

# Quick Start Guide for AWS (Windows)

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

---

<b>Chapter 1: Introduction</b>	<b>5</b>
Overview	6
Terminologies	7
Requirements	9
Software Compatibility	10
<b>Chapter 2: Perform Live Migration</b>	<b>11</b>
Install Components on Master	12
Installing Control Service	13
Installing Engine	20
Configure Amazon EC2	25
Provision VA on Amazon EC2	26
How to Get Windows Password	36
How to Change EC2 VM Password	39
Install Engine on Replica	41
Create Full System Scenario for Amazon EC2	42
Creating Full System Scenario for Amazon EC2	45
Perform Assured Recovery Testing	57
Perform Cut off/Switchover	60

---

## 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.

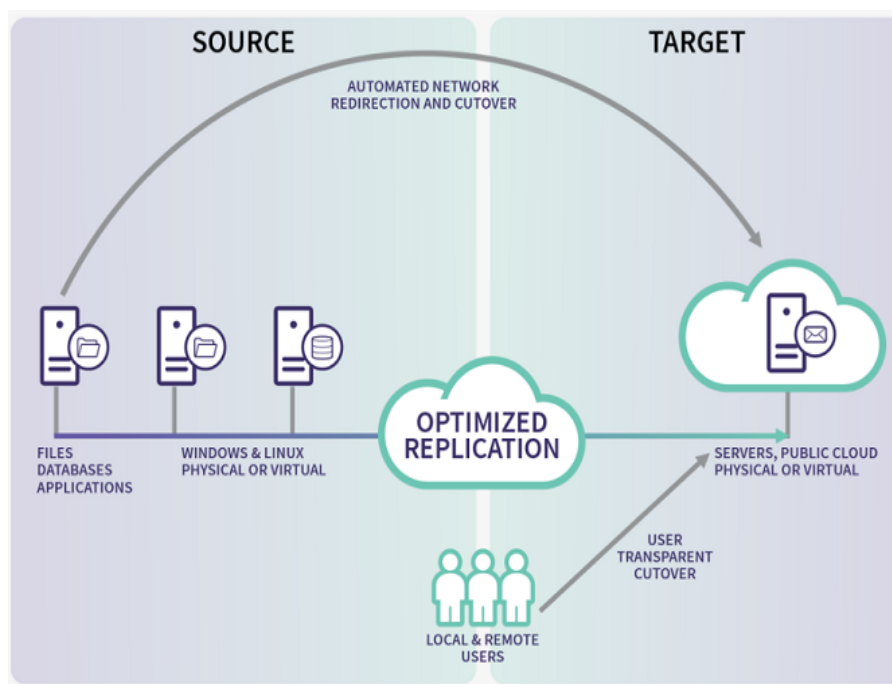
- For each license, Live Migration provides free of cost technical assistance for two incidents.

**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

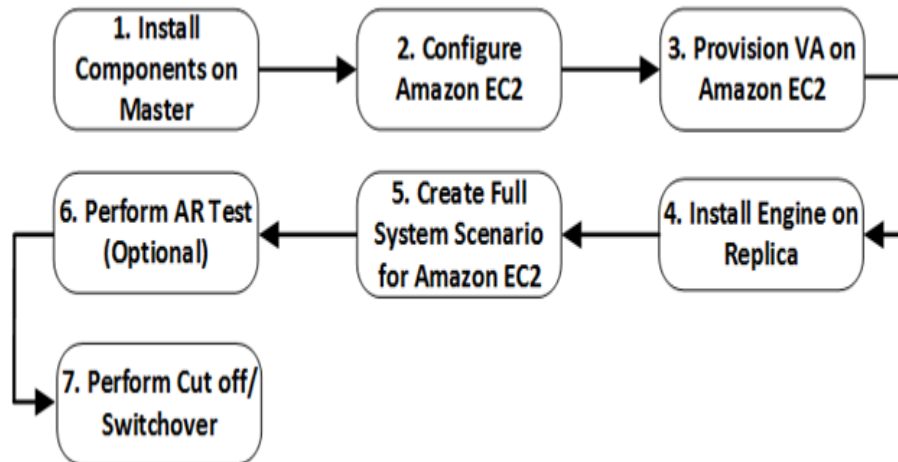
For more information about compatibility, see [Compatibility Matrix](#).

**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

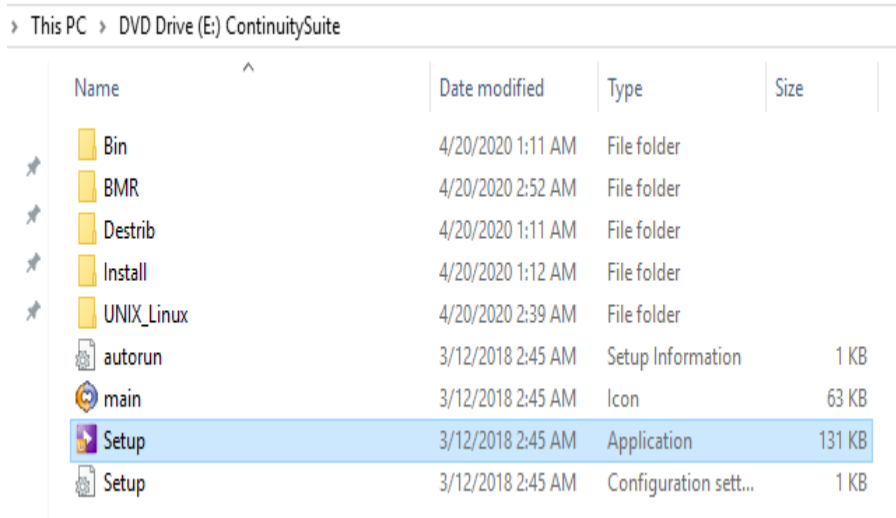
This section describes how to install the Arcserve Continuity Suite Control Service and Engine on Master.

## 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 file 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**.

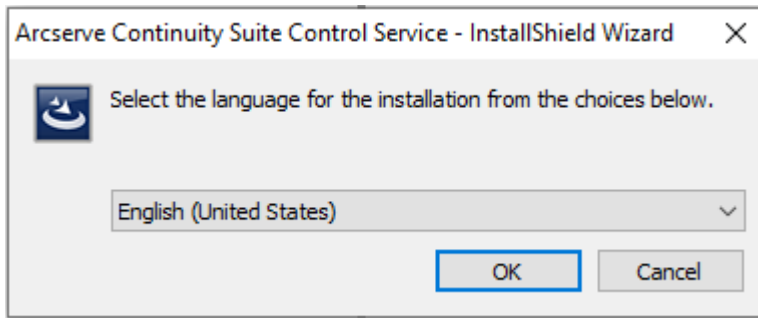


The wizard displays the components.

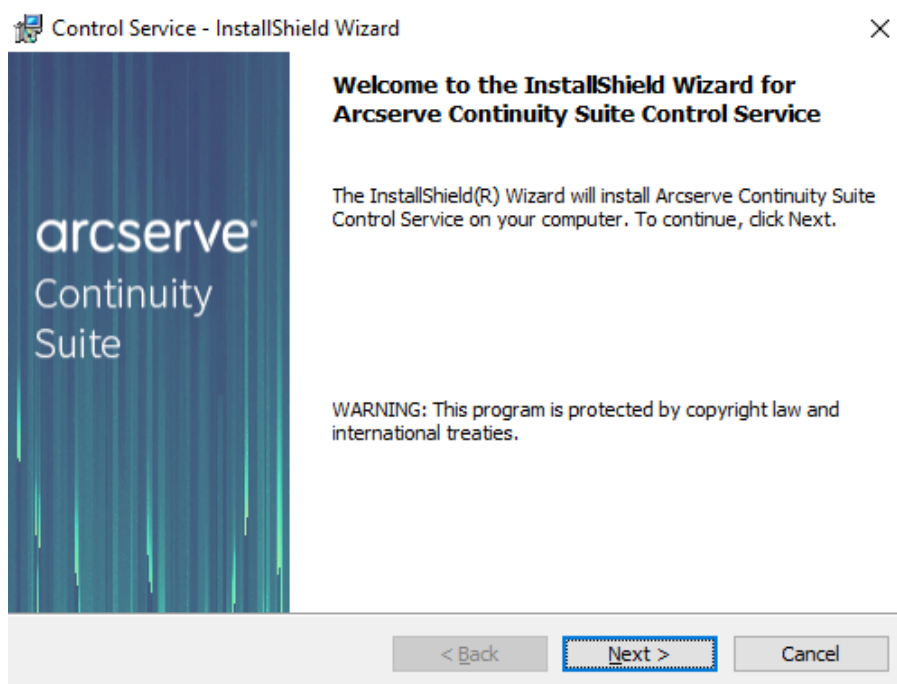
4. Click **Install Control Service**.



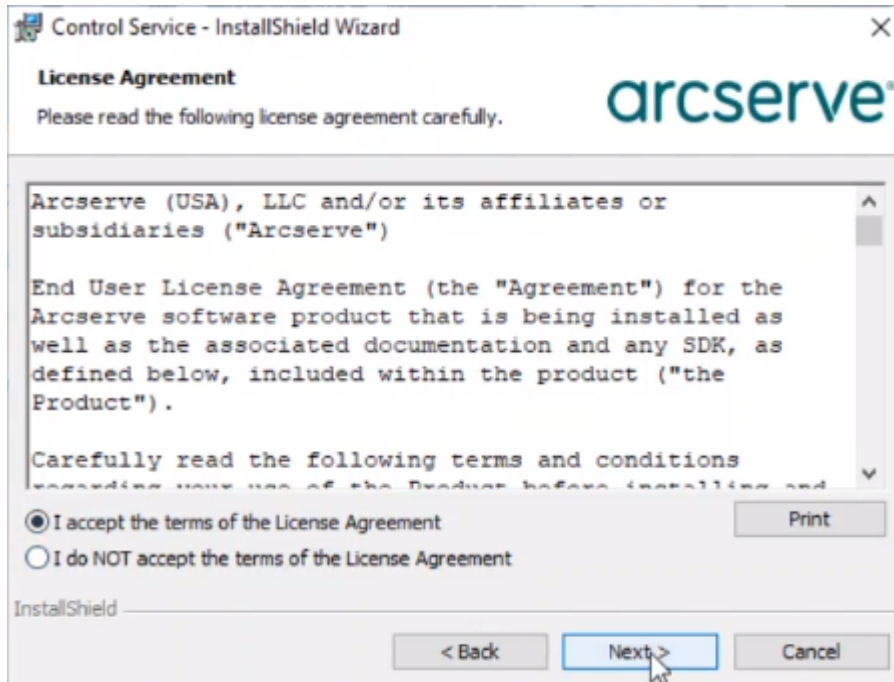
5. On the Arcserve Continuity Suite Control Service - InstallShield Wizard, from the drop-down list, select your preferred language, and then click **OK**.



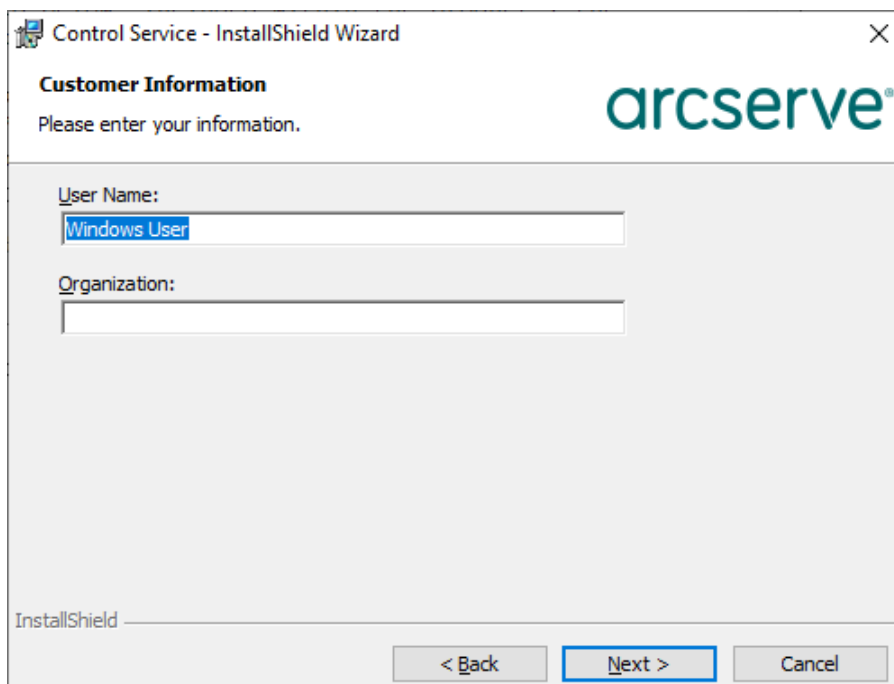
After the initial process is complete, the Welcome page appears.



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**.

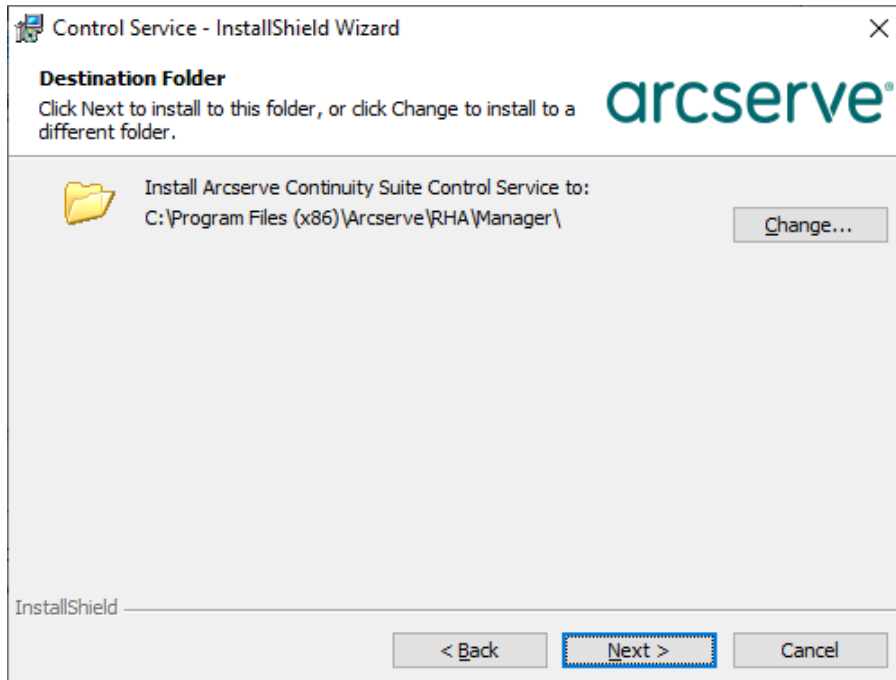


8. On the Customer Information page, enter a user name, and then click **Next**.



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



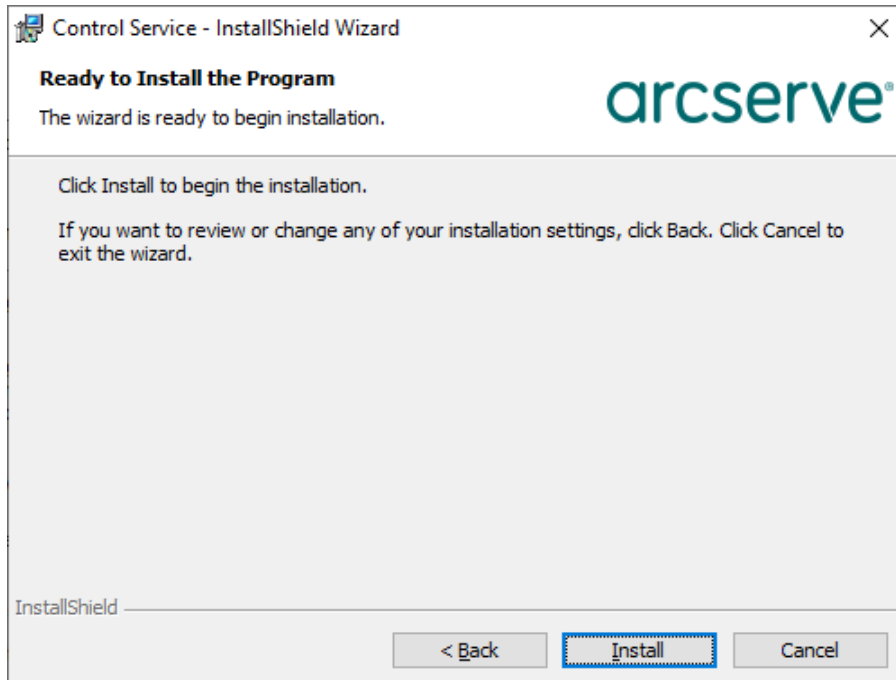


**Note:** The default installation directory is: *C:\Program Files (x86)\Arcserve\RHA\Manager*. All executables, DLLs and configuration files are located within the INSTALLDIR.

