Windows DC-Konfigurationsskript verstehen

Inhalt

Einleitung

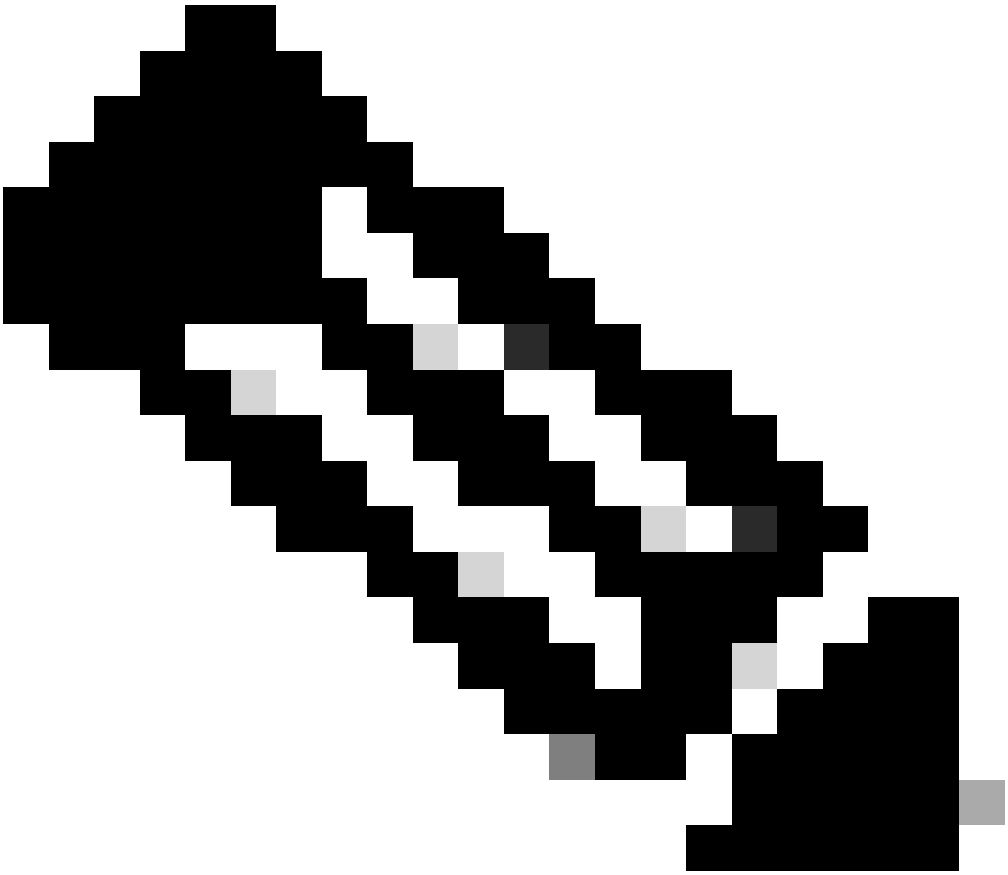
Dieses Dokument beschreibt die Änderungen an Ihrer Windows-Umgebung, die durch unser Konfigurationsskript für den Domänencontroller vorgenommen werden.

- Grundlegende Voraussetzungen finden Sie in der Insights-Dokumentation: https://docs.umbrella.com/deployment-umbrella/docs/2-prerequisites
- Ausführliche Informationen zum manuellen Festlegen dieser Berechtigungen finden Sie in diesem Artikel: Erforderliche Berechtigungen für den OpenDNS_Connector-Benutzer.

Übersicht über das DC-Konfigurationsskript

Jeder Domänencontroller erfordert eine einmalige Registrierung bei der Umbrella API/dem Dashboard. Unser Konfigurationsskript für das Rechenzentrum initiiert dies zusammen mit den folgenden Funktionen:

1. Überprüfen der erforderlichen Berechtigungen und der Konfiguration der Firewall-Regeln
2. (Optional) Diese Berechtigungen automatisch konfigurieren
3. (Optional) Registrieren Sie den Domain Controller nur dann beim Umbrella API/Dashboard, wenn diese Prüfungen erfolgreich waren.



