Active Directory offline integreren na implementatie van virtuele apparaten met beveiligde toegang

Inhoud

uitgeven

Na de implementatie van twee Secure Access Virtual Appliances (VA's) is de Active Directory (AD)-integratie gestopt met functioneren binnen het Secure Access-dashboard. Voorheen was AD-integratie operationeel, maar na de VA-implementatie wordt de AD-connector nu weergegeven als offline in het dashboard voor beveiligde toegang. Hulp is vereist om de AD-connectiviteit te herstellen.

milieu

- Technologie: oplossingsondersteuning (SSPT - contract vereist)
- subtechnologie: beveiligde toegang
- Softwareversie: ALLE
- Veilige toegang (DNS-Advantage/Umbrella)
- Implementatie van twee Virtual Appliances (VA's) voor beveiligde toegang op het hoofdkantoor
- Wijzigingsgebeurtenis: installatie van VA's onmiddellijk voorafgegaan door een storing in de AD-connector
- AD Connector was voorheen operationeel en wordt nu weergegeven als offline in het portaal voor beveiligde toegang

resolutie

Voer de volgende gedetailleerde stappen uit voor probleemoplossing om het probleem van AD-integratie aan te pakken dat als offline wordt weergegeven in het portaal voor beveiligde toegang na VA-implementatie:

Netwerkverkeer vastleggen tijdens opnieuw opstarten van de connector

Voer een wireshark-opname uit op alle interfaces van de AD-connector/domeincontroller terwijl u de connectorservices opnieuw start. Dit helpt bij het identificeren van netwerkcommunicatiefouten of ongeautoriseerde toegangspogingen tijdens de initialisatie van de connector.

Stap 1: Start Wireshark Capture op alle relevante interfaces

Start Wireshark en begin met vastleggen op alle AD-connector/domeincontrollerinterfaces.

Stap 2: Connectorservices opnieuw starten via Windows Services Manager

Open services.msc, zoek OpenDNS Connector-service en klik op Opnieuw starten.

Stap 3: Opname-bestand opslaan voor verdere analyse

Stop het vastleggen en exporteren van het .pcap-bestand.

Connectorlogboeken verzamelen

Verzamel logs van de AD-connector voor dieper inzicht in fouten of verificatieproblemen:

1. Navigeer naar de logdirectory.

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\vX.X.X
```

1. Verzamel relevante logbestanden en bereid ze voor op beoordeling. Kopieer alle logbestanden van de bovengenoemde directory naar een beveiligde locatie.

Rechten AD Connector-account verifiëren

Nadat u virtuele apparaten hebt geïntroduceerd, hebt u voor de AD Connector-account specifieke machtigingen nodig om correct te kunnen functioneren. Als de account de rol van de gebeurtenisloglezer mist, kan deze ongeautoriseerde toegangsuitzonderingen tegenkomen.

1. Wijs rechten voor gebeurtenisloglezers toe aan de AD Connector-account. Gebruik Active Directory Users and Computers (ADUC) of Groepsbeleid om de AD Connector-account toe te voegen aan de groep Gebeurtenisloglezers.
2. Bevestig dat de account de nieuwe machtiging heeft. Controleer het groepslidmaatschap voor de AD Connector-account om de opname van gebeurtenisloglezers te controleren.

Algemene uitzondering gevonden

Tijdens het oplossen van problemen kan deze uitzondering worden waargenomen in logs of uitvoer van de verbindingsstatus:

```
* Exception type: system.unauthorizedaccessexception
message: Attempted to perform an unauthorized operation.
```

Dit geeft aan dat de AD Connector-account niet voldoende machtigingen heeft, met name de rol

Event Log Reader, die verplicht is nadat VA's zijn geïntroduceerd.

Geen CLI-opdracht gevonden die de wijziging van de status van de AD-connector van offline naar online weergeeft.

Oorzaak

De onderliggende oorzaak is onvoldoende rechten voor de AD Connector-account na de implementatie van virtuele apparaten met beveiligde toegang. De account beschikt niet over de machtiging Event Log Reader, die vereist is voor een goede AD-connectorfunctionaliteit. Dit resulteert in een "system.unauthorised access exception"-fout en voorkomt dat de connector online werkt binnen het Secure Access-portaal.

Verwante inhoud

- Cisco Technical Support en downloads

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.