ORACLE

Deploying SD-WAN in Oracle Roving Edge Infrastructure and Compute Cloud@Customer

Step-by-step to deploy SD-WAN in Oracle Roving Edge Infrastructure and Compute Cloud@Customer

May, 2024, Version [1.0]

Purpose Statement

This document provides instructions on the deployment of SD-WAN on Roving Edge Infrastructure, focusing on its capability to interconnect Roving Edge Devices (REDs) for seamless information exchange. Through diverse testing scenarios, we aim to explain how SD-WAN facilitates the synchronization of multiple REDs in varied computing environments. Targeted towards decision-makers, network planners, and technology enthusiasts, this exploration provides valuable insights into leveraging SD-WAN for efficient interconnection of REDs within the Oracle ecosystem.

Disclaimer

Introduction

Software-Defined Wide Area Networking (SD-WAN) has emerged as a transformative technology, offering flexibility, scalability, and efficiency in networking architectures. This document explores the deployment of SD-WAN on Oracle Roving Edge Infrastructure and Compute Cloud@Customer, emphasizing its role in interconnecting Roving Edge Devices for enhanced information exchange.

Scope and Content

In this document, our primary focus revolves around addressing the fundamental requirement of interconnecting the Roving Edge Devices (REDs). We aim to provide comprehensive guidance on achieving seamless interconnection among multiple REDs, thereby facilitating efficient information exchange. Specifically, we will explore the utilization of SD-WAN (Software-Defined Wide Area Networking) deployed on the Roving Edge Infrastructure to fulfill this requirement. By investigating the capabilities of SD-WAN within the context of Roving Edge deployments, we aim to offer practical insights and strategies for establishing robust connectivity and synchronization among REDs. This document will delve into the benefits, challenges, and recommended approaches for leveraging SD-WAN to meet the critical need for interconnectedness within distributed computing environments.

Advantages of Roving Edge Infrastructure

Oracle Roving Edge Infrastructure represents a cutting-edge solution designed to extend cloud services and applications to the edge of the network. With its compact form factor and robust capabilities, it enables organizations to deploy compute, storage, and networking resources closer to where data is generated. This proximity enhances performance, reduces latency, and enables real-time processing of data at the edge. Moreover, Oracle Roving Edge Infrastructure plays a crucial role in facilitating the interconnectivity of Roving Edge Devices (REDs), allowing seamless communication and collaboration between edge devices within distributed environments. Its flexibility and agility make it an ideal solution for a wide range of use cases, including IoT deployments, content delivery, edge analytics, and more.

Advantages of Compute Cloud@Customer

Oracle Private Cloud Appliance is a rack-scale engineered system delivering Oracle Cloud Infrastructure compute, storage, and networking constructs on-premises. It enables rapid deployment of applications, middleware and workloads that are cloud-compatible via automation in an OCI-like environment while being disconnected from the public cloud. Private Cloud Appliance is the ideal platform alongside Oracle Exadata and Oracle Database Appliance platforms offering lowest latency and highest performance between the application and database layers. Private Cloud Appliance is designed for customers who want a cloud-like development and deployment experience while also meeting data residency requirements.

Overview of SD-WAN

SD-WAN, or Software-Defined Wide Area Networking, is a transformative technology that simplifies the management and operation of a wide area network (WAN) by separating the networking hardware from its control mechanism. Unlike traditional WANs, which rely on costly and complex proprietary hardware, SD-WAN utilizes software to dynamically route network traffic across the most efficient paths available. This approach enhances network agility, flexibility, and performance while reducing costs and complexity. SD-WAN enables organizations to optimize connectivity between different locations, prioritize critical applications, and seamlessly adapt to changing network conditions, making it an essential tool for modernizing network infrastructure, and supporting digital transformation initiatives.

What is the Roving Edge Device in more detail?

Roving Edge Device (RED) is the key component of Oracle Roving Edge Infrastructure.

- Each RED is optionally encased in a military-grade, ruggedized case that provides electromagnetic protection to limit emanations and interference.
- Each RED comes in a 2U form factor and weighs 33.6 lb.
- When ruggedized, a protective case is added, making the total weight 84 lb., with handles on both sides, which allow it to be carried by two people.
- Each RED contains 2x Intel Xeon CPUs Gold 6230T at 2.1 GHz.
- 40 total cores (32 usable).
- Memory: 512 GB (390 GB usable).
- Storage: 61 TB NVMe raw.
- Network interface: 2x 10 GbE (1 active).

Enabling Seamless Networking and Oracle Integration

SD-WAN acts as the backbone for seamless communication among Remote Edge Devices (REDs), employing centralized control and dynamic path selection to optimize performance and reliability. By centralizing management tasks, SD-WAN simplifies the configuration, monitoring, and troubleshooting processes.

Furthermore, its integration with Oracle Infrastructure enhances security and efficiency. Secure connectivity is ensured through robust encryption and access control measures. Intelligent traffic steering allows SD-WAN to efficiently direct traffic between various Oracle services and resources, ensuring that REDs can access the most relevant data sources and applications. Leveraging Oracle's network resources, SD-WAN optimizes routing between REDs, minimizing latency and maximizing throughput for an enhanced communication experience and seamless integration with Oracle services.

