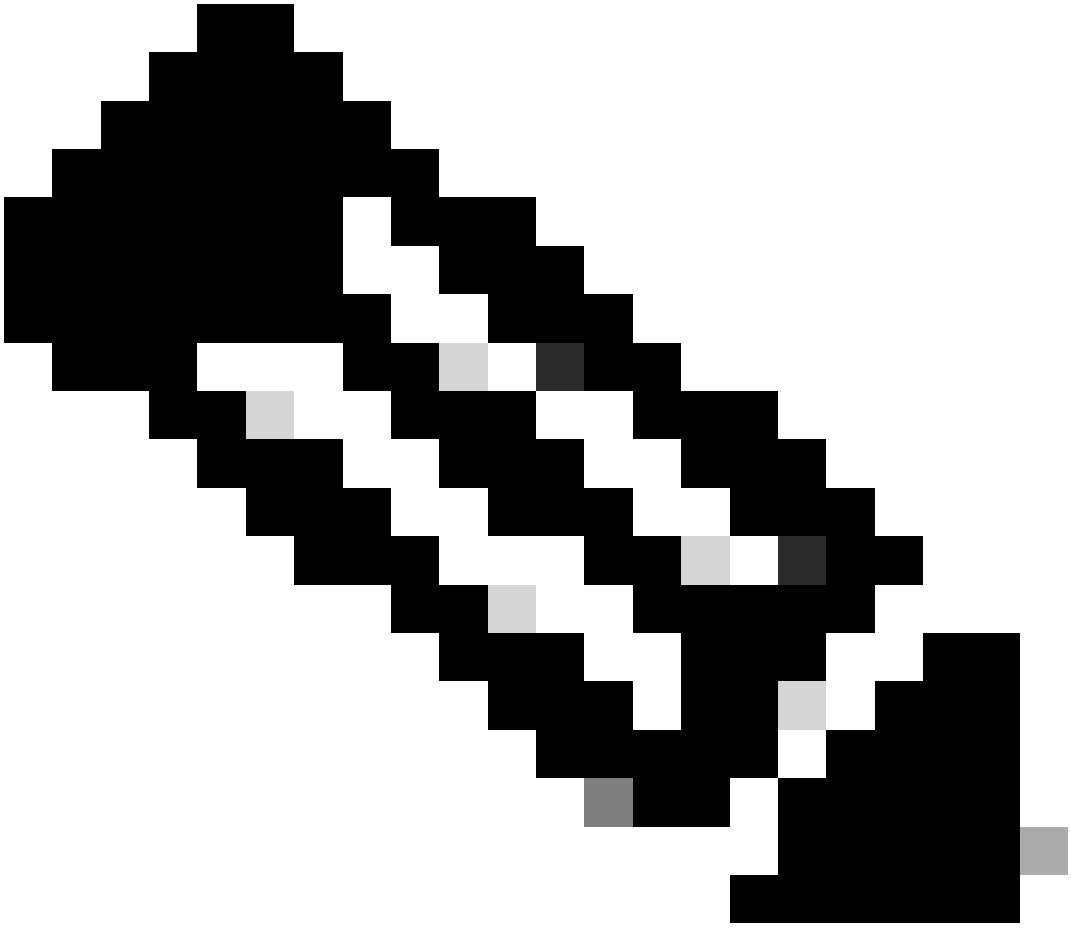
Erforderliche Berechtigungen für den OpenDNS_Connector-Benutzer verstehen

