Comprender el rendimiento del conector de Active Directory

Contenido

Introducción

Este documento describe el rendimiento del conector de Active Directory para Umbrella DNS.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Umbrella DNS.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

El servicio Umbrella Connector se utiliza para supervisar los eventos de inicio de sesión de usuario/equipo como parte de la integración de Active Directory de Umbrella. El servicio del conector OpenDNS lee la información de inicio de sesión del registro de eventos de seguridad de cada controlador de dominio AD de su sitio.

En entornos con una alta frecuencia de eventos de inicio de sesión de usuario, es importante revisar estas directrices de rendimiento. Para una identificación precisa del usuario, el servicio de conector debe poder recuperar la información de inicio de sesión rápidamente.

Número máximo de eventos/segundo

No existe un límite máximo en el número de eventos que se pueden procesar. El servicio Umbrella Connector se prueba para admitir un número continuo de 850 eventos por segundo en todos los controladores de dominio de un "sitio". Se basa en un entorno de laboratorio dedicado sin software de terceros en ejecución. Los resultados reales pueden variar en función de la latencia de la red y otros cuellos de botella.

Los clientes pueden determinar un número aproximado de eventos leyendo la sección "Eventos por segundo" más adelante en este artículo.

Características nuevas

Para clientes en implementaciones más grandes con una alta frecuencia de eventos de inicio de sesión, Umbrella cuenta con nuevas funciones orientadas al rendimiento. Además de las recomendaciones generales sobre el rendimiento, lea las instrucciones que se incluyen más adelante en este artículo sobre el equilibrio de carga, la comunicación paralela y la conexión del lector de registros de eventos directos.

Recomendaciones de rendimiento

Tamaño del conector

El servidor que ejecuta el servicio Conector de Active Directory debe tener recursos de CPU y memoria, tal como se especifica en la Guía de dimensionamiento de la documentación de Umbrella.

Conector dedicado

Aunque el servicio Conector se puede instalar directamente en un controlador de dominio, Cisco Umbrella recomienda que el Conector se instale en un servidor miembro dedicado al servicio Conector. Este servidor miembro no debe tener ningún otro software de terceros instalado. Obtenga más información sobre el proceso de instalación en la documentación de Umbrella.

Sitios de referencia

Siempre que sea posible, las implementaciones de Umbrella deben estar separadas en "Sitios" que restrinjan qué componentes se comunican a través de la red. El servicio Conector sólo puede comunicarse con componentes del mismo sitio de Umbrella. Esta función siempre se debe utilizar cuando los usuarios tienen una implementación distribuida en áreas geográficas grandes.

Normalmente, se crea un sitio de Umbrella para cada ubicación física. Los paraguas deben incluir estas reglas en la documentación de Umbrella.

El uso adecuado de los sitios de Umbrella puede mejorar en gran medida la implementación y evitar que los componentes se comuniquen a través de la red de área extensa.

Latencia de red

Los eventos de inicio de sesión se pueden transferir al conector a través de la red. Es importante que haya una conexión de alta velocidad entre el conector y cada controlador de dominio para reducir los retrasos relacionados con la red. El conector se puede colocar lo más cerca posible de los controladores de dominio y los dispositivos virtuales.

Número de conectores

Se necesita un conector para cada sitio de Umbrella. Es posible tener varios conectores en un sitio de Umbrella, pero solo es necesario para fines de redundancia. Tener conectores adicionales coloca carga adicional en los controladores de dominio ya que están duplicando la misma función que el primer conector. Umbrella recomienda un máximo de 2 conectores para cada sitio de Umbrella.

