

Quick Start Guide for AWS (Linux)

Arcserve® Live Migration

arcserve®

Legal Notices

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Arcserve at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified, or duplicated, in whole or in part, without the prior written consent of Arcserve. This Documentation is confidential and proprietary information of Arcserve and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and Arcserve governing your use of the Arcserve software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and Arcserve.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Arcserve copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Arcserve that all copies and partial copies of the Documentation have been returned to Arcserve or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ARCSERVE PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL ARCSERVE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ARCSERVE IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Arcserve.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

© 2020 Arcserve, including its affiliates and subsidiaries. All rights reserved. Any third-party trademarks or copyrights are the property of their respective owners.

Contact Arcserve

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

<https://www.arcserve.com/support>

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.

You can access other helpful resources appropriate for your Arcserve product.

Providing Feedback About Product Documentation:

If you have comments or questions about Arcserve product documentation, please contact [us](#).

Contents

Chapter 1: Introduction	5
Overview	6
Terminologies	7
Requirements	9
Software Compatibility	10
Chapter 2: Perform Live Migration	11
Install Components on Master	12
Installing Control Service	13
Installing Engine	20
Configure Amazon EC2	24
Provision VA on Amazon EC2	25
How to Convert Your Private Key using PuTTYgen	34
How to Connect to the Linux Instance using PuTTY	38
Install Engine on Replica	43
Create Full System Scenario for Amazon EC2	44
Creating Full System Scenario for Amazon EC2	47
Perform Assured Recovery Testing	59
Perform Cut off/Switchover	62

Chapter 1: Introduction

Arcserve Live Migration simplifies the process of migrating data, applications, and workloads. It allows you to move virtually any type of data or workload to cloud, on-premises, or remote locations, such as the edge, with support for virtual, cloud and physical systems. An assured validation of the migrated workload completes the process of enabling customers to continue operations without risks of losing data.

You can easily migrate:

From	To
On-premises	Cloud
Cloud	Cloud
Cloud	On-premises
Physical	Physical
Physical	Virtual
Virtual	Virtual

Live Migration provides the following:

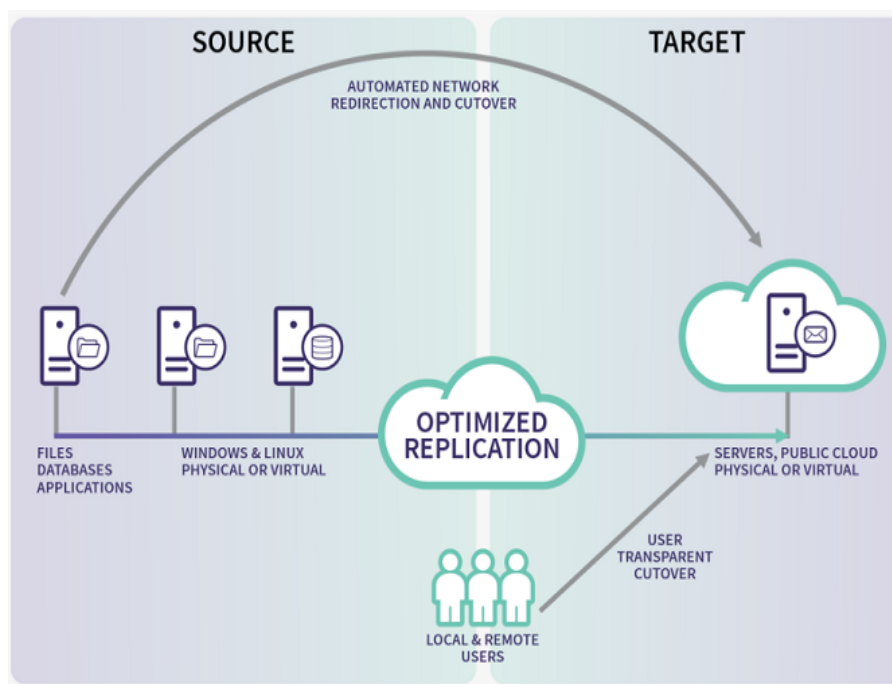
- Unlimited use of the Arcserve Live Migration technology enhanced by Arcserve Continuity Suite.
- Every source that you plan to migrate requires 1 license.
- Seamless access to the entitled software for a period of 90-days.
- On expiry of the license, new scenarios cannot be started, but the existing ones will continue.
- For each license, Live Migration provides free of cost technical assistance for two incidents.

Note: Arcserve currently does not provide professional services to help you with implementation, deployment, and any other migration services.

Overview

Arcserve Live Migration automatically synchronizes files, databases, and applications on Windows and Linux systems with a second physical or virtual environment located on-premises, at a remote location, or in the cloud. After synchronization, changes are replicated in real time to ensure the source and target are in sync prior to the migration.

Encryption enables secure data transfers between local systems and remote locations without the need for a VPN, and automated network redirection makes the switchover process seamless with push-button cutover to ensure availability to the new production environment.



Your typical migration process includes the following steps:

- [Install Components on Master](#)
- [Configure Amazon EC2](#)
- [Provision VA on Amazon EC2](#)
- [Install Engine on Replica](#)
- [Create Full System Scenario for Amazon EC2](#)
- [Perform Assured Recovery Testing](#)
- [Perform Cut off/Switchover](#)

Terminologies

This document uses the following terminologies:

- **Virtual Appliance:** This is a virtual machine that acts as the Replication/Migration proxy server (install the Arcserve Continuity Suite Engine here and deploy on the hypervisor/cloud destination). If you are using a Hyper-V virtual platform, the Virtual Platform Hostname/IP field is disabled (appears dim).
- **Control Service:** Control Service is a management component of Arcserve Continuity Suite. It is a Windows based service that must be deployed first. It hosts web-based information portal and rich Management UI, which is used for creating and monitoring migration scenarios.
- **Engine:** Replication Engine is a background service that moves data from source to destination during migration. Install the Engine on any source that you plan to migrate. You may use the Remote Installer feature to mass deploy Engines.
- **FSHA:** Full System High Availability (FSHA) is a scenario type that allows replication and fail-over of full server. This scenario type is used for migrating full systems.
- **Management UI:** A UI that you use for creating and managing replication/migration scenarios. The Control Server hosts the Management UI. To start the Management UI, log into the Management Portal.
- **Master (Source):** A host/computer that you want to migrate. You can migrate the whole system using the full system migration scenario or the host containing the applications.
- **PowerShell:** Arcserve offers PowerShell Command Line Interface as an alternative if you do not want to manage the replication process using the Manager graphic user interface.
- **Replica (Target):** In case of full system migration, VA (replication proxy) serves as a Replica. Upon completion, VA spins off new VM containing replicated disks or data. For application-based scenarios, the VA hosts and runs replicated application and data.
- **Scenario:** A configuration unit describing migration job/task. You can create and manage scenarios using rich management GUI or PowerShell CLI. Scenarios contain key information about replication/migration jobs to be performed.

- **Switchover:** The cutover to the newly migrated workload from where the operations can begin.
- **Synchronization:** The process of making the set of files identical on the Master and Replica servers. It is usually necessary to synchronize the Master and Replica as the initial step of a replication/migration scenario.
- **Virtual Platform Host:** The machine that hosts the Appliance VM, which acts as a Replica server. Based on the scenario type, it acts as a local hypervisor or cloud platform (AWS or Azure).

Requirements

Before you migrate, make sure to meet the following requirements:

- Arcserve Live Migration supports both Windows and Linux operating systems for Full System migration scenarios. If the source host is Windows, then the Virtual Appliance (VA) must be Windows; if the source host is Linux, then the VA must be Linux as well.

Note: Before deploying Arcserve Live Migration scenarios, see [Limitations](#) in Release Notes.

- When migrating workloads to AWS, corresponding AWS cloud credentials must be registered in Arcserve Continuity Suite Management UI.

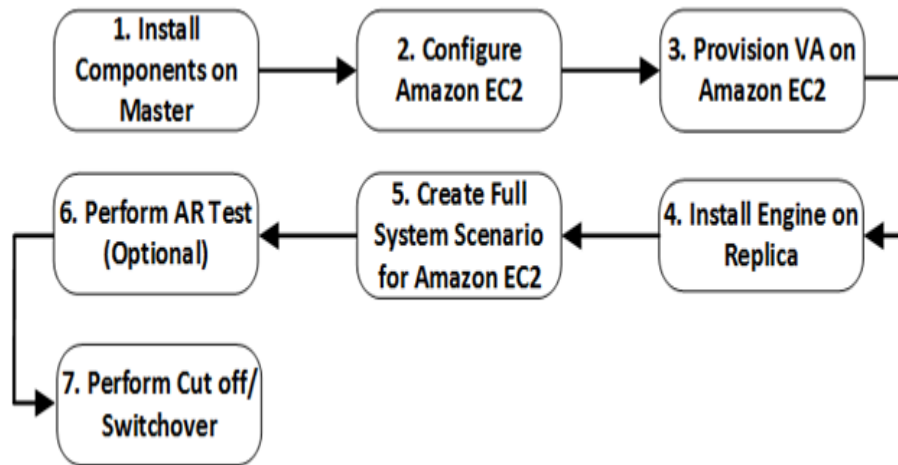
Software Compatibility

For more information about compatibility, see [Compatibility Matrix](#).

Note: Make sure that your source OS and application versions are explicitly listed on the support matrix.

Chapter 2: Perform Live Migration

The following flowchart provides the Live Migration process given in this document:



Install Components on Master

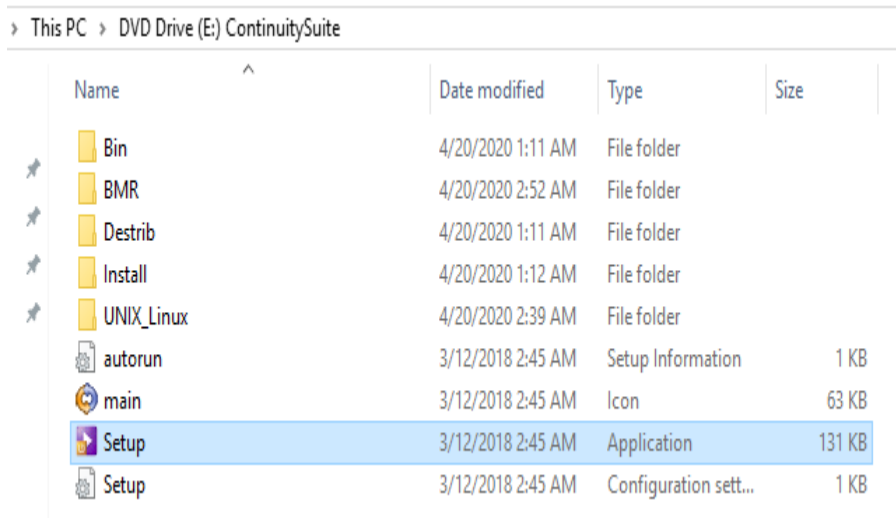
This section describes how to install the Arcserve Continuity Suite Control Service and Engine on Master.

Installing Control Service

The Control Service component functions as the single-point-of-control that contains the entire dataset of the existing scenarios. Control Service communicates with the Engines and the Managers. It is responsible for the management of all scenario-related-tasks, such as creation, configuration, monitoring, and running of the scenarios.

To install Control Service, follow these steps:

1. Download [RHA iso for Continuity Suite](#), and then open the folder.
2. From the mounted directory, double-click **Setup**.



File Explorer window showing the contents of a DVD Drive (E:) named ContinuitySuite. The 'Setup' application is highlighted.

Name	Date modified	Type	Size
Bin	4/20/2020 1:11 AM	File folder	
BMR	4/20/2020 2:52 AM	File folder	
Destrib	4/20/2020 1:11 AM	File folder	
Install	4/20/2020 1:12 AM	File folder	
UNIX_Linux	4/20/2020 2:39 AM	File folder	
autorun	3/12/2018 2:45 AM	Setup Information	1 KB
main	3/12/2018 2:45 AM	Icon	63 KB
Setup	3/12/2018 2:45 AM	Application	131 KB
Setup	3/12/2018 2:45 AM	Configuration sett...	1 KB

3. On the Arcserve Continuity Suite installation wizard, click **Install Components**.

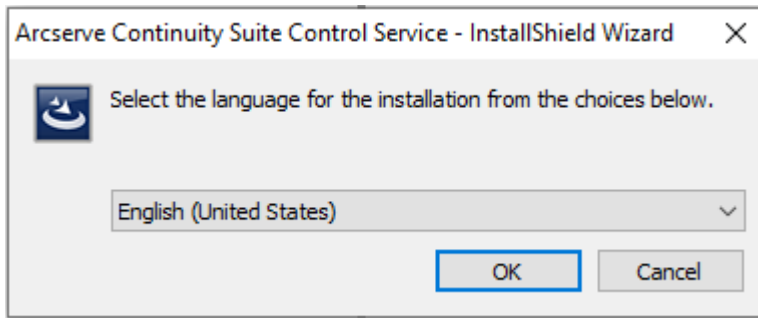


The wizard displays the components.

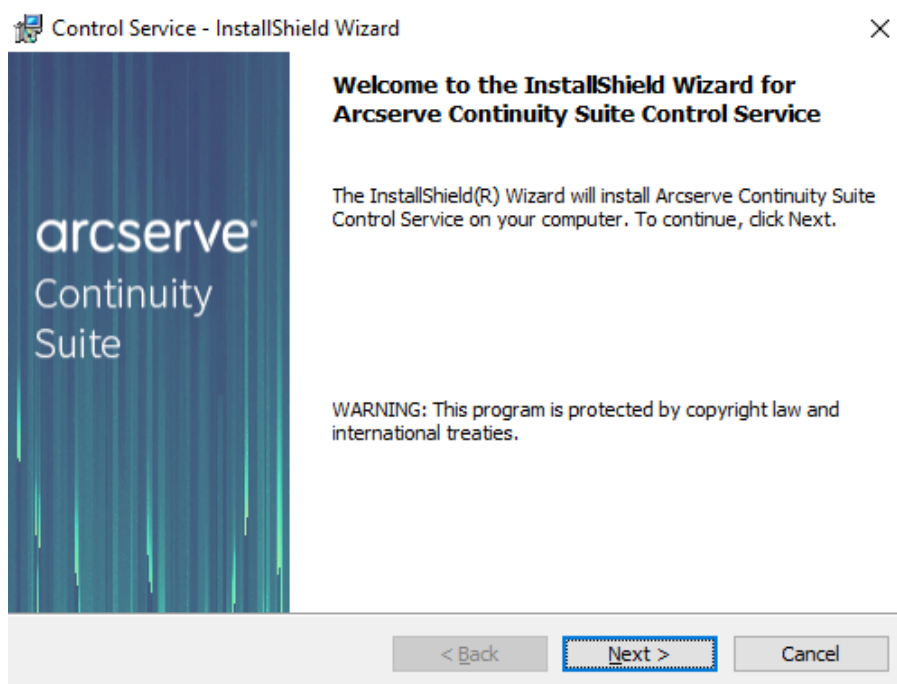
4. Click **Install Control Service**.



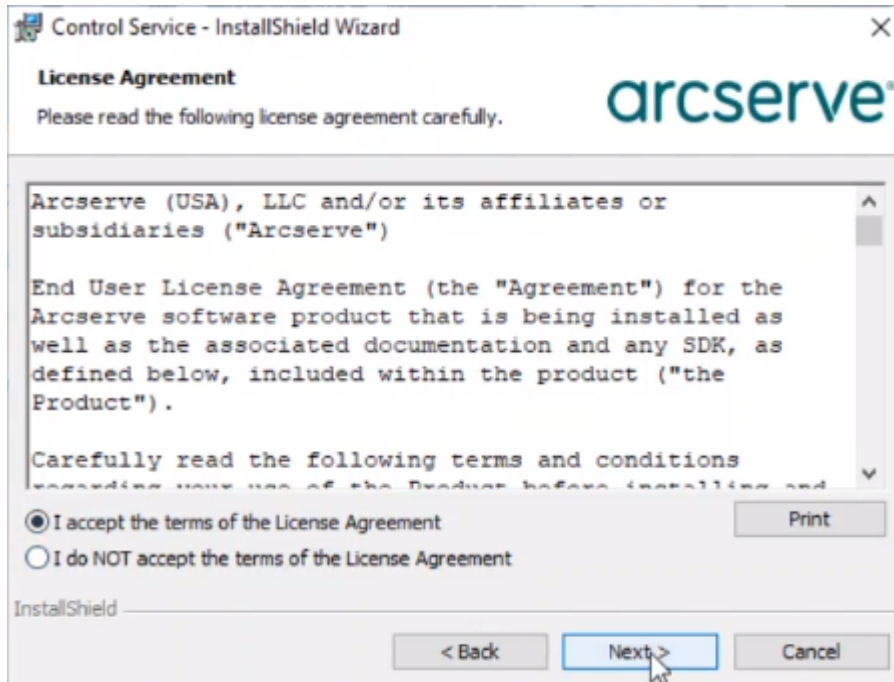
5. On the Arcserve Continuity Suite Control Service - InstallShield Wizard, from the drop-down list, select your preferred language, and then click **OK**.