Inhalt

Einleitung

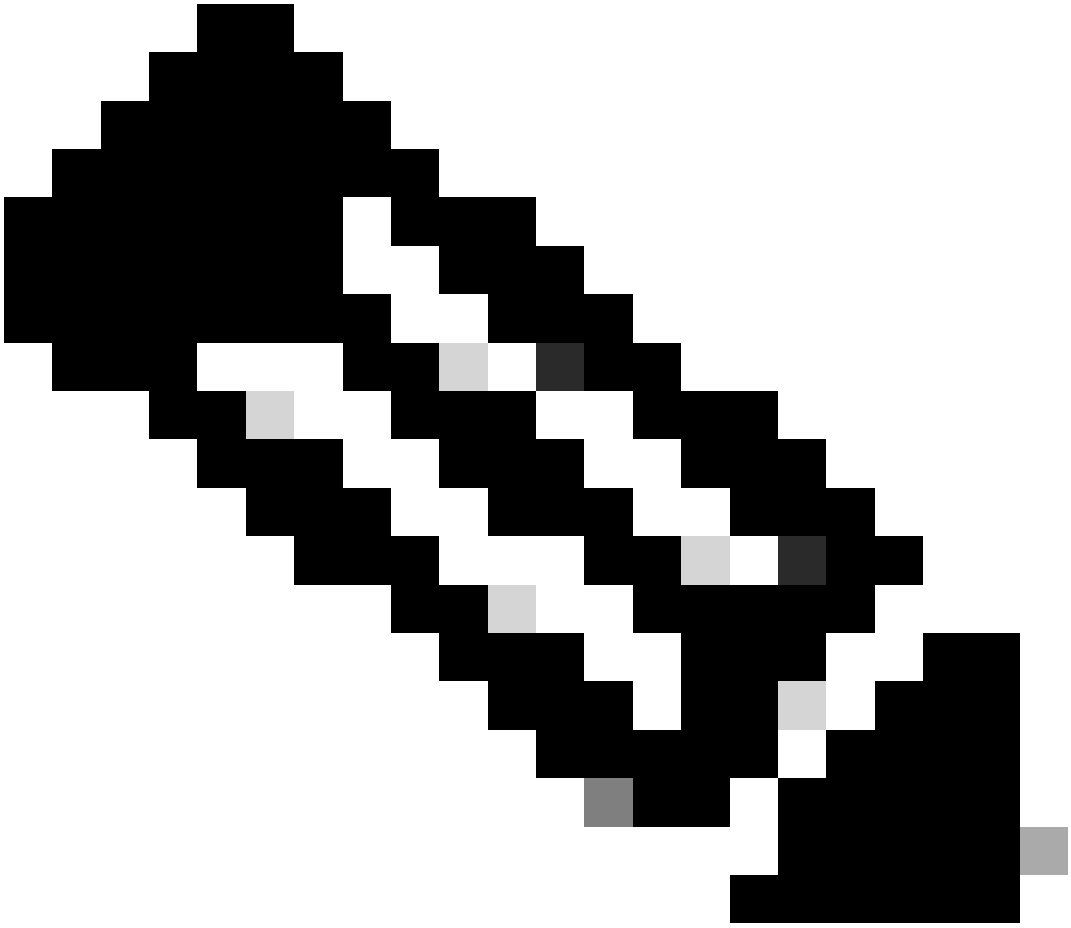
In diesem Dokument werden die erforderlichen Berechtigungen für OpenDNS_Connector-Benutzer beschrieben.



Anmerkung: Entsprechend der Bemühungen zum Rebranding wurde der vermutete AD-Benutzername "OpenDNS_Connector" vor kurzem dahingehend aktualisiert, dass er jetzt "Cisco_Connector" lautet.

Überblick

Das Windows Connector-Skript legt normalerweise die erforderlichen Berechtigungen für den Benutzer Cisco_Connector fest. In Umgebungen mit strikten AD-Vorgaben ist es einigen Administratoren jedoch u. U. nicht gestattet, VB-Skripts auf ihren Domänencontrollern auszuführen. Daher müssen sie die Aktionen des Windows-Konfigurationsskripts manuell replizieren. In diesem Artikel wird erläutert, welche Berechtigungen auf dem Rechenzentrum festgelegt werden müssen.



