STONE
DOOR
GROUP

Stone Door Group - Red Hat Infrastructure for Windows Administrators - Technical Workshop

Integrating RHEL and Windows

5 May 2020

Exercise 1: Lab preparation steps

Task 1: Log into the bastion host and provision the lab systems

1. Log into the bastion host (bastion01.demo1.pd.stonedoor.io) or (3.12.147.128) using ssh, putty, or MobaXterm. Use the user account and password provided to you.
   user##
   sdg2020

2. Run the following commands to provision your lab systems

```
[user##@bastion01 rh-infra-lab]$ git clone \
https://github.com/hightechrdn/rh-infra-lab

[user##@bastion01 rh-infra-lab]$ cd rh-infra-lab; ansible-playbook \
deploy-lab-rh-infra-windows-admins.yml
```

NOTE### The last TASK of the playbook displays the UUID you will be using throughout this workshop. It also lists the name of the txt file (/lab01/????-lab-environment.txt) that has the host names and IP addresses for your lab systems. The UUID is part of the domain name for your hosts. Using a text editor on your local workstation or laptop (I recommend Atom or notepad++) , create a local text file. Give the file a name you will remember. Record the UUID in your local text file

Several places in this lab guide you will see host or domain names that look similar to this:

rhel8-client-0.????.demo1.pd.stonedoor.io

Every time you see the characters, "????" replace the "????" with the UUID you recorded in your local text file. For example, if your UUID is "2f0d" you would change the host name to:

rhel8-client-0.2f0d.demo1.pd.stonedoor.io

The /lab01/????-lab-environment.txt file has the IP address information for the hosts you will be using for your labs.
END NOTE###

3. Remember to replace the ???? characters with the UUID when running the following command to display the contents of your /lab01/????-lab-environment.txt file:

   [user##@bastion01 rh-infra-lab]$ cat /lab01/????-lab-environment.txt

4. In your local text file, record the IP addresses and host names from your /lab01/????-lab-environment.txt file arranged like the example below:

   ```
   10.0.???.???   rhel8-client-0.????.demo1.pd.stonedoor.io
   10.0.???.???   rhel8-idm-server0.????.demo1.pd.stonedoor.io
   10.0.???.???   rhel7-sat6-server-0.????.demo1.pd.stonedoor.io
   ```

5. Leave the ssh, putty, or MobaXterm session connected to your bastion host open. Leave your local text file open.

Exercise 2: Satellite 6.7 Server configuration steps

Task 1: Log into the bastion host and launch the Satellite 6.7 webUI

1. Connect to the bastion host with the user account and password provided to you using an RDP client.

   bastion01.demo1.pd.stonedoor.io
   or
   3.12.147.128

2. When you have connected to the bastion host using an RDP client, click on the word, "Activities" in the upper left corner of the screen. This will open a side bar with some icons along the middle of the left side of the screen. This may take a few seconds so be patient.

3. Click on the Firefox icon in the side bar on the left side of your screen

4. Input the IP address of your Satellite 6.7 server into the URL bar of the Firefox Browser

   A web page will display a warning message: "Warning: Potential Security Risk Ahead"

5. Click the "Advanced" button in the lower right side of that warning web page which will cause additional information and buttons to be added to the bottom of the web page

6. Scroll down and click the "Accept the Risk and Continue" button

   The Red Hat Satellite Login page will be displayed

7. Login as the user account "**admin**" with the password "**redhat**"

8. Click the button for Firefox to save the admin login

   You are now looking at the Red Hat Satellite 6.7 Dashboard
   There are several Main tabs along the left side of the page. If you hold your mouse pointer over a Main tab, the sub-tabs for that main tab will be displayed.

Task 2: Import a Red Hat subscription manifest

1. Click on the "Content" main tab and then the "Subscriptions" sub-tab

2. Click the "Manage Manifest" button and then the "browse" button

3. Navigate to the home directory for your user. /home/user##

4. Double click the manifest zip file to start the import process. The name of the manifest zip file should look very similar to this:
   "manifest_sdg-rh-infra-lab-1_20200501T??????Z.zip"

   When the manifest import process finishes, you will have a total of five Red Hat entitlements

Task 3: Enable and synchronize a Red Hat repository into the Satellite 6.7 server

