User Guide

Arcserve® Live Migration

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.

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

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 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 offers 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.
- On expiry, new scenarios cannot be started, but the existing ones will continue.
- Seamless access to the entitled software for a period of 90-days.
- For each license, Live Migration provides technical assistance for two incidents free of cost.

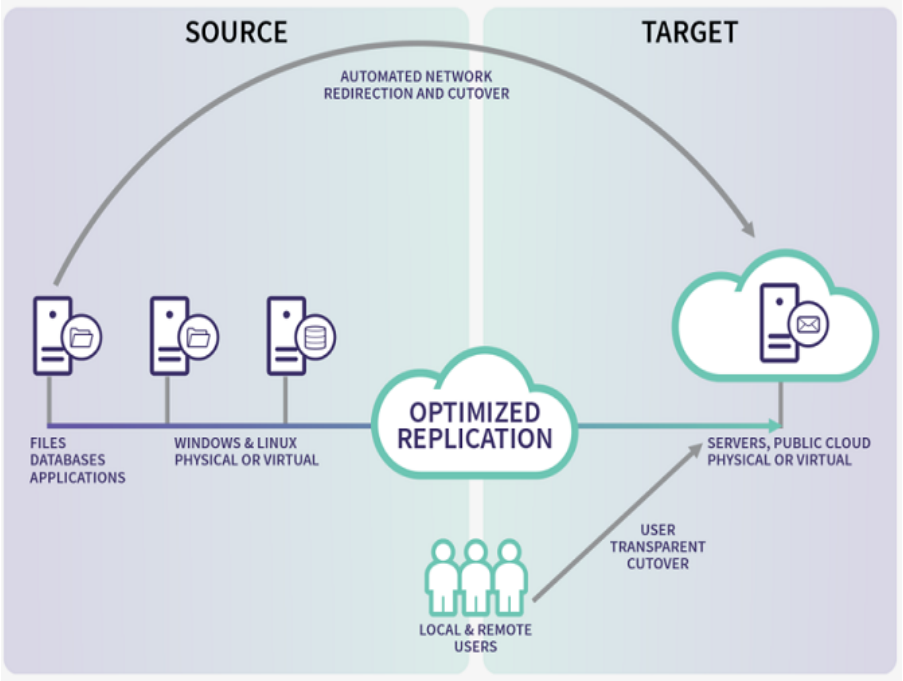
Notes:

- Currently, Arcserve does not provide professional services to help you with implementation, deployment, and any other migration services.
- For any assistance regarding migration issues during the 90-day period, contact our Technical support.

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.



A quick overview of this Live Migration document is as follows:

- **Install Control Service:** This section provides information about how to install the Control Service.
- **Configure Virtualization Platform and Cloud:** This section provides information about how to configure the Virtualization Platform and Cloud.
- **Deploy Virtual Appliance (VA) on EC2/Azure/Hypervisor VM:** This section provides information about how to deploy the Virtual Appliance (VA) server on EC2/Azure/Hypervisor.
- **Install Engine on Source:** This section provides information about how to install the Engine on source.

- **Create Full System Scenario:** This section provides information about how to create full system scenario.
- **Run Scenario and wait for Full Sync:** This section provides information about running a scenario.
- **Perform Assured Recovery Testing:** This section provides information about how to perform Assured Recovery testing.
- **Perform Cut off/Switchover:** This section provides information about how to perform cut off/switchover.

Terminologies

This document uses the following terminologies:

- **Virtual Appliance:** This is a virtual machine that acts as the Replica proxy server (the Arcserve Continuity Suite Engine should be installed here). If you are using a Hyper-V virtual platform, the field **Virtual Platform Hostname/IP** does not apply and is disabled (appears dim).

  Note: If the Master is Windows 2008 or a later version, we recommend using Windows 2012 R2 as the virtual appliance.
- **Control Service:** Control Service is a management component of Arcserve Continuity Suite, and Windows based service that must be deployed first. It hosts Web based info portal and rich Management UI which is used for creating and monitoring migration scenarios.
- **Engine:** Replication Engine is a background service which moves data from source to destination during migration. Engines should be installed on any source that you plan to migrate. You may use Remote Installer feature to mass deploy Engines.
- **FSHA:** FSHA is a scenario type that allows replication and fail-over of full server.
- **Management UI:** A UI that you use for creating and managing replication/migration scenarios. Management UI is hosted by Control Server and can be started after you log into the Management Portal.
- **Master (Source):** A host/computer which you migrate as whole (using full system migration scenario) or a host containing application that you are planning to migrate.
- **PowerShell:** Arcserve provides PowerShell Command Line Interface as an alternative to managing via UI. The PowerShell is offered as an alternative if you do not want to manage the replication process using the Manager graphic user interface. It enlarges and facilitates the capabilities of the CLI provided in previous versions, and it supports Continuous Availability operations.
- **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, Replica hosts and runs replicated application and data.

- **Scenario:** Scenario is a configuration unit which you create and migrate 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 scenario.
- **Virtual Platform Host:** This is the machine that hosts the Appliance VM acting as Replica server.

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 source host is Windows, then the Virtual Appliance (VA) must be Windows; if source host is Linux, then the VA must be Linux as well.

  Note: Before deploying Arcserve Live Migration scenarios, refer to Limitations in Release Notes.

- For Windows or Linux migration to Azure or AWS, register to the Cloud account with Arcserve Live Migration GUI before creating FSHA scenarios.

Software Compatibility

For more information about compatibility, see the Compatibility Matrix.

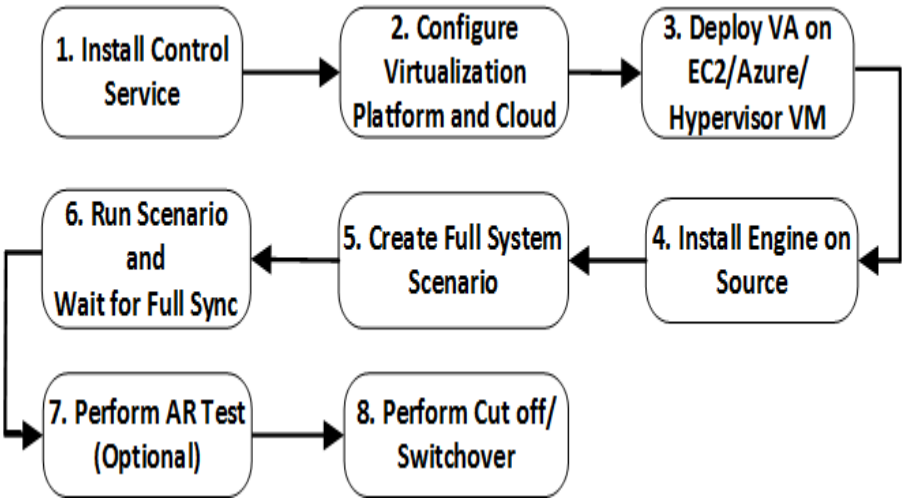
Related Documentation

For information related to migration and replication, use this guide along with the following:

- Arcserve Continuous Availability Administration Guide
- Arcserve Continuous Availability Installation Guide
- Arcserve Continuous Availability for Virtualized Server Environments Operation Guide

Chapter 2: Perform Live Migration

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



Install Control Service

This section describes how to install the Arcserve Continuity Suite Control Service.

Control Service Installation Considerations

You need to install either one Control Service or two Control Services, depending on the type of procedure you want to perform on the Control Service itself:

- For standard Arcserve Live Migration, you need to install only one Control Service. This Control Service functions as the single-point-of-control for all Arcserve Live Migration operations. If you want to replicate the Control Service data WITHOUT performing switchover between two Control Services, you can also install only one Control Service.

  Note: To replicate the Control Service data, create Replication Control Service scenario using the Manager, after the installation of all the Arcserve Live Migration components is completed.

- For replicating the Control Service data and switching roles between the original Control Service and a standby Control Service, you need to install two Control Services. One of the installed Control Services functions as the active Control Service, while the other functions as the standby Control Service. For installing two Control Services, repeat the installation process twice, since you can only install one Control Service at a time.