Anmerkung: Für die Zwecke dieses Artikels wird davon ausgegangen, dass Cisco_Connector der sAMAccountName Ihres Connector-Kontos in AD ist. Wenn Sie stattdessen einen benutzerdefinierten Namen verwenden, verwenden Sie die gleichen Anweisungen für den sAMAccountName des Connector-Kontos anstelle von Cisco_Connector.

Wenn der Benutzer Cisco_Connector nicht über ausreichende Berechtigungen für den Betrieb verfügt, zeigt ein AD Connector im Dashboard einen Warn- oder Fehlerstatus an, und die Meldung, die beim Bewegen des Mauszeigers über die Warnung angezeigt wird, lautet Zugriff verweigert auf einen der registrierten Domänencontroller.

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

- Enterprise Read-only-Domänencontroller
- Ereignisprotokollleser (nur wenn die Bereitstellung virtuelle Appliances umfasst)

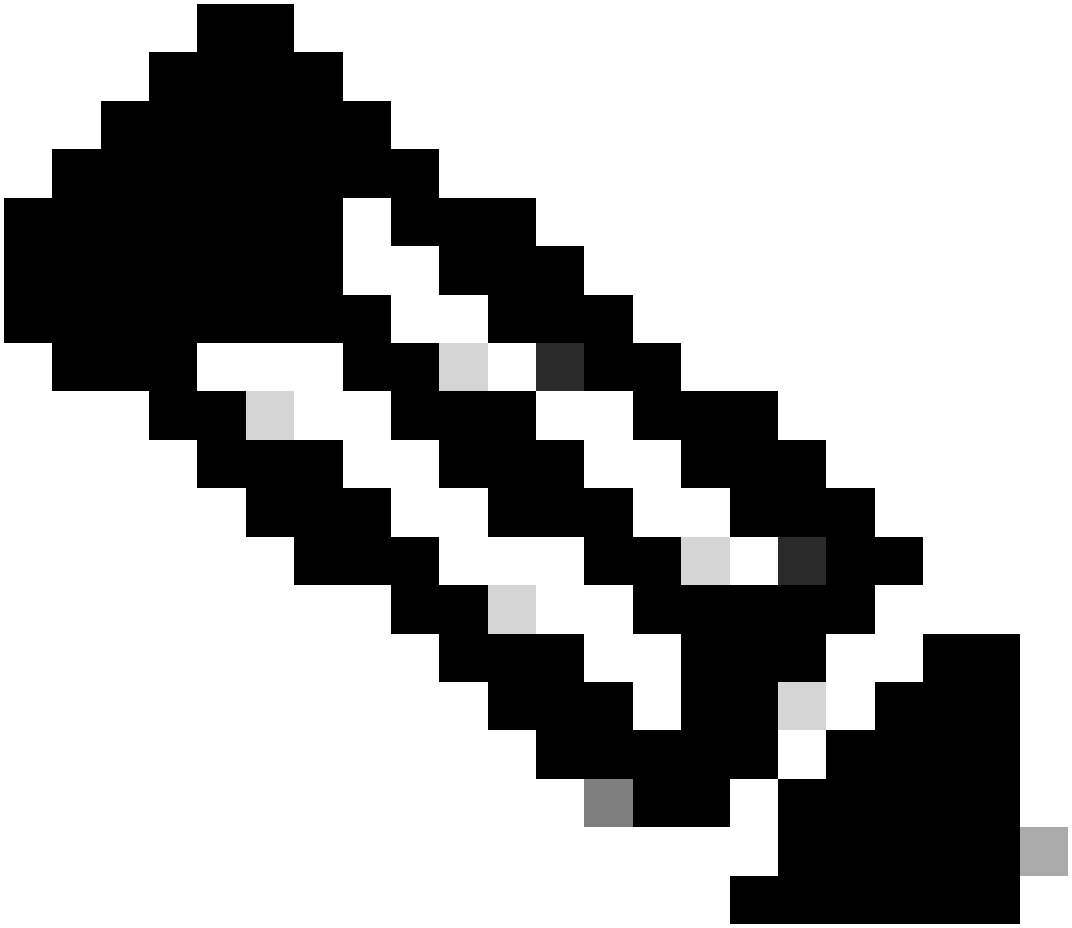
Darüber hinaus muss der Benutzer Cisco_Connector den Gruppen "Domain Users"