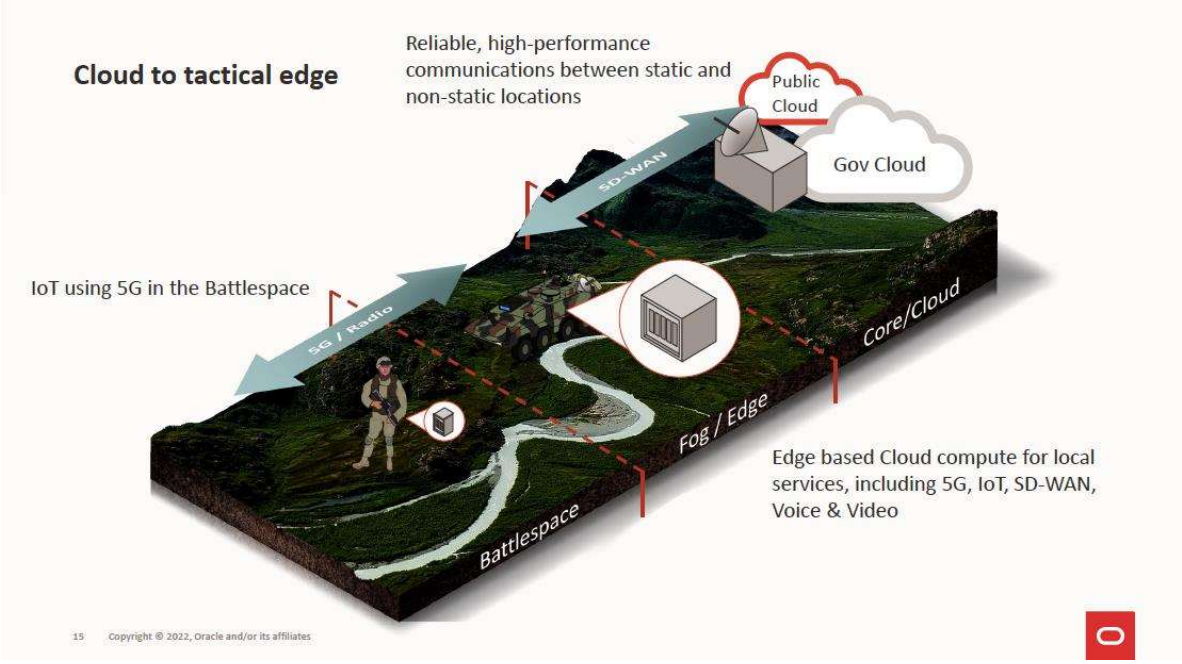
Interconnecting RED’s Using SD-WAN

Testing the interconnection of Roving Edge Devices (REDs) using SD-WAN within Oracle's Roving Edge Infrastructure marks an exciting exploration into cutting-edge networking. Through rigorous testing, we aim to understand how SD-WAN optimizes communication among REDs, unraveling insights for future-edge computing endeavors.

Empowering Tactical Communication: Exploring Use Cases of SD-WAN in RED Networks

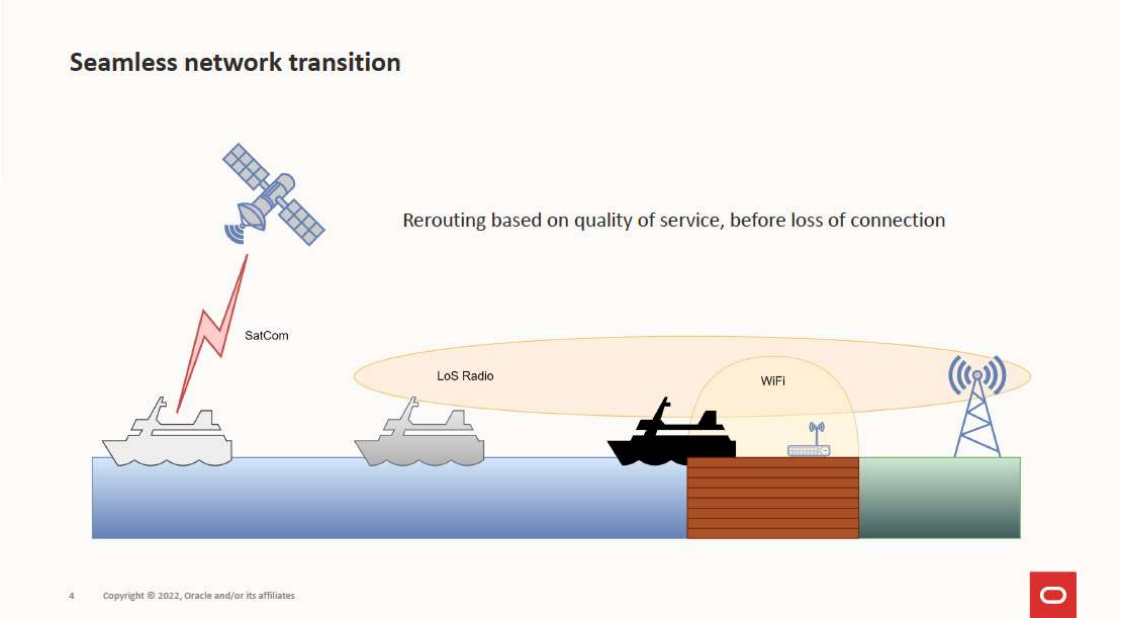
1. Cloud to Tactical Edge

The use case envisions a comprehensive network infrastructure spanning from the battlespace to the cloud, with a focus on optimizing communication and computing capabilities. It involves deploying 5G and SD-WAN technologies to ensure reliable, high-performance connectivity between static and non-static locations within military operations. At the edge of the network, fog computing facilitates local processing and services, including 5G connectivity, IoT applications, and voice/video communication. Both public and government cloud resources are leveraged, extending cloud services seamlessly from centralized data centers to tactical edge deployments, enabling real-time decision-making and mission-critical operations. This setup integrates IoT devices powered by 5G technology into the battlespace, enhancing situational awareness and operational effectiveness. Overall, the architecture prioritizes efficient data processing, low-latency communication, and scalability to support diverse military requirements across dynamic environments.



