Integra Active Directory offline dopo la distribuzione di appliance virtuali di accesso sicuro

Sommario

Problema

Dopo la distribuzione di due appliance virtuali di accesso protetto (VA), l'integrazione di Active Directory (AD) ha smesso di funzionare nel dashboard di accesso protetto. In precedenza, l'integrazione di AD era operativa, ma dopo la distribuzione di AD, il connettore di AD viene visualizzato come non in linea nel dashboard di accesso protetto. Per ripristinare la connettività di AD è necessaria assistenza.

Ambiente

- Tecnologia: Supporto per la soluzione (SSPT - contratto obbligatorio)
- Sottotecnologia: Accesso sicuro
- Versione del software: TUTTO
- Accesso sicuro (DNS-Advantage/Umbrella)
- Installazione di due appliance virtuali (VA) Secure Access nelle sedi centrali
- Evento di modifica: Installazione di VA immediatamente precedente a un errore del connettore AD
- Connettore AD precedentemente operativo e ora visualizzato come non in linea nel portale Secure Access

Risoluzione

Per risolvere il problema dell'integrazione di AD visualizzata come non in linea nel portale di accesso sicuro dopo la distribuzione di VA, eseguire la procedura di risoluzione dei problemi dettagliata seguente:

Acquisisci traffico di rete durante il riavvio del connettore

Eseguire un'acquisizione Wireshark su tutte le interfacce del connettore AD/controller di dominio durante il riavvio dei servizi del connettore. Ciò consente di identificare eventuali errori di comunicazione di rete o tentativi di accesso non autorizzato durante l'inizializzazione del connettore.

Passaggio 1: Avviare l'acquisizione di Wireshark su tutte le interfacce rilevanti

Avviare Wireshark e iniziare l'acquisizione su tutte le interfacce del connettore AD/controller di dominio.

Passaggio 2: Riavviare i servizi Connector tramite Windows Services Manager

Aprire services.msc, individuare il servizio OpenDNS Connector e fare clic su Riavvia.

Passaggio 3: Salvare il file di acquisizione per un'ulteriore analisi

Arrestare l'acquisizione ed esportare il file .pcap.

Raccogli registri connettore

Raccogliere i registri dal connettore AD per una descrizione più dettagliata degli errori o dei problemi di autenticazione:

1. Passare alla directory dei log.

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

1. Raccogliere i file di log rilevanti e prepararli per la revisione. Copiare tutti i file di log dalla directory indicata in precedenza in un percorso sicuro.

Verifica autorizzazioni account connettore AD

Dopo l'introduzione di Virtual Appliance, l'account AD Connector richiede autorizzazioni specifiche per funzionare correttamente. Se l'account non dispone del ruolo Event Log Reader, possono verificarsi eccezioni di accesso non autorizzato.

1. Assegnare l'autorizzazione Lettore registro eventi all'account Connettore Active Directory. Utilizzare Utenti e computer di Active Directory o Criteri di gruppo per aggiungere l'account Connettore Active Directory al gruppo Lettori registro eventi.
2. Confermare che l'account dispone della nuova autorizzazione. Verificare l'appartenenza ai gruppi per l'account AD Connector per verificare l'inclusione dei lettori del registro eventi.

Rilevata eccezione comune

Durante la risoluzione dei problemi, è possibile osservare questa eccezione nei log o nell'output dello stato del connettore:

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

Ciò indica che l'account del connettore AD non dispone di autorizzazioni sufficienti, in particolare il ruolo Event Log Reader, obbligatorio dopo l'introduzione di VA.

Non è stato trovato alcun comando CLI che indica la modifica dallo stato del connettore AD offline a online.

Causa

La causa sottostante è un'autorizzazione insufficiente per l'account Connettore Active Directory dopo la distribuzione di appliance virtuali di accesso protetto. L'account non dispone dell'autorizzazione Lettore registro eventi, necessaria per la corretta funzionalità del connettore Active Directory. Ciò genera un errore "system.unauthorizedaccessexception" e impedisce al connettore di funzionare online all'interno del portale di accesso protetto.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).