

# 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**

© Copyright 2021 Persistent Systems Ltd. All rights reserved.

#### **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**

Introduction4
Deployment Scenarios4
Installation Overview4
Pre-requisites6
Getting AWS Parameters6
Configuring Firewall Rules7
Obtaining SUREedge Software and Documentation8
Obtaining SUREedge Installers8
Obtaining Documentation8
Installing SUREedge DR9
Deploying the SUREedge Store9
Launch a Linux Instance9
Connecting to the Store VM15
Configuring the Store VM OS16
Downloading Software Components19
Installing Software Components19
Deploying the SUREedge MC20
Launch a Windows Instance20
Connecting to the MC VM25
Downloading Software Installers
Installing Packages
Configuring the Instance
AWS Details after Configuration
Obtaining Licenses
Contacting Support
Appendix: Store Sizing Guidelines41

## 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, onpremise 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 <u>enter your AWS account details</u> while <u>deploying your</u> <u>instance's Management Console</u>.

You can find your account's Access Keys on the <u>AWS Management Console</u> as described below. Secret Keys **cannot** be accessed via the console; they are **only** accessible when an access key is created (see

<u>https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_credentials\_access-keys.html</u> 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:

aws Services V	Ç Gregon ▼ Support ▼
AWS Management Console	My Account 903575212390 My Organization My Service Quotas
AWS services	My Billing Dashboard Stay connecte the-go My Security Credentials
Find Services You can enter names, keywords or acronyms. Q. Example: Relational Database Service, database, RDS	Download Sign Out ur iOS or Android mobile device, cean more to
▼ All services () Security,	dentity, & Explore AWS
EC2 Ground Station Complian Lightsail [2] IAM Lambda இ Quantum Resource A Batch Technologies Manager Elastic Beanstalk Amazon Braket Cognito	Amazon Redshift       ccess     Fast, simple, cost-effective data warehouse that can extend queries to your data lake. Learn more 🖸
Serverless Application Secrets Ma Serverless Application GuardDuty Repository Management & GuardDuty AWS Outposts Governance Inspector EC2 Image Builder AWS Organizations Amazon M	nager     Run Serverless Containers with AWS Fargate       AWS Fargate runs and scales your containers without having       acie     to manage servers or clusters. Learn more
Feedback English (US) 🔻	© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

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

aws Services ▼					¢	-	▼ Global ▼ Su	uppoi				
Identity and Access	Vour Securit	y Credentials										
Dashboard	Use this page to manage . To learn more about the	the credentials for your AWS ac	count. To manage credentials for AWS w they're used, see AWS Security Cre	Identity and A	ccess Manag S General Re	jement (IA ference.	M) users, use the IAM Co	onso				
Groups	▲ Password											
Users	▲ Multi-factor authentication (MFA)											
Roles	<ul> <li>Arress keys (arress key ID and serret arress key)</li> </ul>											
Policies		· Miress vens (arress ven in and serier arress ven)										
Identity providers	Use access keys to m	Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, the AWS SDKs, or direct AWS API calls. You can have a										
Account settings	maximum of two acce	ess keys (active or inactive) at a	time. Learn more									
	Created	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions					
Access analyzer	Jan 29th 2019		2019-01-29 16:15 UTC+0530	us-west-1	ec2	Active	Make Inactive   Delete	Э				
Archive rules												
Analyzers	Create New Acces	ss Key										
Settings												
Credential report	IAM user with lim	ited permissions and generating	access keys for that user instead. Lea	eed long-term arn more	access Keys,	we recom	mena creating a new					
Organization activity												
*												

- 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 <a href="https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_credentials\_access-keys.html#Using\_CreateAccessKey">https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_credentials\_access-keys.html#Using\_CreateAccessKey</a> 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 <u>https://console.aws.amazon.com/ec2/</u>.
- 2. From the dashboard console choose Launch Instance dropdown and select Launch Instance from the dropdown:

aws Services 🔻						A Ravender Goyal ▼ Oregon ▼ Support ▼
New EC2     Experience     Tell us what you think	<b>^</b>	Resources			C 0	Account attributes C
EC2 Dashboard New Events New		You are using the following Amazon EC2 resources in t	he US West (Oregon) Region:			Supported platforms 🗹
Tags		Running instances 1	Elastic IPs	5	Dedicated Hosts 0	VPC Default VPC
Limits		Snapshots 54	Volumes	3	Load balancers 0	none
<ul> <li>Instances</li> <li>Instances New</li> </ul>		Key pairs 65	Security groups	1921	Placement groups 0	EBS encryption
Instance Types Launch Templates Spot Requests		Easily size, configure, and deploy Microsoft SQL	. Server Always On availabilit	y groups on AWS using the A	WS Launch Wizard for SQL Server. Learn more X	Zones Default credit specification Console experiments
Savings Plans Reserved Instances Dedicated Hosts New		Launch instance		Service health	C Service Health Dashboard 🛽	Additional information [2]
Scheduled Instances Capacity Reservations		To get started, launch an Amazon EC2 instance, which cloud.	is a virtual server in the	Region US West (Oregon)	Status This service is operating normally	Getting started guide Documentation
▼ Images AMIs	-	Launch instance US West (Orego	n) Region	Zone status		All EC2 resources Forums Pricing
Elastic Block Store     Volumes		Scheduled events	C	Zone	Status	Contact us
Snapshots				us-west-2a (usw2-az2)	⊘ Zone is operating normally	
Lifecycle Manager		US West (Oregon) No scheduled events		us-west-2b (usw2-az1)	Zone is operating normally	
Network & Security     Security Groups New				us-west-2c (usw2-az3)	Zone is operating normally	
Feedback English (US) 🔻	•			us-west-20 (uSw2-az4)	© zone is operating normally	Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

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**.

