ORACLE

Roving Edge as Data Transfer Gateway – OC2/OC3 Regions

Version 3.2
June 5th, 2025

Public

Purpose Statement

The Roving Edge as a Data Transfer Gateway is designed to facilitate seamless data migration from DoD and Defense customers to Oracle Cloud Infrastructure (OCI) object storage within OC2/OC3 restricted regions, specifically in cases where FastConnect infrastructure is unavailable.

Disclaimer

ORACLE

Table of contents

ORACLE

Introduction

Roving Edge as Data Transfer Gateway delivers a seamless, efficient solution for managing data movement, synchronization, and storage across edge locations, on-premises systems, and Oracle Cloud Infrastructure (OCI). It facilitates data transfers of up to 30TB per Roving Edge device model 2 between edge environments, on-premises sites, and OCI Object Storage in environments with limited network bandwidth. With advanced features such as secure data synchronization and robust protocol support, including NFS v4.1, the gateway ensures reliable connectivity and strong data security.

> **NOTE:** For the Data Transfer Gateway use case, the maximum supported storage capacity is 30TB on Roving Edge device model 2, 18TB on Roving Edge device model 1, and 7TB on the Roving Edge Ultra model.

Note: This content is provided for informational purposes and self-supported guidance only. Consultancy or other assistance related to the content is not covered under the Oracle Support contract or associated service requests. If you have questions or additional needs, then please reach out to your Oracle Sales contact directly.

Architecture Overview

This architecture enables efficient data transfer from on-premises environments which do not have access to OCI Fast Connect links or high bandwidth. On this use case, the data is securely stored on the Oracle Linux instance running on the Roving Edge Device and physically shipped to the one os the Oracle Cloud Infrastructure restricted regions, such as: OC2/OC3 for data upload to Object Storage bucket. Listed below are the components of the solution:

- **Oracle Linux data transfer gateway instance:** This instance act as a data transfer gateway (or Data Mule) instance, enabling seamless data movement between edge locations, on-premises environments to OCI Object Storage, especially in areas lacking high-speed connectivity options like Oracle Fast Connect. This instance is powered by a customized Oracle Linux operating system.
    - **Enterprise-Grade Stability:** Oracle Linux is a trusted platform for mission-critical workloads, offering high reliability and long-term support.
    - **Optimized Performance:** With kernel enhancements and optimizations, Oracle Linux delivers high performance for edge use cases, including data processing and storage.
    - **Comprehensive Security:** Oracle Linux integrates advanced security features, such as Security-Enhanced Linux (SELinux) policies and automated vulnerability fixes, to safeguard systems.
    - **Compatibility with OCI:** It is designed to seamlessly integrate with Oracle Cloud Infrastructure, enabling consistent operations between edge and cloud environments.
- **OCI Config Authentication** It is the authentication method used by the **Oracle Cloud Infrastructure (OCI) CLI, SDKs, and APIs** to securely interact with OCI resources. It is based on a configuration file, located at `~/.oci/config`, which contains credentials and connection details for accessing OCI services.
- **OCI Sync Tool:** The OCI Sync is a tool part of the Oracle Cloud Infrastructure (OCI) APIs that enables automatic synchronization of data between a local storage solution (e.g., the Roving Edge device) and OCI Object Storage. It is designed to ensure seamless data updates and consistency across environments, particularly when intermittent or limited connectivity is an issue. Key characteristics of the OCI Sync tool include:
    - **Automatic Synchronization:** It identifies changes or new data and syncs them with OCI Object Storage once connectivity is re-established.
    - **Data Transfer Efficiency:** The tool optimizes bandwidth usage, ensuring only necessary data is transferred (e.g., incremental updates).
    - **Resilience for Edge Use Cases:** Especially useful in edge environments with unpredictable or slow network connections, ensuring data is kept up to date with the cloud.
    - **Security:** Ensures secure data transfers by leveraging OCI's authentication protocols, such as API keys or IAM policies.
- **NFS v4.1 Protocol Support:** Facilitates efficient file sharing and system mounting with NFS v4.1 support for on-premises environments. Oracle Linux data transfer instance includes support for the **NFS v4.1 protocol**, enabling efficient file sharing and system mounting across on-premises environments. This advanced protocol ensures that data is easily accessible and manageable in distributed systems. Key benefits of NFS v4.1 include:
    - **Improved Performance**: NFS v4.1 introduces features which distributes file operations across multiple servers, enhancing throughput and scalability for high-demand workloads.
    - **Simplified Management**: Its unified protocol architecture eliminates the need for multiple versions, streamlining deployment and administration across environments.
    - **Support for Stateful Protocols**: NFS v4.1 maintains stateful sessions, enabling better error recovery and session consistency.

- **Encryption:** Ensures enterprise-grade encryption is applied by default to secure data on the Roving Edge device.
- **Storage Capacity:** Handles up to 30TB of local NVME storage for data transfers with options for parallelism and incremental synchronization

Figure 1 illustrates the architecture of the Roving Edge as a Data Transfer Gateway for DoD/Gov customers with Oracle FastConnect on OC2/OC3 regions.

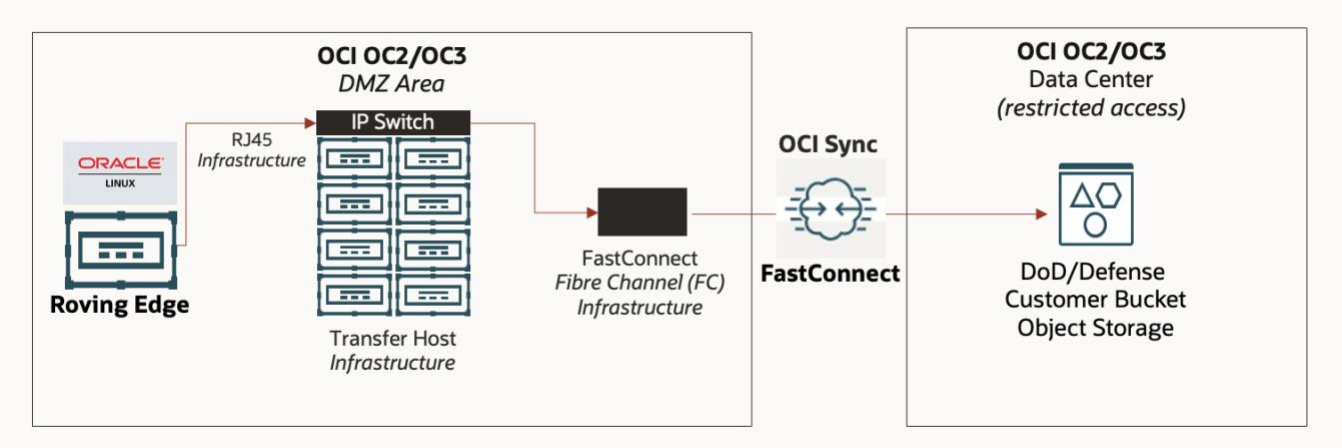


Figure 1. Architecture of the Roving Edge as a Data Transfer Gateway for DoD/Gov customers.

Requesting Roving Edge as Data Transfer Gateway

Listed below are the steps needed to request Roving Edge devices to be utilized as data transfer gateway for defense/Gov customers.

Figure 2. Steps needed to request Roving Edge devices to be utilized as data transfer gateway for defense/Gov customers.

IMPORTANT: Roving Edge Transport and Security Requirements

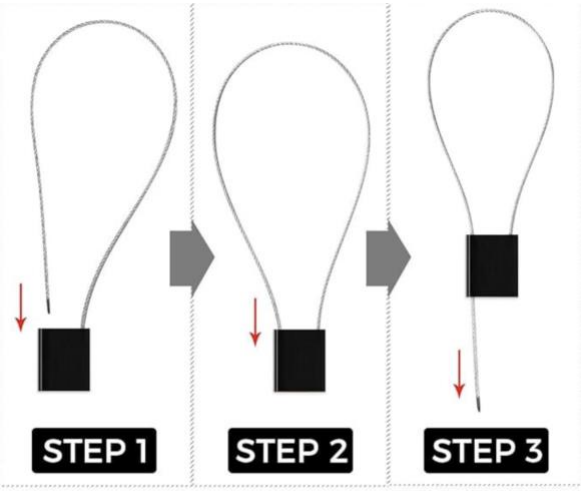
The Roving Edge device is shipped in a ruggedized, tamper-evident transport case specifically designed to protect the hardware during transit between Oracle Cloud regions and customer data centers. This case ensures physical security, shock resistance, and environmental protection to guarantee that the device arrives uncompromised.

To further meet data security and compliance requirements, all Roving Edge devices must be secured with security disposable seals during transit. This applies to both outbound shipments from Oracle to the customer and return shipments from the customer back to Oracle. Upon receipt, both the customer and the Oracle Cloud region Data Center Operations (DC Ops) teams must verify that the security disposable seals are intact.

This verification step is critical to preserving the integrity of the device and protecting any data to be uploaded to Oracle Cloud Object Storage.

If the security disposable seals are missing or found to be compromised, the Roving Edge device will not be permitted to connect to Oracle's cloud network infrastructure for data upload to the customer's Object Storage in Oracle Cloud Infrastructure (OCI).

Listed below are the required steps for properly applying the security disposable seals on the Roving Edge device.



This is a disposable seal. Once locked, it can't be used again.
You can cut it open with a plier.

Step 1. Customers request a new Roving Edge Device on Oracle Cloud Infrastructure OCI console and open a new Service Request. For these steps, refer to the link listed below or contact your sales representative.

- For Roving Edge Devices, see Creating a Roving Edge Infrastructure Device Node.
- For Roving Edge Ultra devices, see Creating a Roving Edge Ultra Node.
- After you have requested your devices, you must establish the certificate authority (CA). See Establishing the Certificate Authority for more information.

