Persistent

SUREedge® DR 6.6.1

Installation Guide for AWS

Legal Notices

Warranty

The only warranties for products and services are set forth in the express license or service agreements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty of any kind, implied, statutory, or in any communication between them, including without limitation, the implied warranties of merchantability, non-infringement, title, and fitness for a particular purpose. Accelerite shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Accelerite or its licensors required for possession, use or copying. No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Accelerite.

Copyright Notices

Trademark Notices

Accelerite and Persistent are trademarks or trade name or service mark or logo of Accelerite/Persistent. All other brands or products are trademarks, trade name, service mark, logo or registered trademarks of their respective holders/owners thereof.

Disclaimer

The SUREedge products are available and support only the English language.

Tables of Contents

Introduction

Welcome to SUREedge DR! Data migration can be a lengthy and difficult, although a necessary, process. SUREedge®DR is a proven enterprise-class Disaster Recovery solution that simplifies DR Testing and DR, taking advantage of the Cloud as a ready-to-use DR infrastructure. SUREedge DR enables enterprises to implement a Disaster Recovery solution locally, at a remote site, in the Cloud, or even all three. Customers can start with local DR and seamlessly expand to a remote site or the Cloud — simply by deploying a SUREedge instance at the target site. With SUREedge-DR's **Any-to-Any** Recovery capability, you can recover physical and virtual systems (any hypervisor) to an alternate hypervisor or your preferred Cloud. This flexibility allows you to avoid hardware, hypervisor, and Cloud lock-ins.

Deployment Scenarios

SUREedge® DR supports many different deployment configurations to meet the needs of various situations:

- **Cloud-targeted DR**: The cloud is leveraged as a failover site for on-premise workloads or workloads in another cloud.
- **Site-to-site DR**: The source and target environments are non-cloud based.
- **Intra-cloud DR**: The goal is to protect against unavailability due to loss of resources in or connectivity to a region or zone within a public or private cloud.
- **Cloud-to-site DR**: Reverses the cloud-targeted scenario and uses a non-cloud, on-premise virtualization environment to protect cloud-based workloads.

In all these scenarios an instance of SUREedge DR is deployed in each of the source and target environments. The source SUREedge DR instance is responsible for capturing images of the protected systems and efficiently transferring them to the target instance. The target SUREedge DR instance receives and manages the system images and orchestrates the transformation and instantiation process when recoveries are performed.

Installation Overview

To set up an environment for Disaster Recovery you should first determine the location(s) where SUREedge DR should be installed according to the scenarios described above. You can then:

- Obtain the required documentation and software for the environment(s) you have identified. You should have an ***Install Guide*** (this document) for each environment and, if required, the software packages for installing SUREedge DR in those environment(s).
- Perform the installation of SUREedge DR software as instructed using the ***Installation Guide***.
- License and configure SUREedge DR as appropriate for each environment, as described in the ***Installation Guide*** and the ***User Guide***.

This Installation Guide covers the steps necessary for installing an instance of SUREedge DR in an AWS virtualization environment. The following sections will take you through the

steps to obtain installation materials and to install, license, and configure SUREedge DR to run in a Windows AWS environment. You can then use the ***User Guide*** to configure and start using SUREedge DR for Backup and Recovery.

Pre-requisites

The following sections outline some operations and settings that need to be done prior to installing SUREedge DR on AWS.

Getting AWS Parameters

During the deployment of SUREedge DR you will need to provide some AWS security credential information in order for the VMs to be installed in your account. Specifically, you will need:

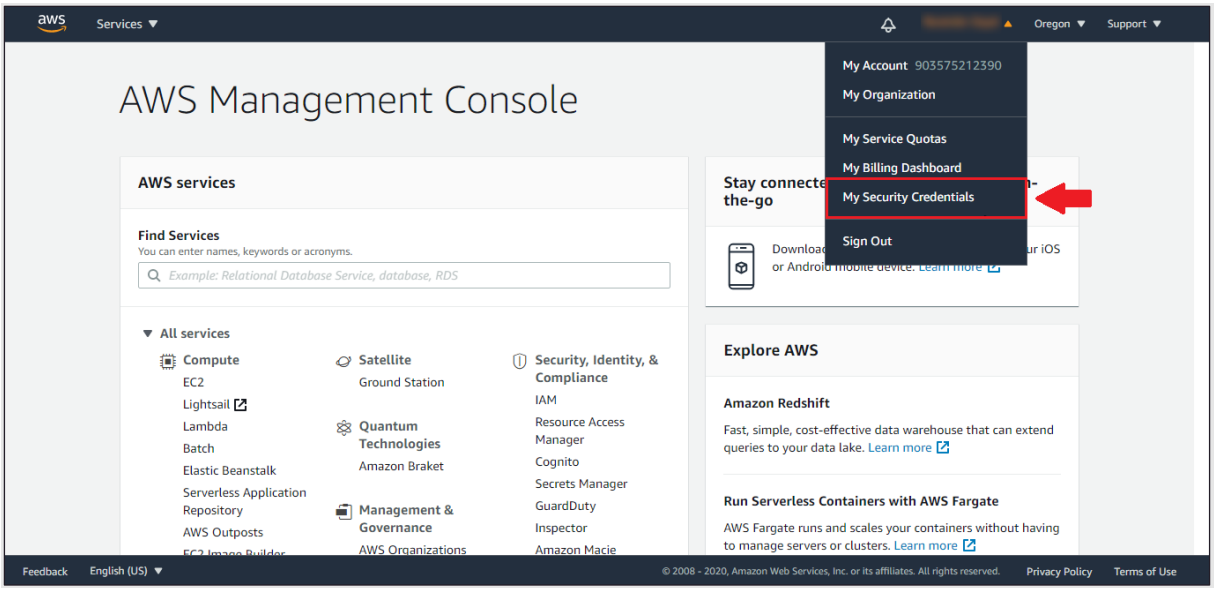
- ✓ an *Access Key* for your account; and
- ✓ that Access key's *Secret Key*.

You will use these keys when you enter your AWS account details while deploying your instance's Management Console.

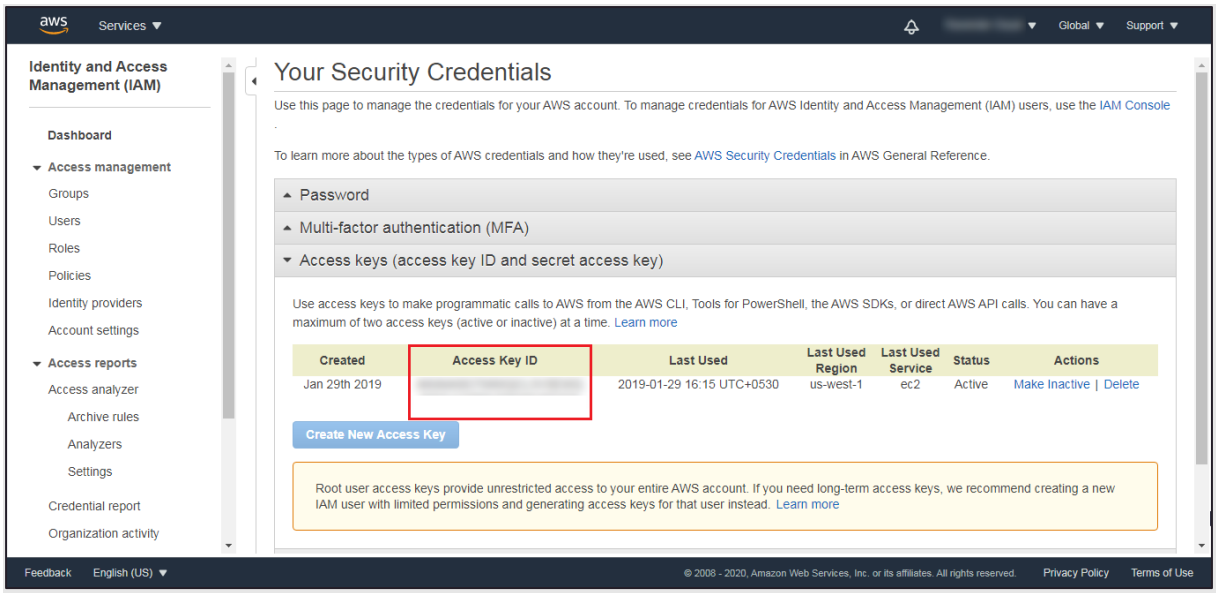
You can find your account's Access Keys on the AWS Management Console as described below. Secret Keys **cannot** be accessed via the console; they are **only** accessible when an access key is created (see https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html for details on Access Keys and their corresponding Secret Keys). If you cannot locate a Secret Key corresponding to an existing Access Key you will need to create a new Access Key (see below).

You can obtain this information using the following steps:

1. Log into the AWS Management Console.
2. Click on your **Username** at the top right of the page and select **My Security Credentials** link from the drop-down menu:



3. Click on the **Access Keys** dropdown section to see the existing Access Keys for your account:



4. To use an existing Access Key, copy the **Access Key ID** (as indicated above) and locate the corresponding Secret Key where you saved it when the Access Key was created.
5. If you don't have access to any Secret Keys that correspond to active the account's Access Keys you will need to create a new Access Key/Secret Key pair to use by your SUREedge DR instance. You can do this using the **Create New Access Key** button, though you may need to inactivate or delete existing access keys to enable it. Follow the on-screen instructions to create a new key pair, being sure to download and save the keys (including the Secret Key) when prompted to do so.
See https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html#Using_CreateAccessKey for details on managing and creating Access Keys and Secret Keys.

Configuring Firewall Rules

To capture and transform servers being recovered in AWS the SUREedge DR instance must be able to communicate with the VMs being created in the cloud. To allow this any firewalls between the SUREedge DR instance and the projects that will contain the recovered VMs must allow the following network communications:

- **ICMP**: Firewalls must allow ICMP packets to be passed between the SUREedge DR instance and the target projects and networks.
- **TCP**: Ports **22**, **25025**, **25026**, **25027**, and **25028** must be open between the SUREedge DR instance and the target project networks.
- **TCP**: Ports 80 and 443 are used to access the SUREedge DR UI and must be open between the SUREedge DR MC VM and any systems where a browser will be used to access the DR UI.

Obtaining SUREedge Software and Documentation

Obtaining SUREedge Installers

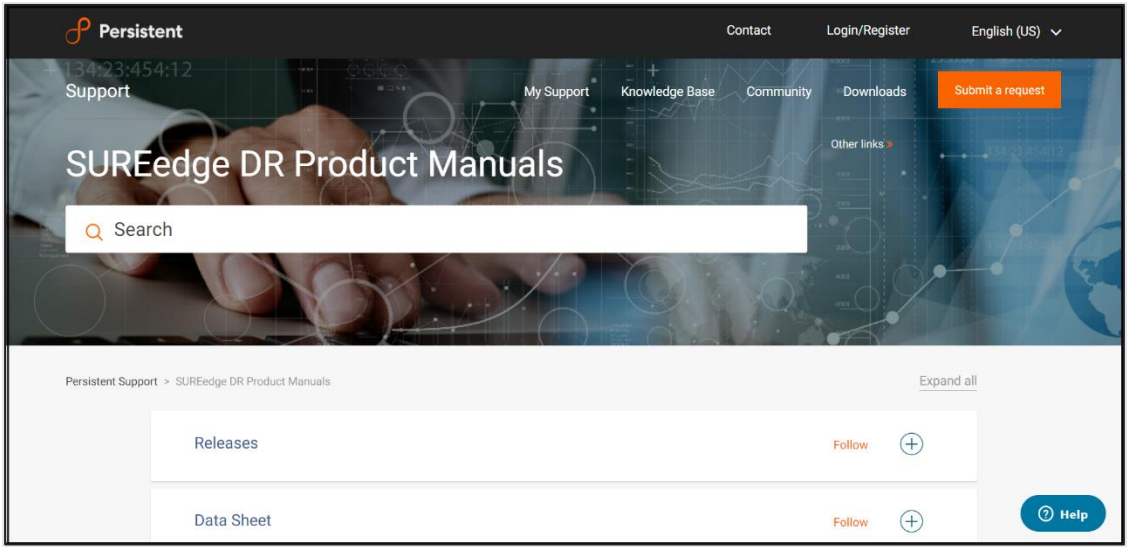
SUREedge DR installers, tools and documentation are all available online for download or deployment. The next sections details you to obtain the documentation and software binaries that you need to get started with SUREedge DR.

Obtaining Documentation

SUREedge DR documentation is available for download as PDF files from the Accelerite portal. To get access to SUREedge DR documentation, navigate to this URL in your browser:

https://support.accelerite.com/hc/en-us/categories/4410194460941-SUREedge-DR-Product-Manuals

You will need an account to log in and access the SUREedge DR documentation. If you are a new user, please click on **Login/Register** and submit a registration request. After the request is approved, you can access the documents:



In the **Releases** section, select the software version for which you want documentation, then find the desired document and click the **PDF** button to download it.

Installing SUREedge DR

Once you have obtained your installation media and documentation you are ready to deploy your SUREedge DR instance in AWS.

A SUREedge DR instance consists of two VMs: a Linux based *Store* VM which stores and manages the images of systems being protected, and a Windows-based *Management Console* (MC) which is responsible for orchestrating all DR operations and presents the SUREedge DR user interface. The following sections will detail the steps to deploy VMs in your AWS account and install the SUREedge DR software components on them to create your DR instance in AWS.

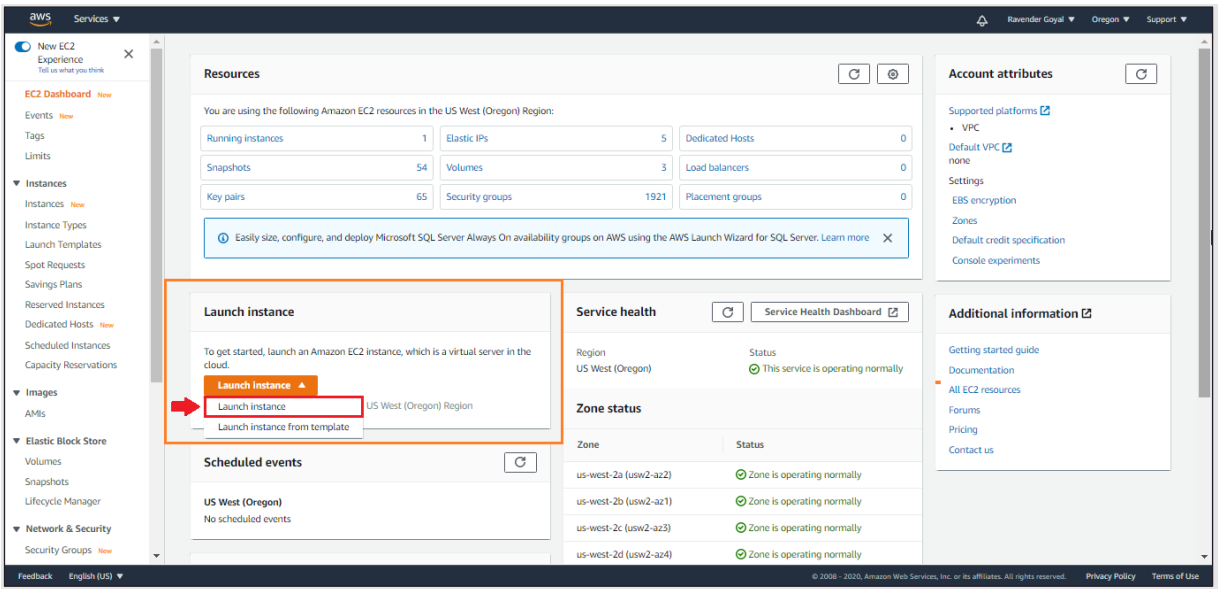
Deploying the SUREedge Store

Creating your SUREedge DR Store is done by deploying a linux-based VM in your Amazon EC2 environment and installing the SUREedge DR Store software components on it.

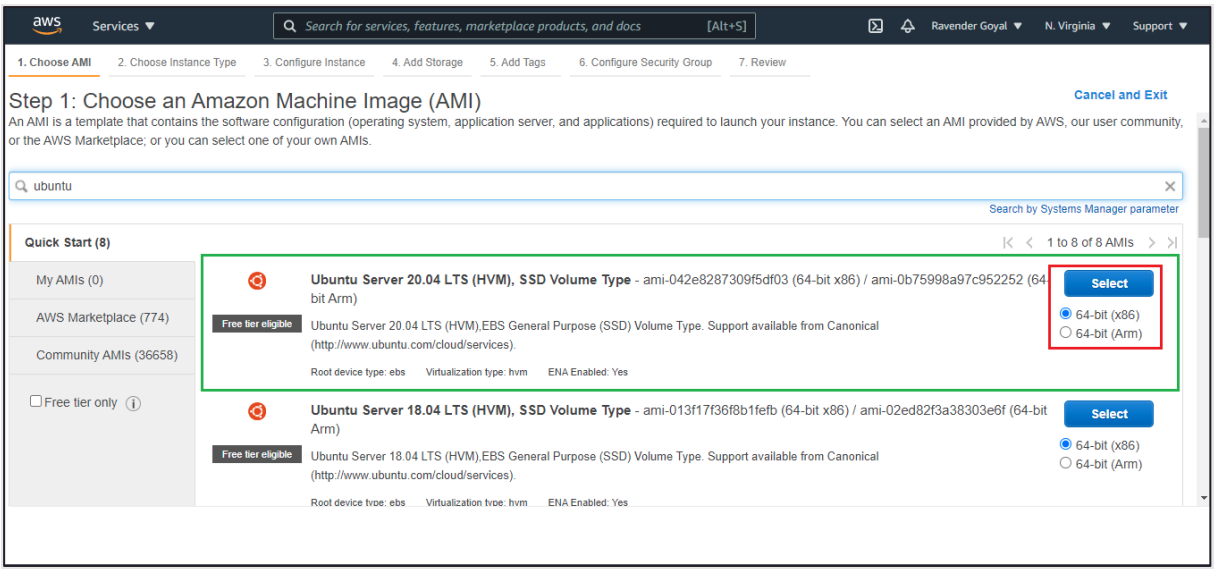
Launch a Linux Instance

First launch an Ubuntu Linux instance using the AWS Management Console as described in the following steps:

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the dashboard console choose **Launch Instance** dropdown and select **Launch Instance** from the dropdown:

