas 24 horas. Una puntuación del estado del 50 % significa que en las últimas 24 horas se han mostrado algunas alertas con una duración total de 12 horas.

- **Conexión**

Muestra el número de agentes disponibles en el entorno y el número de agentes desconectados.

- **CPU máxima**

Muestra primero las tarjetas con el uso de la CPU más elevado.

- **Memoria más alta**

Muestra primero las tarjetas con el uso de memoria más elevado.

5. (Opcional) Haga clic en **Ver como lista**.

La lista es una alternativa a las tarjetas de agente; muestra más datos en una sola página, de forma concisa. Haga clic en un nombre de columna para ordenar los datos por ese nombre de columna. Haga clic en una línea para expandir los datos del agente.

### **Agregación de una tarjeta de agente**

Las tarjetas de agente permiten dividir a los agentes en grupos significativos en función de sus atributos. De forma predeterminada, se dispone de una tarjeta de agente con todos los agentes. Como administrador, puede agregar nuevas tarjetas de agente.

#### **Siga estos pasos:**

1. En Vista de agente, haga clic en el signo más (+) junto a las tarjetas de agente existentes.

Se abrirá una nueva ventana **Agregar tarjeta de agente**.

2. Asigne un nombre a la tarjeta y siga las instrucciones que aparecen en la ventana.

- **Seleccionar un universo**

En la mayoría de los entornos de empresa, el número total de componentes es demasiado grande para visualizarlos de forma eficaz. Los universos permiten al administrador ajustar el número y los tipos de componentes en grupos más significativos. Este grupo que se ha ajustado es un universo. Por razones de seguridad, no hay ninguna asignación predeterminada para todos los usuarios. Debe estar adjudicado a un universo para ver la información.

- **Apply a Filter (Aplicar un filtro)**

Utilice el universo completo o aplique un filtro.

- **Incluir nodo de experiencia**

Experiencia es el primer componente de front-end monitorizado y el principio de la ruta de transacción. Un nodo de experiencia contiene un atributo adicional denominado Experiencia. Si se selecciona Incluir nodo de experiencia, los resultados filtrados incluyen el nodo que muestra donde se inició la transacción.

- **Agrupar por**

Seleccione los atributos de los que desea tener más detalles en la tarjeta de agente.

- **Tipo de gráfico predeterminado**

CPU o memoria dinámica

Número de valores de métrica recopilados/Tiempo de la memoria caché global

### Resumen de los atributos

3. Si desea publicar la tarjeta, seleccione **Hacer que esta tarjeta del agente sea pública**.

#### NOTE

Si no se selecciona esta opción, la tarjeta se mantiene como privada y solamente la podrá ver el usuario. Si selecciona esta opción, la tarjeta se convierte en pública y todos los usuarios que tienen acceso al universo relevante pueden ver la tarjeta.

4. Haga clic en **Guardar**.

Se ha agregado una tarjeta de agente.

### Editar una tarjeta de agente

Se pueden editar las tarjetas de agente. Por ejemplo, si se desea seleccionar diferentes atributos como niveles de la lista desplegable.

#### Siga estos pasos:

1. En Vista de agente, seleccione la tarjeta que desea editar.
2. Haga clic en el botón Configuración de la tarjeta.
3. Haga clic en **Editar tarjeta**.  
Se abre una nueva ventana **Editar tarjeta de agente**.
4. Edite la tarjeta.
5. Haga clic en **Guardar**.

Se ha editado una tarjeta de agente.

### Supresión de una tarjeta de agente

Se pueden suprimir las tarjetas de agente que ya no se desee continuar utilizando.

#### Siga estos pasos:

1. En Vista de agente, seleccione la tarjeta que desea editar.
2. Haga clic en el botón Configuración de la tarjeta.
3. Haga clic en **Editar tarjeta**.  
Se abre una nueva ventana **Editar tarjeta de agente**.
4. Haga clic en **Suprimir tarjeta**.
5. En la ventana emergente de confirmación de la supresión, haga clic en **Suprimir**.

Se ha suprimido una tarjeta de agente.

### Uso compartido de una tarjeta de agente

Como administrador, puede compartir una tarjeta de agente con un usuario dentro de un universo existente.

#### Siga estos pasos:

1. Compruebe que el usuario tiene acceso al universo.
2. En la tarjeta de agente, seleccione **Make This Card Public** (Hacer esta tarjeta pública).  
Aparecerá la tarjeta en la lista de tarjetas.
3. Envíe el vínculo de la tarjeta de agente al usuario.

#### NOTE

Se puede compartir una tarjeta de agente privada con un usuario del mismo universo. El usuario puede ver temporalmente la tarjeta privada.

La página Vista de agentes es una descripción general de toda la información importante del agente y permite que el usuario monitoree el estado y el rendimiento de los agentes que están disponibles en el entorno. Con el agente o la tarjeta de agente, se pueden realizar las acciones siguientes:

- Visualización del estado del agente
- Agregación de una tarjeta de agente
- Editar una tarjeta de agente
- Supresión de una tarjeta de agente
- Uso compartido de una tarjeta de agente

Para obtener más información sobre cómo realizar cualquiera de estas acciones, consulte [Visualización del estado del agente y gestión de tarjetas del agente](#).

## Monitorización de los valores de métrica del agente con la Vista de métrica

Como administrador de APM, puede utilizar la Vista de métrica para obtener una visión general clara de los valores de métrica de agente. Investigue los agentes para ver sus valores de métrica para un intervalo de tiempo determinado.

### Descripción general

DX APM ofrece dos Vistas de métrica:

- **Vista de métrica global:** contiene todas las métricas de todos los agentes que están conectados a la infraestructura de APM durante el intervalo de tiempo seleccionado.
- **Vista de métrica contextual:** muestra un subconjunto de métricas relevante para los componentes seleccionados en el mapa.

Las dos vistas de métrica contienen un árbol de métrica que muestra la métrica y otro tipo de información en formato de árbol. En DX SaaS, las métricas se organizan en la jerarquía `Host | Proceso | Agente`. En DX APM local, las métricas se organizan en una jerarquía `Dominio | Host | Proceso | Agente`.

### Descripción del árbol de métrica

El nivel más alto del árbol representa los hosts del servidor de aplicaciones (DX SaaS) o dominios (DX APM local). El siguiente nivel representa los procesos, seguidos por los agentes instalados en hosts del servidor de aplicaciones individuales. La vista de árbol de agentes, recursos y métricas se actualiza cada 60 segundos para mostrar los datos de métrica actuales.

El Árbol de métrica muestra dos tipos de hosts:

- **Custom Metric Host (Virtual)** (Host de métrica personalizada [Virtual]): Este nodo representa un host virtual que contiene métrica de la que no ha informado un agente determinado. Por ejemplo, aparece métrica agregada bajo este nodo. Este nodo no se corresponde con un equipo host físico.
- **Hosts:** Este nodo representa un equipo que hospeda un agente. Cada nodo de host contiene un nodo de proceso para la instancia de la aplicación monitorizada. Los nodos de proceso a su vez contienen nodos de agente. Los nodos que corresponden a las aplicaciones y a los recursos del sistema y que contienen la métrica se almacenan en los nodos de agente. Los recursos de la aplicación en los nodos del agente difieren en función del tipo de agente (Java o .NET). El nodo de alto nivel representa los siguientes componentes:
  - Componentes de las aplicaciones J2EE o .NET, como servlets, EJB o páginas ASP.
  - Nodos de sistema, incluidos el host que ejecuta el servidor de aplicaciones y el equipo host que ejecuta DX APM.

El Árbol de métrica muestra dos tipos de métrica:



- **Métrica de cadena:** El valor de la métrica es una cadena. El gráfico de métrica solo muestra el valor actual al final del intervalo de tiempo.
- **Métrica numérica:** El gráfico de métrica muestra los valores de métrica, que incluyen los valores máximos y mínimos, la desviación y el historial del estado de la alerta asociada.

### **Visualización de la métrica de agente en la Vista de métrica global**

Es posible visualizar los datos en directo o se puede seleccionar un intervalo de tiempo para consultar los datos históricos. Compare, correlacione y visualice los valores de métrica para un determinado intervalo de tiempo.

#### **Siga estos pasos:**

1. En DX APM, haga clic en **Vista de métrica**, en el panel izquierdo, para abrir la Vista de métrica global. Se abre el árbol de métrica.
2. Seleccione un host de servidor de aplicaciones.
3. Desplácese por el árbol y haga clic en el nodo del agente que desee investigar.

#### **NOTE**

Los agentes desconectados se muestran en gris. Si un agente no envía una métrica durante un tiempo, la métrica se vuelve inactiva y también se muestra en gris.

4. Haga clic en una carpeta del Árbol de métrica para ver la **Descripción general de la métrica**.

La **página de la descripción general de la métrica** consta de las siguientes fichas:

#### – **Gráficos de métrica**

Muestra los valores de la métrica para los nodos seleccionados en el Árbol de métrica.

#### – **Recuento de métricas**

Muestra información resumida de las métricas que se encuentran en las subcarpetas individuales de la carpeta seleccionada.

1. Haga clic en una métrica en el gráfico circular o en la tabla para abrir la subcarpeta relevante.
2. Seleccione la casilla de verificación **Live Metric Only** (Solo métrica en directo) para ver el número de métricas en directo solamente, es decir, las métricas sobre las que está informando el agente ahora mismo.

#### – **Seguimientos**

Muestra la lista de todas las transacciones comerciales asociadas

1. Haga clic en una de las transacciones comerciales de la lista para ver los detalles de los seguimientos y los componentes correspondientes.

#### – **Errores**

Muestra una lista de todas las transacciones comerciales que contienen errores.

1. Haga clic en una transacción comercial para ver los detalles del error.

#### – **Volcados de subprocesos**

Si se selecciona un nodo de agente en el árbol del Explorador de métrica, se muestra **Volcados de subprocesos**. Esta ficha permite recopilar volcados de subprocesos de Java (volcados de subprocesos) y mostrar los datos de los volcados de subprocesos actuales e históricos. Un volcado de subprocesos proporciona información acerca de todos los subprocesos que están en ejecución en una máquina virtual Java en un momento dado. Un volcado de subprocesos proporciona el nombre y el ID de subproceso, el estado, y un seguimiento de la pila, que enumera todos los métodos invocados, para cada subproceso. La ficha Volcados de subprocesos incluye lo siguiente:

- El encabezado muestra la hora del volcado de los subprocesos.
- El panel de búsqueda permite buscar una cadena específica en toda la información del volcado de subprocesos. Los resultados se muestran en la tabla de información de los subprocesos.
- La lista desplegable de estados de los subprocesos filtra la tabla de información de los subprocesos por estado del subproceso. Al seleccionar un estado, se actualiza la tabla de información de los subprocesos.
- La tabla de información de los subprocesos muestra una lista de todos los subprocesos. Cada subproceso proporciona el ID, el nombre y el estado del subproceso, así como el último método invocado por el subproceso inmediatamente antes del volcado de subprocesos.
- La tabla de seguimiento de pilas de subprocesos muestra todos los métodos en el orden en el que se han invocado.
- El gráfico circular Porcentaje de subprocesos por estado muestra los subprocesos en los estados siguientes: Interbloqueado, Bloqueado, En ejecución o En espera.

#### NOTE

Si está realizando una evaluación de problemas para un agente, consulte la métrica `<Nombre_agente> | Threads | Deadlock Count` en el árbol Explorador de métrica. Esta métrica indica si hay subprocesos interbloqueados que afectan al agente. Para activar la métrica Deadlock Count, se debe configurar Introscope. Para obtener más información, consulte [Agente de Java](#).

En la ficha Volcados de subprocesos, se puede realizar lo siguiente:

- **Recopilar nuevo:** Para recopilar un volcado de subprocesos.
- **Guardar como texto:** Para guardar el volcado de subprocesos actual en un archivo de texto.
- **Cargar anterior:** Para cargar un único volcado de subprocesos recopilados previamente y para ver los datos asociados y la marca de tiempo.

No se muestra ningún dato del volcado de subprocesos hasta que se ha recopilado un volcado de subprocesos o hasta que se haya reiniciado una instancia de Enterprise Manager. Para anular la selección de un subproceso en la tabla, mantenga pulsado Ctrl y haga clic en la fila de nuevo.

5. (Opcional) Haga clic en el icono de lupa para buscar métricas específicas en el Árbol de métricas.
  - a. Seleccione **En todas partes** para realizar una búsqueda global o seleccione la opción de la carpeta para realizar una búsqueda local.
6. (Opcional) Para ocultar la métrica que no aporta ningún dato actual al agente, haga clic con el botón derecho del ratón en el nodo del agente y, a continuación, haga clic en **Ocultar las métricas atenuadas**. La métrica ya no aparece en el Árbol de métrica.

#### NOTE

El Árbol de métrica muestra la métrica de nuevo si el agente empieza a recibir los datos actuales de la métrica.

7. Haga clic en una **métrica** como, por ejemplo, **Tiempo medio de respuesta (ms)** para ver sus valores en el gráfico de métrica. Si existe una alerta en la métrica, el gráfico de métrica muestra el historial del estado de la alerta codificado por bandas de colores que indican el estado de la alerta en un momento determinado:
  - **Verde:** Correcto
  - **Amarillo:** Advertencia
  - **Rojo:** Peligro
  - **Sin color:** No existe ninguna alerta para la métrica seleccionada.

#### NOTE

El historial del estado de la alerta aparece en el gráfico de métrica hasta un máximo de 7 días. Si amplía el intervalo de tiempo más allá de 7 días, la información del estado de la alerta no aparecerá.

8. (Opcional) Anule la selección de **Mostrar análisis diferencial** para ocultar la banda de desviación.

**NOTE**

Si la métrica es compatible con el análisis diferencial, una banda resalta automáticamente la desviación dentro de la tendencia de la métrica.

9. (Opcional) Haga clic en **Mostrar núm. mín./máx. de visualización**. Se muestran los valores mínimos y máximos en el gráfico.
10. (Opcional) Seleccione varias métricas en el Árbol de métrica para realizar la comparación en el gráfico de métrica.
  - a. Haga clic en el nombre de métrica fuera de la casilla de verificación para realizar una nueva selección.
  - b. Haga clic en **Combinar** para ver los datos de la métrica en un gráfico.
  - c. Haga clic en **Borrar selección** para seleccionar un conjunto diferente de métricas.

**NOTE**

Puede seleccionar hasta 10 métricas para la comparación en el gráfico de métrica.

11. Utilice la **Escala de tiempo** para seleccionar un intervalo de tiempo específico.
12. Arrastre el puntero sobre el gráfico para acercarse a un intervalo de tiempo más corto.

**NOTE**

La **Escala de tiempo** muestra intervalos dentro de un mínimo de 8 minutos y un máximo de 1 año.

13. Seleccione período de resolución en la lista desplegable **Resolución** (15 minutos, 30 minutos, 1 hora, 2 horas, 6 horas o 12 horas) para ver los valores del período de tiempo. Los posibles valores del intervalo de tiempo son los siguientes: 15 segundos, 30 segundos, 1 minuto, 2 minutos, 5 minutos, 15 minutos, 30 minutos, 1 hora, 2 horas, 6 horas, 12 horas, 1 día, 7 días y 14 días.

**NOTE**

Los valores del intervalo de tiempo de la lista desplegable **Resolución** aparecen en función del intervalo de tiempo seleccionado en la **escala de tiempo**.

14. (Opcional) Comparta la dirección URL con sus compañeros para que puedan ver la misma vista de la métrica específica en el árbol.

**Personalización de los gráficos de métricas**

Se pueden utilizar las siguientes opciones para personalizar el gráfico.

- Seleccione período de resolución en la lista desplegable **Resolución** (15 segundos, 30 segundos, 1 minuto, 2 minutos) para ver los valores del período de tiempo.
- Haga clic en **Combinar** y seleccione **Todo** para ver los datos de la métrica en un gráfico o seleccione **Por nombre** para ver los gráficos de la métrica clasificados por el nombre de la métrica. Esta opción se activa cuando se selecciona más de una métrica en el **Árbol de métrica**.
- Utilice el botón **Elipse** para ver y configurar las siguientes opciones:
  - **Mostrar mínimo y máximo**: seleccione la opción para ver los valores mínimos y máximos en el gráfico.
  - **Combinar**: seleccione más de una métrica en el árbol de métrica y seleccione una opción en Combinar para ver todas las métricas en un gráfico.
  - **Comparación de los intervalos de tiempo**: compare los datos de los gráficos mediante un intervalo de tiempo predefinido o seleccione un intervalo de tiempo personalizado.
  - **Salto de eje**: seleccione la opción para ver los datos desde el intervalo mínimo al máximo en contraposición con la vista predeterminada que muestra los datos de 0 al máximo. Cuando se selecciona la opción Salto de eje, no se pueden ver los datos durante un intervalo de tiempo; por lo tanto, la opción Comparación de los intervalos de tiempo se elimina de la lista desplegable. Además, la opción Salto de eje aparece solamente cuando no se combinan los gráficos de métrica.
  - **Descargar**: seleccione una o más métricas en el árbol de métrica y haga clic en la opción Descargar para descargar los detalles de la métrica en un formato de archivo CSV.

## **Apertura de la Vista de métrica contextual**

Abra la Vista de métrica contextual desde el Mapa o desde el Bloc de notas de análisis para ver un subconjunto de métrica para un nodo específico del mapa.

Para abrir la Vista de métrica contextual desde el mapa, siga los pasos siguientes:

1. En DX APM, haga clic en **Mapa** en el panel izquierdo.
2. En el mapa, seleccione el nodo para el que desea ver la métrica del agente.

### **NOTE**

Si selecciona más de un nodo, el Árbol de métrica une las instancias de métrica que son relevantes para los nodos seleccionados.

3. Haga clic en el panel **Explorador de métrica** para abrir el Árbol de métrica.

Para abrir la Vista de métrica contextual desde el Bloc de notas de análisis, siga los pasos siguientes:

1. En DX APM, haga clic en **Vista de experiencia** en el panel izquierdo.
2. Localice una **tarjeta de experiencia** cuya métrica desee ver y haga clic en **Abrir un bloc de notas de análisis**. Aparece el Bloc de notas de análisis.
3. **Abra** un problema o una anomalía para ver la **Vista de mapa** correspondiente.

### **NOTE**

Si el Bloc de notas de análisis solo muestra un problema o una anomalía, la **Vista de mapa** correspondiente se muestra de forma predeterminada.

4. En el mapa, seleccione el nodo para el que desea ver la métrica del agente.

### **NOTE**

Si selecciona más de un nodo, el Árbol de métrica une las instancias de métrica que son relevantes para los nodos seleccionados.

5. Haga clic en el panel **Árbol de métrica** para abrir el Árbol de métrica.

## **Búsqueda de métricas en el árbol de métricas**

En el **Árbol de métrica**, se pueden buscar métricas específicas o utilizar expresiones regulares para filtrar las métricas necesarias. Además, la barra de búsqueda admite la funcionalidad de búsqueda de texto completo. La barra de búsqueda ahora detecta automáticamente si una entrada tiene el formato de expresión regular y realiza una búsqueda de expresión regular según corresponda.

### **NOTE**

La opción para utilizar expresiones regulares está en desuso.

### **Siga estos pasos:**

1. En DX APM, haga clic en **Vista de métrica**, en el panel izquierdo, para abrir la Vista de métrica global. Se abre el **Árbol de métrica**.
2. Especifique el nombre de la métrica en el cuadro de texto de búsqueda que desee filtrar. La barra de búsqueda detecta si la entrada tiene el formato de expresión regular y realiza una búsqueda en consecuencia.

### **NOTE**

Se puede seleccionar también una frase de búsqueda anterior en la lista desplegable Autocompletar mientras se escribe la frase de búsqueda.

3. Las métricas que coincidan con los criterios de búsqueda se enumeran en el panel derecho.

### **NOTE**

Haga clic en el menú de tres puntos que se muestra a la derecha de la página de resultados de la búsqueda para mostrar u ocultar columnas en la vista de resultados de la búsqueda.

Además, se pueden marcar los elementos del árbol de métrica como favoritos. Esta funcionalidad se extiende hasta las métricas de la gráfica.

#### Siga estos pasos:

1. Para marcar un elemento como favorito, pase el cursor del ratón sobre el elemento en el árbol de métrica. Una estrella aparece en el lado derecho del elemento.
2. Haga clic en el icono de estrella para marcarlo como uno de los favoritos.
3. Al seleccionar **Mostrar favoritos solamente**, se muestran solamente los elementos que se marcan como favoritos.

DX Application Performance Management ofrece dos vistas de métricas: Vista de métrica global y Vista de métrica contextual.

La Vista de métricas proporciona una descripción general clara de los valores de métricas del agente. También ayuda a investigar los agentes para ver sus valores de métrica para un intervalo de tiempo determinado.

Para obtener más información sobre la Vista de métricas, consulte [Monitorización de los valores de métrica del agente con la Vista de métricas](#).

## Incrustación de cuadros de mandos de DX en la Vista de métricas

Se pueden crear cuadros de mandos personalizados en los cuadros de mandos de DX mediante las métricas de APM e incrustarlos en la página Vista de métricas. En la Vista de métricas, el cuadro de mandos incrustado aparece como una ficha si se selecciona cualquier métrica que coincida con la condición.

#### NOTE

De forma predeterminada, los cuadros de mandos Blamepoint y Descripción general del front-end se integran en la Vista de métricas. Estos cuadros de mandos se han configurado previamente y están listos para su uso.

A grandes rasgos, realice lo siguiente:

1. [Creación de un cuadro de mandos](#). Cree el cuadro de mandos, etiquételo y agregue las variables en los cuadros de mandos de DX.
2. [Asignación del cuadro de mandos](#). Asigne el cuadro de mandos que se ha creado anteriormente y la ubicación de las métricas en DX APM a través del mosaico **Cuadros de mandos de DX** en la página **Configuración** de DX APM.
3. [Visualización del cuadro de mandos en DX APM](#).

#### Creación de un cuadro de mandos personalizado en los cuadros de mandos de DX

Cree el cuadro de mandos usando la fuente de datos **AIOPS\_Metrics**. En el generador de consultas, agregue las variables **\$Agent** y **\$Attribute**.

#### Siga estos pasos:

1. Inicie sesión en los cuadros de mandos de DX.
2. Haga clic en **Create > Dashboard** (Crear > Cuadro de mandos) en el panel de navegación izquierdo.
  - a. Haga clic en **Add an empty panel** (Agregar un panel vacío).
  - b. Introduzca el **Panel Title** (Título del panel).
  - c. Seleccione la visualización.
  - d. Genere la consulta:
    - a. Seleccione la fuente de datos **AIOPS\_Metrics**.
    - b. Active **Advanced Query Builder** (Generador avanzado de consultas).
    - c. En la sección **Source Name Specifier** (Especificador del nombre de la fuente),
      - a. Seleccione el especificador como **EXACT**. Es posible también especificar el patrón de expresión regular.
      - b. Especifique el nombre como **\$Agent**.

**NOTE**

Es posible especificar esta variable como **\$Agent** o se puede agregar esta variable con valores. Por ejemplo, puede especificar **\$Agent:SuperDomain\apm\rh7\197\Infrastructure\Agent**.

- d. En la sección **Attribute Name Specifier** (Especificador del nombre del atributo),
  - a. Seleccione el especificador como **EXACT**. Es posible también especificar el patrón de expresión regular.
  - b. Especifique **Pattern** (Patrón) como **\$Attribute**.

**NOTE**

Es posible especificar esta variable como **\$Attribute** o se puede agregar esta variable con valores. Por ejemplo, se puede especificar **\$Attribute: Average Response Time**.

**NOTE**

Además de **\$Agent** y **\$Attribute**, se puede usar una variable personalizada de cualquier nombre.

3. Guarde el cuadro de mandos en la carpeta **APM-MetricView**. Opcionalmente, se puede usar la **carpeta personalizada** para especificar una carpeta diferente para guardar el cuadro de mandos.
4. Etiquete el cuadro de mandos.
  - a. Haga clic en el icono **Settings** (Configuración) para el cuadro de mandos.
  - b. Agregue la etiqueta en la página **General Settings** (Ajustes generales).

**NOTE**

Asegúrese de que la etiqueta sea única.

5. Agregue la variable **\$Agent**:
  - a. Abra la página **General Settings** (Ajustes generales).
  - b. Haga clic en **Variables** en el panel de navegación izquierdo.
  - c. Proporcione la siguiente información:
    - a. **Nombre**: Especifique un nombre para la variable.
    - b. **Tipo**: Seleccione el tipo como **Personalizado**.
    - c. **Values Separated by Comma**: (Valores separados por comas) Introduzca el valor para un agente.
  - d. Haga clic en **Actualizar**.
6. Agregue la variable **\$Attribute**:
  - a. Abra la página **General Settings** (Ajustes generales).
  - b. Haga clic en **Variables** en el panel de navegación izquierdo.
  - c. Proporcione la siguiente información:
    - a. **Nombre**: Especifique un nombre para la variable.
    - b. **Tipo**: Seleccione el tipo como **Personalizado**.
    - c. **Values Separated by Comma**: (Valores separados por comas) Introduzca el valor para cualquier atributo.

**NOTE**

Si se han usado parámetros personalizados, también se deben agregar las variables correspondientes.

7. Haga clic en **Actualizar**.

**Asignación del cuadro de mandos**

Una vez creado el cuadro de mandos, el paso siguiente es asignarlo a través del mosaico **Cuadros de mandos de DX** en la página **Configuración de DX APM**.

**Siga estos pasos:**

1. Inicie sesión en DX Application Performance Management.
2. Haga clic en **Configuración** en el panel de navegación izquierdo.
3. Haga clic en **Cuadros de mandos de DX** en **Ajustes generales**.
4. Haga clic en **Nuevo cuadro de mandos de DX**.
5. Proporcione la siguiente información:

- **Activo:** Active el cuadro de mandos.
  - **Nombre de la ficha:** Introduzca un nombre para la ficha Cuadro de mandos que será visible en la Vista de métricas.
  - **Carpeta del árbol de métrica:**
    - **Expresión de carpeta:** Introduzca la expresión regular de la carpeta de la métrica.
- NOTE**  
Para obtener la ruta completa, vaya a la **Vista de métricas**. Haga clic con el botón secundario en la carpeta en la que está disponible esta métrica y seleccione **Copiar ruta completa como expresión regular**.
- **Métricas secundarias:** Introduzca la métrica que la carpeta de métricas debe contener.
- **Integración de los cuadros de mandos de DX:**
  - **Etiqueta del cuadro de mandos:** Introduzca la etiqueta del cuadro de mandos que se asignará.
  - **Parámetros:** Seleccione los parámetros necesarios:
    - **De:** Indica la hora de inicio actual.
    - **A:** Indica la hora de finalización actual.
    - **Agente:** Indica la ruta del agente seleccionado.
    - **Atributo:** Indica la ruta del atributo seleccionado.
- **Opciones avanzadas:**
  - **Carpeta personalizada:** Si se ha guardado el cuadro de mandos en una carpeta diferente, especifique el nombre aquí. Para la carpeta APM-MetricView, se puede dejar este campo en blanco.
  - **Parámetros personalizados:** Si desea usar los parámetros personalizados, configure los valores siguientes:
    - **Nombre del parámetro:** El nombre del parámetro personalizado.
    - **Expresión regular:** La expresión regular que se usa para ejecutar una búsqueda de coincidencia en la ruta de la carpeta seleccionada. Puede utilizar la captura de grupos (usando paréntesis: ()) o los grupos de captura con nombre (con esta sintaxis: (?<nombre>pattern)).
    - **Valor:** Especifique el grupo que debe utilizarse con el signo \$. Ejemplos: \$1, \$2, \$name.
    - **Valor predeterminado:** El valor predeterminado que se usará si no coincide ningún valor en la ruta de carpeta seleccionada usando la expresión regular.

6. Haga clic en **Guardar**.

Se completó la asignación. Esta página muestra la siguiente información para cada una de las asignaciones:

- Nombre de la ficha
- Condición
- Etiqueta del cuadro de mandos
- Active
- Acciones (ver, editar, suprimir)

### Visualización del cuadro de mandos en la Vista de métricas

Después de asignar el cuadro de mandos a DX APM, el cuadro de mandos incrustado aparecerá como ficha si se selecciona cualquier métrica que coincida con la condición.

#### **Siga estos pasos:**

1. Inicie sesión en DX APM.
2. Abra el mosaico **Cuadros de mandos de DX** en la página **Configuración**.
3. Observe la ruta que se menciona en la columna **Condición** para la ruta al cuadro de mandos.
4. Haga clic en **Vista de métricas** en el panel de navegación izquierdo.
5. Vaya a la ubicación y seleccione la carpeta de métricas.  
El cuadro de mandos se muestra como una de las fichas.



Se pueden crear cuadros de mandos personalizados en los cuadros de mandos de DX mediante las métricas de APM e incrustarlos en la página Vista de métricas. En la Vista de métricas, el cuadro de mandos incrustado aparece como una ficha si se selecciona cualquier métrica que coincida con la condición.

Para crear, asignar y ver un cuadro de mandos personalizado en la Vista de métrica, consulte [Incrustación de cuadros de mandos de DX en la Vista de métricas](#).

## Uso de la escala de tiempo y del resaltado

La escala de tiempo permite ir del modo en directo al pasado para ver qué eventos de estado han ocurrido. El resaltado permite identificar los componentes en el mapa que comparten uno o más atributos.

### Uso de la escala de tiempo

La escala de tiempo permite investigar dónde se ha iniciado un problema. Utilice el control deslizante de escala de tiempo para ver el estado de los componentes seleccionados en los momentos pasados. Cambie eventos para verlos en el intervalo de tiempo seleccionado.

#### Siga estos pasos:

1. Haga clic en **Escala de tiempo**.  
Aparecerá la escala de tiempo. De forma predeterminada, la escala de tiempo está en modo en directo y muestra el resumen de alertas agregadas durante los últimos 8 minutos. El intervalo de tiempo se bloquea y se actualiza cada 30 segundos.
2. Para habilitar el modo **Histórico**, seleccione **EN DIRECTO** y, a continuación, desactive **Actualizaciones en directo**. Seleccione **Aplicar**.  
La sección azul claro de la escala de tiempo muestra el período activo. El mapa muestra el estado y el entorno al final del intervalo de tiempo. Las barras de estado en los nodos muestran los resultados para el período.
3. Cambie el período de tiempo arrastrando y deslizando el período activo en la escala de tiempo.
4. Cambie la escala de la escala de tiempo con la rueda del ratón o el movimiento táctil.
5. Seleccione una hora específica mediante un clic en la parte superior de la escala de tiempo.

#### NOTE

Al hacer clic en la parte superior de la escala de tiempo se cambia la hora de finalización, pero se mantiene el intervalo de tiempo.

Los eventos de estado aparecen como iconos en la escala de tiempo. La vista del bloc de notas filtra los eventos en función del problema o anomalía que se ha seleccionado. Los resúmenes de alerta muestran los resultados correspondientes para el período hasta la hora seleccionada.

#### TIP

Utilice los selectores de tiempo **HORA DE INICIO** u **HORA DE FINALIZACIÓN** para seleccionar una hora específica en cualquier fase.

6. Haga clic en un **nodo** para ver los eventos de dicho nodo en el marco de tiempo seleccionado.
7. Seleccione **Estado**, **Topología** o **Atributo** para incluir estos eventos de cambio en la escala de tiempo.

#### NOTE

La selección del evento de cambio se restablece al abrir el Bloc de notas de análisis.

- a. Haga clic en un **icono de evento** o **de grupo de eventos** para ver los detalles del evento de cambio. Asegúrese de que se ha seleccionado el nodo correcto en el mapa.  
Los nodos que no se ven afectados por los cambios seleccionados aparecen en color gris en el mapa.
- b. Haga clic en un **nodo**.
- c. Haga clic en el **icono de evento de cambio**.  
Los detalles del evento o de la lista cronológica de los eventos del grupo aparecerán en el panel de la derecha.



**NOTE**

La escala de tiempo detecta automáticamente nuevos componentes que se han cargado en APM.

Seleccione **Estado**, **Topología** o **Atributo** para ver los eventos de cambio para los nuevos componentes en la escala de tiempo.

8. Maximice o minimice la escala de tiempo para cambiar la escala.
  - a. Arrastre los deslizadores de inicio y finalización para establecer el intervalo de tiempo necesario.
  - b. Arrastre el intervalo de tiempo activo para los períodos anteriores o posteriores.
  - c. Arrastre la escala de tiempo inactiva (gris) para mover el intervalo visible.  
Si el intervalo de tiempo activo no está visible, haga clic en el valor de tiempo. El marcador final del intervalo de tiempo activo se desplaza hasta la hora seleccionada. Establezca las fechas y horas específicas mediante los selectores de tiempo de la izquierda.
9. Haga clic en un **evento concreto** para ver los nodos afectados en el mapa. Los nodos que no están afectados están en color gris.  
Las barras de estado del nodo muestran el estado agregado para el período de tiempo seleccionado. El mapa muestra el entorno para el período seleccionado.

**Uso del resaltado**

Utilice el resaltado para identificar los componentes en el mapa que comparten uno o más atributos. Una lista muestra los atributos que están disponibles para el resaltado conforme a los atributos de los componentes en la vista de mapa actual.

**Siga estos pasos:**

1. Haga clic en el icono **Mapa** y, a continuación, haga clic en **Resaltado**.  
Se expande una barra resaltada.
2. Haga clic en el icono del signo **más** y seleccione el atributo que desee resaltar.
3. (Opcional) Haga clic en el atributo seleccionado para seguir ordenando o filtrando.  
El mapa muestra el entorno, incluidos los filtros aplicados. El mapa se muestra desde la perspectiva elegida. El valor del atributo seleccionado aparecerá en amarillo.

La escala de tiempo permite investigar dónde se ha iniciado un problema. Utilice el control deslizante de escala de tiempo para ver el estado de los componentes seleccionados en los momentos pasados.

El resaltado permite identificar los componentes en el mapa que comparten uno o más atributos.

Para obtener más información sobre la escala de tiempo y el resaltado, consulte [Uso de la escala de tiempo y resaltado](#).

**Uso de la escala de tiempo y visualización de eventos de cambio**

La escala de tiempo permite ver los eventos de cambio que se producen en la hora actual y los que se han producido históricamente. La escala de tiempo permite investigar dónde se ha iniciado un problema.

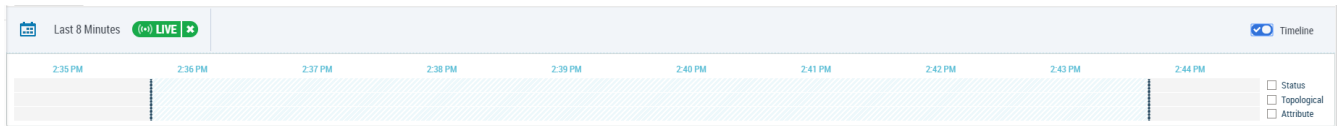
Se puede ver la escala de tiempo en las vistas siguientes:

- Vista de experiencia
- Vista de agente
- Mapa
- Cuadros de mandos
- Vista de métrica

Este artículo incluye los temas siguientes:

## Acciones disponibles en la escala de tiempo

Cuando se activa la alternancia de la **escala de tiempo** en una vista, la escala de tiempo aparece y la sección de color azul claro de la escala de tiempo muestra el período activo. La escala de tiempo se actualiza cada 30 segundos.



Se pueden realizar las siguientes acciones en la escala de tiempo:

### Mover la escala de tiempo

Haga clic en cualquier parte del área gris de la escala de tiempo y arrástrela para ver la hora en el pasado, futuro o la hora actual.

### Cambiar período activo

Se puede seleccionar el área de color azul claro y arrastrarla para ajustar el período de tiempo activo. El período de tiempo activo siempre se encuentra entre la hora actual y la hora pasada.

### Ajustar la escala

Para ajustar la escala activa, seleccione y mueva las barras horizontales que se encuentran al final del período activo. Se puede seleccionar una hora específica haciendo clic en la parte superior de la escala de tiempo o del valor de la hora. Al hacer clic en un valor de tiempo situado en la parte superior de la escala de tiempo se cambia la hora de finalización, pero se mantiene el intervalo de tiempo.

## Visualización de los eventos y los nodos afectados

Se pueden ver los nodos y los eventos afectados mediante la escala de tiempo, el **Mapa** o la **Vista de componente**.

### NOTE

La sección de eventos de la **Vista de componente** aparece solamente cuando se selecciona la casilla de verificación de eventos en la escala de tiempo.

- **Al utilizar la escala de tiempo**

Cuando se selecciona un evento en la escala de tiempo, el nodo en el que se ha producido el evento se resalta en el **Mapa** o en el **Cuadro de mandos** y los nodos restantes aparecen atenuados.

Si el panel **Vista de componente** es visible, los eventos que se seleccionan en la escala de tiempo aparecen resaltados en amarillo en la sección de eventos del panel.

- **Al utilizar el mapa**

Cuando se seleccionan uno o más nodos en el **Mapa**, los eventos correspondientes aparecen en la sección de eventos, *solamente* cuando el panel **Vista de componente** es visible.

- **Al utilizar el panel Vista de componente**

Para realizar cualquier acción en el panel **Vista de componente**, asegúrese de que está visible.

Para los nodos que se seleccionan en el **Mapa**, el panel muestra todos los eventos relacionados en la sección de eventos. Una selección de eventos en la escala de tiempo da lugar a que se resalten en amarillo los eventos correspondientes en la sección de eventos del panel. De forma similar, cuando se selecciona un evento en la sección de eventos del panel, el nodo correspondiente se centra y se resalta en el **Mapa**.

## Visualización de eventos de cambio en la escala de tiempo

En el **Mapa**, **Cuadros de mandos** y las vistas del Bloc de notas, se pueden seleccionar y ver los siguientes eventos de cambio: **Estado**, **Topología** o **Atributo** en la escala de tiempo. La vista del bloc de notas filtra los eventos en función del problema o anomalía que se ha seleccionado. La escala de tiempo detecta automáticamente nuevos componentes que se han cargado en DX APM. Los eventos de cambio están disponibles cuando la escala de tiempo muestra datos históricos o activos. Los eventos de cambio seleccionados aparecen como iconos en la escala de tiempo.



## NOTE

La selección del evento de cambio se restablece al abrir el Bloc de notas de análisis.

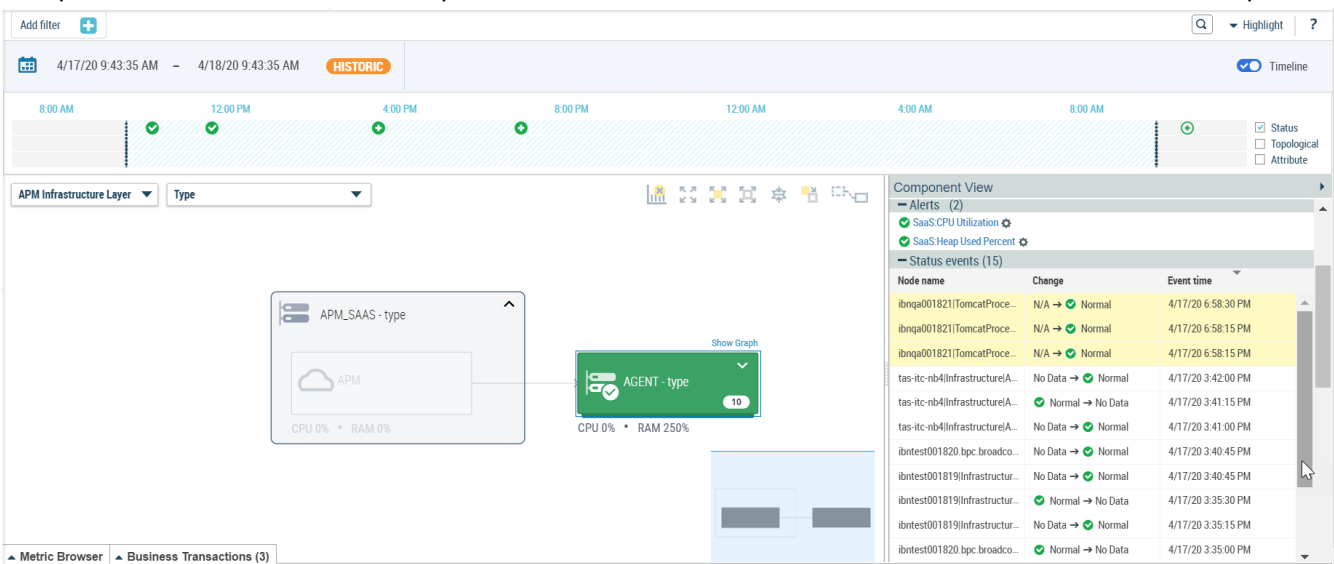
En la vista **Mapa**, los detalles de los eventos están disponibles en la **Vista de componente**.

## Eventos de cambio de estado

En la vista **Mapa** o **Cuadros de mandos**, seleccione un nodo y, a continuación, seleccione la casilla de verificación **Estado** en la escala de tiempo para ver los eventos de cambio de estado.

En la imagen que aparece a continuación, puede ver que se ha seleccionado un nodo en el **Mapa** y que la casilla de verificación **Estado** se ha seleccionado en la escala de tiempo. Como resultado, se pueden ver los eventos de cambio de estado como iconos en la escala de tiempo, que representa la hora en la que se ha producido el cambio de estado para el nodo seleccionado.

Cuando se selecciona un nodo en el **Mapa**, todos los eventos relacionados aparecen en la sección de eventos del panel **Vista de componente**, *solo* si es visible. Se pueden ver los detalles de estado, como cuando el nodo cambió del estado normal a un estado en el que no se ha recibido ningún dato. Y, al seleccionar cualquier evento de la escala de tiempo, se resaltan los eventos en amarillo en la sección de eventos del panel.



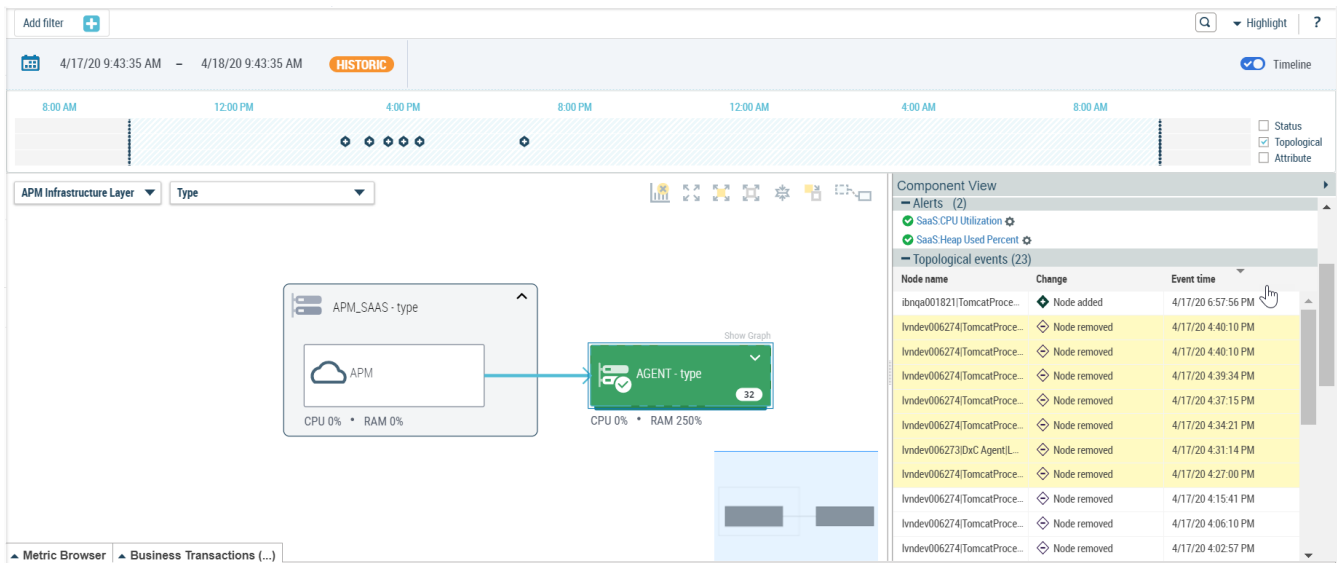
## Eventos de cambio de topología

En la vista **Mapa** o **Cuadros de mandos**, seleccione un nodo y, a continuación, seleccione la casilla de verificación **Topología** en la escala de tiempo para ver los eventos de cambio de topología. Se pueden ver detalles como, por ejemplo, cuando el nodo se eliminó o se agregó a la topología.

En la imagen que aparece a continuación, puede ver que se ha seleccionado un nodo en el **Mapa** y que la casilla de verificación **Topología** se ha seleccionado en la escala de tiempo. Como resultado, se pueden ver los eventos de cambio de topología como iconos en la escala de tiempo, que representan cuándo se produjo el cambio en la topología para el nodo seleccionado.

Cuando se selecciona un nodo en el **Mapa**, todos los eventos relacionados aparecen en la sección de eventos del panel **Vista de componente**, *solo* si es visible. Todos los eventos de cambio de topología que se han producido en el nodo

se enumeran en la sección **Eventos de topología** de la **Vista de componente**. Y, al seleccionar cualquier evento de la escala de tiempo, se resaltan los eventos en amarillo en la sección de eventos del panel.

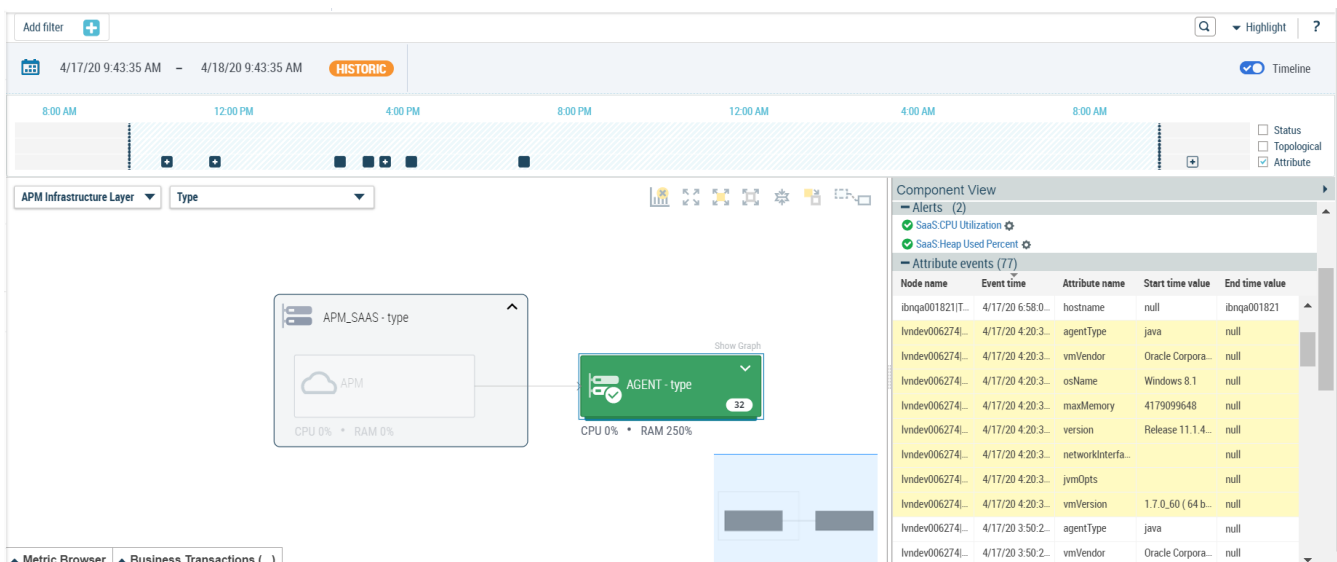


### Eventos de cambio de atributo

En la vista **Mapa** o **Cuadros de mandos**, seleccione un nodo y, a continuación, seleccione la casilla de verificación **Atributo** en la escala de tiempo para ver los eventos de cambio de atributo. Se pueden ver los detalles, como, por ejemplo, cuándo se agregó el atributo, el nombre, el valor al principio y al final.

En la imagen que aparece a continuación, puede ver que se ha seleccionado un nodo en el **Mapa** y que la casilla de verificación **Atributo** se ha seleccionado en la escala de tiempo. Como resultado, se pueden ver los eventos de cambio de atributo como iconos en la escala de tiempo, que representan cuándo se creó el atributo para el nodo seleccionado.

Cuando se selecciona un nodo en el **Mapa**, todos los eventos relacionados aparecen en la sección de eventos del panel **Vista de componente**, solo si es visible. Todos los eventos de cambio de atributo que se han producido en el nodo se enumeran en la sección **Eventos del atributo** de la **Vista de componente**. Y, al seleccionar cualquier evento de la escala de tiempo, se resaltan los eventos en amarillo en la sección de eventos del panel. Para agregar un atributo personalizado, debe estar en el modo en directo.



La escala de tiempo permite ver los eventos de cambio que ocurren en la hora actual y los que ocurrieron históricamente, además de ayudar a investigar dónde comenzó el problema. La escala de tiempo se puede visualizar en las siguientes vistas: Vista de experiencia, Vista de agentes, Mapa, Cuadros de mandos y Vista de métricas.

Para obtener más información sobre las acciones disponibles y ver los eventos de cambio en la escala de tiempo, consulte [Uso de la escala de tiempo y visualización de eventos de cambio](#).

## Utilización de atributos en DX APM

Los atributos son etiquetas que los agentes recopilan de los componentes que se encuentran en el entorno de las aplicaciones. Utilice estos atributos para ver el mapa desde diferentes perspectivas, filtrar los componentes y resaltarlos. Los atributos facilitan la distinción de los componentes e identifican sus relaciones con otros componentes. Cada atributo tiene un nombre y un valor.

DX APM recopila los atributos básicos para cada componente. Los administradores pueden crear atributos personalizados definiendo reglas de atributo. Para obtener más información sobre la creación de atributos personalizados, consulte [Cómo adaptar la monitorización de su entorno con reglas de atributo](#).

### NOTE

Todos los atributos se aplican a DX APM y solo algunos atributos se aplican a la instancia local de DX APM.

### Descripción general

Todos los componentes del mapa contienen un conjunto de atributos. DX APM distingue los siguientes tipos de atributo:

- **Atributos comunes:** DX APM los recopila automáticamente y existen para la mayoría de los componentes.
- **Atributos personalizados:** Permiten definir y recopilar más información utilizando reglas de atributo.
- **Atributos de agente:** Proporcionan información sobre componentes específicos que los agentes instalados monitorizan.
- **Atributos de extensión:** Proporcionan más información que las extensiones del agente recopilan.

Los atributos que están disponibles para su uso en filtros y perspectivas aparecen en la lista desplegable de atributos.

### NOTE

#### Más información:

- [Organización de los componentes utilizando perspectivas](#)
- [Identificación de las áreas de interés mediante filtros](#)
- [Monitorización del estado general del entorno con el cuadro de mandos](#)

### Atributos comunes

DX APM recopila los siguientes atributos comunes:

- `name`  
Define el nombre del componente. Este atributo se deriva de uno o más atributos.
- `type`  
(Vértice)  
Indica el tipo de componente del vértice.
- **Clúster de origen** : Define el clúster de APM al que informa el componente.
- `agent`  
Define el identificador del agente (`hostname|process|agentName` ). Este atributo muestra el origen del vértice.
- `hostname`

Define el nombre del host o contenedor en el que se ejecuta el componente.

- `agentDomain`

Define el dominio del agente.

- `processedBy`

Indica el nombre de clase que ha procesado y creado este componente. Normalmente, este atributo se origina en un seguimiento de la transacción.

- `applicationName`

Define el nombre de la aplicación. Busque `applicationName` en la descripción de la implementación de la aplicación web o busque en la ruta de la métrica del agente `Frontends|Apps|<applicationName>`.

- `containerId`

(Docker) Indica el ID del contenedor de Docker. `containerID` es visible en la capa de la aplicación.

### NOTE

Este ID solo está presente si el Agente de Java, Node JS, PHP o Python se ejecuta dentro del contenedor.

- `remotePort`

Indica el puerto remoto al que llama el componente.

- `backendNode`

Se muestra como `true` si el vértice es el componente de back-end en una aplicación.

- `remoteName`

Indica el nombre de host remoto al que llama el componente.

- `localAddress`

Define la dirección IP local del componente.

- `serviceId`

Identifica el servicio empresarial que se define en CEM.

- `Experience`

Indica el nombre de la experiencia tal y como se muestra en la Vista de experiencia. Por ejemplo, "Apps|ActivityService|URLs|api/v1/ on serv17.ca.com (GENERICFRONTEND)". Este atributo existe solamente si el valor del atributo `IsExperience` es `true`. Para obtener más información sobre las experiencias, consulte [Monitorización del rendimiento utilizando la Vista de experiencia](#).

- `IsExperience`

Indica que el vértice es una experiencia o el componente situado más a la izquierda en el mapa. Para obtener más información sobre las experiencias, consulte [Monitorización del rendimiento utilizando la Vista de experiencia](#).

- `remoteAddress`

Indica la dirección IP remota a la que llama el componente.

- `inferredBackendNode`

Se muestra como `true` si el vértice se infiere de una o más conexiones a este componente de back-end.

- `provider`

Indica el proveedor o distribuidor de la base de datos como, por ejemplo, "Postgres DB" "Oracle DB" o "Derby DB".

- `port`

Indica el puerto en el que escucha la base de datos o Enterprise Manager (EM).

### Atributos personalizados

Los administradores pueden crear atributos personalizados en componentes para que los usuarios puedan ver las perspectivas y filtrar el mapa de acuerdo con los componentes que comparten un nombre de atributo. Se puede agregar un atributo personalizado a un componente individual o a una regla de atributo. Los atributos personalizados permiten que los usuarios identifiquen los componentes fácilmente y los relacionen. A continuación, los analistas ven perspectivas y filtran el mapa según los componentes que comparten el nombre de atributo. Application Performance Management

permite filtrar por cualquier valor de atributo. Los atributos asignados a los componentes de una capa específica de DX APM también están visibles en otras capas.

#### NOTE

##### Más información:

- [Cómo adaptar la monitorización de su entorno con reglas de atributo](#)
- [Capas del mapa](#)

#### Atributos del agente

Los Agentes de Java y Node.js solo recopilan los atributos comunes.

#### Atributos de la extensión

Las extensiones del Agente de la infraestructura recopilan atributos para componentes específicos de la infraestructura. Consulte los siguientes vínculos para obtener una lista completa de los atributos de extensiones disponibles.

#### NOTE

##### Más información:

- [Amazon Web Services](#)
- [Atributos de Azure](#)
- [Atributos de Docker](#)
- [Configuración de los atributos personalizados de Docker](#)
- [Atributos y métricas de F5 LTM](#)
- [Atributos de monitorización del host](#)
- [Atributos de Kubernetes](#)
- [Atributos de OpenShift](#)

Los atributos son etiquetas que los agentes recopilan de los componentes que se encuentran en el entorno de las aplicaciones. Utilice estos atributos para ver el mapa desde diferentes perspectivas, filtrar los componentes y resaltarlos. Los atributos facilitan la distinción de los componentes e identifican sus relaciones con otros componentes. Cada atributo tiene un nombre y un valor.

Para obtener más información sobre los atributos, consulte [Uso de atributos en DX APM](#).

## Organización de los componentes utilizando perspectivas

Las perspectivas permiten agrupar los componentes en el **Mapa** y en el **cuadro de mandos** sin eliminarlos del conjunto de datos. Se pueden crear perspectivas personales que son exclusivas de los universos. Seleccione uno o más atributos compartidos para agrupar los componentes. Los administradores de DX APM pueden editar y crear perspectivas públicas adicionales que están disponibles para todos los usuarios. Las perspectivas listas para su uso (OOTB) visualizan los componentes de la infraestructura y de la aplicación para las pilas de tecnología y para los servicios de alojamiento que se encuentran en el entorno de la aplicación.

#### Descripción general

La lista desplegable Perspectivas se encuentra en el **mapa** y en el **cuadro de mandos**. El marco muestra la perspectiva que está actualmente aplicada. Expandir la lista desplegable para ver las perspectivas definidas.

- Las perspectivas personales aparecen por encima de la línea.
- Las perspectivas públicas, que define el administrador, aparecen debajo de la línea.
- Las perspectivas listas para usar que muestran las relaciones entre los componentes de las distintas capas aparecen por debajo de la línea. Las perspectivas siguientes están definidas como perspectivas listas para usar:

Capa del mapa	Perspectivas listas para usar							
Capa de la aplicación	Type	Valor predeterminado	Hostname	Usuario final, Aplicación	Location	Propietario	Jenkins	Infraestructura de la aplicación
Capa de la infraestructura de APM	Type							
Capa de la infraestructura	Type	Valor predeterminado						
Capa de red	Type							

La última perspectiva de la lista desplegable siempre es **No hay perspectiva**, la cual muestra todos los componentes por separado. Combine una perspectiva con filtros para eliminar los componentes no deseados del **mapa** y del **cuadro de mandos**.

#### NOTE

La perspectiva predeterminada de la capa de la aplicación no comparte los mismos atributos con la perspectiva predeterminada de la capa de la infraestructura.

#### Utilización de las perspectivas listas para su uso

Utilice las perspectivas listas para su uso para ver componentes de la aplicación y sus componentes de la infraestructura asociados.

#### Siga estos pasos:

1. Vaya al **Mapa** o al **Cuadro de mandos**.
2. Vea los componentes de la infraestructura y de la aplicación.  
Para ver los componentes de la infraestructura para un componente específico de la aplicación:
  - a. Seleccione **Capa de la aplicación** en la lista desplegable de la parte superior.
  - b. Seleccione la lista desplegable **Perspectivas** y, a continuación, seleccione **Infraestructura de la aplicación**.

#### NOTE

Si el entorno de la aplicación utiliza contenedores de Docker, seleccione esta perspectiva para ver los contenedores, los hosts y las instancias del servidor asociados de Docker.

- c. Seleccione un componente de la aplicación en el **mapa** o el **cuadro de mandos** para ver los componentes de la infraestructura relacionados.
3. Para obtener más información sobre un componente, vaya a **Vista del componente**, la cual se abre junto al **mapa**.  
Se ha utilizado una perspectiva lista para usar para ver las relaciones de los componentes de las distintas capas.

#### Creación de una perspectiva personal


Las perspectivas permiten agrupar componentes del mapa de acuerdo a un atributo determinado. Los componentes que comparten un valor para ese atributo aparecen en el mapa en grupos discretos. Por ejemplo, la perspectiva **Location** tiene tres grupos:



- Todos los componentes con el valor `London`
- Todos los componentes con el valor `Prague`
- Todos los componentes con el valor `New York`

Los usuarios individuales crean y personalizan grupos de perspectivas personales.

#### Siga estos pasos:

1. En el panel izquierdo, seleccione **Perspectivas**.
2. Seleccione **Crear una perspectiva**.
3. Nombre la perspectiva.
4. Seleccione cada **capa aplicable** en la que desea que se muestre la perspectiva.
5. (Opcional) En **Visibilidad**, active las opciones necesarias:
  - (Opcional) Seleccione la casilla **Pública** para activar los derechos de visibilidad para otros usuarios.
  - Seleccione la casilla **Agrupación automática** para cambiar los vértices del mapa a grupos predeterminados.
6. En la **Jerarquía de la agrupación**, seleccione al menos un atributo.  
 Haga clic en **Agregar atributo** para aplicar atributos adicionales para agrupar los vértices. Tenga en cuenta que cada atributo se puede agregar solamente una vez.  
 Si se ha activado la opción **Agrupación automática**, la agrupación predeterminada se aplica primero a los vértices, seguida de los atributos seleccionados en la sección **Jerarquía de la agrupación**. Los atributos de la sección **Jerarquía de la agrupación** se aplican en orden descendente. Si elimina cualquier atributo, la lista se reorganiza y, a continuación, los atributos se aplican en el nuevo orden descendente.  
 Haga clic en el botón  frente a un atributo y arrastre y suelte para ordenar o cambiar los atributos de la jerarquía. El orden de los atributos es importante, ya que define el orden en el que se aplicarán los filtros y, por lo tanto, la agrupación de vértices.

#### NOTE

Los atributos aparecen en la capa correspondiente. Se pueden seleccionar atributos desde capas que no se han seleccionado como **capas aplicables** para una perspectiva determinada.

7. (Opcional) Cree un grupo de perspectivas de varios niveles. Seleccione otros atributos.
8. Seleccione **Guardar**.

La perspectiva aparece en la lista desplegable **Perspectivas** de la vista **Mapa** cuando se ha seleccionado la capa correspondiente.

#### Personalización de una perspectiva pública

El administrador crea grupos de perspectivas públicas. Estos grupos están disponibles para todos los usuarios de APM. Se puede personalizar una perspectiva pública.

#### Siga estos pasos:

1. En el panel izquierdo, seleccione **Perspectivas**.
2. Identifique la perspectiva pública que desea personalizar y seleccione **Editar**.  
Aparecerá una ventana emergente.
3. (Opcional) Cambie el nombre de la perspectiva.
4. (Opcional) Seleccione una capa diferente o agregue más capas en las que desea que se muestre la perspectiva.  
Para obtener más información, consulte [Capas del mapa](#).
5. En la **Jerarquía de la agrupación**, seleccione al menos un atributo.
6. (Opcional) Cree un grupo de perspectivas de varios niveles. Seleccione otros atributos.
7. (Opcional) Seleccione el símbolo **Más (+)** para agregar más atributos al grupo de perspectivas.
8. Seleccione **Guardar**.

Se ha personalizado una perspectiva pública. La nueva perspectiva creada es personal. La perspectiva personal se puede editar o suprimir. La perspectiva aparece en la lista desplegable **Perspectivas** en el **mapa**.

### Edición de una perspectiva personal

**Siga estos pasos:**

1. En el panel izquierdo, seleccione **Perspectivas**.
2. Seleccione la perspectiva personal y, a continuación, seleccione **Editar**. Aparecerá una ventana emergente.
3. (Opcional) Cambie el nombre de la perspectiva.
4. (Opcional) Seleccione una capa diferente o agregue más capas en las que desea que se muestre la perspectiva. Para obtener más información, consulte [Capas del mapa](#).
5. En la **Jerarquía de la agrupación**, seleccione al menos un atributo.
6. (Opcional) Cree un grupo de perspectivas de varios niveles. Seleccione otros atributos.
7. (Opcional) Seleccione el símbolo **Más (+)** para agregar más atributos al grupo de perspectivas.
8. Seleccione **Guardar**.

Se ha editado la perspectiva personal.

### Supresión de una perspectiva personal

**Siga estos pasos:**

1. En el panel izquierdo, seleccione **Perspectivas**.
2. Identifique la perspectiva personal y seleccione **Suprimir**.
3. Aparecerá una ventana emergente de confirmación. Seleccione **Sí**.

Se ha suprimido la perspectiva personal.

Las perspectivas permiten agrupar los componentes en el Mapa y en el cuadro de mandos sin eliminarlos del conjunto de datos. Se pueden crear perspectivas personales que son exclusivas de los universos. Seleccione uno o más atributos compartidos para agrupar los componentes. Los administradores de DX APM pueden editar y crear perspectivas públicas adicionales que están disponibles para todos los usuarios.

Para obtener más información sobre las perspectivas, consulte [Organización de los componentes utilizando perspectivas](#).

## Visualización de las relaciones de los componentes en el mapa

El mapa utiliza componentes como los nodos, las alertas, el panel de detalles y la descripción general del rendimiento. Los grupos de componentes muestran la información de estado agregado para todos los componentes de ese grupo. El mapa muestra las relaciones entre los componentes individuales dentro del entorno. El paciente cero es el primer componente en una serie de dependencias que indica cuáles son los problemas de rendimiento. Este componente parece ser el origen de la degradación del rendimiento en su entorno de aplicaciones.

### Mapa

El mapa muestra el estado de alerta, el nombre y el tipo de icono para cada componente. DX APM recopila la información de Enterprise Manager y la muestra en cada nodo.

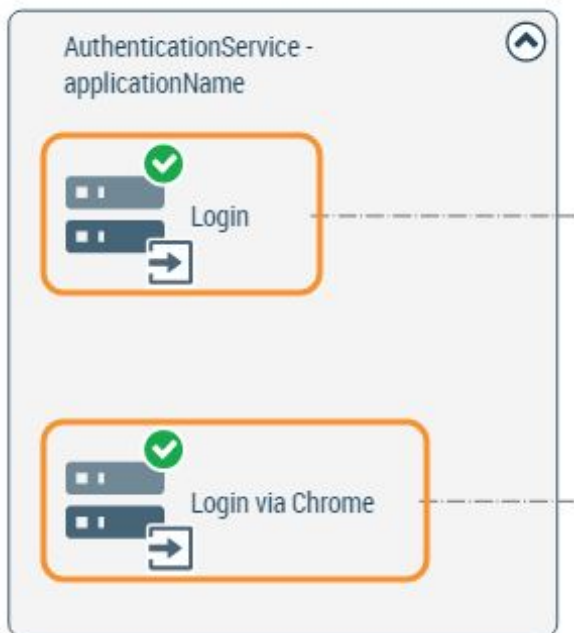
Diversas opciones le permiten limitar el enfoque del mapa, por ejemplo, se puede:

- Seleccionar distintas perspectivas para ver el mapa.
- Utilizar filtros para centrarse en componentes específicos.
- Utilizar la Vista de componentes para ver alertas, métrica y atributos para cada nodo en el mapa. Seleccione las fichas para ver la información de otras capas del mapa.
- Utilizar la escala de tiempo para comparar la información actual con la histórica. La escala de tiempo muestra los marcadores que aparecen cuando se han producido cambios en alertas, topología y atributos. Estos cambios se podrán inspeccionar. Se calcula la información sobre el período de tiempo especificado en la escala de tiempo. En el modo en directo, el período de agregación es de 8 minutos.

DX APM es compatible con Permalink, que contiene todos los detalles de la página que se ve en la dirección URL. Puede enviar la dirección URL de la página a otro usuario. Ese usuario, a continuación, ve la misma vista. También puede marcar estas direcciones URL para volver a la misma vista en una sesión posterior.

### Front-end como una experiencia

El nodo de la experiencia es el primer componente del front-end monitorizado y contiene un atributo que se llama Experiencia. El nodo de la experiencia es el principio de la ruta de la transacción. Una experiencia puede ser, por ejemplo, un servlet o un front-end genérico. El mapa muestra un nodo de la experiencia con un icono de flecha. El ejemplo muestra un nodo de la experiencia llamado *Login* y un nodo de la experiencia llamado *Login via Chrome*.



#### NOTE

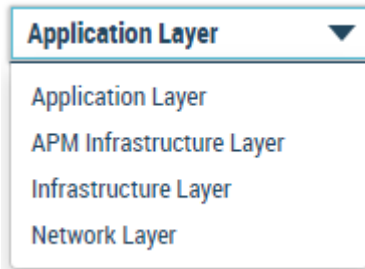
No todos los front-ends son una experiencia. La mayoría de nodos del front-end aparecen en medio de una transacción, por lo que no son experiencias.

### Comprensión del mapa

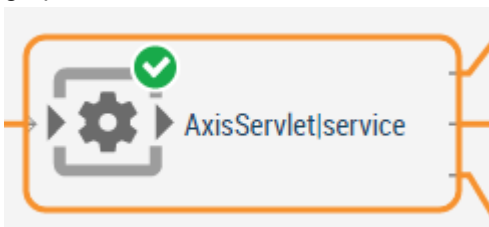
Utilice el siguiente flujo de trabajo de ejemplo para obtener información sobre el mapa. De forma predeterminada, el mapa se actualiza para mostrar la nueva topología cada 5 minutos. Esta función es configurable. Los nuevos componentes se muestran con un borde azul y los componentes eliminados se muestran con un borde de puntos azul.

**Siga estos pasos:**

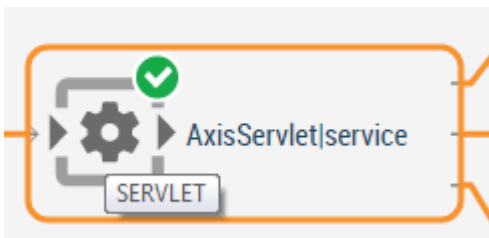
1. Seleccione **Capa de la aplicación** para ver los componentes en el mapa. Los componentes se corresponden con las tarjetas de experiencia en la Vista de la experiencia.



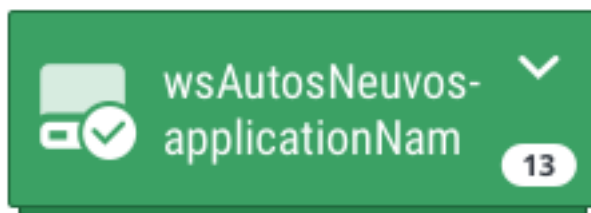
2. Explore los nodos y pase el puntero del ratón por encima de un nodo para ver más información. El nodo es una representación de las transacciones comerciales y de los componentes de software agregados o monitorizados directamente en contexto topológico. El mapa es compatible con 50000 nodos. Si el número de nodos que se va a mostrar en el mapa es lo suficientemente grande como para provocar problemas de rendimiento, el mapa agrupa automáticamente los nodos. Los grupos no representan ningún atributo o perspectiva específicos. De forma predeterminada, la agrupación automática se produce cuando el número de nodos que se debe mostrar está por encima de 150. Agregue filtros o defina perspectivas para reducir el número de nodos que va a mostrar el mapa. La gráfica de estado muestra el último estado al final del intervalo seleccionado que se notifica para ese componente o grupo.



Para averiguar qué tipo de dispositivo representa un nodo, pase el puntero del ratón sobre el icono situado junto al nombre de dispositivo.

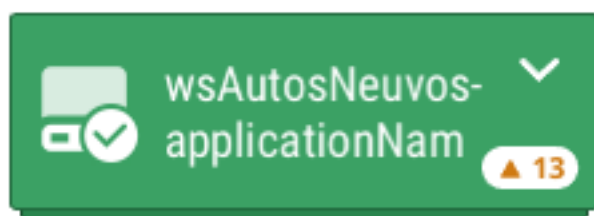


En el ejemplo siguiente, un grupo de nodos comparte el atributo `applicationName`.



75 tx/min • 324 seconds

- El número 13 indica que el grupo incluye 13 nodos.
  - "75 tx/min" indica el número de respuestas por intervalo.
  - "324 seconds" indica el tiempo medio de respuesta.
3. Identifique las conexiones:
- Las conexiones del mapa pueden contener componentes del back-end.
- APM reconoce las siguientes conexiones:
- **Línea sólida:** Un componente del back-end existe en la conexión. Seleccione la conexión para consultar las propiedades del componente del back-end en la vista del componente.
  - **Línea discontinua gris:** No existe ningún componente del back-end en la conexión. La conexión no es seleccionable.
  - (Solo Capa de la infraestructura) **Línea de puntos gris:** La línea entre dos nodos indica que el primer nodo contiene el segundo nodo.
  - (Solo Capa de la infraestructura) **Línea gris:** La línea entre dos instancias de Docker indica que la primera se relaciona con la segunda.
- El color de la línea completa indica el estado de alerta del componente de back-end:
- **Línea gris:** No hay ninguna alerta definida en el componente de back-end.
  - **Línea verde:** Todas las alertas del componente de back-end son verdes.
  - **Línea amarilla:** Al menos existe una alerta amarilla y ninguna roja en el componente de back-end.
  - **Línea roja:** Al menos existe una alerta roja en el componente de back-end.
  - **Línea naranja:** La línea indica un seguimiento de la transacción.
4. Agrupe los componentes en la capa seleccionada para buscar problemas de rendimiento para los componentes compartidos de la infraestructura (componentes de capa cruzada).
- El color del icono de grupo indica el estado de alerta del componente entre varias capas:
- **Icono gris:** Al menos existe un alerta verde para el componente de capa cruzada que agrupa los componentes de la capa seleccionada.
  - **Icono rojo:** Al menos existe una alerta roja para el componente de capa cruzada que agrupa los componentes de la capa seleccionada.
  - **Icono amarillo:** Al menos existe un alerta amarilla para el componente de capa cruzada que agrupa los componentes de la capa seleccionada.
- En el ejemplo siguiente, los grupos de agentes comparten un host. El número 13 indica 1 componente de host y 12 componentes de agente. El triángulo naranja representa una aplicación en un estado de precaución:



5. Pase el puntero del ratón sobre un componente para ver el seguimiento de la transacción.
- El seguimiento de la transacción muestra todos los componentes a los que una transacción se vincula a lo largo del flujo. Pase el puntero del ratón sobre un nodo de la experiencia para ver toda la ruta resaltada de la transacción.
6. Cambie entre las capas del mapa.
- Seleccione **Capa de la infraestructura de APM** para ver los agentes y Enterprise Manager en el mapa. La vista se corresponde a la Vista de agentes. Utilice esta vista si, por ejemplo, desea ver qué Enterprise Manager se está

ejecutando y qué agentes están conectados. Cuando se obtienen detalles desde una tarjeta del agente en la vista de aislamiento, el mapa muestra la Capa de la infraestructura de APM.

- Seleccione **Capa de la infraestructura** para ver la infraestructura de la red del entorno incluidos los Monitores de Docker.

#### NOTE

Para obtener más información sobre las capas del mapa, consulte [Capas del mapa](#).

7. Seleccione **Explorador de métrica** para abrir la Vista de métrica.

### **Investigación de las transacciones comerciales**

La vista del mapa ayuda a encontrar componentes para monitorizarlos. En la ficha Transacciones comerciales, puede ver los detalles y los resúmenes relacionados con el de seguimiento de la transacción. Esta información le ayudará a comprender el rendimiento de la transacción y a solucionar un problema de rendimiento pobre identificando cuándo, dónde y por qué se degrada el rendimiento.

#### **Siga estos pasos:**

1. Seleccione nodos individuales o grupos de nodos para un máximo de 1000 nodos.
2. Haga clic en la ficha **Transacciones comerciales**.  
Los seguimientos que se corresponden con el componente aparecen en una lista de resumen para el intervalo que se selecciona en la escala de tiempo. Los seguimientos muestran las horas de duración. Los seguimientos están codificados por colores para indicar cualquier problema que se asocia con una transacción como, por ejemplo, el color rojo indica un error. Se pueden identificar métodos problemáticos según la duración del seguimiento. Los seguimientos que son largos inesperadamente pueden ser la causa probable de las transacciones lentas.

#### NOTE

La lista se actualiza automáticamente cuando se utiliza el modo en directo.

3. [Investigación del rendimiento de las transacciones con errores](#).

#### NOTE

##### **Más información:**

- [Organización de los componentes utilizando perspectivas](#)
- [Identificación de las áreas de interés mediante filtros](#)
- [Monitorización del rendimiento utilizando la Vista de experiencia](#)

El mapa utiliza componentes como nodos, alertas, panel de detalles y la descripción general del rendimiento para mostrar las relaciones entre los componentes individuales dentro del entorno. Los grupos de componentes muestran la información de estado agregado para todos los componentes de ese grupo.

Para obtener más información sobre el mapa y su relación con los componentes, consulte [Visualización de las relaciones de los componentes en el mapa](#).

### **Capas del mapa**

Como administrador, se puede navegar rápidamente por las capas del mapa para identificar la causa raíz de los problemas de rendimiento. Alterne entre las capas de la asignación para ver los problemas de rendimiento causados por los componentes de la aplicación, de los componentes de la infraestructura o de los componentes de DX APM. Aplique más filtros para ver los tipos específicos de los componentes de las capas. Ajuste el número y los tipos de componentes en grupos fáciles de usar (Universos).

### **Descripción general**

Asigne distintos tipos de componentes de superposición de capas del mapa desde el entorno hacia el mapa. El mapa muestra componentes y conexiones para los componentes que están dentro de la capa seleccionada. Las conexiones

entre los componentes de las distintas capas se denominan conexiones entre capas. Los componentes que tienen conexiones entre capas a los componentes que se encuentran dentro de la capa seleccionada aparecen en la **Vista del componente** de la parte derecha. Por ejemplo, cuando se selecciona un componente de servlet en el mapa, la **Vista del componente** muestra las propiedades del servlet, junto con las propiedades para el agente que monitoriza el servlet. Las conexiones entre capas también pueden verse en el mapa utilizando filtros de atributos entre capas. Para obtener más información, consulte [Cómo adaptar la monitorización de su entorno con reglas de atributo](#).

#### NOTE

DX APM agrega automáticamente varias conexiones de capas entre los agentes y los componentes de la aplicación que monitorizan los agentes.

### Uso de las capas del mapa

Alterne entre las capas del mapa para ver los componentes de una capa específica. Seleccione un componente en el mapa y consulte las conexiones entre capas en la **Vista del componente**.

#### Siga estos pasos:

1. Seleccione una capa del mapa en la lista desplegable. Elija entre las capas siguientes:
  - **Capa de la aplicación**  
Muestra los componentes de la aplicación que monitorizan los agentes de APM. Esta capa se corresponde con los componentes de asignación de versiones anteriores de APM.
  - **Capa de la infraestructura de APM**  
Muestra los componentes de APM, por ejemplo, los agentes y los recopiladores.
  - **Capa de la infraestructura**  
Muestra los hosts, las instancias de docker y otros componentes físicos. Esta capa contiene información sobre los Agentes de la infraestructura y sus extensiones. La capa de la infraestructura también recopila información a partir de las integraciones, por ejemplo, Unified Infrastructure Management (CA UIM).

#### NOTE

DX APM local permite integrar componentes de otros sistemas en la capa de la infraestructura mediante la API de REST. CA UIM utiliza dicha API de REST para integrarse con DX APM local, de modo que DX APM local muestre los componentes de hardware.

- **Capa de red**  
Muestra los elementos de red en la nube, como la nube privada virtual (VPC), los enrutadores, las interconexiones, las subredes y otros elementos de VPC en la nube. Esta capa contiene información de los Agentes de la infraestructura y sus extensiones en la nube.

#### NOTE

Para ver los servicios de monitorización de las extensiones en la nube de GCP en la capa de red, configure los servicios GCP como la nube privada virtual de Google, Google Cloud Interconnect y los servicios Google Cloud Router. Para obtener más información, consulte [Configuración de la extensión de Google Cloud Platform](#).

2. Seleccione un componente en el mapa para abrir la **Vista del componente**.
3. Alterne entre las fichas en la **Vista del componente** para ver las propiedades para los componentes seleccionados y para los componentes conectados desde otras capas.

### Aplicación de filtros en las capas del mapa

Un filtro es una lista de atributos y valores obligatorios que permiten visualizar componentes específicos de la asignación. Aplique un filtro para ver todos los componentes de la capa de filtrado que coinciden con los atributos de filtro. Si se alterna entre las capas, los componentes que tienen conexiones entre capas hacia los componentes filtrados permanecen visibles en la asignación.

Para aplicar un filtro al mapa, seleccione un atributo de filtro en la lista de atributos.

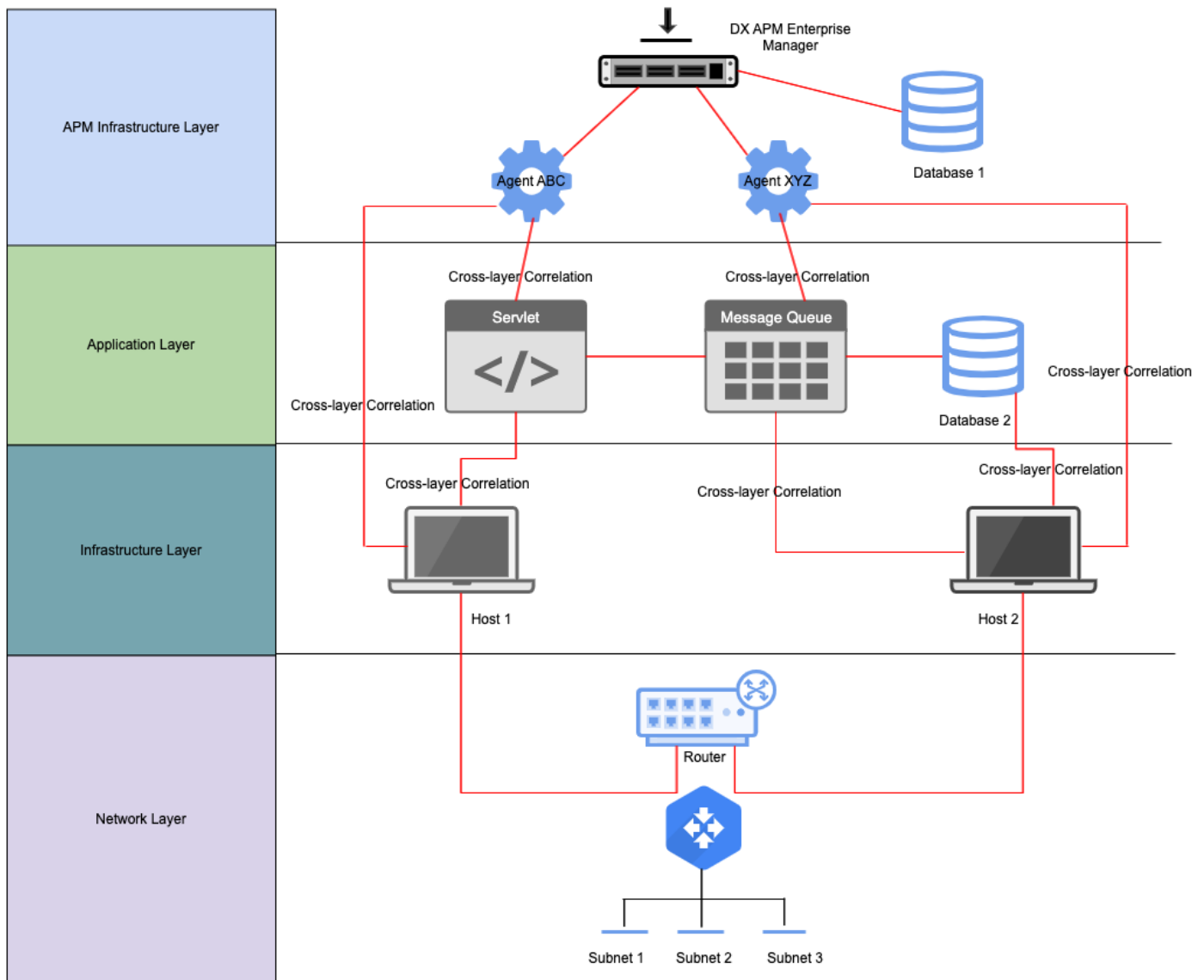
### NOTE

Los atributos aparecen en la capa correspondiente. Se pueden seleccionar atributos de más de una capa.

### Ejemplo:

El siguiente diagrama muestra una asignación sin filtrar que contiene varias conexiones entre capas:

**Figure 6: maplayers1**

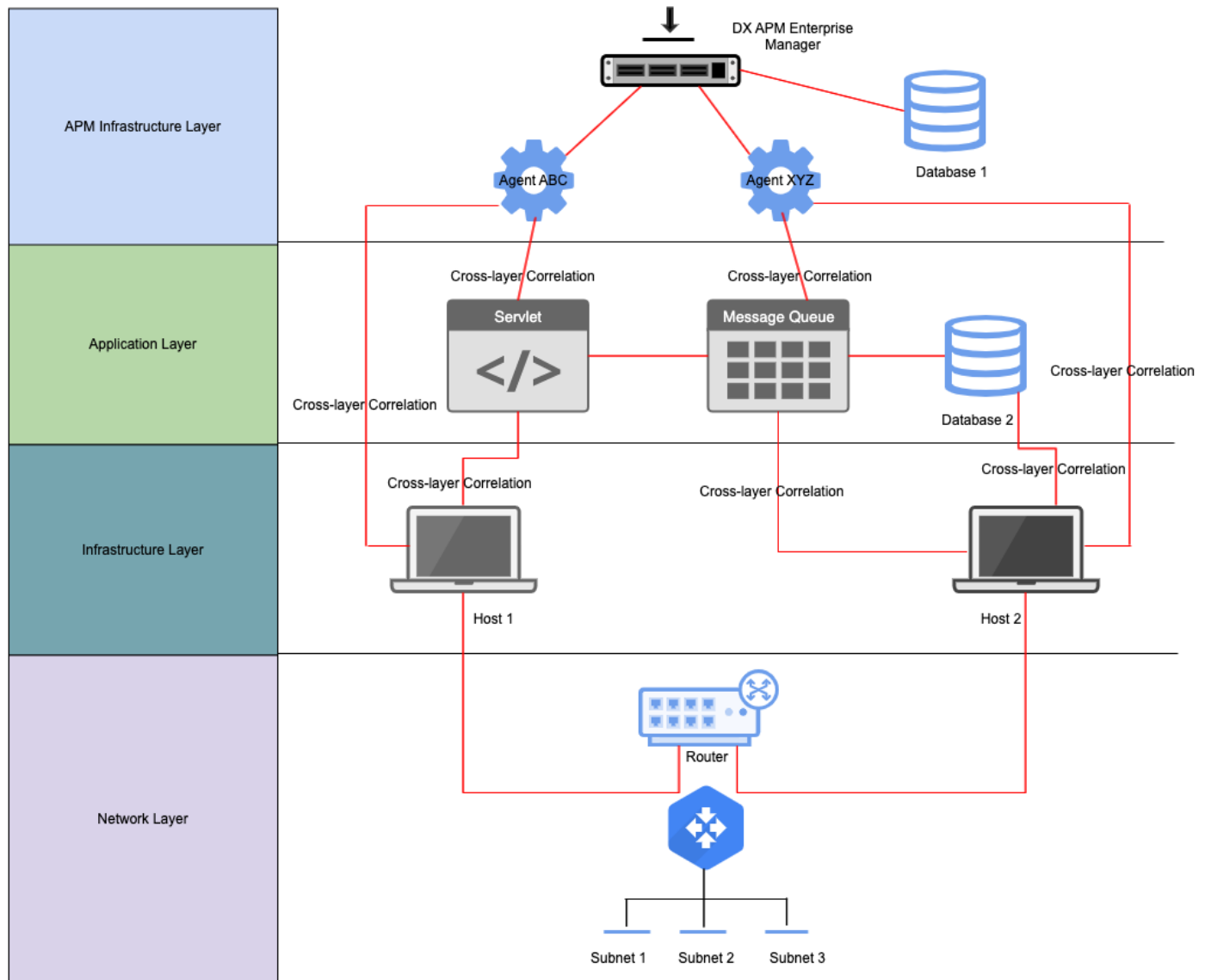


### Acción:

En la capa de la infraestructura de APM, establezca el filtro para devolver los agentes que contengan "ABC" y "XYZ" en sus nombres.

**Resultado:** el siguiente diagrama muestra los resultados filtrados para cada capa del mapa:





## NOTE

La capa de la infraestructura de APM no muestra recopiladores ni bases de datos de EM cuando la capa de filtrado es la capa de aplicación. Los recopiladores y las bases de datos de EM no tienen conexiones entre capas hacia los componentes de la aplicación. Solo los componentes de tipo de agente disponen de conexiones entre capas hacia la capa de aplicación.

## Aplicación de universos en las capas del mapa

Después de configurar un filtro para seleccionar componentes específicos, se puede guardar el filtro como un universo. Autorice a los usuarios para que accedan a todos los componentes del universo, incluyendo los componentes que tienen conexiones entre capas hacia los componentes seleccionados. Para obtener más información sobre la configuración de universos, consulte [Configuración de universos](#).

Los ejemplos siguientes muestran usos posibles de filtros en las capas del mapa.

### Ejemplo 1: Captura de transacciones completas que pasan a través de un dominio específico

Este universo contiene las transacciones monitorizadas completas que pasan por un dominio seleccionado, incluidos los componentes deducidos back-end y los nodos de transacciones comerciales. Este universo también contiene todos los agentes que monitorizan los componentes de la aplicación.

**Siga estos pasos:**

1. Seleccione la **capa de la aplicación** como la capa de filtrado.
2. Seleccione **Agregar filtro** y seleccione **SEGUIR LA RUTA DE LA TRANSACCIÓN**.
3. Seleccione **agentDomain** en la lista de atributos.
4. Introduzca el nombre **agentDomain** en el **filtro** para encontrar las transacciones de ese dominio.

### **Ejemplo 2: Concesión de acceso de administrador a todos los recopiladores y agentes de EM y bases de datos de EM desde un dominio específico**

Este universo contiene los componentes necesarios desde la capa de la infraestructura de APM, junto con los componentes de la aplicación dicho que monitorizan los agentes dentro del dominio especificado. Los resultados no las transacciones de negocio ni las back-end deducidas porque los agentes no monitorizan estas transacciones.

**Siga estos pasos:**

1. Seleccione **Capa de la infraestructura de APM** como la capa de filtrado.
2. Haga clic en **Agregar filtro** y seleccione el atributo **agentDomain**.
3. Introduzca el nombre **agentDomain** en el **filtro**.
4. Seleccione **+** para agregar un nuevo elemento de filtro y seleccione **Agregar un grupo de filtros nuevo**.
5. Seleccione **Tipo** de la lista de atributos.
6. Seleccione todos los valores de atributo excepto el **AGENTE**, por ejemplo, **EM\_COLLECTOR**, **EM\_DATABASE** y otros.

El mapa muestra componentes y conexiones para los componentes que están dentro de la capa seleccionada. Las capas del mapa permiten identificar la causa raíz de los problemas de rendimiento. Se puede alternar entre las capas de la asignación para ver los problemas de rendimiento causados por los componentes de la aplicación, de los componentes de la infraestructura o de los componentes de DX APM.

Para obtener más información sobre las capas del mapa, consulte [Capas del mapa](#).

## **Identificación de las áreas de interés mediante filtros**

Los filtros permiten limitar la búsqueda de componentes por nombre y valor del atributo. Los filtros eliminan información del conjunto de datos que muestra el cuadro de mandos y el mapa. Utilice filtros para identificar áreas de interés mientras se monitoriza su entorno. Filtre los grupos de componentes no afectados para simplificar el cuadro de mandos y el mapa para la monitorización y la Evaluación de errores asistida. Los filtros son acumulativos y funcionan de izquierda a derecha. Puede filtrar los resultados de un filtro con otro. Se pueden generar capas de filtros para desplazarse por áreas específicas de un entorno. Los filtros son persistentes entre el cuadro de mandos y el mapa.

Application Performance Management tiene las siguientes funciones de filtro:

- Filtrar siguiendo una ruta de la transacción
- Filtrar componentes por cualquier atributo
- Aplicar varios grupos de filtros
- Incluir el nodo de experiencia en el resultado del filtro
- Arrastrar y soltar filtros individuales a través de los grupos de filtros

### **Filtrado de grupos y filtros de atributos**

Un grupo de filtros define el conjunto de nombres de atributo y valores que se muestran en el mapa y en el cuadro de mandos. Se eliminan todos los demás componentes del conjunto de datos. Dentro de un grupo único de filtros, cada condición de filtro adicional reduce el conjunto de nodos resultante que aparece. Un filtro de atributo elimina todos los

componentes del conjunto de datos que no tienen valores y nombres de atributo en la condición del filtro. Un filtro de la ruta de la transacción elimina todos los componentes del conjunto de datos que no tienen valores de ruta de la transacción en la condición del filtro.

- Los filtros de dentro de un grupo único de filtros se combinan con un operador Y. Cada condición de filtro puede ser un filtro de atributo o un filtro de la ruta de la transacción. Agregue un grupo de filtro para incluir un segundo conjunto de datos filtrados en el mapa y en el cuadro de mandos.
- Distintos grupos de filtro se combinan con un operador O. El mapa muestra todos los nodos que cumplen con los criterios del grupo de filtros 1 y todos los nodos que cumplen con los criterios del grupo de filtros 2.

Puede arrastrar y soltar las condiciones de filtro para editar los grupos de filtros. Si arrastra y suelta un filtro de la ruta de la transacción entre grupos de filtros, el filtro se convierte en un filtro de atributo. No se pueden mover los filtros de la ruta de la transacción entre grupos de filtros. Se puede editar el filtro y seleccionar la casilla de verificación **Seguir la ruta de la transacción** para activar los seguimientos de transacciones.

Puede cambiar el orden de los filtros utilizando arrastrar y soltar. Puede cambiar el orden de los filtros, moverlos entre grupos de filtros y moverlos dentro o fuera de los filtros de la ruta de la transacción. La única limitación es que no se puede mover el filtro de la ruta de la transacción como un todo. Si mueve la condición del último filtro fuera del marco del filtro de la ruta de la transacción, desaparece el marco.

#### NOTE

##### Más información:

- [Cómo adaptar la monitorización de su entorno con reglas de atributo](#)

### Establecimiento de un filtro de la ruta de la transacción

Application Performance Management genera datos de mapa realizando muestras de los seguimientos de la transacción. Existe un registro de cada ruta de la transacción que pasa por cualquier componente.

#### NOTE

La identificación de todas las transacciones en entornos de gran tamaño puede conducir a generar un gran número de vértices que pueden afectar al rendimiento. Para evitar expansiones de datos en entornos de gran tamaño, se puede desactivar esta función.

Un filtro de la ruta de la transacción identifica todos los componentes de todas las rutas de la transacción con valores de atributo que se especifican en los criterios del filtro. Por ejemplo, desea ver en el mapa todas las transacciones que pasan por cualquier componente que tiene el atributo de ubicación de París. Si configura un filtro de la transacción para la ubicación de París, el mapa muestra todos los componentes de las transacciones que pasan por los nodos de París.

#### NOTE

Se toman rutas de la transacción desde el nodo de experiencia, que es el primer componente monitorizado de front-end y el principio de la ruta de la transacción. Un nodo de experiencia contiene un atributo adicional denominado Experiencia. Si una transacción se bifurca en cualquier etapa, los filtros de la ruta de la transacción identifican todos los componentes de la transacción. Los filtros de la ruta de la transacción también identifican las ramas bifurcadas sin tener en cuenta dónde se encuentra el atributo especificado en la transacción.

### Siga estos pasos:

1. Seleccione **Agregar filtro**, agregue los criterios del filtro y seleccione **Seguir la ruta de la transacción**.
2. (Opcional) Seleccione la casilla de verificación **Incluir nodo de experiencia**. El nodo de experiencia es el primer componente de front-end monitorizado y el inicio de la ruta de la transacción. El atributo Experiencia en los filtros contiene el nodo de experiencia incluidos todos los demás nodos en la ruta de la transacción. Si se selecciona **Incluir el nodo de experiencia**, se agregan todos los nodos de experiencia que utilizan los nodos filtrados.

**TIP**

Se pueden eliminar manualmente nodos concretos. Asigne un atributo personalizado al nodo y, a continuación, filtre por ese atributo.

Se ha establecido un filtro de la ruta de la transacción.

**Creación de un grupo de filtros****Siga estos pasos:**

1. Seleccione el icono del signo más junto a un filtro.  
Aparecerá una lista desplegable de nombres de atributo.
2. (Opcional) Seleccione **Seguimiento de la ruta de la transacción**.
3. Seleccione un nombre de atributo para filtrar.

**NOTE**

Los atributos aparecen en la capa correspondiente.

4. Vuelva a seleccionar el icono del signo más. Seleccione **Agregar nuevo grupo de filtros** y, a continuación, seleccione un nombre de atributo para filtrar.
5. Seleccione la lista desplegable de la condición del filtro y desactive los valores del atributo que desea eliminar con el filtro.  
Los iconos de estado situados junto a los valores de filtro indican el estado de los componentes asociados solo en el modo en directo.
6. (Opcional) Agregue más criterios de filtro. Seleccione el icono del signo más dentro del marco azul y agregue más nombres de atributo a la condición del filtro de la ruta de la transacción.

Se ha creado un grupo de filtros.

**TIP**

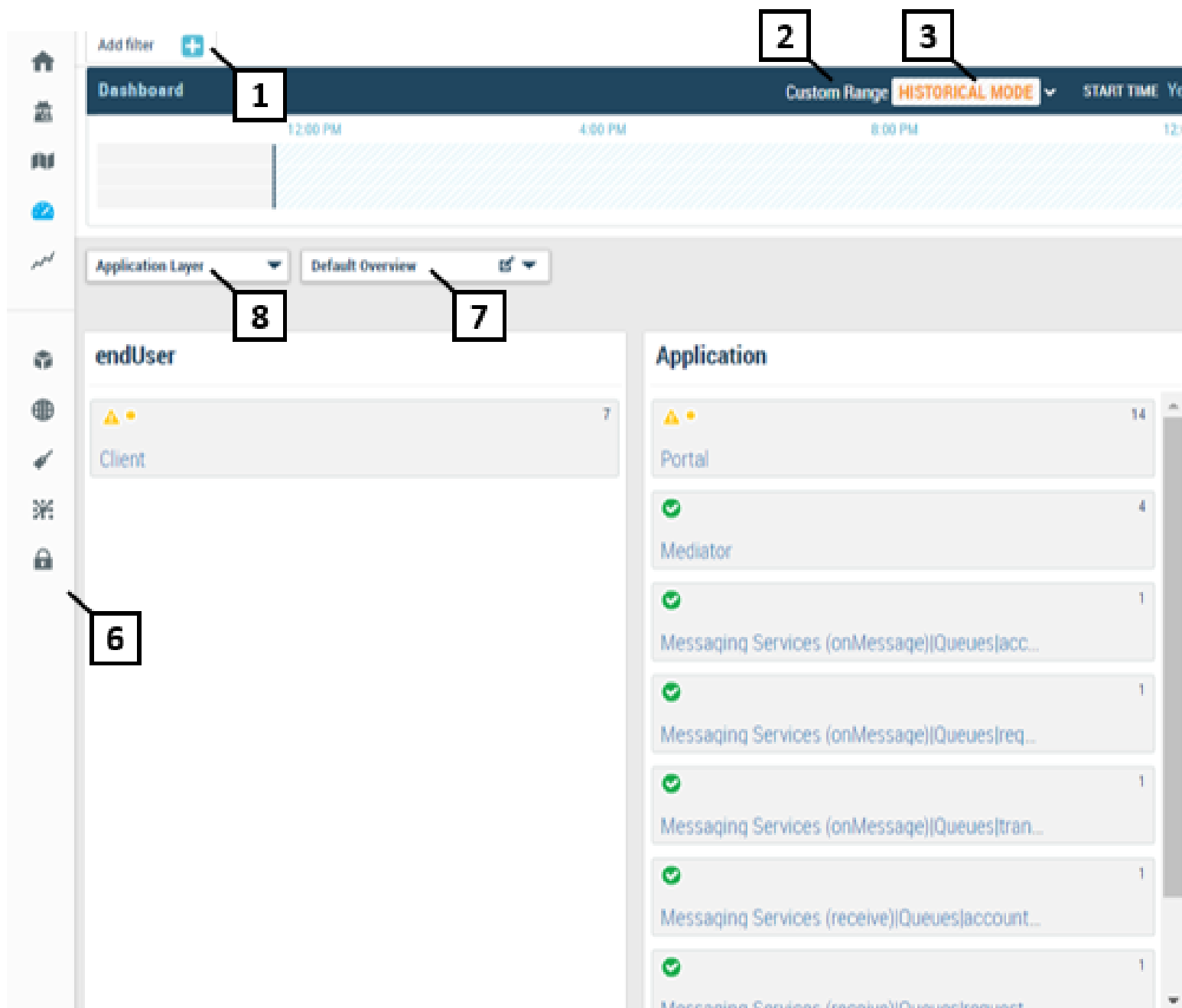
Si decide editar el grupo de filtros más tarde, guarde la dirección URL en primer lugar. Puede utilizar la dirección URL para volver a la configuración anterior del grupo de filtros.

## Monitorización del estado general del entorno con el cuadro de mandos

DX APM proporciona una descripción general de un entorno de aplicación. El cuadro de mandos muestra el estado general del entorno. Un mosaico representa un grupo de todos los componentes que comparten un nombre de atributo y un valor. Los mosaicos muestran el análisis diferencial más significativo y el estado de las alertas de cualquiera de los componentes del grupo.

**Descripción general**

Los mosaicos del cuadro de mandos se organizan en columnas. Cada columna representa un atributo de la perspectiva seleccionada. El nombre del atributo aparece en el encabezado de la columna. Cada mosaico de una columna muestra el estado de todos los componentes que tienen un valor de atributo específico.



La siguiente leyenda identifica cada elemento del mapa con un número y proporciona más información:

Número	Name	Más información
1	Filtro	
2	Intervalo de tiempo	Haga clic para seleccionar un intervalo de tiempo personalizado o establecido anteriormente.
3	Modo de escala de tiempo (histórico o en directo)	

4	Expandir o contraer la escala de tiempo	Seleccione <b>Estado</b> , <b>Topología</b> o <b>Atributo</b> para ver los eventos de cambio en la escala de tiempo. <b>Nota:</b> De forma predeterminada, la escala de tiempo se carga sin una selección de eventos de cambio.
5	Vínculo de la ayuda en línea	
6	Panel de navegación	
7	Perspectivas	Una perspectiva agrupa lógicamente los componentes en función de sus atributos compartidos.
8	Capas	Las capas muestran los componentes que se corresponden con las vistas de Application Performance Management como, por ejemplo, Vista del agente y Vista de la experiencia.
9	Estado de alerta	Las alertas muestran el estado de cualquiera de los componentes del grupo. La intensidad de la alerta en el cuadro de mandos refleja la intensidad del estado de alerta. El estado de alerta se basa en información adicional procedente de las alertas. Los factores incluyen cuánto tiempo se ve afectado el nodo y por cuánto excede la métrica asociada los umbrales. La escala tiene cinco grados del bajo al alto. Cuando no hay ningún grado, significa que no hay suficientes datos para tomar una conclusión.
10	Mosaico	Los mosaicos del cuadro de mandos representan grupos de componentes que comparten un nombre de atributo y un valor. El mosaico muestra el análisis diferencial más significativo y los resultados del estado de alerta para cualquier componente del grupo. El valor del atributo es el encabezado del mosaico. Este encabezado es un vínculo seleccionable. Haga clic en este vínculo para ver este grupo en el mapa.
11	Número de mosaicos en este grupo	

### **Visualización de las capas en el cuadro de mandos**

Las capas le permiten aplicar las vistas estándares de Application Performance Management al cuadro de mandos como, por ejemplo, Vista del agente y Vista de la experiencia. Alterne entre las capas siguientes en el cuadro de mandos:

- **Capa de la aplicación**  
Muestra los componentes en el mapa. Los componentes se corresponden con las tarjetas de experiencia en la Vista de la experiencia.
- **Capa de la infraestructura de APM**  
Muestra los Enterprise Manager y los agentes en el cuadro de mandos. Esta capa se corresponde a la Vista de agente.
- **Capa de la infraestructura**

Muestra la infraestructura de red del entorno incluidos los Monitores de Docker.

### Visualización de las perspectivas en el cuadro de mandos

Una perspectiva es un modo de agrupar componentes en las vistas de Application Performance Management que se basa en los atributos compartidos. Las perspectivas permiten agrupar los componentes del cuadro de mandos sin eliminarlos del conjunto de datos. Para obtener más información sobre las perspectivas, consulte [Organización de los componentes utilizando perspectivas](#).

DX Application Performance Management proporciona una descripción general de un entorno de aplicaciones. El cuadro de mandos muestra el estado general del entorno. Un mosaico representa un grupo de todos los componentes que comparten un nombre de atributo y un valor. Los mosaicos muestran el análisis diferencial más significativo y el estado de las alertas de cualquiera de los componentes del grupo.

Para obtener más información sobre el cuadro de mandos, consulte [Monitorización del estado general del entorno con el cuadro de mandos](#).

## Monitorización de los problemas y las anomalías de la Evaluación de errores asistida

Aparecerá información sobre eventos interesantes como problemas y anomalías (historias) en la Vista de la experiencia o en el Bloc de notas de análisis. La Experiencia es un componente en el entorno donde se inicia una transacción. La Evaluación de errores asistida recopila pruebas para detectar posibles problemas o problemas iniciales en el entorno. La recopilación de las pruebas puede producirse en una primera etapa en la que la prueba no señala aún a ninguna experiencia afectada. Esta evidencia se llama *anomalía*. Cuando la Evaluación de errores asistida tiene información suficiente para identificar las experiencias afectadas, la evidencia se llama *problema*. Las anomalías son como los problemas, pero sin provocar ningún impacto en el usuario.

