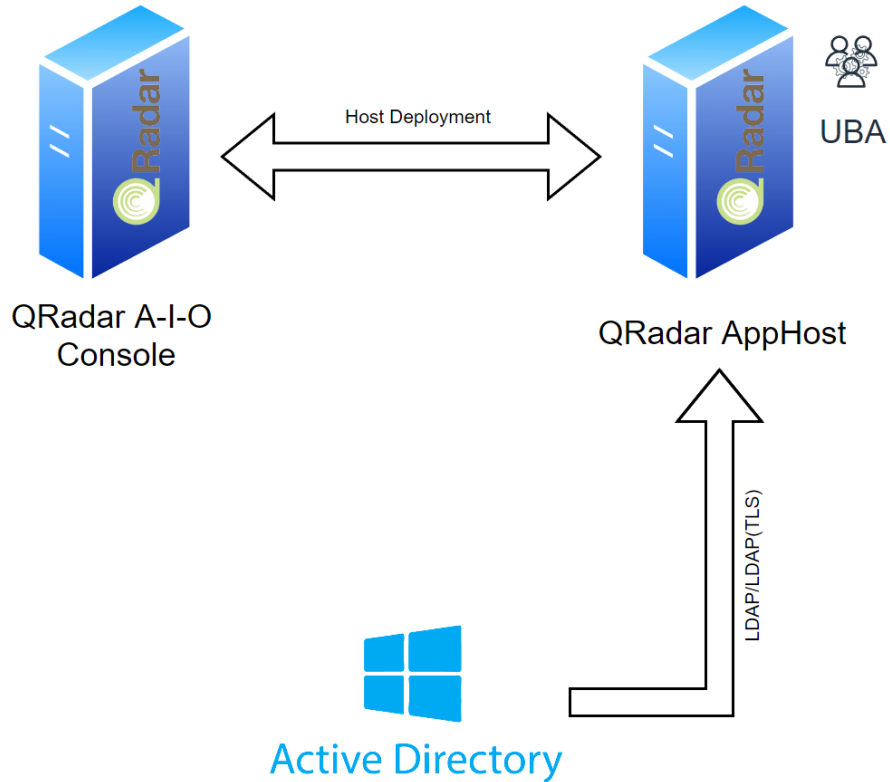


UBA Import Users using AD/LDAP

Lab Deployment & Software details



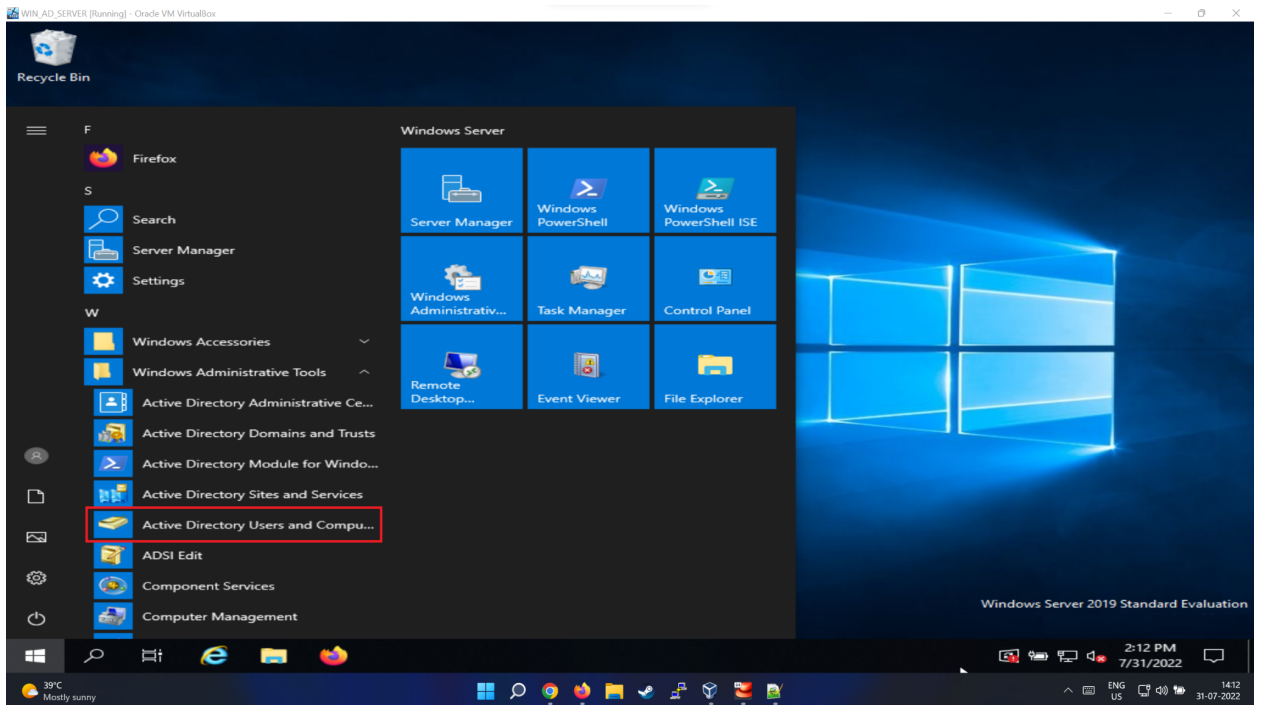
QRadar 7.4.3 All-in-One Console
QRadar 7.4.3 APPHOST
Windows Server 2019
VirtualBox

