

Warum funktioniert die LDAP-Gruppenabfrage nicht mit Active Directory?

Inhalt

[Einführung](#)

[Warum funktioniert die LDAP-Gruppenabfrage nicht mit Active Directory?](#)

Einführung

In diesem Dokument wird erläutert, warum LDAP-Gruppenabfragen möglicherweise nicht auf einer E-Mail-Security-Appliance (ESA) funktionieren.

Warum funktioniert die LDAP-Gruppenabfrage nicht mit Active Directory?

Warum werden die erwarteten Ergebnisse durch die LDAP-Gruppenabfrage nicht ausgegeben, wenn der Benutzer mit Sicherheit Mitglied der angegebenen Gruppe ist?

Bei Gruppenabfragen mit Microsoft Active Directory muss der DN (Distinguished Name, DN) der Gruppe und nicht der gemeinsame Name (CN) verwendet werden. Im Folgenden finden Sie einige Beispiele für diese beiden Elemente:

Common Name (CN):

Administratoren

Phoenix-Benutzer

Distinguished Name (DN):

CN=Administratoren, DC=Beispiel, DC=Com

CN=Phoenix-Benutzer, OU=Phoenix, DC=Cisco, DC=Com

Wenn Sie sich nicht sicher sind, was der DN ist, finden Sie dies unter Active Directory-Benutzer und -Computer:

1. Wählen Sie im Menü "Ansicht" die Option "Erweiterte Funktionen" aus.
2. Klicken Sie in den Eigenschaften des gewünschten Gruppenobjekts auf den "Attribut-Editor".
3. Scrollen Sie zum Attribut "DistinguishedName", und doppelklicken Sie auf das Attribut.
4. Die vollständige Zeichenfolge sollte hervorgehoben werden. Mit der rechten Maustaste klicken und in die Zwischenablage kopieren

Wenn Sie über die DN der Gruppe verfügen, können Sie sie immer verwenden, wenn Sie den Namen der Gruppe angeben. Dazu gehören Testabfragen, Content- und Nachrichtenfilter sowie E-Mail-Richtlinien.

Ein weiterer Ansatz wäre die Verwendung eines der beiden folgenden Programme, um die Verzeichnisnummer zu finden:

ADEplorer:

<http://technet.microsoft.com/en-us/sysinternals/bb963907.aspx>

Softerra-LDAP-Browser:

<http://www.ldapadministrator.com/download.htm>

Der allgemeine Prozess zur Verwendung eines dieser Tools zu diesem Zweck wird nachfolgend beschrieben:

1. Herstellen einer Verbindung mit dem Domänencontroller mithilfe des LDAP-Browsing-Tools
2. Suchen eines Benutzerobjekts, das Mitglied der Gruppe ist
3. Suchen des 'memberOf'-Attributs des Benutzerobjekts
4. Suchen Sie die DN, die der Zielgruppe entspricht
5. Kopieren Sie die DN der Zielgruppe aus diesem Attribut