  Notes:

  - To apply HA solution on the Control Service, create HA Control Service scenario using the Manager, after the installation of all Arcserve Live Migration components is completed.
  - You do NOT need an HA license to apply HA solution on the Control Service. However, you do need to register in Arcserve Live Migration before creating a scenario for the Control Service.
  - For more information about creating Control Service scenarios, see Arcserve Continuous Availability Administration Guide.

Installing Control Service for a Standard Operation

To install the Arcserve Continuity Suite Control Service, follow these steps:

1. Double-click the **Setup.exe** installation file.

   The Arcserve Continuous Availability Installation wizard appears.

2. Click the **Install** option.

   The **Install Components** page appears.

3. Click the **Install Arcserve Continuity Suite Control Service** option.

   The **Choose Setup Language** dialog appears.

4. From the drop-down list, select the language you prefer, and then click **OK**.

   A progress bar appears. Once the initial process is completed, the **Welcome** page appears.

5. Click **Next**.

   The **License Agreement** page appears.

6. Select the **I accept** check box, and then click **Next**.

   The **Customer Information** page appears.

7. Verify that the details in the fields are correct, or change them accordingly, and then click **Next**.

   The **Destination Folder** page appears.

8. To select the Control Service installation location, use the **Change** button, or leave it at the default location, and then click **Next**.

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

   The **SSL Configuration** page appears.

9. The **SSL Configuration** page allows you to use SSL certificate to secure communication with the Control Service.

   If in your IT environment, the software is deployed on a local network and security is not a concern, you can clear the **Use SSL Configuration** check box. Then, the communication with the Control Service will be over HTTP.

   If you want to use SSL configuration, select the **Use SSL Configuration** check box. In this case, the communication with the Control Service will be over HTTPS. After you select this option, you need to enter a port number in the

SSL Port box, and to enter a certificate file in one of the available certificate type boxes.

Notes:

- While selecting the **SSL Configuration** option, by default, the **SSL Port** number is **443**. However, if this port number is in use in your IT environment, use a different port.
- If you have selected the **SSL Configuration** option, when you open the Overview page, you need to enter the hostname of the Control Service machine (instead of its IP Address). Enter the Control Service Host Name and Port No. as follows:

  https://host_name:port_no/start_page.aspx
- The .CER and .PEX certificates are Internet security files provided by a third-party certificate authorities. These certificates are installed on a Web server, to authenticate the validity of a certain website hosted on the server. They are represented by a lock icon near the edge of a browser window when accessing a secure site (beginning with "https://"). After you enter the path and name of a .CER of .PEX certificate in the SSL Configuration page, the Arcserve Continuity Suite Control Service - Install Shield Wizard installs the certificate and adds SSL certificate meta-information to the Web server. Such meta-information is maintained by the HTTP API in a metastore, and is used to locate certificates for certificate exchange in HTTPS sessions.
- If at present you do not have an authorized SSL certificate, you can use the **Self-signed Certificate**. After you select the **Self-signed Certificate** option, when you try to access the Overview page from a remote machine, you need to install the certificate. For more information, see Installing SSL Self-Signed Certificate.

10. Click **Next**.

    The **Service Logon Information** page appears.

11. Select and enter the required information. You can either use Local System Account privileges or provide a username and a password in the form of Domain/Username.

    Note: Running the Control Service in a Domain Account with administrative rights across several machines allows remote deployment and connection to the Engine, without being prompted for authentication on each individual server.

12. Click **Next**.

The **Control Service Role** page appears.

Note: Select the **Allow the Control Service** check box, and then define whether the currently installed Control Service assumes the role of the **Active** or **Standby** Control Service, only if you want to install two Control Services for role switching.

13. For a typical Control Service installation, click **Next**.

    The **Ready to Install the Program** page appears.

    Note: Click the **Back** button to return to the previous pages and change your configuration.

14. Click the **Install** button to install the Control Service.

    The **Installing Control Service** page appears.

15. Once the installation is completed, click **Next**.

16. Click **Finish** to close the wizard.

    The Control Service is now installed on your selected location.

Installing two Control Services for Control Service Role Switching

The installation of two Control Services for role switching is very similar to the standard installation. There are only two main differences:

- You need to repeat the installation procedure twice to install two Control Services.
- You need to define during the installation procedure whether the Control Service you are installing functions as the active Control Service or as the standby Control Service.

To install Control Service for role switching, follow these steps:

1. Double-click the **Setup.exe** installation file.

   The Arcserve Continuous Availability Installation wizard appears.

2. Click the **Install** option.

   The **Install Components** page appears.

3. Click the **Install Control Service** option.

   The **Choose Setup Language** dialog appears.

4. Select from the drop-down list the Installation wizard language you prefer, and then click **OK**.

   A progress bar appears. Once the initial process is completed, the **Welcome** page appears.

5. Click **Next**.

   The **License Agreement** page appears.

6. Select the **I accept** check box, and then click **Next**.

   The **Customer Information** page appears.

7. Verify that the details in the fields are correct, or change them accordingly, and then click **Next**.

   The s.

8. To select the Control Service installation location, use the **Change** button, or leave it at the default location, and then click **Next**.

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

The **SSL Configuration** page appears.

9. The **SSL Configuration** page allows you to use SSL certificate to secure communication with the Control Service.
   - To use the SSL Configuration option, refer to Install a Control Service for a Standard Operation.
   - To use SSL self-signed certificate, refer to Installing SSL Self-Signed Certificate.
10. After you have selected the communication configuration, click **Next**.

    The **Service Logon Information** page appears.

    Select and enter the required information. You can either use Local System Account privileges or provide a username and a password in the form of Domain/Username.

    Note: Running the Control Service in a Domain Account with administrative rights across several machines allows remote deployment and connection to the Engine, without being prompted for authentication on each individual server.
11. Click **Next**.

    The **Control Service Role** page appears.

    To install the Control Service for role switching, select the **Allow the Control Service** check box. Then, define whether the currently installed Control Service will assume the role of the **Active** or **Standby** Control Service.
12. Click **Next**.

    The **Ready to Install the Program** page appears.

    Note: Click the **Back** button to return to the previous pages and change your configuration.
13. Click the **Install** button to install the Arcserve Continuity Suite Control Service.

    The **Installing Arcserve Continuity Suite Control Service** page appears, displaying the progress of the installation.
14. Once the installation is completed, click **Next**.

    The **Install Shield Wizard completed** page appears.
15. Click **Finish** to close the wizard. The Control Service is now installed on your selected location.

16. Repeat this installation process for the second (Active or Standby) Control service.
17. Install the Arcserve Continuity Suite Engine on the destination servers of both Control Services.

Installing Control Service using the CLI

You can install the Arcserve Continuity Suite Control Service using the Command Line Interface.

To install the Arcserve Continuity Suite Control Service using the CLI

- Open the CLI and enter the following:

RHAManager.exe /S "/v/qn LOCALACCOUNT=No XOLOGIN="[Domain/UserName]" XOPASSWORD="[Password]" XOLANG="[Language]"

Parameters

RHAManager.exe

The setup file of the Arcserve Continuity Suite Control Service

S, V, QN

Silent installation parameters

Domain/UserName, Password

Enter the required information according to the platform you use and the solution you implement. For more information, see Supported Applications and Database Servers. If you don't enter the log on account details, the default is Local System.

Language

Select the language, by using one of the following language codes:

- "1033" English
- "1036" French
- "1041" Japanese
- "2052" Chinese (Simplified)
- "1028" Chinese (Traditional)
- "1031" German
- "1034" Spanish
- "1040" Italian
- "1046" Portuguese (Brazilian)

Example: Install the Control Service using the CLI

RHAManager.exe /S "/v/qn LOCALACCOUNT=No XOLOGIN="domain/administrator" XOPASSWORD="abcd" XOLANG="1033"

Note: The value "No" in "LOCALACCOUNT=No" is case-sensitive.

Configure Virtualization Platform and Cloud

This section describes configuration of the following Virtualization Platform and Cloud:

Configure ESXi

No special configuration is needed on ESXi.

