

LDAP グループ クエリはなぜアクティブ ディレクトリを使用しませんか。

目次

[はじめに](#)

[LDAP グループ クエリはなぜアクティブ ディレクトリを使用しませんか。](#)

概要

LDAP グループ クエリが E メール セキュリティ アプライアンス (ESA) でなぜ動作しないかもしれないかこの資料に記述されています。

LDAP グループ クエリがアクティブ ディレクトリを使用しない理由

LDAP グループ クエリはなぜ確定的に特定のグループのメンバーであるユーザとテストされたとき期待された結果を生んでいませんか。

Microsoft Active Directory を使用してグループ クエリによって、それが Common Name (CN) であるよりもむしろグループの識別名 (DN) を使用することは必要です。これら二つの項目が見えるもののいくつかの例は下記にあります:

Common Name (CN):

管理者

フェニックス ユーザ

識別名 (DN):

CN=Administrators、DC=Example、DC=Com

CN=Phoenix-Users、OU=Phoenix、DC=Cisco、DC=Com

DN があるのであるものの確実ではない場合、Active Directory Users and Computers でこれを見つけることができます:

1. 「ビュー」メニューに行き、「進んだ機能を選択して下さい
2. 望ましいグループ オブジェクトのプロパティから、クリックして下さい「属性エディタを」
3. 「distinguishedName」属性にスクロールし、属性をダブルクリックして下さい
4. 完全なストリングは強調表示する必要があります。クリップボードへの右クリックおよびコピー

グループの DN があれば、グループの名前を規定する時はいつでもそれを使用できます。これにはテスト クエリ、内容およびメッセージ フィルターが含まれ、またポリシーを郵送します。

もう一つのアプローチは DN をつけるのに次の 2 つのプログラムのいずれかを使用することです:

ADEplorer:

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

Softerra LDAPブラウザ:

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

これらのツールの 1 つを使用するための一般のプロセスはこのために下記のように説明されています:

1. LDAP を使用してツールを参照しているドメインコントローラに接続して下さい
2. グループのメンバーであるユーザ オブジェクトを見つけて下さい
3. ユーザ オブジェクトの「memberOf」属性を見つけて下さい
4. ターゲットとすることを試みているグループに対応する DN を見つけて下さい
5. この属性からターゲット グループの DN をコピーして下さい