Entender o Desempenho do Conector do Ative Diretory

Contents

Introdução

Este documento descreve o desempenho do conector do Ative Diretory para o Umbrella DNS.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no DNS Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

O serviço Umbrella Connector é usado para monitorar eventos de logon de Usuário/Computador como parte da integração do Ative Diretory do Umbrella. O serviço OpenDNS Connector lê as informações de logon do Log de Eventos de Segurança de cada Controlador de Domínio do AD em seu site.

Em ambientes com uma alta frequência de eventos de login de usuário, é importante revisar essas diretrizes de desempenho. Para uma identificação precisa do usuário, o serviço Connector deve ser capaz de recuperar rapidamente as informações de login.

Máximo de Eventos/Segundo

Não há limite rígido para o número de eventos que podem ser processados. O serviço Umbrella Connector é testado para oferecer suporte a 850 eventos por segundo em todos os controladores de domínio em um "local". Baseia-se em um ambiente de laboratório dedicado, sem software de terceiros em execução. Os resultados reais podem variar com base na latência da rede e em outros gargalos.

Os clientes podem determinar um número aproximado de eventos lendo a seção "Eventos por segundo", mais adiante neste artigo.

Novos recursos

Para clientes em implantações maiores com uma alta frequência de eventos de login, a Umbrella tem novos recursos orientados para o desempenho. Além das recomendações gerais de desempenho, leia as diretrizes mais adiante neste artigo sobre balanceamento de carga, comunicação paralela e conexão direta do leitor de logs de eventos.

Recomendações de desempenho

Dimensionamento do conector

O servidor que executa o serviço Ative Diretory Connector deve ter recursos de CPU e Memória, conforme especificado no Guia de Dimensionamento da documentação do Umbrella.

Conector dedicado

Embora o serviço do Conector possa ser instalado diretamente em um Controlador de Domínio, o Cisco Umbrella recomenda que o Conector seja instalado em um servidor membro dedicado ao serviço do Conector. Este servidor membro não deve ter nenhum outro software de terceiros instalado. Leia mais sobre o processo de instalação na documentação do Umbrella.

Sites de guarda-chuva

Sempre que possível, as implantações do Umbrella devem ser segregadas em "locais" que restrinjam quais componentes se comunicam pela rede. O serviço do Connector só pode se comunicar com componentes no mesmo site do Umbrella. Esse recurso deve ser sempre usado quando os usuários tiverem uma implantação distribuída por grandes áreas geográficas.

Normalmente, um site Umbrella é criado para cada local físico. Os sites de Umbrella devem ter essas regras na documentação do Umbrella.

O uso adequado dos locais Umbrella pode melhorar muito a implantação e impedir que os componentes se comuniquem pela Rede de Longa Distância.

Latência de rede

Os eventos de logon podem ser transferidos ao Conector pela rede. É importante que haja uma conexão de alta velocidade entre o Conector e cada Controlador de Domínio para reduzir atrasos relacionados à rede. O conector pode ser posicionado o mais próximo possível dos controladores de domínio e dos dispositivos virtuais.

Número de conectores

É necessário um conector para cada site Umbrella. É possível ter vários conectores em um local Umbrella, mas isso só é necessário para fins de redundância. Ter conectores adicionais coloca carga extra nos controladores de domínio, pois eles estão duplicando a mesma função que o primeiro conector. A Umbrella recomenda um máximo de 2 conectores para cada site Umbrella.

Tamanho do Log de Eventos

Logs de Eventos de Segurança do Windows grandes podem ter um impacto adverso no desempenho desta operação WMI. O Umbrella recomenda limitar o tamanho do registro de eventos. O melhor desempenho é encontrado com um arquivo de registro < 512 MB; no entanto, ele pode ser ajustado de acordo com seus requisitos de retenção de registro. O tamanho do arquivo de registro pode ser ajustado usando estas instruções:

1. Abra o aplicativo Visualizador de Eventos (eventvwr.msc).

2. Vá para Windows Logs > System

3. Clique com o botão direito do mouse no log do Sistema e selecione Propriedades.

4. Ajuste o tamanho máximo do arquivo de log conforme desejado e selecione OK.

Software de terceiros

Vários outros produtos de software também utilizam o WMI, o que pode criar um gargalo no WMI no controlador de domínio. Isso pode incluir:

- Software de segurança/análise de terceiros que monitora registros de eventos
- Encaminhamento de Log de Eventos do Windows
- Integração do SIEM e outros softwares que monitoram registros de eventos

Se algum desses softwares não for mais necessário, recomendamos desativá-lo. Como alternativa, esse problema pode ser atenuado usando o método "Direct Event Log Reader Connection" descrito no apêndice.