(Domänenbenutzer) und "Users" (Benutzer) angehören. Sie können die Gruppenmitgliedschaft des Cisco_Connector-Benutzers mit dem folgenden Befehl überprüfen:

dsquery-Benutzer - samid Cisco_Connector | dsget user -member of -expand

Der Umbrella AD Connector führt zwei primäre Aufgaben aus, für die diese Berechtigungen erforderlich sind. Zunächst werden LDAP-Informationen aus Active Directory abgerufen, damit Sie auf der Grundlage der AD-Gruppe Richtlinien erstellen und AD-Benutzernamen und Gruppennamen im Umbrella Dashboard anzeigen können. Die Berechtigung `Verzeichnisänderungen replizieren` ermöglicht dies.

Anschließend werden die Anmeldeereignisse von den Domänencontrollern erfasst und an die virtuellen Appliances weitergeleitet. Dadurch können die virtuellen Appliances ihre IP-to-User-Zuordnungen erstellen und Benutzer identifizieren. Alle Berechtigungen gelten für diese mit Ausnahme der Berechtigung `Verzeichnisänderungen replizieren`. Diese Berechtigungen sind nur erforderlich, wenn die Bereitstellung virtuelle Appliances in derselben Umbrella-Site wie die Domänencontroller umfasst.



Anmerkung: Zusätzlich zum Festlegen der erforderlichen Berechtigungen für den Benutzer Cisco_Connector registriert das Konfigurationsskript des Domänencontrollers auch einen Domänencontroller, indem es API-Aufrufe an Umbrella ausgibt. Wenn Sie die Berechtigungen manuell ändern, anstatt das Konfigurationsskript zu verwenden, muss diese Registrierung ebenfalls manuell durchgeführt werden. In der Umbrella-Dokumentation erfahren Sie, wie Sie dem Umbrella Dashboard manuell Domänencontroller hinzufügen.

Erforderliche Berechtigungen

- Verzeichnisänderungen replizieren
- Ereignisprotokollleser
- Remote-Administrator
- Überwachungsrichtlinie

Verzeichnisänderungen replizieren

Mit dieser Berechtigung kann der Benutzer Cisco_Connector LDAP abfragen. Dies ist die erforderliche Berechtigung, die normalerweise von der Gruppe "Schreibgeschützte Enterprise-Domänencontroller" erteilt wird. Auf diese Weise erhält das Umbrella Dashboard die Informationen, die erforderlich sind, um die Namen von AD-Objekten anzuzeigen und Gruppenmitgliedschaften zu bestimmen. Der Connector fordert folgende Attribute an:

`cn`: Der gebräuchliche Name

`dn`: Der Distinguished Name

`dNSHostName`: Der Gerätename, wie er in DNS registriert ist.

`mail`: Dem Benutzer zugeordnete E-Mail-Adressen

`memberOf`: Die Gruppen, die den Benutzer enthalten.

`objectGUID`: Die Gruppen-ID des Objekts. Diese Eigenschaft wird als Hash an Secure Access gesendet.

`primaryGroupId`: Die primäre Gruppen-ID, die für Benutzer und Gruppen verfügbar ist.

`primaryGroupToken`: Das primäre Gruppentoken, das nur für Gruppen verfügbar ist. Kennwörter oder Passwort-Hashes werden nicht abgerufen. Secure Access nutzt die

`primaryGroupToken`-Daten in der Zugriffsrichtlinie, Konfiguration und Berichterstellung. Diese Daten sind auch für die Filterung durch jeden Benutzer oder Computer erforderlich.

`sAMAccountName`: Der Benutzername, mit dem Sie sich bei Cisco AD Connector anmelden.