aws	Services 🔻						🗘 🔻 Orego	n 🔻 Support 🔻			
1. Choose	AMI 2. Choose Instance Type	3. Configure Instance	4. Add Storage 5.	Add Tags 6. Configure	Security Group 7. Review						
Step 2 Amazon E0 and give yo	Choose an Instan provides a wide selection of ir u the flexibility to choose the app	ICE Type Instance types optimiz propriate mix of resou	ed to fit different use cas irces for your application	es. Instances are virtual s s. Learn more about inst	ervers that can run applications.	They have varying combinations of t your computing needs.	CPU, memory, storage, and netwo	orking capacity,	*		
Filter by:	All instance types 🔹	Current generation	Show/Hide Colu	mns							
Currently	selected: t2.xlarge (Variable E	CUs, 4 vCPUs, 2.3 G	Hz, Intel Broadwell E5-2	686v4, 16 GiB memory, E	BS only)						
	Family	т Туре т	vCPUs (j) -	Memory (GiB) -	Instance Storage (GB) () -	EBS-Optimized Available () -	Network Performance (i) 👻	IPv6 Support (i)			
	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes			
	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes			
	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes			
	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes			
	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes			
	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes			
	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes			
	Cancel Previous Review and Launch Next: Configure Instance Details										
Feedback	English (US) 🔻				© 200	8 - 2020, Amazon Web Services, Inc. or its a	affiliates. All rights reserved. Privacy	Policy Terms of Us	se		

aws	Services 🔻										¢		▼ Oregon ▼	Support 🔻
Choose AMI	2. Choose Instance Type	3. C	onfigure Instance	4. Add Storage	5. Add Tags	6. Confi	gure Security G	roup 7. Revie	sw.					
Step 3: ( onfigure the	Configure Instan	ce D	<b>)etails</b> You can launch m	ultiple instances f	from the same AM	I, reques	st Spot instan	ces to take adv	antage of the low	er pricing, assig	n an access m	anagement role to	the instance, ar	nd more.
	Number of instances	(i)	1		Launch into Aut	o Scaling	g Group 🕕							
	Purchasing option		C Request Spo	ot instances										
	Network	()	vpc-28e77d4d No default VPC	SurelineVPC found. Create a	new default VPC	4	C Create n	ew VPC	1					
	Subnet	()	subnet-13520fi 203 IP Address	76   SantoshSubr es available	net   us-west-2b	4	Create n	ew subnet	2					
	Auto-assign Public IP	()	Enable			4			3					
	Placement group Capacity Reservation	() ()	Open	e to placement gro	oup	4								
	Domain join directory	(i)	No directory			\$	C Create r	new directory						
	IAM role		None			4 (	C Create n	ew IAM role						
	Shutdown behavior	()	Stop			4								
S	Stop - Hibernate behavior		Enable hiber	nation as an addi	itional stop behavi	or				Cancel	Previous	Review and L	aunch	t: Add Storag
eedback	English (US) 🔻								© 2008 - 2020, /	Amazon Web Servic	es, Inc. or its affilia	tes. All rights reserved.	Privacy Polic	y Terms of L

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 <u>"Configuring Firewall Rules"</u> 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:

rage options in Amaz	ion EC2.					- Throughput	Delete on	
olume Type (j)	Device ()	Snapsnot (j)	Size (GIB)	volume Type (1)	IOP:	(MB/s) (	Termination (j)	Encryption ()
oot	/dev/sda1	snap-0791d256b38159c1f	127	Magnetic (standard)	✓ 100 /	/ 3000 N/A		Not Encrypted

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:

aws	Services 🔻											¢	Ravender Goyal 🔻	Oregon 🔻	Support	•
1. Choose AMI	2. Choose	Instance Type 3. C	Configure Instance	4. Add Storage	5. Add Tags	6. 0	Configure Security Group	7. Review								
Step 4: A Your instance we edit the settings storage options	dd Stora vill be launche s of the root ve in Amazon E	age id with the following olume. You can also C2.	storage device set attach additional f	ttings. You can a EBS volumes af	attach additional ter launching an	I EBS vo n instanc	olumes and instance sto e, but not instance stor	re volumes e volumes.	to you Learn	r instance, or more about						
Volume Type	()	Device (j)	Snapshot (j)		Size (GiB) (i)		Volume Type 🕕			IOPS (j)	Throughput (MB/s) ()		Delete on Termination ()	Encryption	0	
Root		/dev/sda1	snap-0791d256	b38159c1f	127	(	General Purpose SSD	(gp2)	~	381 / 3000	N/A		2	Not Encrypte	d 🔻	
EBS	~	/dev/sdb ∨	Search (case-in	nsensit	1024	(	Magnetic (standard)		~	N/A	N/A		2	Not Encrypte	d 🔻	⊗
Add New Vol	ume	ers can get up to 30	GB of EBS Gener.	al Purpose (SSI	D) or Magnetic st	storage.	Learn more about free	usage tier e	ligibili	ty and	Cancel	Previou	s Review and L	aunch	xt: Add T	fags
Feedback Er	nglish (US) 🔻								© 20	08 - 2020, Amazon <sup>1</sup>	Web Services, Inc. o	r its affiliat	es. All rights reserved.	Privacy Policy	Terms o	of Use

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, "<u>Appendix</u>" 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

aws Se	ervices 🔻								÷	Ravender Goyal 🔻	Oregon 🔻	Support 🔻
1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review						
Step 5: Ad A tag consists of a A copy of a tag ca Tags will be applie	Id Tags a case-sensitive key-value an be applied to volumes, i ed to all instances and volu	pair. For example, you instances or both. umes. Learn more abo	could define a ta ut tagging your Ar	g with key = Na mazon EC2 res	ame and value = Webserver.							
Key (128 cha	aracters maximum)		v	<b>/alue</b> (256 c	haracters maximum)			Instance	s () Vo	olumes (j)		
				This resource of	currently has no tags							
			Choose th Make sure you	ne Add tag butto ur IAM policy in	on or click to add a Name tag ncludes permissions to create	g. e tags.						
Add Tag	50 tags maximum)											
							Cancel	Previous	Review ar	nd Launch Next	: Configure Se	ecurity Group
Feedback Engl	lish (US) 🔻						© 2008 - 2020, Am	azon Web Service:	s, Inc. or its affilia	tes. All rights reserved.	Privacy Policy	Terms of Use

the Add Tags page is displayed:

aws Services 🔻			Ş	▼ Oregon ▼	Support 🔻
1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Store	age 5. Add Tags 6. Configure Security Group 7. Review				
Step 5: Add Tags A tag consists of a case-sensitive key-value pair. For example, you could define A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. Learn more about tagging yo	e a tag with key = Name and value = Webserver. our Amazon EC2 resources.				
Key (128 characters maximum)	Value (256 characters maximum)	Instances ()	Volumes (j)		
Name	SUREedge-Store			8	
Add another tag (Up to 50 tags maximum)					
	Cance	Previous	Review and Launch	Next: Configure Se	curity Group
Feedback English (US) 🔻	© 2008 - 2020, #	mazon Web Services, Inc.	or its affiliates. All rights rese	rved. Privacy Policy	Terms of Use

