File Storage: Configure NFS Export Options

Lab 15-1 Practices

Get Started

Overview

NFS export options enable you to create more granular access control to limit VCN access. You can use NFS export options to specify access levels for IP addresses or CIDR blocks connecting to file systems through exports in a mount target. Doing this provides better security controls in multi-tenant environments.

Additionally, by using NFS export option access controls, you can limit the clients' ability to connect to the file system and view or write data.

In this lab, you'll learn how to allow read-only access to the file system from one instance and read/write access from the other instance.

In this lab, you'll:

a. Create a Virtual Cloud Network and its components

b. Create two VM instances

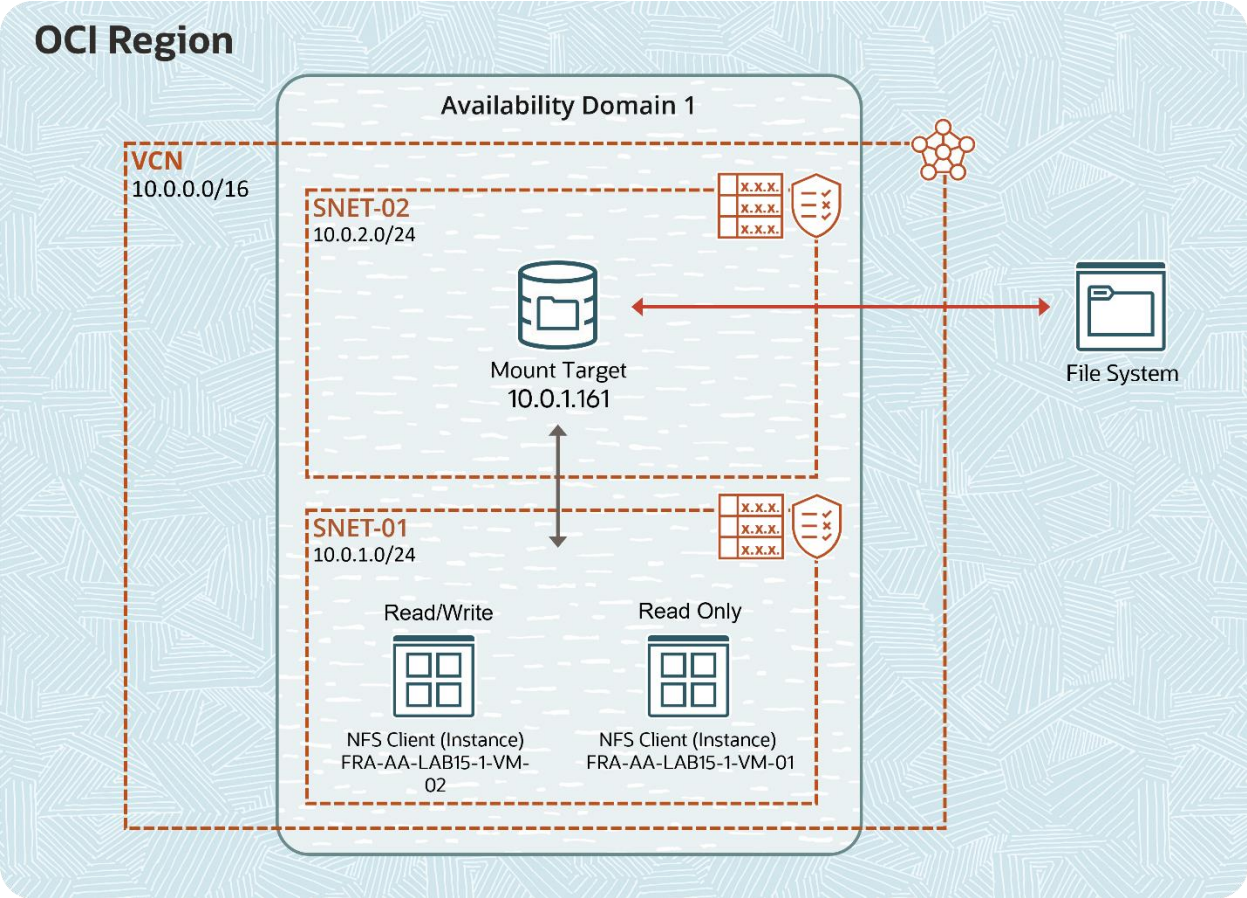
c. Create a file system

d. Configure VCN Security Rules for file storage

e. Set Export Options for the file system

f. Mount the file system from both the Instances

g. Perform testing



Prerequisites

- You must have access to the OCI Console.

