Konfigurieren von Benutzern, Gruppen und Computern in Active Directory für die Synchronisierung mit dem OpenDNS Connector-Dienst

Inhalt

Einleitung

Überblick

- Standardberechtigungen
- Effektiven Zugriff anzeigen
- OpenDNS_Connector-LDAP-Berechtigungen festlegen
- userPerms-Skript

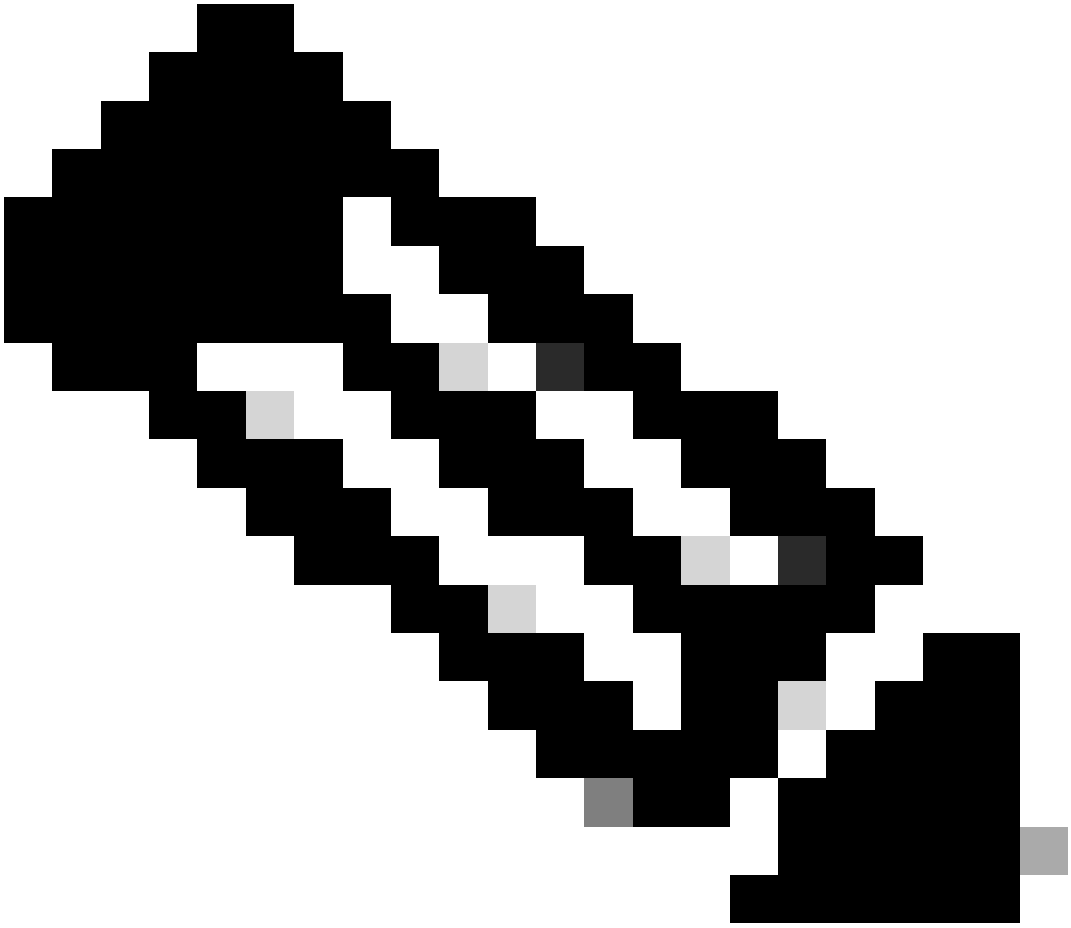
Einleitung

In diesem Dokument wird beschrieben, wie Benutzer, Gruppen und Computer von Active Directory mit dem OpenDNS Connector-Dienst synchronisiert werden.

