Überblick über die Leistung von Active Directory Connectors

Inhalt

Einleitung

In diesem Dokument wird die Leistung des Active Directory-Connectors für Umbrella DNS beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Umbrella DNS.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Der Umbrella Connector-Dienst wird zur Überwachung von Benutzer-/Computeranmeldeereignissen im Rahmen der Active Directory-Integration von Umbrella verwendet. Der OpenDNS Connector-Dienst liest Anmeldeinformationen aus dem Sicherheitsereignisprotokoll jedes AD-Domänencontrollers an seinem Standort.

In Umgebungen mit häufigen Benutzeranmeldungen sollten Sie diese Leistungsrichtlinien unbedingt lesen. Für eine genaue Benutzeridentifizierung muss der Connector-Dienst in der Lage sein, Anmeldeinformationen schnell abzurufen.

Maximale Anzahl Ereignisse/Sekunde

Es gibt keine feste Grenze für die Anzahl der Ereignisse, die verarbeitet werden können. Der Umbrella Connector-Service wurde so getestet, dass alle Domänencontroller eines Standorts 850 Ereignisse pro Sekunde unterstützen. Diese basiert auf einer dedizierten Laborumgebung ohne die Ausführung von Drittanbietersoftware. Die tatsächlichen Ergebnisse können sich je nach Netzwerklatenz und anderen Engpässen unterscheiden.

Im Abschnitt "Ereignisse pro Sekunde" weiter unten in diesem Artikel können Kunden eine ungefähre Anzahl von Ereignissen/s ermitteln.

Neue Funktionen

Für Kunden in größeren Bereitstellungen mit einer hohen Häufigkeit von Anmeldeereignissen bietet Umbrella neue leistungsorientierte Funktionen. Zusätzlich zu den allgemeinen Leistungsempfehlungen lesen Sie die Richtlinien weiter unten in diesem Artikel über Lastenausgleich, Parallelkommunikation und die direkte Verbindung zum Ereignisprotokoll-Lesegerät.

Performance-Empfehlungen

Anschlussgröße

Der Server, auf dem der Active Directory Connector-Dienst ausgeführt wird, muss über CPU- und Speicherressourcen verfügen, wie im Dimensionierungsleitfaden der Umbrella-Dokumentation angegeben.

Dedizierter Anschluss

Obwohl der Connector-Dienst direkt auf einem Domänencontroller installiert werden kann, empfiehlt Cisco Umbrella, den Connector auf einem Mitgliedsserver zu installieren, der für den Connector-Dienst dediziert ist. Auf diesem Mitgliedsserver darf keine andere Software von Drittanbietern installiert sein. Weitere Informationen zum Installationsprozess finden Sie in der Umbrella-Dokumentation.

Umbrella Sites

Umbrella-Bereitstellungen müssen nach Möglichkeit in "Standorte" unterteilt werden, die die Kommunikation der Komponenten im Netzwerk einschränken. Der Connector-Service kann nur mit Komponenten desselben Umbrella-Standorts kommunizieren. Diese Funktion muss immer verwendet werden, wenn eine Bereitstellung auf große geografische Bereiche verteilt ist.

In der Regel wird für jeden physischen Standort ein Umbrella-Standort erstellt. Umbrella-Sites müssen diese Regeln in der Umbrella-Dokumentation enthalten.

Die ordnungsgemäße Verwendung von Umbrella-Standorten kann die Bereitstellung erheblich verbessern und die Kommunikation von Komponenten über das Wide Area Network verhindern.

Netzwerklatenz

Anmeldeereignisse können über das Netzwerk an den Connector übertragen werden. Es ist wichtig, dass eine Hochgeschwindigkeitsverbindung zwischen dem Connector und jedem Domänencontroller besteht, um Verzögerungen im Netzwerk zu reduzieren. Der Connector kann so nahe wie möglich an den Domänencontrollern und den virtuellen Appliances positioniert werden.