Software antivírus

Excluir esta pasta e estes executáveis da verificação de antivírus:

```
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 domínio adicionais

O sistema de notificação WMI no Controlador de Domínio enfileira e processa cada entrada do Log de Eventos e as envia aos assinantes do WMI. Este é efetivamente um mecanismo de envio onde os eventos são enviados pelo DC. Como tal, pode haver um gargalo de desempenho no próprio controlador de domínio, o que afeta a rapidez com que os eventos são enviados.

Esse gargalo pode ser minimizado com a adição de controladores de domínio adicionais ao ambiente do AD. A Umbrella testou um único controlador de domínio com até 850 eventos/s.

Exceções da conta de serviço

Reduza o número de logons do AD detectados pelo Umbrella excluindo as contas de Serviço. Essas contas devem ser excluídas de qualquer forma para a aplicação correta da política. Você também pode excluir servidores e outros dispositivos que não estejam usando políticas de Usuário do AD, mas que possam ter um grande volume de logons de usuário.

Patches WMI

Verifique se o controlador de domínio e o servidor conector estão atualizados com os patches mais recentes da Microsoft. Exemplos de hotfixes que resolvem problemas conhecidos de desempenho do WMI estão aqui.

Memória WMI e Limites de Tratamento

A WMI contém seus próprios limites internos que podem criar um afunilamento. Isso é particularmente verdadeiro quando outro software também está executando operações WMI intensivas. Um exemplo de como aumentar esses limites pode ser encontrado na documentação da Microsoft.

O suporte Umbrella não pode informar os limites corretos para seu ambiente. Entre em contato com a Microsoft para obter assistência.

Balanceamento de carga DC

O Umbrella agora suporta um recurso de balanceamento de carga que é útil quando um site tem vários controladores de domínio e um grande número de eventos de logon. Neste cenário, conectores adicionais são instalados e os controladores de domínio são atribuídos a um conector por meio de um grupo de balanceamento de carga.

Em um ambiente simples, o balanceamento de carga funcionaria da seguinte forma:

- DC_A e DC_B são atribuídos ao balanceamento de carga Group_1 que é tratado por Connector_1.
- DC_C e DC_D são atribuídos ao balanceamento de carga Group_2, que é tratado por Connector_2.
- Os dispositivos virtuais ainda recebem eventos de ambos os conectores, portanto, ainda estão cientes de todos os eventos de logon.
- Se a redundância for necessária, um conector adicional pode ser instalado em cada grupo de balanceamento de carga.

Esse recurso tem os seguintes benefícios:

- A carga de trabalho de cada conector é bastante reduzida. Cada conector está tratando de um número menor de controladores de domínio.
- Isso geralmente ajuda em cenários onde há um alto atraso no recebimento de eventos de um DC.

O balanceamento de carga pode ser ampliado para ser usado em ambientes complexos de vários locais com muitos controladores de domínio. Não há desvantagem em usar o balanceamento de carga além da instalação de conectores adicionais.