Überblick

Der OpenDNS Connector-Dienst synchronisiert eine Liste von Benutzern, Gruppen und Computern aus Active Directory mithilfe des LDAP-Protokolls. In diesem Artikel wird beschrieben, wie Sie überprüfen, ob das OpenDNS_Connector-Konto über die richtigen Berechtigungen zum Lesen dieser Objekte verfügt.

Jedes Objekt (Benutzer/Gruppen/Computer) in Active Directory verfügt über Zugriffskontrolllisten-Sicherheitsberechtigungen, und jedes Objekt muss dem OpenDNS_Connector-Benutzerkonto das Lesen seiner Attribute gestatten.



Anmerkung: In diesem Artikel wird davon ausgegangen, dass die normalen Voraussetzungen für das Konto 'OpenDNS_Connector' bereits überprüft wurden. Wenn AD-Benutzer/Gruppen im Dashboard fehlen, lesen Sie bitte zuerst diesen Artikel: AD-Benutzer/Gruppen fehlen im Umbrella Dashboard.

Standardberechtigungen

Standardmäßig können alle authentifizierten Benutzer die Eigenschaften von Benutzern/Gruppen/Computern lesen, sodass der OpenDNS_Connector-Benutzer keine zusätzlichen Berechtigungen für die LDAP-Synchronisierung benötigt.

Die Standardberechtigungen werden normalerweise wie folgt festgelegt:

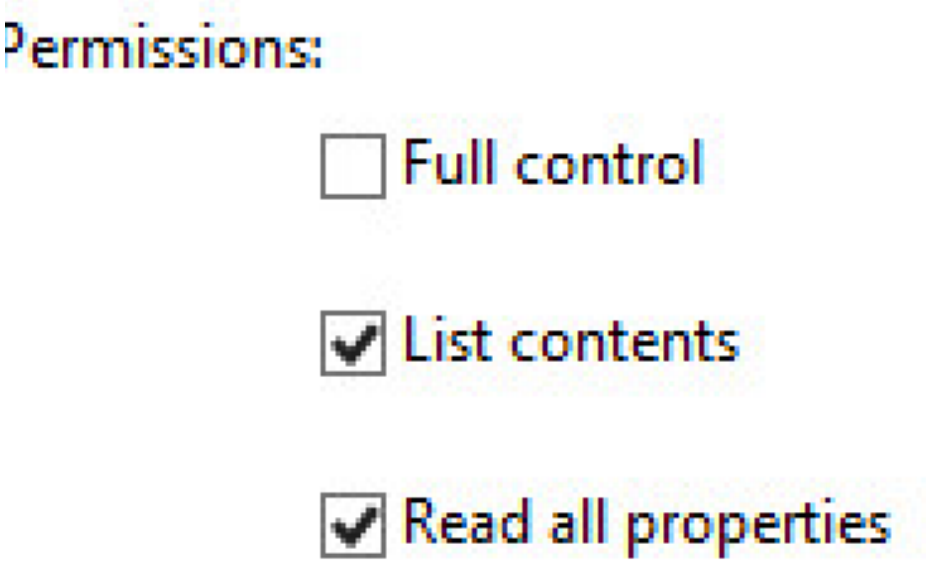
1) Der Gruppe 'Pre-Windows 2000 Compatible Access' werden für 'Descendant User Objects', 'Descendant Group Objects' und 'Descendant Computer Objects' Leseberechtigungen (alle Eigenschaften lesen) für die Domäne zugewiesen.

Sie können dies wie folgt überprüfen:

- Öffnen Sie Active Directory-Benutzer und -Computer.
- Klicken Sie auf 'Anzeigen' und aktivieren Sie die Option 'Erweiterte Funktionen'.
- Klicken Sie mit der rechten Maustaste auf das Domain-Objekt, und wählen Sie 'Eigenschaften' und dann 'Sicherheit > Erweitert' aus.
- Wählen Sie den Eintrag 'Pre Windows 2000 Compatible Access' mit 'Special' Berechtigungen aus:

115011616667

- Klicken Sie auf 'Bearbeiten', um diese Berechtigungen im Detail anzuzeigen.
- Wählen Sie 'Abhängige Benutzerobjekte' im Abschnitt 'Auf' aus.
- Suchen Sie nach diesen Berechtigungen:

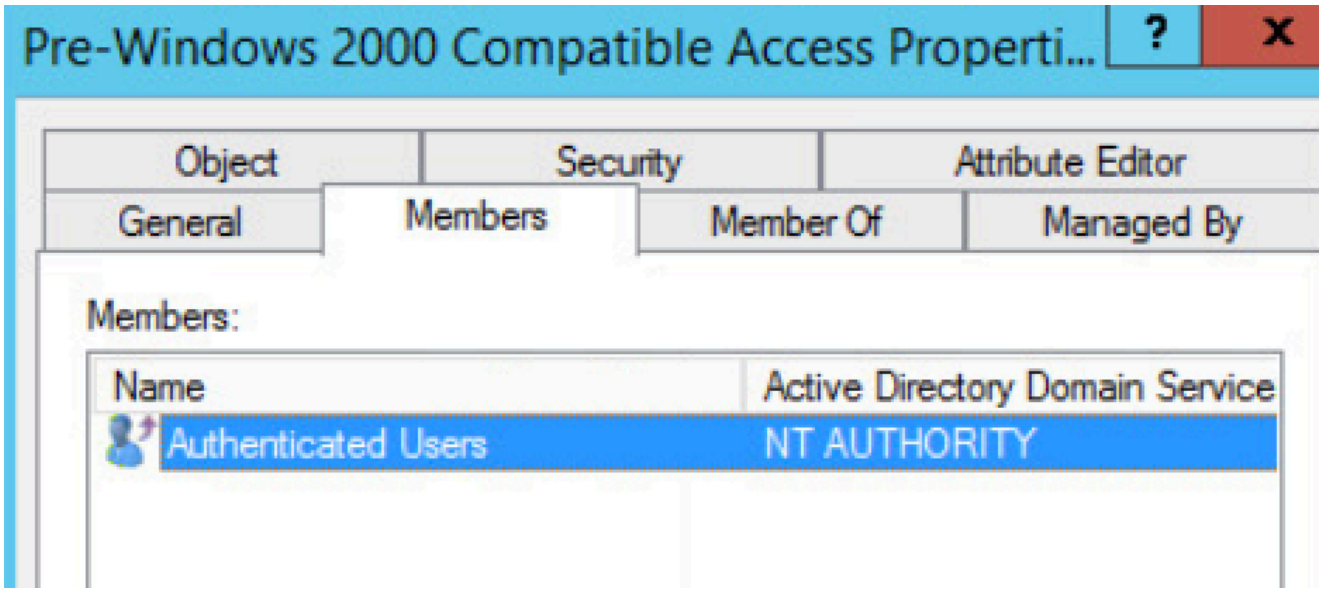


115011616687

- Wiederholen Sie diese Schritte für 'Abhängige Gruppenobjekte' und 'Abhängige Computerobjekte'

2) Die Gruppe "Alle authentifizierten Benutzer" ist Mitglied der Gruppe "Pre-Windows 2000 Compatible Access", die diese Einstellungen für alle Benutzer bereitstellt.