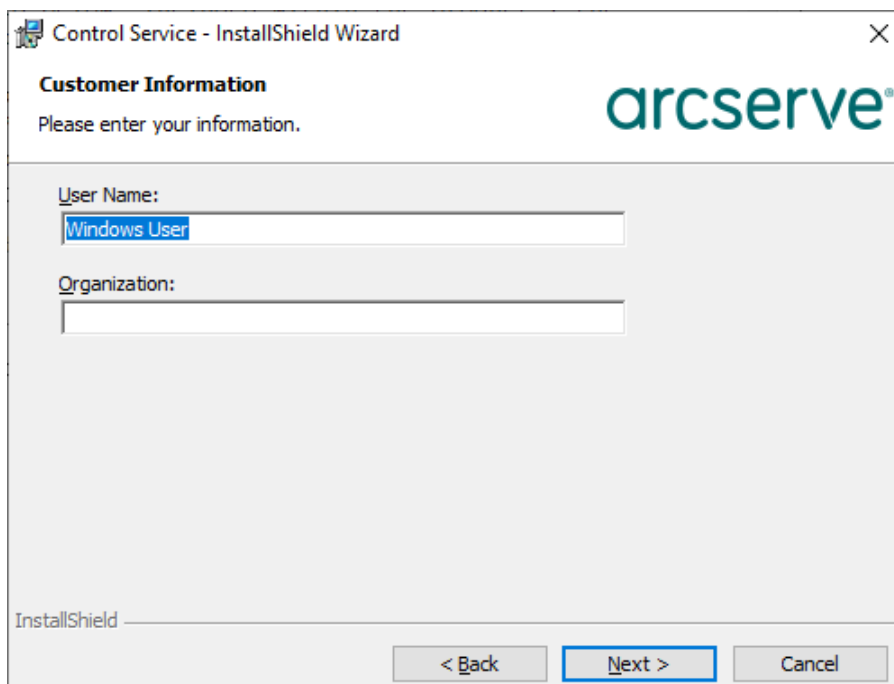
After the initial process is complete, the Welcome page appears.



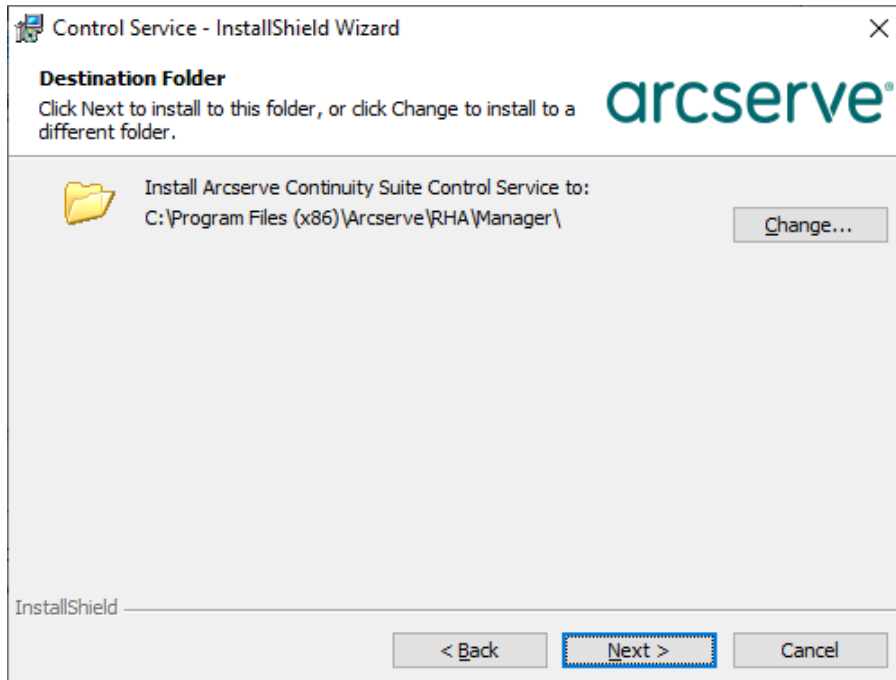
6. Click **Next**.
7. On the License Agreement page, read the terms of the License Agreement, select the **I accept the terms of the License Agreement** option, and then click **Next**.



8. On the Customer Information page, enter a user name, and then click **Next**.



9. On the Destination Folder page, retain the defaults, and then click **Next**. To change the destination folder, click **Change**.

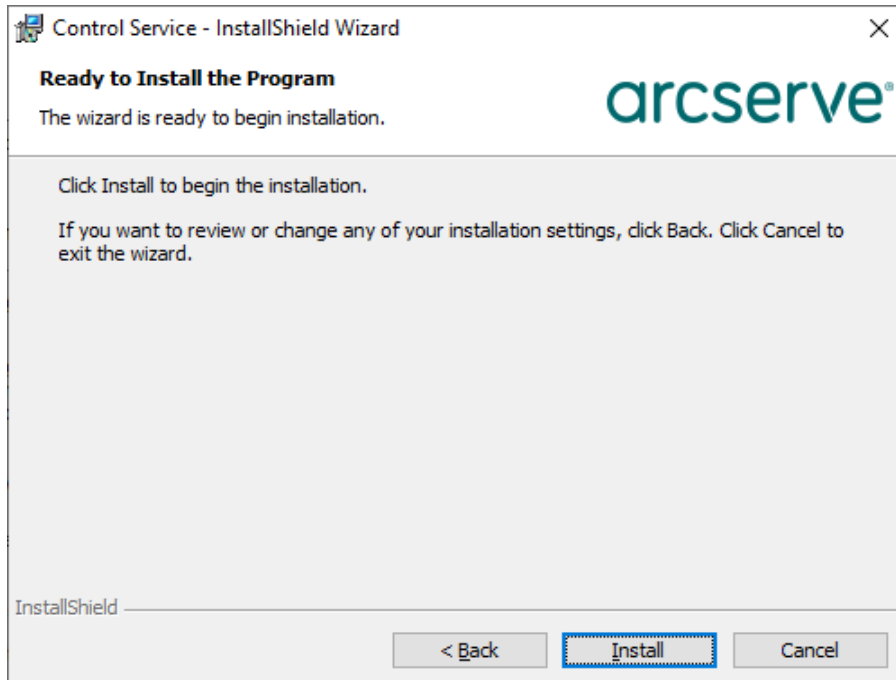


Note: The default installation directory is: *C:\Program Files (x86)\Arcserve\RHA\Manager*. All executables, DLLs and configuration files are located within the INSTALLDIR.

10. For the upcoming screens, retain the defaults, and then click **Next** to continue.

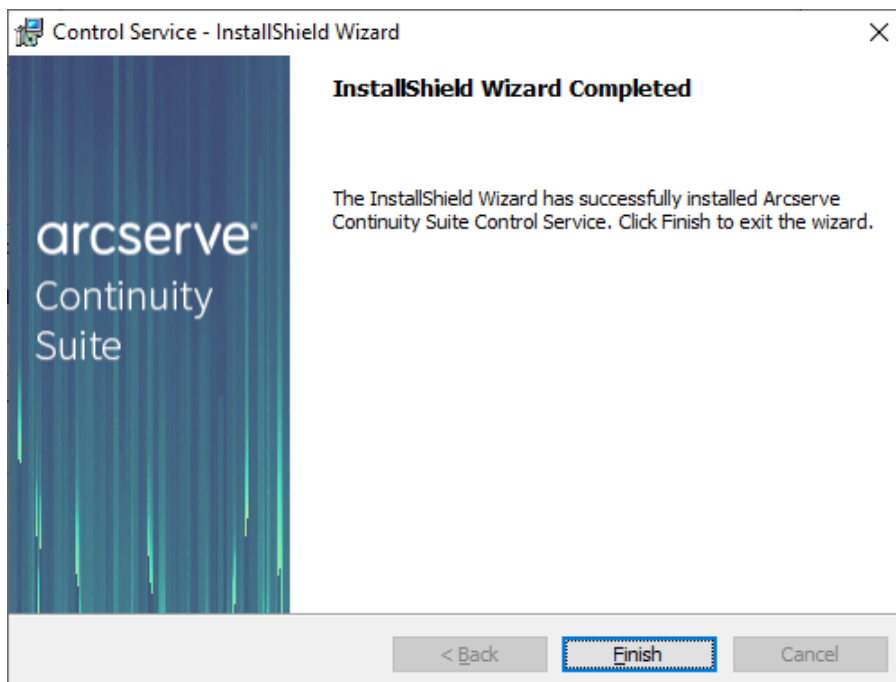
Note: For more information about how to configure SSL Configuration, Service Logon Information, and Control Service Role, see [Install a Control Service for a Standard Operation](#).

11. On the Ready to Install the Program page, click **Install**.



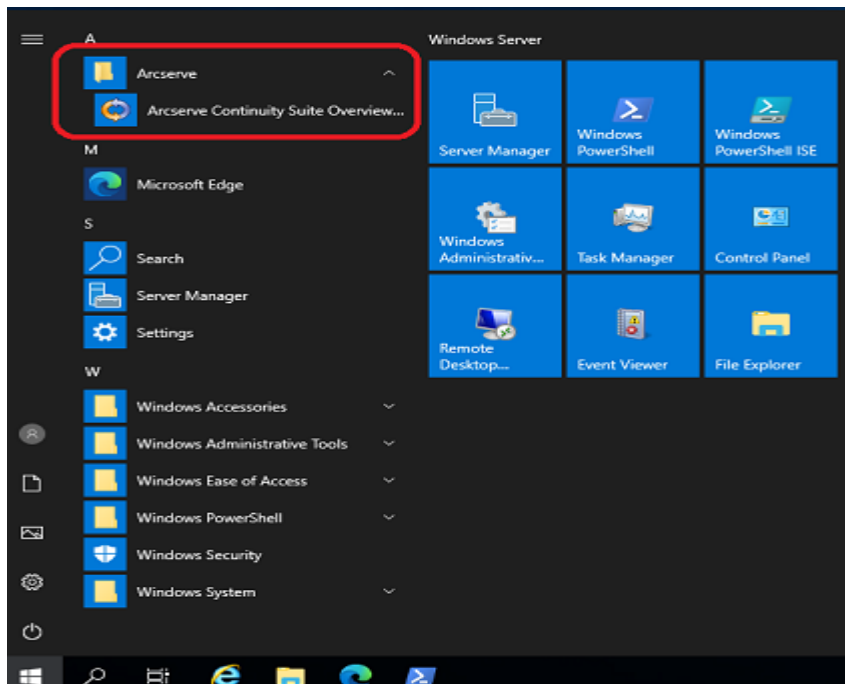
Note: Click the **Back** button to return to the previous pages and change any configuration as needed.

12. After installation is complete, click **Finish** to close the wizard.



The Arcserve Continuity Suite Control Service is installed.

13. To open Control Service in a web portal, go to **Start > Arcserve > Arcserve Continuity Suite Overview**.



The web portal opens in a browser.



Installing Engine

Make sure that the Engine component, which is a service, is running before you start any scenario. Install Engine on every server participating in any given scenario such as the Master (source) and Replica (target) hosts. Each Engine supports both Master and Replica functionality in addition to both Replication and High Availability scenarios. It may participate in multiple scenarios and serve in a different role for each scenario. You can install Engines one by one locally on each host, or concurrently through a remote installer on numerous hosts. You can also install it during scenario creation if needed.

To Install Engine, follow these steps:

1. To extract installation package and start the engine installation, copy *arc-serverha.tar* to your host, and then run the command as a root user.

Note: The script in the following example uses the command for installation of RHEL 8 package.

```
tar xvf arcserverha.tar && tar xzf arcserverha-18.3-0.7024.rhel8.tgz && cd arc-serverha && ./install.sh
```

The installation script for the Continuity Suite Engine is *install.sh*. When you run this script without any option, it initiates the interactive installation process. For silent or non-interactive installation, use *install.sh -q* or *install.sh -y*. The following illustration lists additional customization options that you can use with *install.sh*.

```
Usage:
  install.sh [options]
Where options is
  -l, --license=<Agree/n>   Agree to license*
  -c|g, --caarha-group=<Y/n> Create caarha group if it does not exist.
  -o, --enable-oracle=<y/N> Enable oracle support (default is no)
  -u, --oracle-user=<user>   Specfiy oracle user (req'd for oracle support)
  -h, --ora-home=<path>      Force ORACLE_HOME if not in user's environment
  -b, --ora-base=<path>      Force ORACLE_BASE if not in user's environment
  -i, --install              Install Arcserve Continuity Suite (Answer 'yes' to install)
  -q|y, --quiet              Perform a default installation.
                             - ack and don't display license
                             - ensure caarha group exists or is created
                             - oracle support is not installed
                             - language is auto detected.
  -l, --language=<lang>     Specify language, default is C.UTF-8
  -f, --firewall             Open firewall port 25000
  -v, --virtual              Install Virtual Appliance packages."
  -F, --force               Install even if scenario is running."

NOTE: You must be an admin (root) to install.
```

2. To provide your consent during interactive installation, do the following:

- a. To continue with the installation and accept End User License Agreement, type YES and press Enter.

```
Do you accept Arcserve End User License Agreement?[YES]yes
```

- b. If you already have the Continuity Suite Engine previously installed, a prompt appears that needs your confirmation for product upgrade. To upgrade, type YES and press Enter.

```
Continuity Suite 18.0-0.5503 is already installed.  
Do you want to upgrade Continuity Suite to 18.3-0.7024?[YES]
```

- c. If you plan to use the given host as proxy and install Virtual Appliance packages in Full System HA scenarios, type YES and press Enter.

```
Install packages needed to act as Virtual Appliance for Full System HA?[NO]yes
```

- d. To confirm user group creation for Continuity Suite Engine, type YES and press Enter.

Note: By default, only a root user can authenticate and manage Continuity Suite Engine. Non-root users must be listed in the group to be able to authenticate and manage Continuity Suite Engine.

```
Create "caarha" group?[YES]yes
```

- e. To replicate Oracle and enable its support, type YES and press Enter. The default option is NO.

```
Enable Oracle support[NO]
```

- f. To select the language, type the number corresponding to the specified language, and then press Enter.

```
Please select language to be used:  
1 - Chinese (Simplified)  
2 - Chinese (Traditional)  
3 - English (United States)  
4 - French (France)  
5 - German (Germany)  
6 - Italian (Italy)  
7 - Japanese  
8 - Portuguese (Brazil)  
9 - Spanish (Traditional Sort)  
Please select your language [3]
```

- g. To allow firewall port to be opened for the engine, type YES and press Enter.

The default port value is 25000.

Note: If you plan to use a different port, type NO and later change the engine port manually in the /opt/Arcserve/RHA/bin/ws_rep.cfg file, and then open the corresponding firewall port.

```
Open firewall port 25000? [YES]
```

- h. If you want to enable latest product updates, type YES and press Enter. The default option is NO.

```
Check for latest product updates (recommended)? [NO]
```

3. Do the following NAT settings:

- a. On the Master server, run the following command in /opt/Arcserve/RHA/bin:

```
./natutl
```

- b. To check if any machines are added, run the following command:

```
nat.list
```

- c. To add the NAT settings, run the following command:

```
nat.addhost <VA IP address> 25000
```

- d. To apply the NAT settings, run the following command:

```
nat.apply
```

- e. To check whether the Master can communicate, run the following command:

```
telnet <VA IP address> 25000
```

Notes:

- ◆ If you decide to enable Oracle support, you must provide information such as Oracle Owner, Oracle Home path, and Oracle Base path. The Oracle Owner is primarily required as it allows the product to retrieve the Home path and Base path information using the Oracle Owner user environment. If the Home path and Base path information cannot be found, then you must manually add them. On Solaris, if your Oracle server is installed without the 32-bit Oracle client library, then you must also provide the Oracle Instant Client path.
- ◆ Although the Arcserve Continuity Suite package is installed, you are prompted to reinstall it.
- ◆ To allow non-root users to manage scenarios, you must create the "caarha" group on your machine and make sure the group works with the supplementary group.