  NOTE: You're required to have an Oracle Cloud Infrastructure account to request Roving Edge Infrastructure devices. The account must be a UCM contract or Funded Allocation Model (FAM). It can't be Pay as You Go (PAYG) or Free Tier. If you currently have one of these unsupported Oracle Cloud Infrastructure accounts, contact your Account Team for instructions on how to upgrade to a supported Oracle Cloud Infrastructure account. You must also have a tenancy in an Oracle Cloud Infrastructure Realm and Region where Roving Edge Infrastructure is available. To learn how to request your Roving Edge Infrastructure devices in Oracle Cloud Infrastructure, refer to the following link: Requesting Devices. Refer to the Refer to Roving Edge Infrastructure and Roving Edge device data sheet for additional information regarding Roving Edge platform, contract requirements, and pricing.

- Open a Service Request for the new Roving Edge device to be utilized as Data Transfer Gateway. Refer to: How to create a Technical Service Request (SR) in My Oracle Support (Doc ID 1321379.1) **NOTE:** You must have purchased support, have an active cloud subscription, or have an active cloud trial license to access My Oracle Support.
- OC2/OC3 regions prepare and ships the Roving Edge to the customer.
- The device will be shipped to the customer address specified in the new request.
- Once customer receives the new Roving Edge device, Oracle Edge Cloud Solutions Engineering team along with customer will setup the Roving Edge device as data transfer gateway. **NOTE**: Oracle Linux data transfer gateway image for Roving Edge will be provided by Oracle Edge Cloud Engineering Solutions team via service request.
- Customer updates the service request with the latest status.

Step 2. Customer uploads data to Oracle Linux data transfer gateway instance:

- On-premises systems mount the NFSv4.1 share provided by the Oracle Linux data gateway instance deployed on Roving Edge Device.

  NOTE: NFSv4.1 share is already pre-configured with all tunable options for performance. **/datagateway** is the NFSv4.1 share already available to be mounted by the NFSv4.1 clients Below is the recommended NFS mount options for best performance to be utilized on the NFSv4.1 on-premises clients.

```
mount -t nfs4 -o
rsize=1048576,wsize=1048576,noatime,nodiratime,actimeo=3600,lookupcache=all,timeo=
600,retrans=10,vers=4.1,tcp  <Oracle Linux Data Gateway instance IP
address:/datagateway /tmp
```

- NFSv4.1 clients upload the data to the NFSv4.1 server running on the Oracle Linux data gateway instance deployed on Roving Edge Device.
- Customer confirms via service request data copy completion
- Customer request shipping label via service request
- Customer ships Roving Edge to one of the restricted OCI regions, OC2 or OC3. The Roving Edge Device is physically shipped to one of the restricted OCI regions, OC2 or OC3 for data upload to OCI using Oracle Fast Connect infrastructure. Oracle Data Center Operations team acts as the intermediary point for uploading data to the OC2/OC3 Oracle Cloud Infrastructure customer's object storage.
- Customer updates service request

Step 3. Data transfer process to OCI object Storage using Oracle FastConnect infrastructure

- Rover Operations team opens a new JIRA ticket to OC2 or OC3 DC operations team
- OC2 or OC3 DC operations team receives Roving Edg
- OC2 or OC3 DC operations team along with Edge Cloud Solutions Engineering teams performs data transfer configuration at OC2/OC3 DMZ area, such as: Network connection to DMZ transfer hosts/FastConnect network Infrastructure, and IP addressing change
- OC2 or OC3 DC operations team update internal JIRA ticket
- Oracle Edge Cloud Solutions Engineering teams update service request

Step 4. Data transfer monitoring

- OC2 or OC3 DC operations team along Oracle Edge Cloud Solutions Engineering teams monitor data transfer and confirm data transfer completion

- OC2 or OC3 DC operations team update internal JIRA ticket
- Oracle Edge Cloud Solutions Engineering teams update service request
- The customer verifies and confirms the completion of the data transfer and authorizes the factory reset of the Roving Edge device through a service request

  Note: Once customer approval is received, the Oracle Linux data transfer gateway instance will be terminated, all associated block devices will be deleted, and the Roving Edge device will undergo a factory reset.
- OC2 or OC3 DC operations team along with Edge Cloud Solutions Engineering teams factory reset the Roving edge device
- Roving Edge stays at OC2/OC3 DMZ areas
- Roving Edge billing stops
- OC2 or OC3 DC operations team close internal Jira ticket
- Oracle Edge Cloud Solutions Engineering teams close service request

Figure 3 shows the end-to-end architecture diagram of the Roving Edge as Data Transfer Gateway for DoD/Defense customers without Oracle Fast Connect or low network bandwidth.

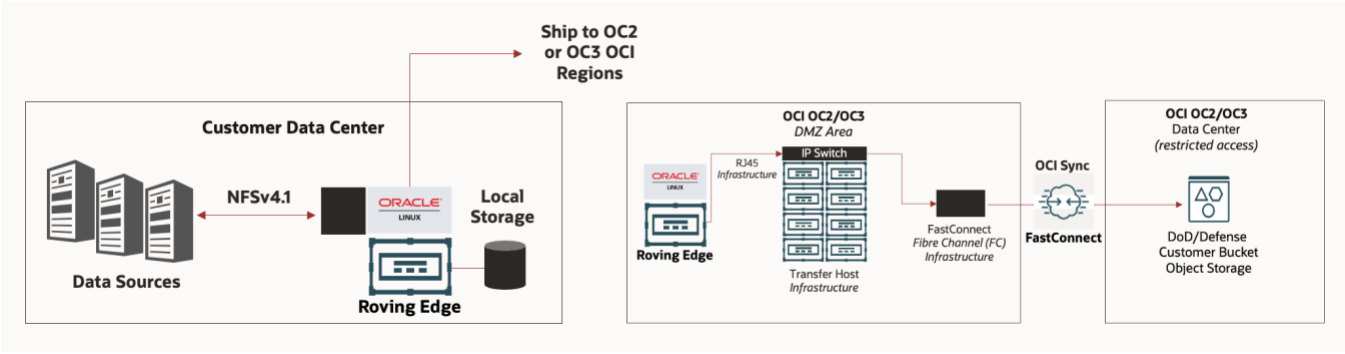


Figure 3. End-to-end architecture diagram of the Roving Edge as Data Transfer Gateway for DoD/Defense customers.

Configuring Roving Edge as Data Transfer Gateway

Step 1. Oracle Edge Cloud Solutions Engineering team will provide the customized Oracle Linux image for to be utilized as Data Transfer Gateway. This template already has all packages installed and tunable options to provide best performance for data sync to OCI.

Step 2. Once deployed the Oracle Linux Data Transfer gateway instance, access via SSH and key utilized during the instance deployment. Ex: ssh -i <your-key> opc@ip-address-of-the-instance.

IMPORTANT: Customer is required to change the password for the Oracle Linux transfer gateway instance. Oracle personnel will not have access to the customer's data or the Oracle Linux transfer gateway instance containing the customer's data. If any issues arise during the data upload to OCI or troubleshooting is required, access to the Oracle Linux transfer gateway instance for troubleshooting must be authorized by the customer through a Service Request. This ensures collaboration between the customer and members of the Edge Cloud Engineering Solutions or the OC2 or OC3 DC operations team for resolving any issues with the customer.

Step 3. Create new block storage volumes on Roving Edge.

- **Log in to the Roving Edge Console**:
  - Navigate to the **Block Volumes** section.

- Click **Create Block Volume**.
- Specify:
  - **Name**: A descriptive name for the volume.
  - **Size**: Set the maximum size for the volume (up to **6TB**).
- Select the **Compartment** where your resources reside.
- Click **Create**.

- **Repeat** for additional block volumes as needed until you reach the storage capacity requested by the customer in the Service Request. Maximum of 30TB.
- Attach the Block Volumes to Oracle Linux Instance. Example below shows five 6TB block storages attached to the Oracle Linux Data Transfer Gateway instance running on Roving Edge.

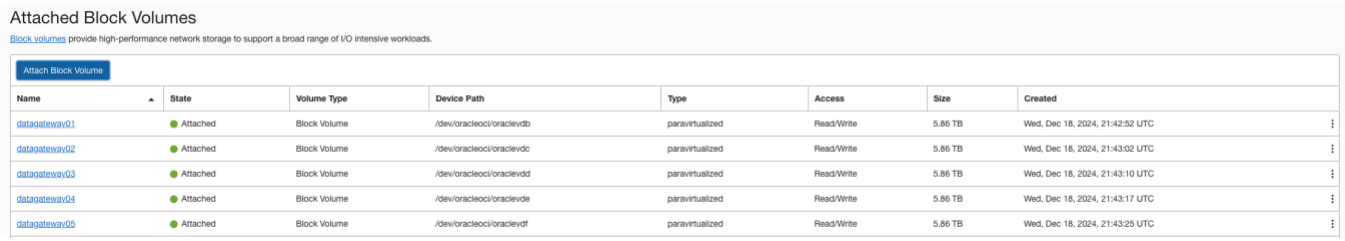


Figure 4. Attached block devices to the Oracle Linux Data Transfer Gateway – Roving Edge console

Step 4. Run **lsblk** to identify the new block devices configured on Roving Edge to be attached to the Oracle Linux Data Transfer Gateway instance.

