Problembehandlung bei "Zugriff verweigert" Warnung in Umbrella AD Connector

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung "Zugriff verweigert" beschrieben, wenn sich der Cisco Umbrella Active Directory (AD) Connector im Warnungs- oder Fehlerstatus befindet.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

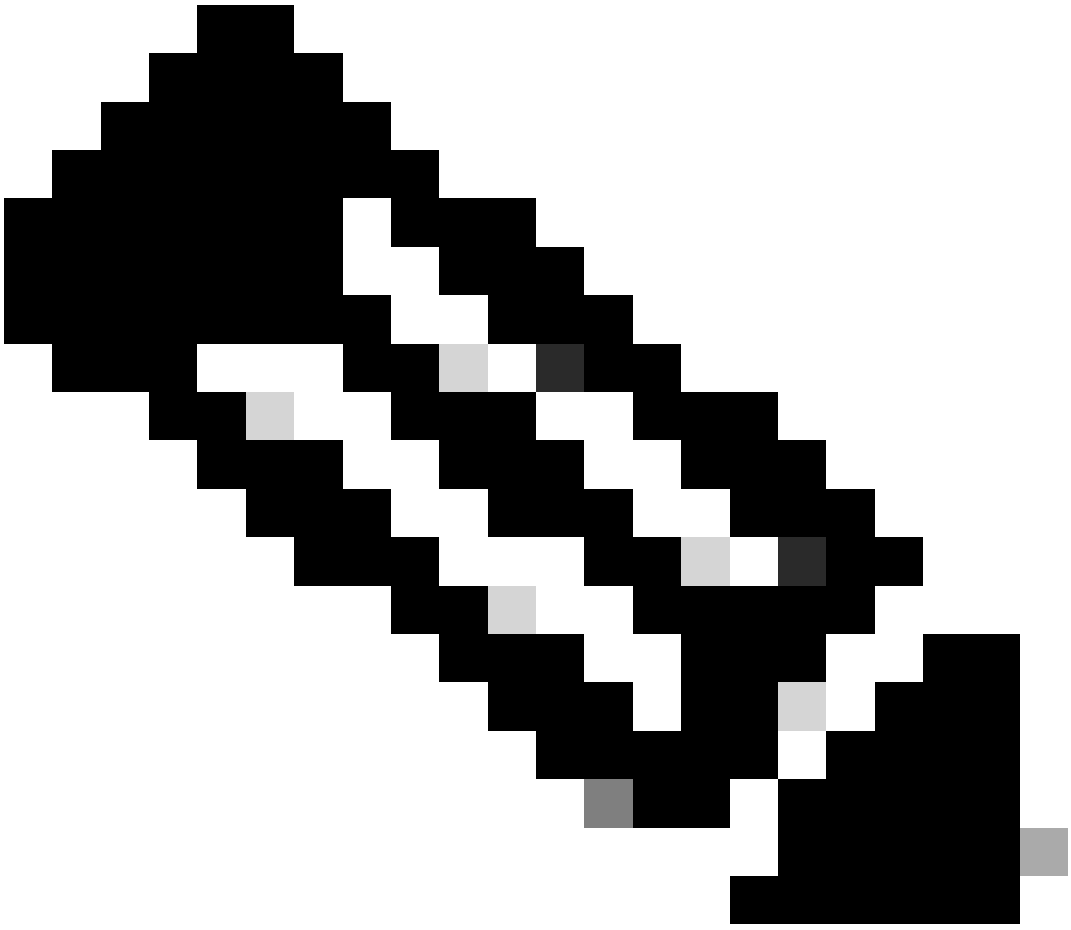
Ein AD Connector zeigt einen Alarm- oder Fehlerstatus an. Wenn Sie den Mauszeiger über die Warnung bewegen, wird die Meldung "Zugriff verweigert" auf einen der registrierten AD-Server angezeigt.

Lösung

Stellen Sie sicher, dass der OpenDNS_Connector-Benutzer Mitglied dieser AD-Gruppen ist:

- Ereignisprotokollleser
- Verteilte COM-Benutzer
- Enterprise Read-only-Domänencontroller

Die Lösung besteht darin, sicherzustellen, dass DCOM, WMI und Manage Audit and Security Log auf dem betreffenden AD-Server richtig eingerichtet sind.