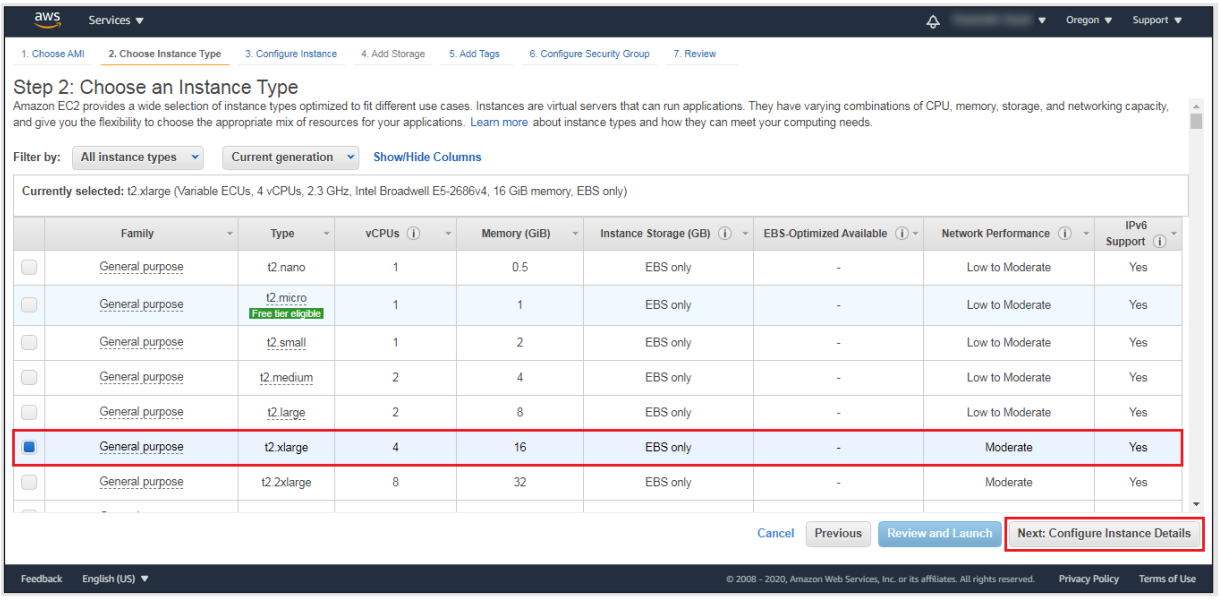


3. You will be presented with the **Choose an Amazon Machine Image (AMI)** page:

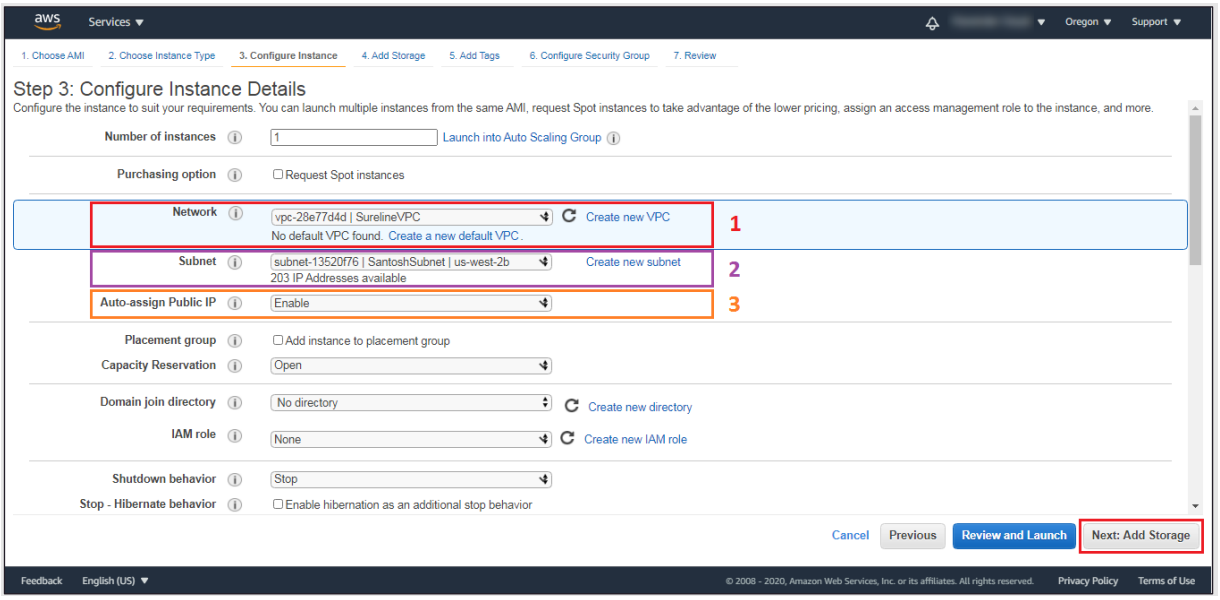


Search for an AMI by entering the term **Ubuntu Server 20.04 LTS (HVM), SSD Volume Type** in the search bar. Select *64-bit x86* for the architecture (below the Select button as shown above) then click the **Select** button.

4. On the **Choose an Instance Type** page select the instance type *t2.xlarge* (with 4 vCPUs and 16 GiB Memory). Click **Next: Configure Instance Details**.



This takes you to the **Configure Instance** Details page:

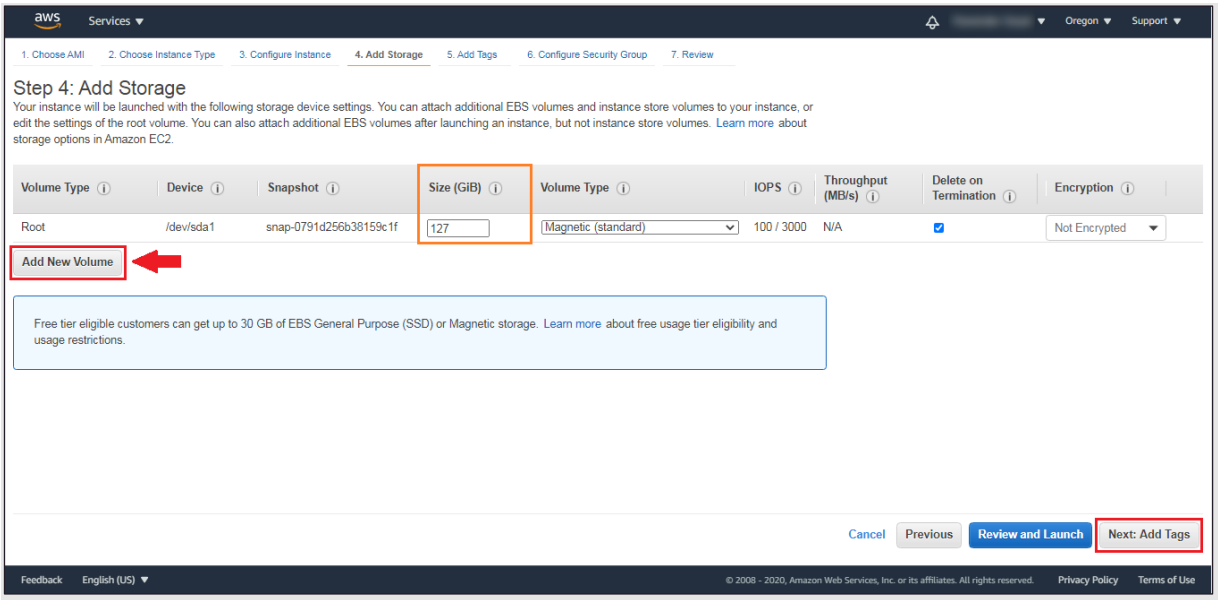


Make the following selections:

a. Use the **Network** and **Subnet** pull down lists (**1** and **2** above) to select the network where the SUREedge Store should be deployed. (This should be a network that has connectivity to all networks where systems may be recovered; see section "Configuring Firewall Rules" for more details.)
b. Select *Enable* for **Auto Assign Public IP** (item **3** in the screenshot above).

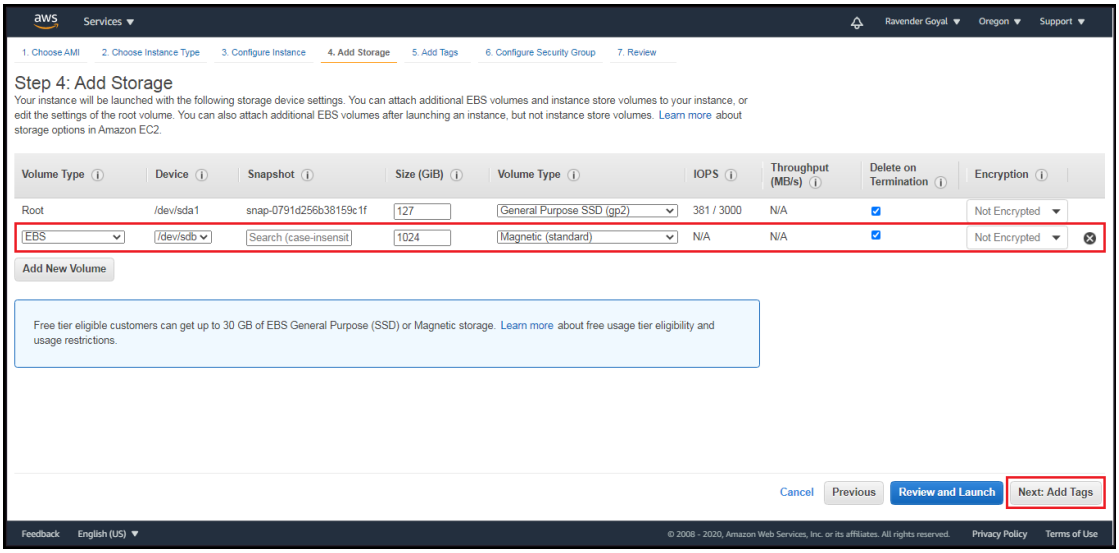
In the remaining fields keep the default values. Click **Next: Add Storage.**

5. You'll next see the **Add Storage** page:



Here you need to:

a. Change the size of the **Root** volume to 127 GB and set the **Volume Type** to *Magnetic (Standard)*.
b. Click **Add New Volume** to attach a virtual disk for storage of the captured images, which will add a new line to the volume list:

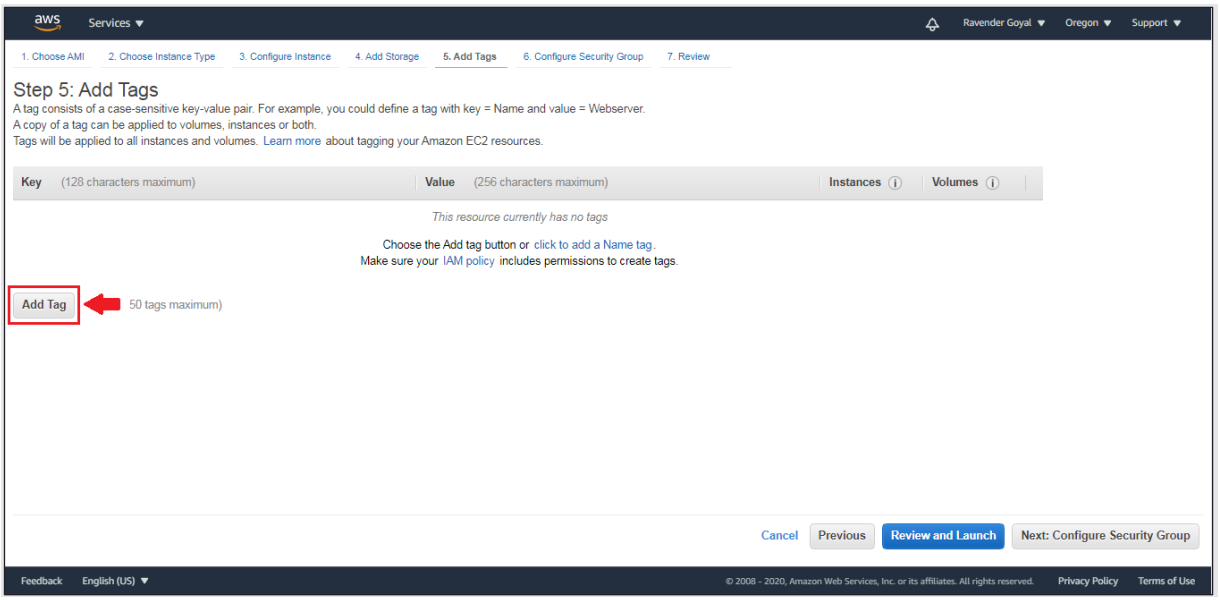


Make the following changes to the default values for the new volume:

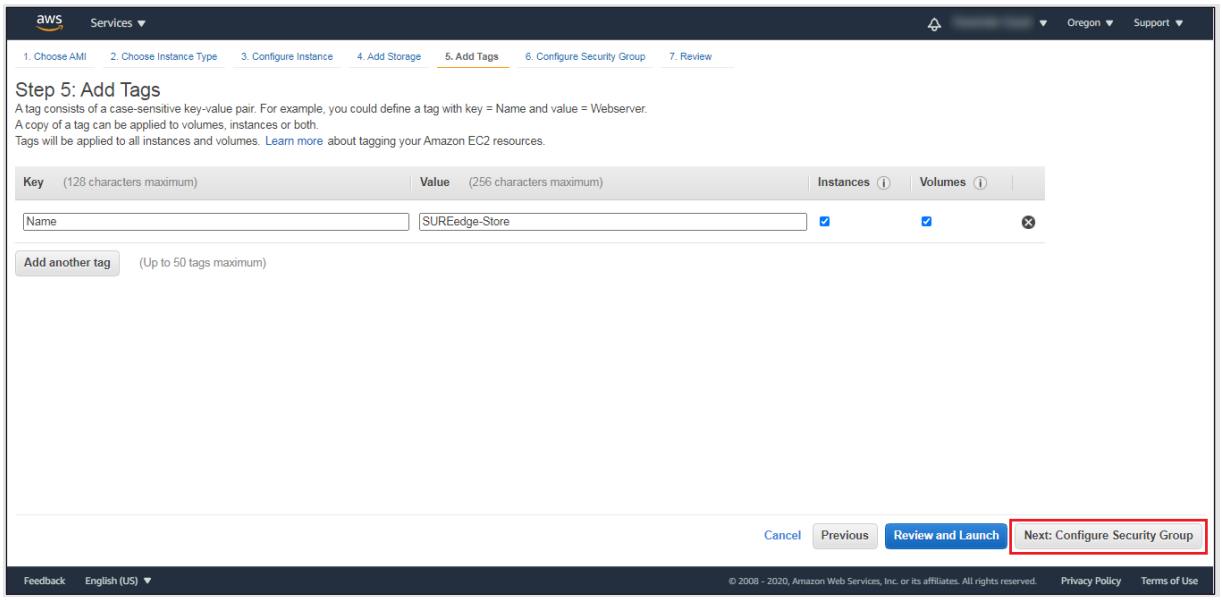
- The recommended initial size for the Store data disk is at least 1024 GB, which is sufficient for most of the disaster recovery projects; see the section, "Appendix" for guidelines on choosing an initial Store device size.
- Select the **Delete on Termination** option.
- Be sure the **Device** name is set to */dev/sdb*.
- Set the **Volume Type** to *Magnetic (Standard)*.

When the attributes have all been set click **Next: Add Tags.**

6. Here you can add any tags to the VM that are desired. (No tags are required for deploying the SUREedge DR instance, but you may wish to add tags to, for example, aid in identifying the VMs that make up the instance.)
   To add a tag (optional), click on **Add Tag** button as shown:
   Once you click on the **Add Tag** button



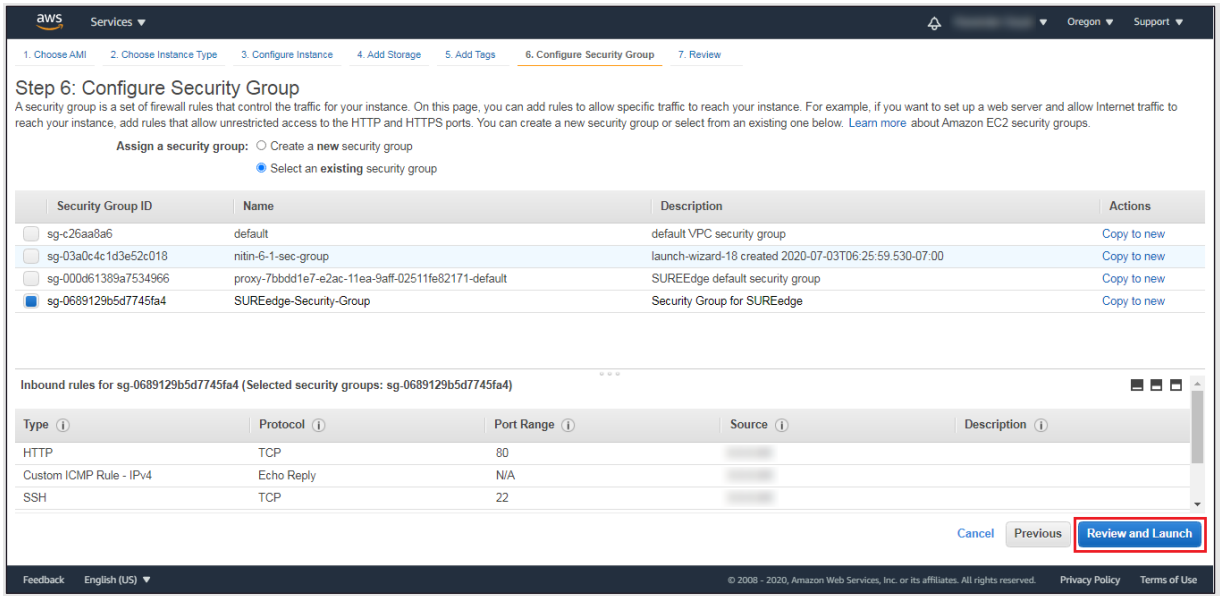
the **Add Tags** page is displayed:



Here you can enter the **Key** and **Value** for the tag. For example, you could define a tag with **Key** = *Name* and **Value** = *SUREedge-Store*.