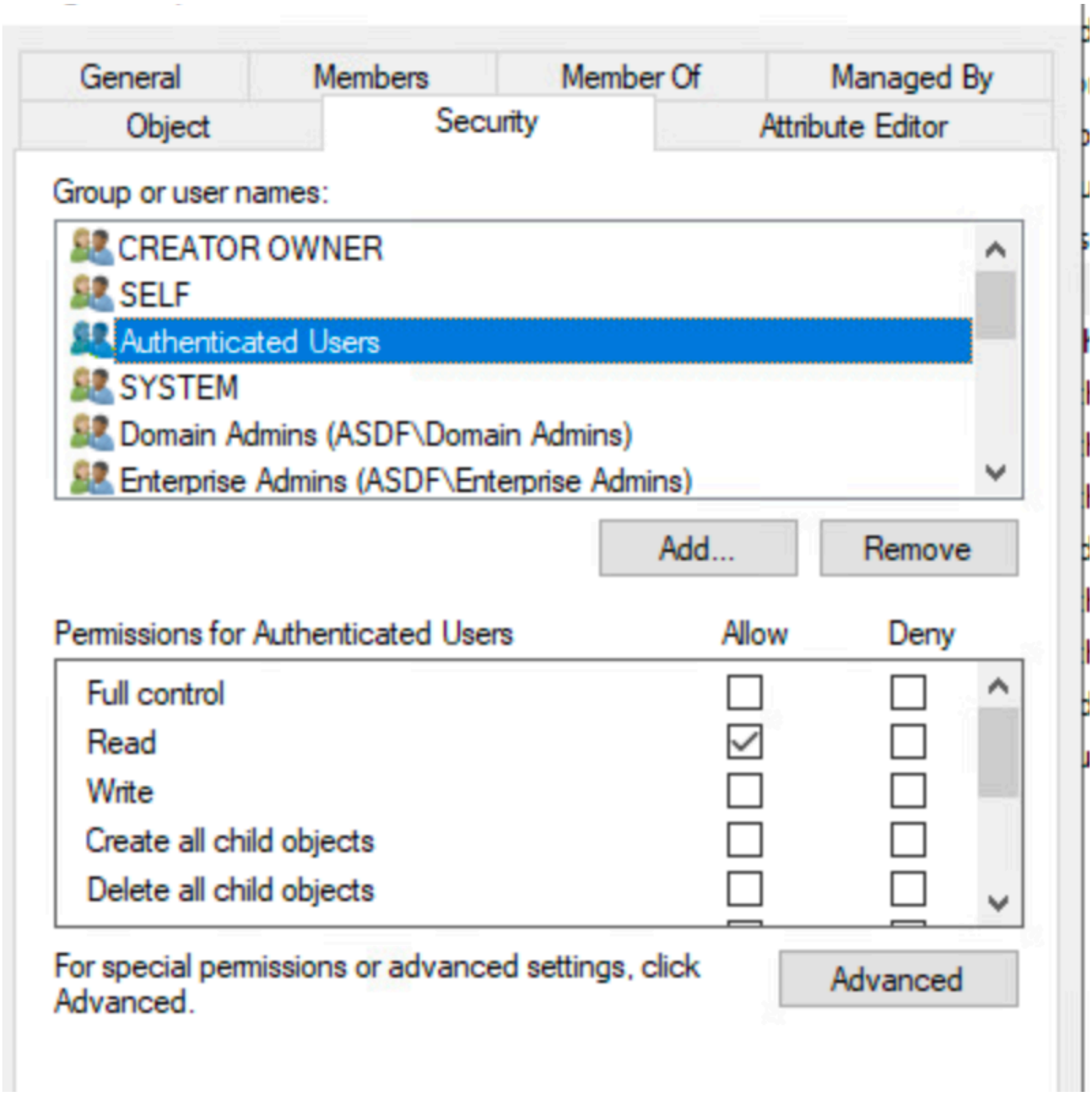
- Klicken Sie mit der rechten Maustaste auf die Gruppe Pre-Windows 2000 Compatible Access (Kompatibler Zugriff vor Windows 2000), die sich normalerweise im Container Builtin AD befindet.
- Wählen Sie 'Eigenschaften' und gehen Sie zur Registerkarte 'Mitglieder'.
- Überprüfen Sie, ob 'Authentifizierte Benutzer' aufgeführt ist.



115011616707

In einigen AD-Umgebungen konnte dieses Berechtigungsmodell jedoch geändert und authentifizierte Benutzer entfernt werden. Dies kann sich dadurch manifestieren, dass einige Benutzer im Umbrella Dashboard fehlen oder dass Gruppenmitgliedschaften falsch sind. Wenn dies der Fall ist, fügen Sie den OpenDNS_Connector-Benutzer zu dieser Gruppe hinzu, starten Sie den Connector-Dienst neu, und die fehlenden Elemente werden in Umbrella angezeigt.