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 "<u>Configuring Firewall Rules</u>":-

aws Services V				
1. Choose AMI 2. Choose Instance Typ	e 3. Configure Instance 4. Add	Storage 5. Add Tags 6. Configure Security G	roup 7. Review	
Step 6: Configure Secu A security group is a set of firewall rule: reach your instance, add rules that allo Assign a security	trity Group that control the traffic for your insta w unrestricted access to the HTTP a group: ○ Create a new security g ● Select an existing secu	nce. On this page, you can add rules to allow sp ind HTTPS ports. You can create a new security ; roup rrity group	wific traffic to reach your instance. For example, if group or select from an existing one below. Learn	'you want to set up a web server and allow Internet traffic to more about Amazon EC2 security groups.
Security Group ID	Name		Description	Actions
sg-c26aa8a6	default		default VPC security group	Copy to new
sg-03a0c4c1d3e52c018	nitin-6-1-sec-group		launch-wizard-18 created 2020-07-03T06:25:5	59.530-07:00 Copy to new
sg-000d61389a7534966	proxy-7bbdd1e7-e2ac-11ea-9a	ff-02511fe82171-default	SUREEdge default security group	Copy to new
sg-0689129b5d7745fa4	SUREedge-Security-Group		Security Group for SUREedge	Copy to new
Inbound rules for sg-0689129b5d77	45fa4 (Selected security groups:	sg-0689129b5d7745fa4) **** Port Range (j	Source ()	Description ()
HTTP	TCP	80		
Custom ICMP Rule - IPv4	Echo Reply	N/A		
SSH	TCP	22		-
				Cancel Previous Review and Launch
Feedback English (US) 🔻			© 2008 - 2020, Amazon Web Services,	Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

When the security group settings are completed click  $\ensuremath{\text{Review}}$  and  $\ensuremath{\text{Launch.}}$ 

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

av	/S Services ▼							\$	▼ Oregon ▼	Support v
1. Cho	ose AMI 2. Choose In	istance Type	3. Configure Instan	oe 4. Add Storage 5	Add Tags 6. Configure Security Group	7. Ravlew				
Step Please	7: Review In review your instance la	istance Li sunch details. Y	aunch ou can go back t	edit changes for each se	ection. Click Launch to assign a key pair	to your instance and complete the launch	process.			*
- AN	11 Details									Edit AMI
	Ubuntu Server     Ubuntu Server     Igible Root Device Type	ver 16.04 LTS 16.04 LTS (HVN ebs Vituelizeti	(HVM), SSD Vo ),EBS General Pu in type: hvm	lume Type - ami-003ba rpose (SSD) Volume Type.	a08113592046f Support available from Canonical (http://ww	w.ubuntu.com/cloud/services).				- 1
	tance Type								Edit inst	tance type
1	nstance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance			
1	2.xlarge	Variable	4	18	EBS only	•	Moderate			
▼ Se	curity Groups								Edit secu	ity groups
Se De	curity group name scription	launch-w launch-w	vizard-48 vizard-48 created	2020-10-13T15:33:49.75	56+05:30					- 1
1	ype ()		Protocol (j)		Port Range ()	Source ()	Description ()			
-	SH		TCP		22					
► Ins	tance Details								Edit instar	nce details
In State	orage								E	dit storage
I Ta	gs									Edit tags
										- 1
<b></b>									Cancel Previou	s Launch
Fredb	rck Foolish (US) 💌							6 2008 - 2020 Amazon Web Services Inc. or its attiliates All rights reser	ed Privary Policy	Terms of like

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:

Select	an existing key pair or create a new key pair	×
A key pair of allow you to obtain the p securely SS	consists of a public key that AWS stores, and a private key file that you store. Together o connect to your instance securely. For Windows AMIs, the private key file is required to bassword used to log into your instance. For Linux AMIs, the private key file allows you t SH into your instance.	r, they o
Note: The s about remo	elected key pair will be added to the set of keys authorized for this instance. Learn more oving existing key pairs from a public AMI.	•
Create Key pa	a new key pair 🔹 🔪	2 🔶
	Download Key Pair	] 🔶
•	You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.	
	Cancel Launch Instance	

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.

aws Services V			↓ Oregon ▼ Support ▼
New EC2 Experience Tell us what you think	Instances (1/2) Info		C Actions A Launch instances View details
EC2 Dashboard New			Connect
Events New	■ Name ▼ Instance ID	Instance state $\  \  \nabla$ Instance type $\  \  \nabla$ Status check	Alar Get Windows password Public
Tags	sups-client1 i-05351a5caacbbb3a8	Terminated t2.medium -	No a <u>Greate template from instance</u>
Limits	✓ sureedge-store i-05bbb9077de417ce9	Running t2.xlarge Ø 2/2 checks	No alarms + us-west-2b ec2-35-
▼ Instances		=	
Instances New	Instance: i-05bbb9077de417ce9 (sureedge-store)		
Instance Types			
Launch Templates	Details Security Networking Storage	Status Checks Monitoring Tags	
Spot Requests			
Savings Plans	Instance summary Info		
Reserved Instances	Instance ID	Public IPv4 address	Private IPv4 addresses
Dedicated Hosts New	i-05bbb9077de417ce9 (sureedge-store)	35.167.64.38   open address	□ 10.0.0.33
Scheduled Instances	Instance state	Public IPv4 DNS	Private IPv4 DNS
Capacity Reservations	⊘ Running	ec2-35-167-64-38.us-west-	ip-10-0-0-33.us-west-2.compute.internal
▼ Images		2.compute.amazonaws.com   open address	
AMIs	Instance type	Elastic IP addresses	VPC ID
▼ Elastic Block Store	t2.xlarge	-	🗇 vpc-28e77d4d (SurelineVPC) 🔀
Volumes 👻	IAM Role	Subnet ID	-
Feedback English (US) 🔻		© 2008 - 2020, Amazon Web Se	rvices, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