On VA Linux VM, run the following command to verify if *virsh* can connect to target ESXi server:

[root@testva ~]# virsh -c esx://root@esxi_IP?no_verify=1 pool-list

The following output indicates successful configuration:

Name	State	Autostart
RHA_datastore1	active	yes

Configure Hyper-V

To configure Hyper-V, follow these steps:

1. On the Hyper-V server, run the following command:

   winrm set winrm/config/service/auth @{Basic="true"}

   winrm set winrm/config/service @{AllowUnencrypted="true"}

2. On VA Linux VM, run the following command to verify if *virsh* can connect to the target Hyper-V server:

   [root@testva]# virsh -c hyperv://administrator@Hyper-V_IP/?transport=http pool-list

   The following output indicates successful configuration:

Name	State	Autostart
F:\HyperVVM\	active	yes

Configure XenServer

No special configuration is needed on XenServer.

Configure KVM

Arcserve Live Migration supports three protocols for VA to communicate with the KVM server: SSH, SSL, and None. Following is an example procedure for configuring SSH protocol. For configuring other protocols, refer to the corresponding KVM documentation.

Use the *root* account to configure the Arcserve Live Migration on a Linux VA, which allows you to use the SSH protocol.

Follow these steps:

1. Run the following command in shell to create the ssh key pair:

   ssh-keygen -t rsa

   You can view two files: *id_rsa* and *id_rsa.pub*.

2. Run the following command in shell to transfer the public key to KVM server.

   ssh-copy-id -i ~/.ssh/id_rsa.pub root@kvm-server

   Type the password to continue.

3. Use the following command to connect to the KVM server from VA using ssh without entering a password:

   Ssh root@kvm-server

4. Run the following command in shell:

   virsh -c qemu+ssh://kvm-server/system pool-lis

   The following output indicates successful configuration:

Name	State	Autostart
Default	active	yes
kvm-datastore1	active	yes

Configure Microsoft Azure

Arcserve Replication and High Availability needs some of the Azure properties for Full System scenario to work with Azure. To configure for Microsoft Azure, you need to add an Azure Cloud Account in the Continuity Suite Manager. The Azure Cloud account must have the following information:

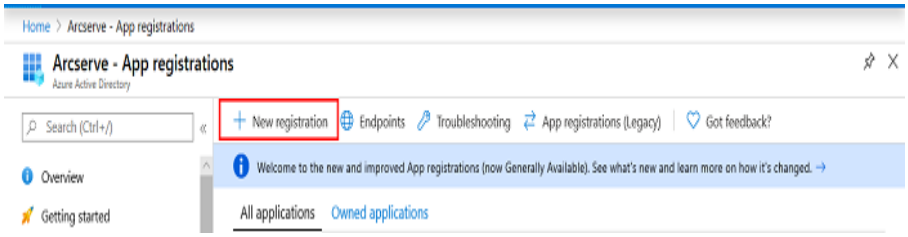
- E-mail Address
- Subscription ID
- Tenant ID (Directory ID)
- Application ID
- Client Key

First, prepare the Azure cloud account and then add the account in Continuity Suite Manager.

To prepare Azure Cloud account, follow these steps:

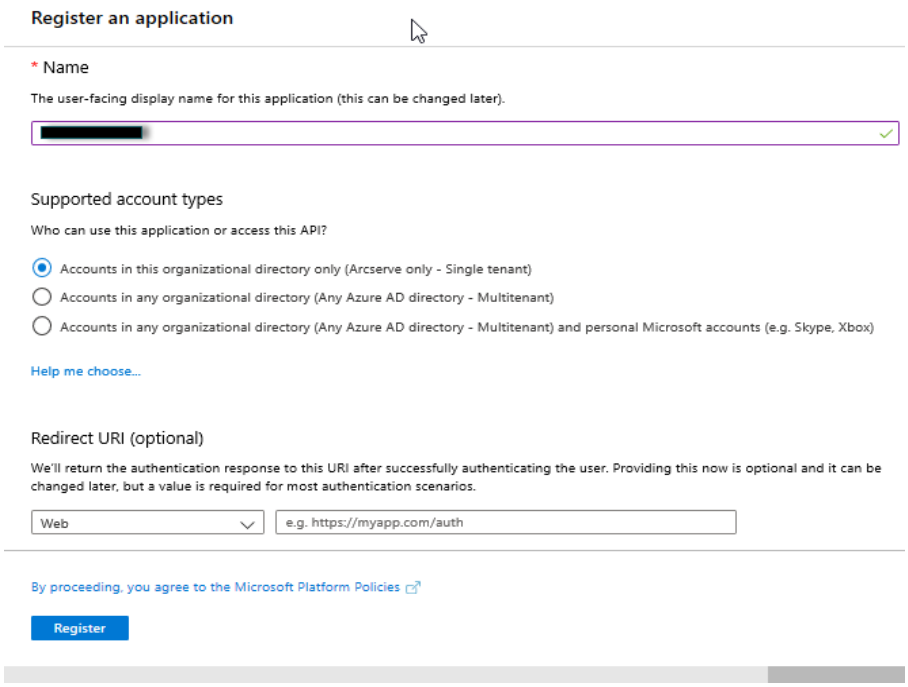
1. Perform the following steps to register an Azure Active Directory application:
   a. Log into the Azure portal.
   b. From the left pane, select **Azure Active Directory**, and then click **App registrations**.

      The **Arcserve- App registrations** page appears.



   c. Click **New registration**.

      The **Register an application** page appears.



d. On the **Register an application** page, do the following, and then click **Register**:

   - **Name:** Type a name for the application.
   - **Supported account types:** Select a supported account type, which determines who can use the application.
   - **Redirect URI (optional):** Select Web or Public client (mobile & desktop) for the type of application you are creating, and then enter the redirect URI for your application.

e. Go to Subscriptions, select your subscription, and then click **Access control (IAM)**.

f. From the respective drop-down lists of Add permissions on the right pane, select the Contributor role and your application, and then click **Save**.

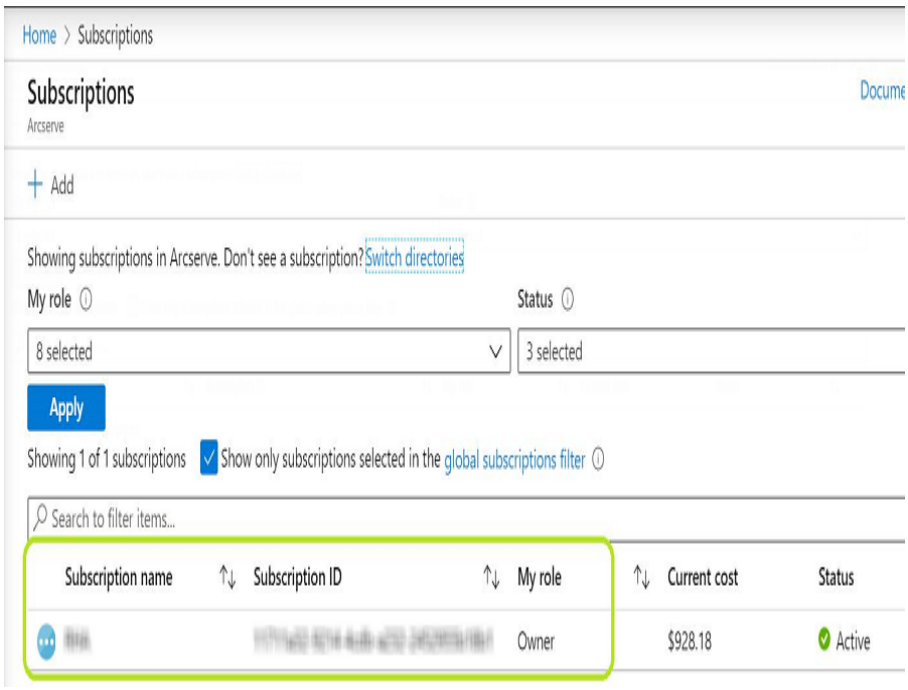
The registration of an Azure Active Directory application is complete. Now, you can perform the next steps using the registered application to get required IDs and Key.

2. Perform the following steps to get the Subscription ID[1]:

[1]The Subscription ID refers to a GUID (Globally Unique Identifier) that uniquely identifies your subscription to use Azure services.

a. From the left navigation pane of Azure portal, click **Subscriptions**.

