De prestaties van de Active Directory-connector begrijpen

Inhoud

Inleiding

Dit document beschrijft de prestaties van de Active Directory-connector voor Umbrella DNS.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Umbrella DNS.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

De Umbrella Connector-service wordt gebruikt om aanmeldingsgebeurtenissen van gebruikers/computers te controleren als onderdeel van de Active Directory-integratie van Umbrella. De OpenDNS Connector-service leest aanmeldingsgegevens uit het Security Event Log van elke AD Domain Controller op zijn site.

In omgevingen met een hoge frequentie van gebruikersaanmeldingsgebeurtenissen is het belangrijk om deze prestatierichtlijnen te bekijken. Voor een nauwkeurige gebruikersidentificatie moet de Connector-service inloggegevens snel kunnen ophalen.

Maximale gebeurtenissen/seconde

Er is geen vaste limiet aan het aantal events dat verwerkt kan worden. De Umbrella Connector-service is getest om een continue 850 gebeurtenissen per seconde over alle domeincontrollers in een "Site" te ondersteunen. Dit is gebaseerd op een speciale laboratoriumomgeving waarin geen software van derden wordt uitgevoerd. De resultaten in de praktijk kunnen verschillen op basis van netwerklatentie en andere knelpunten.

Klanten kunnen een geschat aantal gebeurtenissen/s bepalen door het gedeelte 'Gebeurtenissen per seconde' verderop in dit artikel te lezen.

Nieuwe functies

Voor klanten in grotere implementaties met een hoge frequentie van aanmeldingsgebeurtenissen heeft Umbrella nieuwe prestatiegerichte functies. Naast de algemene aanbevelingen voor prestaties, lees de richtlijnen verderop in dit artikel over taakverdeling, parallelle communicatie en de Direct Event Log Reader Connection.

Prestatieaanbevelingen

Aansluitergrootte

De server waarop de Active Directory Connector-service wordt uitgevoerd, moet beschikken over CPU- en geheugenbronnen zoals gespecificeerd in de Sizing Guide van de overkoepelende documentatie.

Dedicated Connector

Hoewel de Connector-service rechtstreeks op een Domain Controller kan worden geïnstalleerd, raadt Cisco Umbrella aan de Connector te installeren op een lidserver die is toegewezen aan de Connector-service. Op deze ledenserver mag geen andere software van derden zijn geïnstalleerd. Lees meer over het installatieproces in de Umbrella documentatie.

Parapluplaatsen

Waar mogelijk moeten Umbrella-implementaties worden gescheiden in "Sites" die beperken welke componenten over het netwerk communiceren. De Connector-service kan alleen communiceren met onderdelen op dezelfde Umbrella-locatie. Deze functie moet altijd worden gebruikt wanneer gebruikers een implementatie hebben die over grote geografische gebieden is verdeeld.

Meestal wordt voor elke fysieke locatie een overkoepelende site gemaakt. Paraplu-sites moeten deze regels in de Paraplu-documentatie opnemen.

Correct gebruik van overkoepelende sites kan de implementatie aanzienlijk verbeteren en voorkomen dat componenten communiceren via het Wide Area Network.

Netwerklatentie

Aanmeldingsgebeurtenissen kunnen worden overgedragen naar de Connector in het netwerk. Het is belangrijk dat er een snelle verbinding is tussen de Connector en elke Domain Controller om netwerkgerelateerde vertragingen te verminderen. De connector kan zo dicht mogelijk bij de domeincontroller(s) en virtuele apparaten worden geplaatst.

Aantal connectors

Voor elke parapluplaats is één connector vereist. Het hebben van meerdere connectoren in een overkoepelende site is mogelijk, maar is alleen vereist voor redundantiedoeleinden. Het hebben van extra Connectors plaatst extra belasting op de Domain Controllers omdat ze dezelfde functie dupliceren als de eerste Connector. Umbrella beveelt maximaal 2 connectoren aan voor elke Umbrella-site.