Anzahl der Anschlüsse

Für jeden Umbrella-Standort ist ein Connector erforderlich. Die Verwendung mehrerer Anschlüsse an einem Umbrella-Standort ist möglich, wird jedoch nur aus Redundanzgründen benötigt. Zusätzliche Connectors belasten die Domain Controller zusätzlich, da sie dieselbe Funktion wie der erste Connector duplizieren. Umbrella empfiehlt maximal 2 Anschlüsse für jeden Umbrella-Standort.

Größe des Ereignisprotokolls

Große Windows-Sicherheitsereignisprotokolle können sich negativ auf die Leistung dieses WMI-Vorgangs auswirken. Umbrella empfiehlt die Begrenzung der Größe des Ereignisprotokolls. Die beste Performance wird mit einer Log-Datei < 512MB gefunden, diese kann jedoch entsprechend Ihren Anforderungen an die Log-Archivierung angepasst werden. Die Größe der Protokolldatei kann mithilfe der folgenden Anweisungen angepasst werden:

1. Öffnen Sie die Ereignisanzeige (eventvwr.msc).

2. Gehen Sie zu Windows-Protokolle > System

3. Klicken Sie mit der rechten Maustaste auf das Systemprotokoll, und wählen Sie Eigenschaften.

4. Passen Sie die maximale Größe der Protokolldatei wie gewünscht an, und wählen Sie OK.

Software von Drittanbietern

Eine Reihe anderer Softwareprodukte verwenden auch WMI, was zu einem Engpass in WMI auf dem Domänencontroller führen kann. Dies kann Folgendes umfassen:

- Sicherheits-/Analysesoftware von Drittanbietern zur Überwachung von Ereignisprotokollen
- Weiterleiten von Windows-Ereignisprotokollen
- SIEM-Integration und andere Software zur Überwachung von Ereignisprotokollen

Wenn diese Software nicht mehr benötigt wird, empfehlen wir, sie zu deaktivieren. Alternativ kann dieses Problem mithilfe der im Anhang beschriebenen Methode 'Direct Event Log Reader Connection' behoben werden.

Antivirus-Software

Diesen Ordner und die folgenden ausführbaren Dateien vom Anti-Virus-Scanning ausschließen:

```
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
```

Zusätzliche Domänencontroller

Das WMI-Benachrichtigungssystem auf dem Domänencontroller verarbeitet jeden Ereignisprotokolleintrag in Warteschlangen und sendet sie an WMI-Abonnenten. Hierbei handelt es sich im Grunde um einen Push-Mechanismus, bei dem die Ereignisse vom Rechenzentrum gesendet werden. Daher kann es auf dem Domain Controller selbst zu einem Leistungsengpass kommen, der die Geschwindigkeit des Versands von Ereignissen beeinträchtigt.

Dieser Engpass kann durch Hinzufügen zusätzlicher Domänencontroller zu Ihrer AD-Umgebung beseitigt werden. Umbrella hat einen einzigen Domain Controller mit bis zu 850 Ereignissen/s getestet.

Ausnahmen für Dienstkonten

Reduzieren Sie die Anzahl der von Umbrella erkannten AD-Anmeldungen, indem Sie Dienstkonten ausschließen. Diese Konten müssen ohnehin ausgeschlossen werden, damit eine ordnungsgemäße Richtlinienanwendung möglich ist. Sie können auch Server und andere Geräte ausschließen, die keine AD-Benutzerrichtlinien verwenden, aber über eine große Anzahl von

Benutzeranmeldungen verfügen.

WMI-Patches

Stellen Sie sicher, dass der Domänencontroller und der Connector-Server mit den neuesten Microsoft-Patches auf dem neuesten Stand sind. Beispiele für Hotfixes, die bekannte WMI-Leistungsprobleme beheben, finden Sie hier.

Grenzwerte für WMI-Speicher und -Handle

WMI enthält eigene interne Grenzwerte, die zu Engpässen führen können. Dies gilt insbesondere dann, wenn andere Software ebenfalls intensive WMI-Operationen ausführt. Ein Beispiel, wie diese Grenzwerte erhöht werden können, finden Sie in der Microsoft-Dokumentation.