`userPrincipalName`

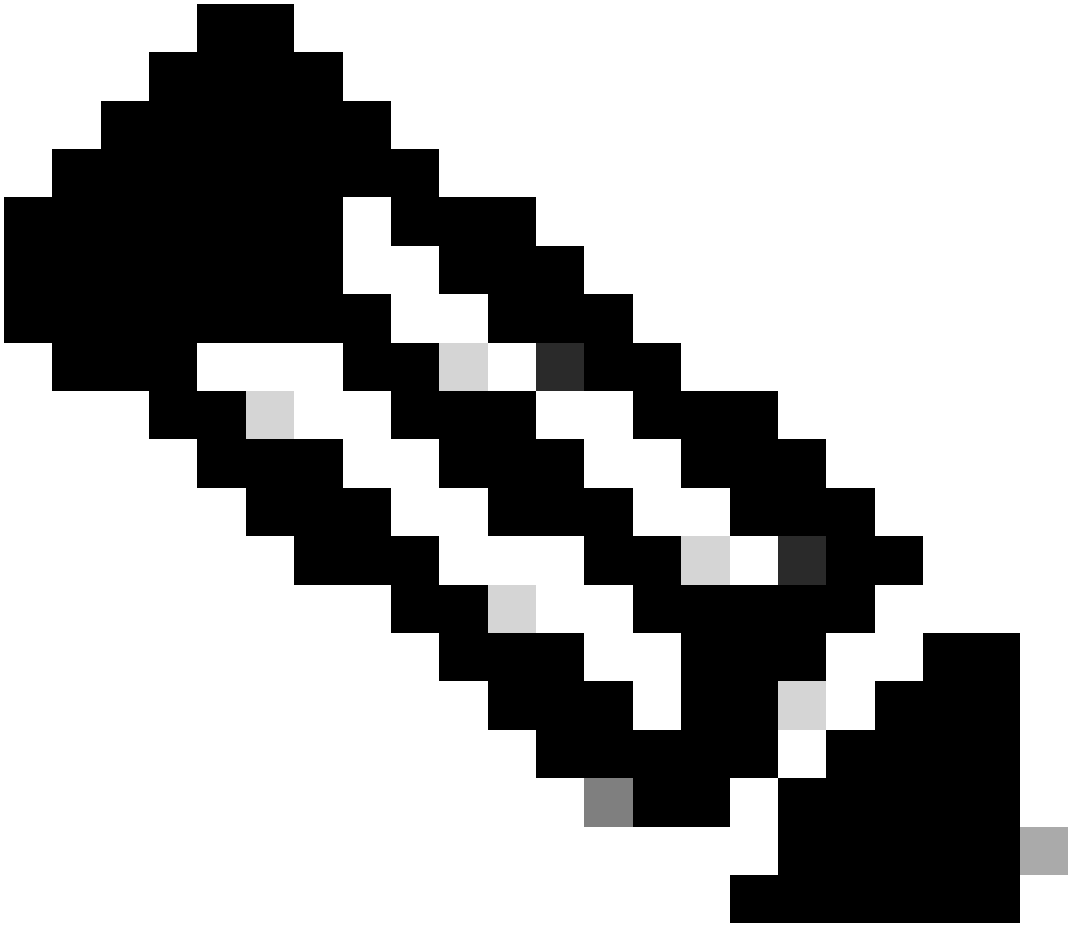
: Der Hauptname des Benutzers.