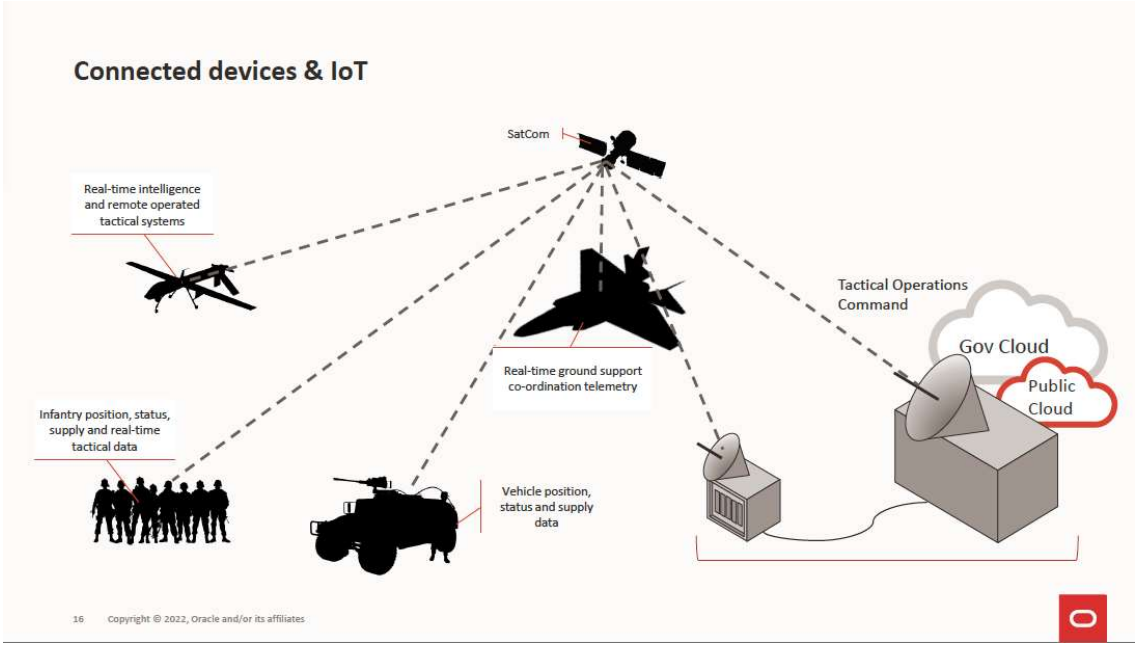
2. Seamless Network Transition

In this use case, seamless network transition is achieved through dynamic rerouting based on quality of service (QoS), ensuring uninterrupted connectivity. A boat connects to radar via Satellite Communication (SatCom), while another utilizes Line-of-Sight (LoS) radio and a third employs WiFi managed by Oracle SD-WAN. This diversified approach allows for flexible communication options, with each boat leveraging its respective network technology for specific needs. The rerouting mechanism ensures that traffic is automatically redirected to alternative paths with better QoS to maintain optimal performance and reliability. Overall, the scenario illustrates a robust network infrastructure that adapts to changing conditions, enabling continuous and efficient communication across different operational environments, such as maritime settings.



3. Connected Devices & IoT

This use case picture depicts a comprehensive network architecture integrating various elements to enhance military operations. At its core is a radar system linked to Satellite Communication (SatCom), serving as a central hub for data transmission. Connected devices and Internet of Things (IoT) technology are deployed across different assets, including airplanes, military groups with infantry positions, and vehicles, providing real-time intelligence and facilitating remote operation of tactical systems. These devices continuously transmit data regarding their position, status, and supply levels, enabling commanders to make informed decisions based on up-to-date tactical information. Additionally, two radar tactical operation commands are depicted, each utilizing both government and public cloud resources, suggesting a hybrid cloud approach for data storage and processing. This setup ensures scalability, resilience, and security in handling sensitive military data. Furthermore, real-time ground support coordination telemetry from an additional airplane underscores the emphasis on seamless communication and collaboration among various airborne assets. Overall, this use case highlights the integration of advanced technologies to enable efficient command and control, situational awareness, and coordination in military operations.



Pre-requisites:

Before you begin provisioning Oracle Roving Edge Infrastructure resources, ensure you have the following:

- Credentials for an Oracle Cloud Tenancy
- A compartment with permission to create and manage resources in it
- A computer, virtual machine, or an Oracle Linux 7/8 Instance in Oracle Roving Edge Infrastructure that has the following software and access to the internet:
  - A utility to generate API signing keys
    - (Most UNIX-like systems have openssl. You can also use Oracle Roving Edge Infrastructure to generate the API signing key and download the private key. Windows users can use git-bash.)
  - A utility to generate SSH key pairs (Most UNIX-like systems have ssh-keygen. Windows users can use PuTTYgen.)
  - A web browser
- Basic knowledge of Oracle SDWAN Edge configuration and deployment. Refer to Oracle SDWAN Implementation Guide

Generate an API Signing Key

To authenticate with Roving Edge Infrastructure, you must provide an RSA key in the privacy-enhanced mail format (PEM). Use OpenSSL to generate the key pair, and store it in a hidden subdirectory in your home folder:

- Create the hidden directory

```
mkdir ~/.rover
```

- Generate a private key (2048 bits or higher)

```
openssl genrsa -out ~/.rover/rover-api-key.pem 2048
```

- Change the permissions of the private key so that only you can read it.

```
chmod 600 ~/.rover/rover-api-key.pem
```

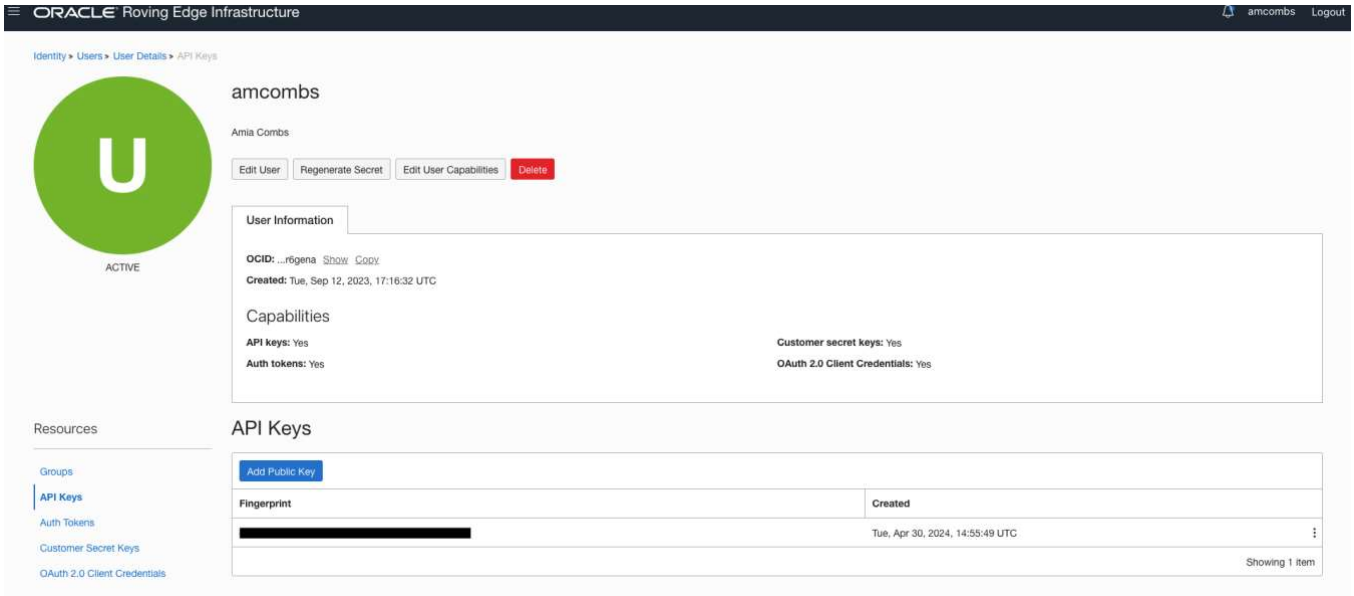
- Generate the public key for the private key

```
openssl rsa -pubout -in ~/.rover/rover-api-key.pem -out ~/.rover/rover-api-key-public.pem
```