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

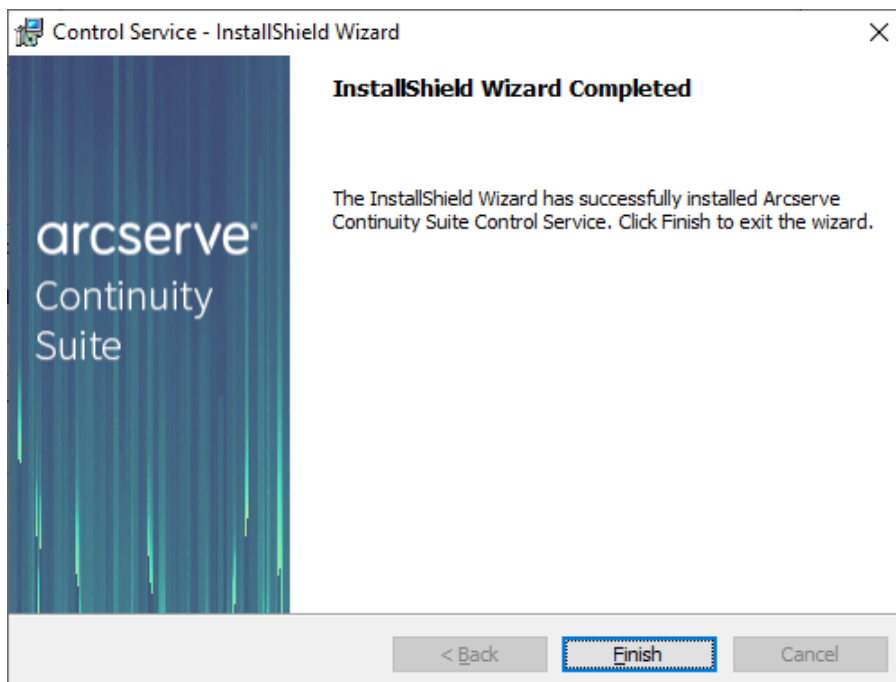
**Note:** For more information about how to configure SSL Configuration, Service Logon Information, and Control Service Role, see [Install a Control Service for a Standard Operation](#).

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



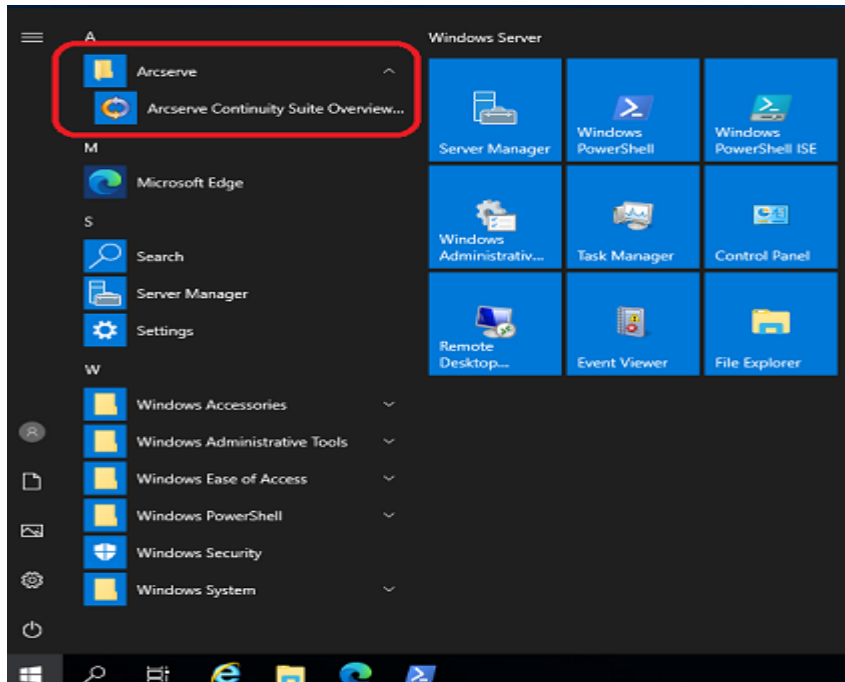
**Note:** Click the **Back** button to return to the previous pages and change any configuration as needed.

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.

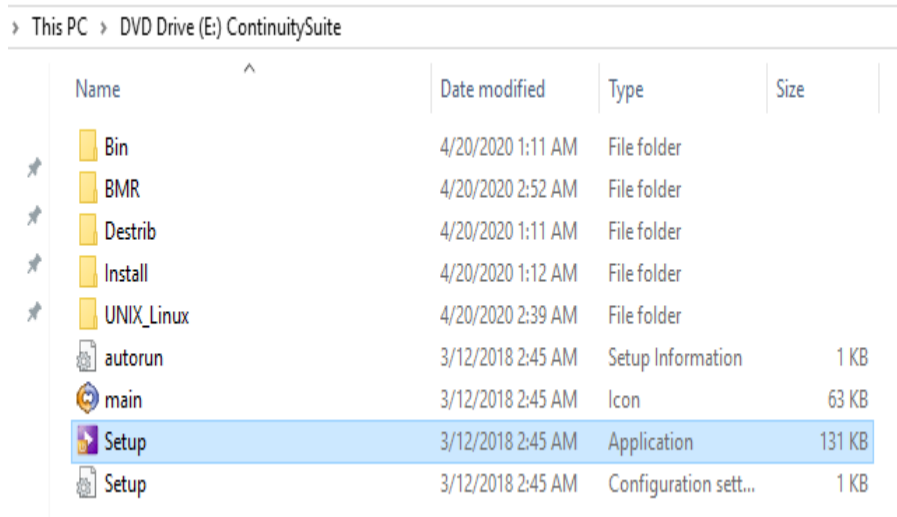


## Installing Engine

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. Download [RHA iso for Continuity Suite](#), and then open the folder.
2. Open the Continuity Suite mounted directory, and then 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**.

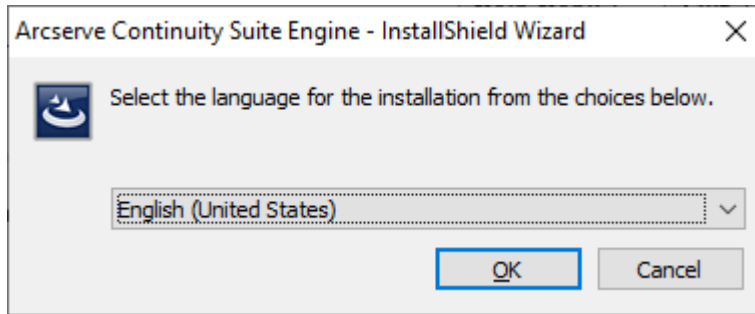


The wizard displays the components.

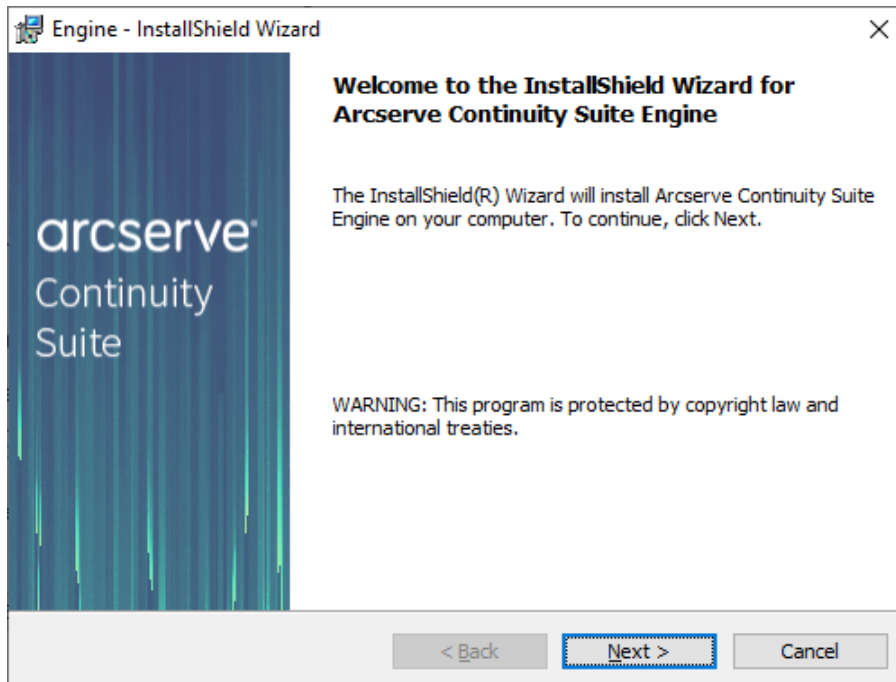
4. Click **Install Engine**.



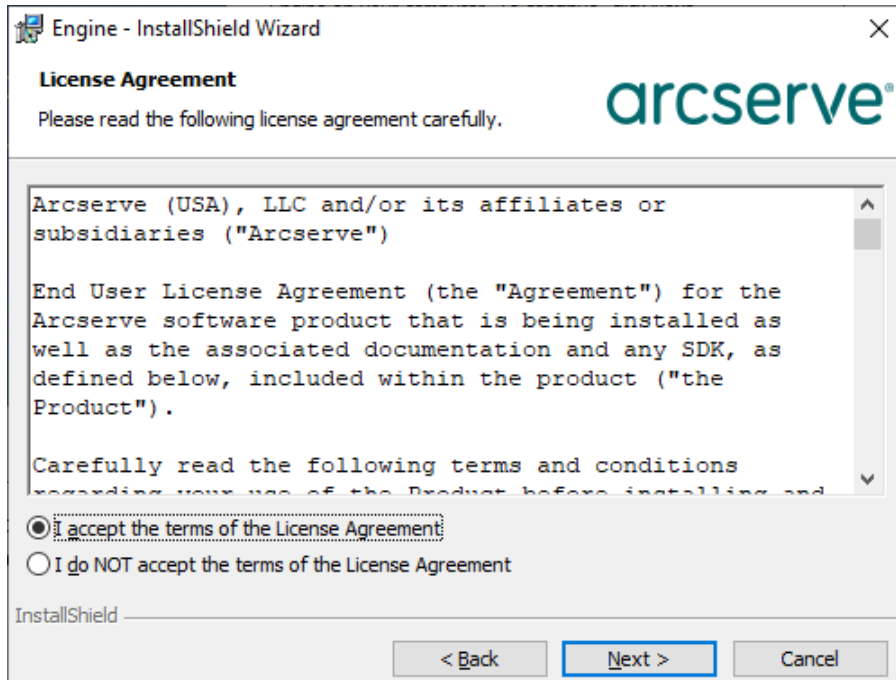
5. On the Arcserve Continuity Suite Engine - InstallShield Wizard, from the drop-down list, select your preferred language, and then click **OK**.



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

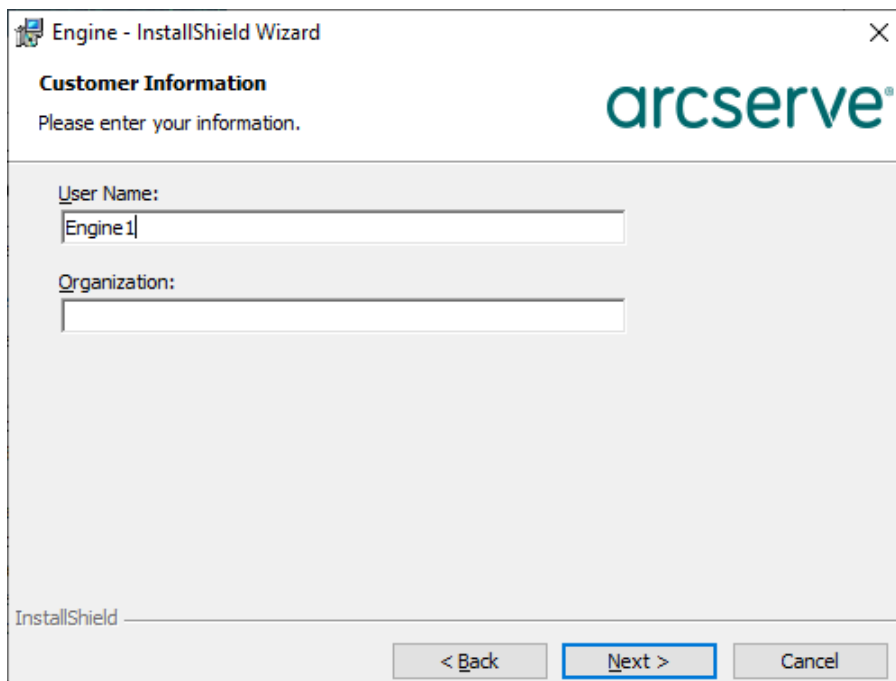


6. Click **Next**.
7. On the License Agreement page, read the terms of the License Agreement, select the **I accept the terms of the License Agreement** option, and then click **Next**.