La Vista de experiencia o el Bloc de notas de análisis proporciona ubicaciones adecuadas para monitorizar todo el sistema. En la aplicación, se producen muchos eventos distintos continuamente, pero muchos eventos pueden no interesar al usuario. La Evaluación de errores asistida ayuda a identificar y priorizar los problemas informando sobre eventos significativos en el sistema de la aplicación. Estos eventos significativos aparecen como historias con titulares en la Vista de experiencia o en el Bloc de notas de análisis y explican los aspectos siguientes:

- Cuál es el problema probable
- A quién afecta el problema
- A quién podría afectar el problema (potencial)
- Qué componentes están implicados en el problema
- Qué tipos de eventos se han producido para los componentes que están implicados en el problema
- Cuándo se ha iniciado este problema y cuándo ha finalizado

Como una página de periódico real, puede echar un vistazo a los titulares periódicamente a lo largo del día. Es el nivel de interés para una experiencia en línea directa con el ámbito de sus responsabilidades como analista. Por ejemplo, uno o varios de los casos siguientes pueden indicar que un problema o una anomalía requiere su atención:

- El ámbito del impacto del cliente es grave. A menudo la Evaluación de errores asistida evalúa el impacto con la información de WHO.
- No se ha especificado el ámbito del impacto del cliente o, de lo contrario, la experiencia es confusa. Por ejemplo, si la información de WHERE indica una aplicación o transacción claves, es posible que deba investigar más.

### Siga estos pasos:

1. Haga clic en el botón **Vista de experiencia**.

La Vista de la experiencia muestra tarjetas de experiencias individuales. Todas las tarjetas muestran un resumen. Este resumen representa el qué (WHAT) y explica el por qué (WHY). Los elementos rojos indican áreas de interés como por ejemplo transacciones con errores.

2. Explore la página y haga clic en el icono **Abrir el Bloc de notas de análisis** en una tarjeta de interés. Los problemas y las anomalías aparecen en el panel Evaluación de errores asistida. El motor de la Evaluación de errores asistida identifica las transacciones que comparten componentes que tienen un mal rendimiento.

#### NOTE

Al obtener detalles de una tarjeta de experiencia de una vista a la otra, las historias Evaluación de errores asistida podrán cambiar de problemas a anomalías. Una transacción comercial puede mostrar un problema y cero anomalías. Cuando se obtienen detalles a partir de una tarjeta de experiencia, una nueva tarjeta puede mostrar cero problemas y una anomalía.

Este comportamiento ocurre porque una historia de la Evaluación de errores asistida puede ser un problema para una de las transacciones comerciales y una anomalía para la otra. Una de las transacciones comerciales que ha experimentado un problema oculta las otras transacciones comerciales para mostrarlas como anomalías. Cuando se intentan obtener detalles para una sola transacción comercial, se podrá ver la anomalía que estaba oculta en la vista anterior.

3. Examine el panel y lea los detalles sobre un problema o una anomalía de interés. Haga clic en el botón **Abrir** para un problema o una anomalía.

El flujo de relaciones muestra las rutas de las transacciones de las experiencias seleccionadas. Este mapa proporciona el contexto para el evento que se ha producido, especialmente el dónde (WHERE). APM *solo* muestra el subconjunto del mapa de la aplicación entera dónde está el problema o anomalía. Por ejemplo, es posible que proporcione detalles sobre cuánto tiempo ha durado el problema y a qué componentes ha afectado. El causante aparece en el panel Evaluación de errores asistida y en el mapa.

#### TIP

Utilice la lista desplegable **Perspectiva** y cree o seleccione una perspectiva. Puede utilizar perspectivas para agrupar los componentes en función de sus atributos compartidos.

El mapa del flujo de relaciones reducirá la vista.

4. En el panel Evaluación de errores asistida, expanda **Duración**, **Experiencias afectadas** o **Componentes de la aplicación** e investigue la causa raíz del problema. Haga clic en **Abrir** para ver la evidencia contribuyente.
5. [Continúe la investigación utilizando las diversas opciones que se encuentran en el Bloc de notas de análisis.](#)

## Evaluación de errores asistida y analistas

La Evaluación de errores asistida es un motor y generador de historias. La Evaluación de errores asistida identifica los eventos más significativos que se han producido en los sistemas ocupados y proporciona información contextualizada (historias) sobre estos eventos. Estas historias aparecen como problemas y anomalías con titulares. La naturaleza fiable e inteligente de las historias que genera la Evaluación de errores asistida le mantiene totalmente informado del estado del dominio de monitorización.

### Cómo funciona la Evaluación de errores asistida

La Evaluación de errores asistida crea problemas y anomalías sobre los eventos en el sistema. La Evaluación de errores asistida reacciona a los siguientes tipos de eventos:

- Detenciones
- Errores
- Alertas
- Tiempos de respuesta inestables

Los problemas y las anomalías explican los aspectos de uno o más eventos. Por ejemplo, estos aspectos incluyen:

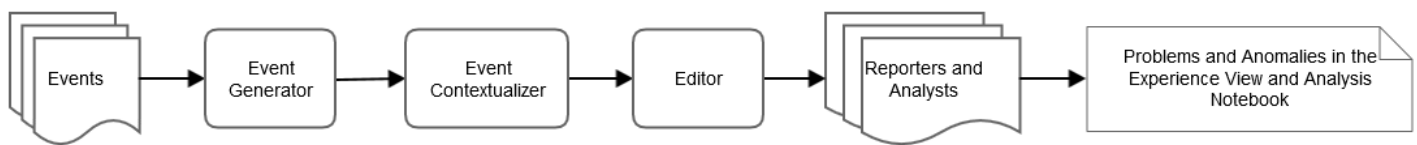


- WHAT resume el evento que incluye cualquier causa sospechosa (WHY). Esta información aparece como un titular para un problema o una anomalía en la Vista de la experiencia y Bloc de notas de análisis.
- WHERE localiza la aparición de un evento, por lo general información como el nombre de host y del agente. WHERE puede tener más detalles cuando está disponible.
- WHO identifica las transacciones que se ven afectadas o que se pueden ver afectadas. Este aspecto también determina cuántas transacciones se ven afectadas.
- WHEN registra la aparición de un evento; normalmente el inicio y final de un evento de detención, un evento de errores o una inestabilidad.
- WHY explica la aparición de un evento. Por ejemplo, la siguiente instrucción explica un problema de tasa alta de llamadas:

```
Potential high call ratio from ViewOrders|service to 138.0.0.1_7080|getService 2 in the order of 214980
```

El siguiente diagrama y los pasos correspondientes describen cómo funciona la Evaluación de errores asistida:

**Figure 7: Arquitectura de evaluación de errores asistida**



1. Se producen eventos en el sistema APM como la intensidad de variación, errores, detenciones, alertas APM, etc. Un evento contiene posibles sospechosos de la causa del problema.
2. Un generador de eventos recopila los datos de eventos de distintas fuentes y envía los datos al procesador de eventos.
3. El contextualizador de eventos recibe los eventos de generadores en un clúster, procesa los eventos y recopila todos los eventos relacionados en un contexto. La información del contexto incluye el impacto potencial del componente situado más a la izquierda y todas las transacciones que suceden en el componente. El contextualizador transmite esta información de contexto al editor.
4. El editor realiza un seguimiento de los distintos contextos y asigna un generador de informes por contexto del evento específico para su análisis.
5. Los generadores de informes conocen los distintos tipos de analistas que están disponibles en el sistema y ejecutan el contexto a través de cada analista. Los analistas analizan el contexto para los tipos de eventos, patrones y posibles repercusiones y, a continuación, cada analista crea una instrucción. Los analistas trabajan juntos para registrar pruebas o crear historias de las instrucciones y después almacenan los datos en la base de datos de APM. Las historias se borran definitivamente de la base de datos cuando son anteriores a 62 días.
6. Las historias aparecen como problemas o anomalías en la Vista de la experiencia y Bloc de notas de análisis.

#### NOTE

Enterprise Manager genera y recopila métricas sobre los componentes de la evaluación de errores asistida. Estas métricas de compatibilidad son útiles para evaluar el estado de Enterprise Manager.

### **Analistas**

Los analistas son como médicos especialistas que saben cómo diagnosticar determinadas clases de enfermedades. La Evaluación de errores asistida utiliza los siguientes tipos principales de analistas. Cada tipo de analista incluye a otros analistas concretos.

Los *analistas de eventos* buscan determinados tipos de eventos y crean instrucciones de eventos que sirvan como pruebas. Estos son unos ejemplos de analistas de eventos:

- Un analista de análisis diferencial busca la intensidad de la variación
- Un analista de errores busca los eventos de error en los contextos
- Un analista de eventos de recursos monitoriza los eventos de alerta en los recursos del sistema

Los *analistas de patrones* buscan determinados patrones en el contexto y crean instrucciones de patrones. Estas instrucciones son una parte del resumen de la historia. Estos son unos ejemplos de analistas de patrones:

- Un analista predeterminado determina el componente más profundo en un contexto (según el mapa de relaciones). Al analista predeterminado también se le conoce como el Identificador de zona.
- Un analista de tasa alta de llamadas busca el componente más profundo en un contexto determinado (según el mapa de relaciones). Este analista observa si el componente llama a los nodos del tipo de back-end una cantidad inusual de veces.

Las instrucciones de los analistas forman un resumen de la historia.

### **Ejemplo de historia: Analista predeterminado (Identificador de zona)**

Este ejemplo explica la historia de un analista predeterminado (o Identificador de zona). Este analista funciona siempre si otros analistas concretos buscan patrones. El analista predeterminado identifica una zona probable. La zona puede ser un front-end, un back-end o un componente interno entre ellos. Por ejemplo, una instrucción del analista predeterminado aparecerá como este titular:

```
Problem isolated to {type} {component}
```

{type} puede ser un front-end, una transacción comercial, un componente interno o un back-end.

{component} es el nombre del componente implicado en la zona.

Por ejemplo, tenga en cuenta los siguientes componentes en el sistema:

- Front-end F
- Back-end B
- Componente interno M

Todos estos componentes están relacionados por poseer una transacción comercial: F->M->B.

Se produce la siguiente secuencia de eventos en el flujo de transacciones:

1. Aparecen solo los eventos que están relacionadas con el front-end F.  
La historia del analista predeterminado informa de un evento aislado al front-end F.
2. Se produce un evento para el componente interno M.  
El analista predeterminado relaciona estos dos eventos debido a que se encuentran en el mismo flujo de transacciones. El analista indica: problema aislado en el componente interno M.
3. Se produce un evento para el back-end B.  
El analista predeterminado combina los tres eventos e indica: problema aislado en el back-end B.

Busque las anomalías y problemas en la Vista de la experiencia y Bloc de notas de análisis para obtener un titular que incluya un tipo y un componente, por ejemplo:

```
Problem isolated to internal component AxisServlet|service
```

Este titular describe una historia del analista predeterminado. Por ejemplo, los detalles pueden describir un problema en la zona entre las transacciones front-end y back-end de la aplicación ACME.

### **Ejemplo de historia: tasa alta de llamadas**

Este ejemplo explica cómo la Evaluación de errores asistida informa sobre una historia de tasa alta de llamadas: Una historia de tasa alta de llamadas se produce cuando un componente de cliente genera demasiadas transacciones propias, ralentizando la transacción superpuesta que la ha iniciado. Es decir, cuando la tasa del autor de la llamada al destinatario da como resultado un número bajo para el autor de la llamada y un número alto para el destinatario, por ejemplo, 1:20. Este número muestra que una llamada al autor de la llamada tiene como resultado 20 llamadas al destinatario. El analista de patrones informa sobre historias de tasa alta de llamadas para los nodos/componentes de back-end como bases de datos o clientes de servicios web.

Los síntomas siguientes pueden indicar un problema de tasa alta de llamadas:

- Si la latencia es alta "frente" a un componente en la pila de llamadas pero la latencia para el componente es baja, indica una alta tasa alta de llamadas en el uso del componente o frente al componente.
- Las transacciones de latencia larga con patrones de "código de barras": el componente A llama al componente B varias veces en un breve intervalo. Este comportamiento generalmente tiene como resultado una latencia normal para B pero una latencia alta para A.

Busque las anomalías y problemas en la Vista de la experiencia y Bloc de notas de análisis para identificar un titular de tasa alta de llamadas. Por ejemplo, las anomalías y problemas muestran el siguiente titular:

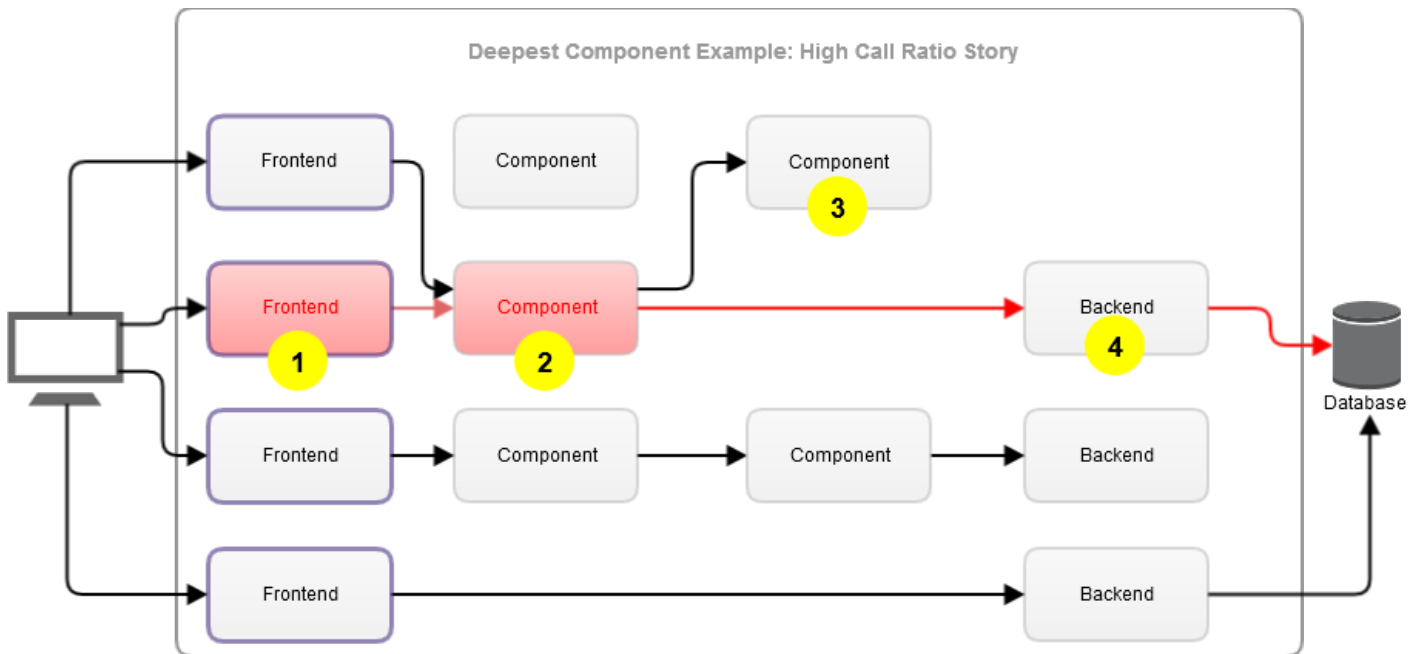
```
Potential high call ratio from {culprit.name} to {calledComp.name} in the order of {ratio}
```

Este titular describe una historia de tasa alta de llamadas. Por ejemplo, los detalles pueden describir un problema de latencia para una conexión de cliente a una base de datos en Nueva York.

### **Ejemplo: Cómo un analista determina el componente más profundo en una historia de tasa alta de llamadas**

El ejemplo siguiente muestra el aspecto de un analista de patrones para el componente más profundo en una historia de tasa alta de llamadas:

1. Los analistas diferenciales activan una alerta: se ha ralentizando una transacción y ahora forma parte de una historia.
2. Se ha producido un evento en la ruta de llamada de la transacción. El analista busca el componente más profundo en el contexto.
3. Un componente es un punto muerto. El componente no llama a un back-end, por lo que el analista lo ignorará.
4. Un componente llama a un back-end. Mediante el uso de datos históricos, el analista compara los números de las Respuestas por intervalo en el componente de llamada con el número de Respuestas por intervalo para las llamadas de back-end. Si la tasa es alta (por ejemplo, > 1:50), la transacción tiene una tasa alta de llamadas anómala que puede afectar negativamente al rendimiento de la aplicación.  
Otros componentes también pueden tener una tasa alta de llamadas a la base de datos. El analista no diagnostica la alta tasa hasta que haya componentes en la ruta de llamada de front-end. El analista no se interesa por la aplicación completa, sino que es un detective de una historia identificada.

**Figure 8: Ejemplo del componente más profundo: historia de tasa alta de llamadas****Soporte del analista de eventos de recursos**

La Evaluación de errores asistida utiliza a un analista de eventos de recursos para monitorizar las alertas sobre eventos de recursos como la CPU y la memoria como se muestra a continuación:

1. Una aplicación experimenta problemas y, o debido a, problemas de recursos del sistema.
2. Los eventos de recursos aparecen como elementos sospechosos para el problema o anomalía determinados.
3. Un componente de recurso o infraestructura se identifica como el posible causante de la infraestructura.

Los analistas de recursos admiten los Agentes de DX APM y DX APM Infrastructure Agent. La Evaluación de errores asistida proporciona el contexto para la información de la infraestructura de la que informa un Agente de la infraestructura para una aplicación. Las alertas que se activan en los componentes de la infraestructura se incorporan en las historias de la Evaluación de errores asistida. Por ejemplo:

1. Una CPU tiene una actividad alta en un servidor, lo que hace que la aplicación se ralentice.
2. El Agente de la infraestructura informa de este problema.
3. La Evaluación de errores asistida asocia este problema del recurso con la aplicación afectada y el componente de la infraestructura.
4. El componente de la infraestructura se muestra como el posible causante de la infraestructura.

**NOTE**

Los requisitos previos siguientes se aplican al analista de eventos de recursos:

1. Asegúrese de que se activa la monitorización del Agente de la infraestructura de DX APM y las alertas se asignan a los componentes de la infraestructura.
2. En la vista de mapa, seleccione la **capa de aplicación** para ver los componentes de la aplicación.
3. Haga clic en un componente de la aplicación del mapa.  
Los valores de correlación deben estar incluidos en el componente correspondiente de la infraestructura.

**Más información:**

Capas del mapa

Agente de la infraestructura

## Investigación del rendimiento de las transacciones con errores

Los datos de la métrica, como el tiempo medio de respuesta de un componente importante, pueden informarle sobre qué experiencia tienen los clientes que utilizan ese componente. Sin embargo, estos datos no ayudan a entender los casos donde el rendimiento es inusualmente lento. Cuando las transacciones son lentas, un seguimiento de la transacción puede ser como una radiografía: se muestran los detalles que no están visibles en la superficie y le permite ver en más detalle en qué gasta su tiempo la transacción. Application Performance Management (originalmente llamado Wily Introscope) fue pionero en el método de seguimiento de la transacción para obtener un profundo conocimiento de las transacciones individuales. El seguimiento de la transacción monitoriza la actividad de las transacciones individuales a medida que fluyen por las aplicaciones monitorizadas por el agente. Mientras que los datos de la métrica indican si hay un cuello de botella en el tráfico, los seguimientos de la transacción pueden informarle sobre la experiencia de un único coche: donde se ha retrasado, durante cuánto tiempo e incluso el por qué. Los seguimientos de la transacción se almacenan para que se puedan consultar sus detalles horas o días después de que se produjeran las transacciones en primer lugar.

### **Búsqueda de seguimientos de transacciones lentas o erróneas**

Como analista, la **Vista de la experiencia** le ayuda a encontrar seguimientos útiles de la transacción para investigarlos. En la ficha **Transacciones comerciales**, puede ver los detalles y los resúmenes del seguimiento de la transacción. Esta información le ayudará a comprender el rendimiento de la transacción y a solucionar un problema de rendimiento pobre identificando cuándo, dónde y por qué se degrada el rendimiento.

#### **Siga estos pasos:**

1. En el panel izquierdo, haga clic en **Vista de la experiencia**.  
La Vista de la experiencia muestra tarjetas de experiencias individuales. Todas las tarjetas muestran un resumen. Los elementos rojos indican las transacciones lentas o erróneas.

#### **NOTE**

Para obtener más información sobre la Vista de experiencia, consulte [Monitorización del rendimiento utilizando la Vista de experiencia](#).

#### **TIP**

También puede iniciar la investigación desde el mapa. En el panel izquierdo, haga clic en **Mapa** y omita el paso siguiente.

2. Busque las tarjetas y haga clic en el icono **Bloc de notas** en una de las tarjetas que le interese.  
El Bloc de notas de análisis muestra detalles sobre la experiencia.
3. En el panel **PROBLEMAS**, haga clic en **Abrir** en un problema que le interese.
  - Un círculo rojo indica que el componente es un actor en al menos un problema o una anomalía. Todos los componentes de una historia se tratan como actores.
  - Un círculo rojo concéntrico indica que el componente es el culpable en al menos un problema o una anomalía. Todos los actores cuentan con evidencias, pero un causante es un actor especial. El causante identifica la causa raíz del problema o de la anomalía en la aplicación o transacción proporcionada. Este componente puede ser el origen de la degradación del rendimiento en su entorno de aplicaciones. El flujo de relaciones muestra las rutas de las transacciones de las experiencias seleccionadas. Este mapa proporciona contexto para el evento que ha ocurrido.
4. Haga clic en los nodos individuales o en los grupos de nodos para un máximo de 1000 nodos. Seleccione la **Capa de la aplicación** o la **Capa de la infraestructura de APM** en el mapa para ver todos los seguimientos recopilados por el host, el agente o la aplicación.

Aparece el gráfico **Descripción general del componente** que muestra las transacciones sin errores y las transacciones con errores.

Haga clic aquí para obtener ayuda para el gráfico de componentes.

El gráfico de componentes muestra un máximo de 20 nodos. Utilice los gráficos de componentes para comparar la métrica en directo o histórica entre nodos arbitrarios. El gráfico de componentes contiene más información de la métrica de la que está disponible en el mapa para todos los componentes. Utilice las opciones de conmutador (puntos) situadas en la parte inferior del gráfico para mostrar la siguiente información.

- **Histograma de TIEMPO DE RESPUESTA:** El histograma muestra el tiempo medio de respuesta agregado por segundo para las transacciones sin errores y para las transacciones con errores. El histograma permite comparar datos fácilmente e identificar tendencias como, por ejemplo, cuándo ha aumentado o disminuido el número de seguimientos.
- **Minigráfico de TIEMPO MEDIO DE RESPUESTA:** El minigráfico muestra la forma general de la variación en el tiempo de la métrica de BlamePoint para todos los componentes. El minigráfico muestra información para el período de tiempo activo seleccionado en la escala de tiempo. Pase el ratón sobre cualquier punto del minigráfico para ver un valor numérico.
- **Gráfico de VOLUMEN DE TRANSACCIONES:** El gráfico de barras le ayudará a determinar rápidamente el nivel de volumen de transacciones. Las barras también facilitan la identificación de tendencias en el volumen.

El componente se resalta en el panel con los **COMPONENTES DE LA APLICACIÓN AFECTADA**.

#### 5. Haga clic en la ficha **Transacciones comerciales**.

Los seguimientos que se corresponden con el componente aparecen en una lista de resumen para el intervalo que se selecciona en la escala de tiempo. Se muestran los seguimientos de los componentes inferidos incluso si los agentes no monitorizan estas transacciones. Por ejemplo, los componentes inferidos pueden ser back-ends, servicios web o sockets. Los seguimientos mostrarán las horas de duración y están codificados por colores. Cada color indica una característica que se asocia con una transacción como, por ejemplo, el rojo indica un error. Se pueden identificar métodos problemáticos según la duración del seguimiento. Los seguimientos que son largos inesperadamente pueden ser la causa probable de las transacciones lentas.

#### NOTE

La lista se actualiza automáticamente cuando se utiliza el modo en directo.

La lista muestra la siguiente información sobre el seguimiento durante un máximo de 2.000 seguimientos.

**Dirección URL:** la dirección URL que se ha invocado para iniciar la transacción o la ruta al componente que ha iniciado la transacción

**Nombre:** El nombre del componente de nivel alto como, por ejemplo, Valor predeterminado.

**Marca de tiempo:** La hora de inicio, según el reloj del sistema del equipo host del agente, de la invocación del componente seleccionado.

**Duración:** El tiempo de ejecución en milisegundos del componente seleccionado.


**Tipo de seguimiento:** El tipo de seguimiento como Otros, Error o Instantánea.

**ID de usuario:** El ID del usuario que ha iniciado la sesión y que está ejecutando la transacción.

Esta información ayuda a entender la secuencia de las llamadas que se realizan en un período de tiempo y a evaluar el rendimiento.

**Nota:** No toda la información está disponible sobre los componentes de visibilidad exhaustiva.

#### 6. Realice una o más de estas acciones:

- Haga clic en el **botón emergente**  para abrir el visor en un cuadro de diálogo de vista completa. Pulse la tecla **Esc** para cerrar el cuadro de diálogo.
- Seleccione una opción en la lista desplegable **Tipo de seguimiento** para categorizar los seguimientos según sus características. Un seguimiento puede tener más de una característica:
  - Otros:** Devuelve todos los seguimientos de la transacción que no sean los seguimientos con errores o detenidos. Naranja claro



indica que el análisis diferencial ha activado una alerta: una transacción tiene una varianza sin control.

**Error:** Devuelve los seguimientos de la transacción con una característica de error. Un error es una excepción que comunican los códigos de error de JVM o HTTP. Por ejemplo, los errores pueden ser un estado de error de HTTP, una excepción de SQL o una excepción de Java. Cuando el Tipo de seguimiento es Normal pero un error ha activado un seguimiento automático de la transacción, el componente se muestra como un error y se tiene en cuenta en el recuento total de errores.

También se devuelven seguimientos de la transacción que tienen un mensaje de error de `Transacción detenida`. Una detención es una transacción o el componente de una transacción que no se ha completado en el umbral de tiempo especificado.

**Instantánea:** Devuelve todas las transacciones que disponen de instantáneas.

- Haga clic en el **encabezado de una columna**.

La lista ordena los seguimientos por tipo de columna como, por ejemplo, por `ID de usuario`. El tipo de seguimiento no se puede ordenar haciendo clic en el encabezado de la columna.

**Nota:** El ID de usuario es la identificación del usuario que ha iniciado la sesión y que está ejecutando la transacción (si este campo está configurado y el ID está disponible).

7. Examine los componentes individuales y los datos de seguimiento. Se puede consultar la secuencia de llamadas y el código para determinar la causa de un problema.

#### Más información:

[Utilización del seguimiento de la transacción entre procesos para solucionar problemas](#)

[Inicio de una nueva sesión de seguimiento de la transacción](#)

[Examen de los componentes individuales y de los datos de seguimiento](#)

[Diagnóstico de problemas de carga del recurso](#)

[Diagnóstico de problemas de rendimiento del sistema](#)

[Detección y análisis de errores y detenciones](#)

[Análisis de las instantáneas de error y detenidas](#)

[Análisis de los seguimientos y colaboración en el análisis de problemas](#)

## Utilización del seguimiento de la transacción entre procesos para solucionar problemas

A menudo las transacciones viajan a través de varias instancias (máquinas virtuales, CLR o Node.js) o servicios de aplicaciones, en función del entorno. El procesamiento pasa de cualquier combinación de instancia (máquina virtual Java, CLR o Node.js) o servidor de aplicaciones a otra. La recopilación de la ruta completa de la transacción requiere realizar el seguimiento de las llamadas síncronas y asíncronas a través de los límites de las instancias de máquina virtual Java, CLR o Node.js. El poder realizar el seguimiento de las transacciones en varias plataformas también puede requerir la ejecución de un agente compatible. El *seguimiento de transacciones entre procesos* recopila la ruta completa de la transacción en varias plataformas. Esta capacidad permite ver los detalles cuando los métodos de las llamadas de transacciones en varias máquinas virtuales Java o CLR que se ejecutan en servidores diferentes.

#### NOTE

El seguimiento de transacciones entre procesos se admite en otros seguimientos de transacciones como los ejecutados manualmente o de ejemplo que utilizan el filtrado de los agentes. Las transacciones entre procesos en seguimientos de transacciones automáticos solo son compatibles con aplicaciones Java.



## **Correlación de transacciones**

Las aplicaciones distribuidas son complejas. Normalmente las transacciones de un solo usuario abarcan varios subprocesos en diferentes máquinas virtuales Java o CLR de los agentes. A menudo una sola transacción incluye llamadas síncronas y asíncronas. El agente también debe tener en cuenta que las llamadas de transacciones individuales deben presentar la ruta completa de la transacción como una unidad lógica.

Normalmente las transacciones están formadas por una serie de llamadas y respuestas que se pasan de un proceso a otro. A menudo diferentes procesos en una transacción realizan llamadas a distintos servidores lógicos o físicos. Los procesos también pueden distribuirse para ejecutarse en distintos componentes o sistemas back-end. El ensamblaje de una transacción completa requiere un agente para identificar todos los procesos incluidos y el orden de las llamadas. El agente también requiere información sobre subprocesos y llamadas síncronas y asíncronas.

El seguimiento de una ruta de transacción completa que incluya llamadas entre procesos requiere que el agente se conecte de forma lógica a los procesos. El agente utiliza un *identificador de correlación (ID de correlación)*, que crea una correlación o crea una vista conectada de los procesos. El agente realiza la conexión insertando el identificador de la correlación en la transacción. El identificador de la correlación se puede pasar de un proceso a otro. Esta vinculación de proceso permite al agente identificar los front-ends y back-ends que forman parte de la misma transacción. En **Detalles del componente** del Visor de seguimiento de transacciones, el ID de correlación es el valor de la propiedad Datos entre procesos.

El ensamblaje de una transacción completa también requiere un agente para determinar cuándo un proceso de una transacción llama a otro. Puede ver el orden en el que los front-ends y back-ends se llaman los unos a los otros en una transacción. Para las transacciones sincrónicas, el orden puede ayudar a identificar las relaciones entre el autor de la llamada y el destinatario de la llamada. Para las transacciones asíncronas, el orden puede ayudar a identificar un flujo de trabajo entre varios procesos para los segmentos complejos de la transacción del servidor y cliente. La combinación del orden de secuencia de la llamada y el identificador de la correlación proporciona un *seguimiento de transacciones correlacionado* o un *seguimiento correlacionado*.

El seguimiento de la transacción entre procesos también es compatible con la correlación entre subprocesos dentro del mismo proceso.

El agente gestiona automáticamente el conjunto de datos del identificador de la correlación y entrega los datos a Enterprise Manager. Enterprise Manager construye la representación gráfica de las transacciones seleccionadas que el Visor de seguimiento de la transacción muestra.

## **Utilización del seguimiento de la transacción para solucionar problemas**

El siguiente proceso describe cómo puede examinar las transacciones en el Visor de seguimiento de la transacción para facilitar la localización de la causa raíz de los problemas.

1. Cuando el Visor de seguimiento de transacciones muestra una pila gráfica, el agente ha realizado el seguimiento de los procesos relacionados en un evento de seguimiento seleccionado. Los procesos de los que se realiza un seguimiento desde varios agentes aparecen en diferentes áreas sombreadas.
2. Puede examinar los componentes vinculados para ver las transacciones entre procesos o entre JVM. Por ejemplo, se puede ver si una transacción determinada ha dejado un proceso y, a continuación, la transacción ha entrado en un proceso diferente.
3. También puede obtener información sobre qué llamadas podrían ser la fuente de las transacciones lentas y detenidas.

## **Ejemplo del seguimiento de la transacción entre procesos**

Este ejemplo describe cómo el seguimiento de la transacción entre procesos puede ayudar a identificar y evaluar los problemas de forma rápida y eficaz.

1. Está revisando un seguimiento de la transacción para una transacción problemática y advierte un tiempo de ejecución de 6 segundos (6000 ms).



2. En la pila gráfica, se ven llamadas de un método del cliente, `dataservice.yourcompany.net/invoke`, al método del servidor, `thirdparty.mycompany.net/invoke`.
3. Se da cuenta que el servicio web del servidor está realizando un gran número de llamadas a un servicio web de terceros. El servicio web de terceros no está instrumentado, por lo que su tiempo de procesamiento no se muestra de forma explícita en el seguimiento.
4. La pila gráfica muestra que el back-end del servicio web de terceros atiende a solicitudes que se repiten de forma muy rápida. Este comportamiento indica que probablemente la lógica de programación, como un bucle anidado, está haciendo que se realicen llamadas repetidas en el servicio del servidor. Se ha determinado que la operación de invocación del servidor es la responsable de la mayoría del tiempo de ejecución de la transacción global.
5. Con esta información, póngase en contacto con el propietario de la aplicación del servicio web del servidor.
6. El propietario solicita una investigación de la lógica de la aplicación que llama al back-end del servicio web de terceros.

## Inicio de una nueva sesión de seguimiento de la transacción

Para ejecutar una sesión de seguimiento de la transacción manualmente, especifique los agentes de cuyas transacciones desea realizar un seguimiento, así como el período de captura de datos. Una vez que se inicia la sesión de seguimiento de la transacción, las transacciones que coinciden con los criterios de filtro aparecen en el Visor de seguimiento de la transacción. Los eventos de transacción incluyen errores y seguimientos de transacciones.

Si un seguimiento se inicia con un período de tiempo establecido, este se detiene al final del período especificado.

### NOTE

Solamente se puede iniciar una sesión de seguimiento para un agente específico con un período de tiempo determinado. Si se reinicia una sesión de seguimiento activa, se recibe una notificación que recuerda que la sesión de seguimiento de transacciones está activa para el agente y muestra el tiempo restante de la sesión activa. Se puede iniciar un nuevo seguimiento para el mismo agente después de que finalice una sesión de seguimiento activa.

Por ejemplo, "Actualmente la sesión de seguimiento de transacciones está activa para este agente. Tiempo restante: menos de un minuto".

Se puede iniciar la sesión de seguimiento de transacciones desde la página Agentes o desde la página Vista de métricas.

Para iniciar la sesión de seguimiento de transacciones en la página **Agentes**, siga estos pasos:

1. En el panel izquierdo, en **Configuración**, haga clic en **Agentes**.  
Aparece una página con una lista de los agentes.
2. (Opcional) Haga clic en la flecha **Aplicaciones**.  
Se enumeran todas las aplicaciones que monitoriza el agente.
3. Seleccione uno o más agentes de cuyas transacciones desea realizar un seguimiento:
  - Para realizar el seguimiento de todos los agentes, haga clic en **Realizar el seguimiento de todos los agentes**.  
Esta opción permite realizar un seguimiento de todos los agentes compatibles que están conectados actualmente y de cualquier agente que se conecte durante la sesión de seguimiento.
  - Para realizar el seguimiento de los agentes seleccionados, haga clic en **Realizar el seguimiento del agente para un agente**.
 Aparece el cuadro de diálogo Sesión de seguimiento de la transacción.
4. Especifique los valores para el seguimiento de las transacciones en los campos del cuadro de diálogo o acepte los valores predeterminados y haga clic en **Iniciar**:
  - Especifique la **Duración mínima de la transacción** en milisegundos para el seguimiento de la transacción. El valor predeterminado es 1000 milisegundos. El valor mínimo es 1 milisegundo.
  - Especifique la **Duración de la sesión de seguimiento** en minutos. El valor predeterminado es 1 minuto con una duración máxima de 5 minutos para una sesión de seguimiento única.
 Un panel muestra el estado de la sesión.

5. (Opcional) Cierre el cuadro de diálogo después de que el seguimiento se haya iniciado correctamente. La sesión de seguimiento continúa ejecutándose en segundo plano.

Para iniciar la sesión de seguimiento de transacciones en la página **Vista de métricas**, siga estos pasos:

1. En el panel izquierdo, haga clic en **Vista de métricas**.
2. En la ficha **Árbol de métrica**, busque el agente de cuyas transacciones desea realizar un seguimiento.
3. Haga clic con el botón secundario del ratón en el agente y haga clic en la opción "Realizar el seguimiento del agente: <Nombre>". Se muestra el cuadro de diálogo Sesión de seguimiento de transacciones.
4. Especifique los valores para el seguimiento de transacciones en el cuadro de diálogo.
  - Especifique la **Duración mínima de la transacción** en milisegundos para el seguimiento de la transacción. El valor predeterminado es 1000 milisegundos. El valor mínimo es 1 milisegundo.
  - Especifique la **Duración de la sesión de seguimiento** en minutos. El valor predeterminado es 1 minuto con una duración máxima de 5 minutos para una sesión de seguimiento única.
5. Haga clic en **Iniciar**. Se muestra un mensaje de confirmación, "Se ha iniciado la sesión de seguimiento de transacciones".
6. Haga clic en **Cancelar** para cerrar el cuadro de diálogo y volver a la página **Vista de métricas**.

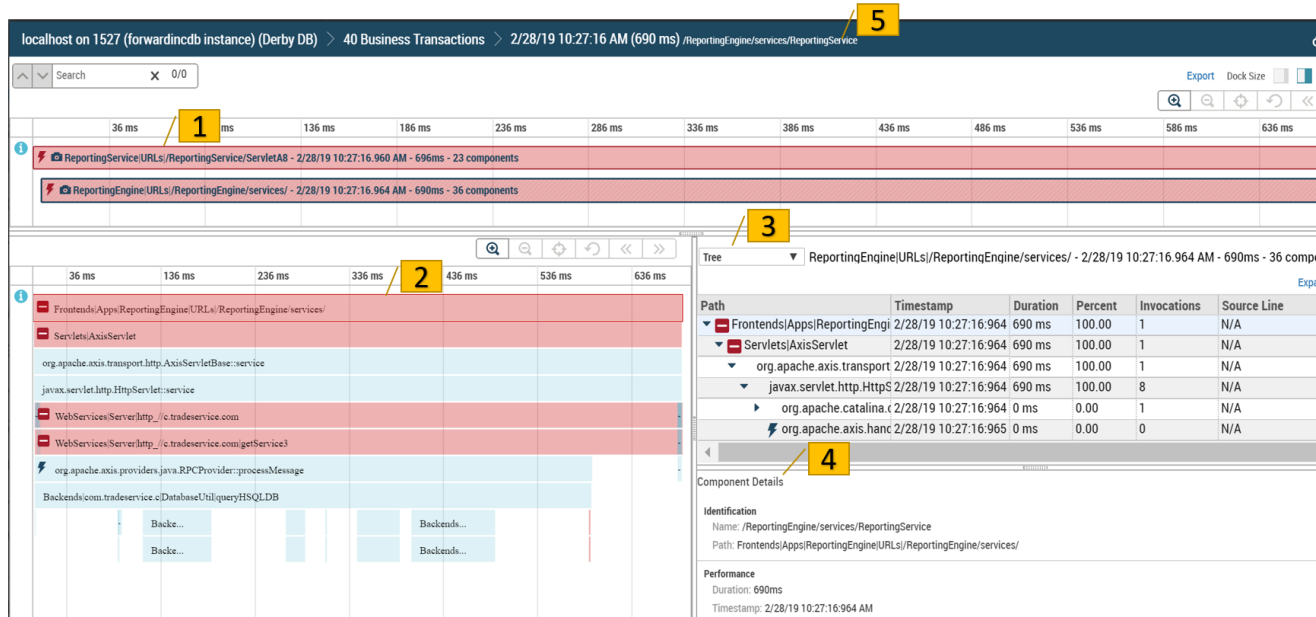
## Examen de los componentes individuales y de los datos de seguimiento

Se puede examinar la información detallada sobre los datos de seguimiento para encontrar el motivo por el cual las transacciones tienen un rendimiento lento o incluso se han interrumpido. El Visor de seguimiento de transacciones muestra varias representaciones de los datos para ayudarle a identificar los componentes que tienen un rendimiento bajo.

**Siga estos pasos:**

1. En el mapa o en el Bloc de notas de análisis, vaya a la ficha **Transacciones comerciales**.
2. Haga clic en la ficha **Transacciones comerciales**.
3. Haga clic en una fila en la lista Seguimiento de la transacción.  
El Visor de seguimiento de transacciones muestra cuatro paneles para mostrar información sobre el seguimiento de la transacción y los componentes.
  - **Seguimiento de la transacción** se muestra en el panel superior.
  - Se muestra el **Detalle del seguimiento de la transacción** en el panel inferior izquierdo.
  - El panel inferior derecho está dividido en dos subpaneles:
    - La **Información de la transacción** sobre el seguimiento de la transacción seleccionada se muestra en el panel secundario superior de la derecha.
    - Los **Detalles del componente** se muestran en el subpanel inferior derecho.

Utilice el siguiente gráfico y su correspondiente leyenda para conocer las distintas funciones del Visor de seguimiento de





transacciones.

La siguiente leyenda identifica cada elemento con un número y proporciona más información:

Número	Name	Más información
1	Seguimientos de la transacción	Examine cada seguimiento de la transacción. Si hay más de uno, la información sobre el seguimiento de la transacción seleccionado aparecerá en otros paneles.
2	Panel Detalles del seguimiento de la transacción	Este panel muestra la pila gráfica, que es el orden de las transacciones de los componentes de arriba abajo. Nos referiremos a la pila gráfica como gráfico de tarta debido a que la representación puede parecer una tarta al revés.
3	Panel Información de la transacción	Este panel muestra información sobre el seguimiento de la transacción seleccionado. Tenga en cuenta que la ruta que aparece a la derecha de la lista desplegable es la ruta del seguimiento de la transacción seleccionada en el panel Seguimiento de la transacción. Se pueden seleccionar estas vistas en la lista desplegable: <b>Árbol, Resumen, Control del tiempo del explorador, Propiedades del sistema e Instantánea.</b>

4	Detalles del componente	Este panel proporciona información sobre el componente seleccionado en la pila gráfica. Cuando no se haya seleccionado un componente, la información se refiere al primer componente de la pila gráfica.
5	Rutas de exploración	La ruta situada encima del Visor de seguimiento de transacciones.

La pila gráfica y los datos del seguimiento de la transacción muestran información para ayudarle a evaluar el rendimiento como, por ejemplo:

Relaciones de llamadas entre componentes	<p>Las filas de componentes se muestran de arriba abajo, en orden de llamada.</p> <p><b>Nota:</b> La llamada y el componente son sinónimos. Cuando se selecciona un componente, se selecciona una llamada de la transacción.</p> <p>Una llamada puede llamar a los hijos, lo que crea la pila o profundidad:</p> <p>1 fila = 1 o más llamadas = 1 o más componentes que pueden hacer invocaciones o llamadas hijo</p> <p>La Vista de árbol muestra a una coincidencia de uno-a-uno de los datos:</p> <p>1 fila = 1 llamada = 1 componente</p> <p>La vista de resumen muestra los datos acumulados, y no una coincidencia de uno-a-uno:</p> <p>1 fila = ruta</p> <p>La ruta es la etiqueta para la llamada y el nivel de la pila. Por ejemplo, se ha realizado una llamada de "inicio de sesión" 5 veces en el mismo nivel de pila. Se muestran 5 componentes en la misma fila. En la Vista de árbol, se muestran 5 filas. El recuento de la Vista de resumen es 5 y la columna Duración total muestra la suma de todas las horas de las 5 llamadas.</p>
Errores e instantáneas	<p>El cuadro rojo que contiene el icono del signo menos</p>  <p>blanco indica que hay un componente con un error.</p> <p>El icono de cámara</p>  <p>identifica una transacción con una instantánea de error o detención relacionada.</p> <p><b>Nota:</b> Para obtener más información, consulte <a href="#">Análisis de las instantáneas de error y de detención</a>.</p>
Puntos de entrada	Generalmente, los puntos de entrada se muestran como el primer componente de la transacción. Si la transacción es de tipo comercial, esta aparece como el primer componente seguido por el punto de entrada.
Secuencia de transacciones	La colocación de los componentes de izquierda a derecha indica la secuencia. En la parte superior de las transacciones, aparece la hora relativa en milisegundos. Si el tiempo de seguimiento es lo suficientemente largo, el tiempo se muestra en segundos, horas y días.

Datos de las transacciones entre procesos y entre JVM	<p>Un identificador único, el ID de correlación vincula las transacciones front-end y back-end de las que se realiza un seguimiento. La secuencia se basa en el orden en que los back-ends llaman a los front-ends en una transacción. El ID de correlación ayuda a detectar qué llamadas pueden ser la fuente del bajo rendimiento o de la interrupción de las transacciones. En <b>Detalles del componente</b> del Visor de seguimiento de transacciones, el ID de correlación es el valor de la propiedad Datos entre procesos.</p> <p>Varias pilas gráficas en el visor muestran los procesos relacionados para el evento de seguimiento seleccionado. Los procesos de los que se realiza un seguimiento desde varios agentes aparecen en diferentes áreas sombreadas. Examine los componentes vinculados en un seguimiento de transacción para ver las transacciones entre procesos o entre JVM. Por ejemplo, puede ver si una determinada transacción ha dejado un proceso y si, a continuación, la transacción ha entrado en un proceso distinto. También puede obtener información sobre qué llamadas podrían ser la fuente de las transacciones lentas e interrumpidas.</p> <p><b>Más información:</b> Para obtener más información sobre la correlación de transacciones, consulte <a href="#">Utilización del seguimiento de la transacción entre procesos para solucionar problemas</a>.</p>
Componentes de visibilidad exhaustiva	<p>Un icono de rayo indica un componente de visibilidad exhaustiva. Este tipo de componente es un método o componente que se detecta automáticamente sin la necesidad de utilizar las directivas de ProbeBuilder. Application Performance Management analiza los métodos para comprobar su complejidad y así poder determinar las llamadas y los componentes que se deben instrumentar y mostrar como componentes de visibilidad exhaustiva.</p>
Visibilidad del intervalo de tiempo de ejecución	<p>Con la visibilidad del intervalo de tiempo de ejecución, los agentes instrumentan y monitorizan automáticamente las aplicaciones en función de su rendimiento en tiempo de ejecución.</p> <p><b>Nota:</b> Para obtener más información, consulte <a href="#">Configuración de la instrumentación inteligente</a>.</p>

4. (Opcional) Realice una o varias de las acciones siguientes:

- Escriba una cadena de texto para filtrar los seguimientos en el campo Buscar. La búsqueda coincide con la información de todos los componentes y seguimientos de la transacción. Los resultados se muestran en todas las vistas y en cualquiera de las propiedades en los **Detalles del componente**. La búsqueda también devuelve coincidencias parciales. Por ejemplo, los criterios de búsqueda son para `node1` . La Vista de **resumen** muestra seguimientos para `node1` , `node124` y `node1_323` . Tanto la pila gráfica como las vistas muestran todos los componentes relacionados. Los componentes que coinciden con la búsqueda se resaltan en amarillo en la pila. Si procede en las vistas, el texto coincidente tiene el fondo amarillo.
- Pase el ratón por encima del **icono de información** (punto azul con un i). La información sobre herramientas muestra el nombre completo del agente. El icono de información y la fila correspondiente representan a cada agente en particular.

5. Examine los seguimientos de la transacción de arriba abajo para comprender los seguimientos que ha capturado el agente.

**NOTE**

Si se ha recopilado un número excesivo de seguimientos, se le indicará que el Visor de seguimiento de transacciones no podrá procesarlos. (Por ejemplo, en Internet Explorer, un cuadro emergente explica que el archivo JSON es demasiado grande para cargarse.)

- Al pasar el puntero del ratón sobre un seguimiento o componente para obtener información sobre herramientas se muestra el resumen de la información del seguimiento de la transacción. Cuando se muestra únicamente una parte del componente, la información sobre herramientas resulta útil.
- Utilice las funciones de navegación para ajustar la vista.  
Haga clic aquí para obtener ayuda de navegación...

Acercar (Mayús + =): Cambia la escala para mostrar más detalles.

Alejar (Mayús + -): Cambia la escala para mostrar menos detalles.

Restablecer (Mayús + R): Devuelve los datos del visor a su estado original.

Centro (Shift + C): Centra los datos del Visor.

Panorámica izquierda (Shift + izquierda): Desplaza el foco a la izquierda.

Panorámica derecha (Mayús + derecha): Desplaza el foco a la derecha.

Seleccionar siguiente (flecha hacia abajo): Selecciona la fila siguiente.

Seleccionar anterior (flecha hacia arriba): Permite seleccionar la fila anterior.

Utilice los separadores que separan los paneles para mostrar más del panel de interés. Haga doble clic en un separador para minimizar o maximizar los paneles izquierdos superiores e inferiores.

Haga clic en la opción **Tamaño de acoplamiento** para aumentar o disminuir el tamaño de los paneles derecho e izquierdo en relación con ellos.

Tenga en cuenta que la selección realizada en cualquier representación se selecciona automáticamente en las otras representaciones cuando hay información asociada y viceversa. Por ejemplo, haga clic en una fila en la pila gráfica. La pila gráfica, el elemento de información de la transacción, los **Detalles del componente** y las vistas relacionadas muestran información que coincide con esa fila.

6. Haga clic en el seguimiento de la transacción que desee.  
Solo se puede seleccionar un seguimiento de la transacción cada vez.
7. Examine los componentes de la pila gráfica de arriba abajo para entender la secuencia de llamada en un período. Un tiempo de transacción del componente anormalmente largo puede indicar la causa raíz del problema. Tenga en cuenta que el nombre y el primer número de línea del archivo de origen de Java del método Java instrumentado aparece entre paréntesis.  
Las filas de color rojo indican una condición de error. Las filas de color azul claro indican que no existe ningún problema. Las filas de color naranja claro indican que el análisis diferencial ha activado una alerta. Las filas de color naranja más oscuro indican una detención. Las filas de color amarillo indican un resultado de búsqueda.  
Las transacciones que duran 0 milisegundos se muestran como un punto en un fondo azul claro.
8. Haga clic en el componente que desee.  
En el panel inferior derecho, los paneles **Información de la transacción** y **Detalles del componente** muestran información detallada en sus respectivos subpaneles.
9. En el subpanel superior, seleccione una opción de la lista desplegable **SELECCIONAR UNA VISTA** para mostrar varias representaciones de los datos. El comportamiento de la selección varía para cada vista. Por ejemplo, la **Vista de árbol** muestra las rutas del seguimiento de la transacción, mientras que **Control del tiempo del explorador** muestra datos de las páginas en disco y recursos asociados a las páginas flexibles. Por lo tanto, la información que puede seleccionar para estas vistas es diferente.

**Árbol**

La **Vista de árbol** muestra las rutas del seguimiento en orden jerárquico de llamada. Cada ruta incluye los nombres de las clases y los métodos de una llamada. Se pueden ver los cambios que se han producido entre un punto de inicio y un punto final de un seguimiento. Los datos de ruta, marca de tiempo, duración, porcentaje e invocación aparecen en columnas ordenables. (La Línea de origen no es ordenable.) Es posible que algunos seguimientos para un componente no tengan información sobre la línea de origen. En este caso, N/D (no disponible) se muestra en la columna Línea de origen. Ajuste la cantidad de información que aparecerá al expandir o contraer rutas. Los iconos de color definen el tipo de seguimiento. Por ejemplo, naranja claro



indica que el análisis diferencial ha activado una alerta: una transacción tiene una varianza sin control. La **Vista de árbol** permite recorrer el examen de datos e ir a componentes específicos para identificar los problemas de rendimiento. Los valores de datos ayudan a entender cómo un valor inicial se ve afectado por una serie de valores intermedios.

### Summary

La **Vista de resumen** muestra los datos con colores que indican el tipo de seguimiento. Los valores de tasa de llamada más elevados tienen un sombreado más oscuro porque las llamadas se presentan superpuestas. Este resumen visual permite identificar rápidamente las áreas del problema de un vistazo. Después de identificar un problema, puede utilizarse la **Vista de árbol** para investigar los detalles de ese tipo de llamada.

Los datos de la columna muestran los totales de cada fila. Por ejemplo: A un componente se le llama 100 veces en la fila de nivel 4 de una transacción. El recuento de filas de nivel 4 es de 100. Cada llamada tiene una duración de 2 milisegundos, de modo que la duración total será de 200 milisegundos ( $100 \times 2$ ). El valor de duración total de la ruta de exploración puede diferir del valor de duración total del **Resumen**. Esta diferencia puede deberse a que el valor de la ruta de exploración incluye todos los seguimientos correlacionados desde un back-end, mientras que la **Vista de resumen** no incluye estos datos.

### Control del tiempo del explorador

El control del tiempo del explorador muestra los datos de las páginas de hardware y sus recursos, y para recursos que están asociados con páginas de software. (No aparecen los datos de una página de software).

#### NOTE

Para obtener más información sobre el control del tiempo del explorador, consulte [Diagnóstico de problemas de carga del recurso](#).

### Propiedades del sistema

Las propiedades del sistema proporcionan el tiempo de la CPU y los datos de monitorización de la contención de subprocesos para el seguimiento de transacciones en el método del servlet.

#### NOTE

Para obtener más información acerca de las propiedades del sistema, consulte [Diagnóstico de problemas de rendimiento del sistema](#).

### Instantánea

La instantánea proporciona información sobre las instantáneas de detención y de error.

#### NOTE

Para obtener más información sobre las instantáneas de error y de detención, consulte [Análisis de las instantáneas de error y detención](#).

### 10. Examine el panel **Detalles del componente**.

Haga clic aquí para obtener los detalles del componente.

#### NOTE

No toda la información sobre los componentes de la visibilidad exhaustiva está disponible.

**Nombre:** El nombre del componente. Por ejemplo: Valor predeterminado.

**Ruta:** El nombre de recurso completo del componente. Por ejemplo: `Frontends|Apps|AuthenticationService|URLs|Default`.

**Duración:** El tiempo de ejecución en milisegundos del componente seleccionado.

**Marca de tiempo (relativa):** La hora de inicio (según el reloj del sistema) de la invocación del componente raíz.



**Porcentaje de duración:** el porcentaje de tiempo total de la transacción

**Propiedades del sistema:** Los datos de tiempo permiten diagnosticar subprocesos de método para los problemas de rendimiento. Los cuadros de colores identifican las diversas propiedades del sistema. Un gráfico de barras representa los valores de los datos para estas propiedades del sistema. Cuando los valores son 0 ms, el gráfico muestra una línea negra. Cada propiedad del sistema y su valor aparecen bajo el gráfico.

**Propiedades:** Una lista de las propiedades opcionales del componente, incluida la propiedad siguiente:

- Línea de origen (solo Agente de Java): El nombre y el primer número de línea del archivo de origen de Java del método Java instrumentado. El Agente de Java no recopila los números de línea del código que llama al método Java instrumentado. Los volcados estándares de la pila de subprocesos de excepción en los depuradores y volcados del núcleo suelen mostrar estos números de línea.

#### TIP

Haga clic en **Expandir** para expandir todo el árbol. Haga clic en **Contraer** para contraer todo el árbol. Haga clic en la flecha hacia la derecha situada junto a un componente para mostrar un único componente secundario.

Cambie el tamaño de cualquier columna para mostrar más o menos información.

Coloque el ratón sobre un **nombre de columna** o un **segmento del gráfico de propiedades del sistema** para ver la información sobre herramientas del elemento.

11. Determine la causa raíz del problema de rendimiento de la aplicación. Utilice la información de identificación para recopilar detalles específicos sobre el problema. Por lo general, se deben buscar los componentes de los niveles más profundos y que lleven más tiempo en ejecución en el seguimiento. Por ejemplo:
  - Una única llamada a una base de datos
  - Una oleada de llamadas rápidas que juntas conllevan una latencia alta

Puede ponerse en contacto con el personal de operaciones para solicitar una revisión del código de la aplicación. El personal determinará si existe un problema de código o un problema de dependencia de la aplicación.

#### NOTE

**Más información:** [Análisis de los seguimientos y colaboración en el análisis de problemas.](#)

## Diagnóstico de problemas de carga del recurso

Para diagnosticar problemas de rendimiento en una página web, debe mirar el control del tiempo de los recursos que HTML y JavaScript están descargando. La vista **Control del tiempo del explorador** en el Visor de seguimiento de transacciones permite visualizar los recursos que se han descargado en respuesta a las solicitudes HTTP asociadas con un seguimiento. El control del tiempo del explorador representa los datos que se generan con carácter acumulativo y de forma secuencial en un seguimiento de la transacción. Puede examinar la información detallada sobre los datos del seguimiento. Los datos aparecen para páginas en disco y sus recursos, así como para los recursos asociados con las páginas flexibles. (No aparecen los datos de una página flexible). Los recursos están en gris de forma predeterminada y cada fase tiene su propio color. Esta representación en cascada le ayudará a comprender cómo los distintos factores contribuyen a realizar un seguimiento de la transacción. Esta vista funciona de forma similar a una vista en cascada en las herramientas de desarrollador del explorador.

#### NOTE

**Más información:** [Examen de los componentes individuales y de los datos de seguimiento.](#)

**Siga estos pasos:**

1. En la ficha **Transacciones comerciales**, haga clic en el seguimiento de la transacción que desee. Los componentes de la transacción individual aparecen en la pila gráfica (gráfico de tarta) del panel **Detalles del seguimiento de la transacción**.



2. Examine los componentes de la pila gráfica de arriba a abajo para entender la secuencia de llamadas durante un período. Un tiempo de transacción del componente anormalmente largo puede indicar la causa raíz del problema.
3. Haga clic en el componente que desee.
4. En el panel **Información de la transacción**, seleccione **Control del tiempo del explorador** en la lista desplegable **SELECCIONAR UNA VISTA**.
5. Examine la información que aparece en la vista para diagnosticar los problemas de carga del recurso:

La vista **Control del tiempo del explorador** consta de tres partes:

- Un área de resumen que contiene información sobre el componente en el seguimiento que ha activado la descarga del recurso.
- Una escala de tiempo que permite reducir el intervalo de tiempo para centrarse en recursos específicos. El intervalo de la escala de tiempo permite ver todos los recursos en contexto y reducir el período que se muestra en la cuadrícula. Se puede cambiar el intervalo arrastrando los marcadores al final o arrastrando toda la línea en el nivel intermedio.
- Una cuadrícula que muestra una fila de detalle para cada recurso.

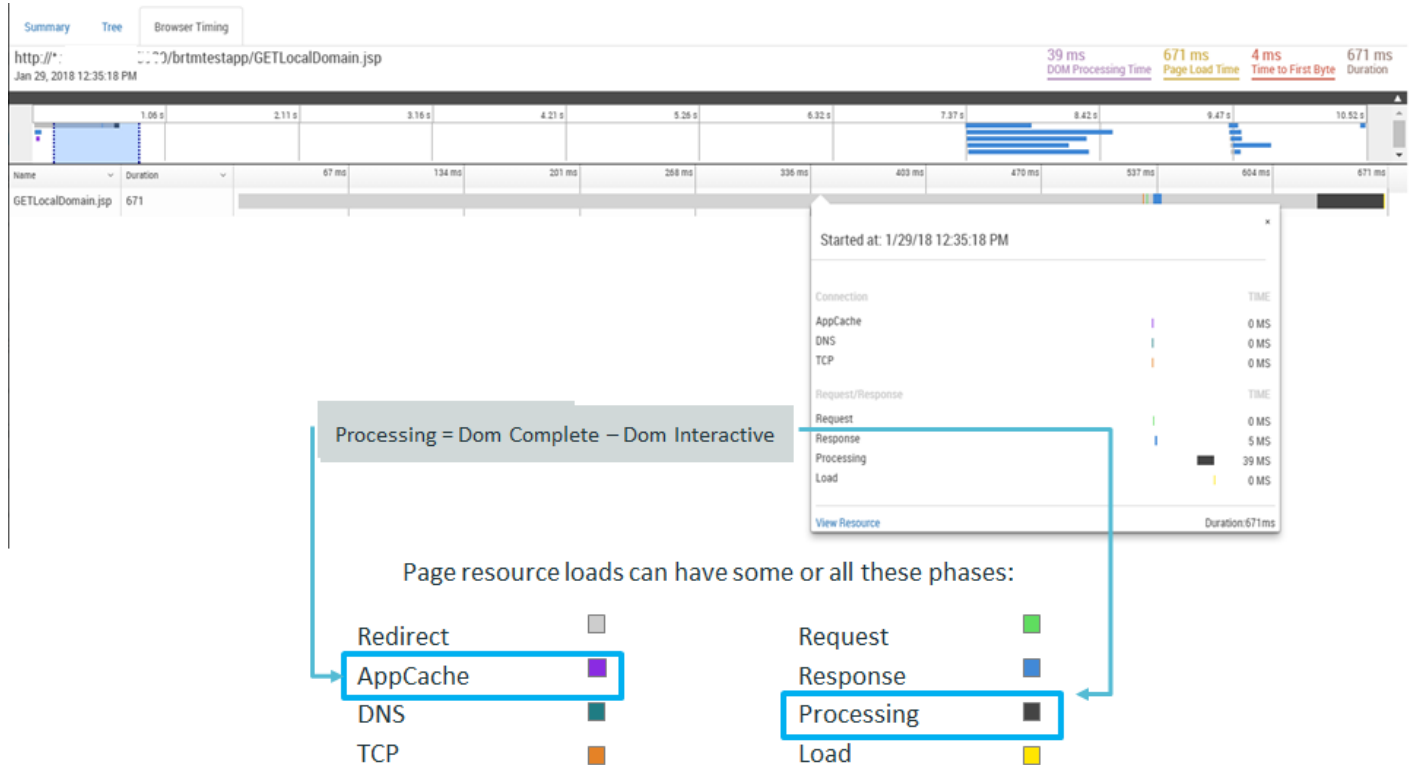
La cuadrícula incluye los siguientes tipos de filas:

- Filas de carga de página  
 Cuando el seguimiento seleccionado representa una carga de página en disco, la propia página se representa en la cuadrícula. (Una carga de página flexible simplemente actualiza la página actual utilizando JavaScript). La última columna de la cuadrícula muestra el intervalo de tiempo seleccionado, que se divide en diez períodos iguales. Una barra gris representa la duración completa de la carga de página y las bandas de color representan diversas "fases" en la carga de página. Es posible que las duraciones de las fases no sumen la duración total de la carga de página porque la duración total incluye la duración del Control de tiempo del explorador. La duración del Control de tiempo del explorador incluye tiempos relacionados con la red y la conmutación de contexto del explorador. Para ver el desglose del tiempo de un seguimiento, pase el puntero del ratón por encima de la fase.  
 Las cargas del recurso de la página pueden tener algunas o todas las fases siguientes:

- – Redirección
- – AppCache
- – DNS
- – TCP
- – Solicitud
- – Respuesta
- – Procesamiento
- – Carga

El Agente del explorador informa directamente sobre la mayoría de las fases, pero hay dos fases que se calculan como se muestra en el siguiente gráfico:

- AppCache: DNS (búsqueda de dominio) - Obtención
- Procesamiento: DOM completo – DOM interactivo



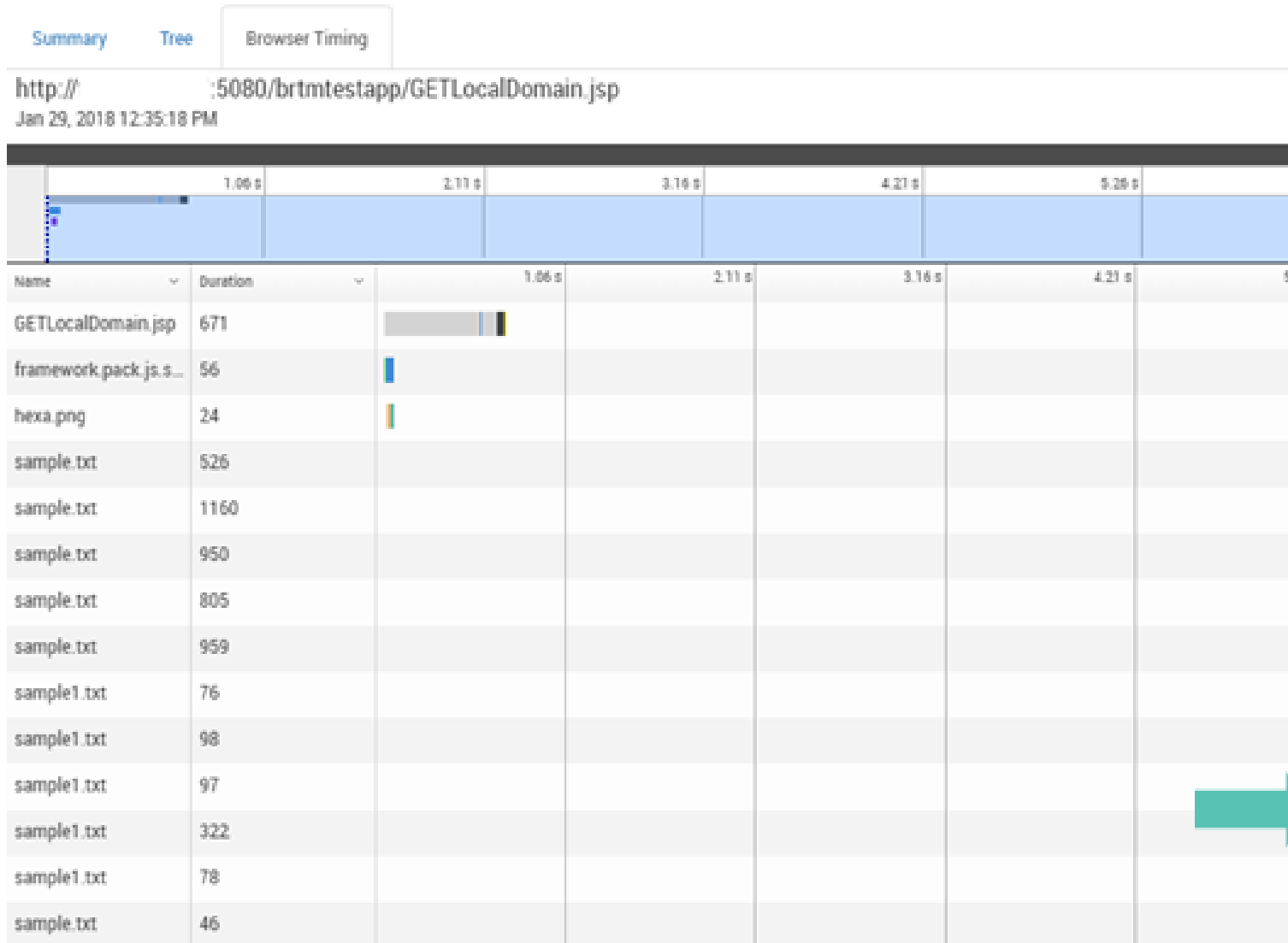
- Filas de carga de recurso

Las fases del recurso no se muestran en la pila (gráfico de tarta), por lo que no se pueden ver los datos sin procesar de las fases. Cada recurso que la página descarga contiene una fila en la cuadrícula Control del tiempo del explorador. De la misma manera que con la información de carga de página, se pueden ver más detalles para cada recurso pasando el puntero del ratón sobre el gráfico en la cuadrícula.

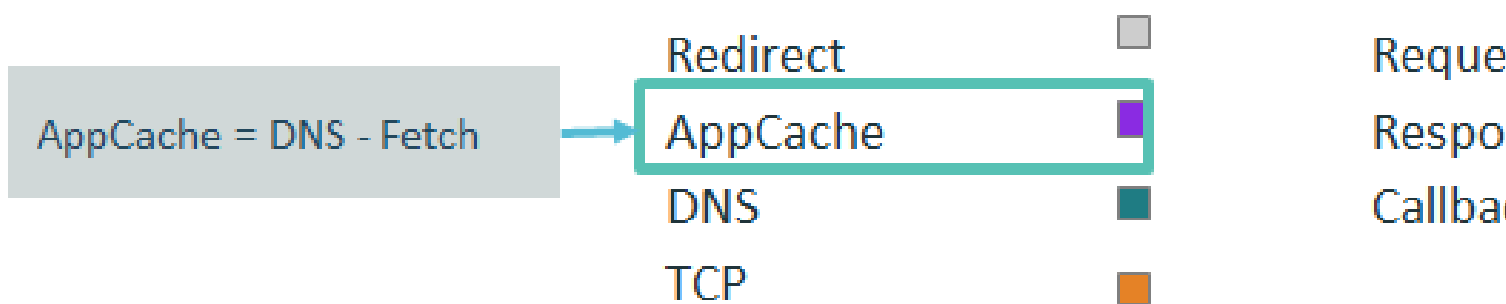
Las cargas de recurso pueden tener algunas o todas las fases siguientes:

- AppCache
- DNS
- TCP
- Solicitud
- Respuesta
- Tiempo de ejecución de la devolución de llamada

Los recursos que la página descarga muestran el mismo modo que las cargas de página, pero las fases son ligeramente diferentes. El Agente del explorador informa sobre todas las fases excepto AppCache. AppCache se calcula como DNS - Obtención. El siguiente gráfico muestra las fases de carga de recurso:



Resource loads can have some o



Es posible que los valores de seguimiento del recurso no coincidan con los valores de tiempo de los mismos seguimientos en la ficha Red de Firefox. Además, la vista **Control del tiempo del explorador** no muestra algunos de los recursos que aparecen en la ficha Red. Los valores no coincidentes se producen para todos los recursos porque el valor de tiempo de la ficha Red de Firefox es desde el inicio de la solicitud al final de la respuesta. Sin embargo, la duración del Control de tiempo del explorador incluye tiempos relacionados con la red y la conmutación de contexto del explorador. De forma predeterminada, se descartan los recursos que faltan en la vista Control del tiempo del explorador (no son configurables). Estos recursos incluyen solicitudes por el cliente para la configuración del perfil y para enviar las respuestas de métrica. El Control del tiempo del explorador no informa sobre la métrica de la página para los recursos necesarios para el Agente del explorador. Es posible que el valor de duración total no coincida en todos los exploradores ya que se agrega el tiempo de ejecución de la devolución de llamada para ajustar el valor de duración.

#### NOTE

Es posible que se redondee el valor de tiempo un milisegundo hacia arriba o hacia abajo.

## Diagnóstico de problemas de rendimiento del sistema

El Visor de seguimiento de transacciones de las propiedades del sistema proporciona el tiempo de la CPU y los datos de monitorización de la contención de subprocesos para el seguimiento de la transacción en los métodos de la API del servlet.

#### NOTE

**Más información:** [Examen de los componentes individuales y de los datos de seguimiento](#).

Los métodos a menudo se ejecutan cuando el usuario hace clic en un vínculo, envía un formulario o realiza otro tipo de acción en un sitio web. Las propiedades del sistema pueden ayudarle a entender el origen de una ralentización, de un servidor que se bloquea o de un uso excepcionalmente elevado de la CPU como, por ejemplo:

- DX APM muestra métricas de detención pero ninguna transacción aparece cuando se ejecuta un seguimiento de la transacción. Esta situación puede deberse a que las transacciones no se están completando y a que Enterprise Manager está obteniendo información incompleta sobre el bloqueo del servidor del agente.
- El uso de la CPU para una aplicación es bajo, pero hay largos tiempos de respuesta. Esta situación puede indicar que todos los subprocesos de una operación están interbloqueados, bloqueados o en espera.
- Un método está tardando mucho tiempo en cargarse; un subproceso puede estar utilizando una gran cantidad de memoria de la CPU.

Los datos de tiempo permiten diagnosticar subprocesos de método para los problemas de rendimiento.

#### Siga estos pasos:

1. En la ficha **Transacciones comerciales**, haga clic en el seguimiento de la transacción que desee. Los componentes de la transacción individual aparecen en una pila gráfica del panel **Detalles de la transacción**.
2. En el panel **Información de la transacción**, seleccione **Propiedades del sistema** en la lista desplegable **SELECCIONAR UNA VISTA**.
3. Examine la información en la cuadrícula. Los valores de datos se muestran como duración en milisegundos, como el porcentaje del tiempo total invertido en cada método o subproceso. Busque los valores altos para saber qué subprocesos utilizan una potencia de procesamiento alta, si están en espera o bloqueados.

#### TIP

Al hacer clic en una fila en la cuadrícula, se resalta el seguimiento correspondiente en la pila gráfica y viceversa.

#### Métricas del Agente de Java

**Tiempo total de la CPU:** el tiempo total de la CPU para el subproceso actual, para cualquier subproceso o para ningún subproceso. El valor es el total del tiempo del sistema de la CPU más el tiempo de usuario de la CPU.

**User CPU Time:** el tiempo que tarda el procesador en ejecutar el código de programa o el código en las bibliotecas para una transacción cuando la máquina virtual Java admite la medición del tiempo de la CPU.

**System CPU Time:** el tiempo que tarda el código en ejecutarse en el kernel del sistema operativo en una transacción de una aplicación monitorizada cuando la máquina virtual Java admite la medición del tiempo de la CPU.

**Wait Time:** el tiempo aproximado que un subproceso de transacción ha estado en el estado WAITING o TIMED\_WAITING cuando la máquina virtual Java admite la monitorización de la contención de subprocesos.

**Blocked:** el tiempo aproximado que un subproceso ha estado en estado BLOCKED cuando la máquina virtual Java admite la monitorización de la contención de subprocesos.

**Otros:** el tiempo aproximado transcurrido distinto a la suma del tiempo de la CPU, el tiempo bloqueado y el tiempo de espera.

**Allocated Memory:** el número aproximado de bytes adjudicados a la memoria dinámica de subprocesos de transacciones cuando la máquina virtual Java admite la medición de la adjudicación de memoria de subprocesos.

**Path:** el nombre del recurso completo del subproceso.

#### **Métricas del Agente de .NET/.NET Core**

**User CPU Time:** el tiempo que tarda el procesador en ejecutar el código de programa o el código en las bibliotecas para una transacción cuando el CLR de .NET/.NET Core admite la medición del tiempo de la CPU.

**System CPU Time:** el tiempo que tarda el código en ejecutarse en el kernel del sistema operativo en una transacción de una aplicación monitorizada cuando el CLR de .NET/.NET Core admite la medición del tiempo de la CPU.

4. Encuentre más detalles sobre las **Propiedades del sistema en Detalle del componente** Los valores de tiempo están en milisegundos. Estas propiedades se aplican al control del tiempo del sistema:

**Block Time (ms):** el tiempo aproximado que un subproceso ha estado en estado BLOCKED cuando la máquina virtual Java admite la monitorización de la contención de subprocesos.

**CPU System Time (ms):** el tiempo que tarda el código en ejecutarse en el kernel del sistema operativo en una transacción de una aplicación monitorizada cuando la máquina virtual Java admite la medición del tiempo de la CPU.

**Tiempo de la CPU (milisegundos):** el tiempo total de la CPU para el subproceso actual, para cualquier subproceso o para ningún subproceso. El valor es el total del tiempo del sistema de la CPU más el tiempo de usuario de la CPU.

**CPU User Time (ms):** el tiempo que tarda el procesador en ejecutar el código de programa o el código en las bibliotecas para una transacción cuando la máquina virtual Java admite la medición del tiempo de la CPU.

**Other Time (ms):** el tiempo aproximado transcurrido distinto a la suma del tiempo de la CPU, el tiempo bloqueado y el tiempo de espera.

**Tiempo de espera (milisegundos):** el tiempo aproximado transcurrido en que un subproceso de transacción ha estado en espera o en el estado TIMED\_WAITING cuando la máquina virtual de Java admite la monitorización de la contención de subprocesos.

## **Detección y análisis de errores y detenciones**

Una *detención* es una transacción o el componente de una transacción que no se ha completado en el umbral de tiempo especificado. Una vez se haya determinado la ubicación de una transacción o componente detenidos, se puede realizar lo siguiente:

### **Cómo analizar errores y detenciones**

#### **Cuándo se debe utilizar este escenario**

Utilice este escenario cuando haya un problema de rendimiento de la aplicación tal y como se muestra en un cuadro de mandos de DX Application Performance Management o cuando se informe al usuario con una notificación.

#### **Requisitos previos**

Aíse la ubicación del problema antes de empezar.

Los agentes recopilan datos de las transacciones y envían estos datos a Enterprise Manager para su procesamiento y visualización. Estos datos incluyen información sobre los errores y las detenciones de la aplicación.

### Error

Un error es una excepción que comunican los códigos de error de JVM o HTTP. Por ejemplo:

- Un estado de error HTTP como, por ejemplo: 404 No se encuentra la página
- Una excepción de SQL
- Una excepción de Java

### Detención

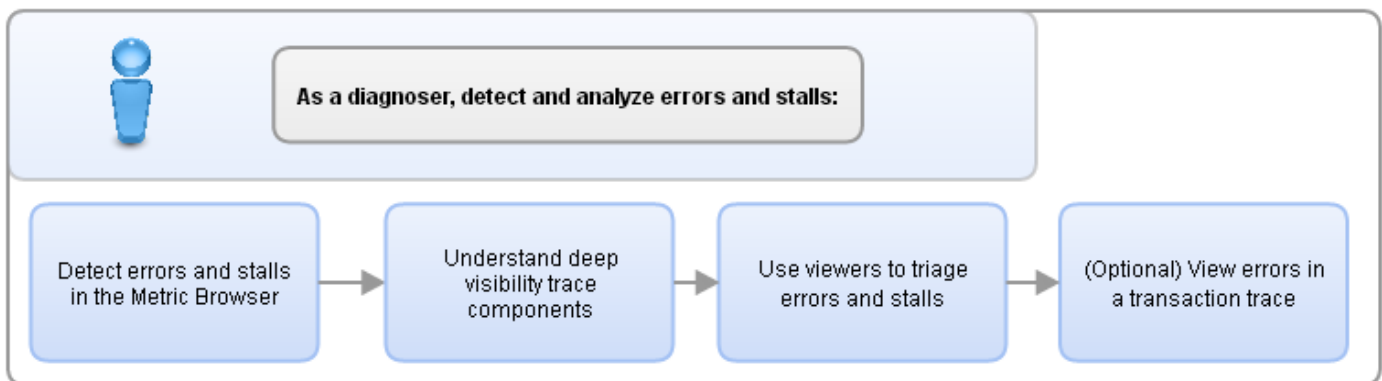
Una detención es una transacción o el componente de una transacción que no se ha completado en el umbral de tiempo especificado.

Se pueden realizar estas tareas:

- Detectar y evaluar la causa de los errores graves y de las detenciones en el momento en que ocurren, así como monitorizar los eventos relacionados.
- Determinar la frecuencia y naturaleza de los errores.
- Determinar la causa raíz de un problema.

El siguiente diagrama describe cómo analizar errores y detenciones para identificar la causa raíz de un problema de rendimiento de la aplicación.

**Figure 9: 9.8 Detección y análisis de errores y detenciones**



### Siga estos pasos:

1. Detecte errores y detenciones en la Vista de métrica.
2. Comprenda los componentes de seguimiento de la visibilidad exhaustiva.
3. Utilice los visores para evaluar los errores y las detenciones.
4. (Opcional) Visualice los errores en un seguimiento de la transacción.

### Detección de errores y detenciones en la Vista de métrica

Puede detectar y evaluar la causa de los errores graves y de las detenciones en el momento en que ocurren. Puede monitorizar agentes y componentes visualizando la información detallada en la ficha **Vista de métrica**.

DX Application Performance Management actualiza la visualización de la información de los errores y detenciones cada 15 segundos.

**Siga estos pasos:**

1. Vaya a Team Center.
2. En la **Vista de métrica**, vaya al agente o componente que desea monitorizar y seleccione la ficha **Errores** en la parte inferior de la página.  
La ficha **Errores** muestra los datos obtenidos de un agente sobre una máquina virtual Java o CLR de .NET. Si se notifica algún error o detención para el agente o componente, aparecerá una lista de errores y detenciones.  
– Descripción de la ficha Error seleccionada.
3. Seleccione la ficha **Seguimientos**.  
Descripción de la ficha Seguimientos seleccionada.
4. Haga clic en Marca de tiempo para ordenar. A medida que se van produciendo nuevos errores o detenciones, irán apareciendo por orden de clasificación.

**Componentes de seguimiento de la visibilidad exhaustiva**

Quando se activa la instrumentación inteligente, los agentes detectan y recopilan automáticamente información detallada sobre los componentes de las transacciones a nivel de método. Los agentes detectan e instrumentan automáticamente los componentes de visibilidad exhaustiva sin tener que utilizar las directivas de ProbeBuilder (PBD). Los componentes de visibilidad exhaustiva que se ven en las transacciones detenidas solo contienen el nombre de la clase, el nombre del método y la duración. En función de los requisitos y del entorno, se puede configurar la profundidad y el alcance de la visibilidad de seguimiento de la visibilidad exhaustiva. Por ejemplo, se puede configurar si el agente detecta e instrumenta automáticamente una cantidad baja, media o alta de código de la aplicación. Para obtener más información, consulte [Configuración de la instrumentación inteligente](#).

**NOTE**

La instrumentación inteligente solo está disponible para los Agentes de Java, pero no para los Agentes de .NET.

**Detección de errores en la Vista de métrica**

Los agentes recopilan datos de las transacciones y envían estos datos a Enterprise Manager para su procesamiento y visualización en un visor de datos. Estos datos incluyen información sobre los errores de la aplicación. Puede detectar y evaluar la causa de los errores en el momento en que ocurren. Puede monitorizar agentes y componentes visualizando la información detallada en la ficha **Vista de métrica**.

DX Application Performance Management actualiza la visualización de la información de los errores cada 15 segundos.

**Siga estos pasos:**

1. Vaya a Team Center.
2. En la **Vista de métrica**, vaya al agente o componente que desea monitorizar.
3. Busque la métrica Errores por intervalo. Si el valor es:  
= 0, no hay ningún error actual.  
> 0, vaya al paso 4 para seleccionar la ficha Seguimientos.
4. Seleccione la ficha **Seguimientos**.
5. Haga clic en el encabezado de una columna para ordenar las filas por el contenido de dicha columna. A medida que se van produciendo nuevos seguimientos, estos irán apareciendo por orden de clasificación. Los errores en la lista de seguimientos aparecen en color rojo.
6. Vea el error en el seguimiento de la transacción que Introscope ha recopilado automáticamente.  
Si no ve los seguimientos automáticos de la transacción, consulte la sección Seguimientos de la transacción recopilados automáticamente.
7. Seleccione la ficha **Errores**.  
La ficha Errores muestra datos que un agente ha obtenido de una máquina virtual Java o CLR de .NET. Si se notifica algún error para el agente o componente, aparecerá una lista de errores. Haga clic en el encabezado de una columna

para ordenar las filas por el contenido de dicha columna. A medida que se van produciendo nuevos errores, estos irán apareciendo por orden de clasificación.

8. Seleccione una instantánea de error para obtener más información sobre el error, incluida la ruta de llamada y los parámetros. Utilice el Visor de eventos históricos y el Visor de errores en directo para evaluar los problemas.

### **Visualización de errores en un seguimiento de la transacción**

Puede ver información sobre el error, incluidos los componentes de visibilidad exhaustiva, dentro de un seguimiento de la transacción.

Puede utilizar dos métodos para recopilar seguimientos de la transacción y ver información sobre el error:

- Ejecute manualmente un seguimiento de la transacción.
- Cuando se activa la instrumentación inteligente, Introscope recopila automáticamente el seguimiento de la transacción cuando se produce un error.

Cuando un error activa el seguimiento automático de transacciones, se muestran los detalles de estos componentes:

- El componente que se ha producido la excepción incluye las propiedades del componente.
- El primer componente del seguimiento de la transacción muestra la propiedad Auto Trace Trigger Criteria como Error.

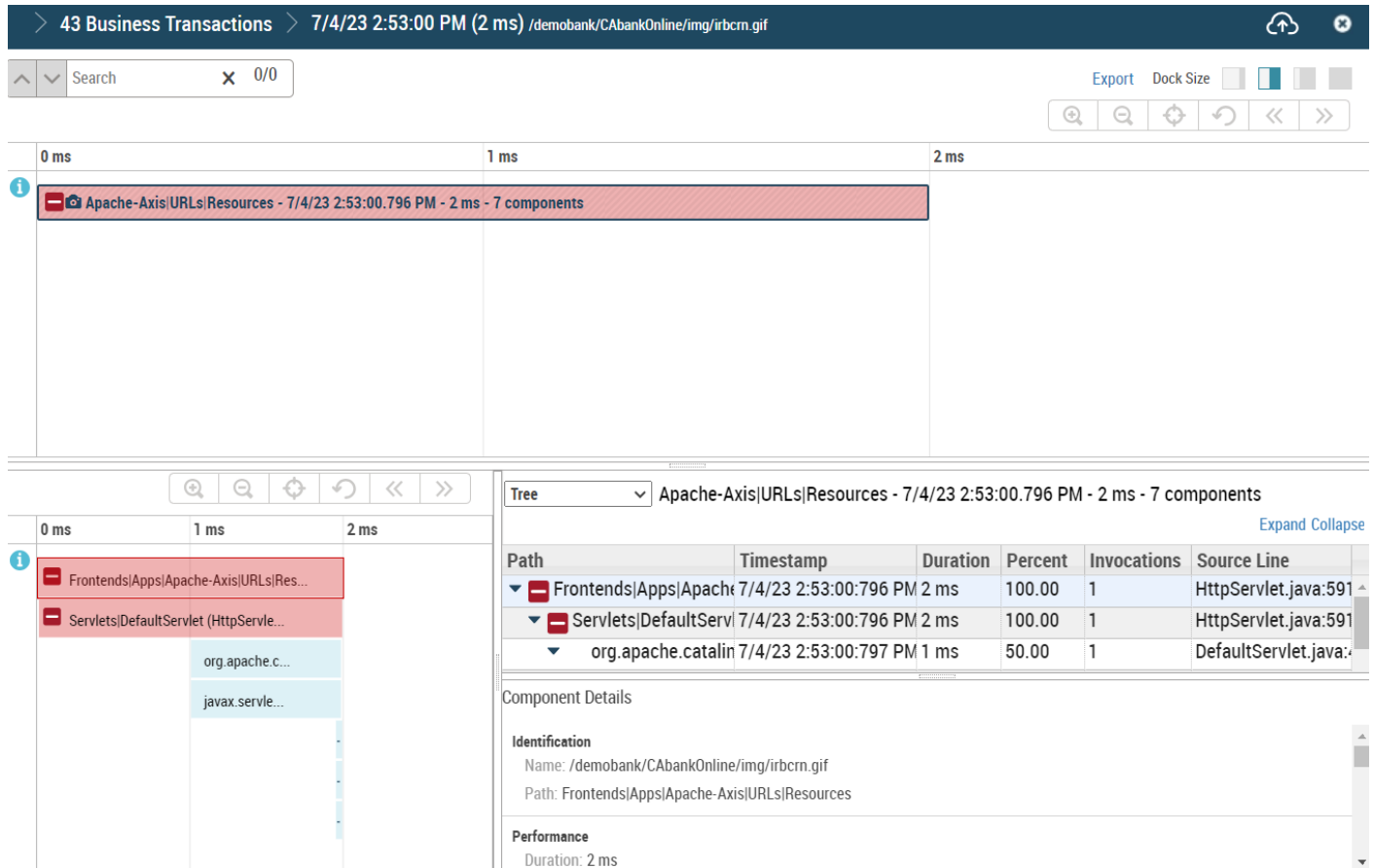
### **Siga estos pasos:**

1. Vaya a Team Center.
2. Haga clic en **Vista de métrica**.
3. Seleccione una aplicación en el árbol de métrica.
4. Haga clic en la ficha **Vista de errores** en el panel inferior.

**Nota:** En el modo en directo, la ficha Seguimientos muestra los eventos de seguimiento de transacciones de los últimos 20 minutos. No se muestran los eventos de seguimiento de transacciones anteriores a 20 minutos en el modo en directo.

5. Seleccione uno de los errores enumerados para ver información detallada.  
Una pantalla muestra la descripción completa del error para el error seleccionado.





6. Determine la causa raíz del problema de rendimiento de la aplicación.
- Utilice la información de identificación que se encuentra en las fichas disponibles para recopilar detalles específicos sobre el problema. Vea estos campos: marca de tiempo, duración, descripción, ID de usuario (si alguno está asociado con el problema), mensaje de error, hora de llamada y ruta.
- Se puede realizar lo siguiente:
- Ordene las columnas para encontrar las llamadas o los métodos con el tiempo de respuesta más largo o con errores.
  - Utilice la ficha Buscar para filtrar los resultados.
  - Utilice los mensajes de error y otro tipo de información para conocer más información sobre el problema.
- Tras identificar a los componentes que aparentemente son responsables de este problema, el personal de operaciones puede solicitar un cambio en el código de la aplicación para solucionar la incidencia.

## Análisis de las instantáneas de error y detenidas

De forma automática, los agentes detectan y recopilan información detallada sobre los componentes de la transacción para el nivel del método. Estos datos incluyen información sobre los errores y las detenciones de la aplicación:

- **Error**

Determinados eventos en una aplicación causan errores de la transacción como, por ejemplo:

  - Un estado de error HTTP como, por ejemplo: 404 No encontrado
  - Una excepción en un método
  - Una excepción en código sin instrumentar como, por ejemplo, en un componente exhaustivo.
  - Una implementación del rastreador de errores personalizados en la lógica del marco de trabajo o de la comunicación
- **Detención**

Una detención es una transacción o el componente de una transacción que no se ha completado en el umbral de tiempo especificado.

Una *instantánea* muestra rutas de seguimiento de la transacción a un error o detención y muestra detalles sobre lo que estaba ocurriendo cuando se ha producido el evento.

Una transacción puede incluir errores y detenciones, y puede activar las instantáneas asociadas. Por ejemplo, una transacción tiene 100 llamadas. La llamada 3 empieza a ejecutarse lentamente y desencadena una instantánea de detención. Tras algunas llamadas, la llamada 6 tiene un error problemático, que activa una instantánea de error. La llamada 81 encuentra un error diferente, activando otra instantánea de error.

En el Visor de seguimiento de transacciones, la vista de **árbol** muestra todas las llamadas de todas las rutas posibles en una transacción. La vista de **instantánea** muestra una ruta a través de una transacción. Se trata de la ruta de llamada directa de una detención o error específicos. Por lo tanto, en vista de **árbol**, normalmente verá varias capas de llamada, mientras que en la vista de instantánea, las instantáneas de error y de detención son solo de una capa.

## NOTE

**Más información:** [Examen de los componentes individuales y de los datos de seguimiento.](#)


## Examine las instantáneas para investigar los errores y detenciones

Una instantánea le ayuda a realizar estas tareas:

- Detectar y evaluar la causa de los errores graves y de las detenciones en el momento en que ocurren, así como monitorizar los eventos relacionados.
- Determinar la frecuencia y naturaleza de los errores.
- Determinar la causa raíz de un problema.

### Siga estos pasos:

1. En la ficha **Transacciones comerciales**, seleccione **Instantánea** en la lista desplegable **Tipo de seguimiento**.
2. Seleccione el seguimiento que desea investigar.  
Los componentes de la transacción individual aparecerán en una pila gráfica (gráfico de tarta) **Detalles de la transacción**.

- Una fila roja y un cuadro rojo con un icono de signo menos blanco  identifican un seguimiento con un error.
3. En la pila gráfica, tenga en cuenta las características de la instantánea utilizando estos identificadores:

Un icono de cámara



identifica una transacción normal con una o más instantáneas relacionadas.

Un prefijo de **Instantánea de error** delante del nombre del componente identifica a una sola transacción con una instantánea, pero sin ninguna ruta de seguimiento relacionada con un error o detención. Es posible que una transacción no tenga ningún seguimiento relacionado en estos casos:

- Está utilizando un agente que no está actualizado a la versión actual.
- Se produce un problema en la transacción antes de que se extraiga la información de correlación de la carga de la solicitud. En este caso, la información de seguimiento no está incluida en el evento.
- El agente no informa sobre cada seguimiento debido a que el agente se basa en muestras. De forma predeterminada, los agentes realizan muestras del comportamiento de las transacciones mediante el seguimiento periódico de cada dirección URL única normalizada en una aplicación. Un evento de error que no tiene ningún seguimiento de la transacción puede producirse a causa de la implementación de la detección de errores (rastreador del agente) o porque se ha alcanzado un umbral de fijación para los seguimientos en Enterprise Manager o en el agente.

4. En el panel **Seguimiento de la transacción**, seleccione un seguimiento de interés.

5. En el panel **Información de la transacción**, seleccione **Instantánea** de la lista desplegable.

La vista de **instantánea** muestra las rutas de seguimiento en orden jerárquico de llamada. Tenga en cuenta que un seguimiento en la cuadrícula es como un árbol con diferentes ramas y hojas. Una instantánea es una ruta desde el conjunto de ramas hasta una hoja. Puede tener varias instantáneas con cada una de ellas representada como una "raíz" en la cuadrícula. Una instantánea ayuda a detectar errores o detenciones que se han producido en varias ramas. El árbol expandido se llama como la instantánea y muestra donde se ha producido el problema en la ruta de la llamada. El árbol permite recorrer el examen de datos e ir a componentes específicos para identificar los problemas de rendimiento. Los valores de datos ayudan a entender cómo un valor inicial se ve afectado por una serie de valores intermedios. El valor **Tipo de instantánea** muestra Error o Detención.

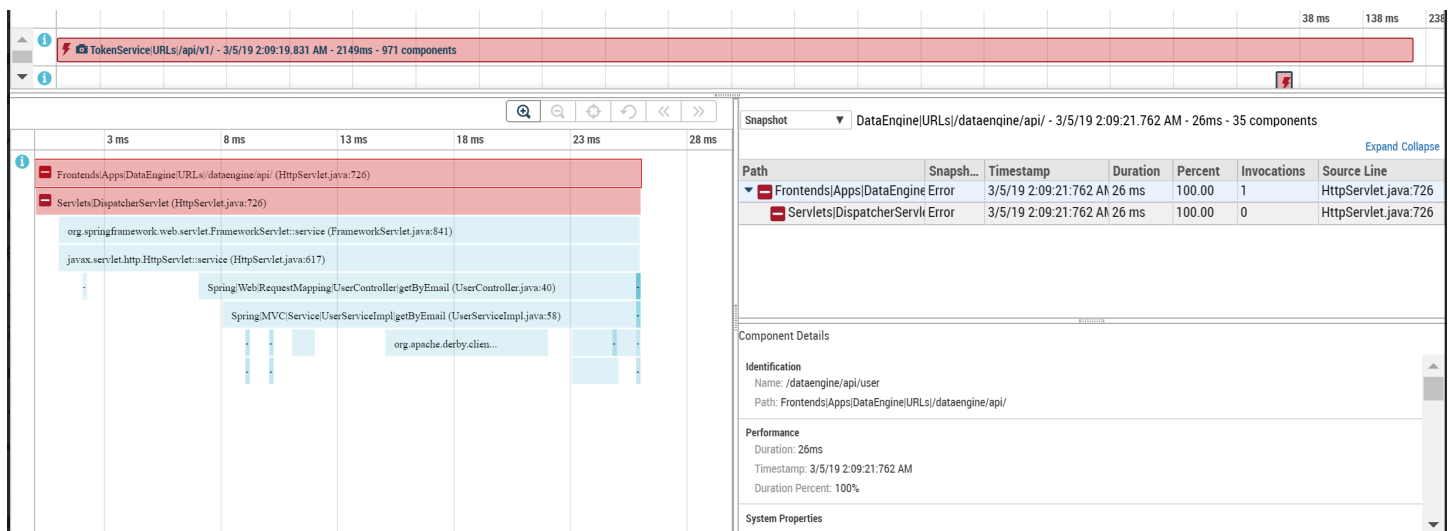
### TIP

Al hacer clic en una fila en la cuadrícula, se resalta el seguimiento correspondiente en la pila gráfica y viceversa.

6. Examine la instantánea para encontrar la causa raíz del problema.
7. Identifique los componentes que aparentemente son la causa del problema. El personal de operaciones puede solicitar un cambio en el código de la aplicación para solucionar el problema.

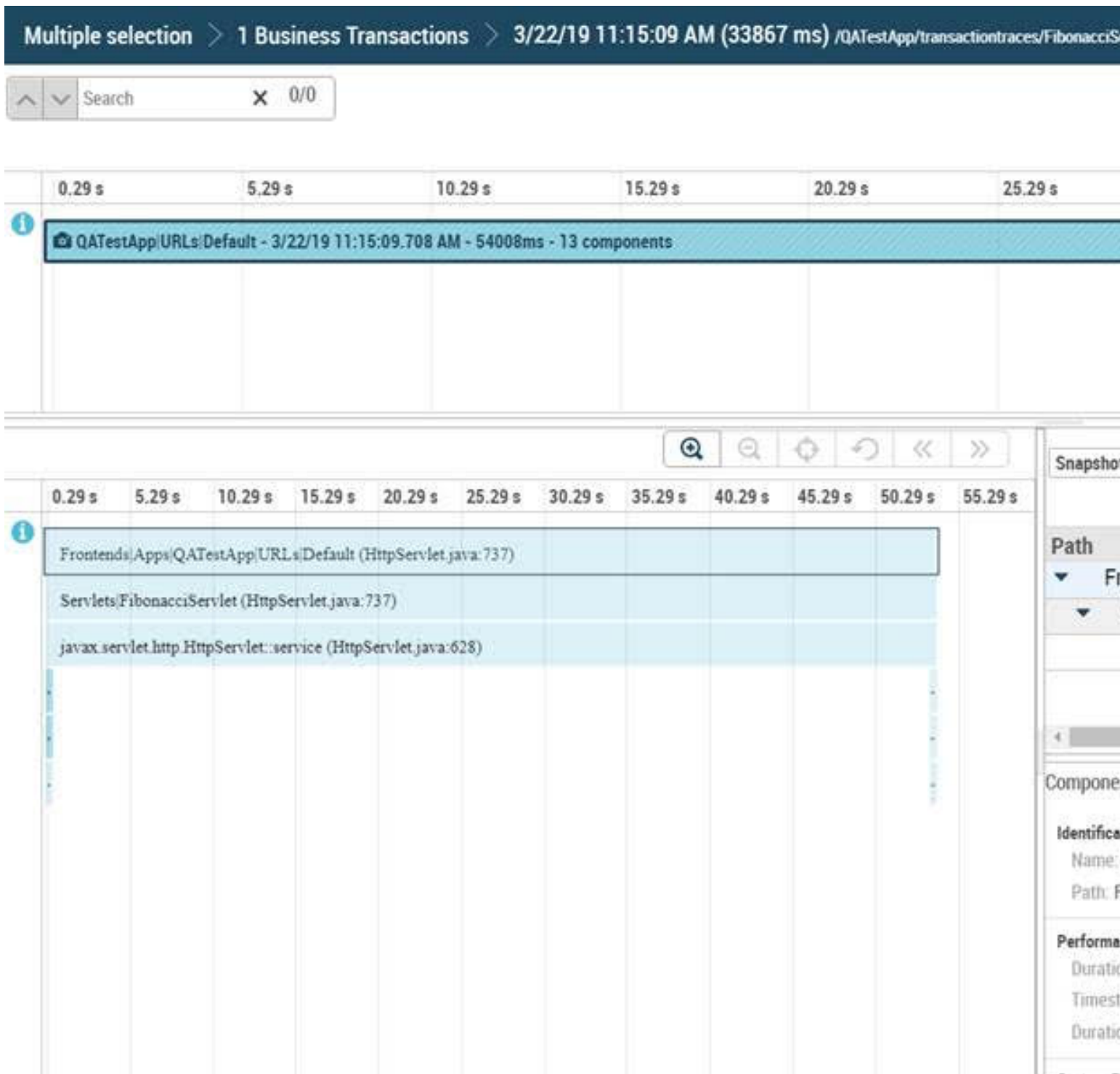
### Ejemplo: Transacción con una instantánea de error relacionada

El siguiente gráfico muestra una transacción con una instantánea de error relacionada. Observe el icono de la cámara en la parte izquierda del seguimiento de la transacción y el valor **Error** en la columna **Instantánea**.



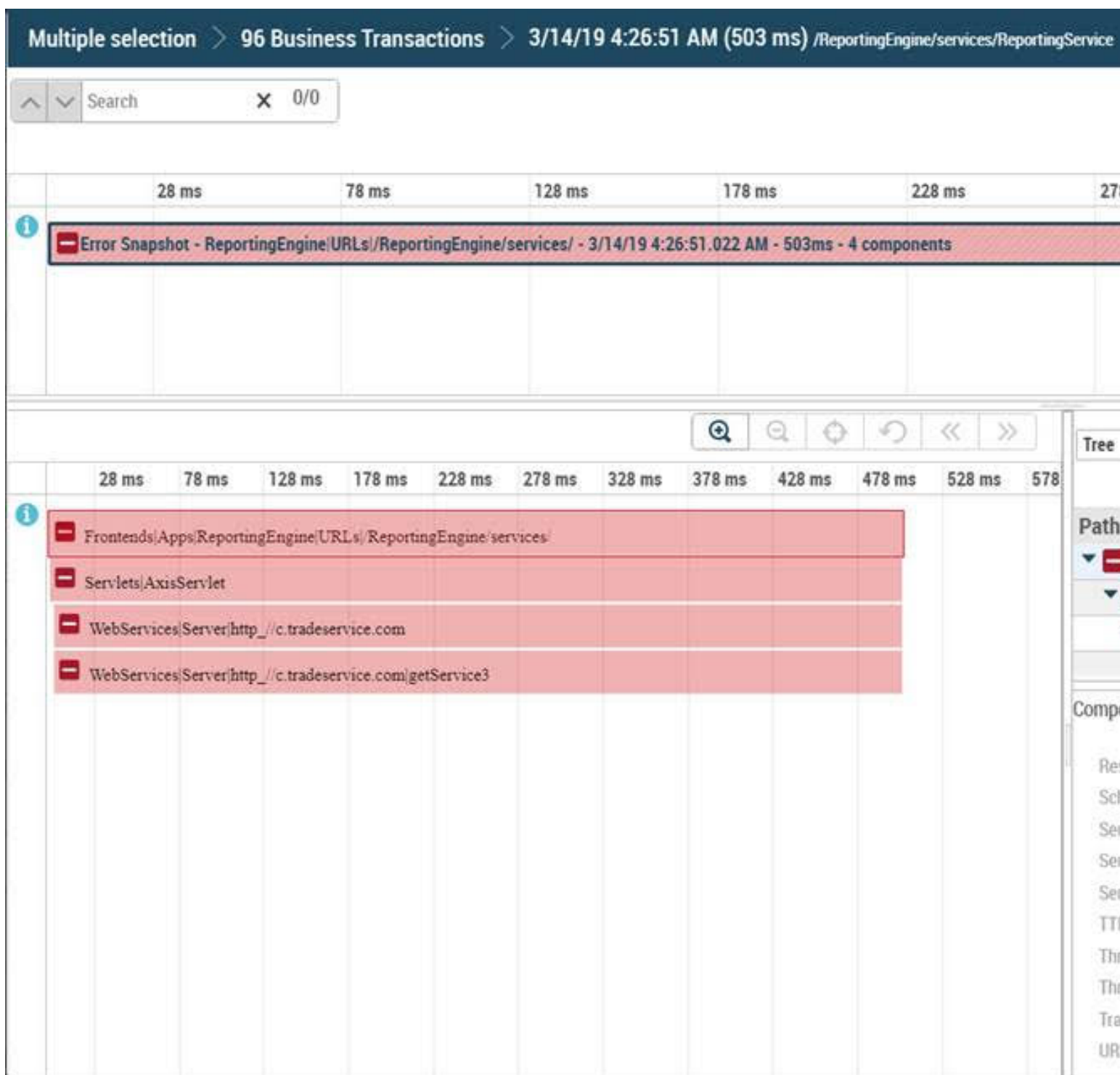
### Ejemplo: Transacción con una instantánea de detención relacionada

El siguiente gráfico muestra una transacción normal con una instantánea de detención relacionada. Observe el icono de la cámara y el valor de **Detención** en la columna **Instantánea**.



### Ejemplo: Transacción única con una instantánea pero sin ningún seguimiento relacionado con errores o detenciones

El siguiente gráfico muestra una sola transacción con una instantánea pero sin ninguna ruta de seguimiento relacionada con un error o detención. Tenga en cuenta el prefijo **Instantánea de error**, pero no el icono de la cámara.



