How to configure a NetScaler appliance for Nested Active Directory Group Extraction of LDAP

Some policies, such as authorization, session, and traffic policies, can be applied to a session on the basis of the user's group membership (for example, to allow or deny an access to a certain resource).

Prerequisites:

- Basic Active Directory authentication must be configured before attempting to filter based on Active Directory groups. For instructions, see Citrix article CTX108876, How to Configure LDAP Authentication on a NetScaler Appliance.
- Nested groups must be configured for users logging on to NetScaler Gateway
- A NetScaler Gateway Virtual server must be configured and bound to the LDAP policy
- This article assumes an understanding of the Active Directory and LDAP protocol.

Background:

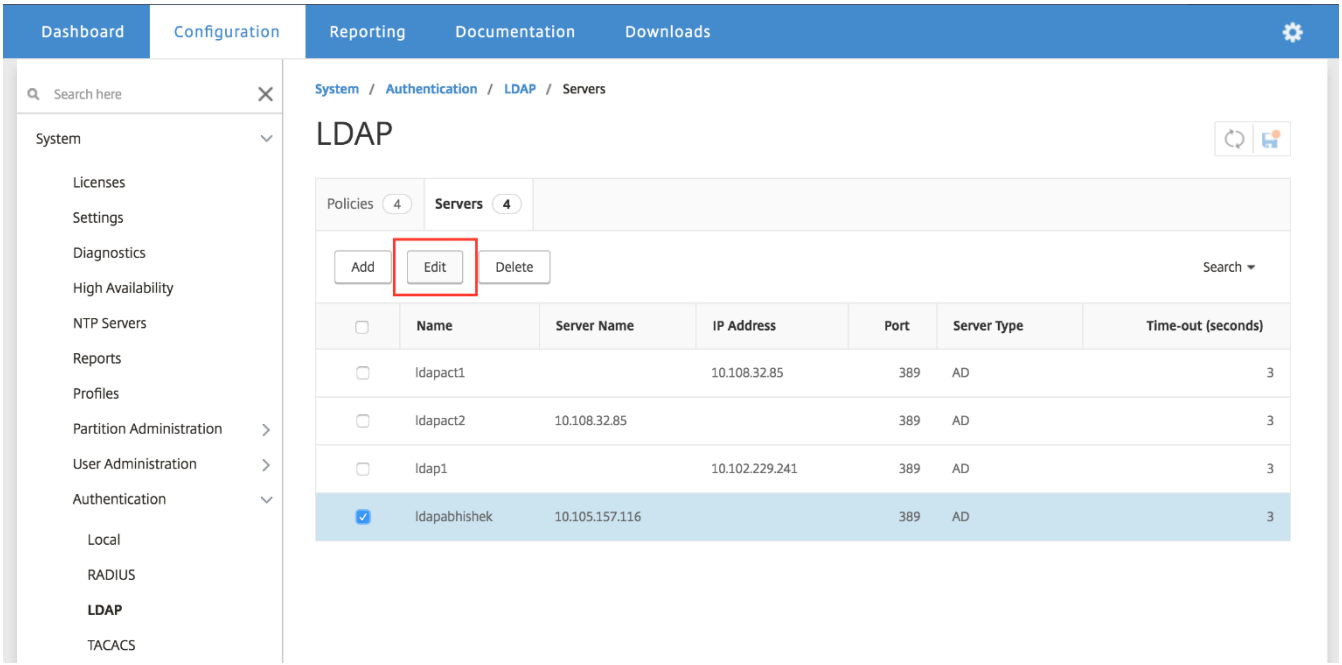
The credentials of a user attempting to log on to NetScaler Gateway are sent to the Active Directory for validation. If the user name and password are valid, the Active Directory sends the user attributes to the NetScaler appliance.

The **memberOf** attribute is one of the attributes that the Active Directory sends to the NetScaler appliance. This attribute contains the name of the group in which the user is defined as a member in the Active Directory. There can be cases in which a user is a member of *GroupA*, and *GroupA* is in turn is a member of *GroupB,* which is a member of *GroupC*, and so on. Group information extraction in such cases can be achieved by taking the following steps.