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

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

aws	Services 🔻	\$ <b>*</b>	Oregon 🔻	Support 🔻
Ξ	Connect to instance Info Connect to your instance I-05bbb9077de417ce9 (sureedge-store) using any of these options			4
	EC2 Instance Connect Session Manager SSH client			
	Instance ID  I +05bb59077de417ce9 (sureedge-store)  O pen an SSH client.  C Locate your private key file. The key used to launch this instance is sureedge-01.pem  R un this command, if necessary, to ensure your key is not publicly viewable.  C chmod 400 sureedge-01.pem  C connect to your instance using its Public DNS: C ec-35-167-64-38.us-west-2.compute.amazonaws.com  Example: C ssh -1 "sureedge-01.pem" ubuntu@ec2-35-167-64-38.us-west-2.compute.amazonaws.com  Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if			
	Cancel		Pairana Palina	v Tamma ofilio
https://us-we	st-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#	© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.	Privacy Policy	Terms of Use

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 <u>launching the Linux</u> <u>instance</u> (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 ("=").

ubuntu@ip-10-0-0-27:~\$
ubuntu@ip-10-0-0-27:~\$ sudo adduser sureline
Adding user `sureline'
Adding new group `sureline' (1001)
Adding new user `sureline' (1001) with group `sureline' .
Creating home directory `/home/sureline'
Copying files from `/etc/skel'
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for sureline
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] Y
ubuntu@ip-10-0-0-27:~\$

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
<pre># 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</pre>
# 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
<pre># Change to no to disable tunnelled clear text passwords PasswordAuthentication yes</pre>
# 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
<pre>sureline@ip-10-0-0-27:~\$ sureline@ip-10-0-0-27:~\$ sureline@ip-10-0-0-27:~\$ sureline@ip-10-0-0-27:~\$ sureline@ip-10-0-0-27:~\$ sureline@ip-10-0-0-27:~\$ uservice - OpenBSD Secure Shell server Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled) Drop-In: /usr/lib/systemd/system/ssh.service.d Lec2-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)</pre>
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 L95487 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 -0 ./SUREedgeLinuxAWSPackage.tar.gz <u>https://sure-builds.s3-us-</u>
west-1.amazonaws.com/dr/661/GA/SUREedgeLinuxAzurePackage.tar.gz
<pre>sureline@ip-172-31-31-28:~\$ cd /home/sureline/ sureline@ip-172-31-31-28:~\$ wget -0 ./SUREedgeLinuxAWSPackage.tar.gz <u>https://sure-builds.s3-us-west-1.amazonaws.com/ dr/661/GA/SUREedgeLinuxAzurePackage.tar.gz</u> 2021-08-10 07:54:29 <u>https://sure-builds.s3-us-west-1.amazonaws.com/dr/661/GA/SUREedgeLinuxAzurePackage.tar.gz</u> 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'</pre>
./SUREedgeLinuxAWSPackage.ta 100%[===================================
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**