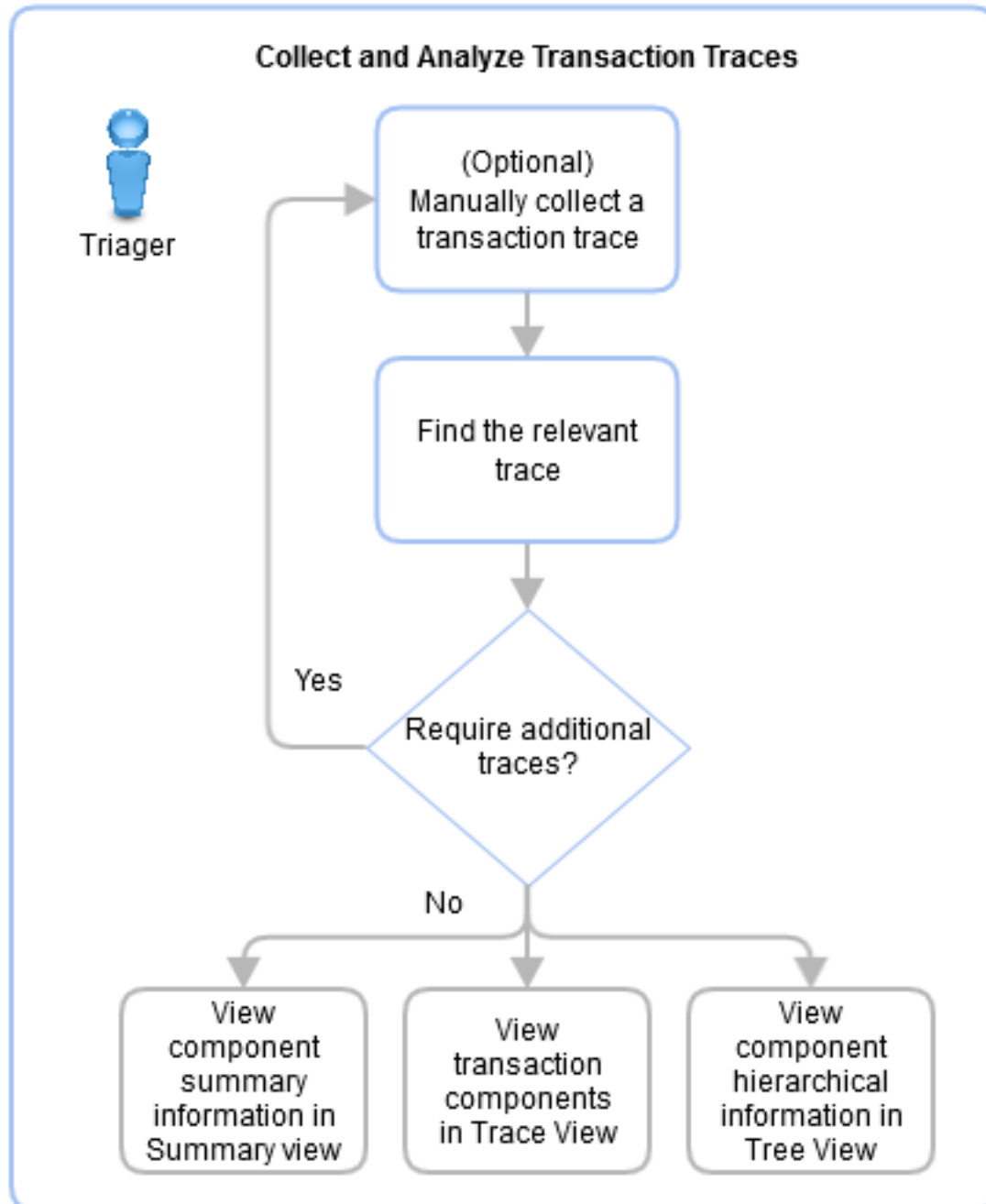
## Recopilación y análisis de los seguimientos de la transacción

Como emisor de diagnósticos, evaluador de errores o administrador, puede ver información detallada acerca de los componentes de seguimiento de la transacción como los métodos. Esta información le ayuda a identificar la causa raíz de los problemas de rendimiento de las aplicaciones. Con Transaction Tracer, puede examinar el seguimiento de las

transacciones recopiladas de forma automática o manual. Aparecerá la información debido a que los componentes se han instrumentado mediante PBD o se ha activado la instrumentación inteligente.

Este diagrama muestra cómo identificar la causa raíz de los problemas de rendimiento de las aplicaciones mediante la visualización de información detallada sobre los componentes de la transacción.

**Figure 10: Recopilación y análisis de los seguimientos de la transacción**



## Descripción general del seguimiento de la transacción

Transaction Tracer monitoriza la actividad de las transacciones individuales a medida que fluyen a través de los límites de los agentes admitidos: Los agentes admiten la monitorización de aplicaciones de Java, .NET y Node.js. El seguimiento de la transacción entre procesos monitoriza las llamadas de las transacciones entre diferentes instancias de máquina virtual de Java, CLR (Common Language Runtime) y Node.js. La monitorización puede producirse en equipos locales o remotos. La visualización de los detalles de la transacción entre procesos le ayuda a realizar investigaciones sobre problemas a través de los procesos de la transacción.

Existen varias formas de recopilar seguimientos de la transacción:

- [Introscope recopila automáticamente los seguimientos de la transacción.](#)
  - Cuando se activa la instrumentación inteligente, Introscope recopila automáticamente el seguimiento de la transacción en determinadas situaciones.  
**Nota:** La instrumentación inteligente solo está disponible para agentes de Java, PHP y Node.js, no en los agentes de .NET.
  - Introscope recopila con regularidad [un seguimiento de la transacción de muestra](#).
- [Recopilación manual de un seguimiento de la transacción](#)

Una vez se inicia la sesión de seguimiento de la transacción, las transacciones que coinciden con los criterios de filtro aparecen en Workstation o en WebView. Puede ver la información de seguimiento en la ficha Transaction Tracer, incluidos los eventos de la transacción como seguimientos y errores de la transacción.

## Seguimientos de transacciones recopilados automáticamente

Cuando se activa la [instrumentación inteligente](#), Introscope recopila automáticamente un seguimiento de la transacción cuando se producen las siguientes acciones:

- El análisis diferencial detecta la inestabilidad de una aplicación.  
**Nota:** Los seguimientos automáticos de la transacción del análisis diferencial requieren la versión del agente 10.0 o posterior.
- Se produce un error.
- El rastreador `ComponentTimeAutoTraceTriggerTracer` se implementa y se supera el tiempo de respuesta de un componente
- Una API activa los seguimientos automáticos de la transacción en función de criterios personalizados.  
**Más información:** Póngase en contacto con los [Servicios de implementación de CA APM](#).

Los seguimientos de sobrecarga baja sumamente optimizados recopilan seguimientos de transacciones automáticos. Los seguimientos automáticos adquieren una menor sobrecarga del rendimiento que las ejecuciones manuales, las muestras u otros seguimientos de la transacción. Estos otros tipos de seguimientos de la transacción utilizan el filtrado del agente, que aumenta la sobrecarga.

Los seguimientos automáticos de la transacción tienen estas características:

- Son compatibles con los agentes de Java, PHP y Node.js. El agente de .NET no es compatible.
- Cada componente instrumentado por PBD tiene una métrica asociada en el árbol Investigator. Los componentes de visibilidad exhaustiva carecen de una métrica asociada.
- Los [componentes de visibilidad exhaustiva](#) contienen solamente el nombre de la clase, el nombre del método y la duración. Para front-ends y back-ends (por ejemplo, servlets, servicios web, llamadas SQL), el nombre se formateará según la función de la configuración de PBD.
- Incluyen seguimientos de las transacciones entre procesos  
**Nota:** Las transacciones entre procesos en seguimientos automáticos de la transacción solo son compatibles con aplicaciones Java.
- Los seguimientos automáticos de la transacción no muestran todas las propiedades de detalles del componente que muestran los otros tipos de seguimientos de la transacción.
- Las siguientes propiedades se muestran en ComponentProperties:

- El tipo de seguimiento es Normal.
- Si un error ha activado el seguimiento de las transacciones, el componente que ha producido la excepción incluye las propiedades del componente.
- El primer componente del seguimiento de la transacción muestra la propiedad `Auto Trace Trigger Criteria`.

Si no ve los seguimientos automáticos de la transacción, puede que sea por una de estas razones:

- La [instrumentación inteligente](#) no está activada.
- Se ha excedido el valor de fijación del número de seguimientos automáticos de la transacción por intervalo (`agent.deep.automatic.trace.clamp` property).

#### NOTE

**Más información:** [Sostenibilidad del agente](#)

Al ejecutar de forma manual un seguimiento y cualquier filtro manual que coincida con un seguimiento automático, Introscope recopila solo el seguimiento manual.

### **Transacciones entre procesos en los seguimientos automáticos de la transacción**

La visualización de las transacciones entre procesos en los seguimientos automáticos de la transacción le permite evaluar las transacciones entre niveles. Puede determinar el nivel donde se encuentra el obstáculo de una transacción problemática.

#### NOTE

Las transacciones entre procesos en seguimientos de transacciones automáticos solo son compatibles con aplicaciones Java.

### **Agentes ascendentes y descendentes**

Los agentes que monitorizan las transacciones puede ser ascendentes, descendentes o pueden ser tanto ascendentes como descendentes de otros agentes que monitorizan la misma transacción. Los agentes ascendentes pueden realizar llamadas entre procesos a los agentes descendentes. Las llamadas de las transacciones pueden realizar un seguimiento de más de dos procesos. Por lo tanto, los agentes que monitorizan procesos entre las primeras y las últimas llamadas de la transacción se colocan de manera ascendente y descendente de los otros agentes. Este es un ejemplo:

1. Está revisando un seguimiento de la transacción para una transacción problemática y advierte un tiempo de ejecución de 6 segundos (6000 ms).
2. En la **Vista de seguimiento**, se ven llamadas de un método del cliente, `dataservice.yourcompany.net/invoke`, al método del servidor `thirdparty.mycompany.net/invoke`.
3. Se puede apreciar que el método del servidor está realizando un gran número de llamadas a terceros

`3PP site data`

de terceros, que se instrumenta.

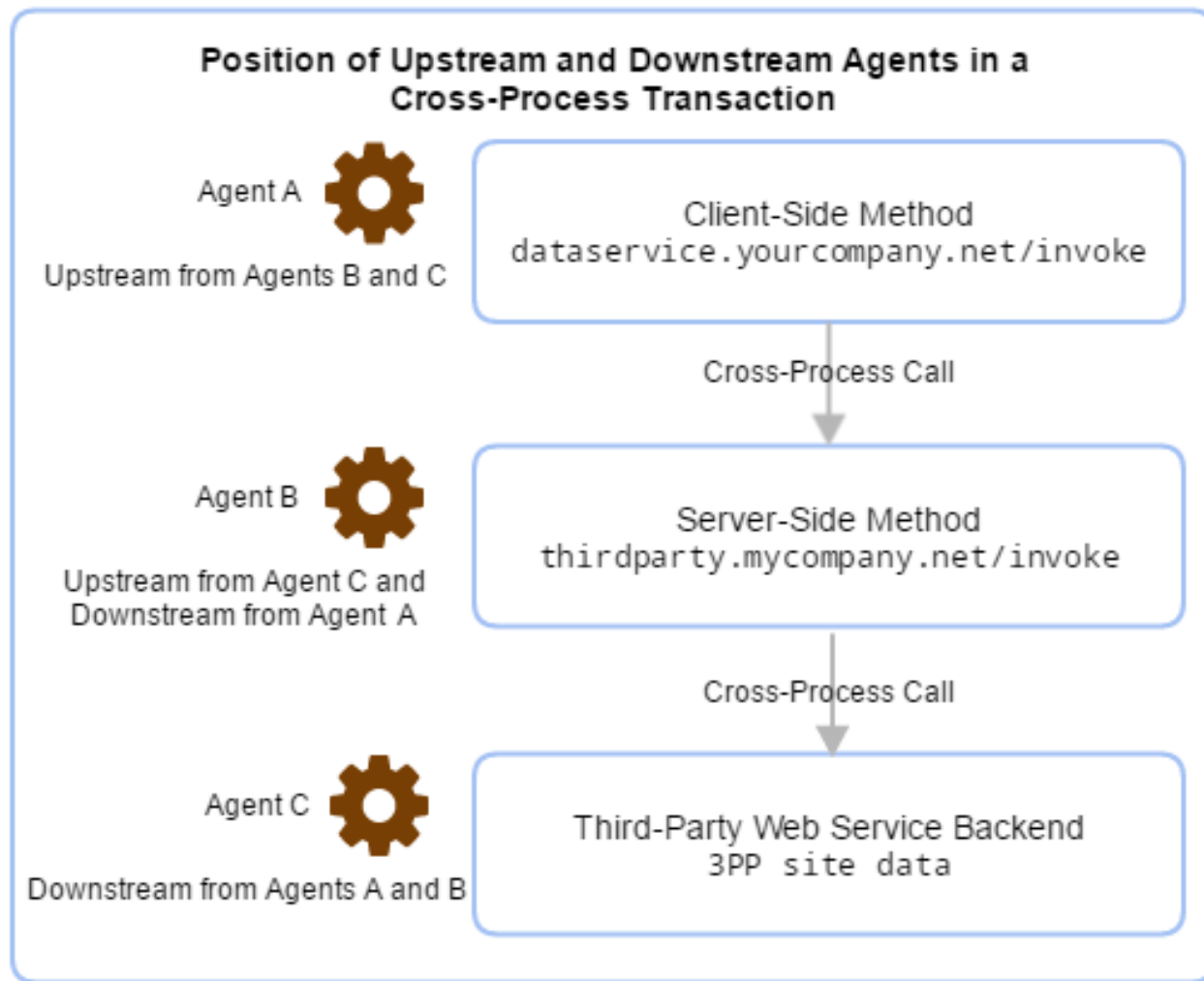
4. La **Vista de seguimiento** muestra que el

`3PP site data`

el back-end del servicio web está atendiendo solicitudes repetidas en una sucesión rápida. Este comportamiento indica que es probable que la lógica de programación, como un bucle anidado, provoque llamadas repetidas en el servicio del servidor. Se ha determinado que la operación de invocación del servidor es la responsable de la mayoría del tiempo de ejecución de la transacción global.

Este gráfico muestra las posiciones del agente en la transacción entre procesos de ejemplo.



**Figure 11: Diagrama de agentes ascendentes y descendentes**

Los agentes notifican problemas cuando se los encuentran y, a veces, inician seguimientos de la transacción. Antes de que el seguimiento automático de la transacción incluya llamadas entre procesos, solo los agentes ascendentes pueden informar de problemas y pueden recopilar seguimientos de la transacción.

#### **Visibilidad antes del seguimiento entre procesos en los seguimientos automáticos de la transacción**

Un agente próximo al inicio de una transacción no sabe si la transacción tiene un problema descendente. Al final de la transacción, un agente descendente informa de cualquier problema descendente al agente ascendente más próximo. Lo único que saben los agentes ascendentes es que la transacción no está acabada hasta que un agente descendente informa sobre su final. Al terminar la transacción, el agente ascendente más próximo al inicio de la transacción informa a Enterprise Manager de los problemas detectados como seguimientos de la transacción. Antes de que el seguimiento automático de la transacción incluyera la monitorización de llamadas entre procesos, los agentes descendentes que detectaban problemas nunca enviaban los seguimientos de la transacción a Enterprise Manager. Si los problemas detectados por los agentes descendentes no se notificaban al agente ascendente superior, estos problemas quedaban sin identificar. Esta situación hacía que no hubiera visibilidad sobre los problemas de las aplicaciones.

## **Visibilidad de extremo a extremo con un seguimiento entre procesos en los seguimientos automáticos de la transacción**

Puesto que se admite el seguimiento entre procesos, los agentes de Java pueden utilizar el almacenamiento en caché inteligente para enviar seguimientos automáticos de la transacción para las transacciones descendentes problemáticas entre procesos. Esta capacidad proporciona visibilidad de extremo a extremo para las transacciones de Java.

Tanto los agentes ascendentes como los descendentes que detectan transacciones problemáticas pueden activar los seguimientos automáticos de la transacción. También pueden enviar información de seguimiento de la transacción a Enterprise Manager. Los agentes que activan seguimientos automáticos pueden decidir al final de la transacción si desean enviar un seguimiento a Enterprise Manager. Este tiempo de toma de decisiones es especialmente útil para el análisis diferencial, cuando los umbrales de línea de referencia de Enterprise Manager activan seguimientos automáticos de la transacción.

Las transacciones pueden utilizar un protocolo compatible, por ejemplo, HTTP o SOAP, para invocar un servicio dentro del mismo proceso. En esta situación, los agentes que realizan llamadas entre procesos pueden posicionarse tanto como ascendentes o como descendentes de otros agentes. Cuando un agente ascendente recopila un seguimiento automático de la transacción, todos los agentes descendentes participantes también recopilan seguimientos automáticos de la transacción. El seguimiento de la transacción entre procesos recopila solamente los seguimientos importantes para el usuario para clasificar los problemas y para analizar la causa raíz.

Cuando un agente ascendente activa un seguimiento, la

`Component Details Auto Tracing Triggered`

propiedad muestra el tipo de activación. Por ejemplo, un error. Cuando un agente descendente activa la recopilación de seguimientos automáticos, la

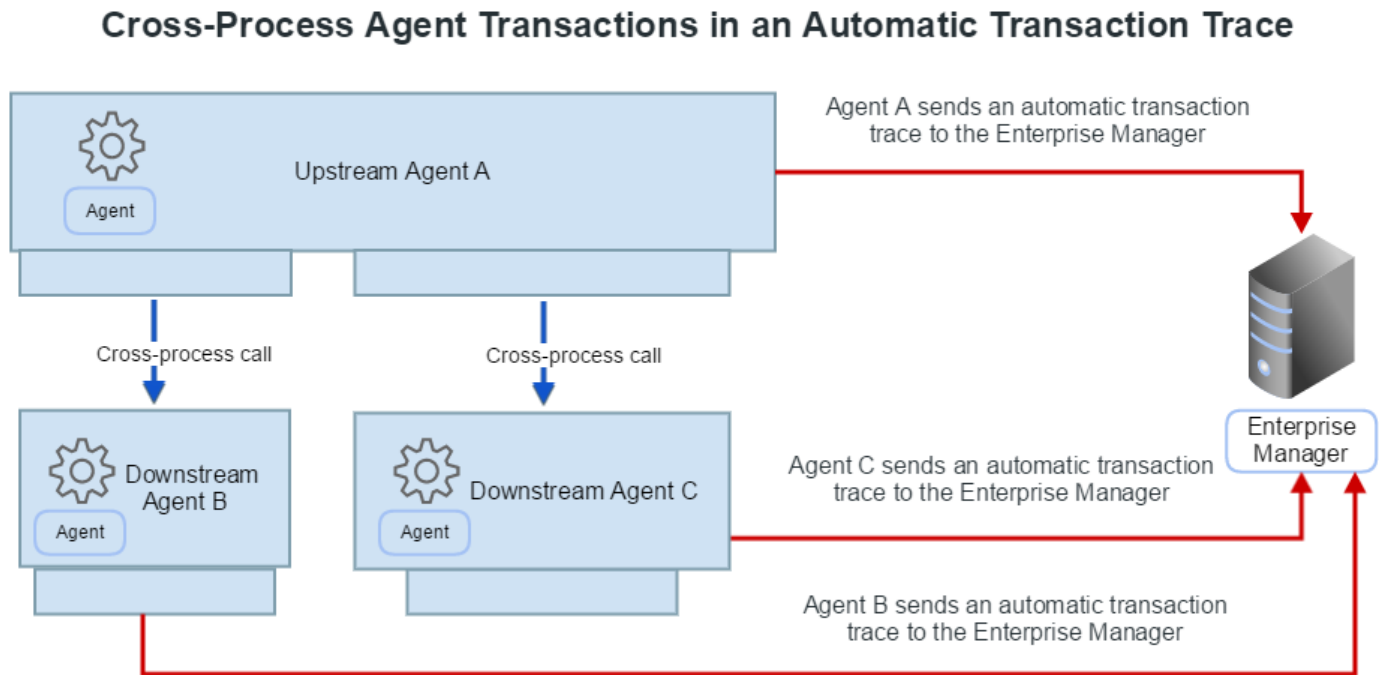
`Component Details Auto Tracing Triggered`

la propiedad es

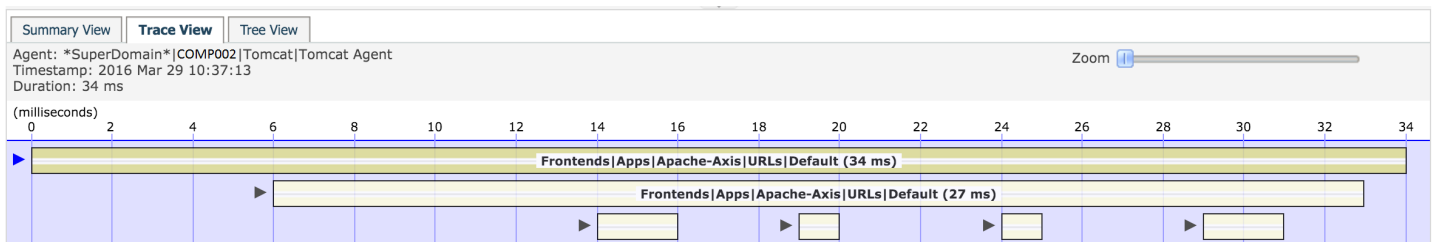
`Cross Process Trigger`

### **Ejemplo: Correlación de seguimiento de la transacción entre procesos del agente en los seguimientos automáticos de la transacción**

Un agente ascendente de otros agentes detecta un problema. El agente ascendente activa la recopilación de un seguimiento automático de la transacción y notifica a los agentes descendentes de que hagan lo mismo. Todos los agentes envían sus seguimientos automáticos de la transacción a Enterprise Manager. Juntos, los agentes crean una transacción correlacionada entre procesos tal y como se muestra en el siguiente diagrama.

**Figure 12: Las transacciones entre procesos activan el agente de seguimiento automático**

Los seguimientos automáticos de la transacción también son compatibles con la correlación entre subprocessos dentro del mismo proceso. Las llamadas de subprocessos pueden realizar un seguimiento de más de una transacción. Una transacción en un proceso puede pasar por distintos subprocessos. En el siguiente gráfico, puede ver cuatro subprocessos entre procesos en la fila inferior de un seguimiento automático de la transacción.

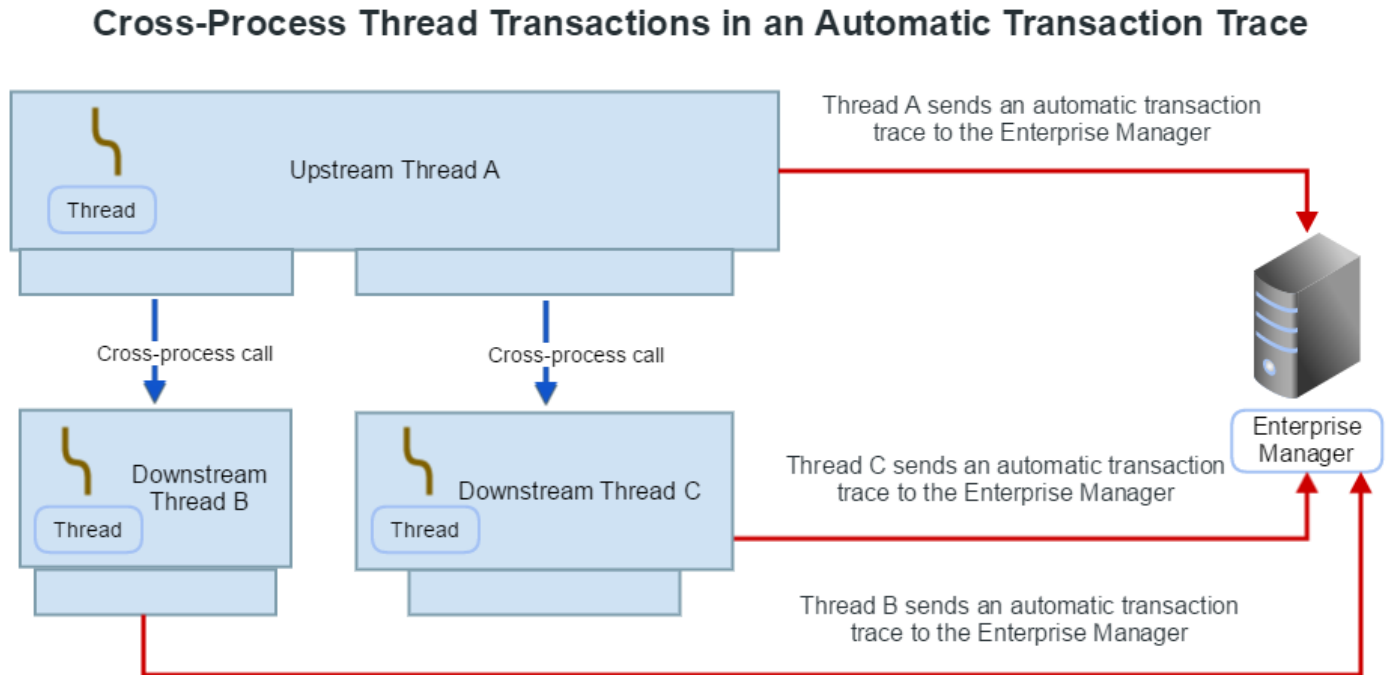


Los subprocessos ascendentes pueden activar seguimientos automáticos de la transacción en cualquier momento, ya sea antes o después de que se invoquen los subprocessos descendentes. Los detalles de la transacción dependen de si el subprocesso es ascendente o descendente del subprocesso de activación inicial de la transacción.

#### **Ejemplo: Correlación de seguimiento de la transacción entre procesos del subprocesso en los seguimientos automáticos de la transacción**

Un subprocesso ascendente detecta un problema. El subprocesso ascendente activa la recopilación de un seguimiento automático de la transacción y notifica a los subprocessos descendentes de que hagan lo mismo. Todos los subprocessos envían sus seguimientos automáticos de la transacción a Enterprise Manager. Juntos, los subprocessos crean una transacción correlacionada entre procesos.

Figure 13: Transacciones entre procesos en el seguimiento automático 2



### Recopilación automática de un seguimiento de la transacción en función de la inestabilidad de la aplicación

El Análisis diferencial realiza un seguimiento de la estabilidad de las aplicaciones. De forma predeterminada, el Análisis diferencial busca una varianza sin control en el Tiempo medio de respuesta de las métricas del front-end y de la métrica de transacciones comerciales. El mapa Análisis diferencial es una exploración visual de la estabilidad y la capacidad de respuesta de muchas aplicaciones. Cada sección del mapa se corresponde con una sola métrica. En un período silencioso y estable la sección es de un tono claro. Cuando se degrada la estabilidad, el tono de la sección se oscurece progresivamente según la severidad de la inestabilidad. Por lo tanto, una única sección le permite ver la estabilidad de una sola aplicación o una transacción comercial a lo largo del tiempo. El mapa ordena las secciones más inestables en la parte superior.

Cuando una aplicación se vuelve ligeramente inestable, el análisis diferencial notifica al agente, que está preparado para recopilar los seguimientos automáticos de la transacción relacionados. Normalmente el agente recopila seguimientos de la transacción hasta que la aplicación vuelve a ser estable. Sin embargo, el agente puede decidir no recopilar un seguimiento de la transacción cuando el período de inestabilidad es breve. Consulte estos seguimientos de la transacción para obtener información detallada específica del cambio de estabilidad y para obtener más información sobre la causa raíz.

#### **NOTE**

Los seguimientos automáticos de la transacción del análisis diferencial requieren la versión del agente 10.0 o posterior.

#### **Siga estos pasos:**

1. En APM Team Center, haga clic en **WebView**.  
Aparecerá APM WebView.
2. Haga clic en **Investigator**.  
Un árbol muestra una vista jerárquica del sistema.
3. En el árbol, seleccione al agente para el que desee obtener información de rendimiento, por ejemplo:

SuperDomain | Host | Process | Agent | Frontends | Apps | App Name

4. Haga clic en la ficha **Análisis diferencial**.

El mapa muestra una representación gráfica de los datos de rendimiento y los últimos 8 minutos de datos. Las principales 100 métricas problemáticas aparecen en la inestabilidad decreciente. Los datos se actualizan cuando consulta, modifica el período de tiempo o selecciona un nodo distinto.

5. Haga clic en una sección de interés del mapa.

Aparecerá el gráfico Análisis diferencial. Este gráfico le ayuda a entender la estabilidad de la métrica en la escala de tiempo que representa la sección. El gráfico muestra el estado del componente monitorizado para que pueda detectar rápidamente el rendimiento normal y el anómalo:

Una línea representa un valor real de la métrica.

Las regiones sombreadas corresponden a secciones de desviación estándar 1, 2 y 3. Cuanto más oscura es la banda, mayor será la desviación del valor previsto. Cualquier métrica en blanco es mejor que la prevista. Cualquier métrica que aparece sobre el área blanca en la parte inferior ha superado el valor previsto. Por ejemplo, si la métrica supera la banda superior, está superando 3 veces la desviación estándar.

6. Pase el ratón sobre la línea.

La información sobre herramientas muestra los valores de la métrica.

7. Haga clic en el hipervínculo de la métrica de interés, por ejemplo, Tiempo medio de respuesta.

8. En el Explorador de métrica, haga clic en el nodo de la carpeta justo encima de la métrica y después haga clic en la ficha **Seguimientos**.

Puede ver los seguimientos automáticos de la transacción generados por la inestabilidad.

9. (Opcional) Haga clic en otros nodos para ver los seguimientos de la transacción que ha generado el Análisis diferencial.

Por ejemplo, haga clic en el nodo **Front-ends** y, a continuación, en la ficha **Seguimientos** para ver los seguimientos automáticos de todas sus aplicaciones de front-end.

Se pueden configurar análisis diferenciales para puntos de entrada y para otras métricas de la aplicación.

### **Activación del seguimiento automático de la transacción cuando se supera el tiempo de respuesta del componente**

Se puede implementar un PBD para activar un seguimiento de la transacción automáticamente cuando se ha superado el tiempo de respuesta del componente. Cree una entrada PBD con un rastreador para recopilar este seguimiento automático. Por ejemplo, para recopilar un seguimiento cuando un tiempo de respuesta específico del servlet es superior a 10 segundos. Utilice la opción del rastreador `ComponentTimeAutoTraceTriggerTracer` para configurar su capacidad.

#### **NOTE**

**Más información:** [Configuración de las opciones de seguimiento de la transacción](#)

### **Recopilación manual de un seguimiento de la transacción**

Para ejecutar una sesión de seguimiento de la transacción manualmente, especifique los agentes de cuyas transacciones desea realizar un seguimiento, así como el período de captura de datos. Especifique filtros para limitar el seguimiento de las transacciones que han superado el tiempo de ejecución del umbral, los valores del parámetro coincidentes o que contienen errores. Una vez se inicia la sesión de seguimiento de la transacción, las transacciones que coinciden con los criterios de filtro aparecen en la tabla de transacciones. Los eventos de transacción incluyen errores y seguimientos de transacciones.

Debe tener el permiso `run_tracer` para ejecutar una nueva sesión de seguimiento de transacciones.

#### **Siga estos pasos:**

1. En APM Team Center, haga clic en **WebView**.  
Aparecerá APM WebView.

2. Haga clic en **Herramientas, Transaction Tracer**.
3. Haga clic en **Iniciar sesión de seguimiento**.
4. En el área Realizar el seguimiento de transacciones:
  - Especifique la duración mínima del seguimiento de la transacción. En la lista desplegable, seleccione milisegundos o segundos. El valor predeterminado es de 5000 milisegundos.
  - (Opcional) Especifique una de las siguientes condiciones de filtro para el seguimiento de la transacción:
    - **Es igual a**  
El valor del parámetro que coincide con las cadenas de las que se está realizando un seguimiento.
    - **No es igual a**  
El valor del parámetro que no coincide con la cadena especificada de la que se está realizando un seguimiento. También se realiza un seguimiento de las transacciones que no incluyen el parámetro al que se aplica el filtro.
    - **Contiene**El valor del parámetro que contiene la cadena especificada de la que se está realizando un seguimiento.
    - **Empieza por**El valor del parámetro que empieza por la cadena especificada de la que se está realizando un seguimiento.
    - **Termina con**  
El valor del parámetro que termina con la cadena especificada de la que se está realizando un seguimiento.
    - **Existe**  
Se realiza un seguimiento de las transacciones que incluyen el parámetro al que se aplica el filtro, sin tener en cuenta el valor del parámetro.
    - **No existe**  
Se realiza un seguimiento de las transacciones que no incluyen el parámetro al que se aplica el filtro.
5. Introduzca la duración de la sesión de seguimiento.
6. En el área **Agentes de seguimiento**, seleccione uno o más agentes de cuyas transacciones desea realizar un seguimiento:
  - Para realizar el seguimiento de todos los agentes, haga clic en **Realizar el seguimiento de todos los agentes compatibles**. Esta opción permite realizar un seguimiento de todos los agentes compatibles que están conectados actualmente y de cualquier agente que se conecte durante la sesión de seguimiento.
  - Para realizar el seguimiento de los agentes seleccionados, haga clic en **Realizar el seguimiento de los agentes seleccionados** y seleccione los agentes de la lista (**CTRL + clic** para seleccionar varios agentes).
7. Haga clic en **Aceptar** para iniciar la sesión de seguimiento de la transacción.  
Después de iniciar la sesión, la barra de estado en el panel inferior muestra la siguiente información:
  - Número de transacciones de las que se está realizando un seguimiento y una breve descripción de la configuración de seguimiento.
  - Tiempo restante de la sesión.

En el modo en directo, la ficha **Seguimientos** muestra eventos de seguimiento de la transacción de los últimos 20 minutos. No se muestran los eventos de seguimiento de transacciones anteriores a 20 minutos en el modo en directo. Se enumeran no más de 500 eventos de seguimiento de la transacción.

### **Detención, reinicio o cambios en las sesiones de seguimiento de la transacción**

Se puede gestionar la sesión de seguimiento en la ficha **Transaction Tracer** como se muestra a continuación:

- Haga clic en **Detener seguimiento** para finalizar la sesión.
- Haga clic en **Reiniciar seguimiento** para acceder a las transacciones de seguimiento en los agentes de destino mediante las mismas condiciones. Puede iniciar una nueva sesión de seguimiento de la transacción:
  - Después de que se haya agotado el tiempo de espera de una sesión.
  - Para reiniciar una sesión que se ha detenido.
  - Para reiniciar una sesión en curso.
- Haga clic en **Cambiar seguimiento** para seleccionar una sesión de seguimiento distinta para ejecutar.

## Búsqueda del seguimiento relevante

Se puede examinar un único seguimiento para recopilar información sobre el problema de la aplicación.

### Siga estos pasos:

1. Analice la información de la actividad de seguimiento de la sesión de seguimiento en la tabla de transacciones. Seleccione una fila de tabla para ver más detalles.
2. Ejecute de nuevo o detenga, reinicie o cambie las sesiones de seguimiento según sea necesario.
3. Examine las fichas **Vista de resumen**, **Vista de seguimiento** y **Vista de árbol** en el panel inferior. La información le puede ayudar a diagnosticar y evaluar problemas de las aplicaciones y problemas de rendimiento.

## Comprensión de los puntos de entrada

La detección automática de puntos de entrada permite monitorizar y evaluar rápidamente las aplicaciones de Java sin configurar manualmente las directivas de ProbeBuilder.

Cuando la detección de puntos de entrada y la instrumentación inteligente están activadas, Introscope monitoriza los subprocesos que están implicados en transacciones de llamada de socket del cliente. La instrumentación inteligente y la detección de puntos de entrada están configuradas como activas de forma predeterminada. Los *puntos de entrada* son los puntos de inicio de la transacción. Un motor de reglas en el agente identifica a los candidatos del punto de entrada. El agente instrumenta y monitoriza al candidato de punto de entrada más antiguo en el subproceso de transacción. Cualquier punto de entrada que un agente detecta y persiste está activado para la monitorización por parte de todos los agentes que comparten el directorio de instalación. Sin embargo, cuando varios agentes comparten la instrumentación, la generación de informes de las métricas dependen del servidor de aplicaciones de JVM que ejecuta las mismas clases de código o de marco.

A continuación, se muestran ejemplos de transacciones en las que la detección de puntos de entrada proporciona visibilidad automáticamente:

- Pilas de tecnología y marcos de trabajo que todavía no monitoriza la instrumentación de Introscope
- Llamadas de API personalizadas o de propiedad
- Subprocesos de fondo que consumen los recursos críticos y que pueden afectar al rendimiento general de la aplicación

### NOTE

La detección del punto de entrada no admite el Protocolo de datagramas de usuario (UDP).

El agente guarda los puntos de entrada en `AutoPersist.pbd`, que se mantiene en el directorio `<Agent_Home>\core\config\hotdeploy`.

### WARNING

El usuario del sistema que ejecuta el servidor de aplicaciones requiere los accesos de lectura y escritura para el directorio `\hotdeploy`. Estos permisos permiten al agente escribir datos en

```
AutoPersist.pbd
```

.

Los puntos de entrada son diferentes de los front-ends. El Agente de Java detecta automáticamente los puntos de entrada que se encuentran junto al inicio de una ruta de llamada de transacciones. Los front-ends se definen manualmente en los archivos PBD y pueden estar en cualquier lugar de la ruta de llamada de transacciones.

### WARNING

No se deben realizar cambios manuales en

```
AutoPersist.pbd
```

. Sin embargo, se pueden copiar puntos de entrada detectados que se pueden utilizar en un PBD distinto.

Las métricas de puntos de entrada se muestran en el árbol centrado en agentes en el subnodo Automatic Entry Points en el nodo del agente.

**NOTE**

: Asegúrese de que la propiedad `introscope.autoprobe.dynamicinstrument.enabled` en `IntroscopeAgent.profile` está configurada como `true`. Esta configuración permite al agente informar sobre métricas de punto de entrada sin tener que reiniciar la aplicación.

Introscope informa sobre las cinco métricas de responsabilidad estándares para cada punto de entrada. Los puntos de entrada se muestran en los seguimientos de la transacción, pero no se muestran en el mapa. El formato de los nombres de punto de entrada es el siguiente: `entry point <class name _ method name>`. Introscope informa sobre las [métricas de compatibilidad de la detección de los puntos de entrada](#).

Se puede configurar la [recopilación de puntos de entrada](#). Por ejemplo, una propiedad de configuración limita el número de puntos de entrada que puede conservar `AutoPersist.pbd`.

**NOTE**

**Más información:** [Creación de archivos PBD para convertir puntos de entrada en front-ends](#)

**Comprensión de back-ends automáticos**

Cuando se activa la detección *automática del back-end*, el agente detecta y monitoriza automáticamente los back-ends de aplicaciones sin una configuración manual.

Un motor de detección en el agente identifica a los candidatos a back-end automáticos. Cualquier back-end automático que detecte un agente y persista está activado para la monitorización por parte de todos los agentes que compartan el directorio de instalación.

A continuación, se describen ejemplos de tipos de back-end que puede encontrar y monitorizar la detección automática de back-ends:

- Pilas de tecnología de back-end y marcos de trabajo que el agente todavía no monitoriza. Algunos ejemplos son back-ends NoSQL como MongoDB y Cassandra.
- Back-ends personalizados o de propiedad

El agente guarda los back-ends automáticos en `AutoPersist.pbd`, que se conserva en el directorio `<Agent_Home>\core\config\hotdeploy`.

**WARNING**

- Importante: El usuario del sistema que ejecuta el servidor de aplicaciones requiere los accesos de lectura y escritura para el directorio `/hotdeploy`. Estos permisos permiten al agente escribir datos en `AutoPersist.pbd`.
- No se deben realizar cambios manuales en `AutoPersist.pbd`. Sin embargo, puede copiar back-ends automáticos detectados que se pueden utilizar en un PBD distinto.

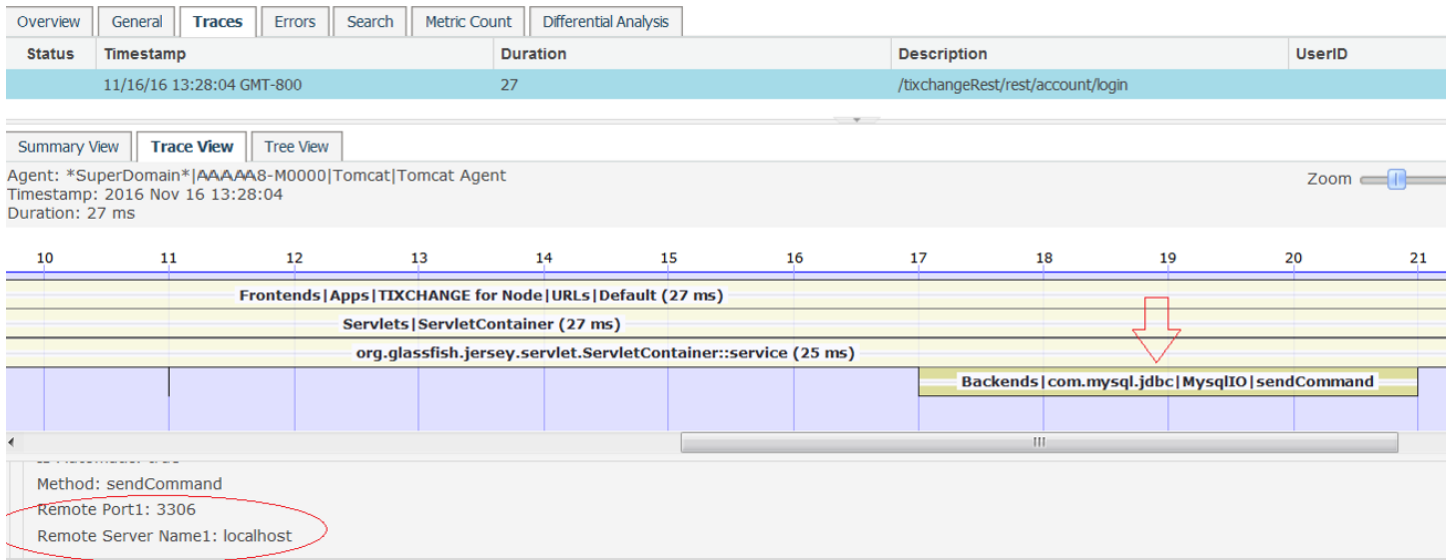
Se puede [configurar la detección automática de back-ends](#). Por ejemplo, una propiedad de configuración limita el número de back-ends automáticos que puede conservar `AutoPersist.pbd`.

En la **Vista de seguimiento**, los parámetros de `nombre de servidor remoto` y `puerto remoto` se muestran en los **detalles del componente**.

Tenga en cuenta la ruta de llamada del back-end y los parámetros en este seguimiento de la transacción:

- El componente de seguimiento de la transacción para la ruta de llamada del back-end es: `Backends|com.mysql.jdbc|MySQLIO|sendCommand`.
- El parámetro del puerto remoto es `3306` y el parámetro del host del servidor remoto es `Name1: localhost`.





### Comprensión de los componentes de la visibilidad exhaustiva

Cuando se activa la instrumentación inteligente, los agentes detectan y recopilan automáticamente información detallada sobre los componentes de las transacciones a nivel de método. Los agentes detectan e instrumentan automáticamente los componentes de visibilidad exhaustiva sin tener que utilizar las directivas de ProbeBuilder (PBD). Introscope analiza los métodos para comprobar su complejidad y así poder determinar las llamadas y los componentes que se deben instrumentar y mostrar como componentes de visibilidad exhaustiva.

**Nota:** La instrumentación inteligente solo está disponible para los Agentes de Java pero no para los Agentes de .NET.

A continuación, se detallan algunas características importantes sobre los componentes de visibilidad exhaustiva:

- Un icono de rayo indica un componente de visibilidad exhaustiva. La etiqueta Componente de seguimiento exhaustivo también aparece en la información sobre herramientas al pasar el ratón sobre este componente.
- Los componentes de visibilidad exhaustiva no incluyen vínculos a las métricas. No se muestran datos de métricas en el árbol Investigator o en el mapa.
- Contienen solamente el nombre de la clase, el nombre del método y la duración.
- En los detalles del componente, se muestran las propiedades siguientes:
  - Nivel de instrumentación  
El nivel de instrumentación inteligente en el que se ha detectado una transacción.
  - Method Level Score (Puntuación a nivel de método)  
El nivel de instrumentación inteligente que se corresponde con la puntuación que el algoritmo de calificación de Introscope asigna a un método de componente de visibilidad exhaustiva. Introscope puede mostrar métodos de componente de visibilidad exhaustiva con varias puntuaciones en el seguimiento de una transacción, un error o una detención. Por ejemplo, una transacción que se ha detectado mediante el nivel medio puede mostrar métodos con una puntuación de nivel medio y nivel bajo.

Utilice estas propiedades para entender la profundidad de visibilidad de la instrumentación inteligente de un seguimiento de la transacción y los métodos dentro de un seguimiento. Por ejemplo, puede comparar el número de métodos que detecta la instrumentación inteligente en dos niveles distintos de instrumentación. Puede tener en cuenta el nivel de instrumentación inteligente en el que Introscope ha puntuado métodos específicos. Se puede ajustar la solución de monitorización a la visibilidad y la sobrecarga del equilibrio de la visibilidad de monitorización deseadas.

Pueden aparecer los componentes instrumentados estándares y los componentes de visibilidad exhaustiva a través de una sesión de seguimiento de la transacción.

En función de los requisitos y del entorno, puede configurar la profundidad de visibilidad de la instrumentación inteligente.

## Análisis de los seguimientos y colaboración en el análisis de problemas

Puede exportar el archivo JavaScript Object Notation (JSON) para uno o varios seguimientos de la transacción. Para ello, utilice un simple editor y busque en el archivo un componente o los parámetros dentro de un componente. Comparta el archivo por correo electrónico o en una unidad de red compartida para permitir que los usuarios colaboren en el análisis de problemas. Otro usuario puede cargar el archivo exportado para ver la misma información. Esta perspectiva compartida ayuda a colaborar para identificar rápidamente si un componente está disponible o si tiene problemas de rendimiento. Por ejemplo, puede examinar si los usuarios pueden iniciar sesión, extraer o ver sus datos. Puede ver los tiempos de respuesta para los usuarios y las causas de los problemas cuando se producen.

Para exportar o cargar el archivo JSON de seguimiento, trabaje desde la ficha **Transacciones empresariales**. Para abrir la ficha, utilice el Bloc de notas de análisis y haga clic en un problema que le interese.

### Exportación del archivo JSON de seguimiento

Exporte los datos de seguimiento como JSON para analizarlos o compartirlos.

#### Siga estos pasos:

1. Haga clic en la ficha **Transacciones comerciales**.
2. Haga clic en un segmento de la transacción o en un componente que le interese y haga clic en **Cargar**. El nombre del archivo descargado aparece en la parte inferior de la página.
3. (Opcional) Abra el archivo y analice los datos:
  - Utilice un editor como el [Editor en línea de JSON](#).
  - Arrastre el archivo a Chrome.

#### NOTE

La información de la vista de **instantánea** no está disponible en el JSON exportado.

### Carga del archivo JSON de seguimiento

Cargue los datos de seguimiento como JSON para ver una perspectiva compartida.

#### Siga estos pasos:

1. Haga clic en la ficha **Transacciones comerciales**. Una lista mostrará los seguimientos que se corresponden con el componente.
2. Haga clic en el icono **Cargar JSON de seguimiento**  para cargar los datos de la lista o haga clic en un segmento de la transacción que le interese y haga clic en el icono **Cargar JSON de seguimiento**.
3. Busque y seleccione el archivo <nombre>.json y haga clic en **Abrir**.

#### NOTE

El tamaño máximo permitido del archivo JSON es 52.4288 MB. La pila gráfica de detalles de la transacción refleja los datos cargados de JSON.

## Monitorización de los eventos y del rendimiento del explorador

El agente de explorador permite monitorizar los errores y la métrica de rendimiento de la carga de página web. Se puede identificar la degradación del rendimiento en el explorador, la red o el servidor de aplicaciones.

Como propietario de la aplicación, siga estos pasos de alto nivel:

1. Siga el procedimiento normal para monitorizar el rendimiento:

**NOTE**

[Monitorización del rendimiento mediante la Vista de la experiencia](#)

[Investigación del rendimiento de las transacciones con errores](#)

[Diagnóstico de problemas de carga del recurso](#)

2. Lea y utilice esta información adicional y específica para el agente del explorador:

**Monitorización del rendimiento de aplicaciones con el agente del explorador**

Se puede monitorizar el tiempo de respuesta del explorador de la aplicación gestionada y ver sus aplicaciones desde perspectivas como los servicios de negocio y sus dependencias. Se genera automáticamente un mapa a partir del rendimiento y del análisis de métrica, errores y eventos.

**NOTE**

Solamente aparecen en el mapa las métricas Carga de página. La métrica para los marcos estructurales como AJAX no aparece en el mapa.

**Siga estos pasos:**

1. En el panel izquierdo, haga clic en **Vista de la experiencia**.  
La Vista de la experiencia muestra tarjetas de experiencias individuales. Todas las tarjetas muestran un resumen. Los elementos rojos indican las transacciones lentas o erróneas.
2. Busque las tarjetas y haga clic en el icono **Bloc de notas** en una de las tarjetas que le interese.  
El Bloc de notas de análisis muestra detalles sobre la experiencia. El flujo de relaciones muestra las rutas de las transacciones de las experiencias seleccionadas. Este mapa proporciona contexto para el evento que ha ocurrido.
3. (Opcional) Seleccione el **Tipo** de la lista desplegable **Perspectiva**.
4. Analice el mapa e identifique el primer componente (el componente de más a la izquierda) en una serie de dependencias que indica cuáles son los problemas de rendimiento. Este componente puede ser el origen de la degradación del rendimiento en su entorno de aplicaciones.
5. Haga clic en el **componente** que le interese del mapa.  
La ficha Métrica muestra la métrica de BlamePoint y W3C.
6. (Opcional) En la ficha **Métrica**, haga clic en el **nombre de la métrica** que desee como, por ejemplo, el siguiente:  
Coincidencias de página por intervalo  
Aparece el árbol de métrica y muestra la métrica específica.
7. Utilice esta información para investigar los problemas de rendimiento.

**Análisis de la métrica de agente del explorador**

Las aplicaciones que tienen un rendimiento lento pueden afectar a la experiencia del usuario final. Se pueden ver datos reales en el árbol de métrica para ayudar a analizar y resolver problemas de rendimiento. La vista de árbol de agentes, recursos y métrica se actualiza cada 15 segundos para mostrar los datos de métrica actuales.

Toda la métrica del agente del explorador aparecen en la siguiente ruta:

- **Nodo Agente de DxC, Segmento de negocio.** Las descripciones de la ruta de la métrica en las secciones siguientes muestran las rutas del **Agente de DxC**.

**NOTE**

Todos los valores de métrica del Agente del explorador se redondean a la baja. Agregue vínculos a la sección Cálculos del agente del explorador o agréguelos, de manera individual, en los temas siguientes a los cálculos específicos.

## Métrica Carga de página

El agente del explorador informa de los tiempos de respuesta del explorador y de los eventos para las páginas web. Cuando está disponible, el agente del explorador informa de los tiempos de respuesta del explorador. Algunos exploradores tienen limitaciones:

- Para una página inicial, no hay ninguna carga asociada de la página anterior.
- Si una carga de la página espera para la entrada del usuario, este tiempo se incluye en la métrica Tiempo medio de carga de página (ms).

La tabla siguiente describe cómo se calcula la métrica Carga de página para los exploradores. La columna Cálculo de la métrica indica el cálculo matemático que utiliza el agente del explorador para obtener una métrica concreta. Por ejemplo, se obtiene el Tiempo medio de procesamiento de la página (ms) mediante la resta de dos horas de eventos desde el explorador: loadEventEnd y domComplete.

Métrica	Descripción	Cálculo de la métrica
Tiempo medio de procesamiento de la página (ms)	El tiempo para representar el contenido después de procesar el modelo de objeto del documento (DOM).	loadEventEnd time - domComplete time
Tiempo medio de establecimiento de la conexión (ms)	El tiempo para que el explorador establezca la conexión TCP al servidor.	connectEnd time - connectStart time
Tiempo medio de búsqueda de dominio (ms)	El tiempo para que el explorador complete la búsqueda de servicios de nombres para el dominio de la página web actual.	domainLookupEnd time - domainLookupStart time
Tiempo medio de procesamiento de DOM (ms)	El tiempo desde el inicio de la navegación hasta cuando el explorador procesa el modelo de objeto del documento (DOM). <b>Nota:</b> No es el momento en que se cargan y recuperan todos los objetos de DOM.	domComplete time - domLoading time
Tiempo medio de carga de la página (ms)	El tiempo desde el inicio de la navegación hasta cuando el explorador carga todos los componentes y la página está completa.	loadEventEnd time - navigationStart time
Tiempo medio de descarga de la página anterior (ms)	El tiempo para descargar la página mostrada previamente. Si no hay ninguna página de descarga (por ejemplo, cuando se inicia una sesión de explorador), no habrá ningún valor disponible.	unloadEventEnd time - unloadEventStart time
Tiempo medio hasta el primer byte (milisegundos)	El tiempo para que el explorador reciba el primer byte de la respuesta a partir de las memorias caché del servidor o de la aplicación.	responseStart time - requestStart time
Tiempo medio hasta el último byte (milisegundos)	El tiempo para que el explorador reciba el último byte de la respuesta a partir de las memorias caché del servidor o de la aplicación.	responseEnd time - requestStart time
Errores de JavaScript por intervalo	El número de apariciones de error de JavaScript en la página web monitorizada dentro de un intervalo determinado.	No aplicable
Coincidencias de página por intervalo	El número de apariciones que se ha solicitado una página web monitorizada dentro de un intervalo determinado.	No aplicable

Tiempo medio de detención de la página	El tiempo que la solicitud de la página ha estado en espera antes de enviarse.	(connectStart time - domainLookupEnd time) + (requestStart time - connectEnd time)
----------------------------------------	--------------------------------------------------------------------------------	------------------------------------------------------------------------------------

El agente del explorador utiliza umbrales donde no se puede crear ni notificar ningún tipo de métrica del explorador. Los umbrales de métrica para la carga de páginas, asíncrona, y para la función de JavaScript tienen varios umbrales predeterminados que son configurables. Los tiempos de explorador deben cumplir los límites de umbral para la métrica que se va a crear.

No se podría crear métrica del explorador en el árbol de métrica porque no se ha notificado. En este caso, la métrica no aparece en el mapa. Por ejemplo, si no se muestra Tiempo medio hasta el primer byte (milisegundos) en el árbol de métrica, no aparecerá en el mapa.

El agente del explorador informa de los tiempos de respuesta del explorador y de los eventos para las páginas web. Cuando está disponible, el agente del explorador utiliza la API de tiempo de navegación de W3C para informar de los tiempos de respuesta del explorador. La API de tiempo de navegación de W3C es una interfaz que implementa exploradores modernos. Algunos de estos exploradores tienen limitaciones:

- Para una página inicial, no hay ninguna carga asociada de la página anterior.
- Si una carga de la página espera para la entrada del usuario, este tiempo se incluye en la métrica Tiempo medio de carga de página (ms).

Cuando no se inicia ninguna transacción comercial para la página de nivel superior, la métrica aparece en:

- Segmento de negocio | <HOST\_URL\_página>/<PUERTO\_URL\_página> | <Ruta\_URL\_página>

Cuando se inicia una transacción comercial para la página de nivel superior, la métrica aparece en:

- Segmento de negocio | <Servicio\_negocio> | <Transacción\_negocio> | <Componente\_transacción\_negocio> | Explorador

#### NOTE

Cuando se producen errores, el Agente del explorador aumenta la métrica Errores de página por intervalo en la ruta de métrica de la página. Esta métrica representa el número total de errores de JavaScript y AJAX en la página.

### **Métrica Carga de página parcial**

Las aplicaciones de página única provocan que una solicitud de página única recupere todo el contenido para esa página al cargar la página inicial. A continuación, las aplicaciones podrán obtener recursos desde el servidor y actualizar de forma dinámica la interfaz de usuario como resultado de las interacciones de usuario. Muchas aplicaciones de página única utilizan las propiedades hash de ubicación de la URI y de las API de historial de HTML5 para indicar la navegación del usuario lógico en la misma página web única. Este tipo de navegación de usuario lógico que desencadena un cambio de ruta sin volver a cargar la página completa se denomina navegación de página parcial. El agente del explorador monitoriza el tiempo de carga de páginas parciales e informa de la métrica Tiempo medio de carga de la página (ms). El agente del explorador también monitoriza el número de apariciones en las que se ha visitado la página parcial monitorizada dentro de un intervalo determinado. El agente del explorador informa de este número como la métrica Coincidencias de página por intervalo. Esta información proporciona información más detallada sobre la experiencia del usuario final de las aplicaciones de página única.

La siguiente métrica está disponible para las aplicaciones de página única y la navegación de página parcial. Estos cálculos de métrica utilizan las variables:

- TSPE = Momento en que se inicia la navegación parcial (cambio de ruta sin cargar la página)
- TSPS = Momento en que la página parcial acaba de cargarse

Métrica	Descripción	Cálculo de la métrica
Tiempo medio de carga de la página (ms)	El tiempo medio se produce desde el momento de la navegación parcial (cambio de ruta sin cargar la página) hasta que la página parcial acaba de cargarse.	TSPE - TSPS
Coincidencias de página por intervalo	El número de apariciones que se ha visitado la página parcial monitorizada dentro de un intervalo determinado.	No aplicable

Cuando se produce una navegación de página parcial, su métrica Tiempo medio de carga de la página (ms) y Coincidencias de página por intervalo aparece en el nodo Hash de página parcial de la página de nivel superior:

- Segmento de negocio | <HOST\_URL\_página>/<PUERTO\_URL\_página> | <Ruta\_URL\_página> | <Ruta\_página> | <Hash\_página\_parcial>

Cuando se inicia una transacción comercial para la página de nivel superior, la métrica de página parcial aparece en:

- Segmento de negocio | <Servicio\_negocio> | <Transacción\_negocio> | <Componente\_transacción\_negocio> | Explorador | <Hash\_página\_parcial>

### **Métrica de AJAX**

Para aplicaciones web, el agente del explorador puede proporcionar tiempos de respuesta para páginas web dinámicas en marcos estructurales como AJAX (Asynchronous JavaScript And XML).

El agente del explorador no admite:

- Devoluciones de llamada de AJAX anidados
  - Solicitudes sincrónicas de AJAX
  - Las funciones de devolución de llamada como `XMLHttpRequest.onerror` y `XMLHttpRequest.ontimeout` (los tiempos de ejecución de la devolución de llamada son compatibles con `XMLHttpRequest.onreadystatechange` y `XMLHttpRequest.onload`).
- Icono

### **NOTE**

Para obtener más información sobre la compatibilidad, consulte [Matriz de compatibilidad del producto](#).

La siguiente métrica está disponible para marcos mediante AJAX. Estos cálculos de métrica utilizan las variables:

- TSE = Momento en que AJAX envía finalizaciones de llamada
- TFB = Momento en que el explorador recibe el primer byte de la respuesta del servidor
- TLB = Momento en que el explorador recibe el último byte de la respuesta del servidor
- TCS = Momento en que empieza la ejecución de la devolución de llamada de AJAX
- TCE = Tiempo en que finaliza la ejecución de la devolución de llamada de AJAX

Métrica	Descripción	Cálculo de la métrica
Tiempo medio de ejecución de la devolución de llamada (ms)	El tiempo medio de <code>XMLHttpRequest.onreadystatechange</code> o <code>XMLHttpRequest.onload</code> funciones de devolución de llamada para procesar la respuesta del servidor.	TCE - TCS
Recuento de invocación por intervalo	El número total de veces que se ha realizado la solicitud de AJAX en un intervalo determinado.	No aplicable
Tiempo medio hasta el primer byte (milisegundos)	El tiempo medio desde el momento en que se emite la solicitud de AJAX para un recurso HTTP hasta la recepción del primer byte de la respuesta del servidor.	TFB - TSE
Tiempo medio de carga del recurso (ms)	El tiempo medio desde el momento en que se emite la solicitud de AJAX para un recurso HTTP hasta que finaliza la devolución de llamada de AJAX (la función responsable de recibir y procesar los datos del servidor).	TCE - TSE
Tiempo medio de descarga de la respuesta (ms)	El tiempo medio entre la recepción del primer byte y el último byte de la respuesta del servidor.	TLB - TFB

#### NOTE

Para las llamadas de AJAX, las métricas Tiempo medio de descarga de la respuesta (ms) y Tiempo medio de ejecución de la devolución de llamada (ms) se notifican de manera independiente. Es posible que esta métrica no se notifique debido a limitaciones de ciertos marcos de AJAX, en particular, para las llamadas de AJAX mediante jQuery 1.x.

- Es posible que el agente del explorador no pueda notificar el Tiempo medio de ejecución de la devolución de llamada (ms) para la llamada de AJAX inicial.
- Es posible que el agente del explorador no notifique el Tiempo medio de descarga de la respuesta (ms) ni el Tiempo medio hasta el primer byte (milisegundos).

Una métrica AJAX puede ocurrir en la página de nivel superior o en la página parcial. La métrica de AJAX se clasifica en solicitudes asíncronas y sincrónicas:

#### Métrica de AJAX sincrónica

Cuando no se inicia ninguna transacción comercial para la página de nivel superior, la métrica de AJAX aparece en el nodo Recursos de la página.

- Segmento de negocio | <HOST/PUERTO> | <Ruta\_página> | Recursos | Llamada de AJAX | Sincronización | <HOST\_URL\_AJAX>/<PUERTO\_URL\_AJAX> | <Ruta\_URL\_AJAX>
- Segmento de negocio | <HOST/PUERTO> | <Ruta\_página> | <Hash\_página\_parcial> | Recursos | Llamada de AJAX | Sincronización | <HOST\_URL\_AJAX>/<PUERTO\_URL\_AJAX> | <Ruta\_URL\_AJAX>

Cuando se inicia una transacción comercial para la página de nivel superior, la métrica de AJAX aparece en:

- Segmento de negocio | <Servicio\_negocio> | <Transacción\_negocio> | <Componente\_transacción\_negocio> | Explorador | Recursos | Llamada de AJAX | Sincronización | <HOST\_URL\_AJAX>/<PUERTO\_URL\_AJAX> | <Ruta\_URL\_AJAX>
- Segmento de negocio | <Servicio\_negocio> | <Transacción\_negocio> | <Componente\_transacción\_negocio> | Explorador | <Hash\_página\_parcial> | Recursos | Llamada de AJAX | Sincronización | <HOST\_URL\_AJAX>/<PUERTO\_URL\_AJAX> | <Ruta\_URL\_AJAX>

Cuando se inicia una transacción comercial para la llamada de AJAX, prevalecerá sobre la transacción comercial que se inicie para la página de nivel superior. La métrica de AJAX aparece en:

- Segmento de negocio | <Servicio\_negocio\_AJAX> | <Transacción\_negocio\_AJAX> | <Componente\_transacción\_negocio\_AJAX> | Explorador | Recursos | Llamada de AJAX | Sincronización | <HOST\_URL\_AJAX>/<PUERTO\_URL\_AJAX> | <Ruta\_URL\_AJAX>

### **Métrica de AJAX asíncrona**

Cuando no se inicia ninguna transacción comercial para la página de nivel superior, la métrica de AJAX aparece en el nodo Recursos de la página.

- Segmento de negocio | <HOST/PUERTO> | <Ruta\_página> | Recursos | Llamada de AJAX | Asincronización | <HOST\_URL\_AJAX>/<PUERTO\_URL\_AJAX> | <Ruta\_URL\_AJAX>
- Segmento de negocio | <HOST/PUERTO> | <Ruta\_página> | <Hash\_página\_parcial> | Recursos | Llamada de AJAX | Asincronización | <HOST\_URL\_AJAX>/<PUERTO\_URL\_AJAX> | <Ruta\_URL\_AJAX>

Cuando se inicia una transacción comercial para la página de nivel superior, la métrica de AJAX aparece en:

- Segmento de negocio | <Servicio\_negocio> | <Transacción\_negocio> | <Componente\_transacción\_negocio> | Explorador | Recursos | Llamada de AJAX | Asincronización | <HOST\_URL\_AJAX>/<PUERTO\_URL\_AJAX> | <Ruta\_URL\_AJAX>
- Segmento de negocio | <Servicio\_negocio> | <Transacción\_negocio> | <Componente\_transacción\_negocio> | Explorador | <Hash\_página\_parcial> | Recursos | Llamada de AJAX | Asincronización | <HOST\_URL\_AJAX>/<PUERTO\_URL\_AJAX> | <Ruta\_URL\_AJAX>

Cuando se inicia una transacción comercial para la llamada de AJAX, prevalecerá sobre la transacción comercial que se inicie para la página de nivel superior. La métrica de AJAX aparece en:

- Segmento de negocio | <Servicio\_negocio\_AJAX> | <Transacción\_negocio\_AJAX> | <Componente\_transacción\_negocio\_AJAX> | Explorador | Recursos | Llamada de AJAX | Asincronización | <HOST\_URL\_AJAX>/<PUERTO\_URL\_AJAX> | <Ruta\_URL\_AJAX>

### **NOTE**

Cuando una llamada de AJAX tiene un error, el Agente del explorador aumenta la métrica Errores de recurso por intervalo en la ruta de la métrica de AJAX.

### **Métrica de recursos web**

El agente del explorador notifica la métrica de recurso web para todos los recursos en la página, como imagen, CSS y JavaScript. Las páginas web se crean a partir de contenido que no se puede mostrar en la descarga inicial de la misma página. Este contenido puede aparecer como una imagen, sonido u otro medio. Por ejemplo, una aplicación web puede utilizar los servicios de entrega de contenido para incluir imágenes y anuncios incrustados. Estos elementos complementarios a los que hace referencia la página y las descargas son recursos con nombre. Como analista, debe saber si el rendimiento deficiente de una aplicación es debido a la aplicación o a los recursos web, que pueden haber sido proporcionados por terceros.

La métrica de recursos web para el resto de recursos de la página aparece en el nodo Recursos, HTML de la página:



- Segmento de negocio | <HOST\_URL\_página>/<PUERTO\_URL\_página> | <Ruta\_URL\_página> | <Ruta\_página> | Recursos | HTML | <HOST\_URL\_recurso>/<PUERTO\_URL\_recurso> | <Ruta\_URL\_recurso>
- Segmento de negocio | <HOST\_URL\_página>/<PUERTO\_URL\_página> | <Ruta\_URL\_página> | <Hash\_página\_parcial> | Recursos | HTML | <HOST\_URL\_recurso>/<PUERTO\_URL\_recurso> | <Ruta\_URL\_recurso>

Cuando se inicia una transacción comercial para la página, la métrica Recurso web aparece en:

- Segmento de negocio | <Servicio\_negocio> | <Transacción\_comercial> | <Componente\_transacción\_negocio> | Explorador | Recursos | HTML | <HOST\_URL\_recurso>/<PUERTO\_URL\_recurso> | <Ruta\_URL\_recurso>
- Segmento de negocio | <Servicio\_negocio> | <Transacción\_negocio> | <Componente\_transacción\_negocio> | Explorador | <Hash\_página\_parcial> | Recursos | HTML | <HOST\_URL\_recurso>/<PUERTO\_URL\_recurso> | <Ruta\_URL\_recurso>

### Siga estos pasos:

1. En el panel izquierdo, haga clic en **Métrica**.  
El árbol de métrica muestra métrica y otra información en un formato de árbol. Los nodos de alto nivel inmediatamente en los nodos de dominio representan a agentes instalados en hosts de servidores de aplicaciones individuales o el equivalente. Un nodo es el lugar donde se recopila y se muestra información específica de la métrica en la vista de árbol que se centra en el agente. Cuando se expande un nodo, se puede ver y buscar información más específica sobre la métrica.
2. Expanda el nodo **Agente de DxC, Segmento de negocio**.  
La vista de árbol de agentes, recursos y métrica se actualiza cada 15 segundos para mostrar los datos de métrica actuales.
3. Consulte la métrica del explorador accediendo a los nodos.
4. (Opcional) Comparta la dirección URL con sus compañeros para que puedan ver la misma vista de la métrica específica en el árbol.

### Análisis de errores

Las aplicaciones web utilizan JavaScript para acciones como:

- Aceptar la información de usuario
- Proporcionar efectos transicionales
- Procesar e incluso presentar datos complejos

Si una sección de una página web no funciona, posiblemente es debido a un error de JavaScript o de AJAX. En estas situaciones de error, la monitorización de errores de AJAX y de JavaScript del agente del explorador proporciona visibilidad.

### Errores de JavaScript

El tratamiento de errores de JavaScript puede ser local con bloques try/catch, pero también global con controladores de eventos. El agente del explorador utiliza un controlador de errores global para capturar todos los errores de JavaScript no capturados en la ventana actual del explorador. El agente del explorador puede:

- Informar del número de errores de JavaScript en la métrica Errores de página por intervalo. Esta métrica aparece en la ruta de métrica de la página en el contexto de URL o en la transacción comercial adecuada.
- Recopilar información sobre errores de JavaScript personalizados y nativos en la ventana del explorador, como la línea y el número de columna, la marca de tiempo y el seguimiento de pila del error.
- Generar instantáneas error por error con detalles del error.

## Errores de AJAX

Los códigos de estado de AJAX podrían indicar un problema con los puntos finales de AJAX. El agente del explorador informa de todas las llamadas de AJAX que tienen los siguientes códigos de estado HTTP de respuesta como errores de AJAX:

- Error de cliente 4XX
- Error de servidor 5XX

El agente del explorador también captura información acerca de una respuesta de error para ayudarle a entender los problemas para cada una de las llamadas de AJAX. El agente del explorador puede:

- Informar del número total de errores de AJAX en la página de la métrica Errores de página por intervalo. Esta métrica aparece en la ruta de métrica de la página en el contexto de URL o en la transacción comercial adecuada.
- Informar sobre Error de recurso por intervalo en la ruta de la métrica de AJAX en el contexto de dirección URL o transacción comercial adecuada.
- Recopilar información sobre una respuesta de error:
  - Código de estado de la respuesta, por ejemplo: 404
  - Texto de estado de la respuesta, por ejemplo: No encontrado
  - Los mensajes de error personalizados de jQuery, por ejemplo, un seguimiento de pila y un mensaje de error del analizador JSON

## Análisis de errores desde la instantánea de error

El agente del explorador crea una instantánea de error de JavaScript o AJAX individual por error. Cada error se produce en una página web monitorizada dentro de un intervalo que contiene la siguiente información:

- Nombre de explorador
- Versión del explorador
- URL de la página web en la que se ha producido el error
- Descripción de error según se ha notificado en el explorador
- Número de línea de error según se ha notificado en el explorador
- Número de columna de error según se ha notificado en el explorador
- Nombre del archivo de origen según se ha notificado en el explorador

Consulte la instantánea de error para obtener más información sobre el error que incluye los parámetros y la ruta de llamada. Cada 15 segundos, una instantánea de error individual muestra los errores de JavaScript o AJAX que se han producido en el intervalo.

### Siga estos pasos:

1. Haga clic en la ficha **Transacciones comerciales**.  
Los seguimientos que se corresponden con el componente aparecen en una lista de resumen. Los segmentos muestran las horas de duración. Los segmentos están codificados por colores para indicar cualquier problema que se asocia con una transacción, por ejemplo, rojo indica un error.
2. Haga clic en el seguimiento de la transacción que desee.  
Los componentes de la transacción individual aparecerán en una pila gráfica (gráfico de tarta).
3. Haga clic en un segmento de negocio rojo, por ejemplo, para un error de JavaScript:  
Segmento comercial | <Page\_Path> o <business transaction>/jserrors/  
error\_SyntaxError.jsp (0 ms)
4. Consulte **Detalles de los componentes** y consulte los detalles del error.

#### NOTE

No todos los exploradores pueden proporcionar un seguimiento de pila. Por ejemplo, Internet Explorer 10, Microsoft Edge y Safari 9.x no proporcionan seguimientos de pilas.

5. Identifique los componentes que parece que sean los causantes del problema y, a continuación, siga el proceso de resolución de incidencias para la organización.

## Acceso y presentación de la estación de trabajo

La estación de trabajo está disponible en DX APM. Obtenga información sobre cómo acceder a la estación de trabajo, dónde encontrar las funciones que se han cambiado de lugar y las funciones que no están disponibles.

- [Acceso a la estación de trabajo](#)
- [Presentación de la estación de trabajo](#)

Acceso a la estación de trabajo

Puede descargar la estación de trabajo desde la interfaz de usuario. Para obtener más información sobre la descarga y conexión de la estación de trabajo, consulte [Conexión de la estación de trabajo](#).

Presentación de la estación de trabajo

En la siguiente tabla se explica qué funciones que no están disponibles en la estación de trabajo. Consulte la columna Más información para obtener información sobre cómo se pueden realizar tareas similares en la interfaz de usuario.

Table 1:

Función (ubicación)	Descripción		Eliminada de la estación de trabajo	Disponible en la interfaz de usuario	Más información
<b>Mapa de evaluación de errores de la aplicación</b> (Investigador de estación de trabajo)	Presenta una vista gráfica de la aplicación gestionada en la que aparecen los errores y el estado de la aplicación.		Sí	Sí	<ul style="list-style-type: none"> <li>• <a href="#">Visualización de las relaciones de los componentes en el mapa</a></li> <li>• <a href="#">Monitorización del rendimiento utilizando la Vista de experiencia</a></li> </ul>
<b>Preferencias de usuario &gt; ficha Investigador</b> (Estación de trabajo, todas las vistas)	Permite activar o desactivar la función de actualización automática de la visualización del mapa de evaluación de errores.		Sí	Sí	<ul style="list-style-type: none"> <li>• <a href="#">Uso de la escala de tiempo y del resaltado</a></li> </ul>
<b>Mapa de dependencia de SOA</b> (Investigador de estaciones de trabajo, Explorador de métrica, hojas de agentes)	Proporciona una representación visual de los servicios que se han implementado en el entorno SOA y le ayuda a controlar y entender cómo se relacionan varios componentes entre ellos.		Sí	No	N/D

Función (ubicación)	Descripción		Eliminada de la estación de trabajo	Disponible en la interfaz de usuario	Más información
<b>Mapa de ubicaciones</b> (Estación de trabajo, investigador, Explorador de métrica, hojas de host y de agente)	Permite consultar la configuración y monitorizar el rendimiento de la infraestructura.		Sí	Sí	<ul style="list-style-type: none"> <li>Visualización de las relaciones de los componentes en el mapa</li> <li>Capas del mapa</li> </ul>
<b>Cierre de Enterprise Manager</b> (Estación de trabajo, editor de módulo de gestión, gestor)	Permite detener Enterprise Manager desde la estación de trabajo y cerrar la sesión de la estación de trabajo.		Sí	No	N/D
<b>Publicar MIB</b> (Estación de trabajo, editor de módulo de gestión, gestor)	Permite capturar los datos de la métrica que se almacenan en las recopilaciones de SNMP.		Sí	No	N/D
<b>Nueva acción</b> (Estación de trabajo, editor de módulo de gestión, elementos)	Permite crear: <ul style="list-style-type: none"> <li>Nueva acción de notificación de consola</li> <li>Nueva acción de notificación de SNMP</li> <li>Nueva acción de envío de correo SMTP</li> <li>Nueva acción de comando de shell</li> <li>Nueva acción de alerta de SNMP</li> </ul>		Sí		<ul style="list-style-type: none"> <li>Creación y configuración de acciones de notificación en Team Center</li> </ul>
<b>Nueva sesión de seguimiento de transacciones.</b> (Estación de trabajo, todas las vistas)	Realiza un seguimiento de la actividad de las transacciones dentro de una aplicación de producción.		Sí	Sí	<ul style="list-style-type: none"> <li>Inicio de una nueva sesión de seguimiento de la transacción</li> <li>Visualización de las relaciones de los componentes en el mapa</li> </ul>
<b>Nuevo visor de errores en directo</b> (Estación de trabajo, todas las vistas)	Permite investigar errores en todos los agentes supervisados por Enterprise Manager en modo <i>en directo</i> .		Sí	Sí	<ul style="list-style-type: none"> <li>Investigación de problemas mediante el Bloc de notas de análisis</li> </ul>

Función (ubicación)	Descripción		Eliminada de la estación de trabajo	Disponible en la interfaz de usuario	Más información
<b>Consulta de eventos históricos</b> (Estación de trabajo, todas las vistas)	Permite investigar errores en todos los agentes supervisados por Enterprise Manager en modo <i>histórico</i> .		Sí	Sí	<ul style="list-style-type: none"> <li><a href="#">Investigación de problemas mediante el Bloc de notas de análisis</a></li> </ul>
<b>Consola de estado de APM</b> (Estación de trabajo, todas las vistas)	Permite consultar estados y eventos importantes de una instancia de Enterprise Manager independiente o agrupada en clúster.		Sí	No	N/D

## Descripción general de Workstation

Workstation proporciona Investigator y la consola para ver los datos y el estado de las aplicaciones.

DX APM, a través de ProbeBuilder, agrega sondas de agente a una aplicación de Java, PHP o .NET. El uso de AutoProbe automatiza este proceso, con ProbeBuilder agregando dinámicamente las sondas cuando se inicia la aplicación. Los archivos de directivas de ProbeBuilder (PBD) indican a ProbeBuilder cómo agregar sondas como temporizadores y contadores a componentes de PHP, .NET o Java. Las sondas instrumentan la aplicación web.

Las sondas miden elementos específicos de información sobre una aplicación sin cambiar la lógica del negocio de la aplicación. Un agente está instalado en el mismo equipo que la aplicación instrumentada. Después de que se hayan instalado las sondas en el código de bytes, la aplicación de Java se denomina *aplicación instrumentada*. Cuando se está ejecutando la aplicación de Java con las sondas, se denomina aplicación gestionada.

DX APM también detecta e instrumenta automáticamente los componentes adicionales sin las directivas de ProbeBuilder definidas.

Mientras se ejecuta una aplicación gestionada, las sondas retransmiten los datos recopilados al agente. A continuación, el agente recopila y resume los datos y los envía a Enterprise Manager.

Se puede acceder a los datos recopilados por Enterprise Manager a través de una o varias Workstations. Puede utilizar la Workstation para ver los datos de rendimiento. También puede configurar Enterprise Manager para realizar tareas tales como la recopilación de información para su posterior análisis y para la creación de alertas.

Mientras se ejecuta una aplicación gestionada, los agentes recopilan datos de rendimiento en tiempo real y envían la información a Enterprise Manager. Workstation permite realizar estas tareas:

- Configuración de Enterprise Manager
- Organización de métricas
- Visualización de la información seleccionada en un formato cómodo

### Monitorización del rendimiento con herramientas de Workstation

Las herramientas de Workstation le ayudan a realizar las siguientes tareas para mejorar la monitorización del rendimiento de las aplicaciones:

- Filtrado y visualización de las métricas de rendimiento para diversos elementos del sistema en el que se ejecuta la aplicación.
- Obtención de detalles para detectar la causa raíz de los problemas de rendimiento del sistema.
- Creación de presentaciones gráficas de las métricas.

## **Acceso a las distintas vistas de datos de métrica**

Utilice Workstation para ver los datos de la métrica en diferentes formularios. Los usuarios autorizados pueden realizar funciones administrativas y de configuración. Workstation presenta información en estas ventanas:

- **Consola**  
Muestra los datos en los cuadros de mandos que contienen visores de datos.
- **Investigator**  
Muestra vistas de árbol de agentes, aplicaciones, recursos y métricas.
- **Editor del módulo de gestión**  
Presenta una vista de árbol de los módulos de gestión, permitiendo crear y editar módulos de gestión.
- **Editor del cuadro de mandos**  
Permite a los usuarios con permisos de *escritura* para un dominio (o superdominio) crear y editar visores de datos y otros objetos del cuadro de mandos como imágenes importadas, formas, líneas y texto.
- **Visores de datos**  
Presentación visual de los datos en función del tipo.

## **Conexión con Workstation**

Workstation está disponible para la descarga desde la sección **Descargas** en el panel izquierdo. De forma predeterminada, Workstation está configurada para comunicarse directamente con la puerta de enlace de la nube. Sin embargo, las organizaciones que requieren comunicación de canal única entre el centro de datos y la puerta de enlace de la nube pueden conectar Workstation con Cloud Proxy.

## **Acerca de la consola de Workstation**

La consola es la vista predeterminada que aparece cuando se inicia Workstation y contiene los cuadros de mandos que muestran los datos de rendimiento en vistas gráficas. Los cuadros de mandos son herramientas básicas para la visualización de datos de gestión de DX APM.

El módulo de gestión predeterminado proporciona un conjunto de cuadros de mandos de muestra. Los usuarios autorizados pueden crear cuadros de mandos personalizados mediante el Editor del cuadro de mandos.

Puede tener más de una ventana de la consola abierta a la vez.

### **Para abrir una nueva ventana de la consola:**

- Seleccione Workstation > Nueva consola.

## **Sobre Workstation Investigator**

Utilice Investigator para ver las métricas en las aplicaciones y sus supuestos back-ends de maneras diferentes. Puede tener más de una ventana de Investigator abierta a la vez.

### **Para abrir una nueva ventana de Investigator:**

- Seleccione Workstation > Nuevo Investigator.

Se abrirá Investigator, que muestra los datos de la aplicación de .NET o Java.

También puede abrir una ventana de Investigator desde la consola haciendo doble clic en algunos elementos del cuadro de mandos, en función de cómo se ha creado el elemento.

## **La ficha Explorador de métrica**

La ficha Explorador de métrica muestra una visión centrada en el agente de las aplicaciones monitorizadas. Se utiliza para realizar las tareas siguientes:

- Visualización de las aplicaciones y las métricas organizadas en una jerarquía de árbol.
- Monitorización de métricas detalladas en cada capa de la tecnología.
- Uso del seguimiento de las transacciones para evaluar errores y anomalías en el rendimiento de las aplicaciones.

### **Acerca del Editor del módulo de gestión**

Utilice el Editor del módulo de gestión para crear o editar un módulo de gestión, que contiene un conjunto de información de configuración de la monitorización de DX APM. Los módulos de gestión se muestran para cada dominio.

**Nota:** Si tiene una licencia de DX APM completa, puede crear, editar o suprimir la información en el Editor del módulo de gestión. Si no tiene una licencia completa, solo podrá consultar la información.

El árbol del Editor del módulo de gestión muestra los módulos de gestión implementados en Enterprise Manager por parte del dominio.

La parte derecha del Editor de módulo de gestión presenta la configuración actual para el elemento seleccionado en el árbol.

Un usuario autorizado puede modificar elementos del Editor del módulo de gestión.

### **Sobre el Editor del cuadro de mandos**

El Editor del cuadro de mandos proporciona herramientas para crear y diseñar visores de datos, formas, líneas, cuadros de texto y conectores. Los usuarios con los permisos adecuados pueden crear y editar los cuadros de mandos y los objetos del cuadro de mandos como imágenes importadas, formas, líneas y texto.

### **Acerca de los Visores de datos**

Los Visores de datos en el panel del visor de la ficha Explorador de métrica o en un cuadro de mandos muestran los datos de una aplicación activada para DX APM de forma visual. Los Visores de datos pueden mostrar datos de una métrica, de un recurso o de un elemento, como una alerta.

**Nota:** El valor de tiempo en los visores de datos es la hora del reloj en el equipo que aloja Enterprise Manager. Sin embargo, el valor de tiempo se ajusta para la zona horaria donde se ejecuta Workstation.

### **Tipos de Visor de datos**

Los tipos de datos tienen un tipo del visor de datos predeterminado visores alternativos.

Tipo de datos	Tipo de Visor de datos predeterminado	También pueden verse como
Métrica	Gráfica	Medidor dial, gráfico de barras, ecualizador gráfico, visor de cadena, visor de texto
Agrupación de métrica	Gráfica	Gráfico de barras, Visor de cadena
Alert	Indicador de alertas	Gráfico, gráfico de barras o visor de cadena
Calculadora	Gráfica	Medidor dial, gráfico de barras, ecualizador gráfico, visor de cadena

Según el tipo de métrica o elemento, Workstation puede mostrar los datos en un Visor de datos con los tipos de visualización de la vista que se muestran a continuación.

### **Gráfica**

Valores del diagrama gráfico a lo largo del tiempo. En las vistas en tiempo real, el gráfico muestra de forma dinámica el período de tiempo más reciente que se ajusta en el gráfico.

Si el gráfico muestra una alerta, los umbrales de precaución y peligro aparecerán como líneas amarillas y rojas, respectivamente.

Puede cambiar la escala de gráficos mientras se visualizan los datos reales para ver los datos en una vista más legible.

### **Gráfico de barras**

Los gráficos de barras muestran los valores de datos actuales como barras horizontales. El gráfico de barras es la vista predeterminada para las vistas filtradas de X principales.

Si un gráfico de barras muestra una alerta, las barras serán verdes, amarillas o rojas según correspondan al estado de la alerta.

El gráfico de barras solamente permite visualizar datos reales.

### **Ecualizador gráfico**

Los ecualizadores gráficos muestran el valor actual de los datos, así como niveles recientes más altos.

### **Visor de cadena**

Los visores de cadena pueden mostrar un valor como una línea de texto. Los visores de cadenas permiten mostrar algunos valores en un espacio relativamente pequeño. También puede utilizar un visor de cadena para valores simples que no cambian, por ejemplo, la hora de inicio o la dirección IP.

**Nota:** Con las métricas en tiempo real de los agentes conectados, la mayoría de los datos sirven solamente para el intervalo de tiempo más reciente de 15 segundos. Por lo tanto, cuando se desconecta un agente, las métricas de cadena no muestra ningún valor. Sin embargo, algunas métricas constantes como, por ejemplo, la hora de inicio original del agente, seguirán siendo válidas si el agente está o no conectado actualmente.

### **Visor de texto**

Los visores de texto muestran el texto para los datos cuando se añaden nuevos valores para, por ejemplo, un sistema o un registro de excepciones.

### **Acerca de las alertas y los indicadores de alerta**

Los indicadores de alerta muestran si una métrica ha superado un umbral:

- Disco verde = estado normal
- Diamante amarillo = precaución, se ha traspasado el umbral
- Octágono rojo = peligro, se ha traspasado el umbral
- Disco gris = la alerta no contiene datos

Los indicadores de alerta pueden aparecer como se explica anteriormente, como una matriz de tres indicadores en la cual el indicador activo indica el estado. Más a menudo, aparecen como un indicador único que cambia el color y la forma cuando se cambia su estado.

Los indicadores de alerta pueden aparecer en varias ubicaciones y modos:

- en los cuadros de mandos
- en la ficha Descripción general
- como líneas de umbral en un gráfico
- como colores en las celdas de la tabla, donde se admite la función
- en lugar de los nodos de árbol

### **Comprensión de la diferencia entre *alertas* e *indicadores de alerta***



Es importante comprender exactamente qué es una alerta. No olvide distinguir entre:

- la **alerta** misma, la definición de la cual incluye atributos guardados como:
  - valores del umbral
  - la agrupación de métrica a la que está vinculada
  - el módulo de gestión al que pertenece
- el **indicador de alerta**, que es una visualización gráfica del estado de la alerta.

## Evaluación de errores con Workstation

Investigator de Workstation proporciona una visión centrada en el agente que permite examinar las métricas e identificar las posibles causas de los problemas del entorno.

### Funciones generales de Investigator

#### Sugerencias de navegación

**Para abrir Investigator:**

- Seleccione **Workstation > Nuevo Investigator**.

**Para desplazarse hacia adelante y hacia atrás:**

- Los botones de flecha Hacia adelante y Hacia atrás se encuentran en la esquina superior derecha. Utilice estos botones para desplazarse hacia adelante o hacia atrás entre los elementos del árbol jerárquico visualizado previamente.
- Seleccione los valores de las listas desplegables que aparecen junto a los botones Hacia adelante o Hacia atrás en la esquina superior derecha de Investigator.

#### Paneles de Investigator

Investigator contiene dos paneles:

- Una jerarquía de árbol en un panel estrecho a la izquierda de la pantalla
- Un panel visor de gran tamaño en el lado derecho de la pantalla
  - El contenido del panel visor varía en función del tipo de elemento seleccionado en el árbol jerárquico.
  - El panel visor se compone de una o más fichas. Cada ficha muestra una vista distinta.

Las gráficas de métrica son la opción de visualización de las métricas más habitual, aunque no la única. Para las métricas, aparece una vista de los datos de métrica. Cada tipo de métrica tiene un valor predeterminado para mostrar en el panel visor.

#### Información sobre herramientas

La información sobre herramientas identifica las rutas y los valores de métrica en los paneles visor y en los árboles jerárquicos. Para acceder a la información sobre herramientas en la ficha Explorador de métrica, pase el ratón sobre el nombre de la métrica en un área de la leyenda del visor de datos.

Se pueden ver varios tipos de información en la información sobre herramientas, en función del elemento de la interfaz de usuario sobre el que el cursor esté en movimiento. Esta información puede incluir los datos siguientes:

- Nombre completo de la métrica, su valor y sus valores mínimos y máximos
- Un recuento de la cantidad de puntos de datos sobre los que se ha informado en el intervalo de tiempo seleccionado
- Una marca de tiempo del valor de datos más cercano al cursor o una nota de comparación

- Por ejemplo, la nota "Valor demasiado alto" cuando el valor de la métrica excede un umbral definido.

### NOTE

La información sobre herramientas ya no está disponibles en los nodos.

### Vista centrada en el agente

Un agente es un componente de software que está instalado en un host en el que se ha implementado una aplicación. El agente recopila las métricas del entorno y de las aplicaciones y las retransmite a Enterprise Manager. La ficha Explorador de métrica permite explorar una lista completa de las métricas sobre las que está informando un único agente. Cada aplicación sobre cuyos datos está informando un agente aparece en un árbol jerárquico de un nodo llamado **Frontends**.

La vista centrada en el agente contiene las siguientes secciones:

- El *árbol centrado en el agente* de la izquierda proporciona información sobre cada host y aplicación que gestiona Enterprise Manager. Las métricas que aparecen en el árbol centrado en el agente son una función de los factores siguientes:
  - Los recursos que utilizan las aplicaciones
  - Los datos sobre los que deben informar los agentes de Introscope configurados
- El *panel Visor*, en la parte derecha de la pantalla, muestra los detalles, a menudo en forma de gráfica, para el recurso o la métrica del árbol. Se pueden seleccionar las fichas de vista para abrir diferentes vistas de datos. Las fichas disponibles varían en función del elemento seleccionado del árbol. Algunas vistas de la sección inferior del panel visor pueden incluir opciones para controlar los datos que se muestran en el visor.
- Una tabla en la parte inferior del panel visor que muestra los datos en formato tabular. Los datos que se muestran en la tabla dependen del elemento que se seleccione en el panel visor o el árbol.

### Fijación de la métrica de agente

Un icono de agente que muestra una cinta roja indica un agente con una métrica fija. Un agente se fija cuando el número de métricas que produce es mayor que el número de métricas que puede procesar Enterprise Manager. Una vez que se fijan las métricas del agente, no se puede saber sobre qué métricas no se informa. Las métricas se pueden fijar desde el agente o desde Enterprise Manager. Si se realiza una fijación de métrica basada en el agente, se muestran distintos mensajes en los registros que indican que se ha aplicado la fijación y que no se informará de ningún valor de métrica nuevo. En el caso de una fijación de la métrica basada en Enterprise Manager, se continúa informando de los valores de las métricas sobre las que ya se informaba antes de aplicar la fijación, aunque no se muestra ningún tipo de métrica nuevo. La métrica de compatibilidad de un agente fijo informa de un valor 1. Un agente fijo indica que se ha activado demasiada instrumentación. Ajuste el nivel de instrumentación en la configuración del agente.

Un agente fijo también puede indicar una expansión de la métrica. En este caso, los componentes de los agentes informan de las constantes variaciones de las métricas. Para obtener más información sobre las expansiones de métricas, consulte [Expansiones de métricas](#).

### Nodo SuperDomain

El nodo **SuperDomain** contiene las métricas para todos los agentes que informan a la instancia de Enterprise Manager a la que está conectada Workstation. Las métricas se organizan en la jerarquía `Host | Process | Agent`.

Los nodos que se muestran inmediatamente debajo del nodo **SuperDomain** son el host virtual y los hosts físicos.

- **Custom Metric Host (virtual):** Este nodo no se corresponde con un equipo de host físico. El nodo es un host virtual que contiene las métricas distintas a las métricas sobre las que informan agentes específicos e individuales. Por

ejemplo, métricas personalizadas que se muestran en el nodo Custom Metric Host. Las métricas personalizadas proceden o bien de calculadoras configuradas, o bien de agentes agregados configurados.

- **Hosts:** Un nodo para cada equipo que hospeda un agente. Cada nodo de host contiene un nodo de proceso para la instancia de la aplicación que se está monitorizando. El nodo de proceso contiene un nodo de agente. El nodo de agente contiene nodos que corresponden a los recursos de las aplicaciones y del sistema y que contienen métricas.  
**Nota:** Los recursos de aplicaciones que aparecen en el nodo de agente son diferentes en función de si el tipo de agente es .NET o Java.

El nodo SuperDomain incluye todos los agentes y dominios definidos por el usuario. El administrador de Enterprise Manager puede configurar Enterprise Manager para que muestre los dominios hijo con permisos independientes.

Las métricas que muestra el árbol centrado en el agente son una función de los dos factores siguientes:

- Las directivas de ProbeBuilder (archivos PBD) utilizadas para instrumentar la aplicación
- La actividad de tiempo de ejecución de la aplicación

Una métrica no aparece en el árbol hasta que el agente empieza a informar sobre ella. La métrica permanece visible en el árbol, aunque el agente deje de informar sobre ella.

Cuando las métricas tienen diferentes tipos de métrica, en Investigator las métricas pueden tener el mismo nombre y pueden aparecer dos veces. Como ocurre con todas las métricas, las métricas inactivas en esta situación aparecen atenuadas.

## **Herramientas para monitorizar el estado de Enterprise Manager**

### **Métricas de compatibilidad**

Las métricas de compatibilidad proporcionan información sobre el estado de Enterprise Manager y el equipo en el que se ejecuta. Se muestran en la ruta `SuperDomain|Custom Metric Host|Custom Metric Agent|Enterprise Manager`.

### **Nodo de dominios**

El administrador de DX APM puede organizar los agentes que informan a Enterprise Manager en dominios. En este caso, el nodo de dominio del árbol centrado en agentes contiene subnodos para cada dominio. Cada nodo de dominio se estructura en la misma jerarquía `Host|Process|Agent` que el nodo SuperDomain. Cada nodo de dominio también puede contener a un agente de métrica personalizada para las métricas personalizadas.

### **Cómo afectan los permisos de usuario a lo que se puede visualizar**

El administrador de DX APM asigna los permisos para los dominios y los componentes que pueden ver los usuarios de Workstation. Los permisos solamente están disponibles cuando un administrador los ha configurado mediante Enterprise Enablement Manager.

El contenido de la ficha **Explorador de métrica** se basa en los permisos de dominio del usuario:

- Los usuarios con el permiso `SuperDomain` (al menos permiso de lectura) pueden visualizar todos los dominios para esa instancia de Enterprise Manager en el árbol centrado en agentes.
- Los usuarios con permisos para varios dominios pueden ver la información sobre el dominio para los dominios del árbol centrado en agentes.
- Los usuarios con permisos para un único dominio no podrán ver la información sobre el dominio en el árbol centrado en agentes. Los usuarios únicamente ven las carpetas para los módulos de gestión y las métricas.

## Ficha Explorador de métrica

La ficha Explorador de métrica muestra las métricas y otra información en un formato de árbol. Los nodos de alto nivel inmediatamente en los nodos de dominio representan a agentes instalados en hosts de servidores de aplicaciones individuales o el equivalente.

Los distintos componentes que representan los nodos de alto nivel son:

- Componentes de las aplicaciones J2EE, PHP o .NET, como servlets, EJB o páginas ASP.
- Nodos de sistema, incluidos el host que ejecuta el servidor de aplicaciones y el equipo host que ejecuta DX APM.
- Eventos, defectos y otras actividades distintivas

Se pueden ver datos en directo en Investigator o se puede seleccionar un intervalo de tiempo para visualizar los datos históricos. La vista predeterminada de los datos es el modo en directo.

### Métricas en la ficha Explorador de métrica

Las métricas predeterminadas que muestra Workstation en la ficha Explorador de métrica varían en función del nodo seleccionado en el árbol jerárquico.

### Métricas estándares

Introscope muestra las cinco métricas estándares, a veces denominadas [métricas de BlamePoint](#), para los componentes de la aplicación front-end y back-end monitorizados y para muchos otros componentes de la aplicación:

- Tiempo medio de respuesta (ms): Una medida de la velocidad de respuesta de la aplicación.
- Invocaciones simultáneas: El número de solicitudes que se gestionan en un momento determinado.
- Errores por intervalo: El número de errores que se producen durante un intervalo de tiempo especificado.
- Respuestas por intervalo: El número de solicitudes que se han completado durante un intervalo de tiempo especificado.
- Recuento de detenciones: El número de detenciones (o solicitudes sin completar) que no se han completado antes de un umbral de tiempo especificado.

Además de las cinco métricas estándares y, a veces, en lugar de estas, Introscope recopila y muestra otras [métricas](#) relevantes para el nodo.

### Front-ends y back-ends

De forma predeterminada, Introscope define un front-end como un archivo .war o .jsp que gestiona primero una transacción entrante para una aplicación. En una aplicación .NET, el equivalente sería una página ASP.

Un *back-end* es un sistema externo del que depende una aplicación web para una parte de su procesamiento. Normalmente se trata de una base de datos, pero puede ser cualquier sistema externo como un servidor de correo, un sistema de procesamiento de transacciones (por ejemplo, IBM CICS o BEA Tuxedo) o un sistema de mensajería (por ejemplo, MQSeries). Introscope identifica automáticamente las bases de datos como sistemas de back-end por el nombre de la base de datos. Para otros sistemas externos, Introscope analiza la actividad del socket de la aplicación y proporciona un nombre al back-end en función de la dirección IP y el puerto a través del cual se comunica la aplicación.

### Visualización de las métricas para los back-ends

El nodo Backends del árbol Explorador de métrica contiene un nodo para cada back-end, incluidos los detectados automáticamente por Introscope o que se han marcado explícitamente como un back-end durante ProbeBuilding.

Normalmente los back-ends son una base de datos, pero pueden ser cualquier sistema externo como un servidor de correo, un sistema de procesamiento de transacciones (por ejemplo, IBM CICS o BEA Tuxedo) o un sistema de mensajería (por ejemplo, MQSeries).

## Métricas de back-end de la base de datos

Cuando el sistema de back-end es una base de datos, estas métricas reflejan la actividad y el rendimiento de back-end en todas las aplicaciones a las que presta servicio:

- Tiempo medio de respuesta (ms)
- Invocaciones simultáneas
- Errores por intervalo
- Connection Count: El número de conexiones a la base de datos durante un intervalo determinado.
- Responses Per Interval
- Recuento de detenciones

## Formato de nomenclatura de back-end de la base de datos

Esta sección explica la convención de nomenclatura de Introscope para los back-ends de base de datos.

### Oracle

El nombre de back-end es una concatenación de la cadena del SID de Oracle, el host y el puerto de la base de datos delimitados por un guión y la cadena (*Oracle DB*).

Por ejemplo:

```
PRODORCL3 sfoprod6.globex.com-1521 (Oracle DB)
```

### DB/2

El nombre de back-end es una concatenación de la cadena de nombre de la base de datos y la cadena (*DB/2 DB*).

Por ejemplo:

```
Inventory4 (DB/2 DB)
```

### Microsoft SQL Server

El nombre de back-end puede ser una concatenación del nombre de la base de datos, el nombre de la instancia, el host y el puerto de la base de datos delimitados por un guión y la cadena (*MS SQL Server DB*), según la configuración del controlador de la base de datos.

Si el controlador tiene un nombre de base de datos y un nombre de instancia, el nombre del back-end en Investigator será similar al siguiente:

```
PRODORCL3 (instance Mx22) on prod6.globex.com-1521 (MS SQL Server DB)
```

Si el controlador no tiene ningún nombre de base de datos, el nombre del back-end en Investigator será similar al siguiente:

```
SQLServer on prod6.globex.com-1521 (MS SQL Server DB)
```

Si el controlador tiene un nombre de base de datos pero no tiene ningún nombre de instancia, el nombre del back-end en Investigator será similar al siguiente:

```
PRODORCL3 on prod6.globex.com-1521 (MS SQL Server DB)
```

Si el controlador tiene un nombre de instancia pero no tiene ningún nombre de base de datos, el nombre del back-end en Investigator será similar al siguiente:

```
(instance Mx22) on prod6.globex.com-1521 (MS SQL Server DB)
```

## Valores predeterminados y de reserva

En casos en los que el controlador de la base de datos no admite consultas para el nombre de la base de datos, se establece la dirección URL de JDBC como valor predeterminado para el nombre de la base de datos, con los caracteres

de dos puntos (:) reemplazados por los caracteres de porcentaje (%). En algunos casos incluso este valor de reserva no está disponible, por lo que se establece el nombre de la clase del controlador de la base de datos como valor predeterminado del nombre de la base de datos. Este comportamiento exacto depende del distribuidor y de la versión del controlador de la base de datos.

### Otras métricas de back-end

También se puede configurar cada sistema back-end para que informe de las siguientes métricas:

- Commits
- Rollbacks
- SQL

### Métricas de alerta en el árbol centrado en agentes

Cada color de alerta se corresponde con un valor de la métrica:

- Gris: 0, no hay datos disponibles
- Verde: 1, correcto
- Amarillo: 2, precaución
- Rojo: 3, peligro

La tabla siguiente muestra cómo determinan las métricas los valores de alerta en la ficha Descripción general.

Tipo de métrica	Significado de un indicador amarillo	Significado de un indicador rojo
Usuario	Errores de front-end anómalos Tiempo de respuesta de front-end anómalo Recuento de detenciones de front-end anómalo	Errores de front-end <i>muy</i> anómalos Recuento de detenciones de front-end <i>muy</i> anómalo
VM	Uso acumulado de la CPU anómalo y superior al 30 % Uso del grupo de conexiones JDBC anómalo	Uso acumulado de la CPU <i>muy</i> anómalo y superior al 50 % Uso del grupo de conexiones JDBC <i>muy</i> anómalo
Backend Summary	Tiempo de respuesta de back-end anómalo Recuento de errores de back-end anómalo Detenciones de back-end anómalas	Recuento de errores de back-end <i>muy</i> anómalo Detenciones de back-end <i>muy</i> anómalas

Se pueden visualizar las métricas de alerta mediante la selección de las métricas User, VM y Backends|*Nombre\_back-end* en el nodo Heuristics en Investigator.

Las métricas subyacentes que determinan las métricas de alerta se muestran en las carpetas de User, VM y Backends|*Nombre\_back-end* del árbol.

### Administración de las conexiones de los agentes desde Workstation

Se pueden ejecutar comandos directamente desde Workstation para desmontar o apagar agentes o métricas individuales.

Cuando se implementa un agente en un servidor de aplicaciones, se inicia automáticamente cuando se inicia el servidor de aplicaciones y aparece en el árbol Explorador de métrica de la instancia de Enterprise Manager a la que informa de los datos de las métricas. Cuando aparece el agente en el árbol, se dice que se ha *montado*.

Cuando falla un servidor de aplicaciones, el agente detiene de forma automática la notificación de datos a Enterprise Manager. Este agente se considera que está *desconectado* y aparece en el árbol Explorador de métrica atenuado en color gris.

Un agente desconectado todavía aparece como montado en el árbol Explorador de métrica y aún se pueden explorar las métricas sobre las que ha informado antes de que se desconectara. Si desea eliminarlo del árbol Explorador de métrica, deberá *desmontar* el agente.

#### Para desmontar un agente:

1. Haga clic con el botón secundario del ratón en un agente desconectado.
2. Seleccione Desmontar <Nombre\_agente>.  
El agente desaparecerá del árbol de exploración.

Si desea ver los datos históricos almacenados en la base de datos de SmartStor para un agente que se ha desmontado, puede volver a montar el agente para que aparezca de nuevo en el árbol Explorador de métrica.

#### Para volver a montar un agente desconectado:

1. Seleccione Gestor > Montar agente.  
Aparecerá el cuadro de diálogo Selector de agente.
2. Seleccione un agente de la lista para volver a montar.
3. Haga clic en Aceptar.

El árbol Explorador de métrica muestra los agentes desconectados y se pueden explorar los datos almacenados en la base de datos de SmartStor.

Si desea que Enterprise Manager deje de almacenar los datos de un agente que aún está en ejecución, puede detener la recopilación de datos sin detener el servidor de aplicaciones seleccionando el comando Apagar.

**Nota:** El comando Apagar realmente no apaga el agente; cierra la conexión entre un agente en ejecución y Enterprise Manager.