The Arcserve Continuity Suite Engine is installed.

Configure Amazon EC2

The Arcserve Replication and High Availability VA virtual machine resides in VPC (default or customized), and the Master servers are replicated to that VPC.

Note: To set up VPC, subnets, IP gateway, and so on according to your DR network requirements, see the Amazon online help.

Consider the following before deploying EC2-based Full System scenarios:

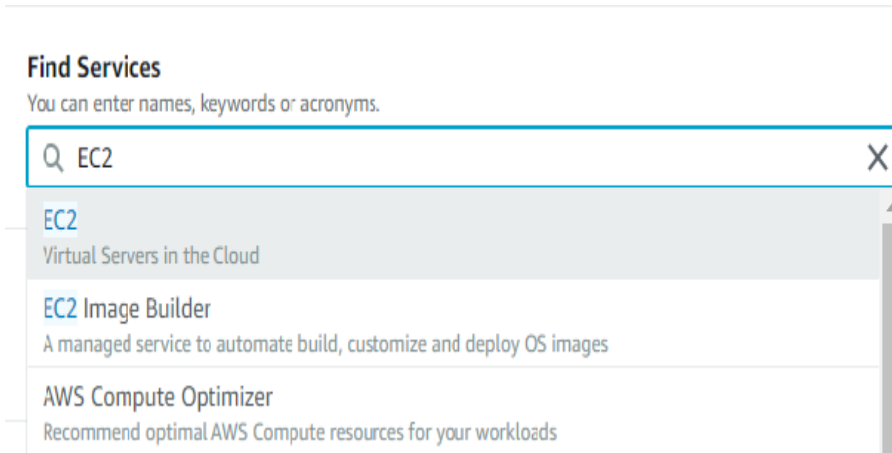
- Arcserve Replication and High Availability needs the Access Key ID and Secret Access Key of Amazon EC2 account to work with EC2. You can get the required information from your administrator.
- The Amazon EC2 user in Arcserve Replication and High Availability should have required permissions. For more information, see the [Arcserve KB article](#).
- If you want Arcserve Replication and High Availability to start the DR VM with a specific public IP address, pre-allocate such Elastic IPs in the Amazon EC2 web portal. Later in the Network Mapping dialog of Continuity Suite Scenario, you can select a public IP from the existing Elastic IP addresses for the DR VM.

Provision VA on Amazon EC2

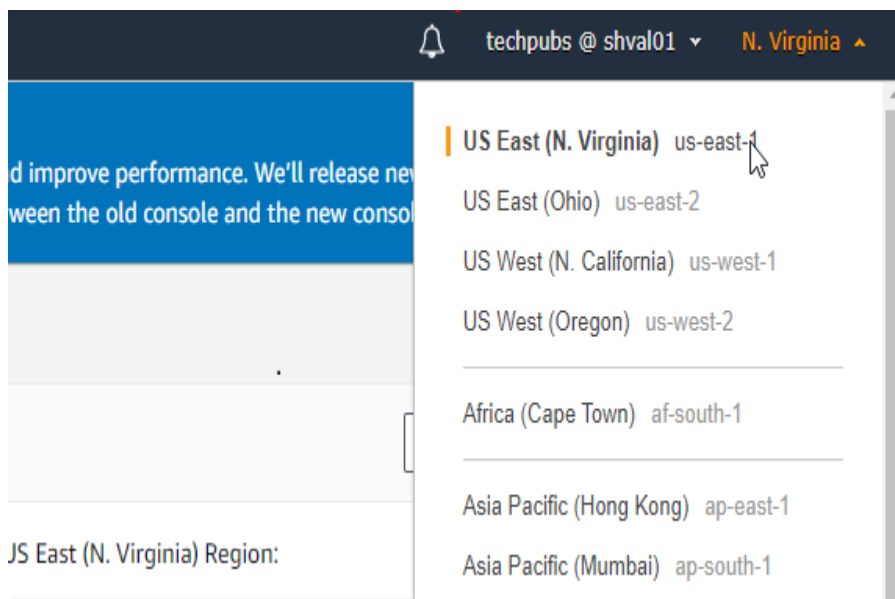
The Continuity Suite Virtual Appliance (VA) is a VM running on the virtualization platform or cloud where you want to replicate the Master servers. The VA acts as Replica in a Continuity Suite Full System scenario. The Master server is replicated to this virtualization platform or cloud. However, the Disaster Recovery VM of Master server starts and runs on this virtualization platform or cloud for multiple reasons, such as Assured Recovery testing, Switchover, and Start VM.

Follow these steps:

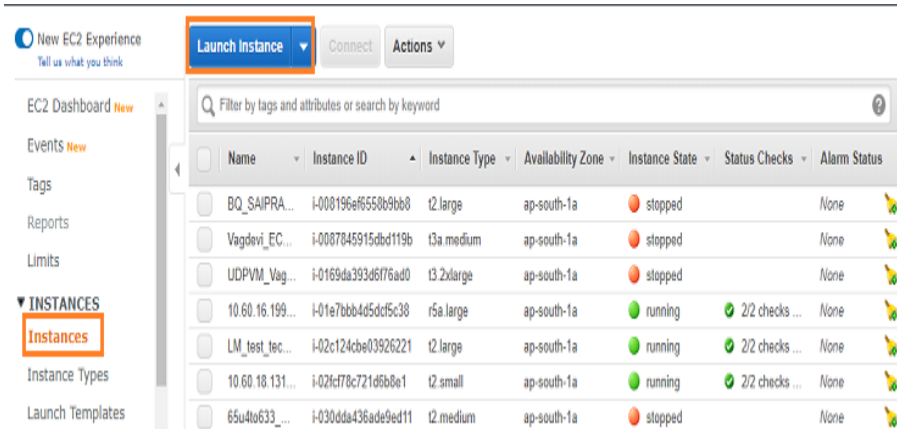
1. Log into [Amazon Web Services](#) as an IAM user.
2. Under Find Services, search for EC2, and then select **EC2**.



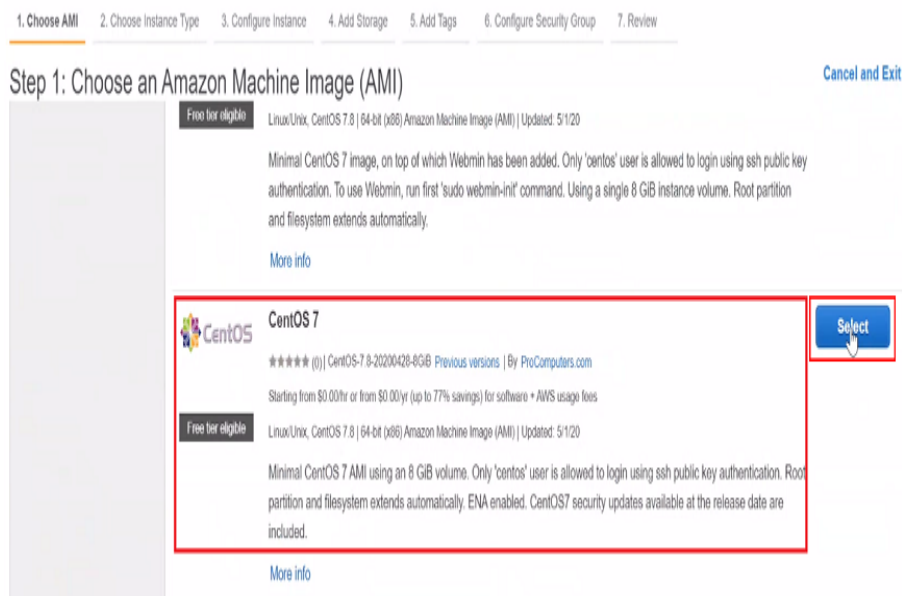
3. On the top right corner of the EC2 dashboard, select the AWS region in which you want to provision the EC2 server.



4. On the left panel, go to **Instances**, and then click **Launch Instance**.



5. On the Step 1: Choose an Amazon Machine Image (AMI) page, from the list of AMI, for CentOS 7, click **Select**.



The CentOS details page appears.

6. Scroll down to the bottom of the page,, and then click **Continue**.

i3.xlarge	\$0.20	\$0.354	\$0.554/hr
i3.2xlarge	\$0.40	\$0.708	\$1.108/hr
i3.4xlarge	\$0.80	\$1.416	\$2.216/hr
i3.8xlarge	\$1.60	\$2.832	\$4.432/hr
i3.16xlarge	\$3.20	\$5.664	\$8.864/hr
i3en.large	\$0.10	\$0.257	\$0.357/hr
i3en.xlarge	\$0.20	\$0.514	\$0.714/hr
i3en.2xlarge	\$0.40	\$1.028	\$1.428/hr
i3en.3xlarge	\$0.80	\$1.542	\$2.342/hr
i3en.6xlarge	\$0.80	\$3.084	\$3.884/hr
i3en.12xlarge	\$2.40	\$6.168	\$8.568/hr
i3en.24xlarge	\$3.20	\$12.336	\$15.536/hr
i3en.metal	\$2.40	\$12.336	\$14.736/hr

EBS General Purpose (SSD) volumes
\$0.114 per GB-month of provisioned storage

You will not be charged until you launch this instance.

Cancel Continue

7. On the Step 2: Choose an Instance Type page, select an instance type, and then click **Next: Configure Instance Details**.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

8. On the Step 3: Configure Instance Details page, select **Enable** from the Auto-assign Public IP field, and then click **Next: Add Storage**.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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 [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)

Auto-assign Public IP

Placement group

- Enable
- Disable

Capacity Reservation [Create new Capacity Reservation](#)

Domain join directory [Create new directory](#)

Cancel Previous **Review and Launch** **Next: Add Storage**

9. On the Step 4: Add Storage page, type the size of VA in the Size field, and then click **Next: Add Tags**.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0450aab2e9dbd2928	<input type="text" value="200"/>	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypt

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous **Review and Launch** **Next: Add Tags**

10. On the Step 5: Add Tags page, click **Add Tag**, enter the Key and Value, and then click **Next: Configure Security Group**.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 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 tag with key = Name and value = Webserver.

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 your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ¹	Volumes ¹
------------------------------	--------------------------------	------------------------	----------------------

This resource currently has no tags

Choose the **Add tag** button or [click to add a Name tag](#).
Make sure your [IAM policy](#) includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 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 tag with key = Name and value = Webserver.

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 your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ¹	Volumes ¹
<input type="text" value="Name"/>	<input type="text" value="LM_User_Guide"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

11. On the Step 6: Configure Security Group page, click **Add Rule**, enter the following values, and then click **Review and Launch**:

- Type: Custom TCP Rule
- Protocol: TCP
- Port Range: 25000
- Source: 0.0.0.0/0
- Description: Engine

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	SSH
Custom TCP f	TCP	25000	Custom 0.0.0.0/0	Engine

[Add Rule](#)

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review and Launch](#)

12. On the Step 7: Review Instance Launch page, review the information, and then click **Launch**.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, CentOS 7-CentOS-7-8-20200428-8GiB-AutogenByAWSMP-, is open to the world. Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

Your instance configuration is not eligible for the free usage tier

To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about [free usage tier](#) eligibility and usage restrictions.

[Don't show me this again](#)

▼ AMI Details [Edit AMI](#)

CentOS 7

CentOS-7-x86_64-Minimal-8GiB-HVM-20200428_104347

Root Device Type: ebs Virtualization type: hvm

[Cancel](#) [Previous](#) [Launch](#)

13. On the Select an existing key pair or create a new key pair page, do one of the following, and then click **Launch Instances**:

- To create a new key pair, follow these steps:
 1. From the drop-down list, select **Create a new key pair**.
 2. Enter key pair name.
 3. To save the key pair, click the **Download Key Pair** button.
 4. Click **Launch Instances**.

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair (1) (3)

Key pair name (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 Instances**

Note: To connect to your EC2 instance, we recommend that you download the key pair. If you launch your instance without a key pair, you cannot connect to your instance.

Important! Copy and save the private key file in a safe place as you cannot download it later.

- To select an existing key pair, follow these steps:
 1. From the drop-down list, select **Choose an existing key pair**.
 2. From the Select a key pair drop-down list, select as needed.
 3. Select the acknowledgment check box, and then click **Launch**

Instances.

×

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

1

Select a key pair

2

AKP

☐ I acknowledge that I have access to the selected private key file (AKP.pem), and that without this file, I won't be able to log into my instance.

3

Cancel

Launch Instances

14. On the Launch Status page, scroll down to the bottom of the page, and then click **View Instances** to return to the console.

Launch Status

▼ Getting started with your software

To get started with CentOS 7

To manage your software subscription

View Usage Instructions

Open Your Software on AWS Marketplace

▼ Here are some helpful resources to get you started

- How to connect to your Linux instance
- Learn about AWS Free Usage Tier

- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

View Instances

The Instances page displays the status of your instance. When the instance is launched, its initial state displays as pending. After the instance starts, the state changes from pending to running.

Notes:

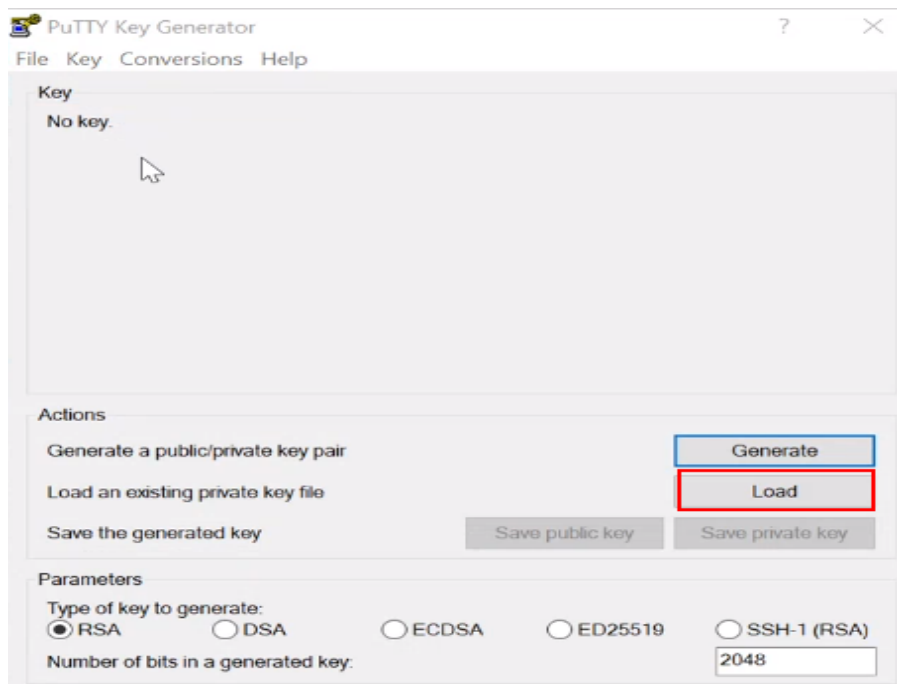
- You can connect to your instance only after the Status Checks changes to 2/2.
- To connect to your instance, see [How to connect to the Linux Instance using PuTTY](#).