The list of your subscriptions is displayed along with the subscription ID.



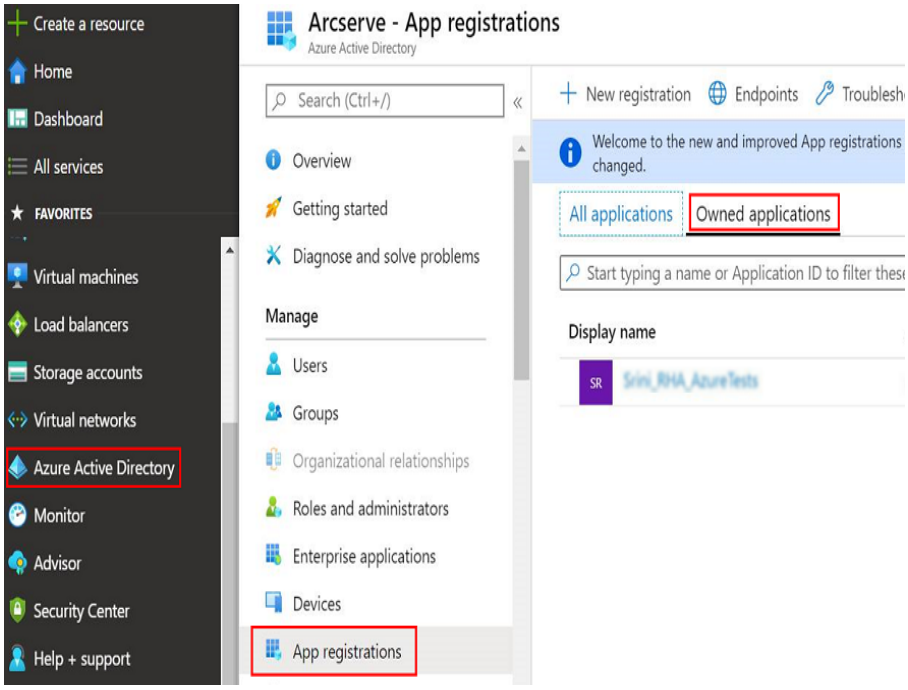
b. Copy the subscription ID to use while adding the account in Continuity Suite Manager.

3. Perform the following steps to get the Tenant ID[1] and Application ID[2]:

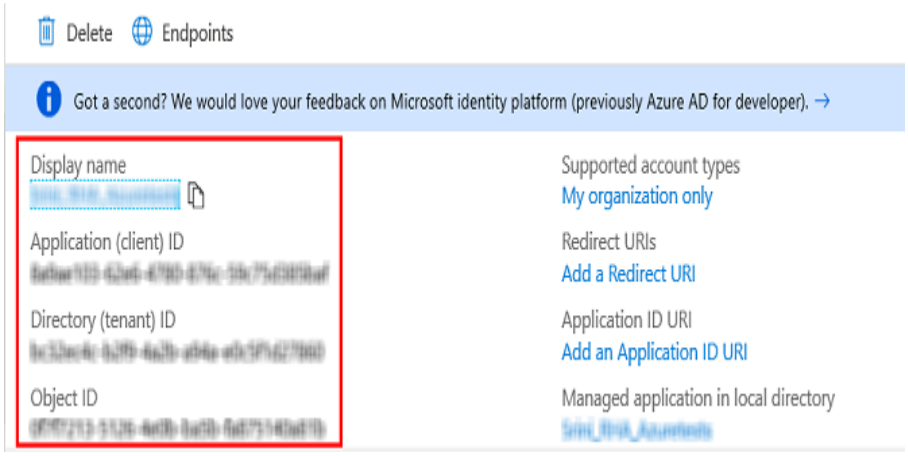
a. Navigate to **Azure Active Directory** > **App registrations** > **Owned applications**.

[1]Tenant ID refers to the ID of the Azure Active Directory where you created the application registration. Tenant ID is called Directory ID inside Azure Active Directory Properties.

[2]An Application ID refers to a GUID that uniquely identifies the app's registration in the Azure Active Directory tenant. Sometimes, it is also referred as Client ID.



b. Select your application from drill-down pane to view Tenant and Application ID's.

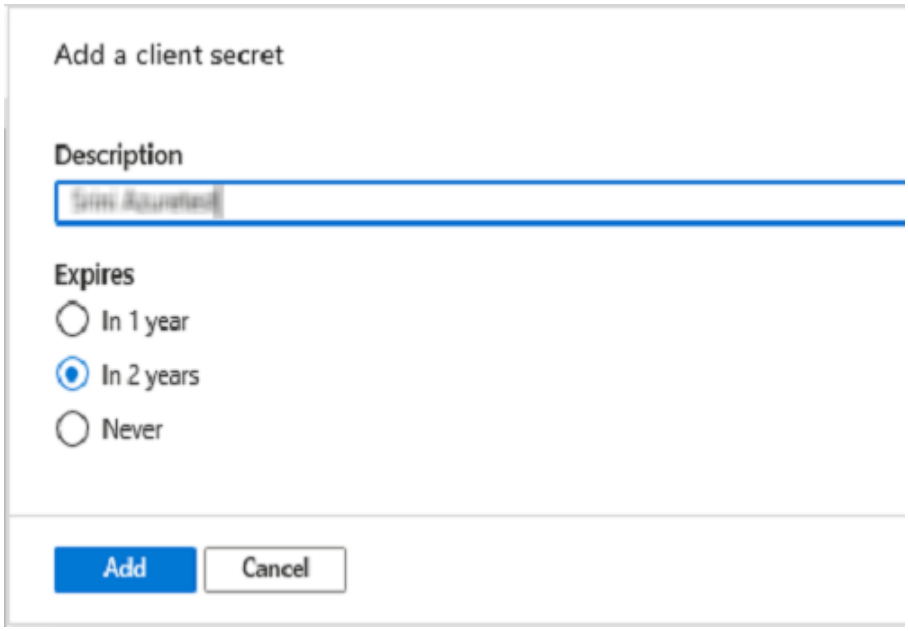


4. Perform the following steps to generate an authentication key and get the Client secret[1]:

   a. Select the application, and then navigate to **Certificates & secrets**. Click **New client secret** to add a client secret.

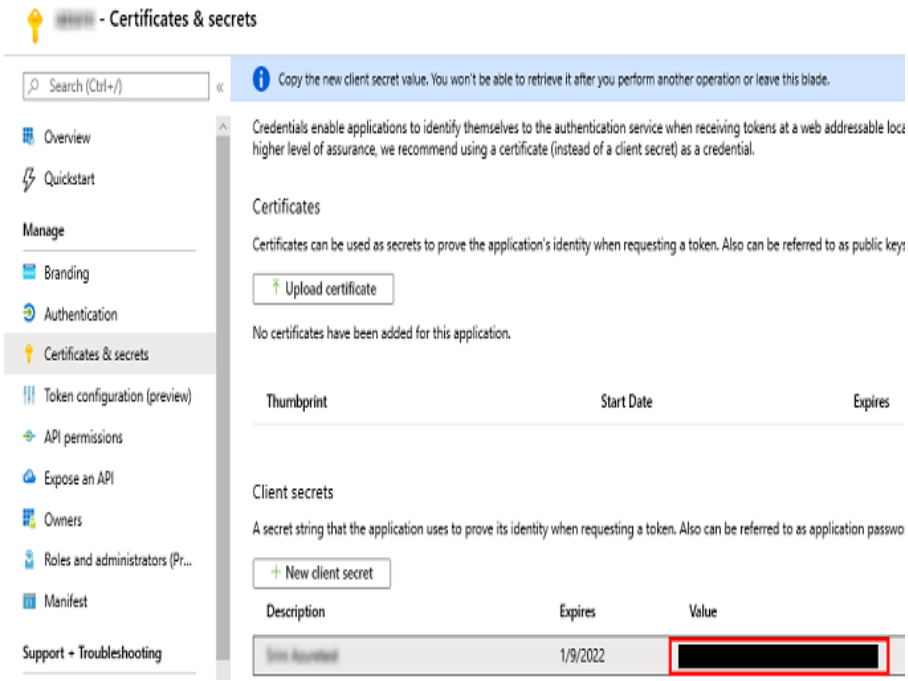
      The **Add a client secret** page appears.