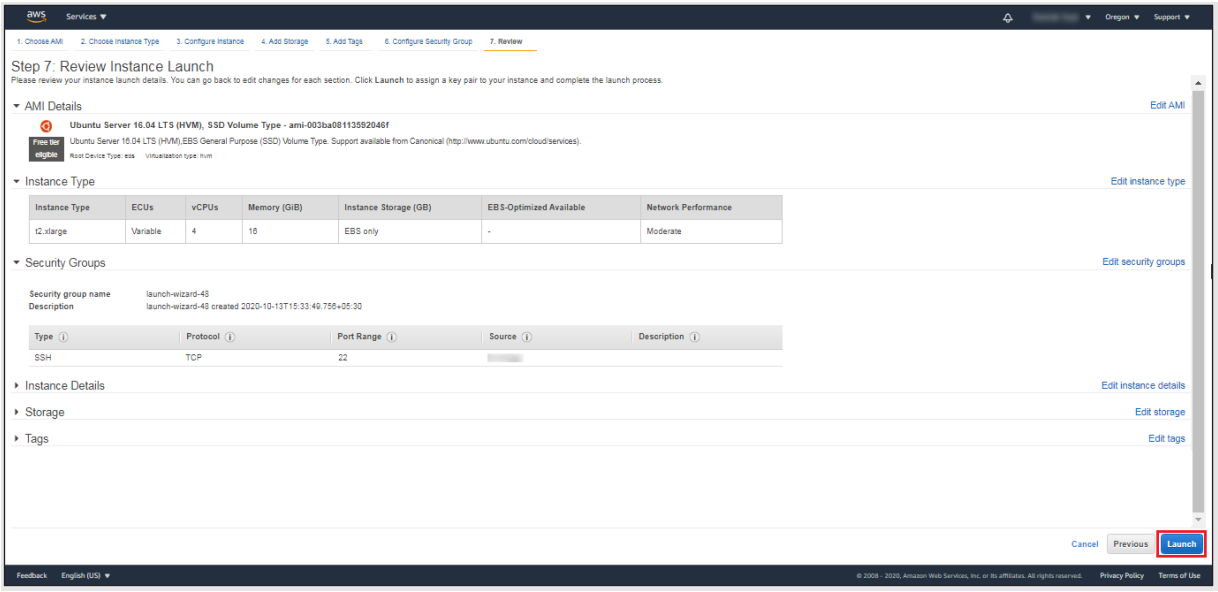
When you have added all the tags you wish to add click **Next: Configure Security Group.**

7. In the **Configure Security Group** page you should choose a group that has the required firewall rules as indicated in Section "Configuring Firewall Rules":-



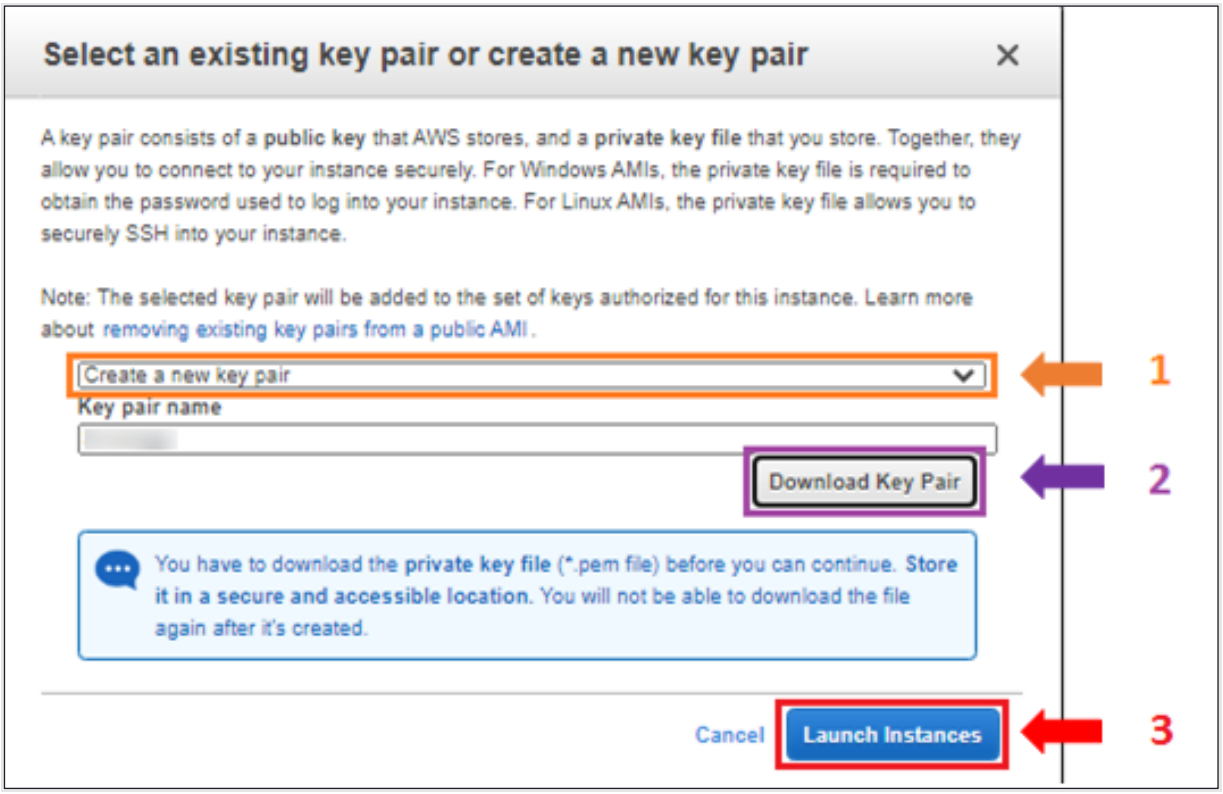
When the security group settings are completed click **Review and Launch.**

8. Review the specifications on the review page to make sure you are satisfied with all of your choices:



When you are ready to deploy the VM click **Launch**.

9. You will see a dialog box regarding the use of a key pair for accessing the VM:



From the dropdown (**1** above) you can choose to either **Create a new key pair** for use by SUREedge DR (recommended) or **Choose an existing key** pair if you have one already created that you wish to use. If creating a new key pair, provide a new **Key pair name** and then click **Download Key Pair** (**2** above). ***You should securely store the newly created Key Pair as it is required in order to access the deployed VM via SSH for OS configuration later in the deployment process.***

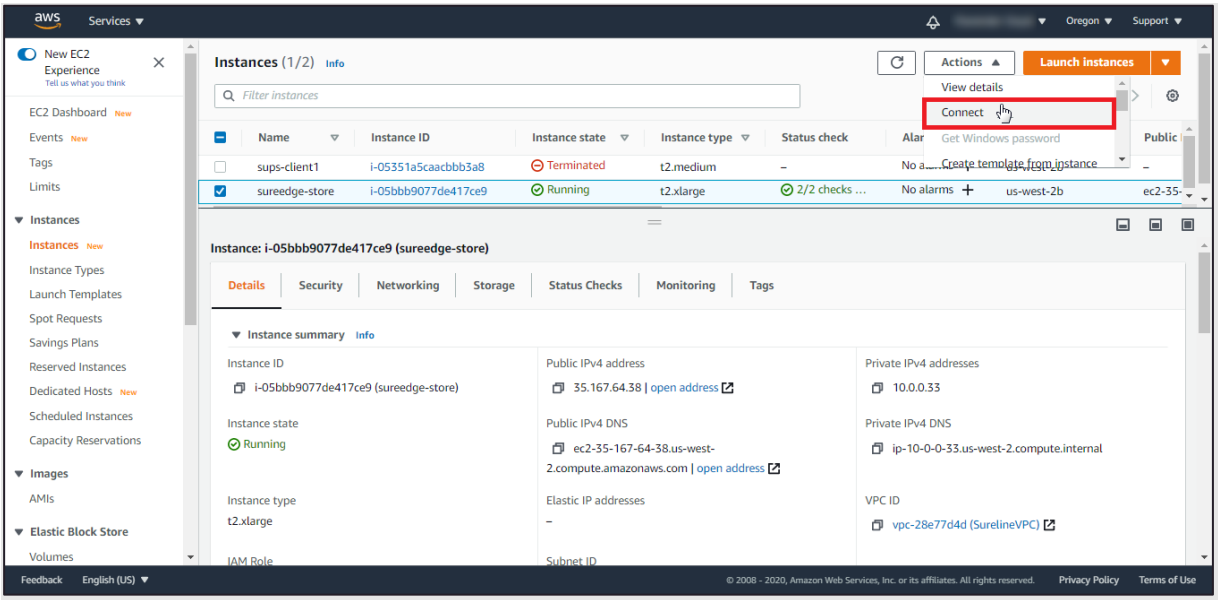
10. Click **Launch Instances** (**3**).

This will launch the Ubuntu Linux VM in your AWS account. Next you will need to configure the newly deployed OS so that it can be used as a SUREedge DR Store.

Connecting to the Store VM

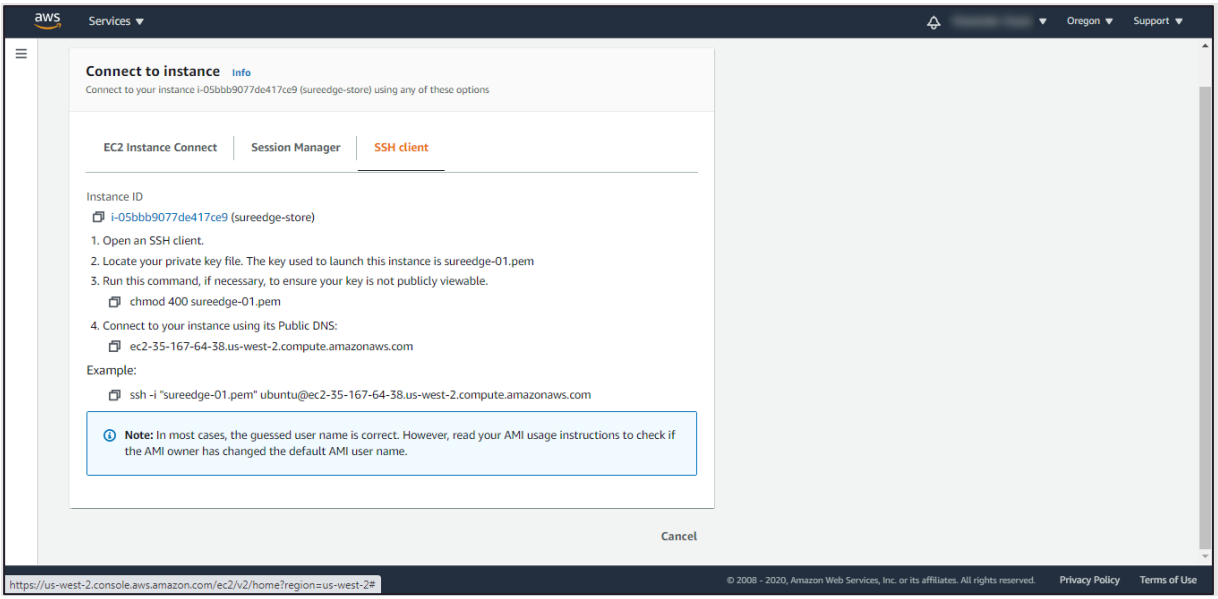
Once the newly deployed Linux VM is in the Running state, you can proceed with the OS level configuration which is required before installing the SUREedge DR software.

1. From the AWS console navigate to the **Instances** section and select the newly deployed instance, then select **Connect** from the **Actions** drop down.



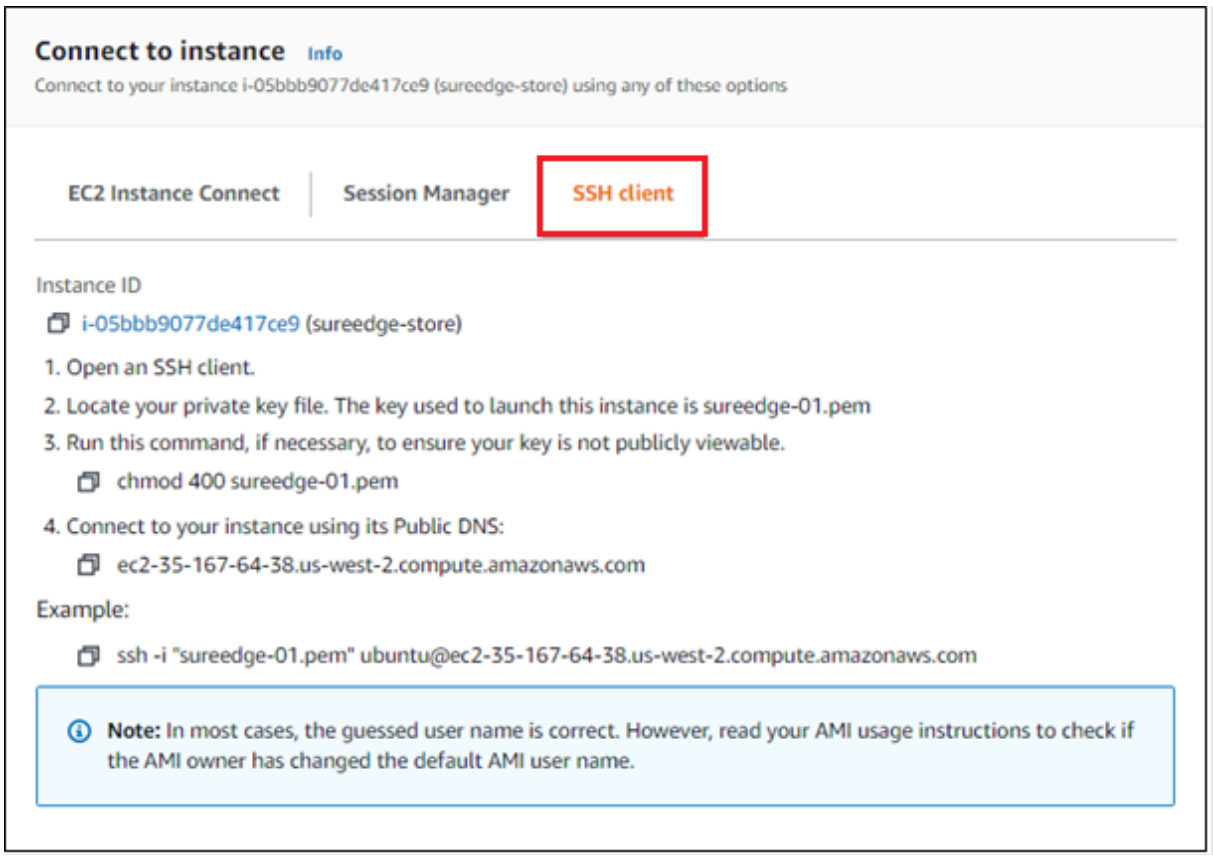
Note: Please note down the **Private Ip Address**, as will be required for connecting to your instance.

Once clicked on **Connect**, the **Connect to Instance** screen will be displayed:



In the **Connect to Instance** dialog box you can choose any one of the three options provided to connect to the Linux instance. Any connection method will work to configure and

Here we are showing how to connect Linux instance using SSH option, click on SSH tab in the Connect to Instance dialog box:



Follow the instructions to connect to the Linux instance. When instructed to use your private key file you should use the one you saved in Step 9 while launching the Linux instance (above).

Configuring the Store VM OS

To configure the deployed Store VM connect to it via SSH (as described in Section "**Connecting to the Store VM**", then follow the instructions below:

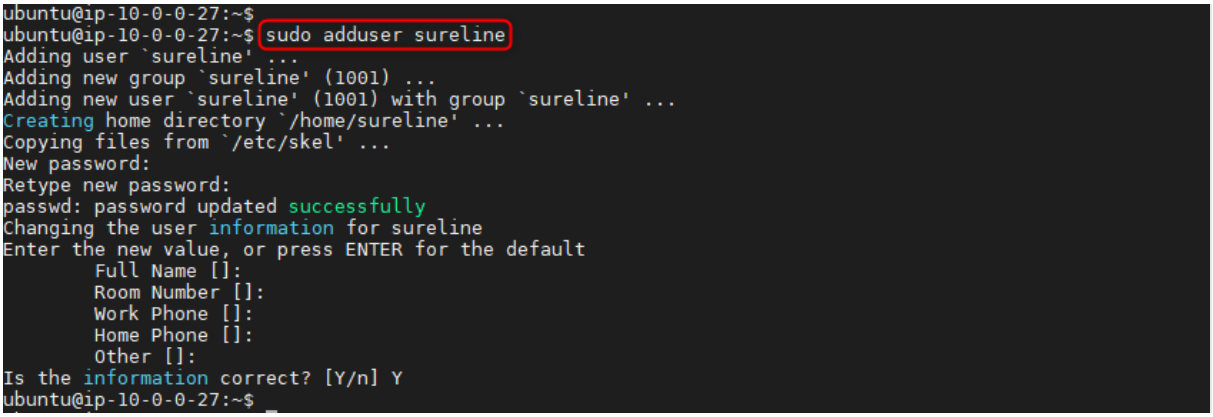
1. At the command line on the VM create a new user called **sureline** using the following command:

   ```
   sudo adduser sureline
   ```

   At the resulting prompt enter a password and confirm it. **You must provide this password later while configuring the SUREedge DR MC system, so be sure to note it down.**

   The system will also prompt you to enter additional information about the user. This includes a name, phone numbers, etc. – these fields are optional, and can be skipped by pressing Enter.

   Note: For the current release you should avoid passwords with these special characters: commas (","), spaces (" "), and equal signs ("=").



2. Next you need to add the **sureline** user to the `sudoers` file and set some options. Edit the `/etc/sudoers` file using below command:

   ```
   sudo visudo
   ```

   Append following text to end of file:

   ```
   sureline ALL=NOPASSWD: ALL
   Defaults:sureline !requiretty
   ```

   Save and exit the file.

3. Next you need to enable the Password Authentication option for the SSH service. To do this set the `PasswordAuthentication` line in the file `/etc/ssh/sshd_config` to `yes`. To edit the file, you can use the command:

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   Then find the line where `PasswordAuthentication` is set. If it is set to `no`, like this:

   ```
   PasswordAuthentication no
   ```

   Change it to `yes`, resulting in this:

   ```
   PasswordAuthentication yes
   ```

```
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin prohibit-password
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile     %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
PasswordAuthentication yes


# Kerberos options
:wq
```

Save the file and exit.