 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.tar.gz
./surestor-linux7-installer.tar.gz
./surestor-linux7-installer.tar.gz
```

sudo chmod 755 install\_sureedge\_store.sh
sudo bash install\_sureedge\_store.sh AWS

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



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 (/LLD/Systemd/system/surestor.service; enabled; vendor preset: enabled)
Active: active (running) since rue 2021-06-10 06:10:51 off; /min ago
Math Fill: 32000 (Sh)
Marray 4 (Cimit: 19200)
Coroup: /system.stice/surestor.service
-92008 /Din/sn -C /Opt/Sureline/Sureage/Din/Surestor >> /Var/Sureline/Sureage/Log/Surestor_stdout.ls
—92010 /opt/suretine/sureage/bin/surestor
Aug 10 00:10:21 in 172 21 21 20 sustand[1]. Starting SureStar Carvar
Aug 10 00:10:51 $(p-1/2-51-51-20)$ systemu[1]: Startug surestor server
Aug 10 06:10:31 (p-1/2-31-31-26 Surescor-pre-start.sh[91966]; /pt/Surettne/Sureeuge/bth/Surescor-pre-start.sh; tth
Aug 10 00:10:51 (p-1/2-51-51-20 Surestor-Post-Starts (151/92005); Started the Surestore Server
Aug 10 08:10:31 (p-1/2-31-31-20 systema[1]: Started Surestor Server.
Aug 10 08:10:31 tp-1/2-31-31-28 systemd 1]: /ltb/systemd/system/surestor.service:14: Unknown key name 'StartLimitin>
Aug 10 08:10:31 tp-1/2-31-31-28 systemd1]: /ltb/systemd/system/surestor.service:14: Unknown key name 'StartLimitin>
Aug 10 08:10:31 up-172-31-31-28 systemd[1]: /lub/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, "<u>Contacting Support</u>" 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 Windowsbased 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.

dws Services V			A Ravender Goyal ▼ Oregon ▼ Support ▼		
New EC2 Experience Tell us what you think	Resources	Account attributes			
Events New	You are using the following Amazon EC2 resources in the US West (Oregon) Regio	n:	Supported platforms 🔀		
Tags	Running instances 1 Elastic IPs	5 Dedicated Hosts 0	VPC Default VPC 12		
Limits	Snapshots 54 Volumes	3 Load balancers 0	none		
▼ Instances	Key pairs 65 Security groups	1921 Placement groups 0	Settings EBS encryption		
Instance Types			Zones		
Launch Templates	Easily size, configure, and deploy Microsoft SQL Server Always On availability	lity groups on AWS using the AWS Launch Wizard for SQL Server. Learn more	Default credit specification		
Spot Requests Savinos Plans			Console experiments		
Reserved Instances Dedicated Hosts New	Launch instance	Service health C Service Health Dashboard 🖪	Additional information 🖸		
Scheduled Instances Capacity Reservations	To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.	Region Status US West (Oregon) © This service is operating normally	Getting started guide Documentation		
▼ Images AMIs	Launch Instance  US West (Oregon) Region Launch instance from template	Zone status	All EC2 resources Forums Define		
Elastic Block Store		Zone Status	Contact us		
Snapshots	Scheduled events C	us-west-2a (usw2-az2)			
Lifecycle Manager	US West (Oregon)	us-west-2b (usw2-az1)			
▼ Network & Security	No scheduled events	us-west-2c (usw2-az3)			
Security Groups New 🔻		us-west-2d (usw2-az4) 📀 Zone is operating normally			

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:

aws Services ▼	\$	▼ Oregon ▼ Support ▼
1. Choose AMI 2. Choose Insta	ance Type 3. Configure Instance 4. Add Storage 5. Add Tags 8. Configure Security Group 7. Review	
Step 1: Choose an A An AMI is a template that contains AMIs.	Amazon Machine Image (AMI) is the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the	Cancel and Exit AWS Marketplace; or you can select one of your own
Q. Microsoft Windows Server 20	019 Base	X Search by Systems Manager parameter
Quick Start (2)		< < 1 to 2 of 2 AMIs > >
My AMIs (0) AWS Marketplace (21)	Microsoft Windows Server 2019 Base - ami-0afb7a78e89642197 Windows     Microsoft Windows 2019 Datacenter edition. [English]     Free for eligible     Root device type: ebs     Vinalization type: htm. EVAEnabled Yas	Select 64-bit (x86)
Community AMIs (96)	Microsoft Windows Server 2019 Base with Containers - am-U285c5f8fbbdbd498     Windows     Microsoft Windows 2019 Datacenter edition with Containers. [English]     Texe star eligible     Roof device type ebs Vinalization type hvm ENA Enabled Yes	Select 64-bit (x86)
	The following results for "Microsoft Windows Server 2019 Base" were found in other catalogs: 21 results in AWS Marketplace AVS Marketplace privides partnered Software that is pre-configured to run on AWS 3 96 results in Community AMIs Community AMIs are AMIs that are shared by the general AWS community	
Feedback English (US) 🔻	© 2008 - 2020, Amazon Web Services, Inc. or its affili	iates. All rights reserved. Privacy Policy Terms of Use

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):

aws	Services 🔻						Ç ▼ Or	egon 🔻 Support 🔻
1. Choose	AMI 2. Choose Instance Type 3. C	onfigure Instance 4. A	dd Storage 5. Add Tags	6. Configure Security Group	7. Review			
Step 2: Choose an Instance Type Imazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose a he appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs. Filter by: All instance types V Current generation V Show/Hide Columns								
Current	ly selected: t2.large (Variable ECUs, 2	vCPUs, 2.3 GHz, Intel E	Broadwell E5-2686v4, 8 GiB	memory, EBS only)				
	Family ~	Туре –	vCPUs () -	Memory (GiB) v	Instance Storage (GB) () -	EBS-Optimized Available () 🔹	Network Performance () *	IPv6 Support
	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
	General purpose	t2.micro Free tier eligible	1	1	EBS only		Low to Moderate	Yes
	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
Cancel Previous Review and Launch Next: Configure Instance Details								
Feedback	English (US) 🔻					© 2008 - 2020, Amazon Web Services,	Inc. or its affiliates. All rights reserved. Prive	acy Policy Terms of Use

Click Next: Configure Instance Details.

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

aws	Services 🔻	👃 🔹 Oregon 💌	Support 🔻						
1. Choose A	MI 2. Choose Instance Type	Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review							
Step 3: Configure th	Step 3: Configure Instance Details Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.								
	Number of instances () 1 Launch into Auto Scaling Group ()								
	Purchasing option	Request Spot instances							
	Network	(vpc-28e77d4d   SurelineVPC         I           No default VPC found. Create a new default VPC.         1							
	Subnet	subnet-13520176   SantoshSubnet   us-west-2b  Create new subnet							
	Auto-assign Public IP	Enable 3							
	Placement group	Add instance to placement group							
	Capacity Reservation	Open 🔹							
	Domain join directory	No directory C Create new directory							
	IAM role	None C Create new IAM role							
