Venstergebeurtenissen/EventID's lezen via een connector begrijpen

Inhoud

Inleiding

In dit document wordt beschreven welke venstergebeurtenissen/eventID's standaard door een connector worden gelezen.

Overzicht

De Umbrella Virtual Appliance (VA) heeft technisch gezien alleen zicht op welk bron-IP-adres het een DNS-query ontvangt. Om een gebruiker te koppelen aan het DNS-verzoek, werkt de VA samen met de connector, wat resulteert in een gebruiker-naar-IP-toewijzing.

De connector leest gebeurtenissen met specifieke gebeurtenis-ID's uit de Security Event Logs op uw domeincontrollers. Deze gebeurtenissen worden vervolgens geparseerd en de gebruikersnaam en het IP-adres van de bron worden naar de VA verzonden, die vervolgens een koppeling maakt tussen die bron-IP en de gebruiker.

Als deze gebeurtenissen niet worden gecontroleerd door uw domeincontrollers, kan het proces voor het toewijzen van VA's niet correct plaatsvinden. In dit artikel wordt precies beschreven voor welk type gebeurtenis-ID's de connector standaard kijkt.

EventID	Beschrijving
4624	Event 4624 documenteert elke succesvolle poging om in te loggen op de lokale computer, ongeacht het aanmeldingstype, de locatie van de gebruiker of het type account.
528	Gebeurtenis 528 wordt geregistreerd wanneer een account zich aanmeldt bij de lokale computer, behalve in het geval van netwerkaanmeldingen. Event 528 wordt geregistreerd, ongeacht of de account die wordt gebruikt voor aanmelding een lokale SAM-account of een domeinaccount is.
540	Gebeurtenis 540 wordt geregistreerd wanneer een gebruiker elders in het netwerk

	verbinding maakt met een bron (zoals een gedeelde map) die wordt geleverd door de serverservice op deze computer.
4768	Deze gebeurtenis wordt alleen geregistreerd op domeincontrollers en zowel de succes- als de faalgevallen van deze gebeurtenis worden geregistreerd.
4769	Windows gebruikt deze gebeurtenis-ID voor zowel succesvolle als mislukte aanvragen voor servicetickets.

Als uw connector gebeurtenissen niet rechtstreeks kan lezen uit de Security Event Logs van de domeincontroller, kunt u een supportticket ophalen bij Umbrella met het verzoek om dit te wijzigen in een WMI-abonnement. In het geval van WMI-abonnementen abonneert de connector zich op alle hierboven vermelde evenementen. Daarnaast abonneert de connector zich ook op afmeldingsevenementen met EventID's, zoals hieronder vermeld. Merk op dat de connector deze afmeldingsgebeurtenissen standaard niet leest uit de Security Event Logs.

EventID	Beschrijving
538	Gebeurtenis 538 wordt geregistreerd wanneer een gebruiker zich afmeldt, of het nu gaat om een netwerkverbinding, interactieve aanmelding of een ander aanmeldingstype (zie Gebeurtenis 528 voor een overzicht van aanmeldingstypen).
4647	Deze gebeurtenis betekent het einde van een aanmeldingssessie en kan met behulp van de aanmeldings-ID worden gekoppeld aan de aanmeldingsgebeurtenis 4624.
4634	Deze gebeurtenis betekent ook het einde van een aanmeldingssessie en kan met behulp van de aanmeldings-ID worden gekoppeld aan de aanmeldingsgebeurtenis 4624.

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.