In einigen seltenen Fällen wird das Problem dadurch immer noch nicht behoben. Wenn dies der Fall ist, überprüfen Sie die Registerkarte Gruppensicherheit in Active Directory, stellen Sie sicher, dass authentifizierte Benutzer hier mit einem Check-in Lesezugriff aufgeführt werden. Wenn dies nicht aktiviert ist, deaktivieren Sie es, und starten Sie den Connector-Dienst neu, um zu sehen, ob die Gruppenmitglieder angezeigt werden. Wenn diese Sicherheitseinstellung in allen Gruppen fehlt, müssen die Änderungen global in großen Mengen auf alle Gruppen angewendet werden.



28728163336852

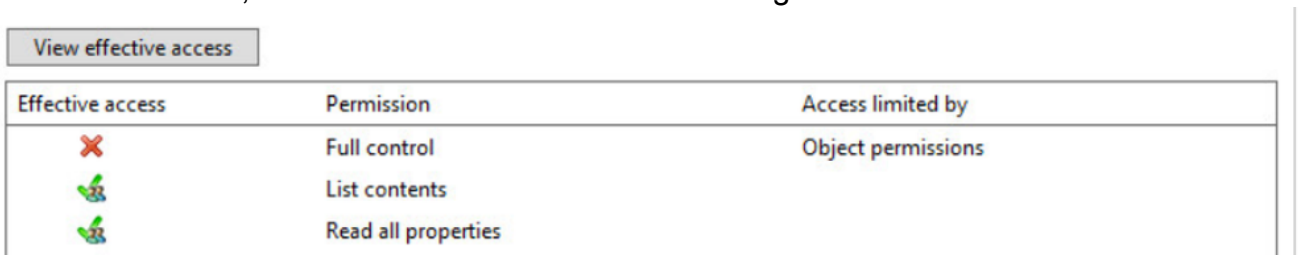
Effektiven Zugriff anzeigen

Sie können das Windows-Tool 'Effective Access' verwenden, um festzustellen, ob der OpenDNS_Connector-Benutzer in der Lage ist, ein bestimmtes Objekt zu lesen, das fehlt (oder das eine falsche Gruppenmitgliedschaft aufweist).

- Öffnen Sie Active Directory-Benutzer und -Computer.
- Klicken Sie auf 'Anzeigen' und aktivieren Sie die Option 'Erweiterte Funktionen'.
- Suchen Sie das Benutzerobjekt, und klicken Sie mit der rechten Maustaste, um

"Eigenschaften" auszuwählen.

- Gehen Sie zu 'Sicherheit > Erweitert > Effektiver Zugriff' (dies kann sagen 'Effektive Berechtigungen')
- Klicken Sie auf 'Benutzer auswählen' und wählen Sie dann das Benutzerkonto 'OpenDNS_Connector' aus.
- Klicken Sie auf "OK" und anschließend "Effektiven Zugriff anzeigen".
- Stellen Sie sicher, dass der Connector-Benutzer alle Eigenschaften lesen kann:

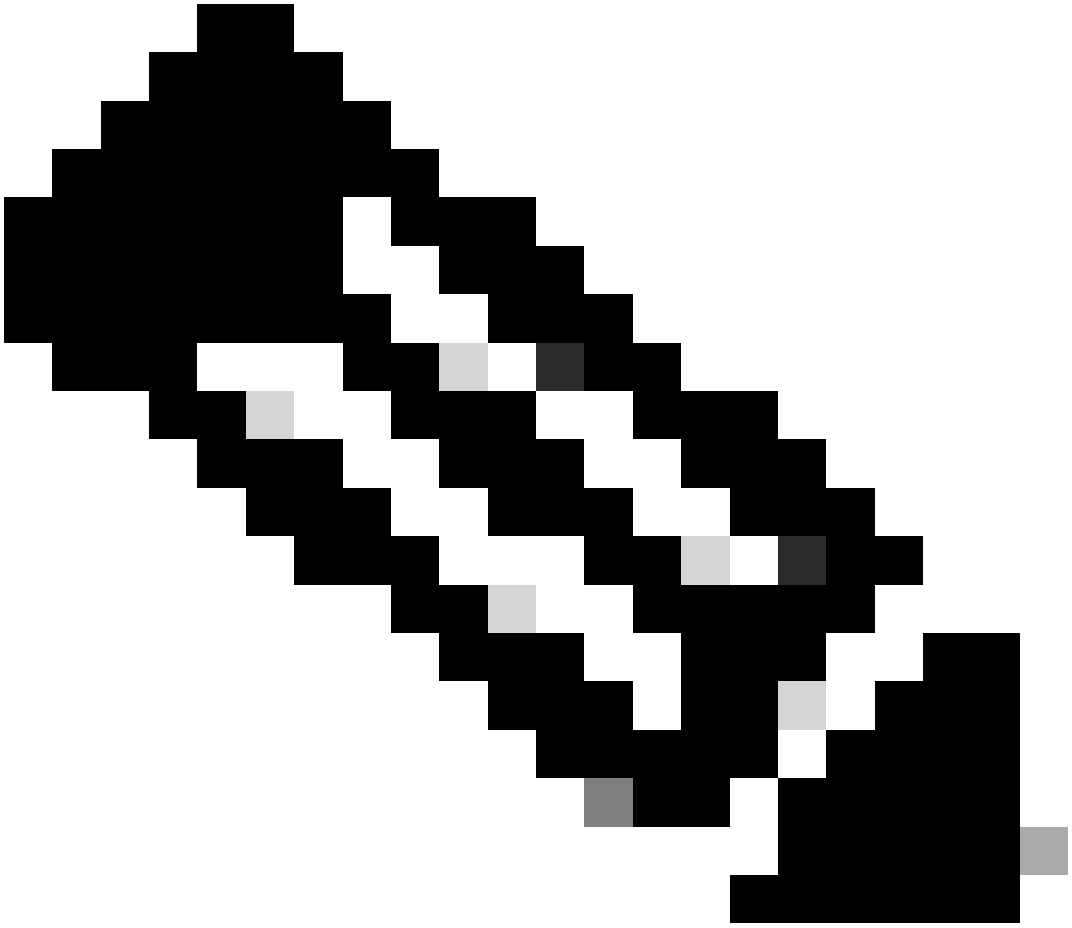


115011616727

OpenDNS_Connector-LDAP-Berechtigungen festlegen

Der Assistent 'Steuerung delegieren' in AD ist eine schnelle Möglichkeit, dem 'OpenDNS_Connector'-Benutzer die erforderlichen Berechtigungen zuzuweisen:

1) Gehen Sie zu Verwaltung, und öffnen Sie das Snap-In Active Directory-Benutzer und -Computer.
2) Klicken Sie mit der rechten Maustaste auf die Domäne, die den OpenDNS_Connector enthält, und wählen Sie "Delegate Control..." aus, und klicken Sie dann auf Weiter.
3) Fügen Sie den Benutzer OpenDNS_Connector hinzu, und klicken Sie dann auf Weiter.
4) Wählen Sie "Alle Benutzerinformationen lesen", und klicken Sie auf "Weiter". [Siehe Bild 3.]
7) Klicken Sie auf Fertig stellen. [Siehe Bild 6.]



Anmerkung: Diese Schritte können fehlschlagen, wenn die Vererbung für einige Objekte deaktiviert ist. Für diese Objekte müssen Sie die Berechtigungen manuell festlegen.

userPerms-Skript

Das angehängte Powershell-Skript ist eine weitere Methode, um die Berechtigungen eines bestimmten Objekts (z. B. user) in AD. Bitte geben Sie die Ausgabe dieses Skripts an, wenn Sie sich an den technischen Umbrella-Support wenden.

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.