&Risoluzione dei problemi;Accesso negato" Avviso in Umbrella AD Connector

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Problema

Soluzione

Causa

Ulteriori informazioni

Introduzione

In questo documento viene descritto come risolvere i problemi di accesso negato quando il connettore Cisco Umbrella Active Directory (AD) è in stato di avviso o di errore.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

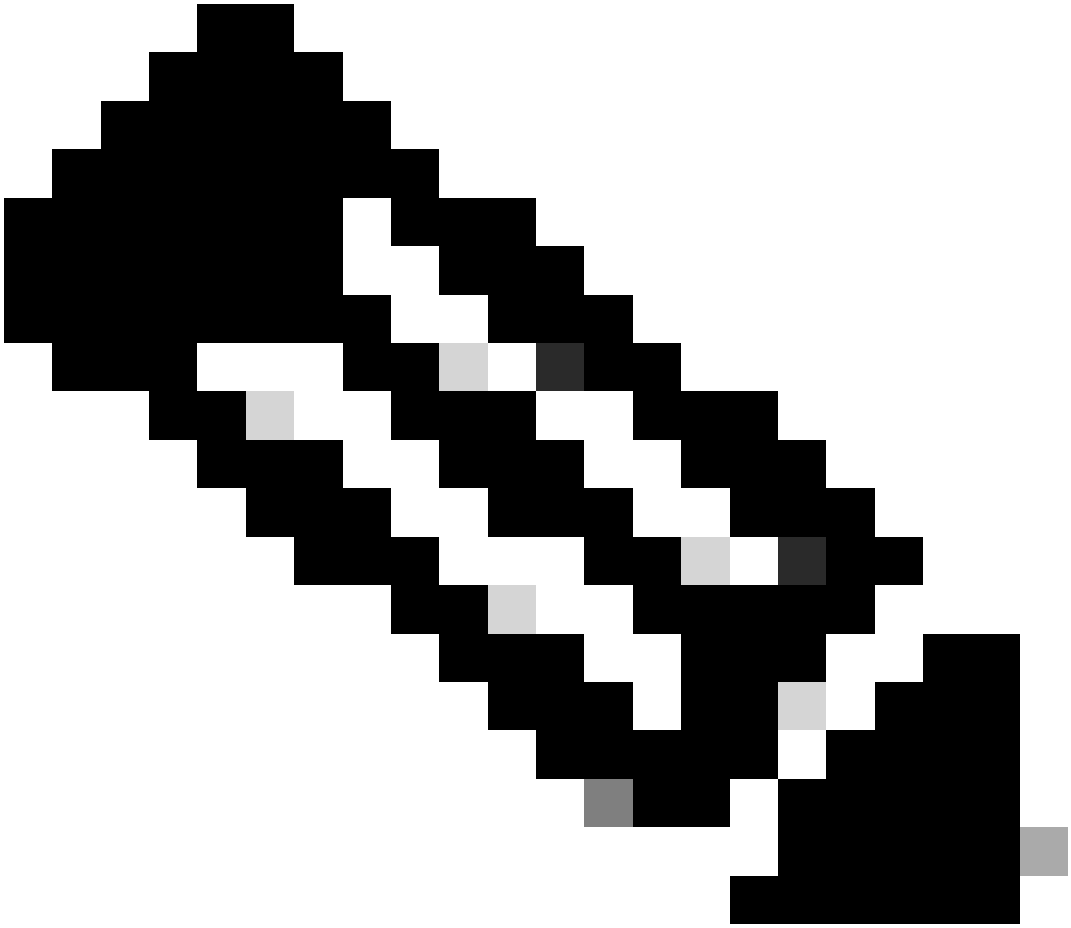
In un connettore AD è visualizzato lo stato di avviso o di errore e il messaggio elencato al passaggio del mouse sull'avviso include "Accesso negato" a uno dei server AD registrati.