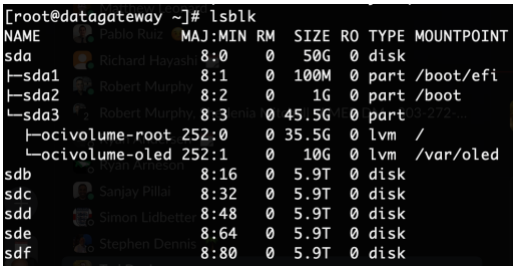


Figure 5. Attached block devices to the Oracle Linux Data Transfer Gateway instance

Step 5. As root user, run the **setup_storage.sh** script to create a new volume group, logical volume, file system, update the instance's fast, and mount the volume. Listed below is the output of the setup_storage.sh script. The script is located on **/usr/local/bin/setup_storage.sh**

```
[root@datagateway ~]# ./setup_storage.sh
Identifying block devices with size 5.9T...
Found devices: /dev/sdb
/dev/sdc
/dev/sdd
/dev/sde
/dev/sdf
Creating Volume Group: vol01...
  Physical volume "/dev/sdb" successfully created.
  Physical volume "/dev/sdc" successfully created.
  Physical volume "/dev/sdd" successfully created.
  Physical volume "/dev/sde" successfully created.
  Physical volume "/dev/sdf" successfully created.
  Volume group "vol01" successfully created
Creating Logical Volume: lvol01 in Volume Group: vol01...
  Logical volume "lvol01" created.
Formatting Logical Volume: /dev/vol01/lvol01 as XFS...
meta-data=/dev/vol01/lvol01      isize=512    agcount=59, agsize=268435455 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=15728629760, imaxpct=1
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=521728, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
Discarding blocks...Done.
Creating mount point: /datagateway...
Mounting /dev/vol01/lvol01 on /datagateway...
Updating /etc/fstab...
Logical Volume mounted and fstab updated successfully!
Script completed successfully.
```

NOTE: The new /datagateway will be mounted and available.

```
/dev/mapper/vol01-lvol01   xfs       29T  419G   29T   1% /datagateway
```

Step 6. Restart the NFS server: systemctl restart nfs-server

Configuring OCI CLI Authentication for Data Transfer

Step 1. Run the Configuration Setup: Configure the CLI with your OCI credentials: **oci setup config**

Step 2. Enter the following details when prompted:

- **User OCID**: Available in the OCI Console under "Identity, My Profile, User Information"
- **Tenancy OCID**: Found in "Tenancy Details" in the OCI Console.
- **Region**: OC2 or OC3 regions

- **Private Key Path**: Path to a private key file (~/.oci/oci_api_key.pem). The setup script generates or uses an existing API signing key.
- **Bucket namespace**: A bucket namespace is a unique identifier assigned to your tenancy. It is used as a top-level container for all Object Storage buckets and is required when performing Object Storage operations (especially from the CLI or SDKs).
- **Directory for the keys:** Enter a directory for your keys to be created [/root/.oci] is the default directory.
- **Enter a name for your key** [oci_api_key] is the default name for the key.
  - **Enter N/A for the passphrase for your private key** ("N/A" for no passphrase): N/A

Step 3. Test the authentication with the customer OCI object storage bucket:

Verify that the CLI is configured correctly: **oci os bucket list --compartment-id <compartment_OCID>**

NOTE: Replace <compartment_OCID> with your compartment OCID provided by the customer via Service Request.
Refer to: Configuring the CLI for additional questions.

Starting the Data Transfer to OCI Object Storage

Step 1. After successfully configuring the OCI CLI for authentication with Oracle Cloud Infrastructure (OCI), upload the data to the NFSv4.1 running on the customized Oracle Linux Instance deployed on Roving Edge Device. Below are the recommended NFS mount options for best performance to be utilized on the clients.

```
mount -t nfs4 -o
rsize=1048576,wsize=1048576,noatime,nodiratime,actimeo=3600,lookupcache=all,timeo=600,retrans=10
,vers=4.1,tcp  <Oracle Linux Data Gateway instance IP address:/datagateway /tmp
```

Step 2. Edit the OCI oci_sync.sh script and enter the correct bucket name on OCI provided by the customer via Service Request. Open the /usr/local/bin/oci_sync.sh script using a text editor (e.g., vi) and update the configuration variables at the top of the file to match your specific environment. After making the necessary changes, save and close the script.
The following variables must be configured:

```
BUCKET_NAME="Your OCI bucket name"
NAMESPACE="Your OCI namespace"
REGION="Your OCI region, e.g., us-phoenix-1"
```

Step 3. Once the date is uploaded on the NFSv4.1 share, execute the following command to start the data transfer from the local NFSv4.1 (datagateway) share to the specified OCI Object Storage bucket:

Step 4. Enable the Data Transfer Gateway service to start on boot:

sudo systemctl enable oci-sync.service

Step 5. Start the Data Transfer Gateway service

sudo systemctl start oci-sync.service

Step 6. Check the service status:

sudo systemctl status oci-sync.service

below is the output of the command:

```
systemctl status oci-sync.service
● oci-sync.service - OCI Object Storage Sync Service
   Loaded: loaded (/etc/systemd/system/oci-sync.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2025-04-12 13:15:06 GMT; 1s ago
 Main PID: 1699391 (oci_sync.sh)
    Tasks: 6 (limit: 48326)
   Memory: 6.8M
   CGroup: /system.slice/oci-sync.service
           ├─1699391 /bin/bash /usr/local/bin/oci_sync.sh
           ├─1699398 /bin/bash /usr/local/bin/oci_sync.sh
           ├─1699399 find /datagateway -type f -print0
           └─1699400 /bin/bash /usr/local/bin/oci_sync.sh

Apr 12 13:15:06 datagateway-stig systemd[1]: Started OCI Object Storage Sync Service.
```

IMPORTANT: The initialization time of the transfer operation may vary based on the number and size of files in the /datagateway filesystem and the available network bandwidth. This is especially true in scenarios where the /datagateway filesystem contains millions of files. Please wait until the /var/log/oci_sync.log progresses past the Starting OCI Sync... phase. Monitoring will begin automatically once the Grafana dashboards become active.

Step 7. Monitor the data upload via Grafana dashboard. Go to: http://<ip address of your Oracle Linux Data Transfer instance:3000

- login with admin user and admin password
    - IMPORTANT: Grafana will ask you to change the password. A screen like the listed below will be available.

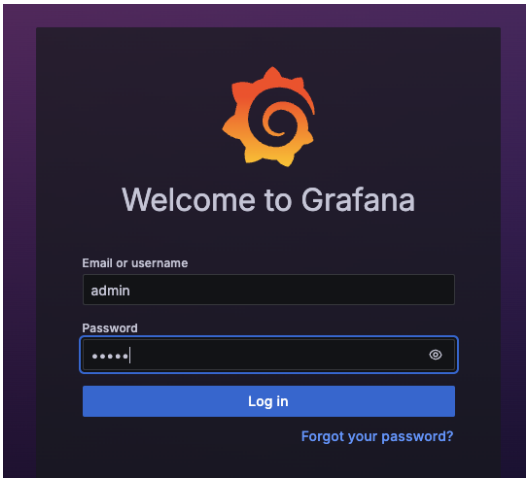


Figure 6. Grafana dashboard access.

- Click Home, Dashboard, then click on Data Transfer Gateway.

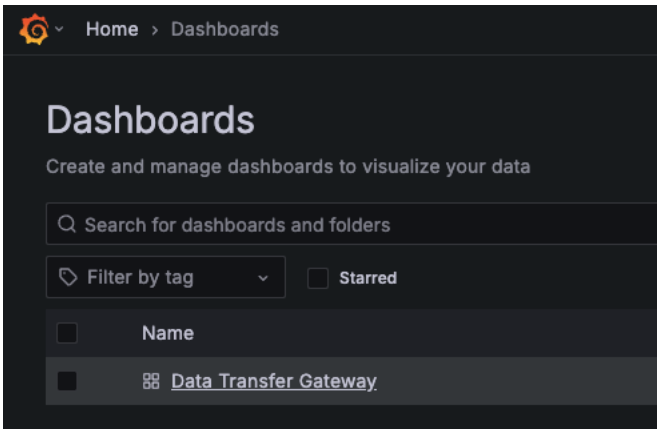


Figure 7. Grafana dashboard for Data Transfer Gateway

- The Grafana dashboard of the Data Transfer Gateway will be available. Use this dashboard to monitor the data transfer operation. The example below demonstrates a successful PoC and performance test, where approximately 3.43 TB of data, comprising 1 million files of varying sizes (from kilobytes to over 100 GB) and diverse file types across thousands of directories, was successfully uploaded to an OCI bucket.