	Shutdown behavior	(Stop 4							
	Stop - Hibernate behavior	Enable hibernation as an additional stop behavior	-						
		Cancel Previous Review and Launch Next: A	dd Storage						
Feedback	English (US) 🔻	© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy	Terms of Use						

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, "<u>Configuring Firewall Rules</u>" 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:

aws Ser	vices 🔻							¢	Ravender Goyal 🔻	Oregon 🔻	Support 🔻
1. Choose AMI	2. Choose Instance Type	3. Configure Instance 4. Add Storag	e 5. Add Tags 6	6. Configure Security Group	7. Review						
Step 4: Add Your instance will be edit the settings of storage options in A	d Storage be launched with the follow the root volume. You can a Amazon EC2.	ing storage device settings. You car also attach additional EBS volumes a	attach additional EBS after launching an insta	volumes and instance stor nce, but not instance store	e volumes to you volumes. Learn	ur instance, or more about					
Volume Type (j	Device ()	Snapshot (j)	Size (GiB) (j)	Volume Type 🕧		IOPS ①	Throughput (MB/s) (j	Delet Term	te on ination (j)	Encryption (	D
Root	/dev/sda1	snap-06bc3b2a14fed97aa	127	General Purpose SSD	gp2) 🗸	100 / 3000	N/A	<ul> <li>✓</li> </ul>		Not Encrypted	•
Add New Volum	e le customers can get up to ons.	30 GB of EBS General Purpose (S	SD) or Magnetic storage	e. Learn more about free	usage tier eligibil	ity and					
							Cancel	Previous	Review and L	aunch	ct: Add Tags
Feedback Englis	sh (US) 🔻				© 20	108 - 2020, Amazo	n Web Services, Inc.	or its affiliates.	All rights reserved.	Privacy Policy	Terms of Use

#### Click Next: Add Tags.

 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:

aws Services 🔻		👌 Ravender Goyal 🔻 Oregon 🔻 Support 🔻
1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Sto	rage 5. Add Tags 6. Configure Security Group 7. Review	
Step 5: Add Tags A tag consists of a case-sensitive key-value pair. For example, you could defin A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. Learn more about tagging y	ie a tag with key = Name and value = Webserver. /our Amazon EC2 resources.	
Key (128 characters maximum)	Value (256 characters maximum) Instances ()	Volumes ()
Che Make su Add Tag 🌪 50 tags maximum)	This resource currently has no tags bose the Add tag button or click to add a Name tag. Ire your IAM policy includes permissions to create tags.	
	Cancel Previous Re	view and Launch Next: Configure Security Group
Feedback English (US) 🔻	© 2008 - 2020, Amazon Web Services, Inc. or	its affiliates. All rights reserved. Privacy Policy Terms of Use

Click once on the Add Button, the Add Tags page is displayed:

aws Services 🔻		¢	▼ Oregon ▼ Support ▼
1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storag	ge 5. Add Tags 6. Configure Security Group 7. Review		
Step 5: Add Tags A tag consists of a case-sensitive key-value pair. For example, you could define A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. Learn more about tagging yo	e a tag with key = Name and value = Webserver. vur Amazon EC2 resources.		
Key (128 characters maximum)	Value (256 characters maximum)	Instances (j) Volumes (j)	1
Name	sureline-mc	] 🛛 🖸	8
Add another tag (Up to 50 tags maximum)			
	Cancel	Previous Review and Launch	Next: Configure Security Group
Feedback English (US) 🔻	© 2008 - 2020, Am	azon Web Services, Inc. or its affiliates. All rights res	served. Privacy Policy Terms of Use
Horo you can onter the Koy and	d Value for the tag. For examp		fino o

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, "<u>Configuring Firewall Rules</u>":-

aws Ser	rvices 🔻						¢	▼ Oregor	n ♥ Support ♥
1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review			
Step 6: Co A security group is reach your instance	a set of firewall rules that ce, add rules that allow ur Assign a security gro	ty Group at control the traffic for y prestricted access to the oup: O Create a new s Select an exist	our instance. On th HTTP and HTTPs ecurity group ing security group	nis page, you ca S ports. You car	an add rules to allow specific tr n create a new security group o	affic to reach your instance. F or select from an existing one	or example, if you want to set up a w below. Learn more about Amazon EC	eb server and allow l 22 security groups.	internet traffic to
Security	Group ID	Name			E	Description			Actions
sg-c26aa8a	16	default			de	fault VPC security group			Copy to new
sg-03a0c4c	1d3e52c018	nitin-6-1-sec-group			lau	inch-wizard-18 created 2020-	D7-03T06:25:59.530-07:00		Copy to new
sg-000d613	89a7534966	proxy-7bbdd1e7-e2ac	11ea-9aff-02511fe	82171-default	SL	SUREEdge default security group			Copy to new
<b>sg-0689129</b>	05d7745fa4	SUREedge-Security-G	roup		Se	curity Group for SUREedge			Copy to new
Inbound rules for	or sg-0689129b5d7745fa	14 (Selected security o	roups: sg-068912	29b5d7745fa4)	0.0.0				
Type (i)		Protocol (i)		Por	t Range (j)	Source (i)	Descri	ption (i)	
HTTP		TCP		80					
Custom ICMP R	ule - IPv4	Echo Reply		N/A					
SSH		TCP		22					-
							Cancel	Previous	eview and Launch
Feedback Engli	ish (US) 🔻					© 2008 - 2020, Amaz	on Web Services, Inc. or its affiliates. All rights	reserved. Privacy F	Policy Terms of Use

#### Click Review and Launch.

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

aws	Services											÷ •	Oregon V	Support V
1. Choose AM	/I 2. Choose Instar	nce Type	3. Configure Instance	4. Add Storage	5. Add Tags 6.	Configure Security Group	7. Review							
Step 7: Please review	Review Inst w your instance laun	ch details. )	.aunch /ou can go back to	edit changes for eac	h section. Click Laur	nch to assign a key pair	r to your instance and	complete the launch	process.					ĺ
▼ AMI De	etails													Edit AMI
Free tier eligible If you pla	Microsoft Windows Root Device Type: eb an to use this AMI for e ce Type	Iows Serve s 2019 Datac s Virtualizat an application	er 2019 Base - an center edition. [Englis fon type: hvm n that benefits from N	ni-Oafb7a78e89642 sh] Microsoft License Mobi	197 lity, fill out the License	t Mobility Form. Don't sh	row me this again						Edit ins	tance type
Instan	псе Туре	ECUs	vCPUs	Memory (GiB)	Instance Sto	rage (GB)	EBS-Optimized A	vailable	Network Performance					
t2.larg	e	Variable	2	8	EBS only				Low to Moderate					
<ul> <li>Securit</li> </ul>	ty Groups												Edit secu	rity groups
Secur	ity Group ID			Name			Descripti	ion						
sg-0689	129b5d7745fa4			SUREedge-Security	-Group		Security Gr	oup for SUREedge						
All sele	cted security group	os inbound	rules											
Type	(i)		Protocol (i)		Port Range		Source (i)		Description (i)					
												Canc	Previou	s Launch
