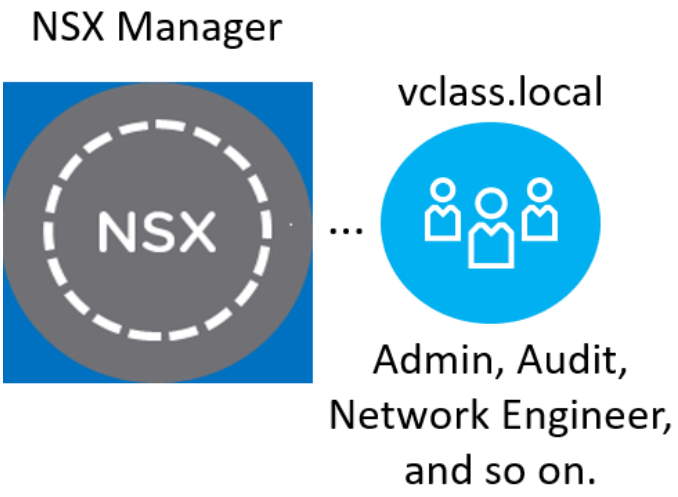
Lab 18 Managing Users and Roles

Objective and Tasks

Integrate NSX Manager with Active Directory over LDAP:

1. Prepare for the Lab
2. Add an Active Directory Domain as an Identity Source
3. Assign NSX Roles to Domain Users and Test Permissions



Task 1: Prepare for the Lab

You log in to the NSX UI.

1. From your student desktop, open Chrome. Perform these tasks from the Production NSX Manager
2. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
3. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Add an Active Directory Domain as an Identity Source

You use LDAP to add an Active Directory Domain to NSX Manager.

1. On the NSX UI Home page, navigate to **System** > **Settings** > **Users and Roles** and click the **LDAP** tab.
2. Click **ADD IDENTITY SOURCE.**
3. Configure the new identity source.

Option	Action
Name	Enter **`VCLASS`**.
Domain Name	Enter **`vclass.local`**.
Type	Select **Active Directory over LDAP** (default).
Base DN	Enter **`CN=Users,DC=vclass,DC=local`**.
LDAP Servers	Click the **Set** link.

4. When the Set LDAP Server window appears, click **ADD LDAP SERVER**.
5. Configure the LDAP server.

Option	Action
Hostname/IP	Enter **`DC.vclass.local`**.
LDAP Protocol	Select **LDAP** (default).
Type	Enter **`389.`** (default).
Bind Identity	Enter **`administrator@vclass.local`**.
Password	Enter **`VMware1!`**.

   Leave all other settings at their default values.
6. Click the **Check Status** link and verify that the connection status is Successful.
7. Click **ADD** and click **APPLY.**
8. Click **SAVE.**
9. Click the **Check Status** link and verify that the connection status is Successful.

Task 3: Assign NSX Roles to Domain Users and Test Permissions

You assign an NSX role to an Active Directory domain user and verify the user's permissions.

1. On the NSX UI home page, navigate to **System** > **Settings** > **Users and Roles** and click the **USERS** tab.
2. Click **ADD** and select **Role Assignment for LDAP.**
3. When the role assignment window appears, select **VCLASS** in the **Search Domain** drop-down menu.
4. Enter **`jdoe`** in the **Users/User Group Name** box and select the **jdoe@vclass.local** user.
5. In the Roles pane, select **Network Engineer** from the **Roles** drop-down menu .
6. Click **SAVE**.
7. ~~At the upper-right corner of the NSX UI, click the **admin** user and select **Log out.**~~
   Open a private browsing / incognito window to test this other user
8. Log in to the NSX UI at https://sa-nsxmgr-01.vclass.local as jdoe.
   a. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
   b. Enter **`jdoe@vclass.local`** as the user name and enter **`VMware1!`** as the password.
   c. Click **LOG IN.**
9. In the upper-right corner of the NSX UI, verify that you are logged in as jdoe@vclass.local.
10. Navigate to **Networking** > **Connectivity** > **Tier-1 Gateways** and verify that the **ADD TIER-1 GATEWAY** option is available.

    The availability of the option indicates that users with the Network Engineer role have permissions to configure Tier-1 gateways.
11. Navigate to **Security** > **East West Security** > **Distributed Firewall**.
12. Click **CATEGORY SPECIFIC RULES** and click the **APPLICATION** tab.
13. Click **+ADD POLICY**.

    The unavailable option indicates that users with the Network Engineer role do not have permissions to configure distributed firewall policies or rules.
14. ~~In the upper-right corner of the NSX UI, click the **jdoe@vclass.local** user and select **Log out.**~~

- Return to the web page where you are logged in as the admin user. Make jdoe a security engineer.
- Return to the web page where you are logged in as jdoe, refresh the browser and create a policy for the Distributed Firewall and a new rule in this policy. (Name test 1 for both, rule content not important.) Publish this change.
- Switch to the admin user and create another policy with a rule (name test 2 for both, rule content not important.) Publish this change
- Return to the web page for jdoe and from the Actions menu in the Distributed Firewall choose Configurations - View. Find the configuration from two saved points back where your new policies did not exist. Load that policy and verify the result. Publish your changes to enable the restored configuration.

- Switch to the browser for the admin user, create a policy with a rule and lock that policy. Publish your changes
- Switch to the jdoe user's web page and try to load a previously saved configuration. This will be prevented because of the locked policy
- Return to the admin web page and remove the lock on the policy
- Set the default rule (nr 2) to allow all traffic for remaining labs