1. Click on the "Content" main tab and the "Red Hat Repositories" sub-tab

2. Input "**satellite-tools-6.7-for-rhel-8-x86_64-rpms**" in the search window

3. Click the small ">" to the left of "Red Hat Satellite tools 6.7 for RHEL 8 x86_64 (RPMs)"

4. Click the blue plus sign to Enable the "Red Hat Satellite tools 6.7 for RHEL 8 x86_64 (RPMs)" repository

5. Click the "Content" main tab and the "Sync Status" sub-tab

6. Click "Select All" and then the "Synchronize Now" button

7. Wait for the Satellite Tools Repository synchronization to finish

8. Click on the "Content" main tab and the "Red Hat Repositories" sub-tab

9. Input "**rhel-8-for-x86_64-baseos-rpms**" in the search window

10. Click the small ">" to the left of "Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)"

11. Click the blue plus sign next to x86_64 8 to Enable the "Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)" repository

12. Click the "Content" main tab and the "Sync Status" sub-tab

13. Click “Expand All” and "Select All" and then click the "Synchronize Now" button

    You do NOT need to wait and watch it until it finishes. Move on to Task 4

Task 4: Create a subscription activation key to use when registering the RHEL 8 client host

1. Click on the "Content" main tab and then the "Activation Keys" sub-tab

2. Click on the blue "Create Activation Key button"

   Clicking the "Create Activation Key" button will open a new web page where you will create and define the Activation Key details.

You can name your Activation Key anything you want.
We recommend giving your Activation Key a name that identifies the OS version and purpose of the Activation Key when working on Satellite servers in your corporate environments. For this lab, we will keep things simple.

3. Enter “**55ak**” in the "Name" field

4. Click in the check box next to "Library" which will open up a selection box under "Content View"

5. Select "Default Organization View" in the selection box and then click the "Save" button

   Clicking the "Save" button will open a new web page where you will define the Activation Key configuration. There are several key word/tabs near the top of this page. You are now in the primary "Details" tab.

6. Click on the "Subscriptions" key word/tab of the 55ak and click on "Add"

7. Click in the top left checkbox right next to the word "Quantity", this will select all subscriptions and then click the "Add Selected" button

8. Click on the "Repository Sets" key word/tab

9. Click in the check box next to "Red Hat Satellite tools 6.7 for RHEL 8 x86_64 (RPMs)" to select it

10. Click the "Select Action" button and select "Override to enabled" from the drop-down list

Task 5: Define an Operating System to be used to register the RHEL 8 Client host with the Satellite 6.7 server

1. Click the "Hosts" main tab and the "Operating Systems" sub-tab

2. Click the blue "Create Operating System" button near the upper right corner

   Clicking the "Create Operating System" button will open a new web page where we will create and define the Operating System details. There are several key word/tabs at the top of this page. You are in the primary "Operating System" tab to start the process of creating an Operating System

3. Input "**RHEL_8.2**" in the Name field
4. Input "**8**" in the "Major Version" field
5. Input "**2**" in the "minor Version" field
6. Input "**RedHat 8.2**" in the "Description" field
7. Select "Red Hat" in the "Family" field
8. Click "x86_64" in the Architectures "All Items" box which will move it to the "Selected Items" box
9. Click the key word/tab "Partition Table"
10. Move "Kickstart Default" from the "All Items" box to the "Selected Items" box
11. Click the key word/tab "Installation Media"
12. Move "Fedora mirror" from the "All Items" box to the "Selected Items" box
13. Click the "Submit" button

Task 6: Create a Host Group which will be used to register the RHEL 8 Client host with the Satellite 6.7 server

1. Click the "Configure" main tab and the "Host Groups" sub-tab
2. Click the blue "Create Host Group" button
3. Click the blue "Create Host Group" button near the middle of the page

   Clicking the "Create Operating System" button will open a new web page where we will create and define the Host Group details. There are several key word/tabs at the top of this page. You are in the primary "Host Group" tab to start the process of creating a host group