#### Para detener la conexión de un agente en ejecución:

1. Haga clic con el botón secundario del ratón en un agente conectado.
2. Seleccione Apagar <Nombre\_agente>.

El agente continúa ejecutándose en el servidor de aplicaciones mientras se sigue ejecutando el servidor de aplicaciones, pero Enterprise Manager ya no está conectado al agente ni almacena datos de métrica para este.

Después de detener la conexión a un agente, se puede volver a activar la conexión.

#### Para activar la conexión de un agente apagado:

1. Haga clic con el botón secundario del ratón en un agente apagado.
2. Seleccione Encender todos los componentes del agente.

Se vuelve a abrir la conexión entre el agente y Enterprise Manager, y el agente empieza de nuevo a informar de datos a Enterprise Manager. Se deben esperar de 30 a 45 segundos para que los datos empiecen a aparecer en Workstation.

**Nota:** El comando Encender todos los componentes del agente únicamente funciona si previamente se ha detenido la conexión del agente a través de Workstation mediante el comando Apagar <Nombre\_agente>.

#### Vistas en la ficha Explorador de métrica

Cuando la ficha Explorador de métrica está seleccionada en el panel izquierdo de Investigator, las vistas que aparecen en el panel derecho varían en función del recurso o la métrica seleccionados en el árbol de la ficha Explorador de métrica. Dependiendo del tipo de nodo seleccionado, se muestran fichas de una o varias de las siguientes vistas:

- Ficha General
- Fichas Descripción general
- Ficha Buscar
- Ficha Seguimientos
- Ficha Errores
- Ficha Recuento de métricas
- Ficha Volcados de subprocesos

### **Ficha General**

Cuando se selecciona una métrica, la ficha General muestra una vista gráfica de la métrica para los datos en directo o para un período histórico seleccionado. Consulte [Visualización de los datos históricos en la ficha Explorador de métrica](#) para obtener una explicación sobre cómo seleccionar intervalos de datos históricos para visualizarlos.

Para algunos nodos del árbol, la ficha General muestra la ruta a dicho objeto de nodo en la jerarquía de Investigator. Por ejemplo, cuando se selecciona el nodo Front-ends, la ficha General muestra la ruta siguiente:

```
SuperDomain | HostName | ProcessName | AgentName | Frontends
```

Para algunos otros nodos del árbol, la ficha General muestra la vista de los 10 más lentos para el nodo seleccionado. Por ejemplo, cuando se selecciona el nodo EJB, la ficha General muestra los tiempos de respuesta de los diez principales componentes invocados del nodo EJB seleccionado.

### **Métricas de los diez más lentos o peores**

Cuando se seleccionan determinados recursos en Investigator, la ficha General del panel Visor muestra las métricas con los diez valores peores o más lentos del recurso seleccionado. Los recursos de Java incluyen los servlets, JSP, EJB y JDBC; los recursos para .NET incluyen ASP.NET, ADO.NET y componentes con servicio.

Estas métricas aparecen en un gráfico de barras en el panel visor de Investigator.

También se pueden visualizar los tiempos de respuesta de los diez mejores componentes invocados de un servlet, EJB o JSP seleccionado para Java o de ASP.NET, ADO.NET y componentes con servicio seleccionados para .NET.

Si se muestran menos de diez barras en el gráfico de barras, se debe a que hay menos de diez componentes monitorizados para ese recurso. Si la métrica no contiene datos, es posible que se muestren los nombres de las métricas en el panel visor, pero sin barras de datos.

### **Fichas Descripción general**

Investigator resume la información en una ficha de descripción general para los datos siguientes:



- Estado general de las aplicaciones (consulte la sección Descripción general de las aplicaciones)
- Estado de Enterprise Manager (consulte la sección Descripción general de Enterprise Manager)
- Datos de las páginas de ASP.NET (consulte la sección Descripción general de ASP.NET)
- Datos de EJB (consulte la sección Descripción general de EJB)
- Datos de los front-ends de la aplicación (consulte la sección Descripciones generales de los front-ends)
- Datos de los sistemas back-end de la aplicación (consulte la sección Descripción general de los back-ends)
- Datos de la memoria dinámica de la recopilación de elementos no utilizados (GC) (consulte la sección Descripción general de la memoria dinámica de la recopilación de elementos no utilizados)
- Recuentos de instancias de clases de Java instanciadas en la JVM (consulte la sección Recuentos de instancias)
- Datos de Java NIO (consulte la sección Descripción general de Java NIO)
- Datos de los componentes de JTA (consulte la sección Descripción general de JTA)
- Datos de los servlets (consulte la sección Descripción general de los servlets)
- Conexiones de socket (consulte la sección Descripción general de los sockets)
- Datos de Struts (consulte la sección Descripción general de Struts)
- Datos de subprocesos en ejecución (consulte la sección Descripción general de los subprocesos)
- Datos de componentes XML (consulte la sección Descripción general de XML)

#### NOTE

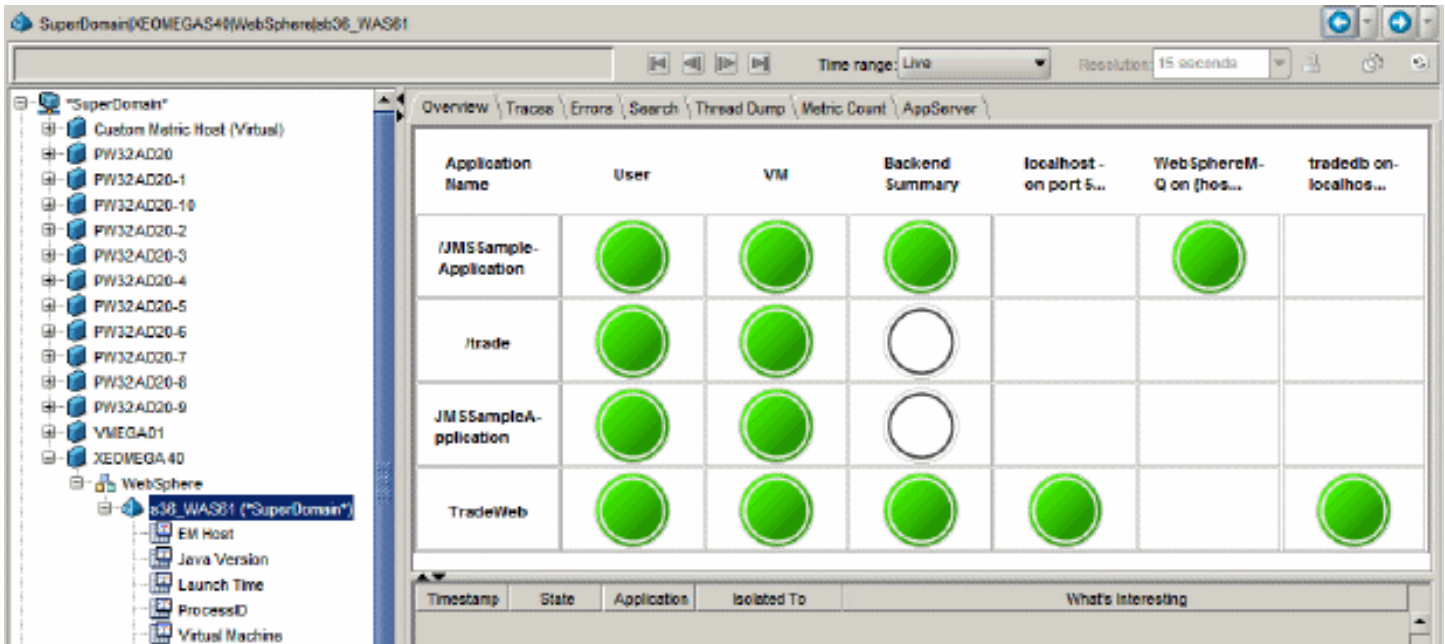
Las fichas de descripción general muestran los valores actuales de las métricas cuando se visualiza en el **modo en directo**. Cuando se utiliza el **modo histórico** para visualizar los datos, las fichas de descripción general muestran los valores acumulados de las métricas (un valor promedio o sumado, en función del tipo de métrica) para el intervalo de tiempo seleccionado.

### **Descripción general de las aplicaciones**

La descripción general de las aplicaciones está disponible cuando se selecciona un agente en el árbol centrado en agentes y se activa la monitorización y la evaluación de errores de las aplicaciones. Esta muestra los indicadores de estado de alto nivel y un registro de los eventos relacionados e información histórica de las métricas.

La ficha Descripción general muestra una fila de indicadores para cada aplicación gestionada por el agente seleccionado actualmente. Introscope presenta estos datos para cada aplicación que detecta. Cuando se ejecuta un servlet, Introscope realiza una llamada a *getServletContextName()* de la interfaz de *ServletContext* para determinar el nombre de la aplicación. Una vez que se ha iniciado la aplicación, la ficha Descripción general se actualiza automáticamente para mostrar una fila de indicadores para la aplicación.

La siguiente imagen muestra la ficha Descripción general para un agente en un servidor de aplicaciones de WebSphere denominado *s36\_WAS61*:



Esta imagen muestra cuatro aplicaciones, una en cada fila de la tabla, gestionadas por este agente. Para esta aplicación, se pueden ver alertas que muestran el estado de:

**User:** Indica el grado de satisfacción probable de las interacciones del usuario final con la aplicación. La satisfacción es una función del tiempo de respuesta, las esperas, las detenciones y los errores.

- Verde: Estado normal, las interacciones del usuario con la aplicación son satisfactorias.
- Amarillo: Un intento de utilizar la aplicación es probable que produzca resultados no satisfactorios, por ejemplo, un tiempo de respuesta lento o errores.
- Rojo: Indica un problema de disponibilidad grave y que si se intenta utilizar la aplicación, probablemente se produzca un error.

**VM:** Indica el estado y la disponibilidad de los recursos del servidor, por ejemplo, la CPU y las agrupaciones de recursos.

- Verde: Estado normal de los recursos del servidor.
- Amarillo: Interrupciones o limitaciones de los recursos.
- Rojo: Interrupciones o limitaciones de los recursos graves.

**Backend Summary:** Indica el estado y la disponibilidad peores de todos los back-ends a los que ha accedido la aplicación. Por ejemplo, si uno de tres back-ends tiene una interrupción o limitación de recursos grave, el indicador para todos los back-ends se mostrará en rojo. La finalidad del indicador para todos los back-ends es la de permitir al usuario que, con el mínimo desplazamiento posible, evalúe rápidamente si alguno de los back-ends tiene problemas que requieran una investigación.

- Verde: Estado y disponibilidad normales de todos los back-ends a los que ha accedido la aplicación.
- Amarillo: Al menos un back-end al que ha accedido la aplicación está experimentando errores o detenciones, o tiempos de respuesta más lentos de lo esperado.
- Rojo: Al menos un back-end al que ha accedido la aplicación está experimentando interrupciones o limitaciones de recursos graves.

**Back-ends:** Cualquier indicador ubicado a la derecha del indicador Backend Summary hace referencia a un back-end individual.

- Verde: Estado y disponibilidad del back-end normales.
- Amarillo: Errores o detenciones del back-end, o tiempos de respuesta más lentos de lo esperado.
- Rojo: Interrupciones o limitaciones de los recursos del back-end graves.

Los indicadores se actualizan cada 15 segundos. Las filas se ordenan primero por color. Las filas con indicadores rojos preceden a aquellas en amarillo que, a su vez, preceden a las filas con todos los tonos de verde para reducir así el desplazamiento necesario para identificar los problemas potenciales. Dentro de una categoría de color, las filas están ordenadas alfabéticamente por nombre de la aplicación.

### **Uso de alertas para obtener datos más detallados**

Se puede hacer doble clic en una alerta desde la ficha Descripción general para mostrar los datos subyacentes para ese nivel de la aplicación. Por ejemplo, si se hace doble clic en la alerta de usuario, Workstation mostrará el nodo URLs para ese agente.

### **Métricas de la descripción general de aplicaciones en modo histórico**

En un intervalo histórico, un color de alerta refleja el valor para el peor caso de la heurística en cualquier momento en el intervalo histórico. Por ejemplo, si en cualquier momento durante un intervalo histórico la heurística de usuario para un agente se muestra en amarillo, pero nunca en rojo, la ficha Descripción general para dicho intervalo histórico se mostrará en amarillo.

### **Métricas de la descripción general de aplicaciones para un agente virtual**

Para los agentes virtuales, la heurística se evalúa en función de las métricas del agente virtual. Por este motivo, la ficha Descripción general para un agente virtual puede indicar un valor distinto al que se muestra para los agentes físicos en el agente virtual.

Por ejemplo, la ficha Descripción general para un agente virtual puede mostrar una alerta de usuario en verde, incluso si la ficha Descripción general para uno de los agentes en ese agente virtual muestra una alerta de usuario en amarillo.

Las métricas heurísticas únicamente se generan si existen las métricas que analizan. Por lo tanto, por ejemplo, si el agente virtual está configurado para que no incluya las métricas de la CPU, JMX o WebSphere PMI, no habrá ninguna carpeta de máquina virtual y la alerta de máquina virtual permanecerá en gris.

### **Descripción general de Enterprise Manager**

Se pueden visualizar distintas métricas en Enterprise Manager seleccionando el nodo EM en Custom Metric Agent.

### **Descripción general de ASP.NET**

En entornos donde Introscope está monitorizando una aplicación .NET, un nodo ASP.NET en el árbol centrado en agentes permite monitorizar las métricas para los componentes de la aplicación.

### **Descripción general de EJB**

La ficha Descripción general de EJB (Enterprise JavaBeans) muestra las estadísticas de los beans de entidad, beans de sesión y beans controlados por mensajes.

### **Descripciones generales de los front-ends**

Las descripciones generales para los nodos Frontend muestran las métricas de las aplicaciones en una gráfica y las estadísticas relacionadas con las transacciones en la aplicación:

Los programas que Investigator muestra bajo el nodo Front-ends representan los componentes de una aplicación que se encarga primero de gestionar una transacción entrante.

## **Descripción general de los back-ends**

Las descripciones generales para los nodos Backend muestran las vistas gráficas de las métricas de la base de datos y una vista de tabla de SQL bajo el nodo.

## **Descripción general de la memoria dinámica de la recopilación de elementos no utilizados**

La ficha Descripción general de la memoria dinámica de la recopilación de elementos no utilizados (GC) muestra el uso de la memoria dinámica.

### **Ficha Descripción general del monitor de recopilación de elementos no utilizados**

Al hacer clic en el nodo GC Monitor en el árbol Explorador de métrica, la ficha Descripción general del monitor de recopilación de elementos no utilizados aparece en el panel visor. La ficha Descripción general muestra tres paneles:

- Superior: Un indicador de alerta en la métrica Porcentaje de la memoria dinámica de Java utilizada para la máquina virtual Java.
- Centro: Una vista tabular de los recopiladores de elementos no utilizados en la máquina virtual Java
- Inferior: Una vista tabular de bloques de memoria en la máquina virtual Java

**Nota:** El indicador de alerta del panel superior de la ficha Descripción general y el sombreado que aparece en las celdas de las tablas de los paneles central e inferior se basan en los umbrales de precaución y peligro predefinidos. Los usuarios no pueden restablecer estos umbrales.

Al seleccionar cualquiera de los nodos individuales Garbage Collector o Memory Pool, las gráficas muestran las mismas métricas que se muestran en la ficha Descripción general.

Para obtener más información:

- Aprenda a [utilizar las métricas del monitor de recopilación de elementos no utilizados](#) para ajustar la asignación de memoria de la máquina virtual Java.

Activación y desactivación del monitor de recopilación de elementos no utilizados

Las métricas del monitor de recopilación de elementos no utilizados están activadas de manera predeterminada.

### **Para desactivar las métricas del monitor de recopilación de elementos no utilizados:**

1. Abra el archivo *IntroscopeAgent.profile*.
2. Edite el valor de la propiedad `introscope.agent.gcmonitor.enable` de `true` a `false`.
3. Guarde y cierre el archivo.

**Nota:** Esta es una propiedad configurable en caliente; no es necesario reiniciar Enterprise Manager para que se apliquen los cambios.

Para obtener más información sobre la edición de `IntroscopeAgent.profile`, consulte [Agente de Java](#).

## **Recuentos de la instancia**

La ficha Descripción general de los recuentos de instancias muestra las clases de las que se ha creado una instancia en la máquina virtual Java.

## **Descripción general de Java NIO**

La descripción general de NIO muestra tablas para datagramas y canales, que incluyen las métricas de cliente y servidor. Cuando se selecciona el nodo JavaNIO, la ficha Descripción general muestra información general sobre el nodo seleccionado, incluyendo todos los puertos con actividad NIO.

---

### **Descripción general de los canales de NIO**

La ficha Descripción general del nodo Channels muestra la información de cliente y servidor para datagramas y sockets.

### **Descripción general de los sockets de NIO**

La ficha Descripción general del nodo Sockets muestra gráficas para los datos de ancho de banda de entrada y salida y los datos de los lectores y editores simultáneos, así como la información de servidor y cliente para los sockets.

### **Descripción general de los datagramas de NIO**

La ficha Descripción general del nodo Datagrams muestra gráficas para los datos de ancho de banda de entrada y salida y los datos de los lectores y editores simultáneos, así como la información de servidor y cliente para los datagramas.

### **Descripción general de JTA**

La ficha Descripción general de JTA muestra datos acerca de los componentes de JTA.

### **Descripción general de los servlets**

La descripción general de servlet muestra una tabla de servlets en el nodo. Cuando se selecciona un servlet, Investigator muestra sus estadísticas en una gráfica.

Seleccione un servlet individual para ver la ficha de resumen Descripción general.

### **Descripción general de los sockets**

La descripción general de los sockets (no confundir con la descripción general de los sockets de NIO) muestra tablas para los sockets de cliente y servidor e información de los sockets para cada puerto. Cuando se selecciona el nodo Socket en el árbol centrado en agentes, el panel visor, a la derecha de la pantalla, muestra todos los puertos con sockets activos. Al seleccionar un puerto de la tabla Server en la parte superior del panel visor, se muestran los puertos de cliente del servidor en la tabla Client en la parte inferior. Cuando se selecciona un puerto del árbol centrado en agentes, se muestran gráficas de las métricas de los eventos y la carga.

### **Descripción general de Struts**

La ficha Descripción general de Struts muestra una descripción general de los componentes de Struts, con la visualización del tiempo medio de respuesta para todos los componentes.

Si se selecciona uno de los nodos de componente, se muestra una descripción general de las métricas para ese nodo.

### **Descripción general de los subprocesos**

La descripción general de los subprocesos muestra todos los subprocesos activos que se están procesando a través de un agente.

### **Descripción general de XML**

La ficha Descripción general para el nodo XML muestra las métricas para los componentes XML.

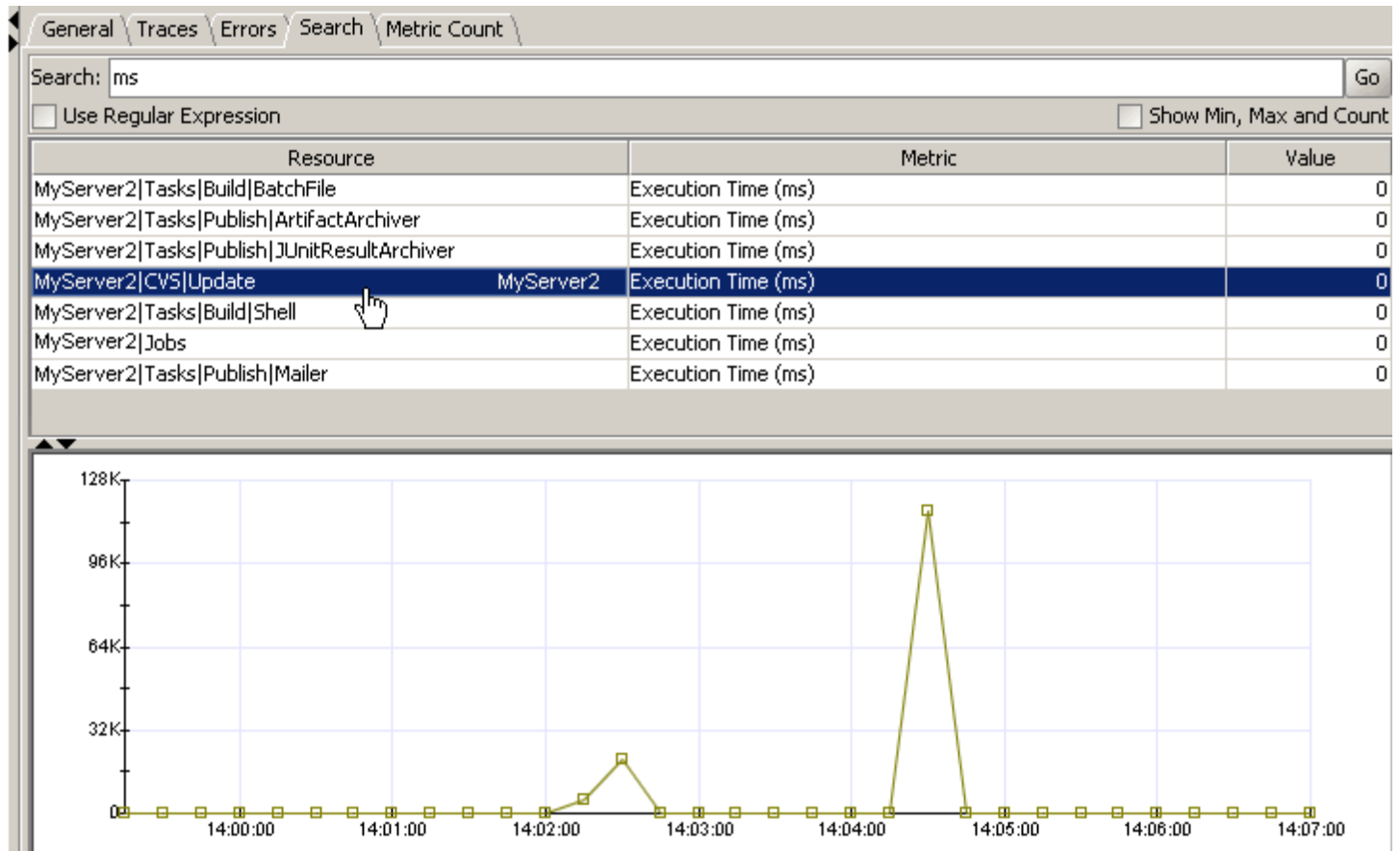
### **Otras fichas**

Además de las fichas Descripción general, existen otras fichas: Buscar, Seguimientos, Errores y Recuento de métricas.

## Ficha Buscar

La ficha Buscar está disponible cuando se selecciona un nodo del árbol centrado en agentes que contiene las métricas. Permite encontrar rápidamente las métricas.

La siguiente imagen muestra cómo aparece la ficha Buscar en el panel visor.



Información a tener en cuenta:

- El nodo seleccionado en el árbol centrado en agentes establece el ámbito de una búsqueda. Por ejemplo, si se selecciona Frontends en el árbol, la búsqueda únicamente buscará los recursos que se encuentra bajo ese nodo.
- Se puede introducir una cadena o una expresión regular en el campo de búsqueda.
- Si se introduce una expresión regular, se debe activar la casilla de verificación Utilizar expresión regular.

**Nota:** Las expresiones regulares no se pueden filtrar por agente, por lo que no es posible buscar el nombre de un agente, el nombre de host o el nombre de un proceso.

El panel derecho muestra los recursos con las métricas que coinciden con el argumento de búsqueda y el valor para cada una. Para mostrar los valores mínimos y máximos y el recuento de columnas, haga clic en Mostrar mín., máx. y recuento.

Si hace clic en una métrica de la lista, aparecerá una vista en la parte inferior del panel derecho.

Si hace clic en un nodo diferente que contiene métricas, el argumento de búsqueda utilizado en la búsqueda anterior permanece activo y se aplica al nuevo nodo seleccionado.

Para obtener información sobre cómo utilizar la búsqueda, consulte [Uso de la búsqueda](#).

## Ficha Seguimientos

La ficha Seguimientos, disponible cuando se selecciona un recurso o un componente del árbol centrado en agentes, es similar a Transaction Tracer (consulte [Uso de Transaction Tracer](#)). La ficha Seguimientos enumera los eventos de seguimiento de transacciones registrados para el recurso o componente seleccionado.

**Nota:** El intervalo de tiempo predeterminado para los seguimientos en el modo en directo es de 20 minutos. Los seguimientos de más de 20 minutos no se muestran en el modo en directo; caducan (no se muestran) cuando sobrepasan el umbral de los 20 minutos.

## Configuración de la unidad de duración

De forma predeterminada, la ficha Seguimientos muestra la duración de las transacciones y de los componentes de las transacciones en milisegundos (ms), es decir, milésimas de segundo.

Se puede cambiar esta unidad a:

- Segundos
- Microsegundos (µs)

Para cambiar la unidad de la columna Duración en la ficha Seguimientos:

1. Haga clic con el botón secundario del ratón en el encabezado de columna Duración (ms).
2. En el menú desplegable, seleccione una unidad:
  - Segundos
  - Milisegundos (valor predeterminado)
  - Microsegundos

La ficha Seguimientos muestra la nueva unidad en el encabezado de columna y representa la duración mediante la nueva unidad en todas las vistas de transacciones, incluido el Visor de seguimiento de transacciones (consulte [Uso del Visor de seguimiento de transacciones](#)).

## Ficha Errores

La ficha Errores, disponible cuando se selecciona un recurso o un componente del árbol centrado en agentes, muestra los errores y los detalles de los errores para el elemento seleccionado. La ficha Errores permite proporcionar soporte al personal para detectar y diagnosticar la causa de los errores graves a medida que se producen, determinar la frecuencia y la naturaleza de los errores que pueden impedir que los usuarios finales completen las transacciones web y proporcionar información específica acerca de la causa raíz a los desarrolladores.

**Nota:** Para ver la ficha Errores, ErrorDetector debe estar activo. Para obtener más información sobre la activación de ErrorDetector, consulte [Configuración de ErrorDetector](#).

La mitad superior de la ficha Errores muestra el tiempo, la descripción y el tipo de cada error. La mitad inferior de la ficha muestra la información detallada para cada componente implicado en el error seleccionado de la lista anterior.

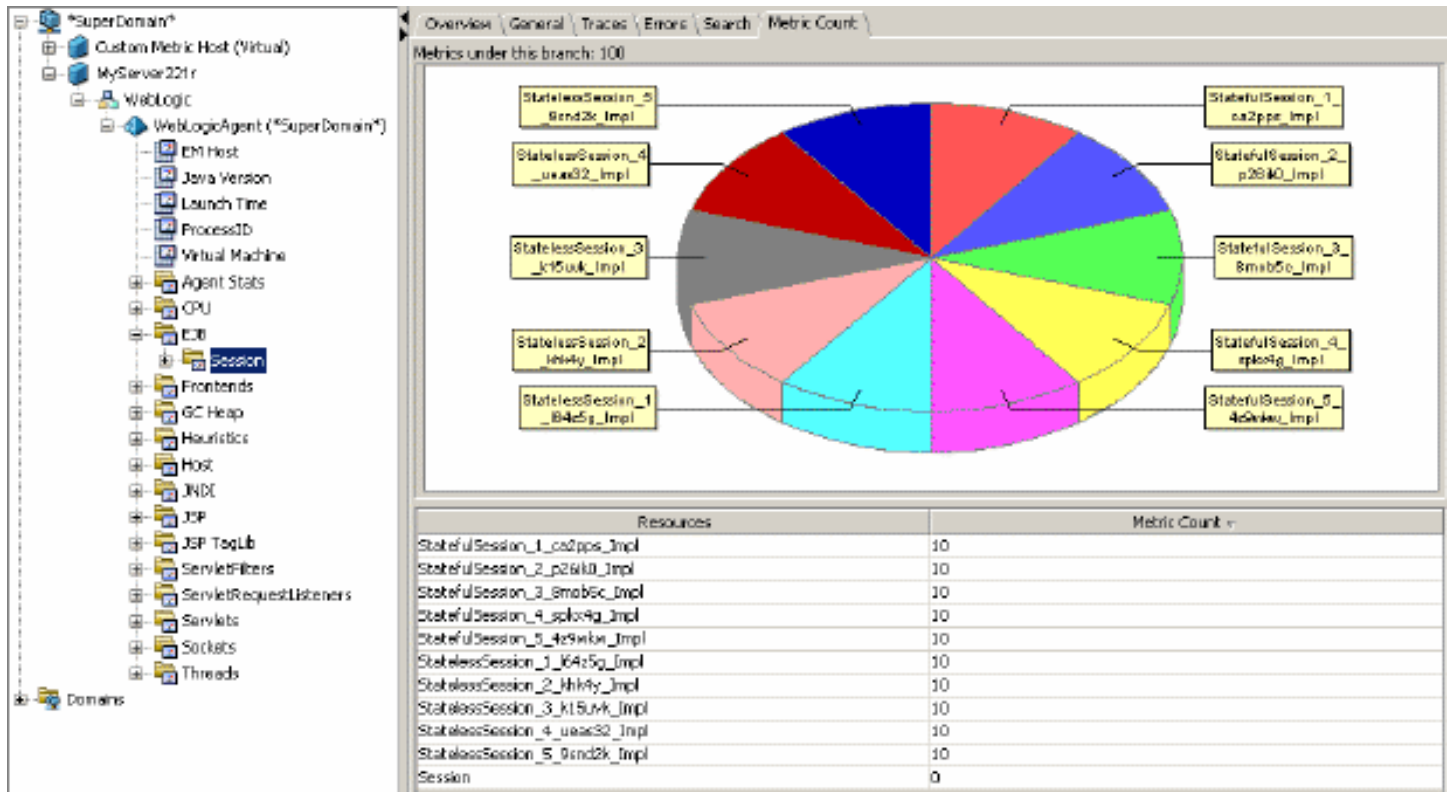
## Ficha Recuento de métricas

Muchos de los nodos del árbol centrado en agentes incluyen la ficha Recuento de métricas que muestra un gráfico circular de la distribución de las métricas para el nodo.

La imagen siguiente muestra el gráfico circular con una vista de tabla de los mismos datos bajo el gráfico.

El gráfico circular muestra un máximo de 50 segmentos. Cuando hay más de 50 recursos en el nodo seleccionado:

- El gráfico circular muestra los recursos con los 50 valores más altos.
- Además de los segmentos que representan los 50 valores más altos, se incluye un segmento adicional con la etiqueta Todas las otras métricas para mostrar la proporción de métricas con datos que no están incluidas en la lista de las 50 primeras.
- La barra de estado muestra el mensaje "Mostrando los 50 recursos principales". Los recursos restantes se agrupan en Todas las otras métricas".



Pase el ratón sobre un área del gráfico circular para mostrar la información sobre herramientas con el recuento y el porcentaje.

Las etiquetas largas se truncan, pero cuando se selecciona un segmento del gráfico circular, se muestra el nombre completo del recurso en la tabla que está ubicada debajo del gráfico.

La ficha Recuento de métricas muestra todos los recuentos de métricas para el período de intervalo de tiempo seleccionado, incluidas las métricas de agentes desconectados durante el mismo período.

Hay un intervalo de 30 minutos para que las métricas de agentes desconectados todavía se muestren en el recuento de métricas. Si el intervalo de tiempo seleccionado es inferior a 30 minutos, las métricas de los agentes desconectados desaparecen después de transcurrir 30 minutos. Si el intervalo de tiempo seleccionado es más alto, las métricas desconectadas estarán presentes durante el intervalo de tiempo completo.

### Vista de la ficha Recursos

La ficha Recursos muestra gráficas de las métricas de los recursos. La ficha Recursos está visible en el árbol Explorador de métrica cuando se selecciona el agente.

Nota:



- Aunque se muestran gráficas para todas las métricas de recursos en la vista de la ficha Recursos, las gráficas no muestran ningún dato cuando esas clases de métricas no están disponibles para el agente.
- El origen de la métrica que aparece en las gráficas Subprocesos en uso y Conexiones JDBC en uso varía de un agente a otro en función del tipo de agente (WebLogic, Tomcat, .NET u otro) y su asignación, especificada en el archivo ResourceMetricMap.properties.

En el árbol Explorador de métrica, aparecen bajo el nodo de agente, tal y como se muestra a continuación:

**Figure 14: nombre del agente**



### **Ficha Volcados de subprocesos**

Cada nodo del agente del árbol Explorador de métrica tiene una ficha Volcados de subprocesos. Esta ficha permite recopilar volcados de subprocesos de Java (volcados de subprocesos) y mostrar los datos de los volcados de subprocesos actuales e históricos. Un volcado de subprocesos proporciona información acerca de todos los subprocesos que están en ejecución en una máquina virtual Java en un momento dado. Un volcado de subprocesos proporciona el nombre y el ID de subproceso, el estado, y un seguimiento de la pila, que enumera todos los métodos invocados, para cada subproceso.

La ficha Volcados de subprocesos incluye las partes siguientes:

- El encabezado muestra la hora del volcado de los subprocesos.
- La barra de resumen del volcado de subprocesos muestra el número total de subprocesos y el número de subprocesos que están en espera, bloqueados y en ejecución.
- El panel de búsqueda permite buscar una cadena específica en toda la información del volcado de subprocesos. Los resultados se muestran en la tabla de información de los subprocesos.
- La lista desplegable de estados de los subprocesos filtra la tabla de información de los subprocesos por estado del subproceso. Al seleccionar un estado, se actualiza la tabla de información de los subprocesos.
- La tabla de información de los subprocesos muestra una lista de todos los subprocesos. Para cada subproceso, se proporciona el ID, el nombre y el estado del subproceso y el último método invocado por el subproceso inmediatamente antes del volcado de subprocesos.
- La tabla de seguimiento de pilas de subprocesos muestra todos los métodos en el orden en el que se han invocado.
- El gráfico circular Porcentaje de subprocesos por estado muestra los subprocesos en los estados siguientes: Interbloqueado, Bloqueado, En ejecución o En espera.
  - Pase el ratón sobre un área para mostrar la información sobre herramientas con el recuento y el porcentaje de subprocesos en cada estado.

La ficha Volcados de subprocesos se muestra en el árbol Explorador de métrica cuando se ha seleccionado un nodo de agente.

**Nota:** Si está realizando una evaluación de problemas para un agente, consulte la métrica <Nombre\_agente>|Threads|Deadlock Count en el árbol Explorador de métrica. Esta métrica indica si hay subprocesos interbloqueados que afectan al agente. Para activar la métrica Deadlock Count, se debe configurar Introscope. Para obtener más información, consulte [Agente de Java](#).

Se pueden llevar a cabo las acciones siguientes:

- Haga clic en el botón Recopilar nuevo para recopilar un volcado de subprocesos.
- Haga clic en el botón Guardar como texto para guardar el volcado de subprocesos actual en un archivo de texto.
- Haga clic en el botón Cargar anterior para cargar un único volcado de subprocesos recopilados previamente y para ver los datos asociados y la marca de tiempo.

No se muestra ningún dato del volcado de subprocesos hasta que se ha recopilado un volcado de subprocesos o hasta que se ha reiniciado una instancia de Enterprise Manager.

La ficha Volcados de subprocesos está disponible en el modo en directo; no se muestra ningún dato histórico de volcados de subprocesos en el modo histórico.

### **Uso de la información sobre herramientas para ver los nombres y los valores de las métricas en el visor de datos**

En un visor de datos, se puede desplazar el cursor sobre un punto de una gráfica para abrir la información sobre herramientas.

Para abrir la información sobre herramientas:

- Pase el ratón sobre cualquier elemento del árbol de métricas de Workstation o en un visor de datos, por ejemplo, sobre un punto en una gráfica.

Un punto de datos concreto de una gráfica muestra la información siguiente:

- El nombre de la métrica
- El valor exacto de la métrica
- Los valores mínimos y máximos de la métrica a lo largo del período representado por el punto de datos. En lugar de redondear los valores de miles y millones con una letra (por ejemplo, M para millones), la información sobre herramientas muestra los valores exactos.  
Esta particularidad se desarrolla en más profundidad en el tema [Cómo afecta el intervalo de tiempo a los puntos de datos](#) que se describe más adelante.
- El recuento de intervalos de 15 segundos representado por el punto de datos.
- La fecha y hora del punto de datos en la gráfica.

Pulsar F2 mientras está activa una información sobre herramientas, permite hacer clic en el texto con un hipervínculo. Al hacerlo, se abre una ventana de Investigator con el árbol expandido con la métrica que se muestra en la información sobre herramientas.

### **Cómo afecta el intervalo de tiempo a los puntos de datos**

Cada punto de datos de una gráfica representa una división igual del tiempo cubierto por la gráfica. Si se configura el intervalo de tiempo para el modo en directo (como en la imagen anterior), cada punto de datos representa un intervalo de 15 segundos.

Si el intervalo de tiempo se establece en otro valor, el intervalo representado por cada punto de datos será diferente. Por ejemplo, si el intervalo de tiempo se establece en 2 horas:

- Cada punto de datos representa 1 intervalo de 2 minutos u 8 intervalos de 15 segundos.
- Dado que hay 8 intervalos de 15 segundos en dos minutos, el recuento de cada punto de datos será 8.

La ficha Explorador de métrica muestra las métricas y otra información en un formato de árbol. Los nodos de alto nivel inmediatamente en los nodos de dominio representan a agentes instalados en hosts de servidores de aplicaciones individuales o el equivalente.

Para obtener más información sobre las métricas, consulte [Ficha Explorador de métrica](#).

## Uso de Transaction Tracer

Los usuarios de Workstation con los permisos apropiados pueden utilizar Transaction Tracer para realizar un seguimiento de la actividad de las transacciones dentro de una aplicación de producción. El seguimiento de las transacciones se realiza a medida que se llevan a cabo a través de una máquina virtual Java o de Common Language Runtime (CLR) en un entorno .NET.

Transaction Tracer permite capturar las transacciones que cumplen determinados criterios. A continuación, Transaction Tracer examina las llamadas que se realizan en todo el sistema para dicha transacción. La interfaz gráfica de usuario permite evaluar fácilmente los fallos de las aplicaciones y los problemas de rendimiento.

Existen dos métodos para recopilar seguimientos de transacciones:

- Utilizar Transaction Tracer.

Para ejecutar manualmente una sesión de seguimiento de transacciones, especifique los agentes de cuyas transacciones desea realizar un seguimiento, así como el período de captura de datos. Puede especificar opciones de filtro para limitar el seguimiento de las transacciones. Se pueden filtrar las transacciones por aquellas que superen el tiempo de ejecución del umbral, coincidan con los valores de los parámetros o contengan errores.

Una vez que se inicia una sesión de seguimiento de transacciones, las transacciones que coinciden con los criterios del filtro aparecen en la tabla de transacciones. Los eventos de transacción incluyen errores y seguimientos de transacciones.

- El agente recopila automáticamente un seguimiento de transacciones.

Cuando se activa la instrumentación inteligente, el agente recopila automáticamente el seguimiento de transacciones en determinadas situaciones.

Transaction Tracer puede realizar el seguimiento de transacciones sincrónicas que sobrepasan los límites de entornos de servidor de aplicaciones homogéneos y compatibles con esta función:

- WebLogic Server 8.0 y versiones posteriores
- WebSphere 6.x

En otro tipo de entornos, se puede realizar un seguimiento de las transacciones dentro de los límites de una máquina virtual (VM) única o CLR.

En la ficha Vista de seguimiento del Visor de seguimiento de transacciones, se pueden visualizar los resultados de las consultas de seguimiento de transacciones entre procesos.

DX APM guarda los datos de la sesión de seguimiento de transacciones en la base de datos de eventos de transacción durante un período de tiempo especificado. Los datos caducan de forma periódica para reducir la sobrecarga.

Se puede configurar el agente para que realice una captura de los datos de un seguimiento de transacciones en función de los valores del servlet o de las variables de ASP.NET. Las variables incluyen los encabezados de las solicitudes HTTP, los parámetros de solicitud, los atributos de sesión, el ID de sesión, el nombre de usuario, las direcciones URL y las cadenas de consulta de dirección URL. Además, de forma predeterminada los agentes llevan a cabo un muestreo de las transacciones.

### NOTE

El estado "apagado" de la métrica no afecta a los datos de seguimiento de las transacciones. Cuando se apaga un agente gestionado, este deja de informar sobre los datos de seguimiento de las transacciones. Un agente se

puede apagar durante una sesión de seguimiento de transacciones. En esta situación, el agente informa de los datos recopilados antes de la solicitud de apagado.

### **Muestreo del seguimiento de transacciones**

De forma predeterminada, los agentes realizan un muestreo del comportamiento de las transacciones mediante el seguimiento de cada dirección URL única normalizada en una aplicación en intervalos de una hora. Las muestras de los seguimientos se pueden visualizar y analizar a partir de un intervalo de tiempo histórico seleccionado:

- en Workstation
- en la ficha **Seguimientos** del Explorador de métrica

También se puede configurar un muestreo del seguimiento de transacciones incluso si no se ha configurado ningún grupo de direcciones URL. Especifique el número de transacciones de las que realizar un muestreo durante un intervalo de tiempo. El valor predeterminado es una transacción cada 2 minutos.

El muestreo del seguimiento de la transacción está activado de forma predeterminada. Se puede desactivar el comportamiento, cambiar el período de muestreo o anular el tiempo de muestreo aleatorio según sea necesario.

#### **NOTE**

**Más información:** [Configuración de las opciones de seguimiento de la transacción](#) (Agente de Java) u [Opciones de Transaction Tracer](#) (Agente de .NET).

### **Sobrecarga del seguimiento de transacciones**

Una sesión de seguimiento de transacciones afecta a la sobrecarga desde que se inicia la sesión hasta que se completan todas las transacciones en proceso al final de la sesión. Se puede especificar el umbral de ejecución en milisegundos, pero ello aumenta la carga en el sistema.

Estas funciones de Transaction Tracer reducen la probabilidad de que las sesiones de seguimiento causen una sobrecarga inaceptable:

- **Tiempo de espera de la sesión de seguimiento de transacciones:** El tiempo de espera de una sesión de seguimiento de transacciones se agota después de un período de tiempo definido por el usuario para que el usuario administrador no pueda dejar activado accidentalmente Transaction Tracer y ello afecte negativamente al rendimiento durante un período de tiempo prolongado. Al final del período de tiempo de espera, el agente detiene el seguimiento de las nuevas transacciones y finaliza el seguimiento de las transacciones en curso.
- **Lógica antidesbordamiento:** Para evitar una sobrecarga excesiva, la lógica antidesbordamiento del agente limita a 200 el número de transacciones de las que realizar un seguimiento a intervalos de 15 segundos. Si se excede este límite, el agente registra que se ha excedido el umbral de antidesbordamiento. El agente no informa sobre los datos del seguimiento de transacciones a Enterprise Manager hasta que ha caducado ese período de 15 segundos. Cuando finaliza el período de 15 segundos, la lógica antidesbordamiento reanuda la comunicación de los datos.

### **Seguimientos de transacciones recopilados automáticamente**

Cuando se activa la instrumentación inteligente, el agente recopila automáticamente el seguimiento de transacciones en los casos siguientes:

- Se produce un error.
- El análisis diferencial detecta una inestabilidad de la aplicación y no se excede el límite fijado para el seguimiento automático por intervalo.

**Nota:** El seguimiento automático de la transacción basado en análisis diferenciales requiere el agente 10.0 como mínimo.

- El rastreador `ComponentTimeAutoTraceTriggerTracer` se implementa y se supera el tiempo de respuesta de un componente
- Una API activa los seguimientos automáticos de la transacción en función de criterios personalizados. Para obtener más información, póngase en contacto con los [Servicios de implementación de DX APM](#).

Los seguimientos de sobrecarga baja sumamente optimizados recopilan seguimientos de transacciones automáticos. Los seguimientos automáticos adquieren una menor sobrecarga del rendimiento que las ejecuciones manuales, las muestras u otros seguimientos de la transacción. Estos otros tipos de seguimientos de la transacción utilizan el filtrado del agente, que aumenta la sobrecarga. Los seguimientos de transacciones automáticos no muestran todas las propiedades de detalles de los componentes que muestran los otros tipos de seguimientos de transacciones.

Los seguimientos automáticos de la transacción tienen estas características:

- Cada componente instrumentado por PBD tiene una métrica asociada en el árbol del Explorador de métrica. Los componentes de visibilidad exhaustiva carecen de una métrica asociada.
- Los [componentes de visibilidad exhaustiva](#) contienen solamente el nombre de la clase, el nombre del método y la duración. Para front-ends y back-ends (por ejemplo, servlets, servicios web, llamadas SQL), el nombre se formateará según la función de la configuración de PBD.
- En los detalles del componente, se muestran las propiedades siguientes:
  - El **Tipo de seguimiento es Normal**.
  - Si un error ha activado el seguimiento de las transacciones, el componente que ha producido la excepción incluye las propiedades del componente.
  - El primer componente del seguimiento de la transacción muestra la propiedad `Auto Trace Trigger Criteria`.
- Se admite el seguimiento de transacciones entre procesos.

## NOTE

### Más información:

- La [Configuración de la instrumentación inteligente](#) describe la configuración de las transacciones entre procesos en los seguimientos de transacciones automáticos.

Si no ve los seguimientos automáticos de la transacción, puede que sea por una de estas razones:

- La instrumentación inteligente no está activada.

## NOTE

La instrumentación inteligente solo está disponible para los Agentes de Java, pero no para los Agentes de .NET.

- Un agente en modo heredado está monitorizando la máquina virtual Java. El modo heredado no es compatible con las capacidades de la instrumentación inteligente.
- Se ha excedido el número de seguimientos de transacciones automáticos por intervalo (propiedad)

`agent.deep.automatic.trace.clamp`

del valor de la fijación. Consulte la métrica de compatibilidad `Deep Tracing|Auto Tracing: Clamped: Clamped Traces`.

## NOTE

### Más información:

- [Configuración de la instrumentación inteligente](#)
- [Propiedades de la instrumentación inteligente](#)

Cuando se ejecuta manualmente un seguimiento de transacciones y cualquier filtro manual coincide con un seguimiento automático, el agente recopila únicamente el seguimiento manual.

## **Seguimiento de transacciones automático cuando se supera el tiempo de respuesta del componente**

Se puede implementar un PBD para activar un seguimiento de la transacción automáticamente cuando se ha superado el tiempo de respuesta del componente. Cree una entrada PBD con un rastreador para recopilar este seguimiento automático. Por ejemplo, para recopilar un seguimiento cuando un tiempo de respuesta específico del servlet es superior a 10 segundos. Utilice la opción del rastreador `ComponentTimeAutoTraceTriggerTracer` para configurar su capacidad.

### **NOTE**

**Más información:** [Configuración de las opciones de seguimiento de la transacción](#)

Cuando `ComponentTimeAutoTraceTriggerTracer` activa un seguimiento de transacciones, el primer componente del seguimiento incluye la propiedad de detalles del componente `Auto Trace Trigger Criteria`. La propiedad muestra el **<valor> excedido para el valor de umbral del tiempo de respuesta <nombre del componente>**.

## **Componentes de visibilidad exhaustiva**

Cuando se activa la instrumentación inteligente, los agentes detectan y recopilan automáticamente información detallada sobre los componentes de las transacciones a nivel de método. Los agentes detectan e instrumentan automáticamente los componentes de visibilidad exhaustiva sin tener que utilizar las directivas de ProbeBuilder (PBD). El agente analiza los métodos para comprobar su complejidad y así poder determinar las llamadas y los componentes que se deben instrumentar y mostrar como componentes de visibilidad exhaustiva.

### **NOTE**

La instrumentación inteligente solo está disponible para los Agentes de Java, pero no para los Agentes de .NET.

A continuación, se detallan algunas características importantes sobre los componentes de visibilidad exhaustiva:

- Los componentes de visibilidad exhaustiva no incluyen vínculos a las métricas. No se muestra ningún dato de métrica en el árbol del Explorador de métrica.
- Contienen solamente el nombre de la clase, el nombre del método y la duración.
- En **Vista de seguimiento**, se muestran las [propiedades de los detalles del componente](#) siguientes:
  - La propiedad con el nombre `Is Unmonitored` indica un componente de visibilidad exhaustiva.
  - Nivel de instrumentación: Nivel de la instrumentación inteligente en el que se ha descubierto una transacción.
  - Nivel de calificación del método: El nivel de instrumentación inteligente que se corresponde con la puntuación que el algoritmo de calificación de DX APM asigna a un método de componente de visibilidad exhaustiva. DX APM puede mostrar métodos de componente de visibilidad exhaustiva con varias puntuaciones en el seguimiento de una transacción, un error o una detención. Por ejemplo, una transacción que se ha detectado mediante el nivel medio puede mostrar métodos con un nivel de puntuación medio y bajo. Utilice las propiedades `Instrumentation Level` (Nivel de instrumentación) y `Method Score Level` (Nivel de puntuación del método) para entender la profundidad de la visibilidad de la instrumentación inteligente de un seguimiento de transacciones. También se puede entender la profundidad de la visibilidad de los métodos sin realizar ningún seguimiento. Por ejemplo, se puede comparar el número de métodos que detecta la instrumentación inteligente en dos niveles distintos de instrumentación. Se puede anotar el nivel de la instrumentación inteligente en el que DX APM califica algunos métodos específicos. Se puede ajustar la solución de monitorización a la visibilidad y la sobrecarga del equilibrio de la visibilidad de monitorización deseadas.
- El icono de rayo que identifica los componentes de visibilidad exhaustiva no se muestra en Workstation.

En función de los requisitos y del entorno, se puede [configurar la profundidad de la instrumentación inteligente](#). Por ejemplo, se puede configurar si el agente detecta e instrumenta automáticamente una cantidad baja, media o alta de código de la aplicación.

## **Puntos de entrada**

La detección automática de puntos de entrada permite monitorizar y evaluar rápidamente las aplicaciones de Java sin configurar manualmente las directivas de ProbeBuilder.

Cuando se activa la detección del punto de entrada y la instrumentación inteligente, el agente monitoriza subprocesos que están implicados en transacciones de llamada de socket del cliente. La instrumentación inteligente y la detección de puntos de entrada están configuradas como activas de forma predeterminada. Los *puntos de entrada* son los puntos de inicio de la transacción. Un motor de reglas en el agente identifica a los candidatos del punto de entrada. El agente instrumenta y monitoriza al candidato de punto de entrada más antiguo en el subproceso de transacción. Cualquier punto de entrada que un agente detecta y persiste está activado para la monitorización por parte de todos los agentes que comparten el directorio de instalación. Sin embargo, el informe de las métricas de punto de entrada requiere las mismas clases de marco o código que existen en otras máquinas virtuales Java de servidor de aplicaciones.

A continuación, se muestran ejemplos de transacciones en las que la detección de puntos de entrada proporciona visibilidad automáticamente:

- Pilas de tecnología y marcos de trabajo que todavía no monitoriza la instrumentación de DX APM
- Llamadas de API personalizadas o de propiedad
- Subprocesos de fondo que consumen los recursos críticos y que pueden afectar al rendimiento general de la aplicación

#### NOTE

La detección del punto de entrada no admite el Protocolo de datagramas de usuario (UDP).

El agente guarda los puntos de entrada en `AutoPersist.pbd`, que se mantiene en el directorio `<Agent_Home>\core\config\hotdeploy`.

#### WARNING

El usuario del sistema que ejecuta el servidor de aplicaciones requiere los accesos de lectura y escritura para el directorio `/hotdeploy`. Estos permisos permiten al agente escribir datos en `AutoPersist.pbd`.

Los puntos de entrada son diferentes de los front-ends. El Agente de Java detecta automáticamente los puntos de entrada que se encuentran junto al inicio de una ruta de llamada de transacciones. Los front-ends se definen manualmente en los archivos PBD y pueden estar en cualquier lugar de la ruta de llamada de transacciones.

#### WARNING

No se deben realizar cambios manuales en `AutoPersist.pbd`. Sin embargo, se pueden copiar puntos de entrada detectados que se pueden utilizar en un PBD distinto.

Las métricas de puntos de entrada se muestran en el árbol centrado en agentes en el subnodo **Automatic Entry Points** en el nodo del agente.

#### NOTE

Asegúrese de que la propiedad `introscope.autoprobe.dynamicinstrument.enabled` en `IntroscopeAgent.profile` está configurada como `true`. Esta configuración permite al agente informar sobre métricas de punto de entrada sin tener que reiniciar la aplicación.

El agente informa sobre las cinco métricas de BlamePoint estándares para cada punto de entrada. Los puntos de entrada se muestran en los seguimientos de las transacciones. El formato de los nombres de entrada es el siguiente: `entry point <class name _ method name>`. El agente informa sobre las métricas de [compatibilidad de los puntos de entrada](#).

Se puede configurar la [recopilación de puntos de entrada](#). Por ejemplo, una propiedad de configuración limita el número de puntos de entrada que puede conservar `AutoPersist.pbd`.

#### NOTE

**Más información:** [Creación de archivos PBD para convertir puntos de entrada en front-ends](#)

### **Back-ends automáticos**

Cuando se activa la detección *automática del back-end*, el agente detecta y monitoriza automáticamente los back-ends de aplicaciones sin una configuración manual.



Un motor de detección en el agente identifica a los candidatos a back-end automáticos. Cualquier back-end automático que detecte un agente y persista está activado para la monitorización por parte de todos los agentes que compartan el directorio de instalación.

A continuación, se describen ejemplos de tipos de back-end que puede encontrar y monitorizar la detección automática de back-ends:

- Pilas de tecnología de back-end y marcos de trabajo que el agente todavía no monitoriza. Algunos ejemplos son los back-ends de NoSQL como MongoDB y Cassandra.
- Back-ends personalizados o de propiedad

El agente guarda los back-ends automáticos en `AutoPersist.pbd`, que se conserva en el directorio `<Agent_Home>\core\config\hotdeploy`.

### WARNING

- El usuario del sistema que ejecuta el servidor de aplicaciones requiere los accesos de lectura y escritura para el directorio `/hotdeploy`. Estos permisos permiten al agente escribir datos en `AutoPersist.pbd`.
- No se deben realizar cambios manuales en `AutoPersist.pbd`. Sin embargo, se pueden copiar los back-ends automáticos detectados y utilizarlos en un PBD distinto.

Se puede [configurar la detección automática de back-ends](#). Por ejemplo, una propiedad de configuración limita el número de back-ends automáticos que puede conservar `AutoPersist.pbd`.

En la **Vista de seguimiento**, los parámetros de `nombre de servidor remoto` y `puerto remoto` se muestran en los **detalles del componente**.

## Inicio, detención y reinicio de un seguimiento de transacciones

### Contenido

Para ejecutar una sesión de seguimiento de transacciones, especifique los agentes de cuyas transacciones desea realizar un seguimiento, así como el período de captura de los datos. Se pueden especificar opciones de filtro para limitar el seguimiento a las transacciones siguientes:

- Transacciones que excedan el tiempo de ejecución del umbral definido
- Transacciones que coincidan con los valores de los parámetros como el ID de usuario, la información de los encabezados de solicitud, etc.
- Transacciones con errores (si `ErrorDetector` está activado)

Cuando se inicia la sesión de seguimiento de transacciones, Introscope captura los datos del seguimiento de las transacciones que se hayan especificado en el perfil del agente, para cada transacción. Las transacciones que coinciden con los criterios de filtro aparecen en la ventana Visor de seguimiento de las transacciones y se guardan en la base de datos de eventos de transacción.

### Inicio de una sesión de seguimiento de transacciones

#### Para iniciar una sesión de seguimiento de transacciones:

1. Seleccione **Workstation > Nueva sesión de seguimiento de transacciones**.  
Se abre la ventana **Nueva sesión de seguimiento de transacciones**.
2. En la sección **Realizar el seguimiento de transacciones** de la ventana, especifique el tiempo mínimo que debe durar el seguimiento de las transacciones. En la lista desplegable, seleccione milisegundos o segundos.  
**Nota:** Las duraciones en fracciones de segundo pueden tener un impacto negativo en el rendimiento.
3. Para especificar un filtro de transacción, seleccione la casilla de verificación que aparece a la izquierda del menú desplegable atenuado denominado **ID de usuario** en la sección *Realizar seguimiento de las transacciones* y seleccione un tipo de la lista:



- ID de usuario: Introduzca un operador y un valor de parámetro.
  - ID de sesión: Introduzca un operador y un valor de parámetro.
  - Dirección URL o Consulta de dirección URL: Introduzca un operador y un valor de parámetro.
  - Encabezado de la solicitud: Introduzca un nombre de tipo de datos, una condición y un valor.
  - Parámetro de la solicitud: Introduzca un nombre de tipo de datos, un operador y un valor de parámetro.
  - Atributo de sesión: Introduzca un nombre de tipo de datos, un operador y un valor de parámetro.
- Nota:** Los datos únicamente están disponibles para utilizarlos en los filtros si se ha configurado el agente para que los capture.

Las condiciones de filtro son las siguientes:

- Es igual a: Se realiza un seguimiento de las transacciones cuyo valor de parámetro coincide con la cadena especificada.
- No es igual a: Se realiza un seguimiento de las transacciones cuyo valor de parámetro no coincide con la cadena especificada.

**Nota:** También se realiza un seguimiento de las transacciones que no incluyen el parámetro al que se aplica el filtro.

- Contiene: Se realiza un seguimiento de las transacciones cuyo valor de parámetro contiene la cadena especificada.
  - No contiene: Se realiza un seguimiento de las transacciones cuyo valor de parámetro no contiene la cadena especificada.
- Nota:** También se realiza un seguimiento de las transacciones que no incluyen el parámetro al que se aplica el filtro.
- Empieza por: Se realiza un seguimiento de las transacciones cuyo valor de parámetro empieza por la cadena especificada.
  - Termina por: Se realiza un seguimiento de las transacciones cuyo valor de parámetro termina por la cadena especificada.
  - Existe: Se realiza un seguimiento de las transacciones que incluyen el parámetro al que se aplica el filtro, sin tener en cuenta el valor del parámetro.
  - No existe: Se realiza un seguimiento de las transacciones que no incluyen el parámetro al que se aplica el filtro.

4. Introduzca la duración de la sesión de seguimiento en minutos.

5. En la sección Realizar el seguimiento de agentes, seleccione uno o más agentes para los que realizar el seguimiento de las transacciones:

- Para realizar el seguimiento de todos los agentes que admiten el seguimiento de transacciones, seleccione Realizar el seguimiento de todos los agentes compatibles. Esta opción permite realizar un seguimiento de todos los agentes compatibles que están conectados actualmente y de cualquier agente que se conecte durante la sesión de seguimiento.
- Para realizar el seguimiento de los agentes seleccionados, haga clic en Realizar el seguimiento de los agentes seleccionados y seleccione los agentes de la lista (CTRL + clic para seleccionar varios agentes).

6. Seleccione Aceptar para iniciar la sesión de seguimiento de las transacciones.

Los resultados del seguimiento de las transacciones aparecen en la ventana [Visor de seguimiento de las transacciones](#).

En el modo en directo, se muestran los eventos de seguimiento de transacciones de los últimos 20 minutos. No se muestran los eventos de seguimiento de transacciones anteriores a 20 minutos en el modo en directo. Se muestran un máximo de 500 eventos de seguimiento de transacciones.

### **Detención de una sesión de seguimiento de transacciones**

**Para detener una sesión de seguimiento de transacciones, realice una de las acciones siguientes:**

- Haga clic en Detener.
- Seleccione Seguimiento > Detener la sesión de seguimiento.

## Reinicio de una sesión de seguimiento de transacciones

Al reiniciar una sesión de seguimiento de transacciones, se restablece el tiempo de espera al período de tiempo definido por el usuario y se continúa realizando el seguimiento de las transacciones en los agentes de destino con los mismos criterios de umbral.

Se puede reiniciar una sesión de seguimiento de transacciones en los casos siguientes:

- Después de que se haya agotado el tiempo de espera de una sesión.
- Para reiniciar una sesión que se ha detenido.
- Para reiniciar una sesión en curso.

**Para reiniciar una sesión de seguimiento de transacciones, realice una de las acciones siguientes:**

- Haga clic en Reiniciar.
- Seleccione Seguimiento > Reiniciar la sesión de seguimiento.

## Uso del Visor de seguimiento de transacciones

El Visor de seguimiento de transacciones muestra la información de seguimiento para las transacciones que cumplen con los criterios especificados en la sesión de seguimiento.

La tabla del panel superior del Visor de seguimiento de transacciones enumera las transacciones de las que se ha realizado un seguimiento durante la sesión. Se pueden ordenar las filas por columna haciendo clic en el encabezado de columna. Las nuevas transacciones se insertan en la tabla en orden alfabético.

Esta tabla contiene las columnas de la tabla de transacciones:

Campo	Descripción
Type	El tipo de información de la fila de seguimiento: Seguimiento de transacciones (T) Error (E) Muestra (R) Una transacción con muestreo aleatorio. Detenida (S) Una transacción detenida. Los datos de los errores únicamente aparecen si ErrorDetector está activado. Asterisco Si aparece un asterisco después del símbolo de tipo, significa que se han truncado o <b>fijado</b> algunos de los componentes de la transacción. Solamente se pueden fijar los tipos de transacciones T y E. Los tipos que se enumeran a continuación se aplican a las transacciones disponibles en el modo en directo. Al consultar transacciones históricas, están disponibles otros tipos de transacción.
Dominio	El dominio al que está asignado el agente con seguimiento.
Host	El host en el que se está ejecutando el agente con seguimiento.
Process	El nombre del proceso del agente.
Agent	Nombre de agente
Timestamp	La hora de inicio (en el reloj del sistema del equipo del agente) de la invocación del componente raíz.
Duration	El tiempo de ejecución del reloj del componente raíz.

Descripción	La dirección URL que se ha invocado para iniciar la transacción o la ruta de Introscope al componente que ha iniciado la transacción.
ID de usuario	El ID del usuario que ha iniciado sesión y que está ejecutando la transacción (si está configurada y disponible).

La ventana Transaction Tracer incluye tres fichas:

- Vista de resumen
- Vista de seguimiento
- Vista de árbol

### **Vista de resumen**

La primera vez que selecciona una transacción de la tabla de transacciones, se abre la vista de resumen. Cuando se selecciona una transacción que ya se ha abierto con anterioridad, se abre en la vista seleccionada más recientemente.

La siguiente información aparece para la transacción seleccionada actualmente en cada ficha:

- El nombre completo del agente.
- La hora de inicio (en el reloj del sistema del equipo del agente) de la invocación del componente raíz.
- El tiempo de ejecución del componente raíz, en milisegundos.

La vista de resumen muestra las métricas para los componentes de la transacción seleccionada. Las métricas incluyen la ruta, el número de llamadas, la duración de la llamada en milisegundos y los tiempos de llamada mínimo, máximo y medio. Haga doble clic en una de las métricas que aparecen en la vista de tabla para abrir la métrica en el árbol de exploración.

En la parte inferior de la ventana de seguimiento, la barra de estado del seguimiento de las transacciones muestra los elementos siguientes:

- El número de transacciones que se han recopilado en la sesión.
- Los criterios de filtrado para la sesión de seguimiento de transacciones.
- El tiempo que resta antes de que caduque el tiempo de espera de la sesión.

### **NOTE**

Para los componentes de una transacción correlacionados, las fichas Vista de resumen y Vista de árbol solamente muestran el ámbito de la primera máquina virtual Java. La ficha Vista de seguimiento muestra todo el ámbito de los componentes de una transacción relacionados. Se debe tener en cuenta esta limitación cuando se cambie de la ficha Vista de seguimiento a las otras fichas de vista.

### **Vista de seguimiento**

La vista de seguimiento muestra una transacción seleccionada en una pila gráfica de los componentes que forman parte de la transacción. Cuando se selecciona uno de los componentes, se muestran los detalles de los componentes en el panel inferior del visor.

La vista de seguimiento muestra la información siguiente:

- Cada componente de la transacción como una barra
- El porcentaje del total del tiempo de ejecución de la transacción para cada componente.
- Relaciones de llamadas entre componentes  
Las barras de componentes se muestran de arriba abajo, en orden de llamada.
- Secuencia de las transacciones con el tiempo

La colocación de los componentes de izquierda a derecha indica la secuencia. En la parte superior de la instantánea de la transacción, aparece la hora en el formato de reloj relativo.

- Los componentes de visibilidad exhaustiva que Introscope detecta e instrumenta automáticamente mediante la instrumentación inteligente sin la necesidad de utilizar los archivos PBD.

#### NOTE

La instrumentación inteligente solo está disponible para los Agentes de Java, pero no para los Agentes de .NET.

- Errores en las transacciones (Detección y análisis de errores y detenciones). si se ha activado ErrorDetector. Los segmentos en rojo de la instantánea de la transacción representan los errores de las transacciones.

#### NOTE

El intervalo de tiempo predeterminado para los seguimientos en el modo en directo es de 20 minutos. Los eventos de seguimiento de transacciones anteriores a 20 minutos no se muestran en el modo en directo. Los seguimientos caducan (no se muestran) cuando sobrepasan el umbral de los 20 minutos.

En la vista de seguimiento se pueden realizar las acciones siguientes:

- Pase el puntero del ratón sobre un componente para abrir la información sobre herramientas.
- Haga clic con el botón secundario del ratón en un componente para abrir el Árbol de métrica y consultar las métricas del componente.
- Selecione un componente de la vista de seguimiento para abrir el panel Detalles del componente de la transacción.

### Detalles del componente de la transacción

Los detalles del componente de la vista de seguimiento muestran la información siguiente:

- Tipo:** El componente de alto nivel (por ejemplo, EJB, Servlet, JSP en Java y ASPX en .NET).
- Nombre:** El nombre del componente.
- Ruta:** El nombre de recurso completo del componente.
- Duración:** El tiempo de ejecución del componente seleccionado. La unidad predeterminada son los milisegundos.
- Marca de tiempo (relativa):** La hora de inicio, según el reloj del sistema del equipo host del agente, de la invocación del componente seleccionado.
- % del tiempo total de la transacción:** El porcentaje del total del tiempo de ejecución que utiliza el componente seleccionado.
- Propiedades:** Las propiedades opcionales notificadas por el componente (por ejemplo, la dirección URL, la consulta de la dirección URL o el SQL dinámico) o definidas para la recopilación en el perfil del agente (el ID de usuario, el encabezado de solicitud, `RequestParameter` o el atributo de sesión). Se puede seleccionar el texto de cualquier campo en los detalles de las propiedades y copiarlo mediante CTRL + C.

Propiedad	Descripción
ID de usuario (Servlet, JSP o ASPX)	El ID de usuario del usuario que invoca la solicitud de servlet HTTP.
Dirección URL (Servlet, JSP o ASPX)	La dirección URL que se transfiere al servlet o JSP, sin incluir la cadena de consulta (texto después del delimitador "?" en la dirección URL).
Consulta de dirección URL (Servlet, JSP o ASPX)	La parte de la dirección URL que especifica los parámetros de la consulta en la solicitud HTTP (texto después del delimitador "?" en la dirección URL).
ID de sesión (Servlet, JSP o ASPX)	El ID de la sesión HTTP asociada a la solicitud de servlet, si lo hay.

Dynamic SQL (SQL dinámico) (instrucciones JDBC o ADO.NET dinámicas cuando el Agente de SQL está instalado)	Las instrucciones SQL dinámicas generalizadas, tal y como deberían verse en su forma agregada en el Agente de SQL.
Callable SQL (SQL invocable) (instrucciones JDBC o ADO.NET invocables cuando el Agente de SQL está instalado)	Las instrucciones SQL invocables (con el delimitador "?" todavía presente).
Prepared SQL (SQL preparado) (instrucciones JDBC o ADO.NET preparadas cuando el Agente de SQL está instalado)	Las instrucciones SQL preparadas (con el delimitador "?" todavía presente).
Método (rastreadores culpables; todos exceptuando los servlets, los JSP y las instrucciones JDBC para Java, ASPX y ADO.NET para .NET)	El nombre del método del que se está realizando un seguimiento.
Is Unmonitored (No monitorizado)	La instrumentación inteligente detecta el nombre del componente con seguimiento. No se recopila ninguna métrica para este componente.
Trace Truncated (Seguimiento truncado)	El seguimiento de las transacciones se ha truncado en el último método del seguimiento. El truncamiento generalmente se debe a la emisión de llamadas recursivas profundas.
Auto Trace Trigger Criteria (Criterios de la activación automática del seguimiento)	<p>El desencadenador de Introscope para recopilar el seguimiento de transacciones automático. Por ejemplo, un error o un tiempo de respuesta excedido del componente cuando se implementa el rastreador <code>ComponentTimeAutoTraceTriggerTracer</code>. Cuando <code>ComponentTimeAutoTraceTriggerTracer</code> es la activación, <code>Auto Trace Trigger Criteria</code> muestra <code>Response time of &lt;nombre componente&gt; exceeds threshold &lt;valor&gt;</code>.</p> <p><code>Auto Trace Trigger Criteria</code> muestra los desencadenadores siguientes cuando los agentes recopilan transacciones entre procesos en los seguimientos de transacciones automáticos:</p> <ul style="list-style-type: none"> <li>• Cuando un agente ascendente activa una transacción entre procesos, <code>Auto Trace Trigger Criteria</code> muestra la activación de Introscope. Por ejemplo, <code>error</code> o <code>Response time of &lt;nombre componente&gt; exceeds threshold &lt;valor&gt;</code>.</li> <li>• Cuando un agente descendente activa una transacción entre procesos, <code>Auto Trace Trigger Criteria</code> muestra <code>Cross Process Trigger</code>.</li> </ul>
Nivel de instrumentación	El nivel de instrumentación inteligente en el que se ha detectado una transacción.
Method Level Score (Puntuación a nivel de método)	El nivel de instrumentación inteligente que se corresponde con la puntuación que el algoritmo de calificación de Introscope asigna a un método de componente de visibilidad exhaustiva. Introscope puede mostrar métodos de componente de visibilidad exhaustiva con varias puntuaciones en el seguimiento de una transacción, un error o una detención. Por ejemplo, una transacción que se ha detectado mediante el nivel medio puede mostrar métodos con una puntuación de nivel medio y nivel bajo.

### Información sobre herramientas en el Visor de seguimiento de transacciones

Se puede desplazar el cursor sobre cualquiera de los componentes individuales o capas de la representación gráfica de una transacción. La información sobre herramientas muestra los detalles de un componente.

La información sobre herramientas muestra la información siguiente:

- Ruta
- Duration
- Marca de tiempo (relativa)
- % del tiempo total de la transacción

### **Vista de secuencia**

La ficha Vista de secuencia muestra los componentes de una transacción en el orden de llamada.

### **ID de correlación en las transacciones entre procesos**

Introscope Workstation utiliza un identificador único, el ID de correlación, para vincular las transacciones de front-end y back-end de las que se realiza un seguimiento. El orden en el que los front-ends llaman a los back-ends en una transacción determina la secuencia de este ID.

Se puede utilizar este ID de correlación para reconocer y realizar un seguimiento de la ruta de los componentes vinculados en un seguimiento de transacciones. Esta información puede proporcionar detalles que ayuden a detectar qué llamadas pueden ser la fuente del bajo rendimiento o de la interrupción de transacciones.

#### **NOTE**

**Más información:** [Utilización del seguimiento de la transacción entre procesos para solucionar problemas](#)

### **Transacciones fijas**

Una propiedad de fijación impide que se consuman demasiados ciclos cuando se dan resultados inusuales para el seguimiento de transacciones. El valor de fijación predeterminado para los componentes del seguimiento de transacciones está establecido en 5000. Esta propiedad, `introscope.agent.transactiontrace.componentCountClamp`, se especifica en `IntroscopeAgent.Profile`. Se pueden configurar las propiedades del [Agente de Java](#) y del [Agente de .NET](#).

Los componentes del seguimiento de transacciones que excedan los límites de `introscope.agent.transactiontrace.componentCountClamp` se marcan con un asterisco.

Información a tener en cuenta:

- Se selecciona la primera fila de seguimientos.
- El símbolo de tipo se marca con un asterisco. El asterisco indica que algunos de los componentes de la transacción se han truncado o fijado.
- La información sobre herramientas indica la cantidad de componentes que se han truncado. En el ejemplo anterior, 15 de los componentes del seguimiento seleccionado han superado el número de la propiedad `introscope.agent.transactiontrace.componentCountClamp` especificada.
- Los componentes que se han truncado aparecen en la ficha Vista de resumen en la parte inferior del visor.
- Cada agente tiene un valor heurístico `IsClamped`, siendo 0 = no fijado y 1 = fijado.

### **Apariencia del archivo XML exportado con transacciones fijas**

Al fijar un componente del seguimiento, el archivo XML exportado está bien formado e incluye un parámetro similar al siguiente:

```
<Parameter Value="15" Name="Components Not Shown"/>
```

#### **Para ver la información sobre herramientas con más información acerca de un seguimiento:**

1. Seleccione uno de los seguimientos de la tabla.
2. Pase el cursor sobre el seguimiento seleccionado.  
La información sobre herramientas muestra el tipo de seguimiento y el número de componentes truncados o fijos.

**Para ordenar los seguimientos por tipo:**

- Haga clic en el encabezado de la columna Tipo en la tabla.

**Búsqueda de transacciones fijas**

Se pueden buscar transacciones fijas mediante la emisión de una consulta de eventos históricos. Utilice una cadena de ejemplo en la consulta, tal como se muestra a continuación:

```
componentsNotShown:[1 TO 9999]
```

El uso de una cadena garantiza que la consulta devuelva seguimientos que tenían transacciones fijas.

**NOTE**

Dado que la búsqueda del visor de eventos históricos utiliza la sintaxis de Lucene, estas reglas de sintaxis se aplican a las consultas de eventos históricos:

- La palabra "TO" en la cadena distingue mayúsculas de minúsculas.
- La sintaxis de búsqueda es lexicográfica, no numérica. Por este motivo, realizar consultas históricas utilizando `componentNotShown` como un filtro de consulta puede devolver resultados incorrectos.
- No se permiten las cadenas que empiezan por \* (asterisco) o ? (signo de interrogación).

**Visualización de errores con Transaction Tracer**

Cuando se activa [Detección y análisis de errores y detenciones](#), se puede utilizar Transaction Tracer para identificar y visualizar errores.

**Acerca de la vista de árbol en Transaction Tracer**

Los componentes de una transacción se pueden visualizar desde una vista jerárquica de información. Se puede navegar al componente e identificar los problemas de rendimiento.

Se pueden visualizar los componentes que se han instrumentado mediante PBD y los componentes de visibilidad exhaustiva. Introscope detecta e instrumenta automáticamente los componentes de visibilidad exhaustiva sin la necesidad de utilizar las PBD.

**NOTE**

La instrumentación inteligente solo está disponible para los Agentes de Java, pero no para los Agentes de .NET.

**Siga estos pasos:**

1. En WebView, haga clic en Herramientas, Transaction Tracer.
2. Seleccione el seguimiento de una transacción de la tabla.
3. Haga clic en la ficha Vista de árbol en el panel inferior.
4. Expanda el nodo en el árbol.  
Cada nodo del árbol muestra el componente, su nombre, su duración y el porcentaje de la duración total de la transacción. El color del icono de círculo indica la duración:
  - Rojo: La duración del componente es superior al 25 % de la duración total
  - Amarillo: La duración del componente está entre el 9 % y el 25 % de la duración total
  - Verde: La duración del componente es igual o inferior al 9 % de la duración total



En la gráfica, se pueden seguir los indicadores rojos circulares por el árbol. Consulte los métodos que están implicados en la mayoría del tiempo de la transacción. Por ejemplo, el método `AxisServer::invoke` ha estado un 95 % de los 37 ms que se ha tardado en ejecutar la transacción.

Realice el seguimiento de los componentes que no representan una cantidad de tiempo significativa para la transacción. Estos están codificados con un icono de color verde.

5. Seleccione un componente para ver la siguiente información en el área Detalles del componente:
  - Nombre, tipo y ruta del componente
  - Duración, marca de tiempo y tiempo total de la transacción

#### NOTE

Para los componentes de una transacción correlacionados, las fichas Vista de resumen y Vista de árbol solamente muestran el ámbito de la primera máquina virtual Java. La ficha Vista de seguimiento muestra todo el ámbito de los componentes de una transacción relacionados. Se debe tener en cuenta esta limitación cuando se cambie de la ficha Vista de seguimiento a las otras fichas de vista.

### Datos acumulados para varias transacciones

En Transaction Tracer, se pueden seleccionar varias transacciones para ver los datos acumulados para todos los componentes de los seguimientos.

#### Siga estos pasos:

1. Abra una lista de transacciones mediante la ejecución de un seguimiento de transacciones.
2. Seleccione varias transacciones mediante CTRL + clic o tecla MAYÚS + clic.
3. Abra la vista de árbol o de resumen para ver los datos acumulados de las transacciones.
  - Transaction Tracer muestra los datos acumulados en la tabla.  
Es posible que necesite desplazarse hacia abajo para ver todos los datos.
  - La vista de árbol muestra los datos acumulados.  
En la vista de árbol, Transaction Tracer agrega un nodo si las transacciones seleccionadas no comparten un nodo raíz común. El nodo se denomina Root.

#### NOTE

#### Más información:

- [Imprimir, guardar y exportar la información del seguimiento de transaccioneshttps://techdocs.broadcom.com](https://techdocs.broadcom.com)

### Consulta de eventos almacenados

Los resultados de una sesión de seguimiento de transacciones se almacenan automáticamente en la base de datos de eventos de transacción. Los eventos de transacción incluyen los seguimientos, los errores y las detenciones de transacciones (si se ha instalado Introscope ErrorDetector). La base de datos de eventos de transacción contiene los seguimientos de transacciones de los que Introscope ha realizado un muestreo automático. La base de datos también contiene los resultados de las sesiones de seguimiento de transacciones que ejecuta el usuario.

La base de datos de eventos de transacción admite los tipos de consulta siguientes:



- Eventos históricos (consulta básica): Consulte la sección Consulta de eventos históricos.
- Eventos similares (selección)
- Eventos correlacionados (selección)

**Nota:** Asegúrese de ejecutar algunas sesiones de seguimiento de transacciones antes de utilizar la consulta histórica para que haya datos para consultar.

### **Sintaxis de consulta**

Las siguientes secciones describen cómo utilizar la función de consulta histórica para consultar los errores almacenados. A continuación, se describen las características de la función de consulta:

- **Distingue mayúsculas de minúsculas:** Utilice esta opción para las cadenas o valores de consulta para las opciones de consulta.
- **Admite el carácter comodín asterisco (\*):** Introduzca un fragmento de un término de búsqueda seguido de un asterisco (No se puede empezar un término de búsqueda con el carácter de asterisco). Por ejemplo, para buscar errores asociados a un componente cuyo nombre incluye la cadena Compra, utilice la cadena de consulta Compra\*.
- **Admite los operadores booleanos:** Los términos de búsqueda pueden utilizar la lógica booleana como "Y", "O", "No" y agrupaciones de ().
- **Admite condiciones de exclusión:** Utilice "+JDBC -CICS" para buscar las transacciones con JDBC, pero no CICS.
- **Admite opciones de consulta:** Utilice las opciones que se describen en la sección Sintaxis y opciones de consulta para limitar la consulta de eventos de error que se han producido en un período de tiempo determinado o que se han asociado con usuarios concretos o elementos del entorno host (identificado por dominio, agente, host o proceso).

### **Consulta de eventos históricos**

Se pueden consultar los eventos de transacción históricos.

#### **Siga estos pasos:**

1. Seleccione Workstation > Consultar eventos históricos.  
Se abre el Visor de consultas históricas.  
El campo Consulta mostrará, en una lista desplegable, hasta doce búsquedas anteriores de esta sesión o sesiones anteriores emitidas por el mismo usuario de Workstation. Ello permite seleccionar una de las búsquedas guardadas en lugar de tener que volver a escribirla.  
**Sugerencia:** De forma predeterminada, el campo recuerda hasta 12 búsquedas; se puede designar un número diferente de búsquedas para el campo editando la propiedad `introscope.workstation.historical.query.history.limit` property en *IntroscopeWorkstation.properties*.
2. En el campo Consulta, introduzca una combinación de los elementos siguientes:
  - *Tipo* de opción de consulta: Para incluir todos los eventos de transacción que coincidan con el tipo especificado.
  - Cadena de consulta: Para buscar errores que contengan o coincidan con una cadena. Si no se introduce una cadena de consulta, se devuelven todos los eventos de error.
  - Opciones de consulta: Para limitar la búsqueda basada en los parámetros de evento, tal como se define en la sección Sintaxis y opciones de consulta.**Sugerencia:** A medida que se escribe en el campo Consulta, las búsquedas que se muestran en la lista desplegable se limitan a aquellas que coinciden con lo que se ha escrito.
3. Si lo desea, puede utilizar la opción Intervalo de tiempo para filtrar la consulta en función de un intervalo de tiempo. Para obtener más información sobre cómo utilizar la opción Intervalo de tiempo, consulte [Visualización de los datos históricos](#).  
Si no se selecciona un intervalo de tiempo, la consulta utiliza el valor predeterminado Todo y no aplica ningún filtro.
4. Haga clic en Ir.  
Las transacciones que coinciden con la consulta se muestran en la ventana Consulta histórica. El formato de la ventana es similar al del Visor de seguimiento de transacciones. Para obtener más información, consulte [Uso del Visor de seguimiento de transacciones](#).

**Nota:** Únicamente se muestran hasta 500 eventos. Si hay más de 500 eventos que coinciden con la consulta, se muestran los 500 más antiguos.

### Sintaxis y opciones de consulta

Las consultas utilizan la sintaxis de expresiones regulares de Lucene para buscar y sustituir las cadenas de texto.

**Nota:** Para obtener más información sobre la sintaxis de Lucene, consulte el sitio web de Lucene ([lucene.apache.org](http://lucene.apache.org)) y localice "query syntax".

Campo	Descripción	Ejemplo
agent	Limita la búsqueda a eventos notificados por un agente concreto.	agent:ControlledRangeAgent
domain	Limita la búsqueda a eventos relacionados con uno o más componentes de un determinado dominio.	domain:AcmeWest
fullAgent	Limita la búsqueda a eventos notificados por uno o varios agentes concretos, de acuerdo con lo que se especifica en la ruta completa: <i>dominio proceso host agente.</i>	fullAgent:AcmeWest  Custom Metric Host  ControlledRange Agent
host	Limita la búsqueda a eventos que han ocurrido en un host concreto.	host:Wmiddle01
process	Limita la búsqueda a errores relacionados con uno o más componentes de una aplicación específica.	process:Custom Metric Host
root	Limita la búsqueda a eventos asociados a uno o más componentes específicos, de acuerdo con lo que se especifica en la ruta de la métrica.	root:servlets accountServlet
type	Especifica el tipo de evento para incluir en los resultados de la consulta. <b>errorsnapshot:</b> Limita la búsqueda a eventos de error. <b>normal:</b> Devuelve los eventos de transacción que se han capturado en los seguimientos de transacciones iniciados por el usuario. <b>sampled:</b> Devuelve los eventos de transacción que se han capturado como resultado del muestreo de transacciones predeterminado de Introscope.	type:errorsnapshot type:normal type:sampled
url	Limita la búsqueda a eventos asociados con el prefijo de la ruta de la dirección URL de la transacción especificado. El prefijo de ruta es la parte de la dirección URL que sigue al nombre de host. En la siguiente dirección URL: <i>http://burger1.com/bWar/burgerServlet?ViewItem&amp;category=11776&amp;item=55562630&amp;rd=1</i> ... el prefijo de la ruta es: <i>/bWar/burgerServlet</i>	url:/bWar/burgerServlet

urlParams	Limita la búsqueda a eventos asociados con los parámetros de la dirección URL de la transacción especificados. Los parámetros de la dirección URL se emplazan detrás de un signo de interrogación (?) en la dirección URL. En esta dirección URL: http://ubuy.com/ws/shoppingServlet?category=734&item=3772&tc=photo la parte del parámetro de la dirección URL es: ?category=734&item=3772&tc=photo <b>Nota:</b> urlParams no puede comenzar por un carácter comodín.	urlParams:category=734*
user	Limita la búsqueda a eventos de transacciones que están asociadas con el nombre de usuario especificado.	user:jdoe
duration	Limita la búsqueda por duración del evento (valor predeterminado: milisegundos).	
componentsNotShown	Limita la búsqueda a eventos para los que no se muestra un determinado componente.	
durationencoded	(Ninguna definición disponible)	
time	Limita la búsqueda a eventos que ocurren antes o después de un tiempo específico.	time:[yyyyMMddHH] donde y = año, M = mes, d = día y H = hora del día
traceID	Limita la búsqueda a eventos con un ID de seguimiento concreto.	traceID:1340419311156\3957 <b>Nota:</b> Se requiere un carácter de barra invertida (\) antes de los segundos dos puntos (:).

La sintaxis de Lucene permite escapar los siguientes caracteres especiales con un carácter de barra invertida (\) en una consulta:

+ - & | ! ( ) { } [ ] ^ " ~ \* ? : \

Por ejemplo, para buscar (1 + 1) : 2, utilice la consulta:

\(1\+1\)\:2

**Nota:** Los caracteres de asterisco (\*) y signo de interrogación (?) no se admiten al principio de una consulta.

### Consulta de eventos similares

En Introscope, se pueden consultar eventos que sean similares al evento seleccionado. Por ejemplo, eventos similares podrían ser eventos que contengan todos los mismos componentes (Servlet > EJB > SQL) pero con tiempos de respuesta distintos. Introscope considera que dos eventos son similares cuando se solapan el 60 % de sus cadenas (nombres de los componentes, nombres de las tablas SQL y así sucesivamente).

**Nota:** Aunque se seleccione un evento de tipo transacción, en los resultados se pueden devolver tanto transacciones como errores (solamente se devolverán errores si ErrorDetector está instalado).

#### Siga estos pasos:

1. En una ventana de resultados de la consulta abierta, seleccione una fila de la tabla.
2. Seleccione Seguimiento > Eventos similares.

Introscope muestra los eventos similares en la ventana Consulta histórica.

### **Consulta de eventos correlacionados**

En Introscope, se pueden consultar eventos correlacionados: aquellos que forman parte de la misma transacción de mayor tamaño. Por ejemplo, un evento de tiempo de respuesta del explorador está correlacionado con un evento de transacción de servlet.

**Nota:** Aunque se seleccione un evento de tipo transacción, en los resultados se pueden devolver tanto transacciones como errores.

#### **Siga estos pasos:**

1. En una ventana de resultados de la consulta abierta, seleccione una fila de la tabla.
2. Seleccione Seguimiento > Eventos correlacionados.

Introscope incluye los eventos correlacionados en la ventana Consulta histórica.

### **Imprimir, guardar y exportar la información del seguimiento de transacciones**

Con la información del seguimiento de transacciones, se pueden realizar las actividades siguientes:

- Imprimir una ventana de seguimiento de transacciones.
- Guardar los datos del seguimiento de las transacciones como un archivo XML que se puede abrir más tarde en una ventana de seguimiento de transacciones.
- Exportar los datos del seguimiento de las transacciones como un archivo de texto para revisarlos en un editor de texto.

#### **Imprimir una ventana de seguimiento de transacciones.**

##### **Siga estos pasos:**

1. Seleccione la ventana Workstation > Imprimir.  
Se abre la ventana Page Setup (Configuración de la página). Los valores predeterminados de impresión son orientación vertical y tamaño carta.
2. Haga clic en Aceptar para continuar o cambie las opciones y, a continuación, haga clic en Aceptar.  
Aparecerá la ventana Imprimir.
3. Seleccione las opciones de impresión y, a continuación, haga clic en Aceptar.  
**Nota:** No se puede imprimir un intervalo de páginas; todo el contenido se imprime en una sola página.

El contenido de toda la ventana de seguimiento de transacciones se imprime a escala para que se ajuste todo el contenido a una página.

#### **Guardar los datos del seguimiento de transacciones**

Guarde los datos de un seguimiento de transacciones en un archivo XML. Más adelante, se podrá abrir el archivo en una ventana de seguimiento de transacciones para reproducir el seguimiento de las transacciones.

##### **Siga estos pasos:**

1. En el Visor de seguimiento de transacciones, seleccione los seguimientos de transacciones que desea guardar:
  - Pulse CTRL + clic para seleccionar varios seguimientos de transacciones.
  - Vaya a Editar > Seleccionar todo para seleccionar todos los seguimientos de transacciones en la ventana.
2. Haga clic en Guardar como.
3. Abra el archivo o seleccione una ubicación para guardar el archivo.
4. Si guarda el archivo, introduzca un nombre de archivo y haga clic en Guardar.

## **Abrir los datos XML de Transaction Tracer guardados**

Los datos del seguimiento de transacciones guardados se pueden abrir y visualizar en una nueva ventana de seguimiento de transacciones. Los archivos guardados se pueden compartir a través de correo electrónico o almacenarlos en una unidad de red compartida. El uso compartido de los archivos permite a los usuarios colaborar en el análisis de problemas.

Al abrir los datos guardados del seguimiento de las transacciones:

- No se puede reiniciar la sesión de seguimiento de transacciones que se está viendo.
- Los vínculos de los componentes del seguimiento de transacciones a sus rutas métricas no están disponibles si las rutas de las métricas no están activas en la instancia de Enterprise Manager a la que está conectado Workstation.

### **Para abrir los datos guardados del seguimiento de transacciones en un archivo XML:**

1. Seleccione Workstation > Consultar eventos históricos.
2. Seleccione Seguimiento > Abrir eventos guardados.
3. Seleccione el archivo XML en la ventana del explorador y haga clic en Abrir.  
Los datos del archivo XML aparecen en una nueva ventana de consulta histórica.

**Nota:** Cuando se visualizan eventos históricos guardados en un archivo XML, se muestran los eventos correlacionados, pero no se muestran como correlacionados. Para ver la correlación de eventos históricos de un seguimiento de transacciones, consulte un seguimiento activo (consulte [Consulta de eventos correlacionados](#)).

Ahora se pueden realizar las acciones siguientes:

- Exportar un seguimiento de transacciones como un archivo de texto.
- Seleccionar los seguimientos de transacciones dentro de los datos y guardarlos como un nuevo archivo XML.

## **Exportación de un seguimiento de transacciones a un archivo de texto**

### **Para exportar seguimientos de transacciones a un archivo de texto:**

1. En el Visor de seguimiento de transacciones, seleccione los seguimientos de transacciones que desea exportar:
  - Pulse CTRL + clic para seleccionar varios seguimientos de transacciones.
  - Vaya a Editar > Seleccionar todo para seleccionar todos los seguimientos de transacciones en la ventana.
2. Seleccione Seguimiento > Exportar.
3. Seleccione una ubicación para guardar el archivo y denomine el archivo (nombre predeterminado: *<tipo de componente raíz>\_<nombre del componente raíz>.txt.*) y haga clic en Aceptar.

### **Ejemplo de archivo XML de seguimiento de transacciones**

```
<?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>
 </CalledComponents>
 </CalledComponent>
 </CalledComponents>
 </CalledComponent>
 </TransactionTrace>
</TransactionTracerSession>
```

```

 </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>

```

## Monitorización con Workstation

Los usuarios avanzados de DX APM entienden que DX APM se utiliza mejor no solo al investigar problemas de las aplicaciones, sino también al monitorizar el rendimiento nominal de las aplicaciones. Una vez que se entiende cuál es el rendimiento nominal de la aplicación, los usuarios estarán mejor equipados para comprender los signos de problemas e interrupciones del rendimiento de la aplicación.

Esta sección contiene los temas siguientes:

- [Comprensión del rendimiento nominal](#)
- [Lectura y comprensión de las notificaciones](#)
- [Diagnóstico del problema con la ficha Explorador de métrica](#)

## Diagnóstico del problema con la ficha Explorador de métrica

Las herramientas de la ficha Explorador de métrica ayudan a detectar e investigar incidencias.

### Contenido

Las siguientes herramientas en la ficha **Explorador de métrica** ayudan a obtener más información sobre una incidencia:

- Métricas históricas
- Búsqueda
- Transaction Tracer

### Uso de métricas en directo e históricas

De forma predeterminada, las vistas son de métricas en directo con datos que se actualizan cada 15 segundos. Enterprise Manager guarda los datos que no se muestran en un gráfico en directo como datos históricos. Para diagnosticar un problema que puede haber empezado hace algunos minutos u horas, consulte los datos históricos.

## Visualización de los datos históricos en la ficha Explorador de métrica

Para ver los datos históricos, seleccione un intervalo de tiempo. El uso de un intervalo de tiempo puede ayudarle a identificar rápidamente la hora en que ocurrió un problema. Por ejemplo, se cree que el problema ocurrió en la última hora. Configure el intervalo de tiempo en una hora y mire los datos desde la hora actual hacia atrás. Si no ve el problema dentro de ese intervalo de horas, puede usar los controles para avanzar o retroceder. Mueva el intervalo hasta localizar la hora en que ocurrió el problema.

### Para ver los datos históricos:

1. Seleccione la métrica o el cuadro de mandos para el que desea ver los datos históricos.
2. Seleccione un intervalo de tiempo para la vista de historial en el menú desplegable **Intervalo de tiempo**. Los datos se muestran para ese intervalo. El intervalo utiliza la duración seleccionada y establece la hora de finalización en la hora actual.  
**Nota:** DX APM aplica el intervalo de tiempo que se selecciona para ver los datos históricos a otras métricas y cuadros de mandos en la misma ventana. Ese intervalo de tiempo se aplica a cualquier ventana nueva que se abra.
3. Para seleccionar una resolución para ajustar el nivel de detalle de la vista, aumente o disminuya el número de puntos de datos que aparecen.  
Cada intervalo de tiempo predefinido se asocia con una resolución predeterminada. Por lo general, no se deberá cambiar la resolución. Cambie la resolución para ver un mayor nivel de detalle o más granularidad de los datos.
4. Se puede ajustar un intervalo de tiempo después de seleccionar el intervalo. Use los controles para desplazarse en incrementos que se basan en el intervalo de tiempo que se ha seleccionado:
  - Arrastre el control deslizante en la barra de tiempo para cambiar el intervalo de tiempo.
  - Haga clic en las flechas para moverse hacia atrás y hacia adelante en el tiempo.  
Las flechas se mueven hacia atrás o hacia adelante en pequeños incrementos de tiempo. Las flechas dobles se mueven hacia atrás o hacia adelante en incrementos que se encuentran alrededor del intervalo de tiempo seleccionado.
  - Haga clic en el icono **Restablecer** para restablecer la hora de finalización del intervalo a la hora actual.

## Uso del zoom en los datos históricos en las gráficas

Cuando se consultan datos históricos en una gráfica, se puede aplicar el zoom para acercar los datos.

### Para ampliar los datos en una gráfica:

- Realice una de estas acciones:
  - Haga clic con el puntero del ratón en una posición de la gráfica y arrastre para especificar el intervalo de tiempo.
  - Haga clic con el botón derecho del ratón en la gráfica y haga clic en **Acercar** para ajustar los datos.

Los datos en el visor se actualizan en función de la nueva consulta y el intervalo de tiempo del visor muestra el nuevo intervalo.

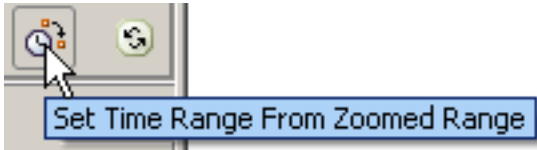
### Para alejar:

1. Haga clic con el botón secundario del ratón en la gráfica aumentada.
2. Haga clic en **Alejar** o en **Alejar del todo**.

El intervalo de tiempo global de la ventana y el control Intervalo de tiempo no cambian automáticamente cuando se acercan los datos. Por ejemplo, se acerca un período de 10 minutos en una gráfica con el intervalo de tiempo configurado en 1 hora. La gráfica muestra el período de 10 minutos, pero el control permanece en 1 hora. La barra de tiempo aún muestra el intervalo de horas.

### Para establecer el intervalo de tiempo global y el control Intervalo de tiempo para que coincidan con la vista ampliada:

- Haga clic en el botón **Establecer intervalo de tiempo desde el intervalo ampliado**:



### **Uso de la búsqueda**

La ficha Buscar (consulte [Ficha Buscar](#)) está activa en todos los nodos del árbol Explorador de métrica. En esta ficha se puede buscar cualquiera de las métricas en un nodo concreto.

#### **Para encontrar la ficha Buscar:**

1. Seleccione un nodo en el árbol Explorador de métrica.
2. Seleccione la ficha Buscar.

#### **Para utilizar la búsqueda de texto sin formato:**

1. Introduzca una cadena en el panel de búsqueda.
2. Pulse la tecla **Ir** o **Intro**.

Los resultados de la búsqueda se muestran en formato de tabla. Los resultados muestran todos los recursos cuyo nombre incluya la cadena de búsqueda.

#### **TIP**

Al seleccionar cualquiera de las métricas que se muestran en la tabla se mostrará un gráfico que muestra una vista en directo de la métrica.

#### **Para mostrar los resultados, incluidos los valores mínimo y máximo, así como el recuento de cada resultado:**

- Seleccione **Mostrar mín., máx. y recuento**.

#### **TIP**

Puede seleccionar **Mostrar mín., máx. y recuento** después de buscar y se actualizarán los resultados con las nuevas columnas.

### **Utilización de las expresiones regulares**

El panel de búsqueda acepta cualquier expresión regular utilizando el lenguaje de expresiones regulares Perl 5.

#### **TIP**

El lenguaje de expresiones regulares Perl 5 también permite definir agrupaciones de métrica.

#### **Para utilizar las expresiones regulares en la búsqueda:**

1. Seleccione **Utilizar expresiones regulares**.
2. Introduzca una expresión regular en el panel de búsqueda.
3. Pulse la tecla **Ir** o **Intro**.  
La ficha **Buscar** muestra los resultados.

### **Utilización del seguimiento de la transacción**

Transaction Tracer es una potente herramienta para realizar un seguimiento de la actividad de las transacciones a medida que fluyen a través de una aplicación. Se ejecutan seguimientos de transacciones para monitorizar las transacciones que se producen en una máquina virtual Java (JVM) en un entorno de Java o que se producen en Common Language Runtime (CLR) en un entorno .NET.

Consulte [Uso de Transaction Tracer](#).



## Lectura y comprensión de las notificaciones

### Notificaciones de alerta en los cuadros de mandos

El formato más obvio es una notificación visual en un cuadro de mandos de la Consola. La imagen siguiente muestra un cuadro de mandos con una única gráfica que se ha configurado con una línea amarilla que muestra el umbral de precaución establecido en 3000 ms y el umbral de peligro establecido en 4000 ms.

La gráfica muestra la información siguiente:

- El tiempo medio de respuesta ha excedido el umbral de precaución varias veces en los últimos varios minutos.
- El tiempo medio de respuesta ha excedido el umbral de peligro una vez, hace unos dos minutos.
- De acuerdo con la última medición, el rendimiento de la aplicación se encuentra en un estado de precaución.

Los indicadores bajo la gráfica muestran otra forma de indicar el estado de alerta. La forma en que aparecen en los cuadros de mandos dependerá de la configuración del usuario o administrador.

Cuando aparece un cuadro de mandos que muestra una condición de precaución o peligro, el indicador de alerta generalmente acumula las métricas desde varias fuentes. En este escenario, se debe averiguar qué métricas subyacentes están provocando la condición.

#### **Para cambiar la vista de alerta:**

- Muestre una alerta en el panel Vista previa de Investigator y seleccione Propiedades > Vista de alertas.

### Mensajes de alerta

Los mensajes de alerta se activan por una acción asociada a un estado de alerta. Los mensajes de alerta aparecen automáticamente. También se pueden visualizar mensajes de alerta mediante la selección de Workstation > Mostrar mensajes de alerta.

## Comprensión del rendimiento nominal

Comprender el rendimiento normal de la aplicación ayuda a estar familiarizado con el sistema y las herramientas y utilidades de DX APM. Este conocimiento proporciona un contexto más amplio para comprender los problemas inevitables. Cuando se produce algún error, se dispone entonces de los conocimientos para detectar el problema.

Existen tres nodos en el árbol del Explorador de métrica que son especialmente útiles, los cuales permiten monitorizar el rendimiento de la aplicación. Estos nodos (**GC Heap**, **Frontends** y **Backends**) pueden considerarse como las señales vitales de la aplicación.

### Monitorización del rendimiento con las métricas de la memoria dinámica de la recopilación de elementos no utilizados

La recopilación de elementos no utilizados es el proceso de liberar la memoria ocupada por objetos que ya no están en uso; una vez que se ha liberado la memoria, ya se puede utilizar para otros objetos. Las métricas del nodo **GC Heap** (memoria dinámica de la recopilación de elementos no utilizados) proporcionan una buena herramienta para monitorizar y comprender el rendimiento de la aplicación.

#### **Memoria dinámica de Recopilación de elementos no utilizados|Bytes en uso**

Memoria dinámica de Recopilación de elementos no utilizados|Bytes en uso informa sobre la cantidad de memoria que utilizan actualmente los objetos.

#### **Memoria dinámica de Recopilación de elementos no utilizados|Bytes totales**

La métrica GC Heap|Bytes Total informa sobre la cantidad total de memoria que está asignada a la máquina virtual Java.

La asignación de demasiada, o de demasiada poca, cantidad de memoria a la máquina virtual Java puede provocar problemas de rendimiento. Tenga en cuenta las directrices siguientes:

- Cuando se asigna muy poca memoria, el proceso de recopilación de elementos no utilizados se ejecuta con mayor frecuencia, lo que provoca problemas de degradación del rendimiento breves pero frecuentes.
- Cuando se asigna demasiada memoria, el proceso de recopilación de elementos no utilizados tarda relativamente mucho tiempo en ejecutarse y provoca una disminución del rendimiento durante ese tiempo.

Se pueden utilizar estas métricas para ayudar a determinar el tamaño correcto de la memoria dinámica.

Después de determinar el tamaño correcto, se pueden observar las métricas de la memoria dinámica de la recopilación de elementos no utilizados a lo largo del tiempo para comprender el estado del rendimiento nominal. La métrica **Bytes in Use** debe mostrar los aumentos y las disminuciones periódicos. Con el tiempo, las métricas forman un patrón recursivo y no muestran ninguna evidencia de una pérdida de memoria.

### **Monitorización del rendimiento con las métricas del monitor de la recopilación de elementos no utilizados**

La métrica del nodo GC Monitor (monitor de recopilación de elementos no utilizados) proporciona un conjunto de métricas sobre el funcionamiento interno de la máquina virtual Java, incluida la asignación de memoria y la tasa de crecimiento de la memoria dinámica. El monitor de recopilación de elementos no utilizados ayuda a asignar la memoria dinámica de la máquina virtual Java verificando que todos los recopiladores de elementos no utilizados y sus bloques de memoria están asignados correctamente. De esta forma, se pueden detectar los problemas de la recopilación de elementos no utilizados que afectan negativamente al rendimiento.

#### **Máquinas virtuales Java compatibles**

El monitor de recopilación de elementos no utilizados es compatible únicamente con las máquinas virtuales Java siguientes:

- Sun JVM, versión 1.5.0 o posterior, de 32 y 64 bits
- IBM, versión 1.5.0 o posterior, de 32 y 64 bits

**Se pueden utilizar las métricas del monitor de recopilación de elementos no utilizados para ajustar la asignación de memoria:**

1. En el árbol Explorador de métrica, vaya al nodo del agente en el host cuya actividad de recopilación de elementos no utilizados desea monitorizar. Expanda el nodo **GC Monitor**.
2. Monitorice las métricas y el uso del bloque de memoria de cada recopilador de elementos no utilizados.
3. En función de las métricas, vuelva a asignar el tamaño de los bloques de memoria para aumentar la eficacia de la recopilación de elementos no utilizados.

Si desea obtener más información sobre la reasignación del tamaño de los bloques de memoria, consulte la documentación adecuada relativa a su máquina virtual Java.

### **Monitorización del rendimiento con las métricas de front-ends**

Se puede utilizar el nodo **Frontends** de dos maneras distintas para monitorizar el rendimiento general de la aplicación: monitorizando las métricas estándares e identificando las direcciones URL principales.

#### **Monitorización de las métricas de front-ends estándares**

DX APM muestra las [cinco métricas de BlamePoint básicas](#) para cada front-end. Consulte estas métricas en el árbol del Explorador de métrica, en `Frontends|Apps|<Frontend_Name>`

#### **Rendimiento óptimo**

Una aplicación se está ejecutando correctamente cuando un gran volumen de solicitudes gestionadas (**respuestas por intervalo**) se corresponde con una latencia baja (**tiempo de respuesta medio** bajo). Una regla óptima es aproximadamente un segundo por transacción.