How to Convert Your Private Key using PuTTYgen

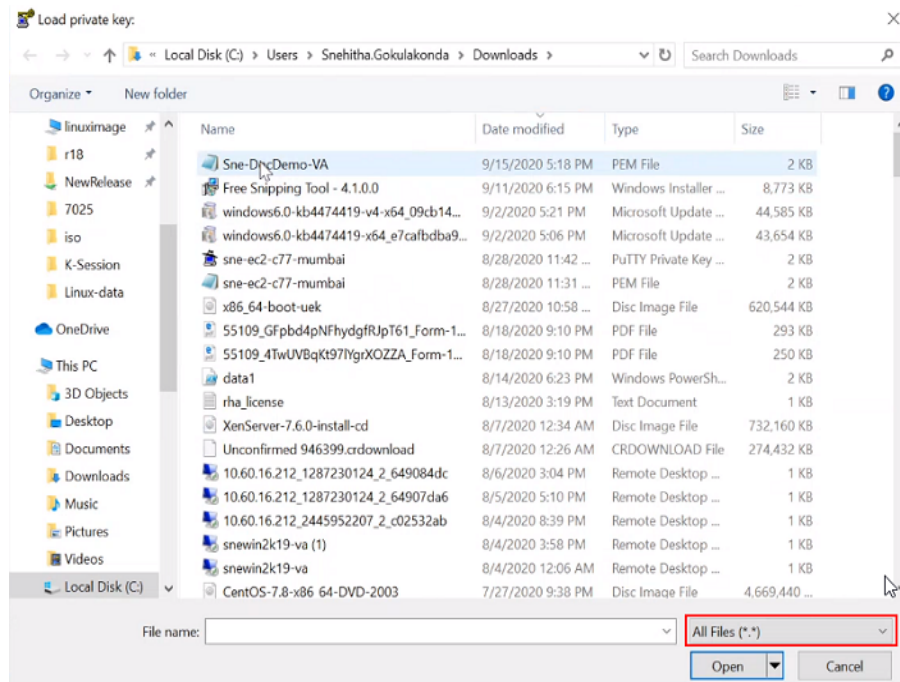
This section provides information about how to convert your private key using PuTTYgen.

Follow these steps:

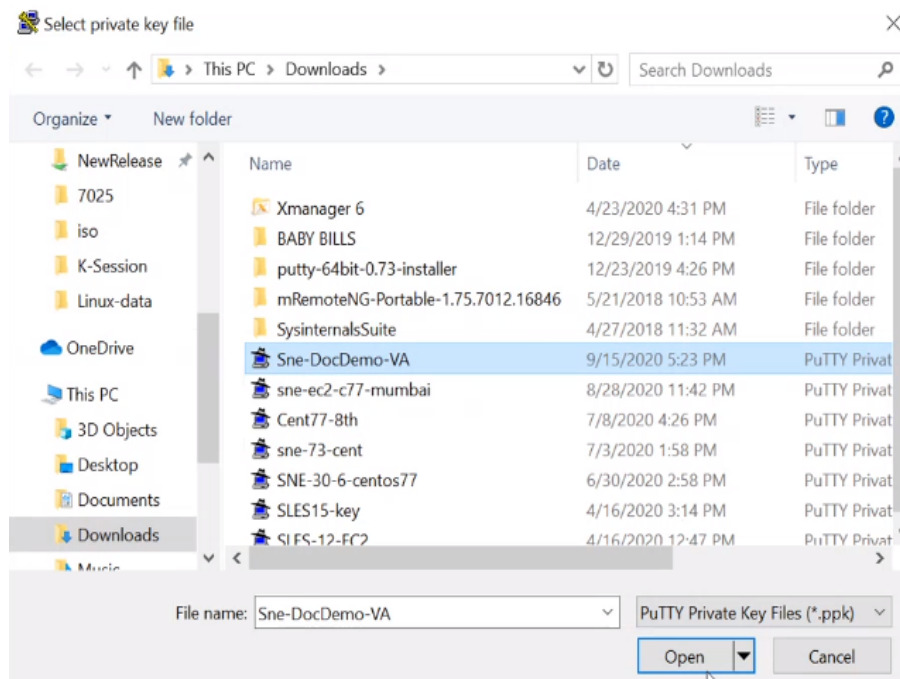
1. Search for PuTTYgen in the search bar next to the start menu, and then click **PuTTYgen**.
2. On the PuTTY Key Generator screen, click **Load**.



3. On the Load private key: window, to locate your .pem file, do the following:
 - a. From the drop-down list in the lower-right corner of the window, select **All Files (*.*)**, type the file name, and then click **Open**.

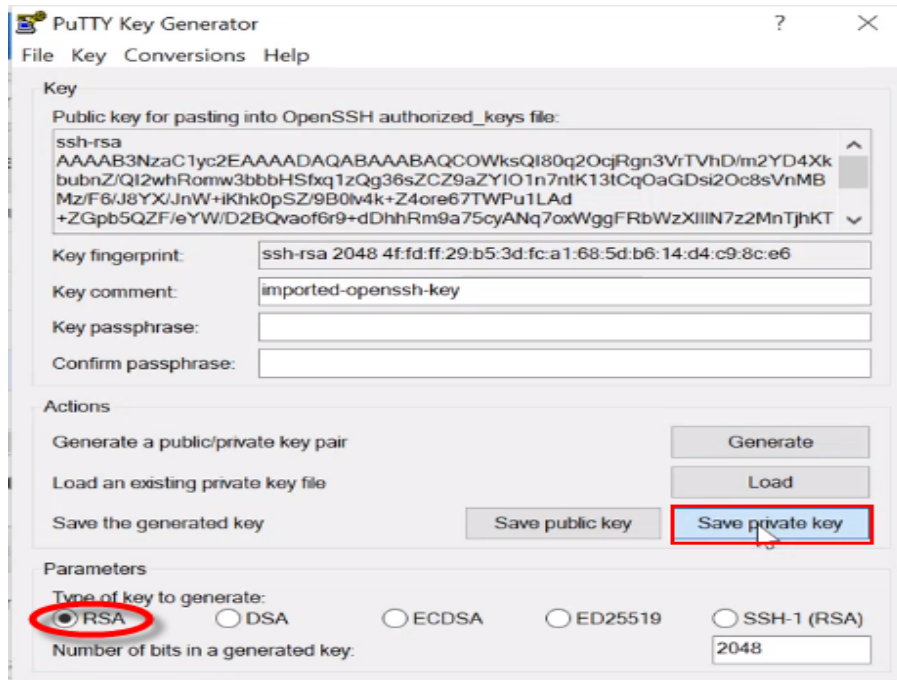


- b. On the Select private key file screen, select your private key file (.pem), and then click **Open**.



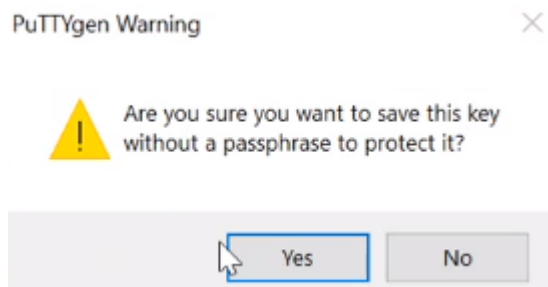
The PuTTYgen Notice dialog appears.

4. To close the PuTTYgen Notice dialog, click **OK**.
5. On the PuTTY Key Generator window, under Parameters, for Type of key to generate, select RSA, and then click **Save private key**.

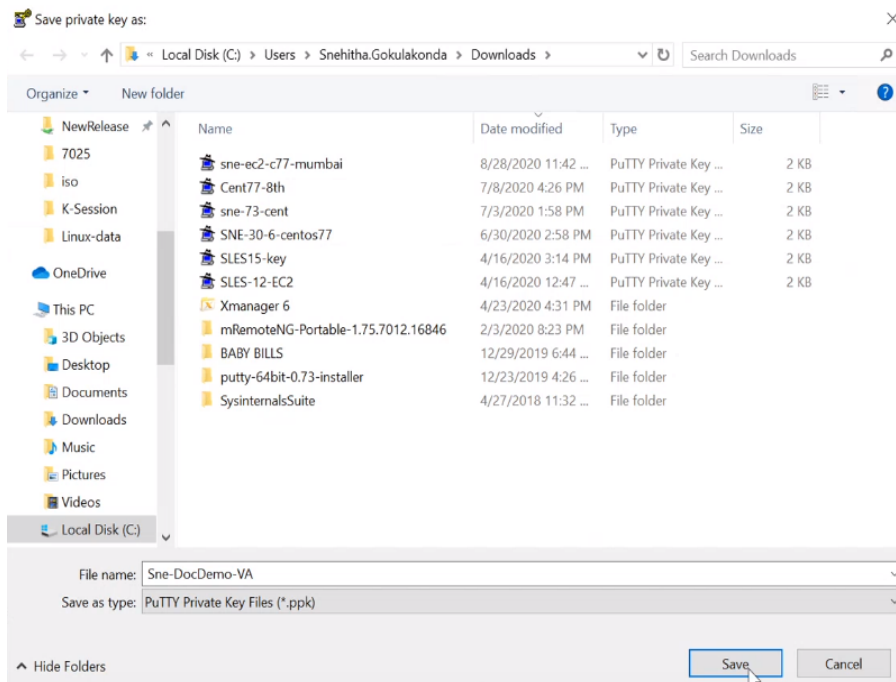


The PuTTYgen Warning dialog appears.

6. Click **Yes** to save the key without a passphrase.



7. On the Save private key as: window, navigate to the location you want to save your PuTTY Private Key file (.ppk). For File name, type the same name for the key that you used for the key pair, and then click **Save**.



Close the PuTTY Key Generator window.

You can now connect to your instance using PuTTY's SSH client.

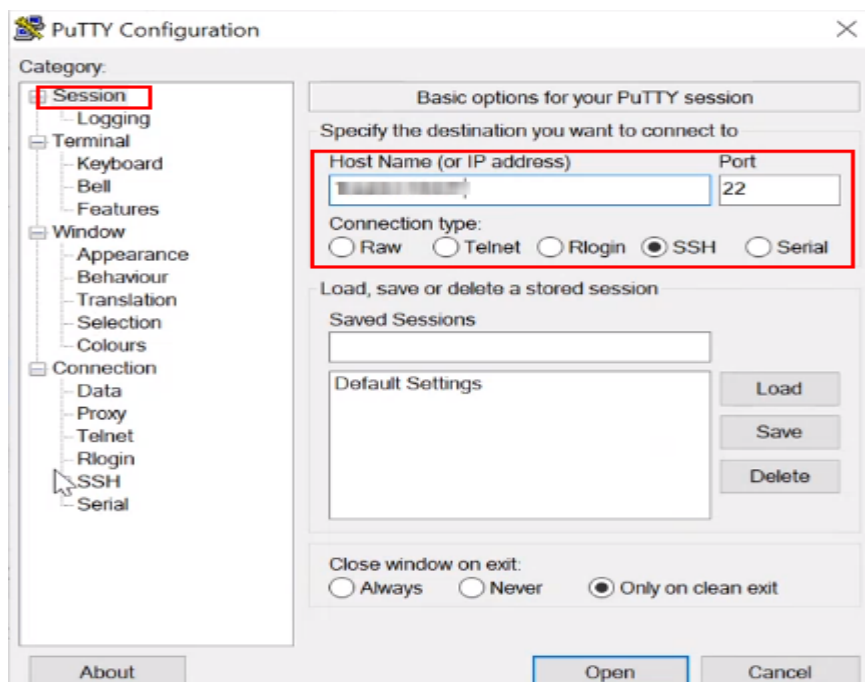
How to Connect to the Linux Instance using PuTTY

This section provides information about how to connect to the Linux instance using PuTTY.

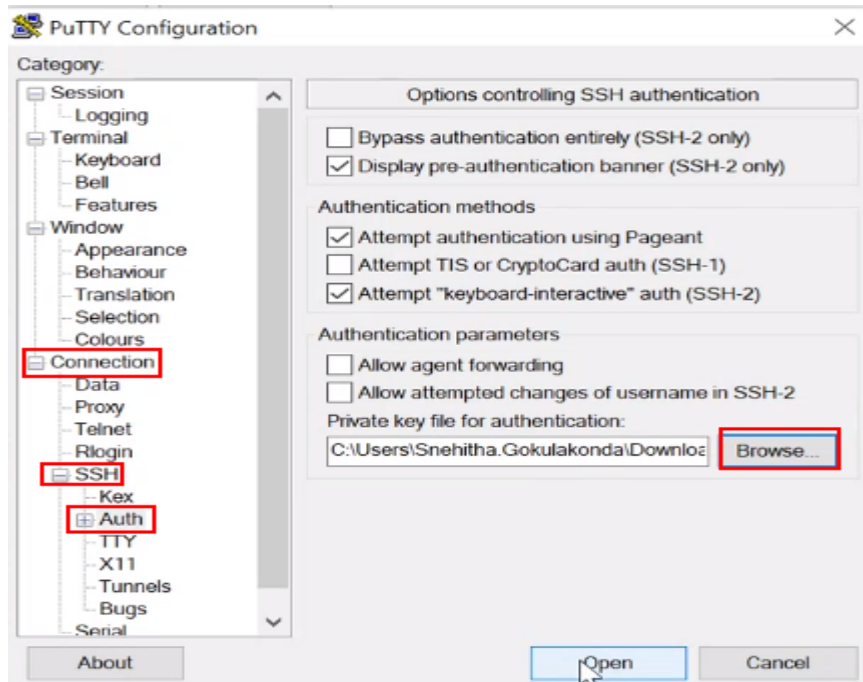
Note: PuTTY does not support the private key file (.pem) created during the instance launching process. Before connecting to your Linux instance using PuTTY, you need to convert your private key file (.pem) into the PuTTY required format (.ppk). To convert your private key into the PuTTY required format, see [How to Convert Your Private Key using PuTTYgen](#).

Follow these steps:

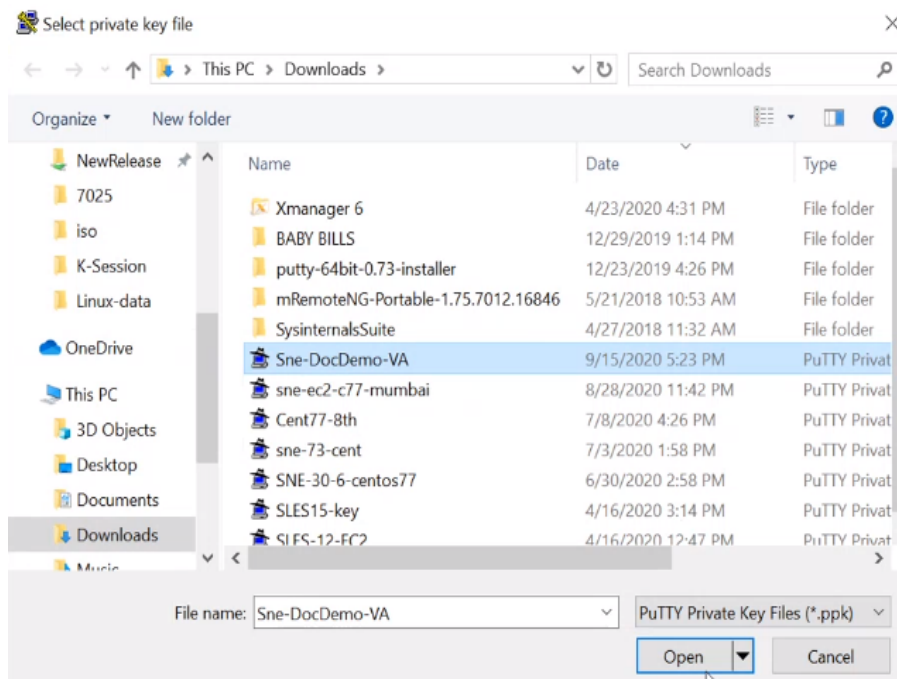
1. Search for PuTTY in the search bar next to the start menu, and then click **PuTTY**.
2. In the Category pane, select **Session**, and do the following:
 - Host Name (or IP address) – Type the IP address or host name.
 - Connection type – Select **SSH** as connection type.
 - Port – Type the port value. The default port value is 22.