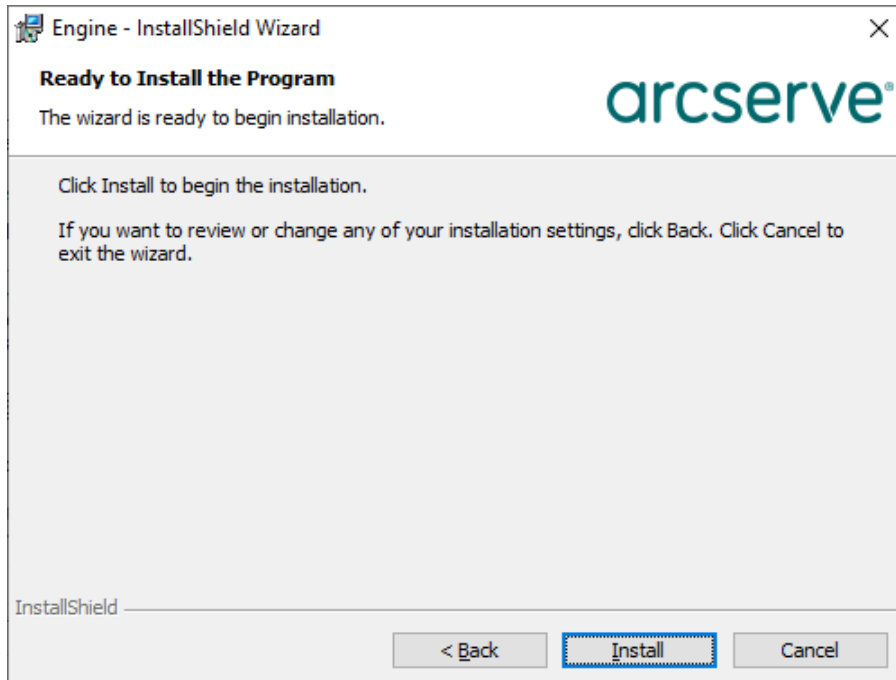


**Note:** If an Engine from the previous version exists on your server, the information about the previous version page appears with an option to uninstall the Engine.

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

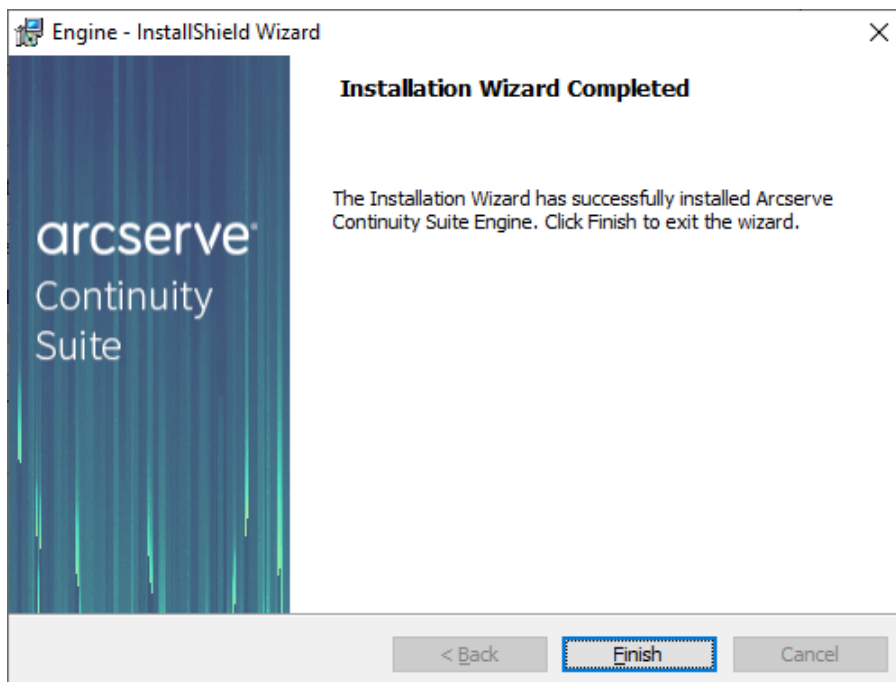


9. For the upcoming screens, retain the defaults, and then click **Next** to continue.
10. On the Ready to Install the Program page, click **Install**.



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

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



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](#).

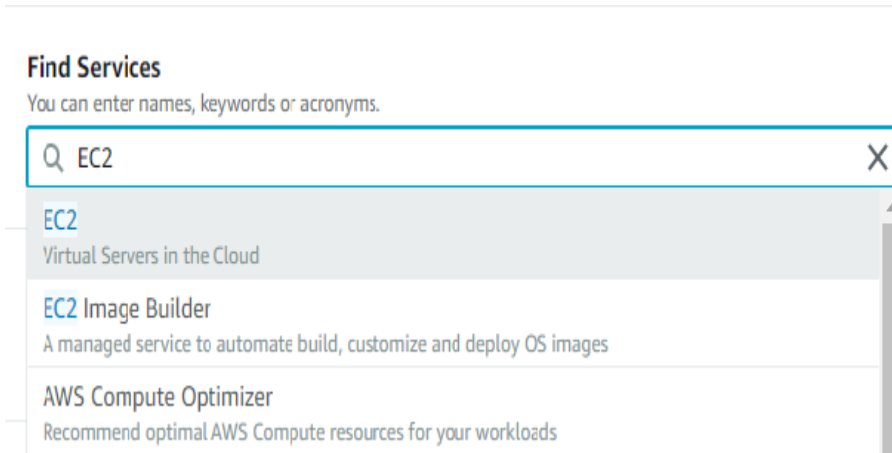
If you want Arcserve Replication and High Availability to start the DR VM with a specific public IP address, pre-allocate such Elastic IPs in the Amazon EC2 web portal. Later in the Network Mapping dialog of Continuity Suite Scenario, you can select a public IP from the existing Elastic IP addresses for the DR VM.

## Provision VA on Amazon EC2

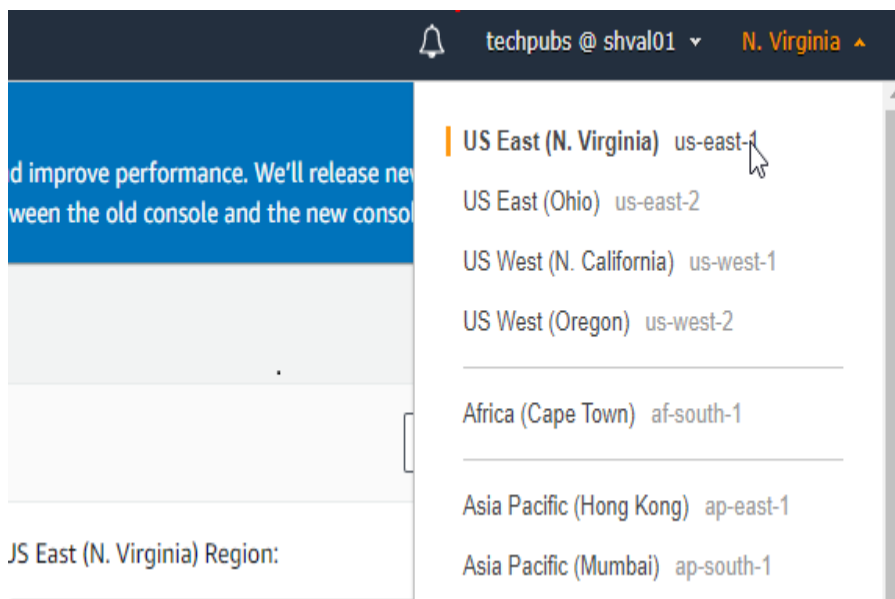
The Continuity Suite Virtual Appliance (VA) is a VM running on the virtualization platform or cloud where you want to replicate the Master servers. The VA acts as Replica in a Continuity Suite Full System scenario. The Master server is replicated to this virtualization platform or cloud. However, the 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:

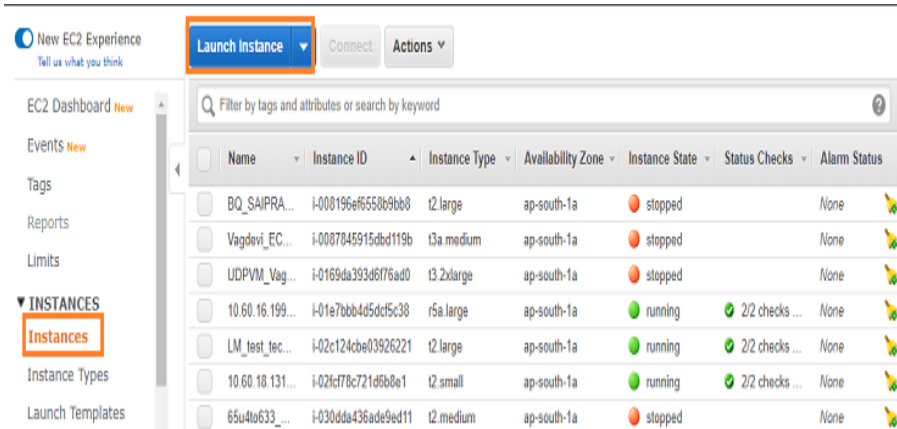
1. Log into [Amazon Web Services](#) as an IAM user.
2. Under Find Services, search for EC2, and then select **EC2**.



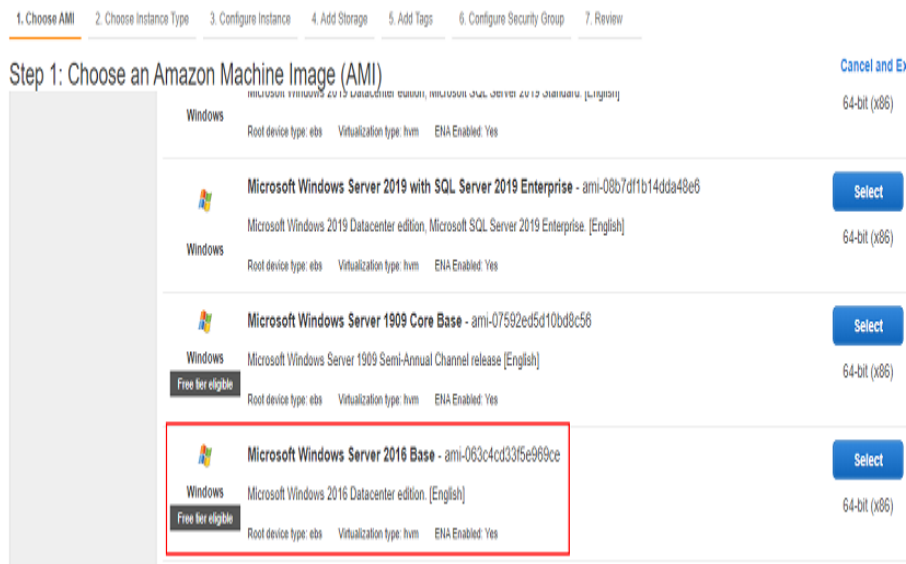
3. On the top-right corner of the EC2 dashboard, select the AWS region in which you want to provision the EC2 server.



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 Microsoft Windows Server 2016 Base, click **Select**.



6. 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 <small>Free tier eligible</small>	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

7. 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

Capacity Reservation  Create new Capacity Reservation

Domain join directory  Create new directory

Cancel Previous Review and Launch Next: Add Storage

8. On the Step 4: Add Storage page, retain the defaults, 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-044650a984953f7b7	30	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

9. 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 ⓘ	Volumes ⓘ
------------------------------	--------------------------------	-------------	-----------

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 <sup>(i)</sup>	Volumes <sup>(i)</sup>
Name	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](#)

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

Port Range: 25000

Source: 0.0.0.0/0

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

Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group

☐ Select an existing security group

Security group name: launch-wizard-53

Description: launch-wizard-53 created 2020-06-25T13:01:01.891+05:30

Type <sup>(i)</sup>	Protocol <sup>(i)</sup>	Port Range <sup>(i)</sup>	Source <sup>(i)</sup>	Description <sup>(i)</sup>
RDP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCP	TCP	25000	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

[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](#)

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

## 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, launch-wizard-53, 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

**Microsoft Windows Server 2016 Base - ami-063c4cd33f5e969ce**

Free tier eligible

Microsoft Windows 2016 Datacenter edition (English)

Root Device Type: ebs    Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). Don't show me this again

[Edit AMI](#)

Cancel

Previous

**Launch**

12. 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

**Key pair name**

██████████ ← 2

3

↓

**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 you that 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** X

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

AKP ← 2

☐ 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

13. On the Launch Status page, click the launch ID.



## Launch Status

✓ **Your instances are now launching**  
The following instance launches have been initiated: [REDACTED] [View launch log](#)

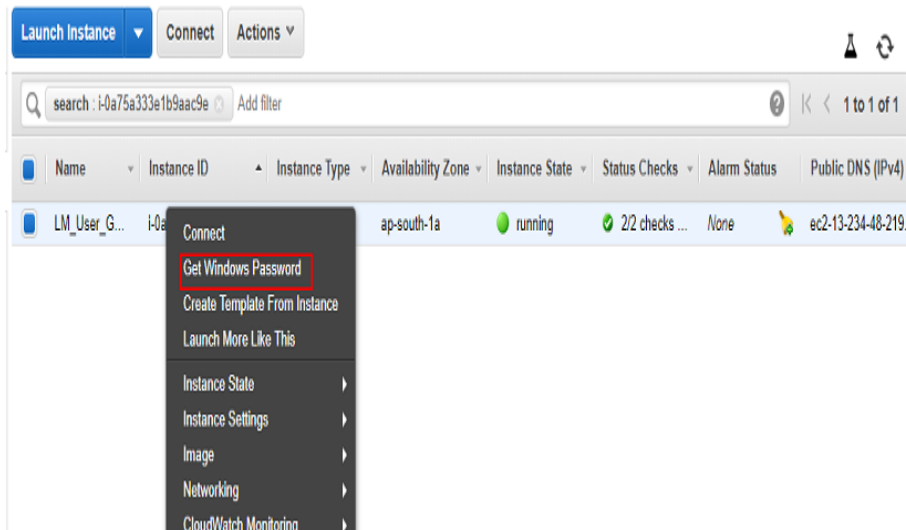
ℹ **Get notified of estimated charges**  
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

## How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your in

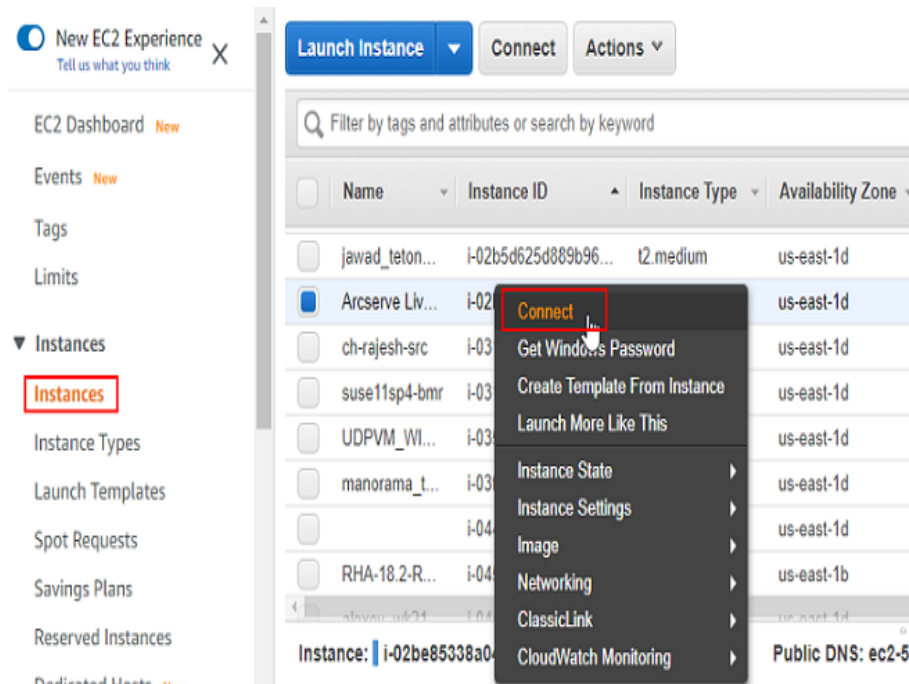
14. To get the Windows password, right-click the instance, and then select **Get Windows Password**.