Assumptions

- You must be familiar with navigating the OCI Console.
- In this lab, we are considering Germany Central (Frankfurt) as your region.

Create a Virtual Cloud Network and Its Components

In this practice, you will learn how to create a Virtual Cloud Network (VCN), Subnet, Internet Gateway, and Security List, and add route rules in the Route Table.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console.
2. Open the **Main Menu**, click **Networking**, and then click **Virtual Cloud Networks.**
3. Click **Create VCN.**
4. Enter the following:
    a. **Name:** Enter **`FRA-AA-LAB15-1-VCN-01`**.
    b. **Create in Compartment:** Select the <*compartment name*> assigned to you.
    c. **IPv4 CIDR Block:** Enter **10.0.0.0/16**. Press **Enter** to add.

    Note: You can leave all the other options as default.
5. Click **Create VCN**. The VCN is now created successfully.
6. Click **Create Subnet**.
7. In the Create Subnet dialog box, enter the following:
    a. **Name**: Enter **`FRA-AA-LAB15-1-SNET-01`**.
    b. **Create in Compartment:** Select the <*compartment name*> assigned to you.
    c. **Subnet Type:** Select **Regional**.
    d. **IPv4 CIDR Block:** Enter **`10.0.1.0/24`**.
    e. **Subnet Access:** Select **Public Subnet.**

    Note: You can leave all the other options as default.
8. Click **Create Subnet.** The subnet is now created successfully and the state is Available.

9. Click **Create Subnet** to create another subnet. In the Create Subnet dialog box, enter the following:

    a. **Name**: Enter **`FRA-AA-LAB15-1-SNET-02`**.

    b. **Create in Compartment**: Select the <*compartment name*> assigned to you.

    c. **Subnet Type**: Select **Regional.**

    d. **IPv4 CIDR Blocks:** Enter `10.0.2.0/24`.

    e. **Subnet Access**: Select **Public Subnet.**

    f. **DNS Label**: Enter **`FRAAALAB151SNE2.`**

    g. **Note:** Leave all the other options in their default setting.

10. Click **Create Subnet**.

11. In the left navigation pane, under **Resources**, click **Internet Gateways**.

12. Click **Create Internet Gateway.**

13. Enter the following:

    a. **Name**: Enter **`FRA-AA-LAB15-1-IG-01`**.

    b. **Create in Compartment**: Select the <*compartment name*> assigned to you.

14. Click **Create Internet Gateway.** The Internet Gateway is now created successfully, and the state is Available.

15. In the left navigation pane, under **Resources**, click **Route Tables.**

16. Click **Default Route Table for FRA-AA-LAB15-1-VCN-01**.

17. Click **Add Route Rules** and enter the following:

    a. **Target Type**: Select **Internet Gateway**.

    b. **Destination CIDR Block:** Enter `0.0.0.0/0`.

    c. **Target Internet Gateway:** Select **FRA-AA-LAB15-1-IG-01**.

18. Click **Add Route Rules**. The route rule is successfully added in the default Route Table.

19. Using the breadcrumb trail at the top of the screen, return to your VCN page.

20. In the left navigation pane, under **Resources**, click **Security Lists**.

21. Click **Create Security List.**

22. Enter the following:

    a. **Name:** Enter **`FRA-AA-LAB15-1-SL-01`**.

    b. **Create in Compartment:** Select the <*compartment name*> assigned to you.

    c. Do not add any Ingress or Egress rules.

23. Click **Create Security List.** The security list is created and displayed on the **Security Lists** page.

    Note: As of now, both the Subnets FRA-AA-LAB15-1-SNET-01 and FRA-AA-LAB15-1-SNET-02 are using the Default Security List.

24. Leave Subnet FRA-AA-LAB15-1-SNET-01 as is with the Default Security List. Change the Security List for Subnet FRA-AA-LAB15-1-SNET-02 by doing the following:

    a. Click **Subnets**.

    b. Click the subnet **FRA-AA-LAB15-1-SNET-02**.

    c. In the left navigation pane, under **Resources**, click **Security Lists**.

    d. To add a security list, click **Add Security List**, and select **FRA-AA-LAB15-1-SL-01**.

    e. To remove the default security list **Default Security List for FRA-AA-LAB15-1-VCN-01**, click the three dots on the right to open the Actions menu, and then select **Remove**.

    f. Click **Remove** when prompted to confirm removal.