## Rendimiento problemático

Los métodos simultáneos son métodos que se inician durante un intervalo pero no finalizan en ese mismo intervalo. Puesto que los usuarios generalmente desean que los métodos se completen rápidamente, no se recomienda obtener un número excepcionalmente elevado de invocaciones simultáneas. Pueden observarse picos temporales en las invocaciones simultáneas, pero la métrica debe volver a un valor 0 cada vez. Una métrica que no vuelve a un valor de 0 puede indicar un cuello de botella de subprocesos, problemas con el número de conexiones de la base de datos o incidencias con algún otro recurso compartido.

### Reconocimiento de las transacciones con el peor rendimiento

Otra buena forma de monitorizar el rendimiento es observar qué transacciones tienen una ejecución lenta continuada. Se puede configurar un visor de datos para que muestre las transacciones más lentas mediante un gráfico de barras.

Una de las mejores maneras de mostrar las transacciones más lentas es mediante la configuración de grupos de direcciones URL como base para la agrupación de métricas.

### Monitorización del rendimiento con las métricas de back-ends

El nodo **Backends** del árbol del Explorador de métrica muestra las cinco métricas estándar para cada sistema de back-end conectado.

Existen dos métricas diferentes en el nodo **Backends** para ayudar a reconocer el rendimiento nominal.

### Frecuencia de las instrucciones SQL

Conocer qué instrucciones SQL se procesan con mayor frecuencia es una buena manera de familiarizarse con el rendimiento de la aplicación.

#### Para utilizar la frecuencia con la que se ejecutan las instrucciones SQL como medida de rendimiento:

1. En el nodo **Backends**, abra el nodo para la aplicación que desea monitorizar.
2. En la aplicación, abra el nodo para la aplicación que desea monitorizar.  
La ficha **Descripción general** muestra una lista de las consultas y otras instrucciones SQL que se ejecutan en el recurso de la base de datos.
3. En la sección **Consultas** del panel derecho, haga clic en el encabezado de columna **Respuestas** para ordenar la tabla por el número de respuestas.
4. Anote las consultas SQL que se envían con mayor frecuencia.

### Patrones de conexión de la base de datos

Conozca los patrones de conexión de la base de datos de la aplicación y cuando se interrumpe el patrón.

La forma en la que la aplicación establece y mantiene las conexiones de la base de datos depende de la plataforma.

## Uso de Workstation

La Consola de Workstation muestra información de la métrica en los cuadros de mandos. Los cuadros de mandos son ventanas preconfiguradas que presentan vistas gráficas del rendimiento actual o histórico y las métricas disponibles.

Cuando se abre la Consola, se muestran los datos de rendimiento y disponibilidad en directo. Se pueden ver los datos históricos seleccionando un intervalo de tiempo.

## Navegación por los cuadros de mandos de la Consola

### Contenido

Los cuadros de mandos de la Consola se pueden seleccionar de varias maneras diferentes:

- Lista desplegable de cuadros de mandos
- Botones Adelante y Atrás
- Lista de historiales
- Botón Página principal
- Hipervínculos

### **Lista desplegable de cuadros de mandos**

Los cuadros de mandos se pueden seleccionar de la lista desplegable que aparece en la parte superior de la página de la Consola. Se puede escribir parte o todo el nombre del cuadro de mandos para limitar las selecciones de la lista.

Una vez que se han visualizado los distintos cuadros de mandos, se puede navegar entre ellos mediante uno de los métodos siguientes:

- Flechas adelante y atrás
- La lista desplegable junto a las flechas adelante y atrás
- Si se ha definido un cuadro de mandos principal en las preferencias de usuario, se podrá abrir haciendo clic en el botón Página principal.

### **Navegación mediante hipervínculos**

Se pueden utilizar hipervínculos para navegar entre los cuadros de mandos de Introscope e Investigator:

- Hipervínculos automáticos: Introscope vincula automáticamente un visor de datos a la agrupación de métricas en la que se basa. El menú Vínculos para el visor contiene un vínculo a la definición de la agrupación de métricas subyacentes en el Editor del módulo de gestión. Del mismo modo, los cuadros de mandos que contienen los visores de datos que se basan en la misma agrupación de métricas se vinculan automáticamente, lo que permite poder desplazarse entre ellos mediante el menú Vínculos.
- Hipervínculos personalizados: Se pueden definir vínculos personalizados para los elementos de los cuadros de mandos para vincularlos a otros cuadros de mandos o páginas web. Si se dispone del permiso de edición para los cuadros de mandos, se pueden definir vínculos personalizados.

**Nota:** Algunos cuadros de mandos de la Consola listos para usar (por ejemplo, EM Capacity [Capacidad de EM]) no contienen automáticamente los vínculos a los datos subyacentes. Edite estos cuadros de mandos predeterminados o crear nuevos cuadros de mandos con vínculos.

### **Para ver una lista de los vínculos de cuadro de mandos disponibles:**

1. Haga clic con el botón secundario del ratón en un objeto del cuadro de mandos.
2. Seleccione Propiedades > Vínculos.

Si no hay ningún vínculo disponible para un objeto, el menú Vínculos aparece desactivado.

### **Para seguir los vínculos de cuadro de mandos:**

1. Pase el cursor sobre un objeto del cuadro de mandos que tenga un hipervínculo.  
El puntero cambia a una mano.
2. Haga doble clic en el objeto para seguir el vínculo a su destino predeterminado.

### **Creación de cuadros de mandos favoritos**

Para simplificar el acceso a los cuadros de mandos que se utilizan con frecuencia, se pueden agregar al menú Favoritos de la Consola.

### **Para agregar un cuadro de mandos a Favoritos:**

1. Vaya al cuadro de mandos.

2. Seleccione Favoritos > Agregar a Favoritos.

**Nota:** Los vínculos favoritos no se conservan cuando se renombra o suprime un cuadro de mandos favorito. Actualice el vínculo o suprima el vínculo anterior y cree uno nuevo.

#### **Para suprimir un cuadro de mandos de Favoritos:**

1. En la Consola, seleccione Favoritos > Organizar Favoritos.
2. Seleccione un cuadro de mandos.
3. Seleccione Suprimir.

#### **Para editar la lista de favoritos:**

1. En la Consola, seleccione Favoritos > Organizar Favoritos.
2. Seleccione un cuadro de mandos.
3. Seleccione Editar.

#### **Inicio de Investigator desde la Consola**

Si se están visualizando los datos en directo en la Consola y se inicia Investigator de Workstation desde esta Consola, también se pueden visualizar los datos en directo en Investigator. Sin embargo, en Investigator, el valor predeterminado para el intervalo de tiempo es de 8 minutos y la resolución es de 15 segundos. No se pueden especificar un intervalo de tiempo y una resolución personalizados para el modo en directo en Investigator.

Si se están visualizando los datos históricos en la Consola y se inicia Investigator de Workstation desde esta Consola, también se pueden visualizar los datos históricos en Investigator para el mismo intervalo de tiempo y resolución que se han seleccionado para los datos históricos de la Consola.

#### **Inicio de la Consola desde Investigator**

Si se están visualizando los datos en directo en Investigator y se inicia la Consola de Workstation desde Investigator, también se pueden visualizar los datos en directo en la Consola. Sin embargo, en la Consola, el valor predeterminado para el intervalo de tiempo es de 8 minutos y la resolución es de 15 segundos. Se pueden especificar un intervalo de tiempo y una resolución personalizados para el modo en directo en la Consola.

Si se están visualizando los datos históricos en Investigator y se inicia la Consola de Workstation desde Investigator, también se pueden visualizar los datos históricos en la Consola para el mismo intervalo de tiempo y resolución que se han seleccionado para los datos históricos de Investigator.

#### **Más información en los cuadros de mandos**

Si desea obtener más información acerca de los datos que se presentan en los cuadros de mandos, se pueden utilizar métodos abreviados para obtener más información.

#### **Siga estos pasos:**

1. Haga clic con el botón secundario del ratón en una gráfica o alerta, seleccione Vínculos y vaya a la alerta correspondiente en el Módulo de gestión o en otro cuadro de mandos que esté asociado con la gráfica o alerta.
2. Haga doble clic en una métrica del gráfico que muestra los datos de las X métricas principales (por ejemplo, las 10 o 25 más lentas) para ver sus detalles en Investigator.

#### **Filtrado por agente con la lente de la Consola**

Utilice la lente de la Consola para filtrar los datos de las métricas para los agentes que informan de datos. En un cuadro de mandos que muestra datos de más de un agente, se puede utilizar la lente de la Consola para ver los datos de solamente los agentes seleccionados.

Al aplicar la lente de la Consola, el filtro se sigue aplicando hasta que se cierra la ventana de la Consola, se cierra la sesión de Workstation o se utiliza el comando Desactivar lente.

## Aplicación de la lente de la Consola

### Para aplicar la lente de la Consola:

1. Seleccione el botón Lente (o seleccione Cuadro de mandos, Lente).  
Si la Consola se encuentra en el modo en directo, el cuadro de diálogo enumera los agentes que están conectados actualmente. Si se está visualizando un intervalo de tiempo de datos históricos, el cuadro de diálogo enumera los agentes conectados para el intervalo histórico seleccionado.
2. En el cuadro de diálogo Seleccionar agentes, seleccione uno o varios agentes (seleccione los agentes y arrástrelos, o bien haga CTRL + clic) en los que desea aplicar el filtro.  
**Nota:** Puede empezar a escribir un nombre de agente, nombre de host o nombre de proceso en el campo de búsqueda. A medida que escriba, se filtrará la lista de agentes para que aparezcan únicamente resultados que coincidan con lo que está escribiendo.
3. Seleccione Aplicar o pulse la tecla Intro.  
El cuadro de mandos se actualiza para mostrar solamente los datos para el agente o agentes seleccionados. La flecha de la lente cambia de azul claro a negro cuando se aplica una lente.

### Widgets no compatibles

Algunos widgets del cuadro de mandos no son compatibles con la función de lente:

- Gráficas con calculadoras
- Gráficas que se basan en un agente virtual con una alerta simple Esto incluye la gráfica Top 10 Connected Agents (Los 10 agentes conectados principales) del cuadro de mandos Descripción general.

**Nota:** Al editar un cuadro de mandos para agregar una nueva alerta simple, tenga en cuenta que cuando se aplica una lente al cuadro de mandos, puede transcurrir algún tiempo antes de que la nueva alerta muestre datos de estado.

## Desactivación de la lente de la Consola

### Para desactivar la lente de la Consola:

1. Seleccione Lente.
2. Desactive la lente haciendo clic en el botón Desactivar en el cuadro de diálogo Aplicar lente de la consola.

## Lente de la Consola y vistas de ficha en los cuadros de mandos

El efecto que tiene una lente de la Consola en una vista de Investigator en un cuadro de mandos depende del tipo de elemento del árbol al que está asociada la vista.

Si el elemento de Investigator asociado a la vista es:	y...	entonces
un dominio	solamente hay un agente seleccionado en la lente...	...la asociación del elemento cambia a la selección de un solo agente. Si la vista no admite la selección del agente, aparecerá un mensaje de error.
un agente	solamente hay un agente seleccionado en la lente...	...la asociación del elemento cambia a la selección de un solo agente.
una métrica	solamente hay un agente seleccionado en la lente...	...la misma métrica en el agente seleccionado se convierte en la selección actual. Si no existe esa métrica, aparece un mensaje de error.
una ruta de métrica	solamente hay un agente seleccionado en la lente...	...la misma ruta de métrica en el agente seleccionado se convierte en la selección actual. Si no existe esa ruta, aparecerá un mensaje de error.

otro tipo de elemento		...aparecerá un mensaje de error.
-----------------------	--	-----------------------------------

Si se selecciona más de un agente, aparecerá un mensaje de error.

Si el agente con lente es un agente virtual, la vista muestra datos para ese agente si admite ese tipo de selección. Se puede determinar qué vistas se admiten para un tipo de elemento determinado seleccionando un elemento del árbol y observando las fichas de vista que están disponibles.

Un agente virtual es un grupo de agentes físicos que se configura para funcionar como un solo agente, lo que permite ver una vista acumulada de las métricas de los distintos agentes.

### **Manipulación del contenido de los visores de datos**

Los visores de datos del panel visor de Investigator o de un cuadro de mandos muestran los datos de una aplicación instrumentada de forma visual. Los datos se muestran en un visor de datos que se basa en el tipo de datos, por ejemplo, las métricas aparecen como gráficas y las alertas aparecen como indicadores coloreados. Los Visores de datos pueden mostrar datos de una métrica, de un recurso o de un elemento, como una alerta.

En los visores de datos, se pueden realizar las acciones siguientes:

- Mostrar los valores mínimos y máximos de las métricas en una gráfica.
- Mostrar u ocultar los datos de las métricas en una gráfica.
- Cambiar la escala de las gráficas.
- Mover las métricas hacia el frente o hacia el fondo en las gráficas.
- Exportar los datos.

### **Visualización de los valores máximos y mínimos de las métricas en una gráfica**

Se puede configurar una gráfica para que se muestren los valores mínimos y máximos.

#### **Para mostrar los valores mínimos y máximos de las métricas y las agrupaciones de métricas de una gráfica:**

1. Seleccione la gráfica en la Consola.
2. Muestre los valores mínimos y máximos de dos posibles maneras:
  - Haga clic con el botón secundario del ratón en el visor de datos y seleccione Mostrar mínimo y máximo.
  - Seleccione el menú Propiedades y, a continuación, seleccione Mostrar mínimo y máximo.

**Nota:** Este cambio permanece activo solamente mientras se visualiza el cuadro de mandos actual. Si se abre una nueva consola o se cambia a un cuadro de mandos distinto, se establece de nuevo la configuración predeterminada, la cual no muestra los valores mínimos y máximos de las métricas. Para mostrar los valores mínimos y máximos de las métricas de forma predeterminada en una gráfica, active esta opción mientras edita un cuadro de mandos con el Editor de cuadro de mandos.

### **Cómo mostrar u ocultar datos de las métricas en una gráfica**

Si se están visualizando los datos de varias métricas en una gráfica, se pueden mostrar u ocultar los datos de una métrica determinada.

#### **Para mostrar u ocultar una métrica en una gráfica:**

1. Muestre una gráfica en el cuadro de mandos de la Consola.
2. Se puede realizar lo siguiente:
  - Mostrar la métrica seleccionando la casilla de verificación.
  - Ocultar la métrica anulando la selección de la casilla de verificación.

**Nota:** Las opciones para mostrar u ocultar una métrica no están disponibles cuando se visualizan gráficas o gráficos de barras que muestran datos ordenados o filtrados.

## **Cambio de la escala de los gráficos**

Se puede cambiar la escala de los gráficos mientras se visualizan los datos en directo en Workstation para proporcionar una vista más legible. Cambie la escala de un gráfico mediante la configuración de un valor mínimo y un valor máximo para el eje de datos del gráfico.

La función de escala para gráficos solamente está disponible para gráficos en el modo en directo. No está disponible para cualquier otro tipo de visor como un gráfico de barras, un gráfico "diez principales" o un visor de cadenas.

**Nota:** Los cambios realizados en un gráfico son temporales; la configuración no se guarda con el cuadro de mandos. Cuando se selecciona un cuadro de mandos nuevo o se cierra la ventana de la Consola, Introscope descarta los valores de configuración y vuelve a utilizar las opciones de escala que se aplicaron al crear el cuadro de mandos.

### **Para ver la escala de un gráfico:**

- Haga clic en un gráfico para seleccionarlo y, a continuación, realice una de las acciones siguientes:
- Seleccione Visor > Opciones de escala.
- Haga clic con el botón secundario del ratón en el gráfico y seleccione Opciones de escala en el menú contextual. Se abre el cuadro de diálogo Opciones de datos.

Al establecer los valores mínimo y máximo predeterminados para la escala automática, se proporciona una vista de los gráficos en el modo en directo más legible.

### **Para cambiar la escala mediante los valores mínimo y máximo:**

1. Haga clic en un gráfico para seleccionarlo y, a continuación, realice una de las acciones siguientes:
  - Seleccione Visor > Opciones de escala.
  - Haga clic con el botón secundario del ratón en el gráfico y seleccione Opciones de escala en el menú contextual.
2. Introduzca los valores mínimo y máximo para el eje de datos de la gráfica.
3. Haga clic en Aceptar.  
 Por ejemplo, si los valores de los datos del gráfico se encuentran principalmente entre 350 y 550, pero el eje de valores del gráfico muestra 0-1000, puede resultar útil establecer el valor mínimo de la escala en 300 y el valor máximo en 600 para obtener una mejor visión de los datos relevantes.

### **Para forzar los valores mínimo y máximo:**

1. Haga clic en un gráfico para seleccionarlo.
2. Seleccione Visor > Opciones de escala.
3. Seleccione Anclar en ambos lados (mínimo y máximo) del cuadro de diálogo e introduzca un valor para los puntos mínimo y máximo del acceso de datos.
4. Haga clic en Aceptar.

Configurar un valor mínimo y otro máximo para un gráfico que muestra datos en directo es arriesgado; sin embargo, si existe la posibilidad, los datos probablemente excedan los valores establecidos.

Para evitar este problema, utilice la opción Aplicar escala automáticamente para establecer que la gráfica cambie la escala de forma automática en función de los datos que muestre.

### **Para cambiar la escala automáticamente:**

1. Haga clic en un gráfico para seleccionarlo.
2. Seleccione Visor > Opciones de escala.
3. Seleccione Aplicar escala automáticamente tanto en el lado del valor mínimo como en el lado del valor máximo en el cuadro de diálogo.
4. Haga clic en Aceptar.

El eje de datos del gráfico resultante se restablece en función de los datos que aparecen en el gráfico. Ello, a menudo, da lugar a picos y valles más definidos en la gráfica.



También se pueden establecer las opciones de escala para la expansión automática. Esta opción utiliza el valor 0 para la parte inferior del eje de datos y expande y cambia la escala del eje de datos automáticamente para mostrar todos los datos para el intervalo de tiempo.

#### **Para cambiar la escala mediante la expansión automática:**

1. Haga clic en un gráfico para seleccionarlo.
2. Seleccione Visor > Opciones de escala.
3. Seleccione Expandir automáticamente tanto en el lado del valor mínimo como en el lado del valor máximo en el cuadro de diálogo.
4. Haga clic en Aceptar.

#### **Desplazamiento de las métricas hacia el frente o hacia el fondo en la gráfica**

Cuando una gráfica contiene varias métricas, es posible que los puntos de datos se superpongan entre sí. Se pueden utilizar las opciones Traer al frente o Enviar atrás para elegir qué métrica debe aparecer al inicio de la lista de métricas.

**Nota:** Las opciones Traer al frente y Enviar atrás no están disponibles cuando se visualizan gráficas que muestran datos ordenados o filtrados.

#### **Para cambiar el orden de solapamiento de las métricas en una gráfica:**

1. Abra la Consola y muestre una gráfica en un cuadro de mandos.
2. Haga clic con el botón secundario del ratón en la etiqueta de la métrica que desea cambiar y seleccione una opción del menú:
  - Traer al frente: La métrica seleccionada se mueve al inicio de las métricas que aparecen en pantalla.
  - Enviar atrás: La métrica seleccionada se mueve al final de las métricas que aparecen en pantalla.
 La métrica se mueve a la posición elegida.

#### **Copia de un visor de datos en el Portapapeles**

Se puede copiar una instantánea de los datos de un visor de datos en el Portapapeles como una imagen de mapa de bits. A continuación, se puede pegar la imagen en un correo electrónico u otro documento o en cualquier aplicación que acepte imágenes de mapa de bits. Ello resulta útil si, por ejemplo, se desea mostrar los datos de un visor de datos a un compañero o usarlos en una presentación.

#### **Para copiar un visor de datos en el Portapapeles:**

1. Abra la Consola y seleccione un visor de datos.
  2. Seleccione Visor > Copiar al Portapapeles como imagen.
- Nota:** No se pueden copiar varios visores de datos.

#### **Exportación de datos desde los visores de datos**

Se puede crear una instantánea de los datos actuales en un visor de datos y exportarla a un archivo de valores separados por comas (.csv). Se pueden exportar datos desde todos los tipos de visor de datos, exceptuando las alertas.

#### **Para exportar datos desde un visor de datos:**

1. En la Consola, seleccione un visor de datos.
2. Seleccione Visor > Exportar datos.
3. En el cuadro de diálogo Guardar, seleccione una ubicación para guardar el archivo .csv y seleccione Guardar.

### **Datos históricos y en directo en la Consola de Workstation**

Se pueden ver datos en directo en la Consola o se puede seleccionar un intervalo de tiempo para consultar datos históricos. La vista predeterminada de los datos es el modo en directo.

Se puede saber si Workstation está en modo en directo, basta con mirar la lista desplegable Intervalo de tiempo.

### **Visualización de datos de consulta en directo en la Consola de Workstation**

#### **Siga estos pasos:**

- Haga clic en En directo para activarla y ver datos en directo.

El valor predeterminado para el intervalo de tiempo es de 8 minutos y la resolución es de 15 segundos. No se pueden especificar un intervalo de tiempo y una resolución personalizados para el modo en directo en la Consola.

**Nota:** Haga clic en En directo para desactivar esta opción y seleccione un intervalo de tiempo y una resolución en la lista desplegable para ver los datos históricos. También puede especificar un intervalo de tiempo personalizado.

#### **Para ver los datos de consulta en directo y los datos históricos en la Consola de Workstation:**

- Para ver los datos de consulta en directo para un intervalo de tiempo mayor de 8 minutos, edite la propiedad `introscope.enterprisemanager.workstation.extendedLiveQuery` en el archivo `IntroscopeEnterpriseManager.properties` en el `<directorio_principal_EM>\config` tal y como se muestra a continuación:

`introscope.enterprisemanager.workstation.extendedLiveQuery=true`

Cuando esta propiedad se establece en `true`, se pueden utilizar las listas desplegables Intervalo de tiempo y Resolución en el cuadro de mandos de Workstation en el modo en directo. Estas opciones permiten especificar el intervalo de tiempo y la resolución personalizados para el modo en directo en lugar de utilizar el intervalo de tiempo predeterminado de 8 minutos y la resolución predeterminada de 15 segundos.

Se puede establecer el intervalo de tiempo para un período mayor que el intervalo de tiempo predeterminado de 8 minutos.

**Nota:** El intervalo de tiempo máximo durante el que se pueden ver datos en directo es de 30 días. Si se especifica un intervalo de tiempo superior a 30 días, el intervalo de tiempo se establece en 8 minutos de forma predeterminada. El número de puntos de datos que se muestran en el cuadro de mandos es igual a (Intervalo de tiempo/Resolución). Si el valor de (Intervalo de tiempo/Resolución) es inferior a 2, la resolución se establece en 15 segundos de forma predeterminada.

#### **WARNING**

Al establecer el intervalo de tiempo a un valor superior a 8 minutos es posible que se afecte al rendimiento de Enterprise Manager debido a las operaciones de E/S del disco deben recuperar datos de SmartStor.

### **Activación y desactivación del modo en directo**

En la Consola de Workstation, el modo en directo está activado de forma predeterminada. Se puede activar o desactivar el modo en directo haciendo clic en el botón En directo.

**Nota:** Cuando la Consola está en modo en directo y la resolución es de 15 segundos, la resolución que se muestra en la Consola (barra de herramientas) se utiliza para mostrar los datos en directo. Cuando la Consola está en modo en directo y la resolución es un número mayor de 15 segundos, se utiliza la resolución del widget para mostrar los datos en directo.

### **Visualización de los datos históricos**

Para ver los datos históricos, seleccione un intervalo de tiempo. Cuando se selecciona un intervalo de tiempo, Introscope muestra inmediatamente los datos de ese intervalo, establece la hora de finalización a la hora actual y basa la duración en la selección del intervalo de tiempo.

#### **Para cambiar de datos en directo a datos históricos:**

- Haga clic en el botón En directo.

Con el modo en directo desactivado, se podrá realizar lo siguiente:

- Seleccionar un intervalo de tiempo y una resolución en las listas desplegables.
- Especificar un intervalo de tiempo personalizado.
- Consultar datos históricos.

Los controles del intervalo de tiempo pueden ayudar a identificar la hora en la que se ha producido un problema. Por ejemplo, cree que el problema se ha producido en la última hora, por lo que establece el intervalo de tiempo en una hora y consulta los datos desde la hora actual hacia atrás. Si no ve el problema dentro de ese intervalo de hora, utilice los controles para moverse hacia atrás o hacia delante para localizar la hora en la que se produjo el problema.

#### Para ver los datos históricos:

1. Seleccione la métrica o el cuadro de mandos para el que desea ver los datos históricos.
2. Seleccione un intervalo de tiempo para la vista de historial en la lista desplegable Intervalo de tiempo. Introscope muestra los datos de ese intervalo, utilizando la duración que se ha seleccionado en la lista desplegable Intervalo de tiempo y estableciendo la hora de finalización en la hora actual.  
**Nota:** Si el intervalo de tiempo histórico incluye un año, se deberá especificar un año de cuatro dígitos. Por ejemplo, supongamos que selecciona un intervalo de tiempo a las 4:06:45 con una duración de 8 minutos. Por lo tanto, la hora de finalización del intervalo se establece en 4:06:45 y la hora de inicio en 3:59:30.  
**Nota:** Cuando se utiliza el control del intervalo de tiempo para consultar datos históricos, el intervalo que se selecciona se aplica a otras métricas o cuadros de mandos de la misma ventana y a las ventanas nuevas que se abran.
3. Ahora se puede seleccionar una resolución para ajustar el nivel de detalle de la vista aumentando o disminuyendo el número de puntos de datos que aparecen.  
 Cada intervalo de tiempo predefinido se asocia con una resolución predeterminada. Normalmente no es necesario cambiar esta configuración. El cambio de la resolución es útil cuando se desea visualizar un mayor nivel de detalle de los datos que aparecen de forma predeterminada.  
 Desde aquí, puede realizar lo siguiente:
  - Seleccionar un intervalo de tiempo predefinido en la lista desplegable, o
  - Especificar un valor en el campo Resolución. Especifique valores numéricos, seguidos por la duración: segundos, minutos, horas o días. Por ejemplo, 90 segundos.
4. Después de seleccionar un intervalo de tiempo, se podrá ajustar utilizando los controles del intervalo de tiempo.

#### Las alertas del modo histórico no reflejan el estado histórico de la alerta

Los valores de la alerta no se capturan en ninguna base de datos, por lo que si un cuadro de mandos en el modo histórico muestra alertas, estas alertas *no* reflejen el estado histórico. Si se está informando de datos para las alertas en el momento actual, las alertas reflejan valores en directo y no históricos.

#### Controles del intervalo de tiempo

Se pueden utilizar controles del intervalo de tiempo para desplazarse en incrementos que se basan en el intervalo de tiempo que se ha seleccionado.

#### Control deslizante

Arrastre el control deslizante en la barra de tiempo para cambiar el intervalo de tiempo.

#### Flechas



Haga clic en las flechas para moverse hacia atrás y hacia delante en el tiempo.

Las flechas únicas se mueven hacia atrás o hacia delante en incrementos pequeños; las flechas dobles se mueven hacia atrás o hacia delante en incrementos de tiempo que casi son iguales a la cantidad de tiempo del intervalo de tiempo seleccionado.

## Icono Restablecer



Haga clic en el icono Restablecer para restablecer la hora de finalización del intervalo a la hora actual.

## Icono Bloquear



Al hacer clic en el icono Bloquear se mantiene la resolución seleccionada mientras se seleccionan los diferentes intervalos de tiempo acercándose a los datos.

## Definición de un intervalo de tiempo personalizado

### Para definir un intervalo de tiempo personalizado para consultar datos históricos:

1. Seleccione la métrica o el cuadro de mandos para el que desea ver los datos históricos.
2. En la lista desplegable Intervalo de tiempo, seleccione Intervalo personalizado.  
Se abrirá la ventana Intervalo personalizado, que muestra la fecha actual (hoy) resaltada con un borde.
3. Seleccione las fechas:
  - a. Utilice los controles del calendario para seleccionar las fechas y las horas de inicio y finalización.
  - b. Use los controles del menú situados en la parte superior del calendario para seleccionar el mes y año, seleccione la fecha en el calendario y escriba la hora en el campo de hora situado en la parte inferior del calendario.
  - c. Haga clic en Aceptar.
 Workstation muestra los datos para el intervalo personalizado.

## Cómo acercar los datos históricos en gráficas

Cuando se visualizan datos históricos en una gráfica, se pueden acercar los datos haciendo clic con el puntero del ratón en una posición de la gráfica y arrastrando para especificar el intervalo de tiempo.

Introscope actualiza los datos en el visor en función de la nueva consulta y el intervalo de tiempo del visor muestra el nuevo intervalo.

El intervalo de tiempo global de la ventana y el control Intervalo de tiempo no cambian automáticamente cuando se acercan los datos. Por ejemplo, si se acerca a un período de 10 minutos en una gráfica con el Intervalo de tiempo establecido en 1 hora, la gráfica muestra el período de 10 minutos pero el control permanece en 1 hora y la barra de tiempo continúa mostrando el intervalo de una hora.

Se pueden anular las acciones de acercar predeterminadas de las siguientes formas:

- Establezca el intervalo de tiempo global y el control Intervalo de tiempo para que coincidan con la vista ampliada: seleccione Visor > Establecer intervalo de tiempo desde el intervalo ampliado o haga clic en el icono Establecer intervalo de tiempo desde el intervalo ampliado.
- Bloquee la resolución seleccionada haciendo clic en el icono Bloquear.
- Mantenga pulsada la tecla MAYÚS mientras se acerca para restringir el zoom al eje de tiempo.

## Métricas de DX APM

DX APM muestra datos de rendimiento de las aplicaciones que se recopilan como métricas desde sistemas locales y remotos.

## **Cómo DX APM proporciona métricas**

DX APM monitoriza el rendimiento de las aplicaciones de métodos individuales mientras varios componentes de la aplicación los ejecutan.

1. Las sondas que se insertan en el código de bytes del componente de la aplicación notifican los datos a los agentes.
2. Los agentes informan sobre los datos a Enterprise Manager. También otros subsistemas como JMX y PMI informan sobre los datos que recopilan los agentes.
3. Enterprise Manager recopila estos datos en métricas, es decir, el rendimiento de las aplicaciones tal y como se ha medido en numerosos puntos de los subsistemas de la aplicación.

### **NOTE**

Enterprise Manager registra el tiempo de rendimiento de los eventos del sistema en un archivo de registro de rendimiento, <EM\_Home>/logs/perflog.txt. Como alternativa a las métricas que se muestran en Investigator, el archivo perflog.txt puede contener información útil.

4. Las métricas se muestran en la interfaz de usuario.
5. Las métricas se pueden exportar a una base de datos externa.

## **Términos comunes**

Para comprender las métricas, a continuación se definen algunos términos comunes de DX APM.

Podrá encontrar más términos en el [Glosario de DX APM](#).

### **back-end**

Un back-end es un sistema externo, como una base de datos, un servidor de correo, un sistema de procesamiento de transacciones (como, por ejemplo, CICS o Tuxedo) o un sistema de mensajería (como, por ejemplo, WebSphere MQ).

### **simultaneidad e invocaciones simultáneas**

Los métodos simultáneos son métodos que se inician durante un intervalo pero no finalizan en ese mismo intervalo. Puesto que los usuarios generalmente desean que los métodos se completen rápidamente, no se recomienda indicar un valor excepcionalmente elevado de invocaciones simultáneas.

### **errores**

Son los errores generados por la aplicación o el sistema que se está monitorizando.

### **eventos**

Un evento es cualquier acción para la que los agentes capturan datos, además de valores de métrica. Los eventos de ejemplo son seguimientos de la transacción, errores y detenciones. Los agentes registran eventos en situaciones específicas, que incluyen:

- Seguimientos de la transacción
- Detenciones
- Errores: Captura excepciones y realiza un seguimiento de todas las ubicaciones donde se inician y proceden las excepciones.

### **NOTE**

Desactive la captura de excepciones en el entorno de producción debido a que puede provocar una degradación significativa del rendimiento.

### **front-end**

Un front-end es el componente de una aplicación que primero gestiona una solicitud entrante. El componente puede ser un servlet, JSP, una base de datos de gestión, un EJB o algún otro componente.

### **recolección**

La recolección es el proceso en el que Introscope recopila datos de los recopiladores.

## interval

Un intervalo es un intervalo de tiempo definido por el usuario que se utiliza para definir y realizar el promedio de las métricas. En Introscope, este período normalmente es de 7,5 segundos. Algunos de los sistemas monitorizados capturan los datos a intervalos diferentes.

## respuesta

La respuesta siempre se refiere a la ejecución del método. La respuesta se mide de las siguientes maneras:

- Recuento: El número de transacciones finalizadas durante ese intervalo.
- Tiempo: El tiempo que se ha tardado en ejecutar un método en milisegundos.

Las respuestas por intervalo es la métrica de rendimiento estándar de Introscope.

## tiempo de respuesta

El tiempo de respuesta es el período necesario para ejecutar un método que se mide de la siguiente manera:

- Tiempo medio de respuesta (ms): El tiempo medio, en milisegundos, que se ha tardado en ejecutar el método durante el intervalo.
- Tiempo de respuesta, mínimo y máximo: Los tiempos de respuesta más alto y más bajo durante el intervalo.

## tasa

Es el número de ejecuciones del método por segundo o por intervalo de tiempo.

## detención

Una detención es una instancia donde la hora de invocación de un método ha superado un umbral definido por un administrador.

## Tipos de métricas

Los tipos de métricas incluyen los siguientes:

- [Métricas de recuento](#)
- [Métricas de porcentaje](#)
- [Datos de cadena](#)

## Métricas de recuento

El recuento es un número entero. Por ejemplo, el recuento puede representar lo siguiente:

- El número de puntos de datos con los que se ha realizado una media para calcular una métrica.
- El número de eventos desde un determinado punto en el tiempo.
- El número de subprocesos en uso.

Los recuentos de errores y detenciones son ejemplos de métricas de recuento.

## Métrica de porcentaje

Los *porcentajes* se utilizan para medir el uso de los recursos en contra de los recursos máximos disponibles. Algunos ejemplos son los siguientes:

- Uso de la CPU
- El porcentaje de tiempo invertido en la recopilación de elementos no utilizados durante los últimos 15 minutos.

## Datos de cadena

Además de las medidas y el estado, Introscope recopila información que identifica los sistemas y las aplicaciones que se monitorizan. Los ejemplos de este tipo de datos son nombres de componentes del sistema como, por ejemplo, el nombre de una base de datos, las versiones de la máquina virtual Java o la dirección IP.

## Métricas de BlamePoint

DX APM utiliza cinco métricas básicas llamadas *las métricas de BlamePoint*. La métrica de BlamePoint proporciona una dirección inicial para que los evaluadores puedan identificar qué expertos del sistema pueden ayudar a resolver un problema.

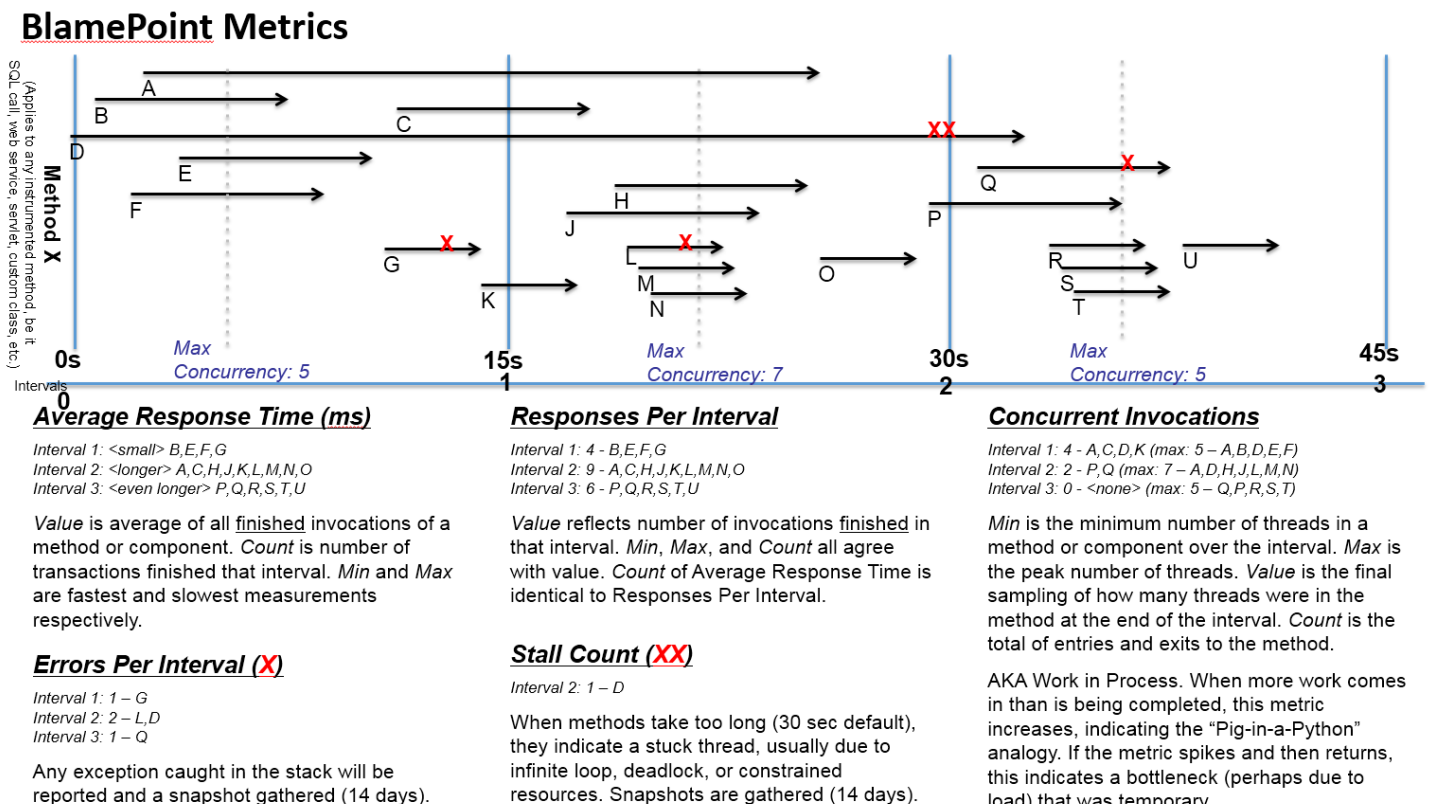
**Nota:** La métrica de BlamePoint también se denomina la "métrica estándar".

APM informa de esta métrica siempre que se monitorizan métodos de Java, por ejemplo:

- Front-ends
- Back-ends
- SQL
- Servlets
- Servicios web (incluida la métrica de errores SOAP)
- EJB
- JSP
- Todas las clases y métodos de Java personalizados

Los métodos más instrumentados informan de estas cinco instancias de métrica:

La siguiente ilustración muestra cómo APM informa de la métrica de BlamePoint para los métodos de Java:

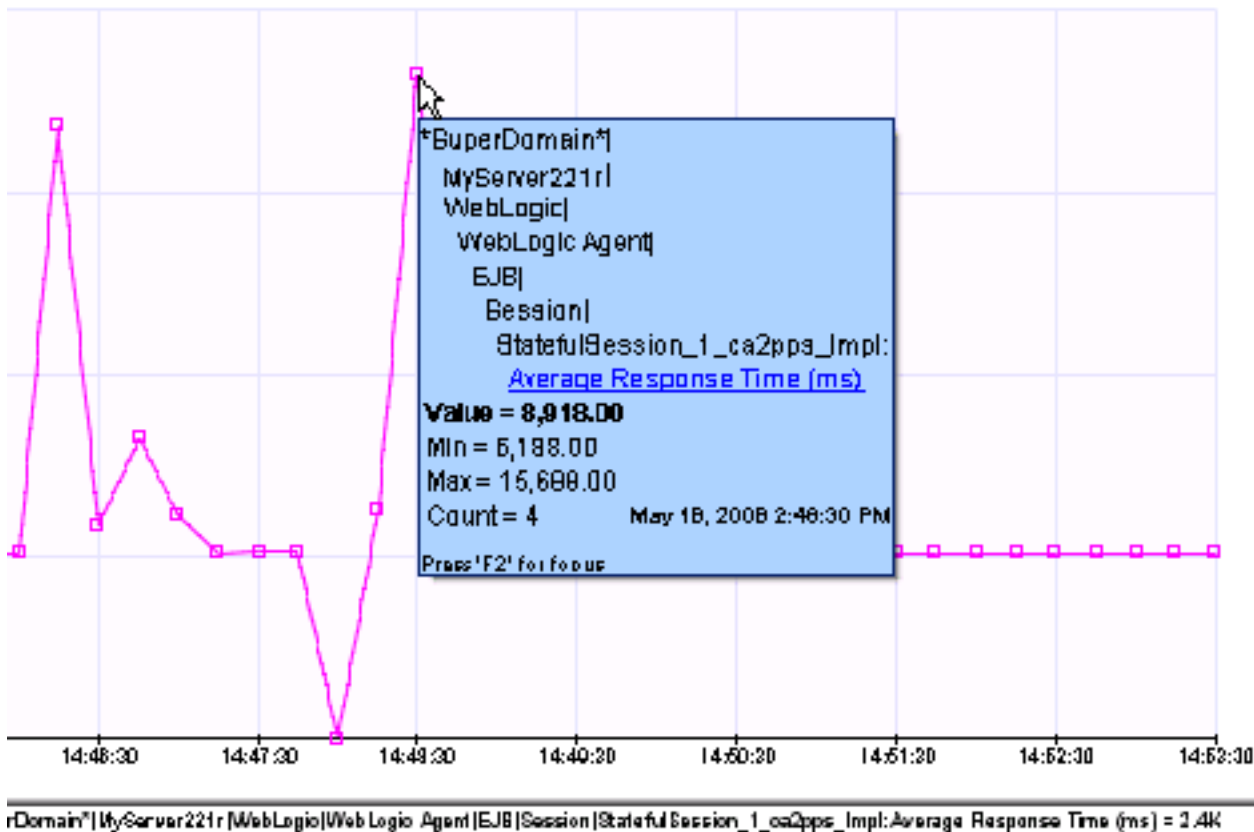


## Tiempo medio de respuesta (ms)

La métrica Tiempo medio de respuesta genera un promedio de los tiempos de respuesta de todas las solicitudes completadas durante un intervalo de tiempo específico. El tiempo de respuesta es el período de tiempo que tarda una solicitud en completarse. Este tiempo proporciona una medida básica de velocidad de respuesta de la aplicación, por lo tanto:

- Los tiempos de respuesta bajos son idóneos.
- Los tiempos de respuesta altos significa que hay un problema.

**Nota:** El recuento de Tiempo medio de respuesta es idéntico al valor de Respuestas por intervalo.



La ilustración muestra un gráfico del tiempo medio de respuesta para una sesión de EJB, tal y como se ve en Workstation. Información a tener en cuenta:

- Pase el ratón por encima de un punto de datos para ver la información sobre herramientas con más detalles sobre el punto de datos.
- En el ejemplo:
  - El valor del punto de datos de 8919 ms es el tiempo medio de respuesta de las solicitudes que se han completado durante el intervalo.
  - El recuento 4 significa que se han completado cuatro solicitudes durante el intervalo seleccionado.
- Además del valor y el recuento, cada punto de datos tiene datos mínimos y máximos.



- Min es el valor único más bajo de las solicitudes que se representan en el recuento. En este ejemplo, la solicitud que tardó menos tiempo en completarse.
- Max es el valor único más alto de las solicitudes que se representan en el recuento. En este ejemplo, la solicitud que ha tardado más tiempo en completarse.

Tenga en cuenta la siguiente información sobre el tiempo de respuesta medio:

- **Evaluación de errores mediante el tiempo medio de respuesta**

Utilice las tendencias de la métrica Tiempo medio de respuesta junto con los cambios en otras instancias de métrica para identificar y diagnosticar los problemas.

- **Problemas persistentes**

Cuando van acompañados por un recuento bajo de subprocesos disponibles, los tiempos medios de respuesta altos persistentes pueden indicar los siguientes problemas:

- Código ineficaz
- Un uso excesivo del sistema externo
- Back-end lento
- Demasiadas capas

- **Problemas periódicos**

Los picos periódicos en un gráfico muestran tiempos medios de respuesta altos que más adelante se normalizan. Cuando van acompañados de un recuento bajo de subprocesos disponibles, los tiempos medios de respuesta altos periódicos pueden indicar:

- Frecuentes pérdidas de la memoria caché global
- Cuellos de botella del back-end relacionados con la carga

Cuando van acompañados por una lectura baja del uso de la CPU, los tiempos medios de respuesta altos periódicos pueden indicar:

- Cuello de botella interno

- **Problemas progresivos**

Cuando un aumento constante en el tiempo medio de respuesta durante un largo período de tiempo va acompañado de un número bajo de respuestas por intervalo, puede indicar una pérdida de memoria.

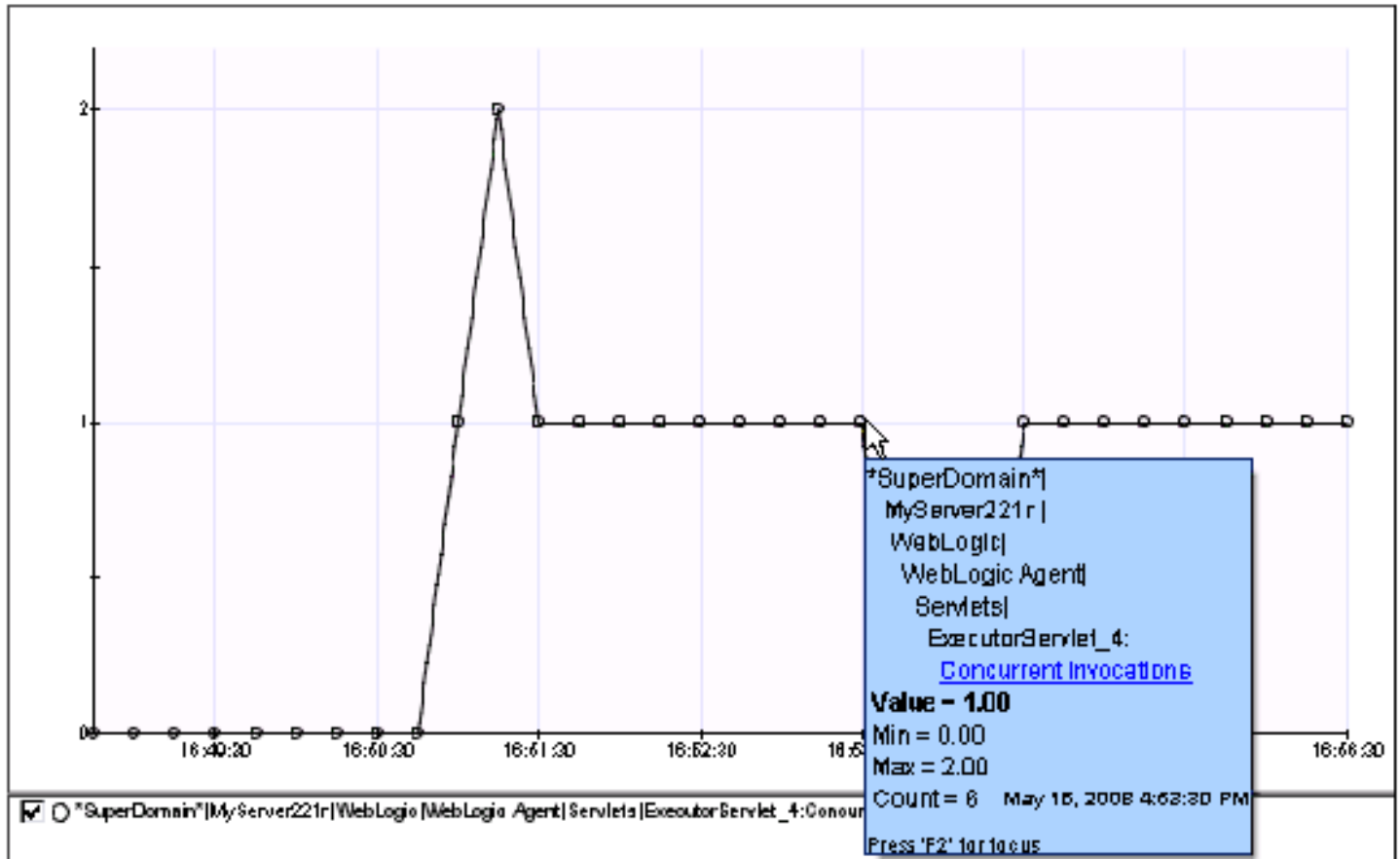
## **Invocaciones simultáneas**

Las invocaciones son solicitudes que gestionan la aplicación y sus componentes. Las invocaciones simultáneas son las solicitudes que se gestionan en un momento determinado.

DX APM calcula la métrica Invocaciones simultáneas contando el número de solicitudes que todavía estaban gestionándose al final de un intervalo determinado.

- Se recomienda un valor bajo de invocaciones simultáneas.
- Un valor alto de invocaciones simultáneas sugiere un problema.

Las invocaciones simultáneas se inician durante un intervalo pero no finalizan en ese mismo intervalo. Puesto que los usuarios generalmente desean que los métodos se completen rápidamente, no se recomienda obtener un número excepcionalmente elevado de invocaciones simultáneas. Pueden producirse picos temporales en las invocaciones simultáneas, pero la métrica debe volver a un valor 0 cada vez. Una métrica que no vuelve a un valor de 0 puede indicar un cuello de botella de subprocesos, problemas con el número de conexiones de la base de datos o incidencias con algún otro recurso compartido.



En la imagen, el valor 1 indica que todavía se estaba gestionando una solicitud al final del intervalo seleccionado. Las solicitudes que todavía estaban en curso al cierre del intervalo seleccionado probablemente se hayan completado durante los intervalos subsiguientes. Estas solicitudes que no se completan antes de que terminen los umbrales especificados se denominan "detenciones" (consulte [Recuento de detenciones](#)).

Tenga en cuenta la siguiente información sobre las invocaciones simultáneas:

- **Evaluación de errores mediante invocaciones simultáneas**

Utilice las tendencias de la métrica Invocaciones simultáneas junto con los cambios en otras instancias de métrica para identificar y diagnosticar los problemas.

- **Problemas persistentes**

Unos valores altos de invocaciones simultáneas persistentes pueden indicar los problemas siguientes: un uso excesivo del sistema externo o un back-end lento.

Cuando van acompañados por una lectura baja de las respuestas por intervalo, los valores altos de invocaciones simultáneas persistentes pueden indicar:

- Código ineficaz
- Demasiadas capas

- **Problemas periódicos**

Los valores periódicamente altos de invocaciones simultáneas se muestran en una gráfica con picos periódicos que más adelante se normalizan. Este aumento puede indicar un cuello de botella del back-end relacionado con la carga. Cuando vienen acompañados por una lectura baja de las conexiones disponibles, los valores periódicamente altos de invocaciones simultáneas pueden indicar pérdidas frecuentes de basura recopilada.

Cuando van acompañados de un recuento bajo de subprocesos disponibles, los valores periódicamente altos de las invocaciones simultáneas pueden indicar un cuello de botella interno.

- **Problemas progresivos**

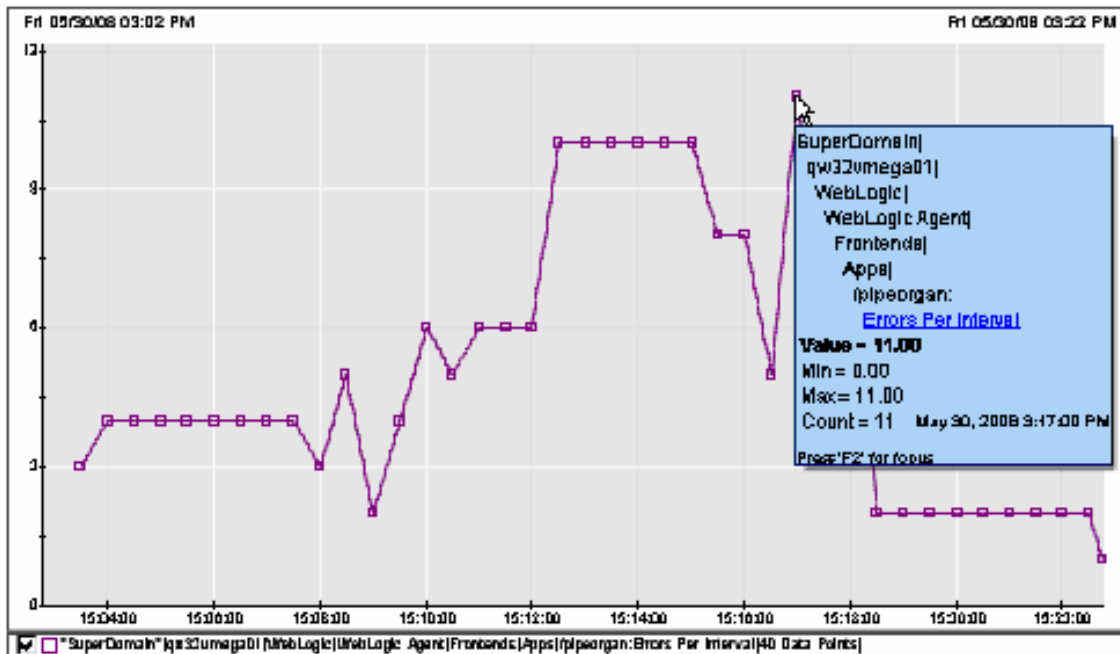
Un aumento constante en las invocaciones simultáneas durante un largo período de tiempo, especialmente cuando va acompañado de una lectura baja de las respuestas por intervalo, puede indicar una pérdida de memoria.

### Errores por intervalo

Los errores son el número de excepciones notificados por los códigos de error de JVM y HTTP. A continuación, se muestran ejemplos de errores:

- A 404 Page Not Found status reported by the HTTP server
- An SQL exception
- A Java exception

Se recomienda un recuento de errores bajo.



La métrica es un simple recuento de los errores que se notifican durante el intervalo. La imagen muestra un punto de datos seleccionado con un valor de 11; significa que se ha informado de 11 errores durante ese intervalo de tiempo. Dado que esta métrica es un recuento simple, el valor y el valor máximo serán siempre el mismo.

La ruta de la métrica situada debajo de la gráfica identifica la aplicación que informa de las excepciones. Para obtener más información sobre los errores que se muestran en una gráfica, consulte los registros de dicha aplicación.

En los sistemas con ErrorDetector activado, los errores también generan instantáneas de error. Las instantáneas de error proporcionan detalles sobre lo que estaba ocurriendo cuando se ha producido el error. Esta información se almacena en la base de datos de eventos de transacción. Un gran número de errores genera una gran cantidad de información documental. Evitar que se genere esta información es otra razón para minimizar errores.

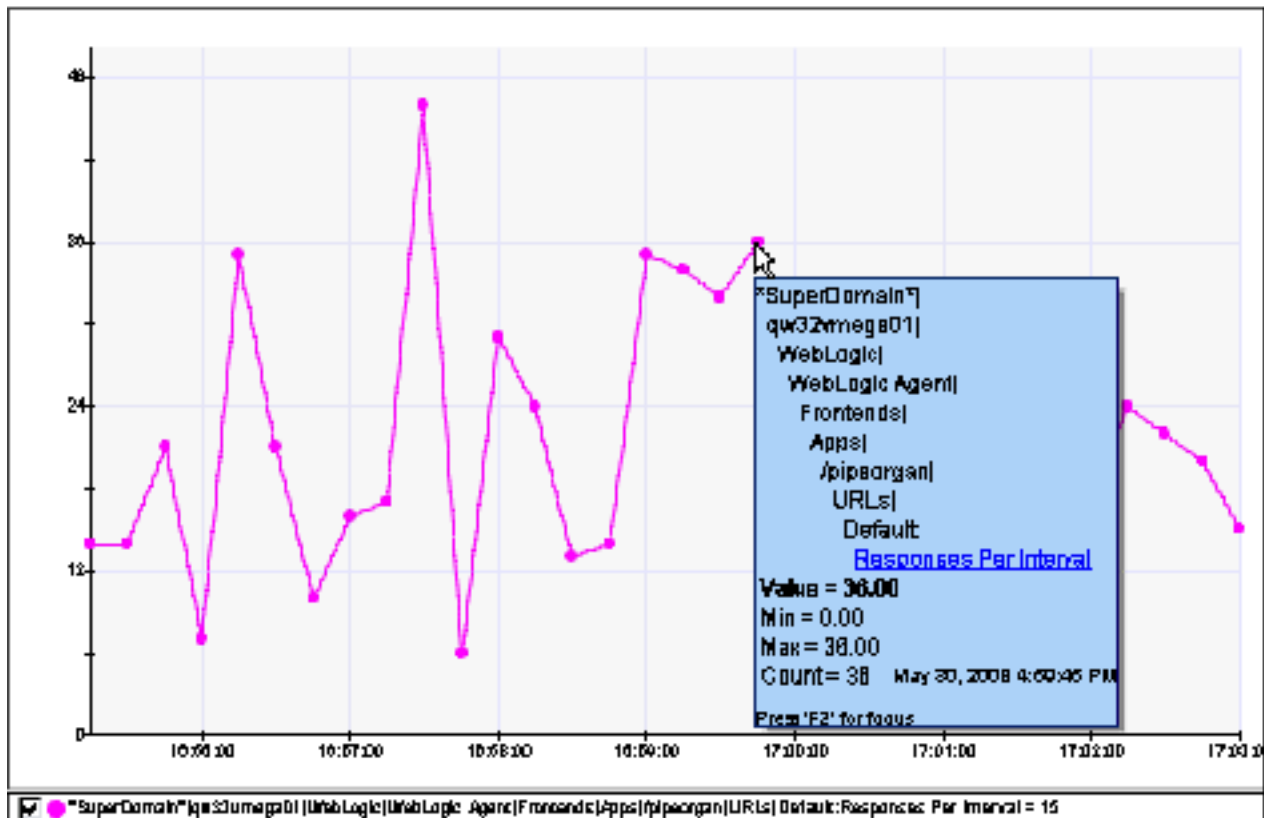
### Responses Per Interval

Las respuestas por intervalo reflejan el número de invocaciones terminadas en ese intervalo. Esta métrica es una medida de rendimiento de datos y, por consiguiente, de rendimiento de las aplicaciones. La métrica es un simple recuento de las solicitudes que se completan durante un intervalo.

- El valor de la métrica Respuestas por intervalo siempre es el mismo que el recuento de la métrica Tiempo medio de respuesta.
- Las respuestas por intervalo es una métrica de tipo IntCounter. Esta métrica no es un promedio del número de respuestas; siempre es el valor máximo del número de respuestas durante el intervalo.

Por lo general:

- Un número alto es recomendable.
- Un número bajo no es recomendable.
- Un pico inesperado en respuestas podría indicar un uso excesivo del sistema externo, tal como un ataque de denegación de servicio en un sitio web.



En la imagen, la información sobre herramientas muestra el valor del punto de datos seleccionado. Dado que esta métrica es un recuento simple, el valor y el valor máximo serán siempre el mismo.

Tenga en cuenta la siguiente información sobre las respuestas por intervalo:

- **Evaluación de errores con respuestas por intervalo**  
Utilice las tendencias de la métrica Respuesta por intervalo junto con los cambios en otras instancias de métrica para identificar y diagnosticar los problemas.
- **Problemas persistentes**  
Unos valores altos persistentes de respuestas por intervalo pueden indicar un uso excesivo del sistema externo.

### Recuento de detenciones

Las solicitudes detenidas son aquellas solicitudes que no se han completado dentro de un umbral de tiempo especificado. (El umbral de detención predeterminado es 30 segundos). Una solicitud se considera "detenida" cuando su ejecución ha excedido el umbral de detención.

- Se recomienda un recuento bajo.
- Un recuento alto no es recomendable.

Las detenciones pueden representar cualquiera de los casos siguientes. Puede haber otros motivos por lo que se produzca una detención, pero los casos que se describen a continuación son los más comunes.

- **Un subproceso en un bucle infinito**

A veces, los programadores escriben código en el que un bucle que debería salir normalmente no lo hace. Cuando un subproceso entra en un bucle infinito, los componentes que lo invocan sufren un aumento en el recuento de detenciones. Los bucles infinitos tienen la característica adicional de provocar que el núcleo de una CPU permanezca ocupado. Por ejemplo, en un sistema con cuatro núcleos de poca actividad, si un subproceso entra en un bucle infinito, la utilización total de la CPU puede aumentar aproximadamente un 25 %. Si un segundo subproceso entra en el bucle infinito, la CPU podría elevarse hasta el 50 %, y así sucesivamente.

- **Un subproceso en espera durante un largo período de tiempo o un subproceso que nunca agotará el tiempo de espera**

Cuando un subproceso intenta abrir un recurso como un socket en un sistema remoto, el programador puede especificar que se detenga después de un determinado número de segundos. Si este período es suficiente (por ejemplo, cinco minutos), el recuento de detenciones aumentará y permanecerá incrementado durante cinco minutos. A veces, el intento de conexión nunca agota el tiempo de espera, en cuyo caso el subproceso permanece ocupado y el recuento de detenciones nunca disminuye.

En muchos sistemas, existen subprocesos que realizan este tipo de bloqueo por motivos rutinarios. Este comportamiento es la razón por la que el recuento de detenciones a veces puede ser distinto de 0 para un componente, incluso cuando el sistema está inactivo. Preste atención al recuento de subprocesos "natural" y considérela una incidencia solo cuando se produzcan cambios anormales.

- **Un subproceso implicado en un interbloqueo o bloqueo activo**

Los programadores utilizan bloqueos para asegurarse de que los datos no resultan dañados. A veces, pueden adquirirse los bloqueos en el orden incorrecto, en cuyo caso el programa puede desarrollar lo que se conoce como "interbloqueo". Un interbloqueo significa que dos o más subprocesos se detienen a la espera de que uno de ellos progrese. Los subprocesos no son capaces de avanzar sin los recursos que ya han extraído los otros subprocesos. Los interbloqueos constituyen errores de sistema catastróficos en casi todos los casos. Los volcados de subprocesos a menudo son la técnica más útil para identificar el código dañado. Un bloqueo activo es un interbloqueo en el que uno o varios subprocesos utilizan activamente la CPU. Los interbloqueos son diferentes de los bucles infinitos en tal que un bucle infinito es solo el resultado de una condición de interrupción de un bucle, mientras que un interbloqueo implica la semántica de bloqueo (o código "sincronizado") de la aplicación en el que se produce.

**Nota:** La información sobre los eventos de detención se almacena en la base de datos de eventos de transacción.

Tenga en cuenta la siguiente información sobre el recuento de detenciones:

- **Medición del recuento de detenciones**

Un seguimiento de transacciones puede mostrar varias solicitudes que no se han completado durante el umbral de tiempo especificado (detenciones), pero Investigator muestra un número diferente como el recuento de detenciones. Esta diferencia en los números se produce porque el recuento de detenciones se registra como un valor de punto (en un momento dado durante un intervalo) y no como un valor de intervalo (durante un período de tiempo). Puede haber varios valores de detención representando las transacciones largas que se han completado durante un intervalo, pero solamente se utilizará el recuento disponible durante un momento único como el punto de datos.

- **Evaluación de errores con recuento de detenciones**

Utilice las tendencias de la métrica Recuento de detenciones junto con los cambios en otras instancias de métrica para identificar y diagnosticar los problemas.

- **Problemas persistentes**

Unos valores altos persistentes para el recuento de detenciones pueden indicar un sistema back-end lento.

- **Problemas periódicos**

Unos valores periódicamente altos para el recuento de detenciones pueden indicar un cuello de botella del back-end relacionado con la carga.

- **Problemas progresivos**

Un aumento constante de los valores del recuento de detenciones durante un largo período de tiempo, especialmente cuando va acompañado por un recuento bajo de subprocesos disponibles, puede indicar una pérdida de recursos (subprocesos).

## Métricas de JMX

Las siguientes métricas están disponibles en el árbol de Investigator bajo el nodo JMX con el formato:: JMX\(|(.\*)\| (Type=)?<Nombre MBean>:<Nombre atributo>.

- **ServerRuntime: OpenSocketsCurrentCount**  
El número actual de sockets abiertos en el servidor.
- **ServerRuntime: SocketsOpenedTotalCount**  
El número total de sockets que se han abierto en el servidor.
- **ExecuteQueueRuntime: ExecuteThreadCurrentIdleCount**  
El número de subprocesos inactivos que se han asignado a la cola.
- **ExecuteQueueRuntime: PendingRequestCurrentCount**  
El número de solicitudes en espera en la cola.
- **ExecuteQueueRuntime: ServicedRequestTotalCount**  
El número de solicitudes que esta cola procesa.
- **JDBCDataSourceRuntime: ActiveConnectionsCurrentCount**  
El número de conexiones de JDBC que actualmente están en uso en esta fuente de datos.
- **JDBCDataSourceRuntime: ConnectionsTotalCount**  
El número total de conexiones de JDBC creadas en esta fuente de datos desde el momento en que se ha implementado.
- **JDBCDataSourceRuntime: LeakedConnectionCount**  
El número de conexiones de JDBC que han tenido pérdidas.
- **JDBCDataSourceRuntime: WaitingForConnectionCurrentCount**  
El número de solicitudes de conexión esperando una conexión de JDBC.
- **JDBCDataSourceRuntime: NumAvailable**  
El número de conexiones de JDBC que están disponibles actualmente en esta fuente de datos.
- **EJBCacheRuntime: ActivationCount**  
El número total de beans de este directorio principal de EJB que se han activado.
- **EJBCacheRuntime: CacheAccessCount**  
El número total de intentos para acceder a un bean desde esta memoria caché.
- **EJBCacheRuntime: CachedBeansCurrentCount**  
El número actual de beans desde este directorio principal de EJB que se encuentran en la memoria caché de EJB.
- **EJBCacheRuntime: CacheHitCount**  
El número de intentos de acceso a la memoria caché que se han realizado correctamente.
- **EJBLockingRuntime: TimeoutTotalCount**  
El número total de subprocesos que han excedido el tiempo de espera esperando un bloqueo en un bean.
- **EJBPoolRuntime: BeansInUseCount**  
El número de instancias de bean de esta agrupación que se usan actualmente.
- **EJBPoolRuntime: IdleBeansCount**  
El número de instancias de bean de esta agrupación que actualmente están libres.
- **EJBPoolRuntime: TimeoutTotalCount**  
El número total de subprocesos que han excedido el tiempo de espera esperando un bean disponible de esta agrupación.
- **EJBPoolRuntime: WaiterCurrentCount**

Proporciona un recuento del número de subprocesos que actualmente están esperando una instancia de bean disponible de la agrupación libre.

- **EJBTransactionRuntime: TransactionCommittedTotalCount**  
El número total de transacciones que se han confirmado para este EJB.
- **JMSRuntime: ConnectionsTotalCount**  
El número total de conexiones de JMS realizadas en este servidor WebLogic después del último restablecimiento.
- **JMSRuntime: JMSServersCurrentCount**  
El número total de servidores JMS que se implementan en esta instancia del servidor de WebLogic.
- **JMSPooledConnectionRuntime: NumAvailable**  
El número de sesiones de JMS disponibles en la agrupación que no se están utilizando actualmente.
- **JMSDestinationRuntime: BytesReceivedCount**  
El número de bytes recibidos en este destino después del último restablecimiento.
- **JMSDestinationRuntime: ConsumersTotalCount**  
El número total de consumidores que han accedido a este destino después del último restablecimiento.
- **JMSDestinationRuntime: MessagesReceivedCount**  
El número de mensajes recibidos en este destino después del último restablecimiento.
- **JMSDestinationRuntime: BytesCurrentCount**  
El número actual de bytes almacenados en el destino.
- **JMSDestinationRuntime: ConsumersCurrentCount**  
El número actual de consumidores que acceden a este destino.
- **JMSDestinationRuntime: MessagesCurrentCount**  
El número actual de mensajes en el destino.
- **JMSDurableSubscriberRuntime: MessagesReceivedCount**  
El número de mensajes que este suscriptor duradero recibe después del último restablecimiento.
- **JMSDurableSubscriberRuntime: BytesCurrentCount**  
El número de bytes que este suscriptor duradero recibe.
- **JMSDurableSubscriberRuntime: MessagesCurrentCount**  
El número de mensajes que siguen estando disponibles para este suscriptor duradero.
- **JMSServerRuntime: BytesReceivedCount**  
El número total de bytes que este servidor JMS recibe después del último restablecimiento.
- **JMSServerRuntime: BytesCurrentCount**  
El número actual de bytes almacenados en este servidor JMS.
- **JMSConnectionRuntime: SessionsCurrentCount**  
El número actual de sesiones para esta conexión.
- **TransactionNameRuntime: TransactionAbandonedTotalCount**  
El número total de transacciones que se han abandonado después del último restablecimiento.
- **TransactionNameRuntime: TransactionCommittedTotalCount**  
El número total de transacciones que se han confirmado después del último restablecimiento.
- **TransactionNameRuntime: TransactionHeuristicsTotalCount**  
El número total de transacciones que se han completado con el estado heurístico después del último restablecimiento.
- **TransactionNameRuntime: TransactionRolledBackTotalCount**  
El número total de transacciones que se han revertido después del último restablecimiento.
- **TransactionNameRuntime: TransactionRolledBackTimeoutTotalCount**  
El número total de transacciones que se han revertido debido a una experiencia de tiempo de espera después del último restablecimiento.
- **TransactionNameRuntime: TransactionTotalCount**  
El número total de transacciones procesadas (confirmadas/revertidas/heurísticas) desde el último restablecimiento.
- **TransactionResourceRuntime: TransactionCommittedTotalCount**  
El número total de transacciones que se han confirmado desde el último restablecimiento.
- **TransactionResourceRuntime: TransactionHeuristicsTotalCount**

El número total de transacciones realizadas con el estado heurístico desde el último restablecimiento.

- **TransactionResourceRuntime: TransactionRolledBackTotalCount**  
El número total de transacciones que se han revertido desde el último restablecimiento.
- **TransactionResourceRuntime: TransactionRolledBackTimeoutTotalCount**  
El número total de transacciones que se han revertido debido a una experiencia de tiempo de espera desde el último restablecimiento.
- **TransactionResourceRuntime: TransactionTotalCount**  
El número total de transacciones procesadas (confirmadas/revertidas/heurísticas) desde el último restablecimiento.
- **JTARuntime: TransactionAbandonedTotalCount**  
El número total de transacciones que se han abandonado desde el último restablecimiento.
- **JTARuntime: TransactionCommittedTotalCount**  
El número total de transacciones que se han confirmado desde el último restablecimiento.
- **JTARuntime: TransactionHeuristicsTotalCount**  
El número total de transacciones realizadas con el estado heurístico desde el último restablecimiento.
- **JTARuntime: TransactionRolledBackTotalCount**  
El número total de transacciones que se han revertido desde el último restablecimiento.
- **JTARuntime: TransactionRolledBackTimeoutTotalCount**  
El número total de transacciones que se han revertido debido a una experiencia de tiempo de espera desde el último restablecimiento.
- **JTARuntime: TransactionTotalCount**  
El número total de transacciones procesadas (confirmadas/revertidas/heurísticas) desde el último restablecimiento.
- **Server: IdleConnectionTimeout**  
El valor actual del tiempo de espera de la sesión HTTP.

### **Métricas agregadas de JMX**

Las siguientes métricas están disponibles en el árbol de Investigator bajo el nodo WebLogic, JMX Aggregate.

- **Thread Pool: Waiting Request Count**  
Proporciona un recuento del número total de subprocesos que actualmente están solicitando una instancia disponible de la agrupación libre.
- **JDBC Connection Pool: Waiting Thread Count**  
Proporciona un recuento del número total de subprocesos que actualmente están esperando una instancia de conexión disponible de la agrupación libre.
- **EJB Pool: Waiting Thread Count**  
Proporciona un recuento del número total de subprocesos que actualmente están esperando una instancia de bean disponible de la agrupación libre.

## **Métricas de la transacción**

Las métricas de la transacción miden una parte específica de una transacción. En función de la arquitectura del sistema, pueden aparecer las siguientes métricas de Java en Investigator. La mayoría aparecen en el Árbol de métrica.

El Agente de Java también informa sobre el contexto de la aplicación de Java como atributos del tiempo de ejecución para los vértices de Team Center. El conjunto de atributos sobre los que informa el Agente de Java son los [atributos comunes](#) que existen en la mayoría de componentes. DX APM recopila automáticamente los atributos comunes. Puede crear [sus propias perspectivas](#) utilizando los atributos de Java.

### **NOTE**

Algunas de estas métricas, como Base de datos y XML, también se aplican al Agente de .NET.



## **EJB**

Allí donde Enterprise JavaBeans (EJB) forman parte de la arquitectura, pueden ser de los siguientes tipos:

- Bean de entidades de EJB
- Bean de sesiones de EJB
- Bean de mensajes de EJB

Para cada uno de estos tipos, aparecen las dos métricas siguientes:

- Average Method Invocation Time (ms)
- Method Invocations Per Interval

Para cada clase o método de EJB que aparece como nodo hijo en los tipos EJB, Enterprise Manager informa sobre las cinco métricas de BlamePoint:

- Tiempo medio de respuesta (ms)
- Invocaciones simultáneas
- Errores por intervalo
- Responses Per Interval
- Recuento de detenciones

## **Servlets**

El nodo Servlets normalmente muestra las cinco métricas básicas de BlamePoint para cada servlet que la aplicación monitorizada invoca:

- Tiempo medio de respuesta (ms)
- Invocaciones simultáneas
- Errores por intervalo
- Responses Per Interval
- Recuento de detenciones

El nodo Servlets también muestra estas métricas relacionadas con la CPU:

### **NOTE**

Estas métricas relacionadas con la CPU no son compatibles con los servlets asíncronos.

- Average Block Time (ms)  
El tiempo aproximado transcurrido en milisegundos que un subproceso ha estado en estado bloqueado cuando la máquina virtual Java admite la monitorización de la contención de subprocesos.
- Average Bytes Allocated  
El número aproximado de bytes adjudicados a la memoria dinámica de subprocesos de transacciones cuando la máquina virtual Java admite la medición de la adjudicación de la memoria de subprocesos.

### **NOTE**

Las máquinas virtuales Java de IBM no admiten esta métrica.

- Average System CPU Time (ms)  
El tiempo que tarda el código en ejecutarse en el kernel del sistema operativo en una transacción de una aplicación monitorizada cuando la JVM admite la medición del tiempo de la CPU.
- Average User CPU Time (ms)  
Cantidad de tiempo que tarda el procesador en ejecutar el código de programa o el código en las bibliotecas para una transacción cuando la JVM admite la medición del tiempo de la CPU.
- Average Wait Time (ms)

El tiempo aproximado transcurrido en milisegundos que un subproceso de transacción ha estado en el estado WAITING o en el estado TIMED\_WAITING cuando la máquina virtual Java admite la monitorización de la contención de subprocesos.

### **JSP (JavaServer Pages)**

#### **Tiempo medio de respuesta (ms)**

Tiempo medio de respuesta de los métodos `_jspService()` de todas las JSP que se ejecutan en la máquina virtual Java. Se hace la media de los tiempos de respuesta de todas las JSP individuales para calcular este valor.

#### **Responses Per Interval**

El número de invocaciones completadas de los métodos `_jspService` de todas las JSP que se han ejecutado en la máquina virtual Java en los últimos 15 segundos del período de tiempo.

#### **Average Response Time (ms) by class name**

Tiempo medio de respuesta en milisegundos de la JSP identificada por el nombre de clase. Cada invocación del método `_jspService()` se ha agotado y se ha hecho la media para llegar a este valor.

#### **Responses Per Interval**

Número de invocaciones completadas del método `_jspService()` de la JSP identificado por el nombre de clase en el último intervalo de 15 segundos.

#### **Responses Per Second**

Velocidad a la que se completan los métodos `_jspService()` de todas las JSP que se ejecutan en la máquina virtual Java.

#### **Responses Per Second by class name**

Velocidad a la que se completan las invocaciones del método `_jspService()` de JSP identificadas mediante un nombre de clase en particular.

#### **Stalled Methods by class name and by method name**

El número de JSP que está tardando más que un umbral definido en completar la ejecución del método `_jspService()`.

#### **Invocaciones simultáneas**

El número de subprocesos ejecutando el método `_jspService()`.

### **Bibliotecas de etiquetas de JSP (TagLib JSP)**

Las bibliotecas de etiquetas son recopilaciones de etiquetas personalizadas que se utilizan en las páginas JSP para invocar acciones personalizadas. La especificación de JSP proporciona seis acciones estándares. Una acción personalizada es cualquier acción que no está incluida en el conjunto de las seis acciones estándares. Los ejemplos de tareas que las acciones personalizadas invocan son el control del formulario, el acceso a sistemas externos como bases de datos y correo electrónico, y el control del flujo.

Las siguientes métricas están disponibles para las bibliotecas de etiquetas de 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)

### **JSP IO TagLibrary**

- Warning Count
- Exception Count

### **RMI (Remote Method Invocations)**

Remote Method Invocations son invocaciones de métodos de objetos Java distribuidos, que son objetos Java que pueden estar en más de un host.

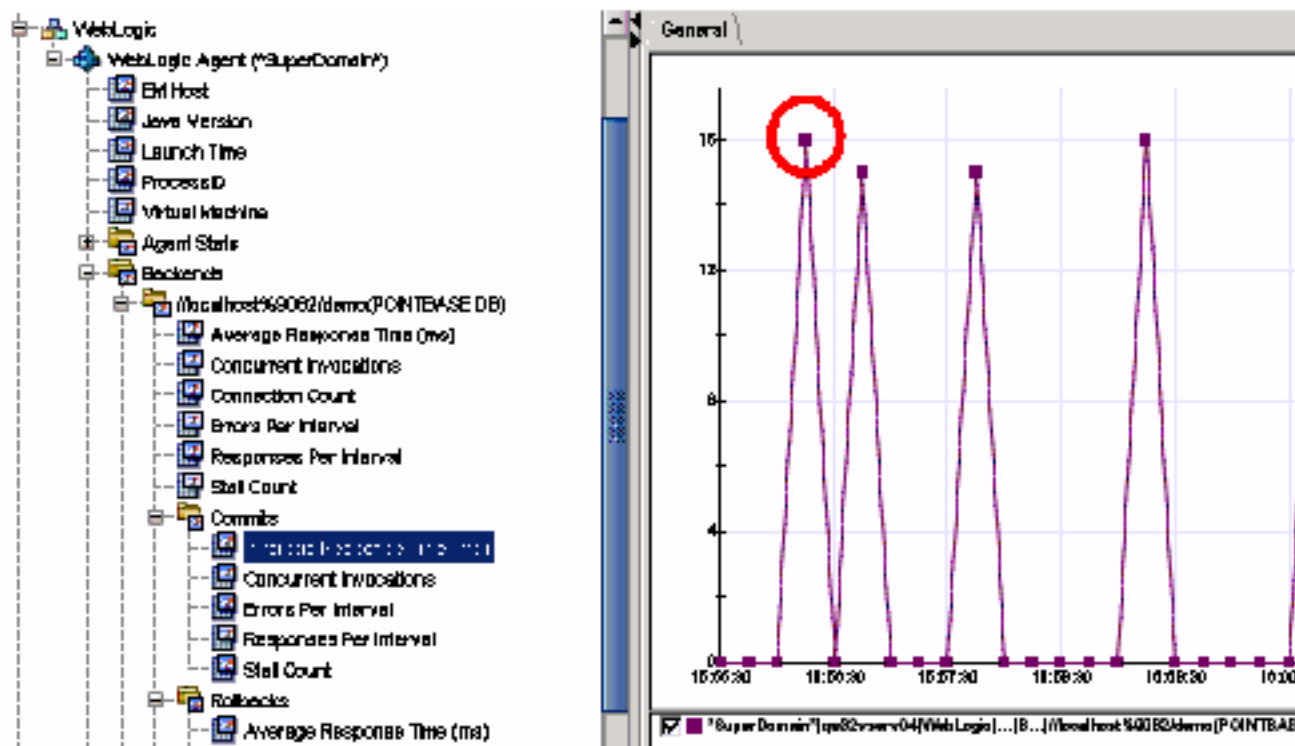
Las métricas siguientes están disponibles tanto para clientes RMI como para servidores RMI.

- 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

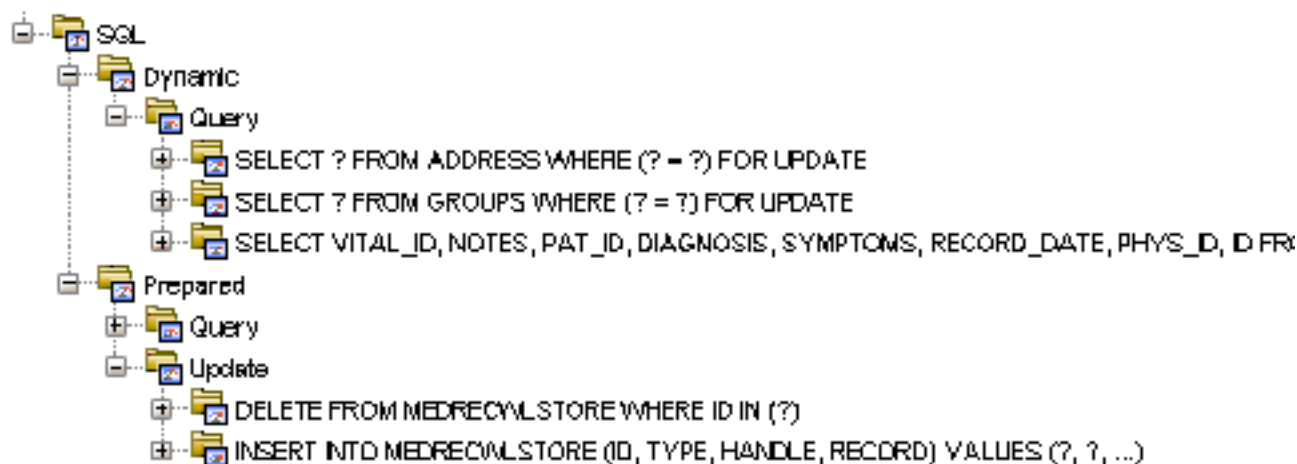
### **Métricas de la base de datos (SQL)**

Cada back-end de la base de datos se puede configurar para informar sobre las métricas siguientes:

- Confirmaciones: Cada transacción completa de consulta y respuesta se conoce como una *confirmación*. Las cinco métricas estándares se recopilan y muestran para todas las transacciones que realizan una confirmación en un intervalo determinado. Por ejemplo, en la captura de pantalla que aparece a continuación, el punto de datos dentro de un círculo muestra el tiempo medio de respuesta de todas las transacciones de la base de datos confirmadas en ese intervalo.



- Reversiones: Una reversión es una transacción de consulta y respuesta que no se ha completado correctamente. Las cinco métricas estándares se recopilan y muestran para todas las transacciones que se han revertido en un intervalo determinado.
- SQL:



Para cada una de las instrucciones que procesa la base de datos durante un intervalo, el agente informa sobre estas seis métricas:

- Tiempo medio de respuesta (ms)
- Invocaciones simultáneas
- Errores por intervalo
- Active Connection Object Count
- Responses Per Interval
- Recuento de detenciones

Información a tener en cuenta:

- Las instrucciones se separan por subnodo según si son Prepared o Dynamic.
- Cada tipo de instrucción SQL como, por ejemplo, GRANT, UPDATE, QUERY, REVOKE y DROP, se muestra en un subnodo para ese tipo de instrucción.

### **Back-ends automáticos**

Las métricas de back-end automático tienen una ruta de métrica ligeramente distinta a las métricas de back-end estándar.

Backends|<Java Package>|<classname > |<method >

Por ejemplo: Backends|com.mysql.jdbc|MySQLIO|sendCommand

Las métricas de resumen de diferentes back-ends en el mismo paquete de Java se muestran aquí:

Backends|<Paquete de Java>

Por ejemplo: Backends|com.mysql.jdbc

Introscope informa sobre las métricas de compatibilidad del back-end automático.

### **XML (Extensible Markup Language)**

Las métricas de XML pueden ser de los siguientes tipos.

#### **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 de 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)**

A continuación se muestran las métricas de JNDI:

- [JNDI lookup](#)
- [JNDI lookupLink](#)
- [JNDI search](#)
- [JNDI called metrics](#)

---

## **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

## **JNDI Called Metrics**

- File system I/O

## **JMS (Java Messaging Service)**

JMS tiene cuatro subnodos:

- message listener
- message consumer
- topic publisher
- queue sender

Las siguientes métricas pueden aparecer en cualquiera de los subnodos:

- 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 las API de recepción de JMS sincrónicas, las siguientes métricas se muestran en el nodo Frontends de Investigator:

- [Messages Received Per Interval](#)
- [Errors Per Interval](#)
- [Estimated Message Processing Time \(ms\)](#)

Los valores de las métricas individuales `{queuenam}` y `{topicname}` se agregan en los valores de los nodos Colas y Temas, respectivamente.

### **Messages Received Per Interval**

La métrica Messages Received Per Interval se incrementará en uno cada vez que se complete correctamente el método `receive()` con un valor de retorno no nulo.

### **Errores por intervalo**

La métrica Errors Per Interval se incrementará en uno si cualquiera de los métodos instrumentados devuelve una excepción. Además, ErrorDetector genera una instantánea del error.

#### **NOTE**

Cuando el método `receive()` de IBM WebSphere MQ JMS termina con una excepción MQRC\_NO\_MSG\_AVAILABLE, APM no informará de algunos resultados. La métrica Errors Per Interval no aumenta y ErrorDetector no genera una instantánea del error.

### **Estimated Message Processing Time (ms)**

Esta métrica muestra la hora aproximada entre la terminación correcta del método `receive()` con un valor de retorno no nulo y el inicio de la siguiente invocación del método `receive()`. Esta métrica recopila los datos cuando los métodos que están en el mismo objeto del consumidor y en el mismo subproceso. Cuando el agente no puede identificar cualquier recepción posterior, el rastreador de JMS utiliza JMS para recibir el método principal de llamada para calcular el valor de la métrica. En este caso, el valor de la métrica es el tiempo entre el final del método de recepción actual y la finalización del método principal. Solo después de que el agente identifique el método principal de recepción de JMS y lo instrumente correctamente con `JMSReceiveParentTracer`, el agente podrá generar un seguimiento de la transacción. El seguimiento muestra el valor de tiempo del procesamiento de la métrica. Consulte la sección siguiente.

### **Identificación e instrumentación del método principal**

El método principal de una llamada JMS `Receive` es el método que se encarga de procesar el mensaje recibido llamando a `JMS Receive`. A veces el rastreador no puede encontrar una llamada `receive` después de la recepción actual. En este caso, es esencial identificar el método principal para proporcionar el valor de la métrica y el seguimiento de la transacción.



La identificación del método principal funciona del siguiente modo:

1. En un seguimiento de pila que se recopila en el rastreador `receive method`, se pueden etiquetar las clases con el método `run` o `call`. Las clases con etiquetas implementan el método `interfaces java.lang.Runnable` o el método `java.lang.Callable`. Las clases que se etiquetan con el método `run` o `call` se identifican como métodos principales. Cuando hay más métodos principales en el seguimiento de pila, el método más cercano a la llamada `receive` se marca como principal.

#### NOTE

Introscope ignora los diversos componentes al identificar la clase principal y el método del seguimiento de pila. Introscope ignora todas las clases de JDK, los métodos y clases lambda dinámicos y las clases de proxy.

2. Es posible que un seguimiento de pila no tenga un método `run` o `call` que puede utilizar el agente para identificar el método principal. En este caso, el agente basa la identificación en el valor de índice constante. De forma predeterminada, la clase en el índice 7 se identifica como el método principal. Una vez la clase en el índice 7 es una clase de JDK, una clase de lambda dinámico o una clase de proxy, Introscope omite la clase. Introscope tiene en cuenta la clase en el siguiente índice inferior (más próxima a la llamada `receive`) y se repite hasta que se marca una clase como principal.

Se pueden encontrar los procesos principales identificados que se almacenan en el archivo `JMSParentMethodPersist.pbd` en el `<Directorio_principal_agente>/core/hotdeploy`.

#### NOTE

Más información: [Un método que nunca se cierra se identifica como método principal](#)

### Java Mail

Java Mail tiene dos subnodos:

- Java Mail (Send)
- Java Mail (sendMessage)

Las métricas siguiente pueden aparecer en los subnodos `Send` o `sendMessage`:

- Transport:Average Method Invocation Time (ms)
- Transport:Method Invocations Per Interval
- 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

## **Sostenibilidad del agente**

Las métricas de sostenibilidad del agente aparecen en el nodo **Agent Stats**. Estas métricas proporcionan información sobre el estado interno del agente en lugar de proporcionar el estado interno de la aplicación que el agente está monitorizando. Las métricas de sostenibilidad del agente pueden proporcionar datos útiles cuando se está investigando el comportamiento del agente.

### **Métricas de sostenibilidad del seguimiento exhaustivo**

El subnodo **Deep Tracing** se encuentra bajo el subnodo **Sustainability**. El seguimiento exhaustivo muestra las siguientes métricas sobre los recursos del agente que se utilizan para proporcionar visibilidad exhaustiva del seguimiento de la transacción:

### **Visibilidad exhaustiva del seguimiento de la transacción y métricas de sostenibilidad de la instrumentación inteligente**

#### **Analyzed Methods Count**

Número total de métodos que Introscope ha analizado para la instrumentación inteligente. El número incluye los métodos que la instrumentación inteligente instrumenta y no instrumenta.

#### **Average Component Array Size**

Tamaño de la estructura de datos de la matriz del componente de instrumentación inteligente interno tal y como lo notifican las transacciones en directo.

#### **Average Component Count Per Transaction**

Promedio del número de componentes de la visibilidad exhaustiva y de responsabilidad por transacción.

#### **Average Deep Component Count Per Transaction**

Promedio del número de componentes de la visibilidad exhaustiva por transacción.

#### **Classes Processed Per Interval**

Número de clases que ProbeBuilder ha procesado para la instrumentación inteligente.

#### **Instrumented Methods Count**

Número total de métodos que la instrumentación inteligente está instrumentando actualmente.

#### **Max Instrumentable Methods Count**

Número máximo de métodos que Introscope califica para la instrumentación cuando el nivel de instrumentación inteligente se ha establecido en alto.

---

**ProbeInfo Collection Size**

El tamaño de la lista de matriz ProbeInfo Collection interna.

**Auto Tracing: Cached Transaction Count Per Interval**

Número de transacciones que están almacenadas en una memoria caché interna por intervalo de 15 segundos.

**Auto Tracing: Clamped Traces**

Número de seguimientos de la transacción automáticos que se han fijado y no se han enviado a Enterprise Manager ni se muestran en la interfaz de usuario.

**Auto Tracing: Downstream GUID Count Per Interval**

Número de identificadores de seguimiento descendentes agregados a una memoria caché interna por intervalo de 15 segundos.

**Auto Tracing: Sent Traces**

Número de seguimientos de la transacción automáticos que se envían a Enterprise Manager y se muestran en la interfaz de usuario.

**Auto Tracing: Trace Cache Hits**

Número de seguimientos de la transacción automáticos que se envían desde un agente descendente por intervalo de 15 segundos.

**Auto Tracing: Trace Cache Misses**

Número de identificadores del seguimiento que no coincidan con los identificadores de una memoria caché interna por intervalo de 15 segundos.

**Auto Tracing: Upstream GUID Count Per Interval**

Número de identificadores del seguimiento ascendentes agregados a una memoria caché interna por intervalo de 15 segundos.

**Instrumentation Level: Number Of Candidate Classes For Reinstrumentation**

Número total de clases que se pueden volver a cargar después de aplicar un cambio de nivel en la instrumentación inteligente. Este número no cambia cuando Introscope está procesando un cambio de nivel. El número se convierte en cero cuando termina el procesamiento.

**Instrumentation Level: Current Instrumentation Level**

El nivel actual de la instrumentación inteligente. Valores: 1 = bajo, 2 = medio, 3 = alto. Cuando Introscope procesa un cambio del nivel X al nivel Y, el valor de la métrica muestra el nivel X hasta que finalice el procesamiento.

**Métricas de sostenibilidad de la detección de puntos de entrada****Entry Point Detection: Analyzed Stack Snapshots**

Número total de pilas de subprocesos que se analizan para los candidatos de punto de entrada después de iniciar la aplicación monitorizada.

**Entry Point Detection: Candidates Discarded**

Número total de candidatos de punto de entrada de los que se realiza un seguimiento y que se descartan como inadecuados antes de convertirse en puntos de entrada.

**Entry Point Detection: Entry Points Discarded**

Número de puntos de entrada que el agente ha descartado como inadecuados. Estos puntos de entrada se omiten permanentemente.

**Entry Point Detection: Entry Points Discovered**

Número de puntos de entrada que este agente ha detectado después de iniciar la aplicación monitorizada.

**Entry Point Detection: Initial Candidates Current**

Número actual de candidatos de punto de entrada que el agente ha encontrado, pero que el motor de reglas todavía no ha procesado.

**Entry Point Detection: Initial Candidates Total**

Número total de candidatos de punto de entrada que el agente ha encontrado después de iniciar la aplicación monitorizada.

**Entry Point Detection: Stack Snapshot Queue Length**

Número actual de instantáneas recopiladas de la pila de subprocesos que están en espera para ser analizadas para ver si son candidatos de punto de entrada.

**Entry Point Detection: Total Entry Points**

Número total de puntos de entrada en AutoPersist.pbd.

**Entry Point Detection: Total Entry Points Discarded**

Número total de puntos de entrada prohibidos y omitidos que se mantienen en AutoPersist.pbd.

**Entry Point Detection: Tracked Candidates Current**

Número actual de candidatos de punto de entrada de los que el agente realiza el seguimiento para obtener un rendimiento adecuado.

**Entry Point Detection: Tracked Candidates Total**

Número total de candidatos de punto de entrada de los que el agente realiza el seguimiento después de iniciar la aplicación monitorizada.

**Entry Point Detection: Tracked Threads**

Número actual de subprocesos de los que el agente realiza el seguimiento para la detección de un posible punto de entrada.

**Métricas de sostenibilidad de la detección automática de back-ends****Automatic Backend Detection: Analyzed Stack Snapshots**

Número total de instantáneas de la pila analizadas para los candidatos de back-end después de iniciar la aplicación monitorizada.

**Automatic Backend Detection: Backends Discovered**

Número total de back-ends que el agente ha detectado después de iniciar la aplicación monitorizada.

**Automatic Backend Detection: Backends Persisted**

Número total de back-ends que persisten en AutoPersist.pbd.

**Métricas de sostenibilidad de las extensiones**

Las métricas de sostenibilidad de las extensiones se encuentran en el subnodo **Extension Bundles**, que se encuentra en el subnodo **Sustainability**. Las métricas de las extensiones proporcionan información sobre las extensiones del agente. Las métricas proporcionan datos sobre la implementación, la carga y la descarga de las extensiones.

## **Métricas específicas de la implementación de extensiones**

### **Deployment|Count|All Cycles:Count**

El número total de ciclos de la implementación que se han producido después de iniciar el agente. Cada ciclo empieza por adquirir un bloqueo de implementación y termina con la liberación del bloqueo.

### **Deployment|Count|Failed Cycles:Count**

Número total de ciclos de la implementación en los que se ha producido un error después de iniciar el agente. Cada ciclo empieza por adquirir un bloqueo de implementación y termina con la liberación del bloqueo. Se pueden producir errores en los ciclos de la implementación por varias razones. Por ejemplo, descompresión de archivos .tar propensos a los errores, supresión de archivos .tar, cálculo de la suma de comprobación, etcétera.

Un valor mayor de cero y creciente indica que el implementador de la extensión tiene dificultades para descomprimir una o más extensiones.

### **Deployment|Count|Successful Cycles:Count**

Número total de ciclos de la implementación correctos después de iniciar el agente. Cada ciclo empieza por adquirir un bloqueo de implementación y termina con la liberación del bloqueo. Idealmente, este valor es igual al valor de la métrica All Cycles Count.

### **Deployment|Current Cycle|Status**

Estado del subproceso `ExtensionDeployer` que se ejecuta para implementar y anular la implementación de extensiones del archivo .tar en el directorio `<Agent_Home>/extensions/deploy/`. Esta métrica tiene dos valores: 0 indica que la extensión se ha implementado y 1 significa que la extensión se está implementando. Lo ideal es tener el valor 0, que indica el estado implementado. Cuando el valor de la métrica permanece en 1 durante más de unos minutos, significa que el subproceso `ExtensionDeployer` está interbloqueado. Investigue el subproceso y, a continuación, reinicie la aplicación monitorizada.

### **Deployment|Last Cycle|Time (milliseconds)**

Tiempo transcurrido en milisegundos para llevar a cabo el ciclo de la implementación `ExtensionDeployer` más reciente. Este valor es la cantidad de tiempo que se ha invertido entre adquirir y liberar el bloqueo de la implementación.

## **Métricas de carga de la extensión**

### **Failed: Count**

Número total de extensiones que no se han podido cargar. Este error se debe a cualquier combinación defectuosa de PBD, archivos JAR u otros artefactos de extensión opcionales.

Un valor mayor de 0 significa que no se ha podido cargar la extensión, probablemente debido a un conflicto de PBD.

### **Loaded: Count**

Número total de extensiones que se han cargado correctamente.

### **Total: Count**

Número total de extensiones del agente en el `<Directorio_principal_agente>/extensions`.

## **Métricas de sostenibilidad de la fijación de JMX**

El subnodo **JMX Clamp** se encuentra bajo el subnodo **Sustainability**.

### **Clamp Status**

Cuando el valor de la propiedad `introscope.agent.jmx.clamp` está por encima del umbral, el valor es 1. Cuando el valor de la propiedad está por debajo del umbral, el valor es 0.

## **Métricas de la visibilidad del intervalo de tiempo de ejecución de la instrumentación inteligente**

El subnodo **Runtime Visibility** se encuentra bajo el subnodo **Sustainability**.

### Gaps Found Per Interval

Número de intervalos que la visibilidad del intervalo de tiempo de ejecución ha encontrado durante el intervalo. El intervalo está determinado por la propiedad `introscope.agent.deep.instrumentation.visibility.processor.interval`.

### Runtime Components Per Transaction

El promedio de los componentes de la visibilidad del intervalo de tiempo de ejecución por transacciones de 15 segundos.

### Methods Instrumented Per Interval

Número de métodos que la visibilidad del intervalo de tiempo de ejecución ha instrumentado durante el intervalo. El intervalo está determinado por la propiedad `introscope.agent.deep.instrumentation.visibility.processor.interval`.

### Methods Uninstrumented Per Interval

Número de métodos que la visibilidad del intervalo de tiempo de ejecución no ha instrumentado durante el intervalo. El intervalo está determinado por la propiedad `introscope.agent.deep.instrumentation.visibility.processor.interval`.

### Total Methods Instrumented

Número de métodos instrumentados actualmente mediante la visibilidad del intervalo de tiempo de ejecución.

## Métricas de sostenibilidad de SQL

El subnodo **SQL** se encuentra en el subnodo **Sustainability**.

### SQL: SQL Statement Count

Número actual de instrucciones SQL únicas para las cuales el Agente de SQL ha creado las métricas.

## Métricas de registro de sostenibilidad

Las métricas de registro de sostenibilidad se encuentran en el subnodo **Configuration** bajo el subnodo **Sustainability**. Estas métricas proporcionan recuentos de advertencias y errores notificados por el agente en el archivo de registro.

### AutoProbe Errors Count

Esta métrica tiene dos valores: 0 indica que no ha habido errores de AutoProbe; 1 indica que ha habido errores de AutoProbe notificados.

### Error Count

Número total de errores notificados por el agente en el archivo **IntroscopeAgent.log** desde que se ha iniciado el agente.

### Errors Per Interval

Número total de errores notificados por el agente en el archivo **IntroscopeAgent.log** en el intervalo de generación de informes actual.

### Warnings Count

Número total de advertencias notificadas por el agente en el archivo **IntroscopeAgent.log** desde que se ha iniciado el agente.

### Warnings Per Interval

Número total de advertencias notificadas por el agente en el archivo **IntroscopeAgent.log** en el intervalo de generación de informes actual.

## Métricas del Gestor de sobrecarga

Las métricas del Gestor de sobrecarga se encuentran bajo el subnodo **Sustainability**. Estas métricas indican si el agente está recopilando datos de monitorización en el servidor de aplicaciones. La propiedad que lo controla es la propiedad `introscope.agent.overhead.level`. Para obtener más información sobre esta propiedad, consulte [Propiedades del agente de Java](#).

## Modo de sobrecarga

El valor 1 indica una monitorización normal del agente en el servidor de aplicaciones. Un valor 0 indica ninguna monitorización del agente en el servidor de aplicaciones.

## Métricas relacionadas con la memoria

Informe sobre las métricas relacionadas con la memoria en la función Recopilación de elementos no utilizados.

### NOTE

- Todas las métricas que se enumeran se aplican de manera local en DX APM y solamente algunas de ellas se aplican a DX APMSaaS.
- Los recuentos de la instancia son especiales: estas métricas no aparecen de forma predeterminada. Los recuentos de la instancia están relacionados con la memoria (pero solo cuenta el número, no el tamaño) e informan sobre los datos de objetos transaccionales.

### Recopilación de elementos no utilizados

La recopilación de elementos no utilizados es la recuperación automática de la memoria dedicada a los objetos que ya no utiliza una aplicación. Cuando el proceso detecta un objeto que no se utiliza, se recupera la memoria. Cuando el proceso detecta un objeto que está todavía activo, se copia en un bloque de memoria de generación posterior. Cuando se rellenan los bloques de memoria de generación reciente, se produce la recopilación secundaria de elementos no utilizados. Los objetos activos se copian en el segundo bloque de memoria de espacio restante. Cuando este segundo espacio restante no sea suficiente para contener todos los objetos, los objetos activos también se copiarán en los espacios del bloque de la memoria principal.

La recopilación de elementos no utilizados podría realizarse con frecuencia con el fin de maximizar la cantidad de memoria recuperada. Sin embargo, este comportamiento requeriría demasiada sobrecarga destinada al proceso. Por el contrario, esta recopilación de elementos no utilizados dejaría muy poca memoria de no realizarse con suficiente frecuencia. Cuando se produjera el proceso de Recopilación de elementos no utilizados, también requeriría la ejecución de una sobrecarga significativa. Por lo tanto, la recopilación de elementos no utilizados es más eficaz cuando transcurre el período correcto entre las recopilaciones de elementos no utilizados menores. La eficiencia equilibra el número de objetos que se limpian con la cantidad de sobrecarga necesaria para limpiarlos.

En un proceso eficaz de recopilación de elementos no utilizados, los bloques de memoria de generación reciente tienen el tamaño adecuado. Si los bloques de memoria son demasiado pequeños, la recopilación automática ocurre con demasiada frecuencia. Si los bloques de memoria son demasiado grandes, se acumularán demasiados objetos sin utilizar. Esta acumulación hace que el proceso de recopilación de elementos no utilizados menos frecuente utilice demasiada sobrecarga al ejecutarse. La sobrecarga causaría un aumento en el porcentaje de tiempo que se invierte en la recopilación de elementos no utilizados.

- **Métricas de la memoria dinámica del Recopilador de elementos no utilizados:** Introscope realiza informes sobre las métricas de la memoria dinámica de Recopilación de elementos no utilizados de forma predeterminada. Esta métrica utiliza los bytes como unidad de medida.
- **Métricas del Monitor del Recopilador de elementos no utilizados:** Estas métricas proporciona información adicional sobre el uso de la memoria. Esta métrica no se recopila o notifica hasta que la activa un administrador.
- **Las métricas del sistema de archivos, UDP y sockets** son medidas del rendimiento de datos.

### Métrica de la memoria dinámica de Recopilación de elementos no utilizados

Esta métrica está activada de forma predeterminada.

- **Memoria dinámica de Recopilación de elementos no utilizados|Bytes en uso**

Memoria dinámica de Recopilación de elementos no utilizados|Bytes en uso informa sobre la cantidad de memoria que utilizan actualmente los objetos.

- **Memoria dinámica de Recopilación de elementos no utilizados|Bytes totales**

Memoria dinámica de Recopilación de elementos no utilizados|Bytes totales informa sobre la cantidad de memoria que JVM adjudica.