4. Input “**55hg”** in the name field

5. Select "Library" in the "Lifecycle Environment" field
6. Select "Default Organization View" in the "Content View" field
7. Select the name of your Satellite 6.7 server in the "Content Source" field
8. Select "production" in the "Puppet Environment" field
9. Scroll back up to the top of the page and click the "Operating System" key word/tab
10. Select "x86_64" in the "Architecture" field
11. Select "RedHat 8.2" in the "Operating system" field
12. Select "Fedora mirror" in the "Media" field
13. Select "Kickstart default" in the "Partition Table" field
14. Click the "Locations" key word/tab
15. Make sure "LAB" is in the "Selected Items" box
16. Click the "Organizations" key word/tab
17. Make sure "SDG" is in the "Selected Items" box
18. Click the "Activation Keys" key word/tab
19. Input “**55ak**” in the "Activation Keys" field
20. Scroll down and click the "Submit" button

Exercise 3: Register the RHEL 8 Client host to the Satellite 6.7 server

Task 1: Display the list of current content hosts registered to the Satellite 6.7 server

1. Click the "Hosts" main tab and the "Content Hosts" sub-tab

   This page will display the Content Hosts known by your Satellite 6.7 server.
   Your Satellite 6.7 server will be listed with a red "X" icon in the "Subscription Status" column. The red "X" is normal for the Satellite server due to the fact that the Satellite server is subscribed to Red Hat directly and not subscribed to itself.

2. Leave the RDP session with the Satellite 6.7 webUI page open

Task 2: Log into the RHEL 8 Client host and register it to the Satellite 6.7 server

1. Return to the ssh, putty, or MobaXterm session you have connected to the bastion host

2. Remember to use your user account name and your RHEL 8 client IP address when running the following ssh command to connect to your RHEL 8 client:

   ```
   [user##@bastion1 ~]$ ssh user##@10.0.???.???
   ```

3. You will now add your Satellite 6.7 server and IdM server information to the /etc/hosts file on your RHEL 8.1 client. Remember to use the correct IP address and host name including the UUID for the Satellite 6.7 server when running the following command:

   ```
   [user##@rhel8-client-0 ~]$ sudo echo 10.0.???.???  \
   rhel7-sat6-server-0.????.demo1.pd.stonedoor.io | sudo tee -a /etc/hosts
   ```

4. Remember to use the correct IP address and host name including the UUID for the IdM server when running the following command:

   ```
   [user##@rhel8-client-0 ~]$ sudo echo 10.0.???.???  \
   rhel8-idm-server-0.????.demo1.pd.stonedoor.io | sudo tee -a /etc/hosts
   ```

5. Download the bootstrap.py python script from the Satellite 6.7 server

```
[user##@rhel8-client-0 ~]$ curl -O \
rhel7-sat6-server-0.????.demo1.pd.stonedoor.io/pub/bootstrap.py
```

6. Change the permissions to make bootstrap.py executable by everyone

   ```
   [user##@rhel8-client-0 ~]$ chmod a+x bootstrap.py
   ```

7. Run the bootstrap.py python script to register the RHEL 8 client with the Satellite 6.7 server. You will have to provide the password for the Satellite 6.7 server user named admin. The password is: **redhat**

   ```
   [user##@rhel8-client-0 ~]$ sudo /usr/libexec/platform-python bootstrap.py \
   -l admin -s rhel7-sat6-server-0.????.demo1.pd.stonedoor.io -o SDG -L LAB \
   -g 55hg -a 55ak
   ```

   Continue to watch the progress of the bootstrap.py script running in your ssh, putty, or MobaXterm session.
   bootstrap.py will reach a point where it will stop and wait for up to 10 minutes for you to approve a certificate in the webUI.
   Watch the bootstrap.py progress output for a line very similar to the following(only the date/time may be different):

   ```
   [RUNNING], [2020-05-05 13:50:32], [/opt/puppetlabs/puppet/bin/puppet agent --test
   --noop --tags no_such_tag --waitforcert 10]
   ```

8. When you see that line, return to the Satellite 6.7 server webUI in your RDP session and click on the "Infrastructure" main tab and the "Capsules" sub tab

9. Click on the name of your Satellite 6.7 server in the list of Capsules. It will be the only Capsule listed.

   Clicking on the name of your Satellite 6.7 server in the list of Capsules will open a new web page where you can see and change details about the Capsule services on your Satellite 6.7 server. There are five key word/tabs across the top of the page.

10. Click on the "puppet CA" key word/tab.

    In the middle left section of the page you will see a small yellow triangle and a number "1" just to the right of the triangle.

11. Click the number "1".

12. Clicking the number 1 will bring up a page listing all pending host certificates. The only certificate is for the host you are registering with the bootstrap.py python script.