Upload the API Signing Key

After you generate an API signing key, upload the public key for the appropriate user in Roving Edge:

- Sign in to the Roving Edge web console
- In the Roving Edge web console click the user avatar in the top right corner and under Profile click your user account name. You should now be on User Details page.
- On the user details page, click the **API Keys** link (bottom left of the page)
- Click **Add API Key**, an **Add API Key** options window will appear
- Select the **Paste Public Key** option
- Copy your public key value from the ~/.rover/rover-api-key-public.pem file and paste it in as the **PUBLIC KEY** file.
- Click the **Add** button



The key will upload, and its fingerprint will be displayed in the APIs Keys table

Note: *After the API signing public key is uploaded the API fingerprint will be displayed with additional information such as user's OCID, Tenancy OCID, and region you can copy this information to your notepad for later use.*

Generate an SSH Key Pair for the SD-WAN Edge Instance

SSH key pair will be used for secure access to the SD-WAN Edge instance. Generate the key pair on

your local host. The public key created will be uploaded as part of the Terraform code when the SD-

WAN Instance is created. Use the ssh-keygen utility and generate an SSH key pair. Do not use a passphrase for the key-pair.

```
# ssh-keygen -t rsa -N "" -b 2048 -C "rover-sdwan-key" -f ~/.ssh/rover-sdwan-key
```

- `-t rsa` : indicates that the key pair should be generated using the RSA algorithm
- `-N ""` : Passphrase, do not put anything between the quotation marks
- `-C "rover-sdwan-key"` : the name of the key, you can use your own key names, this name is stored in the keyfile, it is not the key file name.
- `-f ~/.ssh/rover-sdwan-key` : the directory and file name where the ssh keys will be saved. In this example we are using local user's hidden .ssh directory to store the keys. The public key will have a .pub extension.

Change the SSH private key permissions so that only you can access the private key in your .ssh

directory with the following command:

```
# chmod 600 ~/.ssh/rover-sdwan-key
```

The SSH key pair is generated and saved in the directory that you specified. Make a note of the path.

ORACLE

Creating an Instance in Roving Edge Infrastructure & Compute Cloud@Customer

Deploying SD-WAN on most applications allows for effortless instance launching from the Marketplace. However, with Roving Edge Infrastructure and Compute Cloud@Customer, **converting VT800 to UEFI boot is necessary**. To facilitate this process, follow the instructions below:

1. Starting with Custom Image:
    a. Begin by ensuring you have a custom image available for your system. It's crucial to have a custom image as marketplace images typically cannot be edited to support UEFI boot.
2. Convert Disk Partitioning:
    a. Switch to the root user using the command `` `sudo su -` `` to gain necessary permissions.
    b. Convert the disk partitioning from MBR (Master Boot Record) to GPT (GUID Partition Table), which is required for UEFI boot.
    c. Create space for the GPT BIOS by adjusting partition sizes. Unlike MBR, GPT requires space in two sectors at the beginning and end of the disk.
    d. Identify the existing first partition and ensure there's space prior to it for the first GPT sector.
        i. Note that the last GPT sector may overlap with the existing last partition unless resized.
    e. If needed, increase the size of the disk in the hypervisor. For instance, in Oracle Cloud Infrastructure (OCI), increase the boot volume size via the console and then reboot the instance.
    f. Rescan the disk to recognize the new size using the command: `` `echo "1" > /sys/class/block/sda/device` ``
    g. Ensure that packages such as gpt, grub2, and efi are up to date by following the appropriate update procedures for your system.
3. Configure Grub2 Boot Loader:
    a. Use the `` `gdisk` `` tool to manage GPT partitioning. Run `` `gdisk /dev/sda` `` to access disk management functionalities.
    b. Define the first GPT BIOS sector within `` `gdisk`. ``
    c. Adjust partition sizes as necessary to accommodate the new partitioning scheme
    d. Shrink the filesystem partition back to its original size to avoid data loss.
    e. Write the partitioning changes and reformat using `` `gdisk`. `` Confirm the changes by typing `` `w` `` and `` `y`. ``
    f. Refresh partition information using `` `partprobe` `` and verify changes using `` `fdisk -l /dev/sda`. ``
4. Create EFI Boot Partition:
    a. Create a new partition for the EFI boot system using `` `gdisk`. ``
    b. Reformat the newly created EFI partition as `` `vfat` `` using the command `` `mkfs -t vfat -v /dev/disk/by-partlabel/EFI-system` ``.
    c. Ensure necessary EFI files are present by installing grub2-efi, grub2-efi-modules, and shim packages.
    d. Generate the GRUB configuration file using `` `grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg`. ``

e. Mount the EFI system partition and move EFI files to it.

f. Update the `/etc/fstab` file to ensure the EFI partition is mounted at boot time.

5. Configure Grub2 for EFI:

   a. Install grub2 for EFI using the command `grub2-install --target=x86_64-efi /dev/sda`.

   b. Manually create a menu entry for Talari in `/boot/efi/EFI/redhat/grub.cfg`.

   c. Ensure proper configuration of the menu entry to reflect the changes made.

6. Reconfigure Hypervisor:

   a. If necessary, reconfigure the hypervisor to use UEFI boot mode for the VM.

   b. Start the VM and ensure it boots successfully using UEFI.