Prerequisites for user imports to UBA using LDAP/AD

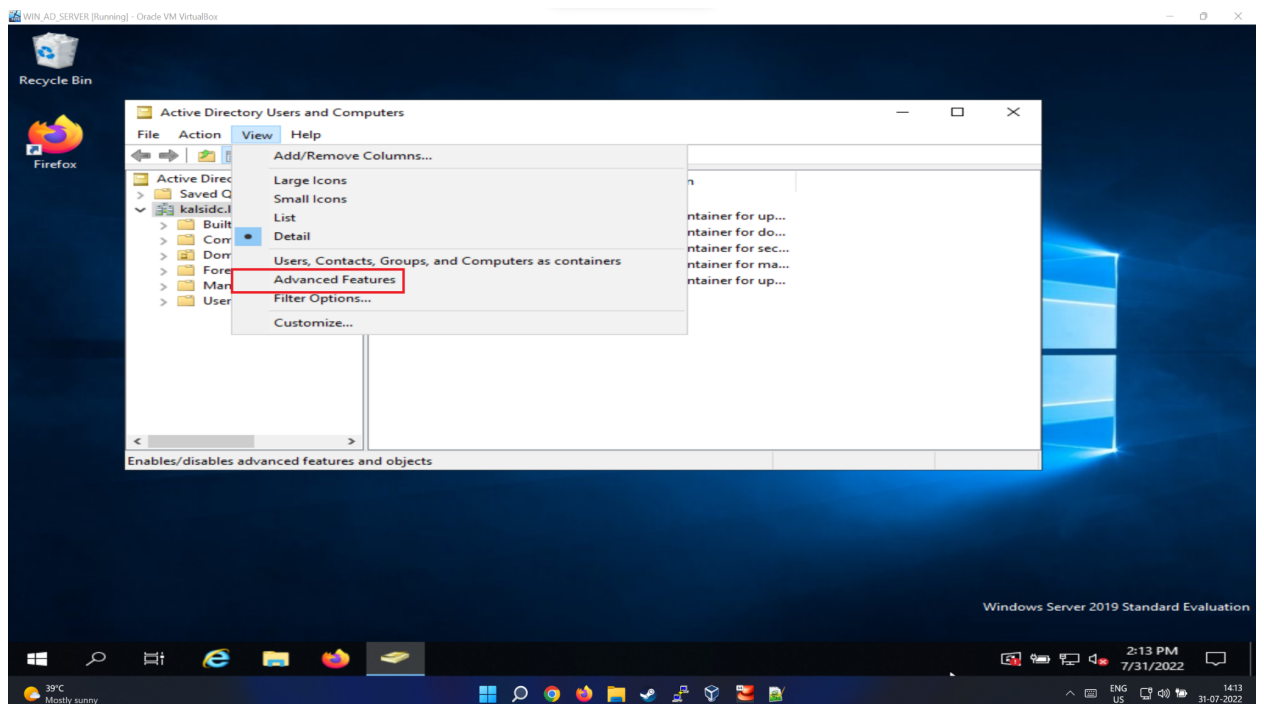
LDAP/AD - <IP or Hostname>
Username - <Bind DN Format>
Password
Base DN
Filter - (&(sAMAccountName=*)(samAccountType=805306368))

1. Creating User for UBA authentication

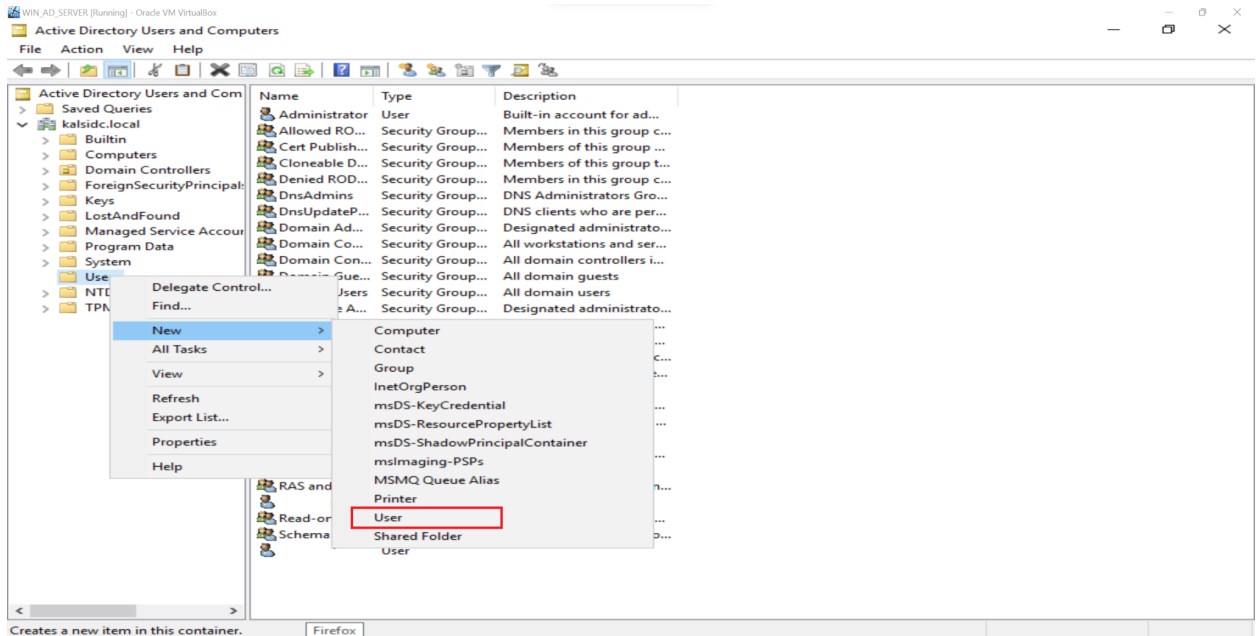
1.1. Select Start->Windows Administrative Tools->Active Directory Users and Computers