[1]Client secret is referred as an authentication key in Azure.



b. Enter the description, select the desired expiry interval and then click **Add**.

The value of client key is displayed.



c. Copy and use this value while adding the account in the Continuity Suite Manager.

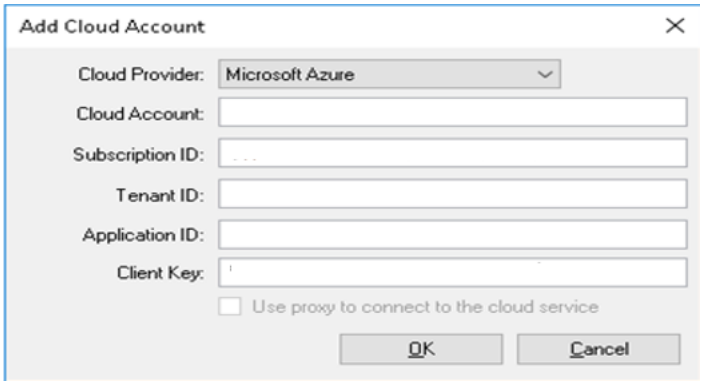
Note: Copy and save this value as you cannot retrieve it later.

Preparation of Azure Cloud Account is complete. Now, add details in the Continuity Suite Manager.

Add an Azure Cloud Account in Continuity Suite Manager

1. From the Continuity Suite Manager, navigate to **Cloud** > **Manage Cloud Accounts** and then click **Add**.

   The **Add Cloud Account** screen appears.



2. Enter the following details in the required fields, and then click **OK**.

   - Cloud Account - Provide the cloud account, which is a user name you have defined. For more information, see
   - Subscription ID - Provide the Subscription ID. For information about how to get a Subscription ID, see step 2 of the previous
   - Tenant ID - Provide the Tenant ID. For more information about how to get the Tenant ID, see step 3 of the previous
   - Application ID - Provide the Application ID. For more information about how to get the Tenant ID, see
   - Client Key - Provide the Client Key. For more information about how to get the Tenant ID, see

   The Azure account for Live Migration is now configured.

Configure Amazon EC2

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

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

Considerations before deploying EC2-based Full System scenarios are as follows:

- 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 required information from your administrator.
- The Amazon EC2 user in Arcserve Replication and High Availability should have required permissions. For details, refer to 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 pick one public IP from existing Elastic IP addresses for the DR VM.

Deploy VA on EC2/Azure/Hypervisor VM

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, and the Disaster Recovery VM of Master starts and runs on this virtualization platform or cloud for multiple reasons, such as Assured Recovery testing, Switchover, and Start VM.

Note: For Windows Full System scenario replicating to Hyper-V, no additional VA virtual machine is required. The Disaster Recovery Hyper-V server takes the role of VA as well as virtualization platform.

Hardware Configuration for Virtual Appliance (VA)

Following are minimal hardware configuration settings recommended for VA VM:

CPU	2 cores
Memory	8 GB
Spool Space	Approximately 15% - 30% of master data size of free space should be considered for volume where Continuity Suite spool directory is set, depending on total data size and data change rate on the master server. When multiple master servers replicate to the same VA, the required spool space on VA needs to add up to avoid possible spool exceeding that in turn causes scenario to stop.

Considerations for VA Running on Cloud and Local Environments

Note: For cloud, log into Microsoft Azure or Amazon EC2 portal and create a virtual machine to work as Arcserve Replication and High Availability VA.

Important! Do not manually delete the virtual machine, its configuration, and virtual disk files, otherwise, the scenario can fail.

The following are the considerations for Virtual Appliance VM:

- For Xen platforms, install XenServer Tools on the Appliance VM.

  Note: If your virtual platform is Citrix Xen 6.0, install the .NET 4.0 Framework on the protected master. The .NET 4.0 Framework is required for installing the Xen tool on the virtual machine that the appliance created.
- For ESXi and vCenter platforms, install VMware Tools on the Appliance VM.
- Install the Continuity Suite Engine on the Appliance VM.
- For Amazon EC2, ensure that the date and time are correct and synchronized to your system, and the network can access AWS.
- For Azure, from Disks configuration screen, select **Use managed disks**. Arcserve Replication and High Availability does not support unmanaged disks on Azure.
- Continuity Suite Engine port (TCP 25000 by default) is allowed for incoming connections.
- Assign a public Static (for Azure) or Elastic (for EC2) IP address to VA so that the IP address does not change after restart.
- For Linux Virtual Appliance VM running on Azure or EC2, you must enable *PasswordAuthentication* in */etc/ssh/sshd_config*.
- After the Continuity Suite Engine is installed on VA, verify that Continuity Suite Master and Control Service can reach Arcserve Replication and High Availability VA by running the following command separately on Master and Control Service:

  telnet <VA-public-IP> 25000

  Press Space bar to get Continuity Suite Engine version information.

Continuity Suite Engine for Virtual Appliance (VA) Installation

Configure Continuity Suite Engine on Windows and Linux.

OS	Platforms Supported as VA
Windows	Windows 2012 R2, Windows 2016, Windows 2019
Linux	CentOS 7.5 and 7.6, Red Hat Enterprise Linux (RHEL) 7.5 and 7.6

Configure Continuity Suite Engine for Virtual Appliance (VA) Installation in Windows

Configure the Continuity Suite Engine on Windows. For more information, see Compatibility Matrix.

To install Engine component on virtual appliance, see Install Engine. Usually no additional configuration is required.

The following platforms are supported as VA on Windows:

- Windows 2012 R2
- Windows 2016
- Windows 2019

Configure Continuity Suite Engine for Virtual Appliance (VA) Installation in Linux

The following platforms are supported as VA on Linux:

- CentOS 7.5 and 7.6
- Red Hat Enterprise Linux (RHEL) 7.5 and 7.6

To install Virtual Appliance (VA) server on Linux, follow these steps:

1. Mount **ContinuitySuite.iso** to the VA server, double-click *.iso to open the Unix_Linux directory, and then enter into the Unix_Linux directory.
2. Run the following commands to extract the Unix_Linux directory, and then change directory to the extracted directory:

   tar xvf arcserverha.tar

   tar xzf arcserverha-xxxx.rhel7.tgz

   cd arcserverha

3. Run installation script in one of the following modes:
   - **Interactive mode**:
     a. Run the following command:

        ./install.sh

     b. Type **q** and then press **Enter** to accept EULA and continue.

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

        Install Arcserve RHA version xxxx?[YES]

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

     c. Type **y** to install VA module. The installation wizard is ready for use.
   - **Silent mode**: Run the following command to install Continuity Suite Engine and VA module silently:

     ./install.sh -y -v y

4. To verify the installed **qemu-guest-agent** packages for Linux VA, run the following command:

```
# yum list qemu-guest-agent

Installed Packages

qemu-guest-agent.x86_64 10:2.12.0-3.el7 @base
```

By default, this package gets installed on CentOS/RHEL 7. If it does not get installed, then use the following command:

```
# yum install qemu-guest-agent
```

Install Engine on Source

This section describes how to install the Arcserve Continuity Suite Engine.

Use the following ways to install the Arcserve Continuity Suite Engine:

- Using the Setup.exe file - install the Engine on one host at a time. This installation method automatically detects an Engine from a previous version and enables you to remove it during the installation of the new Engine. The installation steps are similar to the Control Service installation steps, as described on Installing the Arcserve Continuity Suite Control Service.
- Using the Scenario Creation Wizard - remotely install the Engine on the Master and Replica hosts, during the creation of a new scenario.
- Using the Remote Installer - remotely install the Engine on one or more hosts at the same time.
- Using the Command Line Interface (CLI)- install the Arcserve Continuity Suite Engine on the Master and Replica servers using the Command Line Interface.

Note: Before you install the Continuity Suite engine on a Windows 2008 R2 Server Core, register the ieproxy.dll and install the Visual C++ 2005 redistributable package.