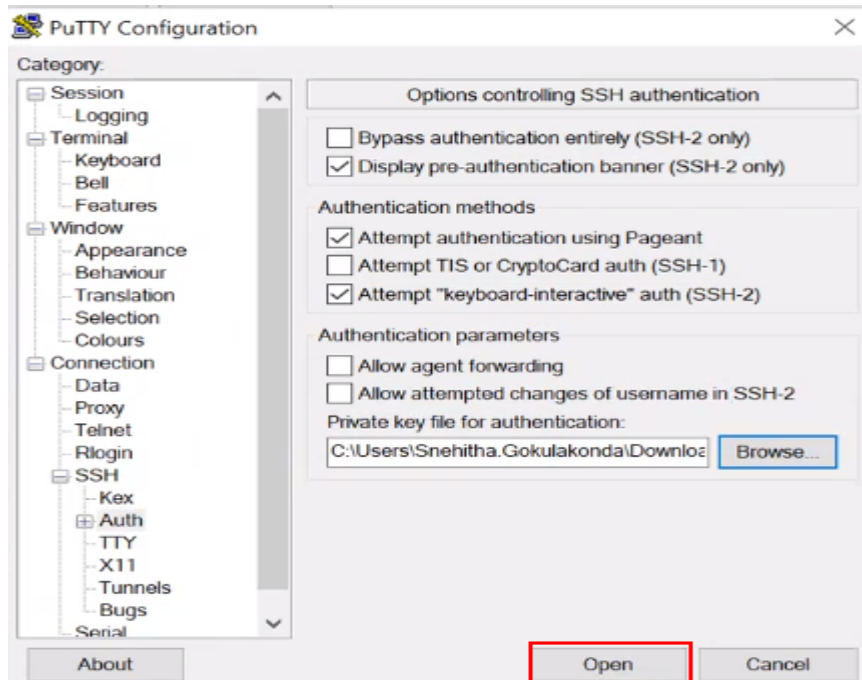
3. In the Category pane, navigate to **Connection** -> **SSH** -> **Auth**, and then click **Browse**.



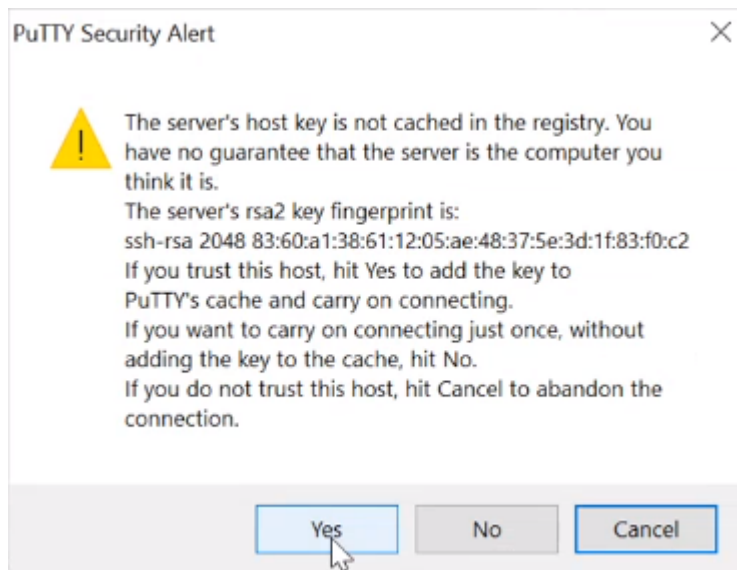
4. On the Select private key file window, select the private key file (.ppk) that you previously generated, and then click **Open**.



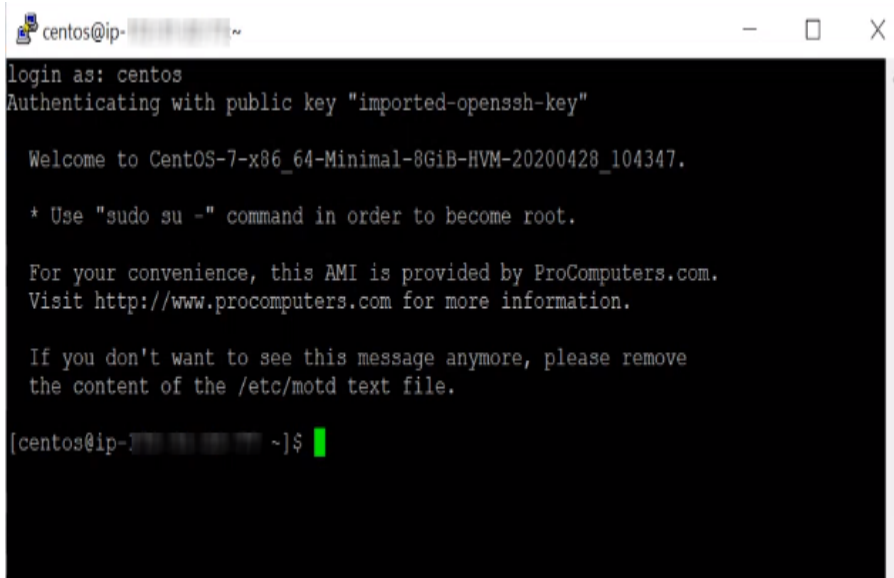
5. On the PuTTY Configuration window, click **Open** to connect to your instance.



6. If you are connecting to the instance for the first time, PuTTY displays a security alert message asking whether you trust the host you are connecting to. Click **Yes**.



A window opens and you are connected to your Linux instance.



```
centos@ip-...  
login as: centos  
Authenticating with public key "imported-openssh-key"  
  
Welcome to CentOS-7-x86_64-Minimal-8GiB-HVM-20200428_104347.  
  
* Use "sudo su -" command in order to become root.  
  
For your convenience, this AMI is provided by ProComputers.com.  
Visit http://www.procomputers.com for more information.  
  
If you don't want to see this message anymore, please remove  
the content of the /etc/motd text file.  
  
[centos@ip-... ~]$
```

7. Do the following:

- a. To change the password for root user, run the following command:

```
sudo passwd
```

- b. To open the sshd server system-wide configuration file, run the following command:

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

- c. To permit root login, type Yes. The default option is Yes.

```
PermitRootLogin yes
```

- d. To allow password authentication, type Yes. The default option is No.

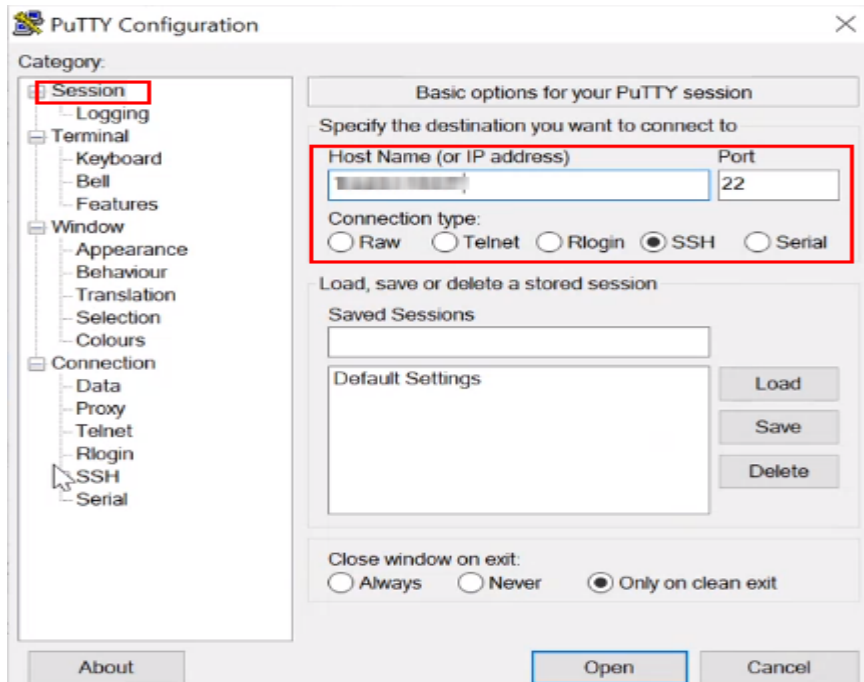
```
PasswordAuthentication no
```

Type Yes, and run the following command:

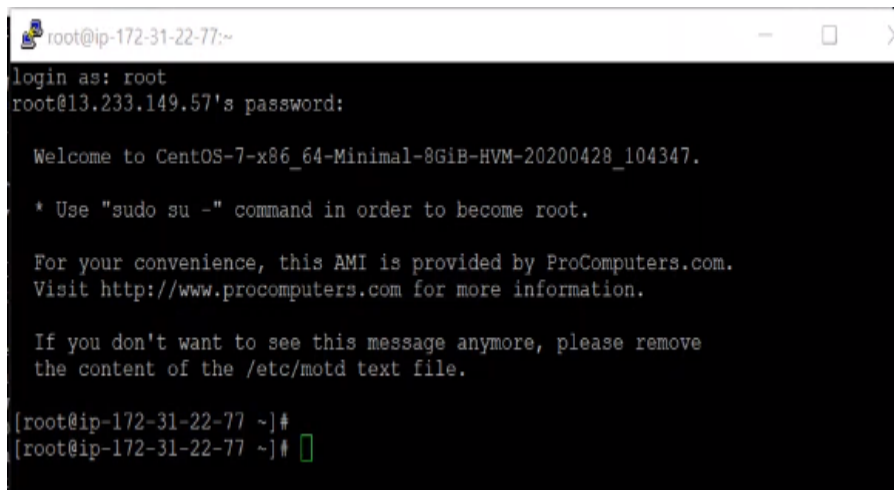
```
sudo systemctl restart sshd
```

8. Open a new PuTTY session, do the following, and then click **Open**:

- Host Name (or IP address) – Type the IP address or host name.
- Connection type – Select **SSH** as connection type.
- Port – Type the port value. The default port value is 22.



9. Log into the VM as a root user.



10. To transfer files to your Linux instance, use WinSCP. For more information, see [Transferring Files to Linux Instance using WinSCP](#).

Install Engine on Replica

To install Engine on Replica server, see [Installing Engine](#).

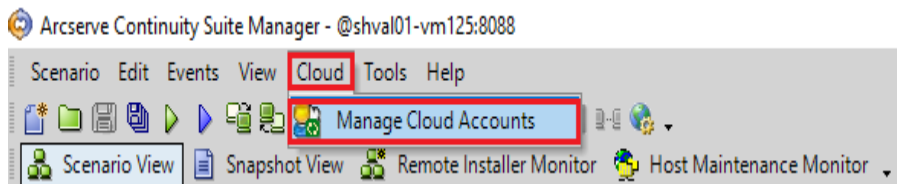
Create Full System Scenario for Amazon EC2

Arcserve Live Migration supports both Windows and Linux for Full System scenario. If the source server is Windows, then the Virtual Appliance (VA) must be Windows. If the source server is Linux, then the VA must be Linux as well.

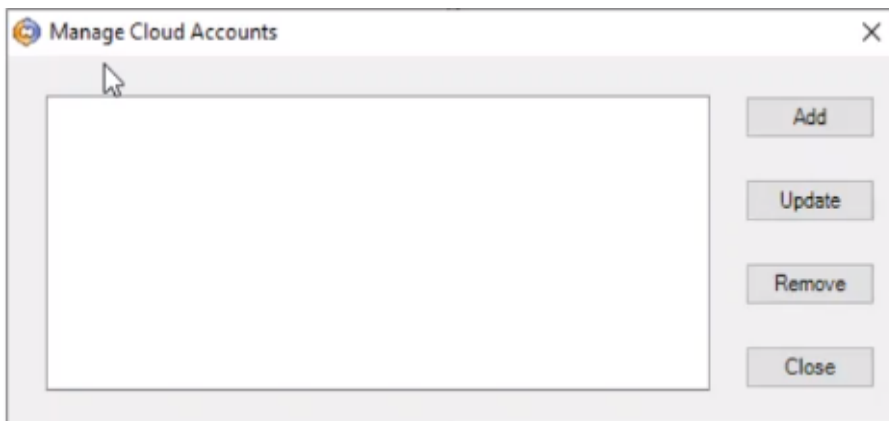
Before you create a scenario, add Amazon EC2 Cloud Account in Continuity Suite Manager.

To Add an Amazon EC2 Cloud Account in Continuity Suite Manager, follow these steps:

1. On the Continuity Suite Manager, navigate to **Cloud > Manage Cloud Accounts**.



2. On the Manage Cloud Accounts screen, click **Add**.

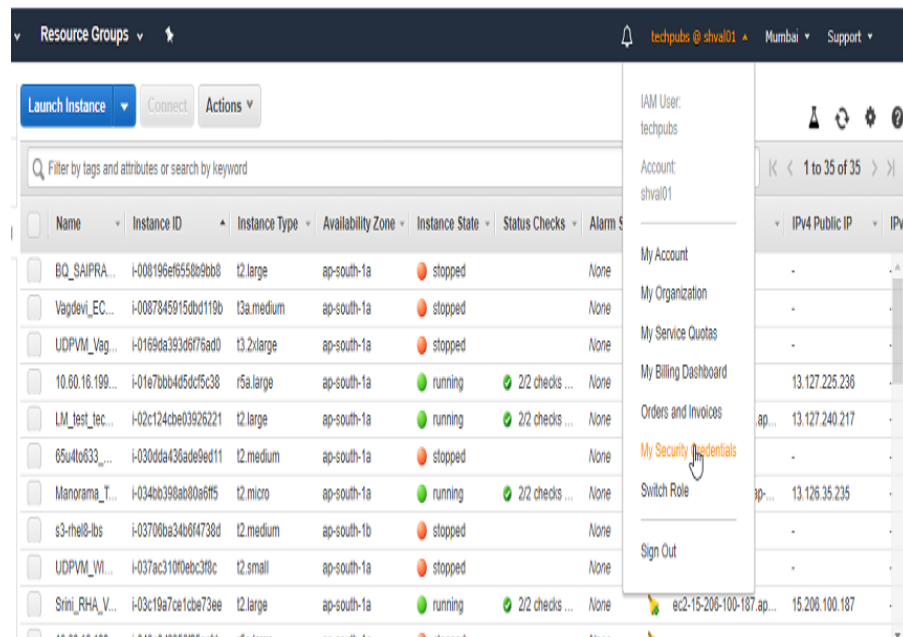


3. On the Add Cloud Account screen, enter the following details in the required fields, and then click **OK**.
 - **Cloud Provider** - Select Amazon EC2 as a Cloud Provider.
 - **Cloud Account** - Enter the account name you had defined while creating the AWS account.
 - **Access Keys (access key ID and secret access key)** - Access keys are long-term credentials for an IAM user or the AWS account root user. Access Key Id (for example, AKIAIOSFODNN7EXAMPLE) and Secret Access Key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY) are used to sign

programmatic requests to the AWS CLI or AWS API, like a user name and password are used to access your AWS Management Console.

To generate Access Keys, follow these steps:

- a. On the top right corner, go to your Amazon account name, and then select **My Security Credentials**.



- b. On the My security credentials page, click the **Create access key** button.



Important! If you lose or forget your secret access key, you cannot retrieve it later. Instead, create a new access key, and make the old key inactive.

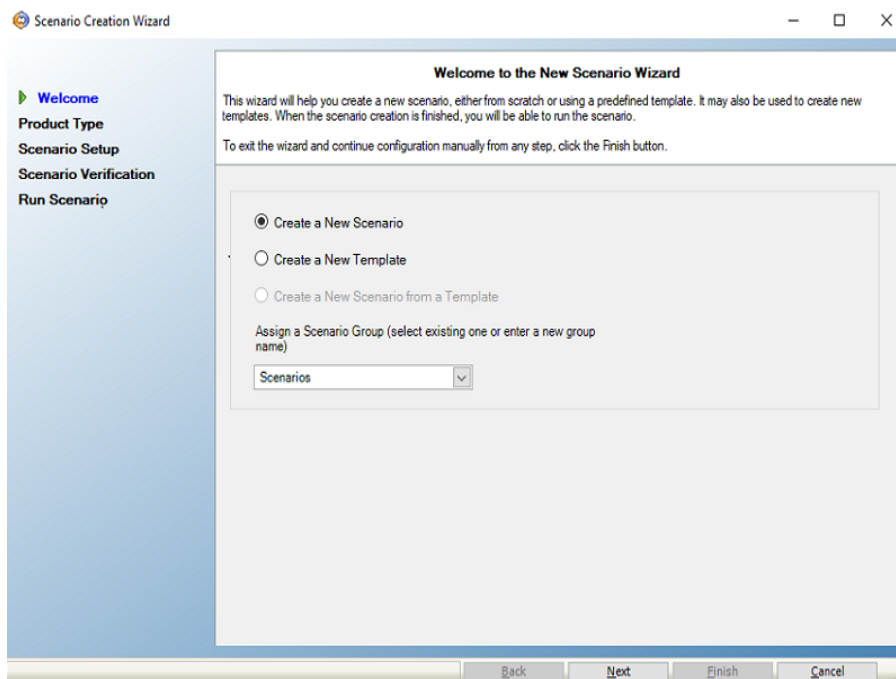
The Amazon EC2 account for Live Migration is now configured.