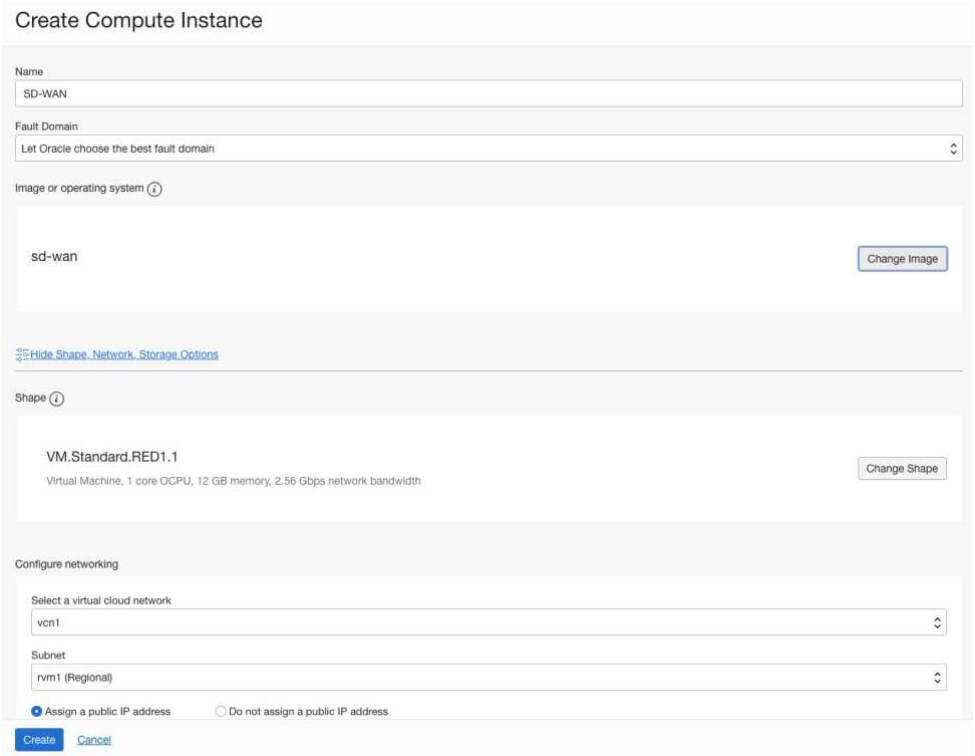
7. Troubleshooting:

   a. If any issues arise during the process, use the BIOS command line to locate partitions holding kernel and initrd images.

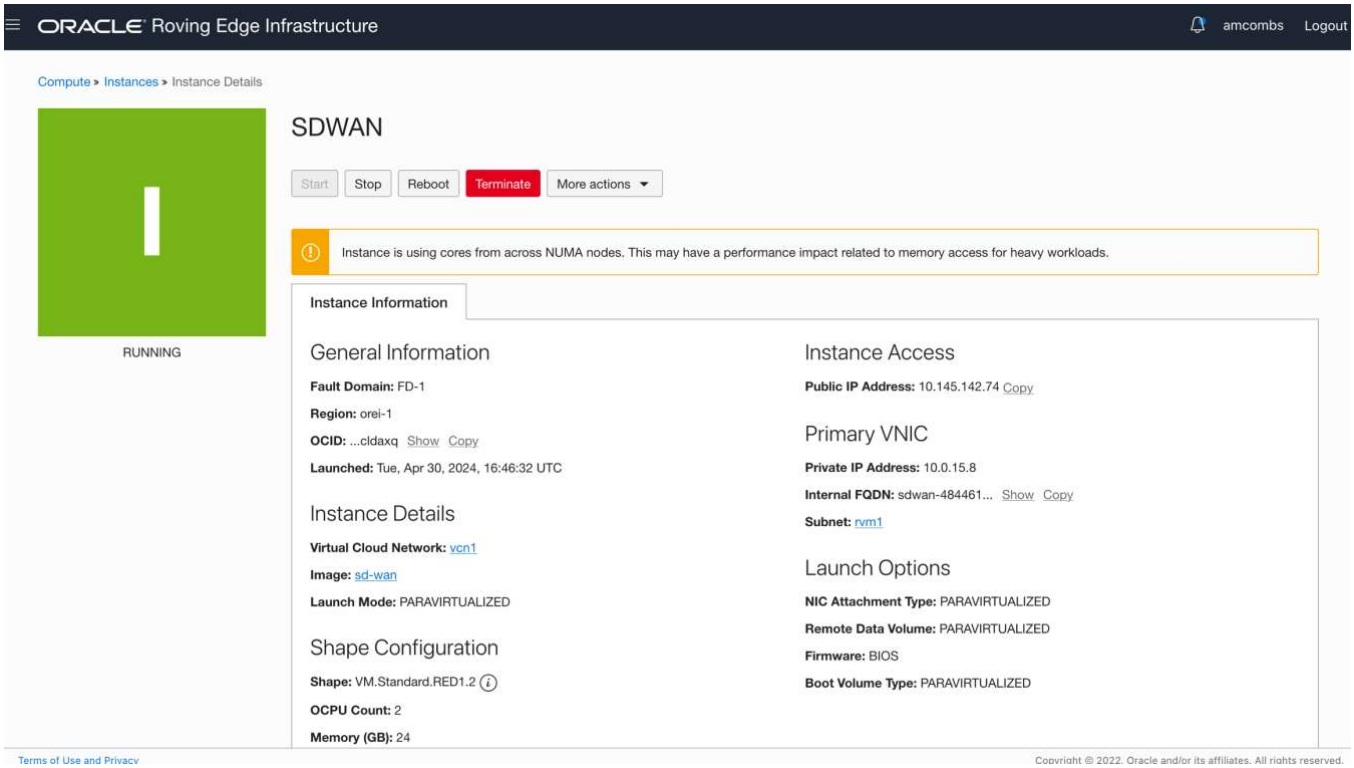
   b. Verify and adjust menu entries in the GRUB configuration file (`/boot/efi/EFI/redhat/grub.cfg`) to ensure they are configured correctly for UEFI boot.

By following these detailed steps, you can effectively convert VT800 to UEFI boot in place while ensuring a smooth transition and avoiding any potential issues. After completing the customization of the image, the image is now ready for export. Fully prepared to proceed with exporting this image to create an instance on Roving Edge for SD-WAN follow below:

- Login to Roving Edge web console
- Navigate to Instances and click **Create Instance**
- Fill out the **Create Compute Instance** form. Include instance name, select the custom image and other instance details (Shape, configure networking, ssh keys and so on) and click **Create**.



- Once you hit create your instance should now be up and running with your custom image



Verify SSH Access to SDWAN Instance and set a password for HTTPs access

After the successful creation of your instance, the subsequent imperative is to verify SSH access to your SDWAN Instance. Following this, it is paramount to establish heightened security measures by setting a password for HTTPS access. These steps are pivotal in fortifying your system's defenses, ensuring robust protection against unauthorized access and potential threats.

- The ssh commands are in the following format:

```
ssh -i <privateKeyPath> talariuser@<mgt-public-ip>
```

Next lets set a new password for talariuser

- Once you are logged in with SSH type in the following command:sudo passwd talariuser Note: *The password is used for HTTPs access only, you cannot use the password for SSH logins to the SDWAN Instance.*

```
================================================================

       Oracle SD-WAN Operating System 7.0.5.0.0 on VT800v1
       Host IP = 10.10.0.10

================================================================
talariuser@Talari-:~#
talariuser@Talari-:~#
talariuser@Talari-:~#
talariuser@Talari-:~#
talariuser@Talari-:~# sudo passwd talariuser
Changing password for user talariuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
talariuser@Talari-:~#
talariuser@Talari-:~#
```

- Once you have the password is set, exit the SD-WAN Instance CLI console.