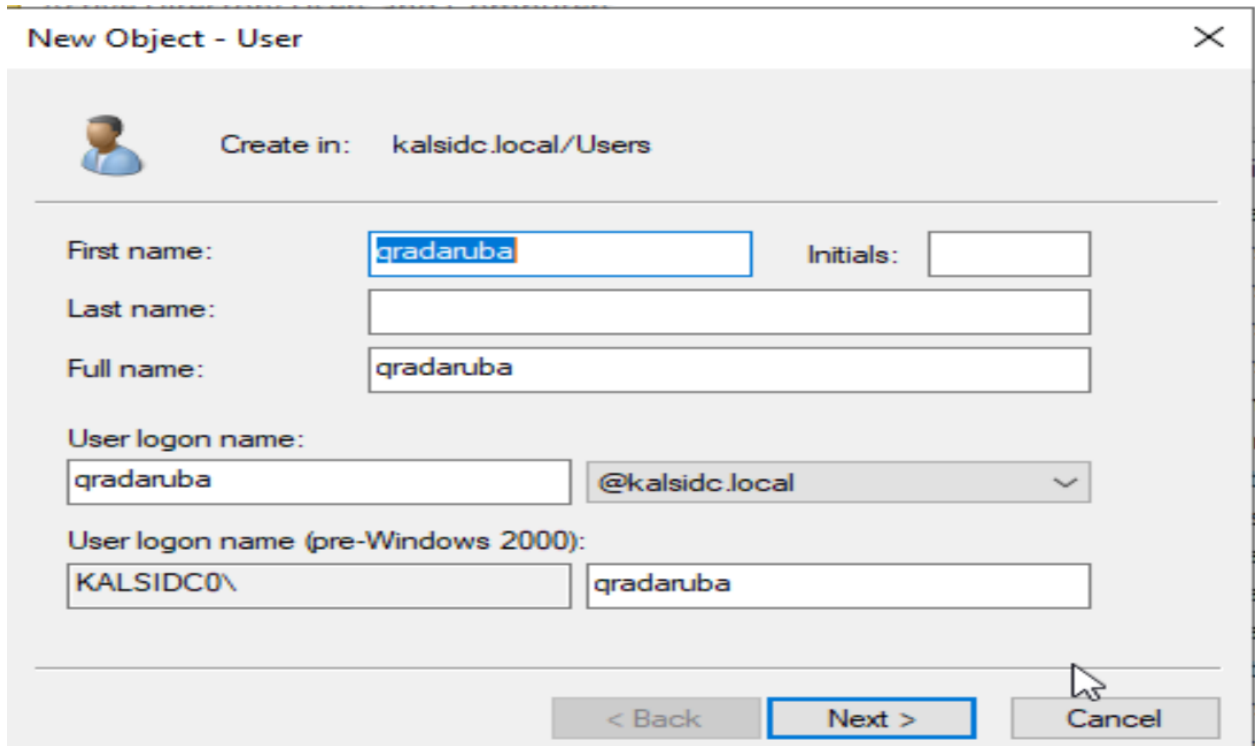
1.2. Select View->Advanced Feature.(ignore this step if already selected)



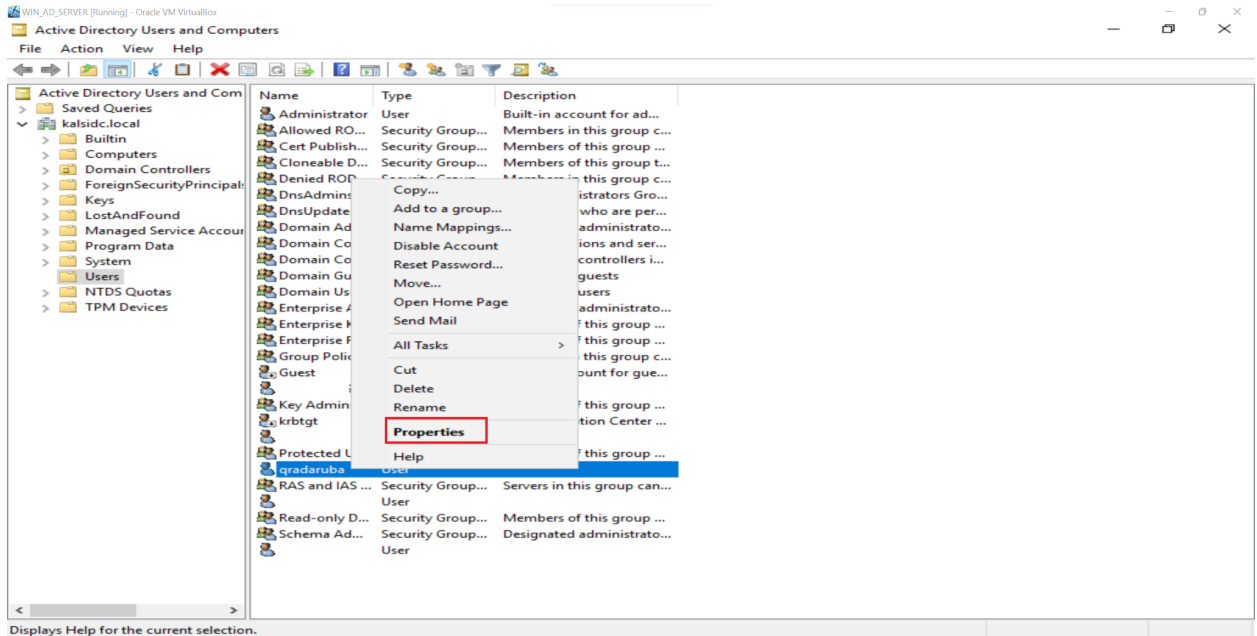
1.3. Create new user by Right Click on Users->New->User