4. Once the SSH service has been reconfigured it needs to be restarted. To do this run the following command:

   ```
   sudo service ssh restart
   ```

5. To check the SSH status run the following command:

   ```
   sudo service ssh status
   ```

```
sureline@ip-10-0-0-27:~$
sureline@ip-10-0-0-27:~$ sudo service ssh restart
sureline@ip-10-0-0-27:~$
sureline@ip-10-0-0-27:~$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
    Drop-In: /usr/lib/systemd/system/ssh.service.d
             └─ec2-instance-connect.conf
     Active: active (running) since Wed 2021-05-12 16:43:22 UTC; 4s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 95472 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 95487 (sshd)
      Tasks: 1 (limit: 4706)
     Memory: 1.3M
     CGroup: /system.slice/ssh.service
             └─95487 sshd: /usr/sbin/sshd -D -o AuthorizedKeysCommand /usr/share/ec2-instance-connect/ei>

May 12 16:43:22 ip-10-0-0-27 systemd[1]: Starting OpenBSD Secure Shell server...
May 12 16:43:22 ip-10-0-0-27 sshd[95487]: Server listening on 0.0.0.0 port 22.
May 12 16:43:22 ip-10-0-0-27 systemd[1]: Started OpenBSD Secure Shell server.
May 12 16:43:22 ip-10-0-0-27 sshd[95487]: Server listening on :: port 22.
sureline@ip-10-0-0-27:~$
```

6. Run the following command at store:

   ```
   touch /etc/rc.local
   ```

Downloading Software Components

You now need to download the SUREedge Linux Aws Package to the Linux VM instance. Connect to the SUREedge store instance using SSH (see Section **Connecting to the Store VM**), logging in as the user sureline (created above). Then run following commands:

```
cd /home/sureline
wget -O ./SUREedgeLinuxAWSPackage.tar.gz https://sure-builds.s3-us-west-1.amazonaws.com/dr/661/GA/SUREedgeLinuxAzurePackage.tar.gz
```

```
sureline@ip-172-31-31-28:~$ cd /home/sureline/
sureline@ip-172-31-31-28:~$ wget -O ./SUREedgeLinuxAWSPackage.tar.gz https://sure-builds.s3-us-west-1.amazonaws.com/dr/661/GA/SUREedgeLinuxAzurePackage.tar.gz
--2021-08-10 07:54:29--  https://sure-builds.s3-us-west-1.amazonaws.com/dr/661/GA/SUREedgeLinuxAzurePackage.tar.gz
Resolving sure-builds.s3-us-west-1.amazonaws.com (sure-builds.s3-us-west-1.amazonaws.com)... 52.219.116.225
Connecting to sure-builds.s3-us-west-1.amazonaws.com (sure-builds.s3-us-west-1.amazonaws.com)|52.219.116.225|:443...
 connected.
HTTP request sent, awaiting response... 200 OK
Length: 330346356 (315M) [application/x-tar]
Saving to: './SUREedgeLinuxAWSPackage.tar.gz'

./SUREedgeLinuxAWSPackage.ta 100%[=============================================>] 315.04M  12.1MB/s    in 34s

2021-08-10 07:55:04 (9.19 MB/s) - './SUREedgeLinuxAWSPackage.tar.gz' saved [330346356/330346356]

sureline@ip-172-31-31-28:~$
```

Installing Software Components

1. Connect to the SUREedge store instance using SSH (see Section **Connecting to the Store VM**), logging in as the user **sureline** (created above). Then run following commands:

   ```
   cd /home/sureline
   tar -xvzf SUREedgeLinuxAWSPackage.tar.gz
   ```

   ```
   sureline@ip-172-31-31-28:~$ cd /home/sureline/
   sureline@ip-172-31-31-28:~$ tar -xvzf SUREedgeLinuxAWSPackage.tar.gz
   ./
   ./sureedge-centos-proxy-prereq-installer.tar.gz
   ./install_sureedge_store.sh
   ./surestor-installer.tar.gz
   ./surestor-installer-scripts.tar.gz
   ./surestor-linux7-installer.tar.gz
   ./surestor-prereq-installer.tar.gz
   sureline@ip-172-31-31-28:~$
   ```

   ```
   sudo chmod 755 install_sureedge_store.sh
   sudo bash install_sureedge_store.sh AWS
   ```

   ```
   sureline@ip-10-0-0-27:~$
   sureline@ip-10-0-0-27:~$ sudo chmod 755 install_sureedge_store.sh
   sureline@ip-10-0-0-27:~$
   sureline@ip-10-0-0-27:~$ sudo bash install_sureedge_store.sh AWS
   W: --force-yes is deprecated, use one of the options starting with --allow instead.
   sureedge store install successfully
   sureline@ip-10-0-0-27:~$
   ```

2. Verify that the `surestor` service is running by issuing the following command:

   ```
   sudo systemctl status surestor.service
   ```

   Verify that the status is **active (running)** in the resulting output:

```
sureline@ip-172-31-31-28:~$ sudo systemctl status surestor.service
● surestor.service - SureStor Server
     Loaded: loaded (/lib/systemd/system/surestor.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2021-08-10 08:10:31 UTC; 7min ago
   Main PID: 92008 (sh)
      Tasks: 14 (limit: 19200)
     Memory: 1.0G
     CGroup: /system.slice/surestor.service
             ├─92008 /bin/sh -c /opt/sureline/sureedge/bin/surestor >> /var/sureline/sureedge/log/surestor_stdout.l>
             └─92010 /opt/sureline/sureedge/bin/surestor

Aug 10 08:10:31 ip-172-31-31-28 systemd[1]: Starting SureStor Server...
Aug 10 08:10:31 ip-172-31-31-28 surestor-pre-start.sh[91966]: /opt/sureline/sureedge/bin/surestor-pre-start.sh: lin>
Aug 10 08:10:31 ip-172-31-31-28 surestor-post-start.sh[92009]: Started the SureStore Server
Aug 10 08:10:31 ip-172-31-31-28 systemd[1]: Started SureStor Server.
Aug 10 08:10:31 ip-172-31-31-28 systemd[1]: /lib/systemd/system/surestor.service:14: Unknown key name 'StartLimitIn>
Aug 10 08:10:31 ip-172-31-31-28 systemd[1]: /lib/systemd/system/surestor.service:14: Unknown key name 'StartLimitIn>
Aug 10 08:10:31 ip-172-31-31-28 systemd[1]: /lib/systemd/system/surestor.service:14: Unknown key name 'StartLimitIn>
Aug 10 08:10:32 ip-172-31-31-28 systemd[1]: /lib/systemd/system/surestor.service:14: Unknown key name 'StartLimitIn>
lines 1-18/18 (END)
```

If the service is not running or the commend otherwise returns an error, contact the Persistent support team (refer to Section, “Contacting Support” for more details).

This completes the deployment of the SUREedge DR Store VM. You can now proceed to deploy the MC VM.

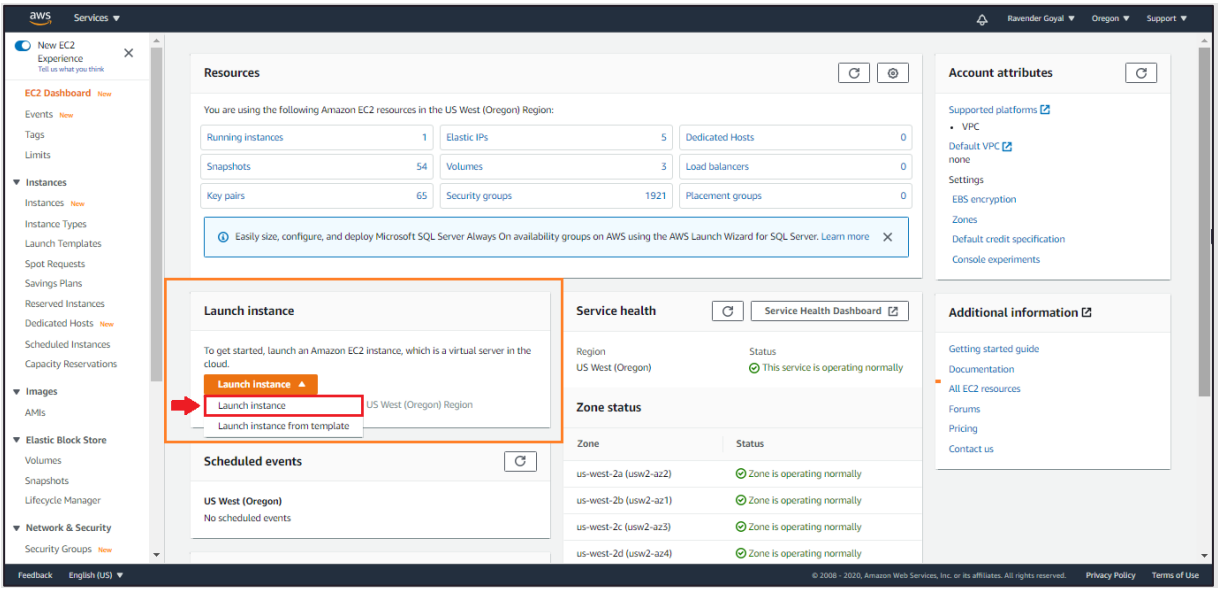
Deploying the SUREedge MC

Creating your SUREedge Management Console (MC) is done by deploying a Windows-based VM in your Amazon EC2 environment and installing the SUREedge DR MC software components on it.

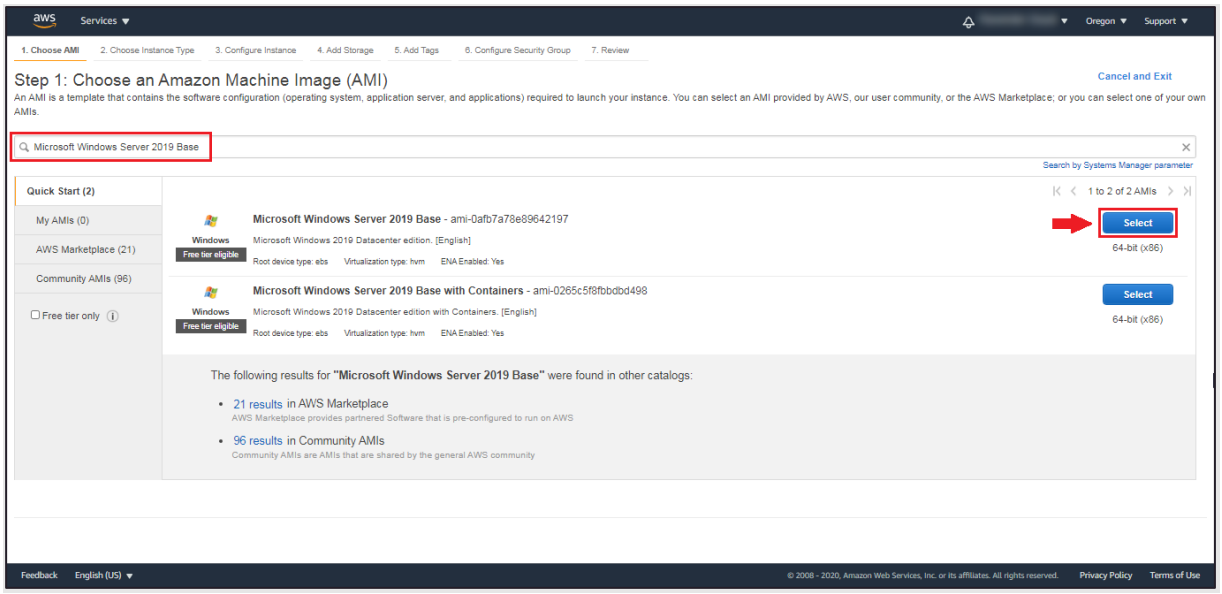
Launch a Windows Instance

You first need to launch a Windows instance from the AWS Management Console as described in the following steps:

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the dashboard console choose **Launch Instance** dropdown and select **Launch Instance** from the dropdown.

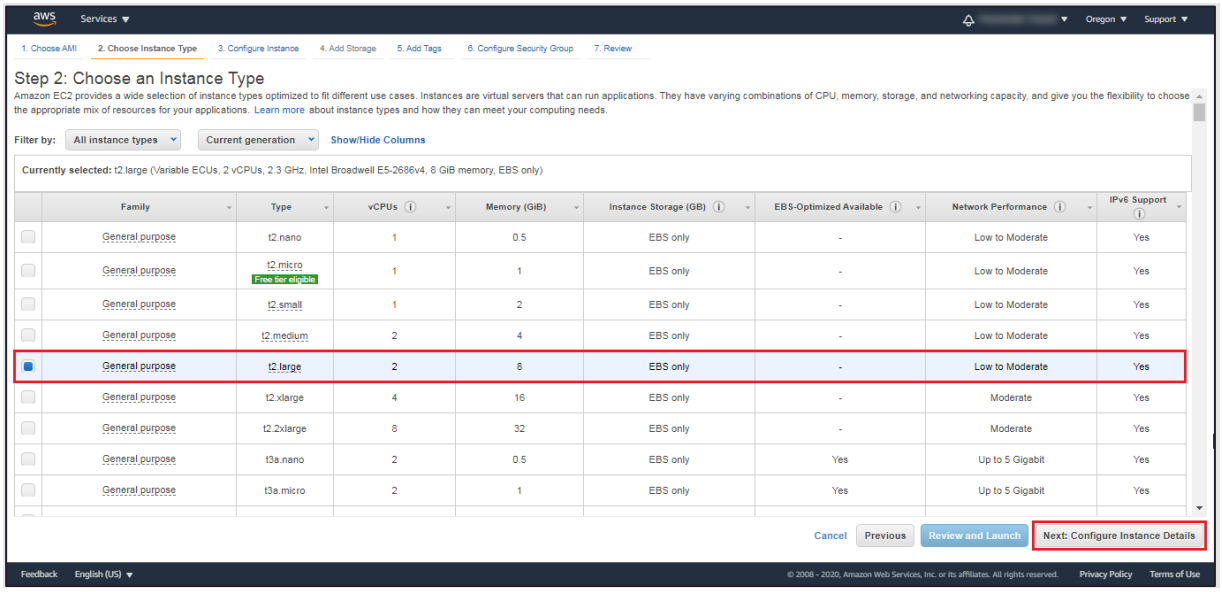


3. On the **Choose an Amazon Machine Image (AMI)** page search for an AMI by entering the term “**Microsoft Windows Server 2019 Base”** in the Search bar:



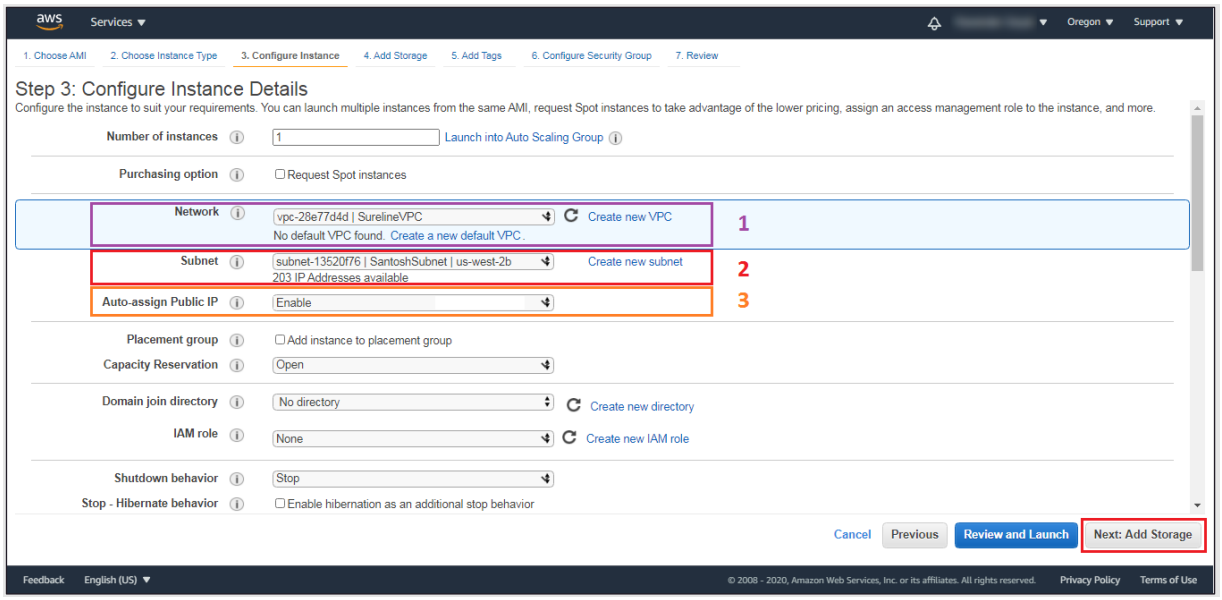
Locate the image that matches the provided name and click its **Select** button.

4. This takes you to the **Select an Instance Type page**. Select the instance type *t2.large* (with 2 vCPUs and 8 GiB of Memory):



Click **Next: Configure Instance Details**.

5. This takes you to the **Configure Instance** Details page:



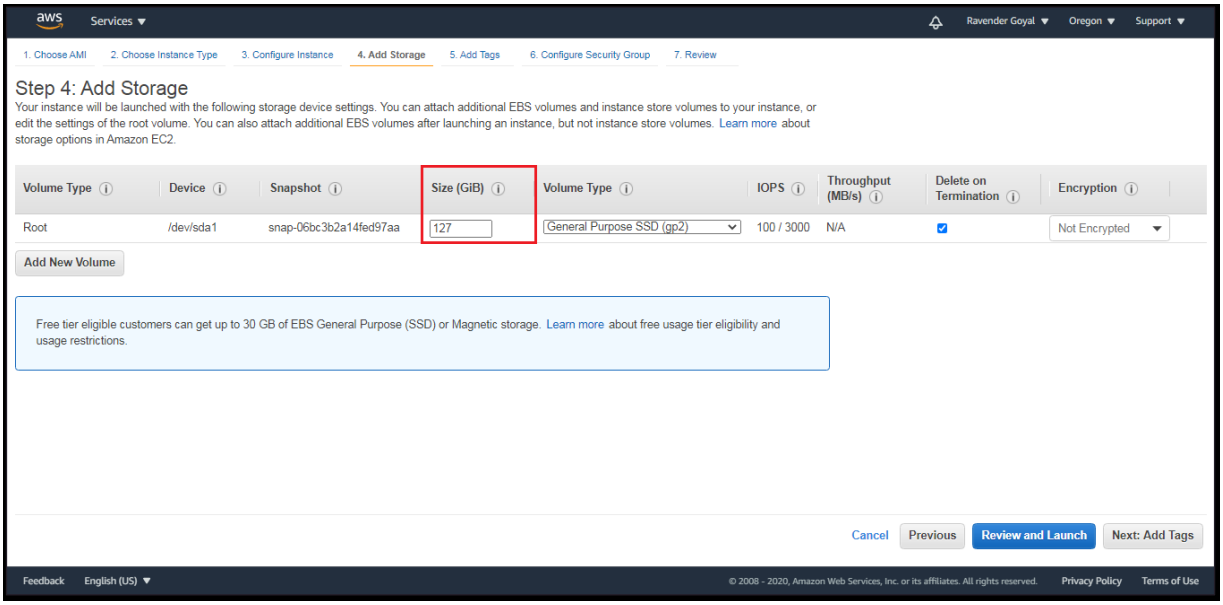
Make the following selections:

a. From the **Network** and **Subnet** down lists choose the network where the SUREedge store should be deployed. (This should be a network that has connectivity to all networks where systems may be recovered; see section, "Configuring Firewall Rules" for more details.)