       Note: The changes take effect within a few seconds.

Create a VM Instance

In this practice, you will learn how to create SSH keys using Cloud Shell and launch an instance.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console.
2. In the console ribbon at the top of the screen, click the **Cloud Shell** icon next to the Region selection menu.
3. After the Cloud Shell is ready, enter the following commands:

   ```
   $ mkdir .ssh
   ```

   - **Important:** In case you get an error message that says “Cannot create director: File exists,” you can skip running this first command.

   ```
   $ cd .ssh
   ```

   ```
   $ ssh-keygen -b 2048 -t rsa –f <<sshkeyname>>
   ```

   - **Remember:** After entering this third command, press **Enter** twice for no passphrase.

   Note: Replace `<<sshkeyname>>` with `ociaalab15key`. Choose the key name you can remember. This will be the key name you will use to connect to the compute instance you create.

   Reminder: The angle brackets «» should not appear in your code.

   Reminder: Do not include the `$` symbol when pasting code into Cloud Shell.

4. Examine the two files that you just created by running the following command:

   ```
   $ ls
   ```

   Note: In the output, there are two files, a private key: *<<sshkeyname>>* and a public key: *<<sshkeyname>>.pub*, keep the private key safe and don’t share its content with anyone. The public key will be needed for various activities and can be uploaded to certain systems as well as copied and pasted to facilitate secure communications in the cloud.

5. To list the contents of the public key, use the following command:

   ```
   $ cat <<sshkeyname>>.pub
   ```

   Note: Replace `<<sshkeyname>>` with `ociaalabkey`.

   Reminder: The angle brackets «» should not appear in your code.

6. Copy the contents of the public key as you will need this in a subsequent step. Make sure that you remove any hard returns that may have been added when copying. The `.pub` key should be one line.

7. Open the **Main Menu** and click **Compute**. Under **Compute**, click **Instances.**

8. Click **Create instance** and enter the following:

   a. **Name:** Enter **`FRA-AA-LAB15-1-VM-01`**.

   b. **Create in compartment:** Select the <*compartment name*> assigned to you.

   c. **Placement:** Select Availability Domain **AD1**. Click **Show advanced options** and select **On-demand capacity** under the **Capacity type** menu.

   d. **Image and shape**: Choose the image **Oracle Linux 8** and shape **VM.Standard.A1.Flex** (1 OCPU, 6GB Memory) [Shape series: Ampere].

   e. **Networking**: Select the existing virtual cloud network **FRA-AA-LAB15-1-VCN-01** and existing subnet **FRA-AA-LAB15-1-SNET-01 (regional)**. Under **Public IP address** select **Assign a public IPv4 address.**

   f. **Add SSH keys**: Select **Paste public keys** and paste the contents of the public key, which you copied in Step 6, in the box.

   g. **Boot volume:** Keep the default selections.

9. Click **Create**.

10. To create a second Instance, repeat steps 7–9. Keep all settings the same except enter the **Name** as **FRA-AA-LAB15-1-VM-02**.

    Note: Once finished, you see that the both the instances are created successfully and in the Running state.

11. To connect to the instances, on the **Instance information** tab and under **Instance access**, copy the **Public IP address**.

12. Open **Cloud Shell** and use SSH to connect to your instance by using the following commands:

    Note: Enter **`yes`** in response to "Are you sure you want to continue connecting (yes/no)?"

    ```
    $ ssh -i <private_key_file> <username>@<public-ip-address>
    ```

    Reminders:

    - `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.
    - `<username>` is the default user `opc`.
    - `<public-ip-address>` is the Public IP address of the instance.

Create a File System

You can create a shared file system in the cloud using the File Storage service. Network access to your file system is provided through a mount target. Exports control how NFS clients access file systems when they connect to a mount target. When you use the console to create your file system, the workflow also creates a mount target and an export for it.