To install the Arcserve Continuity Suite Engine on a Windows Server 2008 R2 Server Core, follow these steps:

1. Navigate to the %programfiles%\Internet Explorer folder on a Windows Server 2008 R2 (non Server Core installation).
2. Locate the ieproxy.dll file and copy it to the following location on the Server Core:

   %systemRoot%\system32
3. To register, enter the following command at the command prompt:

   regsvr32 %systemRoot%\system32\ieproxy.dll
4. Install the Microsoft Visual C++ 2005 Redistributable Package (x64). Download the Redistributable Package from www.microsoft.com.

Installing Engine Using the Setup.exe Installation File

To install Arcserve Continuity Suite Engine using the Setup.exe file, follow these steps:

1. Double-click the **Setup.exe** installation file.

   The Arcserve Live Migration Installation wizard appears.

   Important! On Windows 2008, you may get digital signature error during installation and then the installation rolls back. You need to update the Windows root certificate to avoid this error. Download and install the update from the Microsoft website.

2. Click the **Install** option.

   The Install Components page appears.

3. Click the **Install Arcserve Continuity Suite Engine** option.

   The Choose Setup Language dialog appears.

4. Select from the drop-down list the Installation wizard language you prefer, and then click **OK**.

   A progress bar appears. Once the initial process is completed, the Welcome page appears.

5. Click **Next**.

   The License Agreement page appears.

   Note: If an Engine from a previous version exists on your server, the Information about previous version page appears, providing you the option to uninstall the Engine.

6. On the License Agreement page select the **I accept** check box, and then click **Next**.

   The Destination Folder page appears.

7. Verify that the details in the fields are correct, or change them accordingly, and then click **Next**.

   The Custom Setup page appears.

   Note: When you select the **Engine** option, the **Space** button is enabled. To see the disk space required for the installation of the selected feature, click the **Space** button.

8. Click **Next**.

   The Service Logon Information page appears.

9. Enter the required information according to the platform you use and the solution you implement. For more information, see Supported Applications and Database Servers.

   For File Server, use the following guidelines:

   - For Replication scenarios - it is sufficient to use the Local System Account.
   - For clusters (Replication scenarios) - you need to run under the same account as the Cluster Service or under equivalent permissions.
   - For High Availability scenarios (including clusters) -
     - You need to run under an account with the Domain Administrative privileges. If the Domain Admins group is not a member of the built-in domain local group Administrators, you must use an account that is.
     - The account also needs to be a member of the local machine Administrators Group. If the Domain Admins group is not a member, add the account manually. For servers in a workgroup, use the Local System account.

10. Click **Next**.

    The Ready to Install the Program page appears.

11. Click **Install**.

    The Installing Arcserve Continuity Suite Engine page appears.

12. Once the installation is completed, click **Next**.

    The Install Shield Wizard Completed page appears.

13. Click **Finish** to finish the installation.

Installing Engine Using the Scenario Creation Wizard

To install the Engine using the Scenario Creation Wizard, follow these steps:

1. Open the Manager, select Scenario, **New** or click the **New Scenario** button to launch the wizard.

   The Welcome screen opens.

2. Select **Create a New Scenario**, select a Group from the list, and then click **Next**

   The Select Server and Product Type page appears.

3. Select the required scenario options, as follows:

   - **Select Server Type:** Select the type of server that is used in the scenario.
   - **Select Product Type:** Select **Replication and Data Recovery Scenario (DR)** or **High Availability Scenario (HA)** according to your license.

4. Click **Next**.

   The Master and Replica Hosts page appears.

5. On the Master and Replica Hosts page, do the following, and then click **Next**:

   - Scenario Name - accept the default scenario name or enter a new name for the scenario.
   - Master Hostname/IP and Replica Hostname/IP - enter the name or IP of the Master and Replica hosts, or use the *Browse* button to find the Master and Replica hosts.

     Note: When creating an HA scenario, we recommend you enter the host IP address (and not the hostname).

   - User credentials for hosts verification - enter user credentials that enable you to access the remote hosts on which the Engines gets installed.

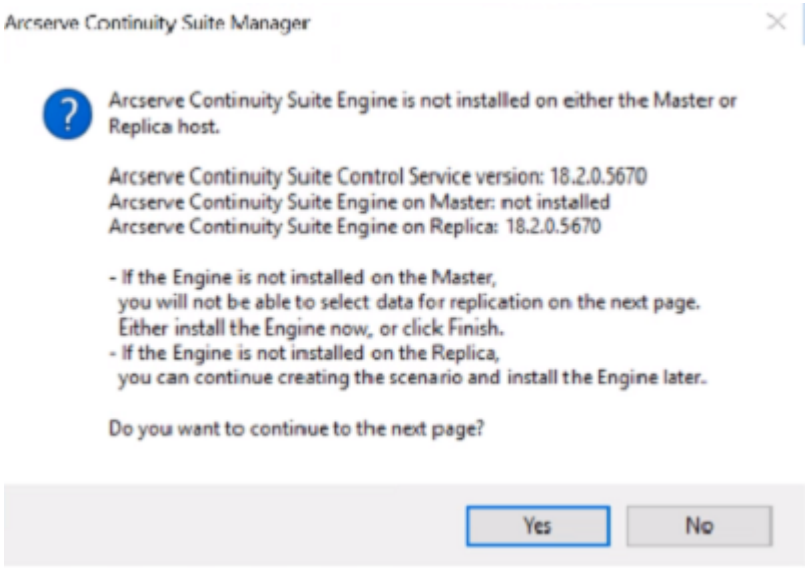
   The Engine Verification page appears.

6. The system verifies the connectivity of the Master and Replica hosts you have selected in the previous page. Once the connections are verified, the system checks whether an Engine is installed on each host.

   Note: An Error message indicates that a connection could not be established to the specified host. If any errors are reported, you cannot continue until they are resolved.

Check whether an Engine is installed on the selected hosts using the **Server Status** column:

- If all the hosts have an **Installed** version, you can move to the next page.
- If any of the hosts have **Not Installed** under the Current Version column, then you need to install the Engine on these hosts.
- If an Engine is not installed on one or both hosts, and you click the **Next** button, the following message appears:



Click **No** to return to the Engine Verification page and install the Engine.

7. On the Engine Verification page, click the **Install** button to remotely install the Engine on the selected host.

   Note: You can install the Engine on both hosts at the same time. To perform this, select the check box of both the hosts, and then click the **Install** button.

   Wait until the installation is complete. The version number of the Engine appears in the *Current Version* column.

8. Click **Next**.

   The Master Root Directories page appears.

   Follow the wizard instructions to complete the scenario creation. For more information about the creation of a new scenario, see Arcserve Continuous Availability Administration Guide.

Installing Engine Using the Remote Installer

You can use the Remote Installation Wizard to deploy the Engine to any number of servers, or cluster nodes, in one step.

If you are running a firewall on the machine where you plan to install the Engine, you must enable the Engine as an exception for Windows Management Instrumentation (WMI) in the Windows Firewall Exception List. If you are running Windows 2003 or Windows XP, please go the Microsoft MSDN website and search for the Connecting Through Windows Firewall document.

Note: In some setups, the remote WMI requests are disabled. This causes verification to fail while deploying the Arcserve Continuity Suite Engine using the Remote Installer. To resolve this issue, see Troubleshooting Verification Failure when Using the Remote Installer.

To install Engine using the Remote Installer, follow these steps:

1. On the Continuity Suite Manager, from the **Tools** menu, select **Launch Remote Installer**.

   The Remote Installer view opens, and the Remote Installation Wizard appears, displaying the Host Selection page.

   Notes:

   - If you currently have scenarios on the Manager, the hosts that participate in these scenarios appear in the **Selected Hosts** pane. This enables you to easily update the Engine version that is installed on them.
   - If you want to access other Manager features while you are using the Remote Installer, you can minimize the Remote Installation Wizard, and return to it later. The wizard is bound to the Remote Installer Monitor view. If you switch views, the wizard is automatically minimized.