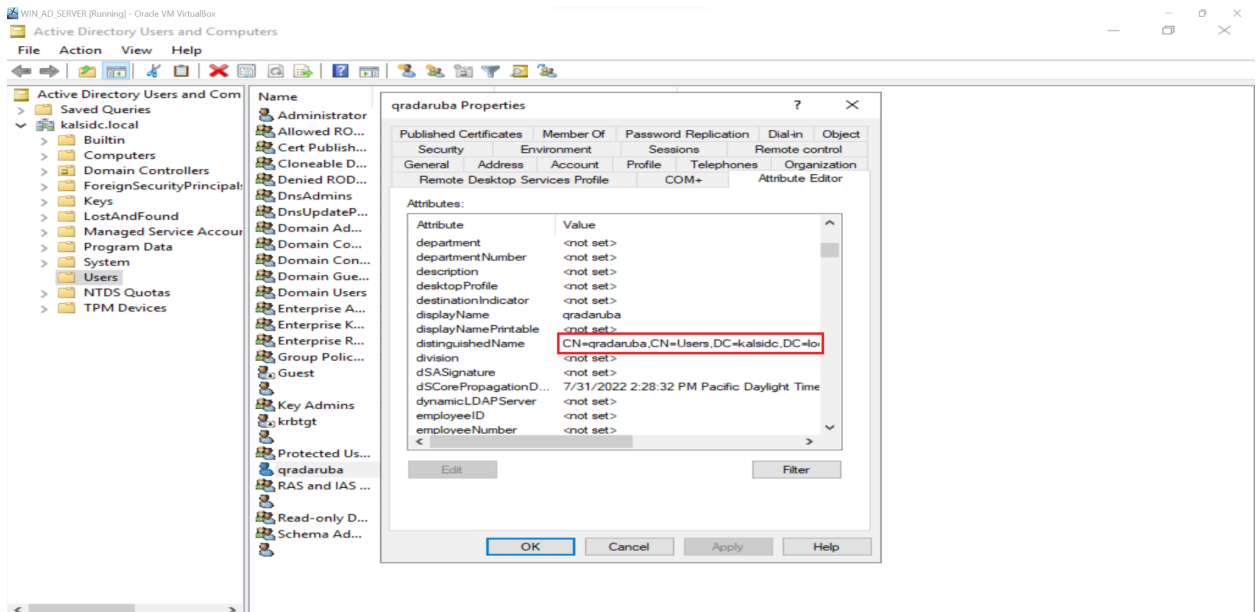
1.4. Create a user with any name - In our case we used username "qradaruba". Without any special privilege



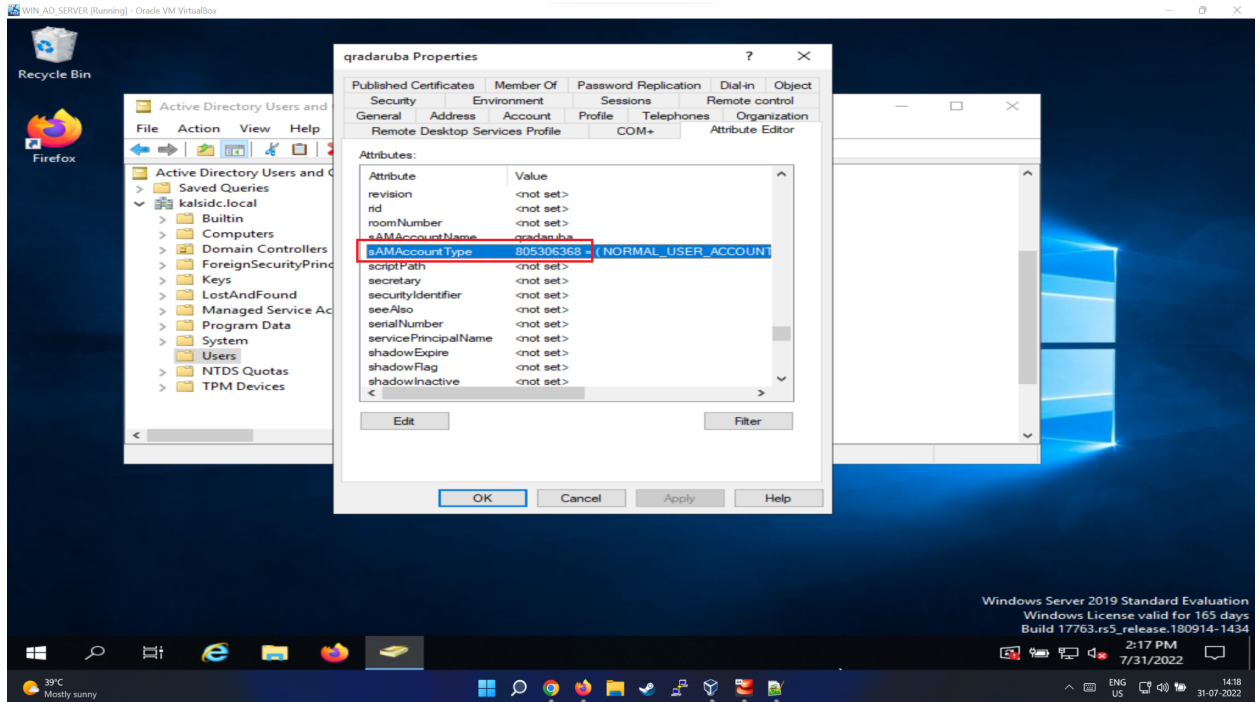
1.5. Select the properties option of user “qradaruba”