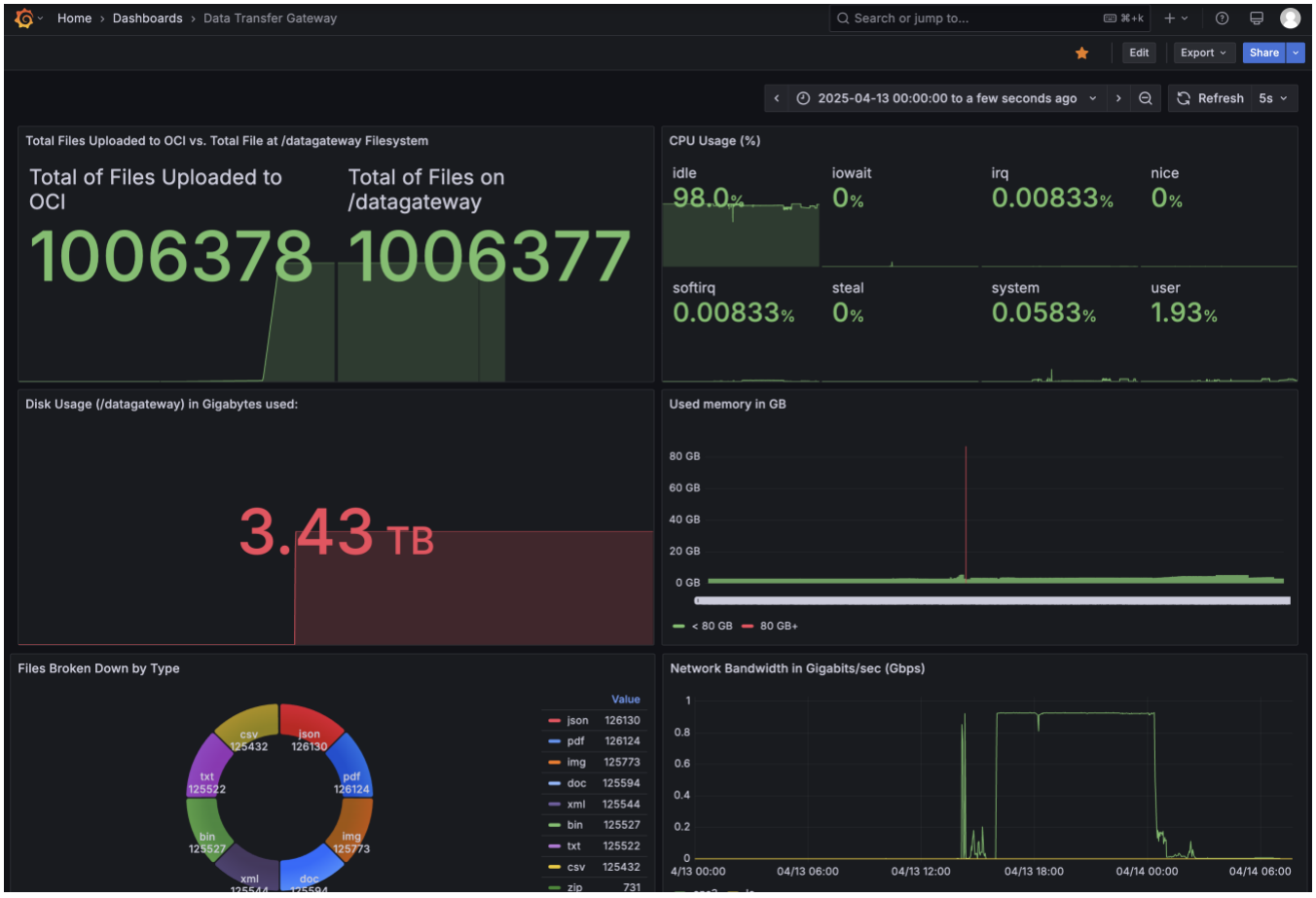


Figure 8. Grafana dashboard overview for Data Transfer Gateway

NOTE: All logs of the data transfer operation are also available on /var/log/oci_sync.log

Listed below is the overview of the OCI bucket with all objects uploaded from the Data Transfer Gateway:

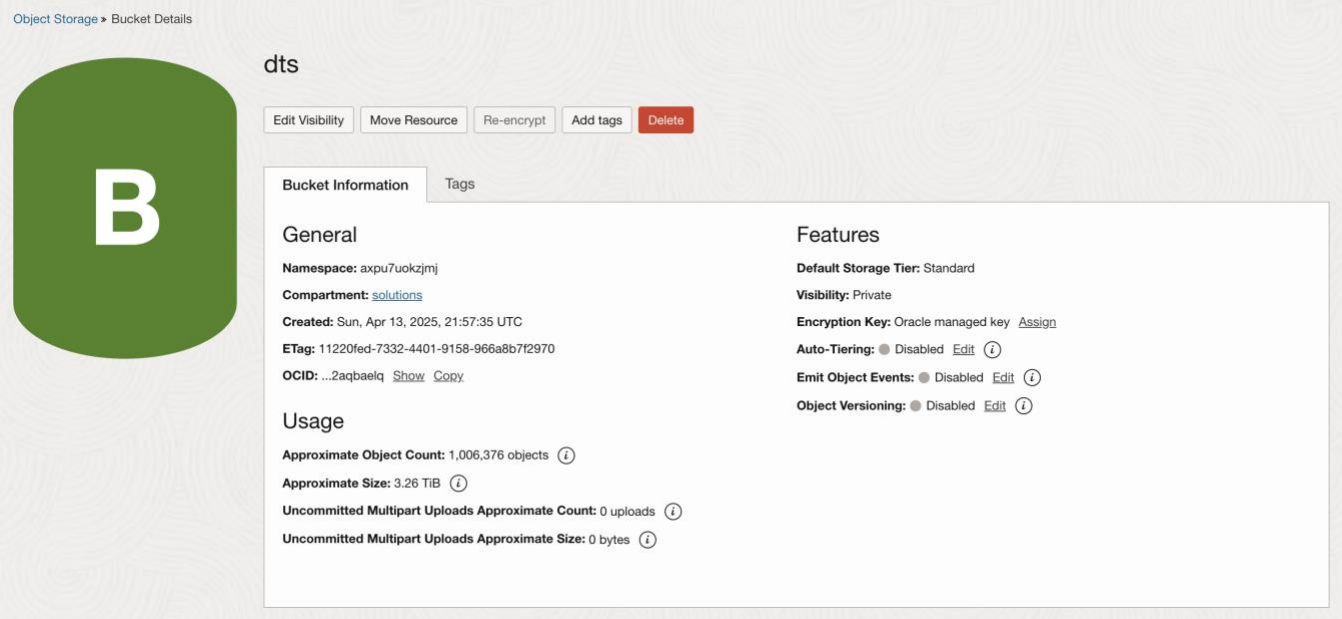


Figure 9. OCI Object storage overview.

DC Operations Runbook – Data Upload Process

Due to varying IP address and CIDR block configurations on customer Roving Edge devices, it is necessary to adjust the Roving Edge's public pull IP address and management IPs to align with the OC2/OC3 DMZ area network CIDR when the device is returned. This ensures the Oracle Linux Data Transfer Gateway instance on the Roving Edge device can access the OCI bucket.

The solution requires a total of three IP addresses, they are:

- One for the Rover management interface. Free IP address from the DHCP pool set manually on the Rover.
- One from the public IP pool, which will be assigned to the Oracle Linux instance (used to communicate with OCI Object Storage). Free IP address from the DHCP pool set manually on the Rover.
- One for the laptop that will access the Rover management interface. Automatically received from the DHCP server.

IMPORTANT:

- Due to network infrastructure constraints, the solution supports **only one Roving Edge device** at a time for data transfer and connectivity to the DMZ network.
- The Roving Edge device **requires static IP addressing** and does not support DHCP. However, IP addresses from a DHCP pool can be used if they are **manually and statically assigned** to the Roving Edge device's management interface, as well as to the pool of public IP address configurations.
- By default, Oracle Linux Data Transfer Gateway instance has MTU 1500 configured by default.

Roving Edge device public and management IP addressing configuration

To update the public pull IP address, access the Roving Edge device console and follow the steps outlined below.

Step 1. Using a laptop, connect to the Roving Edge using the terminal emulation to identify the IP address/CIDR configuration.

Microsoft Windows: PuTTY
Mac OS X: ZOC or screen (for example: screen /dev/ttyusbserialX 115200)
Linux: PuTTY, Minicom, screen (for example: screen /dev/ttyUSBX 115200)

Based on your host OS, use the appropriate method to ensure that the pl2303 USB driver is installed. This USB driver is required for connectivity to the Roving Edge Device DB-9 serial or console port. The USB driver is preinstalled on Oracle Unbreakable Enterprise Kernel. The following command shows that the USB driver is present:

```
[root@localhost ~]# modprobe pl2303
[root@localhost ~]# lsmod | grep -i pl2303
pl2303 24576 0
[root@localhost ~]# modinfo -d pl2303
Prolific PL2303 USB to serial adaptor driver
```

If the driver isn't installed, use the appropriate method to install the driver. For example, go to the Microsoft Windows or Apple store to obtain and install the driver.

Step 2. Configure the terminal emulator software settings as follows:

```
Terminal Type: VT100+
Bits per second: 115200
Data Bits: 8
Parity: None
Stop Bits: 1
Flow Control: None
```

NOTE: With PuTTY, you can't configure all these settings individually. However, you can configure the PuTTY default settings by selecting the Serial connection type and specifying 115200 for the Serial Line baud speed. This configuration is sufficient to use PuTTY as a terminal emulator for the device.

For additional information, refer to Roving Edge Device Setup Guide and Roving Edge Operating Serial Console

Step 3. Unlock the Roving Edge device and activate web console user account.

Anytime you reboot the Roving Edge device, it reverts to a locked state. Receiving a **Device is locked** message after trying to connect to an API endpoint or console is indicative that the device is in a locked state. Unlock the device to proceed.

NOTE: To unlock the Roving Edge device, the passphrase configured when the customer created the device node will be needed. Customer needs to provide the passphrase via SR.

- From the serial console you will be asked to **Enter the passphrase to unlock the screen**:
- Enter the unlock passphrase to unlock the device.

```
Enter the passphrase to unlock the screen: ***************
The screen is unlocked successfully!
Press ENTER to return...
```

- Select the Unlock Device options from the menu, then enter the passphrase.

NOTE: For security, once the Roving Edge Device is unlocked, you will be asked to change the passphrase. Below is the screenshot with the step-by-step.

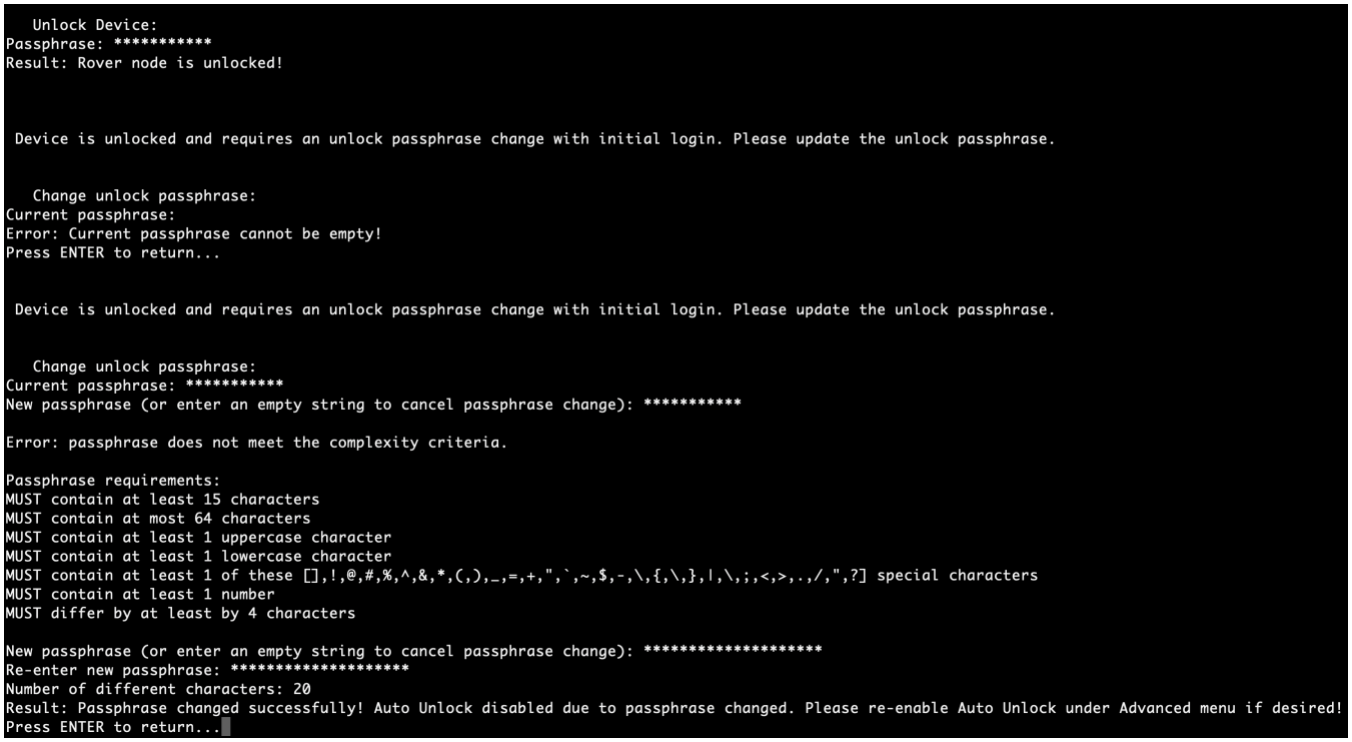


Figure 9. Roving Edge Device unlocking and passphrase change process.