2. On the Host Selection page, select the hosts where you want to install the Engine. You can select the hosts automatically and manually:

   - To automatically discover the existing hosts in your domain, click the **Start Hosts Discovery** button. The discovered hosts appear on the Discovered Hosts pane on the left. To select a host, double-click it. The host then appears on the Selected Hosts pane on the right.
   - To manually select a host, enter its hostname or IP address in the Host Name/IP Address field, and then click **Add**. The host you have entered appears on the Selected Hosts pane.

Note: When using clusters, you need to install the Engine on all physical nodes and select a physical node instead of a cluster name.

3. Repeat the selection as many times as needed. The Engine gets installed only on the servers that appear on the **Selected Hosts** pane.

   Note: To remove hosts from the **Selected Hosts** pane, select the host, and then click the **Remove** button.

4. After you select the host, click **Next**.

   The **User Credentials** page appears.

5. Set the user account that is used to access each target host. You need Local Administrator credentials for all selected hosts.

   Notes:

   - You must enter the same **User Credentials** you used for logging into the remote host.
   - If you do not need to provide a Domain value to the selected host, leave the **Domain** field empty, and enter "**.**" before the Username.
   - If you log in using the non-admin local account or domain account without the admin rights, the default setting changes from *Current User* to the *Following User*.

6. Click **Next**.

   The **Preinstall Verification** page appears.

   The Remote Installer automatically checks the existence, connectivity and configuration of the servers you have selected on the previous page. After the verification process is complete, the results are displayed.

   Note: If a server's status is reported as an error, and you have verified that the server exists and is properly connected, select the server, and then click the **Verify Again** button. The Remote Installer repeats the verification process.

7. After the status of all servers has reported **Not Installed**, click **Next**.

   Note: If an older Engine version is reported as **Installed**, to uninstall it, click the **Uninstall** button. After you uninstall, click **Next**.

   The **Installation Settings** page appears.

8. On the **Service Logon Information** section, select the account type to set the service logon information.

   Local System Account

   Specifies to use Windows Local system account.

Current User

Specifies to use the user account you logged in with.

This Account

Specifies to use a different user by typing the username, password and domain.

Note: Select the **Use the service log on account for existing installations** check box, if you want to upgrade an existing Engine and you want Arcserve Live Migration to use the log on account details under which the Engine is installed.

9. Click **Next**.

   The **Ready to Install** page appears.

10. Verify that all desired servers are listed, and then click the **Install** button to install the Engine on these servers. A confirmation message appears.

11. Click **Yes** to install the Engine. The **Remote Installer** status pane appears. Wait until the **Server Status** is reported as **Installed.**

12. Close the **Remote Installer** status pane. On the Remote Installer view, the installation status is reported as *Installation complete*.

    The Engine is now installed on all selected servers or cluster nodes.

Installing Engine using the CLI

You can install the Arcserve Continuity Suite Engine on the Master and Replica servers using the Command Line Interface.

To install Arcserve Continuity Suite Engine using the CLI

- Open the CLI and enter the following:

```
RHAEngine.exe /S "/v/qn LOCALACCOUNT=No XOLOGIN="[Domain/UserName]"
XOPASSWORD="[Password]" XOPORT="[Port]" XOLANG="[Language]"
```

Parameters

RHAEngine.exe

The setup file of the Arcserve Continuity Suite Engine

S, V, QN

Silent installation parameters

Domain/UserName, Password

Enter the required information according to the platform you use and the solution you implement. For more information, see Supported Applications and Database Servers. If you don't enter the log on account details, the default is Local System.

Port

Enter the port number. The default port value is 25000.

Language

Select the language, by using one of the following language codes:

- "1033" English
- "1036" French
- "1041" Japanese
- "2052" Chinese (Simplified)
- "1028" Chinese (Traditional)
- "1031" German
- "1034" Spanish
- "1040" Italian
- "1046" Portuguese (Brazilian)

Example: Install the Engine using the CLI

RHAEngine.exe /S "/v/qn LOCALACCOUNT=No XOLOGIN="domain/administrator" XOPASSWORD="abcd" XOPORT="25000" XOLANG="1033"

Note: The value "No" in "LOCALACCOUNT=No" is case-sensitive.

Create Full System Scenario

This section provides instructions on the Arcserve Live Migration process.

Creating Live Migration Scenarios

Arcserve Live Migration protects servers in the context of user-defined scenarios. Scenario is a configuration unit which you create and migrate using rich management GUI or PowerShell CLI, and consists of a definition set that includes:

- The type of application or database server to be protected.
- The type of data protection solution.
- Special tasks, such as Integrity Testing for Assured Recovery.
- The connection details of the Master and Replica hosts.
- The directories, sub-directories, databases and files that gets replicated, and their location on the Master and the Replica.
- Configurable properties of the scenario and the Master and Replica hosts, which affect different settings and operations, such as, synchronization method, replication mode, spool size, report and event handling rules, and more.
- Recovery and Switchover/Failover parameters.

Each scenario defines a replication tree that sets the flow of information from the Master server to any number of designated Replicas. It establishes the data recovery procedure, and, if applicable, the switchover parameters. You can configure, add or remove servers from a scenario and select or modify directories. This enables easy, complete control of the migration process over any network, large or small. Each scenario is saved as an XML file.

Migrating Full System Scenarios to Virtualization Platforms and Cloud

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

Full system scenarios require three hosts instead of two:

- Master server - The host that you want to protect. This host can be physical or virtual. For more information about configuring the Master server, see Configure Master Server.
- Virtual Appliance - A VM where you installed the Arcserve Continuity Suite Engine. For more information about configuring Virtual Appliance, see Deploy VA on EC2/Azure/Hypervisor VM.
- Virtual Platform Host - The server where the Appliance VM is running. For more information about configuring Virtual Platform Host, see Configure Virtualization Platform and Cloud.

Consider the following when planning Full System scenario:

- **Engine Service Account:** For Windows, Local System account is recommended for Continuity Suite Engine Service Log On account for both Master and Replica/VA. You can also use Domain administrator or local administrator account. Make sure that such an account has Full Control permission on all protected volumes, spool directories, and virtual disks mount points on Replica/VA, which is Engine *<installation dir>\vm* by default.

  For Linux, Continuity Suite Engine runs with root account after installation, and cannot be changed.
- **Engine package dependencies on Linux:** Continuity Suite Engine installation on Linux requires dependent packages pre-installed, or a proper yum repository is configured. If you want to manually install packages required by Continuity Suite Engine, run the following command to get the list of required packages:

  rpm -qpR arcserverha_rhel7_x86_64.rpm

Migrating Full System Scenarios for Hypervisors

The following procedure applies to vCenter, ESXi, Hyper-V, XEN, and KVM Full System scenarios.

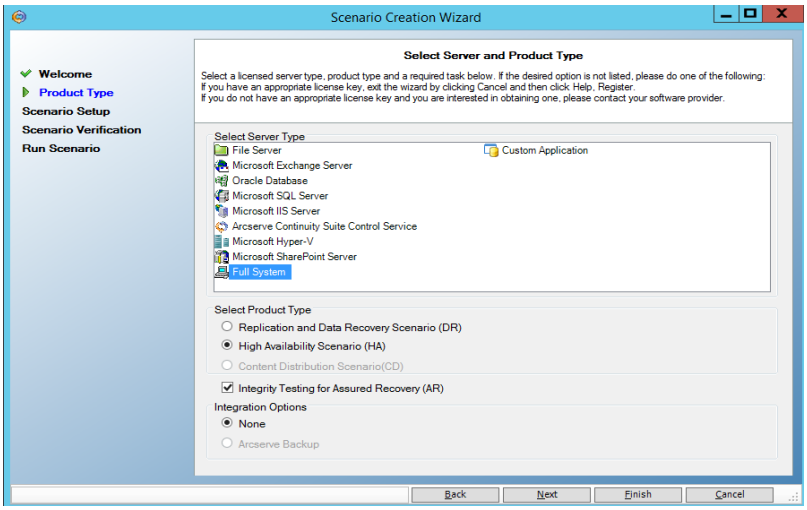
To migrate full system scenarios for all platforms except Hyper-V, follow these steps:

1. Open the Manager, select Scenario, **New** or click the **New Scenario** button to launch the wizard.

   The Welcome screen opens.