Creating Full System Scenario for Amazon EC2

This section provides instructions on how to create full system scenario for Amazon EC2.

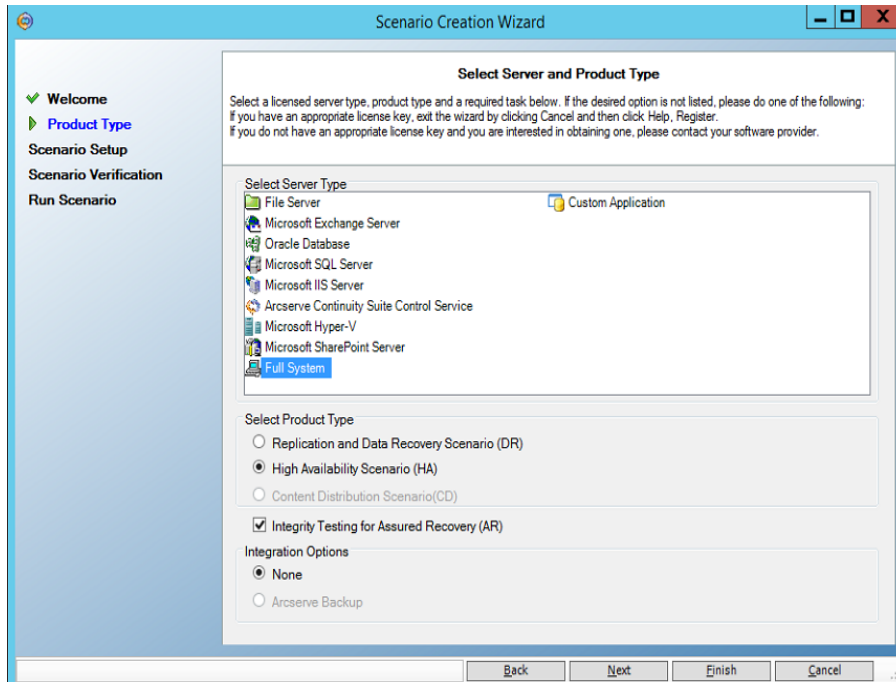
Follow these steps:

1. Open the Arcserve Continuity Suite Manager, navigate to **Scenario>New** or click the **New Scenario** button to launch the wizard.
2. On the Welcome to the New Scenario Wizard screen, select **Create a New Scenario**, select a Scenario Group from the **Assign a Scenario Group** drop-down list, and then click **Next**.

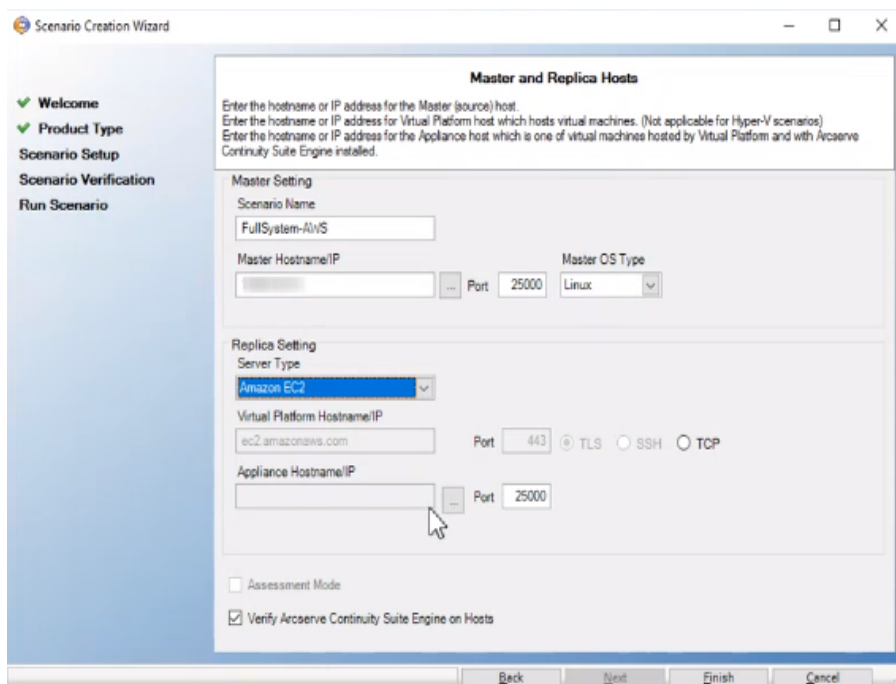


3. On the Select Server and Product Type screen, select Full System, High Availability Scenario (HA), and then click **Next**.

Note: To perform Assured Recovery testing, select the **Integrity Testing for Assured Recover (AR)** check box.



4. On the Master and Replica Hosts screen, do the following, and then click **Next**:

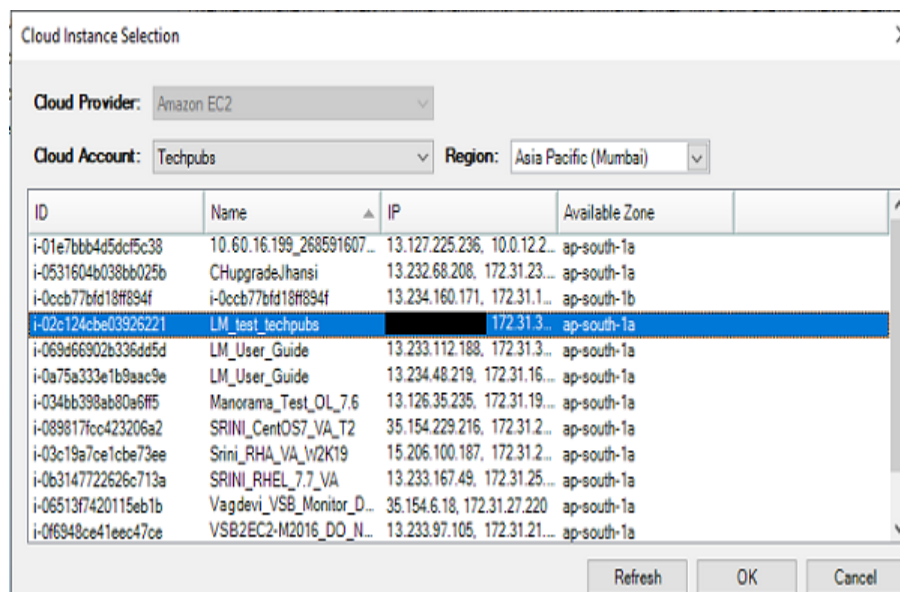


- **Scenario Name** - Enter a Scenario Name. The default value is the scenario type, for example, Full System.
- **Master Hostname/IP** - Enter the IP address of a physical machine you want to protect.
- **Master OS Type** - Select Linux as the Master OS Type.

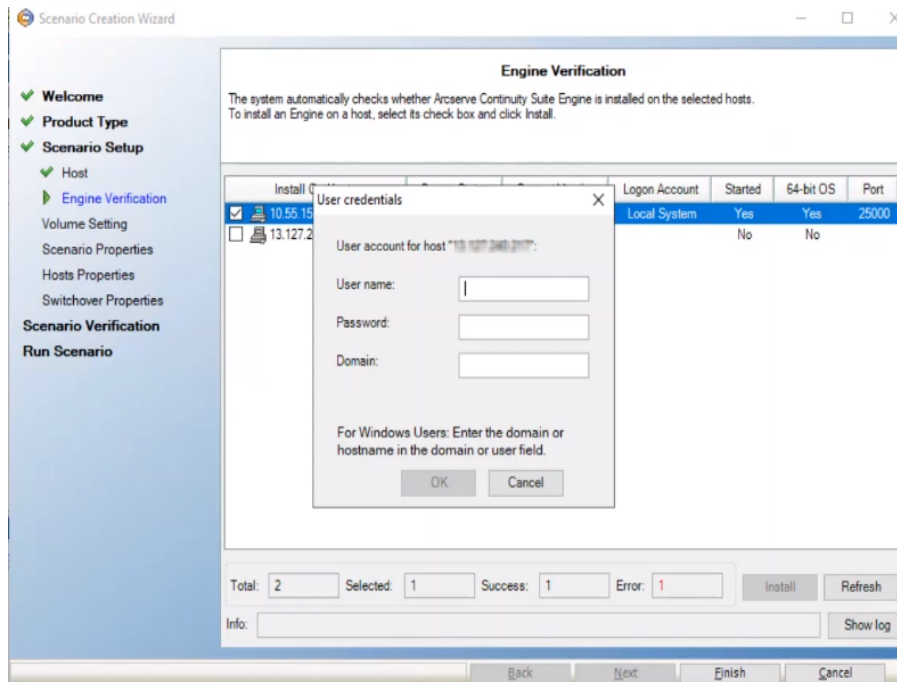
- **Server Type** - Select Amazon EC2 as the Replica server.
- **Appliance Hostname/IP** - Browse the Appliance Hostname/IP to select the Replica server.

Note: Use the **Verify Arcserve Continuity Suite Engine on Hosts** to verify the connectivity between Master and Replica. It verifies that the engines are installed on the Master. To skip verification, clear the check box.

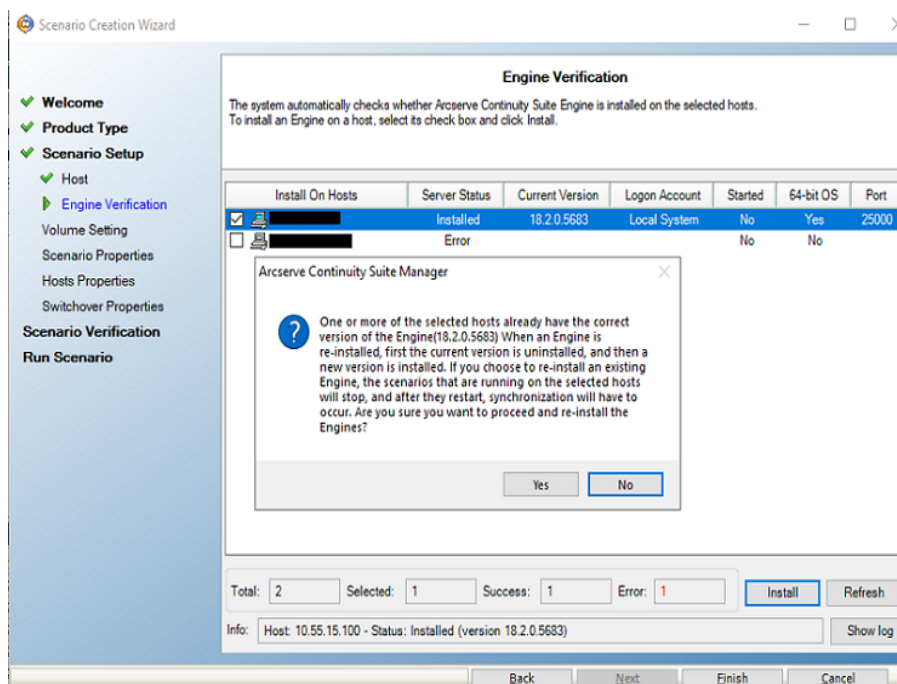
On the Cloud Instance Selection dialog, from the Region drop-down list, select the region. The list refreshes to display the relevant EC2 instances. From the list, select the EC2 instance you had created, and then click **OK**.



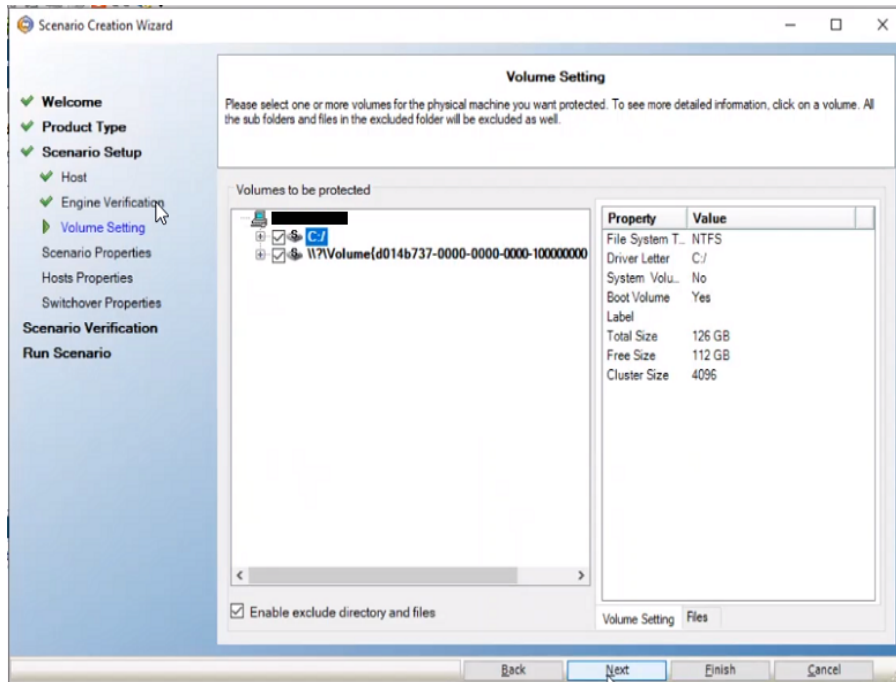
5. On the Engine Verification screen, the User credentials screen appears. Enter the User name and Password, and then click **OK**.



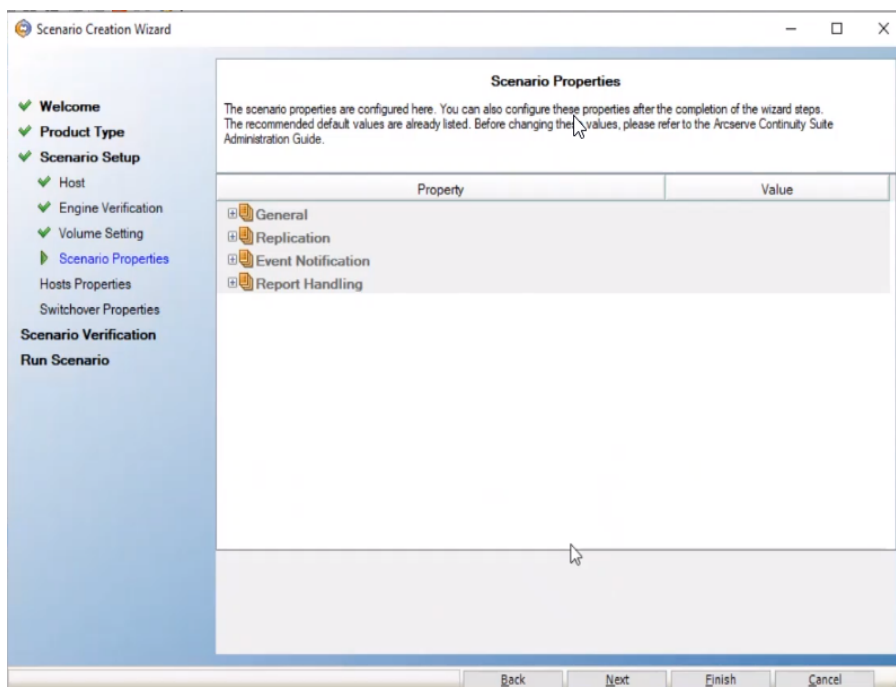
Wait for Engine verification to complete, and then click **Next**.



- On the Volume Setting screen, select one or more volumes for the physical machine you want to protect, and then click **Next**.



