Lab Exercise 3: ISE Admin CLI Access by Active Directory Users

ISE 2.6 adds support to authenticate users to the Admin CLI of an ISE node by a single AD domain. This reduces the overhead of maintaining local users on each of ISE nodes in the deployment.

3.1: Configure AD Users with uidNumber and gidNumber

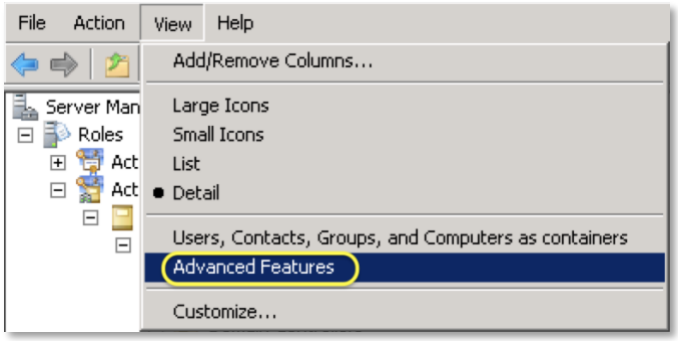
In order to grant ISE Admin CLI access, each of the permitted AD users need the attribute uidNumber set to some unique numeric value (a value greater than *60,000* recommended) and the attribute gidNumber set to either *110* (ISE CLI admin with full administrative role privileges) or *111* (ISE CLI user with read-only role privileges).

Step 1 If the previous remote desktop session to the AD still open, resume it. Otherwise, from the admin PC desktop, use Remote Desktop (mstsc.exec) to access AD (10.1.100.10).

Step 2 Login as admin / `ISEisC00L`

Step 3 (AD RDP) Either use the Server Manager window to navigate to **Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers [ad.demo.local] > demo.local**. Or, launch **Active Directory Users and Computers** via **Start > Administrative Tools**, and then navigate to the same location.

Step 4 (AD RDP) In order to show the Attribute Editor in a user's properties, enable **Advanced Features** under the menu **View**.



Configure staff1 and staff2 with ISE CLI Admin Role

Step 5 (AD RDP) From ***demo.local***, navigate to **HCC > Users > staff1**.

Step 6 (AD RDP) Double click on the user name *staff1* to open its properties.

Step 7 (AD RDP) Select the tab Attribute Editor in the properties window.

Step 8 (AD RDP) Click any attribute and then start typing *gid* to locate the attribute ***gidNumber***. If no gidNumber attribute found, click on the button [Filter] and un-tick [Show only attributes that have values]. Double click on the attribute *gidNumber* to edit. Replace the value <not set> with ***110*** (ISE CLI admin), and click [OK].

Step 9 (AD RDP) While the focus on *gidNumber*, start typing uid to locate the attribute ***uidNumber*** right below *uid*. Double click on *uidNumber* to edit. Replace the value <not set> with ***60001***, and click on [OK]. Click another [OK] to finalize the changes to *staff1* and to close the properties window.

Step 10 (AD RDP) Repeat Steps 5 to 9 for *staff2* but set the uidNumber to ***60002*** for *staff2*.

Configure user1 and user2 with ISE CLI User Role

Step 11 (AD RDP) Repeat Steps 5 to 9 for *user1* but set the gidNumber to ***111*** (ISE CLI user) and the uidNumber to ***60101*** for *user1*.

Step 12 (AD RDP) Repeat Steps 5 to 9 for *user2* but set the gidNumber to ***111*** (ISE CLI user) and the uidNumber to ***60102*** for *user2*.

Step 13 Minimalize the remote desktop window to AD.

3.2: Join ISE Admin CLI to AD domain

ISE 2.6 introduces this feature with a new CLI configuration command ***identity-store active-directory domain-name*** <*aDomainFQDN*> ***user*** <*adUserNameWithJoinPrivs*>. ISE 2.6 supports this feature with one and only one AD domain for each ISE node. We need perform this join operation individually at the ISE admin CLI for each of the ISE nodes in the deployment. If the same AD domain already joined in ISE admin web UI, we need to re-join again after the join operation in ISE admin CLI. Also, ISE updates the cache every 5 minutes so please allow 5 minutes to ensure the changes in AD synchronized to ISE.