To configure a NetScaler appliance for Nested Active Directory Group Extraction

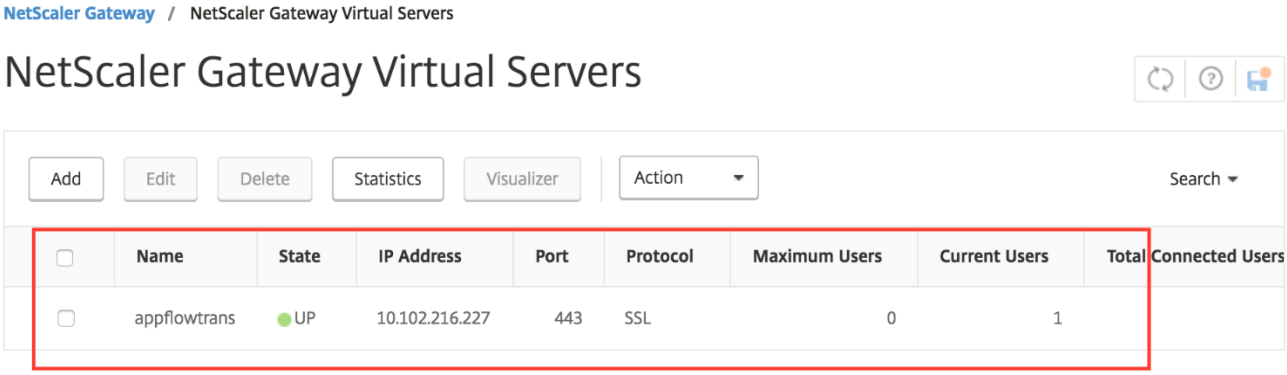
1. Log on to the NetScaler GUI and, on the **Configuration** tab, do one of the following:

   Navigate to **System** > **Authentication** > **LDAP** > **Servers** and jump to step 4.



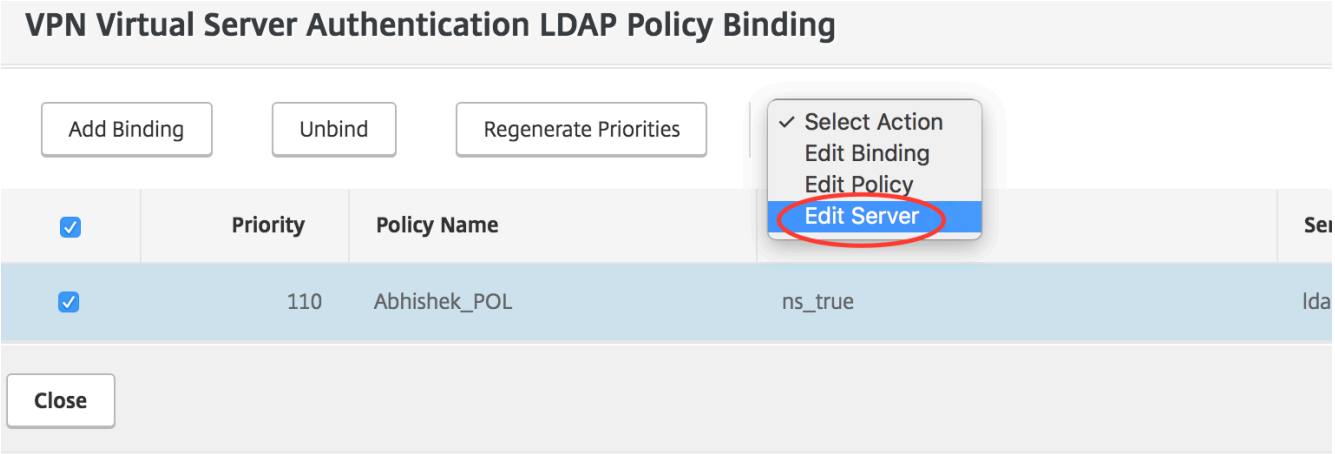
OR

Navigate to **NetScaler Gateway ->Virtual Servers** and select the VPN vserver for which the nested group extraction option needs to be set.

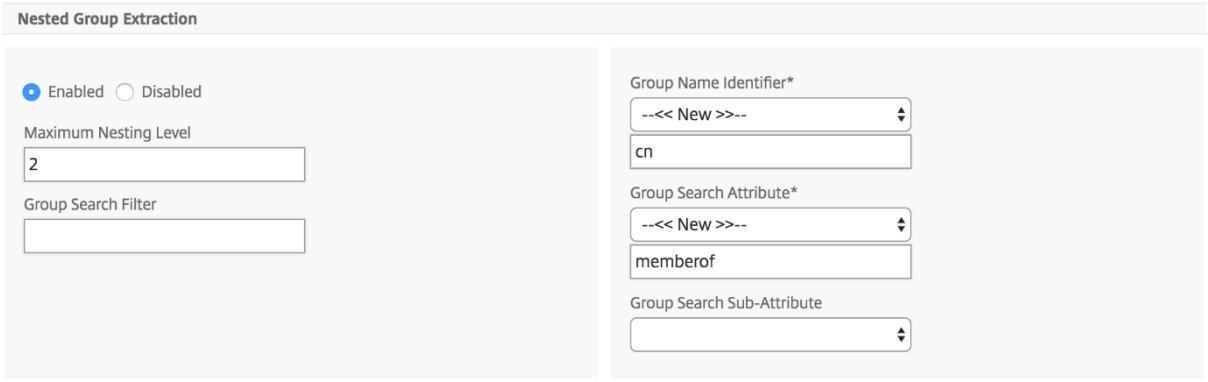


2. In the Basic Authentication section, click **LDAP Policy**.

3. Select the LDAP policy that you want to edit, and click **Edit**.



4. Navigate to **Nested Group Extraction**, set the Group Name Identifier as `--<< New >>--` and type `cn` in the text field below it, select Group Search Attribute `as --<< New >>--` and type memberOf in the text field below it shown in the screen below. You can also set the **memberOf** attribute to match the search filter parameter set on the appliance. If the attribute matches, you are allowed to log on to the network. You can also set the maximum nesting level for group extraction.