13. Click the "Sign" button to sign the pending certificate for your REHL 8 Client host.

14. Return to your ssh, putty, or MobaXterm session and wait for bootstrap.py to finish registering your RHEL 8 Client host

15. When bootstrap.py finishes, run the following command to exit out of the RHEL 8 Client

    ```
    [user##@rhel8-client-0 ~]$ exit
    ```

16. Return to the Satellite 6.7 webUI in the RDP session.

17. Click the "Hosts" main tab and the "content Hosts" sub-tab. You will now see your RHEL 8 Client listed as a Content Host

Exercise 4: Configure the IdM server

Task 1: Install the IdM server

1. Remember to use the correct user name and IP address or hostname when running the following command to connect to your IdM server:

    ```
    [user##@bastion01 ~]$ ssh user##@10.0.???.???
    ```
    or
    ```
    ssh user##@rhel8-idm-server-0.????.demo1.pd.stonedoor.io
    ```

2. Run the following command and answer the questions to install your IdM server:

    ```
    [user##@rhel8-idm-server-0 ~]$ sudo ipa-server-install --no-ntp --setup-dns
    ```

    The ipa-server-install command will stop every time it requires you to answer a question. The default answers are in square brackets. Pressing the Enter key on your keyboard will select the default answer but that is not always going to be the correct choice.

3. Verify the Server host name and correct it if required. It must be the FQDN of your IdM server. The default is the hostname of the server where you are running the ipa-server-install so it should be correct.

4. Verify the domain name and correct it if required. It must be the FQDN of your IdM domain. The default is determined based on the FQDN of the server where you are running the ipa-server-install so it should be correct.

5. Verify the realm name and correct it if required. It must be the FQDN of your IdM domain converted to all uppercase letters. The default is determined based on the FQDN of the server where you are running the ipa-server-install so it should be correct.

6. Set and confirm the Directory Manager password as “**dirmgrpw01”** for this workshop

7. Set and confirm the IP admin password as “**ipaadminpw01**” for this workshop

8. Select yes to configure the default DNS forwarders using the DNS servers from the /etc/resolv.conf file

9. Press Enter to skip adding any additional DNS forwarders

10. Ignore the messages regarding DNSSEC

11. The system has no reverse zones available to find while searching so entering yes or no will end with the same result.

12. The ipa-server-install command will list details regarding the IPA Master Server, the CA, and the BIND DNS server and will ask if you want to "Continue to configure the system with these values? [no]:" **FULL STOP. SEE NEXT STEP (13)**

13. The default answer to the question in the square brackets is "no". **That is not the answer you are looking for.** Input “**yes**” and press the Enter key

14. The ipa-server-install command takes a few minutes to complete. Wait for it to finish and then continue on with Task 2

Task 2: Install the Active Directory trust components

1. Run the following command and answer the questions to install the Active Directory trust components

```
[user##@rhel8-idm-server-0 ~]$ sudo ipa-adtrust-install
```

2. Input the IdM server admin password “**ipaadminpw01**” you created during the ipa-server-install steps.

3. Ignore the warning about smb.conf and input “**yes**” to continue

4. Press the Enter key to accept the default for "Enable trusted domains support in slapi-nis? [no]:"

5. Press Enter to accept the default for the NetBIOS domain name

6. Input “**yes”** and press the Enter key to override the default for running the ipa-sidgen task

7. Wait for the ipa-adtrust-install command to finish

Task 3: Establish a cross forest trust with the Microsoft Active Directory server

1. Run the following command to obtain an admin user kerberos ticket:

   ```
   [user##@rhel8-idm-server-0 ~]$ kinit admin
   ```

2. Input “**ipaadminpw01**” for the IdM server admin user password

3. Run the following command and answer the questions to establish a cross forest trust with the Microsoft Active Directory server:

   ```
   [user##@rhel8-idm-server-0 ~]$ ipa trust-add --type=ad demo1.pd.stonedoor.io
   ```

4. Input “**idmtrustuser**” for the Active Directory domain administrator

5. Input “**Idmtru$tuserpw01**” for the Active Directory domain administrator's password

Task 4: Configure IdM user groups to enable Microsoft Active Directory user access to RHEL resources