b. Select *Enable* for **Auto Assign Public IP.**

In the remaining fields keep the default values. Click **Next: Add Storage.**

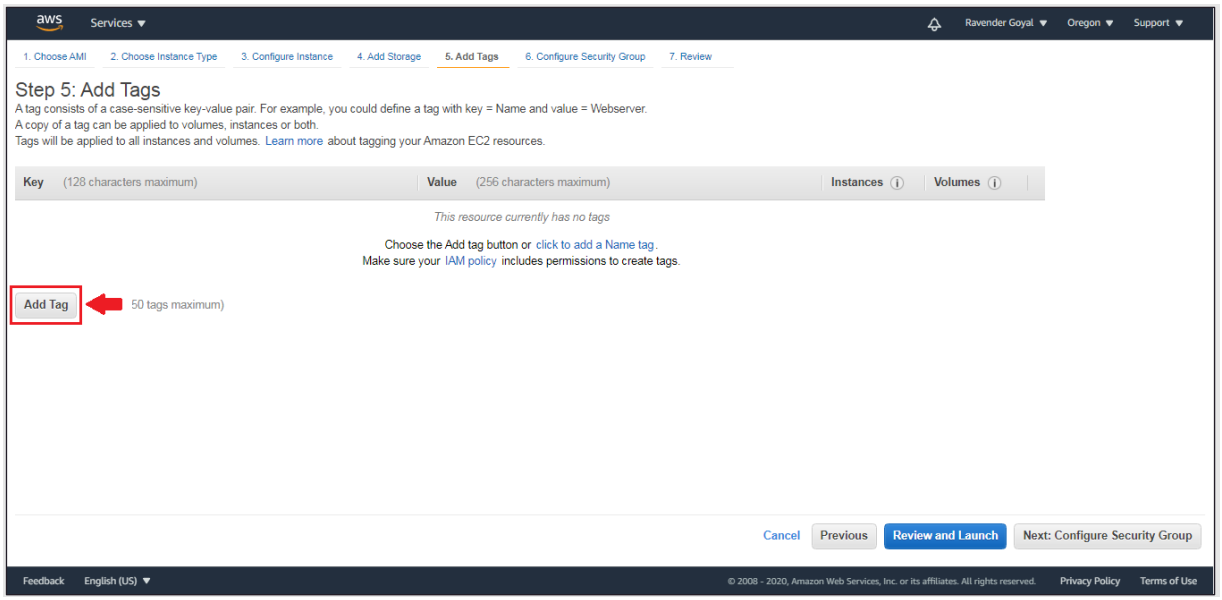
6. In the **Add Storage** page set the size of the **Root** volume to 127 GB:



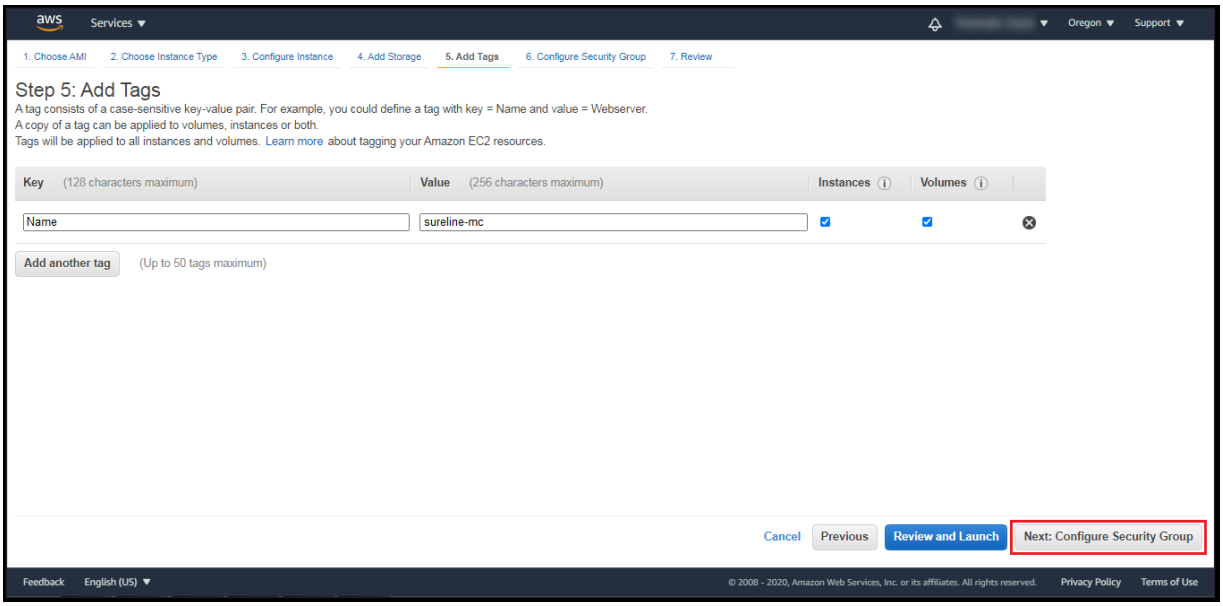
Click **Next: Add Tags.**

7. Here you can add any tags to the VM that are desired. (No tags are required for deploying the SUREedge DR instance, but you may wish to add tags to, for example, aid in identifying the VMs that make up the instance.)

To add a tag (optional), click on **Add Tag** button as shown:

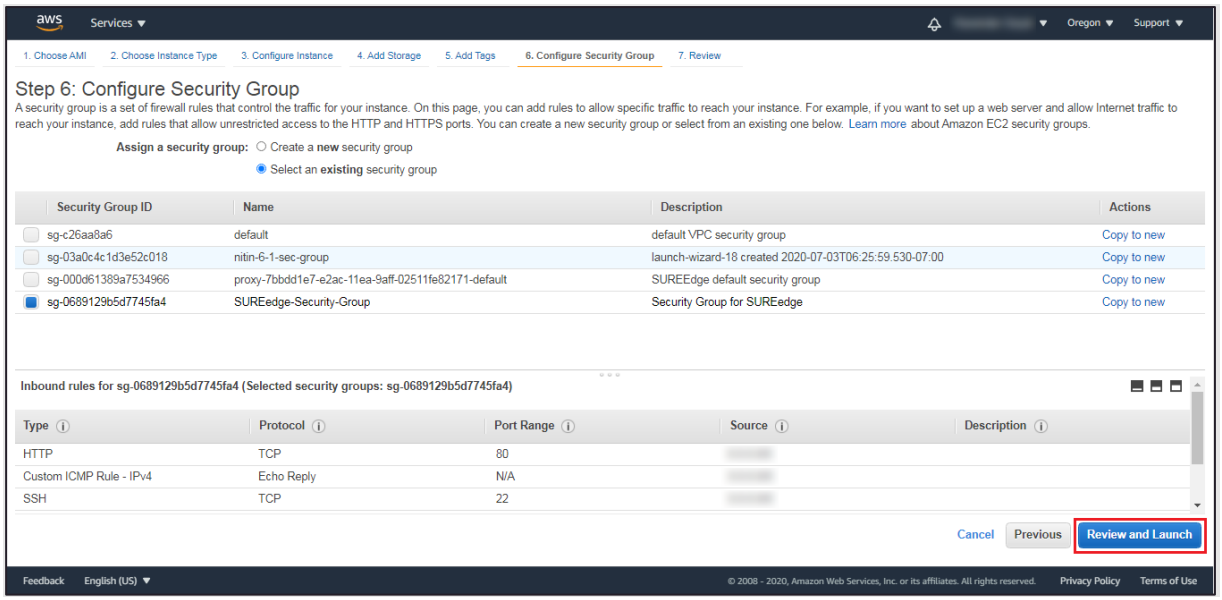


Click once on the **Add B**utton, the **Add Tags** page is displayed:



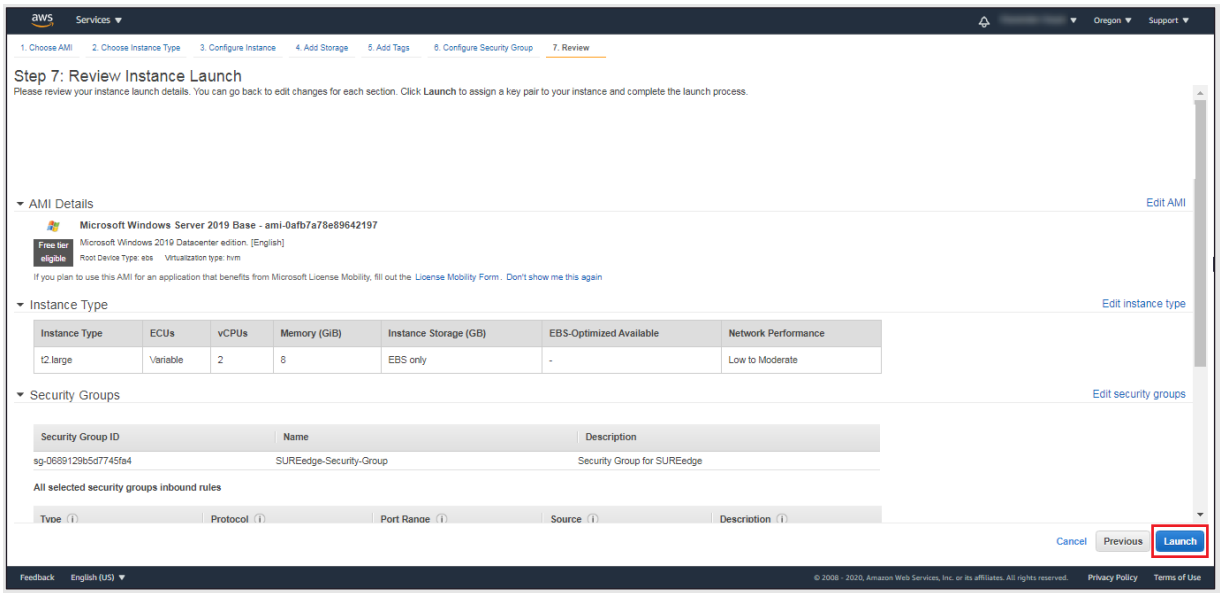
Here you can enter the **Key** and **Value** for the tag. For example, you could define a tag with **Key** = *Name* and **Value** = *Sureedge-Store*.
When you have added all the tags you wish to add click **Next: Configure Security Group.**

8. In the **Configure Security Group** you should choose a group that has the required firewall rules as indicated in Section, "Configuring Firewall Rules":-



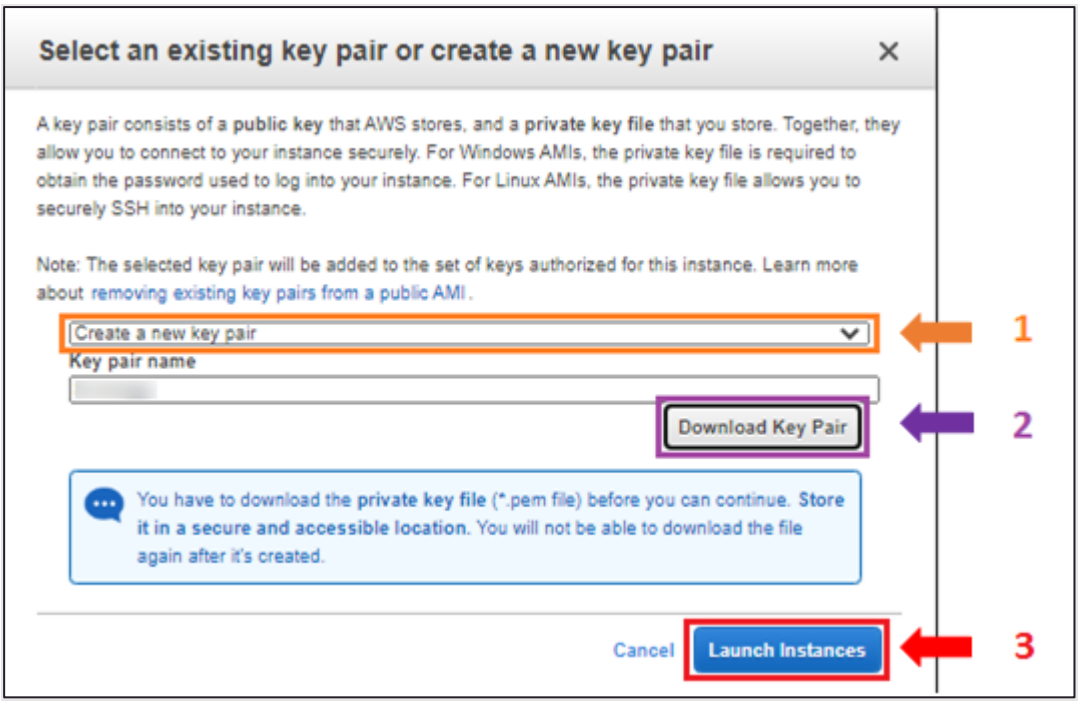
Click **Review and Launch.**

9. Review the specifications on the review page to make sure you are satisfied with your choices:



When you are ready to deploy the VM click **Launch**.

10. You will see a dialog box regarding the use of a key pair for accessing the VM:



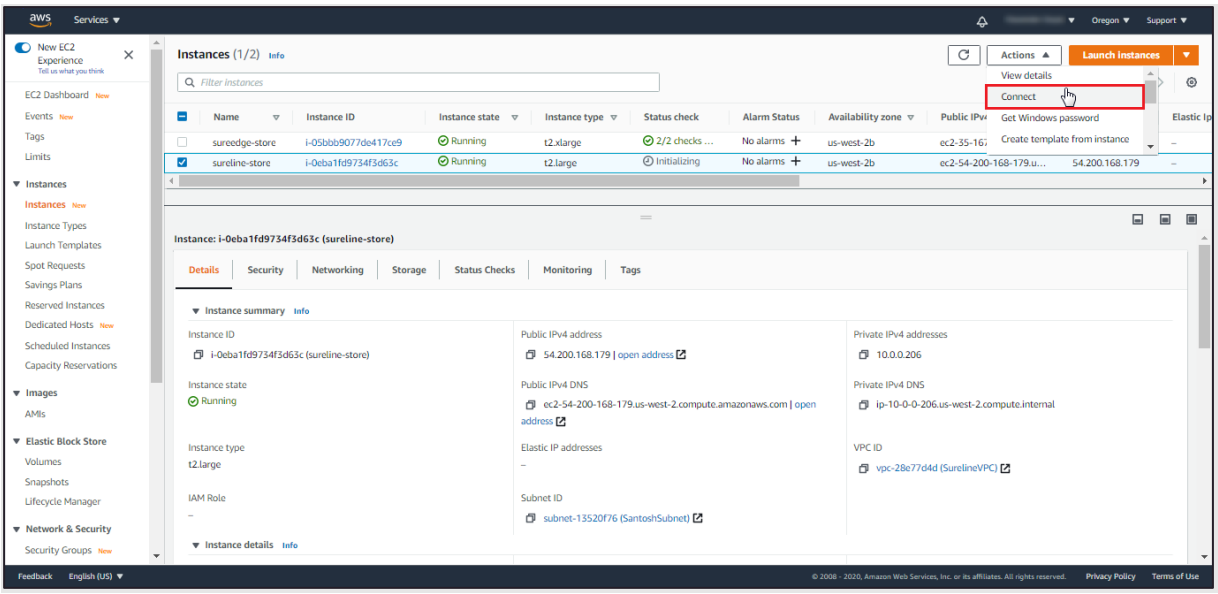
From the dropdown (**1** above) you can choose to either **Create a new key pair** for use by SUREedge DR (recommended) or **Choose an existing key** pair if you have one already created that you wish to use. If creating a new key pair provide a new **Key pair name** and then click **Download Key Pair** (**2** above). ***You should securely store the newly created Key Pair as it is required in order to connect to the VM via RDP.***

11. Click **Launch Instances** (**3**).

Connecting to the MC VM

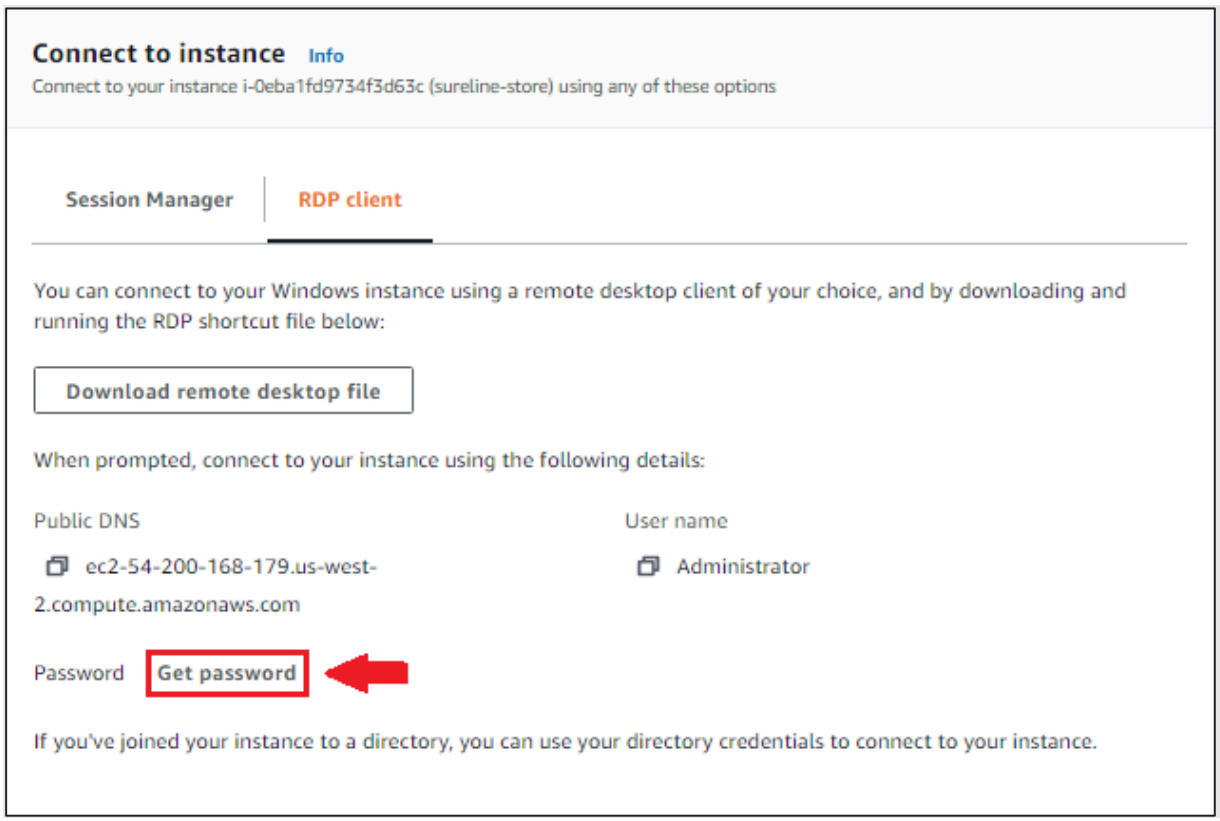
In order to install the SUREedge DR MC software components on the Windows VM you will need to connect to it via RDP. Once your deployed VM is in the Running state use the following steps set up RDP and connect to it:

1. From the AWS console navigate to the **Instances** section, select the VM and select **Connect** from the **Actions** drop down.