**Notes:**

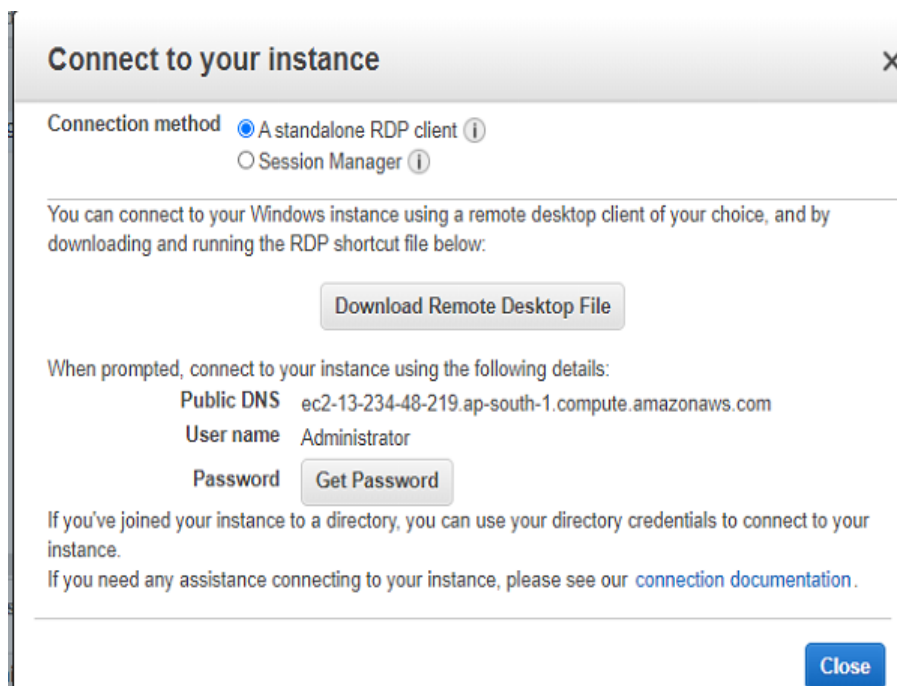
You can get the password only after the Status Checks displays 2/2 checks.

To get the Windows password, see [How to Get Windows Password](#).

15. On the left panel, go to **Instances**, right-click the instance you have launched, and then click **Connect**.

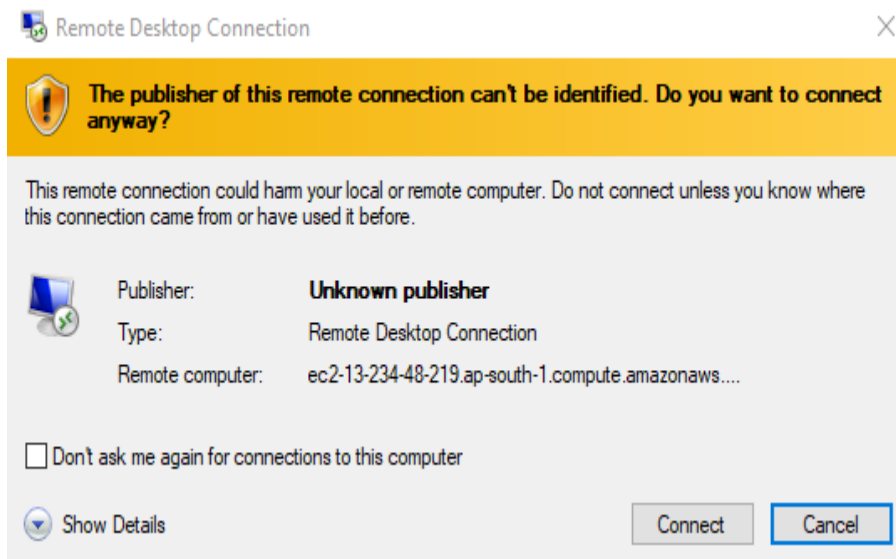


16. On the Connect to your instance page, click the **Download Remote Desktop File** button, and then click **Close**.



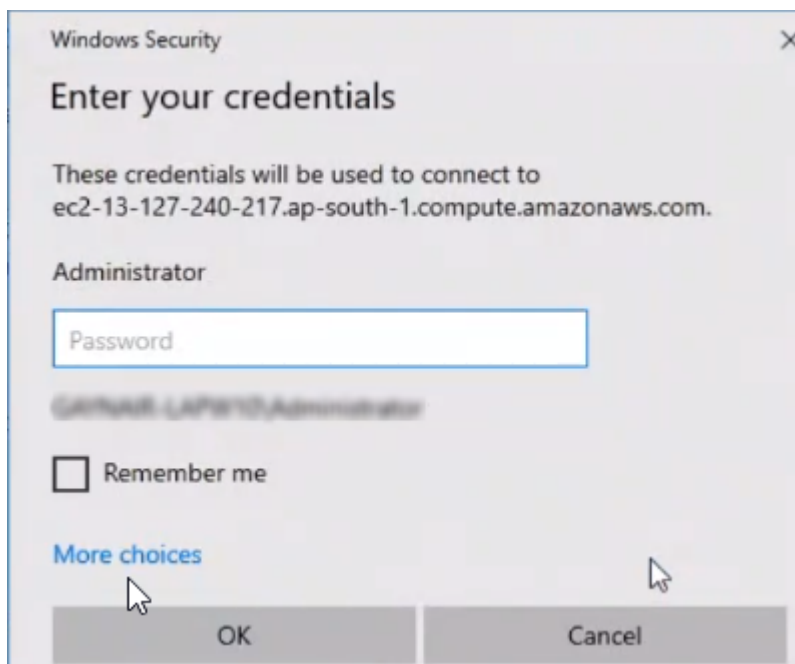
17. Double-click the downloaded file.

The Remote Desktop Connection screen appears.



18. Click **Connect**.

The Enter your credentials screen appears.



19. Paste the password you have copied to the clipboard, and then click **OK**.

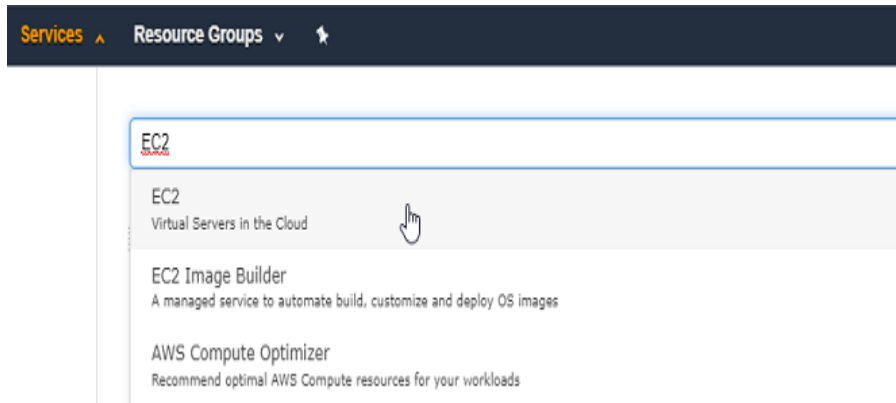
The virtual machine is now created on AWS.

## How to Get Windows Password

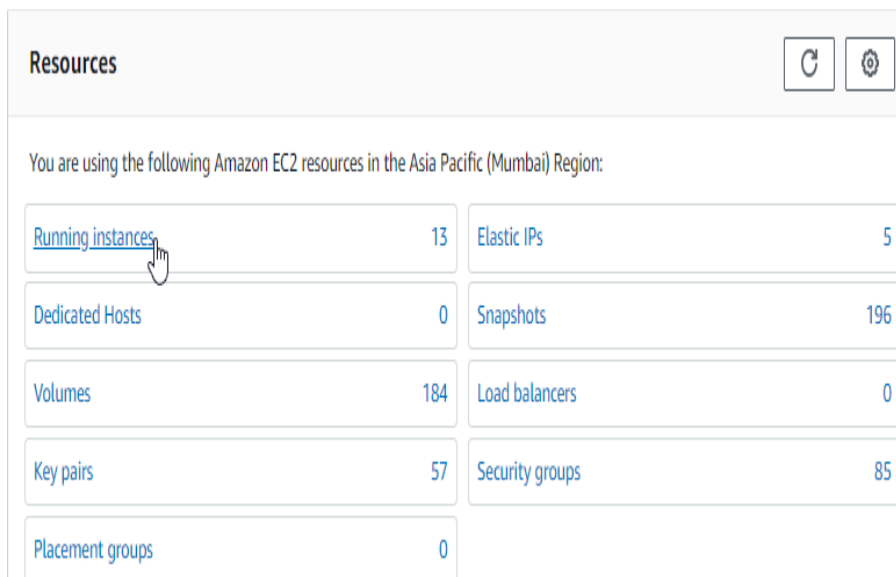
This section provides information about how to get the Windows password.

**Follow these steps:**

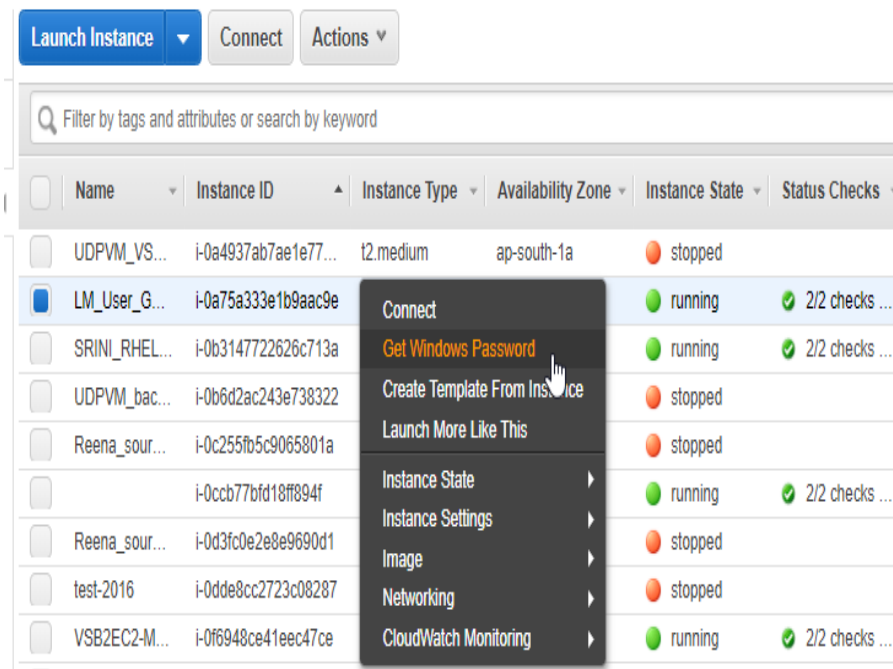
1. Navigate to the AWS console > **Services**.
2. Search for EC2 in the search bar, and then select **EC2**.



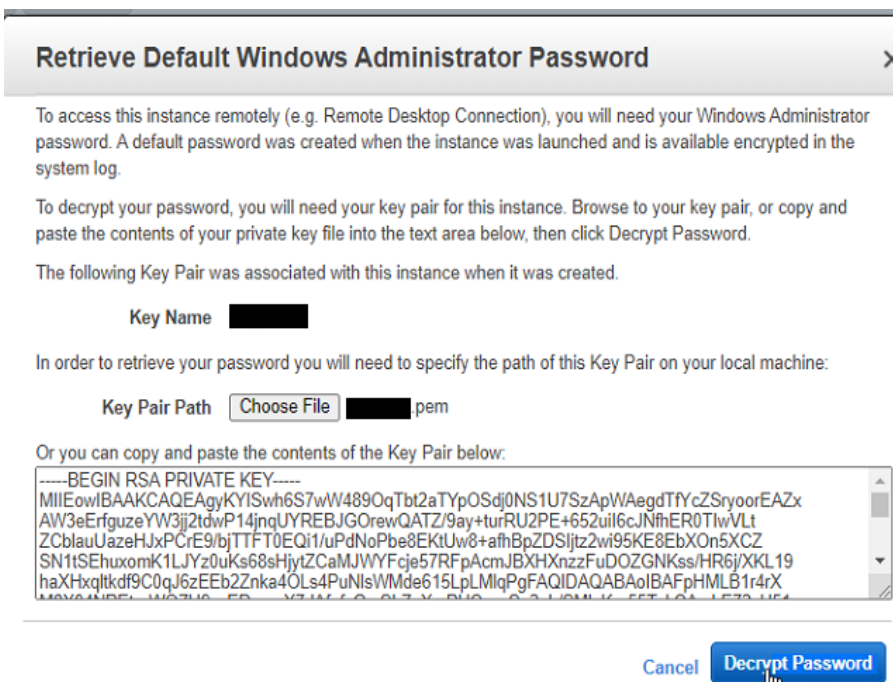
3. On the Resources page, click **Running instances**.



4. From the list of instances, select and right-click the instance, and then click **Get Windows Password**.




- On the Retrieve Default Windows Administrator Password page, click **Choose File**, select the downloaded .pem file, and then click **Decrypt Password**.




On the Retrieve Default Windows Administrator Password page, the *Password Decryption Successful* message appears.

- Copy password to the clipboard, and then click **Close**.

### Retrieve Default Windows Administrator Password

**Password Decryption Successful**

The password for instance i-069d66902b336dd5d (LM\_User\_Guide) was successfully decrypted.

**Password change recommended**

We recommend that you change your default password. Note: If a default password is changed, it cannot be retrieved through this tool. It's important that you change your password to one that you will remember.