Compare esta métrica con la métrica Current Capacity (bytes), que está disponible cuando el Monitor de Recopilación de elementos no utilizados de DX APM está activado. La métrica Current Capacity proporciona información acerca de la cantidad de memoria que se confirma para todos los segmentos de memoria de JVM. La métrica Bytes Total proporciona la cantidad de memoria que se ha confirmado para la máquina virtual Java en total.

### **Métrica del Monitor de Recopilación de elementos no utilizados**

La métrica del Monitor de Recopilación de elementos no utilizados informa sobre los recopiladores de elementos no utilizados y bloques de memoria, ayudando a detectar problemas de memoria que afectan negativamente al rendimiento.

Las métricas del Monitor de Recopilación de elementos no utilizados aparece en el árbol Explorador de la métrica directamente debajo del nodo de **Memoria dinámica de Recopilación de elementos no utilizados**. La métrica se activa de forma predeterminada. Algunas de las métricas tienen umbrales preestablecidos que activan indicadores de alerta en la ficha **Descripción general del Monitor de Recopilación de elementos no utilizados**.

#### **NOTE**

Para obtener más información sobre las limitaciones del Monitor del Recopilador de elementos no utilizados y las JVM compatibles, consulte la Matriz de compatibilidad de productos.

### **Métricas genéricas**

Las métricas genéricas son las siguientes:

- **Política de Recopilación de elementos no utilizados**

Identifica los nombres de los elementos no utilizados para la máquina virtual de Java.

- **Tipo de máquina virtual de Java**

Identifica la máquina virtual de Java que se está monitorizando.

- **Porcentaje de memoria dinámica de Java utilizada**

Identifica el porcentaje de la memoria dinámica disponible que se utiliza en el equipo donde se ha implementado el agente.

- El umbral de advertencia es del 60 %.

- El umbral de riesgo es del 80 %.

De forma predeterminada, la máquina virtual aumenta o reduce la memoria dinámica en cada recopilación. Esta acción mantiene la proporción de espacio libre para los objetos activos dentro de un intervalo específico. El intervalo de destino se establece a través de los parámetros tal y como se muestra a continuación:

- `-XX:MinHeapFreeRatio=<minimum>`

- `-XX:MaxHeapFreeRatio=<maximum>`

El tamaño total se basa en `-Xms` y `-Xmx`.

A menudo, el tamaño predeterminado es demasiado pequeño.

#### **WARNING**

Mantenga la métrica en un 60 %. Si la métrica está por encima del 80 %, ajuste el tamaño de la memoria dinámica de JVM. Para conceder memoria suficiente y asequible para la máquina virtual, ajuste los parámetros `-Xms` y `-Xmx`.

Los valores predeterminados del intervalo de destino son el 30 % de mínimo y el 70 % de máximo. Las aplicaciones mayores a menudo producen algún problema con los valores predeterminados. Un problema podría ser un inicio lento, que se produce cuando la memoria dinámica inicial es pequeña y debe cambiarse de tamaño durante muchas recopilaciones. La configuración de los parámetros `-Xms` y `-Xmx` con el mismo valor aumenta la capacidad de



predicción eliminando la decisión de tamaño más importante de la máquina virtual. Por otro lado, la máquina virtual no puede compensar si se realiza una elección escasa.

Asegúrese de aumentar la memoria a medida que aumenta el número de procesadores, ya que la adjudicación se puede ejecutar en paralelo.

### **Métricas del recopilador de elementos no utilizados**

Las métricas del recopilador de elementos no utilizados son las siguientes:

- **Algoritmo de Recopilación de elementos no utilizados**  
Muestra el algoritmo de recopilación de elementos no utilizados para el gestor de la memoria correspondiente.
- **Invocación de la Recopilación de elementos no utilizados por intervalo**  
Muestra una métrica de recuento que informa sobre el número de recopilaciones de elementos no utilizados que se ha producido en cada intervalo de 15 segundos. La métrica se agrega y calcula desde el recuento total de invocación de la Recopilación de elementos no utilizados realizando el seguimiento de la diferencia entre el intervalo actual y el más reciente.  
Esta métrica indica la recopilación por intervalo que se realiza en el bloque de memoria. Si la métrica aumenta a lo largo del tiempo, se producen recopilaciones frecuentes en un bloque de memoria que no tiene el tamaño adecuado. Aumentar el tamaño del bloque de memoria ayuda a reducir la frecuencia de la recopilación de elementos no utilizados.
- **Recuento total de invocación de la Recopilación de elementos no utilizados**  
El número total de recopilaciones de elementos no utilizados que se han producido desde que se ha iniciado la JVM. Esta métrica indica el número de recopilaciones desde la hora de inicio del servidor. La métrica crece lentamente en intervalos regulares.  
Los picos de la métrica indican recopilaciones frecuentes que afectan al rendimiento general de la aplicación. Para reducir la frecuencia de las recopilaciones y aumentar el rendimiento, aumente el tamaño del bloque de memoria.
- **Tiempo de Recopilación de elementos no utilizados por intervalo (ms)**  
Muestra la cantidad de tiempo que ha tardado la Recopilación de elementos no utilizados durante el intervalo de 15 segundos. Esta métrica agregada se calcula a partir del tiempo total de la recopilación de elementos no utilizados realizando el seguimiento de la diferencia en el tiempo de la recopilación entre el intervalo actual y el más reciente. Durante su funcionamiento normal, esta métrica permanece constante o crece lentamente mientras aumenta el tiempo necesario para la recopilación de elementos no utilizados.  
Los drásticos aumentos indican un tiempo de ejecución lento de la aplicación mediante el aumento de los tiempos de pausa de la recopilación de elementos no utilizados. Para evitar este problema, configure la memoria máxima utilizando el indicador `-Xmx` con un valor óptimo. El ajuste correcto hace que se reduzcan los tiempos de pausa de la Recopilación de elementos no utilizados y que mejore su rendimiento. Si la memoria se establece demasiado alta, la frecuencia de la recopilación disminuye; y mejora su rendimiento/eficiencia. Sin embargo, la aplicación experimenta tiempos largos de pausa mientras el sistema intenta mantener un espacio de memoria dinámica demasiado grande. Un tamaño óptimo de la memoria dinámica garantiza tiempos bajos de pausa y de recopilación de elementos no utilizados.
- **Memory Reclaimed Per Interval**  
Calcula e informa de la cantidad de memoria en bytes reclamados por un recopilador de elementos no utilizados durante el intervalo actual. Cuando hay varias invocaciones de un recopilador de elementos no utilizados determinado, esta métrica muestra la suma de todas las memorias de invocaciones del recopilador de elementos no utilizados.
- **Percentage of Heap Used After GC Invocation**  
Calcula e informa sobre el porcentaje de memoria dinámica que ha utilizado la máquina virtual Java después del evento de recopilación de elementos no utilizados. La métrica muestra un valor de 0 para intervalos sin invocación de recopilación de elementos no utilizados. Cuando hay varias invocaciones de un recopilador de elementos no utilizados determinado en un intervalo, esta métrica muestra el porcentaje medio de la memoria dinámica de todas las invocaciones.

DX APM admite esta métrica en las versiones 1.7 y posteriores de la máquina virtual Java de Oracle.

- **Porcentaje de tiempo invertido en la Recopilación de elementos no utilizados durante los últimos 15 minutos**  
Muestra una métrica agregada que se calcula utilizando una calculadora de Enterprise Manager. El porcentaje de este valor se calcula mediante esta fórmula:

$$(\text{total GC time spent/length of time in ms}) * 100$$

Ejemplo de un intervalo de 15 minutos:

$$45600 / (15 * 60 * 1000) * 100 = 5 \%$$

Un aumento drástico del tiempo indica un tiempo de ejecución lento de la aplicación mediante el aumento de los tiempos de pausa de la recopilación de elementos no utilizados. Configure la memoria máxima utilizando el indicador `-Xmx` con un valor óptimo.

Una métrica constante con picos que se producen de repente indica que una recopilación única de elementos no utilizados ha tardado más tiempo de lo normal. Después de este aumento, la métrica vuelve a la normalidad y no es necesaria ninguna acción.

- **Tiempo total de la Recopilación de elementos no utilizados (ms)**

Muestra el tiempo total para el proceso de recopilación de elementos no utilizados, en milisegundos.

Durante su funcionamiento normal, la métrica aumenta de forma gradual.

Los drásticos aumentos del tiempo indican un tiempo de ejecución lento de la aplicación mediante el aumento de los tiempos de pausa de la recopilación de elementos no utilizados. Para evitar este problema, configure la memoria máxima utilizando el indicador `-Xmx` con un valor óptimo. El ajuste correcto hace que se reduzcan los tiempos de pausa de la Recopilación de elementos no utilizados y que mejore su rendimiento.

### **Activación y uso de métricas de la Recopilación de elementos no utilizados de Morel**

La recopilación de elementos no utilizados y la gestión de la memoria pueden tener un efecto significativo sobre el rendimiento de las aplicaciones. La métrica básica de la memoria dinámica de Recopilación de elementos no utilizados está disponible de forma predeterminada. Puede activar métricas opcionales para proporcionar más detalles sobre el uso del bloque de memoria y el procesamiento de la recopilación de elementos no utilizados. Estas métricas adicionales se muestran en el nodo del **monitor de recursos no utilizados** del Explorador de métrica cuando están activadas. La métrica del Monitor de Recopilación de elementos no utilizados proporciona información para ayudarle a optimizar la adjudicación del bloque de memoria y el procesamiento de la recopilación de elementos no utilizados. Por lo tanto, normalmente se activan estas métricas para un uso específico. Por ejemplo, al desarrollar o probar aplicaciones, o al investigar problemas de rendimiento de la aplicación. En muchos casos, las métricas no se utilizan para la gestión de aplicaciones en tiempo real en un entorno de producción y están desactivadas de forma predeterminada.

Cuando la propiedad `introscope.agent.gcmonitor.enable` se establece en `true` (valor predeterminado), puede ver detalles sobre los recopiladores de elementos no utilizados y bloques de memoria de la máquina virtual de Java que se está monitorizando.

### **Métricas del bloque de memoria**

Las métricas del bloque de memoria son las siguientes:

- **Cantidad de espacio utilizado (bytes)**

Muestra la cantidad de espacio de memoria utilizado. La cantidad incluye todos los objetos de la agrupación incluidos los objetos accesibles y los no accesibles.

Durante su funcionamiento normal, la métrica aumenta de forma gradual. La métrica puede reducirse cuando haya finalizado la recopilación de elementos no utilizados y se recupere la memoria.

Un aumento temporal que vuelve a la normalidad podría ser un mensaje de advertencia de los problemas de memoria.

En un rápido aumento la métrica puede alcanzar el límite de memoria máxima, lo cual produce excepciones de falta de memoria. Para evitar este problema, establezca el tamaño máximo del bloque de memoria en un valor más asequible.

- **Capacidad actual (bytes)**

La cantidad de memoria que se ha confirmado para esta agrupación; y todos los segmentos de memoria de JVM. Se garantiza esta cantidad de memoria para que la utilice la máquina virtual de Java.

#### NOTE

Al agregar todas las métricas de la capacidad actual de segmentos de memoria individuales se iguala aproximadamente la métrica Bytes Total (consulte [Métricas de la memoria dinámica del recopilador de elementos no utilizados](#)). Si la cantidad de espacio alcanza la capacidad actual, se producen excepciones de memoria. Para evitar este problema, planifique la necesidad de gestionar las operaciones diarias y los picos inesperados.

- **Tasa de crecimiento**

La tasa de crecimiento medio de la memoria utilizada, expresada en bytes por segundo; en un bloque de memoria, en bytes por segundo durante el último minuto. Esta métrica agregada se calcula de la siguiente manera:

- Buscando el último valor del punto de datos en bytes (lastValue).
- Buscando el primer valor del punto de datos en bytes (firstValue).

También incluye el espacio en el intervalo de 1 minuto más reciente. La tasa se calcula mediante esta fórmula:

```
(lastValue - firstValue) / 60
```

Esta métrica crece lentamente, permanece constante o disminuye si la memoria sin utilizar se devuelve a la agrupación.

Un aumento drástico de 15 minutos o más indica que la memoria no se ha reciclado después de la recopilación de elementos no utilizados. Este comportamiento indica una posible pérdida de memoria. Es necesario realizar una investigación.

- **Capacidad máxima (bytes)**

La cantidad máxima de memoria (en bytes) utilizada para la gestión de la memoria. Esta cantidad de memoria no se garantiza que esté disponible para la gestión de la memoria si es mayor que la capacidad actual (cantidad de memoria confirmada).

Esta métrica permanece constante a lo largo del tiempo.

- **Tipo de memoria**

Tipo de memoria; una de las siguientes:

- Memoria dinámica
- No dinámica

- **Porcentaje de capacidad máxima utilizada actualmente**

Muestra la representación del porcentaje de uso de la memoria actual (por encima de la cantidad máxima). Esta métrica indica el porcentaje de memoria que se utiliza a lo largo del tiempo.

Esta métrica crece lentamente, permanece constante o disminuye si la memoria sin utilizar se devuelve a la agrupación.

Si la métrica supera el 70-80%, establezca la memoria máxima en un valor óptimo y superior.

## **Sistema de archivos, sockets, UDP**

Como las respuestas por intervalo, las métricas del sistema de archivos, socket y UDP son medidas del rendimiento de datos. Se miden en bytes por segundo:

### **Sistema de archivos**

- Tasa de salida del archivo (bytes por segundo)
- Tasa de entrada del archivo (bytes por segundo)

### **UDP (Protocolo de datagramas de usuario)**

- Ancho de banda de salida (bytes por segundo)
- Ancho de banda de entrada (bytes por segundo)

### **Sockets (el total, así como información específica del host/puerto)**

- Ancho de banda de salida (bytes por segundo)
- Ancho de banda de entrada (bytes por segundo)

Un gran número de métricas relacionadas con el puerto indica que las métricas de la tasa del socket se deben desactivar, debido a que esta situación es posiblemente un problema de expansión de la métrica.

### **Recuentos de la instancia**

La métrica de recuentos de la instancia mide el número de instancias del objeto de una clase concreta en la memoria dinámica.

- Recuento aproximado de la instancia por nombre de paquete y de clase

## **Métricas de compatibilidad del clúster**

Un clúster integra los recursos de dos o más dispositivos informáticos (que pueden funcionar por separado) juntos para un fin común. El agrupamiento en clúster permite a Enterprise Manager gestionar otros Enterprise Manager o a servir como Manager of Managers (MOM). APM mide la compatibilidad de las aplicaciones midiendo el rendimiento de los distintos componentes de la aplicación y proporciona las siguientes métricas:

Los siguientes datos se notifican para el equipo que hospeda Enterprise Manager y para cada equipo con los métodos instrumentados.

- Host de EM: nombre de host del servidor de Enterprise Manager
- Puerto de EM: puerto de Enterprise Manager al que está conectado el agente
- Java Version

Las métricas de compatibilidad muestran información acerca de Enterprise Manager en lugar de la aplicación que se está monitorizando. Estas métricas aparecen en el árbol de Investigator, en:

Custom Metric Host (Virtual)

Custom Metric Process (Virtual)

Custom Metric Agent (Virtual)(SuperDomain)

Debajo de este nivel, las métricas de compatibilidad se organizan según la siguiente jerarquía. Las definiciones de algunas de estas métricas siguen la lista.

### **Nodo del agente**

Los agentes tienen la jerarquía siguiente:

```
<Host_Name>
 <Process_Name>
 <Agent_Name>
```

<Nombre\_proceso> y <Nombre\_agente> se pueden configurar en IntroscopeAgent.profile.

Para cada <Nombre\_agente>, se encuentran disponibles las siguientes métricas:

- ConnectionStatus, con uno de los siguientes valores:
  - 3 = desconectado
  - 2 = conectado, ritmo lento o sin datos
  - 1 = conectado
  - 0 = desmontado
- IsClamped, con uno de los siguientes valores:

- 1 = Fijado
- 0 = Sin fijar

**Nota:** Para obtener más información sobre la fijación de métricas, consulte [Uso del Visor de seguimiento de transacciones](#).

- Recuento de métricas
- Raw Metric Count

### **Calculadora de conectividad del agente**

La calculadora de conectividad del agente copia el estado de conectividad del agente en una ubicación fija. Actualmente, el estado se almacena en la carpeta Collectors, pero cuando el agente se vuelve a conectar a un recopilador diferente, la métrica continúa recopilándose en una carpeta diferente. En este caso, la calculadora de conectividad del agente copia todos los estados de la carpeta Collectors en la carpeta MOM, un único lugar permanente.

#### **NOTE**

La calculadora de conectividad del agente está desactivada de forma predeterminada y el administrador debe activarla en la instancia de MOM y reiniciar MOM estableciendo la propiedad `introscope.apm.calculator.agentconnectivity.enabled=true`

La calculadora genera las siguientes métricas en `Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|<NombreAgente>`:

- Uptime: un valor que aumenta regularmente y que es útil para ver cuándo se conecta exactamente el agente. Baja a 0 cuando el agente se desconecta.
- Metrics: el número de métricas sin formato que proporciona un agente.
- ConnectionState: la conectividad del agente. Puede ser cualquiera de los siguientes valores enteros:
  - 4 - Alive, el agente está conectado y envía métricas.
  - 5 - Stopped, el agente se ha detenido correctamente.
  - 6 - Reconnected, el agente ha cambiado a un recopilador diferente.
  - 7 - Interrupted, el agente no se ha desconectado correctamente, pero APM no recibe ninguna métrica del mismo.
  - 8 - AgedOut, el agente se ha detenido o se ha interrumpido durante más de 24 horas.

La calculadora también genera un pequeño resumen de los recuentos del agente para cada `ConnectionState` en `Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Agents|Agent States`.

### **Métricas del agente**

#### **<Nombre\_agente> | ErrorSnapshot Events Per Interval**

El número total de eventos de instantáneas de error por agente y por intervalo.

### **Nodo de Enterprise Manager**

En el nodo de Enterprise Manager, están disponibles las siguientes métricas de compatibilidad:

- Host
- Name
- Overall Capacity (%)
- Port
- CPU
  - EM CPU Used (%)
- Configuration

- Agent Clusters Metric Load
- Number of Agent Clusters
- Number of Map Entity Metric Groupings
- Number of Metric Groupings
- Conexiones
  - Disallowed Agents Clamped: indica si se ha excedido el número máximo de agentes no permitidos conectados al MOM, al recopilador o a la instancia independiente de Enterprise Manager. Si el valor es 0, la fijación no ha surtido efecto. Si el valor es 1, la fijación ha surtido efecto.
  - EM Historical Metric Clamped
  - EM Live Metric Clamped
  - Métrica Max Number of Agent Connection Limit Exceeded Per Interval: indica si se ha excedido el número máximo de agentes conectados al MOM, al recopilador o a la instancia independiente de Enterprise Manager. Si el valor es 0, la fijación no ha surtido efecto. Si el valor es 1, la fijación ha surtido efecto.
  - Metrics From External Agents: muestra el recuento de métricas del Enterprise Manager que generan los agentes virtuales del Enterprise Manager.
  - Metrics Queued (%)
  - Number of Agents
  - Number of Applications: el número de aplicaciones del agente que actualmente informan sobre datos.
  - Number of Disallowed Agents: Muestra el número de agentes no permitidos que están conectados a un MOM, un recopilador o una instancia independiente de Enterprise Manager. Los agentes conectados de forma pasiva no envían datos de métrica.
  - Number of Events Processed
  - Number of Events Processed Limit Exceeded
  - Number of Metrics Handled: el número de métricas entrantes procesadas durante un intervalo de 15 segundos. Este número varía, pero puede estar alrededor del mismo valor que el de Number of Metrics. Un valor inferior a Number of Metrics indica que Enterprise Manager puede estar sobrecargado y que no está procesando los datos entrantes lo suficientemente rápido.
  - Number of Metrics: muestra la carga de métrica total en Enterprise Manager.
  - Number of Unique Applications
  - Number of Workstations

### **Nodo del almacén de datos**

En el nodo del almacén de datos, las siguientes métricas están disponibles:

- SmartStor
  - Metrics Appended To Query Per Interval
  - Metrics Converted From Spool to Query Per Interval
  - SmartStor Disk Usage (mb)
  - MetaData
    - Agent Metric Cache Size  
El número de métricas del agente en la memoria caché.
  - Tareas
    - Converting Spool To Data
    - Data Append
    - Reperiodizing
- Transacciones
  - 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)

### **Subnodo del estado**

- CPU Capacity (%): Porcentaje de las CPU utilizadas. Por ejemplo, 300 % significa que tres núcleos de la CPU están completamente utilizados.
- GC Capacity (%)
- Harvest Capacity (%)
- Heap Capacity (%)
- Incoming Data Capacity (%)
- SmartStor Capacity (%)

### **Subnodo interno**

Las siguientes métricas aparecen en el subnodo interno:

- Number of Connection Tickets
- Number of Dependent Calculator Input Metrics  
El número total de métricas que son entradas para las calculadoras dependientes. Las calculadoras dependientes se utilizan para entrar los valores de métricas que producen otras calculadoras. Este recuento hace referencia a todas las métricas dadas a las calculadoras dependientes, no solo a las métricas que producen otras calculadoras.
- Number of Non-Dependent Calculator Input Metrics  
El número total de métricas que son entradas para las calculadoras no dependientes. Las calculadoras no dependientes no utilizan valores de métricas que producen otras calculadoras. Por ejemplo, las métricas que vienen de los 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
  - *<Nombre\_módulo\_gestión>*
    - Agent Connection Status
      - Number of Evaluated Metrics
  - Total Number of Evaluated Metrics  
El número total de métricas que se evalúan para todas las alertas.
- Calculadoras
  - Total Number of Evaluated Metrics  
El número total de métricas que se evalúan para todas las calculadoras. Esta métrica es la suma del número de métricas de entrada de la calculadora dependiente y del número de métricas de entrada de la calculadora no

dependiente. Cuando este recuento sube, Enterprise Manager está realizando muchos cálculos en tiempo real, lo que puede sobrecargar los recursos de la CPU.

- <nombre calculadora> | Total Number of Evaluated Metrics  
El número total de métricas que se evalúan para una única calculadora.

#### NOTE

Esta métrica solo aparece en Investigator cuando se define la calculadora.

- GC Heap
  - Recopiladores
    - <Nombre\_recopilador>
      - Collection Count Per Interval
      - GC Duration (ms)
  - Agrupaciones
- Harvest
  - Alert Action Processing Time (ms)  
Tiempo transcurrido que Enterprise Manager tarda en procesar todas las acciones de la alerta.
  - Calculator Queries Wait Time (ms)  
Tiempo transcurrido para que el subproceso de las consultas de la calculadora finalice su trabajo actual, incluida la espera a que finalice el bucle de consulta que no es de la calculadora. El nuevo procesamiento de consultas de la calculadora se inicia después de que se completen todas las entregas que no son de la calculadora del intervalo de tiempo anteriores a los clientes.
  - Non Calculator Queries Delivery Time (ms)  
Tiempo que Enterprise Manager ha tardado en ejecutarse y entregar consultas que no son de la calculadora a todos los clientes solicitantes en un intervalo de tiempo.  
Después de ejecutar todas las consultas de la calculadora, Enterprise Manager ejecuta consultas que no son de la calculadora y envía los resultados a todos los clientes que las han solicitado.
  - Non Calculator Queries Excess Time (ms)  
Tiempo de espera excesivo para que las consultas que no son de la calculadora se completen más allá de un intervalo de tiempo.  
Los clientes envían solicitudes de consulta que no son de la calculadora a Enterprise Manager, que devuelve los resultados. Si este proceso no finaliza en un intervalo de tiempo, se llevará a cabo hasta que se complete. Esta métrica muestra cuánto tiempo se han ampliado las consultas que no son de la calculadora más allá de un intervalo de tiempo.
  - Metrics From All Agents  
El número total de métricas únicas generadas por todos los agentes conectados que han enviado datos en el último intervalo de tiempo. Este recuento no incluye métricas históricas. La configuración de la fijación no afecta a este recuento.
  - Spooling Data File Write Time (ms)  
El tiempo que Enterprise Manager ha tardado en escribir los datos recolectados en el archivo de trabajos en cola (.spool) en un intervalo de tiempo.
  - Spooling Preparation Time (ms)  
El tiempo que Enterprise Manager ha tardado en preparar los datos recolectados para guardarlos en el archivo de trabajos en cola (.spool) en un intervalo de tiempo.
- Calculadora del módulo de gestión
  - Total Number of Evaluated Metrics  
El número de métricas que son la entrada de las calculadoras del módulo de gestión.
- Mensajería
  - Active Incoming Threads
  - Active Outgoing Threads
  - Corrupted Messages Per Interval
  - Post Offices



- *<Nombre\_oficina\_postal>*
  - Number of Mailboxes
  - Queued Messages
- Grupo de métricas
  - Metric Matches Per Interval  
El número total de métricas que se han evaluado en todas las consultas en el último intervalo de tiempo.
  - Queued Queries Per Interval  
El número de consultas que actualmente están a la espera de procesamiento en el intervalo del ciclo de recolección. En general, el valor es cero después del inicio.
- Consulta
  - Cache Queries Duration (ms)
  - Cache Queries Per Interval
  - SmartStor Queries Duration (ms)
  - SmartStor Queries Per Interval
- Subprocesos
  - *<Nombre\_subproceso>*
    - Blocked Count
    - Blocked Time (ms)
    - CPU Time (ms)
    - User Time (ms)
    - Wait Count
    - Wait Time (ms)

### **Subnodo de problemas**

Módulos de gestión

- Warning Count

### **Subnodo de tareas**

Harvest Duration (ms)

SmartStor Duration (ms)

### **Métricas de recolección**

#### **Harvest Capacity**

La métrica Harvest Capacity muestra el porcentaje de tiempo necesario para la recolección de datos en un intervalo de tiempo de 15 segundos. Por ejemplo, si la recolección de datos tarda 15 segundos, el valor de la métrica será 100. Investigator muestra esta métrica en la ubicación.

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Health | Harvest Capacity (ms)
```

#### **Harvest Duration**

La métrica Harvest Duration muestra el tiempo en milisegundos (durante un intervalo de tiempo de 15 segundos) invertido en la recolección de datos. Por lo general, la métrica es un buen indicador para determinar si Enterprise Manager está manteniendo el rendimiento con la carga de trabajo actual. Se puede encontrar esta métrica en la siguiente ubicación en el árbol de Investigator.

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Tasks | Harvest Duration (ms)
```

## Incoming Data Capacity (%)

La capacidad de Enterprise Manager para gestionar los datos entrantes. La métrica se calcula multiplicando la capacidad total de la métrica por 2. Por ejemplo, si 150000 métricas están en cola a la espera de ser procesadas y Enterprise Manager tiene una capacidad para gestionar 300000 métricas, el valor de Incoming Data Capacity es del 25 %.

Se puede encontrar esta métrica en la siguiente ubicación en el árbol del Explorador de métricas:

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Health | Incoming Data Capacity (%)
```

## Métricas del recopilador

Las siguientes métricas son métricas del recopilador.

- **EM Live Metric Clamped**

Indica si el número de métricas en directo que gestiona Enterprise Manager es menor o mayor que el límite máximo especificado en la propiedad `introscope.enterprisemanager.metrics.live.limit` para las fijaciones de Enterprise Manager. El valor de la métrica es 0 si el número de métricas en directo para Enterprise Manager es menor que el límite especificado. El valor de la métrica es 1 si el número de métricas en directo para Enterprise Manager es mayor que el límite especificado.

### NOTE

Se puede definir el límite de fijación para la propiedad `introscope.enterprisemanager.metrics.live.limit` en el archivo `apm-events-thresholds-config.xml`. El archivo `apm-events-thresholds-config.xml` se encuentra en el directorio `<EM_Home>\config`.

- **EM Historical Metric Clamped**

Indica si el número de métricas en directo que gestiona Enterprise Manager es menor o mayor que el límite máximo especificado en la propiedad `introscope.enterprisemanager.metrics.historical.limit` para las fijaciones de Enterprise Manager. El valor de la métrica es 0 si el número de métricas en directo para Enterprise Manager es menor que el límite especificado. El valor de la métrica es 1 si el número de métricas en directo para Enterprise Manager es mayor que el límite especificado.

### NOTE

Se puede definir el límite de fijación para la propiedad `introscope.enterprisemanager.metrics.historical.limit` en el archivo `apm-events-thresholds-config.xml`. El archivo `apm-events-thresholds-config.xml` se encuentra en el directorio `<EM_Home>\config`.

- **Max Number of Agent Connection Limit Exceeded Per Interval**

El número de veces que se ha excedido el límite de fijación definido en la propiedad `introscope.enterprisemanager.agent.connection.limit` para un intervalo determinado.

### NOTE

Se puede definir el límite de fijación para la propiedad `introscope.enterprisemanager.agent.connection.limit` en el archivo `apm-events-thresholds-config.xml`. El archivo `apm-events-thresholds-config.xml` se encuentra en el directorio `<EM_Home>\config`.

- **Number of Events Processed**

Indica el número total de todos los eventos como los seguimientos de transacciones y los errores que Enterprise Manager procesa en cada intervalo.

- **Number of Events Processed Limit Exceeded**

El número de veces que se ha excedido el límite de fijación definido en la propiedad `introscope.enterprisemanager.events.limit` para un intervalo determinado.

**NOTE**

Se puede definir el límite de fijación para la propiedad `introscope.enterprisemanager.events.limit` en el archivo `apm-events-thresholds-config.xml`. El archivo `apm-events-thresholds-config.xml` se encuentra en el directorio `<EM_Home>\config`.

**Métricas de la consulta****Data Points Retrieved From Disk Per Interval**

El número de puntos de datos que se recuperan de SmartStor por intervalo.

**Data Points Returned Per Interval**

El número de puntos de datos que Enterprise Manager ha devuelto a los clientes por intervalo.

**Metrics Read From Disk Per Interval**

El número de métricas que se leen de SmartStor por intervalo.

**Metrics Returned Per Interval**

El número de métricas únicas que Enterprise Manager ha devuelto a los clientes.

**Queries Exceeding Max Data Points Read From Disk Limit Per Interval**

Indica si se excede el número máximo de puntos de datos de la métrica especificado en la propiedad `introscope.enterprisemanager.query.datapointlimit` que Enterprise Manager devuelve para una consulta por lotes concreta. Si el número de puntos de datos de la métrica que devuelve Enterprise Manager es menor que el límite especificado, el valor de la métrica es 0. Si el número de puntos de datos de la métrica que devuelve Enterprise Manager excede el límite especificado, el valor de la métrica es 1.

**NOTE**

Defina el límite de fijación para

```
introscope.enterprisemanager.query.datapointlimit
```

la propiedad en el

```
IntroscopeEnterpriseManager.properties
```

archivo. Busque el

```
IntroscopeEnterpriseManager.properties
```

archivo en el directorio

```
<EM_Home>\config
```

.

**Queries Exceeding Max Data Points Returned Limit Per Interval**

Indica si se excede el número máximo de puntos de datos de la métrica especificado en la propiedad `queryintroscope.enterprisemanager.query.returneddatapointlimit` que Enterprise Manager devuelve para una consulta por lotes concreta. Si el número de puntos de datos de la métrica que devuelve Enterprise Manager es menor que el límite especificado, el valor de la métrica es 0. Si el número de puntos de datos de la métrica que devuelve Enterprise Manager excede el límite especificado, el valor de la métrica es 1.

**NOTE**

Defina el límite de fijación para

```
introscope.enterprisemanager.query.returneddatapointlimit
```

la propiedad en el

```
IntroscopeEnterpriseManager.properties
```

archivo. El

```
IntroscopeEnterpriseManager.properties
```

archivo se encuentra en el directorio

```
<EM_Home>\config
```

### Métrica Converting Spool to Data

La métrica Converting Spool to Data realiza un seguimiento de si la tarea de conversión de spool a datos se está ejecutando. Se puede encontrar esta métrica en la siguiente ubicación en el árbol de Investigator:

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Data Store | SmartStor | Tasks | Converting Spool to Data
```

Si esta métrica permanece en 1 durante más de 10 minutos por hora, esta métrica indica que la reorganización del archivo de spool de SmartStor está tardando demasiado tiempo.

### Métrica Overall Capacity (%)

La métrica Enterprise Manager Overall Capacity (%) estima el porcentaje de la capacidad de Enterprise Manager que se consume. Se puede encontrar en esta ubicación en el árbol de Investigator:

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager: Overall Capacity (%)
```

Overall Capacity (%) es un valor máximo de CPU Capacity (%), Harvest Capacity (%), Heap Capacity (%), SmartStor Capacity (%), Incoming Data Capacity (%) y GC Capacity (%).

### Métrica SmartStor Capacity (%)

La métrica SmartStor Capacity (%) muestra el porcentaje de tiempo necesario para el proceso de escritura de SmartStor durante un intervalo de tiempo de 15 segundos, donde 15 segundos equivale al 100 %.

Se puede encontrar en esta ubicación en el árbol de Investigator:

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Health | SmartStor Capacity (%)
```

### Métrica Heap Capacity (%)

La métrica Heap Capacity (%) está determinada por el porcentaje de memoria dinámica que está utilizando la máquina virtual Java (en función de la memoria dinámica de GC: métrica In Use Post GC (mb)).

### Métrica Number of Agents

Esta métrica muestra el número de agentes conectados actualmente. La ubicación de la métrica es la siguiente:

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Connections
```

### Number of Metrics

Esta métrica muestra la carga de métrica total en Enterprise Manager. La ubicación de la métrica es la siguiente:

```
Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SuperDomain*) |
Enterprise Manager | Connections
```

## Métricas de compatibilidad de la evaluación de errores asistida

APM proporciona métricas de compatibilidad de la evaluación de errores asistida mediante la medición del rendimiento de los distintos componentes de la aplicación de evaluación de errores asistida. Enterprise Manager genera y recopila métricas sobre los componentes de la evaluación de errores asistida. Estas métricas de compatibilidad son útiles para evaluar el estado de Enterprise Manager.

**Nota:** Para obtener más información sobre la evaluación de errores asistida, consulte [Monitorización de problemas y anomalías en la evaluación de errores asistida](#).

### Monitorización del rendimiento del componente de evaluación de errores asistida

Las métricas de compatibilidad de la evaluación de errores asistida permite monitorizar el rendimiento de los distintos componentes de la evaluación de errores asistida.

Pueden aparecer otras métricas, por ejemplo:

- Métricas para eventos del Análisis diferencial que se crean cuando la intensidad de la variación supera un valor determinado
- Métricas para eventos de error que se crean cuando la evaluación de errores asistida recibe un error de instantánea o de detención

#### Siga estos pasos:

1. En APM Team Center, haga clic en el vínculo **WebView**.
  2. Haga clic en la ficha **INVESTIGATOR**.
  3. Expanda el nodo de dominio de interés.
  4. Vaya al nodo **Enterprise Manager, Evaluación de errores asistida**.
  5. Expanda un nodo de interés como, por ejemplo, **Generador de eventos**.
- A continuación aparecen las métricas de compatibilidad para el Generador de eventos:

DA : Average Processing Time (ms)

Esta métrica proporciona el tiempo medio de procesamiento en milisegundos de los eventos del Análisis diferencial (DA) que ha recibido el procesador de eventos de la evaluación de errores asistida.

### Generador de eventos

La evaluación de errores asistida utiliza generadores de eventos que generan eventos y que dependen de diferentes tipos de fuentes. Por ejemplo, una fuente son las alertas de APM que los administradores definen en los módulos de gestión. Los ejemplos de eventos incluyen lo siguiente:

- Eventos del Análisis diferencial que se crean cuando la intensidad de la variación excede un valor determinado
- Eventos de error y de detención

APM proporciona las siguientes métricas para monitorizar el componente del generador de eventos. Estas métricas aparecen en el nodo Event Generator en Investigator:

Enterprise Manager | Assisted Triage | Event Generator | <Metric>

- **DA : Average Processing Time (ms)**  
Proporciona el tiempo medio de procesamiento en milisegundos de los eventos del Análisis diferencial (DA) que ha recibido el procesador de eventos de la evaluación de errores asistida.
- **DA : Raw States Received Per Interval**  
Proporciona el número de eventos del Análisis diferencial (DA) que el procesador de eventos de la evaluación de errores asistida ha recibido por intervalo.
- **DA : Events Sent Per Interval**

Proporciona el número de eventos agregados del Análisis diferencial (DA) que se envían de nuevo al procesador de eventos del Análisis diferencial.

- **Alert : Average Processing Time (ms)**  
Proporciona el promedio de tiempo de procesamiento en milisegundos de todos los eventos de alerta que procesó el generador de alertas.
- **Alert : Raw Alert States Received Per Interval**  
Proporciona el número de alertas recibidas por el intervalo por el generador de alertas.
- **Alert : Events Sent Per Interval**  
Proporciona el número de eventos de alerta agregados que se envían de nuevo a los procesadores de eventos de la evaluación de errores asistida.

## Métricas de compatibilidad principales

Las métricas de compatibilidad ayudan a evaluar los problemas de rendimiento que implican a Enterprise Manager (EM). Las siguientes cinco métricas de compatibilidad suelen causar problemas de rendimiento en diversos entornos de APM.

### SmartStor Duration (ms)

**Nombre de la ruta de la métrica:** SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Enterprise Manager|Tasks:Smartstor Duration (ms)

**Descripción:** La cantidad de tiempo que EM o el recopilador tardan en guardar los datos recopilados en el disco.

**Producto:** APM

**Componente:** Enterprise Manager

**Versión:** Todas las versiones admitidas

**Impacto:** Si esta métrica excede 1 segundo, significa que posiblemente EM o los recopiladores están experimentando problemas de rendimiento relacionados con la E/S. Si la métrica es superior a 3,5 segundos, pueden retrasarse otras tareas dentro de EM o del recopilador.

**Configuración:** Configure un disco (controlador) independiente para los datos de SmartStor editando la propiedad `introscope.enterprisemanager.smartstor.directory` en el archivo `config/IntroscopeEnterpriseManager.properties`.

**Intervalo:** Correcto: <1000 ms, Peligro: >3500 ms, Peligro extremo: >15 s

**Reparación:** Cada base de datos de SmartStor debe residir en un disco físico dedicado diferente. Se recomienda encarecidamente tener una unidad de estado sólido (SSD) con una velocidad de lectura/escritura de 220 MBPS con un tamaño de bloque de 4 k.

### Harvest Duration (ms)

**Nombre de la ruta de la métrica:** SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Enterprise Manager|Tasks:Harvest Duration (ms)

**Descripción:** La cantidad de tiempo que EM o el recopilador tardan en agregar métricas de intervalo de 15 segundos para prepararlas para escribirlas en la base de datos de SmartStor.

**Producto:** APM

**Componente:** Enterprise Manager

**Versión:** Todas las versiones admitidas

**Impacto:** Si esta métrica excede 1 segundo, significa que posiblemente la instancia de EM en las instancias de MOM y de los recopiladores está experimentando problemas de rendimiento. Compruebe los valores para Enterprise

Manager|Internal|Calculators:Total Number of Evaluated Metrics y Enterprise Manager|Internal:Number of [Non] Dependent Calculator Input Metric . Si los valores son superiores a 3,5 segundos, pueden retrasarse otras tareas dentro de EM o del recopilador.

### Configuración:

- Compruebe los siguientes recuentos de métricas para evaluar si el número de métricas está sobrecargando la instancia de 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
- Reduzca el número de métricas en alertas y calculadoras.

**Intervalo:** Correcto: <1000 ms, Peligro: >3500 ms, Peligro extremo: >15 s

**Reparación:** Reduzca los componentes siguientes:

- Métricas en alertas y calculadoras
- Consultas CLW
- Conexiones de Workstation

### GC Duration (ms)

**Nombre de la ruta de la métrica:** SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Enterprise Manager|ApplicationTriageMap|Ontology engine:Average Process Time (ms)

**Descripción:** La cantidad de tiempo que pasa la máquina virtual Java liberando la memoria sin usar (recopilación de elementos no utilizados) en un intervalo de 15 segundos.

**Producto:** APM

**Componente:** Enterprise Manager

**Versión:** Todas las versiones admitidas

**Impacto:** Si esta métrica excede 1 segundo, significa que posiblemente la instancia de EM en las instancias de MOM y de los recopiladores está experimentando problemas de rendimiento. Es posible que desee aumentar el tamaño de la memoria dinámica y cambiar la configuración o los algoritmos de la recopilación de elementos no utilizados (GC).

**Intervalo:** Correcto: <1000 ms, Peligro: >3500 ms

**Reparación:** Póngase en contacto con Soporte de CA.

### Ontology Engine:Average Process Time (ms)

**Nombre de la ruta de la métrica:** SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)|Enterprise Manager|ApplicationTriageMap|Ontology engine:Average Process Time (ms)

**Descripción:** La cantidad de tiempo que tarda EM en procesar los cambios en el mapa de topología en un intervalo de 15 segundos.

**Producto:** APM

**Componente:** Enterprise Manager

**Versión:** Todas las versiones admitidas

**Impacto:** Si esta métrica excede 1 segundo, significa que posiblemente la instancia de EM en las instancias de MOM y de los recopiladores está experimentando problemas de rendimiento.

**Configuración:** N/D

**Intervalo:** Correcto: <1000 ms, Peligro: >3500 ms

**Reparación:** Póngase en contacto con Soporte de CA.

## Monitorización del rendimiento de CA APM utilizando métricas de compatibilidad

Monitoree el rendimiento de la implementación de APM con las herramientas de monitorización del rendimiento de APM. Para monitorizar eficazmente el entorno de producción, es importante que las instancias de Enterprise Manager (EM) se encuentren en buen estado.

CA APM proporciona las herramientas siguientes que permiten detectar problemas e impedir que los cambios inesperados comprometan el entorno de monitorización:

- Métricas de compatibilidad
- Alertas

### Monitorización del rendimiento utilizando las métricas de compatibilidad de Enterprise Manager

Cada 15 segundos, Enterprise Manager recopila y registra las métricas de estado sobre sí mismo. Para solucionar los problemas de rendimiento de Enterprise Manager, se pueden visualizar estas métricas mediante el examen de estas fuentes:

- Árbol del Explorador de métrica de Investigator
- Archivo de registro
- Ficha Descripción general de Enterprise Manager

### Visualización de las métricas de compatibilidad en el árbol del Explorador de métrica

Para una instancia independiente de Enterprise Manager o MOM, las métricas de compatibilidad aparecen en el árbol del Explorador de métrica, en el nivel superior \*SuperDomain\* :

```
Custom Metric Host (Virtual)
 Custom Metric Process (Virtual)
 Custom Metric Agent (Virtual) (SuperDomain)
 Enterprise Manager
```

En un entorno agrupado en clúster, las métricas de compatibilidad del recopilador tienen una ruta de métrica similar, pero el nivel de Agente de métrica personalizado incluye el nombre de equipo y el puerto del recopilador.

En el siguiente ejemplo se muestra un árbol de Investigator que tiene una instancia de MOM y un recopilador:

```
Custom Metric Host (Virtual)
 Custom Metric Process (Virtual)
 Custom Metric Agent (Virtual) (SuperDomain)
 Enterprise Manager
 Custom Metric Agent (Virtual) (Collector1@5001) (SuperDomain)
 Enterprise Manager
```

### Visualización de las métricas de compatibilidad en el archivo de registro

De forma predeterminada, las instancias de Enterprise Manager escriben las métricas de compatibilidad en un archivo de registro denominado `perflog.txt`. Las métricas de compatibilidad se generan en intervalos de 15 segundos. La ubicación predeterminada para este archivo está en el directorio `<EM_Home>/logs`.



De forma predeterminada, `perflog.txt` se genera en modo comprimido. Los valores están separados por comas, con encabezados de columna. En este formato, `perflog.txt` se puede importar fácilmente en una hoja de cálculo para su análisis.

La desactivación del modo comprimido hace que Enterprise Manager escriba `perflog.txt` en un formato más detallado destinado a la legibilidad humana.

#### **Siga estos pasos:**

1. Abra el archivo `IntroscopeEnterpriseManager.properties`.
2. Configure los valores de configuración siguientes:
  - `introscope.enterprisemanager.performance.compressed=false`
  - `log4j.logger.Manager.Performance=DEBUG, performance, logfile`
3. Guarde y cierre el archivo `IntroscopeEnterpriseManager.properties`.

### **Visualización de las métricas de compatibilidad en la ficha Descripción general de Enterprise Manager**

Para ver la información de resumen sobre las métricas de compatibilidad para Enterprise Manager, seleccione la carpeta Enterprise Manager en el árbol Explorador de métrica. Esta información incluye la ficha Descripción general, que muestra gráficas que muestran las métricas de compatibilidad más importantes en una única vista. La ficha Descripción general de Enterprise Manager es una herramienta útil para realizar un análisis rápido de la carga de Enterprise Manager y de la utilización de los recursos.

### **Realización de una comprobación del estado del rendimiento del clúster de APM**

Como administrador, use el archivo `perflog.txt` para revelar problemas de estado comunes que afectan a los recopiladores en un clúster. Una comprobación estándar del estado del rendimiento incluye los pasos siguientes:

- **Comprobación del tamaño de la cola de mensajes**
- **Comprobación del tamaño máximo de la memoria dinámica**
- Análisis

#### **NOTE**

Para obtener una comprobación del estado completa del entorno del clúster, póngase en contacto con CA Services.

### **Comprobación del tamaño de la cola de mensajes**

#### **Siga estos pasos:**

1. Abra el archivo `IntroscopeEnterpriseManagerSupport.log` y busque `transport.outgoingMessageQueueSize`.

#### **NOTE**

Si el archivo de registro no contiene una entrada para esta métrica, el tamaño predeterminado de la cola de mensajes es 3000.

2. Para mejorar el rendimiento de la cola de mensajes entre los recopiladores y MOM, abra los archivos `IntroscopeEnterpriseManager.properties` para todos los recopiladores y MOM:
  - a. Aumente el valor de la propiedad `transport.outgoingMessageQueueSize` a 6000.
  - b. Establezca el valor de `transport.override.isengard.high.concurrency.pool.min.size` en 10.
  - c. Establezca la `transport.override.isengard.high.concurrency.pool.max.size` a 10.

**WARNING**

El aumento del tamaño de la cola de mensajes y de la agrupación por encima de un determinado punto puede hacer que Introscope consuma más recursos. No establezca el valor de `transport.outgoingMessageQueueSize` en más de 9000. El tamaño mínimo y máximo de la agrupación no debe exceder de 20.

3. Reinicie todas las instancias de Enterprise Manager.

**Comprobación del tamaño máximo de la memoria dinámica****Siga estos pasos:**

1. En los parámetros de inicio de JVM, verifique que el tamaño inicial de la memoria dinámica (`-Xms`) y que el tamaño máximo de la memoria dinámica (`-Xmx`) coinciden con el MOM y todos los compiladores. Estos valores deben ser lo más grandes posible teniendo en cuenta la máquina virtual Java implementada y la memoria RAM disponible. Por ejemplo, para una instancia de EM que se está ejecutando en una máquina virtual Java de 32 bits, el límite máximo de la memoria dinámica es de 1,5 GB en Windows o 2 GB en Linux.

**NOTE**

Si EM se está ejecutando en una máquina virtual Java de 64 bits, el tamaño máximo de la memoria dinámica solo está limitado por la cantidad de memoria RAM disponible.

2. Para establecer el tamaño de la memoria dinámica, abra el archivo `Introscope_Enterprise_Manager.lax` en el directorio `<EM_HOME>` y edite la propiedad `lax.nl.java.option.additional`.

**Ejemplo:** En este ejemplo,

`-Xms`

como

`-Xmx`

están configurados en 1024 m.

```
lax.nl.java.option.additional=-Xms1024m -Xmx1024m
```

3. Reinicie Enterprise Manager.

**Análisis de Perflog.xlsx**

Para realizar análisis adicionales en Microsoft Excel, convierta el archivo `perflog.txt` al formato `.xlsx`.

**Siga estos pasos:**

1. Cambie el nombre del archivo `<EM_HOME>/logs/perflog.txt` a `perflog.csv`.
2. Abra `perflog.csv` con Microsoft Excel y realice los siguientes pasos de formato:
  - a. Seleccione la primera fila que contenga los mosaicos:
    - a. Haga clic con el botón secundario en la fila y seleccione **Format Cells...**
    - b. Seleccione **Alignment** y, a continuación, **Wrap Text**.
    - c. Haga clic en **OK**.
  - b. Suprima cualquier fila que se encuentre por encima de la fila que contenga los mosaicos.
  - c. Seleccione **View**, **Freeze Panes** y seleccione **Freeze Top Row**.
  - d. Seleccione la primera fila que contenga los mosaicos, seleccione **Data** y seleccione **Filter** para agregar filtros a las columnas.
  - e. Seleccione los valores para los filtros y desplácese a través del contenido de la ventana de filtro.
  - f. Haga clic en **File**, seleccione **Save As** y guarde el archivo en formato `.xlsx`.

Analice el archivo convertido utilizando filtros en las siguientes columnas de métrica de rendimiento:

- **Total JVM Memory (Column B)**

Informa sobre la memoria total disponible para la máquina virtual Java. Si la memoria dinámica inicial (`-Xms`) y la memoria dinámica máxima (`-Xmx`) son iguales, el valor permanece relativamente sin cambios a lo largo del tiempo. Esta integridad se debe a la adjudicación de la memoria dinámica máxima inmediatamente después del inicio en lugar de a través de la recopilación de la máquina virtual Java.

- **Total JVM Free Memory (Column C)**

Informa sobre la cantidad de memoria libre disponible de la máquina virtual Java en cualquier intervalo. Si la memoria libre se reduce a un número de dos dígitos o menos en el recopilador, aumente el tamaño de la memoria dinámica que está disponible para la máquina virtual Java. Agregue memoria al servidor si es necesario. Si ya ha adjudicado suficiente memoria de la máquina virtual Java, investigue las otras columnas de la hoja de cálculo. Este problema es poco común en una instancia de MOM.

- **Harvest Duration (Column F)**

Informa sobre la duración de la recopilación. Esta métrica indica la cantidad de tiempo que el recopilador pasa agregando las métricas del intervalo de 15 segundos antes de guardarlas en la base de datos de SmartStor. Por ejemplo, si Harvest Duration excede frecuentemente los 3000 ms (3 segundos), es probable que el recopilador tenga dificultades para agregar las métricas de intervalo entrantes.

- **Smartstor Duration (Column G)** Reports SmartStor Duration. Esta métrica indica la cantidad de tiempo que el recopilador pasa escribiendo los datos recopilados en el disco. Céntrese en valores que superen los 5000 ms (5 segundos).

#### NOTE

Se recomienda usar un disco aparte en un controlador dedicado para almacenar datos de SmartStor. Verifique la ubicación del directorio `/data` de SmartStor para garantizar que la base de datos de SmartStor no comparta el disco con Enterprise Manager. Verifique que la propiedad `introscope.enterprisemanager.smartstor.dedicatedcontroller` se establece en `true` en el archivo `IntroscopeEnterpriseManager.properties`.

### **Métricas importantes de compatibilidad de Enterprise Manager**

Las siguientes métricas de compatibilidad son útiles para predecir tendencias, detectar problemas e identificar las causas raíz de los problemas de capacidad de Enterprise Manager. Cada métrica se describe con información sobre cómo se puede utilizar.

#### NOTE

#### Más información:

- [Métricas de compatibilidad principales](#)

### **Harvest Duration**

La métrica `Harvest Duration` muestra el tiempo en milisegundos (durante un intervalo de tiempo de 15 segundos) invertido en la recolección de datos. Por lo general, esta métrica es un buen indicador para determinar si Enterprise Manager está manteniendo el rendimiento con la carga de trabajo actual.

Dado que el tiempo de ejecución de la calculadora es un componente principal de la duración de la recolección, la métrica `Harvest Duration` es una buena aproximación del uso de la CPU. Un valor óptimo de la métrica `Harvest Duration` es inferior a 3500 ms [3,5 segundos]. Un valor superior a 7500 ms [7,5 segundos] indica que Enterprise Manager tiene una capacidad insuficiente de la CPU para la carga de la métrica y de la calculadora.

Se puede ver la métrica en estas ubicaciones:

- Árbol del Explorador de métrica en `Enterprise Manager | Tasks`.
- `perflog.txt` en `Performance.Harvest.HarvestDuration`

## SmartStor Duration

La métrica `SmartStor Duration` muestra la cantidad de tiempo que tardan en escribirse en la base de datos de SmartStor las métricas recibidas y generadas durante un intervalo de tiempo.

La métrica `SmartStor Duration` es un indicador del rendimiento de escritura de E/S del disco SmartStor. Los valores incoherentes indican contención en los recursos relacionados con el disco. Los valores coherentemente altos indican que el ancho de banda de escritura de disco no es adecuado para la carga de la métrica que se está gestionando.

En las condiciones estándares de Enterprise Manager, el valor medio de `SmartStor Duration` debe ser inferior a 3500 ms (3,5 segundos). El valor de `SmartStor Duration` *debe* ser inferior a 15000 ms (15 segundos). Un valor de métrica superior a 15 segundos indica que Enterprise Manager está sobrecargado de forma crítica.

Se puede ver la métrica en estas ubicaciones:

- Árbol del Explorador de métrica en Enterprise Manager | Tasks
- `perflog.txt` en Performance.SmartStor.Duration

## Number of Collector Metrics

La métrica `Number of Collector Metrics` muestra el número total de métricas de las que se está realizando un seguimiento actualmente en un clúster. Esta métrica es la suma de los valores de las métricas de compatibilidad de Enterprise Manager | Connections | Number of Metrics en todos los recopiladores del clúster.

Se puede ver la métrica en estas ubicaciones:

- Árbol del Explorador de métrica en Enterprise Manager | MOM | Number of Collector Metrics.
- `perflog.txt` en Performance.MOM.NumberOfCollectorMetrics

## Collector Metrics Received Per Interval

La métrica `Collector Metrics Received Per Interval` es la suma de los puntos de datos de la métrica del recopilador que MOM ha recibido para cada período de tiempo de 15 segundos. Los puntos de datos vienen de estas fuentes:

- Suscripciones a métricas en nombre de los módulos de gestión como, por ejemplo, cuadros de mandos, calculadoras o alertas
- Consultas que generan los clientes como, por ejemplo, consultas a Workstation y CLW
- Consultas para las métricas que generan las alertas y las calculadoras incrustadas

La métrica `Collector Metrics Received Per Interval` es un indicador de la carga de la consulta del clúster y del consumo del ancho de banda de red para la comunicación entre el recopilador y MOM. Se espera cierta variación. Los picos grandes indican una gran actividad de consultas espontáneas. El valor de `Collector Metrics Received Per Interval` se aproxima al número de métricas que están procesando las calculadoras.

Se puede ver la métrica en estas ubicaciones:

- Árbol del Explorador de métrica en Enterprise Manager | MOM | Collector Metrics Received Per Interval.
- `perflog.txt` en Performance.MOM.CollectorMetricsReceivedPerInterval

## Alerts: Total Number of Evaluated Metrics

Las alertas son *calculadoras dependientes* porque las alertas actúan en la salida de otras calculadoras. Las calculadoras dependientes no se pueden ejecutar paralelamente a las calculadoras que proporcionan su entrada. Por este motivo, las alertas pueden prolongar la duración de la recolección más que las calculadoras no dependientes. La métrica de compatibilidad Alerts: Total Number of Evaluated Metrics muestra el número de métricas que las alertas han procesado durante cada intervalo de tiempo.

Se puede ver la métrica en el árbol del Explorador de métrica en `Enterprise Manager | Internal | Alerts`.

Si un aumento de la duración de la recolección se correlaciona con un aumento de las métricas que evalúan las alertas, se puede aumentar la capacidad de EM mediante la optimización de las alertas. Para identificar las alertas que consumen la mayoría de recursos, busque y ordene por valor todas las métricas cuyo nombre coincida con la expresión regular siguiente:

```
(.*)Enterprise Manager|Internal|(.*)Alerts(.*)Number of Evaluated Metrics
```

Si Introscope tiene alertas que evalúan un gran número de métricas (especialmente métricas de varios recopiladores), considere estas acciones:

- Desactivación de las alertas que proporcionan poco valor.
- Ajuste de las expresiones regulares en los grupos de métricas alertados para incluir solamente las métricas mínimas necesarias para indicar la condición de alerta.
- División de las alertas que evalúan métricas de varios recopiladores en varias alertas que solo evalúan las métricas de un único recopilador. Esta acción no reduce necesariamente el número de métricas que procesa MOM, pero mejora el rendimiento de las consultas en el clúster.

### **Overall Capacity (%)**

La métrica `Overall Capacity (%)` estima el porcentaje de la capacidad de Enterprise Manager que se consume.

Se puede ver la métrica en el árbol del Explorador de métrica en `Enterprise Manager`.

La métrica `Overall Capacity (%)` se calcula en parte a partir de las siguientes métricas que contribuye al proceso, que se pueden ver en el árbol del Explorador de métrica en `Enterprise Manager | Health`:

- CPU Capacity (%)
- GC Capacity (%)
- Harvest Capacity (%)
- [Heap Capacity \(%\) metric](#)
- Incoming Data Capacity (%)
- SmartStor Capacity (%)

La métrica `Overall Capacity (%)` es más valiosa durante un período largo que para un intervalo de tiempo específico de 15 segundos. Dado que la métrica `Overall Capacity (%)` se basa en las métricas en tiempo real, el valor de `Overall Capacity (%)` puede aumentar bastante por encima del 100 %. El pico puede ocurrir, por ejemplo, porque el subsistema de E/S del hardware se sobrecarga brevemente. Sin embargo, Enterprise Manager tiende a recuperarse automáticamente de estas situaciones de pico cuando no son duraderas. En general, un pico de hasta el 200 por ciento, por ejemplo, no es motivo de preocupación si es transitorio. Sin embargo, en un largo período de tiempo, el valor medio ideal de `Overall Capacity (%)` es del 75 % o menos.

Durante los períodos de tiempo que se dispara la métrica `Global Capacity (%)` a valores altos, probablemente también al menos una de las otras métricas que contribuyen muestren un pico. La investigación y la comprensión del origen del pico secundario puede ayudar a identificar la causa raíz del problema del recurso. Por ejemplo, puede encontrar el problema mirando [Heap Capacity \(%\) metric](#) que incluye la métrica `Overall Capacity (%)`.

La visualización de la métrica `Overall Capacity (%)` en el modo histórico es útil para obtener una visión general y comparativa del estado de la capacidad de Enterprise Manager. Sin embargo, la carga de trabajo de Enterprise Manager es compleja y diversos aspectos de la carga de trabajo afectan a la métrica `Overall Capacity (%)` de diferentes maneras no lineales. Por ejemplo, la duración de las tareas de mantenimiento de SmartStor (trabajos en cola para la conversión de datos y reperiodización) puede ser un indicador importante de la capacidad de Enterprise Manager. Sin embargo, estas tareas de mantenimiento no participan directamente en el cálculo de `Overall Capacity (%)`. Las tareas de mantenimiento de SmartStor causan un aumento en el uso de la CPU y de la memoria dinámica. El aumento de la utilización da lugar a un aumento en el porcentaje de la capacidad. Sin embargo, la magnitud del aumento no refleja el impacto completo de los problemas de mantenimiento de SmartStor.

La métrica `Overall Capacity (%)` se centra en cómo Enterprise Manager gestiona la carga de trabajo de la métrica del agente. Esta métrica no evalúa directamente la capacidad en lo que se refiere a los datos de CA CEM. Por ejemplo, la métrica `Overall Capacity (%)` no refleja los servicios de Enterprise Manager sobrecargados ni los problemas de E/S de la base de datos de APM.

### **Heap Capacity (%)**

La métrica `Heap Capacity (%)` muestra cuánta memoria dinámica asignada está en uso. Esta métrica se normaliza en el 75 % de la memoria dinámica asignada para proporcionar un búfer de seguridad y evitar bloqueos. Un valor de métrica de 100 significa que la memoria dinámica asignada solo se utiliza el 75 %.

La métrica `Heap Capacity (%)` permite evaluar si la memoria dinámica que se asigna a Enterprise Manager es suficiente para la carga. Esta métrica también permite detectar las tendencias que afectan al uso de la memoria dinámica. A veces, el uso alto de la CPU o la duración alta de la recopilación o ambos pueden ser el resultado del uso alto de la memoria dinámica.

Se puede ver la métrica en el árbol del Explorador de métrica en `Enterprise Manager | Health`.

### **Number of Historical Metrics**

La métrica `Number of Historical Metrics` es el número total de métricas que Enterprise Manager ha visto y persistido en SmartStor. Este número aumenta a medida que los agentes informan sobre nuevas métricas y disminuye a medida que caducan las métricas de SmartStor. La desconexión temporal del agente y la generación de más datos en una métrica existente no cambian este número.

El número de métricas históricas afecta el rendimiento histórico de las consultas y los gastos generales de la reperiodización nocturna de SmartStor. Un valor creciente puede indicar los problemas siguientes:

- **Pérdida de métrica**  
Un número de métricas que aumenta gradualmente debido a un entorno de monitorización inestable con conexiones con agentes no controlados.
- **expansión de la métrica**  
Un número de métricas que aumenta rápidamente debido a la aparición de muchos nuevos agentes o a las métricas de SQL especificadas incorrectamente.

Se puede ver la métrica en el árbol del Explorador de métrica en `Enterprise Manager | Connections`.

### **Partial Metrics without Data**

La métrica `Partial Metrics without Data` indica el número de métricas del agente que ya no se notifican en directo. Estas métricas consumen memoria dinámica y afectan negativamente al rendimiento de la consulta, ya que contribuyen al recuento de métricas de `Historical Metrics`.

Las sanciones de rendimiento son leves, a menos que el valor de la métrica `Partial Metrics without Data` llegue a ser grande.

Si tiene problemas con la capacidad de respuesta de la consulta histórica o con un tiempo largo de reperiodización de SmartStor, compare el valor de la métrica `Partial Metrics without Data` con el valor de la métrica `Partial Metrics with Data`. Se puede ver la métrica `Partial Metrics with Data` en el árbol del Explorador de métrica en `Enterprise Manager | Data Store | SmartStor | MetaData`. Si la métrica `Partial Metrics without Data` aborda el valor de la métrica `Partial Metrics with Data`, utilice SmartStor Tools para eliminar los metadatos innecesarios de la métrica.

Se puede ver la métrica en esta ubicación:

- Árbol del Explorador de métrica en `Enterprise Manager | Data Store | SmartStor | MetaData`

### **Number of Traces in Insert Queue**

Enterprise Manager intenta insertar todos los eventos entrantes en una cola de inserción del seguimiento de transacciones. La métrica `Number of Traces in Insert Queue` muestra el promedio de eventos en la cola durante el intervalo de tiempo anterior.

La métrica `Number of Traces in Insert Queue` indica si Enterprise Manager está manteniendo el nivel de procesamiento del seguimiento de transacciones. Si la cola de inserción del seguimiento de transacciones está llena cuando aparece un nuevo evento, se descarta el evento. Se puede ver la métrica `Transactions: Number of Dropped Per Interval` para ver el número de seguimientos de transacciones que Enterprise Manager no ha podido gestionar durante el intervalo y que se han descartado.

Se puede ver la métrica `Transactions: Number of Dropped Per Interval` en las ubicaciones siguientes:

- **Árbol del Explorador de métrica** en Enterprise Manager | Data Store | Transactions
- `perflog.txt` en `Performance.Transactions.Num.Dropped.Per.Interval`

Se puede ver la métrica `Number of Traces in Insert Queue` en las ubicaciones siguientes:

- **Árbol del Explorador de métrica** en Enterprise Manager | Data Store | Transactions
- `perflog.txt` en `Performance.Transactions.TT.Queue.Size`

### **SmartStor Queries Per Interval**

La métrica `SmartStor Queries per Interval` muestra el número de consultas para los datos de métricas que se han recibido durante el intervalo de tiempo anterior.

El equilibrio de las escrituras de métricas que se comparan con las consultas de métrica determina los requisitos de configuración del disco de SmartStor.

Para evaluar el rendimiento de la carga de la consulta de métrica, consulte estas métricas:

- **Métrica `SmartStor Queries per Interval`**
- **Métrica `SmartStor Queries Duration (ms)`**  
Esta métrica muestra la duración media de la consulta durante el intervalo de tiempo anterior.

Se puede ver la métrica `SmartStor Queries Duration (ms)` y la métrica `SmartStor Queries per Interval` en estas ubicaciones:

- **Árbol del Explorador de métrica** en Enterprise Manager | Internal | Query
- `perflog.txt`

### **Más métricas de compatibilidad con Enterprise Manager**

Utilice la siguiente lista de otras métricas de compatibilidad útiles.

- **EM CPU Used (%)**  
Utilización del procesador por subprocesos de Enterprise Manager (EM) durante el período de tiempo medido. En un intervalo de tiempo de 15 segundos, la utilización es:  $\text{<ms utilizados del procesador por EM> / (15000 * \text{<núm. de procesadores>})$ .  
Se encuentra en el árbol de Investigator en `Enterprise Manager|CPU`.

#### **NOTE**

Este número no refleja el uso total del procesador durante el intervalo de tiempo. Esta métrica solo mide la participación de Enterprise Manager en el total de uso del procesador.

- **Number of Agents**  
El número de agentes conectados actualmente.  
Consulte el árbol del Explorador de métrica en `Enterprise Manager|Connections`.
- **Harvest Capacity (%)**



El porcentaje de tiempo para la recopilación de datos en un intervalo de tiempo de 15000 ms (15 segundos), donde el 100 % son los 15 segundos. Por ejemplo, si la duración de la recolección es 15000 ms, este valor de la métrica es 100.

#### NOTE

En un entorno de monitorización correcto, la capacidad de recolección se mantiene por debajo del 25 %.

Consulte el árbol del Explorador de métrica en `Enterprise Manager|Health`.

- **Number of Metrics**

La carga de métrica en Enterprise Manager. Cuando un agente se desconecta, este número se reduce.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Connections`.

- **SmartStor Capacity (%)**

El porcentaje de tiempo que el proceso de escritura de SmartStor tarda en un intervalo de tiempo de 15000 ms (15 segundos), donde el 100 % son los 15 segundos. Por ejemplo, si la duración de la escritura de SmartStor es 15000 ms, este valor de métrica es 100.

#### NOTE

En un entorno de monitorización correcto, la capacidad de SmartStor se mantiene por debajo del 25 %.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Health`.

- **Active Incoming Threads**

El número de subprocesos que administran activamente mensajes de los clientes.

La métrica Active Incoming Threads proporciona información sobre la simultaneidad de la ejecución de la consulta. Varias consultas de métrica simultáneas pueden interferir con la otra actividad de SmartStor y pueden aumentar la duración de SmartStor.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal|Messaging`.

- **Active Outgoing Threads**

El número de subprocesos que entregan activamente datos a los clientes.

Esta métrica es un indicador de la simultaneidad de consulta. Un aumento en el número de subprocesos que trabajan en la entrega de datos puede indicar problemas de red.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal|Messaging`.

- **Number of Dependent Calculator Input Metrics**

El número total de métricas que son entradas para las calculadoras dependientes.

Las calculadoras dependientes funcionan según los valores de métricas que producen otras calculadoras. Las entradas de las calculadoras dependientes también pueden incluir valores de métricas notificados por los agentes. Este recuento hace referencia a todas las métricas dadas a las calculadoras dependientes, no solo a las métricas que otras calculadoras producen.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal`.

- **Number of Non Dependent Calculator Input Metrics**

El número total de métricas que son entradas para las calculadoras no dependientes.

Las calculadoras no dependientes funcionan en métricas notificadas por los agentes y no en las métricas que envían otras calculadoras.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal`.

- **Total Number of Evaluated Metrics (Calculators)**

El número total de métricas que se evalúan para todas las calculadoras. La suma de Number of Dependent Calculator Input Metrics y Number of Non-dependent Calculator Input Metrics.

Cuando este recuento sube, Enterprise Manager está realizando muchos cálculos en tiempo real, lo que puede sobrecargar los recursos de la CPU.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal|Calculators`.

- **<Nombre calculadora> | Total Number of Evaluated Metrics**

El número total de métricas que se evalúan para una única calculadora.



El valor de esta métrica indica cuánto contribuye la calculadora asociada a la duración de la recolección. Céntrese en las calculadoras que evalúan un gran número de métricas para optimizar la capacidad de Enterprise Manager.

#### NOTE

Esta métrica solo aparece en Investigator cuando se define la calculadora.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal`.

- **Alert Action Processing Time (ms)**

El tiempo transcurrido que Enterprise Manager tarda en procesar todas las acciones de la alerta.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal|Harvest`.

- **Calculator Queries Wait Time (ms)**

El tiempo transcurrido para que el subproceso de las consultas de la calculadora finalice su trabajo actual, incluida la espera a que finalice el bucle de consulta que no es de la calculadora.

El nuevo procesamiento de consultas de la calculadora se inicia después de que se completen todas las entregas que no son de la calculadora del intervalo de tiempo anteriores a los clientes. Cuando este recuento sube, Enterprise Manager está realizando muchos cálculos en tiempo real, lo que puede sobrecargar los recursos de la CPU.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal|Harvest`.

- **Non Calculator Queries Delivery Time (ms)**

El tiempo que Enterprise Manager ha tardado en ejecutarse y entregar consultas que no son de la calculadora a todos los clientes solicitantes en un intervalo de tiempo.

Después de ejecutar todas las consultas con la calculadora, Enterprise Manager ejecuta consultas que no son de calculadora. A continuación, EM envía los resultados a todos los clientes que los solicitaron. Cuando este número aumenta, Enterprise Manager envía muchos resultados de las consultas que no son de calculadora a los clientes, lo que puede sobrecargar la red.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal|Harvest`.

- **Non Calculator Queries Excess Time (ms)**

El tiempo de espera excesivo para que las consultas que no son de la calculadora se completen más allá de un intervalo de tiempo.

Los clientes envían solicitudes de consulta que no son de la calculadora a Enterprise Manager, que devuelve los resultados. Si este proceso no finaliza en un intervalo de tiempo, se llevará a cabo hasta que se complete. Esta métrica muestra cuánto tiempo se han ampliado las consultas que no son de la calculadora más allá de un intervalo de tiempo.

Utilice esta métrica para determinar si las consultas que no son de calculadora están sobrecargando Enterprise Manager. Este valor de métrica normalmente es 0 cuando Introscope está bajo una carga pequeña. Un valor mayor de 0 indica que Enterprise Manager está sobrecargado y no puede procesar las consultas de métricas en un intervalo de tiempo.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal|Harvest`.

- **Metrics From All Agents**

El número total de métricas únicas generadas por todos los agentes conectados que han enviado datos en el último intervalo de tiempo. Este recuento no incluye métricas históricas. La configuración de la fijación no afecta a este recuento.

Cuando se activa la fijación de `introscope.enterprisemanager.agent.metrics.limit`, el valor de esta métrica indica por cuánto se ha excedido el límite.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal|Harvest`.

- **Spooling Data File Write Time (ms)**

El tiempo que Enterprise Manager ha tardado en escribir los datos recolectados en el archivo de trabajos en cola (`.spool`) en un intervalo de tiempo.

Use esta métrica para monitorizar el ciclo de recolección.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal|Harvest`.

- **Spooling Preparation Time (ms)**

El tiempo que Enterprise Manager ha tardado en preparar los datos recolectados para escribirlos en el archivo de trabajos en cola (`.spool`) en un intervalo de tiempo.

Use esta métrica para monitorizar el ciclo de recolección.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|Internal|Harvest`.

- **Total Number of Evaluated Metrics (Management Module Calculators)**

El número de métricas que son la entrada de las calculadoras del módulo de gestión.

Cuando este número se dispara, indica que una consulta o una calculadora con una consulta coinciden con demasiadas métricas.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|InternalManagement Module Calculators`.

- **Metric Matches Per Interval**

El número total de métricas que se han evaluado en todas las consultas en el último intervalo de tiempo.

Esta métrica muestra un valor cuando ocurren estas acciones:

- Nuevos agentes se conectan a Enterprise Manager.
- Se utilizan expresiones regulares en las consultas internas y las consultas generadas por usuarios, incluidas las agrupaciones de métricas del módulo de gestión.
- Los usuarios seleccionan las métricas en el árbol del Explorador de métrica.
- Los usuarios abren los cuadros de mandos que contienen gráficas.

Cuando el valor de esta métrica es alto, se producen muchas consultas en poco tiempo.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|InternalMetric Group`.

- **Queued Queries Per Interval**

El número de consultas que actualmente están a la espera de procesamiento en el intervalo del ciclo de recolección.

En general, el valor es cero después del inicio.

Se encuentra en el árbol del Explorador de métrica en `Enterprise Manager|InternalMetric Group`.

## **Métricas de compatibilidad de la agrupación de conexiones de la base de datos de APM**

Los servicios de Enterprise Manager proporcionan métricas que describen la adjudicación y el uso de las agrupaciones de conexiones de la base de datos de APM. Estas agrupaciones permiten el intercambio de datos entre los servicios de Enterprise Manager y la base de datos de APM. Las métricas de compatibilidad de la agrupación de conexiones de la base de datos de APM se muestran en Workstation Investigator en:

`Custom Metric Agent|Enterprise Manager|Internal|Database|Connection Pools`

Además están disponibles en el archivo de registro `tessperflog.txt` y tienen el prefijo

`Internal.Database.Connection Pools`.

Se proporcionan métricas para las fuentes de datos de APM:

El nombre `apmDataSource` identifica la fuente de datos de APM.

La lista siguiente describe las métricas de compatibilidad de la agrupación de conexiones de la base de datos de APM:

- **numBusyConnections**  
Número de conexiones en uso actualmente
- **numConnections**  
Número de conexiones abiertas
- **numIdleConnections**  
Número de conexiones abiertas no en uso
- **numUnclosedOrphanedConnections**  
Número de conexiones abiertas que permanecieron sin usar después de superar un umbral de tiempo de espera.
- **threadPoolNumTasksPending**  
Número de tareas en cola a la espera de una conexión

## **Monitorización de las conexiones de Workstation utilizando métricas de compatibilidad**

La métrica `Connections: Number of Workstations` muestra el número actual de conexiones de Workstation. Para los recopiladores en un entorno agrupado en clúster, el valor de esta métrica es 0.

Consulte la métrica `Connections:Number of Workstations` en el árbol del Explorador de métrica:

```
SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|
Custom Metric Agent (Virtual)(*SuperDomain*)|Enterprise Manager|
Connections:Number of Workstations
```

#### NOTE

La

`Connections:Number of Workstations`

La métrica no refleja las conexiones de Command Line Workstation o WebView.

## Istio Support

DX APM Istio Support informa sobre las métricas y los seguimientos de transacciones de las aplicaciones (normalmente microservicios) que se instrumentan con rastreadores compatibles con OpenTracing.

[Istio](#) es una malla de servicios de código abierto y proveedor neutral que utilizan las organizaciones para reducir la complejidad de la nube híbrida y de los entornos de varias nubes. Istio inserta un proxy de sidecar en el pod en el que se está ejecutando un contenedor de aplicaciones. El proxy de sidecar monitoriza las solicitudes de aplicaciones de tráfico de red entrante y saliente (normalmente microservicios).

DX APM amplía Prometheus Importer del Agente de monitorización universal (UMA) para informar de los datos de solicitud del proxy de sidecar de Istio. Istio Support informa sobre las métricas de estado de Istio y de la aplicación, y muestra los seguimientos de transacciones y los datos del mapa de Team Center.

### Versiones admitidas de Istio

- Istio 1.4.x

### Activación del back-end de Prometheus Importer compatible con Istio

Active el back-end de Prometheus Importer de Istio Support antes de instalar el Agente de monitorización universal (UMA).

**Siga estos pasos:**

1. Abra el archivo apropiado para el entorno en un programa de edición de texto:
  - (Operador de UMA) Vaya al directorio `uma-operator` y abra el archivo `uma_cr.yaml`.
  - (Gráfico de Helm) Vaya al directorio `helm-chart/uma` y abra `values.yaml`.
  - (Archivo YAML de UMA) Vaya al archivo YAML de la aplicación, que se llama `ca-uma-agent.yaml`.
2. (Operador de UMA/Gráfico de Helm) Configure la propiedad `prometheus.backend.enabled`.

#### NOTE

Omita este paso si utiliza el archivo YAML de UMA para instalar UMA. El archivo `ca-uma-agent.yaml` activa la compatibilidad del back-end de Prometheus Importer de forma predeterminada.

- a. Busque la propiedad `prometheus.backend.enabled`.
  - b. Establezca la propiedad `prometheus.backend.enabled` en `true`. El valor predeterminado es `false`.
3. Defina la dirección URL de back-end de Prometheus Importer.
    - a. (Operador de UMA/Gráfico de Helm) En el archivo adecuado (`uma_cr.yaml` para el operador de UMA/`values.yaml` para el gráfico de Helm), agregue la dirección URL del back-end de Prometheus Importer después de `url`. Consulte esta sección del archivo:
 

```
container: | prometheus: | backend: | endPoint: | url: <URL>
```
    - b. (Operador de UMA/Gráfico de Helm) Cuando la dirección URL de back-end de Prometheus Importer está protegida, proporcione el nombre de usuario y la contraseña.

En el archivo adecuado (`uma_cr.yaml` para el operador de UMA o `values.yaml` para el gráfico de Helm), introduzca las credenciales en las propiedades del nombre de usuario y de la contraseña en estas secciones del archivo:

```
container: | prometheus: > backend: | endPoint: | username: | and prometheus: | backend: | endPoint: |
username:

container: | prometheus: | backend: > endPoint: | username: | and prometheus: | backend: | endPoint: |
password:
```

Estos son los valores de configuración de `uma_cr.yaml` y `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
```

(Archivo YAML de UMA)

En el archivo YAML de la aplicación, establezca la propiedad `Prometheus_server_url` especificada en `Prometheus_server_url: "<URL>"`. Asegúrese de incluir las comillas dobles " antes y después de la dirección URL. A continuación, se muestra un ejemplo:

```
Prometheus_server_url: "http://10.80.89.157:30007/"
```

## Instalación de Istio Support utilizando el Agente de monitorización universal

Después de configurar la conexión al back-end de Prometheus, instale UMA utilizando una de estas opciones:

- Kubernetes Operator
- Gráfico de Helm
- Archivo YAML de UMA

Consulte [Instalación y configuración del Agente de monitorización universal para Kubernetes](#) para instalar UMA.

## Métricas de Istio

UMA implementa el pod **cluster-performance-prometheus** con Prometheus Importer activado, tal y como se muestra en esta captura de pantalla de ejemplo:

NAME	READY	STATUS	RESTARTS	AGE
pod/app-container-monitor-bndgx	2/2	Running	0	21h
pod/app-container-monitor-rngq5	2/2	Running	0	21h
pod/app-container-monitor-tsmhg	2/2	Running	0	21h
pod/cluster-performance-prometheus-5bbb87b6bf-q4lbv	1/1	Running	0	21h
pod/cluster-info-86688b1491-mb5tt	1/1	Running	0	21h
pod/container-monitor-8655dfd798-ffs4q	1/1	Running	0	21h

El Agente de DX APM Prometheus extrae métricas del servidor de Prometheus e informa sobre las métricas del nodo **Istio**. A continuación se muestra la ruta del Explorador de métrica:

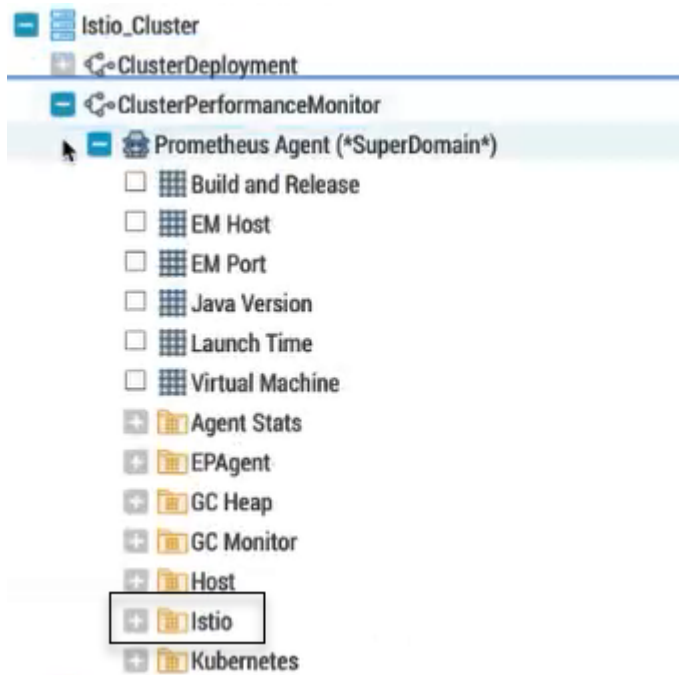
SuperDomain | `<clusterName>` | ClusterPerformanceMonitor | Prometheus Agent | Istio

Proporcione el nombre de clúster en la propiedad `clusterName` del archivo `uma_cr.yaml` (operador de UMA) o del archivo `values.yaml` (gráfico de Helm).

- Ejemplo: `DevelopmentCluster`
- Valor predeterminado: `SandBox`

En este caso, la ruta del Explorador de métrica es SuperDomain | DevelopmentCluster o SandBox | ClusterPerformanceMonitor | Prometheus Agent | Istio

Después de instalar el UMA, DX APM muestra el nodo **Istio** debajo del nodo del **Agente de Prometheus** tal y como se muestra en esta captura de pantalla:



Istio Support proporciona dos categorías de métricas. La primera categoría es métricas de servicios y carga de trabajo, que proporcionan datos de rendimiento sobre las aplicaciones que se ejecutan en Istio Service Mesh. La segunda categoría son las métricas de estado específicas de Istio.

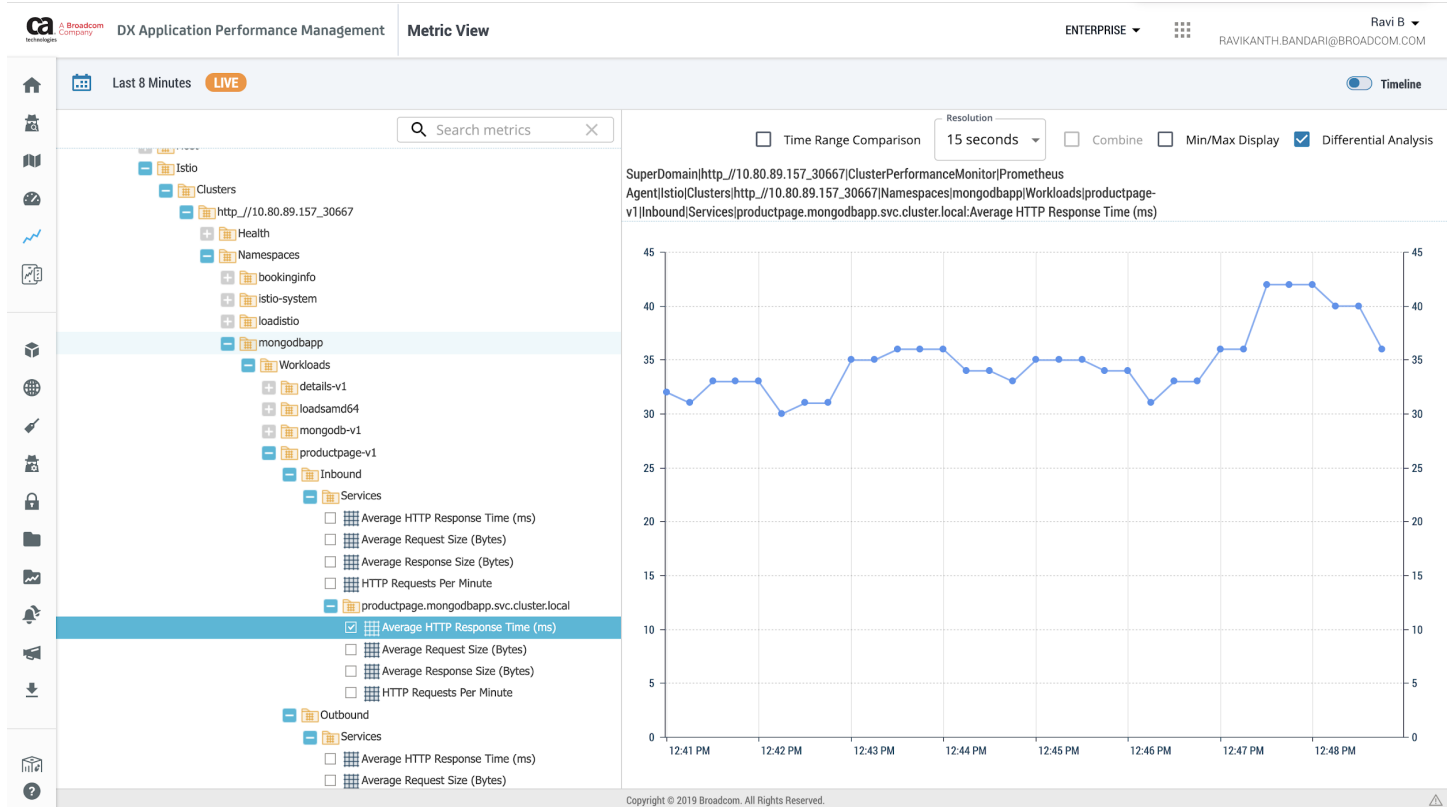
### **Métricas de los servicios y la carga de trabajo de Istio Support**

En Istio Support, un *servicio* hace referencia a un servicio de Kubernetes o OpenShift. Una *carga de trabajo* hace referencia a una implementación de Kubernetes o OpenShift. Los términos *entrante* y *saliente* hacen referencia al tráfico de red que entra o sale de un servicio o carga de trabajo de Kubernetes o OpenShift.

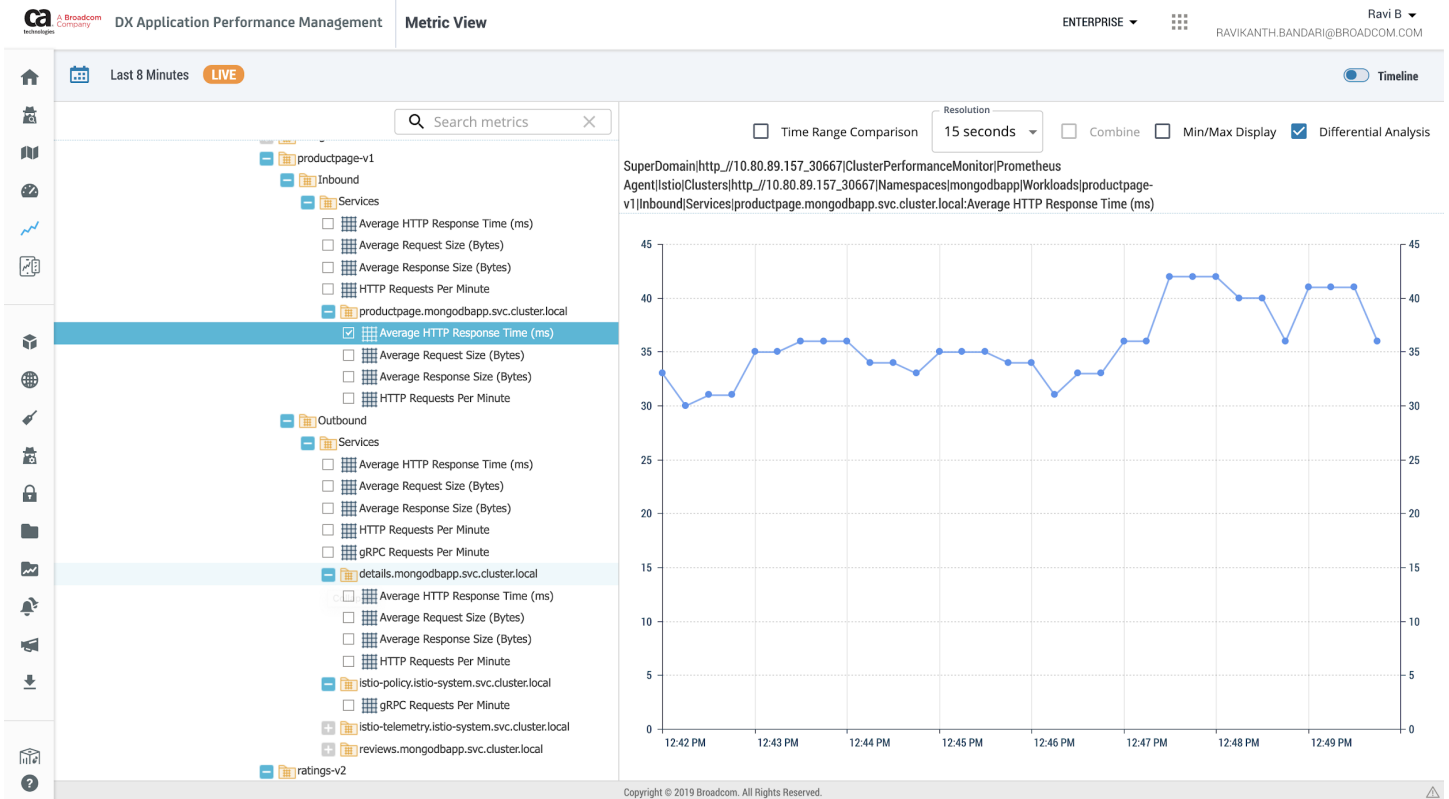
Istio Support notifica estas métricas por servicio o carga de trabajo. Istio Support no notifica todas las métricas para cada servicio o carga de trabajo. Las métricas de Istio Support dependen del tipo de tráfico que fluye a través del servicio o carga de trabajo: llamadas de procedimiento remoto de HTTP, gRPC (gRPC) y protocolo de control de transmisión (TCP). Por ejemplo, cuando el tráfico HTTP y gRPC fluye a través de un servicio o carga de trabajo, Istio Support notifica todas las métricas que se relacionan con HTTP y gRPC. A continuación se muestra la ruta del Explorador de métrica para las métricas de servicios y de carga de trabajo:

SuperDomain | <clusterName> | ClusterPerformanceMonitor | Prometheus Agent | Istio | Clusters | <Prometheus Importer Backend URL> | namespaces | <application name> | Workloads | <Workload Name> | Inbound/Outbound | Services | <Service Name> |

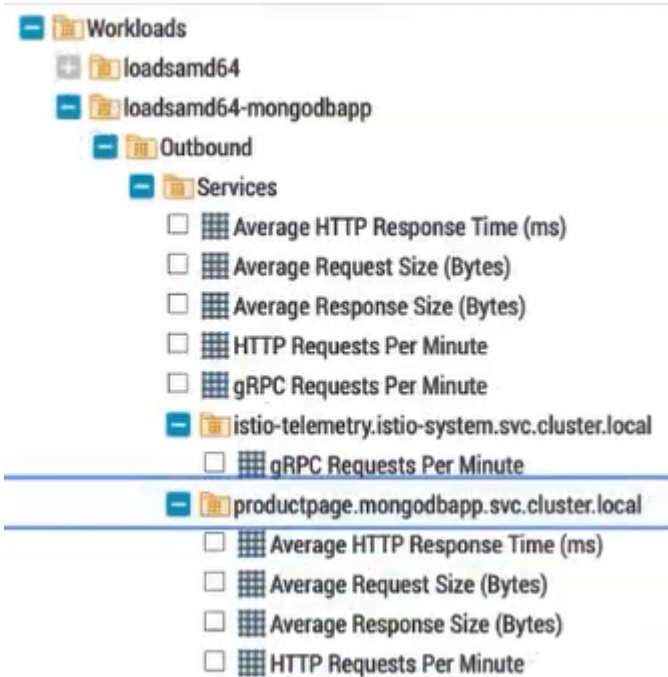
En la primera de las dos capturas de pantalla siguientes, el Explorador de métrica muestra las métricas para todos los **servicios Entrantes** y algunos de los **salientes** para la aplicación **mongodbapp**. En ambas capturas de pantalla, el gráfico muestra los datos de la métrica **Average Response Time** para la aplicación **mongodbapp**, la carga de trabajo **productpage-v1** y el servicio entrante **productpagemongodbapp.svc.cluster.local**. Tenga en cuenta que la carga de trabajo **productpage-v1** también tiene servicios entrantes y salientes.



En la siguiente captura de pantalla, el Explorador de métrica muestra las métricas para algunos los **servicios Entrantes** y algunos de los **salientes** para la aplicación **mongodbapp**.

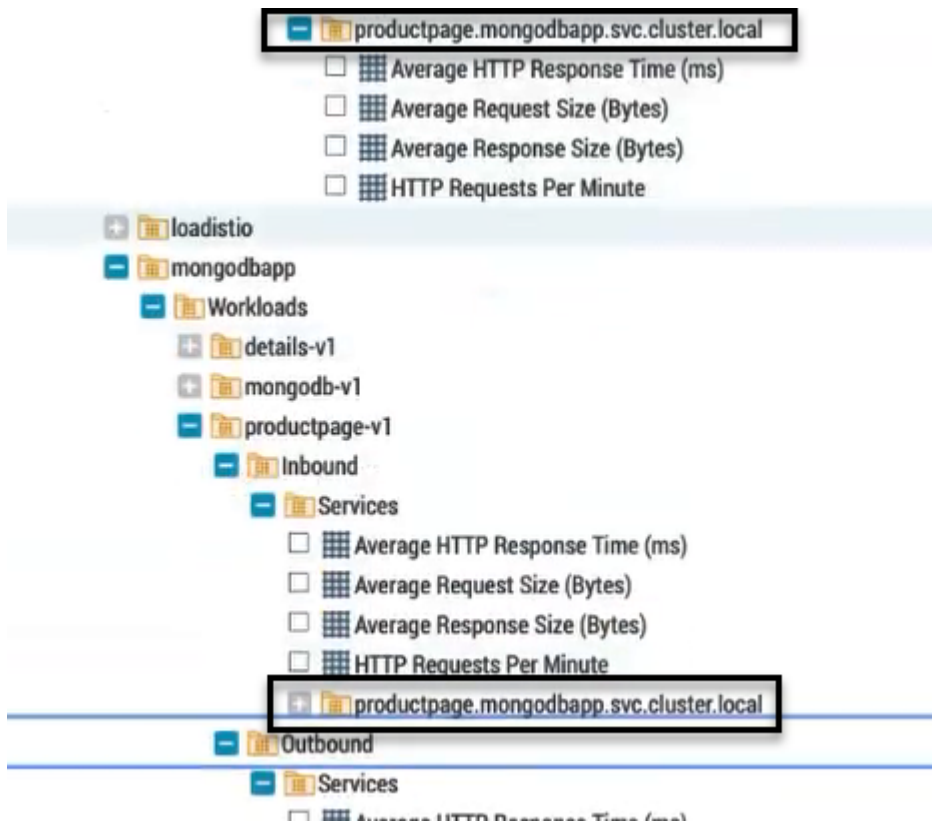


A veces, una carga de trabajo tiene solamente tráfico saliente. En esta captura de pantalla, el Explorador de métrica muestra una carga de trabajo de MongoDB denominada **loadsamd64-mongod**. Esta carga de trabajo solo tiene comunicación saliente, enviando tráfico a dos servicios: uno para telemetría(**istio-telemetry.istio-system.svc.cluster.local**) y productpage (**productpage.mongodbapp.svc.cluster.local**).





En la captura de pantalla siguiente, observe que el tráfico entrante muestra la solicitud que viene del servicio **productpage.mongoddb.svc.cluster.local**.



Estas son las métricas de los servicios y la carga de trabajo de Istio Support

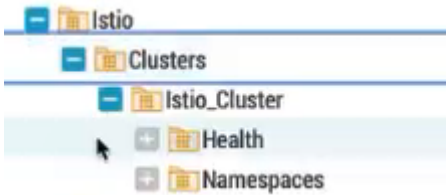
- Average HTTP Response Time (ms)
- Average Request Size (Bytes)
- Average Response Size (Bytes)
- HTTP Requests Per Minute
- HTTP Errors Per Minute
- gRPC Errors Per Minute
- gRPC Requests Per Minute
- TCP Bytes Received Per Minute
- TCP Bytes Sent Per Minute
- TCP Connections Closed Per Minute
- TCP Connections Closed Per Minute

### **Métricas de estado de Istio Support**

Las métricas de estado de Istio Support proporcionan información sobre el rendimiento específico de Istio y se muestran en el directorio **Health**. A continuación se muestra la ruta completa del Explorador de métrica:

SuperDomain | <nombreClúster> | ClusterPerformanceMonitor | Prometheus Agent | Istio | Clusters | Istio Cluster o <Dirección URL del back-end de Prometheus Importer> | Health





Las métricas de estado se extraen de los componentes Citadel, Pilot y Galley Istio. En esta tabla, se describen las métricas de estado por componente:

#### Métricas de Citadel

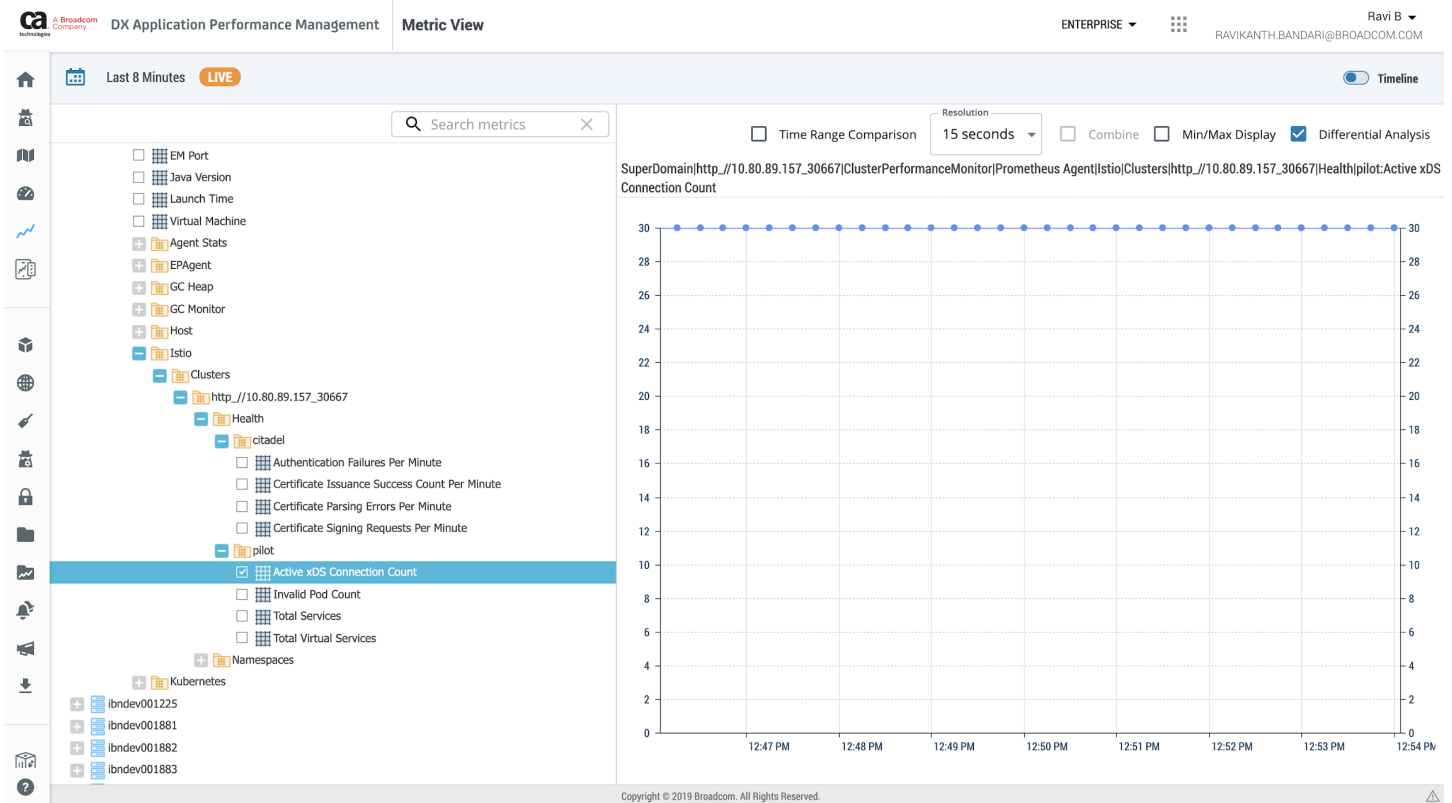
- **Authentication Failures Per Minute**  
El número de errores de autenticación por minuto.
- **Certificate Issuance Success Count Per Minute**  
El número de emisiones de certificados que se han emitido correctamente por minuto.
- **Certificate Parsing Errors Per Minute**  
El número de errores por minuto que se producen al analizar las solicitudes de firma de certificado (CSR).
- **Certificate Signing Requests Per Minute**  
El número de CSR que recibe el servidor de Citadel por minuto.

#### Métricas de Pilot

- **Active xDS Connection Count**  
La cantidad de proxies de puntos finales/envíos conectados a este piloto usando el protocolo [Envoy XDS](#).
- **Invalid Pod Count**  
El número de proxies que no son seleccionados por ningún servicio. Esta métrica de error se produce cuando la lista Punto final de un servicio no se actualiza en Pilot.
- **Total Services**  
El número total de servicios que Pilot conoce.
- **Total Virtual Services**  
El número total de servicios virtuales que Pilot conoce.

#### Métrica de Galley

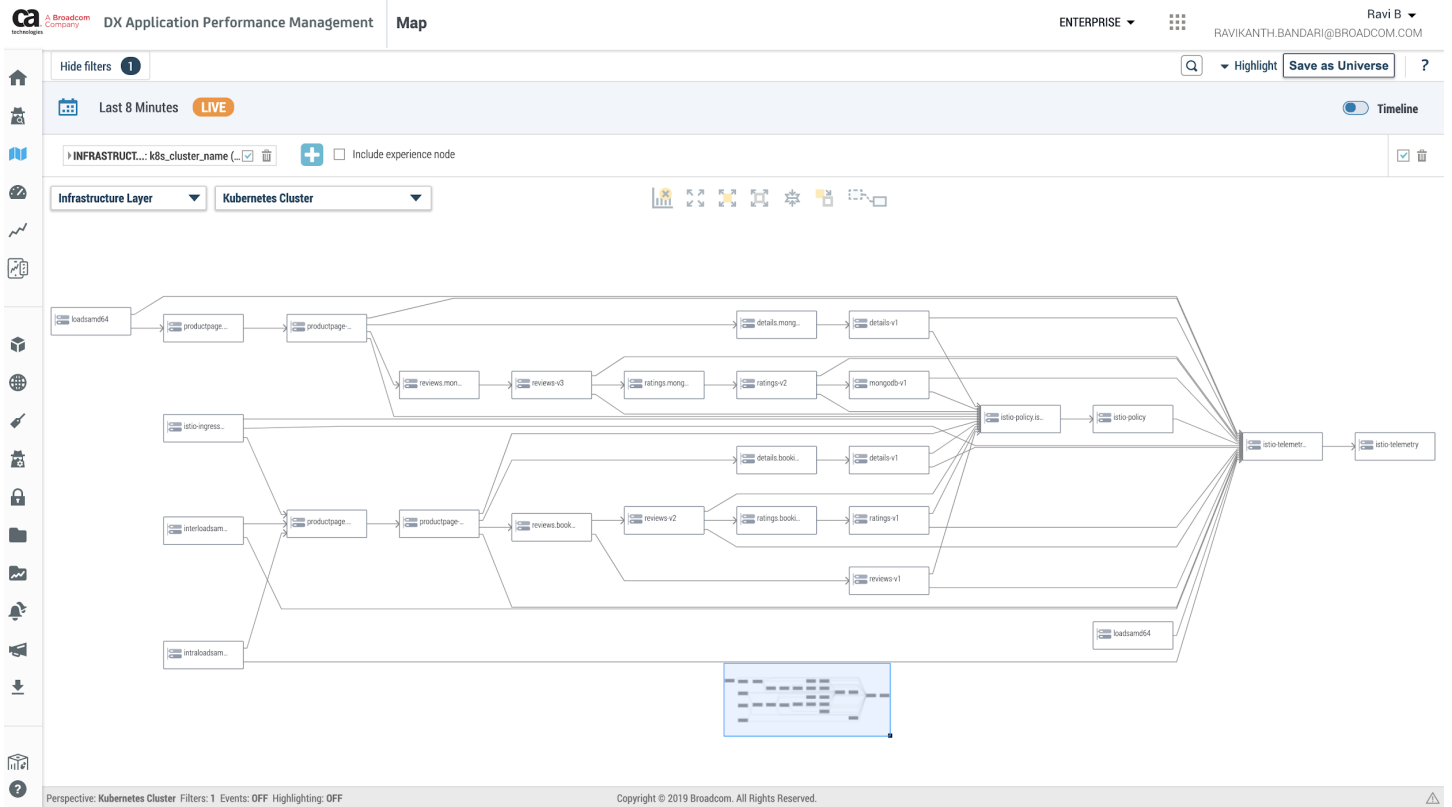
- **Validation Failures Per Minute**  
Número de validaciones en las que se ha producido un error en el webhook de validación de la configuración, por minuto.