Step 14 (ADMIN) If the PuTTY session to ISE ended, open a PuTTY new session to SSH to ise-1 (*fd0a::15*) and login as admin / *ISEisC00L*

Step 15 (ISE CLI) Once logged-in, join it to *demo.local* as below:

```
ise-1/admin# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ise-1/admin(config)# identity-store active-directory domain-name demo.local user admin
If the domain demo.local is already joined via UI, then you must rejoin the domain demo.local from UI
after this configuration. Until the rejoin happens, authentications to demo.local will fail
Do you want to proceed? Y/N [N]: Y
Password for admin: ISEisC00L
Joined to domain demo.local successfully
ise-1/admin(config)# end
```

3.3: Test AD User Login to ISE Admin CLI

Step 16 (ADMIN) Open a PuTTY new session to SSH to ise-1 (*fd0a::15*) and login as *staff1* / *ISEisC00L*

Step 17 (ISE CLI as staff1) Once logged-in, issue '?' at the command prompt to see what's available. As shown below, we should see a full set of the exec commands.

```
ise-1/staff1# ?
Exec commands:
  application   Application Install and Administration
  backup        Backup system
  backup-logs   Backup system and application logs
  banner        Configure login banners
  clock         Set the system clock
  configure     Enter configuration mode
  copy          Copy commands
  crypto        Crypto operations
  debug         Debugging functions (see also 'undebug')
  delete        Delete a file
  dir           List files on local filesystem
  esr           Enter the Embedded Services Router console
  exit          Exit from the EXEC
  forceout      Force Logout all the sessions of a specific system user
```

```
  halt           Shutdown the system
  license        License operations
  mkdir          Create new directory
  nslookup       DNS lookup for an IP address or hostname
  password       Update password
  patch          Install System or Application Patch
  ping           Ping a remote ip address
  ping6          Ping a remote ipv6 address
  reload         Reboot the system
  reset-config   Reset network and time settings
  restore        Restore system
  rmdir          Remove existing directory
  show           Show running system information
  ssh            SSH to a remote ip address
  tech           TAC commands
  terminal       Set terminal line parameters
  traceroute     Trace the route to a remote ip address
  undebug        Disable debugging functions (see also 'debug')
  write          Write running system information


ise-1/staff1#
```

Step 18 (ADMIN) Open a PuTTY new session to SSH to ise-1 (*fd0a::15*) and login as *user1* / *ISEisC00L*

Step 19 (ISE CLI as user1) Once logged-in, issue '?' at the command prompt to see what's available. As shown below, we should see a limited set of the exec commands.

```
ise-1/user1> ?
Exec commands:
  crypto       Crypto operations
  exit         Exit from the EXEC
  license      License operations
  nslookup     DNS lookup for an IP address or hostname
  password     Update password
  ping         Ping a remote ip address
  ping6        Ping a remote ipv6 address
  show         Show running system information
  ssh          SSH to a remote ip address
  terminal     Set terminal line parameters
  traceroute   Trace the route to a remote ip address

ise-1/user1>
```

3.4: Re-Join ISE Auth Services to AD domain

ISE Authentication Services were previously joined to *demo.local* so we need repeat the join after ISE Admin CLI joined to *demo.local*.

Step 20 (ADMIN) If the browser window to ISE admin web console ended, use Google Chrome to access ise-1 admin Web console at https://[fd0a::15]/admin, select the Identity Source *Internal*, and login as admin / *ISEisC00L*

Step 21 (ISE Web) Navigate ISE admin web to **Administration > Identity Management > External Identity Sources**.

Step 22 (ISE Web) In the left-hand pane, select **Active Directory > demoAD**.

Step 23 (ISE Web) In the right-hand pane, the status for *ise-1.demo.local* might appear *Operational*, but we will receive errors by performing **Test User** with either MS-RPC or Kerberos authentication type. Below shows a sample authentication result with MS-RPC:

```
Test Username            : employee1
ISE NODE                 : ise-1.demo.local
Scope                    : Default_Scope
Instance                 : demoAD

Authentication Result    : FAILED

Error                    : An Error was encountered when negotiating with RPC


Processing Steps:
04:43:34:195:  Resolving identity - employee1
04:43:34:195:  Search for matching accounts at join point - demo.local
04:43:34:197:  Single matching account found in forest - demo.local
04:43:34:197:  Identity resolution detected single matching account
04:43:34:201:  RPC Logon request failed - STATUS_ACCESS_DENIED,ERROR_RPC_ERROR,employee1@demo.local
04:43:34:201:  Communication with domain controller failed - ad.demo.local,ERROR_RPC_ERROR
04:43:34:206:  RPC Logon request failed - STATUS_ACCESS_DENIED,ERROR_RPC_ERROR,employee1@demo.local
04:43:34:206:  Communication with domain controller failed - ad.demo.local,ERROR_RPC_ERROR
04:43:34:211:  RPC Logon request failed - STATUS_ACCESS_DENIED,ERROR_RPC_ERROR,employee1@demo.local
04:43:34:211:  Communication with domain controller failed - ad.demo.local,ERROR_RPC_ERROR
04:43:34:211:  Failover threshold has been exceeded
```

Step 24 (ISE Web) In order to re-join, we leave ISE from demo.local. In the right-hand pane, select the ISE node ☑ ise-1.demo.local and click on the tool icon [Leave]. In the pop-up [Leave Domain], select ☑ Leave domain without credentials and click [OK]. Wait until the node status **Completed**, and then [Close] the Leave Operation Status window.

