Nested LDAP Group Search for Microsoft AD

The Nested LDAP Group Search for Microsoft AD feature allows you to retrieve the complete nested-user-group chain information of a user in a particular Microsoft Active Directory domain.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Nested LDAP Group Search for Microsoft AD

Nested Lightweight Directory Access Protocol (LDAP) group search supports nested-group searches only in Microsoft Active Directory (AD) on Windows Server 2003 and later versions. This feature does not support searches in generic LDAP servers.

Information About Nested LDAP Group Search for Microsoft AD

Overview of Nested-User Groups on an LDAP Server

The Lightweight Directory Access Protocol (LDAP) search query is used to retrieve a user's authorization profile from an LDAP server to find direct user group members. Each of these direct user groups can be part of multiple groups and thus form a nested-user group.

To find nested-user groups on an LDAP server, an LDAP client must send multiple queries to the LDAP server. Hence, excessive system and network resources are required to find nested-user groups.

Instead of sending multiple LDAP queries, an LDAP client uses a customized, Microsoft-supported search filter to perform a server-based search to find all the non-primary nested groups to which a user belongs. To limit the number of user groups found by Microsoft Active Directory (AD), you can configure a base distinguished name (DN) configuration within the limit you require.

How to Configure Nested LDAP Group Search for Microsoft AD

Configuring Nested LDAP Group Search

Perform this task to configure a search request sent by a Lightweight Directory Access Protocol (LDAP) client to a server to find a user's nested-group information in Microsoft Active Directory (AD).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ldap server** *name*
4. **bind authenticate root-dn** *user-name* **password** [**0 string** | **7** *string*] *string*
5. **search-type nested**
6. **base-dn** *string*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ldap server** *name* **Example:** `Device(config)# ldap server server1`	Configures a device to use an LDAP server and enters LDAP server configuration mode.
Step 4	**bind authenticate root-dn** *user-name* **password** [**0** **string** | **7** *string*] *string* **Example:** `Device(config-ldap-server)# bind authenticate root-dn cn=user1,cn=users,dc=sns,dc=example,dc=com password example123`	Binds an attribute testmap to the LDAP server.
Step 5	**search-type nested** **Example:** `Device(config-ldap-server)# search-type nested`	Specifies the search filter to be used in nested-group search requests.
Step 6	**base-dn** *string* **Example:** `Device(config-ldap-server)# base-dn dc=sns,dc=example,dc=com`	(Optional) Configures the base distinguished name (DN) that you want to use to perform search operations in an LDAP server.
Step 7	**end** **Example:** `Device(config-ldap-server)# end`	Exits LDAP server configuration mode and returns to privileged EXEC mode.

Verifying Nested LDAP Group Search for Microsoft AD

Perform this task to verify if the nested LDAP user groups are being downloaded.

SUMMARY STEPS

1. **enable**
2. **show ip admission cache ip-addr** *ip-address*
3. **debug ldap all**

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show ip admission cache ip-addr *ip-address*

Displays the current list of network admission entries for a client IP address associated with LDAP.

Example:

```
Device# show ip admission cache ip-addr 192.0.2.3

Authentication Proxy Cache

Authentication Method   : NTLM
User Name               : Administrator
Client IP               : 1.1.3.240
Client Port             : 34512
Timeout                 : 60
Time  Remaining         : 60
Failed Authentications  : 0
HTTP Contexts (hwm/max) : 0 (1/30)
Connection state        : ESTAB

EPM information : Authproxy
    Admission feature:  AUTHPROXY
         AAA Policies:
     Supplicant-Group:  firewall_group
     Supplicant-Group:  Group Policy Creator Owners
     Supplicant-Group:  Domain Admins
     Supplicant-Group:  Enterprise Admins
     Supplicant-Group:  Schema Admins
     Supplicant-Group:  IIS_IUSRS
     Supplicant-Group:  Administrators
     Supplicant-Group:  Denied RODC Password Replication Group

EOU information
--------------------------------------------------------------------------------
Address         Interface              AuthType   Posture-Token Age(min)
--------------------------------------------------------------------------------

EPM information : EOU
```

Step 3 debug ldap all

Displays all event, legacy, and packet-related messages associated with LDAP.