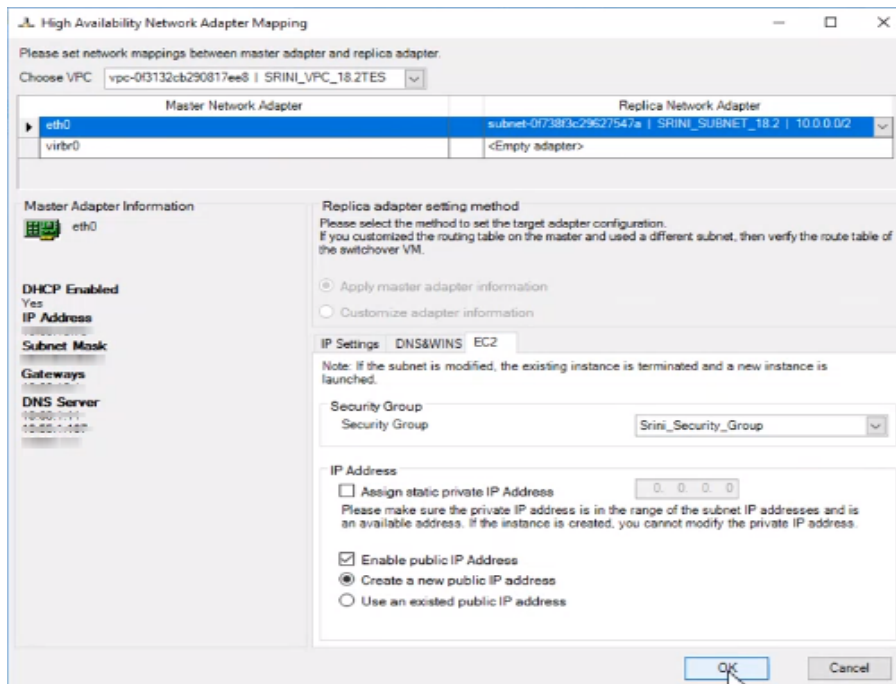
7. On the Scenario Properties screen, click **Next**.



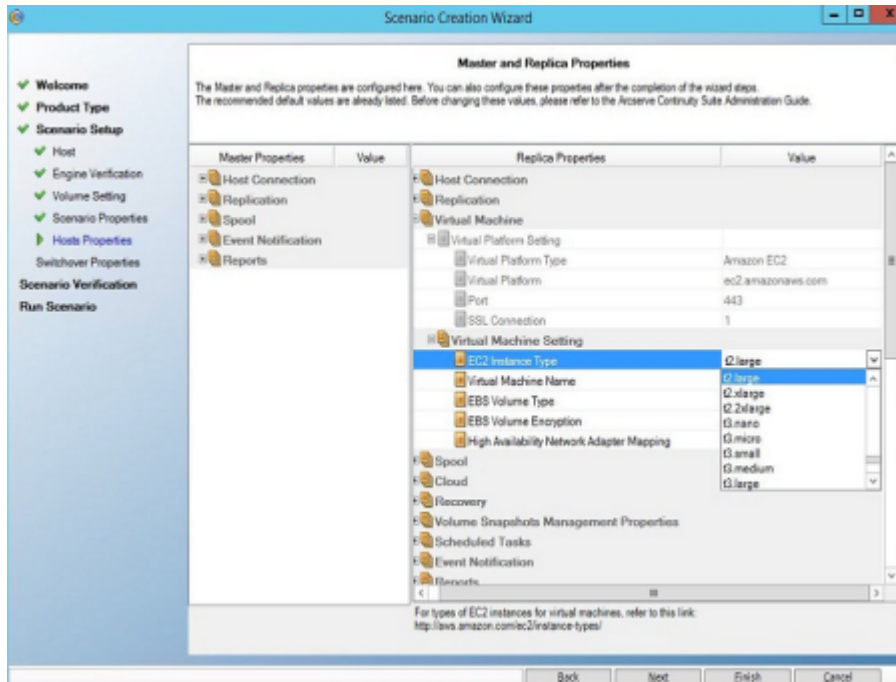
8. On the High Availability Network Adapter Mapping dialog, enter the following details, and then click **OK**.

- **Choose VPC** - Select VPC from the drop-down list.
- **Replica Network Adapter** - Select the Replica network adapter from the drop-down list.
- **Security Group** - Select **default** from the drop-down list.

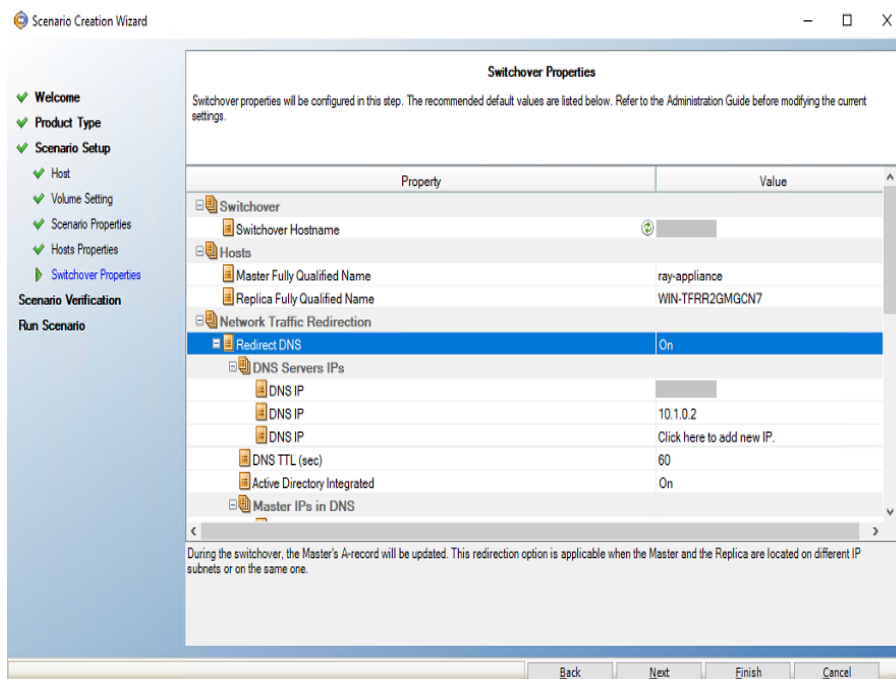
- **IP Address** - Select one of the following:
 - Assign static private IP Address
 - Enable public IP address
 - If you want to create a new public IP address, enable the **Create a new public IP address** option.
 - If you want to connect to the virtual machine from outside your network, enable the **Use an existed public IP address** option.



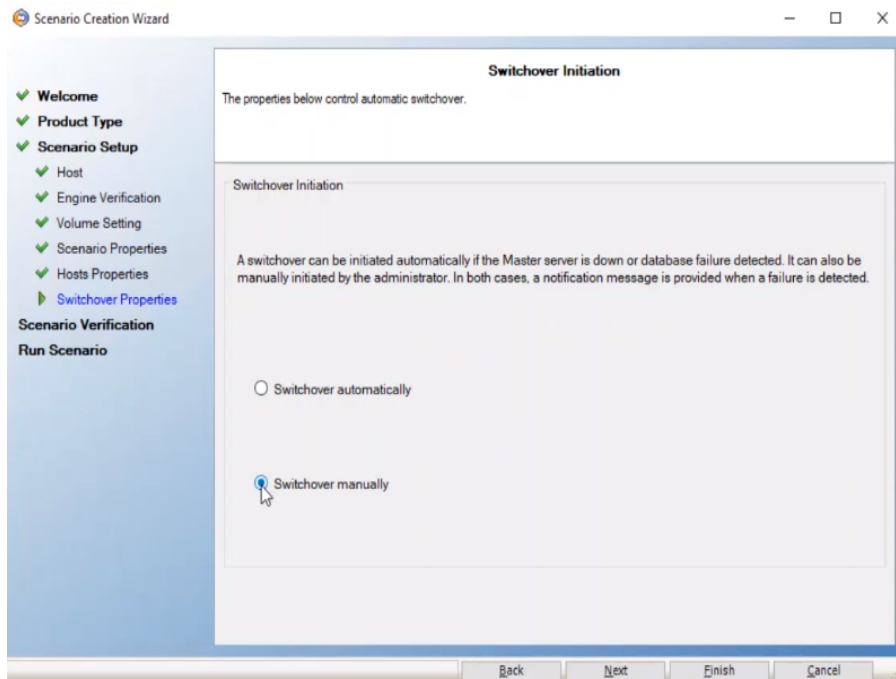
9. On the Master and Replica Properties screen, navigate to **Virtual Machine > Virtual Machine Setting > EC2 Instance Type**, select the instance type, and then click **Next**.



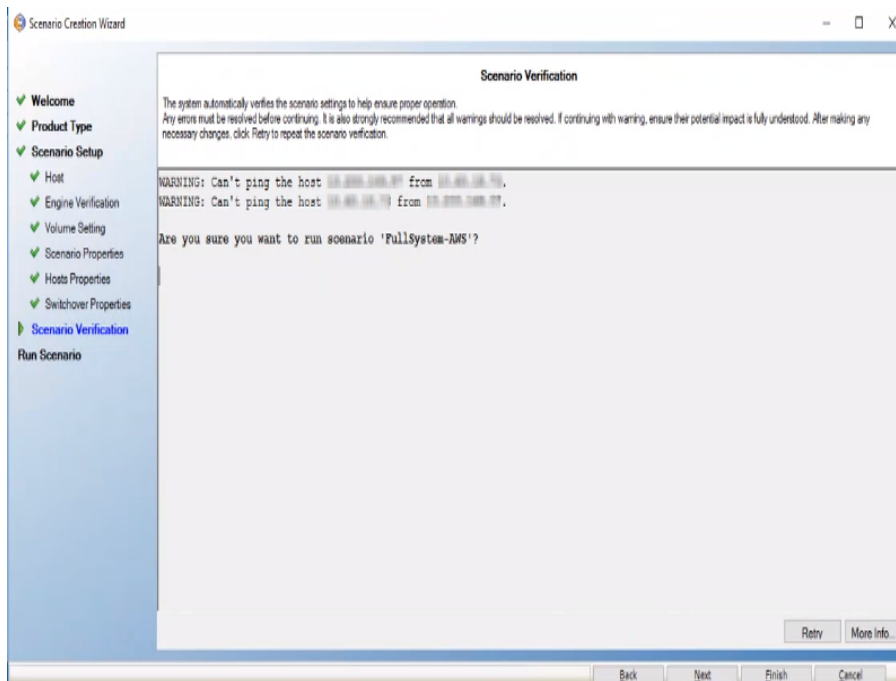
10. On the Switchover Properties screen, accept the default values or modify the values, and then click **Next**.



11. On the Switchover Initiation screen, specify if the switchover start automatically or manually, and then click **Next**.

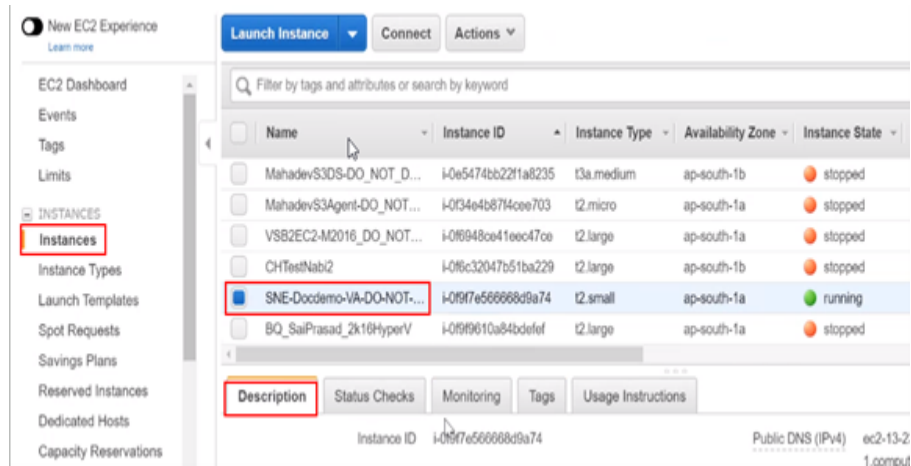


12. On the Scenario Verification screen, click **Next**.

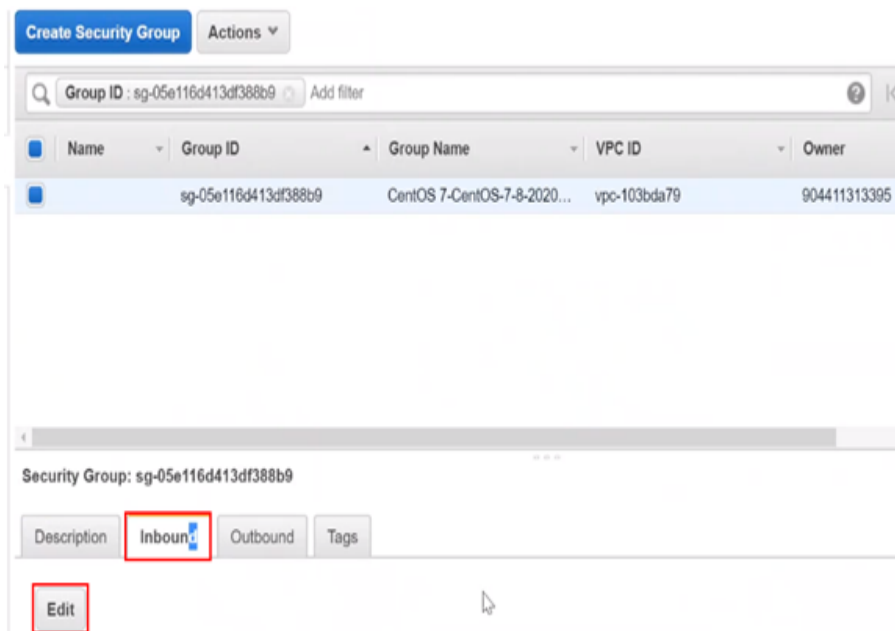


If the Master and Replica servers fail to ping each other, do the following ICMP settings:

- On the Instances page, select your Linux instance, click **Description**, and then click the link beside Security group.



- b. On the Create Security Group page, select **Inbound**, and then click **Edit**.



- c. On the Edit inbound rules page, do the following, and then click **Save**:
- Type: Custom ICMP Rule - IPv4
 - Protocol: All
 - Port Range: N/A
 - Source: 0.0.0.0/0
 - Description: Ping

Type	Protocol	Port Range	Source	Description
Custom TCP	TCP	25000	Custom 0.0.0.0/0	Engine
Custom ICMP	All	N/A	Custom 0.0.0.0/0	Ping
SSH	TCP	22	Custom 0.0.0.0/0	SSH

Add Rule

Now, the Master server can communicate with Replica server.

- On the Scenario Run screen, to start synchronization immediately and activate the scenario, click **Run Now**. To save and run the scenario later, click **Finish**.

Scenario Run

The scenario has been configured and is ready to run. Press Run Now to start the scenario. Initial data synchronization will start automatically after pressing the Run Now button. To run scenario later press the Finish button.