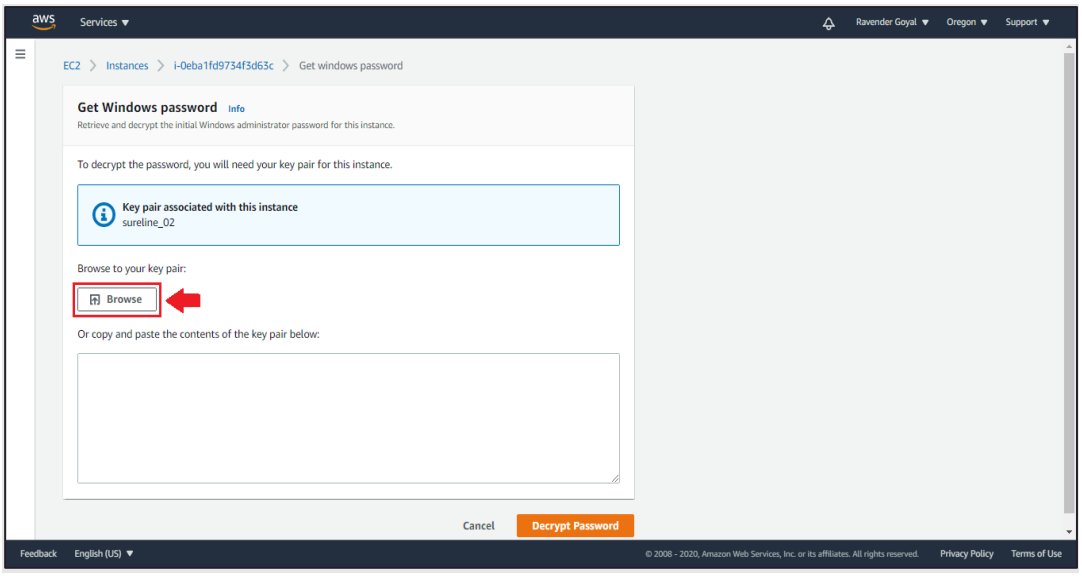
Note: Please note down the **Private Ip Address**, **Username** and **Password,** as will be required for connecting your instance.

2. In the resulting **Connect To Instance** dialog box you can choose either of the two options provided (**Session Manager** or **RDP Client**) to connect to the Windows instance:

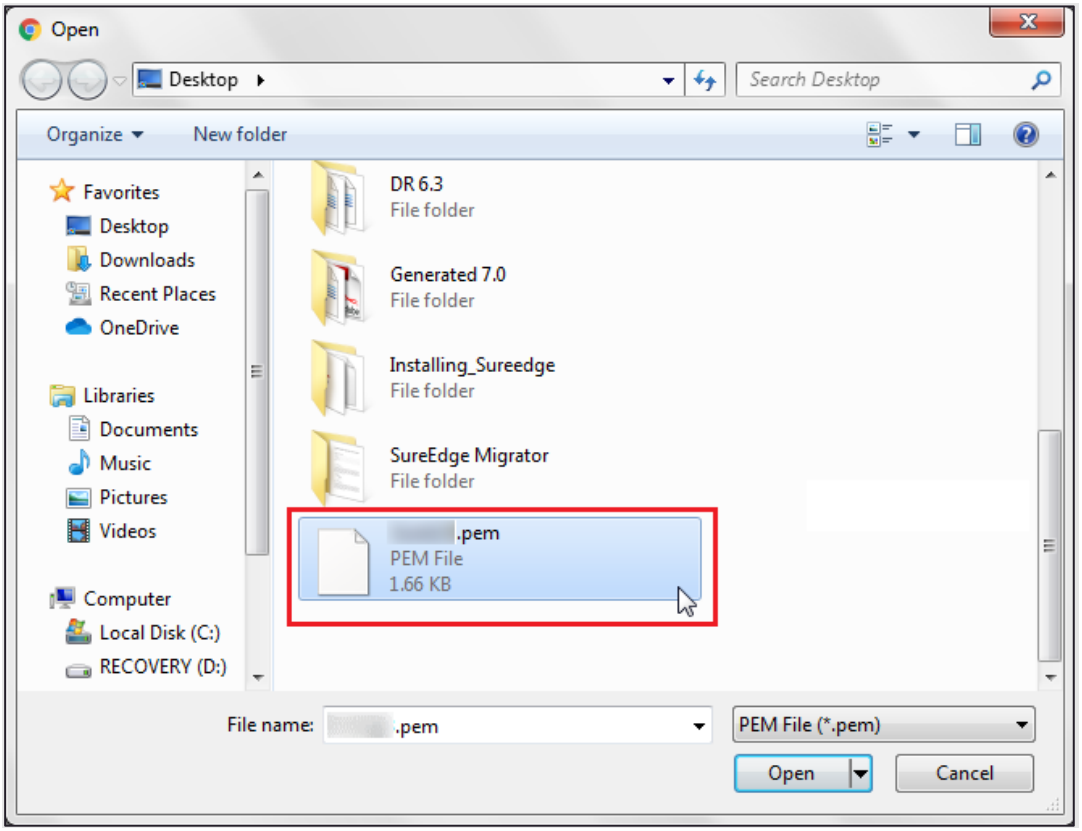


The screenshot above shows connecting via the **RDP** option which allows you to download an RDP configuration file for connecting to your MC instance.

   a. First you should obtain the password which will be needed when you connect via RDP. To retrieve it click on the **Get Password** button.
   b. Click **Browse** to choose a file from your computer:

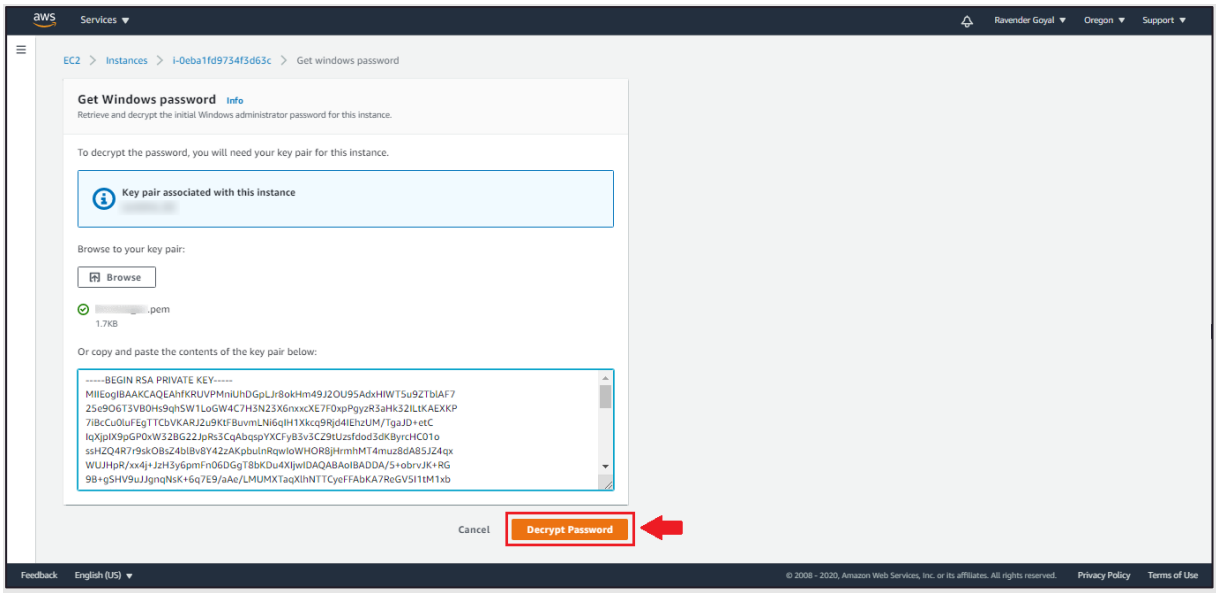


c. In the file selector popup browse to your private key file that you created and downloaded when you launched the instance (Step 10 in Section Launch a Windows Instance0)

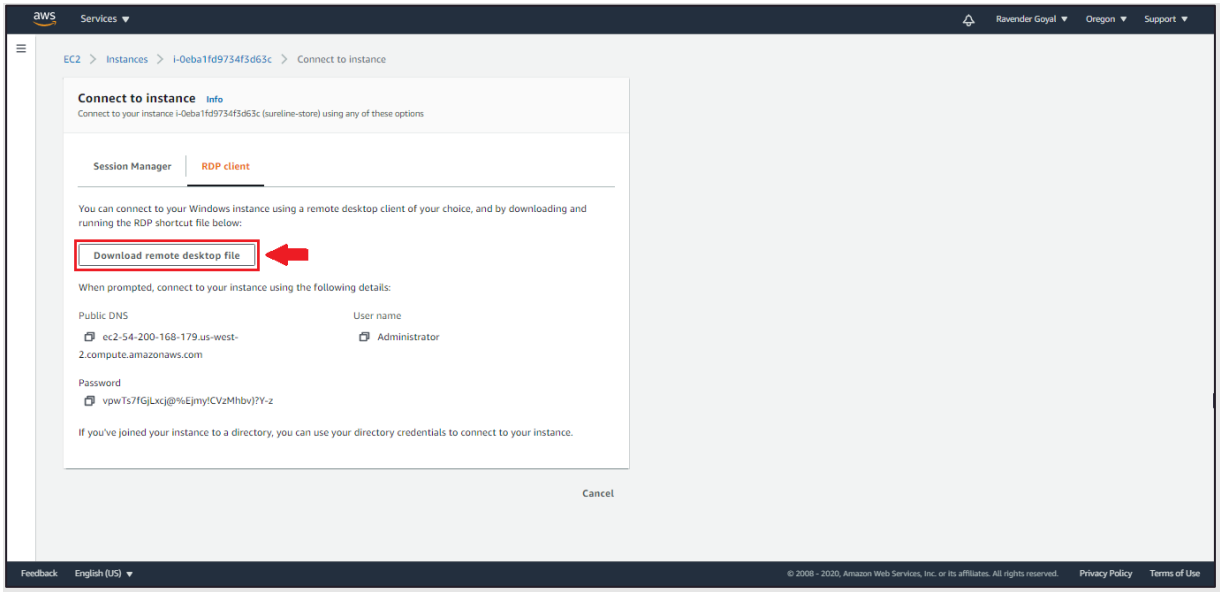


Select the **Key** file and click on **Open button**.

d. Back in the **Get Windows Password** dialog click on **Decrypt Password** button and note it down for use when you connect.

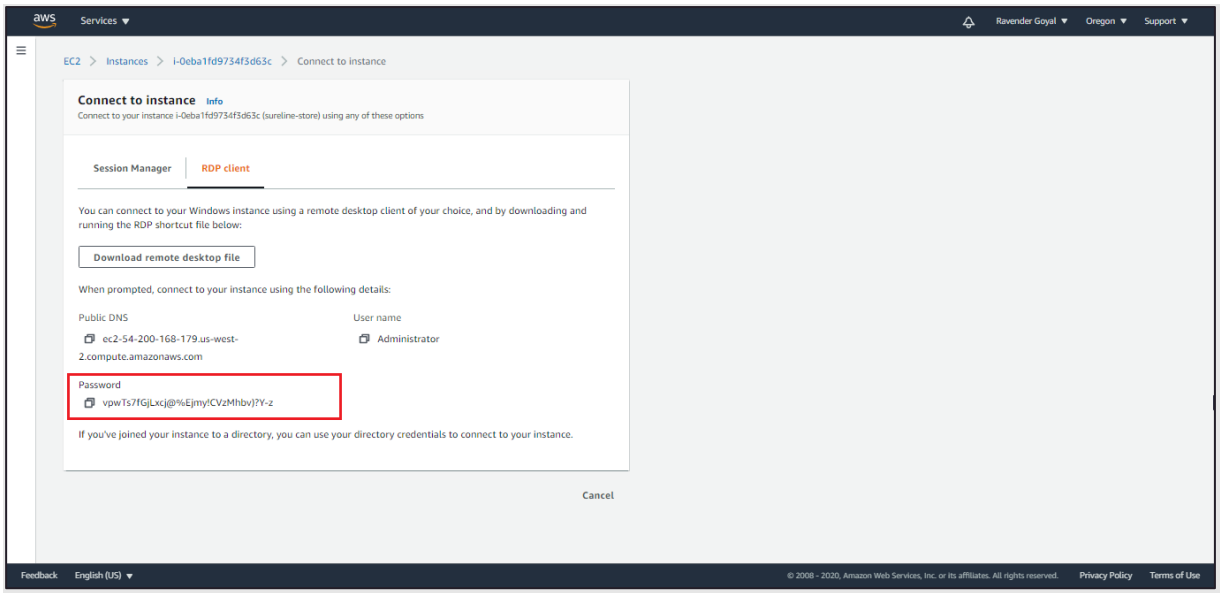


3. Back in the **Connect To Your Instance** dialog click **Download Remote Desktop File**:

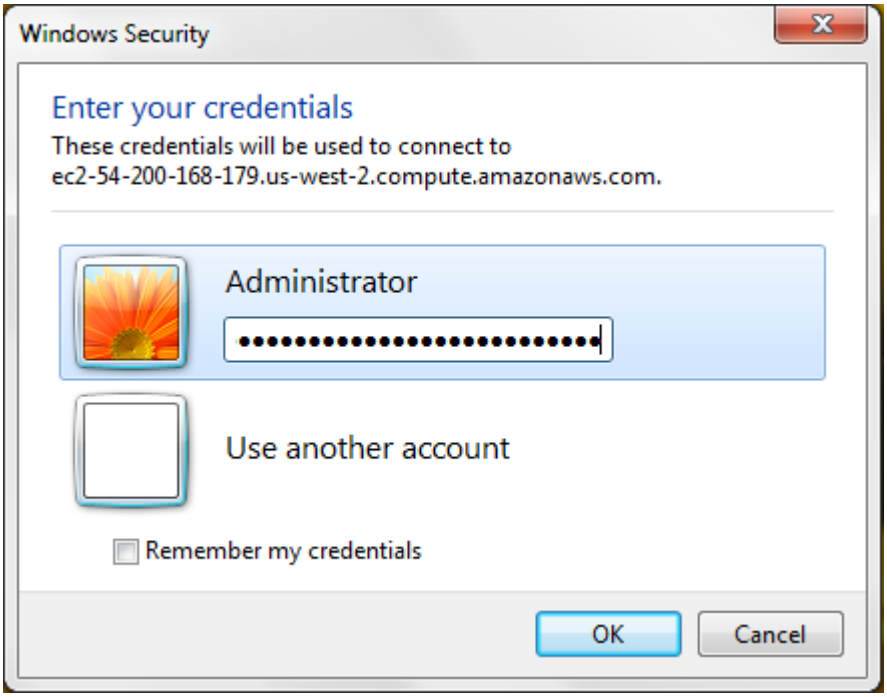


You'll get a save file dialog from your browser; save the RDP configuration file to your computer.

4. Copy the password as shown in the screenshot for connecting to your windows instance.



5. You can now connect to your Windows instance using the RDP file by double-clicking it:

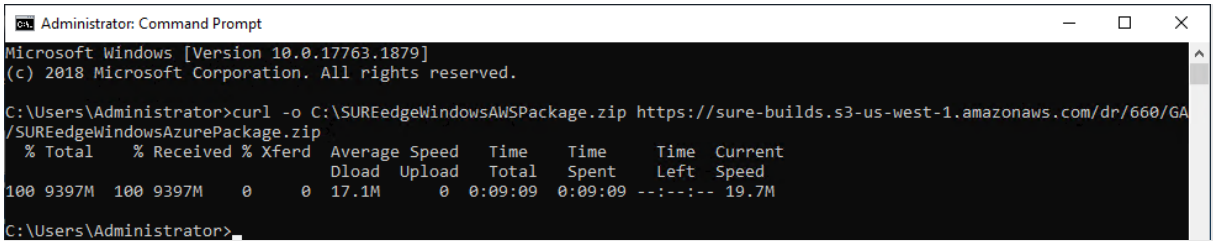


Fill in the password prompt using the password you obtained earlier in the **Get Password** dialog (Step 4above).
Click on the **OK** button to connect. (You may get a warning that the security certificate could not be authenticated. Simply choose **Yes** or **Continue** to continue if you trust the certificate to verify the identity of your instance.)

Downloading Software Installers

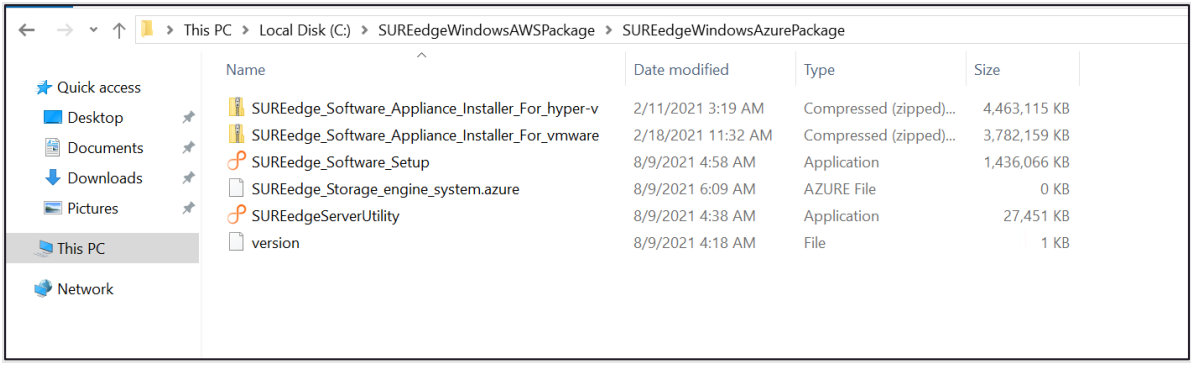
You now need to download the SUREedge Windows AWS Package to the Windows VM instance.
Run the following command in Windows Command Prompt:

```
curl -o C:\SUREedgeWindowsAWSPackage.zip https://sure-builds.s3.us-west-1.amazonaws.com/dr/661/GA/SUREedgeWindowsAzurePackage.zip
```

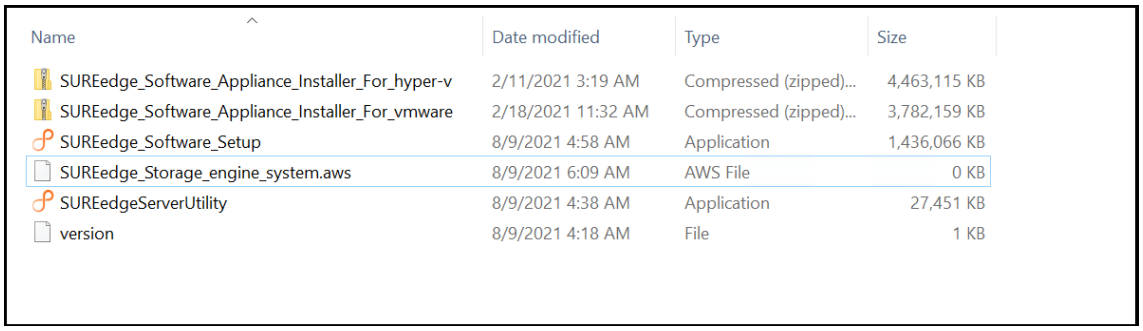


This command will download the SUREedge Windows AWS Package file on your Windows VM Instance with the file name `C:\SUREedgeWindowsAWSPackage.zip`

Once you have downloaded the SUREedge Windows AWS Package to your Windows VM instance you will need to unzip and extract the zip folder for installing the SUREedge Migrator Setup.