Soluzione

Verificare che l'utente OpenDNS_Connector sia membro dei seguenti gruppi AD:

- Lettori registro eventi
- Utenti DCOM
- Controller di dominio di sola lettura organizzazione

La soluzione consiste nel verificare che DCOM, WMI e Gestione registro di controllo e di protezione siano configurati correttamente nel server AD in questione.



> Nota: Più domini o più foreste non sono supportati per impostazione predefinita. Fare riferimento all'annuncio Supporto di domini Multi-AD in Umbrella. È inoltre possibile contattare il supporto Umbrella per informazioni sulla configurazione per ottenere assistenza in caso di problemi.

Per verificare le autorizzazioni WMI:

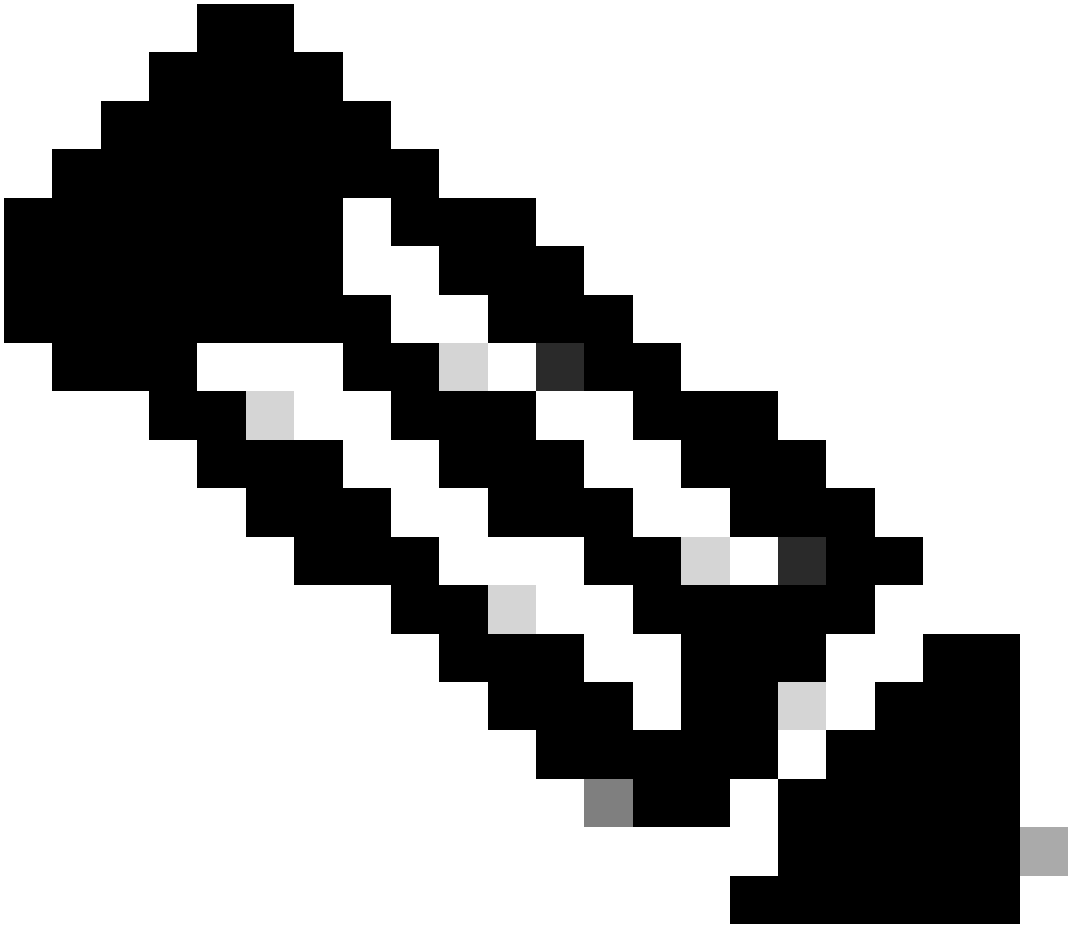
1. Selezionare Start > Esegui > wmimgmt.msc per accedere alla console di controllo di Windows Management Infrastructure.
2. Fare clic con il pulsante destro del mouse su Controllo WMI > Proprietà > scheda Protezione.