In this practice, you will learn how to create a file system.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console.
2. Open the **Main Menu** and click **Storage**. Under **File Storage**, click **File Systems**.
3. In the left navigation pane, in the **List Scope** section, under **Compartment**, select the <*compartment name*> assigned to you.
4. Click **Create File System**.
5. In **File System Information**, click **Edit Details** and enter the following:
    a. **Name:** Enter **`FRA-AA-LAB15-1-FS-01.`**
    b. **Availability Domain:** Select the first availability domain.
    c. **Create in Compartment:** Select the <*compartment name*> assigned to you.
    d. **Encryption:** Keep the default **Encrypt using Oracle-managed keys** selection.
6. In the **Export Information** click **Edit Details** and enter the following:
    a. **Export Path**: Enter **`/FRA-AA-LAB15-1-EP-01.`**
    b. Do not select **Use Secure Export Options**.
7. In the **Mount Target Information**, click **Edit Details** and specify the following:
    a. Select the **Create New Mount Target** option.
    b. Enter **`FRA-AA-LAB15-1-MNT-01`** in the **New Mount Target Name** field.
    c. Select **FRA-AA-LAB15-1-VCN-01** from the **Virtual Cloud Network** drop-down list.

d. Select **FRA-AA-LAB15-1-SNET-02 (regional)** from the **Subnet** drop-down list.

e. Do not select the **Use network security groups to control traffic** check box.

8. Click **Create.**

   Note: The File Storage service typically creates the file system and mount target within a few seconds.

Configure VCN Security Rules for File Storage

Before you can mount a file system, you must configure security rules to allow traffic to the mount target's VNIC using specific protocols and ports. Security rules enable traffic for the following:

- Open Network Computing Remote Procedure Call (ONC RPC) rpcbind utility protocol
- Network File System (NFS) protocol
- Network File System (MOUNT) protocol
- Network Lock Manager (NLM) protocol

In this practice, you'll learn how to configure security rules for both the mount target and the instance in a security list.

Note

In this lab scenario, the mount target that exports the file system is in a different subnet (FRA-AA-LAB15-1-SNET-02) than the instance on which you want to mount the file system (FRA-AA-LAB15-1-SNET-01) .

You need to set up the following security rules in **FRA-AA-LAB15-1-SL-01** for the mount target. You also need to specify the instance IP address or CIDR block 10.0.1.0/24 as the source for ingress rules and the destination for egress rules:

- Stateful ingress from ALL ports in the source instance CIDR block to TCP ports 111, 2048, 2049, and 2050
- Stateful ingress from ALL ports in the source instance CIDR block to UDP ports 111 and 2048
- Stateful egress from TCP ports 111, 2048, 2049, and 2050 to ALL ports in the destination instance CIDR block
- Stateful egress from UDP port 111 to ALL ports in the destination instance CIDR block

Next, you need to set up the following security rules in **Default Security List for FRA-AA-LAB15-1-VCN-01** for the instance. You also need to specify the mount target IP address or CIDR block 10.0.2.0/24 as the source for ingress rules and the destination for egress rules:

- Stateful ingress from source mount target CIDR block TCP ports 111, 2048, 2049, and 2050 to ALL ports
- Stateful ingress from source mount target CIDR block UDP port 111 to ALL ports
- Stateful egress from ALL ports to destination mount target CIDR block TCP ports 111, 2048, 2049, and 2050.
- Stateful egress from ALL ports to destination mount target CIDR block UDP ports 111 and 2048.

Tasks

1. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks.**
2. Click **FRA-AA-LAB15-1-VCN-01** from the list of VCNs.
3. In the left navigation pane, under **Resources**, click **Security Lists**.
4. Click **FRA-AA-LAB15-1-SL-01**.
5. In the left navigation pane, under **Resources**, click **Ingress Rules**.
6. Click **Add Ingress Rule** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Source Type:** Select **CIDR**.
    c. **Source CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **TCP.**
    e. **Source Port Range:** By default, it will be All, even if you leave the field blank.
    f. **Destination Port Range:** Enter `111`.
7. Click **Add Ingress Rules**.

8. Click **Add Ingress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Source Type:** Select **CIDR.**
    c. **Source CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **TCP.**
    e. **Source Port Range:** By default, it will be All, even if you leave the field blank.
    f. **Destination Port Range:** Enter `2048-2050`.
9. Click **Add Ingress Rules**.
10. Click **Add Ingress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Source Type:** Select **CIDR.**
    c. **Source CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **UDP.**
    e. **Source Port Range:** By default, it will be All, even if you leave the field blank.
    f. **Destination Port Range:** Enter `111`.
11. Click **Add Ingress Rules**.
12. Click **Add Ingress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Source Type:** Select **CIDR.**
    c. **Source CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **UDP**.
    e. **Source Port Range:** By default, it will be All, even if you leave the field blank.
    f. **Destination Port Range:** Enter `2048`.