Tamaño del registro de eventos

Los grandes registros de sucesos de seguridad de Windows pueden tener un impacto adverso en el rendimiento de esta operación WMI. Umbrella recomienda limitar el tamaño del registro de eventos. El mejor rendimiento se encuentra con un archivo de registro < 512 MB, sin embargo, esto se puede ajustar en línea con sus requisitos de retención de registros. El tamaño del archivo de registro se puede ajustar siguiendo estas instrucciones:

1. Abra la aplicación Visor de eventos (eventvwr.msc).

2. Vaya a Registros de Windows > Sistema

3. Haga clic con el botón derecho del ratón en el registro del sistema y seleccione Propiedades.

4. Ajuste el tamaño máximo del archivo de registro como desee y seleccione Aceptar.

Software de terceros

Varios otros productos de software también utilizan WMI, que puede crear un cuello de botella en WMI en el controlador de dominio. Esto puede incluir:

- Software analítico/de seguridad de terceros que supervisa los registros de eventos
- Reenvío del registro de eventos de Windows
- Integración con SIEM y otro software que supervisa los registros de eventos

Si alguno de estos programas ya no es necesario, se recomienda desactivarlo. Como alternativa, este problema se puede mitigar mediante el método 'Conexión directa del lector de registros de eventos' descrito en el Apéndice.

Software antivirus

Excluir esta carpeta y estos ejecutables del análisis antivirus:

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\OpenDNSAuditService.exe
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>OpenDNSAuditClient.exe
```

Controladores de dominio adicionales

El sistema de notificación WMI del controlador de dominio pone en cola y procesa cada entrada del registro de eventos y las envía a los suscriptores WMI. Este es efectivamente un mecanismo de empuje donde el DC envía los eventos. Como tal, puede haber un cuello de botella de rendimiento en el propio controlador de dominio que afecta la rapidez con la que se envían los eventos.

Este cuello de botella se puede mitigar agregando controladores de dominio adicionales a su entorno AD. Umbrella ha probado un único controlador de dominio hasta 850 eventos/s.

Excepciones de cuenta de servicio

Reduzca el número de inicios de sesión de AD detectados por Umbrella excluyendo las cuentas de servicio. Estas cuentas deben excluirse de todos modos para que la aplicación de políticas sea correcta. También puede excluir servidores y otros dispositivos que no utilicen las directivas de usuario de AD, pero que puedan tener un gran volumen de inicios de sesión de usuarios.

Parches WMI

Asegúrese de que el controlador de dominio y el servidor conector están actualizados con los parches más recientes de Microsoft. Aquí encontrará ejemplos de revisiones que resuelven problemas conocidos de rendimiento de WMI.

Límites de memoria y manejo de WMI

WMI contiene sus propios límites internos que pueden crear un cuello de botella. Esto es especialmente cierto cuando otro software también realiza operaciones WMI intensivas. En la documentación de Microsoft encontrará un ejemplo de cómo aumentar estos límites.

Umbrella support no puede aconsejar los límites correctos para su entorno. Póngase en contacto con Microsoft para obtener ayuda.

Equilibrio de carga de DC

Umbrella ahora admite una característica de equilibrio de carga que resulta útil cuando un sitio tiene varios controladores de dominio y un gran número de eventos de inicio de sesión. En esta situación, se instalan conectores adicionales y, a continuación, se asignan controladores de dominio a un conector a través de un grupo de equilibrio de carga.

En un entorno simple, el Balanceo de Carga funcionaría de la siguiente manera:

- DC_A y DC_B se asignan al balanceo de carga Group_1 que es manejado por Connector_1.
- DC_C y DC_D se asignan al balanceo de carga Group_2, que es manejado por Connector_2.
- Los dispositivos virtuales siguen recibiendo eventos de ambos conectores, por lo que siguen siendo conscientes de todos los eventos de inicio de sesión.
- Si se requiere redundancia, se puede instalar un conector adicional en cada grupo de balanceo de carga.

Esta función ofrece las siguientes ventajas:

- La carga de trabajo de cada conector se reduce considerablemente. Cada conector administra un número menor de controladores de dominio.
- Esto suele ser útil en situaciones en las que hay un gran retraso al recibir eventos de un DC.

El equilibrio de carga puede ampliarse para utilizarse en entornos complejos de varios sitios con muchos controladores de dominio. No hay inconveniente en utilizar el Balanceo de Carga más allá de la instalación de conectores adicionales.

En este momento, la función de equilibrio de carga debe estar habilitada por el soporte de Umbrella. Póngase en contacto con el servicio de asistencia de Umbrella para hablar sobre sus requisitos.

Comunicación paralela del dispositivo virtual

El conector ahora puede enviar eventos de inicio de sesión a varios dispositivos virtuales en

paralelo, en lugar de utilizar el método serial predeterminado. Esto resulta útil cuando un sitio tiene varios dispositivos virtuales y un gran número de eventos de inicio de sesión.

Esta función ofrece las siguientes ventajas:

- Minimiza cualquier retraso en el envío de la información de inicio de sesión cuando hay varios dispositivos. Un evento se puede enviar a todos los dispositivos a la vez.
- Evita que se produzca un problema de comunicación o una interrupción con un dispositivo que repercute en otros dispositivos. Se mantiene una cola de eventos independiente para cada uno.

Esta función ahora se habilita automáticamente, pero solo cuando el servidor cumple las recomendaciones de CPU y memoria .

Transmisión acelerada de eventos de inicio de sesión de usuarios

El conector ahora puede transmitir eventos de inicio de sesión de usuario en lotes, lo que aumenta significativamente el número de eventos por segundo que se pueden enviar al dispositivo virtual (por segundo). Esto es especialmente importante para los conectores que se comunican con dispositivos virtuales en ubicaciones remotas.

Esta función ahora se puede activar automáticamente, pero tiene estos requisitos:

- La comunicación en paralelo (arriba) debe estar habilitada. El servidor debe cumplir las recomendaciones de CPU y memoria.
- Se requiere ADC versión 1.8+
- Se requiere conector versión 3.2.0+

Conexión del lector de registro de eventos directo

La versión 1.4+ del conector de Active Directory admite un nuevo método para conectarse directamente al registro de eventos de seguridad de los controladores de dominio sin utilizar una consulta WMI. Esto elimina WMI como intermediario y mejora significativamente el rendimiento en los casos en los que WMI es un cuello de botella. Esto es especialmente útil en escenarios donde los controladores de dominio individuales están procesando un gran número de eventos de inicio de sesión.

Esta función funciona mediante un mecanismo de extracción en el que el conector extrae nuevos eventos cada 5 segundos, por lo que se produce un breve retraso (por ejemplo, 5 segundos) en la identificación del usuario correcto.

Esta optimización está ahora activada de forma predeterminada. Para obtener más información sobre esta función, póngase en contacto con el servicio de asistencia de Umbrella.

Eventos por segundo

Es posible contar el número de eventos recientes en un controlador de dominio para estimar los eventos por segundo. Umbrella recomienda hacer esto en horas pico:

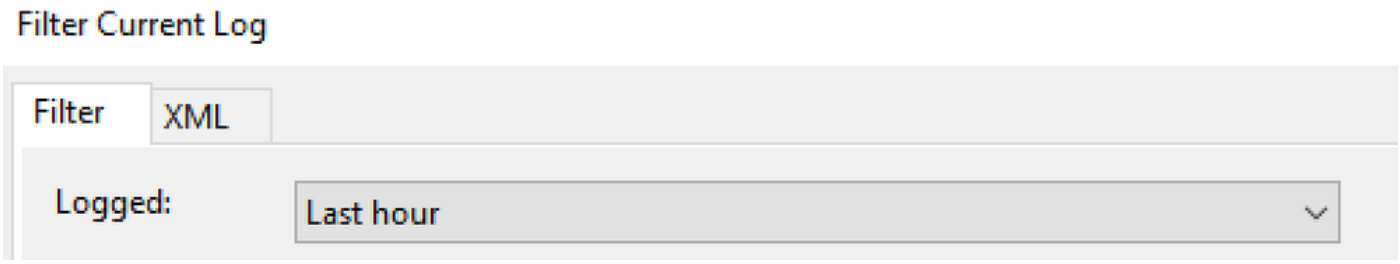
1. Abra la aplicación Visor de eventos (eventvwr.msc).

2. Vaya a Windows Logs > System.

3. Seleccione Filtrar registro actual y seleccione los eventos registrados en Última hora.

4. Seleccione Aceptar.

Una vez cargado el filtro, el registro de eventos puede mostrar el número de eventos en la última hora. Este valor se puede dividir por 3600 para estimar los eventos por segundo.



360024901511

360024894112

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).