3. Selezionare Root > CIMV2 namespace e selezionare il pulsante Security.
4. Aggiungere l'utente OpenDNS_Connector e consentire le autorizzazioni seguenti:

- Abilita account
- Attivazione remota
- Sicurezza lettura

Per verificare le autorizzazioni DCOM:

1. Dalla riga di comando, eseguire dcomcnfg.
2. Passare a Radice console > Servizi componenti > Computer.
3. Fare clic con il pulsante destro del mouse su Risorse del computer e selezionare Proprietà.
4. Da Proprietà - Risorse del computer, selezionare la scheda Protezione COM.
5. Nella sezione Autorizzazioni di avvio e attivazione, selezionare Modifica limiti.
6. Aggiungere l'utente OpenDNS_Connector e consentire le autorizzazioni Avvio remoto e Attivazione remota.
7. Selezionare OK per confermare e chiudere Proprietà Risorse del computer.



Nota: Nella maggior parte dei casi, se vengono apportate modifiche DCOM, per rendere effettive le modifiche è necessario riavviare il controller di dominio.

Per verificare "Gestione registri di controllo e di protezione" sui server Windows 2003:

1. In un controller di dominio, aprire un prompt dei comandi e digitare questo comando (se si esegue Windows 2003, sostituire /r con /v):

```
gpresult /scope computer /r
```

2. Cercare la riga Oggetti Criteri di gruppo applicati. Sotto è riportato un elenco di criteri applicati a quel controller di dominio. Prendere nota di un nome che possa essere applicato a tutti i controller di dominio.
(ad esempio "Criterio controller di dominio predefiniti"). Se non ne esistono, è necessario crearne una e applicarla.

Per modificare il criterio appropriato:

3. Aprire il pannello Gestione Criteri di gruppo (tramite Start/Strumenti di amministrazione). Selezionare il criterio desiderato. È probabile che nella cartella "Controller di dominio" sia presente un elemento candidato.

4. Fare clic con il pulsante destro del mouse sul criterio e selezionare Modifica per visualizzare Editor Gestione Criteri di gruppo.

5. Accedere alla cartella Configurazione computer\Criteri\Impostazioni di Windows\Impostazioni sicurezza\Criteri locali\Assegnazione diritti utente e selezionare Gestisci registro di controllo e di sicurezza per visualizzarne le proprietà.

6. Selezionare Definisci le impostazioni relative ai criteri **>** Aggiungi utente o gruppo. Individuare e selezionare l'utente OpenDNS_Connector.

7. Eseguire il comando "gpupdate /force" sul controller di dominio per verificare che il criterio sia applicato.

Causa

Questo errore indica in genere che l'utente OpenDNS_Connector non dispone di autorizzazioni sufficienti per operare.

Lo script di Windows Connector in genere imposta le autorizzazioni necessarie per l'utente OpenDNS_Connector. Tuttavia, in ambienti AD rigorosi, ad alcuni amministratori non è consentito eseguire script VB nei controller di dominio e pertanto è necessario replicare manualmente le azioni dello script di configurazione di Windows.

Ulteriori informazioni

Per ulteriori informazioni sulla risoluzione di questo problema, visitare gli argomenti completi relativi alla risoluzione dei problemi di accesso negato.

Se dopo aver confermato/modificato le impostazioni di cui sopra, si continuano a visualizzare messaggi di accesso negato nel dashboard, inviare al supporto i log del connettore come descritto in questo articolo: Fornire supporto con i log del connettore AD.

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).