Aus diesen objectClasses:

```
(&(objectCategory=person)(objectClass=user))
(objectClass=organizationalunit)
(objectClass=computer)
(objectClass=group)
```

Die integrierte Gruppe "Schreibgeschützte Enterprise-Domänencontroller" muss diese Berechtigung bereitstellen. Der Benutzer Cisco_Connector muss daher Mitglied dieser Gruppe sein. Sie können die Berechtigungen der Gruppe überprüfen oder die Berechtigungen speziell für den Benutzer Cisco_Connector angeben (wenn die Gruppe diese Berechtigungen nicht bereitstellt):

- Öffnen des Snap-Ins "Active Directory-Benutzer und -Computer"
- Klicken Sie im Menü Ansicht auf Erweiterte Funktionen.
- Klicken Sie mit der rechten Maustaste auf das Domänenobjekt, z. B. "company.com", und klicken Sie dann auf Eigenschaften.
- Wählen Sie auf der Registerkarte Sicherheit entweder "Enterprise Read-only Domain Controllers" oder den Benutzer "Cisco_Connector" aus.
    - Bei Bedarf können Sie den Benutzer "Cisco_Connector" hinzufügen, indem Sie auf "Hinzufügen" klicken.
    - Wählen Sie im Dialogfeld Benutzer, Computer oder Gruppen auswählen das gewünschte Benutzerkonto aus, und klicken Sie dann auf Hinzufügen.
    - Klicken Sie auf OK, um zum Dialogfeld Eigenschaften zurückzukehren.
- Aktivieren Sie in der Liste die Kontrollkästchen Verzeichnisänderungen replizieren und Lesen.
- Klicken Sie auf Übernehmen und dann auf OK.
- Schließen Sie das Snap-In.

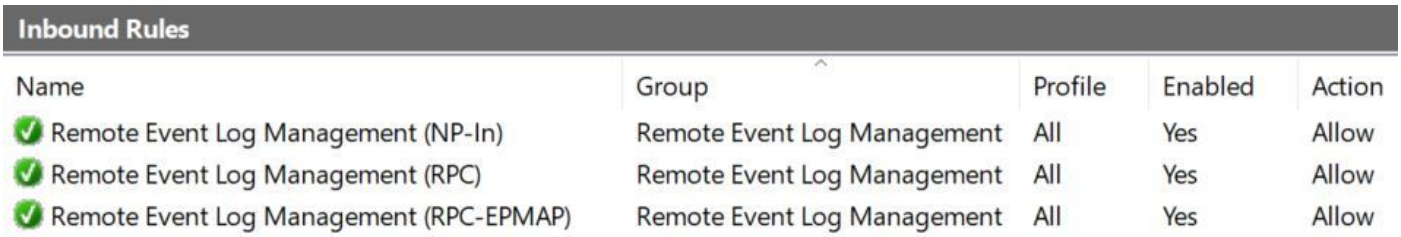


Anmerkung: In einem Parent/Child-Domänenszenario ist der "Enterprise Read-only Domain Controller" nur in der übergeordneten Domäne vorhanden. In diesem Fall müssen die Berechtigungen für Cisco_Connector manuell hinzugefügt werden, wie dargestellt.

Ereignisprotokollleser

Diese Änderung ist nur erforderlich, wenn die Bereitstellung virtuelle Appliances im selben Umbrella-Standort wie den Domain Controller umfasst. Durch die Mitgliedschaft in dieser Gruppe kann der Benutzer von Cisco_Connector die Anmeldeereignisse aus den Ereignisprotokollen lesen.

Auf dem Domänencontrollercomputer stellen die erweiterten Windows-Firewalleinstellungen sicher, dass die eingehenden Regeln für die Remoteereignisprotokollverwaltung (NP-In, RPC und RPC-EPMAP) zulässig sind. Der Umbrella AD Connector protokolliert möglicherweise einen Fehler mit der Meldung "Der RPC-Server ist nicht verfügbar" und kann möglicherweise keine Anmeldeereignisse lesen, wenn diese Regeln nicht zulässig sind.