Der Umbrella-Support kann nicht die richtigen Grenzwerte für Ihre Umgebung angeben. Wenden Sie sich an Microsoft, um Unterstützung zu erhalten.

Gleichstrom-Lastenausgleich

Umbrella unterstützt jetzt eine Lastverteilungsfunktion, die nützlich ist, wenn ein Standort über mehrere Domänencontroller und eine große Anzahl von Anmeldeereignissen verfügt. In diesem Szenario werden zusätzliche Connectors installiert, und die Domänen-Controller werden dann einem Connector über eine Lastenausgleichsgruppe zugewiesen.

In einer einfachen Umgebung funktioniert der Lastenausgleich wie folgt:

- DC_A und DC_B werden der Lastverteilungsgruppe Group_1 zugewiesen, die von Connector_1 verwaltet wird.
- DC_C und DC_D werden der Lastverteilungsgruppe Group_2 zugewiesen, die von Connector_2 verwaltet wird.
- Virtuelle Appliances empfangen weiterhin Ereignisse von beiden Connectors und erkennen daher weiterhin alle Anmeldeereignisse.
- Falls Redundanz erforderlich ist, kann in jeder Lastenausgleichsgruppe ein zusätzlicher Connector installiert werden.

Diese Funktion bietet folgende Vorteile:

- Die Arbeitslast der einzelnen Steckverbinder wird erheblich reduziert. Jeder Connector verarbeitet eine geringere Anzahl von Domänencontrollern.
- Dies ist in der Regel dann hilfreich, wenn der Empfang von Ereignissen von einem Rechenzentrum sehr verzögert ist.

Load Balancing kann für den Einsatz in komplexen Umgebungen mit mehreren Standorten und zahlreichen Domain Controllern skaliert werden. Die Verwendung des Lastenausgleichs über die Installation zusätzlicher Anschlüsse hinaus hat keinen Nachteil.

Zu diesem Zeitpunkt muss die Lastenausgleichsfunktion von der Umbrella-Unterstützung aktiviert werden. Wenden Sie sich an den Umbrella Support, um Ihre Anforderungen zu besprechen.

Parallele Kommunikation über virtuelle Appliances

Der Connector kann jetzt Anmeldeereignisse parallel an mehrere virtuelle Appliances senden, anstatt die serielle Standardmethode zu verwenden. Dies ist nützlich, wenn eine Site über mehrere virtuelle Appliances und eine große Anzahl von Anmeldeereignissen verfügt.

Diese Funktion bietet folgende Vorteile:

- Minimiert Verzögerungen beim Senden von Anmeldeinformationen, wenn mehrere Appliances vorhanden sind. Ein Ereignis kann gleichzeitig an alle Appliances gesendet werden.
- Verhindert Kommunikationsprobleme oder -ausfälle bei einer Appliance, die einen Anstoßeffekt für andere Appliances haben. Für jedes Ereignis wird eine separate Warteschlange verwaltet.

Diese Funktion ist nun automatisch aktiviert, allerdings nur dann, wenn der Server die CPU- und Speicherempfehlungen erfüllt.

Beschleunigte Übertragung von Benutzeranmeldeereignissen

Der Connector kann jetzt Benutzeranmeldeereignisse in Batches übertragen, wodurch sich die Anzahl der Ereignisse pro Sekunde, die an die virtuelle Appliance gesendet werden können, erheblich erhöht (pro Sekunde). Dies ist besonders wichtig für Connectors, die mit virtuellen Appliances an Remote-Standorten kommunizieren.

Diese Funktion kann jetzt automatisch aktiviert werden, hat jedoch folgende Anforderungen:

- Parallel Communication (oben) muss aktiviert sein. Der Server muss die CPU- und Speicherempfehlungen erfüllen.
- ADC Version 1.8+ erforderlich
- Connector Version 3.2.0+ erforderlich

Direkte Verbindung zum Ereignisprotokollleser

Version 1.4+ des Active Directory-Connectors unterstützt eine neue Methode zur direkten Verbindung mit dem Sicherheitsereignisprotokoll der Domänencontroller ohne Verwendung einer WMI-Abfrage. Dadurch wird WMI als "Mittelsmann" eliminiert und die Leistung in Fällen, in denen WMI ein Engpass ist, deutlich verbessert. Dies ist besonders in Szenarien nützlich, in denen einzelne Domänencontroller eine große Anzahl von Anmeldeereignissen verarbeiten.