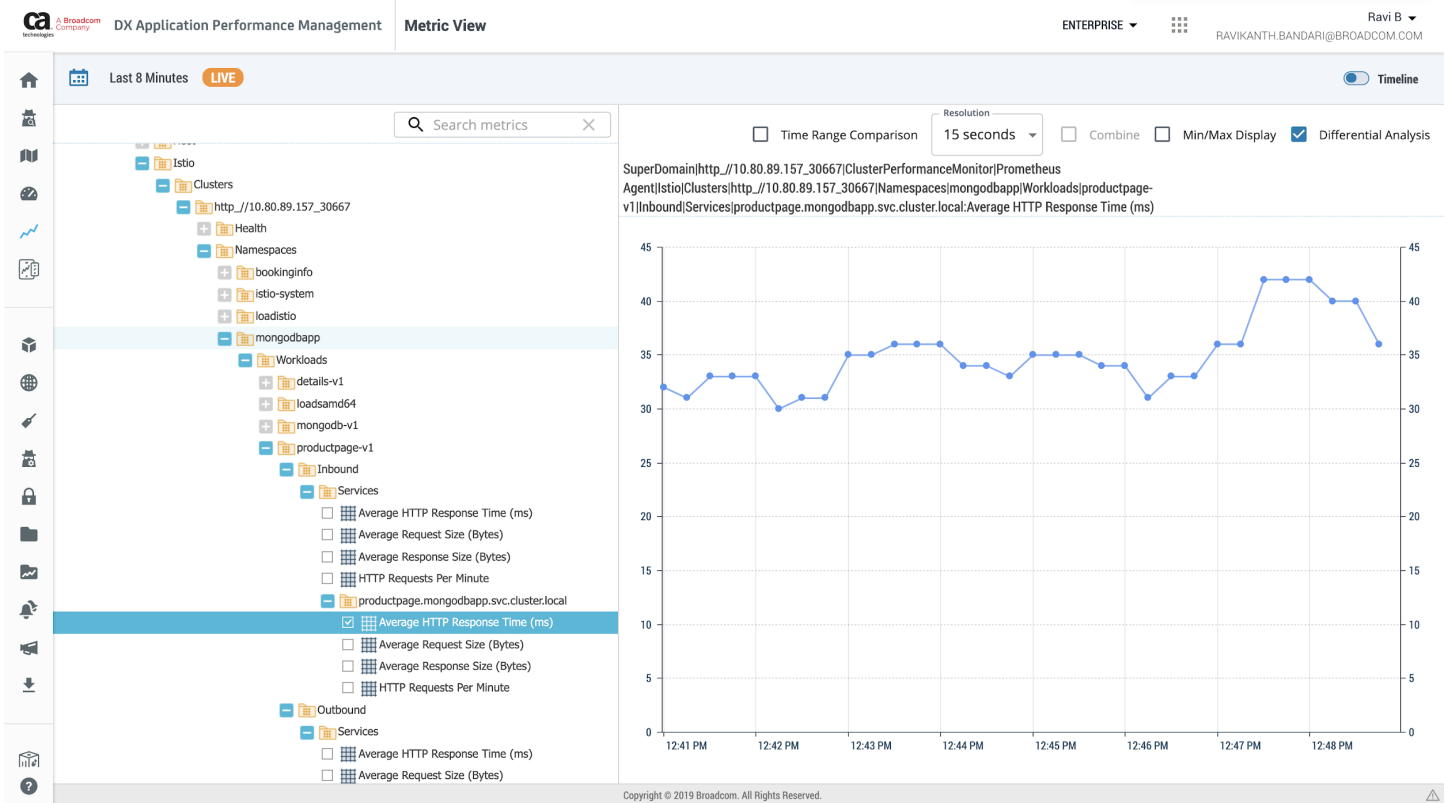
### Istio Support se muestra en el mapa

Istio Support permite visualizar la topología de Istio Service Mesh en el mapa, que muestra los servicios específicos que se comunican entre sí.

En esta captura de pantalla, la **capa de la infraestructura** del mapa muestra ocho minutos del flujo de tráfico de red de Istio en un clúster de Kubernetes.

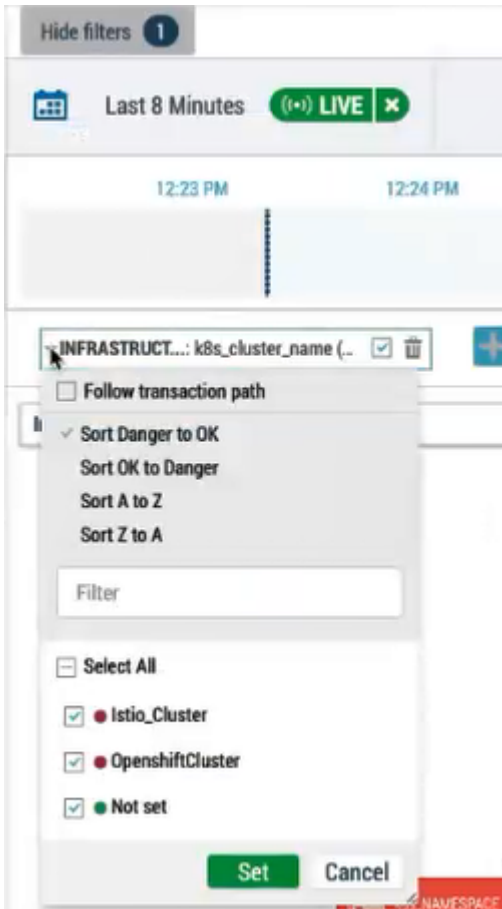


También se pueden ver los mismos componentes que están implicados en el tráfico de red en el árbol del Explorador de métrica, tal y como se muestra en esta captura de pantalla.



### Uso de filtros para limitar los componentes de Istio Support que se muestran en el mapa

Es posible aplicar filtros para hacer que el mapa muestre datos más específicos de la investigación actual. Por ejemplo, se puede configurar un filtro para el nombre de clúster. En esta captura de pantalla, el usuario seleccionó dos nombres de clúster: **Istio\_Cluster** y **OpenshiftCluster**.



Siga estos pasos:

1. En la parte superior izquierda del mapa, haga clic en el lado izquierdo de la lista desplegable de la capa del mapa **Infraestructura**.
2. Configure uno o más filtros.
3. Haga clic en **Establecer**.

El mapa muestra más o menos datos dependiendo de la configuración del filtro.

**Más información:** [Capas del mapa](#)

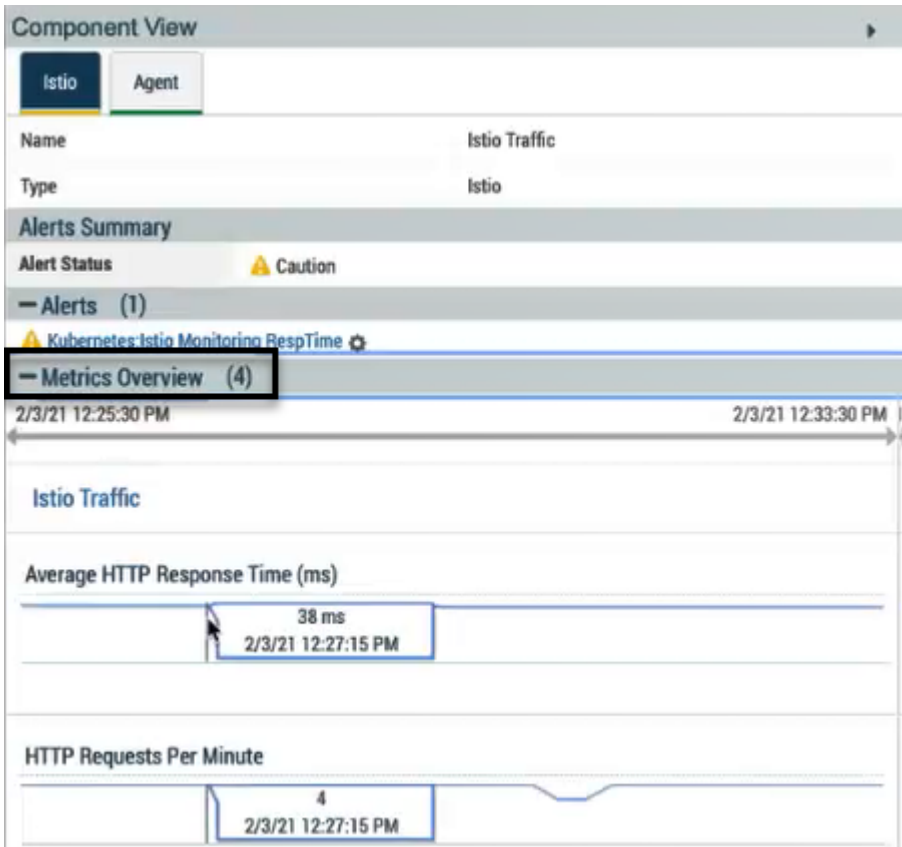
### Visualización de las latencias y las tasas de tráfico de red de Istio Support

Haga clic en un borde (línea que conecta dos componentes) para mostrar la **Vista del componente**, en la que se pueden ver las métricas sobre las tasas de tráfico de red y las latencias entre los componentes. En la siguiente captura de pantalla, el usuario hizo clic en la línea que muestra el tráfico que entra en la carga de trabajo **productpage-v1**. (Tenemos información sobre este tráfico de las capturas de pantalla anteriores usadas como ejemplos). Se abre la **Vista del componente**, donde se muestran datos acerca de una alerta y 18 **atributos básicos** asociados con la **descripción general de las métricas**.

The screenshot displays the DX APM interface. On the left, a service graph shows a component 'productpage-v1' with a green status icon. A yellow line connects it to a 'details' panel. On the right, the 'Component View' panel is open, showing the 'Istio' tab. The 'Name' is 'Istio Traffic' and the 'Type' is 'Istio'. The 'Alerts Summary' section shows an 'Alert Status' of 'Caution' and one alert: 'Kubernetes:Istio Monitoring RespTime'. The 'Metrics Overview' section shows 'Basic Attributes (18)' with a table of live values.

Name	Live Value
agent	Istio_Cluster ClusterPerformanceMonitor Prometh-
backendNode	true
cluster_name	Istio_Cluster
Istio_Connection_Security_Policy	mutual_tls
k8s_agent_data_source	prometheus
k8s_cluster_name	Istio_Cluster
k8s_destination_name	productpage-v1
k8s_destination_project	mongodbapp

El usuario ha hecho clic en un borde en otro momento para mostrar la **Vista del componente** para ver las métricas para una carga de trabajo específica en la **Descripción general de las métricas**. El usuario desea examinar las métricas **Average HTTP Response Time** y **HTTP Requests Per Minute** durante un tiempo específico, tal como se muestra en la siguiente captura de pantalla.



### **Solución de problemas de Istio Support**

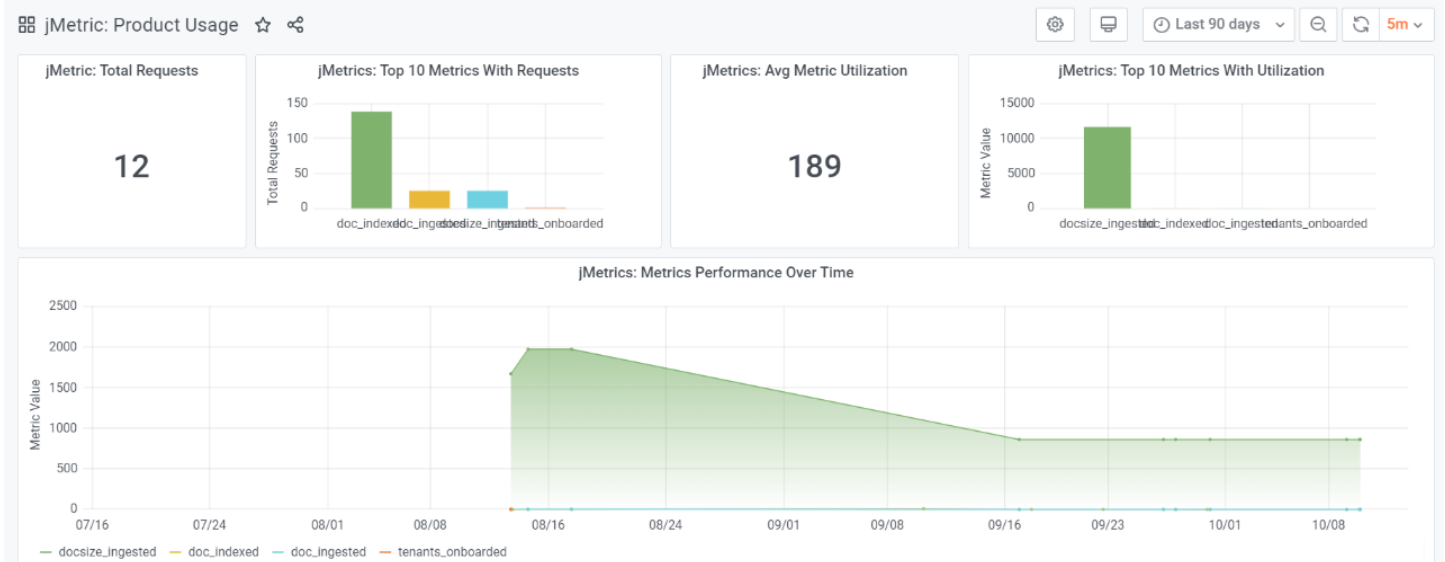
Cuando se experimenta el tipo de problema de Istio Support, realice estas tareas de solución de problemas:

- Compruebe el pod **cluster-performance-prometheus** para ver si hay errores de conexión del servidor de Prometheus. Si hay errores de conexión, asegúrese de que los detalles del usuario, la contraseña y los tokens de Prometheus sean correctos.
- Asegúrese de que las métricas de Istio se notifican en Prometheus. Para hacerlo, inicie sesión en la dirección URL de Prometheus y ejecute la consulta **istio\_requests\_total**. La consola se completa.

**A continuación se muestra un ejemplo de los archivos `uma_cr.yaml` y `values.yaml`**

## Cuadros de mandos de DX





Los Cuadros de mandos de DX presentan las siguientes ventajas:

- Permite visualizar el inventario, el estado, las alarmas, las métricas y los registros
- Admite la función multicliente
- Admite anotaciones de gráficas
- Permite a los usuarios explorar en profundidad diferentes capas
- Proporciona un análisis detallado de Data Lake de AIOps

#### NOTE

Las fuentes de datos de los Cuadros de mandos de DX no son compatibles con una instancia externa de Grafana. Sin embargo, se pueden implementar Cuadros de mandos de DX como una instancia independiente y conectarse con cualquiera de las fuentes de datos. Para obtener más ayuda, póngase en contacto con **Soporte de Broadcom**.

Para obtener más información sobre los Cuadros de mandos de DX, consulte la documentación de [Cuadros de mandos de DX](#).

# Solución de problemas

La sección de solución de problemas facilita la resolución de los síntomas problemáticos de la implementación.

**Más información:** [Enfoque general de la solución de problemas de DX Application Performance Management.](#)

- [Resolución de problemas del agente](#)
- [Solución de problemas de DX APM](#)
- [Solución de problemas de las transacciones](#)
- [Solución de problemas de Workstation](#)

## Resolución de problemas del agente

La información de resolución de problemas del agente proporciona las preguntas frecuentes o relaciona síntomas que experimenta un usuario con una o más soluciones.

### General

- [El agente se inicia, pero no está visible](#)
- [El agente no detecta automáticamente un back-end conocido](#)
- [El agente que monitoriza un front-end no detecta automáticamente el back-end](#)
- [Excepción ClassNotFoundException por parte del agente al cargar las extensiones dinámicas](#)
- [Solución de problemas del cuadro de diálogo de descarga del agente](#)
- [¿Se está decorando el encabezado de la cookie de respuesta del agente del explorador para .NET?](#)
- [El valor de la dirección URL ConfigurationServer no se puede rellenar](#)
- [Pico en los recuentos de la métrica](#)

### Agente de Java

- [La agrupación de direcciones URL no funciona](#)
- [No se puede instrumentar una aplicación con DX APM](#)
- [Bloqueos del agente de Java](#)
- [Error de desbordamiento de la pila del agente de Java](#)
- [Ninguna detección automática del back-end debido a un error inesperado al cargar la extensión](#)
- [Cloud Foundry Java Buildpack no puede encontrar la versión solicitada del Agente de Java](#)
- [Error en el controlador de ACC en la generación del informe de diagnóstico](#)

### Agente .NET

- [El agente del explorador y los seguimientos de las transacciones del agente .NET no están correlacionados](#)
- [Error de visualización de las métricas de .NET tras la activación de la inserción automática de fragmentos de código del Agente del explorador para .NET.](#)

## El agente se inicia, pero no está visible

El Agente de DX APM se inicia correctamente, pero no está visible en el Explorador de métrica, en WebView o en Team Center.

### Síntoma:

El Agente de DX APM se inicia correctamente, pero no está visible en el Explorador de métrica, en WebView o en Team Center. Enterprise Manager es la versión 10.7.

El agente es uno de los siguientes:

- un agente de DX APM SaaS con la versión 20.x o posteriores
- un agente de DX APM local con la versión 11.x o posteriores

Este síntoma se aplica a cualquier agente. Por ejemplo, el Agente de Java, el Agente de .NET, extensiones de monitorización del Agente de la infraestructura, etc.

El registro del agente muestra un mensaje de error parecido a los siguientes ejemplos:

- El registro indica que el agente está conectado, pero en un modo no permitido.

```
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.
```

- El registro indica que el agente no se puede conectar debido a un cliente incompatible.

```
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.).
```

### Solución:

El agente de versión superior está intentando conectarse con CA APM 10.7 Enterprise Manager, pero no se puede conectar debido a la incompatibilidad de la versión. Actualice el archivo `IntroscopeAgent.profile` para el agente local de DX APM SaaS o DX APM en función del entorno. Esta solución se aplica a cualquier tipo de agente. Por ejemplo, el Agente de Java, el Agente de .NET, extensiones del Agente de la infraestructura, etc.

### Configuración de todos los agentes excepto las aplicaciones de Java en Cloud Foundry

1. Vaya al archivo `<Directorio_principal_Agente>\releases\<número_versión>\core\config\IntroscopeAgent.profile` para el agente de DX APM SaaS o el agente local de DX APM.
2. Abra el archivo `IntroscopeAgent.profile` en un editor de texto.
3. Agregue la propiedad `introscope.agent.connection.compatibility.version=10.7`.
4. Anule la propiedad `agentManager.credential`.

La configuración `introscope.agent.connection.compatibility.version=10.7` proporciona compatibilidad solamente cuando la propiedad `agentManager.credential` se comenta o no se ha configurado. A continuación aparecen dos ejemplos:

```
#agentManager.credential=<your agent token>
agentManager.credential=
```

Si se produce un error al establecer correctamente `agentManager.credential`, se produce un error de **FailedToAuthenticateException**.

#### NOTE

Al configurar las credenciales del agente utilizando el archivo `IntroscopeAgent.profile` o los argumentos de la máquina virtual, no utilice comillas dobles (") para proporcionar un valor vacío para la propiedad `agentManager.credential`. Por ejemplo, `agentManager.credential=`.

5. Elimine el protocolo **ws://** o **wss://** desde el principio de la propiedad `agentManager.url`.

Para utilizar el agente de DX APM con CA APM 10.7 Enterprise Manager, se debe eliminar el protocolo **ws** de la propiedad `agentManager.url`. Este cambio de configuración permite que el agente de DX APM utilice el protocolo TCP predeterminado de CA APM 10.7 para la comunicación de socket directa.

Ejemplo de configuración incorrecta:

```
agentManager.url.1=ws://apmhost:5001
```

#### Ejemplo de configuración correcta:

```
agentManager.url.1=apmhost:5001
```

Se ha producido un error al eliminar el protocolo **ws** de la cadena de propiedad da lugar a un error similar a este ejemplo:

```
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
```

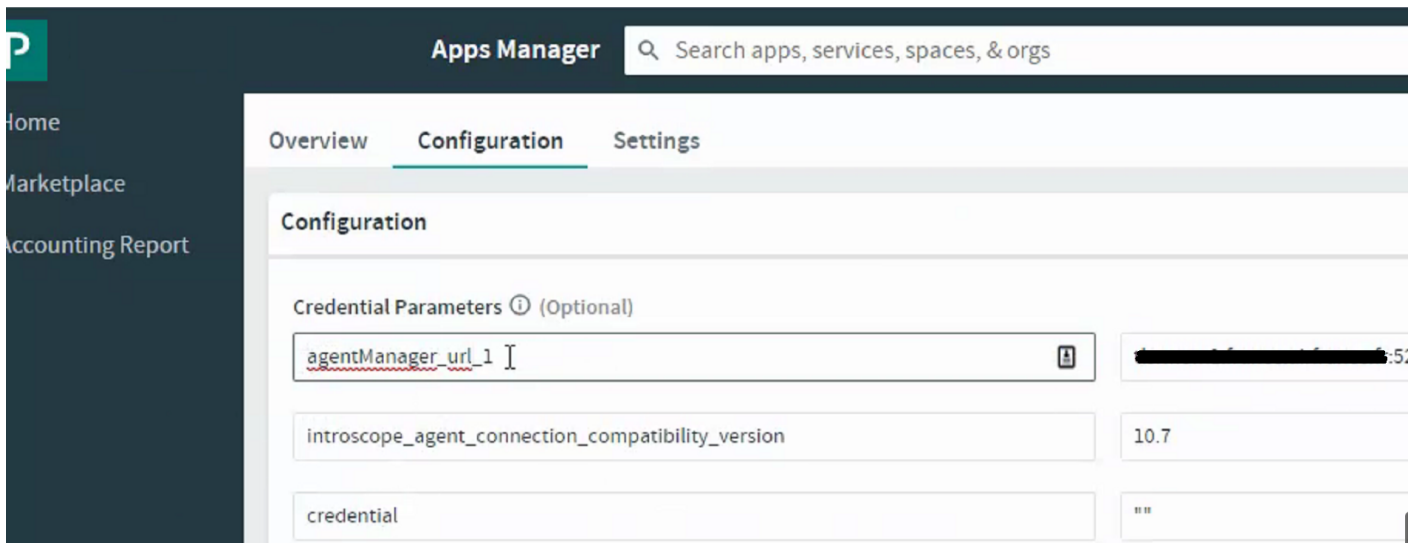
6. Guarde el archivo `IntroscopeAgent.profile`.
7. Reinicie la aplicación gestionada.

## Aplicaciones de Java en Cloud Foundry

Cuando monitoree aplicaciones de Java en Cloud Foundry, configure la compatibilidad mediante *una* de estas opciones:

- Ejecute este comando en una línea de comandos de Cloud Foundry:
 

```
cf cups introscope -p '{"agent_manager_url":"host:port",
"introscope_agent_connection_compatibility_version":"10.7", "credential":""}'
```
- Actualice la configuración en el gestor de aplicaciones de Pivotal Web Services (PWS) tal y como se muestra en este gráfico y se describe en los pasos siguientes.



1. Vaya a la ficha **Configuración**.
2. En el campo **Credential Parameters (Optional)**, introduzca este valor:
 

```
agentManager_url_1
```
3. Asegúrese de que el campo situado a la *derecha* del campo **Credential Parameters (Optional)** esté vacío.
4. En el *siguiente* campo **Credential Parameters (Optional)**, introduzca este valor:
 

```
introscope_agent_connection_compatibility_version
```
5. En el campo a la *derecha* de `introscope_agent_connection_compatibility_version`, introduzca este valor:
 

```
10.7
```
6. En el campo *debajo* de `introscope_agent_connection_compatibility_version`, introduzca este valor:
 

```
credential
```
7. En el campo a la *derecha* de `credential`, introduzca este valor (comillas dobles):

""

#### NOTE

Al configurar las credenciales del agente para las aplicaciones de Java en Cloud Foundry utilizando la interfaz de usuario del gestor de aplicaciones de Pivotal Web Services (PWS), utilice comillas dobles ("" ) para proporcionar un valor vacío para la propiedad `agentManager.credential`. Por ejemplo, `agentManager.credential=""`.

8. Guarde la configuración.
9. Reinicie la aplicación gestionada.

## El agente no detecta automáticamente un back-end conocido

### Síntoma

Sé que una transacción incluye un back-end sin monitorizar, pero el agente no lo detecta automáticamente.

El registro de nivel Información del agente no contiene mensajes sobre la detección de candidatos de back-end. Esperaba encontrar un mensaje parecido a este ejemplo:

```
[INFO] [IntroscopeAgent.AutomaticBackendDetection] Backend Candidates: [<my-expected backend1>,<my-expected backend2>...]
```

Estos valores de métricas de sostenibilidad del agente muestran el valor 0:

- Automatic Backend Detection: Analyzed Stack Snapshots
- Automatic Backend Detection: Backends Discovered

### Solución

La detección automática del back-end requiere que el agente detecte y monitorice cualquier tipo de front-end en primer lugar. Verifique que la transacción está monitorizando un front-end, un punto de entrada o un componente personalizado.

#### NOTE

Es posible que el agente necesite unos minutos para detectar e instrumentar automáticamente una transacción que incluya back-ends automáticos.

## El agente que monitoriza un front-end no detecta automáticamente el back-end

### Síntoma

Una transacción que estoy investigando incluye un front-end monitorizado y, a continuación, un back-end sin monitorizar. El agente no detecta el back-end.

Estos son los valores de las métricas de compatibilidad del agente relevantes:

- Sostenibilidad|Detección automática del back-end: las instantáneas de pila analizadas son > 0.
- Sostenibilidad|Detección automática del back-end: los back-ends detectados son 0.

### Solución

Agregue la instrumentación personalizada para monitorizar el back-end.

Es posible que la detección automática del back-end no detecte los back-ends en casos poco comunes. Por ejemplo, las llamadas de comunicación de socket a través de los sockets de datagramas.

## Excepción `ClassNotFoundException` por parte del agente al cargar las extensiones dinámicas

### Síntoma

Al eliminar rápidamente y, a continuación, agregar extensiones dinámicas en el directorio `<Agent_Home>/extensions/deploy`, el agente provoca un error `ClassNotFoundException`. El registro del agente muestra un mensaje de error similar al mensaje de ejemplo siguiente:

```
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
```

### Solución

1. Descargue todas las extensiones dinámicas que están a la espera de cargarse para su implementación en el directorio `<Dir_principal_Agente>/extensions/deploy`.
2. Asegúrese de que todas las extensiones dinámicas se descargan.
3. Vuelva a cargar las extensiones dinámicas en el directorio `<Agent_Home>/extensions/deploy`.

## El agente del explorador y los seguimientos de las transacciones del agente .NET no están correlacionados

### Síntoma

No puedo ver el seguimiento de las transacciones del agente del explorador correlacionado con el seguimiento de las transacciones del agente .NET. El motivo es que el Agente de .NET omite automáticamente la codificación `gzip`.

### Solución

Compruebe el tipo de contenido de respuesta para la propiedad de codificación no compatible:

```
introscope.agent.browseragent.encodings.skip.
```

## El valor de la dirección URL `ConfigurationServer` no se puede rellenar

### Síntoma

Falta la configuración de `configurationServer.url` realizada en el controlador del agente en ACC cuando se descarga e implementa el paquete en los servidores.

Esta incidencia se produce cuando no se agrega ningún esquema (`http[s]` o `ws[s]`) a la dirección URL. La cadena de conexión se considera como una cadena heredada que se utiliza para la comunicación isengard (el puerto predeterminado es 5001). El controlador de ACC se comunica solo a través de la llamada de REST a través de `http(s)/ws(s)`.

### Solución

Como solución, es necesario habilitar `http(s)/ws(s)` en Cloud Proxy siguiendo *uno* de estos procesos:

- Habilite `HTTP(s)/ws` en Cloud Proxy y use una conexión a través de `HTTP(s)/ws(s)`. Se puede actualizar Cloud Proxy en el panel de creación de paquetes y la dirección URL de conexión se establece para los grupos `em-connection` y `acc-controller`.
- Habilite `HTTP(s)/ws(s)` en Cloud Proxy y establezca la dirección URL de conexión en la propiedad `introscope.agent.acc.controller.configurationServer.url` del grupo `acc-controller`.

## ¿Se está decorando el encabezado de la cookie de respuesta del agente del explorador para .NET?

### ¿Se está decorando el encabezado de la cookie de respuesta del agente del explorador para .NET?

#### **Síntoma:**

No estoy seguro de si se está decorando el encabezado de la cookie de respuesta del agente del explorador para .NET.

#### **Solución:**

Investigue si el agente .NET ha enviado la cookie de respuesta. Pulse la tecla <F12> y compruebe el explorador.

## Bloqueos del agente de Java

### Síntoma

El agente de Java se bloquea o se sobrecarga el uso de la CPU.

### Solución

Los problemas de los agentes pueden ser el resultado de:

- Una configuración no compatible
- Un error JVM que se produce debido al uso de DX APM en el mecanismo de instrumentación de la plataforma de Java para la monitorización
- Expansión de una métrica o instrumentación

Para solucionar estos problemas, pruebe las sugerencias siguientes:

- ¿Se ha actualizado algo recientemente?
- ¿Hay alguna instrumentación personalizada o extensiones implementadas por los servicios profesionales de Broadcom?
- ¿Se admite la configuración?
- Determine si el problema está relacionado con la instrumentación o con un error de la máquina virtual de Java como se muestra a continuación:
  - a. Detenga el servidor de aplicaciones.
  - b. Abra `IntroscopeAgent.profile` y establezca `introscope.autoprobe.enable=false`.
  - c. Inicie el servidor de aplicaciones.

Si el problema persiste, el problema no está relacionado con la instrumentación de DX APM. Pruebe las soluciones siguientes:

  - Intente cambiar de `-javaagent a -Xbootclasspath`.
  - Actualice a la última versión de JVM o utilice una JVM alternativa.
  - Abra un incidente de soporte con el distribuidor de JVM.
- Para ayudar a identificar la causa del problema, reduzca temporalmente la cantidad de instrumentación:
  - a. Detenga el servidor de aplicaciones.
  - b. Abra `IntroscopeAgent.profile` y establezca `introscope.autoprobe.enable=false`.
- Algunas aplicaciones utilizan un gran número de cadenas de instrucción SQL únicas, especialmente cuando se crea dinámicamente el SQL. Esta acción genera un extraordinario aumento de la métrica de `SQLAgent`. Para realizar pruebas, desactive `SQLAgent` eliminando `<Agent_Home>/core/ext/SQLAgent.jar` fuera del directorio del agente. Si esta acción no es posible, establezca `introscope.agent.sqlagent.sql.maxlength=120` (valor predeterminado 990).

No hay límites en la longitud de las instrucciones SQL más allá de los límites que impone la base de datos, `maxlength` permite truncar la longitud de las instrucciones SQL. El objetivo de esta acción es evitar una expansión de la métrica de SQL.

- Desactive los rastreadores de red, del sistema de archivos y de las métricas del sistema de archivos en `PBD` alternativos. No se recomienda que estén activados en producción.
 

```
TurnOn: SocketTracing
TurnOn: UDPTracing
TurnOn: FileSystemTracing
```
- Desactive la recopilación de JMX. El sondeo de muchas métricas JMX tiene un consumo elevado en la CPU. Si es posible, establezca de momento `introscope.agent.jmx.enable=false`. Nunca establezca la cadena de filtro en un valor nulo, como por ejemplo: `introscope.agent.jmx.name.filter=`. Un agente único puede producir decenas de miles de métricas JMX con ningún filtro configurado.
- Desactive cualquier complemento del Agente de Java adicional como, por ejemplo: `ErrorDetector`, `Leakhunter` u otras extensiones. `Leakhunter` es una herramienta de diagnóstico, no una herramienta de monitorización 24/7. Recomendación: no active esta herramienta en un entorno de producción. Las extensiones pueden generar demasiadas métricas que son un gasto general elevado.
- Desactive cualquier `pbid` personalizado adicional. Evite el uso de las directivas: `TraceAllMethodsOfClass` y `TraceComplexMethodsOfClass`. Elija cuidadosamente los métodos para monitorizar.

Si el problema persiste, antes de ponerse en contacto con el soporte de Broadcom, recopile la información siguiente:

- `<Agent_Home>/logs` en un archivo zip
- `IntroscopeAgent.profile`
- Genere una serie de cinco volcados de subprocesos en el servidor de aplicaciones cuando se produce la sobrecarga de memoria, una falta de memoria, un bloqueo o un elevado uso de la CPU, espaciados entre 5-10 segundos.
- Para los problemas de sobrecarga, genere un volcado de la memoria dinámica. Agregue el siguiente conmutador de JVM para Sun JVM:
 

```
XX:+HeapDumpOnOutOfMemoryError
```

 Reinicie el agente.
- Active el registro de GC. Agregue los siguientes conmutadores de JVM para Sun JVM:
 

```
-Xloggc:<File_Name>.log -XX:+PrintGCDetails
```
- Archivos de registro del servidor de aplicaciones para cargar al soporte de Broadcom:
  - WebSphere: `System.out`, `system.err`, `native_stdout`, `native_stderr` y `server.xml`
  - WebLogic: script de inicio del servidor de aplicaciones y archivo de registro
  - Tomcat: archivo de registro y `catalina.sh/bat`
  - JBoss: archivo de registro y `run.bat/sh`
- Volcado del núcleo completo, si procede

## Error de desbordamiento de la pila del agente de Java

Válido para: DX APM 8.x, 9.x

### Síntoma

Se produce un error en una transacción de una aplicación monitorizada y se registra un mensaje `StackOverflowError` en el registro del servidor de aplicaciones.



### **Solución**

El agente agrega instrucciones a una aplicación en ejecución. Cuando una aplicación con una ruta de llamada recursiva profunda tiene un tamaño de pila cercano al máximo, las instrucciones del agente agregado pueden exceder el límite del tamaño de pila.

1. Aumente el tamaño de pila JVM en el argumento de inicio de java -Xss. Por ejemplo:  
-Xss10024k
2. Reinicie el servidor de aplicaciones.

## **Error de visualización de las métricas de .NET tras la activación de la inserción automática de fragmentos de código del Agente del explorador para .NET.**

### **Síntoma:**

No se muestra la métrica de .NET después de activar la inyección automática de fragmentos de código del Agente del explorador para .NET.

### **Solución:**

Revise la fuente del explorador. Busque la etiqueta del script del Agente del explorador.

## **Ninguna detección automática del back-end debido a un error inesperado al cargar la extensión**

### **Síntoma**

La detección automática del back-end no detecta back-ends automáticos. Aparece un mensaje de error similar a este ejemplo en el registro del agente debido a una falta de coincidencia en la versión de la máquina virtual Java:

```
[ERROR] [IntroscopeAgent.Agent] Unexpected error loading extension
java.lang.UnsupportedClassVersionError: com/wily/introscope/agent/intelligent/entrypoint/
tracers/AbstractDetectionHelperTracer : Unsupported major.minor version 51.0
```

### **Solución**

Compruebe que la versión de la máquina virtual Java es 1.7 o posterior.

## **Pico en los recuentos de la métrica**

### **Síntoma**

Los valores del pico son valores agregados y no valores separados.

### **Solución**

La API de temporización web informa sobre el tiempo de red como parte de una carga anterior de la página. El Agente del explorador (anteriormente BRTM) no puede excluir estos valores.

## No se puede instrumentar una aplicación con DX APM

### Síntoma

No puedo instrumentar una aplicación con DX APM.

### Solución

Compruebe lo siguiente:

- O bien el script de inicio de appserver o los archivos de configuración contienen las dos entradas clave de DX APM:  

```
-javaagent and - Dcom.wily.introscope.agentProfile
```
- Si no hay ningún archivo de registro en `\wily\logs`. Si lo hay, compruebe el `Autoprobe.log`; si su tamaño es de 0 o 1 KB, es probable que se esté utilizando un pbd personalizado o que se haya modificado uno de los existentes incorrectamente.

### Recopilación de datos antes de ponerse en contacto con Soporte de Broadcom

Si ha revisado las sugerencias anteriores y todavía detecta problemas, recopile los datos siguientes antes de ponerse en contacto con Soporte de Broadcom. Esta información permitirá a Soporte de Broadcom ayudarle de forma eficiente y eficaz.

- `<Agent_Home>\logs` en un archivo ZIP
- Archivo de registro del servidor de aplicaciones
- Script de inicio del servidor de aplicaciones o archivo de configuración que contiene las entradas de DX APM

## La agrupación de direcciones URL no funciona

### Síntoma

La agrupación de direcciones URL no funciona.

### Solución

Revise la sección Problemas conocidos sobre la [agrupación de direcciones URL](#) de las Notas de la versión. Pruebe la incidencia utilizando una definición de agrupación de direcciones URL sencilla.

Si el problema persiste, antes de ponerse en contacto con el Soporte al cliente, recopile la información siguiente:

- `<EM_Home>/logs/*` en un archivo ZIP; estos archivos ayudan a determinar si el problema está relacionado con el rendimiento.
- Archivo `IntroscopeAgent.profile`
- Captura de pantalla de la muestra de direcciones URL de la ficha Investigator.

## Cloud Foundry Java Buildpack no puede encontrar la versión solicitada del Agente de Java

### Síntoma

Cuando se implemente una aplicación de Java en Cloud Foundry, actualice el manifiesto de la aplicación a la versión 10.x. Para ello, ejecute el comando siguiente:

```
JBP_CONFIG_INTROSCOPE_AGENT: '{ version: 10.x.0_xx}
```

Ejecute el comando **cf push** para obtener el buildpack de Java que contiene el Agente de Java 10.x. La CLI de Cloud Foundry muestra el error **No version resolvable error** similar a este mensaje de ejemplo:

```
[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
```

## Solución

Está utilizando un buildpack de Java sin conexión. Los buildpacks sin conexión incluyen algunas, pero no todas, versiones del Agente de Java. Si desea utilizar una versión del Agente de Java anterior o posterior, descargue y utilice la versión adecuada del buildpack sin conexión.

Descargue los buildpacks de Java sin conexión de este sitio web: <https://github.com/cloudfoundry/java-buildpack/releases>. También puede utilizar el buildpack de Java en línea.

### NOTE

**Más información:** [Implementación y monitorización de una aplicación Java en Cloud Foundry](#)

## Solución de problemas del cuadro de diálogo de descarga del agente

A continuación, se muestra una lista de posibles causas para mostrar las incidencias y las acciones para corregirlas:

- **Las propiedades de configuración no aparecen**
  - Examine el registro de ACC para ver los errores y las advertencias de contenido del cuadro de diálogo de descarga.
  - Analice downloadPackageConfig.json en busca de errores de configuración.
- **El contenido no está localizado**
  - Examine el registro de ACC para ver los errores y las advertencias de contenido del cuadro de diálogo de descarga.
  - Examine los archivos de propiedades en busca de claves que faltan o no están localizadas.
- **El formato de las instrucciones de instalación está dañado**
  - Compruebe la sintaxis del contenido de Markdown en el archivo de propiedades.
  - Asegúrese de que las claves de instrucciones de instalación tengan un sufijo de Markdown.
- **La lista de aplicaciones de AXA no está visible en la configuración del Agente del explorador**
  - **Causa posible:**
    - AXA no está disponible.
    - La integración de AXA no está configurada correctamente.
  - **Intente lo siguiente:**
    - Compruebe la configuración de EM.
    - Compruebe la consola del desarrollador del explorador en busca de errores.

## Solución de problemas de DX APM

La información sobre la solución de problemas de DX APM proporciona preguntas frecuentes o relaciona síntomas que experimenta un usuario con una o más soluciones.

[No se muestra la métrica del componente](#)

[La variación del análisis diferencial no aparece en los nodos](#)

[No hay datos de métrica en la Vista de la experiencia](#)

[Datos enviados por los agentes incompletos o ausentes en el mapa](#)

[Error de visualización de la información del agente en el mapa](#)

[El mapa muestra solo 50.000 nodos](#)

[El selector de atributos de la tarjeta de experiencia no muestra los atributos relacionados con Docker](#)

[La propagación de atributos entre capas no funciona](#)

[Dónde buscar las incidencias potenciales relacionadas con las asignaciones](#)

## No se muestra la métrica del componente

### Síntoma

La métrica no aparece para un componente.

### Solución

Denomine los componentes mediante un máximo de 250 caracteres. Si un nombre de componente supera los 250 caracteres, el nombre se reducirá a 250 caracteres. Como resultado, los nodos asociados no muestran métricas ni alertas asociadas cuando el atributo del nombre se utiliza para calcular la métrica, por ejemplo, SOCKET, EJBCLIENT, DATABASE, BUSINESS TRANSACTION, GENERICBACKEND, GENERICFRONTEND.

## La variación del análisis diferencial no aparece en los nodos

### Síntoma

La métrica de variación del análisis diferencial no aparece en los nodos.

### Solución

El estado del análisis diferencial no está asociado a una métrica cuando la ruta de la métrica supera los 1000 caracteres. Las configuraciones del análisis diferencial y la barra del análisis diferencial no están visibles en la descripción general de rendimiento para esta métrica.

## No hay datos de métrica en la Vista de la experiencia

### Síntoma

No se pueden ver los datos en la Vista de la experiencia. Aparece el siguiente error en el explorador:

```
That's a lot of data. The number of metrics exceeds the display maximum.
```

El mensaje de error se muestra al intentar mostrar más de 500 transacciones comerciales en modo en directo o más de 50 transacciones comerciales en modo histórico. La Vista de la experiencia limita el número de transacciones comerciales mostradas por motivos de rendimiento.

### **Solución**

Existen varias formas de limitar el número de transacciones comerciales que se muestran.

- Desplazarse a otros niveles de tarjetas de experiencia. El nivel siguiente muestra métricas porque hay menos transacciones comerciales.
- Aplicar filtros en el nivel superior de las tarjetas de experiencia.
- Crear universos con menos transacciones comerciales.

## **Datos enviados por los agentes incompletos o ausentes en el mapa**

### **Síntoma**

Después de conectar un nuevo agente o implementar una nueva aplicación, la topología correspondiente no aparece en el mapa o solo parte de los datos aparecen al instante. Los datos completos aparecen al cabo de uno o dos minutos.

### **Solución**

Inicie un seguimiento de transacciones en el agente para agilizar la recopilación de datos inicial en la **Vista de mapa**. Cuando se ejecuta un seguimiento de transacciones en un agente, se recopila un gran volumen de seguimientos de transacciones. Esta acción permite al servidor reconstruir rápidamente la Vista de mapa. Para ejecutar una sesión de seguimiento de transacciones manualmente, especifique los agentes de cuyas transacciones desea realizar un seguimiento y el período de captura de datos. Una vez que se inicia la sesión de seguimiento de transacciones, las transacciones que coinciden con los criterios de filtro aparecen en el visor de seguimiento de transacciones. Los eventos de transacción incluyen errores y seguimientos de transacciones.

Si un seguimiento se inicia con un período de tiempo establecido, este se detiene al final del período especificado. Solamente se puede iniciar una sesión de seguimiento para un agente específico con un período de tiempo determinado. Si se reinicia una sesión de seguimiento activa, se recibe una notificación en la que se recuerda que la sesión de seguimiento de transacciones está activa para el agente. La notificación muestra el tiempo restante de la sesión activa. Se puede iniciar un nuevo seguimiento para el mismo agente después de que finalice una sesión de seguimiento activa.

### **Siga estos pasos:**

1. En el panel izquierdo, en CONFIGURACIÓN, haga clic en **Agentes**.  
Aparece una página con una lista de los agentes.
2. (Opcional) Haga clic en la flecha **Aplicaciones**.  
Se enumeran todas las aplicaciones que monitoriza el agente.
3. Seleccione uno o más agentes de cuyas transacciones desea realizar un seguimiento:
  - Para realizar el seguimiento de todos los agentes, haga clic en **Realizar el seguimiento de todos los agentes**. Esta opción permite realizar un seguimiento de todos los agentes admitidos que están conectados actualmente y de cualquier agente que se conecte durante la sesión de seguimiento.
  - Para realizar el seguimiento de los agentes seleccionados, haga clic en **Realizar el seguimiento del agente para un agente**.
 Aparece el cuadro de diálogo Sesión de seguimiento de la transacción.
4. Especifique los valores para el seguimiento de las transacciones en los campos del cuadro de diálogo o acepte los valores predeterminados y haga clic en **Iniciar**:

- Especifique la **duración mínima de la transacción** en milisegundos para el seguimiento de las transacciones. El valor predeterminado es 1000 milisegundos. El valor mínimo es 1 milisegundo.
- Especifique la **Duración de la sesión de seguimiento** en minutos. El valor predeterminado es 1 minuto con una duración máxima de 5 minutos para una sesión de seguimiento única.

Un panel muestra el estado de la sesión.

5. (Opcional) Cierre el cuadro de diálogo después de que el seguimiento se haya iniciado correctamente. La sesión de seguimiento continúa ejecutándose en segundo plano.

#### NOTE

#### Más información:

[Análisis de los seguimientos y colaboración en el análisis de problemas](#)

## Error de visualización de la información del agente en el mapa

### Síntoma

El mapa no muestra la información del agente correctamente.

### Solución

Sincronice los relojes del sistema para todos los agentes que monitoriza DX APM para una ruta de transacciones específica.

Se recomienda sincronizar los relojes del servidor de aplicaciones con el Protocolo de tiempo de redes (NTP).

## El mapa muestra solo 50.000 nodos

### Síntoma

El mapa muestra solo 50.000 nodos.

### Solución

DX APM está configurado para mostrar mapas con un máximo de 50000 nodos para mantener el rendimiento. Más allá de ese límite, los datos quedan fijados.

#### Siga estos pasos:

1. Haga clic en Cuadro de mandos.
2. Agregue filtros para reducir el número de nodos que se muestran por debajo de 50.000.

## El selector de atributos de la tarjeta de experiencia no muestra los atributos relacionados con Docker

### Síntoma

Cuando creo o edito una tarjeta de experiencia, no veo los atributos relacionados con Docker en la lista desplegable.

### Solución

En la **Vista de mapa**, consulte Experiencias para verificar si alguna experiencia contiene los atributos que no aparecen en la lista desplegable.

**NOTE****Más información:**

- [KB000115511 APM 10.7 Docker Attributes and Experience Cards](#)
- [Configuración de la Vista de experiencia](#)

## La propagación de atributos entre capas no funciona

**Síntoma**

La propagación de atributos de la capa de la infraestructura a la capa de la aplicación no funciona.

**Solución**

Compruebe la **Vista de componentes** para verificar que los nodos relativos están conectados y que comparten atributos.

**NOTE****Más información:**

- [KB000115511 APM 10.7 Docker Attributes and Experience Cards](#)
- [Configuración de la Vista de experiencia](#)

## Dónde buscar las incidencias potenciales relacionadas con las asignaciones

Se pueden comprobar las siguientes opciones para encontrar incidencias potenciales relacionadas con las asignaciones:

- Abra la consola del desarrollador y busque las excepciones.
- En caso de "500 Internal Server Error", busque información adicional en la respuesta del servidor.

## Solución de problemas de las transacciones

La información sobre la solución de problemas de las transacciones proporciona las preguntas frecuentes o relaciona síntomas que experimenta un usuario con una o más soluciones.

[Un método que nunca se cierra se identifica como método padre](#)

### Un método que nunca se cierra se identifica como método padre

**Síntoma**

Después de identificar el método principal de una llamada de recepción de JMS, tal y como se describe en [Métricas de la transacción](#), un método que nunca se cierra se identifica como el principal.

**Solución**

Defina el método principal manualmente mediante uno de los siguientes procedimientos:

- Abra el archivo `JMSParentMethodPersist.pbd` en la carpeta **hotdeploy** en un editor de texto y añada la definición de rastreador del método principal en la parte inferior:

```
TraceOneMethodOfClass: <class name> <method> JMSReceiveParentTracer "JMSParentInstrumentation"
```

- Cambie el valor del índice constante (consulte el paso 2 anterior) con el valor que pertenece al método principal correcto tal y como se muestra en el seguimiento de la pila, cambiando el valor de la propiedad `jms.receive.parent.lookupFallback.maximumDepth` en el archivo del perfil del agente.

## Solución de problemas de Workstation

La información sobre la solución de problemas de Workstation proporciona las preguntas frecuentes o relaciona los síntomas que experimenta un usuario con una o más soluciones. A continuación se muestran algunos de los artículos sobre la solución de problemas:

[Se ha producido un error en Workstation al recopilar un volcado de subprocesos nuevo](#)

[Cambios del tipo de operación en las calculadoras del módulo de gestión](#)

[Los cuadros de mandos tienen paneles vacíos](#)

[No hay resultados para la consulta de eventos históricos](#)

[Solución de los problemas del tiempo de espera automático de la sesión en Workstation](#)

[El tiempo de espera de Workstation se agota al iniciar sesión en Enterprise Manager](#)

## Se ha producido un error en Workstation al recopilar un volcado de subprocesos nuevo

### Error en Workstation

**Síntoma:** Cuando el Agente de Tomcat se ejecuta con un tamaño de pila de 50 MB, aparece el error **ConnectionExceptionErrorStatus** en Workstation y los registros de EM muestran el siguiente registro de errores.

```
[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
```



## **Resolución**

Aumente la pila en el servidor de aplicaciones (servidor del agente en ejecución). Este error solo aparece cuando la máquina virtual Java (servidor de aplicaciones) se está ejecutando con un espacio bajo de pila.

## **Cambios del tipo de operación en las calculadoras del módulo de gestión**

### **Síntoma**

Cuando se edita una calculadora en un módulo de gestión, al cambiar el tipo de operación se redefine el significado de la métrica de salida de la calculadora. Por ejemplo, se cambia el tipo de operación de mínimo a máximo y se mantiene el nombre de la métrica de salida de la calculadora. La métrica de salida muestra los valores antiguos en el historial (por ejemplo, MIN) con los nuevos valores (por ejemplo, MAX). No aparece la ninguna indicación de donde se produjo la modificación en el procesamiento.

### **Solución**

Cambie el nombre de la métrica de salida de la calculadora al cambiar el tipo de operación si piensa que estos valores pueden causar confusión.

## **Los cuadros de mandos tienen paneles vacíos**

### **Síntoma**

Los cuadros de mandos tienen paneles vacíos.

### **Solución**

Está viendo paneles vacías debido a que la aplicación no utiliza esas métricas.

Los cuadros de mandos muestran un conjunto general de métricas de rendimiento de forma predeterminada.

## **No hay resultados para la consulta de eventos históricos**

### **Síntoma**

No se muestra ningún resultado cuando se emite una consulta para eventos históricos.

### **Solución**

- ¿El problema se produce al usar filtros básicos, como el tipo: sampled? Esto permite confirmar que los datos se escriben en la base de datos de seguimientos.
- El problema puede deberse a que el índice de seguimientos esté dañado. Detenga Enterprise Manager, suprima el directorio \traces\index y ejecute la herramienta de reindexación para volver a indexar la base de datos de seguimientos.

### **Recopilación de datos antes de ponerse en contacto con Soporte de Broadcom**

Si ha revisado las sugerencias anteriores y todavía detecta problemas, recopile los datos siguientes antes de ponerse en contacto con Soporte de Broadcom. Esta información permitirá a Soporte de Broadcom ayudarle de forma eficiente y eficaz.

- `<EM_Home>/logs/*` en un archivo .zip
- `<Agent_Home>/logs/*` e `IntroscopeAgent.profile` en un archivo .zip
- Capturas de pantalla de la ventana Transaction Tracer y detalles de la clase que espera ver

## Solución de los problemas del tiempo de espera automático de la sesión en Workstation

### Síntomas

El tiempo de espera automático de la sesión se ha interrumpido y se muestra al menos uno de los síntomas siguientes:

- Las ventas de Workstation no se cierran automáticamente cuando se alcanza el período de inactividad.
- No se muestra ningún mensaje de cierre de sesión en la ventana de inicio de sesión.

### Solución

Solo los administradores de DX SaaS pueden modificar el archivo `<EM_Home>/config/IntroscopeEnterpriseManager.properties`. Póngase en contacto con el administrador para asegurarse de que el valor de la propiedad `introscope.apmserver.ui.inactivityLogoutTimeout` se establece en un número entero mayor de 0 para activar el tiempo de espera de la sesión.

### Solución

Abra el archivo `IntroscopeWorkstation.log` o un archivo de registro independiente que realice el seguimiento de los eventos de Workstation. Confirme que los mensajes siguientes están presentes en el archivo de registro:

- **Session timeout configured to <x> minute(s)**  
Indica que el tiempo de espera automático de la sesión está configurado correctamente.
- **User activity check: there has been no user action for more than several minutes, therefore logging out.**  
Indica la notificación de tiempo de espera de la sesión agotado.

## El tiempo de espera de Workstation se agota al iniciar sesión en Enterprise Manager

### Síntoma

El tiempo de espera de Workstation se agota al iniciar sesión en Enterprise Manager.

### Solución

El tiempo de espera predeterminado de conexión para Workstation es de 60 segundos. El tiempo de espera de Workstation se puede agotar por las razones siguientes:

- La latencia de red entre Workstation y Enterprise Manager
- Workstation tiene una cantidad demasiado elevada de datos para recuperar (métricas, módulos de gestión) y 60 segundos no es suficiente tiempo para extraer todos estos datos, incluso en condiciones de red normales.

Se puede aumentar el tiempo de espera de la conexión de cliente mediante la agregación de la propiedad siguiente al archivo `IntroscopeEnterpriseManager.properties`:

```
introscope.enterprisemanager.workstation.timeout=[value in seconds]
```

Reinicie EM para que se apliquen los cambios.

## Referencia de API

Application Performance Management consta del siguiente conjunto de API de servicios web:

Los usuarios que se especifican a continuación son el público al que están dirigidas estas API:

- Desarrolladores y administradores de Application Performance Management
- Desarrolladores de CA Technologies o de productos de terceros, servicios profesionales o ingenieros de preventas
- Cada una de las API de los servicios web de Application Performance Management proporcionan a los desarrolladores y administradores la capacidad de ampliar sus soluciones de gestión de aplicaciones. Se puede recuperar información relevante de Application Performance Management y se pueden integrar los datos en soluciones de productos de terceros o personalizadas.

## API de APM Command Center

Una descripción general de las API de RESTful implementadas para APM Command Center. Para cada servicio web disponible, se muestran los parámetros de solicitud y de verbos de HTTP compatibles.

Esta sección proporciona una descripción general de las API de RESTful implementadas para APM Command Center. Para cada servicio web disponible, se muestran los parámetros de solicitud y de verbos de HTTP compatibles. Se recomienda que también lea la sección [API de hipermedia de APM](#) para obtener información general sobre cómo se implementa la API RESTful en DX APM.

### Descargar el último paquete desde APM Command Center

Mediante la API de Command Center se pueden descargar los paquetes más recientes desde APM Command Center y personalizar el comportamiento de la descarga al definir las propiedades necesarias. Por ejemplo, se puede personalizar la carga y establecer determinadas propiedades como ocultas durante la descarga.

La dirección URL para descargar el paquete se puede obtener desde esta ubicación: **ACC, Paquetes, Pantalla de información del paquete, URL del paquete**

Los puntos finales para descargar los paquetes se han ampliado para agregar una solicitud POST. Por ejemplo:

```
POST /acc/apm/acc/downloadpackage/uid/SsApAZq75k3G/version/latest?
format=archive&layout=bootstrap_preferred&packageDownloadSecurityToken=d19a78c5a88bfe750f3a7a4bc
```

En la carga útil, defina la lista de propiedades de JSON en el formato siguiente:

```
{
 "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
 }
}

```

De forma similar, se pueden definir propiedades adicionales en la carga útil.

Nombre de la propiedad	Descripción	Ejemplo/Valor predeterminado
bundleName	Opcional. Defina el nombre del conjunto.	El punto final puede obtener la lista de conjuntos dentro del paquete específico con el ID 2 (con UID: SsApAZq75k3G): <ul style="list-style-type: none"> <li>GET /acc/apm/acc/package/2/bundles</li> </ul>
propertyName	Obligatorio. Defina el nombre de la propiedad.	El punto final puede obtener la lista de los nombres de propiedad del bundleName especificado (es decir, el paquete con el ID: 91): <ul style="list-style-type: none"> <li>/acc/apm/acc/package/2/bundles/91/profile</li> </ul>
propertyValue	Obligatorio. Defina el valor de la propiedad.	Ninguno
oculto	Opcional. Defina un valor booleano: <b>true</b> o <b>false</b> si desea que el parámetro se oculte durante la descarga del paquete.  Si se establece el valor como <b>true</b> , su valor se comentará en el archivo de archivado del paquete de resultados.	Valor predeterminado: <b>false</b>
allowOnlyExistingProperties	Opcional. Defina un valor booleano: <b>true</b> o <b>false</b> .  Si se establece el valor como <b>true</b> , las validaciones durante la descarga producen el error HTTP 400 en caso de que el nombre de la propiedad especificado en cuerpo de POST no esté dentro de ninguna propiedad del conjunto de paquetes.  Se recomienda establecer la propiedad como <b>true</b> si se desea sobrescribir solamente las propiedades existentes y realizar la ejecución de la comprobación de validación durante la llamada REST.	Valor predeterminado: <b>false</b>

### Validación y solución de problemas

Cuando el punto final completa correctamente la validación, devuelve el paquete binario de tipo ZIP o TAR, en función de la plataforma determinada, es decir, Windows o UNIX/Linux. Este paquete contiene los parámetros sustituidos o nuevos con el código de respuesta 200 Correcto.

Sin embargo, si se produce un error en la validación, se devuelve el código de respuesta 400 Solicitud incorrecta al usuario con el mensaje de error detallado.

APM Command Center es compatible con los siguientes servicios web públicos de RESTful:

Las direcciones URL de los recursos se encuentran en el formato siguiente:

`https://<APMtenanthost>/apm/appmap/acc/apm/acc/<resource name>`

El host de cliente de APM Command Center incluye el nombre del pod de Enterprise Manager en Kubernetes y el nombre DNS del enrutador de Kubernetes. Por ejemplo: 10-778046.KUBERNETES-ROUTER. El primer número es el número de cliente. El segundo número es distinto para cada cliente. KUBERNETES-ROUTER es el enrutador de Kubernetes que está instalado.

La tabla siguiente muestra todos los recursos disponibles de la API de APM Command Center, así como los verbos y parámetros de HTTP que son compatibles con los recursos.

Resource	Verbos de HTTP						Parámetros				
	GET	HEAD	POST	DELETE	OPTIONS	formato	proyección	page	size	ordenar	Q
<b>agent</b> Una lista de agentes gestionados, incluidas sus propiedades.	Sí	Sí	No	No	Sí	JSON, CSV	lista	Sí	Sí	Sí	Sí
<b>agentUpdateTask</b> Capacidad de modificar el nivel de registro de un agente individual.	Sí	Sí	Sí	No	Sí	JSON	No	Sí	Sí	Sí	No
<b>diagnosticReport</b> Una lista de informes de diagnóstico, incluida la capacidad para descargar los informes.	Sí	Sí	No	No	Sí	JSON, ZIP	lista	Sí	Sí	Sí	Sí

<b>diagnosticReportTask</b> Proporciona la capacidad de generar un nuevo informe de diagnóstico para un agente.	Sí	Sí	No	Sí	JSON	No	Sí	Sí	Sí	No
<b>controladores</b> Una lista de controladores de agente conectados al servidor de configuración.	Sí	No	No	Sí	JSON, CSV	No	Sí	Sí	Sí	No
<b>agentFileOperationTask</b> Proporciona la posibilidad de insertar (o suprimir) un archivo en un directorio de un sistema remoto.	Sí	Sí	No	Sí	JSON	No	Sí	Sí	Sí	No
<b>archivo</b> Una lista de archivos almacenados en el servidor de configuración.	Sí	Sí	Sí	Sí	JSON	No	Sí	Sí	Sí	No

<b>auditRecords</b> Una lista de registros de auditoría asociados a las operaciones que cambian el entorno.	Sí	Sí	No	No	Sí	JSON	lista	Sí	Sí	Sí	Sí
<b>paquete</b> Una lista de paquetes de agente creados.	Sí	Sí	Sí	Sí	Sí	ZIP, TAR, archivo de archivado	lista	Sí	Sí	Sí	Sí
<b>agentPackageTask</b> Capacidad para insertar conjuntos de agente en el directorio de instalación del agente.	Sí	Sí	Sí	No	Sí	JSON	No	Sí	Sí	Sí	No
<b>conjunto</b> Una lista de conjuntos de agentes disponibles.	Sí	Sí	Sí	Sí	Sí	JSON, archivo de archivado	No	Sí	Sí	Sí	Sí

Tenga en cuenta que los parámetros formato, proyección, página, tamaño, orden y q distinguen entre mayúsculas y minúsculas y deben estar en minúscula (por ejemplo, Formato = csv no funcionará).

### **Autenticación**

Un token de seguridad es una cadena de texto generada aleatoriamente casi idéntica a una contraseña cifrada. Este token proporciona a la API acceso al servicio web de Command Center.

Se pueden generar tantos tokens como sean obligatorios. Puede cambiar la descripción de un token o suprimir un token mediante el botón Editar. Los tokens solo se pueden revocar suprimiéndolos. Cualquier usuario puede suprimir un token.

También se puede ver cuando se ha generado un token y cuando se ha utilizado por última vez.

**Siga estos pasos:**

1. En la interfaz de usuario de DX APM, seleccione la ficha **Seguridad**.
2. Haga clic en **Generar un token nuevo**.
3. Seleccione **API pública**.
4. (Opcional) Seleccione cuándo caduca el token.
5. Haga clic en **Generar token**.
6. Copie el token generado.

**Nota:** Asegúrese de que el token se almacena de forma inmediata y segura para su uso futuro. No se puede volver a mostrar en la interfaz de usuario de DX APM.

7. Utilice el token en el encabezado de autorización de la solicitud. Consulte [Autenticación y autorización de la API](#) para obtener más información.

**Más información:**

- [Mensajes y códigos de error de API generales](#)
- [Mensajes de error de la API de Command Center](#)

## Mensajes de error de API

En esta sección se enumeran los mensajes de error de API devueltos por DX APM Command Center. Para obtener una descripción general de todos los mensajes y códigos de error de API de DX APM Hypermedia, consulte la sección [Mensajes y códigos de error](#).

**De EA0100 a EA0599**

Los errores del intervalo EA0100-EA0599 son códigos de estado HTTP estándares. Para obtener información detallada, consulte [RFC 7231](#).

**EA1001****Consulta de búsqueda no válida****Razón:**

Se devuelve cuando una solicitud de filtro o búsqueda produce un error debido a una consulta que no cumple con la sintaxis de Lucene.

**EA1002****Paquete en uso actualmente por {0} agentes****Razón:**

No tiene permiso para eliminar paquetes que tengan agentes que hagan referencia a ellos actualmente.

**EA3100****Actualización del agente en curso: {agent id}****Razón:**

Otra tarea de actualización del agente está en curso en el agente determinado.

**Solución:**

Espere a que finalice la tarea de actualización actual.



**EA3101****La actualización ya está en curso para el controlador en {serverName}****Razón:**

Solo se puede ejecutar una ControllerUpgradeTask en un controlador del agente. Si intenta iniciar una nueva ControllerUpgradeTask mientras la actual sigue ejecutándose, se generará este mensaje de error.

**Solución:**

Espere a que finalice la tarea de actualización actual.

**EA3102****El archivo ya se está actualizando para el agente****Razón:**

Solo se puede ejecutar una AgentFileOperationTask para la misma combinación de agente y archivo de destino.

**Solución:**

Espere a que finalice la tarea de operación actual.

**EA3103****El controlador no está conectado****Razón:**

Se ha intentado actualizar un controlador del agente que no se está ejecutando. No se puede iniciar una ControllerUpgradeTask para los controladores del agente que no se estén ejecutando actualmente.

**Solución:**

Inicie el controlador del agente.

**EA3104****No se permite la actualización automática del controlador****Razón:**

No se puede activar la actualización automática del controlador del agente porque la inserción del paquete del controlador del agente está deshabilitada.

**Solución:**

Consulte la sección Solución de problemas del proceso de actualización para obtener instrucciones.

**EA3105****El paquete está archivado y no se puede utilizar para esta operación****Razón:**

No se pueden usar los paquetes archivados para ninguna operación. Por ejemplo, no se puede descargar un paquete archivado.

**Solución:**

Elija otro paquete para descargar o desarchiva el paquete solicitado y vuelva a intentarlo.

**EA3108**

Otros filtros utilizan el filtro con nombre {name}: {otherFilters}

**Razón:**

El filtro con nombre no se puede eliminar porque otros filtros están utilizándolo (o haciendo referencia a dicho filtro).

**Recurso del agente**

Este servicio web devuelve información sobre los agentes registrados con APM Command Center (ACC). Verbos compatibles: GET, HEAD, OPTIONS. Parámetros compatibles: [page](#), [size](#), [sort](#), [q](#), [format](#), [projection](#)

**GET**

```
GET https://<ACC tenant HOST>/apm/appmap/acc/apm/acc/agent
```

Utilice la solicitud siguiente para obtener información exclusivamente sobre el agente con el ID 2:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent/2
```

**HEAD**

El método HEAD devuelve los encabezados con información sobre el servicio, incluidos, por ejemplo, los campos de búsqueda permitidos.

```
HEAD https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent/
```

**Respuesta de ejemplo:**

```
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
```

Propiedades de recurso. Se encuentran disponibles las siguientes propiedades que contienen información sobre el recurso:

Nombre de la propiedad	Type	Descripción	Versión de la API
tenant	número entero	ID de cliente.	1.1
id	número entero	ID interno del recurso del agente.	1.0
agentName	cadena	El "nombre" del agente tal y como lo proporciona el agente cuando se registra con ACC. Forma parte del triple agente.	1.0
serverName	cadena	El servidor en el que se encuentra el agente registrado. Forma parte del triple agente.	1.0
processName	cadena	El nombre del proceso de agente como lo conoce el agente y EM. Forma parte del triple agente.	1.0

Nombre de la propiedad	Type	Descripción	Versión de la API
status	enumeración	Indica si el agente se considera activo. Puede esta "activo" o "ausente". De forma predeterminada, "ACTIVO" indica que el agente se ha revisado en las últimas 24 horas.	1.0
type	enumeración	El tipo de agente, como parte del registro de agente comunicado a ACC. Actualmente, siempre es "JavaAgent".	1.0
version	cadena	La versión del agente tal y como se define en el manifiesto del agente (por ejemplo, 9.7.1).	1.0
build	cadena	La compilación del agente tal y como se define en el manifiesto del agente.	1.0
logLevel	enumeración	El nivel de registro actual del agente (FATAL, ERROR, WARN, INFO, VERBOSE, DEBUG, TRACE).	1.0
registrationTimestamp	fecha	La hora en la que el agente se registró con ACC, representada en formato UTC.	1.0
registrationUnixTimestamp	fecha	La hora en la que el agente se registró con ACC, representada en formato Unix.	1.0
lastContact	fecha	La hora en la que el agente se puso en contacto con ACC por última vez, representada en formato UTC.	1.0
emCollectorHost	cadena	El nombre del recopilador EM al que está conectado el agente, como lo conoce el agente.	1.0
emCollectorPort	número entero	El puerto del recopilador EM al que está conectado el agente, como lo conoce el agente.	1.0
appServerName	cadena	El servidor de aplicaciones en el que se está ejecutando el agente (donde se conoce), por ejemplo, "Apache Tomcat".	1.0
appServerVersion	cadena	La versión del servidor de aplicaciones en el que se está ejecutando el agente (donde se conoce).	1.0

Nombre de la propiedad	Type	Descripción	Versión de la API
platformName	cadena	La plataforma en la que se ejecuta el agente (Java Runtime), por ejemplo, "Oracle Corporation".	1.0
platformVersion	cadena	La versión de la plataforma (Java Runtime) en la que se ejecuta el agente, por ejemplo, 1.7.0.	1.0
platformArch	cadena	La arquitectura de la plataforma (Java Runtime) en la que se ejecuta el agente, en caso de que se detecte.	1.0
osName	cadena	El sistema operativo en el que se está ejecutando el agente (Windows, RedHat, etc.).	1.0
osVersion	cadena	La versión del sistema operativo en el que se está ejecutando el agente.	1.0
osArch	cadena	La arquitectura del procesador del sistema operativo en el que se está ejecutando el agente, por ejemplo, AMD64.	1.0
metricCount	número entero	El número de métricas que el agente cree que está recopilando.	1.0
registrationErrors	matriz de cadenas	Errores devueltos por los complementos al descubrir información adicional acerca del agente.	1.0
installPath	cadena	La ruta completa en la que está instalado el agente.	1.0
agentProfile	cadena	La ruta completa al perfil del agente.	1.0
platformProperties	mapa	Pares clave/valor de las propiedades del sistema Java conocidas por el agente.	1.0
environmentVariables	mapa	Pares clave/valor de las variables de entorno conocidas por el proceso del agente.	1.0
controllerId	UUID	UUID del controlador de ACC al que está conectado este agente.	1.0

## Recurso agentUpdateTask

El servicio web de agentUpdateTask se puede utilizar para actualizar el perfil del agente (actualmente limitado a un cambio a nivel de registro).

El servicio web de agentUpdateTask se puede utilizar para actualizar el perfil del agente (actualmente limitado a un cambio a nivel de registro). Este recurso también se puede utilizar para obtener una lista de todas las solicitudes previas.

Verbos compatibles: GET, HEAD, POST, DELETE, OPTIONS. Parámetros compatibles: [page](#), [size](#), [sort](#)

### acceso a los recursos GET

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agentUpdateTask/
```

### POST

Mediante el método POST se puede actualizar el perfil de agente. Este ejemplo cambia el nivel de registro del agente con el ID 1 a información:

```
POST https://<ACC tenant host>/apm/appmap/acc/apm/acc/agentUpdateTask{ "agent": "agent/1",
 "property" : "log4j.logger.IntroscopeAgent", "value": "INFO"}
```

Propiedades de recurso. Se encuentran disponibles las siguientes propiedades que contienen información sobre el recurso:

Nombre de la propiedad	Type	Descripción	Versión de la API
tenant	número entero	ID de cliente.	1.1
status	enumeración	Estado de la operación (sigue la definición del recurso de la tarea).	1.0
creationTimestamp	fecha	Hora en la que se creó el recurso (en UTC).	1.0
completionTimestamp	fecha	Hora en la que se completó la operación (en UTC).	1.0
expectedDuration	número entero	Cuánto tiempo se espera que dure la operación en curso.	1.0
property	cadena	La propiedad del perfil que se está actualizando.	1.0
value	cadena	El valor solicitado.	1.0
currentValue	cadena	El valor que se sabe que tiene el agente.	1.0
pendingValue	cadena	El valor que se escribió por última vez en el perfil.	1.0
agentId	número entero	Identificador único del agente en el que se realiza la operación.	1.0
user	cadena	El usuario que ha iniciado la operación.	1.0
updateErrors	matriz	Matriz de errores que se devolvieron durante la operación.	1.0

## Recurso diagnosticReport

Este servicio web devuelve información sobre los informes de diagnóstico.

Este servicio web devuelve información sobre los informes de diagnóstico. Un informe de diagnóstico incluye todos los detalles de un agente. Verbos compatibles: GET, HEAD, OPTIONS. Parámetros compatibles: [page](#), [size](#), [sort](#), [projection](#), [q](#)

### GET

GET `https://<ACC tenant host>/apm/appmap/acc/apm/acc/diagnosticReport/`

Propiedades de recurso. Se encuentran disponibles las siguientes propiedades que contienen información sobre el recurso:

**Table 2:**

Nombre de la propiedad	Type	Descripción	Versión de la API
tenant	número entero	ID de cliente	1.1
id	número entero	ID interno del recurso diagnosticReport.	1.0
reportName	cadena	Nombre de visualización del informe.	1.0
requestTimestamp	fecha	Hora en la que se solicitó el informe (en UTC).	1.0
completionTimestamp	fecha	Hora en la que se completó el informe (en UTC).	1.0
generationDuration	número entero	Tiempo total que se ha tardado en generar el informe en milisegundos.	1.0
status	enumeración	El estado de la generación del informe.	1.0
commandCenterInfo	mapa	Pares de clave/valor que proporcionan información sobre el servidor de configuración y el controlador del agente que se utilizan para generar el informe.	1.0
agentProfile	mapa	Pares de clave/valor que proporcionan información sobre el perfil utilizado para configurar el agente. Incluye un vínculo al contenido.	1.0
generationErrors	matriz	Matrices de errores encontradas al generar el informe.	1.0
agentProperties	mapa	Pares de clave/valor que representan información sobre el agente cuando se generó el informe (copiado del recurso del agente).	1.0

Nombre de la propiedad	Type	Descripción	Versión de la API
environmentVariables	mapa	Pares de clave/valor que representan variables de entorno conocidas por el agente en el momento en el que se generó el informe (copiado del recurso del agente).	1.0
platformProperties	mapa	Los pares de clave/valor que representan las propiedades de la plataforma (propiedades del sistema Java) que conoce el agente en el momento en que se genera el informe (copiado desde el recurso del agente).	1.0
platformParameters	cadena	Línea de comandos utilizada para iniciar el proceso en el que se está ejecutando el agente.	1.0
extensionDirectory	cadena	Ruta completa del directorio de extensiones de agente.	1.0
extensionFiles	mapa	Subrecurso que contiene detalles de los archivos de extensión que se ejecutan en el agente, incluido el nombre, la fecha de modificación, el tamaño y la versión.	1.0
logFiles	mapa	Subrecurso que contiene detalles de los archivos de registro del agente, incluido el nombre, la ruta, la fecha de modificación, el tamaño y el vínculo al contenido.	1.0
pbdPblFiles	mapa	Subrecurso que contiene detalles de los archivos de PBD que se ejecutan en el agente, incluido el nombre, la fecha de modificación, el tamaño y el vínculo al contenido.	1.0

## Recurso diagnosticReportTask

El servicio web de diagnosticReportTask se puede utilizar para solicitar un informe de diagnóstico.

El servicio web de diagnosticReportTask se puede utilizar para solicitar un informe de diagnóstico. La creación de un recurso diagnosticReportTask inicia una generación de informes. Se puede monitorizar el progreso de la generación de informes recuperando (sondeando) el recurso diagnosticReportTask creado. Este recurso también se puede utilizar para obtener una lista de todas las solicitudes previas. Verbos compatibles: GET, HEAD, POST, DELETE, OPTIONS. Parámetros compatibles: [page](#), [size](#), [sort](#)

### GET

La solicitud siguiente devuelve información acerca de la tarea de informe de diagnóstico con el ID 2:

GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/diagnosticReportTask/2/

**POST** Al utilizar el método POST, puede empezar a generar un informe de diagnóstico para un agente específico. A continuación se muestra un ejemplo de una solicitud que crea una nueva tarea de informe de diagnóstico para el agente con el 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"}
```

**Propiedades de recurso.** Se encuentran disponibles las siguientes propiedades que contienen información sobre el recurso:

Nombre de la propiedad	Type	Descripción	Versión de la API
tenant	número entero	ID de cliente.	1.1
id	número entero	Identificador único para este recurso.	1.0
status	enumeración	El estado de la operación (sigue la definición del recurso de la tarea).	1.0
creationTimestamp	fecha	Hora en la que se creó el recurso (en UTC).	1.0
completionTimestamp	fecha	Hora en la que se completó la operación (en UTC).	1.0
expectedDuration	número entero	Cuánto tiempo se espera que dure la operación en curso.	1.0
diagReportId	número entero	El identificador único que crea el recurso diagnosticReport.	1.0
agentId	número entero	Identificador único del agente en el que se realiza la operación.	1.0

## Recurso del controlador

Este servicio web devuelve información acerca de los controladores de agente conectados al servidor de configuración.

Este servicio web devuelve información acerca de los controladores de agente conectados al servidor de configuración.

Verbos compatibles: GET, HEAD, OPTIONS. Parámetros compatibles: [page](#), [size](#), [sort](#)

### GET

GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/controller



Propiedades de recurso. Se encuentran disponibles las siguientes propiedades que contienen información sobre el recurso:

Nombre de la propiedad	Type	Descripción	Versión de la API
tenant	número entero	ID de cliente.	1.1
id	UUID	UUID del recurso del controlador.	1.0
version	cadena	Versión del controlador del agente, tal y como se define en su manifiesto.	1.0
messagingApiVersion	número entero	Versión máxima de la interfaz de mensajería compatible con este controlador.	1.0
buildNo	cadena	Número de compilación del controlador, tal y como se define en su manifiesto.	1.0
hostNames	matriz de cadenas	Matriz de todos los nombres de host conocidos para este controlador.	1.0
ipAddresses	matriz de cadenas	Matriz de todas las direcciones IP conocidas (v4 y v6) para este controlador.	1.0
osArch	cadena	La arquitectura del sistema operativo en el que se ejecuta el controlador, por ejemplo amd64.	1.0
osName	cadena	El nombre del SO en el que se ejecuta el controlador, por ejemplo, "Windows Server 2008 R2".	1.0
osVersion	cadena	La versión del sistema operativo en el que se está ejecutando el controlador, por ejemplo, 6.1.	1.0
registrationTimestamp	fecha	La fecha/hora en la que el controlador se registró con el servidor de configuración en formato UTC.	1.0
registrationUnixTimestamp	fecha	La fecha/hora en la que el controlador se registró con el servidor de configuración en formato Unix.	1.0
pluginRuntimeVersion	número entero	La versión máxima del tiempo de ejecución del complemento compatible con este controlador (utilizado para determinar la compatibilidad del script).	1.0

Nombre de la propiedad	Type	Descripción	Versión de la API
pluginsUpdatable	Valor booleano	Indica si el controlador permite que los complementos nuevos (versiones de estos) se envíen a él.	1.0

## Mensajes de error

En esta sección se explican los mensajes de error de DX APM Command Center.

### **EC1001**

#### **No se ha podido guardar el complemento {0}: {1}**

El controlador del agente tiene un complemento desactualizado, pero no se ha podido guardar el complemento actualizado que se descargó del servidor de DX APM Command Center.

#### **Razón:**

El host en el que se está ejecutando el controlador del agente puede tener problemas de espacio libre en disco o el controlador del agente se puede ejecutar como un usuario que no tenga permisos de escritura suficientes en el directorio "plugins".

#### **Solución:**

Compruebe el espacio libre en disco disponible en el host del controlador del agente y que el usuario en el que se esté ejecutando tenga permisos de escritura en el directorio "plugin" y los archivos que se encuentren en él.

### **EC1002**

#### **La actualización del controlador no se ha completado en el tiempo esperado**

#### **Razón:**

Se inició la tarea de actualización del controlador del agente, pero el controlador no se registró de nuevo en el servidor en el tiempo esperado.

#### **Solución:**

Si el controlador todavía no se ha vuelto a conectar, revise el archivo upgrade.log en el sistema del controlador para determinar la causa.

### **EC1003**

#### **Se ha producido un error en la actualización del controlador del agente. No se ha cambiado la versión.**

#### **Razón:**

Se inició la actualización del controlador del agente, pero no se pudo completar. Se ha restaurado la versión original.

Las causas comunes son:

- No hay suficiente espacio en el sistema de archivos
- El controlador no tiene un permiso de escritura en un directorio al que se accede durante el proceso de actualización (por lo general, /tmp y el directorio de instalación del controlador)
- Uno de los archivos está bloqueado por un proceso existente. Esto es más probable que suceda en los sistemas operativos Windows. Asegúrese de que ninguna ventana o símbolo del sistema del explorador utilice ni bloquee el directorio de actualización del controlador.

**Solución:**

Genere un informe de diagnóstico para uno de los agentes de este servidor y revise el archivo upgrade.log en la tarjeta "Archivos de registro del controlador". Consulte el mensaje de error e intente resolver la incidencia.

**EC1004****No se han agregado los siguientes grupos: {0}**

Se ha instalado un paquete en un agente, pero el agente no ha podido agregar todos los grupos del paquete.

**Razón:**

Se ha insertado un paquete que contiene nuevos grupos en un agente en ejecución. Sin embargo, el agente no ha podido agregar todos estos grupos. Los que no se han podido agregar se incluyen en el mensaje.

**Solución:**

La ejecución de un informe de diagnóstico para el agente permite examinar de manera remota los archivos de registro del agente. Los registros explicarán el motivo por el cual no se ha podido cargar el grupo; por ejemplo, es posible que el propio grupo esté dañado.

**EC1005****No se han eliminado los siguientes grupos: {0}**

Se ha insertado un paquete en un agente, pero el agente no ha podido eliminar todos los grupos necesarios del paquete.

**Razón:**

Se ha insertado un paquete en un agente que contiene menos grupos de los que está utilizando actualmente el agente. Estos grupos deben eliminarse del agente en ejecución. Sin embargo, el agente no ha podido eliminar todos estos grupos. Los que no se han podido eliminar se incluyen en el mensaje.

**Solución:**

La ejecución de un informe de diagnóstico para el agente permite examinar de manera remota los archivos de registro del agente. Los registros explicarán el motivo por el cual no se ha podido eliminar el grupo, por ejemplo, es posible que el directorio del grupo se esté utilizando.

**EP1000****No se ha podido acceder al proceso {0}**

No se ha podido acceder al proceso del servidor de aplicaciones.

**Razón:**

El proceso del servidor de aplicaciones ya no se está ejecutando o el controlador del agente no tiene privilegios suficientes para ver el proceso.

**Solución:**

Compruebe si el proceso del servidor de aplicaciones se está ejecutando con el Id. del proceso especificado. Si se está ejecutando, asegúrese de que el controlador del agente se esté ejecutando con los permisos suficientes para ver ese proceso, por ejemplo, ejecutándose como el mismo "usuario" o utilizando el mismo "grupo".

**EP1001****{0} no existe**

El archivo o el directorio no existe.

**Razón:**

No se ha podido encontrar el archivo especificado.

**Solución:**

Si el archivo hace referencia a un archivo de directiva de Probe Builder, asegúrese de que el archivo exista y de que se le haya nombrado correctamente en cualquier lista de directivas de Probe Builder.

**EP1002****Permiso de lectura de {0} denegado**

No se ha podido leer el archivo o el directorio.

**Razón:**

El controlador del agente no tiene permisos suficientes para leer el archivo nombrado.

**Solución:**

El controlador del agente debe ejecutarse con los permisos suficientes para leer los archivos que produce el Agente de APM. Por ejemplo, el controlador del agente debe ejecutarse como el mismo "usuario" que el servidor de aplicaciones o utilizar el mismo "grupo".

**EP1003****Se ha producido un error de E/S al leer {0}**

No se ha podido leer el archivo dado.

**Razón:**

Otro proceso podría haber "bloqueado" el archivo o el controlador del agente no tiene los permisos suficientes para leer el archivo.

**Solución:**

El controlador del agente debe ejecutarse con los permisos suficientes para leer los archivos que produce el Agente de APM. Por ejemplo, el controlador del agente debe ejecutarse como el mismo "usuario" que el servidor de aplicaciones o utilizar el mismo "grupo".

**EP1004****El sistema operativo {0} no es compatible**

El controlador del agente no puede determinar los parámetros de línea de comandos para el Id. de proceso especificado ya que el sistema operativo actual no es compatible.

**Solución:**

Póngase en contacto con el Soporte de CA para averiguar cuándo está planificado que este sistema operativo sea compatible.

**EP1005****No se ha podido determinar el servidor de aplicaciones {0}. Detalles del error: {1}**

No se ha podido determinar el tipo de servidor de aplicaciones.

**Razón:**

El tipo o la versión del servidor de aplicaciones siguen sin ser compatibles, o el controlador del agente no tiene los privilegios suficientes para determinar el tipo de servidor. El error contiene otros detalles de la causa.

**Solución:**

Asegúrese de que el controlador del agente tenga los permisos suficientes para acceder a los archivos del servidor de aplicaciones. Por ejemplo, el controlador del agente debe ejecutarse como el mismo "usuario" que el servidor de aplicaciones o utilizar el mismo "grupo".

### **EP1006**

**Falta el valor de la propiedad `introscope.autoprobe.directivesFile` en {0}.**

**Razón:**

La propiedad `introscope.autoprobe.directivesFile` de `IntroscopeAgent.profile` no está definida o está vacía.

**Solución:**

Verifique la validez del archivo `IntroscopeAgent.profile`.

### **EP1007**

**Permiso de escritura de {0} denegado**

**Razón:**

El controlador del agente no dispone de los derechos de acceso suficientes para escribir en el archivo nombrado. Esta situación puede ocurrir en varias circunstancias:

- Al intentar cambiar el nivel de registro del agente de Introscope.
- Al intentar actualizar la instalación del controlador del agente.
- Al intentar copiar un archivo en el directorio de instalación del agente de Introscope.

**Solución:**

Asegúrese de que el controlador del agente se esté ejecutando con los permisos suficientes para escribir en ese archivo y directorio. Por ejemplo, al ejecutarlo como el mismo "usuario" o utilizar el mismo "grupo".

### **EP1010**

**No se ha podido copiar el archivo de {0} a {1}. Detalles del error: {2}**

No se puede acceder a la dirección URL {0} por problemas de red. Consulte los detalles completos del error {2}.

**Razón:**

Aplicó un nuevo paquete del agente o actualizó el controlador.

**Solución:**

Asegúrese de que la conexión de red entre el controlador y el servidor de Command Center funcione. Repita la acción.

### **EP1012**

**La versión {0} ya existe.**

**Razón:**

Se devuelve este mensaje si el directorio de la versión se creó manualmente durante la aplicación del paquete del agente.

**Solución:**

Reinicie el agente para volver a detectar el agente y registrarlo correctamente.

**EP1013****El agente no es del tipo agente de arranque****Razón:**

La actualización del arranque del agente falla porque el agente no es un agente de arranque. Sin embargo, el Command Center ha registrado el agente como capaz de iniciar el arranque.

**Solución:**

Reinicie el agente para volver a detectar el agente y registrarlo correctamente.

**EP2000****Error de script con mensaje {1}**

Se ha detectado un problema al intentar recuperar los detalles de un agente.

**Razón:**

Este problema puede tener muchas causas. Puede haber un error de sintaxis en el script que se está ejecutando (solo ocurre para los scripts personalizados). Puede haber problemas de acceso a los archivos que necesite el script.

Otro motivo puede ser el uso de una versión o implementación de Java no compatibles.

**ES1000****Error al cambiar el nivel de registro****Razón:**

Otro usuario cambió el nivel de registro para el mismo agente al mismo tiempo. El complemento del controlador del agente ya ha actualizado IntroscopeAgent.profile con un nuevo nivel de registro establecido por el otro usuario, pero el cambio no se ha mostrado aún en la interfaz de usuario.

**Solución:**

Compruebe el nivel de registro actual y vuelva a aplicar el cambio si es necesario.

**ES1002****Error: se ha producido un error de HTTP {0} al crear la petición de cambio de agente.****Razón:**

Se ha producido un error en la petición de cambio de propiedad y no se ha iniciado el trabajo de cambio de la propiedad.

**Solución:**

Es muy probablemente que se trate de un problema de back-end. Compruebe el archivo de registro y póngase en contacto con el administrador del sistema.

**EU3106****El paquete {packageName} no existe.****Razón:**

El DX APM Command Center no conoce el paquete utilizado por este agente.

**EU3400****Se ha producido un tiempo de espera {0}**

**Razón:**

La conexión es lenta o el servidor no está disponible.

**Solución:**

Si el problema persiste o está accediendo al APM Command Center con una conexión lenta, considere aumentar el tiempo de espera de la solicitud (opción predeterminada: 10 segundos [10 000 ms]).

Para ello, agregue la propiedad siguiente al archivo `config/apmccsrv.properties` del servidor de configuración y establezca su valor en 30 000 para aumentar el tiempo de espera a 30 segundos:

```
com.ca.apm.acc.ui.requestTimeout=30000
```

Reinicie el servidor de configuración para que el cambio surta efecto.

**Propiedades que permiten la búsqueda**

En esta sección se muestran todas las propiedades que se pueden utilizar en las búsquedas de agentes, informes, paquetes o grupos en la interfaz de usuario de DX APM Command Center.

En la siguiente tabla se muestran las propiedades que se pueden utilizar en una búsqueda. En la primera columna, encontrará la cadena de búsqueda que debe escribir en el cuadro de búsqueda (las cadenas coinciden con las llamadas de API reales). La segunda columna muestra el nombre correspondiente de la propiedad tal y como aparece en las tarjetas de la interfaz de usuario.

Para obtener más información sobre la búsqueda mediante el lenguaje de consulta de Command Center, consulte [Búsqueda mediante el lenguaje de consulta de Command Center](#).

Se utiliza el patrón siguiente: Nombre de página - (Nombre de la tarjeta) - Nombre del campo.

Cadena de búsqueda	Campo de la IU correspondiente	Notas
agentCompatibility	Grupos - Compatibilidad	Versiones del agente con las que es compatible el grupo. La búsqueda de intervalo no se admite. Escriba "10" para que los grupos sean compatibles con las versiones 10.x.
agentId	n/d	Identificador único del agente.
agentName	Agentes, Informes - Nombre del agente	
agentProfile	Informes - Directorio del perfil del agente	Ruta al perfil del agente.
agentProfile.name	Informes - Nombre de perfil del agente	Devuelve informes para los agentes con el nombre de perfil especificado.
agentVersion	Paquetes - Versión del agente	Devuelve los paquetes diseñados para los agentes de la versión determinada.
appServerName	Agentes - Servidor de aplicaciones	Nombre del servidor de aplicaciones en el que se está ejecutando el agente.
appServerVersion	Agentes - Versión del servidor de aplicaciones	La versión del servidor de aplicaciones en el que se está ejecutando el agente.
author	Grupos - Autor	Devuelve los grupos creados por el usuario especificado.
build	n/d	
categoría	Grupos - Categoría	Categoría del conjunto: principal, entorno, función, personalizado.

Collections	n/d	Utiliza una cadena de búsqueda guardada como Recopilación.
comment	Paquetes - Comentario	Devuelve los paquetes que contienen el comentario especificado.
controllerId	n/d	Devuelve los agentes conectados al controlador del agente especificado.
suprimido	n/d	Devuelve una lista de grupos suprimidos o activos. Use "true" o "false".
dependencies	Grupos - Dependencias	Devuelve los grupos que dependen de las facetas especificadas.
description	Grupos - Descripción	Devuelve los grupos con la descripción especificada.
dynamic	Grupos - Implementable sin reinicio	Indica si el grupo es explícitamente implementable en caliente o no. Los valores válidos para la búsqueda son "true" y "false".
emCollectorHost	Agentes - Enterprise Manager	Host del recopilador de Enterprise Manager
emCollectorPort	Agentes - Enterprise Manager	Puerto del recopilador de Enterprise Manager
enhances	Grupos - Mejoras	Devuelve los grupos que mejoran las facetas especificadas.
environmentVariables.value	Informes - Variables de entorno	Asignación de variables de entorno (pares clave-valor). Solo los valores permiten la búsqueda.
extensionFiles.name	Informes - Directorio de extensiones	Ruta al directorio de extensiones de un agente. Solo el nombre del archivo permite la búsqueda.
facets	Grupos - Facetas	Devuelve los grupos que contienen las facetas especificadas.
id	n/d	ID literal del grupo como se utiliza en la definición del paquete.
installPath	n/d	Devuelve los agentes instalados en la ruta especificada.
isBootstrapped	n/d	Devuelve los agentes que se pueden actualizar mediante una actualización de arranque en frío.
lastContact	Agentes - Último contacto	
logLevel	Agentes - Nivel de registro	Valores: desconocido, información, seguimiento, depurar, advertencia, error
name	n/d	El nombre real del grupo, no el nombre que se muestra en el nombre archivado en la página Grupos.
osArch	Informes - Propiedades del sistema Java	Arquitectura del sistema operativo. Ejemplo: x64
osName	Agentes - Tipo de SO, Informes - SO, Paquetes - Tipo de SO	Nombre del sistema operativo. Ejemplo: Linux. En el caso de los grupos, los valores que permiten la búsqueda son "unix" o "windows".
osVersion	Agentes - Versión de SO, Informes - Versión de SO	Versión del sistema operativo.



packageName	Agentes - Paquete - Nombre, Paquetes - Nombre	Devuelve los paquetes que coinciden con la cadena de búsqueda y todos los agentes que utilizan el paquete.
packageVersion	Agentes - Paquete - Versión del paquete	Devuelve todos los agentes que utilizan la versión del paquete especificada.
pbdPblFiles.name	Informes - Directivas de ProbeBuilder	Lista de archivos de un agente cuando se generó el informe. Contiene solamente archivos PBD y PBL y solo el nombre del archivo permite la búsqueda.
platformArch	n/d	Arquitectura de la plataforma. Ejemplo: x86
platformName	Agentes - Entorno - Máquina virtual Java	Plataforma en la que se está ejecutando el agente (Open Java, Oracle Java, .Net 4.0)
platformParameters	Informes - Propiedades del sistema Java	Cadena de parámetros de plataforma. Utilice los parámetros de inicio de la máquina virtual Java o un equivalente para .Net.
platformProperties.value	Informes - Propiedades del sistema Java	Asignación de propiedades de plataforma (pares clave-valor). Utilice las propiedades del sistema de la máquina virtual Java o un equivalente para .Net. Solo los valores permiten la búsqueda.
platformVersion	Agentes - Entorno - Versión de la máquina virtual Java	
process	Paquetes - Entorno - Proceso	Devuelve los paquetes diseñados para el servidor de aplicaciones especificado.
processName	Agentes - Nombre del proceso, Informes - Agente - Nombre del proceso	Devuelve los agentes (y sus informes) que se ejecutan en el servidor de aplicaciones especificado.
reportName	Informes - Nombre del informe	
restartRequired	n/d (un icono junto al nombre del agente)	Devuelve una lista de agentes que se han modificado recientemente y requiere un reinicio para que los cambios se apliquen.
serverName	Agentes - Nombre del servidor, Informes - Agente - Nombre del servidor	Devuelve los agentes (y sus informes) que se ejecutan en el servidor especificado.
specificationVersion	n/d	Versión de los metadatos utilizados en el grupo.
status	Agentes - Estado del agente	Estado del agente. Valores: activo, abajo, fuera
type	n/d	Tipo de agente (por ejemplo, Agente de Java).
version	Agentes - Versión del agente, Informes - Versión del agente, Grupos - Versión	Devuelve los agentes de la versión pertinente o los informes generados para tales agentes o grupos de la versión pertinente.

## Búsqueda mediante el lenguaje de consulta de Command Center

Especifique una consulta personalizada en la barra de búsqueda situada en la parte superior de la página de Command Center (ACC) que filtra los elementos mostrados en una vista. La consulta personalizada utiliza el lenguaje de consulta de ACC (AQL), que sustituye al idioma Lucene utilizado anteriormente. Para obtener más información sobre las diferencias entre Lucene y AQL, consulte [Propiedades que permiten la búsqueda](#).

### **Creación de consultas simples**

Escriba una palabra en la barra de búsqueda para filtrar todos los resultados coincidentes basados en la consulta de palabra. La búsqueda se realiza en una propiedad determinada, normalmente, un nombre.

Para buscar una propiedad específica, escriba la consulta con este formato: **propertyName:search\_query\_word**

#### **NOTE**

El valor **propertyName** distingue entre mayúsculas y minúsculas. Mientras se escribe, la barra de búsqueda muestra las propiedades disponibles. Utilice la propiedad **all** para realizar la búsqueda en varias propiedades.

### **Búsqueda sencilla - Ejemplo:**

`osName:windows`

## Propiedades relacionadas con las entidades

En la siguiente tabla se muestran las propiedades predeterminadas, las propiedades disponibles y las propiedades que se buscan al usar la palabra clave **all**.

Entidad	Propiedad predeterminada	Propiedades en la palabra clave all	Propiedades disponibles
Agent	spaName Esta propiedad realiza una búsqueda en processName y agentName de serverName.	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
Informe de diagnóstico	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
Paquete	packageName	bundles, comment, emHost, facets, packageName	agentVersion, all, bundles, comment, draft, emHost, exported, facets, id, isAutogenerated, isFromTeamCenter, latest, modified, originId, osName, packageName, process, version

Entidad	Propiedad predeterminada	Propiedades en la palabra clave all	Propiedades disponibles
Grupo	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

### Crear consultas de combinación

Escriba varias consultas en la barra de búsqueda separadas por espacios o escriba varias subconsultas utilizando los operadores AND, OR o NOT.

Los operadores distinguen entre mayúsculas y minúsculas y se pueden utilizar paréntesis para agrupar operadores. AND es el operador predeterminado para las consultas separadas por espacios.

#### Consulta de combinación con el operador AND - Ejemplo

Los siguientes ejemplos de consulta muestran los resultados donde se encuentran todas las palabras.

```
word1 AND word2 AND word3
word1 AND word2 word3
word1 word2 word3
```

#### Consulta de combinación con el operador OR - Ejemplo

Este ejemplo filtra los resultados donde se encuentra una de las palabras.

```
word1 OR word2 OR word3
```

#### Consulta de combinación con el operador NOT - Ejemplo

Este ejemplo filtra los resultados que no contienen la palabra *myquery*.

```
NOT myquery
```

Existen símbolos alternativos que se pueden utilizar en lugar de los operadores con nombre:

Operator	Alternativo
AND	&&
OR	
NOT	! o -

#### Consulta de combinación con símbolo alternativo - Ejemplo

Este ejemplo filtra los resultados que no contienen la palabra *myquery*

```
-myquery
```

#### Consulta de combinación con paréntesis - Ejemplo

El ejemplo agrupa los operadores y filtra los resultados.

```
(word1 AND word2) OR word3
word1 AND (word2 OR word3)
```

### Otras consultas de búsqueda

Se pueden utilizar cadenas, caracteres comodín, números, expresiones regulares y consultas de intervalo como patrones de búsqueda para filtrar los resultados.

### Uso de cadenas y caracteres comodín

Escriba una cadena de palabras o caracteres entre comillas (" ") o la barra diagonal (/) para filtrar los resultados de búsqueda. Los resultados son una coincidencia exacta de la cadena de búsqueda. Con los caracteres comodín se pueden filtrar los resultados que contienen la cadena. Se pueden utilizar los siguientes tipos de caracteres comodín: \* para coincidir con cualquier subcadena y ? para coincidir con un carácter. El uso de un carácter especial dentro de una cadena se trata como un carácter ordinario.

#### **Consulta de cadena - Ejemplo**

La siguiente consulta filtra todos los resultados que coinciden **exactamente** con la cadena.

```
"abc xyz"
```

#### **Consulta de comodines - Ejemplo**

La siguiente consulta filtra **todos** los resultados que contienen la cadena de búsqueda.

```
"abc xyz"
```

#### **Consulta de combinación de cadena y comodín - Ejemplo**

La siguiente consulta muestra un patrón de búsqueda utilizando caracteres comodín, cadenas y una única palabra.

```
word*"quoted string"?
```

### Consulta de intervalo

Una consulta de intervalo puede ser un intervalo de números, versiones o fechas.

La siguiente consulta filtra los resultados incluidos en el intervalo **del 0 al 5** en la propiedad numérica: **prop**

```
prop:[0 TO 5]
```

La siguiente consulta muestra un patrón de búsqueda con un intervalo exclusivo y un inicio que no denota ningún límite máximo en la propiedad numérica: **prop**

```
prop:{10 TO *}]
```

### Guardar la búsqueda

En la barra de búsqueda, utilice la opción **Guardar como nueva recopilación** para guardar un patrón de búsqueda que se utiliza frecuentemente. También se puede utilizar la búsqueda guardada en una consulta.

#### **Uso de la recopilación en una consulta - Ejemplo**

```
collection:"Tomcat Agents" AND reportName:Linux
```

Expresión regular

La consulta de expresiones regulares permite realizar búsquedas mediante expresiones regulares. Comienza y termina con un carácter de barra diagonal. Se puede utilizar una barra diagonal invertida para citar el siguiente carácter de expresión regular. Es posible incluir la barra diagonal como carácter dentro de una consulta.

**Ejemplo:** `name:/^test [3-4][0-9]/`

## Recurso agentFileOperationTask

Este servicio web se puede utilizar para insertar archivos (por ejemplo, archivos de configuración del agente) en un directorio de agente de un sistema remoto.

Este servicio web se puede utilizar para insertar archivos (por ejemplo, archivos de configuración del agente) en un directorio de agente de un sistema remoto. También permite suprimir un archivo de un directorio. Este recurso también se puede usar para obtener una lista de operaciones de copia de archivos realizadas con respecto a un agente.

Verbos admitidos: GET, HEAD, POST, DELETE, OPTIONS  
Supported parameters: [page](#), [size](#), [sort](#)

### NOTE

De forma predeterminada, los métodos POST y DELETE y la inserción de archivos en el recurso de archivo de la API se desactivan y dan como resultado una respuesta no permitida. Para activar esta funcionalidad, edite el archivo `theapmccsrv.properties`.

La siguiente solicitud POST copia el archivo con el ID 12 en el directorio config del agente con el ID 2 como archivo "my-new-app.pbd". Esta solicitud se envía desde el servidor en el que se está ejecutando el agente.

```
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"}
```

La solicitud siguiente suprime el archivo de configuración "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"}
```

Se debe tener en cuenta que solo se pueden publicar los archivos que se han insertado previamente en el [recurso de archivo](#) del servidor de configuración (URL `https://<host cliente ACC>/apm/appmap/acc/apm/acc/file`) o los archivos que forman parte de un informe de diagnóstico. Propiedades de recurso: se encuentran disponibles las siguientes propiedades que contienen información sobre el recurso:

Nombre de la propiedad	Type	Descripción	Versión de la API
tenant	número entero	ID de cliente.	1.1
status	enumeración	El estado de la operación (sigue la definición del recurso de la tarea).	1.0
creationTimestamp	fecha	Hora en la que se creó el recurso (en UTC).	1.0
completionTimestamp	fecha	Hora en la que se completó la operación (en UTC).	1.0
expectedDuration	número entero	Cuánto tiempo se espera que dure la operación en curso.	1.0
source	cadena	El archivo que desea enviar al agente, en relación con el directorio <code>fileUploads</code> del servidor de configuración.	1.0

Nombre de la propiedad	Type	Descripción	Versión de la API
destination	cadena	La ubicación del archivo que desea actualizar o suprimir, en relación con el directorio de instalación del agente.	1.0
operation	enumeración	Operación que desea realizar: "COPY" o "DELETE".	1.0
agentId	número entero	Identificador único del agente en el que se realiza la operación.	1.0
user	cadena	El usuario que ha iniciado la operación.	1.0
updateErrors	matriz	Matriz de errores que se devolvieron durante la operación.	1.0

## Recurso de archivo

Este servicio web devuelve información acerca de los archivos almacenados en el servidor de configuración.

Este servicio web devuelve información acerca de los archivos almacenados en el servidor de configuración. Los archivos están relacionados principalmente con informes de diagnóstico (archivos de registro, perfiles de agente y directivas PBD), pero este recurso además se usa como almacenamiento para los archivos que están diseñados para publicarse en sistemas remotos. Se pueden cargar archivos a este recurso mediante el método POST.