Example:

```
Device# debug ldap all

.
.
.
LDAP: LDAP Messages to be processed: 1
LDAP: LDAP Message type: 101
LDAP: Got ldap transaction context from reqid 43608ldap_parse_result
LDAP: resultCode: 0 (Success)
LDAP: Received Search Response resultldap_parse_result
LDAP: Ldap Result Msg: SUCCESS, Result code =0
LDAP: * LDAP SEARCH DONE *
LDAP: SASL NTLM authentication and first stage search done.. Execute nested search now
LDAP: Next Task: Send search req
LDAP: Transaction context removed from list [ldap reqid=43608]
LDAP: Check the default map for aaa type=username
LDAP: Construct nested search filter
LDAP: Nested Filter: (objectclass=group)(member:1.2.840.113556.1.4.1941:=
LDAP: Free nested search filter string malloced
LDAP: Ldap Search Req sent
ld 531960512
base dn DC=aaaldapipv6,DC=com
scope 2
filter
(&(objectclass=group)(member:1.2.840.113556.1.4.1941:=CN=Administrator,CN=Users,DC=aaaldapipv6,DC=com))ldap_req_encode
put_filter
"(&(objectclass=group)(member:1.2.840.113556.1.4.1941:=CN=Administrator,CN=Users,DC=aaaldapipv6,DC=com))"
put_filter: AND
put_filter_list
"(objectclass=group)(member:1.2.840.113556.1.4.1941:=CN=Administrator,CN=Users,DC=aaaldapipv6,DC=com)"
put_filter "(objectclass=group)"
put_filter: simple
put_filter "(member:1.2.840.113556.1.4.1941:=CN=Administrator,CN=Users,DC=aaaldapipv6,DC=com)"
put_filter: simple
extensible match
Doing socket write
LDAP: lctx conn index = 58
LDAP: LDAP search request sent successfully (reqid:43609)
LDAP: free entry in perform next taskldap_msgfree
ldap_result
wait4msg (timeout 0 sec, 1 usec)
ldap_select_fd_wait (select)
ldap_err2string
.
.
.
ldap_match_request succeeded for msgid 53 h 0

LDAP: LDAP Messages to be processed: 1
LDAP: LDAP Message type: 100
LDAP: Got ldap transaction context from reqid 43609
LDAP: Attribute               Length    Valueldap_get_dn

LDAP: dn                      50        CN=Administrators,CN=Builtin,DC=aaaldapipv6,DC=com
LDAP: Check the default map for aaa type=password
LDAP: objectClass             3         top
LDAP: objectClass             5         group
LDAP: cn                      14        Administrators
  1:25 PM
LDAP: Got ldap transaction context from reqid 43609
LDAP: Attribute               Length    Valueldap_get_dn
.
.
.
LDAP: dn                      45        CN=IIS_IUSRS,CN=Builtin,DC=aaaldapipv6,DC=com
LDAP: Check the default map for aaa type=password
LDAP: objectClass             3         top
LDAP: objectClass             5         group
```

```
LDAP: cn                        9         IIS_IUSRS
LDAP: description               53        Built-in group used by Internet Information Services.
LDAP: member                    47        CN=Administrator,CN=Users,DC=aaaldapipv6,DC=com
LDAP: distinguishedName         45        CN=IIS_IUSRS,CN=Builtin,DC=aaaldapipv6,DC=com
```

Configuration Example for Nested LDAP Group Search for Microsoft AD

Example: Nested LDAP Group Search

The following example shows a configuration of nested-group search requests:

```
Device> enable
Device# configure terminal
Device(config)# ldap server ldap_dir_1
Device(config-ldap-server)# bind authenticate root-dn
cn=administrator,cn=users,dc=nac-blr2,dc=example,dc=com password example123
Device(config-ldap-server)# search-type nested
Device(config-ldap-server)# base-dn dc=sns,dc=example,dc=com
Device(config-ldap-server)# end
```

Additional References for Nested LDAP Group Search for Microsoft AD

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z
LDAP configuration tasks	“Configuring LDAP” chapter in *AAA LDAP Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 4511	*Lightweight Directory Access Protocol (LDAP)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Nested LDAP Group Search for Microsoft AD

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Nested LDAP Group Search for Microsoft AD

Feature Name	Releases	Feature Information
Nested LDAP Group Search for Microsoft AD	15.3(3)M	The Nested LDAP Group Search for Microsoft AD feature allows you to retrieve the complete nested-user-group chain information of a user in a particular Microsoft Active Directory domain. The following command was introduced: **search-type nested**.