Grootte gebeurtenissenlogboek

Grote Windows Security Event-logs kunnen een negatieve invloed hebben op de prestaties van deze WMI-bewerking. Umbrella beveelt aan de grootte van het gebeurtenissenlogboek te beperken. De beste prestaties worden gevonden met een logbestand < 512MB, maar dit kan worden aangepast in overeenstemming met uw vereisten voor logboekbehoud. De grootte van het logbestand kan met de volgende instructies worden ingesteld:

1. Open de toepassing Event Viewer (eventvwr.msc).

2. Ga naar Windows-logs > Systeem

3. Klik met de rechtermuisknop op het systeemlogboek en selecteer Eigenschappen.

4. Tune de maximale grootte van het logbestand naar wens en selecteer OK.

Software van derden

Een aantal andere softwareproducten maken ook gebruik van WMI, waardoor een knelpunt in WMI op de domeincontroller kan ontstaan. Dit kan het volgende omvatten:

- Beveiligings- / analysesoftware van derden die gebeurtenislogboeken bewaakt
- Windows-gebeurtenissenlogboek doorsturen
- SIEM-integratie en andere software die gebeurtenislogboeken bewaakt

Als een van deze software niet langer nodig is, raden we aan deze uit te schakelen. Als alternatief kan dit probleem worden verholpen met behulp van de methode 'Direct Event Log Reader Connection' die in de bijlage wordt beschreven.

antivirussoftware

Sluit deze map en de volgende uitvoerbare bestanden uit van antivirusscans:

```
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
```

Extra domeincontrollers

Het WMI-meldingssysteem op de domeincontroller zorgt voor wachtrijen en verwerkt elk item uit het gebeurtenissenlogboek en verzendt deze naar WMI-abonnees. Dit is in feite een push-mechanisme waarbij de gebeurtenissen door de DC worden verzonden. Als zodanig kan er een prestatieknelpunt op de domeincontroller zelf zijn dat bepaalt hoe snel gebeurtenissen worden verzonden.

Dit knelpunt kan worden verkleind door extra domeincontrollers aan uw AD-omgeving toe te voegen. Umbrella heeft één domeincontroller getest voor maximaal 850 events/s.

Uitzonderingen voor serviceaccount

Verminder het aantal AD-aanmeldingen dat door Umbrella wordt gedetecteerd door serviceaccounts uit te sluiten. Deze rekeningen moeten hoe dan ook worden uitgesloten voor een correcte toepassing van het beleid. U kunt ook servers en andere apparaten uitsluiten die geen beleidsregels voor AD-gebruikers gebruiken, maar wel een groot aantal gebruikersaanmeldingen kunnen hebben.

WMI-patches

Zorg ervoor dat de domeincontroller en connectorserver up-to-date zijn met de nieuwste Microsoft-patches. Voorbeelden van hotfixes die bekende WMI-prestatieproblemen oplossen, vindt u hier.

Limieten voor WMI-geheugen en -handgreep

WMI heeft zijn eigen interne limieten die een bottleneck kunnen creëren. Dit geldt met name wanneer andere software ook intensieve WMI-bewerkingen uitvoert. Een voorbeeld van hoe u deze limieten kunt verhogen, vindt u in Microsoft-documentatie.

Umbrella support kan niet de juiste limieten voor uw omgeving adviseren. Neem contact op met Microsoft voor hulp.

gelijkstroomlastverdeling

Umbrella ondersteunt nu een functie voor taakverdeling die handig is wanneer een site meerdere domeincontrollers en een groot aantal aanmeldingsgebeurtenissen heeft. In dit scenario worden extra connectors geïnstalleerd en worden domeincontrollers via een taakverdelingsgroep aan een connector toegewezen.

In een eenvoudige omgeving zou Load Balancing als volgt werken:

- DC_A en DC_B worden toegewezen aan load-balancing Group_1 die wordt afgehandeld door Connector_1.
- DC_C en DC_D worden toegewezen aan load-balancing Group_2 die wordt afgehandeld door Connector_2.
- Virtuele apparaten ontvangen nog steeds gebeurtenissen van beide connectors, dus zijn nog steeds op de hoogte van alle aanmeldingsgebeurtenissen.
- Als redundantie vereist is, kan in elke taakverdelingsgroep een extra connector worden geïnstalleerd.

