Problemen oplossen Paraplu Connector blokkeren van een Active Directory Service-account

Inhoud

Inleiding

In dit document wordt beschreven hoe u kunt oplossen waarom een Active Directory-serviceaccount wordt geblokkeerd door de Umbrella Connector.

Overzicht

De Umbrella Connector-service maakt WMI-verbindingen met de gebeurtenislogboeken van elke geregistreerde domeincontroller (DC) die deel uitmaakt van dezelfde overkoepelende site, om informatie over aanmeldingsgebeurtenissen te lezen. Deze aanmeldingsgebeurtenissen worden vervolgens geparseerd en geüpload naar alle virtuele apparaten (VA's) op dezelfde overkoepelende site. De VA maakt vervolgens een tijdelijke User-to-IP-toewijzing voor dat gebruikersnaam/bron-IP-adres. Er zijn een paar punten die het vermelden waard zijn:

- Umbrella Insights ondersteunt slechts één ingelogde gebruiker per IP-adres tegelijk
- De meest recent verwerkte aanmeldingsgebeurtenis van een bron IP 'wint'

Aangezien alle aanmeldingsgebeurtenissen gelijk zijn, heeft de connector een hardgecodeerde lijst met algemene AD-serviceaccounts waarvan de gebeurtenissen worden genegeerd. U kunt aanmeldingsgebeurtenissen van deze accounts zien die zijn opgehaald in het connectorlogbestand. Voorbeeld:

Gebeurtenis van gebruiker op zwarte lijst genegeerd: OpenDNS_Connector

Dit wordt gedaan om te voorkomen dat serviceaccounts (die net als standaardgebruikers aanmeldingsgebeurtenissen genereren in de DC-beveiligingsevenementlogboeken) de toewijzing van de gebruiker aan IP van de daadwerkelijke aangemelde gebruiker overschrijven.

In grote omgevingen kunnen ze, afhankelijk van het proces/de toepassing waarvoor een serviceaccount wordt gebruikt, ook elke minuut duizenden aanmeldingsgebeurtenissen genereren. Dit is ook extra belasting voor de connector, wat zich kan manifesteren als een vertraging tussen het aanmelden van de gebruiker en het juiste beleid dat wordt toegepast, of een correct beleid dat

later verloren gaat.

Lijst van geblokkeerde accounts

- _vmware_user_
- administrateur
- ANONIEM
- Anonieme aanmelding
- ASPNET
- lokale dienst
- McAfeeMVSUser
- MHCcontrol
- netwerkdienst
- netrix
- OpenDNS_Connector
- persyncsvc
- S-pcadmin
- SophosUpdateMgr
- SophosUpdMgr
- SVC-Altiris
- svc.iCreate

Meer informatie

U kunt ook andere aanmeldingsgebeurtenissen voor een AD-account uitsluiten van verwerking door de connector. Zie dit artikel voor instructies:

https://support.umbrella.com/hc/en-us/articles/231266088

Daarnaast zijn er AD-groepen die kunnen worden uitgesloten van de AD Sync van de connector, die wordt uitgevoerd om het beleidsgebied Dashboard te vullen met een lijst met AD-gebruikers, computers en groepen. Dit is hier te vinden:

https://support.umbrella.com/hc/en-us/articles/115005206526

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.