13. Click **Add Ingress Rules**.
14. In the left navigation pane, under **Resources**, click **Egress Rules**.
15. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **TCP.**
    e. **Source Port Range**: Enter `111`.
    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.
16. Click **Add Egress Rules**.
17. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **TCP**.
    e. **Source Port Range**: Enter `2048-2050`.
    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.
18. Click **Add Egress Rules**.
19. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **UDP**.

e. **Source Port Range**: Enter `111`.

f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.

20. Click **Add Egress Rules**.
21. Click the VCN **FRA-AA-LAB15-1-VCN-01**.
22. In the left navigation pane, under **Resources**, click **Security Lists**.
23. Click **Default Security List for FRA-AA-LAB15-1-VCN-01**.
24. In the left navigation pane, under **Resources**, click **Ingress Rules**.
25. Click **Add Ingress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Source Type:** Select **CIDR.**

    c. **Source CIDR:** Enter `10.0.2.0/24`.

    d. **IP Protocol:** Select **TCP.**

    e. **Source Port Range:** Enter `2048-2050`.

    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank).

26. Click **Add Ingress Rules.**
27. Click **Add Ingress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Source Type:** Select **CIDR.**

    c. **Source CIDR:** Enter `10.0.2.0/24`.

    d. **IP Protocol:** Select **TCP.**

    e. **Source Port Range:** Enter `111`.

    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.

28. Click **Add Ingress Rules**.

29. Click **Add Ingress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Source Type:** Select **CIDR**.
    c. **Source CIDR:** Enter `10.0.2.0/24`.
    d. **IP Protocol:** Select **UDP.**
    e. **Source Port Range:** Enter `111`.
    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.
30. Click **Add Ingress Rules**.
31. In the left navigation pane, under **Resources**, click **Egress Rules**.
32. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.2.0/24`.
    d. **IP Protocol:** Select **TCP**.
    e. **Source Port Range**: By default, it will be All, even if you leave the field blank.
    f. **Destination Port Range:** Enter `2048-2050`.
33. Click **Add Egress Rules.**
34. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.2.0/24`.
    d. **IP Protocol:** Select **TCP**.
    e. **Source Port Range**: By default, it will be All, even if you leave the field blank.
    f. **Destination Port Range:** Enter `111`.

35. Click **Add Egress Rules**.

36. Click **Add Egress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Destination Type:** Select **CIDR**.

    c. **Destination CIDR:** Enter `10.0.2.0/24`.

    d. **IP Protocol:** Select **UDP**.

    e. **Source Port Range**: By default, it will be All, even if you leave the field blank.

    f. **Destination Port Range:** Enter `111`.

37. Click **Add Egress Rules**.

38. Click **Add Egress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Destination Type:** Select **CIDR**.

    c. **Destination CIDR:** Enter `10.0.2.0/24`.

    d. **IP Protocol:** Select **UDP**.

    e. **Source Port Range**: By default, it will be All, even if you leave the field blank.

    f. **Destination Port Range:** Enter `2048`.

39. Click **Add Egress Rules.**

Set Export Options for the File System

In this practice, you'll learn how to allow read-only access to the file system FRA-AA-LAB15-1-FS-01 from the Instance FRA-AA-LAB15-1-VM-01 and read/write access from the Instance FRA-AA-LAB15-1-VM-02.

Tasks

1. From the **Main Menu**, select **Compute**. Under **Compute**, click **Instances.**
2. Make a note of the Private IP addresses of both the instances FRA-AA-LAB15-1-VM-01 and FRA-AA-LAB15-1-VM-02.

   Note: In this lab, the Private IP addresses are as follows:

   - 10.0.1.15 for instance FRA-AA-LAB15-1-VM-01
   - 10.0.1.161 for instance FRA-AA-LAB15-1-VM-02

   Reminder: In your case, the Private IP address can be different.
3. From the **Main Menu**, click **Storage**. Under **File Storage**, click **File Systems**.
4. Click the file system **FRA-AA-LAB15-1-FS-01**.
5. From the **Exports** list, select the Export Path **/FRA-AA-LAB15-1-EP-01**.
6. Click **Edit NFS Export Options.**
7. In the existing Export Options window, make the following changes:

   a. **Source:** Enter `10.0.1.15/32`**.**

      Reminder: The Private IP address of FRA-AA-LAB15-1-VM-01 is **10.0.1.15**. However, when you perform the lab, it might be a different IP address.

   b. **Ports:** Select **Any.**

   c. **Access:** Select **Read Only.**

   d. **Squash:** Select **None.**
8. Click **+ Another Option** to create a new export option entry.