1.6. Copy the username in Bind DN format. E.g., CN=qradaruba,CN=Users,DC=kalsidc,DC=local

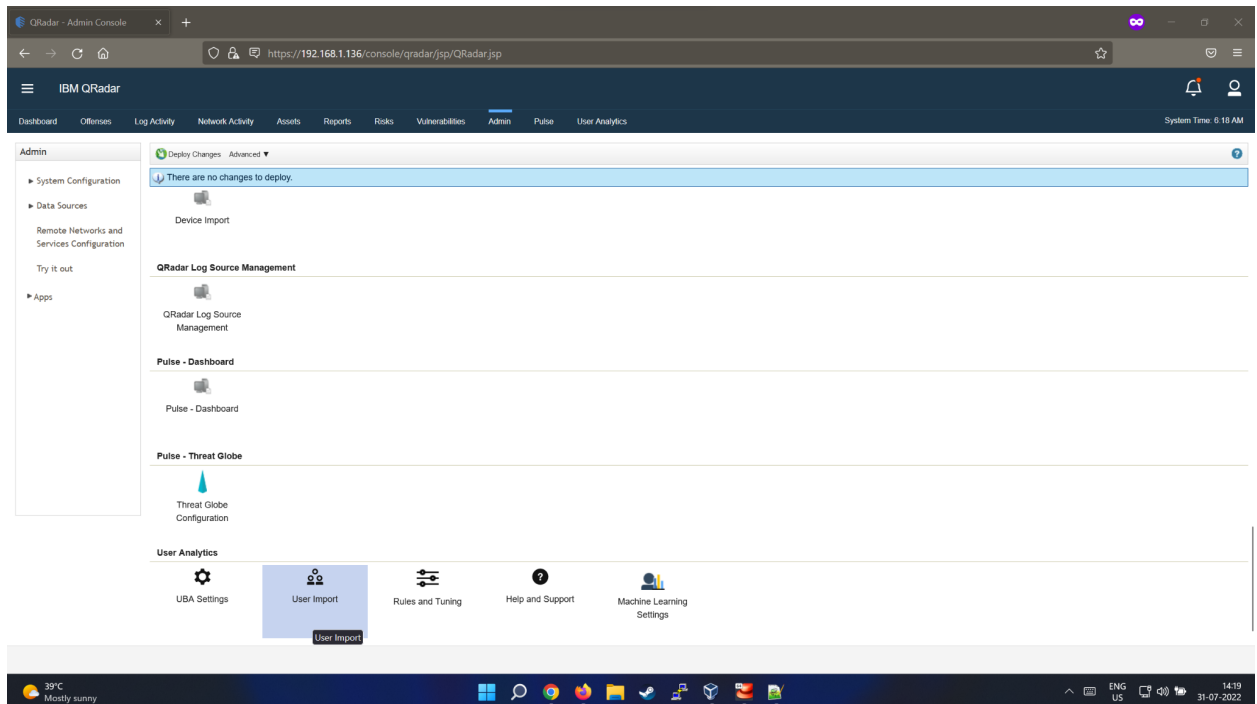


1.7. Copy the sAMAccountType
E.g., (sAMAccountType=805306368)

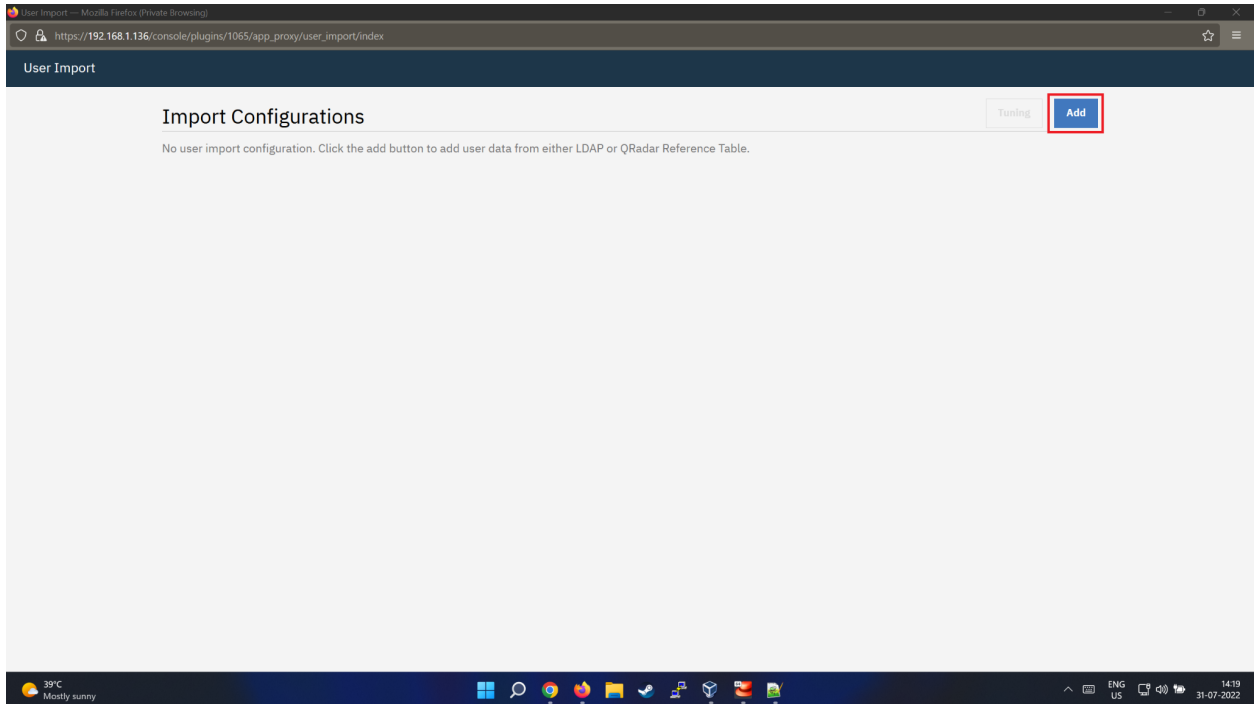


2. Configuring User Import in QRadar using AD Authentication

2.1. Login to QRadar->Admin Tab->User Import



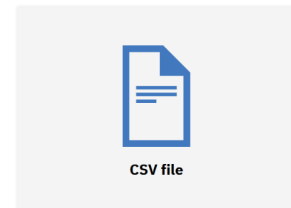
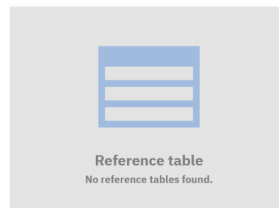
2.2. Select Add



2.3. Select LDAP/AD Option



Which source do you want to import user data from?



2.4. Enter the required details gathered from step 1.6. And 1.7.

User Import > Add

LDAP server configuration

Enter the LDAP server information to retrieve user data. Before going to the next step, click Test connection.