360090909832

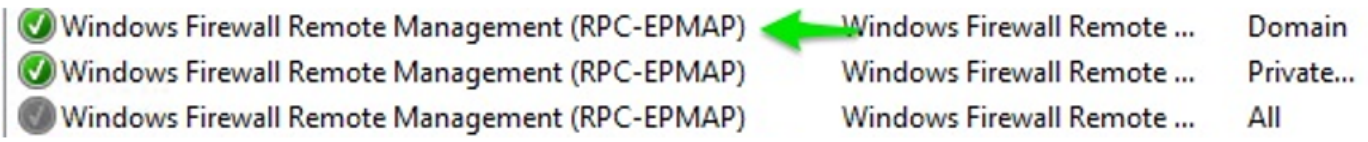
Sie können diese Regeln auch mit dem folgenden Befehl aktivieren:netsh advfirewall set rule group="Remote Event Log Management" new enable=yes

Remote-Administrator

Die Remote-Verwaltung ist erforderlich, damit der Connector Anmeldeereignisse auf dem Domänencontroller lesen kann. Diese Berechtigung ist nur erforderlich, wenn die Bereitstellung virtuelle Appliances in demselben Umbrella-Standort wie den Domänencontroller umfasst.

Führen Sie an der Eingabeaufforderung folgende Befehle aus:

```
netsh advfirewall firewall set rule group="remote administration" new enable=yes
netsh advfirewall set currentprofile settings remotemanagement enable
```



4413613529492

Überwachungsrichtlinie

Diese Änderung ist nur erforderlich, wenn die Bereitstellung virtuelle Appliances im selben Umbrella-Standort wie den Domain Controller umfasst. Die Überwachungsrichtlinie definiert, welche Ereignisse im Ereignisprotokoll des Domänencontrollers protokolliert werden. Der Connector erfordert, dass Anmeldeversuche aufgezeichnet werden, damit Benutzer ihren IP-Adressen zugeordnet werden können.

In normalen Windows Server 2008+-Umgebungen muss die Einstellung "Anmeldeversuche überwachen" konfiguriert werden. Insbesondere muss die Richtlinie "Anmeldeereignisse überwachen" auf "Erfolg" gesetzt werden. Dies kann überprüft werden, indem der folgende Befehl an einer Eingabeaufforderung ausgeführt wird:

```
GPRESULT /z
```