Step 25 (ISE Web) In the right-hand pane, select the ISE node ☑ ise-1.demo.local and click on the tool icon [Join].

Step 26 (ISE Web) In **Join Domain** pop-up window, fill in

* AD User Name	***admin***
* Password	***ISEisC00L***
☐ Specify Organization Unit	
☐ Store Credentials	

Step 27 (ISE Web) Click **OK** to start the join operation. A window **Join Operation Status** will pop up. Wait until the node status turns **Completed**, and then click **Close**.

Step 28 (ISE Web) The **Connection** tab shall show *ad.demo.local* as the domain controller and Default-First-Site-Name as the site.

Step 29 (ISE Web) Repeat the Test User with MS-RPC for employee1 (password ***ISEisC00L***) to verify no error. Below is a sample authentication result:

```
Test Username            : employee1
ISE NODE                 : ise-1.demo.local
Scope                    : Default_Scope
Instance                 : demoAD

Authentication Result    : SUCCESS

Authentication Domain    : demo.local
User Principal Name      : employee1@demo.local
User Distinguished Name  : CN=employee1,OU=Users,OU=HCC,DC=demo,DC=local

Groups                   : 4 found.
Attributes               : 37 found.

Authentication time      : 27 ms.
```

```
Groups fetching time     : 6 ms.
Attributes fetching time: 10 ms.
```

Step 30 Repeat *3.3: Test AD User Login to ISE* Admin CLI to ensure CLI admin access still OK.

☑ End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 4: Manufacture Usage Description

Manufacture Usage Description (MUD) Phase 1 is included in ISE 2.6. MUD is an authoritative identifier of IoT devices on the network, as it allows manufacturers to expose the identity and intended use of their devices using an IETF approved standard. This bridges the gap between the manufacturer and the user, and facilitates a level of trust and security that network and security administrators truly value. Device manufacturers can thus enhance the security of their devices, and Integrators can leverage this to segment a network with 'Things.'

This exercise is **OPTIONAL** and it go through the MUD sandbox available at Cisco DevNet.

4.1: MUD at Cisco DevNet

The info on MUD is at Cisco DevNet https://developer.cisco.com/site/mud/. Go to the URL above, and scroll down to the section ***Try out MUD in the Sandbox***. Click on [Try it out] and reserve a session.

4.2: Access MUD Sandbox

We may use the AnyConnect VPN client on our own MAC/PC to connect to the sandbox environment or that on the VM wx-corp. Below shows the steps using wx-corp.

Step 1 (ADMIN) If VMware vSphere client not yet connected to the local ESXi at `10.0.0.1`, locate the desktop short-cut **ESXi-core** and double click on it.

Step 2 (vSphere) Once it connected, use the Virtual Machine tab to sort by State with "Powered-On" on top, and look for the VM p##_**wx-corp**, where ## denotes your pod number.

Step 3 (vSphere) Right click on the VM name and select Open Console from the context menu.

Step 4 (wx-corp console) In the VM guest console window, use menu **VM > Guest > Send Ctrl-Alt-del**. Then, login as admin / *`ISEisC00L`*

Step 5 (wx-corp console) Double-click on the desktop short-cut **wx-corp Network Connections**. Verify that the **inside** interface is enabled while the **outside** interface is disabled.

Note 1 The outside interface is used in another lab to test for remote-access VPN.

Step 6 (wx-corp console) Use the sandbox VPN credentials provided by the proctor(s) to connect to the sandbox.

Step 7 (wx-corp console) Use Firefox and go to http://10.10.20.40/, once VPN connected.

Step 8 (wx-corp console) In the bottom of the page, select ⊙ **Demo** and [Submit]

Step 9 (wx-corp console) Scroll down, and click [Submit to ISE]

4.3: Check IoT Endpoint Created by MUD

Step 10 (wx-corp console) Use Firefox and go to the sandbox ISE web console at https://10.10.20.70 and login as admin/*`C1sco12345!`*

Step 11 (wx-corp console) Navigate to **Context Visiblity** > **Endpoints**

Step 12 (wx-corp console) Click on the MAB address of the only endpoint shown to drill into its details.