Protocol: ldap:// LDAP server host: example ldap.com Port: 389

Username (Bind DN):
Password:

> Advanced settings

Test connection

A sample LDAP will appear after you test the connection.

Next

2.5. Validate below details

User Import > Add

LDAP server configuration

Enter the LDAP server information to retrieve user data. Before going to the next step, click Test connection.

Protocol: ldap:// LDAP server host: 192.168.1.129 Port: 389

Username (Bind DN): cn=qradaruba,cn=Users,cn=kalsidc,cn=local

Password:

Advanced settings

Base DN: cn=Users,cn=kalsidc,cn=local

Filter: (&(sAMAccountName=*)(samAccountType=805306368))

Certificate: Click to upload the certificate file for the root certificate authority. File size is limited to 10 KB.

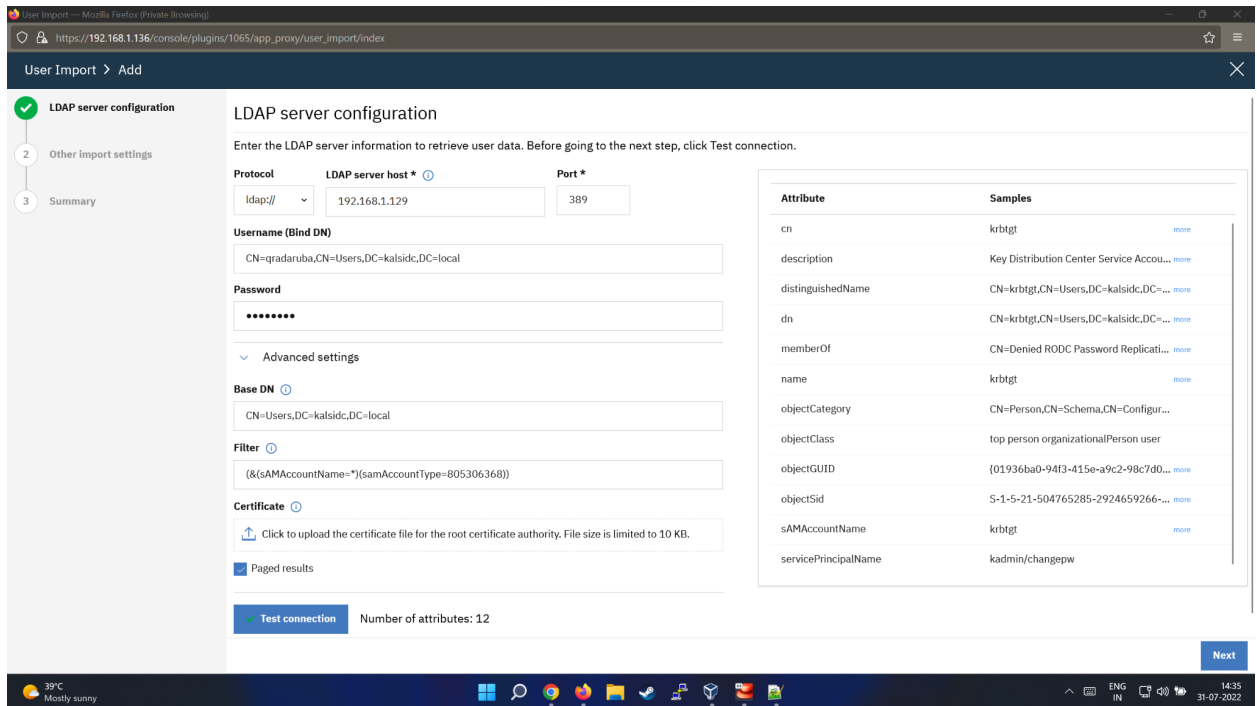
Paged results

Test connection

A sample LDAP will appear after you test the connection.

Next

2.6. Run test connection



The screenshot shows the 'LDAP server configuration' step in a user import process. The interface includes a sidebar with steps: 1. LDAP server configuration (active), 2. Other import settings, and 3. Summary. The main area contains the following fields and options:

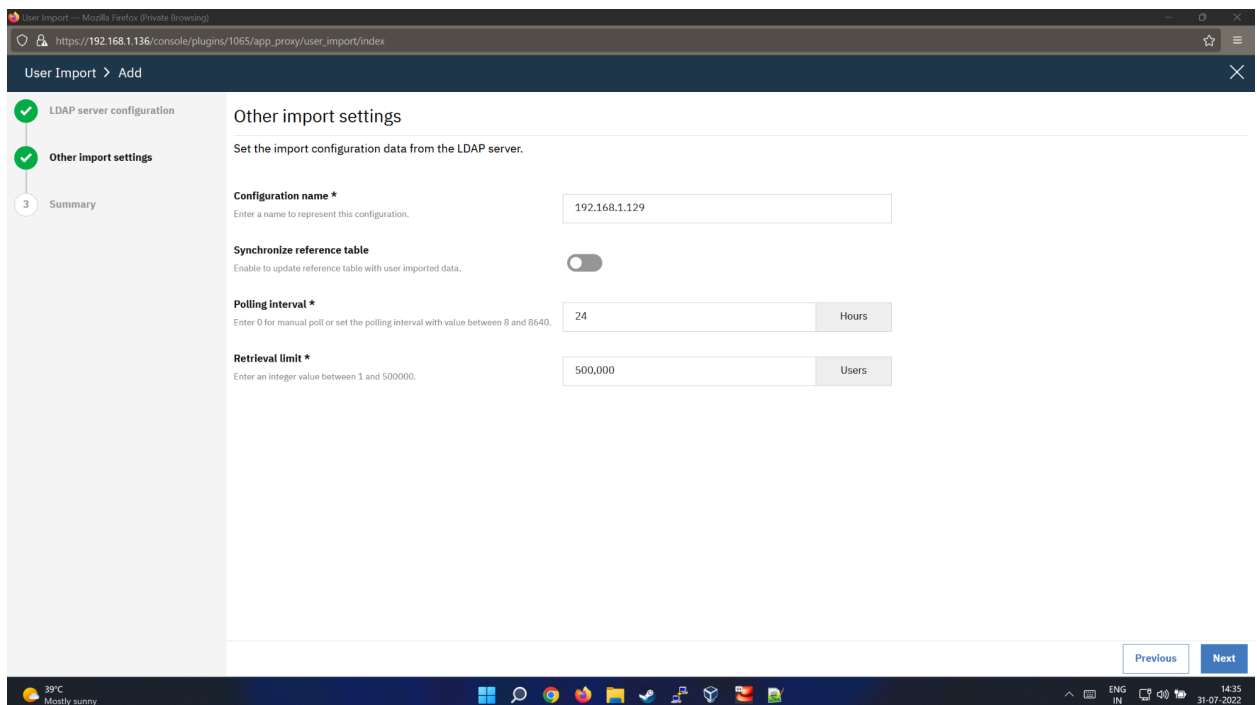
- Protocol:** ldap://
- LDAP server host *:** 192.168.1.129
- Port *:** 389
- Username (Bind DN):** CN=qradaruba,CN=Users,DC=kalsidc,DC=local
- Password:** [Redacted]
- Advanced settings:** Expanded to show:
 - Base DN:** CN=Users,DC=kalsidc,DC=local
 - Filter:** (&(sAMAccountName=*)(samAccountType=805306368))
 - Certificate:** [Upload button]
 - Paged results
- Test connection:** A button that has been clicked, showing 'Number of attributes: 12'.

