How to configure a NetScaler appliance for Active Directory Group Extraction by using 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.
- 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 protocols.

Background:

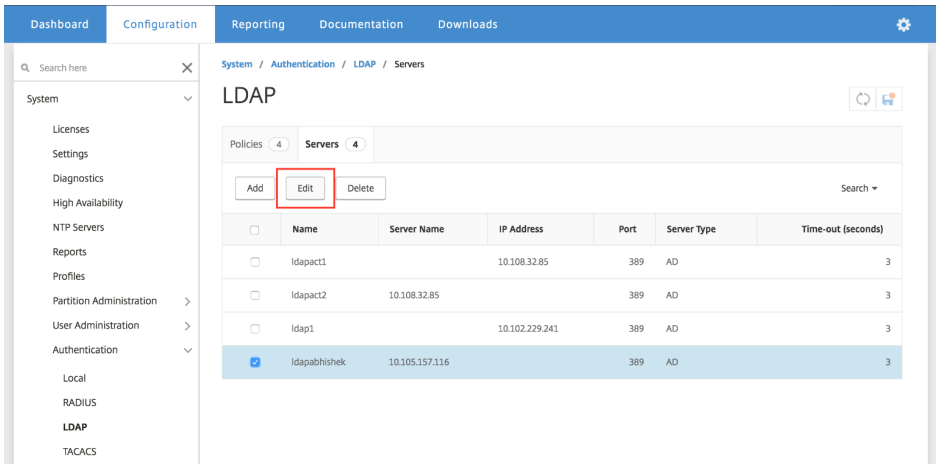
The credentials of a user attempting to log on to NetScaler Gateway are sent to the Active Directory for validation. If the user name and password are valid, the Active Directory sends the user attributes to the NetScaler appliance.

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. If the user is a member of more than one Active Directory group, multiple **memberOf** attributes are sent to the NetScaler appliance.

If you want to base VPN-user logons on group membership (user name only, no password field), see: https://support.citrix.com/article/CTX201742?_ga=1.259122893.658188677.1474538419

To configure Active Directory Group Extraction

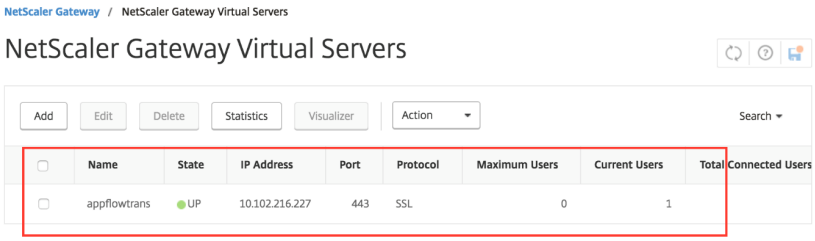
1. Log on to the NetScaler GUI and do the following:



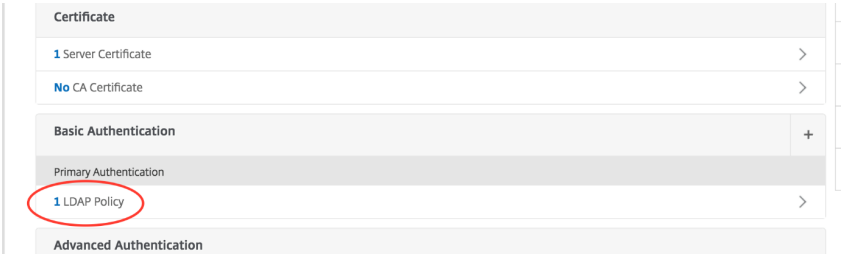
a) On the **Configuration** Tab, take one of the following actions:
Navigate to **System** > **Authentication** > **LDAP** > **Servers** and jump to step 1.d.