Anmerkung: Eine Liste der Domänencontroller kann auch manuell vom Umbrella-Support registriert werden. Dies ist in der Regel nützlich in Szenarien, in denen die API / Internet-Zugang ist nicht möglich für den Domain-Controller. Die beschriebenen Berechtigungsänderungen MÜSSEN jedoch weiterhin konfiguriert werden, daher wird die Ausführung des Konfigurationsskripts weiterhin nachdrücklich empfohlen.

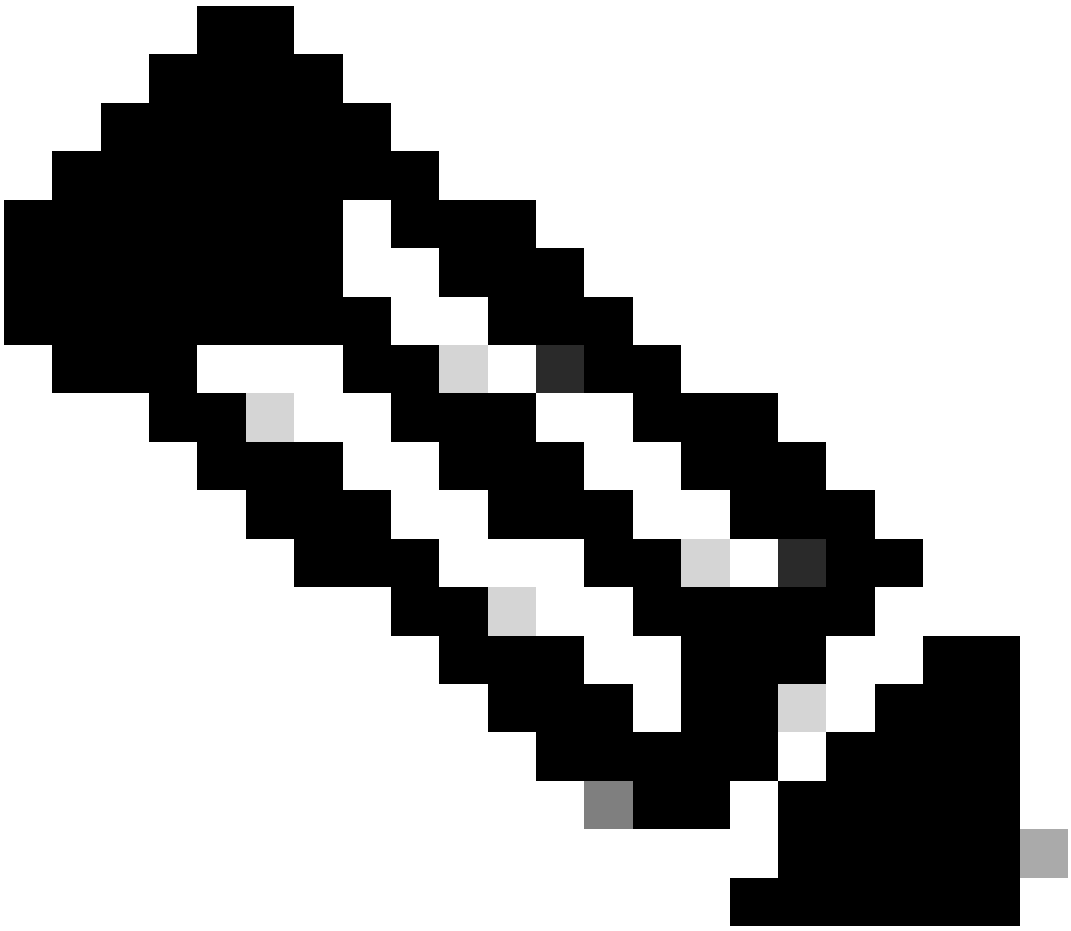
Beim Ausführen des Skripts werden zunächst keine Änderungen an der Umgebung vorgenommen. Das Skript überprüft, ob alle erforderlichen Berechtigungen vorhanden sind. Wenn ein Problem auftritt, werden Sie aufgefordert (`J/N`), Änderungen vorzunehmen.

Nach Abschluss des Registrierungsskripts ist keine Software erforderlich, um auf dem Domänencontroller selbst ausgeführt zu werden. Der OpenDNS Connector-Dienst muss jedoch auf mindestens einem Computer installiert sein (z. B. Domänencontroller oder Mitgliedsserver).