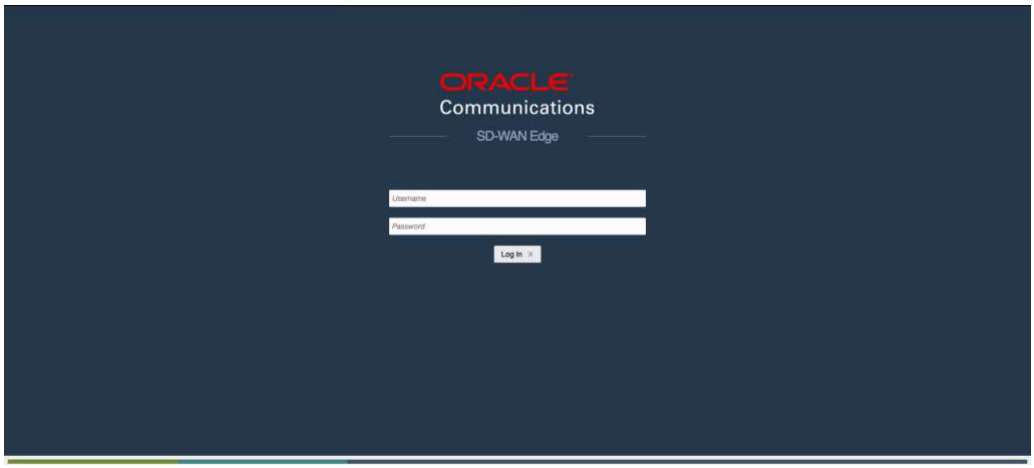
Access the SD-WAN Instance via HTTPS

- To access the SD-WAN host's web console you can tunnel HTTPS in SSH with the following command:

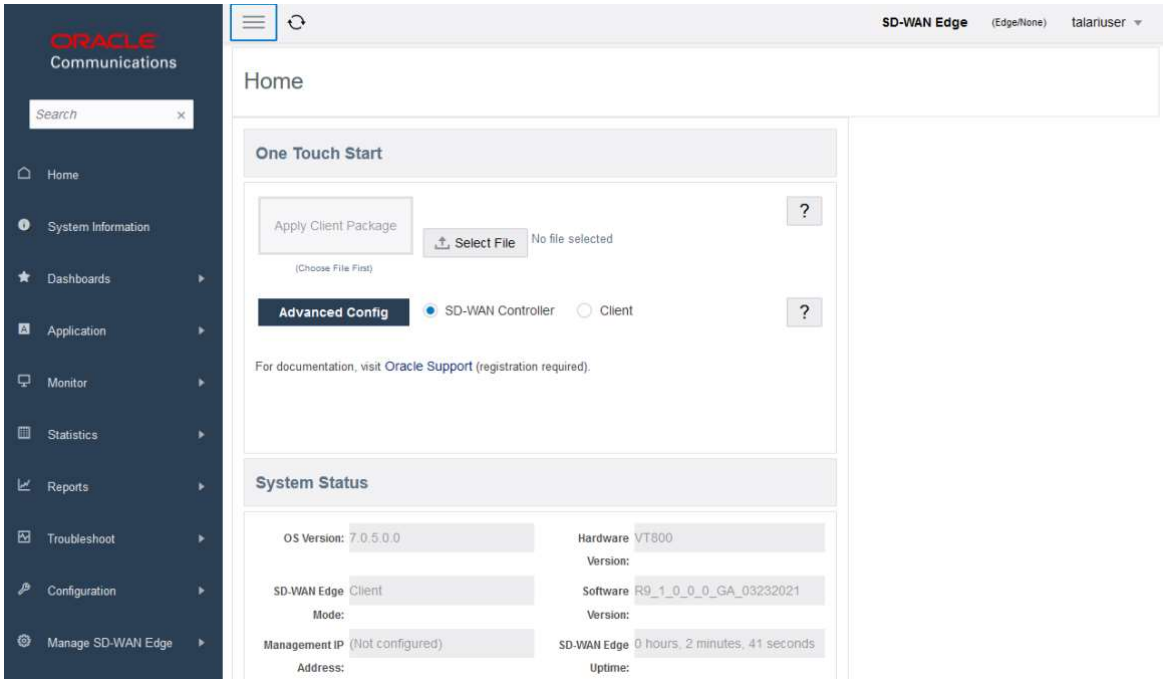
```
ssh -i <privateKeyPath> talariuser@<mgt-public-ip>
```

- Open your web browser and in address bar go to: https://<mgt-public-ip>
- Log in credentials:
  - Username: talariuser
  - Password: the password you created during the first SSH login

Oracle SD-WAN Web Console Login page:



When you login to the Oracle SDWAN Instance the One Touch Start will be your landing page. Here you can upload the software and configuration package for the SDWAN Instance. See the Oracle SDWAN Deployment Guide for details.