Verbos compatibles: GET, HEAD, POST, DELETE, OPTIONS

Parámetros compatibles: [page](#), [size](#), [sort](#)

### GET

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/file/
```

### POST

Este es un ejemplo de una carga de archivos que utiliza curl:

```
curl -k -H "Authorization:Bearer 3f77f1e5-6985-4019-8f49-af1ed04e0119" -F name=my-new-app.pbd -F file=@mylocalFile.pbd https://<ACC tenant host>/apm/appmap/acc/apm/acc/file
```

Se obtiene una respuesta similar a la siguiente:

```
{ "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://<ACC tenant host>/apm/appmap/acc/apm/acc/file/1/content" } } }
```

El valor "id" es un identificador del archivo que se utiliza más adelante en la solicitud de agentFileOperationTask POST para el campo "file" (por ejemplo, "file": "file/32").

### Propiedades del recurso

Se encuentran disponibles las siguientes propiedades que contienen información sobre el recurso:

Nombre de la propiedad	Type	Descripción	Versión de la API
tenant	número entero	ID de cliente.	1.1
id	número entero	Identificador único para este recurso.	1.1
name	cadena	Nombre del archivo.	1.1
size	número entero	Tamaño en bytes del archivo no comprimido.	1.1
createdBy	cadena	Nombre de usuario que ha publicado el archivo, nulo si forma parte de un informe de diagnóstico.	1.1
modificado	fecha	La hora de modificación del archivo. Se establece en "hora actual" si un usuario ha registrado el archivo.	1.1
archivo	archivo de varias partes	Parámetro de formulario utilizado en los comandos POST para cargar el recurso de archivo.	1.1

## Recurso del paquete

Este servicio web devuelve información sobre los paquetes de agente disponibles en APM Command Center.

Este servicio web devuelve información sobre los paquetes de agente disponibles en APM Command Center. También puede descargar estos paquetes en formato ZIP o TAR. Verbos compatibles: GET, HEAD, POST, PATCH, DELETE, OPTIONS

Parámetros compatibles: [page](#), [size](#), [sort](#), [q](#), format, [projection](#)

### GET

```
GET https://<host del cliente de ACC>/apm/appmap/acc/apm/acc/package
```

Utilice la solicitud siguiente para obtener información sobre el paquete con el ID 1:

```
GET https://<host del cliente de ACC>/apm/appmap/acc/apm/acc/package/1
```

Para descargar el paquete, acceda al vínculo disponible en la página de detalles del paquete de Command Center en la IU.

Utilice la siguiente solicitud para obtener las instrucciones de instalación (en formato Markdown) del paquete:

```
GET https://<host del cliente de ACC>/apm/appmap/acc/apm/acc/package/1/installInstructions
```

Utilice la solicitud siguiente para obtener información sobre los conjuntos que contiene el paquete:

```
GET https://<host del cliente de ACC>/apm/appmap/acc/apm/acc/package/1/bundles
```

Utilice la solicitud siguiente para obtener información sobre los conjuntos necesarios para el paquete:

```
GET https://<host del cliente de ACC>/apm/appmap/acc/apm/acc/package/1/requiredBundles
```

Utilice la solicitud siguiente para obtener información sobre todos los conjuntos que son compatibles con el paquete, incluidos los que ya están incluidos en el paquete:



GET https://<host del cliente de ACC>/apm/appmap/acc/apm/acc/package/1/compatibleBundles

Utilice la solicitud siguiente para obtener información sobre todos los paquetes que sean compatibles con el paquete especificado:

GET https://<host del cliente de ACC>/apm/appmap/acc/apm/acc/package/1/compatiblePackages

**POST:** La siguiente solicitud crea un paquete del agente con las propiedades especificadas.

```
POST https://<host del cliente de ACC>/apm/appmap/acc/apm/acc/package{ "name": "WebSphere
Windows Package", "description": "Example WebSphere Package", "environment": { "osName":
"windows", "process": "websphere", "agentVersion": "10.2" }}
```

**PATCH:** Las solicitudes de PATCH permiten agregar o actualizar una propiedad del conjunto en el paquete. En el ejemplo siguiente se actualizan las propiedades patched.via.rest.api e introscope.agent.acc.port con los valores especificados:

```
PATCH https://<ACC tenant host>/apm/appmap/acc/apm/acc/package/111{ "bundleOverrides":
{ "acc": { "preamble": null, "properties": [{ "name": "new.via.ui",
"description": null, "type": null, "value": "yes it is",
"validator": null, "hidden": false, "id": null }, { "name":
"patched.via.rest.api", "value": "from a patch" }, { "name":
"introscope.agent.acc.port", "value": 55555 }] } }}
```

**DELETE:** La siguiente solicitud suprime el paquete del agente con el ID 2:

DELETE https://<host del cliente de ACC>/apm/appmap/acc/apm/acc/package/2

### Propiedades del recurso

Se encuentran disponibles las siguientes propiedades que contienen información sobre el recurso:

Nombre de la propiedad	Type	Descripción	Versión de la API
tenant	número entero	ID de cliente.	1.1
id	número entero	Identificador único para este recurso.	1.1
name	cadena	Nombre del paquete.	1.1
description	cadena	Comentario para el paquete introducido por el usuario.	1.1
version	número entero	Número de versión de este paquete (se incrementa después de la descarga del paquete editado).	1.1
bundles	subrecurso	Conjuntos que contiene el paquete.	1.1
emHost	cadena	Nombre de host o dirección IP y el puerto de las instancias de Enterprise Manager a las que se conecta el agente.	1.1
latest	Valor booleano	Indica qué versión del paquete es la actual.	1.1
origin	número entero	ID de la versión original del paquete.	1.1
draft	Valor booleano	Indica si el paquete debe estar disponible para su uso.	1.1

## Recurso bundle

Este servicio web devuelve información acerca de los conjuntos disponibles en APM Command Center. Verbos compatibles: GET, HEAD, POST, DELETE, OPTIONS. Parámetros compatibles: [page](#), [size](#), [sort](#), [q](#)

### GET

GET <https://<ACC tenant host>/apm/appmap/acc/apm/acc/bundle>

### POST

A continuación se muestra un ejemplo de una carga de conjuntos que utiliza curl:

```
curl -k -H "Authorization:Bearer <TOKEN>" -F file=@leakhunter-10.5.tar.gzhttps://<ACC tenant host>/apm/appmap/acc/apm/acc/bundle
```

Se obtiene una respuesta similar a la siguiente:

```
{ "id": 26, "name": "leakhunter", "addedBy": null, "author": "Not Specified",
 "displayName": "Leak Hunter", "description": "This bundle tracks the size of most
 default Java Collections.", "version": "10.5", "agentVersion": "10.5", "path":
 "leakhunter-10.5.tar.gz", "facets": ["leakhunter"], "dependencies": ["java-agent",
 "process"], "enhances": [], "excludes": [], "compatibility": { "osName": null,
 "agentVersion": "10.5" }, "specificationVersion": "1", "type": "java", "dynamic":
 null, "links": { "self": { "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/
 bundle/26" }, "profile": { "href": "https://<ACC tenant host>/apm/appmap/acc/apm/acc/
 bundle/26/profile" }, "download": { "href": "https://<ACC tenant host>/apm/appmap/acc/apm/
 acc/bundle/26?format=archive" } } }
```

### DELETE

La solicitud siguiente suprime el conjunto con el ID 21:

DELETE <https://<ACC tenant host>/apm/appmap/acc/apm/acc/bundle/21>

Cuando se suprime un conjunto:

- Ya no será visible cuando se realice un GET en el recurso.
- Ya no se mostrará como un conjunto disponible cuando se cree un paquete nuevo o cuando se edite uno existente.
- Aparecerá en los paquetes existentes que lo utilizan, pero se marcará como un conjunto suprimido. Una vez que el conjunto se haya eliminado de un paquete, no será posible agregarlo de nuevo.

**Nota:** No es posible suprimir las propiedades fundamentales bundles.Resource.

Se encuentran disponibles las siguientes propiedades que contienen información sobre el recurso:

Nombre de la propiedad	Type	Descripción	Versión de la API
tenant	número entero	ID de cliente.	1.1
id	número entero	Identificador único del recurso.	1.1
name	cadena	Nombre interno del conjunto	1.1
displayName	cadena	Nombre del conjunto en formato práctico.	1.1
description	cadena	Breve descripción del conjunto.	1.1
version	cadena	Versión del conjunto.	1.1
agentVersion	cadena	Versión del Agente de APM para el que está diseñado el conjunto.	1.1

Nombre de la propiedad	Type	Descripción	Versión de la API
ruta	cadena	Ruta del archivo de archivado del conjunto.	1.1
facets	matriz	Lista de facetas que identifican al conjunto.	1.1
dependencies	matriz	Lista de facetas de las que depende el conjunto.	1.1
enhances	matriz	Lista de facetas que mejora el conjunto.	1.1
compatibility	subrecurso	Define las restricciones de compatibilidad del conjunto como "osName" y "agentVersion".	1.1
specificationVersion	cadena	Versión de la especificación de metadatos del conjunto.	1.1
type	cadena	Tipo de conjunto. Actualmente, siempre es "Java".	1.1
suprimido	Valor booleano	Determina si el conjunto está suprimido (true) o activo (null o false).	1.1
categoría	cadena	Categoría del conjunto: principal, entorno, función, personalizado.	1.1

## Recurso agentPackageTask

El servicio web de agentPackageTask se puede utilizar para actualizar un paquete de agente con conjuntos de implementación en caliente nuevos o modificados.

El servicio web de agentPackageTask se puede utilizar para actualizar un paquete de agente con conjuntos de implementación en caliente nuevos o modificados. Este servicio web proporciona un paquete con las modificaciones realizadas en el directorio de instalación del Agente de APM. Verbos compatibles: GET, HEAD, POST, OPTIONS. Parámetros compatibles: [page](#), [size](#), [sort](#).

### GET

GET <https://<ACC tenant host>/apm/appmap/acc/apm/acc/agentPackageTask/>

**POST** La API de REST siguiente inicia una solicitud de inserción. Los conjuntos no se pueden implementar directamente en los agentes, sino que se deben incluir en un paquete que se inserta en el agente. Especifique el ID del agente que se desea actualizar y el ID del paquete que se va a entregar.

POST <https://<ACC tenant host>/apm/appmap/acc/apm/acc/agentPackageTask>{agent: agent/1,package: package/5}

Propiedades de recurso. Se encuentran disponibles las siguientes propiedades que contienen información sobre el recurso:

Nombre de la propiedad	Type	Descripción	Versión de la API
tenant	número entero	ID de cliente.	1.1
agent	número entero	Identificador único del agente en el que se realiza la operación.	1.1
paquete	número entero	Identificador único del paquete implementado en el agente.	1.1
status	enumeración	El estado de la solicitud.	1.1
extStatus	cadena	Explica el estado "FAILED". Según las directrices de la API de REST, solo es necesario un único estado "Failed". Da más información sobre la causa de los errores, como que el controlador no responde o el agente no vuelve a registrarse en el tiempo.	1.1
creationTimestamp	fecha	Hora en la que se creó el recurso (en UTC).	1.1
completionTimestamp	fecha	Hora en la que se completó la operación (en UTC).	1.1
expectedDuration	número entero	Cuánto tiempo se espera que dure la operación en curso.	1.1
user	cadena	El usuario que ha iniciado la operación.	1.1
updateErrors	matriz	Una matriz de errores relacionados con los complementos como, por ejemplo, problemas de permisos al copiar conjuntos en el directorio wily.	1.1
addedBundles	matriz	La lista de nombres de conjuntos que se van a agregar (puede estar vacía).	1.1
removedBundles	matriz	La lista de nombres de conjuntos que se van a eliminar (puede estar vacía).	1.1

## API de hipermedia de DX APM

DX APM proporciona varias API de hipermedia públicas que los usuarios pueden utilizar. Esta sección trata sobre los conceptos básicos y los mecanismos comunes compartidos a través de las API de hipermedia de DX APM:

La arquitectura de la aplicación REST HATEOAS (Hypermedia as the Engine of Application State) permite a un cliente interactuar con DX APM a través de hipermedia. Para poder utilizar la API de hipermedia solo deberá conocer la

dirección [URL base](#): todos los recursos y acciones disponibles se proporcionan dinámicamente a través del servidor de aplicaciones mientras trabaja.

Las API RESTful de DX APM utilizan HTTP como el protocolo predeterminado y el [Hypertext Application Language \(HAL\)](#) y [JSON](#) para las representaciones.

Tenga en cuenta que no todas las funciones descritas en esta especificación se implementan en todas las API. Para obtener más información acerca de cada API, consulte [API de REST de DX APM](#).

Puede utilizar varias herramientas para interactuar con las API de hipermedia de DX APM. Por ejemplo:

- Extensión de Postman Chrome
- cURL (herramienta de línea de comandos)
- lenguajes de programación (Python)

### **Códigos de estado de la respuesta**

La API devuelve códigos de estado HTTP junto con la respuesta.

Por lo general, los códigos de estado HTTP se agrupan en distintas categorías:

- los códigos **1xx** son informativos
- **2xx** indican éxito
- **3xx** dan instrucciones a un redireccionamiento
- **4xx** indican errores del cliente (el cliente ha hecho algo incorrecto)
- **5xx** definen errores del servidor (el servidor ha hecho algo incorrecto)

La tabla siguiente muestra los códigos de estado correctos según el método utilizado:

Método	Resultado correcto	Acompañamiento del encabezado	Cuerpo de la respuesta
GET	200 Correcto	varía	varía
POST	201 Creado	Ubicación: señala al recurso creado	vacío
POST - asincrónico	202 Aceptado	Ubicación: señala a un recurso que se va a crear en breve	vacío
POST	200 Correcto	-	recurso creado
PUT (nuevo recurso)	201 Creado	Ubicación: señala al recurso creado	vacío
PUT (nuevo recurso)	200 Correcto	-	recurso creado
PUT (nuevo recurso) - asincrónico	202 Aceptado	Ubicación: señala a un recurso que se va a crear en breve	vacío
PUT (recurso existente)	204 Sin contenido	-	vacío
PUT (recurso existente) - asincrónico	202 Aceptado	Ubicación: señala a un recurso que se va a actualizar en breve	vacío
PATCH	204 Sin contenido	-	vacío
PARCHE - asincrónico	202 Aceptado	-	vacío
DELETE	200 Correcto	-	-
DELETE - asincrónico	202 Aceptado	-	-

## Autorización y autenticación de la API

La autenticación de las API de RESTful de APM se basa en los tokens de portador que se pueden crear en la interfaz de usuario de la aplicación asociada. El token proporciona el acceso de API a los servicios web de la aplicación.

Los clientes pueden crear tokens asociados a su cuenta. También se pueden actualizar, recuperar y suprimir (revocar) los tokens que poseen o que tienen acceso de lectura/escritura, siempre que se autentifiquen y autoricen.

### Creación de tokens de portador

Consulte la documentación de la API específica para obtener más información sobre cómo crear un token de portador.

### Uso de los tokens de portador

El cliente debe enviar un token con cada solicitud. La demostración de un token es suficiente para que el servidor de recursos autentique al cliente y aplique las reglas de autorización a la solicitud.

El token portador se envía al servidor de recursos en el campo de encabezado de la solicitud de autorización. Por ejemplo:

```
GET /resource HTTP/1.1
Host: server.example.com
Authorization: Bearer f47ac10b-58cc-4378-a567-0e02b2c3d479
```

### Códigos de error y estados HTTP de la autenticación

Si se produce un error en la autenticación de la solicitud por algún motivo, el servidor de recursos devuelve un código de error de HTTP relevante y un encabezado de respuesta con los detalles del error.

- 401 no autorizado
- 403 prohibido

Consulte [Definiciones de código de estado HTTP](#) para obtener más información.

## Acceso a los recursos

La recuperación de recursos puede implementarse con solicitudes HTTP GET simples. Al acceder a la dirección URL base con el explorador web, se puede recuperar el recurso raíz que informa de los recursos y acciones disponibles. Se pueden solicitar recursos individuales o recopilaciones de recursos, se puede controlar la paginación o el orden, y se puede filtrar y buscar recursos.

Las API de RESTful para DX APM admiten el tipo de medio de Internet HAL y devuelven un documento con el formato HAL de forma predeterminada. Algunas API también admiten otros formatos, tales como aplicación/xml, texto/csv, texto/sin formato, etc.

### Recurso raíz

Todas las API públicas de DX APM exponen un recurso raíz. El recurso raíz contiene los vínculos (HAL) a todos los recursos disponibles y también información adicional como metadatos, versiones, etc.

El recurso raíz se puede recuperar accediendo a la dirección URL base de la API.

```
GET https://<host>:<port>/apm/<service>
```

Por ejemplo, utilice la siguiente solicitud para obtener el recurso raíz de APM Command Center:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc
```

El recurso raíz que se recibe como respuesta es el siguiente:

```
{
 "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
 },
 .
 .
 .
 }
}
```

El recurso raíz incluye la siguiente información:

- vendor: Broadcom
- apiVersion: La versión de la API
- serverVersion: La versión de la aplicación o del componente que expone su lógica de negocios mediante esta API de RESTful.
- serviceProvider: El nombre del servicio completo
- \_links: Una lista de los vínculos a todos los recursos disponibles

### **Recopilación de recursos**

El cliente puede solicitar recursos individuales o una recopilación de recursos. Las recopilaciones se representan como matrices (según el formato JSON) de los recursos individuales.

GET https://<host>:<port>/apm/<service>/resource

Se incrusta una matriz de los recursos individuales dentro de la propiedad \_embedded del recurso:

```
{
 "_links": {
 << list of related links >>
 },
 "_embedded": {
 "<< resource name >>": [
 {
 << resource 1 data >>
 },
 {
 << resource 2 data >>
 },

]
 },
 "_page" : {
 <paging information>
 }
}
```

```
}
```

Cuando se solicita un recurso individual, la respuesta contiene solamente el recurso solicitado.

```
GET https://<host>:<port>/apm/<service>/resource/1
```

Respuesta de ejemplo:

```
{
 "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"
 }
 }
}
```

### **Parámetros de solicitud comunes**

Al acceder a recopilaciones de recursos, el número de recursos puede llegar a ser muy elevado y resultar poco práctico. Los clientes pueden utilizar las siguientes propiedades como parámetros de consulta HTTP GET para que las solicitudes sean más específicas:

- [página y tamaño](#)
- [ordenar](#)
- [proyección](#)
- [formato](#)
- [q](#)

### **Página y tamaño**

Se puede controlar la página que se desea que se devuelva o cuántos resultados debe contener una página. De forma predeterminada, se devuelven los primeros 20 resultados.

Utilice los siguientes parámetros:

- **page**  
El número de la página que se va a devolver (valor predeterminado 0 = se devuelve la primera página).
- **size**  
El tamaño de la página deseado. Size=0 significa que se muestran todos los recursos.

### **Ejemplos:**

La siguiente solicitud devuelve los primeros 50 resultados:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?page=0&size=50
```



La siguiente solicitud devuelve los resultados 51-60:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?page=5&size=10
```

### **Ordenación**

Las recopilaciones se pueden ordenar por propiedades de recurso específicas. Los clientes pueden utilizar el parámetro "sort" para controlar la ordenación.

### **Ejemplos:**

La siguiente solicitud ordena los agentes por nombre:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?sort=agentName
```

La siguiente solicitud recupera el primer (size=1) recurso de agente de la lista ordenada por nombre de agente en modo descendente y por ruta de instalación en modo ascendente. El orden de los parámetros se tiene en cuenta.

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?
sort=name,DESC&sort=installPath,ASC&size=1
```

### **Proyección**

Las proyecciones devuelven un subconjunto predefinido de datos. Existen dos tipos de proyecciones disponibles:

- **Proyecciones estáticas**

Las proyecciones estáticas son subconjuntos predefinidos de propiedades disponibles del recurso. Tienen un nombre documentado y se pueden transferir con el parámetro HTTP "projection" al solicitar una recopilación de recursos o un recurso específico.

- **Proyecciones dinámicas**

Las proyecciones dinámicas permiten al cliente definir explícitamente las propiedades del recurso que se devolverán. Cuando se utilizan recursos dinámicos, el parámetro HTTP "fields" define una lista separada por comas de los campos de recurso esperados.

Las proyecciones (cuando están disponibles) se describen en la documentación de la API correspondiente.

### **Ejemplo:**

La siguiente solicitud devuelve una lista de agentes con información básica:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?projection=list
```

Respuesta de ejemplo:

```
{ "_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 }}

```

### **Formato**

Devuelve datos en el formato especificado. El parámetro "format" tiene precedencia sobre el encabezado HTTP "Accept", que es el mecanismo predeterminado para solicitar un formato específico (por ejemplo, Accept: text/csv; q=1.0).

### **Ejemplo:**

La siguiente solicitud devuelve información sobre los agentes en formato CSV:

```
GET https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?format=csv
```

Respuesta de ejemplo:

```
"id","agentName","serverName","processName","status","type","version","build","logLevel","registries"
"1","Tomcat
Agent","ACCLinuxServer01","Tomcat","ACTIVE","JavaAgent","9.7.1","16","INFO","2015-04-29
05:15:46 +0100","2015-04-30 05:20:45 +0100","ACCWinServer01","5001","Apache
Tomcat","5.5.34.0","Oracle Corporation","1.7.0",,"Red Hat Enterprise Linux
Server","6.1, kernel 2.6.32-131.0.15.el6.x86_64","amd64","59"
"2","Tomcat
Agent","ACCWinServer01","Tomcat","ACTIVE","JavaAgent","9.7.1","16","INFO","2015-04-29
05:16:26 +0100","2015-04-30 05:16:26 +0100","ACCWinServer01","5001","Apache
Tomcat","5.5.34.0","Oracle Corporation","1.7.0_51",,"Windows Server 2008
R2","6.1","amd64","66"
```

## Q

Busca o filtra la recopilación. Esta opción puede utilizarse para transferir [consultas de búsqueda o filtro](#) al servidor de recursos.

### Fecha y hora

La fecha y la hora se representan mediante el formato [ISO 8601](#).

## Búsqueda y filtrado de recursos

La **búsqueda** es una funcionalidad que permite a un cliente recuperar información de la API. El resultado es normalmente un documento que contiene múltiples y distintos recursos.

La búsqueda utiliza un recurso explícito (/search) que acepta cualquier solicitud GET que transfiera la cadena de búsqueda como el valor del parámetro de consulta HTTP "q" o cualquier solicitud POST que envíe la cadena de búsqueda con el cuerpo de la solicitud. La respuesta contiene un documento JSON con los resultados en forma de recursos\_embedded.

El **filtrado** es la capacidad de la API para devolver una recopilación filtrada de un recurso específico.

El filtrado se implementa como parte de cada recurso que admite el filtrado. Los recursos que admiten el filtrado anuncian la capacidad de filtrado en los vínculos con plantillas HAL (tenga en cuenta el parámetro "q" del ejemplo siguiente):

```
{
 "_links": {
 "self": {
 "href": "/agent{?q,page,projection,size,sort}",
 "templated": true
 }
 }
 ...
 ...
}
```

Los clientes pueden utilizar las capacidades de filtrado de un recurso mediante una solicitud GET (transfiere la cadena de búsqueda como el valor del parámetro de consulta HTTP "q") o una solicitud POST (envía la cadena de búsqueda con el cuerpo de la solicitud).

### Ejemplo:

`https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=agentName:Tomcat`

#### **NOTE**

El recurso de búsqueda no está siempre disponible en una API; la capacidad de filtrado tampoco está siempre implementada. Los usuarios deben leer la documentación de las API individuales para comprobar si las funciones están disponibles.

La [sintaxis de Lucene](#) es compatible con las capacidades de búsqueda y filtrado. Los siguientes párrafos describen la sintaxis de cadena de consulta que admiten las API de RESTful para CA APM.

#### **Términos**

Una consulta puede constar de un solo término o de una frase entre comillas dobles. Se pueden combinar varios términos juntos con los operadores booleanos para formular una consulta más compleja.

#### **Campos**

Al realizar una búsqueda, se puede especificar un campo. Se puede buscar cualquier campo escribiendo el nombre del campo seguido de dos puntos y, a continuación, el término que se desea buscar. Utilice comillas para frase de varias palabras. Si no se especifica ningún campo, se buscan todos los campos.

#### **Ejemplo:**

La siguiente consulta busca todos los agentes denominados Apache Tomcat:

`https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=agentName:"Apache Tomcat"`

#### **Búsquedas con caracteres comodín**

La búsqueda admite las búsquedas con uno o varios caracteres comodín dentro de un único término (pero no en las consultas de tipo frase):

- Para realizar una búsqueda con un único carácter comodín, utilice el símbolo "?".
- Para realizar una búsqueda con varios caracteres comodín, utilice el símbolo "\*".

#### **Ejemplo:**

La siguiente consulta busca todos los agentes que se ejecutan en un servidor cuyo nombre incluye "Linux":

`https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=serverName:*Linux*`

#### **Búsquedas con expresiones regulares**

La búsqueda admite las búsquedas con expresiones regulares que coincidan con un patrón entre barras diagonales hacia delante "/". La sintaxis puede variar de versión a versión, pero la sintaxis compatible actual está documentada en la clase [RegExp](#).

#### **Ejemplo:**

La siguiente consulta busca informes cuyo nombre incluye los caracteres indicados. Tanto la cadena "ACCServerWin01|Tomcat|Tomcat Agent" como la cadena "ACCServerLinux01|Tomcat|Bobcat Agent" coinciden con esta consulta.

`https://<ACC tenant host>/apm/appmap/acc/apm/acc/diagnosticReport?q=/ACCServer.*01\|Tomcat\|.*Agent/`

## **Búsquedas de intervalo**

Las búsquedas de intervalo permiten combinar documentos cuyos valores de campo se encuentren entre el límite superior y el límite inferior especificados por la búsqueda de intervalo. Las búsquedas de intervalo pueden ser inclusivas o exclusivas de los límites superior e inferior. Las búsquedas de intervalo incluidas se indican mediante corchetes y las búsquedas de intervalo excluidas se indican por medio de llaves. La ordenación se realiza lexicográficamente.

Además de las fechas exactas, también se pueden utilizar períodos de tiempo, como semanas (w), días (d), horas (h), minutos (m) y segundos (s).

### **Ejemplos:**

La siguiente consulta busca todos los agentes cuya última marca de tiempo de contacto sea entre el 1 de abril de 2015 (incluido) y el día de hoy:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=lastContact:[2015-04-01 TO NOW]
```

Esta consulta busca todos los agentes cuya última marca de tiempo de contacto sea entre el 1 de abril y el 1 de junio de 2015 pero excluyendo esos días:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=lastContact:{2015-04-01 TO 2015-06-01}
```

Esta consulta busca los agentes cuya última marca de tiempo de contacto no sea superior a cinco días:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=lastContact:[-5d TO NOW]
```

La siguiente consulta busca los agentes cuya última marca de tiempo de contacto sea dos o más días atrás, pero sin sobrepasar las cinco semanas:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=lastContact:[-5w TO -2d]
```

## **Promoción de un término**

La sintaxis de búsqueda puede proporcionar cierto nivel de relevancia a los documentos coincidentes en función de los términos encontrados. Para promover un término, utilice el acento circunflejo (^), símbolo con un factor de aumento (número), al final del término que está buscando. Cuanto mayor sea el factor de aumento, más importante será el término.

## **Operadores booleanos**

Los operadores booleanos permiten combinar los términos mediante operadores lógicos.

- **OR**

El operador OR es el operador de conjunción predeterminado. Esto significa que si no hay ningún operador booleano entre dos términos, se utilizará el operador OR. El operador OR enlaza dos términos y encuentra un documento coincidente si alguno de los términos existe en un documento. El símbolo || puede utilizarse en lugar de la palabra OR.

- **AND**

El operador AND coincide con documentos en los que ambos términos existen en algún lugar de un texto de un único documento. El símbolo && puede utilizarse para sustituir la palabra AND.

- **+**

"+" o el operador "necesario" requiere que el término que sigue al símbolo "+" exista en algún punto en el campo de un único documento.

- **NOT**

El operador NOT excluye los documentos que contengan el término que sigue a NOT. El símbolo "!" puede utilizarse para sustituir la palabra NOT.

- **-**  
"-" o el operador "prohibido" excluye los documentos que contienen el término que sigue al símbolo "-".

### Ejemplos:

La siguiente consulta detecta los agentes cuyo nombre es Tomcat y su nivel de registro está establecido en "debug":

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=agentName:Tomcat AND
logLevel:debug
```

La siguiente consulta busca todos los agentes activos que se ejecutan en un servidor Linux:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=osName:Linux NOT status:away
```

La siguiente consulta busca recursos que contengan "Linux" y que puedan contener "server":

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=+Linux server
```

### Agrupación

La sintaxis admite el uso de paréntesis para agrupar frases para formar subconsultas. Esto puede resultar útil si se desea controlar la lógica booleana para una consulta.

#### Ejemplo:

La siguiente consulta busca agentes cuyo nombre sea Tomcat y estén en ejecución en el servidor de aplicaciones versión 5.4 o 5.5:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=(appServerVersion:5.5* OR
appServerVersion:5.4*) AND agentName:Tomcat
```

### Agrupación de campos

La sintaxis admite el uso de paréntesis para agrupar varias cláusulas en un único campo.

#### Ejemplo:

La siguiente consulta busca agentes que se ejecuten en servidores Windows o Linux:

```
https://<ACC tenant host>/apm/appmap/acc/apm/acc/agent?q=osName:(Windows OR Linux)
```

### Escape de caracteres especiales

La sintaxis permite escapar los caracteres especiales siguientes: + - && || ! ( ) { } [ ] ^ " ~ \* ? : \ /

Para activar el escape de estos caracteres, utilice una barra invertida "\" antes del carácter.

## Creación y actualización de recursos

Los recursos se crean mediante las solicitudes POST o PUT HTTP:

- POST se utiliza cuando el cliente no necesita especificar el ID del recurso que se genera. La API crea el ID y lo devuelve al cliente.
- PUT se utiliza cuando se el ID es conocido por el cliente.

Un recurso se puede actualizar mediante PUT o PATCH:

- PUT requiere una representación completa de la entidad que se va a proporcionar, pero se pueden omitir campos opcionales, en cuyo caso el servidor de recursos conserva los valores existentes. El campo Tipo de contenido define el tipo de medio de Internet de la representación.
- PATCH se interpreta mediante el servidor de recursos como una solicitud para aplicar un "parche" a un recurso existente. El cuerpo de la solicitud debe contener toda la información necesaria para el cambio.

### NOTE

No todos los recursos sirven de apoyo de estos métodos puesto que algunos recursos son de solo lectura. Consulte la documentación de la API específica antes de utilizar solicitudes no seguras (crear, actualizar, suprimir).

### Hoja de referencia sobre el método HTTP

La tabla siguiente puede ayudarle a decidir qué verbo HTTP se debe utilizar para la creación, actualización o supresión de recursos.

Acción	Método HTTP	URL	Cuerpo de solicitud
Crear nuevo recurso sin especificar el ID	POST	Utilice la URL de recopilación. Por ejemplo: <code>http://host:port/apm/acc/agents</code>	Incluye todas las propiedades no nulas del recurso en la carga útil. Al omitir una propiedad se establece su valor como valor predeterminado si se permite, o como error si la propiedad no tiene un valor predeterminado.
Crear un nuevo recurso con un ID específico	PUT	Especifique el ID exacto en la dirección URL. Por ejemplo: <code>http://host:port/apm/acc/agents/14</code> para crear un agente con ID 14.	Incluye todas las propiedades no nulas del recurso en la carga útil. Al omitir una propiedad se establece su valor como valor predeterminado si se permite, o como error si la propiedad no tiene un valor predeterminado.
Actualizar un recurso con uno nuevo (actualización completa)	PUT	Especifique el ID exacto en la dirección URL. Por ejemplo: <code>http://host:port/apm/acc/agents/14</code> para crear un agente con ID 14.	Incluye todas las propiedades no nulas del recurso en la carga útil. Al omitir una propiedad se establece su valor como valor predeterminado si se permite, o como error si la propiedad no tiene un valor predeterminado.
Actualizar parcialmente un recurso	PATCH	Especifique el ID exacto en la dirección URL. Por ejemplo: <code>http://host:port/apm/acc/agents/14</code> para crear un agente con ID 14.	Incluye solo las propiedades que se desean actualizar. La omisión de una propiedad significa que el servidor utilizará el valor actual del recurso.

Suprimir un recurso	DELETE	Especifique el ID exacto en la dirección URL. Por ejemplo: http://host:port/apm/acc/agents/14 para suprimir un agente con ID 14.	n/d
---------------------	--------	-------------------------------------------------------------------------------------------------------------------------------------	-----

## Ejemplos

Para obtener ejemplos del uso del método POST, PUT o PATCH, consulte la documentación de las implementaciones específicas de la API.

## Encabezados HTTP comunes

### Encabezados de solicitud

La siguiente tabla enumera los encabezados de las solicitudes HTTP que normalmente son compatibles con las API de RESTful para DX APM.

Encabezado HTTP	Caso de uso/Finalidad
Accept-Language	El cliente solicita un idioma específico para utilizarlo al crear las representaciones. El campo de encabezado de la solicitud Accept-Language es similar al encabezado Accept, pero restringe el conjunto de idiomas naturales preferibles como respuesta a la solicitud.
Content-Type	Se utiliza cuando el cliente envía un cuerpo de mensaje con una solicitud POST, PUT o PATCH. Describe el tipo de medio de Internet que se utiliza para codificar el cuerpo de la solicitud HTTP.
Authorization	Se utiliza cuando el cliente desea autenticar la solicitud. El cliente envía las credenciales que contienen la información de autenticación.
Accept-Encoding	El cliente solicita al servidor que utilice la compresión de respuestas (si es posible).
Host	Encabezado obligatorio según el protocolo HTTP. El campo de encabezado de solicitud Host especifica el número de puerto y el host de Internet del recurso solicitado, tal y como se ha obtenido del URI original proporcionado por el usuario o el recurso al que hace referencia.
If-None-Match	El cliente utiliza este encabezado para enviar el valor e-tag de la representación en memoria caché.
If-Match	El cliente desea procesar la operación solicitada (por ejemplo, DELETE) solamente si coincide con una condición previa de e-tag. El encabezado contiene el valor de una respuesta e-tag de la llamada anterior. El servidor deberá actuar solo si ningún otro cliente ha modificado el recurso.
If-Modified-Since	El cliente utiliza este encabezado para enviar la fecha de la última modificación del recurso en la memoria caché.



## Encabezados de respuesta

La siguiente tabla enumera los encabezados de respuesta HTTP que puede devolver el servidor.

Encabezado HTTP	Caso de uso/Finalidad
Content-Type	Describe el tipo de medio de Internet que se utiliza para codificar el cuerpo de la respuesta HTTP.
Content-Encoding	Si está presente, el valor indica los códigos de contenido adicionales que se han aplicado al cuerpo de la entidad (por ejemplo, la compresión .gzip).
Cache-Control	El campo de encabezado general Cache-Control se utiliza para especificar las directivas que deben obedecer todos los mecanismos de almacenamiento en caché a lo largo de la cadena de solicitud/respuesta.

### Más información:

Para obtener información detallada acerca de las definiciones de campo de encabezado, consulte el [sitio web de W3C](#).

## Mensajes y códigos de error

La API devuelve un error para todas las operaciones con un resultado inesperado. El error contiene la información siguiente:

- Código de error
- Mensaje de error
- Marca de tiempo
- Un vínculo a la documentación con la descripción completa del error

A continuación, se muestra un ejemplo del mensaje de error:

```
{ "_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 códigos de error

Los códigos de error de la API comienzan por EA seguido de cuatro dígitos. Los errores se dividen en dos categorías: errores comunes (para todas las API) y errores específicos del recurso. Para obtener descripciones de errores específicos de recursos, consulte la documentación de la API correspondiente.

Intervalo de códigos de error	Proveedor de recursos
1000-1014	Códigos de error heredados de EPAgent
EA0000-EA0999	Errores estándares del sector (códigos de estado HTTP)
EA1000-EA1999	Errores generales de la API de CA APM
EA2000-EA2999	Errores de la API de REST de Enterprise Manager
EA3000-EA3999	Errores de la API de REST de Command Center
EA4000-EA4999	Nuevos códigos de error de EPAgent

## Errores estándares del sector

Los errores del intervalo EA0100-EA0599 son códigos de estado HTTP estándares. Para obtener información detallada, consulte [RFC 7231](#).

## Errores generales de la API de CA APM

Código de error (intervalo)	Descripción	Uso
EA1001	Consulta de búsqueda no válida	Se devuelve cuando una solicitud de filtro o búsqueda produce un error debido a una consulta que no cumple con la sintaxis de Lucene.

## Mensajes y códigos de error específicos de la API

Error Code	Tipo de error
<b>403 prohibido</b>	
1000	ACCESS_FORBIDDEN
1001	LOGIN_FAILED
<b>405 Method Not Allowed</b>	
2000	METHOD_NOT_ALLOWED
2001	ATTRIBUTE_CANNOT_BE_DELETED
2002	ATTRIBUTE_CANNOT_BE_UPDATED
<b>400 Bad Request</b>	
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
<b>404 Not Found</b>	
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

Error Code	Tipo de error
4008	SETTINGS_NOT_FOUND
4009	UNIVERSE_NOT_FOUND
<b>409 Conflict</b>	
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
<b>500 Internal Server Error</b>	
6000	INTERNAL_SERVER_ERROR
<b>415 Unsupported Media Type</b>	
7000	UNSUPPORTED_MEDIA_TYPE
<b>503 Service Unavailable</b>	
8000	SERVICE_UNAVAILABLE
8001	ACC_SERVER_UNAVAILABLE

## La API de REST de DX APM

Utilice la API de REST de DX APM en scripts automatizados para crear, actualizar y suprimir atributos del vértice. Para cada servicio web disponible, se muestran los parámetros de solicitud y de verbos de HTTP compatibles.

### NOTE

**Más información:** [API de hipermedia de DX APM](#)

DX APM es compatible con los siguientes servicios web de RESTful:

- [Regla de atributo](#)
- [Gráfica](#)
- [Vértice del gráfico](#)
- [Gráfico incremental](#)
- [Id del vértice del gráfico](#)
- [Gráfico Vertexstatus incremental](#)
- [Recurso raíz](#)
- [Universo](#)
- [Vértice](#)
- [ID del vértice](#)
- [Ejemplo de Java de la API de REST para obtener actualizaciones incrementales](#)

Esta API incluye **nuevos** recursos que no estaban disponibles anteriormente. Los recursos originales root, /vertex/ y /vertex/{id} son compatibles. Se recomienda migrar a la nueva interfaz para aprovechar las ventajas de las nuevas funciones.

Todas las direcciones URL de los recursos tienen los formatos siguientes:

- DX APM local:  
http://{hostname}:8081/{tenantId}/apm/atc/api/
- DX SaaS:  
https://{hostname}/{tenantId}/apm/atc/api/

La tabla siguiente muestra todos los recursos disponibles de la API de REST de DX APM, así como los verbos y parámetros de HTTP que son compatibles con los recursos.

Resource	Descripción	Verbos de HTTP	Parámetros	Otros
/tenantId/apm/atc/api/vertex (recopilación)	Representa una recopilación de vértices	<ul style="list-style-type: none"> <li>• GET: Sí</li> <li>• POST: No</li> <li>• PATCH: Sí</li> <li>• PUT: No</li> <li>• DELETE: No</li> </ul>	<ul style="list-style-type: none"> <li>• /vertex? projection=full: para recuperar toda la proyección</li> <li>• /vertex? projection=compact: para recuperar la proyección compacta</li> </ul>	<ul style="list-style-type: none"> <li>• Compatibilidad con ETC: No</li> <li>• Marca de tiempo: Sí</li> <li>• Filtrado: Sí</li> </ul>
/tenantId/apm/atc/api/vertex/{id}	Representa un agente.	<ul style="list-style-type: none"> <li>• GET: Sí</li> <li>• POST: No</li> <li>• PATCH: Sí</li> <li>• PUT: No</li> <li>• DELETE: No</li> </ul>	No	<ul style="list-style-type: none"> <li>• Compatibilidad con ETC: No</li> <li>• Marca de tiempo: Sí</li> <li>• Filtrado: No</li> </ul>
/tenantId/apm/atc/api/	Representa un agente.	<ul style="list-style-type: none"> <li>• GET: Sí</li> <li>• POST: No</li> <li>• PATCH: No</li> <li>• PUT: No</li> <li>• DELETE: No</li> </ul>	No	<ul style="list-style-type: none"> <li>• Compatibilidad con ETC: Sí</li> <li>• Marca de tiempo: No</li> <li>• Filtrado: No</li> </ul>
/tenantId/apm/atc/api/graph/vertex	Representa una recopilación de vértices	<ul style="list-style-type: none"> <li>• GET: Sí</li> <li>• POST: No</li> <li>• PATCH: Sí</li> <li>• PUT: No</li> <li>• DELETE: No</li> </ul>	<ul style="list-style-type: none"> <li>• /vertex? timestamp=1970-01-01T00:00:01Z: recupera la instantánea a partir de una fecha específica. El valor predeterminado es ahora.</li> <li>• /vertex? projection=full: para recuperar toda la proyección</li> <li>• /vertex? projection=compact: para recuperar la proyección compacta</li> <li>• /vertex: la carga específica una consulta.</li> </ul>	<ul style="list-style-type: none"> <li>• Compatibilidad con ETC: No</li> <li>• Marca de tiempo: Sí</li> <li>• Filtrado: Sí</li> </ul>

Resource	Descripción	Verbos de HTTP	Parámetros	Otros
/{{tenantId}}/apm/atc/api/graph/vertex/{id}	Representa un único vértice.	<ul style="list-style-type: none"> <li>GET: Sí</li> <li>POST: No</li> <li>PARCHE: Sí</li> <li>PUT: No</li> <li>DELETE: No</li> </ul>	/vertex? timestamp=1970-01-01T00:00:01Z: recupera la instantánea a partir de una fecha específica. El valor predeterminado es ahora.	<ul style="list-style-type: none"> <li>Compatibilidad con ETC: Sí</li> <li>Marca de tiempo: Sí</li> <li>Filtrado: No</li> </ul>
/{{tenantId}}/apm/atc/api/graph	Representa una gráfica con bordes y vértices	<ul style="list-style-type: none"> <li>GET: Sí</li> <li>POST: No</li> <li>PATCH: No</li> <li>PUT: No</li> <li>DELETE: No</li> </ul>	<ul style="list-style-type: none"> <li>GET /{{tenantId}}/apm/atc/api/graph: devuelve vértices, estados de vértice y bordes a partir de ahora</li> <li>Filtrado en formato json, igual que /graph/vertex.</li> <li>/graph?timestamp=1970-01-01T00:00:01Z: recupera la instantánea a partir de una fecha específica. El valor predeterminado es ahora. Devuelve un error para una fecha futura.</li> </ul>	<ul style="list-style-type: none"> <li>Compatibilidad con ETC: Sí</li> <li>Marca de tiempo: Sí</li> <li>Filtrado: Sí</li> </ul>
/{{tenantId}}/apm/atc/api/graph/incremental	Actualizaciones a vértices y bordes desde la última llamada	<ul style="list-style-type: none"> <li>GET: Sí</li> <li>POST: No</li> <li>PATCH: No</li> <li>PUT: No</li> <li>DELETE: No</li> </ul>	<ul style="list-style-type: none"> <li>GET /{{tenantId}}/apm/atc/api/graph/incremental?sinceVersion=0: esta llamada inicial devuelve vértices y bordes a partir de ahora. La respuesta incluye lastVersion para obtener actualizaciones incrementales.</li> <li>GET /{{tenantId}}/apm/atc/api/graph/incremental?sinceVersion=XXXVersion4 : devuelve todos los cambios incrementales desde XXXVersion4. La respuesta contiene información sobre los bordes y vértices actualizados y suprimidos.</li> </ul>	<ul style="list-style-type: none"> <li>Compatibilidad con ETC: Sí</li> <li>Marca de tiempo: No</li> <li>Filtrado: Sí</li> </ul>

Resource	Descripción	Verbos de HTTP	Parámetros	Otros
/{{tenantId}}/apm/atc/api/graph/vertexstatus/incremental	Instantánea y actualizaciones incrementales en los estados del vértice.	<ul style="list-style-type: none"> <li>GET: Sí</li> <li>POST: No</li> <li>PATCH: No</li> <li>PUT: No</li> <li>DELETE: No</li> </ul>	<ul style="list-style-type: none"> <li>GET /{{tenantId}}/apm/atc/api/vertexstatus/incremental?sinceVersion=0: esta llamada inicial devuelve todos los estados a partir de ahora. La respuesta incluye lastVersion para obtener actualizaciones incrementales.</li> <li>GET /{{tenantId}}/apm/atc/api/vertexstatus/incremental?sinceVersion=XXXVersion4 : devuelve todos los cambios incrementales desde la versión XXXVersion4. La respuesta contiene información sobre los estados actualizados.</li> </ul>	<ul style="list-style-type: none"> <li>Compatibilidad con ETC: Sí</li> <li>Marca de tiempo: No</li> <li>Filtrado: No</li> </ul>
/{{tenantId}}/apm/atc/api/apmData/query	Sirve como la interfaz de consulta real. Se pueden transferir consultas de SQL mediante las capacidades que devuelve la tabla de esquema.	<ul style="list-style-type: none"> <li>GET: No</li> <li>POST: Sí</li> <li>PATCH: No</li> <li>PUT: No</li> <li>DELETE: No</li> </ul>	<ul style="list-style-type: none"> <li>POST http://&lt;EM Host&gt;:8081/{{tenantId}}/apm/atc/api/apmData/query</li> <li>{"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"}: devuelve un recuento de las métricas agrupadas por host de agente.</li> </ul>	<ul style="list-style-type: none"> <li>Compatibilidad con ETC: Sí</li> <li>Marca de tiempo: Sí</li> <li>Filtrado: Sí</li> </ul>
/{{tenantId}}/apm/atc/api/apmData/schema	Describe todas las tablas virtuales conocidas que puede devolver la interfaz.	<ul style="list-style-type: none"> <li>GET: Sí</li> <li>POST: No</li> <li>PATCH: No</li> <li>PUT: No</li> <li>DELETE: No</li> </ul>	GET http://<EM_HOST>:8081/{{tenantId}}/apm/atc/api/apmData/schema : devuelve el esquema de la base de datos	<ul style="list-style-type: none"> <li>Compatibilidad con ETC: Sí</li> <li>Marca de tiempo: Sí</li> <li>Filtrado: Sí</li> </ul>

**Nota:** Los parámetros distinguen mayúsculas de minúsculas y deben estar en minúscula.

Filtrado admitido en la sintaxis de Lucene

- Es compatible con el filtrado en la sintaxis de Lucene. La descripción de la sintaxis completa está disponible en [https://lucene.apache.org/core/4\\_7\\_0/queryparser/org/apache/lucene/queryparser/classic/package-summary.html](https://lucene.apache.org/core/4_7_0/queryparser/org/apache/lucene/queryparser/classic/package-summary.html)

## Autenticación

Un token de seguridad es una cadena de texto generada aleatoriamente casi idéntica a una contraseña cifrada. Este token proporciona a la API acceso al servicio web de DX APM. Se pueden generar tantos tokens como sean obligatorios. Puede establecer una caducidad para un token y también revocar un token. Los tokens pueden revocarse en cualquier momento por parte de cualquier usuario. Los tokens son permanentes y nunca desaparecen de la lista que se encuentra en la ficha **Seguridad**.

### Siga estos pasos:

1. En la interfaz de usuario, seleccione **Configuración, Seguridad**.
2. Haga clic en el botón **Generar un token nuevo**.
3. Establezca la caducidad y agregue una etiqueta.
4. Seleccione **API pública** para el **Tipo**.
5. Haga clic en **Generar token**.

#### WARNING

Por razones de seguridad, no es posible mostrar un token más de una vez. Es el único momento en que el token aparece tras hacer clic en **Nuevo token**.

6. [Utilice el token en el encabezado de la autorización de la solicitud](#).

#### NOTE

##### Más información:

- [Autorización y autenticación de la API](#)
- [Mensajes y códigos de error de API generales](#)

## Configuration

#### NOTE

La configuración de la API de REST de DX APM solo está disponible en DX APM local.

## API de la aplicación

La API de la aplicación se documenta con OpenAPI versión 3. El documento de OpenAPI se puede descargar desde una instalación de APM. Se puede usar para generar clientes para varios idiomas o con algunos clientes HTTP/REST interactivos.

Siga los pasos que se mencionan a continuación para acceder al documento de OpenAPI 3 que describe la API pública del servidor de configuración de APM para la incorporación de aplicaciones y utilícela para generar clientes de tipo Java utilizando openapi-generator.

### Siga los pasos siguientes:

1. Descargue el documento actual de OpenAPI.
  - a. Inicie sesión como un usuario que puede acceder al servidor de configuración de APM.
  - b. Abra la dirección URL `https://<HOST>/acc/apm/acc/versioned.api.json` y descárguelo.

#### NOTE

En la dirección URL anterior, reemplace <HOST> con el nombre de host/nombre DNS real.

2. Cree un script para descargar y ejecutar `openapi-generator`. Este script es para el shell de Bash, pero se puede adaptar para ejecutarse en otros entornos. Colóquelo en un directorio nuevo y proporcione un nombre como, por ejemplo, `generate.sh`.

```
#!/bin/bash
```

```
if [! -f openapi-generator-cli*.jar]; then
```

```
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}')
```

- ```
package com.example;
```

```
import java.util.ArrayList;
import java.util.List;
import java.util.TreeMap;
```

```
defaultClient.setBearerToken("eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJURUU5BTlxQxIiwiaXNlbnRlbiJpbnVlLCJ0aWQiOiJpcCNYNHl7Jr5tSvs88jNycqTg10m5Ueao-nUHRnfvUBG2aLJV7Vt0ZRrfA");
```

500


```

        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(TierConfigurationItemPropertyValueTypes.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.addItemItem(itemsItem);
        System.out.println("Publishing the application.");
        applicationApi.publishApplication(createdApplication.getEntityId(), draftChangeListDto);

        System.out.println("Creation is complete.");
    }
}

```

NOTE

Este programa Java utilizará el cliente generado para crear una aplicación y se le debe agregar un nivel que describa el Agente de la infraestructura para Linux configurado para monitorizar PostgreSQL.

5. Obtenga un token de la API en la interfaz de usuario de ATC de APM. Vaya a **Configuración > Seguridad > Generar un token nuevo**. Seleccione el tipo como "API pública".
6. Actualice la llamada al método `setBearerToken` con un token válido en el origen de la clase `ClientTestTool`.
7. Compile y ejecute la clase `ClientTestTool`.
 - a. Puede hacerlo a través de cualquier IDE que admita Java y Maven.
 - b. Puede hacerlo a través de Java y Maven directamente en la línea de comandos.
 - a. Compile con el comando `mvn clean install` en el directorio `spring-openapi-generator-api-client`.
 - b. Ejecute con `mvn exec:exec -Dexec.executable=java -Dexec.args="-cp %classpath com.example.ClientTestTool"`.
8. El resultado debe ser una nueva aplicación con un nivel que defina el monitor de infraestructura de PostgreSQL para Linux.

NOTE

Si desea utilizar el documento de OpenAPI para generar un cliente con un modelo con tipo con otros lenguajes o marcos de destino, asegúrese de que las propiedades del objeto JSON desconocidas se ignoren en la deserialización y de que el cliente envíe correctamente los encabezados `Accept` y `Content-Type` de acuerdo con el documento de OpenAPI para lograr la compatibilidad con futuras versiones de APM.

Solución de problemas

| Síntoma | Solución |
|--|---|
| Para la instalación local de APM, se puede producir un error en el cliente con la excepción <code>javax.net.ssl.SSLHandshakeException</code> cuando APM se configura con un certificado HTTPS autofirmado o firmado por una autoridad de certificación no conocida públicamente. | Necesita un almacén de confianza con un certificado correspondiente a lo que se usa en el servidor para conectar el cliente. Por ejemplo, se utilizará un almacén de confianza llamado <code>trust.jks</code> (en el directorio <code>spring-openapi-generator-api-client</code>):

<pre>mvn exec:exec -Dexec.executable=java -Dexec.args="-cp %classpath -Djavax.net.ssl.trustStore=trust.jks -Djavax.net.ssl.trustStorePassword=changeit com.example.ClientTestTool"</pre> |

Regla de atributo

Las directrices para los métodos `Post` y `PutUse` las siguientes directrices para crear (`POST`) y actualizar (`PUT`) reglas de atributo.

Las siguientes directrices y métodos están disponibles para este recurso:

- Directrices para los métodos Post y Put
- Métodos

Directrices para los métodos Post y Put

Utilice las directrices siguientes para crear (POST) y actualizar (PUT) reglas de atributo.

Campos de carga útil

Los campos obligatorios para todas las solicitudes de carga útil son los siguientes:

| | | | | | |
|-------|--------------|------------|-------------|----------|---------|
| layer | existingName | customName | customValue | operator | operand |
|-------|--------------|------------|-------------|----------|---------|

Field Values

Operator

Los valores permitidos para el campo `operator` son los siguientes:

Nota: Los valores que terminan con `_CI` no distinguen entre mayúsculas y 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 |

Nota: Si el valor de `operator` es igual a `IS_EMPTY` o `IS_NOT_EMPTY`, `operator` debe ser una cadena vacía:

```
"operator": "IS_NOT_EMPTY",
"operand": "",
```

Layer

Los valores permitidos para el campo `layer` son los siguientes:

| | | |
|-----|--------------------|----------------|
| ATC | APM_INFRASTRUCTURE | INFRASTRUCTURE |
|-----|--------------------|----------------|

UniverseId

Si se proporciona un valor nulo para el campo `UniverseId` o no se especifica el campo `UniverseId`, la regla de atributo se crea en el universo Empresa. Si la regla de atributo ya existe, la regla de atributo se transfiere al universo Empresa.

Enabled

Si no se especifica el campo `enabled`, el valor se establece como falso de forma predeterminada. Este valor falso desactiva la visibilidad de la regla de atributo en la interfaz gráfica de usuario.

Id y _links

Los campos `id` y `_links` son de solo lectura. Si se proporcionan valores para estos campos, los valores se ignorarán.

outputclass="bc-h2" id="Methods">Methods

Métodos

GET /{tenantId}/apm/atc/api/attribute/rule

Este método devuelve la lista de reglas de atributo para todos los universos a los que tiene acceso un usuario.

```

{
  "_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}

Este método utiliza un ID de regla de atributo para devolver una única regla 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

Este método crea una regla de atributo. A continuación se muestra un ejemplo de la carga útil de la solicitud:

```

{
  "existingName": "agent",
  "operator": "IS_NOT_EMPTY",
  "operand": "",
  "customName": "aaaa",
  "customValue": "aaaa",
  "universeId": null,
  "layer": "APM_INFRASTRUCTURE",
  "enabled": false
}

```

A continuación se muestra un ejemplo de la respuesta:

```

{
  "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}

Este método utiliza un ID de regla de atributo para actualizar la regla de atributo que coincide con el ID especificado. A continuación se muestra un ejemplo de la carga útil de la solicitud:

```

{
  "existingName": "agent",
  "operator": "CONTAINS",
  "operand": "name",
  "customName": "sample",
  "customValue": "2144",
  "universeId": null,
}

```

```

"layer": "ATC",
"enabled": true
}

```

A continuación se muestra un ejemplo de la respuesta:

```

{
  "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}

Este método utiliza un ID de regla de atributo para suprimir la regla de atributo que coincide con el ID especificado.

Gráfica

Este recurso devuelve una gráfica completa que incluye vértices, estados de vértices y bordes según la marca de tiempo y los criterios de filtrado especificados. Puede utilizar sus propios scripts o una biblioteca de terceros para atravesar la gráfica y extraer la información que necesite. Por ejemplo, vértices ascendentes, vértices descendentes, ruta más corta entre dos vértices.

- Une gráficos a través de todos los universos a los que tiene acceso.
- Si ETC gestiona varios clústeres, el punto final combina vértices entre clústeres.
- Permite las consultas históricas a partir de la marca de tiempo. Los atributos, alertas y otros campos tienen historial. La marca de tiempo predeterminada es ahora.

Se puede invocar este punto final de dos maneras:

1. Con un formulario GET sencillo si no se necesita un filtro.
2. GET /{tenantId}/apm/atc/api/graph?timestamp=2016-01-01T00:00:01Z
3. La opción POST es útil si necesita un filtro. A continuación, se envía la condición de filtro como carga POST. Para obtener más información sobre filtros, consulte [Vértice del 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 del gráfico

Este recurso devuelve la lista de vértices según los criterios de filtro y la proyección especificados.

- Permite las consultas históricas a partir de la marca de tiempo. Los atributos, alertas y otros campos tienen historial. La marca de tiempo predeterminada es ahora.
- Es compatible con las proyecciones estáticas: "completas" y "compactas". El valor predeterminado es "compacto".

Se puede invocar este punto final de dos maneras:

1. Con un formulario GET más sencillo si no se utiliza un filtro.
GET `/{{tenantId}}/apm/atc/api/graph/vertex?timestamp=2016-01-01T00:00:01Z&projection=full`
2. La opción POST es útil si se utiliza el filtro: la condición de filtro se envía después como 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"
        }
      ]
    }
  ]
}
```

Capacidades y formato de filtro

1. Operaciones compatibles: IN, NOT_IN, MATCHES, NOT_MATCHES
2. IN: coincidencia exacta

```
// 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: no es igual a.

```
// 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: coincidencia de carácter comodín que utiliza '*'. Un asterisco (*) en el patrón puede coincidir con cero o más caracteres en el 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: el carácter comodín no coincide.

```

// 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 ]
    }
]
}
]
}

```

EL filtro puede combinar más de una condición de filtrado:

```

{
    "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 "attributeName", el filtro es compatible con:

- Nombres de atributo de vértice válidos: por ejemplo, "agente" o "nombre de host"
- "serviceld": para filtrar por "Servicio empresarial," igual puesto que es visible en la interfaz de usuario
- "transactionId: para filtrar por "Transacción comercial," igual puesto que es visible en la interfaz de usuario

Proyecciones

Compacta (valor predeterminado)

```

?{
  "_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"
  }
}
}
}

```

Parche

Actualiza los valores del atributo para un vértice seleccionado.

- Los nombres del atributo deben ser únicos. Los atributos duplicados se descartarán.
- El valor nulo suprime el atributo.
- Si existe un atributo para un determinado vértice, entonces se actualizará; de lo contrario, el parche crea un atributo personalizado.
- Los atributos CUSTOM pueden crearse, actualizarse o suprimirse. Si el parche crea un atributo, siempre es personalizado.
- Se pueden actualizar los atributos personalizados creados por reglas de atributos.
- Los atributos básicos no se pueden actualizar o suprimir.

Ejemplo de la carga de la solicitud:

```

?{ "items" : [
  {
    "id":"Enterprise Team Center:8",
    "attributes": {
      "Attr1":["newValue", "newValue2"],
      "Attr2": null
    }
  },
  {...},
  {...}
]
}

```

Gráfico incremental

Devuelve las actualizaciones incrementales a la estructura del gráfico. Cada respuesta contiene **lastVersion** que se utilizará para la llamada siguiente.

- Une gráficos a través de todos los universos a los que tiene acceso.
- La respuesta no contiene todas las actualizaciones. Si hay más de una actualización con el mismo vértice/borde, solo se notifica la última actualización efectiva.
- En una configuración de varios clústeres, realice una correlación a través de los clústeres del consumidor; consulte el ejemplo.

GET /{tenantId}/apm/atc/api/graph/incremental?sinceVersion=0

Esta llamada inicial devuelve vértices y bordes a partir de ahora. La respuesta incluye **lastVersion** para obtener las actualizaciones incrementales. Los resultados de la memoria caché del consumidor como instantánea 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"
    },
  },
}
```

GET /{tenantId}/apm/atc/api/graph/incremental?sinceVersion=XXXXYYYYZZZZZ

La respuesta contiene información sobre los vértices nuevos/modificados y eliminados, bordes nuevos/modificados y bordes eliminados. Aplique la respuesta a la instantánea. Se guarda en la memoria caché del cliente. Consulte el ejemplo.

518

[illegible]

Id del vértice del gráfico

Representa un solo 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"
}

```

Parche

Actualiza los valores del atributo para un vértice seleccionado.

- Los nombres del atributo deben ser únicos. Los atributos duplicados se descartarán.
- El valor nulo suprime el atributo
- Si existe un atributo para un determinado vértice, entonces se actualizará; de lo contrario, el parche crea un atributo personalizado.
- Los atributos CUSTOM pueden crearse, actualizarse o suprimirse. Si el parche crea un atributo, siempre es personalizado.
- Se pueden actualizar los atributos personalizados creados por reglas de atributos.
- Los atributos básicos no se pueden actualizar o suprimir.

Ejemplo de la carga de la solicitud:

```

{
  "attributes": {
    "Attr1": ["newValue3", "newVal3"],
    "Attr2": null
  }
}

```

Gráfico Vertexstatus incremental

Devuelve las actualizaciones incrementales a los estados del vértice. Cada respuesta contiene **lastVersion** que se utilizará para la llamada siguiente.

- Une los estados del vértice en todos los universos a los que un usuario tiene acceso
- La respuesta no contiene todas las actualizaciones. Si hay más de una actualización para el mismo estado, se notifica solamente la última actualización efectiva.

GET /{tenantId}/apm/atc/api/graph/vertexstatus/incremental?sinceVersion=0

Esta llamada inicial devuelve todos los estados a partir de ahora. La respuesta incluye **lastVersion** para obtener las actualizaciones incrementales. Esta llamada se guarda en la memoria caché del cliente como una instantánea inicial.

[illegible]

GET /{tenantId}/apm/atc/api/graph/incremental?sinceVersion=XXXXYYYYZZZZZ

Devuelve los cambios incrementales desde la última llamada. La última llamada se identifica mediante el campo **lastVersion** en la respuesta.

La respuesta contiene información sobre los vértices nuevos/modificados y eliminados, bordes nuevos/modificados y bordes eliminados. Aplique esta respuesta a la instantánea. Se guarda en la memoria caché del cliente. Consulte este ejemplo:

```
{
  "_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
    ]
  }
}
```

NOTE

- Repita las llamadas para obtener actualizaciones incrementales tan a menudo como sea necesario. Cada vez que se llame se realizarán todos los cambios sin fijaciones ni paginaciones. Las cargas muy grandes se gestionan a través de una respuesta de transmisión JSON en lugar de mantenerse en la memoria.
- En cualquier momento se puede obtener una nueva instantánea de datos. Utilice **GET /{tenantId}/apm/atc/api/graph/incremental?sinceVersion=0**. Por ejemplo, puede utilizarse esta llamada si se reinicia la aplicación. Esta llamada proporciona una nueva lastVersion para obtener actualizaciones incrementales.

Devuelve la lista de opciones disponibles para la API junto con información general acerca de la API en cuestión. Se puede acceder públicamente al recurso desde SSL sin necesidad de un token de autorización. El recurso raíz sirve como punto de partida para explorar la API, ya que vincula todas las rutas disponibles que son accesibles. El vínculo a un recurso puede ser una plantilla URI. En ese caso, el recurso contiene una propiedad `templated:true`. Si la propiedad no está presente o si su valor es diferente, el recurso contiene un URI simple.

Ejemplo de respuesta:

```

{
  "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
      }
    ]
  }
}

```

Propiedades del recurso:

| Nombre de la propiedad | Type | Descripción | Versión de la API |
|-------------------------------|-------------|---|-------------------|
| serviceProvider | Cadena | Describe el proveedor del servicio: com.ca.apm.appmap. | 1.0.0 |
| serverVersion | Cadena | La versión del servidor que proporciona la API (versión de APM). | 1.0.0 |
| apiVersion | Cadena | La versión de la API. | 1.0.0 |
| vendor | Cadena | Distribuidor del servicio - Broadcom | 1.0.0 |
| _links | Matriz | Enumera todas las opciones disponibles para esta API. | 1.0.0 |
| _links.self | Vínculo HAL | Contiene la dirección URL para el recurso raíz. | 1.0.0 |
| _links.doc | Vínculo HAL | Contiene la dirección URL a la documentación de la API pública. | 1.0.0 |
| _links.* Por ejemplo, vertex. | Vínculo HAL | Muestra todos los puntos finales disponibles para un recurso determinado. | 1.0.0 |

Universo

Este recurso devuelve las propiedades básicas de los universos individuales o de todos los universos a los que tiene acceso un usuario.

Este recurso devuelve las propiedades básicas de los universos individuales o de todos los universos a los que tiene acceso un usuario.

Se puede invocar este punto final de dos maneras:

- **GET /{tenantId}/apm/atc/api/universe**

Devuelve una lista de los universos a los que tiene acceso un usuario.

```
{
  "_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}**

Devuelve las propiedades del universo individual que coincide con el ID del universo especificado.

```
{
  "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

Devuelve la lista de vértices según los criterios de filtro y la proyección especificados.

- Permite las consultas históricas a partir de la marca de tiempo. Los atributos, alertas y otros campos tienen historial. La marca de tiempo predeterminada es ahora.
- Es compatible con las proyecciones estáticas: "completas" y "compactas". El valor predeterminado es "compacto".

Verbos compatibles: GET, PATCH

Parámetros compatibles: projection, timestamp, q

GET

Filtrado admitido de la recopilación

Por marca de tiempo para recuperar una instantánea de la recopilación a partir de la marca de tiempo. El valor predeterminado es ahora.

- GET /{tenantId}/apm/atc/api/vertex?timestamp:1970-01-01T00:00:01Z
- Es compatible con el filtrado en la sintaxis de Lucene. La descripción de la sintaxis completa está disponible en https://lucene.apache.org/core/4_7_0/queryparser/org/apache/lucene/queryparser/classic/package-summary.html

Ejemplos de filtrado:

- GET /{tenantId}/apm/atc/api/vertex?q=city:Paris AND sky:blue se pueden combinar expresiones de filtrado mediante operadores lógicos
- GET /{tenantId}/apm/atc/api/vertex?q=(city:Paris AND sky:blue) OR (city:London AND sky:grey) agrupación de expresiones lógicas usando llaves
- GET /{tenantId}/apm/atc/api/vertex?q=sky\ color:deep\ bluespaces y otros caracteres especiales se deben escapar

/vertex/ admite proyecciones compactas y completas, el valor predeterminado es una proyección 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

Actualiza los valores del atributo para un vértice seleccionado.

- Los nombres del atributo deben ser únicos. Los atributos duplicados se descartarán.
- Si existe un atributo para un determinado vértice, se actualizará. De lo contrario, PATCH crea un atributo CUSTOM con un nombre determinado.
- Los atributos CUSTOM pueden crearse, actualizarse o suprimirse. Los atributos que se crean mediante PATCH son siempre CUSTOM.
- Se pueden actualizar los atributos DECORATED. Si se actualizan, se convierten en CUSTOM.
- Los atributos recopilados no se pueden actualizar ni suprimir.

Ejemplo de la carga de la solicitud:

- Los nombres del atributo proporcionados deben ser únicos. PATCH ignora cualquier atributo duplicado.

```
[{
  "id": "3",
  "attributes": {
    "Attr1": "newValue",
    "Attr2": null // NULL deletes attribute
  }
},
...]
```

Parámetros admitidos

| Nombre de la propiedad | Type | Descripción |
|------------------------|--------|--|
| vértice | matriz | matriz de vértices - depende de la proyección. |

ID del vértice

El recurso devuelve información detallada para un solo vértice.

La estructura de retorno es igual que en GET /vertex,

Verbos compatibles: todos

Parámetros compatibles: 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> }
  }
}
```

Parámetros HTTP adicionales

- timestamp: recupera una instantánea del recurso a partir de la marca de tiempo. El valor predeterminado es ahora.
GET /{tenantId}/apm/atc/api/vertex/123?timestamp=1970-01-01T00:00:01Z

PATCH

Actualiza los valores del atributo para un vértice seleccionado.

- Los nombres del atributo deben ser únicos. Los atributos duplicados se descartarán.
- Si existe un atributo para un determinado vértice, entonces se actualizará; de lo contrario, el parche crea un atributo personalizado con un nombre determinado.
- Los atributos CUSTOM pueden crearse, actualizarse o suprimirse. Los atributos que se crean mediante PATCH son siempre personalizados.
- Se pueden actualizar los atributos DECORATED. Si se actualizan, se convierten en CUSTOM.
- Los atributos recopilados no se pueden actualizar o suprimir.

Ejemplo de la carga de la solicitud:

- Los nombres del atributo proporcionados deben ser únicos. PATCH ignora cualquier atributo duplicado.

```
{
  "attributes": {
    "Attr1": "newValue",
    "Attr2": null // NULL deletes attribute
  }
}
```

Parámetros admitidos

| Nombre de la propiedad | Type | Descripción |
|------------------------|----------------------------|---|
| id | Matriz de una única cadena | El ID del vértice |
| Marca de tiempo | Timestamp | <i>Marca de tiempo de la instantánea proporcionada en el formato 1970-01-01T00:00:01Z</i> |
| attributes | Matriz | Lista de todos los atributos definidos en el vértice |
| attributes.name | Cadena | Nombre del atributo |
| attributes.value | Cadena | Valor del atributo |
| attributes.type | Cadena | Tipo de atributo. Los tipos admitidos actualmente son "Personalizado", "Representativo" y "Recopilado". |

Ejemplo de Java de la API de REST para obtener actualizaciones incrementales

El siguiente ejemplo muestra cómo utilizar la API de REST pública para obtener actualizaciones incrementales.

```
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 de REST de SQL

Utilice la API de REST de SQL pública para extraer datos de métrica sin formato de APM e integre estos datos con herramientas personalizadas. Como otras API de REST de APM, la interfaz de la API de REST de SQL utiliza la autenticación basada en tokens. Esta API de REST se ejecuta en los siguientes modos de Enterprise Manager (EM):

- Independiente
- recopilador
- Manager of Managers (MOM)
- Enterprise Team Center

NOTE

- La función API de REST de SQL se ha introducido en 10.7 Service Pack 1 (SP1).
- Esta función no proporciona todas las capacidades de SQL como, por ejemplo, uniones y subselecciones.

IMPORTANT

Utilice *solamente* la API de REST de SQL pública para extraer datos de métricas de APM. Para extraer datos de métricas de APM o que no sean de APM, utilice la [API de REST de consulta de métrica](#).

Conexión a la API de REST de SQL

Siga estos pasos:

1. Inicie sesión en Team Center y haga clic en **Seguridad**.
2. Haga clic en **Generar un token nuevo**.
Aparecerá un cuadro de diálogo.
3. Especifique la **Etiqueta** (nombre) y seleccione **API pública** para el **Tipo**.
4. Establezca la fecha de caducidad o seleccione **Nunca caduca**.
5. Haga clic en **Generar token**.
El sistema genera un nuevo token.

WARNING

Por razones de seguridad, solo verá un token una vez. Guarde el token en un lugar seguro antes de cerrar este cuadro de diálogo. No revele nunca el token a personal no autorizado.

El token ahora aparece entre los otros tokens en la ficha **Seguridad**.

6. Pruebe la conexión con una consulta de muestra como, por ejemplo:

```
URL
    http://<EM Host>:8081/{tenantId}/apm/atc/api/apmData/schema
GET
Header
    Accept: application/json
    Authorization: Bearer <Security Token>
```

Se ha conectado a la API de REST.

Métricas de compatibilidad

Las métricas de compatibilidad de la API de REST de SQL tienen el prefijo `Enterprise Manager|Data Store|SQL API` en sus nombres. La siguiente tabla enumera las métricas de compatibilidad disponibles:

| Nombre de la métrica de compatibilidad | Descripción |
|--|---|
| Tiempo medio de respuesta (ms) | Tiempo medio para procesar la consulta entrante |
| Bytes Sent Per Interval | Número de bytes enviados como resultado en un intervalo |
| Responses Per Interval | Consultas correctas realizadas en un intervalo |
| Invocaciones simultáneas | Número de conexiones en paralelo realizadas a un punto final de la consulta |
| Clamped Connections Per Interval | Número de conexiones rechazadas debido al límite de la fijación |
| Errores por intervalo | Número de conexiones erróneas realizadas en un intervalo |

Recursos de la API de REST

La API de REST de SQL contiene los siguientes recursos:

```
{tenantId}/apm/atc/api/apmData/schema
```

Describe todas las tablas virtuales conocidas que puede devolver la interfaz.

```
{tenantId}/apm/atc/api/apmData/query
```

Sirve como la interfaz de consulta real. Se pueden transferir consultas de SQL mediante las capacidades que devuelve la tabla de esquema.

Se pueden definir consultas utilizando las funciones count, minimum, maximum y average. La siguiente función aggregate solo se admite en la columna agg_value de la tabla metric_data: sum; apm_average; apm_aggregate. La función aggregate da como resultado lo siguiente:

- La función sum aggregate proporciona la suma de los valores de la columna agg_values
- apm_aggregate proporciona la suma o el promedio ponderado en función de las métricas consultadas
- apm_average solo proporciona el promedio ponderado

Ejemplos de consulta

Utilice los siguientes ejemplos para realizar una consulta a la API:

- Ejemplo 1: **Obtención del recuento de métricas agrupadas por el host del agente**

Este ejemplo utiliza una solicitud POST en el 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"}
```

Ejemplo 2: Obtención del esquema

Este ejemplo utiliza una solicitud GET en el 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"
        ]
    }
]
}
}}

```

• Ejemplo 3: Obtención de datos de la métrica con una cláusula where

Este ejemplo utiliza una solicitud POST en el 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 ]
]
```

- **Ejemplo 4: Obtención de datos de métricas con una función aggregate**

Este ejemplo utiliza una solicitud POST en el 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
    ]
  ]
}
```

Ejemplos de consulta URL

Utilice los siguientes ejemplos para realizar una consulta a la API en cURL:

- **Ejemplo 1: Obtención del 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
```

- **Ejemplo 2: Obtención de un esquema en lenguaje natural sin capacidades 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
```

- **Ejemplo 3: Obtención de todas las fuentes**

```
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" ]
] }
```

- **Ejemplo 4: Obtención de todas las métricas para los agentes con caracteres específicos introducidos en la columna 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]

,...

```

- **Ejemplo 5: Obtención del recuento 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]
]]
```

- **Ejemplo 6: Obtención de todos los datos de la métrica durante la última hora**

NOTE

Esta consulta devuelve un archivo JSON grande. Ejecútela con precaución.

```
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}\" }"
```

- **Ejemplo 7: Obtención del máximo valor agrupado por ruta de métrica a partir de datos de la métrica para todos los promedios de métricas (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]
```

• Ejemplo 8: Obtención de la utilización media de la CPU para los 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 ]
  ]
}
```

- **Ejemplo 9: Obtención del recuento máximo de métricas para los recopiladores**

```
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 de REST de Team Center

Utiliza la API de REST de Team Center para proporcionar diversas funciones de consulta de datos, tanto de métricas como de nivel de cuadro de mandos de Team Center. Como otras API de REST de APM, la interfaz de la API de REST de Team Center utiliza la autenticación basada en tokens. Para obtener más información sobre cómo obtener el token, consulte [Generación de un token de seguridad](#).

La API de REST de Team Center contiene los siguientes recursos:

| Resource | Descripción | Ejemplo |
|---|---|---------------------------------|
| /atc/private/apmData/query | Obtiene los datos de métricas mediante la consulta de sintaxis SQL estándar en la carga. | POST /atc/private/apmData/query |
| /atc/private/apmData/schema | Obtiene las capacidades de esquema de SQL (es decir, tablas compatibles, detalles de las columnas) que se pueden utilizar en la consulta SQL de REST. | GET /atc/private/apmData/schema |

IMPORTANT

Utilice *solamente* la [API de REST de SQL](#) pública para extraer datos de métricas de APM. Para extraer datos de métricas de APM o que no sean de APM, utilice la [API de REST de consulta de métrica](#).

Recursos de la API de REST de Team Center

Se pueden definir consultas utilizando las funciones count, minimum, maximum y average. Las siguientes funciones aggregate solo se admiten en la columna agg_value de la tabla metric_data: sum; apm_average; apm_aggregate.

La función aggregate da como resultado lo siguiente:

- La función sum aggregate proporciona la suma de los valores de la columna agg_values
- apm_aggregate proporciona la suma o el promedio ponderado en función de las métricas consultadas
- apm_average solo proporciona el promedio ponderado

La API de REST de Team Center contiene los siguientes recursos:

Recurso 1:

```
/atc/private/apmData/query
```

Obtiene los datos de métricas mediante la consulta de sintaxis SQL estándar en la carga.

Ejemplo: POST /atc/private/apmData/query

Carga:

```
{ "query": <SQLQuery(string)> //sql query string} // Example:{ "query": "select * from metric_data where ts >= 1572518520000 and ts <= 1572518535000"}
```

Respuesta:

```
{
  "columns": [ // The columns specified in the query or all the columns(*) of the table as per the schema
    {
      "name": "source_name",
      // Source name of the metric, empty as it is no longer valid
      "type": "string"
    },
    {
      "name": "agent_host",
      // Host name of the agent
      "type": "string"
    }
  ]
}
```

```

// Indicates the type of column value
},
{
    "name": "agent_process",
    // Process name
    "type": "string"
},
{
    "name": "agent_name",
    // Agent name of the metric
    "type": "string"
},
{
    "name": "domain_name",
    // Domain name of the metric
    "type": "string"
},
{
    "name": "metric_path",
    // Metric path containing folder name and metric attribute
    "type": "string"
},
{
    "name": "metric_attribute",
    // Attribute name of the metric
    "type": "string"
},
{
    "name": "attribute_type",
    // Integer that defines type of metric
    "type": "long"
},
{
    "name": "frequency",
    // Width of interval in number of seconds
    "type": "long"
},
{
    "name": "ts",
    // Denotes timestamp of the metric
    "type": "timestamp"
},
{
    "name": "min_value",
    // min value of the metric
    "type": "long"
},
{
    "name": "max_value",
    // max value of the metric
    "type": "long"
},
{

```



```

        "name": "value_count",
        // Count of metric occurrences
        "type": "long"
    },
    {
        "name": "agg_value",
        // aggregate value of the metric
        "type": "long"
    }
],
"rows": [
    [
        <empty(string)>,
        <agent_host(string)>,
        <agent_process(string)>,
        <agent_name(string)>,
        <domain_name(string)>,
        <metric_path(string)>,
        <metric_attribute(string)>,
        <attribute_type(long)>,
        <frequency(long)>,
        <first_ts_value(timestamp)>,
        <min_value(long)>,
        <max_value(long)>,
        <value_count>,
        <agg_value(long)>
    ]
    //next row
]]// Example:{
"columns": [
    {
        "name": "source_name",
        "type": "string"
    },
    {
        "name": "agent_host",
        "type": "string"
    },
    {
        "name": "agent_process",
        "type": "string"
    },
    {
        "name": "agent_name",
        "type": "string"
    },
    {
        "name": "domain_name",
        "type": "string"
    },
    {
        "name": "metric_path",
        "type": "string"
    }
]

```

```

    },
    {
      "name": "metric_attribute",
      "type": "string"
    },
    {
      "name": "attribute_type",
      "type": "long"
    },
    {
      "name": "frequency",
      "type": "long"
    },
    {
      "name": "ts",
      "type": "timestamp"
    },
    {
      "name": "min_value",
      "type": "long"
    },
    {
      "name": "max_value",
      "type": "long"
    },
    {
      "name": "value_count",
      "type": "long"
    },
    {
      "name": "agg_value",
      "type": "long"
    }
  ],
  "rows": [
    [
      "",
      "brtlvltsl719sl",
      "WebLogic",
      "WLP_LOGIN_MOBILE_PROD/WLP_LOGIN_MOBILE_PROD_Cluster/WLP_LOGIN_MOBILE_PROD_Srv23",
      "SuperDomain",
      "WebServices|Client|http_//www.gvt.com.br/CustomerManagement/CustomerInformationManagement/
CustomerProfileManagement:SOAP Faults Per Interval",
      "SOAP Faults Per Interval",
      8194,
      15000,
      1572518520000,
      0,
      0,
      0,
      0
    ]
  ]

```

```

        "",
        "brtlvltsl719sl",
        "WebLogic",
        "WLP_LOGIN_MOBILE_PROD/WLP_LOGIN_MOBILE_PROD_Cluster/WLP_LOGIN_MOBILE_PROD_Srv23",
        "SuperDomain",
        "WebServices|Client|http_//www.gvt.com.br/CustomerManagement/CustomerInformationManagement/
CustomerProfileManagement:SOAP Faults Per Interval",
        "SOAP Faults Per Interval",
        8194,
        15000,
        1572518535000,
        0,
        0,
        0,
        0
    ]
}

```

Recurso 2:

/atc/private/apmData/schema

Obtiene las capacidades de esquema de SQL (es decir, tablas compatibles, detalles de las columnas) que se pueden utilizar en la [consulta SQL](#) de REST.

Ejemplo: GET /atc/private/apmData/schema

Respuesta:

```

{
  "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",

```

La API de REST de consulta de métrica utiliza la API de consulta de métrica para consultar las métricas para diferentes intervalos de tiempo, frecuencias y métricas. Al igual que otras API de REST de APM, la interfaz de la API de REST de consulta de métrica utiliza la autenticación basada en token. Para obtener más información sobre cómo obtener el token, consulte [Generación de un token de seguridad](#).

| Resource | Descripción | Ejemplo |
|----------------------|--|---------------------------|
| /metrics/queryMetric | Ejecute una consulta para métricas y recupere los valores de la métrica en función de los criterios de consulta especificados y el intervalo de tiempo. <QuerySpecifier> puede ser cualquier combinación de especificadores de consulta. | POST /metrics/queryMetric |

Se puede utilizar la API de REST de consulta de métrica para generar datos de métrica de APM o que no sean de APM. La API de REST de SQL pública también se puede utilizar para generar datos de métrica de APM.

Para obtener más información sobre la generación de datos de métrica de APM mediante la API de REST de SQL pública, consulte [API de REST de SQL](#).

Ejemplo: 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
}
```

Respuesta:

```
{
  "metrics": [{
    "id": <MetricId(string)>,
    "source": <SourceName(string)>,
    "attribute": <AttributeName(string)>,
    "attributes": <Attributes_Optional(NameValue Pairs - strings)>,
    "type": <type(32bit Integer)>,
    "values": [
      [<time(unixTimestamp/seconds)>, <interval/seconds>, <min>, <max>, <value>, <count>]
      // next data point
    ]
  }]
}
```

```

    // next metric
  ]
}

// Example:
{
  "metrics": [
    {
      "id": "0P-BAB-B-jt9BQG",
      "source": "SuperDomain|Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)",
      "attribute": "Enterprise Manager:Overall Capacity (%)",
      "attributes" : { // attributes are optional
        "attribName1" : "attribValue1",
        "hostname" : "test.broadcom.com"
      },
      "type":2050,
      "values": [
        [1518521415, 15, 2, 4, 3, 4],
        [1518521430, 15, 2, 3, 3, 4],
        [1518521445, 15, 3, 4, 3, 4],
        [1518521460, 15, 2, 5, 3, 4],
        [1518521475, 15, 2, 3, 3, 4],
        [1518521490, 15, 86, 86, 86, 1],
        [1518521505, 15, 5, 19, 11, 4],
        [1518521520, 15, 4, 51, 17, 5],
        [1518521535, 15, 3, 11, 7, 4]]
      ]
    }
  ]
}

```

Agregaciones compatibles

La API es compatible con los siguientes especificadores de agregación:

- Direct MetricSpecifier
- Bucket MetricSpecifier

Direct MetricSpecifier

TopK: obtenga las primeras X de peor rendimiento en el que los ejemplos de X en APM sean direcciones URL, back-end, front-end, etc.

Ejemplos:

1. Obtener las dos primeras direcciones URL de peor rendimiento
2. Obtener las dos primeras JVM que consumen más memoria

Ejemplo: POST /metrics/queryMetric

Carga: las dos primeras direcciones URL de peor rendimiento según el tiempo de respuesta medio (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
      }
    }
  ]
}

```

Respuesta:

```

{
  "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: obtenga la última X de peor rendimiento en la que los ejemplos de X en APM sean direcciones URL, back-end, front-end, etc.

Carga: las dos últimas direcciones URL de peor rendimiento según el tiempo de respuesta medio (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
      }
    }
  ]
}

```

Respuesta:

```

{
  "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,
      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
    ]
]
}
]
}
}

```

Bucket MetricSpecifier

Agrupe X en Y y obtenga la primera N de Y. Por ejemplo: obtenga las 10 primeras máquinas virtuales Java que atiendan el número máximo de solicitudes, donde la solicitud máxima es la suma de respuestas de todos los puntos de entrada.

Ejemplo: POST /metrics/queryMetric

Carga: los dos primeros JVM en función del número de solicitudes servidas (agrupar front-end en JVM y obtener los 10 primeros de JVM)

```

{
  "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 compatibles para la operación de depósito:

| Operation(OP) | Valor |
|-----------------------|--|
| BUCKET_ATTRIBUTE | <Custom AttributeName> |
| BUCKET_SOURCE | <ul style="list-style-type: none"> hostname domain Process agent |
| BUCKET_ATTRIBUTE_NAME | <ul style="list-style-type: none"> metricpath metricname |

Respuesta:

```

{
  "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
        ]
    ]
}
]
}
}

```

Uso de direcciones URL públicas cortas en DX APM

DX APM proporciona direcciones URL públicas cortas para evitar que las direcciones URL largas se corten y para facilitar su uso. Se pueden utilizar estas direcciones URL para enviar a otros usuarios directamente a los diseños preconfigurados en DX APM. Se pueden proporcionar las direcciones URL cortas a los otros usuarios para la vista de mapa y la vista de métrica. Además, también se pueden utilizar las direcciones URL públicas cortas en las alertas y las notificaciones por correo electrónico.

NOTE

Los usuarios no pueden acceder a estos vínculos sin un nombre de usuario y una contraseña para DX APM.

Los parámetros para la dirección URL completa pueden cambiar a lo largo del tiempo. Se pueden utilizar los siguientes parámetros para asignar las direcciones URL públicas.

Para obtener información sobre los parámetros para las API, consulte [Referencia de la API](#).

Rutas

La tabla siguiente muestra cómo se asignan las rutas públicas a las rutas internas.

| Ruta pública | DX APM Ruta interna de |
|-----------------|------------------------|
| /public/vertex | /map |
| /public/alerts | /alert |
| /public/metrics | /metrics |

Parámetros

Utilice los siguientes parámetros públicos para designar valores específicos.

| Ruta | Parámetro público | Obligatorio | Valor | Valor predeterminado |
|-----------------|-------------------|-------------|---|--|
| /public/vertex | id | Sí | ID del vértice | |
| | endTime | No | Hora de finalización en milisegundos | Modo en directo si no se ha especificado ningún valor para endTime |
| | intervalo | No | Intervalo en milisegundos | 480000 |
| | layer | No | [ATC INFRAESTRUCTURA_APM] | ATC |
| /public/alerts | name | Sí | <<nombre del dominio>>:<<módulo de gestión>>:<<NombreAlerta>> | |
| /public/metrics | items | Sí | Matriz de rutas de métricas delimitadas por comas | |
| | endTime | No | Hora de finalización en milisegundos | |
| | intervalo | No | Intervalo en milisegundos | 480000 |

Ejemplos

Los ejemplos siguientes muestran cómo asignar las direcciones URL abreviadas.

```
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
```

Compatibilidad internacional

Un producto internacionalizado es un producto inglés que funciona correctamente en las versiones de idioma local del sistema operativo y en los productos de terceros necesarios. Un producto internacionalizado también admite datos de idioma local de entrada y salida. Los productos internacionalizados también admiten la capacidad de especificar las convenciones del idioma local para los formatos de fecha, hora, moneda y número.

Un producto traducido es un producto internacionalizado que incluye compatibilidad del idioma local para la interfaz de usuario del producto, ayuda en línea y otra documentación. Un producto traducido también incluye la configuración predeterminada del idioma local para los formatos de fecha, hora, moneda y número. Un producto traducido a veces se denomina producto localizado.

DX Application Performance Management admite las siguientes opciones internacionales. El producto se localiza completamente y es compatible con la configuración regional de formato de fecha, hora y número. La interfaz de usuario está disponible en los siguientes idiomas:

- Inglés
- Francés
- Portugués (Brasil)
- Español

La documentación del producto está disponible en los siguientes idiomas:

- Inglés
- Francés
- Portugués (Brasil)
- Español

Funciones de accesibilidad del producto

Nos comprometemos a garantizar que todos los clientes, independientemente de sus conocimientos, puedan utilizar correctamente nuestros productos y la documentación complementaria para desempeñar sus tareas de negocio vitales. Esta sección describe las funciones de accesibilidad de DX Application Performance Management.

Mejoras del producto

DX APM ofrece mejoras en la accesibilidad en las siguientes áreas:

- Visualización
- Sonido
- Teclado
- Ratón

La siguiente información se aplica a aplicaciones de Windows y Macintosh. Las aplicaciones de Java que se ejecutan en varios sistemas operativos de host, algunos de los cuales ya tienen a su disposición las tecnologías de asistencia. Estas tecnologías de asistencia existentes necesitan dos funcionalidades relacionadas con la máquina virtual de Java (JVM) para proporcionar acceso a los programas escritos en JPL. Las tecnologías de asistencia necesitan el soporte de accesibilidad de Java que está disponible desde la máquina virtual de Java. Las tecnologías asistenciales también necesitan un puente entre ellas mismos en los entornos nativos. El puente tiene un final en la máquina virtual de Java y el otro en la plataforma nativa. Por lo tanto, el puente es ligeramente diferente para cada plataforma a la que se dirige el puente de JVM. Sun está desarrollando tanto la parte JPL como la Win32 de este puente.

Visualización

Para aumentar la visibilidad en la pantalla del equipo, puede ajustar las siguientes opciones:

- **Estilo de fuente, color y tamaño de los elementos**

Define el color de la fuente, el tamaño y otras combinaciones visuales.

- **Resolución de pantalla**

Define el número de píxeles para ampliar los objetos en la pantalla.

- **Ancho del cursor y velocidad de intermitencia**

Define la tasa de anchura y la intermitencia del cursor para que sea más fácil buscar o minimizar la intermitencia del cursor.

- **Tamaño de los iconos**

Define el tamaño de los iconos. Puede agrandar los iconos más grandes para la visibilidad o reducirlos para aumentar el espacio de la pantalla.

- **Esquemas de contraste alto**

Define las combinaciones de colores. Puede seleccionar los colores que sean fáciles de ver.

Sonido

Para utilizar el sonido como alternativa visual, así como para facilitar o distinguir mejor los sonidos del equipo, ajuste las siguientes opciones:

- **Volumen**

Establece el volumen del equipo.

- **Texto a voz**

Permite oír las opciones del comando y leer textos en voz alta.

- **Advertencias**

Define las advertencias visuales.

- **Avisos**

Define las pistas de audio o visuales cuando se activan o desactivan las funciones de accesibilidad.

- **Esquemas**

Asocia los sonidos del equipo con eventos específicos del sistema.

- **Títulos**

Permite mostrar los títulos de las voces y sonidos.

Teclado

Se pueden realizar los ajustes de teclado siguientes:

- **Velocidad de repetición**

Define la rapidez con que se repite un carácter cuando se pulsa una tecla.

- **Tonos**

Define los tonos al pulsar algunas teclas.

- **Teclas especiales**

Define la tecla modificadora, por ejemplo, Mayús, Ctrl, Alt o la tecla del logotipo de Windows, para las combinaciones de teclas de acceso directo. Las teclas especiales permanecen activas hasta que se pulsa otra tecla.

Ratón

Puede utilizar las siguientes opciones para hacer que el ratón vaya más rápido y sea más fácil de usar:

- **Velocidad de clic**

Permite elegir la velocidad al hacer clic en el botón del ratón para realizar una selección.

- **Bloqueo del clic**

Permite al ratón resaltar o arrastrar algo sin tener que mantener pulsado el botón del ratón.

- **Acción de inversión**

Establece la función de inversión que se controla mediante las teclas de izquierda y derecha del ratón.

- **Velocidad de intermitencia**

Define la velocidad de intermitencia del cursor.

- **Opciones del puntero**

Permite definir los comportamientos siguientes:

- – Ocultar el puntero mientras se escribe
- – Mostrar la ubicación del puntero
- – Establecer la velocidad a la que se mueve el puntero en la pantalla
- – Seleccionar el tamaño del puntero y el color para una mejor visibilidad
- – Desplazar el puntero hasta una ubicación predeterminada en un cuadro de diálogo

Accesos directos del teclado

DX APM admite estos accesos directos del teclado:

- **Ctrl+X** - Cortar
- **Ctrl+C** - Copiar
- **Ctrl+K** - Buscar Siguiente
- **Ctrl+F** - Buscar y Reemplazar
- **Ctrl+V** - Pegar
- **Ctrl+S** - Guardar
- **Ctrl+Mayús+S** - Guardar todo
- **Ctrl+D** - Eliminar línea
- **Ctrl+Derecha** - Siguiente palabra
- **Ctrl+Abajo** - Av Pág
- **Fin** - Final de línea

Accesos directos del teclado para vídeos del producto

La documentación de DX APM incluye vídeos del tutorial del producto que se encuentran en YouTube. Para ver estos vídeos del producto puede utilizar los siguientes accesos directos del teclado:

- **Tab** - Se desplaza hacia adelante a través de las funciones
- **Tab+Mayús** - Se desplaza hacia atrás
- **Entrar**: Selecciona la función que está resaltada en una lista
- **Flecha hacia adelante y hacia atrás**: Controla el volumen del vídeo

Datos de uso (telemetría)

La telemetría es un elemento fundamental del modelo del acuerdo de licencia de la cartera (PLA) del software empresarial. El requisito inicial del esfuerzo de telemetría es recopilar e informar sobre el uso específico del producto de forma diaria para admitir el nuevo modelo de consumo. Si la organización es un cliente de Broadcom en el PLA del software empresarial, se debe activar la telemetría y se deben compartir los datos de uso. Este artículo describe cómo activar la telemetría y enrutar los datos de uso al Portal de informes de uso. Para obtener más información, consulte la sección [Portal de informes de uso](#).

- [Datos recopilados por telemetría](#)
- [Frecuencia de recopilación de datos](#)
- [Configuración del usuario en IntroscopeEnterpriseManager.properties](#)
- [Configuración del proxy HTTP](#)
- [Cómo se calculan las métricas de la licencia](#)
- [Cómo informar sobre los datos de uso de forma automática](#)
- [Cómo informar sobre los datos de uso de forma manual](#)

Datos recopilados por telemetría

La telemetría recopila dos tipos de detalles para cada cliente del PLA:

- **Datos del cliente:** Estos datos identifican el cliente y el sitio del cliente a través del ID del sitio. Los datos también incluyen un ID de reembolso opcional para identificar la división o grupo a la que se hará el cargo por el uso.
- **Datos de uso:** Se recopilan los datos de uso reales en función del consumo. Es necesario activar la carga de los datos de uso. Para obtener más información sobre los datos de uso que se recopilan, consulte la documentación del producto correspondiente.

NOTE

La telemetría no recopila información de identificación personal (PII) ni información confidencial. Para obtener más información sobre cómo se recopila y se usa su información, lea la [declaración de privacidad](#).

Frecuencia de recopilación de datos

De forma predeterminada, la telemetría recopila y almacena los datos diariamente a las 12.00 h. Si el programador no está activo a las 12.00 h., los datos se recopilan solamente en la ejecución del día siguiente. Los datos se recopilan solamente una vez al día.

Configuración del usuario en IntroscopeEnterpriseManager.properties

Para cargar los datos, el usuario debe configurar las siguientes propiedades en el archivo `IntroscopeEnterpriseManager.properties` y, a continuación, establecer el valor de `introscope.platelemetry.upload.enabled` (configurable en caliente) en `true`. Las propiedades siguientes están disponibles para la configuración.

| Nombre de la propiedad | Descripción |
|---|--|
| <code>introscope.platelemetry.instance.id</code> | ID generado internamente para cada instancia del producto. |
| <code>introscope.platelemetry.customer.email</code> | El nombre de dominio del cliente (no una dirección de correo electrónico). |
| <code>introscope.platelemetry.customer.siteid</code> | El ID del sitio del cliente. |
| <code>introscope.platelemetry.customer.incremental</code> | Indicador para determinar si una instalación o actualización está relacionada con un uso incremental como resultado del PLA (valor predeterminado: <code>false</code>). |

| Nombre de la propiedad | Descripción |
|---|--|
| <code>introscope.platetelemetry.customer</code> | Optional. Se utiliza para identificar la división o grupo para hacer referencia al uso del consumo para informar a broadcom.com. |

Configuración del proxy HTTP

Para obtener una descripción de las propiedades estándar de EM para un proxy HTTP, como `transport.http.proxy.host`, `transport.http.proxy.port`, `transport.http.proxy.username` y `transport.http.proxy.password` (valor cifrado), consulte [Configuración de Workstation](#).

Datos recopilados

Se recopilan los datos siguientes para DX Application Performance Management:

- Dispositivos

Las tablas siguientes muestran las cargas de telemetría:

Table 3: Cargas de telemetría

| Propiedades de la carga de telemetría | Descripción |
|--|---|
| <code>domain_name</code> | Nombre de dominio (por ejemplo, href="http://customer.com/">customer.com, bank.eu). |
| <code>site_id</code> | ID de sitio empresarial que el cliente usa para acceder al sitio de soporte. Para obtener el ID de sitio desde el portal de soporte, vaya a Mi cuenta, Perfil, Soporte de CA (ficha), ID del sitio de inicio de sesión. |
| <code>pla_agreement</code> | Valor booleano con formato numérico (1 == true, 0 == false). Este valor indica si el cliente participa en el Acuerdo de licencia de la cartera de suscripción. |
| <code>chargeback_id</code> | El valor proporcionado por el cliente para identificar el grupo o el área de cargo para su uso interno como realizar la facturación en los grupos. |
| <code>product_sku</code> | El valor del SKU específico del producto se proporciona a la biblioteca subyacente por el producto en el momento de la inicialización. |
| <code>sku_description</code> | La descripción del SKU del producto proporcionada a la biblioteca subyacente por el producto en el momento de la inicialización. |
| <code>product_version</code> | Versión del producto. |
| <code>instance_id</code> | UUID generado por el producto en la primera instalación. Varias instalaciones requieren que los productos generen un nuevo valor de ID de instancia cada vez. |
| <code>multiple telemetry metrics key_name</code> | Todos los pares de clave/valor contienen un prefijo de espacio de nombres para hacerlos únicos en comparación con los valores anteriores. La telemetría debe ser el prefijo para esta propiedad. Los pares clave/valor se agregan a la carga. Estos pares clave/valor contienen métricas de uso específicas del producto. |
| <code>date_collected</code> | La fecha en la que se recopilaron los datos de telemetría. El formato de fecha es AAAA-MM-DD (por ejemplo, 2018-02-20). |

Variables de entorno

En la tabla siguiente se enumeran las variables con valores de ejemplo que se utilizan para la telemetría:

| Variable | Descripción |
|--|---|
| APMMANAGER_TELEMETRY_ENVTYPE=onpremise | Esta variable es para el tipo de instalación. |
| APMMANAGER_TELEMETRY_CUSTOMERINFO=onpremise
to/customer/info/file> | Es el nombre de archivo de las propiedades de la información del cliente. |
| APMMANAGER_TELEMETRY_UPLOADENABLED=false | Esta variable se utiliza para cargar los datos de telemetría. |

Cómo se calculan las métricas de la licencia

Las métricas de DX Application Performance Management se calculan para cada agente de aplicaciones de la siguiente manera:

| Aplicaciones | Asignación |
|--------------------|---|
| Java | Cada instancia en ejecución de una máquina virtual Java monitorizada consume 4 dispositivos. |
| .NET y .NET CorePS | Cada instancia del SO que ejecuta una aplicación de .NET monitorizada o CLR (Common Language Runtime) consume 4 dispositivos. |
| PHP | Cada instancia en ejecución del Agente de la sonda de PHP consume 2 dispositivos. |
| Nodejs | Cada proceso monitorizado de NodeJS consume 0,4 dispositivos. |
| Python | Cada instancia del SO que ejecuta una aplicación de Python monitorizada consume 4 dispositivos. |

Cómo informar sobre los datos de uso de forma automática

Una vez que la instalación se haya realizado correctamente, configure los valores necesarios para enviar los datos de telemetría a Broadcom.com.

Siga estos pasos:

1. Copie el contenido del archivo **opt/dxplatelemetry/configcommon/esdplatelemetry_onpreminfo.properties.template** en el archivo **opt/dxplatelemetry/configcommon/esdplatelemetry_onpreminfo.properties**.
2. Edite el archivo **opt/dxplatelemetry/configcommon/esdplatelemetry_onpreminfo.properties** y rellene las siguientes claves con la información correcta:
 - **dxitenantid**: Introduzca el ID de cliente para almacenar los datos de telemetría del PLA en NASS.

NOTE

 - Introduzca el ID de cliente y no el ID de cohorte.
 - **dxitenantid** distingue entre mayúsculas y minúsculas.
 - **perform_upload**: Determina si los cálculos de telemetría del PLA se envían a Broadcom.com. Introduzca True para cargar los cálculos de telemetría. Valores: true, false
3. Reinicie el pod de telemetría de PLA para completar la configuración.

Cómo informar sobre los datos de uso de forma manual

Se puede informar sobre el uso de la telemetría manualmente siguiendo estos pasos. Solo se debe informar sobre el uso manualmente si es cliente de PLA y hay un motivo válido por el que no se puede configurar la telemetría para informar sobre el uso automáticamente.

Es posible configurar esto como parte de los pasos posteriores a la instalación. Para obtener los pasos completos, consulte [Cómo rellenar la información y configurar la telemetría](#). Es posible que también se deba configurar el uso de la telemetría mediante la API del recopilador del uso del producto. Para obtener más información sobre el uso de esta API, consulte [Recopilador del uso del producto](#).

Aviso Legal de Documentación

Esta documentación, que incluye sistemas incrustados de ayuda y materiales distribuidos por medios electrónicos (en adelante, referidos como la "Documentación") se proporciona con el único propósito de informar al usuario final, pudiendo Broadcom proceder a su modificación o retirada en cualquier momento. Esta documentación es propiedad de Broadcom. Queda prohibida la copia, transferencia, reproducción, divulgación, modificación o duplicación de la totalidad o parte de esta Documentación sin el consentimiento previo y por escrito de Broadcom.

No obstante lo anterior, si Usted es licenciataria de los productos informáticos a los que se hace referencia en la Documentación, puede imprimir o hacerse de alguna otra forma un número razonable de copias de la Documentación, que serán exclusivamente para su uso interno y de sus empleados en relación con dichos productos. En cualquier caso, en dichas copias deberán figurar los avisos e inscripciones relativas a los derechos de autor de Broadcom.

El derecho a realizar copias de la Documentación sólo tendrá validez durante el período en que la licencia para el uso del software en cuestión esté en vigor. En caso de terminarse la licencia por cualquier razón, Usted es el responsable de certificar por escrito a Broadcom que todas las copias, totales o parciales, de la Documentación, han sido devueltas a Broadcom o, en su caso, destruidas.

EN LA MEDIDA EN QUE LA LEY APLICABLE LO PERMITA, BROADCOM PROPORCIONA ESTA DOCUMENTACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN FIN CONCRETO Y NO VULNERACIÓN DE DERECHOS DE TERCEROS. BROADCOM NO RESPONDERÁ EN NINGÚN CASO, ANTE USTED NI ANTE TERCEROS, EN LOS SUPUESTOS DE DEMANDAS POR PÉRDIDAS O DAÑOS, DIRECTOS O INDIRECTOS, QUE SE DERIVEN DEL USO DE ESTA DOCUMENTACIÓN INCLUYENDO A TÍTULO ENUNCIATIVO PERO SIN LIMITARSE A ELLO, LA PÉRDIDA DE BENEFICIOS Y DE INVERSIONES, LA INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL, LA PÉRDIDA DEL FONDO DE COMERCIO O LA PÉRDIDA DE DATOS, INCLUSO CUANDO BROADCOM HUBIERA ADVERTIDO CON ANTELACIÓN Y EXPRESAMENTE DE LA POSIBILIDAD DE DICHAS PÉRDIDAS O DAÑOS.

El uso de cualquier producto informático al que se haga referencia en la Documentación se regirá por el acuerdo de licencia aplicable, el cual no se verá modificado, en modo alguno, por este aviso.

Broadcom Inc es el fabricante de esta Documentación.

Esta documentación presenta "Derechos Restringidos". El uso, la duplicación o la divulgación por parte del gobierno de los Estados Unidos está sujeta a las restricciones establecidas en las secciones 12.212, 52.227-14 y 52.227-19(c)(1) - (2) de FAR y en la sección 252.227-7014(b)(3) de DFARS, según corresponda, o en la que pueda serle de aplicación en su momento.

Copyright © 2005-2024 Broadcom. Todos los Derechos Reservados. El término "Broadcom" hace referencia a Broadcom Inc. o sus filiales. Todas las marcas, nombres comerciales, logotipos y marcas de servicio a los que se hace referencia en este documento pertenecen a sus respectivas empresas.