1. Run the following command to restart the Kerberos version 5 Authentication Service and Key Distribution Center:

   ```
   [user##@rhel8-idm-server-0 ~]$ sudo systemctl restart krb5kdc
   ```

2. Run the following command to restart the System Security Services Daemon:

   ```
   [user##@rhel8-idm-server-0 ~]$ sudo systemctl restart sssd
   ```

3. Run the following command to create an IdM external user group:

   ```
   [user##@rhel8-idm-server-0 ~]$ ipa group-add \
   --desc='AD Linux Users External Group' ad_linux_users_external --external
   ```

4. Run the following command to create an IdM internal user group:

   ```
   [user##@rhel8-idm-server-0 ~]$ ipa group-add \
   --desc='AD Linux Users Internal-Posix' ad_linux_users_posix
   ```

5. Run the following command to add the IdM external user group to the IdM internal user group:

   ```
   [user##@rhel8-idm-server-0 ~]$ ipa group-add-member \
   ad_linux_users_posix --groups ad_linux_users_external
   ```

6. Run the following command to add an AD domain user group to the IdM external user group:
   The single quotes around the AD user group identifier are CRITICAL!!!

   ```
   [user##@rhel8-idm-server-0 ~]$  ipa group-add-member \
   ad_linux_users_external --external 'DEMO1.PD.STONEDOOR.IO\ADrhelusers'
   ```

   Press the Enter key to accept the defaults for all four questions

Task 5: Login to the IdM server webUI and create an IdM user

1. Return to the firefox web browser in the bastion host RDP session

2. Open a new tab in the firefox browser

3. Enter the IdM server host name or IP address in the URL bar.

   A web page will display a message informing you of a "Warning: Potential Security Risk Ahead"

4. Click the "Advanced" button in the lower right side of that warning web page which will cause additional information and buttons to be added to the bottom of the web page

5. Scroll down and click the "Accept the Risk and Continue" button

   The Red Hat Identity Management Login page will be displayed

6. Login as the user account “**admin**” with the password “**ipaadminpw01**”

   You are now looking at the Red Hat Identity Management webUI
   There are five main tabs across the top of the page and each main tab has two or more sub-tabs
   You are in the "Identity" main tab and the "Users" sub-tab looking at the list of IdM Active users

7. Click the "+ Add" button

   Clicking the "+ Add" button opens a dialog box that is used to define and add a new user

8. Input “**idmuser01**” into the "User login" field

9. Input “**John**” into the "First name" field

10. Input “**Doe**” into the "Last name" field

11. Input “**idmu01pw01**” in the "New Password" and "Verify Password" fields

12. Click the "Add" button to add the new user

13. Idmuser01 now appears in the list with the other Active users

Exercise 5: Configure the RHEL 8 client as an IdM client and CIFS client

Task 1: Enroll the RHEL 8 Client as an IdM client

1. Return to your ssh, putty, or MobaXterm session

2. Run the following command to exit the IdM server:

   ```
   [user##@rhel8-idm-server-0 ~]$ exit
   ```

3. Remember to use your correct username and the correct IP address when running the following command to log into the RHEL 8 Client:

   ```
   [user##@bastion01 ~]$ ssh user##@10.0.???.???
   ```

4. Run the following command to input the IdM server IP address as a nameserver into the RHEL 8 Client /etc/resolv.conf file

   ```
   [user##@rhel8-client-0 ~]$ echo “# Generated by NetworkManager
   search demo1.pd.stonedoor.io ????.demo1.pd.stonedoor.io
   nameserver 10.0.???.???
   nameserver 10.0.0.10
   nameserver 10.0.32.10” | sudo tee /etc/resolv.conf
   ```

5. Run the following command and answer the questions to enroll the RHEL 8 Client as a client host to the IdM server. Remember to replace the ???? characters with the UUID

   ```
   [user##@rhel8-client-0 ~]$ sudo ipa-client-install \
   --domain ????.demo1.pd.stonedoor.io --enable-dns-updates
   ```

6. Press Enter to accept the default "no" for configuring chrony with NTP server or pool address

7. The ipa-client-install command will display some information about the realm, domain, IPA Server and BaseDN and then ask if you want to "Continue to configure the system with these values? [no]:" **FULL STOP. SEE NEXT STEP (8)**

8. The default answer to the question in the square brackets is "no". **That is not the answer you are looking for.** Input “**yes**” and press the Enter key