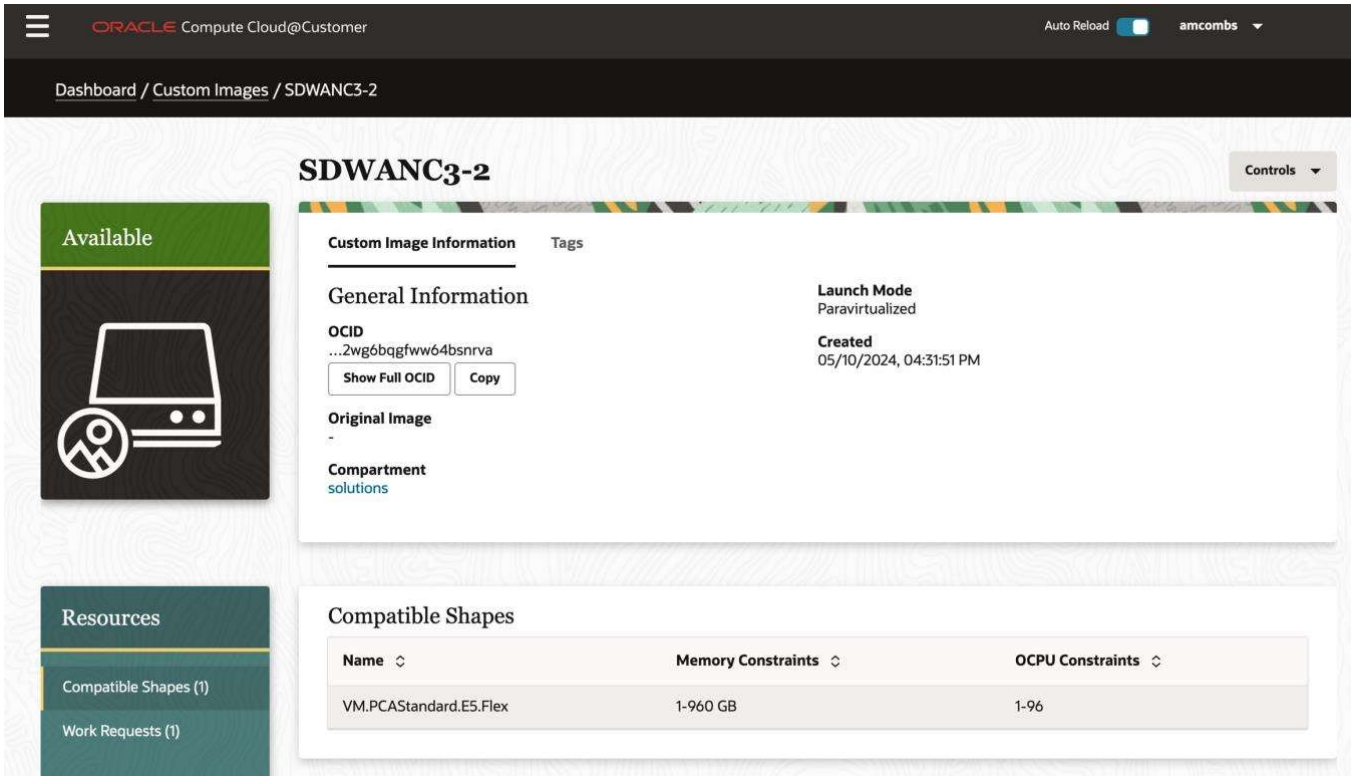


Congratulations! You have successfully deployed the Oracle SD-WAN Instance in Roving Edge Infrastructure. See the SDWAN deployment guide for instruction on configuration and deployment best practices, and installation of SDWAN software and configuration package at: Oracle® SD-WAN Implementation Guide

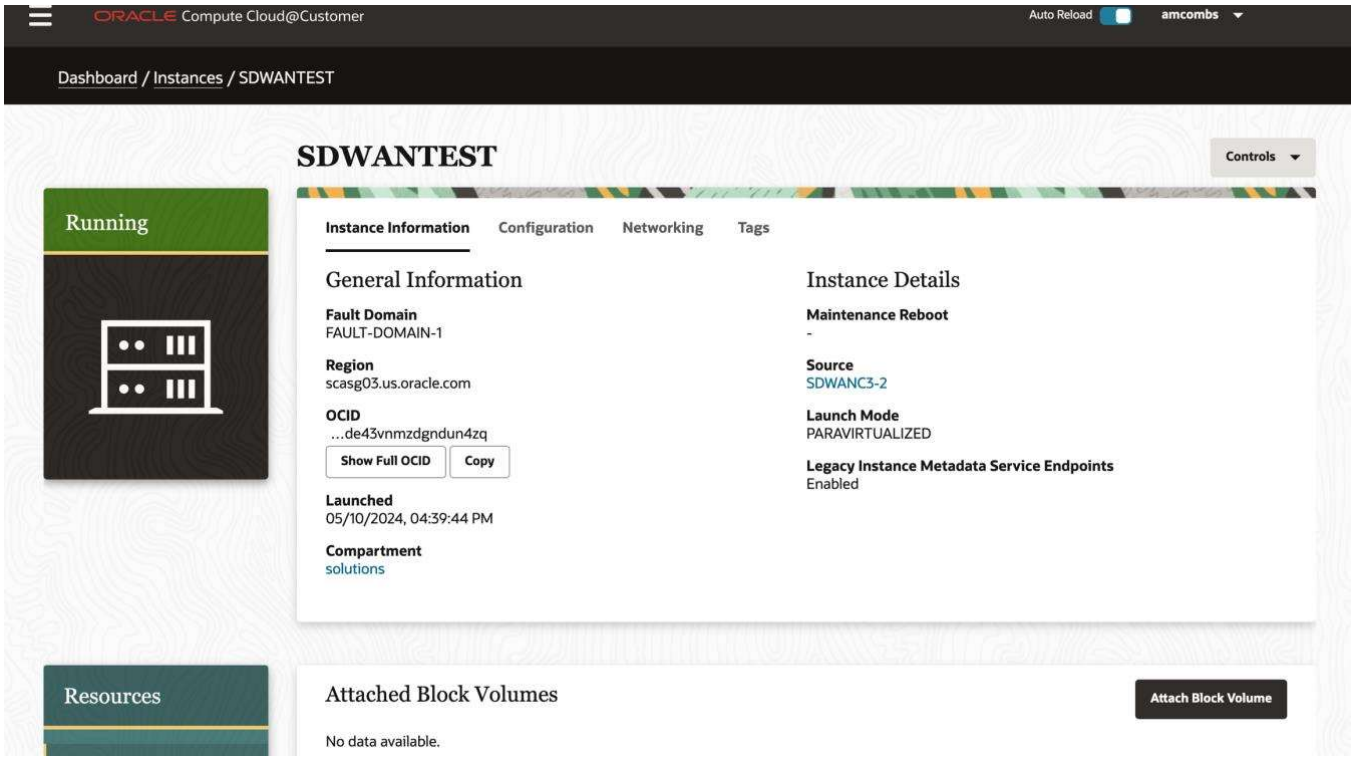
Deploying SD-WAN on Compute Cloud@Customer

When deploying SD-WAN on Compute Cloud@Customer, the process closely mirrors deploying it on Roving Edge infrastructure. Following the instructions outlined in the Pre-requisites section, you ensure that all necessary components are in place for a seamless deployment. Generating an API Signing Key and uploading it guarantees secure communication between components. Similarly, generating an SSH Key Pair for the SD-WAN Edge Instance enables secure access and management. Whether creating an instance in Roving Edge Infrastructure or Compute Cloud@Customer, the steps remain consistent, ensuring uniformity and ease of deployment. Additionally, converting VT800 to UEFI boot ensures compatibility and optimal performance across different infrastructures. After completing the customization of the image, the image is now ready for export. Fully prepared to proceed with exporting this image to create an instance on Compute Cloud@Customer for SD-WAN follow below:

- Login to Compute Cloud@Customer web console
- Navigate to Compute (View Images)
- Import your Custom image you created via VT800 UEFI boot



- Navigate to Instances and click **Create Instance**
- Fill out the **Create Compute Instance** form. Include instance name, select the custom image and other instance details (Shape, configure networking, ssh keys and so on) and click **Create**.