Diese Richtlinie wird als Gruppenrichtlinienobjekt definiert. Bearbeiten Sie zum Ändern die entsprechende Gruppenrichtlinie für das Rechenzentrum (in der Regel die "Standard-Domänencontrollerrichtlinie"), und legen Sie fest, dass diese Richtlinie "Success"-Ereignisse enthält:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit lo
```

Stellen Sie sicher, dass Sie die Gruppenrichtlinie im Rechenzentrum aktualisieren, nachdem Sie diese Änderung vorgenommen haben.

Windows Server 2008 hat jedoch auch die erweiterte Überwachungsrichtlinienkonfiguration eingeführt. Die älteren Windows-Überwachungsrichtlinien können zwar weiterhin verwendet werden, sie werden jedoch ignoriert, wenn eine der erweiterten Überwachungsrichtlinien definiert ist. In der Microsoft-Dokumentation erfahren Sie, wie die beiden Überwachungsrichtlinien interagieren.

Für die Zwecke des Connectors MÜSSEN die erweiterten Überwachungsrichtlinien verwendet werden, wenn erweiterte Überwachungsrichtlinien definiert sind (einschließlich solcher, die nicht speziell mit der Anmeldung zusammenhängen).

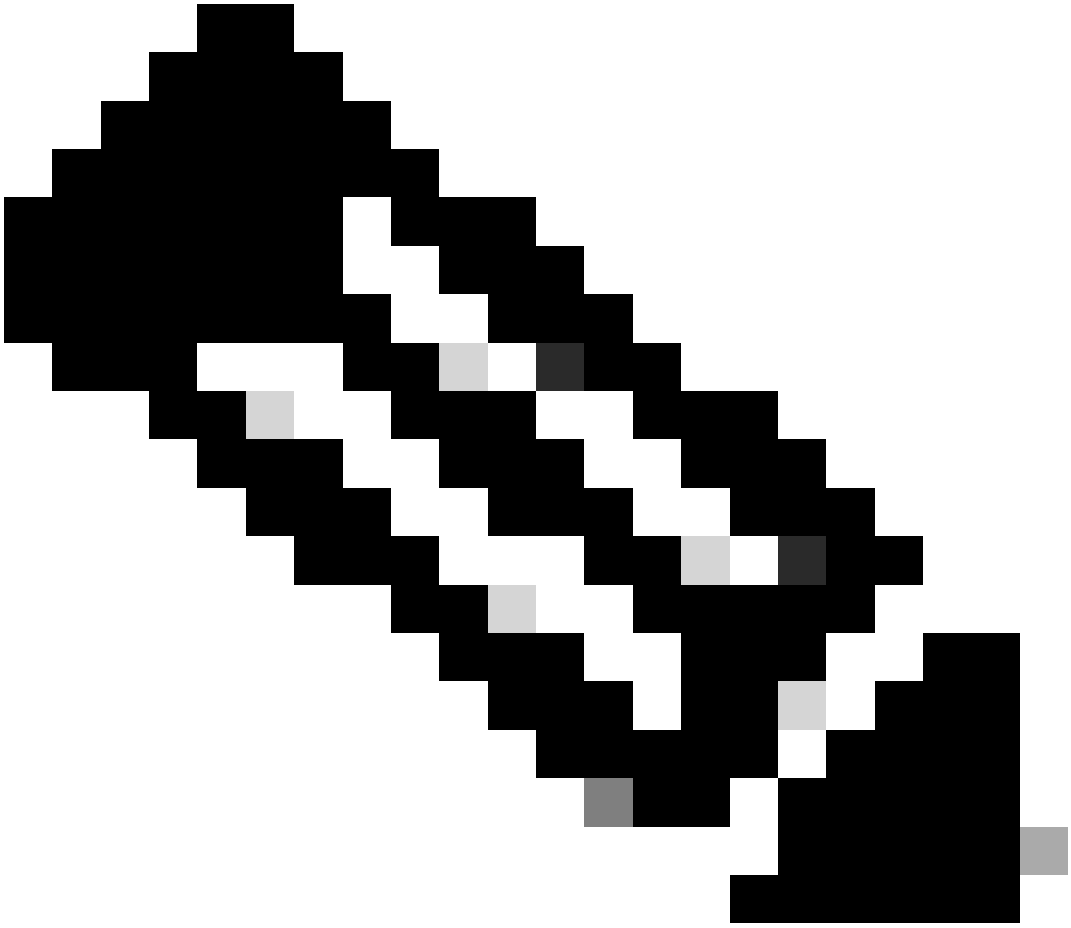
Die erweiterte Überwachungsrichtlinie muss für alle Rechenzentren festgelegt werden, die die Gruppenrichtlinie verwenden. Bearbeiten Sie die entsprechende Gruppenrichtlinie für Ihr Rechenzentrum (in der Regel die "Standard-Domänencontrollerrichtlinie"), und gehen Sie zu folgendem Abschnitt:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\
```

Legen Sie in diesem Abschnitt fest, dass diese Richtlinien sowohl Erfolgs- als auch Fehlerereignisse enthalten:

```
Audit Logon
Audit Logoff
Audit Other Logon/Logoff Events
```

Stellen Sie sicher, dass Sie die Gruppenrichtlinie im Rechenzentrum aktualisieren, nachdem Sie diese Änderung vorgenommen haben.



Anmerkung: Wenn Sie den AD Connector mit virtuellen Appliances bereitstellen, müssen die Firewall-Regeländerungen und Überwachungsrichtlinieneinstellungen auf allen Domänencontrollern in der Domäne vorgenommen werden, mit der der Connector kommuniziert.

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

Wenn Sie diese Informationen für den Support bereitstellen, geben Sie die folgenden beiden Befehle aus:

```
auditpol.exe /get /category:* > DCNAME_auditpol.txt
GPRESULT /H DC_NAME.htm
```

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.