9. Input “**admin**” for the "User authorized to enroll computers:"

10. Input “**ipaadminpw01**” for the "Password for the admin@????.DEMO1.PD.STONEDOOR.IO:"

11. Wait for the ipa-client-install command to finish

12. Return to the IdM server webUI in the bastion host RDP session

13. In the "Identity" main tab, click the "Hosts" sub-tab and notice the RHEL 8 Client is now enrolled as an IdM client

Task 2: Configure CIFS on the RHEL 8 Client and mount a Windows shared file system

1. Return to your ssh, putty, or MobaXterm session

2. Run the following command to refresh and display the rhel repositories on the RHEL 8 Client:

   ```
   [user##@rhel8-client-0 ~]$ sudo yum repolist enabled
   ```

3. Run the following command to install the tools required to connect to a shared Windows file system:

   ```
   [user##@rhel8-client-0 ~]$ sudo yum install -y cifs-utils
   ```

4. Run the following command to create a local directory mount point for the shared Windows file system:

   ```
   [user##@rhel8-client-0 ~]$ sudo mkdir /ad-data
   ```

5. Run the following command to mount the shared Windows file system to the local directory mount point:

   ```
   [user##@rhel8-client-0 ~]$ sudo mount -t cifs -o username=adwsuser01
   //dc1/idm_home /ad-data
   ```

   Input “**Adw$userpw01**” for the “Password for adwsuser01@//dc1/idm_home:”

6. Run the following command to display the available space on all file systems including the shared Windows file system:

   ```
   [user##@rhel8-client-0 ~]$ df -h
   ```

7. Remember to use your correct user name as part of the file name when running the following command which will put the output of the hostname command into a file on the shared Windows file system:

   ```
   [user##@rhel8-client-0 ~]$ echo $(hostname) | sudo tee /ad-data/user##-testfile.txt
   ```

8. Run the following command to display the files in the shared Windows file system:

   ```
   [user##@rhel8-client-0 ~]$ sudo ls -l /ad-data
   ```

   You can see the file you created as well as the files created by the other workshop participants

Task 3: Log into the RHEL 8 Client as an IdM user

1. Run the following command to exit the IdM client

   ```
   [user##@rhel8-client-0 ~]$ exit
   ```

2. Remember to use the correct IP address when running the following command to log into the RHEL 8 client. You will log in as the IdM user you created in Exercise 4, Task 5, Steps 7 through 12:

   ```
   [user##@bastion01 ~]$ ssh idmuser01@10.0.???.???
   ```

3. Input “**idmu01pw01**” for “Password:”

NOTE### Logging in as an IdM user for the first time will result in that IdM user being forced to change their password.

4. Input “**idmu01pw01**” for “Current Password:”

5. Input “**idmu01npw01**” for “New password:”

6. Input “**idmu01npw01**” for “Retype new password:”

   NOTE### Ignore the error messages about Red Hat Insights and the home directory. Notice the user account in the prompt

7. Run the following command to see the information about the IdM user

```
[idmuser01@rhel8-client-0 ~]$ id
```

Task 4: Log into the RHEL 8 Client as an AD user

1. Run the following command to exit the IdM user ssh session

```
[idmuser01@rhel8-client-0 ~]$ exit
```

   NOTE### You will now log in as an Active Directory user. The AD user can log into the IdM client hosts due to the steps you completed in Exercise 4, Tasks 2, 3, and 4

2. Remember to use the correct IP address when running the following command to log into the IdM client:

```
[user##@bastion01 ~]$ ssh adwsuser01@demo1.pd.stonedoor.io@10.0.???.???
```

   Input “**Adw$userpw01**” for the password

   NOTE### Ignore the error messages about Red Hat Insights and the home directory. Notice the user account in the prompt

3. Run the following command to see the information about the AD user

4. **[user##@bastion01 ~]$ id**

5. Return to the IdM server webUI in the bastion host RDP session

6. In the "Identity" main tab, click the "Users" sub-tab and notice that the AD user (adwsuser01@demo1.pd.stonedoor.io) is not listed as an Active user.

   The AD user is not listed because that user exists in the Microsoft Active Directory data store on the AD server. That user does not exist in IdM.

   The steps in this lab configured the RHEL 8 Client as an IdM client to the IdM server and set up the IdM server to trust the AD server. You were able to log into the RHEL 8 Client with the AD user because the RHEL 8 Client(IdM client) trusts the IdM server which in turn trusts the AD server.