Feedback	English (US) 🔻								© 20	008 - 2020, Ama	azon Web Services, Inc. or its a	ffiliates. All rights reserved.	Privacy Policy	Terms of Use

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.

aws, Services 🔻			Qregon ▼ Support ▼
New EC2     Experience     Tell us what you think     EC2 Dashboard New	Instances (1/2) Info Q. Filter instances		C Actions A Launch Instances V View details
Events New Tags Limits	Name         v         Instance ID         Instance state           suredge-store         I-05bbb9077de417cc9         Ø Running           sureine-store         I-0eba1169734f3663c         Ø Running		Availability zone         Public IPw         Get Windows password         Elastic Ip           rs-vest-2b         ec2-35-16;         Create template from instance         -           s-vest-2b         ec2-45-200-166-179 u         54.200.168.179         -
▼ Instances	₹		•
Instances New Instance Types Launch Templates	Instance: i-Oeba1fd9734f3d63c (sureline-store)	=	
Spot Requests Savings Plans Reserved Instances	Details Security Networking Storage Status Chec      Instance summary Info	ks Monitoring Tags	
Dedicated Hosts New Scheduled Instances Capacity Reservations	Instance ID D i-Oeba1fd9734f3d63c (sureline-store)	Public IPv4 address D 54.200.168.179   open address Z	Private IPv4 addresses
▼ Images AMIs	Instance state Ø Running	Public IPv4 DNS D ec2-54-200-168-179.us-west-2.compute.amazonaws.com   open address 2	Private IPv4 DNS
<ul> <li>Elastic Block Store</li> <li>Volumes</li> </ul>	Instance type t2.large	Elastic IP addresses -	VPC ID D vpc-28e77d4d (SurelineVPC)
Snapshots Lifecycle Manager	IAM Role	Subnet ID  Subnet-13520f76 (SantoshSubnet)	
Network & Security     Security Groups New	▼ Instance details Info		•
Feedback English (US) 🔻		6 20	08 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

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

 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:

Connect to instance Connect to your instance i-0	Connect to instance Info Connect to your instance i-Oeba1fd9734f3d63c (sureline-store) using any of these options					
Session Manager RDP client						
You can connect to your running the RDP shortco	You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:					
Download remote o	lesktop file					
When prompted, conne	ct to your instance using the follo	wing details:				
Public DNS		User name				
🗇 ec2-54-200-168-1	79.us-west-	Administrator				
2.compute.amazonaws.	:om					
Password Get password						
If you've joined your ins	ance to a directory, you can use y	your directory credentials to connect to your 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:

aws	Services 🔻			Ą	Ravender Goyal 🔻	Oregon 🔻	Support 🔻
=	EC2 > Instances > i-Oeba1fd9734f3d63c > Get windows password						<b>^</b>
	Get Windows password Info Retrieve and decrypt the initial Windows administrator password for this instance.						
	To decrypt the password, you will need your key pair for this instance.						
	Key pair associated with this instance sureline_02						
	Browse to your key pair:						
	Or copy and paste the contents of the key pair below:						
		Cancel	Decrypt Password				
Feedback	English (US) 🔻			© 2008 - 2020, Amazon Web Services, Inc. or its affil		Privacy Policy	Terms of Use

 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.

aws	Services 🔻	¢	Ravender Goyal 🔻	Oregon 🔻	Support 🔻
=	EC2 > Instances > i-0eba1fd9734f3d63c > Get windows password				
	Get Windows password Info Retrieve and decrypt the initial Windows administrator password for this instance.				
	To decrypt the password, you will need your key pair for this instance.				
	Key pair associated with this instance				
	Browse to your key pair:				
	Browse				
	⊘pem				
	1.7/8 Or copy and paste the contents of the key pair below:				
	••••••BEGIN RSA PRIVATE KEY-••••         •           MillogiBAACKAQEAhRRUVPMniUhDGpLirBokHms492QU95AdxHWT5u92TDIAF7         •           25:e90673W09s9ghW1L06W04715M23X6mxxXEF70pap9gxR3sHk32LLKAEXKP         •           7/BcCu0fuFEgTTCbVKAR22u9KFBuvmLNi6gH1Xlxcq9Rjd4lEhzUM/TgaJD+etC         •           1(a)Xjh9bg6P0W32Bdc22Jjh83CqAbqaBYXCF98x3C29H12tdod3dKByrcHC010         •           sH2Q4R795k82A4Blb8/4V2AXbpLinBqw0M0H0BgHm1M14madbd8J5ZJ4x         •           WUJHpR/xx4j+JzH3y6pmfn06DC9GTBbK0u4Xjjw1DAQABA0BADDA/5+obr/XF+RG         •           98+g5HV9uJJgnQNxK+6q7E9/aac/LMUMXTaqXIhNTCycFFAbKA7ReGV511M11xb         •				
	Cancel Decrypt Password				
Feedback	English (US) 🔻 (0.2008 - 2020. Amazon Web Servic	es. Inc. or its affiliat	es. All rights reserved.	Privacy Policy	Terms of Use

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

aws	Services V		\$	Ravender Goyal 🔻	Oregon 🔻	Support 🔻
E	2 > Instances > i-Oeba1fd9734f3d63c > Connect to instance					
	Connect to instance Info Connect to your instance i-Oeba1fd9734f3d53c (sureline-store) using any of the	se options				
	Session Manager RDP client					
	You can connect to your Windows instance using a remote desktop of running the RDP shortcut file below:	lient of your choice, and by downloading and				
	Download remote desktop file					
	When prompted, connect to your instance using the following details	5.				
	Public DNS User na	me				
	🗇 ec2-54-200-168-179.us-west-	dministrator				
	Password					
	Vpw1s/TGJEXCJ@%EJmy!CV2MINDV)?Y-2					
	If you've joined your instance to a directory, you can use your directo	ry credentials to connect to your instance.				
		Cancel				
Feedback	English (US) 🔻		© 2008 - 2020, Amazon Web Services, Inc. or its affiliat	tes. All rights reserved.	Privacy Policy	Terms of Use

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.

aws	Services 🔻	🗘 Ravender Goyal 🤊	Oregon ▼	Support 🔻
=	C2 > Instances > i-Oeba1fd9734f3d63c > Connect to instance			
	Connect to instance Info Connect to your instance i-Oeba1fd9734f365c (sureline-store) using any of these options			
	Session Manager RDP client			
	You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:			
	Download remote desktop file			
	When prompted, connect to your instance using the following details:			
	Public DNS User name			
	🗇 ec2-54-200-168-179.us-west- 🗗 Administrator 2.compute.amazonaws.com			
	Password			
	vpwTs7fGjLxcj@%Ejmy!CVzMhbv)?Y-z			
	If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.			
	Cancel			
	Contex			
Feedback	English (US) 🔻	© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.	Privacy Policy	Terms of Use

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

t:	
Windows Security	×
Enter your of These credentia ec2-54-200-168	credentials als will be used to connect to 3-179.us-west-2.compute.amazonaws.com.
	Administrator
	Use another account
Remer	mber my credentials
	OK Cancel

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
```