Deze functie heeft de volgende voordelen:

- De werklast van elke connector wordt aanzienlijk verminderd. Elke connector verwerkt een kleiner aantal domeincontrollers.
- Dit helpt meestal in scenario's waarbij er een hoge vertraging is bij het ontvangen van gebeurtenissen uit een DC.

Load Balancing kan geschaald worden uitgebreid om te worden gebruikt in complexe omgevingen met meerdere locaties met veel domeincontrollers. Er is geen nadeel aan het gebruik van load balancing buiten de installatie van extra connectoren.

Op dit moment moet de functie Load Balancing worden ingeschakeld via Umbrella-ondersteuning. Neem contact op met Umbrella Support om uw wensen te bespreken.

parallelle communicatie van virtueel apparaat

De Connector is nu in staat om aanmeldingsgebeurtenissen naar meerdere Virtuele Toestellen

parallel te verzenden, in plaats van de standaard seriële methode te gebruiken. Dit is handig wanneer een site meerdere virtuele apparaten en een groot aantal aanmeldingsgebeurtenissen heeft.

Deze functie heeft de volgende voordelen:

- Minimaliseert elke vertraging bij het verzenden van aanmeldingsgegevens wanneer er meerdere toestellen zijn. Een evenement kan in één keer naar alle apparaten worden verzonden.
- Voorkomt een communicatieprobleem of een storing met één apparaat die een domino-effect heeft op andere apparaten. Voor elk evenement wordt een aparte wachtrij bijgehouden.

Deze functie wordt nu automatisch ingeschakeld, maar alleen als de server voldoet aan de CPU- en geheugenaanbevelingen.

Versnelde overdracht van gebeurtenissen bij gebruikersaanmelding

De Connector is nu in staat om User Login Events in Batches te verzenden, waardoor het aantal gebeurtenissen per seconde dat naar het Virtuele Toestel kan worden verzonden (per seconde) aanzienlijk toeneemt. Dit is vooral belangrijk voor connectors die communiceren met virtuele apparaten op externe locaties.

Deze functie kan nu automatisch worden ingeschakeld, maar heeft de volgende vereisten:

- Parallelle communicatie (hierboven) moet worden ingeschakeld. De server moet voldoen aan de aanbevelingen voor CPU en geheugen.
- ADC versie 1.8+ vereist
- Connector versie 3.2.0+ vereist

Direct Event Log Reader-verbinding

Versie 1.4+ van de Active Directory-connector ondersteunt een nieuwe methode om rechtstreeks verbinding te maken met het Security Event Log van de domeincontroller(s) zonder een WMI-query te gebruiken. Dit snijdt WMI uit als een "tussenpersoon" en verbetert de prestaties aanzienlijk in gevallen waarin WMI een knelpunt is. Dit is vooral handig in scenario's waarin individuele domeincontrollers een groot aantal aanmeldingsgebeurtenissen verwerken.

Deze functie werkt met een trekmechanisme waarbij de Connector elke 5 seconden nieuwe gebeurtenissen aantrekt, omdat er een korte (bijvoorbeeld 5 seconden) vertraging is in het identificeren van de juiste gebruiker.

Deze optimalisatie is nu standaard ingeschakeld. Neem voor meer informatie over deze functie contact op met Umbrella Support.

Gebeurtenissen per seconde

Het is mogelijk om het aantal recente gebeurtenissen op een domeincontroller te tellen om de gebeurtenissen per seconde te schatten. Umbrella raadt aan om dit op piektijd te doen:

1. Open de toepassing Event Viewer (eventvwr.msc).

2. Ga naar Windows-logs > Systeem.

3. Selecteer Huidig logboek filteren en selecteer Gebeurtenissen die zijn aangemeld Laatste uur.

4. Selecteer OK.

Nadat het filter is geladen, kan het eventlogboek het aantal gebeurtenissen in het laatste uur weergeven. Deze waarde kan worden gedeeld door 3600 om de gebeurtenissen per seconde te schatten.

360024901511

360024894112

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.