Scenario 'FullSystem' is ready to run

Product type	High Availability Scenario (HA)
Server type	Full System
Integrity Testing for Assured Recovery	Off
Replication mode	Online

Master

Name	
Spool size (MB)	Unlimited
Spool path	[INSTALLDIR]/tmp/spool

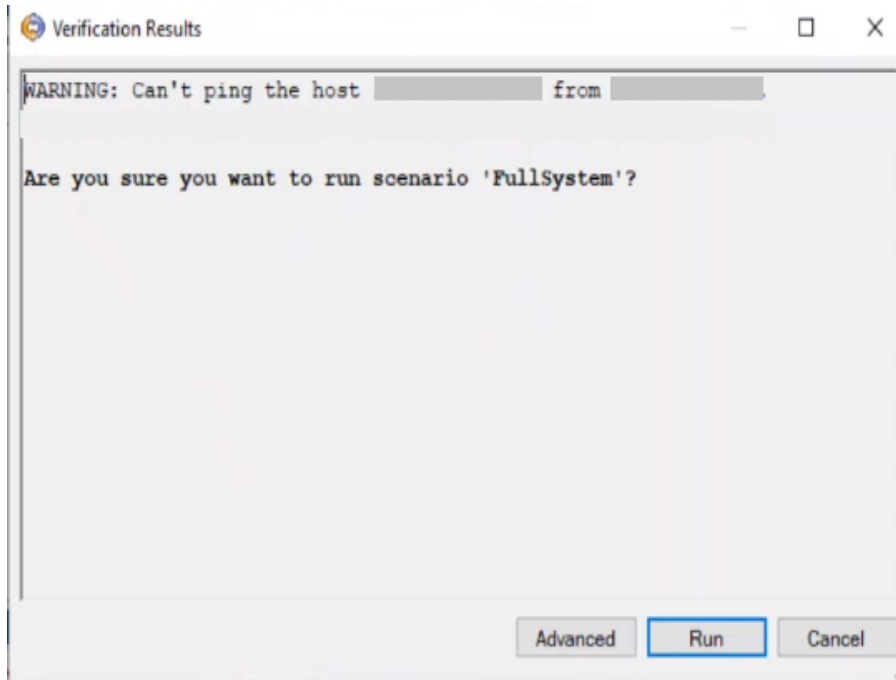
Replica

Name	
Spool size (MB)	Unlimited
Spool path	[INSTALLDIR]/tmp/spool

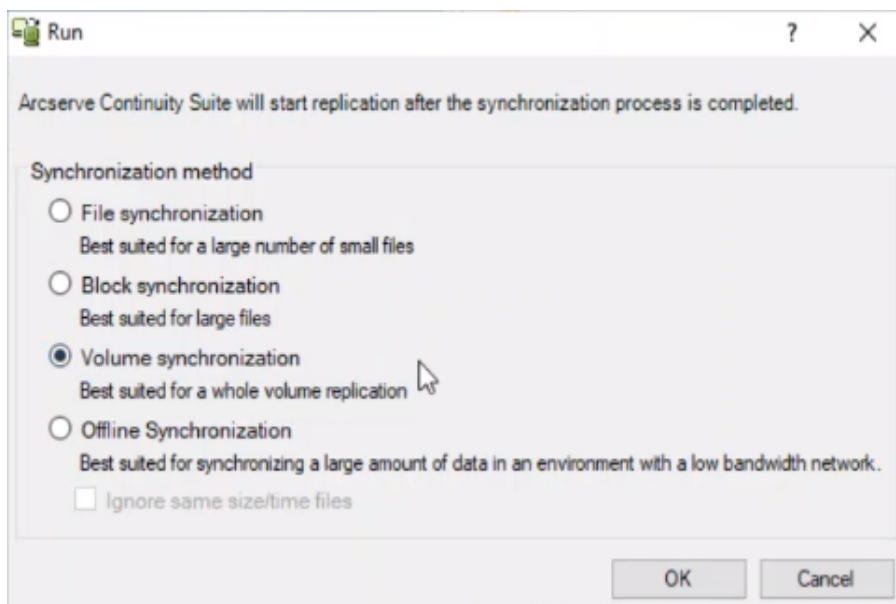
Back Run Now Finish Cancel

The scenario verification runs automatically, and the Verification Results screen appears.

- On the Verification Results screen, click **Run**.



15. On the Run screen, select **Volume synchronization**, and then click **OK**.



Note: For initial synchronization, we recommend that you select **Volume synchronization**, as it usually provides better synchronization performance over LAN or WAN.

The synchronization between Master and Replica servers starts. Wait for synchronization to complete.

Scenarios

Scenario	Status	Position	Source	Mode
FullSystem-AWS	Running	HA/HA	Full System	Online
Home	Changed	Set Data	Set File	In good
71.77 KB	2.76 MB	0	2.76 MB	9.05 MB
0.00 B/s	-	-	2.76 MB	14.40 MB

Scenario Statistics

Active: 1% of total, 1.1% of total, 7.17 KB, 7.17 KB

StandBy: 1% of total, 1.1% of total, 14.40 MB, 14.40 MB

Synchronization in progress

Logs

Message ID	Sequence	Severity	Host Scenario	Time	Event
SM00165	31	Significant	Backward FullSystem-AWS	9/15/2020 5:57:07 PM	Connected to 10.100.100.100
SM00164	30	Significant	Backward FullSystem-AWS	9/15/2020 5:57:06 PM	Connection with 10.100.100.100 is lost
SP00402	29	Significant	10.100.100.100	9/15/2020 5:56:46 PM	Suspend to allow checks
SP00401	28	Significant	10.100.100.100	9/15/2020 5:56:46 PM	Resume to allow checks
PS0001	27	Info	10.100.100.100	9/15/2020 5:56:43 PM	The replica environment is ready for use
PS00106	26	Info	10.100.100.100	9/15/2020 5:56:37 PM	Mounting disk 2510270400_01204000707661
PS00104	25	Info	10.100.100.100	9/15/2020 5:56:33 PM	Creating disk 2510270400_01204000707661
PS00010	24	Info	10.100.100.100	9/15/2020 5:56:33 PM	Preparing replica environment
SP000129	23	Significant	10.100.100.100	9/15/2020 5:56:28 PM	Starting Block Synchronization (Include files with the same size and modification time) (from WIN-RTMAPPON.ARCserve.COM by user WIN-RTMAPPON Administrator)
SP00014	22	Significant	10.100.100.100	9/15/2020 5:56:27 PM	Starting scenario FullSystem-AWS (from WIN-RTMAPPON.ARCserve.COM by user WIN-RTMAPPON Administrator)
PS00102	21	Info	10.100.100.100	9/15/2020 5:56:05 PM	Save scenario (from WIN-RTMAPPON.ARCserve.COM by user WIN-RTMAPPON Administrator)

Perform Assured Recovery Testing

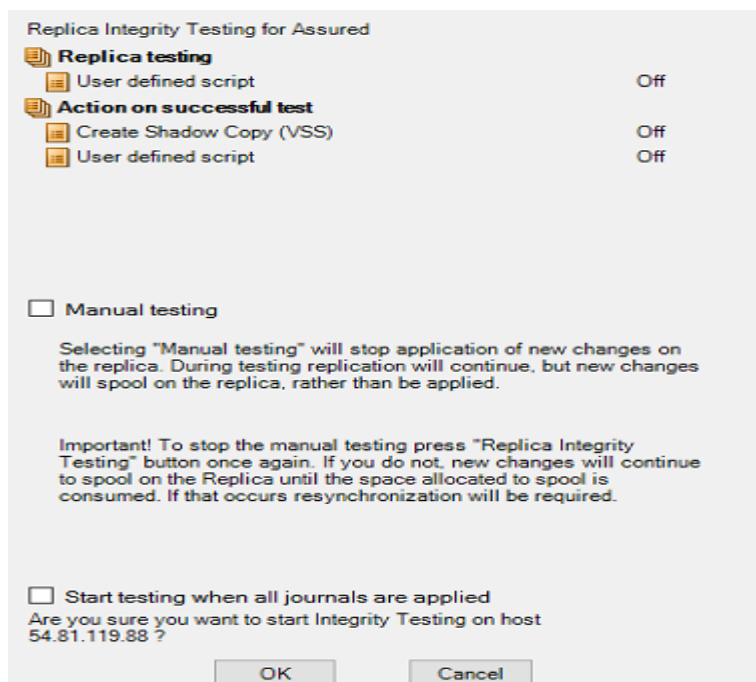
Note: Perform the Assured Recovery test only if you have enabled the **Integrity Testing for Assured Recovery (AR)** option on the Select Server and Product Type screen.

You can fully automate the Assured Recovery tests and schedule these tests as often as needed. On completion, an alert is sent to the appropriate personnel with the test status. You can also trigger additional actions such as taking a VSS snapshot of the data or running a backup. Alternatively, you can perform AR testing in a non-scheduled mode, and initiate the tests automatically or manually.

To perform AR test automatically, follow these steps:

1. On the Arcserve Continuity Suite Manager, verify that the AR scenario is running.
2. On the Standard toolbar, click the **Replica Integrity Testing** button, or right-click the Replica and select **Replica Integrity Testing** from the shortcut menu.

The Replica Integrity Testing for Assured dialog opens.

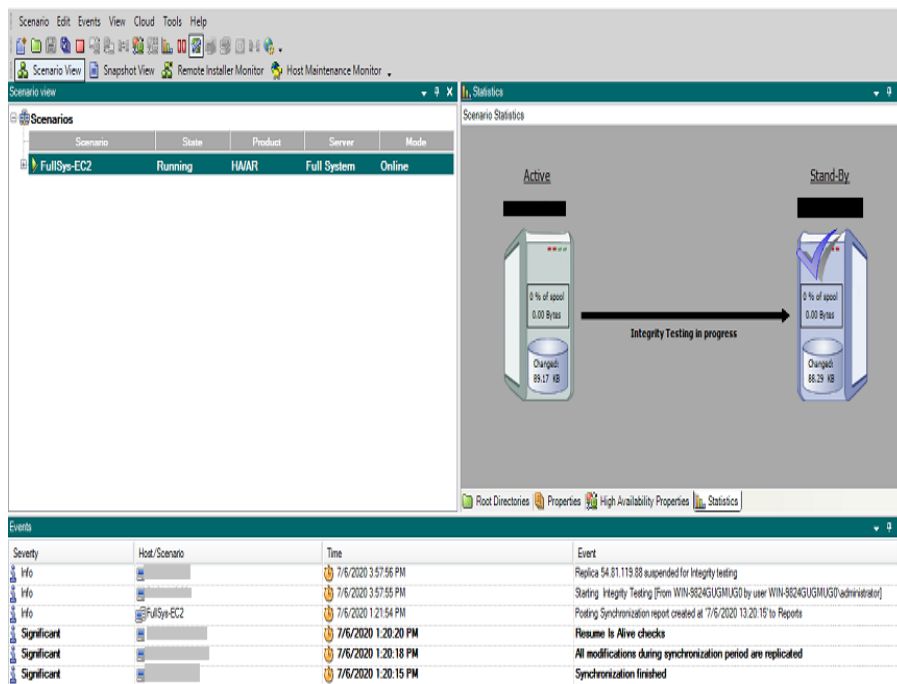


3. To start automatic AR test using the existing configuration, click **OK**.

Notes:

- To start the AR test manually, select the **Manual testing** checkbox, and then click **OK**.
- To change the test configuration before running the test, click **Cancel**. For more information, see [Configure Assured Recovery Properties](#).
- Before the test begins to run, Arcserve Live Migration verifies that no synchronization, AR test or replication suspension tasks are in progress on any of the hosts that participate in the current scenario.

After the verification completes, the AR test begins.



The steps of the test are displayed as messages in the Event pane.

After the test is finished, the Replica is automatically restored to the same state it was when the replication was suspended. The changes that were accumulated in the spool gets applied, and the replication resumes.

The screenshot displays the Veeam Backup & Replication interface. The top-left pane shows the 'Scenarios' list with columns for Scenario, State, Product, Server, and Mode. The 'FullSystem-RH8-EC2' scenario is selected and in a 'Running' state. The top-right pane shows 'Scenario Statistics' with a diagram of two servers, 'Active' and 'Stand-By', connected by a 'Replication' arrow. The bottom pane shows the 'Events' log with columns for Severity, Host/Scenario, Time, and Event. The events list shows four entries related to the FullSystem-RH8-EC2 scenario, including information about replication, integrity testing, and report generation.

Scenario	State	Product	Server	Mode
FullSys-Cent8.1	Editing	HAVAR	Full System	Online
FullSys-RH8-EC2	Running	HAVAR	Full System	Online

Hosts	Changed	Sent Data	Sent Files	Received Data	Received Files	In pool
Full4cndd7a060	147.04 MB	2.00 GB	65886	-	-	0.00 Bytes

Severity	Host/Scenario	Time	Event
Info	FullSys-RH8-EC2	7/8/2020 3:58:12 PM	Replication to replica 3.89.233.115 resumed after integrity testing
Significant	FullSys-RH8-EC2	7/8/2020 3:58:11 PM	FullSystem Integrity Testing on replica 3.89.233.115 is finished
Error	FullSys-RH8-EC2	7/8/2020 3:58:11 PM	Automatic FullSystem testing on replica 3.89.233.115 is unsuccessful
Info	FullSys-RH8-EC2	7/8/2020 3:58:12 PM	Posting Assured Recovery report created at 7/8/2020 15:58:11 to Reports

By default, after the AR test is performed, an Assured Recovery Report is generated.

Notes:

- If the Assured Recovery Report is not generated, on the Replica Properties list, under the Reports group, check the value of the Generate Assured Recovery Report property.
- To view the report, see [View a Report](#).

All the tasks that were performed during the AR test are listed in the AR Report, along with their activation time and status.

Perform Cut off/Switchover

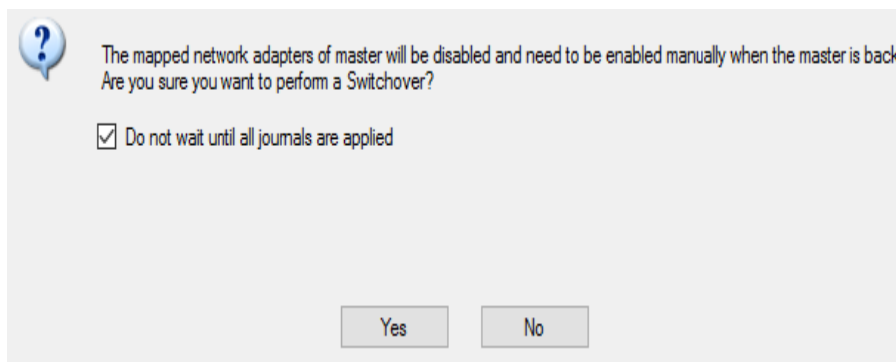
Switchover (or failover) is the process of changing roles between the Master and Replica, that is, making the Master server the standby server, and the Replica server the active server.

Switchover can be triggered automatically by Arcserve Live Migration when it detects that the Master is unavailable (failover). Alternatively, Arcserve Live Migration can simply alert you to the problem, and then you can manually initiate switchover from the Manager.

To perform switchover, follow these steps:

1. Open the Manager and then select the required scenario from the Scenario pane. Verify if it is running.
2. On the standard toolbar, click the **Perform Switchover** button, or select the Perform Switchover option from the **Tools** menu.

A confirmation message appears.



3. [Optional] Select the **Do not wait until all journals are applied** check box to immediately perform switchover even before all journals are applied. If you do not select this check box, the switchover process gets initiated only after all journals are applied.
4. Click **Yes** on the confirmation message. This procedure initiates a switchover from the Master server to the Replica server.

During switchover, the Event pane gives detailed information about the switchover process.

The screenshot shows the 'Scenario view' and 'Statistics' panels. The 'Scenario view' table lists scenarios with columns: Scenario, State, Product, Server, and Mode. The 'Statistics' panel shows a diagram of two servers, 'Active' and 'Stand-By', connected by a 'Replication' arrow. The 'Active' server has 1% of data replicated, and the 'Stand-By' server has 1% of data replicated. The 'Statistics' panel also shows 'Root Directories', 'Properties', 'High Availability Properties', and 'Statistics' tabs.

Scenario	State	Product	Server	Mode
FullSys-Cent8.1	Editing	HA/AR	Full System	Online
FullSys-RH8-EC2	Running	HA/AR	Full System	Online

Hosts	Changed	Sent Data	Sent Files	Received Data	Received Files	In pool
Full4cedd2a960	147.04 MB	2.00 GB	65886	-	-	0.00 Bytes

After the switchover is complete, the scenario gets stopped.

Note: The only case in which the scenario may continue to run after switchover is when **automatic reverse replication** is defined as **Start automatically**.

When the switchover is completed, the Event pane displays the *Switchover completed* message.

The screenshot shows the 'Scenario view' and 'High Availability Properties' panels. The 'Scenario view' table lists scenarios with columns: Scenario, State, Product, Server, and Mode. The 'High Availability Properties' panel shows a list of properties: Switchover, Hosts, Network Traffic Redirection, Is Alive, DB Management, and Action upon Success. The 'Events' panel shows a list of events with columns: Host/Scenario, Time, and Event.

Scenario	State	Product	Server	Mode
FullSys-Cent8.1	Editing	HA/AR	Full System	Online
FullSys-RH8-EC2	Connecting...	HA/AR	Full System	Online

Hosts	Changed	Sent Data	Sent Files	Received Data	Received Files	In pool
Full4cedd2a960						

Property	Value
Switchover	
Hosts	
Network Traffic Redirection	
Is Alive	
DB Management	
Action upon Success	

Host/Scenario	Time	Event
	7/8/2020 4:08:18 PM	Switchover completed. The Amazon EC2 instance i-062956b8bd7a5114 with same name of master is currently active
3.89.233.115	7/8/2020 4:08:18 PM	The virtual machine is now online.
3.89.233.115	7/8/2020 4:04:34 PM	Checking the alive status of the virtual machine.
3.89.233.115	7/8/2020 4:04:34 PM	Enable Full System resources successfully

Now, the original Master becomes the Replica, and the original Replica becomes the Master.