Step 4. Press ENTER to return to the main menu, then select option **13) Advanced Menu** to reset the password of the root user so access to the web interface to manage the Roving Edge device can be granted.

```
1) Unlock Device
2) Change Passphrase
3) Configure Networking
4) Show Status
5) Show System Diagnostics
6) Shutdown Device
7) Reboot Device
8) Enter Safe-Mode
9) Exit Safe-Mode
10) Shred Key
11) Recover Key
12) Reset Device
13) Advanced Menu
14) Cluster Health
15) Node Health
16) Diagnostics
17) Help
```

- Under Advanced Menu option, select option **7) Identity Management, then option 1) Reset Web Console User Account**

```
        Advanced Menu
   -------------------------

1) Banner Management
2) Network Management
3) Password Management
4) System Upgrade Management
5) Storage Management
6) Auto Unlock Management
7) Identity Management

       Identity Management
   ------------------------------

1) Reset Web Console User Account
2) Help
3) Go Back

Enter command number (or press Ctrl+C to go back): 1
Reset Web Console User Account
WARNING! By resetting the Reset Web Console User Account, you will receive an one time password
in
the screen below after the reset success.
Confirm to reset web console user account (Y/y):
Please Enter: y
Please confirm by entering the unlock passphrase: ********************
Please enter the web console username for the reset request: root
Result: Success!
Temporary Web Console User Account Password: <the new password of root user>

Press ENTER to return...
```

- The Red is now accessible via web console with the root user and temporary password generated above.

Step 5. On the serial connection, go to the main menu, then check the IP address currently setup on the Roving Edge Device. On the main menu, select option **3) Configure Network**, then select option **2) Display Settings**. The current IP address of the management interface will be listed.

```
1) Unlock Device
2) Change Passphrase
3) Configure Networking
4) Show Status
5) Show System Diagnostics
6) Shutdown Device
7) Reboot Device
8) Enter Safe-Mode
9) Exit Safe-Mode
10) Shred Key
11) Recover Key
12) Reset Device
13) Advanced Menu
14) Cluster Health
15) Node Health
16) Diagnostics
17) Help
```

```
1) Set Node IP Settings (Current Node Only)
2) Display Settings
3) Set Public IP Pool Range for Compute Instances (Cluster-Wide)
4) Display Public IP Pool Status
5) Control Network Ports
6) Configure DNS (Cluster-Wide)
7) Configure NTP (Cluster-Wide)
8) Configure Subnet Gateway (Cluster-Wide)
9) Reset Network
10) Configure Ethernet Bonding
11) Help
```

Step 6. Direct connect with a RJ-45 cable to the Roving Edge device network interface 1 using a laptop, then setup the laptop network interface to the same IP address, CIDR, and subnet currently configured on the Roving Edge Device.

Step 7. Access the Roving Edge Device administration console via **https://IP address of the roving edge device:8015** with the current IP address setup on the Rover Edge device and credentials configured on step 4.

> **NOTE:** Download the Root CA Certificate. Download the root CA certificate from the Roving Edge Device to your host. The host is the system you plan to use to manage services on the device. The root CA certificate acts as a credential to validate the identity of the host and enables communication between the device and host.

Use one of the following procedures to download the root CA certificate from a Roving Edge Device to your host.

Linux and Mac OS

A. On your host, use the following command to download the root CA certificate from the Roving Ede device:

echo -n | openssl s_client -showcerts -connect <RED_ip_address>:8015 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > redroot.pem

B. Based on the OS you're using, perform one of the following actions:
    1. If you're using a Mac OS system on a Safari or Chrome browser, use the MacOS Keychain. Open the Finder and look for the redroot.pem file. Double-click the file and install the certificate.
    2. If you're using a Linux system on a Chrome browser, go to **Chrome Settings (or Preferences) > Security and Privacy > Security> Manage certificates > Authorities tab > Import > Browse** and choose the redroot.pem file in the location where you created it. Next, click **Open** and select the **Trust this certificate for identifying websites** option. The certificate appears in the list of certificate authorities.

Microsoft Windows

A. Use the following command to download the root CA certificate from the Roving Edge device:
    a. execute command - openssl.exe s_client -connect <RED_ip_address>:8015 -showcerts
B. Copy and paste the root CA certificate from the browser to Notepad and save the file with the filename redroot.cer. The certificate starts with a line containing: BEGIN CERTIFICATE and end with the line containing: END CERTIFICATE
C. Using an Edge or a Chrome browser, perform these steps:
    a. Add the certificate to the trust store by opening the File Explorer and double-clicking the redroot.cer file.
    b. Install the certificate.
    c. Place all certificates in the Trusted Root Certificate Authorities folder.

NOTE: For security reasons, the first time you login into the Roving Edge Web Console, you will be asked re generate a new secret. To complete this task, click on Regenerate Secret button once asked in the web console, then on copy option to copy the new and permanent password of the root user. Login again with the new password.

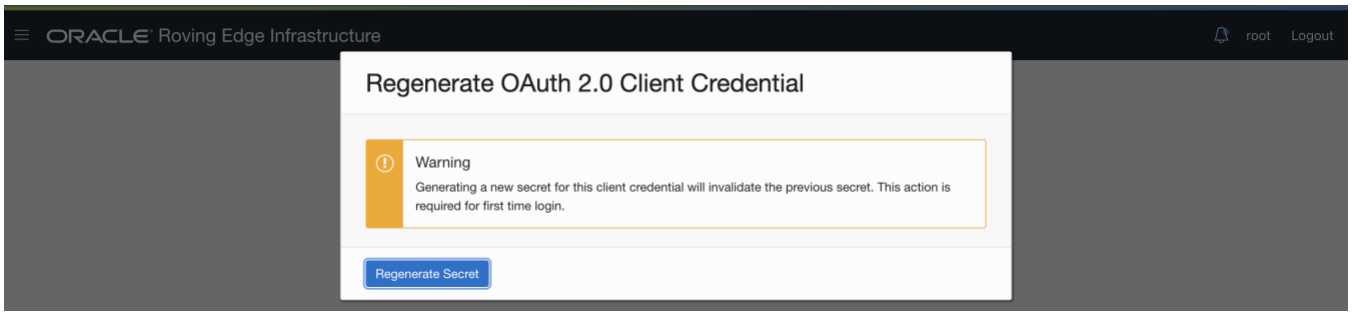


Figure 10. Roving Edge Device – Regenerate OAuth credentials 1.

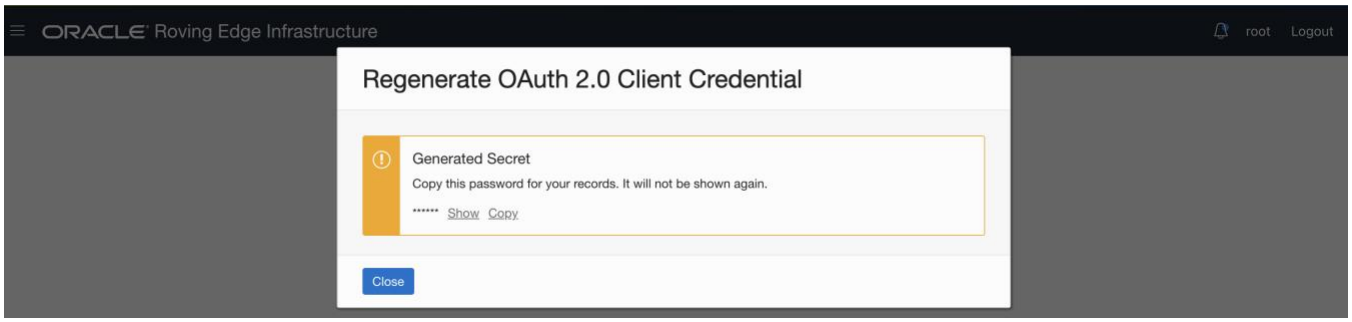


Figure 11. Roving Edge Device – Roving Edge Device – Regenerate OAuth credentials 2.

Step 8. Stop the Oracle Linux Data Transfer instance, then go to **Networking, Public IPs,** then select the three dots in front of the reserved public IP address pool and click **terminate**.

Step 9. Go to Compute, click on the instance name, under resources, click on attached VNICs. Click on the primary VNIC name.