On the right, a table displays LDAP attributes and their sample values:

Attribute	Samples
cn	krbtgt
description	Key Distribution Center Service Account...
distinguishedName	CN=krbtgt,CN=Users,DC=kalsidc,DC=...
dn	CN=krbtgt,CN=Users,DC=kalsidc,DC=...
memberOf	CN=Denied RODC Password Replicati...
name	krbtgt
objectCategory	CN=Person,CN=Schema,CN=Configur...
objectClass	top person organizationalPerson user
objectGUID	{01936ba0-94f3-415e-a9c2-98c7d0...
objectSid	S-1-5-21-504765285-2924659266-...
sAMAccountName	krbtgt
servicePrincipalName	kadmin/changepw

At the bottom, there is a 'Next' button and a system tray showing 39°C and 'Mostly sunny'.

2.7. After successful test, choose the required settings

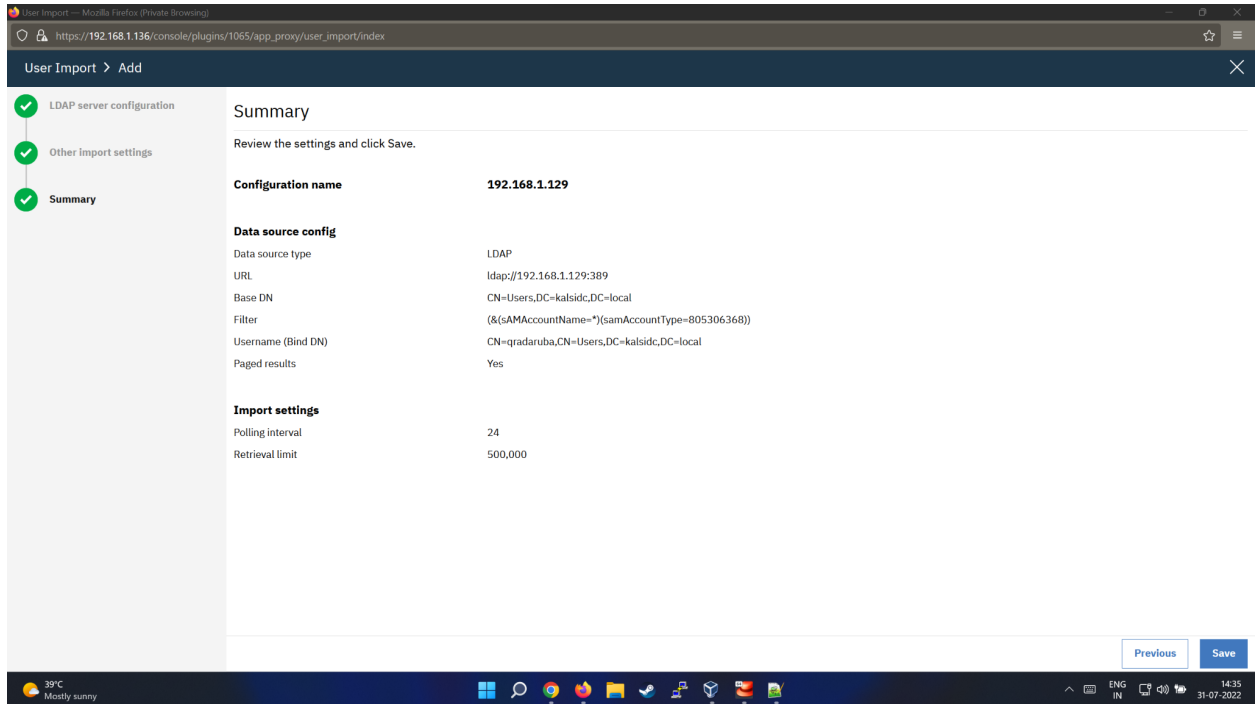


The screenshot shows the 'Other import settings' step in the user import process. The sidebar now highlights step 2: Other import settings. The main area contains the following configuration options:

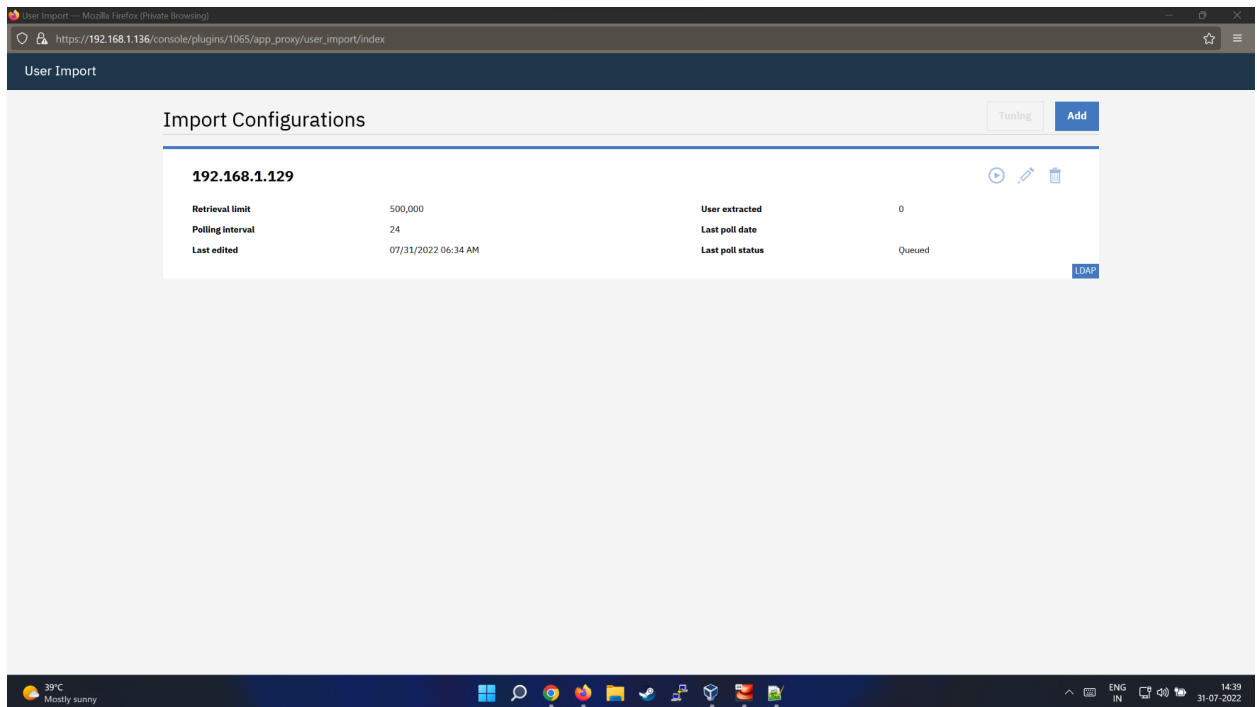
- Configuration name *:** 192.168.1.129
- Synchronize reference table:** A toggle switch is currently turned off.
- Polling interval *:** 24 Hours
- Retrieval limit *:** 500,000 Users

At the bottom, there are 'Previous' and 'Next' buttons, and the system tray shows 39°C and 'Mostly sunny'.

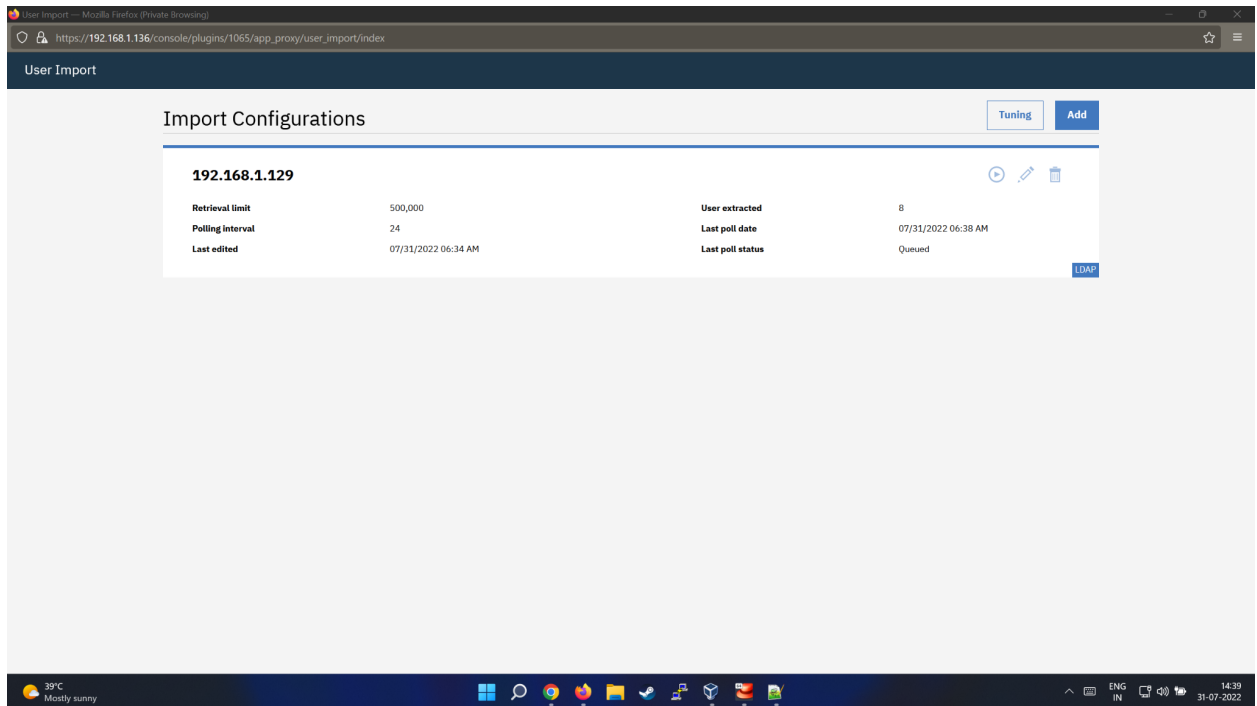
2.8. Review the summary of connection & Save.



2.9. Connection is ready for AD. Select Start option and wait for several minutes.



2.10. Wait for "Idle" result for Last poll status



2.11. User Import activity completed.