9. In the new entry boxes, specify the following information:

    a. **Source:** Enter `10.0.1.161/32`.

    Reminder: The Private IP address of FRA-AA-LAB15-1-VM-02 is **10.0.1.161**. However, when you perform the lab, it might be a different IP address.

    b. **Ports:** Select **Any**.

    c. **Access:** Select **Read/Write**.

    d. **Squash:** Select **None**.

10. When you're finished with your entries, click **Update**.

Mount the File System from Both the Instances

In this practice, you will learn how to mount a file system from two instances.

Tasks

1. From the **Main Menu**, select **Storage**. Under **File Storage**, click **File Systems**.
2. In the **File Systems** list, click the file system **FRA-AA-LAB15-1-FS-01**.
3. In the left navigation pane, under **Resources**, click **Exports**.
4. Locate /FRA-AA-LAB15-1-EP-01 and click the three dots on the right to open the Actions menu, and then select **Mount Commands.**
5. In **Image**, choose **Oracle Linux** from the drop-down menu.
6. Click the **Copy** links to copy the three commands listed.
7. Connect to your instance **FRA-AA-LAB15-1-VM-01**.

   Note: For help with this, refer to Steps 11–12 in the **Create a VM Instance** practice.

8. Paste and run the commands that you copied in the previous step into your instance session window.

   Important: Please run the commands that you copied and not the following commands which are just for reference:

   ```
   $ sudo yum install nfs-utils

   $ sudo mkdir -p /mnt/FRA-AA-LAB15-1-EP-01

   $ sudo mount 10.0.2.227:/FRA-AA-LAB15-1-EP-01 /mnt/FRA-AA-LAB15-1-
   EP-01
   ```

9. View the file system by entering the following:

   ```
   $ df –h
   ```

10. To mount the file system from the second instance FRA-AA-LAB15-1-VM-02, perform the following steps:

    a. Open a new duplicate tab in your browser.

    b. Repeat steps 7–8 of this practice.

    Note: The file system is now mounted from both instances, FRA-AA-LAB15-1-VM-01 and FRA-AA-LAB15-1-VM-02.

Perform Testing

In this practice, you will validate that you have read-only access to the file system FRA-AA-LAB15-1-FS-01 from the Instance FRA-AA-LAB15-1-VM-01, and read/write access from the Instance FRA-AA-LAB15-1-VM-02.

Tasks

1. Connect to your instance **FRA-AA-LAB15-1-VM-01**.

   Note: For help with this, refer to Steps 11-12 in the **Create a VM Instance** practice.

2. Try to write a file to the file system by entering the following:

   ```
   $ sudo touch /mnt/yourmountpoint/helloworld
   ```

   Note: Replace `yourmountpoint` with the path to the local mount point.

   For example:

   ```
   $ sudo touch /mnt/FRA-AA-LAB15-1-EP-01/helloworld
   ```

   Important: You will receive an error that validates that the instance FRA-AA-LAB15-1-VM-01 does not have write access to the file system.

3. Connect to your instance **FRA-AA-LAB15-1-VM-02.**

   Reminder: For help with this, refer to Steps 11–12 in the **Create a VM Instance** practice.

4. Try to write a file to the file system by entering the following:

   ```
   $ sudo touch /mnt/yourmountpoint/helloworld
   ```

   Note: Replace `yourmountpoint` with the path to the local mount point.

   For example:

   ```
   $ sudo touch /mnt/FRA-AA-LAB15-1-EP-01/helloworld
   ```

5. Once the file is successfully written, verify that you can view the file by entering the following.

   ```
   $ cd /mnt/yourmountpoint
   ```

   Note: Replace `yourmountpoint` with the path to the local mount point.

For example:

```
$ cd /mnt/FRA-AA-LAB15-1-EP-01

$ ls
```

6. Verify that you can view the file by enter the Step 5 commands from the instance **FRA-AA-LAB15-1-VM-01.**

   Note: You now see that the instance FRA-AA-LAB15-1-VM-01 has read-only access to the file system.