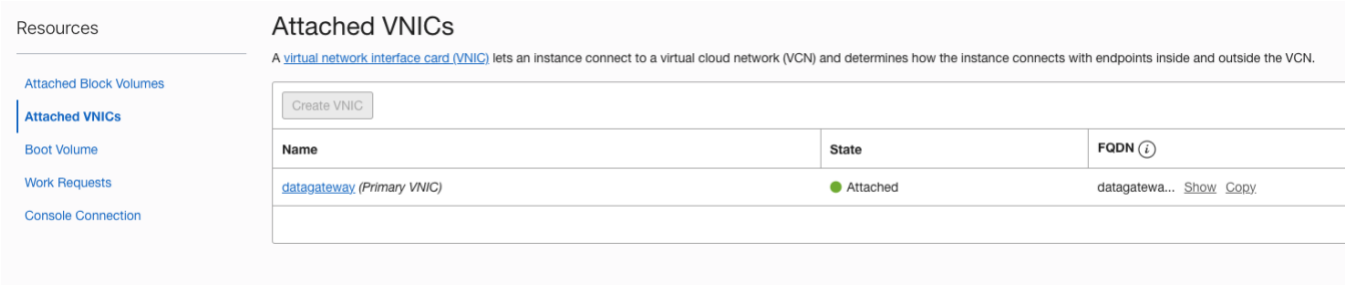


Figure 12. Attached VNICs on Roving Edge Device.

Step 10. On the IP addresses screen, click on the three dots as listed below, then click edit.

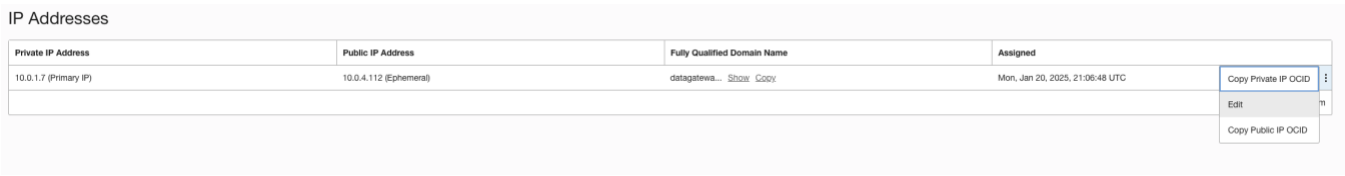


Figure 13. Roving Edge IP Address screen.

Step 11. Select **No public IP** option, then click update. This will unassign the ephemeral public IP address previously setup on this instance, so the new IP address public pool range can be configured.

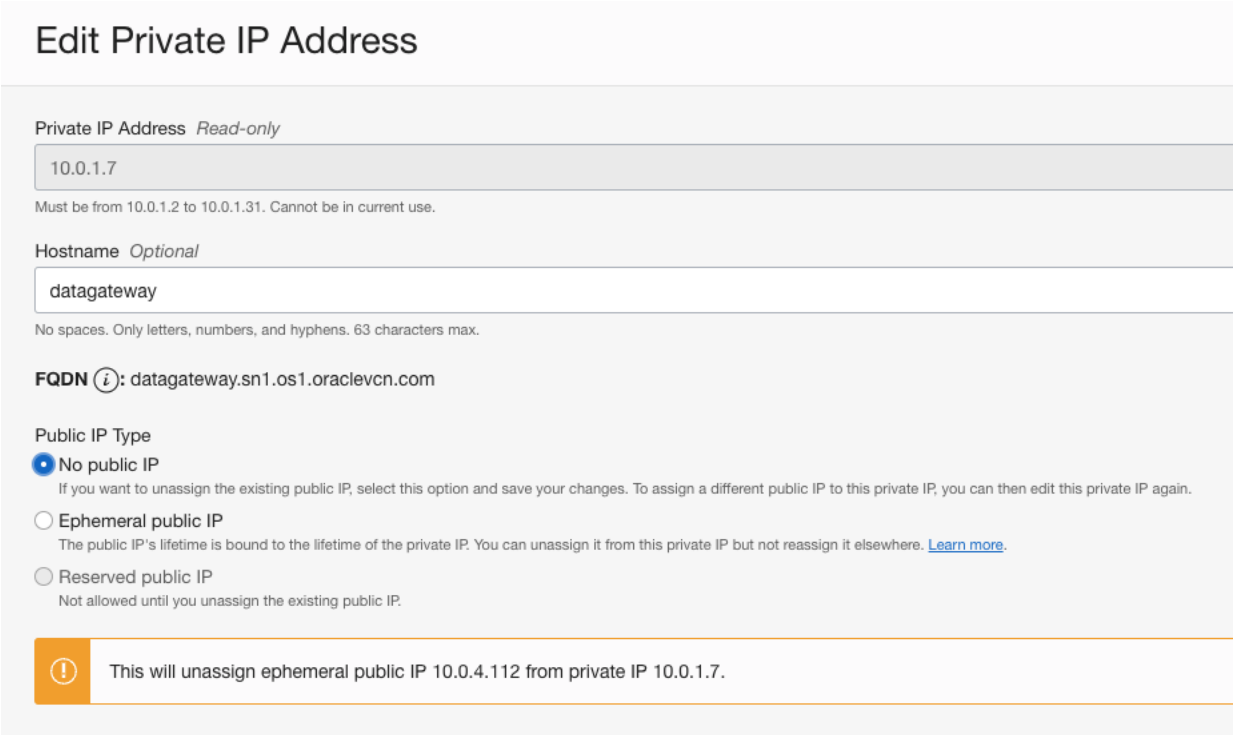


Figure 14. Ephemeral public IP address configuration on Roving Edge Device.

Step 12. Confirm the public IP address has been successfully removed from the Oracle Linux Data Transfer Gateway instance.

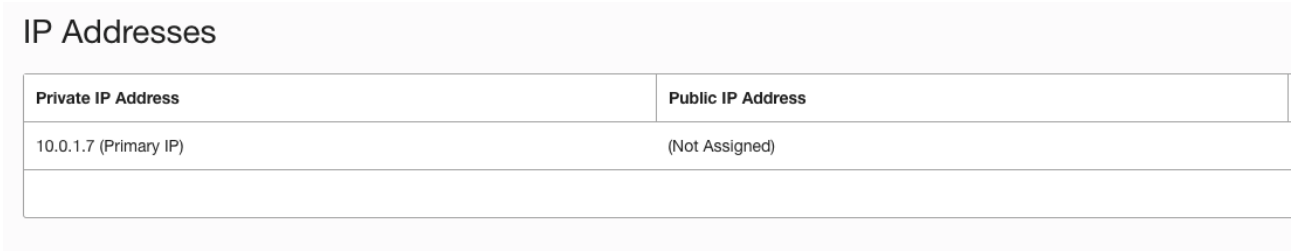


Figure 15. Ephemeral public IP address status on Roving Edge Device.

Step 13. Next step, a new public IP address pool needs to be configured. Using your laptop, connect to the Roving Edge device serial port using the same command line mentioned on steps 1 and 2.

Step 14. If asked again, unlock the Roving Edge device and activate web console user account.

- From the serial console you will be asked to **Enter the passphrase to unlock the screen**:
- Enter the unlock passphrase to unlock the device.

```
Enter the passphrase to unlock the screen: ***************
The screen is unlocked successfully!
Press ENTER to return...
```

- Select the Unlock Device options from the menu, then enter the passphrase.

```
1) Unlock Device
2) Change Passphrase
3) Configure Networking
4) Show Status
5) Show System Diagnostics
6) Shutdown Device
7) Reboot Device
8) Enter Safe-Mode
9) Exit Safe-Mode
10) Shred Key
11) Recover Key
12) Reset Device
13) Advanced Menu
14) Cluster Health
15) Node Health
16) Diagnostics
17) Help
```

- The device is unlocked, and the serial console menu is displayed.

Step 15. Set Node IP Setting

Via terminal emulation, adjust the IP address, subnet, gateway, DNS and NTP information on the Roving Edge device to match the local network CIDR infrastructure.

- From the Roving Edge Device serial console, select **Configure Networking** and **Set Node IP Settings** options:

```
1) Unlock Device
2) Change Passphrase
3) Configure Networking
4) Show Status
5) Show System Diagnostics
6) Shutdown Device
7) Reboot Device
8) Enter Safe-Mode
9) Exit Safe-Mode
10) Shred Key
11) Recover Key
12) Reset Device
13) Advanced Menu
14) Cluster Health
15) Node Health
16) Diagnostics
17) Help

                    Network Configuration
   ------------------------------------------------------------

1) Set Node IP Settings (Current Node Only)
2) Display Settings
3) Set Public IP Pool Range for Compute Instances (Cluster-Wide)
4) Display Public IP Pool Status
5) Control Network Ports
6) Configure DNS (Cluster-Wide)
7) Configure NTP (Cluster-Wide)
8) Configure Subnet Gateway (Cluster-Wide)
9) Reset Network
10) Configure Ethernet Bonding
11) Help

Enter command number (or press Ctrl+C to go back): 1
```

Step 16. Enter the new IP address for the Roving Edge management interface, the subnet mask length (in CIDR black, ex: 22, 24, etc..), and Gateway.

```
Configuring IP address, subnet mask length, gateway
Example:
        IP Address          : 10.0.0.2
        Subnet Mask Length  : 24
        Gateway             : 10.0.0.1
Subnet mask length 24 <=> 255.255.255.0

IP Address: X.X.X.X
```

- For DNS configuration, select options **6) Configure DNS (Cluster-Wide)** from the **Network Configuration** menu and select option **2) Update DNS Configuration.** Enter the DNS server IP addresses (primary and secondary), then press Enter to save the change and return to the DNS Configuration menu. Press Ctrl+C to move back to the **Network Configuration menu.**

> NOTE: Ensure to set the DNS server currently utilized by the network infrastructure. Oracle Linux instance will point to the DNS server information set on the Rover edge device for name resolution and connection with the OCI Object Storage.

```
                    Network Configuration
   ------------------------------------------------------------

1) Set Node IP Settings (Current Node Only)
2) Display Settings
3) Set Public IP Pool Range for Compute Instances (Cluster-Wide)
4) Display Public IP Pool Status
5) Control Network Ports
6) Configure DNS (Cluster-Wide)
7) Configure NTP (Cluster-Wide)
8) Configure Subnet Gateway (Cluster-Wide)
9) Reset Network
10) Configure Ethernet Bonding
11) Help


      DNS Configuration
   -------------------------

1) Display DNS Configuration
2) Update DNS configuration

Enter command number (or press Ctrl+C to go back): 2
Enter primary nameserver ip: X.X.X.X
```

- For NTP configuration, select options **7) Configure NTP (Cluster-Wide)** from the **Network Configuration** menu and select option **2) Update NTP Configuration.** Enter the NTP server IP addresses (primary and secondary), then press Enter to save the change and return to the DNS Configuration menu. Press Ctrl+C to move back to the **Network Configuration menu.**

```
                    Network Configuration
   ------------------------------------------------------------

1) Set Node IP Settings (Current Node Only)
2) Display Settings
3) Set Public IP Pool Range for Compute Instances (Cluster-Wide)
4) Display Public IP Pool Status
5) Control Network Ports
6) Configure DNS (Cluster-Wide)
7) Configure NTP (Cluster-Wide)
8) Configure Subnet Gateway (Cluster-Wide)
9) Reset Network
10) Configure Ethernet Bonding
11) Help
```

Step 17. Adjust the public ip addressing pull of the Roving Edge device

Via terminal emulation, adjust the public IP address pull of the Roving Edge device to the available public (or private) CIDR range of the FastConnect infrastructure. Only one public IP address is need for the Oracle Linux Data Gateway instance on the Roving Edge device, enter the new public IP address as listed below.