> Anmerkung: Standardmäßig werden mehrere Domänen oder Gesamtstrukturen nicht unterstützt. Weitere Informationen finden Sie in der Multi-AD Domain Support in Umbrella Ankündigung. Sie können sich bezüglich Ihrer Konfiguration auch an den Umbrella Support wenden, um Unterstützung zu erhalten, wenn diese Probleme auftreten.

So überprüfen Sie WMI-Berechtigungen:

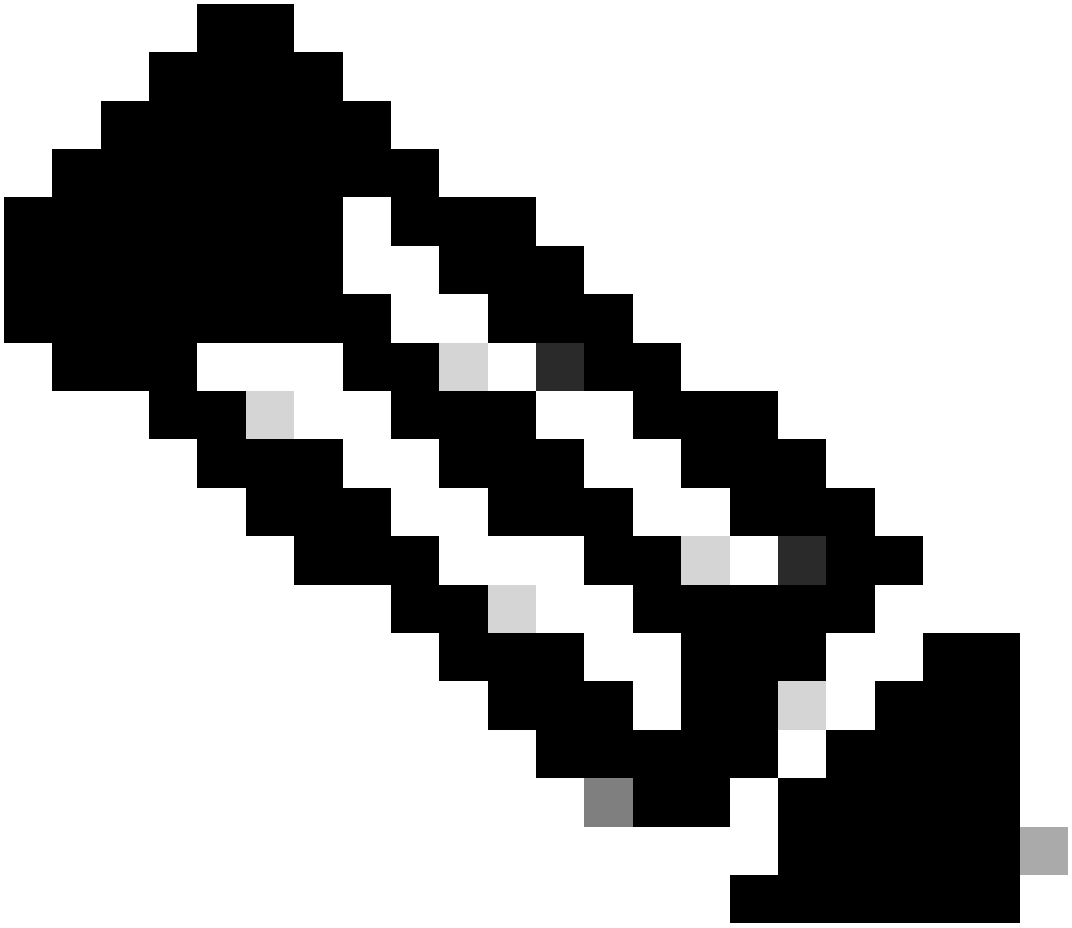
1. Wählen Sie Start > Ausführen > wmimgmt.msc, um auf die Windows Management

Infrastructure Control-Konsole zuzugreifen.
2. Klicken Sie mit der rechten Maustaste auf WMI-Steuerelement > Eigenschaften > Registerkarte Sicherheit.
3. Wählen Sie Root > CIMV2-Namespace aus, und klicken Sie auf die Schaltfläche Security.
4. Fügen Sie den Benutzer OpenDNS_Connector hinzu und lassen Sie folgende Berechtigungen zu:

- Konto aktivieren
- Remote-Aktivierung
- Sicherheit lesen

So überprüfen Sie die DCOM-Berechtigungen:

1. Führen Sie dcomcnfg über eine Befehlszeile aus.
2. Navigieren Sie zu Konsolenstamm > Komponentendienste > Computer.
3. Klicken Sie mit der rechten Maustaste auf Arbeitsplatz und wählen Sie Eigenschaften.
4. Wählen Sie aus Eigenschaften von Arbeitsplatz die Registerkarte COM-Sicherheit.
5. Wählen Sie im Abschnitt Launch and Activation Permissions die Option Edit Limits.
6. Fügen Sie den OpenDNS_Connector-Benutzer hinzu, und erlauben Sie Berechtigungen für Remote-Start und Remote-Aktivierung.
7. Wählen Sie OK, um die Eigenschaften von Arbeitsplatz zu bestätigen und zu schließen.



Anmerkung: In den meisten Fällen ist bei DCOM-Änderungen ein Neustart des DC erforderlich, damit die Änderungen wirksam werden.

So überprüfen Sie "Überwachungs- und Sicherheitsprotokolle verwalten" auf Windows 2003-Servern:

1. Öffnen Sie auf einem Domänencontroller eine Eingabeaufforderung, und geben Sie diesen Befehl ein (wenn Sie Windows 2003 ausführen, ersetzen Sie /r durch /v):

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

2. Suchen Sie nach der Zeile Angewandte Gruppenrichtlinienobjekte. Darunter befindet sich eine Liste der Richtlinien, die auf diesen Domänencontroller angewendet werden. Notieren Sie sich einen, der auf alle Domänencontroller angewendet werden kann.
(wie "Standard-Domänencontrollerrichtlinie"). Wenn keine vorhanden sind, müssen Sie eine

erstellen und anwenden.

So bearbeiten Sie die entsprechende Richtlinie:

3. Öffnen Sie den Bereich Gruppenrichtlinienverwaltung (über Start/Verwaltung). Wählen Sie die gewünschte Richtlinie aus. Etwas im Ordner "Domain Controller" ist ein wahrscheinlicher Kandidat.

4. Klicken Sie mit der rechten Maustaste auf diese Richtlinie, und wählen Sie Bearbeiten aus, um den Gruppenrichtlinienverwaltungs-Editor aufzurufen.

5. Navigieren Sie zum Ordner Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten, und wählen Sie Überwachungs- und Sicherheitsprotokoll verwalten aus, um dessen Eigenschaften anzuzeigen.

6. Wählen Sie Diese Richtlinieneinstellungen definieren > Benutzer oder Gruppe hinzufügen aus. Durchsuchen Sie den OpenDNS_Connector-Benutzer, und wählen Sie ihn aus.

7. Führen Sie den Befehl "gpupdate /force" auf dem Domänencontroller aus, um sicherzustellen, dass die Richtlinie angewendet wird.

Ursache

Dieser Fehler weist in der Regel darauf hin, dass der OpenDNS_Connector-Benutzer nicht über ausreichende Berechtigungen für den Betrieb verfügt.

Das Windows Connector-Skript legt normalerweise die erforderlichen Berechtigungen für den OpenDNS_Connector-Benutzer fest. In strikten AD-Umgebungen ist es einigen Administratoren jedoch nicht gestattet, VB-Skripts auf ihren Domänencontrollern auszuführen, und sie müssen daher die Aktionen des Windows-Konfigurationsskripts manuell replizieren.

Zusätzliche Informationen

Weitere Informationen zur Behebung dieses Problems finden Sie unter Vollständige Themen zur Behebung von Zugriffsverweigerungen.

Wenn Sie nach der Bestätigung/Änderung der oben genannten Einstellungen im Dashboard immer noch die Meldung "Zugriff verweigert" sehen, senden Sie bitte Support für die Connector-Protokolle wie in diesem Artikel beschrieben: Support für AD Connector-Protokolle bereitstellen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.