Neste momento, o recurso de Balanceamento de Carga deve ser habilitado pelo suporte Umbrella. Entre em contato com o suporte da Umbrella para discutir suas necessidades.

Comunicação paralela de dispositivo virtual

O Conector agora pode enviar eventos de login para vários dispositivos virtuais em paralelo, em vez de usar o método serial padrão. Isso é útil quando um site tem vários dispositivos virtuais e um grande número de eventos de logon.

Esse recurso tem os seguintes benefícios:

- Minimiza qualquer atraso no envio de informações de login quando há vários dispositivos. Um evento pode ser enviado a todos os dispositivos de uma só vez.
- Evita problemas de comunicação ou interrupções com um dispositivo tendo um efeito de arrastamento para outros dispositivos. Uma fila de eventos separada é mantida para cada um.

Esse recurso agora é habilitado automaticamente, mas somente quando o servidor atende às recomendações de CPU e memória .

Transmissão acelerada de eventos de login de usuário

O Conector agora pode transmitir Eventos de Logon do Usuário em Lotes, o que aumenta significativamente o número de eventos por segundo que podem ser enviados para o Dispositivo virtual (por segundo). Isso é particularmente importante para conectores que se comunicam com dispositivos virtuais em locais remotos.

Este recurso agora pode ser habilitado automaticamente, mas tem estes requisitos:

- A comunicação paralela (acima) deve ser habilitada. O servidor deve atender às recomendações de CPU e memória.
- ADC Versão 1.8+ Necessário
- Versão 3.2.0+ do Conector Necessária

Conexão Direta do Leitor de Log de Eventos

A versão 1.4+ do conector do Ative Diretory dá suporte a um novo método para se conectar diretamente ao Log de Eventos de Segurança do(s) Controlador(es) de Domínio sem usar uma consulta WMI. Isso elimina a WMI como um "intermediário" e melhora significativamente o desempenho nos casos em que a WMI é um gargalo. Isso é particularmente útil em cenários onde controladores de domínio individuais estão processando um grande número de eventos de login.

Esse recurso funciona com o uso de um mecanismo de puxamento, no qual o conector extrai novos eventos a cada 5 segundos, de modo que há um pequeno atraso (por exemplo, 5 segundos) na identificação do usuário correto.

Essa otimização agora está habilitada por padrão. Para obter mais informações sobre esse recurso, entre em contato com o suporte do Umbrella.

Eventos por Segundo

É possível contar o número de eventos recentes em um Controlador de Domínio para estimar os eventos por segundo. A Umbrella recomenda fazer isso no horário de pico:

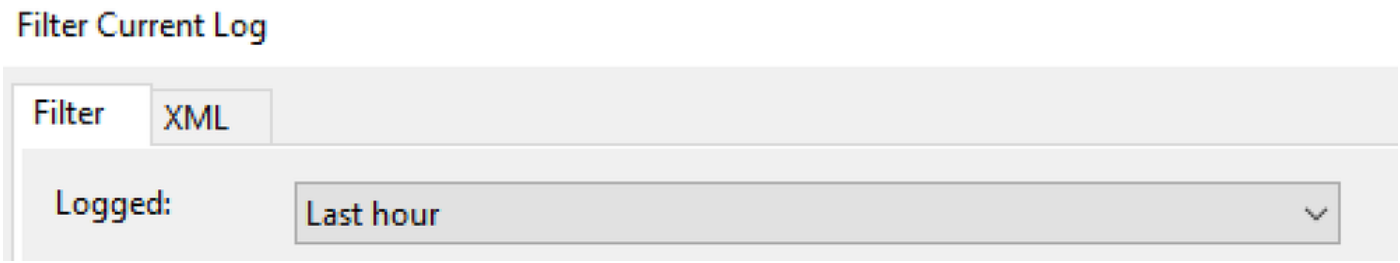
1. Abra o aplicativo Visualizador de Eventos (eventvwr.msc).

2. Vá para Windows Logs > System.

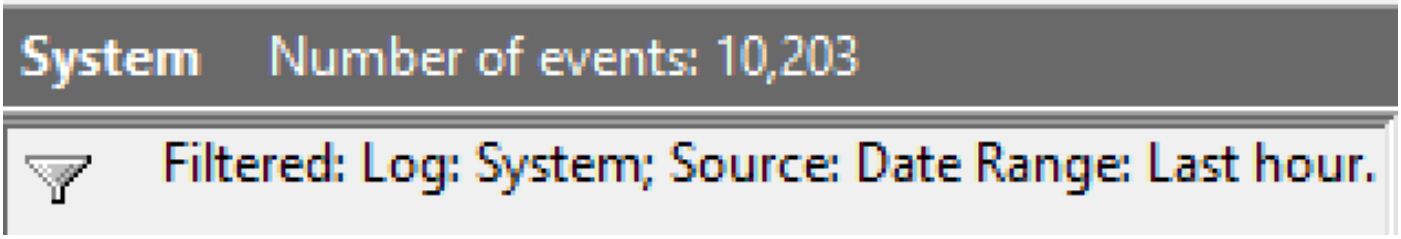
3. Selecione Filtrar log atual e selecione eventos registrados em Última hora.

4. Selecione OK.

Depois que o filtro for carregado, o Log de eventos poderá mostrar o número de eventos na última hora. Esse valor pode ser dividido por 3600 para estimar os eventos por segundo.



360024901511



360024894112

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.