OR

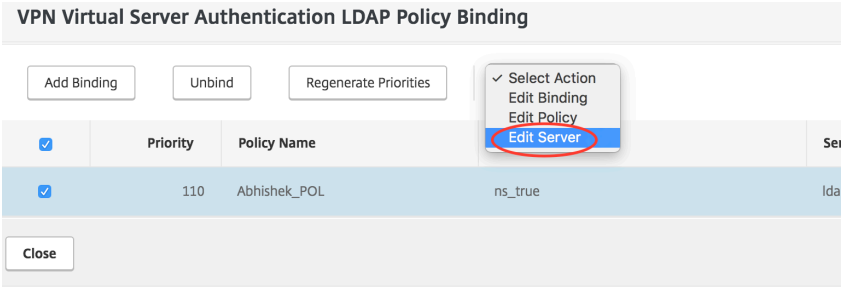
Navigate to > **NetScaler Gateway** > **Virtual Servers** and select the VPN vserver for which to enable the group extraction option.



b) In the Basic Authentication section, click **LDAP Policy**.



c) Select the LDAP Policy that you want to edit. Then, from the **Select Action** list, select **Edit server**.



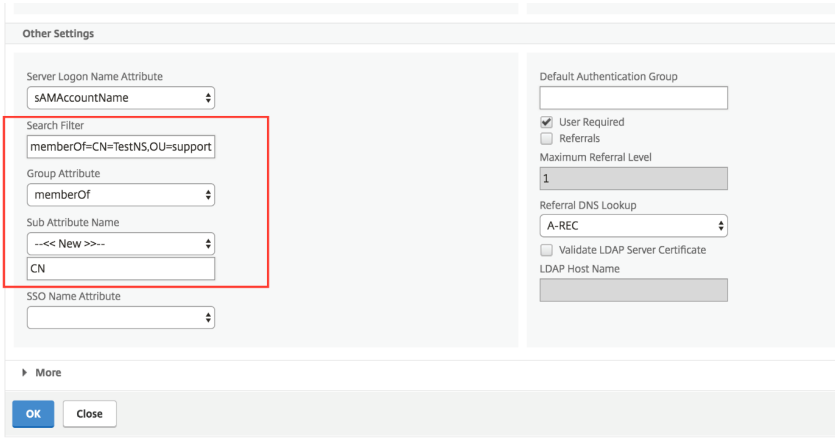
d) Navigate to **Other Settings** and, as shown in the following screen shot, enter the following information:

* Set the **Group Attribute** value to `memberOf`.
* Set **Sub Attribute Name** to `--<< New >>--`, and in the next text field type **CN**.

Alternatively, you can 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.

Deleted: `attribute`

Formatted: Font:(Default) Courier New



2. Attempt to log on to the NetScaler Gateway appliance as a member of one of the user groups defined in the Active Directory.
3. Log on to the CLI and verify that the group information for the logged on user has been extracted:
   a) Open a command line editor and log on to the NetScaler appliance
      ssh nsroot@<NetScaler IP>
   b) 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
 Done
```

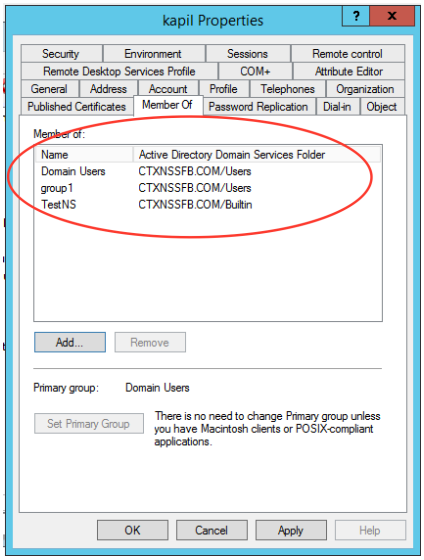
   c) If the group is not listed, create a group by entering the following command

add aaa group <groupname>

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

Example

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



The command's output should match what the **Member Of** tab shows for this user in Active Directory