Verify SSH Access to SDWAN Instance and set a password for HTTPs access

After the successful creation of your instance, the subsequent imperative is to verify SSH access to your SDWAN Instance. Following this, it is paramount to establish heightened security measures by setting a password for HTTPS access. These steps are pivotal in fortifying your system's defenses, ensuring robust protection against unauthorized access and potential threats.

- The ssh commands are in the following format:

```
ssh -i <privateKeyPath> talariuser@<mgt-public-ip>
```

Next lets set a new password for talariuser

- Once you are logged in with SSH type in the following command:sudo passwd talariuser

Note: *The password is used for HTTPs access only, you cannot use the password for SSH logins to the SDWAN Instance.*

- Once you have the password is set, exit the SD-WAN Instance CLI console.

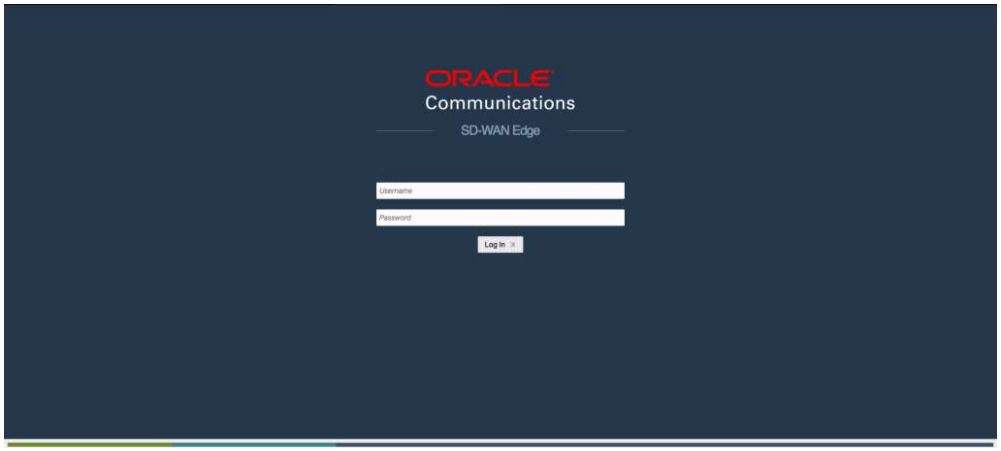
Access the SD-WAN Instance via HTTPS

- To access the SD-WAN host's web console you can tunnel HTTPS in SSH with the following command:

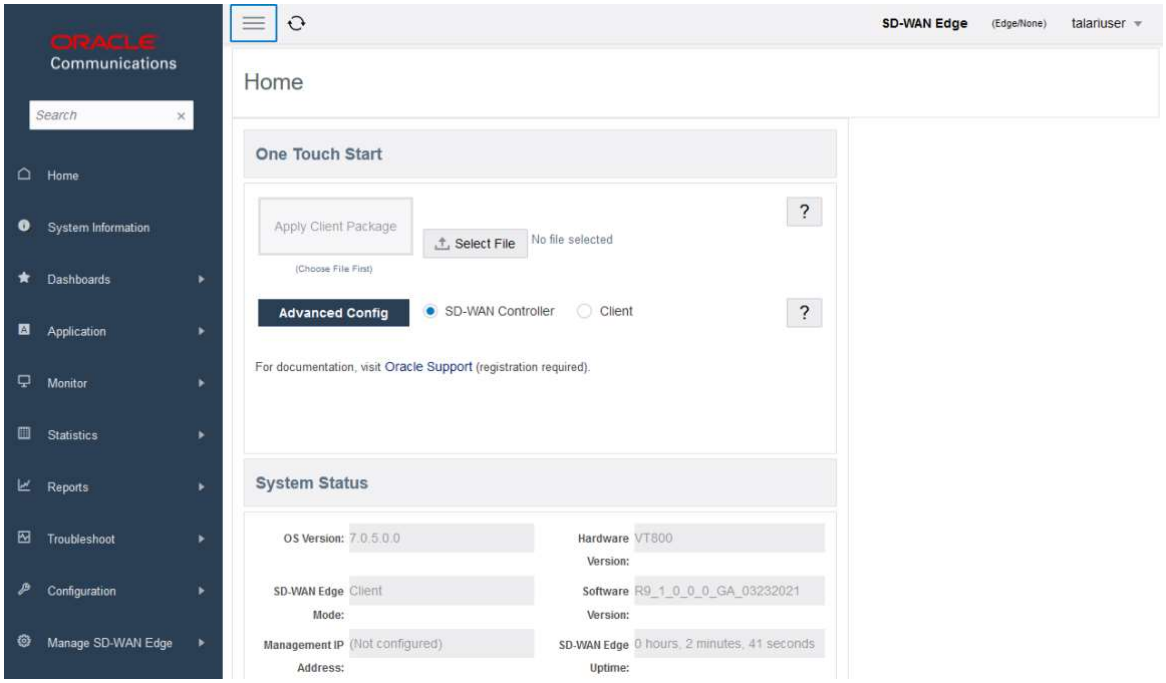
```
ssh -i <privateKeyPath> talariuser@<mgt-public-ip>
```

- Open your web browser and in address bar go to: https://<mgt-public-ip>
- Log in credentials:
  - Username: talariuser
  - Password: the password you created during the first SSH login

Oracle SD-WAN Web Console Login page:



When you login to the Oracle SDWAN Instance the One Touch Start will be your landing page. Here you can upload the software and configuration package for the SDWAN Instance. See the Oracle SDWAN Deployment Guide for details.



Congratulations! You have successfully deployed the Oracle SD-WAN Instance in Compute Cloud@Customer. See the SDWAN deployment guide for instruction on configuration and deployment best practices, and installation of SDWAN software and configuration package at: Oracle® SD-WAN Implementation Guide

Additional Resources:

- Oracle® SD-WAN Implementation Guide
- Oracle® SD-WAN Edge Virtual Appliance Installation Guide

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: Amia Combs