You can connect remotely using this information:

Public DNS ec2-13-233-112-188.ap-south-1.com

User name Administrator

Password

Copy to clipboard

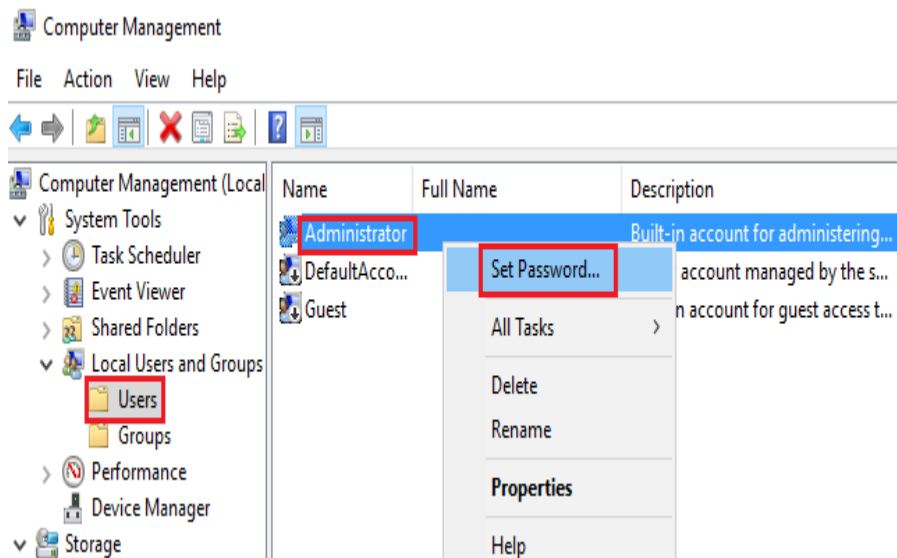
Close

## How to Change EC2 VM Password

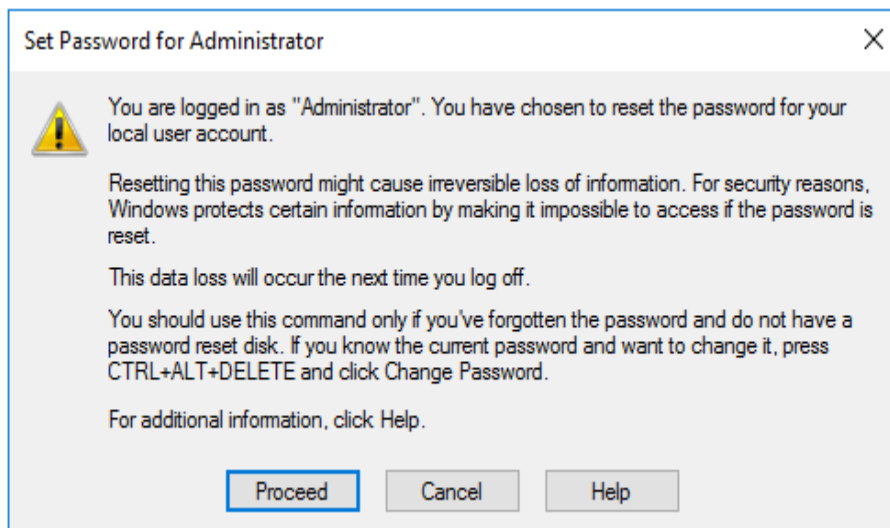
This section provides information about how to change EC2 VM password.

**Follow these steps:**

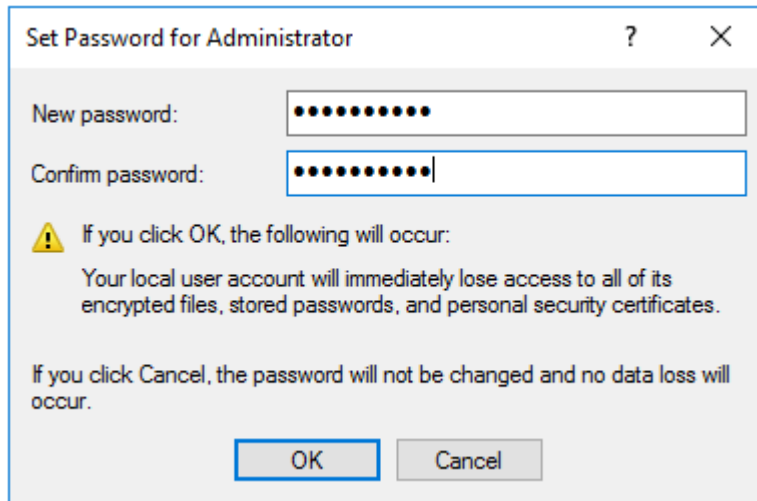
1. Go to virtual machine, right-click the start menu, and then select **Computer Management**.
2. On the Computer Management page, from the left pane, navigate to **Local Users and Groups > Users**, right-click **Administrator**, and then click **Set Password**.



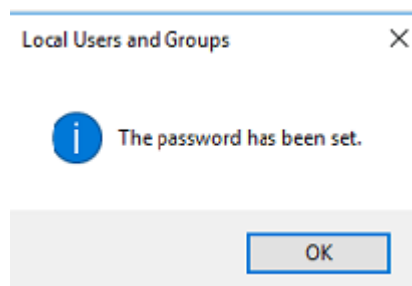
3. On the Set Password for Administrator screen, click **Proceed**.



4. Enter the new password, confirm the new password, and then click **OK**.



The Local Users and Groups screen appears, and displays the message “The password has been set”.



5. Click **OK** to close the Local Users and Groups screen.



## Install Engine on Replica

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

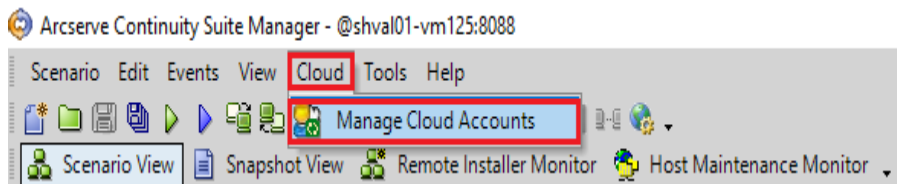
## Create Full System Scenario for Amazon EC2

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.

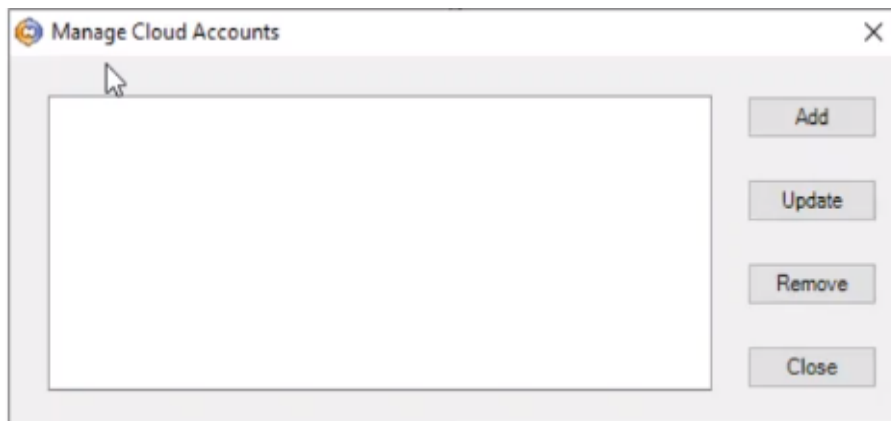
Before you create a scenario, add Amazon EC2 Cloud Account in Continuity Suite Manager.

**To Add 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.

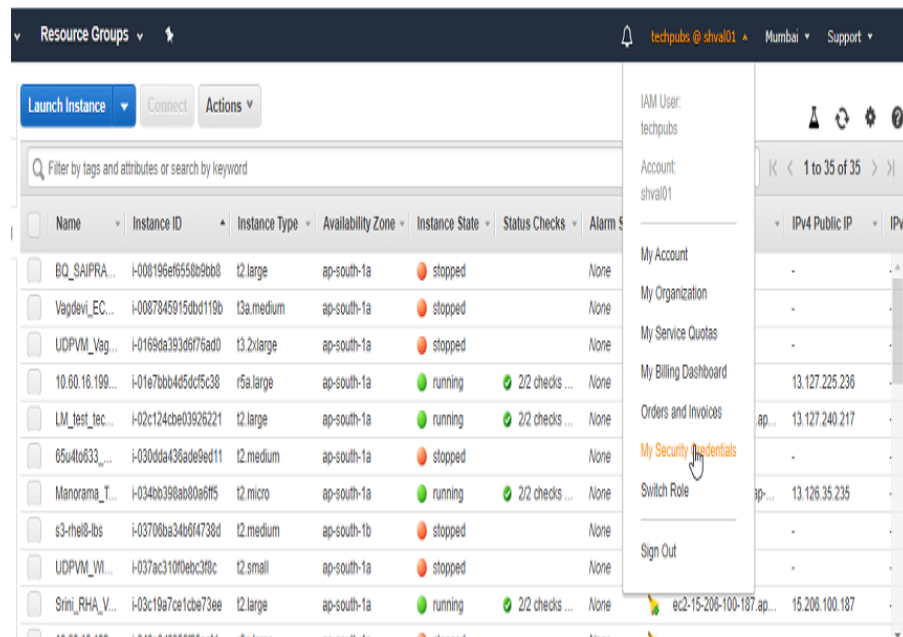
**Cloud Account** - Enter the account name you had defined while creating the AWS account.

**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

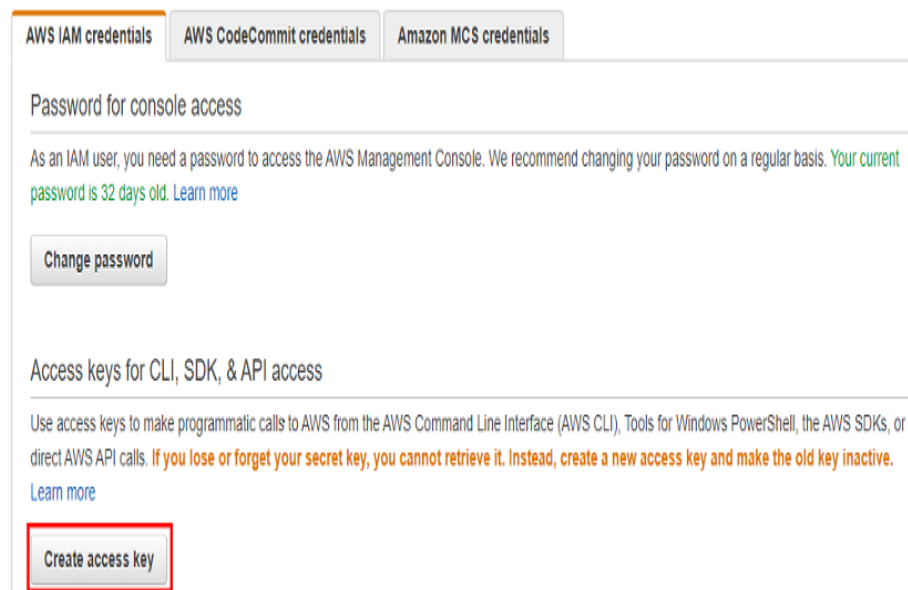
programmatic requests to the AWS CLI or AWS API, like a user name and password are used to access your AWS Management Console.

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.

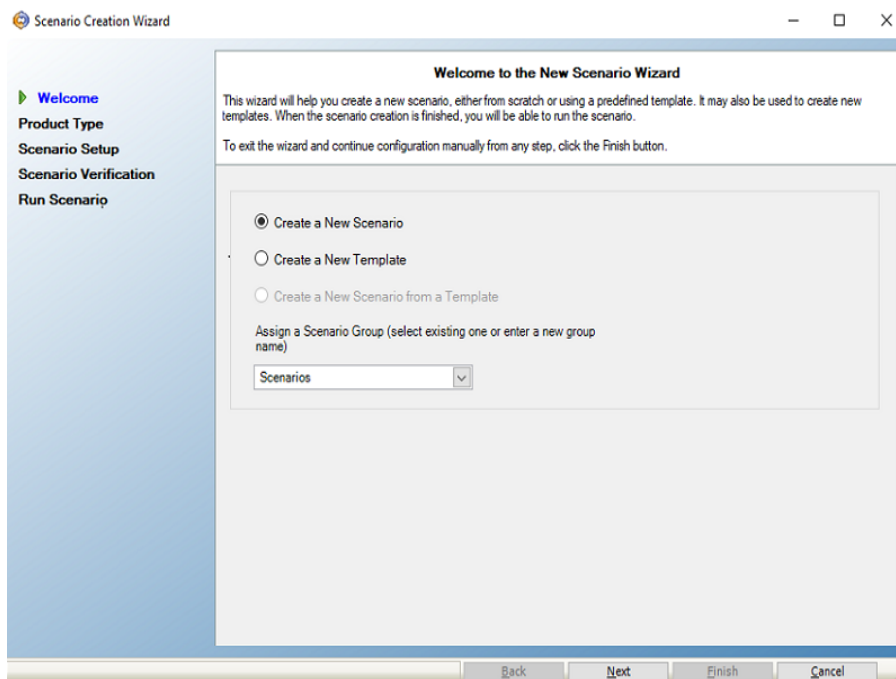
The Amazon EC2 account for Live Migration is now configured.

## Creating Full System Scenario for Amazon EC2

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

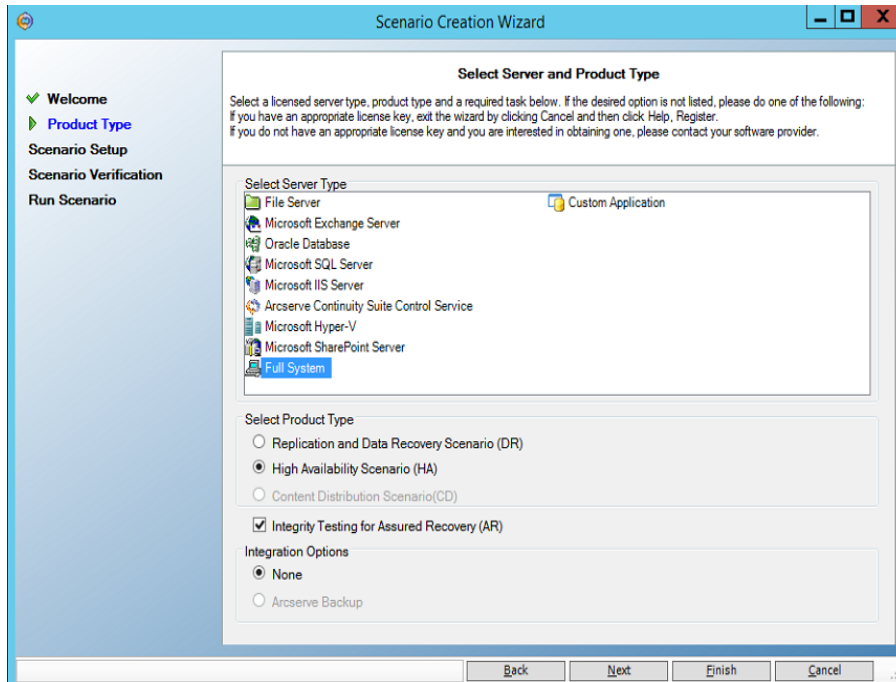
### Follow these steps:

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**.