Phase 1 - Tests

Das Skript erfasst zunächst folgende Informationen:

- Überprüft die Betriebssystemversion und die Gesamtstruktur-Funktionsebene.
- Überprüft, ob das Skript als Administrator ausgeführt wird.
- Ruft die Informationen zu IP-Adresse, Hostname und Domänenname des Servers ab
- Überprüfen Sie, ob die Windows-Firewall aktiviert ist und ob die integrierte Regel "Remoteverwaltung" zulässig ist.
- Sucht nach dem erforderlichen Domänenbenutzerkonto 'OpenDNS_Connector'



> Anmerkung: Wenn der OpenDNS_Connector-Benutzer nicht vorhanden ist, druckt das Skript die Ergebnisse und bricht ab. Dieser Domänenbenutzer muss manuell erstellt werden, bevor das Skript ausgeführt wird. Wenn das OpenDNS_Connector-Konto vorhanden ist, wird das Skript mit diesen Prüfungen fortfahren.

- Überprüft, ob der OpenDNS_Connector-Benutzer über Berechtigungen für 'Remote Enable' und 'Read Security' im WMI-Namespace root\cimv2 verfügt.
- Überprüft, ob das OpenDNS_Connector-Konto über die Active Directory-Berechtigung

"Änderungen am Replikationsverzeichnis" verfügt, die normalerweise durch die Mitgliedschaft in der Gruppe der schreibgeschützten Enterprise-Domänencontroller gewährt wird.
- Überprüft, ob das OpenDNS_Connector-Konto Mitglied der Gruppe "Ereignisprotokollleser" ist.
- Überprüft, ob das OpenDNS_Connector-Konto Mitglied der Gruppe "Verteilte COM-Benutzer" ist
- Prüft den resultierenden Richtliniensatz (RSOP), um festzustellen, ob "Anmeldeereignisse überwachen" über die Gruppenrichtlinie aktiviert ist.
- Überprüft den resultierenden Richtliniensatz (RSOP), um festzustellen, ob dem OpenDNS_Connector-Konto das Recht "Überwachungs- und Sicherheitsprotokoll verwalten" zugewiesen wurde.

Phase 1b - Testergebnisse

Die vom Konfigurationsskript gedruckten Ergebnisse unterscheiden sich je nach Betriebssystemversion.

Auf Server 2003 und neuer werden folgende Ergebnisse angezeigt:

```
AD User Exists:                true/false
WMI Permissions Set:           true/false
DCOM Permissions Set:          true/false
RDC Permissions Set:           true/false
Audit Policy Set:              true/false
Manage Event Log Policy Set:   true/false
Distributed COM MemberOf:      true/false
```

Auf Server 2008 und höher (nur wenn die Gesamtstrukturfunktionsebene 2008+ ist) werden diese Informationen ebenfalls angezeigt. (Diese Gruppe ist in früheren Versionen nicht vorhanden.):

```
Event Log Readers MemberOf:     true/false
```

Phase 2 - Änderungen der automatischen Konfiguration

Wenn diese Überprüfung fehlschlägt, werden Sie gefragt `"Möchten Sie, dass wir diesen Domänencontroller (J oder N) automatisch konfigurieren?"` bevor Sie Änderungen vornehmen.

Diese Änderungen werden vorgenommen:

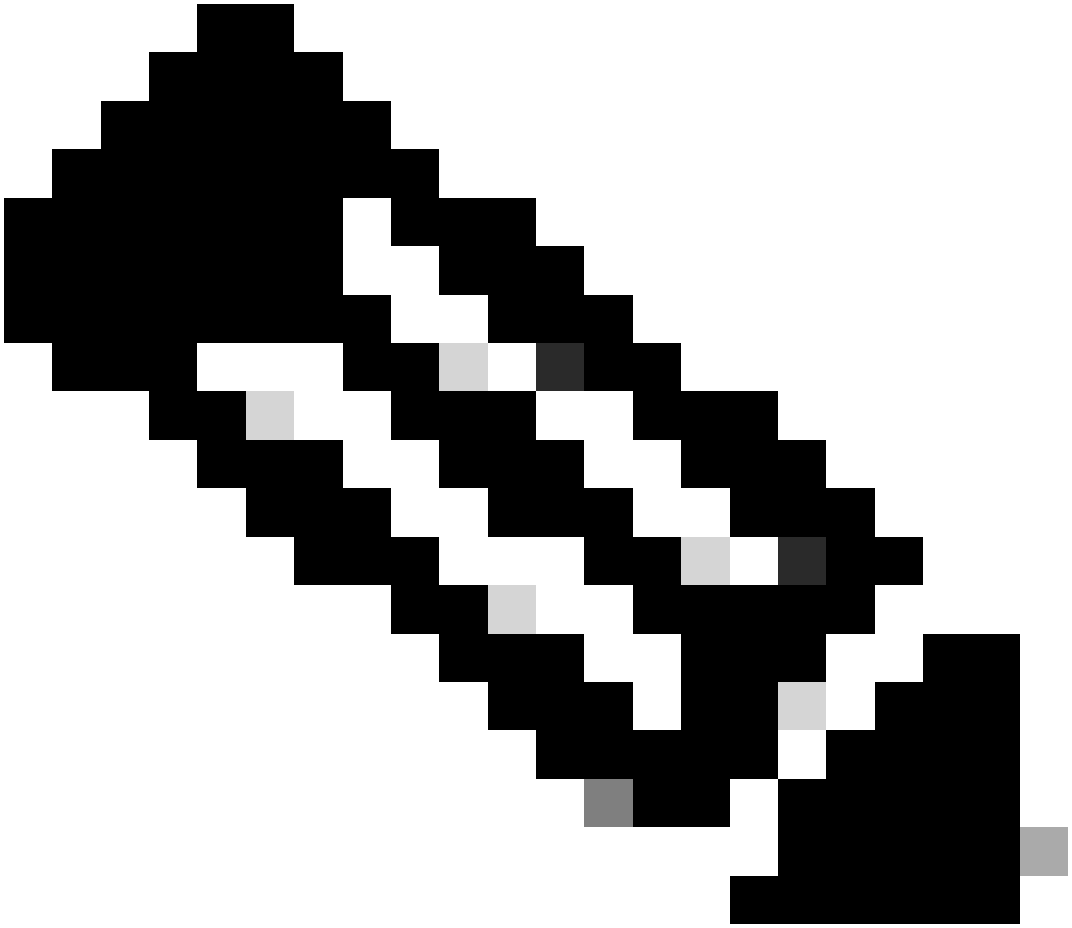
- Aktiviert bei Bedarf die integrierte Windows-Firewall-Regel "Remoteverwaltung"
- Gewährt explizit die Berechtigungen 'Remote Enable' und 'Read Security' des 'OpenDNS_Connector'-Kontos im WMI-Namespace root\cimv2.

- Gewährt dem OpenDNS_Connector-Konto 'Replikation von Verzeichnisänderungen' explizit Berechtigungen
- Fügt das Konto 'OpenDNS_Connector' der Gruppe 'Verteilte COM-Benutzer' hinzu

Ab 2008 erfolgt diese Änderung auch:

- Fügt das Konto 'OpenDNS_Connector' der Gruppe 'Ereignisprotokollleser' hinzu

---



> Anmerkung: Wenn die automatische Konfiguration abgelehnt wird oder diese Änderungen fehlschlagen, wird die Registrierung nicht fortgesetzt.