- From the Roving Edge Device serial console, select **Configure Networking** option:

```
   Roving Edge Device
   ----------------------

1) Unlock Device
2) Change Passphrase
3) Configure Networking
4) Show Status
5) Show System Diagnostics
6) Shutdown Device
7) Reboot Device
8) Enter Safe-Mode
9) Exit Safe-Mode
10) Shred Key
11) Recover Key
12) Reset Device
13) Advanced Menu
14) Cluster Health
15) Node Health
16) Diagnostics
17) Help

Enter command number: 3
```

- Under Network Configuration, **Set Public IP Pool Range for Compute Instances (Cluster-Wide)**

```
                        Network Configuration
   ------------------------------------------------------------

1) Set Node IP Settings (Current Node Only)
2) Display Settings
3) Set Public IP Pool Range for Compute Instances (Cluster-Wide)
4) Display Public IP Pool Status
5) Control Network Ports
6) Configure DNS (Cluster-Wide)
7) Configure NTP (Cluster-Wide)
8) Configure Subnet Gateway (Cluster-Wide)
9) Reset Network
10) Configure Ethernet Bonding
11) Help

Enter command number (or press Ctrl+C to go back): 3
```

NOTE: While the explanation below covers the full configuration steps, only a single IP address is required for the public IP pool range. This IP will serve as the public address used by the Oracle Linux Data Transfer Gateway to connect with the OCI bucket specified in step 18.

When prompted to provide the IP address range, enter the public IP in the first field and leave the second field blank.

```
Enter a list of IP address ranges for public IP pool separated by ENTER.

Expected IP address range format is: x.x.x.x-y.y.y.y
Where "x.x.x.x" and "y.y.y.y" are IP addresses representing range boundaries.
For example, an input string "172.10.20.1-172.10.20.30" represents a range
starting with 172.10.20.1 and ending with 172.10.20.30 address (inclusive).

Individual IP addresses can be entered as: 172.10.20.35

WARNING: This will empty current public IP pool (if present),
         and re-populate it with new ranges from the input.

Enter IP address range followed by ENTER (or an empty string to stop):
 > 10.0.4.151
 >
Validating public IP pool. Please wait...
Applying changes. Please wait...

Complete!
Press ENTER to exit...
```

- Wait for the new Public IP pool configuration to take effect.

```
Validating public IP pool. Please wait...
Applying changes. Please wait...

Complete!
```

Step 18. Check if the new Public IP address have been correctly set to the Oracle Linux Data Gateway instance on the Roving Edge device

- Connect to the Roving Edge administration console using the new IP address setup for the management interface and create a new reserved IPs pool. On the Roving Edge administration console, click on **Networking, Public IPs**, then **Create Reserved Public IP.** Enter a name for the new reserved public IP pool, then click on **Create Reserved Public IP.**

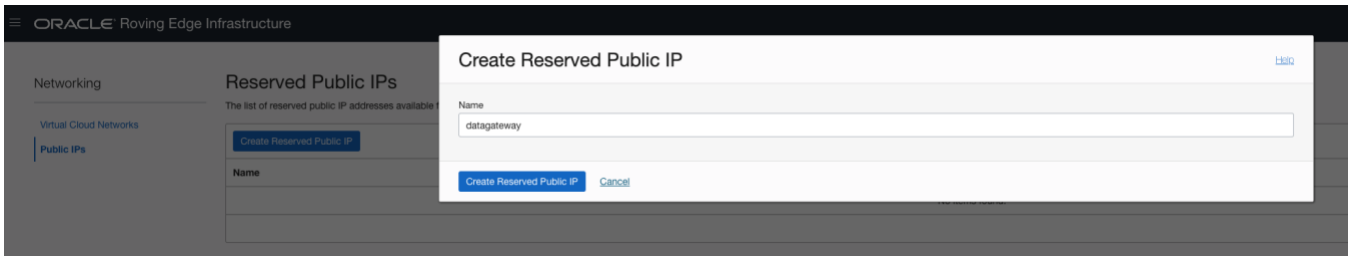


Figure 16. Roving Edge Device – Creating reserved public IP.

- Go to **Compute**, click on the instance name, under resources, click on **attached VNICs**. Click on the primary VNIC name. On the IP addresses screen, click on the three dots as listed in-front of the (Primary IP), then click edit.
- Select Ephemeral public IP option, then click update. A new public IP address from the new reserved public IP address pool will be assigned to the interface.

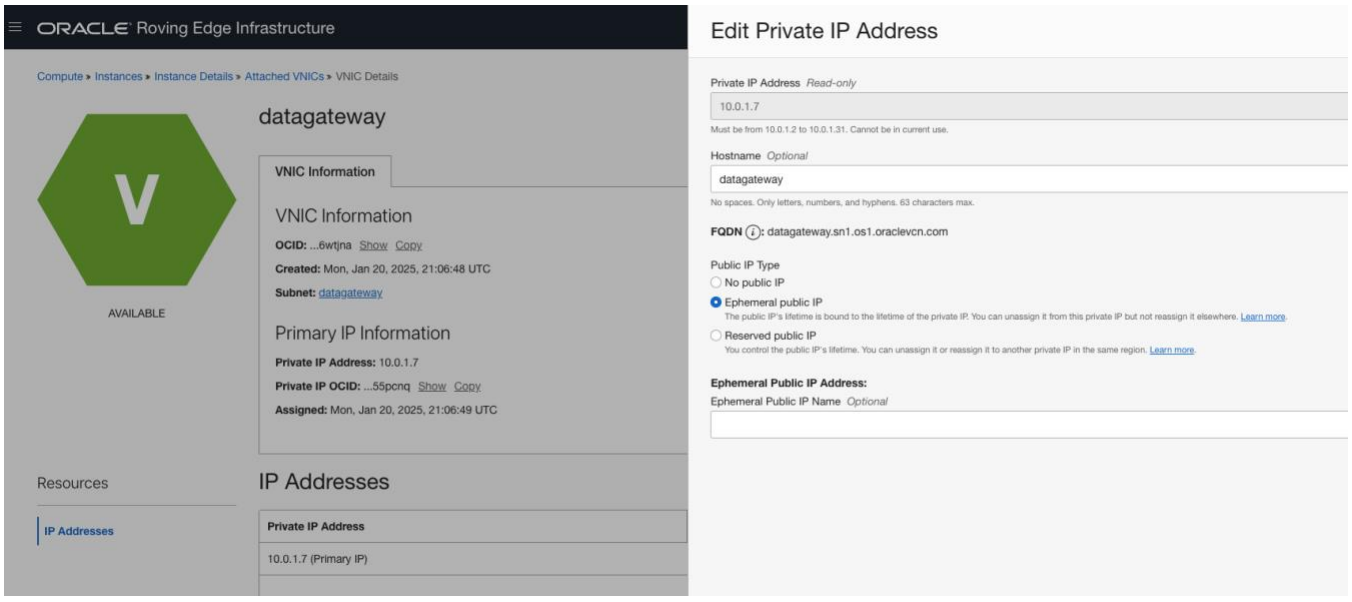


Figure 17. Roving Edge Device – Ephemeral public IP configuration.

NOTE: Make sure the FastConnect network segment that the Roving Edge device connects to does not require an internal proxy to access OCI Object Storage. If an internal proxy is required, you'll need access the Oracle Linux Transfer Gateway instance and setup the proxy, so OCI Sync can connect to the OCI bucket via proxy. ex:

export http_proxy=http://proxy.example.com:8080

export https_proxy=http://proxy.example.com:8080

- Start the Oracle Linux Data Gateway instance, and check if the new Public IP address has been correctly assigned.