G Administrator: Command Prompt	-		×
Microsoft Windows [Version 10.0.17763.1879] (c) 2018 Microsoft Corporation. All rights reserved.			^
C:\Users\Administrator≻curl -o C:\SUREedgeWindowsAWSPackage.zip https://sure-builds.s3-us-west-1. /SUREedgeWindowsAzurePackage.zip	amazonaws.com	/dr/66	0/GA
% Total % Received % Xferd Average Speed Time Time Time Current			
100 9397M 100 9397M 0 0 17.1M 0 0:09:09 0:09:09::- 19.7M			
C:\Users\Administrator>_			

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.

← → × ↑ 🖡 > This PC > Local Disk (C:) > SUREedgeWindowsAWSPackage > SUREedgeWindowsAzurePackage						
🛨 Quick access		Name	Date modified	Туре	Size	
	*	👔 SUREedge_Software_Appliance_Installer_For_hyper-v	2/11/2021 3:19 AM	Compressed (zipped)	4,463,115 KB	
		SUREedge_Software_Appliance_Installer_For_vmware	2/18/2021 11:32 AM	Compressed (zipped)	3,782,159 KB	
Documents		$ m complexed P$ SUREedge_Software_Setup	8/9/2021 4:58 AM	Application	1,436,066 KB	
Downloads	×.	SUREedge_Storage_engine_system.azure	8/9/2021 6:09 AM	AZURE File	0 KB	
Pictures	*	🕂 SUREedgeServerUtility	8/9/2021 4:38 AM	Application	27, <b>4</b> 51 KB	
🧢 This PC		version	8/9/2021 4:18 AM	File	1 KB	
🇳 Network						
~						

After extraction of zip file rename the file SUREedge\_Storage\_engine\_system.azure to SUREedge\_Storage\_engine\_system.aws

Name	Date modified	Туре	Size
SUREedge_Software_Appliance_Installer_For_hyper-v	2/11/2021 3:19 AM	Compressed (zipped)	4,463,115 KB
SUREedge_Software_Appliance_Installer_For_vmware	2/18/2021 11:32 AM	Compressed (zipped)	3,782, <b>1</b> 59 KB
SUREedge_Software_Setup	8/9/2021 4:58 AM	Application	1,436,066 KB
SUREedge_Storage_engine_system.aws	8/9/2021 6:09 AM	AWS File	0 KB
	8/9/2021 4:38 AM	Application	27,451 KB
version	8/9/2021 4:18 AM	File	1 KB

#### **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:

- 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:

<i>P</i> SUREedge 6.6.1 Setup	×
License Agreement	0
Please review the license terms before installing SUREedge 6.6.1.	J
Press Page Down to see the rest of the agreement.	
END USER LICENSE AGREEMENT: TERMS AND CONDITIONS OF USE	^
IMPORTANT NOTICE. THIS LICENSE AGREEMENT (THE AGREEMENT) IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AND Persistent Systems, Inc., AND ITS THIRD-PARTY LICENSORS ("Persistent Systems"). BY INSTALLING OR USING THIS SOFTWARE IN ANY WAY YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTOOD AND AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT INSTALL OR USE THIS SOFTWARE IN ANY WAY, AND PROMPTLY RETURN THE SOFTWARE WITH PROOF OF PURCHASE TO THE PARTY FROM WHOM YOU ACQUIRED IT AND OBTAIN A REFUND OF THE AMOUNT YOU PAID, IF ANY. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON	. ~
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install SUREedge 6.6.1.	
< Back I Agree Can	cel

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:

		_		×
Select Product Select Product for SUREedge 6.6.1			(	ſ
Product to be installed :				
<ul> <li>SUREedge Migrator</li> <li>SUREedge DR</li> </ul>				
Persistent Systems - SUREedge				
	< Back N	ext >	Cano	el

#### Click Next.

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

		_		×
AWS Details AWS Identity And Access Management Details.				ീ
Access Key				
Secret key				
Persistent Systems - SUREedge	< Back	Next >	Ca	ncel

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

P SUREedge 6.6.1 Setup		_	-	×
Store Details				P
				0
IP Address				
	]			
Username				
sureline	]			
Password				
	]			
Development Systems SUDSedan				
Persistent bystellis - bokceuge				
	< Back	Next >		Cancel

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:

P SUREedge 6.6.1 Setup	_		×
SUREedge Configuration			ρ
			0
Instance Name (optional)			
SUREedge			
Instance Location (optional)			
SUREedge MC Password For "EC2AMAZ-IEO9MBE\Administrator "			
Persistent Systems - SUREedge			
< Back N	ext >	Car	ncel

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, "<u>Connecting to the MC VM</u>".

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 Consol to evit without installing.

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:

♂ SUREedge 6.6.1 Setup	_		×
Install Installing SUREedge 6.6.1			പ
			<u> </u>
Verification of inputs completed. Click 'Install' to start installation of system.	SUREedge 6	.6.1 on y	our
Persistent Systems - SUREedge	To a to II	6	
< Back	Install	Car	icel

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

SUREedge 6.6.1 Setup	- 🗆 🗙	
<b>Installing</b> Please wait while SUREedge 6.6.1 is being installed.	ீ	
Execute: "C:\SureEdgePre-Requisites Setup.exe"		
Preparing store machine Installing SUREedg Installing required Output folder: C: Extract: SureEdge Execute: "C: \SureEdgePre-Requisites Setup.exe"		
Persistent Systems - SUREedge	> Cancel	

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: (<u>https://localhost/sureedge/index.php/</u>). 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:

DISASTER RECOVERY Protect business-critical applications on any virtual, container, or physical server with SUREedge DR to any cloud or to a remote site.	Persistent
E Register	Username
Protect	Password
	Log in
For more information see the Getting Started Guide	

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

P Persistent			Aug 10, 2021 3:39 PM Administrator ~
먦 Dashboard 🛛 🗮 Register 😯 Pro	otect 🖸	Recover 🙋 Jobs 😰 Reports 🎄 Settings	
భ్రు Settings Configuration	Data	encryption settings	Save
Data encryption settings	ι.	Keys used to encrypt data over-the-wan and at rest.	
Appliance		Encryption password *	
Licensing		The eccyclisic password must be a minimum of a and maximum of 32 characters long. It must contain at least 1 uppercase letter, 1 lowercase letter and 1 special character (space, single quoter) and double quoter() are not aboved.) Contim password.	
Job Concurrency	4	<u></u>	
Dual Instance		Encryption passphrase *	
Support		The encryption passphrase must be a minimum of 8 and maximum of 64 characters long. Single quote (), double quote (), preceding and trailing spaces use not alkneed and will be trimmed.	
Advanced		- Contem passprase -	
SUREedge DR, Version: 6.6.1.29650		Соругіз	ht © 2021 Persistent Systems Limiled. All rights reserved.

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:

🕂 Persistent		Aug 10, 2021 3 43 PM Administrator V
12 Dashboard 🗮 Register 🥹 Protect	ා Recover . එ Jobs ළ Reports ද Settings	
ô: Settings Configuration	Appliance	
Appliance	SUREedge Instance Management Console SUREedge Store VM SUREedge Store	Hypervisor Configuration
Licensing	Type : Amazon Cloud Access Key : AKASEYKHSFTBOMMMENE	
Job Concurrency	EDIT REFRESH	
Support		
Advanced		
SUREedge DR, Version: 6.6.1.20650	Instance name: SUREedge - Instance location: AWS	Copyright © 2021 Persistent Systems Limited. All rights reserved.

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 <a href="mailto:support@accelerite.com">support@accelerite.com</a>.

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 <u>deploying</u> 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.