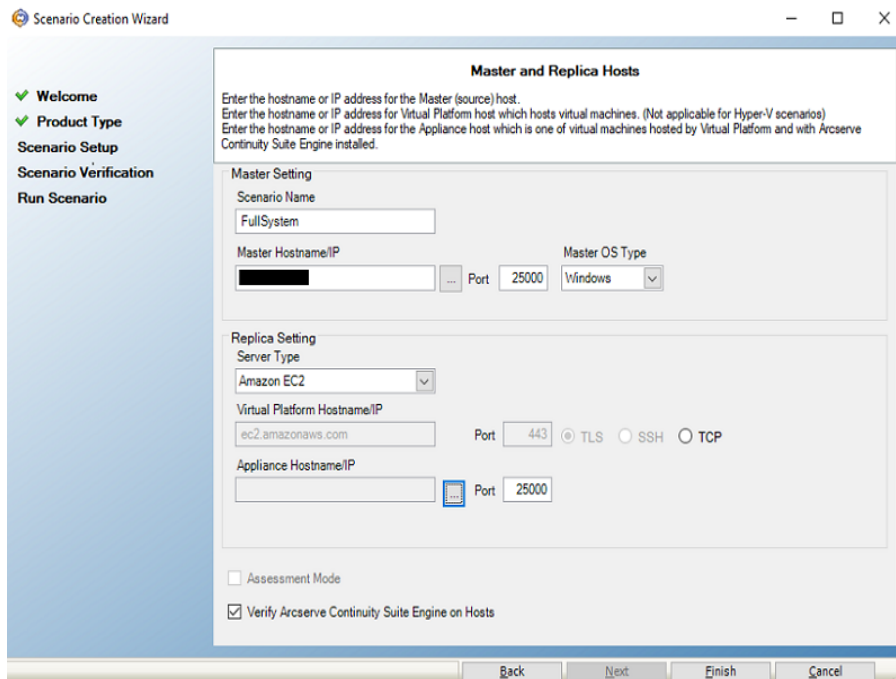


3. On the Select Server and Product Type screen, select Full System, High Availability Scenario (HA), and then click **Next**.

**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.

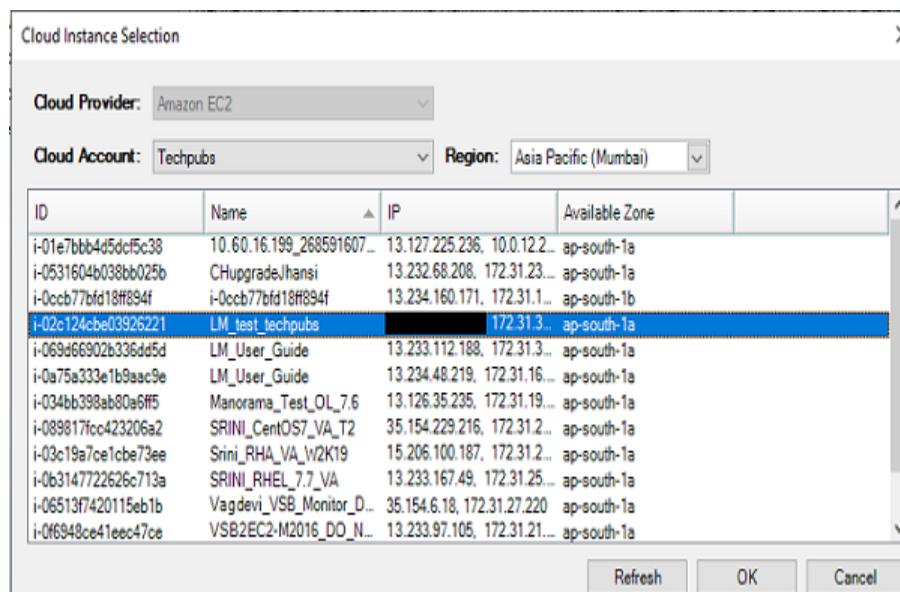
**Master OS Type** - Select Windows as the Master OS Type.

**Server Type** - Select Amazon EC2 as the Replica server.

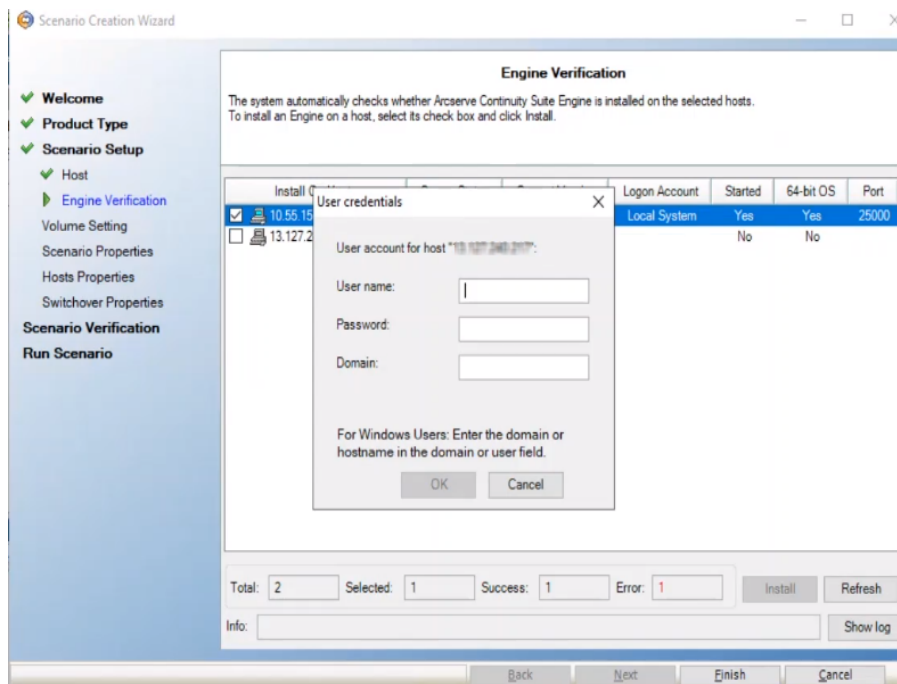
**Appliance Hostname/IP** - Browse the Appliance Hostname/IP to select the Replica server.

**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**.



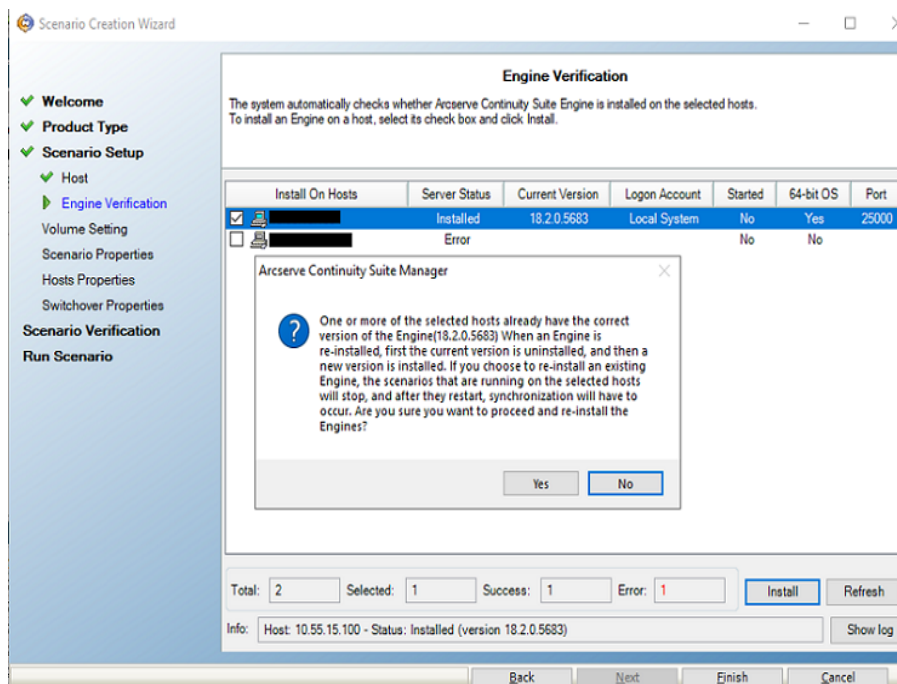
- On the Engine Verification screen, the User credentials screen appears. Enter the User name and Password, and then click **OK**.



**Note:** Use the password that you had copied to the clipboard while creating an AWS account. To retrieve a forgotten password, see [How to get Windows Password](#).

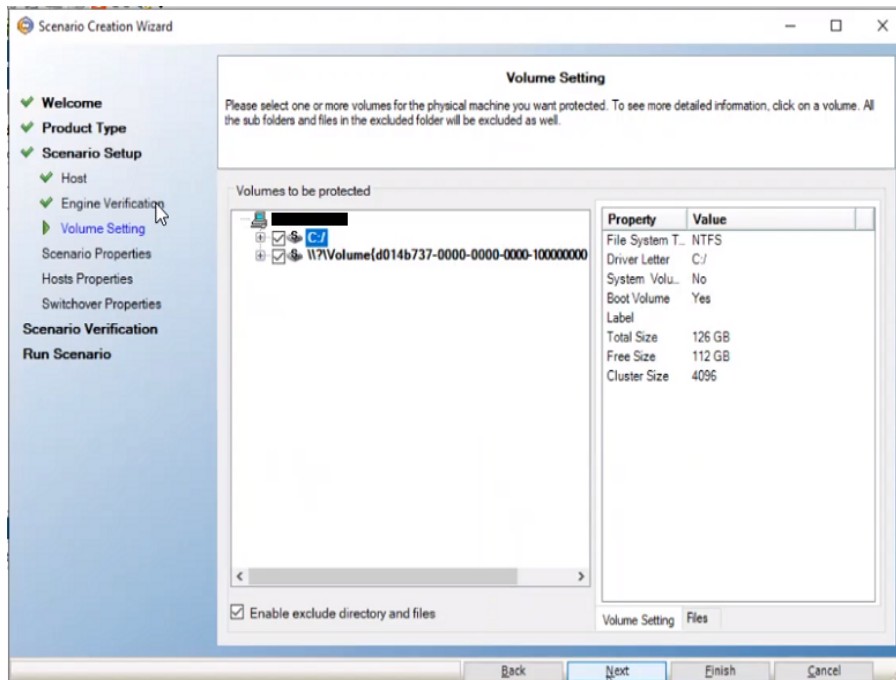
Wait for Engine verification to complete, and then click **Next**.

**Note:** If an error occurs, click **Install**. A confirmation message appears asking if the Engine can be upgraded on one or both servers; click **Yes**, and then click **Next**.

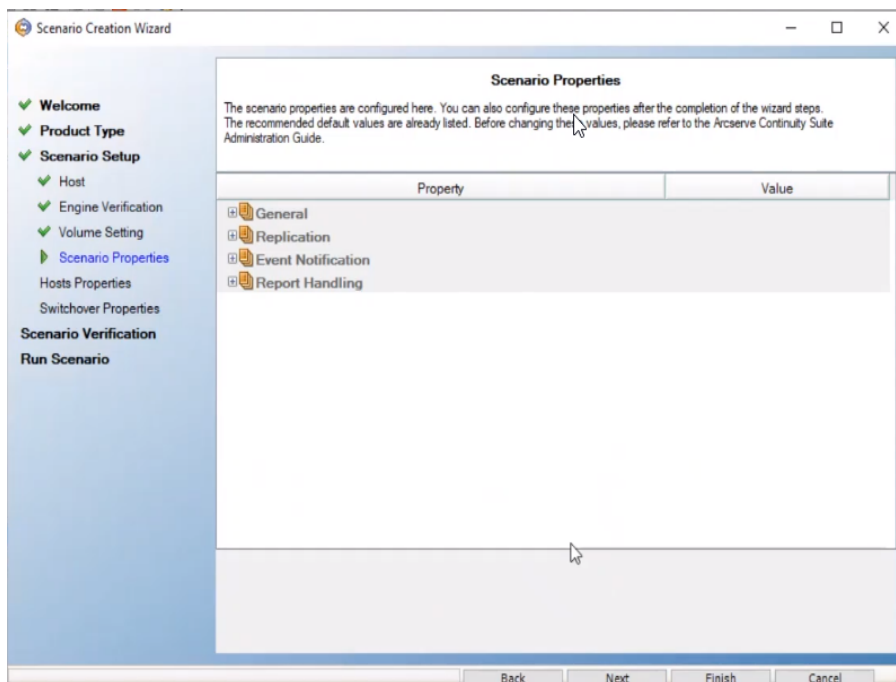




- On the Volume Setting screen, select one or more volumes for the physical machine you want to protect, and then click **Next**.



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



- 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.