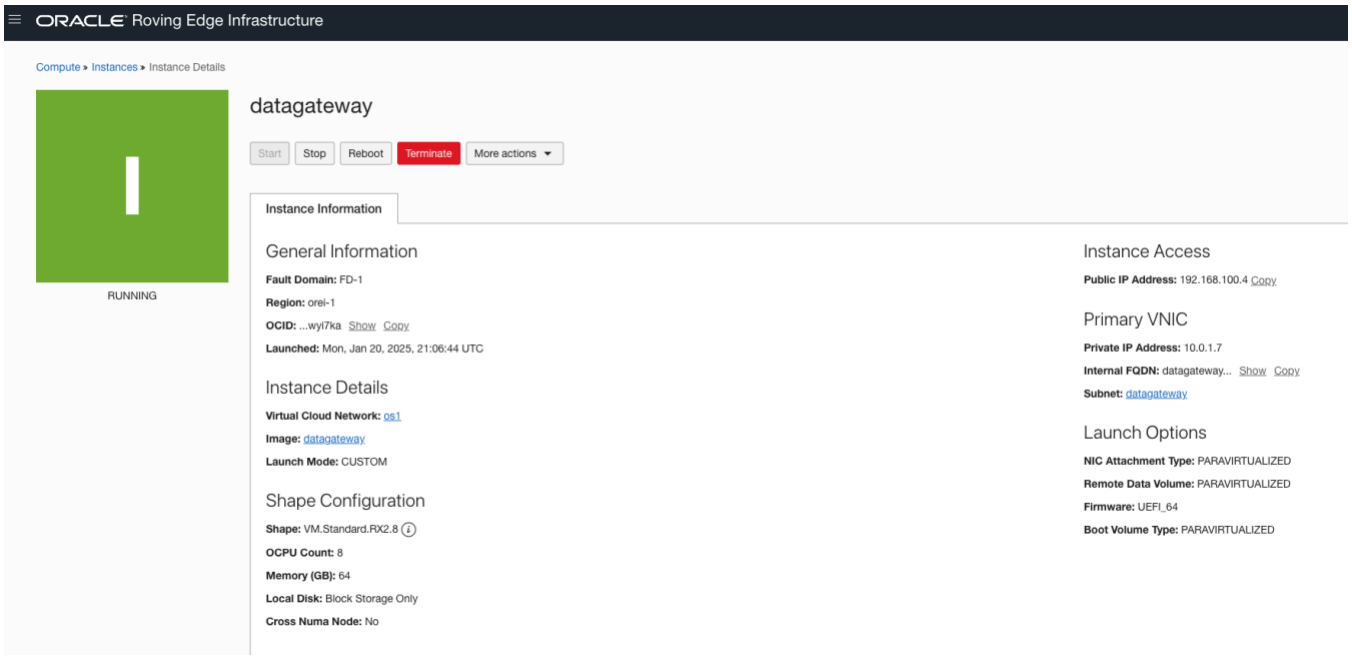


Figure 18. Starting Oracle Linux Gateway instance.

- Oracle Linux Data Gateway instance will start the Oracle Data Transfer service and upload the data to the customer's OCI Object Storage.

Step 19. Monitor the data upload via Grafana dashboard. Go to: https://<ip address of your Oracle Linux Data Transfer instance:3000

- Login with admin user and the password previously configured

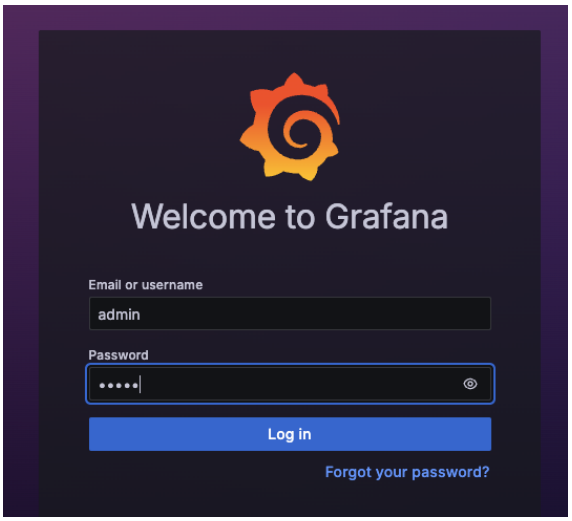


Figure 19. Grafana dashboard access.

- Click Home, Dashboard, then click on Data Transfer Gateway.

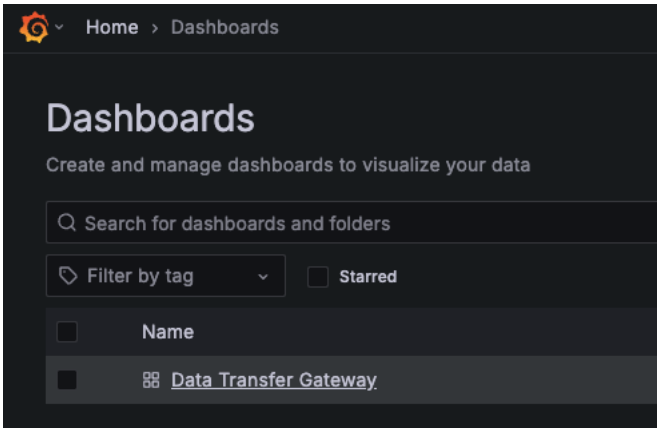


Figure 20. Grafana dashboard for Data Transfer Gateway

- The Grafana dashboard of the Data Transfer Gateway will be available. Use this dashboard to monitor the data transfer operation.

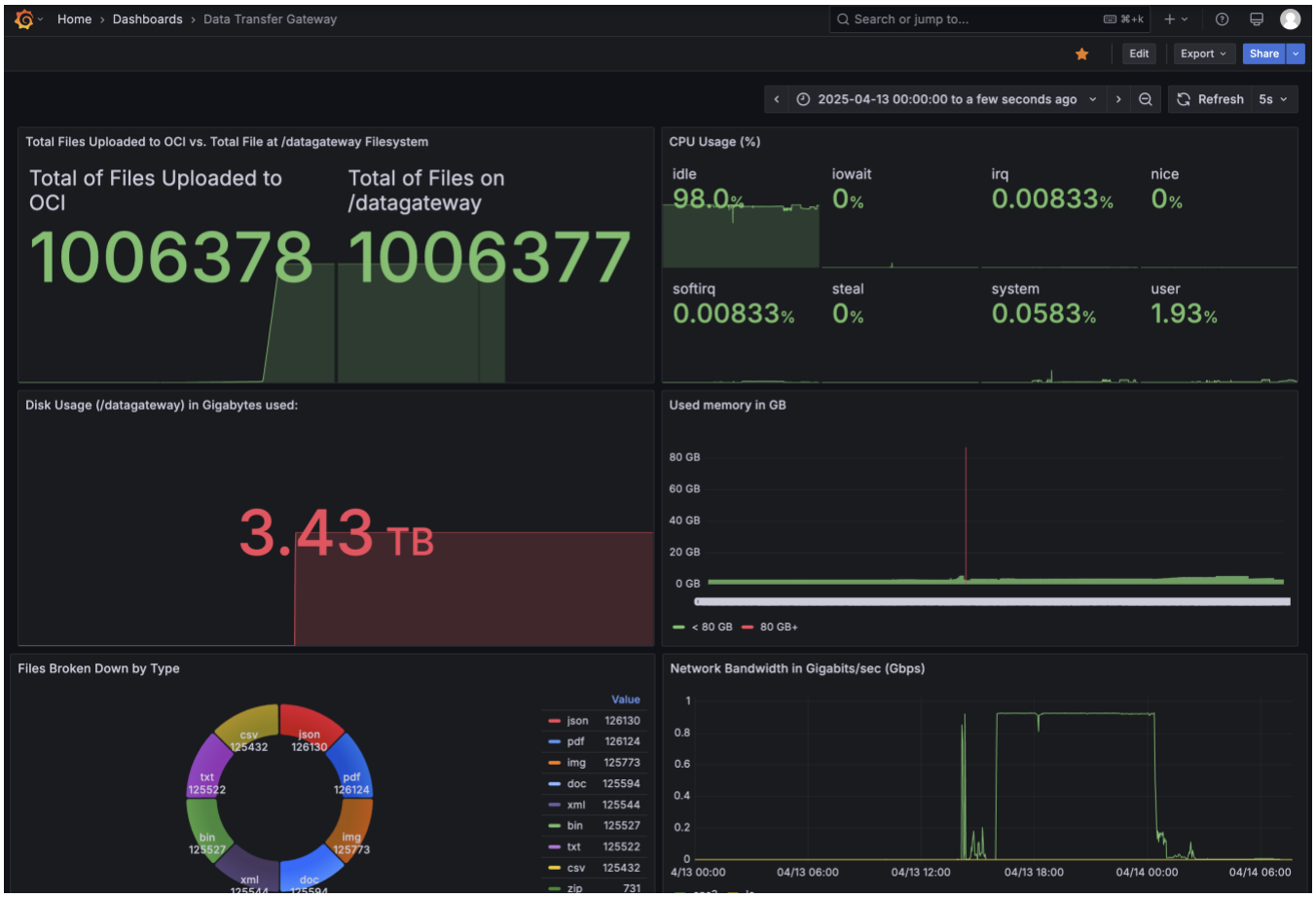


Figure 21. Monitoring OCI Sync data upload.

NOTE: All logs of the data transfer operation are also available on /var/log/oci_sync.log

Step 20. DC Ops team monitors data transfer and confirm data transfer completion via DO ticket.

Step 21. Engineering solutions team update service request to request the customer to verifies/confirms the completion of the data transfer, and authorizes the factory reset of the Roving Edge device.

NOTE: Once customer approval is received, the Oracle Linux data transfer gateway instance will be terminated, all associated block devices will be deleted, and the Roving Edge device will undergo a factory reset.

- DC Ops team factory reset the Roving edge device and close the DO ticket.

Step 22. Factory reset the Roving Edge device. From the Roving Edge Device serial console, select **Reset Device**, **Factory Reset** options, then enter **no** when asked to **preserve objects in object storage**.

IMPORTANT: The Factory Reset option permanently deletes all VM instances, boot volumes, and block volumes on the device. Any system upgrades are rolled back, and all user data is erased, leaving only a single root user. All objects in the object storage, including VM images and audit logs, are removed. Once a Factory Reset is performed on the Roving Edge Device, any data stored on the device or within the Oracle Linux Data Transfer gateway instance becomes irrecoverable.

```
1) Unlock Device
2) Change Passphrase
3) Configure Networking
4) Show Status
5) Show System Diagnostics
6) Shutdown Device
7) Reboot Device
8) Enter Safe-Mode
9) Exit Safe-Mode
10) Shred Key
11) Recover Key
12) Reset Device
13) Advanced Menu
14) Cluster Health
15) Node Health
16) Diagnostics
17) Help
Enter command number: 12

    Reset Device
   -------------

1) Factory Reset
2) Service Reset
3) Network Reset
4) Help
Enter command number (or press Ctrl+C to go back): 1
Factory Reset
   -------------
Do you want to preserve objects in object storage? (yes/no): no
```

ORACLE

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Author: Anderson Souza