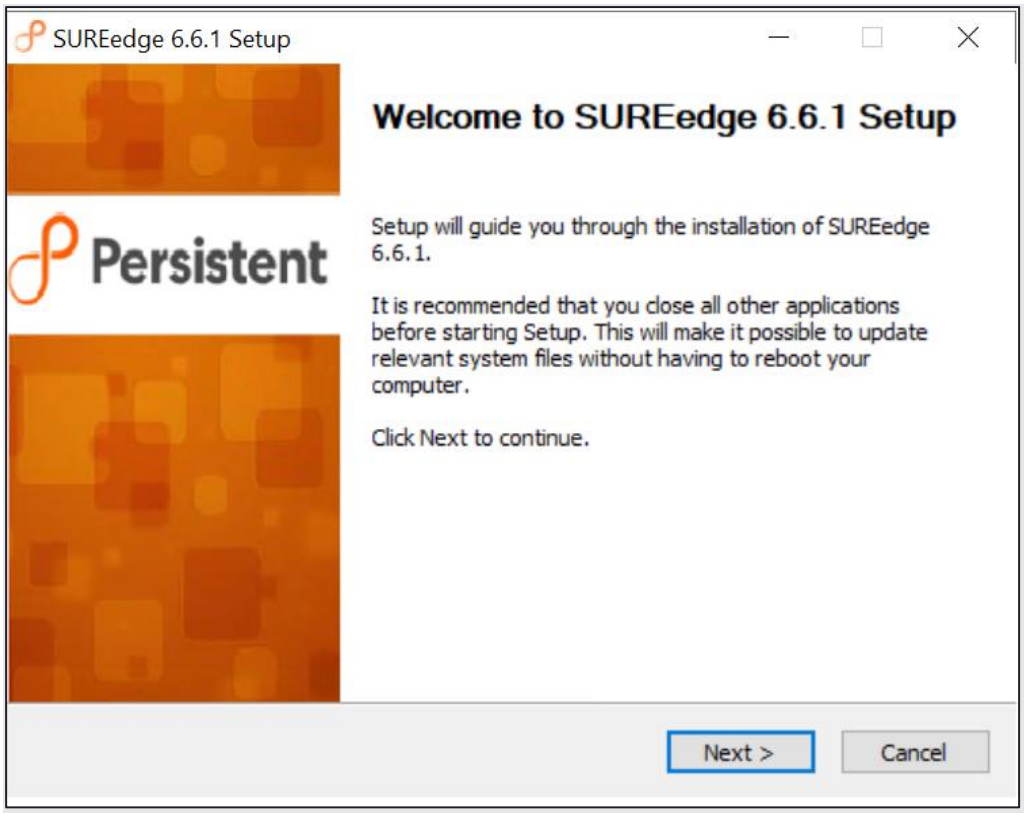
After extraction of zip file rename the file `SUREedge_Storage_engine_system.azure` to `SUREedge_Storage_engine_system.aws`



Installing Packages

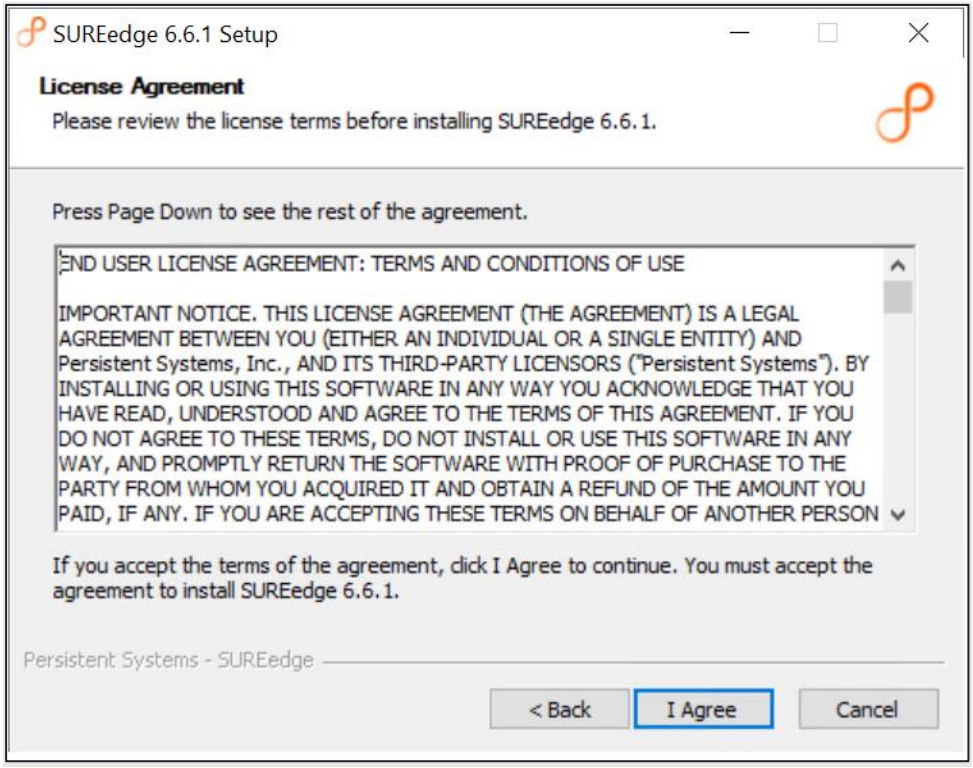
Once the installer files have been copied to the Windows VM use the following steps to install the SUREedge DR MC components on it:

1. Execute the file `SUREedge_Software_Setup.exe` as administrator by right-clicking on it, and selecting **Run as administrator**. This will display a popup that says “Validating installer pre-checks…” for a few moments; wait for the validation to complete.
2. The first installer screen you’ll see is the Welcome screen:



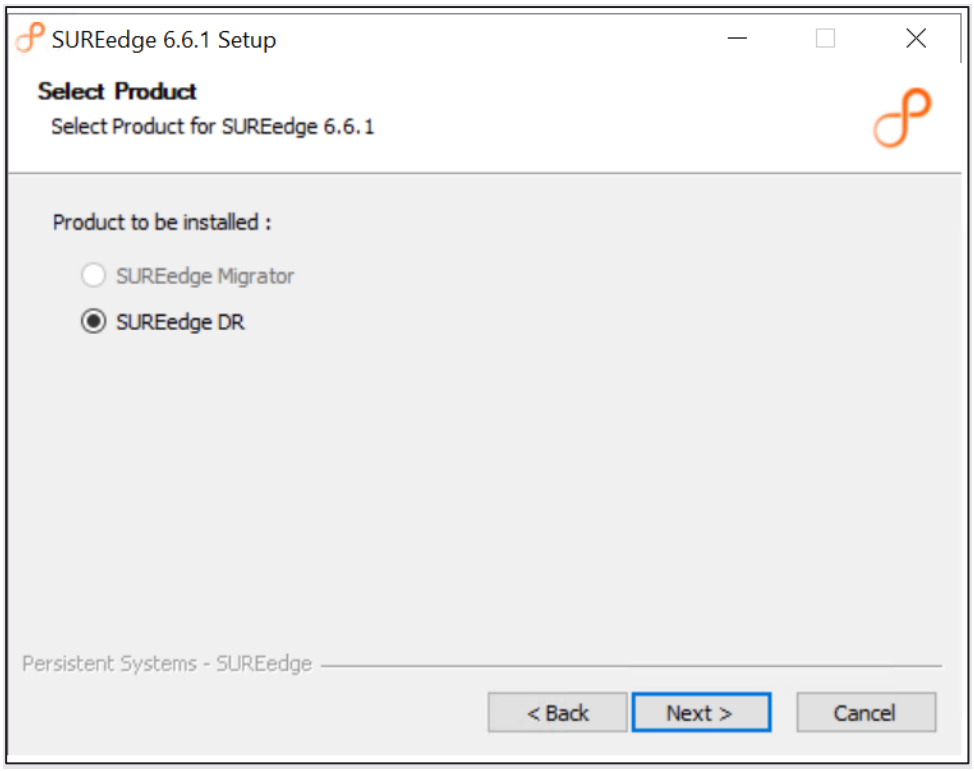
Click **Next**.

2. This will display your **License Agreement:**



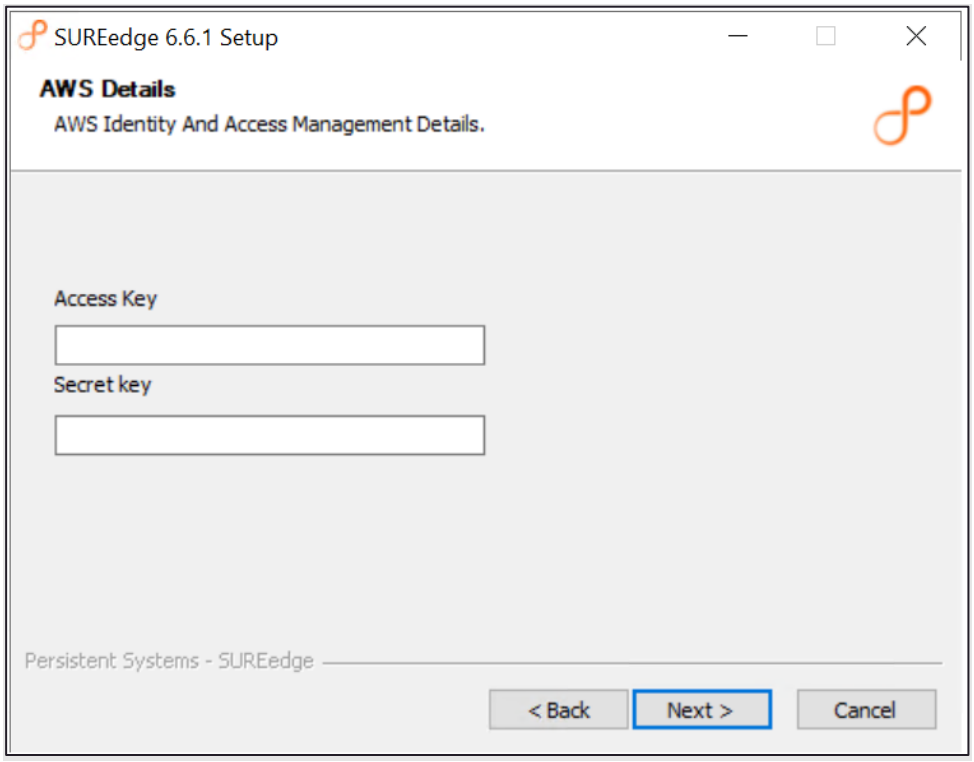
Please read the license agreement and click **I Agree** to continue.

3. The next page allows you to select the software package to install; by default, *SUREedge DR* is selected:

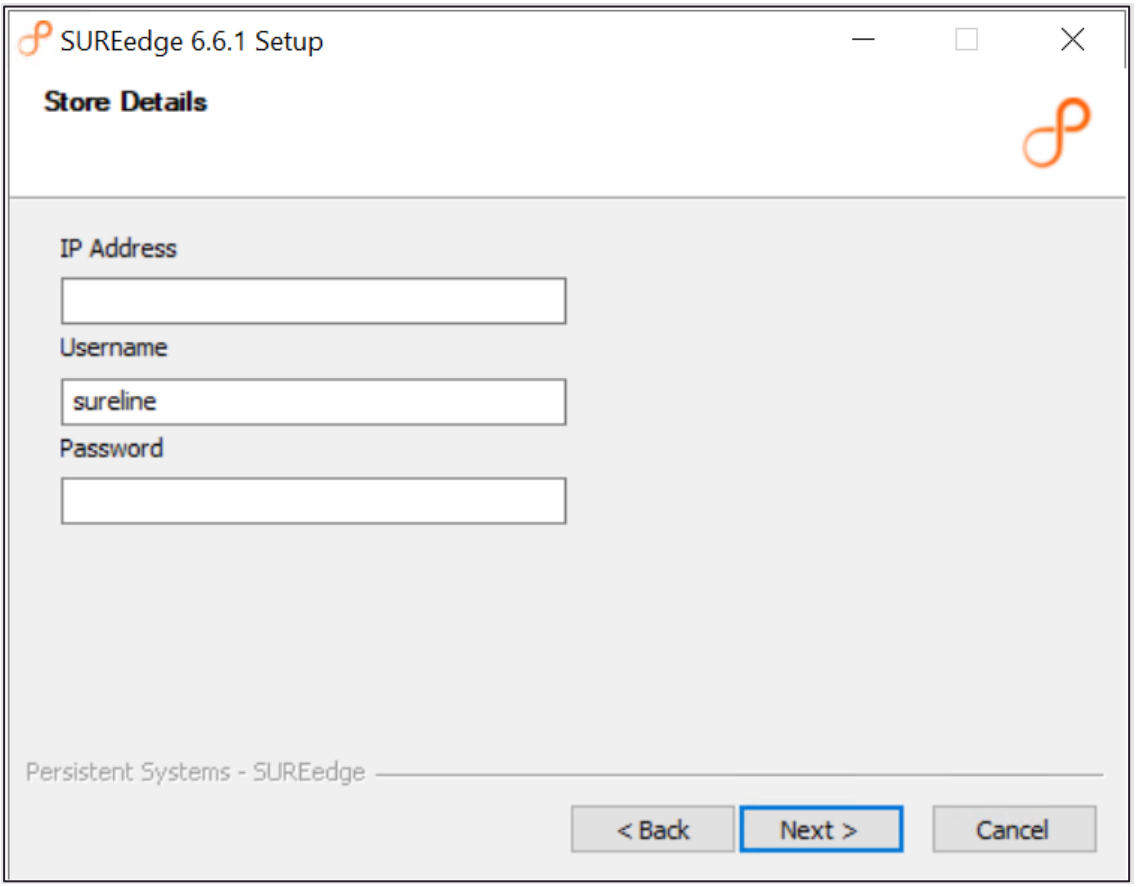


Click **Next**.

4. The next screen allows you to specify the **AWS Access and Identity managements Details**:

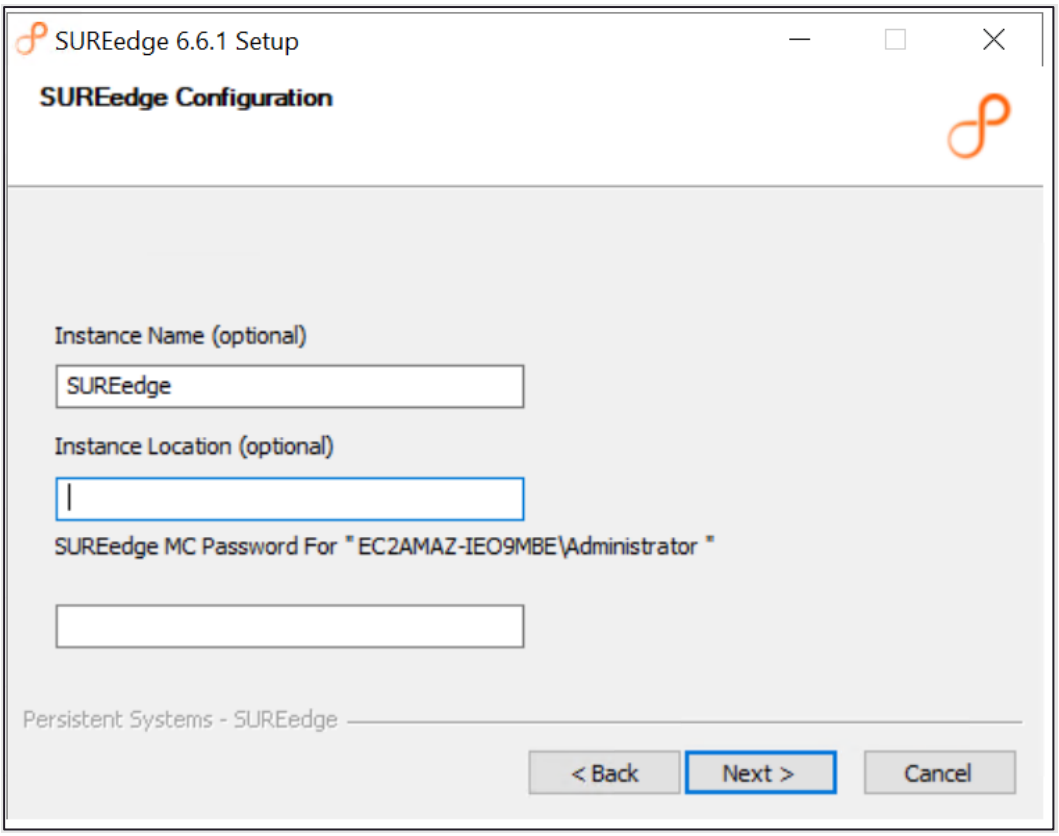


5. The next screen allows you to specify the **Store Details**:



Provide the *internal IP address* for the store and the credentials: the username **sureline** and the password you set for the **sureline** account you created in Step 5 in the section.
Then click **Next**. This starts the validation of the store parameters that were provided.