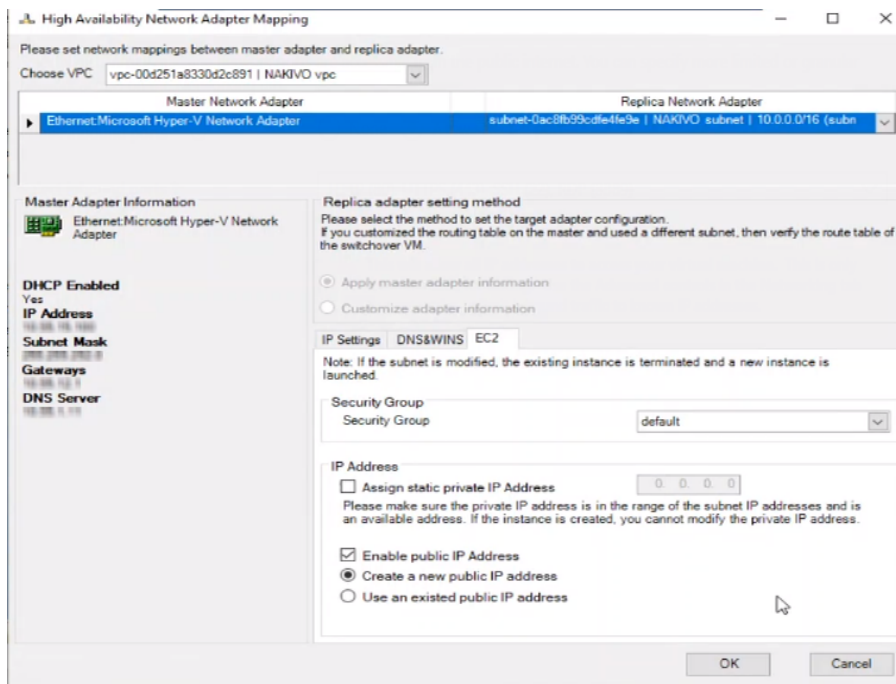
**IP Address** - Select one of the following:

Assign static private IP Address

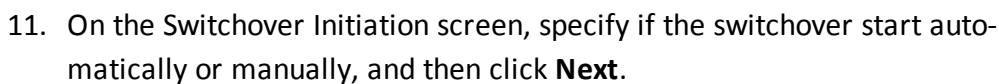
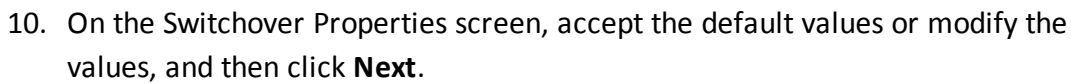
Enable public IP address

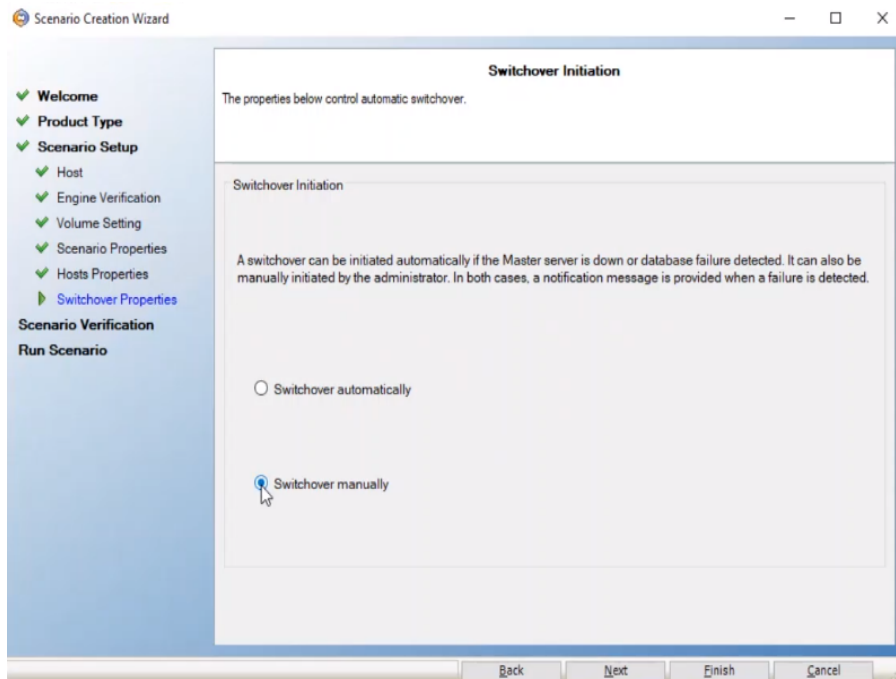
If you want to create a new public IP address, enable the **Create a new public IP address** option.

If you want to connect to the virtual machine from outside your network, enable the **Use an existed public IP address** option.

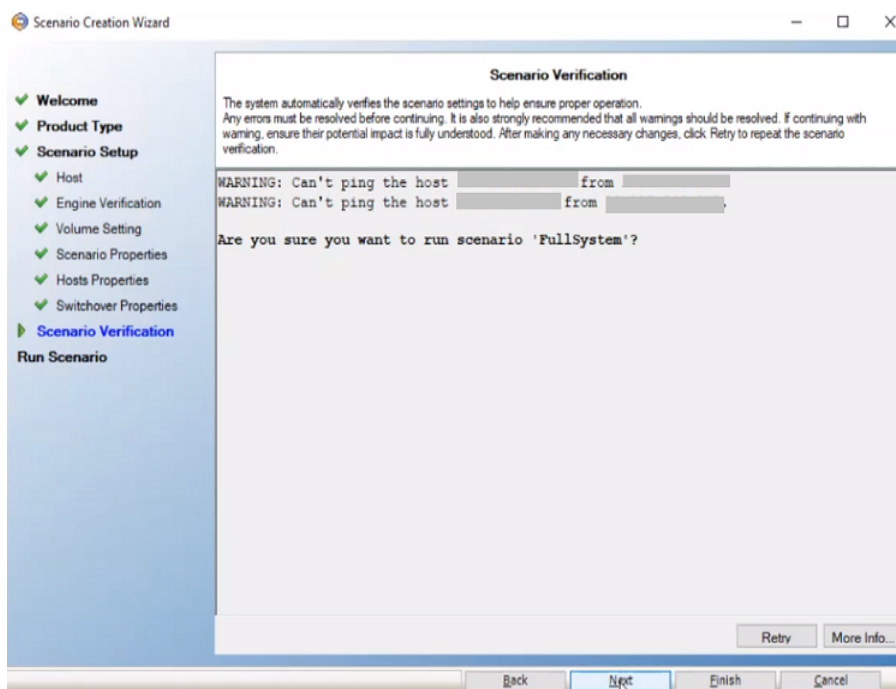


9. On the Master and Replica Properties screen, navigate to **Virtual Machine > Virtual Machine Setting > EC2 Instance Type**, select the instance type, and then click **Next**.





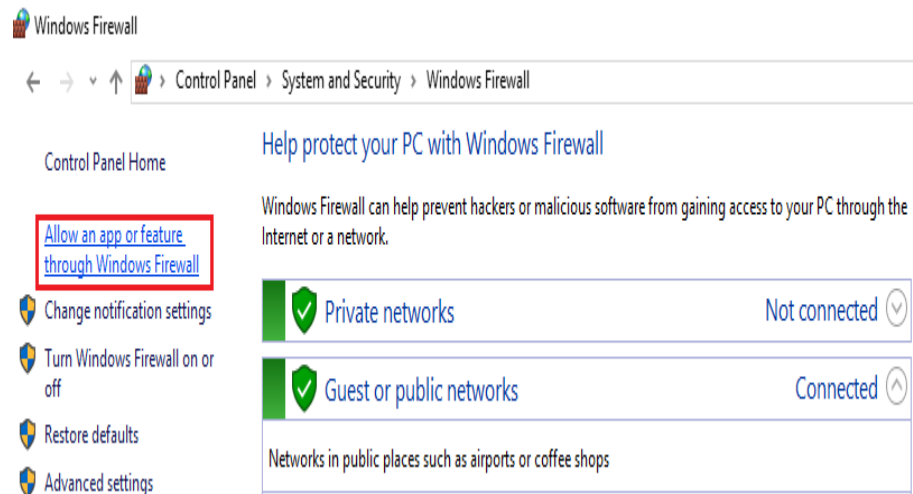
12. On the Scenario Verification screen, click **Next**.



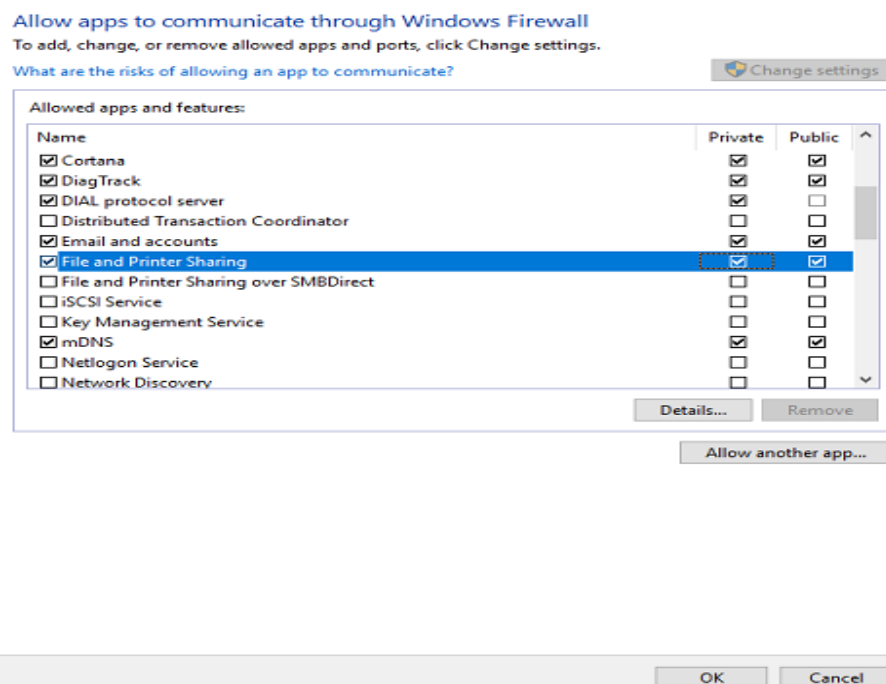
If the Master and Replica servers fail to ping each other, do the firewall and NAT settings.

To do the firewall settings on both the Master server and the EC2 VM, follow these steps:

- a. Navigate to **Control Panel > System & Security > Windows Firewall > Allow an app or feature through Windows Firewall**.



- b. On the **Allow apps to communicate through Windows Firewall** page, select **File and Printer Sharing** check box, enable **Private** and **Public** options, and then click **OK**.



To do the NAT settings on the Master server, do the following:

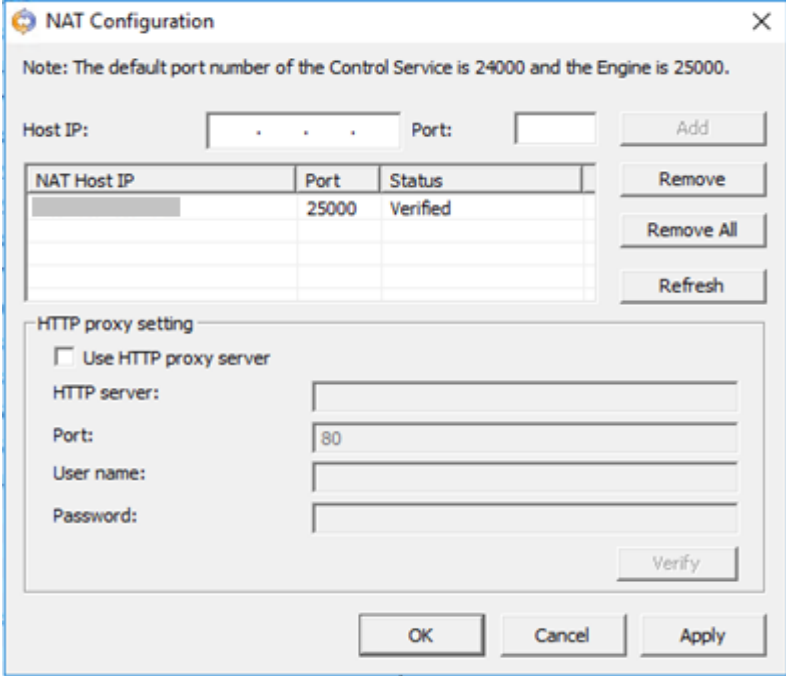
- a. Open the natutilgui from the engine installation directory.

**Note:** The default installation directory is: C:\Program Files\Arcserve\RHA\Engine

- b. On the NAT Configuration dialog, do the following, and then click **Add**:

Host IP: Type the EC2 VM IP address.

Port: Enter the port value as 25000.



The NAT Configuration dialog box is shown. It includes a note about default ports (24000 for Control Service, 25000 for Engine). The Host IP field is empty, and the Port field is set to 25000. The Add button is highlighted. Below the input fields is a table with columns for NAT Host IP, Port, and Status. The table contains one entry: NAT Host IP (empty), Port 25000, and Status Verified. To the right of the table are buttons for Remove, Remove All, and Refresh. Below the table is the HTTP proxy setting section, which is currently unchecked. It includes fields for HTTP server, Port (set to 80), User name, and Password, with a Verify button. At the bottom are OK, Cancel, and Apply buttons.

NAT Host IP	Port	Status
	25000	Verified

- c. Click **Apply**, and then click **OK**.

Now, the Master server can communicate with Replica server.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.LNDARCSERVE>ping [redacted]

Pinging [redacted] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for [redacted]:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

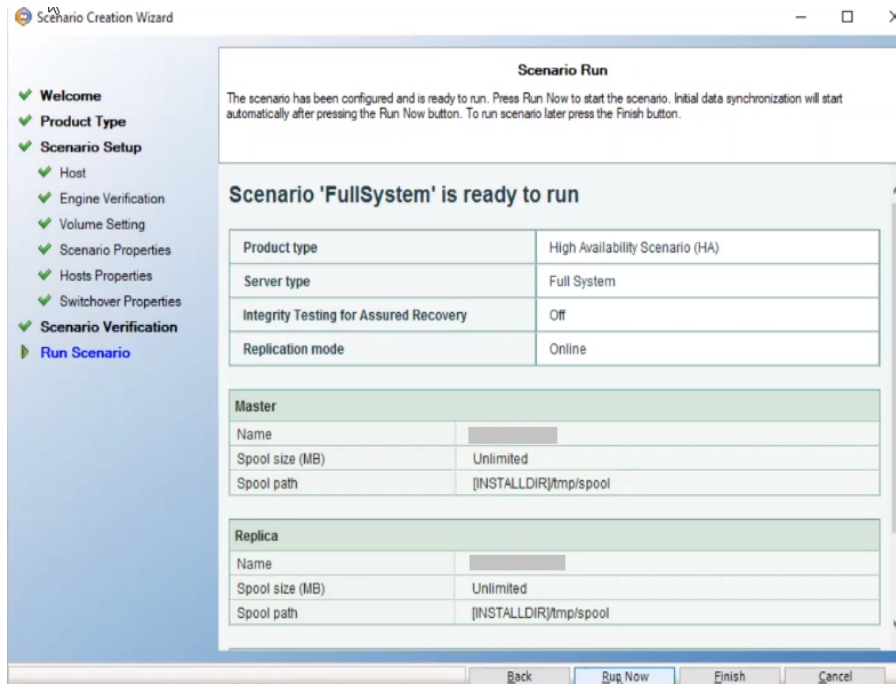
C:\Users\Administrator.LNDARCSERVE>ping [redacted]

Pinging [redacted] with 32 bytes of data:
Reply from [redacted]: bytes=32 time=57ms TTL=113
Reply from [redacted]: bytes=32 time=28ms TTL=113
Reply from [redacted]: bytes=32 time=28ms TTL=113
Reply from [redacted]: bytes=32 time=28ms TTL=113

Ping statistics for [redacted]:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 28ms, Maximum = 57ms, Average = 35ms