Phase 2b - Warnungen zur automatischen Konfiguration

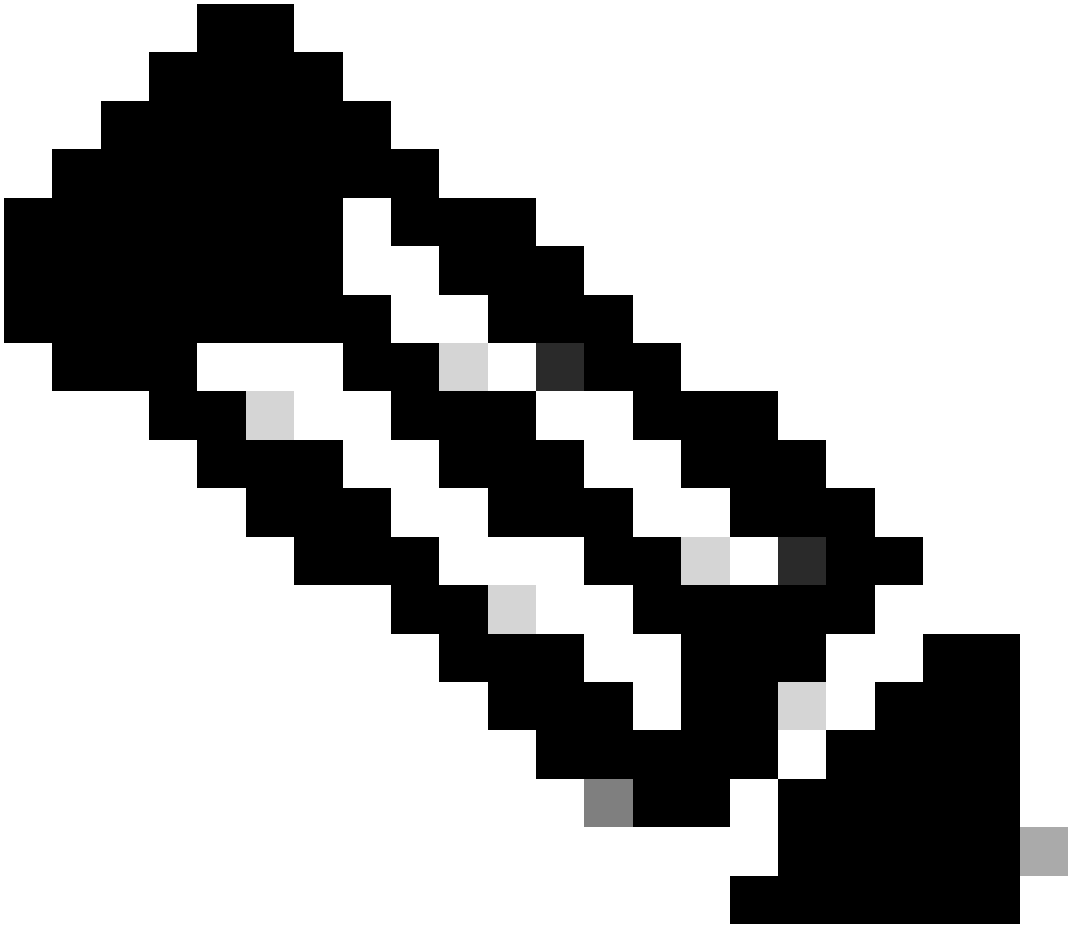
Das Skript gibt Warnungen aus, wenn die Gruppenrichtlinieneinstellungen nicht richtig konfiguriert sind. Das Skript kann diese Probleme nicht beheben.

Alle Betriebssysteme:

- Das Skript WARNT, wenn die Einstellung 'Anmeldeereignisse überwachen' in der Gruppenrichtlinie nicht korrekt konfiguriert ist, die Gruppenrichtlinie jedoch nicht ändert.

Zu 2003 (und 2003 auf funktionaler Ebene):

- Das Skript WARNT, wenn das Recht 'Überwachungs- und Sicherheitsprotokoll verwalten' in der Gruppenrichtlinie nicht korrekt konfiguriert ist, die Gruppenrichtlinie jedoch nicht ändert.



> Anmerkung: Beheben Sie das Problem manuell, und führen Sie das Konfigurationsskript erneut aus. Das Skript beginnt erst mit der Registrierung, wenn diese korrigiert wurden.

Phase 3 - Registrierung

Das Skript fordert vor der Registrierung des Domänencontrollers bei Umbrella "`Möchten Sie diesen Domänencontroller (J oder N) registrieren?" an.`Diese Informationen werden an Umbrella gesendet:

- Hostname/Label des Domänencontrollers
- Domänenname
- IP-Adresse
- Ihre eindeutige Organisations-ID und Ihr Token (in Ihrem Skript enthalten) zur eindeutigen Identifizierung des Rechenzentrums mit Ihrer übergeordneten Organisation.

Die Registrierung erfolgt sicher über https://api.opendns.com

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.