6. Once the Store address and credentials are validated you will see the **SUREedge Configuration** screen:

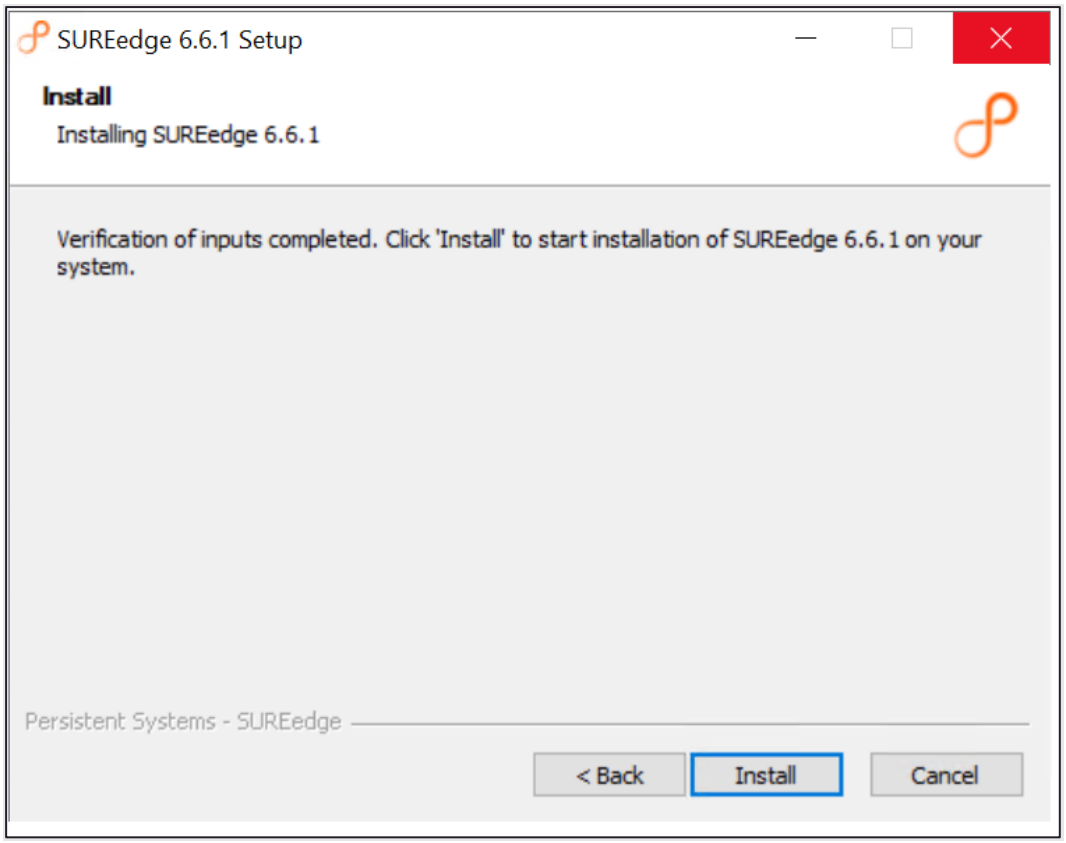


Fill these fields in as follows:

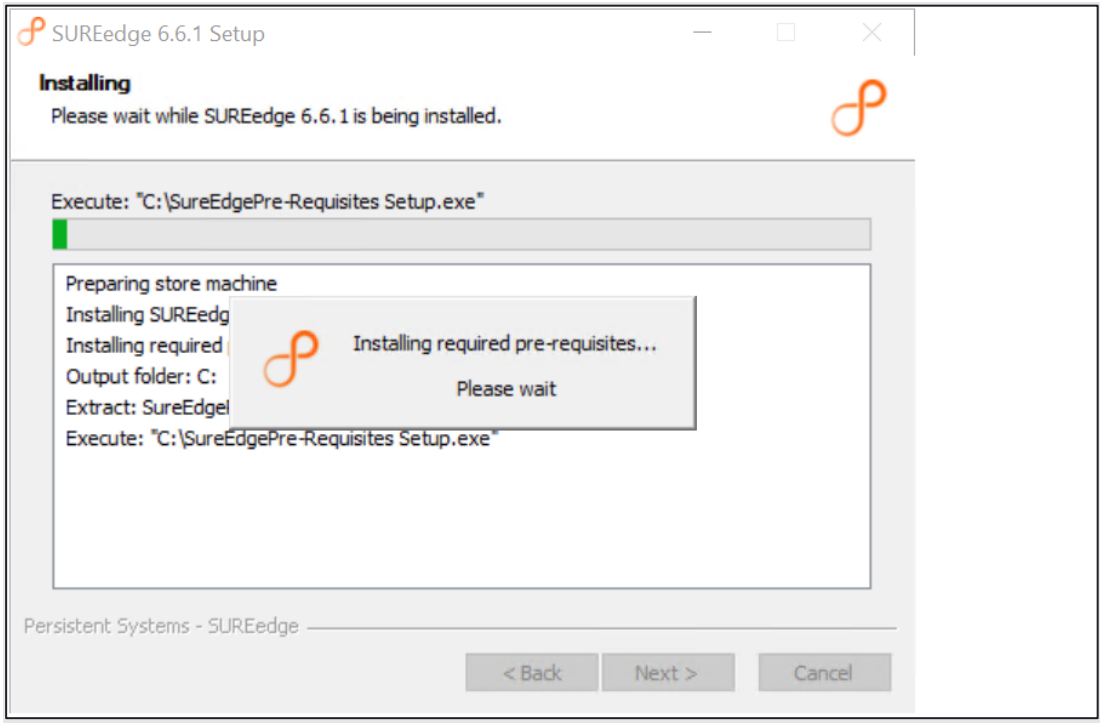
a. The **Instance Name** and **Instance Location** fields are optional strings that you can specify; they are displayed on the SUREedge DR UI screen which makes it easier while managing multiple SUREedge DR instances.
b. Set **SUREedge MC Password** to the login password for the MC instance that you saved in Step 5 in section, "Connecting to the MC VM".

When you have filled details in the above fields click **Next**.

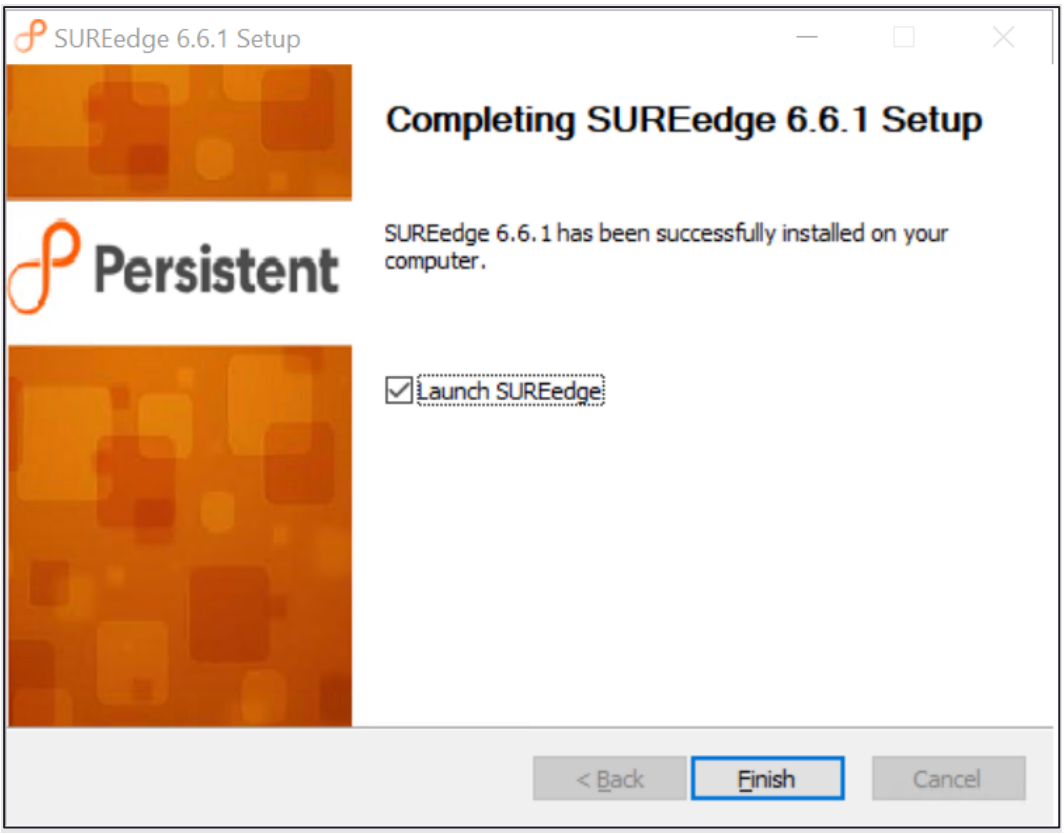
7. The installer will now verify all the supplied parameters and if any are found to be invalid, an error message will be displayed. When verification completes successfully you will be shown the **Installation Conformation** screen:
   Click **Install** to proceed with the installation or **Cancel** to exit without installing.
8. During the installation process, installer will display a monitoring window where you can see the progress of the installation:



The progress of the installation will be displayed while the installation is ongoing.



The time required to complete the installation will vary depending on the performance and load on the systems involved, the availability of resources, etc.
Once the installation is completed you will see the completion screen:

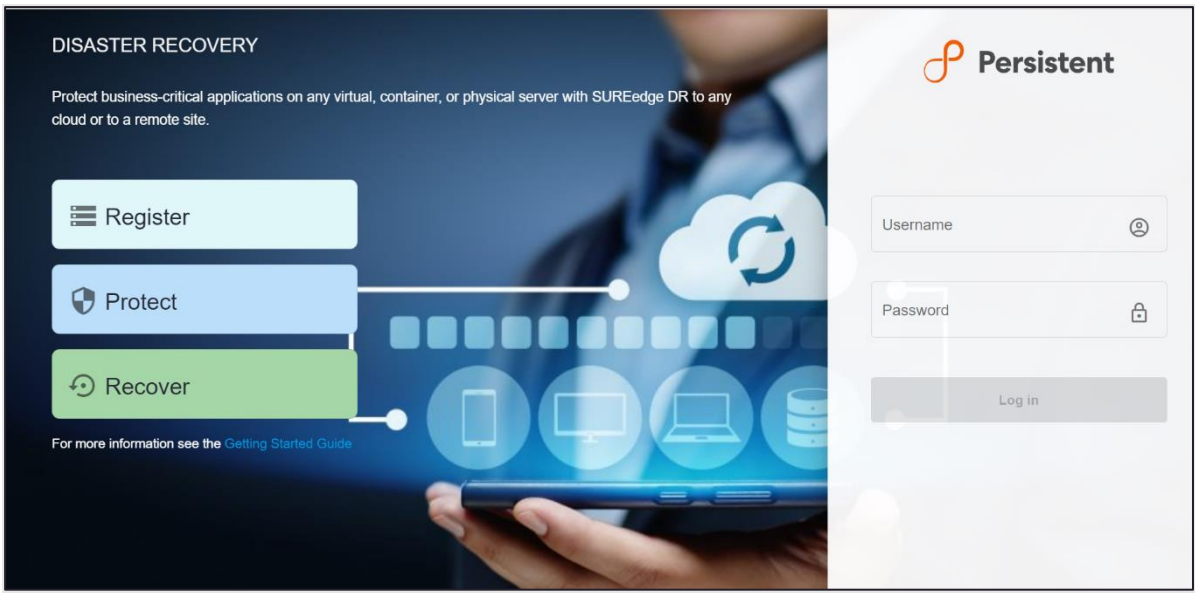


Click **Finish** to dismiss the installer. If you have selected the **Launch SUREedge** button a browser window will be launched with a URL to the localhost for accessing the SUREedge DR User Interface.

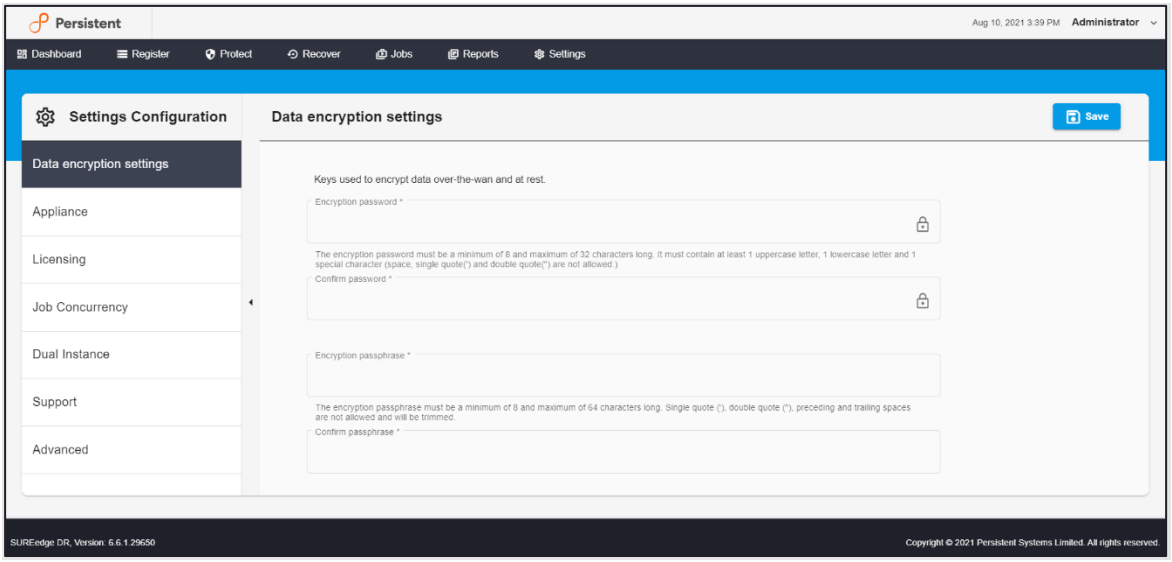
Configuring the Instance

Once installation is completed you will need to connect to the SUREedge DR User Interface to perform instance configuration. You can do this using a browser on the Windows MC VM using this URL: (https://localhost/sureedge/index.php/) . Or you can connect from a remote browser by substituting the MC VM's IP address for "localhost".

When you connect you will be presented with the DR UI login screen:



Log into the SUREedge DR instance, using the login password for the MC instance that you saved in Step 5 in the section, "Connecting to the MC VM". You will be presented with the **Data Encryption Settings** page:



Here you need to enter the **Encryption Password** and the **Encryption Passphrase** that were set at GCP site DR instance when you deployed it. **The Encryption Password** and **Encryption Passphrase must match those given for the target site** as these will be used to encrypt system data that is transferred over the WAN and when it is placed into persistent storage. Once you provide a password and passphrase, click on the **Save** button.

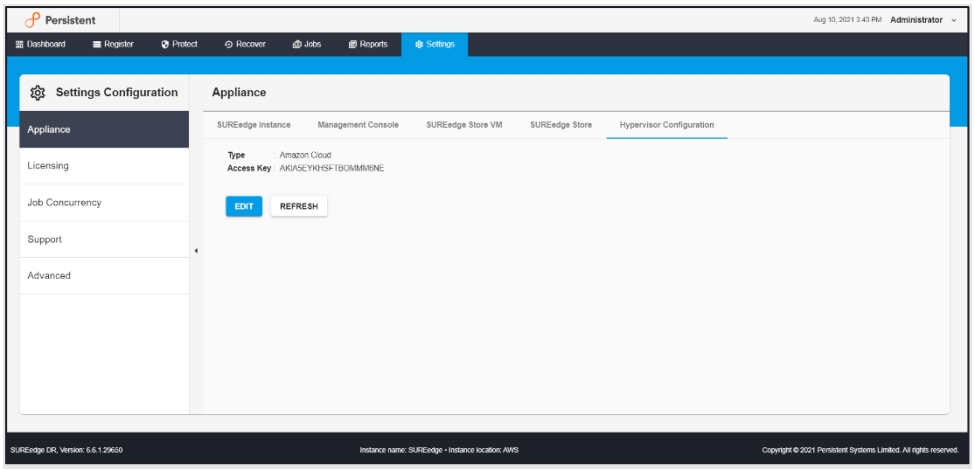
You now need to configure your DR Instance with details about your AWS environment and account.

AWS Details after Configuration

1. Prefilled details are displayed for your AWS account.

   Note: You can edit the details for the AWS account, such as the access key and secret key.

Click on the **REFRESH** button to retrieve settings and information from your AWS account:



Your deployment of SUREedge DR in AWS environment is now compelte!

Obtaining Licenses

Each instance of SUREedge DR must be licensed to perform recovery. If you have not received your license(s) you can obtain it (them) through your designated contact at Accelerite Systems or by contacting the Accelerite Systems Support Team at support@accelerite.com.

Once you purchase the SUREedge DR, you will get a permanent GUID license. These licenses are tied to a specific SUREedge DR instance. To obtain your GUID licenses you will need to supply the Appliance Serial Number to Accelerite Systems for all your SUREedge DR instances after they have been installed. Detailed instructions on getting your Appliance Serial Number(s), obtaining your permanent licenses and applying them to your SUREedge DR instance(s) can be found in your *SUREedge DR User Guide(s)*.

Once you have license(s) for your SUREedge DR instance(s) they will need to be installed before you can perform recovery operations. Instructions for installing licenses on the SUREedge DR instances can be found in the **Settings** section of *SUREedge DR User Guide*.

Contacting Support

Accelerite Software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by being able to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Submit enhancement requests online
- Download software patches
- Look up Accelerite support contacts
- Enter into discussions with other software customers
- Research and register for software training

To access the Self-serve knowledge base, visit the Accelerite Support home page at

https://support.accelerite.com/hc/en-us

Most of the support areas require that you register on the Accelerite Support Portal. Many also require a support contract.

To register an account at the Accelerite Support Portal, visit

https://support.accelerite.com/hc/en-us

To know more about registration process at Accelerite support portal, visit

https://support.accelerite.com/hc/en-us/articles/202042570-New-user-registration-process

Appendix: Store Sizing Guidelines

The Deduplicated Store is kept in a virtual disk device attached to the Store VM in your SUREedge DR instance where all data within captured system images is stored. You will need to set an initial size for the Deduplicated Store's virtual disk device while deploying the Store VM. You can also manage the Deduplicated Store size from the SUREedge DR user interface, including setting up automatic growth when it is needed (see the *SUREedge DR User Guide* for details on this feature). Thus, while choosing a size for the Store when you first deploy your DR instance is important the choice is not permanent, and you can change it later if you do not get it exactly right.

The deployment process defaults to a Store device size of 1024 GB, which is sufficient to protect systems whose storage adds up to around 800GB. If you have a large number of systems and/or the total storage space you are protecting is larger, you can adjust the disk size to match your workload.

The optimal size for the Deduplicated store can be difficult to estimate as it depends on several factors, such as:

- the capture schedules that you configure for your servers;
- the types of captures (full versus incremental);
- the rate of change and overwrite factors of your data;
- the compressibility of your data;
- the deduplication factor of your data.

It is usually easier to initially deploy your DR instance with a safe, rough estimate for the deduplicated store size and then adjust it later as you learn more about the nature of your systems and data rate change or allow it to grow automatically using the SUREedge DR Auto Grow feature.

You can determine a safe Store size for your deployment using the formula as mentioned below:

Recommended disk size = [**sum of all server storage to capture**] * **1.25**

This leaves enough room for complete images for all your systems and data, as well as a few updates for those images, given a reasonable average data deduplication rate.