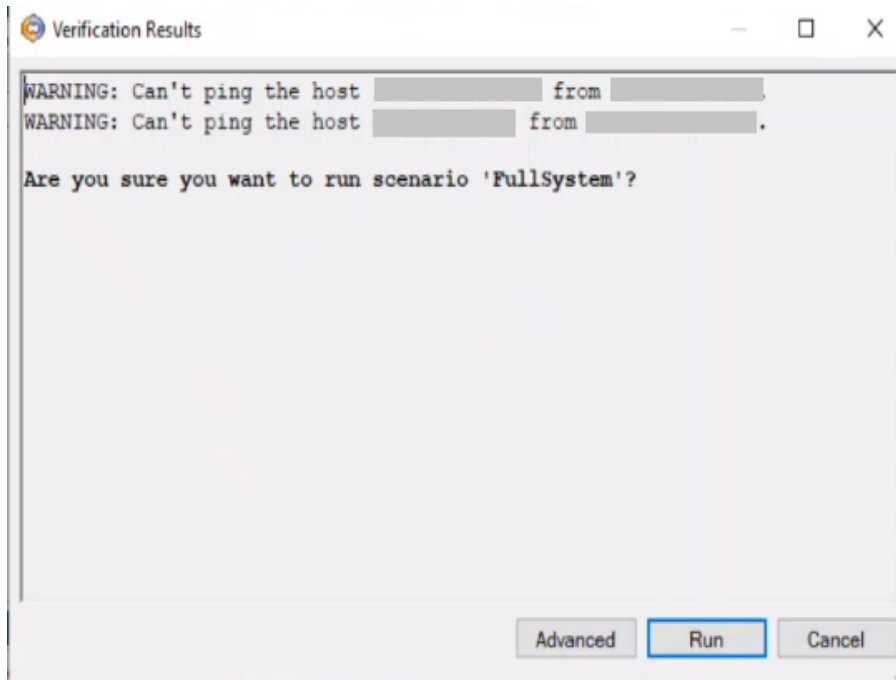
C:\Users\Administrator.LNDARCSERVE>
```

13. 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**.



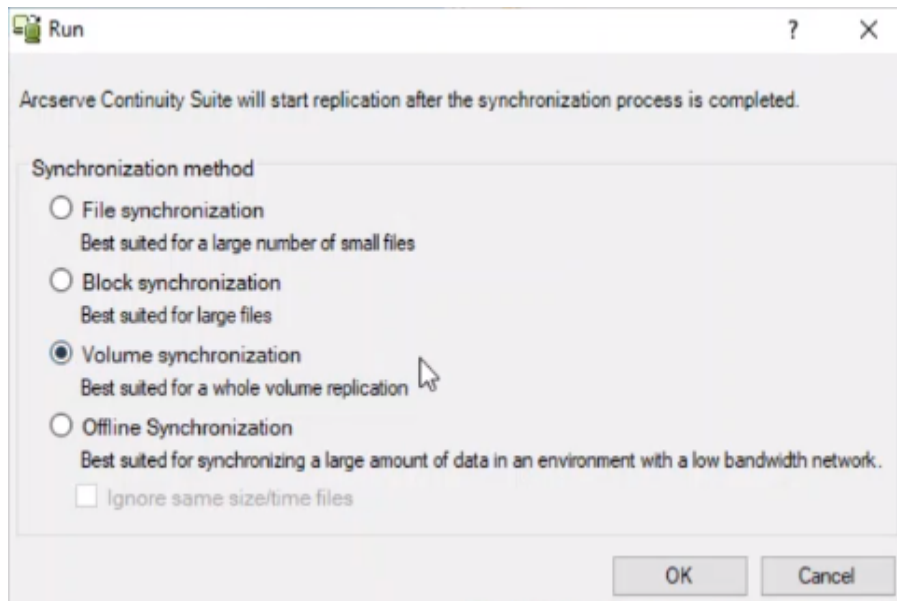
The scenario verification runs automatically, and the Verification Results screen appears.

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



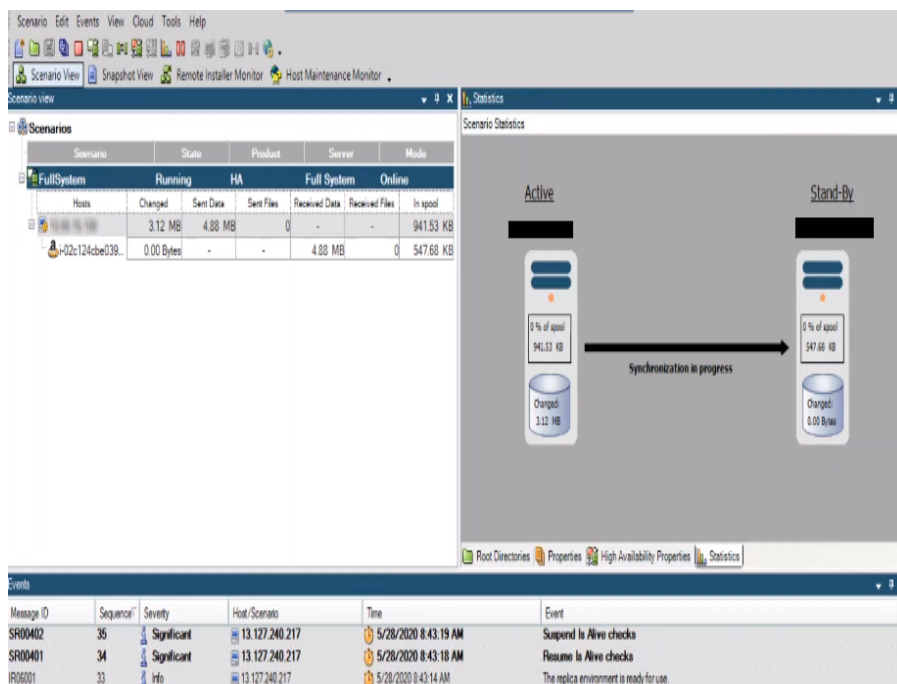
15. On the Run screen, select **Volume synchronization**, and then click **OK**.





**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.





## Perform Assured Recovery Testing

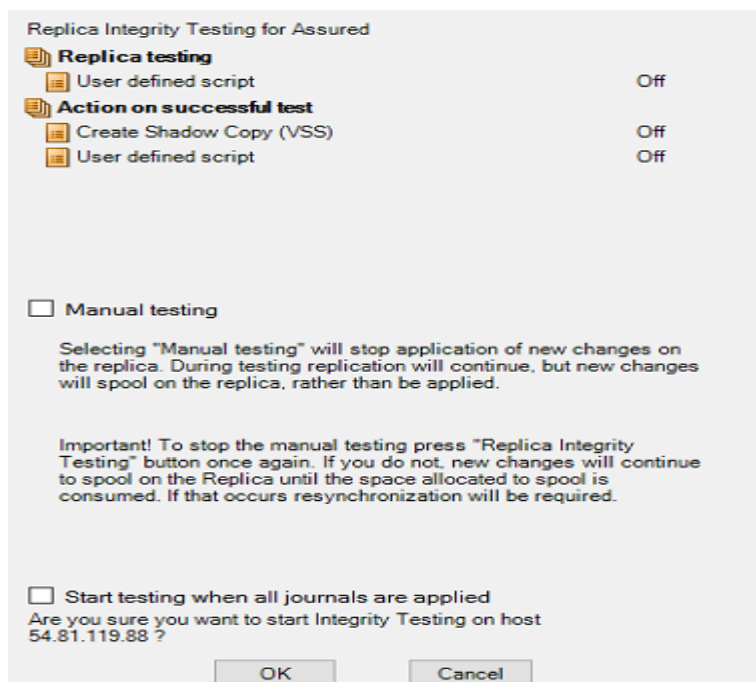
**Note:** Perform the Assured Recovery test only if you have enabled the **Integrity Testing for Assured Recovery (AR)** option on the Select Server and Product Type screen.

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

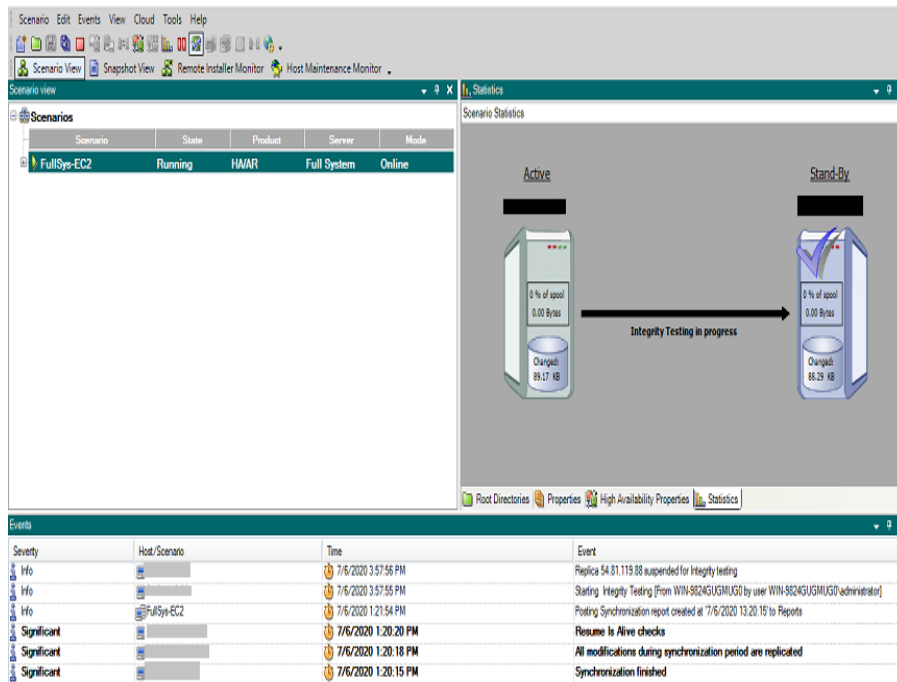
**Notes:**

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: Scenario, State, Product, Server, and Mode. The selected scenario is 'FullSystem-RH8-EC2', which is in the 'Running' state. Below this, a table shows the progress of the scenario:

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

The top-right pane shows the 'Statistics' for the scenario, including a diagram of the 'Active' and 'Stand-By' replicas and a 'Replication' arrow. The bottom pane shows the 'Events' log with columns: Severity, Host/Scenario, Time, and Event. The events listed are:

Severity	Host/Scenario	Time	Event
Info	Full4cndd7a060	7/8/2020 3:58:12 PM	Replication to replica 3.89.233.115 resumed after integrity testing
Significant	Full4cndd7a060	7/8/2020 3:58:11 PM	FullSystem Integrity Testing on replica 3.89.233.115 is finished
Error	Full4cndd7a060	7/8/2020 3:58:11 PM	Automatic FullSystem testing on replica 3.89.233.115 is unsuccessful
Info	Full4cndd7a060	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

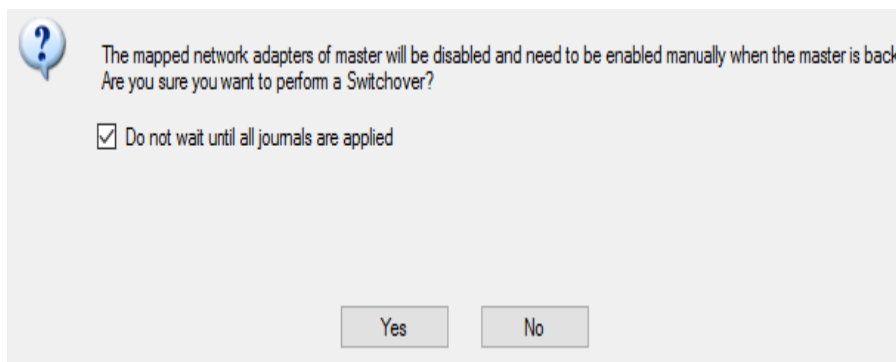
Switchover (or failover) is the process of changing roles between the Master and Replica, that is, making the Master server the standby server, and the Replica server the active server.

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:**

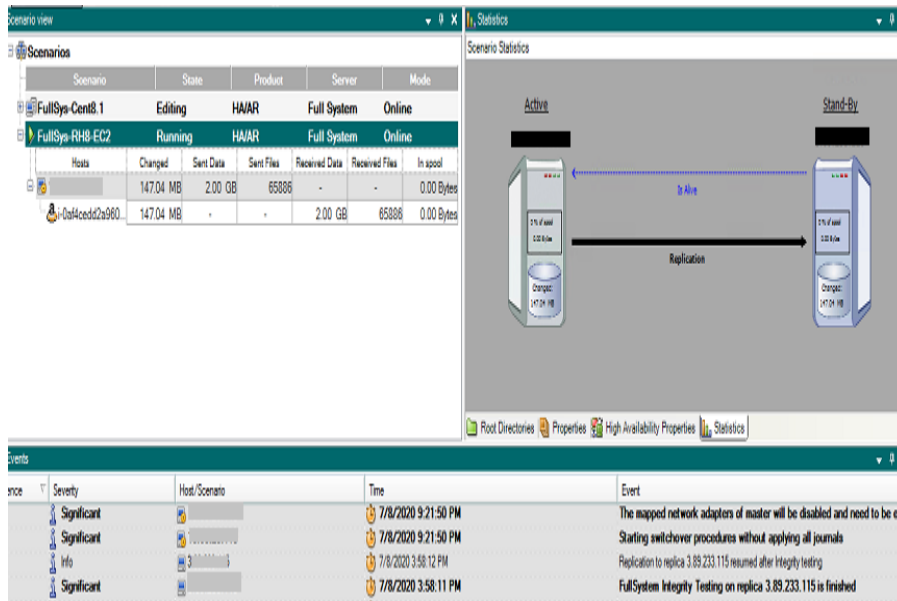
1. Open the Manager and then select the required scenario from the Scenario pane. Verify if it is running.
2. On the standard toolbar, click the **Perform Switchover** button, or select the **Perform Switchover** option from the Tools menu.

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.

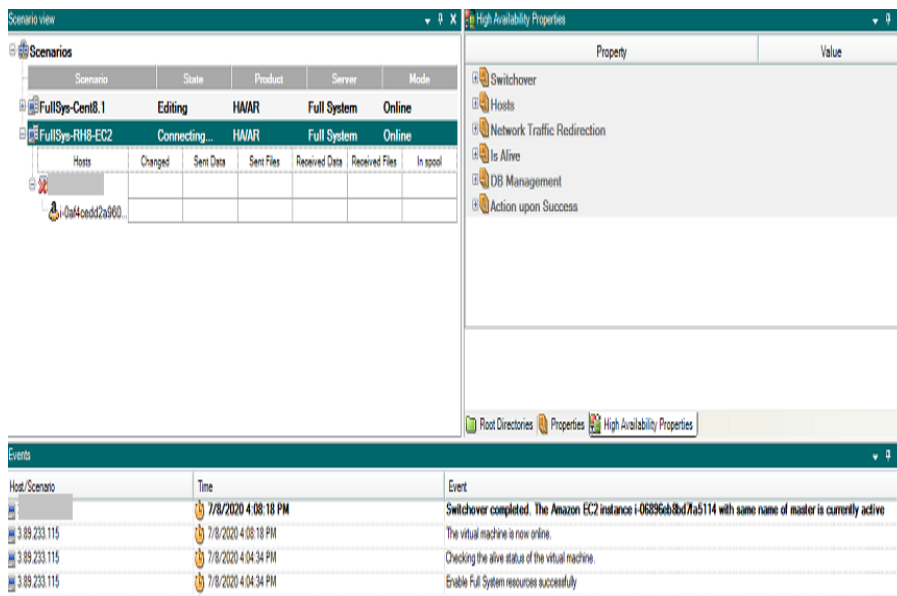
During switchover, the Event pane gives detailed information about the switchover process.



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.



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