5. Attempt to log on to NetScaler Gateway as a member of one of the nested user groups defined in the Active Directory.

6. To verify that the group information for the logged on user has been extracted, open a command line editor and log on to the NetScaler appliance.

   1.1. Verify that the group you logged on as a member of is included in the groups defined on the NetScaler appliance.

   Example

```
> sh aaa group
1)  GroupName: TestGRP
2)  GroupName: group1
3)  GroupName: TestNS
4)  GroupName: Group2
 Done
```

7. If the group is not listed, create a group using the below command:

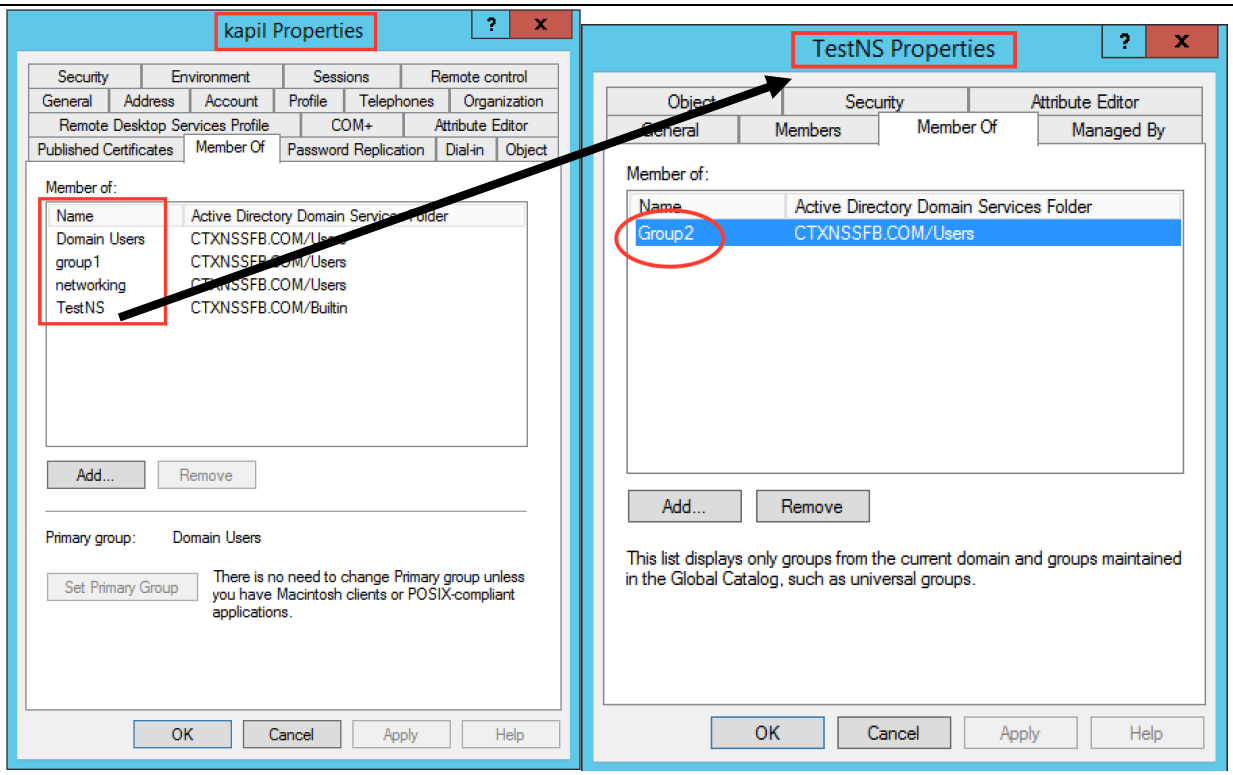
```
> add aaa group <groupname>
```

8. Use command shown in the following example to check for the logged-on groups.

   Example

```
> sh aaa group -loggedIn
Group name: group1
Group name: TestNS
Group name: Group2
Done
```

Which should match the '*Member Of*' tab when checked for this user in Active Directory as shown in the below screenshots.


kapil Properties
Security
Environment
Sessions
Remote control
General
Address
Account
Profile
Telephones
Organization
Remote Desktop Services Profile
COM+
Attribute Editor
Published Certificates
Member Of
Password Replication
Dial-in
Object
Member of:
Name
Active Directory Domain Services Folder
Domain Users
CTXNSSFB.COM/Users
group1
CTXNSSFB.COM/Users
networking
CTXNSSFB.COM/Users
TestNS
CTXNSSFB.COM/Builtin
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help
TestNS Properties
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Member of:
Name
Active Directory Domain Services Folder
Group2
CTXNSSFB.COM/Users
Add...
Remove
This list displays only groups from the current domain and groups maintained in the Global Catalog, such as universal groups.
OK
Cancel
Apply
Help