Diese Funktion verwendet einen Pull-Mechanismus, bei dem der Connector alle 5 Sekunden neue Ereignisse abruft, sodass der richtige Benutzer eine kurze Verzögerung (z. B. 5 Sekunden) erhält.

Diese Optimierung ist nun standardmäßig aktiviert. Für weitere Informationen zu dieser Funktion wenden Sie sich bitte an den Umbrella Support.

Ereignisse pro Sekunde

Es ist möglich, die Anzahl der letzten Ereignisse auf einem Domänencontroller zu zählen, um die Ereignisse pro Sekunde zu schätzen. Umbrella empfiehlt, dies zu Spitzenzeiten zu tun:

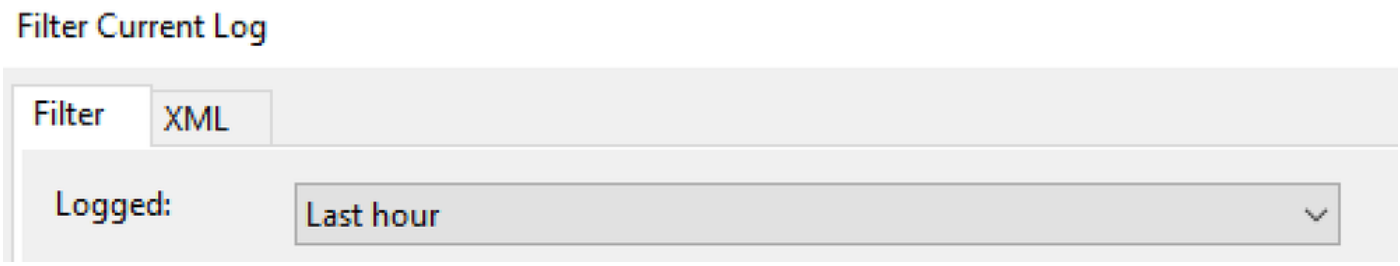
1. Öffnen Sie die Ereignisanzeige (eventvwr.msc).

2. Gehen Sie zu Windows-Protokolle > System.

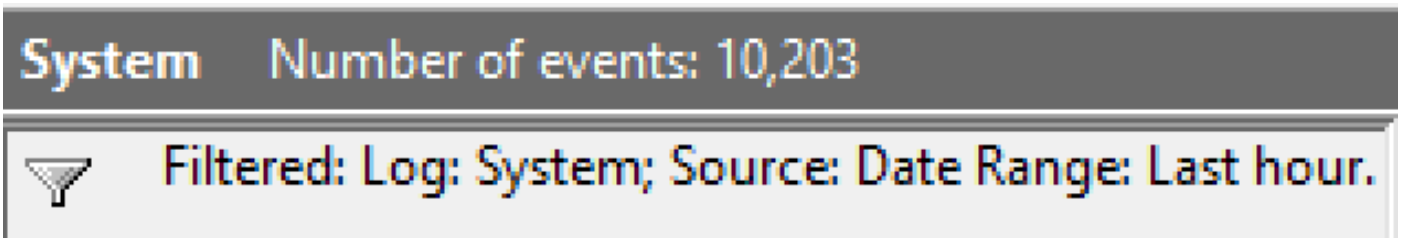
3. Wählen Sie Aktuelles Protokoll filtern und Letzte Stunde protokollierte Ereignisse aus.

4. Wählen Sie OK.

Nach dem Laden des Filters kann im Ereignisprotokoll die Anzahl der Ereignisse in der letzten Stunde angezeigt werden. Dieser Wert kann durch 3600 dividiert werden, um die Ereignisse pro Sekunde zu schätzen.



360024901511



360024894112

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.