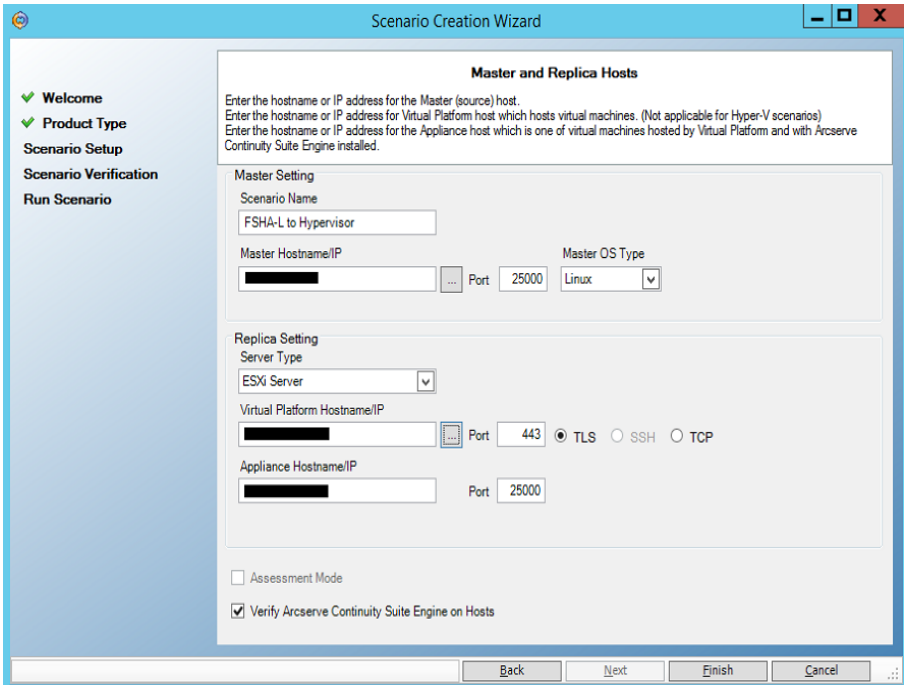
2. Select **Create a New Scenario**, select a Group from the list, and then click **Next**.

   The Select Server and Product Type screen opens.



3. Select Full System, select HA or DR and the desired tasks on Replica, and then click **Next**.

   The Master and Replica Hosts screen opens.



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

   - **Scenario Name:** Type a Scenario Name. The default value is the scenario type, for example, Full System.
   - **Master Hostname/IP and Port:** Specify the physical machine you wish to protect or browse to select the Master server.
   - **Master OS Type:** Specify Windows or Linux as the Master OS Type.

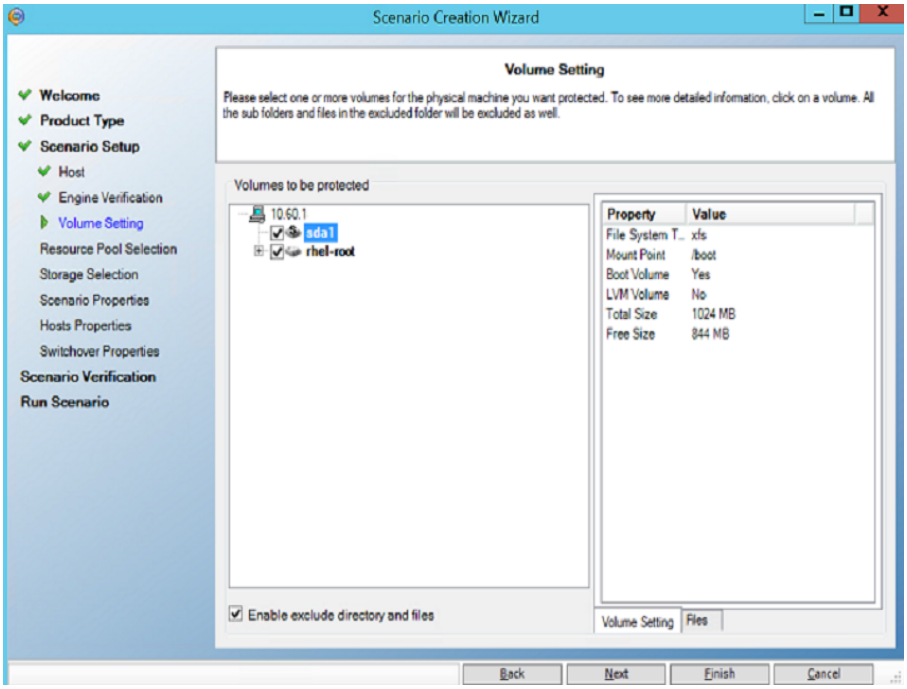
     Note: For Windows, enter IP address or hostname of the Windows server to be migrated.
   - **Server Type:** Select the virtual platform of the machine that will host the VM, for example, ESXi Server.
   - **Virtual Platform Hostname/IP and Port:** Specify the physical machine running the virtual machine platform you have selected in Server Type or browse to select the virtual machine.
   - **Appliance Hostname/IP and Port:** Specify the virtual machine hostname or IP address of the VM to act as the Replica server in this scenario. If the server type is Hyper-V, this field is not available.
   - **Verify Arcserve Continuity Suite Engine on Hosts:** Enable this option to confirm the latest version of the Engine is installed on all servers specified in the scenario.

   Enter the appropriate credentials for the specified machines, if prompted.

Wait for the verification to complete. If desired, you may install the Arcserve Continuity Suite Engine on any server. If errors occur, click **Verify Again** to resolve the errors. Contact your security administrator if any RPC Services errors occur.

5. Click **Next** when the Engine is verified on hosts.

   The Volume Setting screen opens. Arcserve Continuity Suite auto-discovers the volumes on the specified Master server.



6. Specify the volumes you want to protect. (Optional) Enable the option, Enable exclude directory and files. This option filters pagefile.sys, hiberfil.sys, System Volume Information, Recycler, and Recycled files and folders by default.

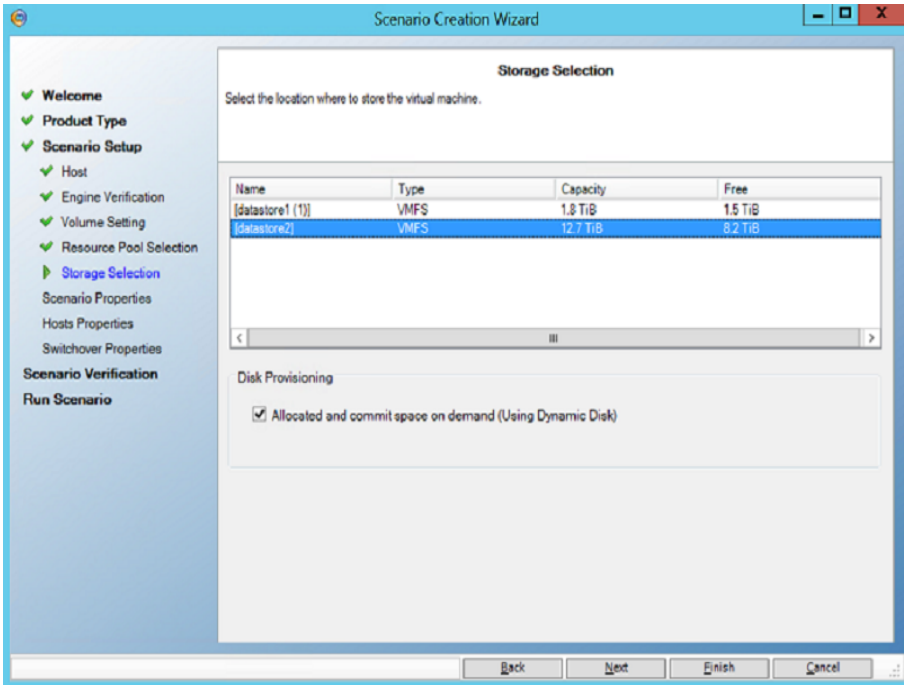
7. Click **Next**.

   You may be prompted to enter credentials for the server.

   The Resource Pool Selection screen opens.

8. Click **Next**.

   The Storage Selection screen opens.

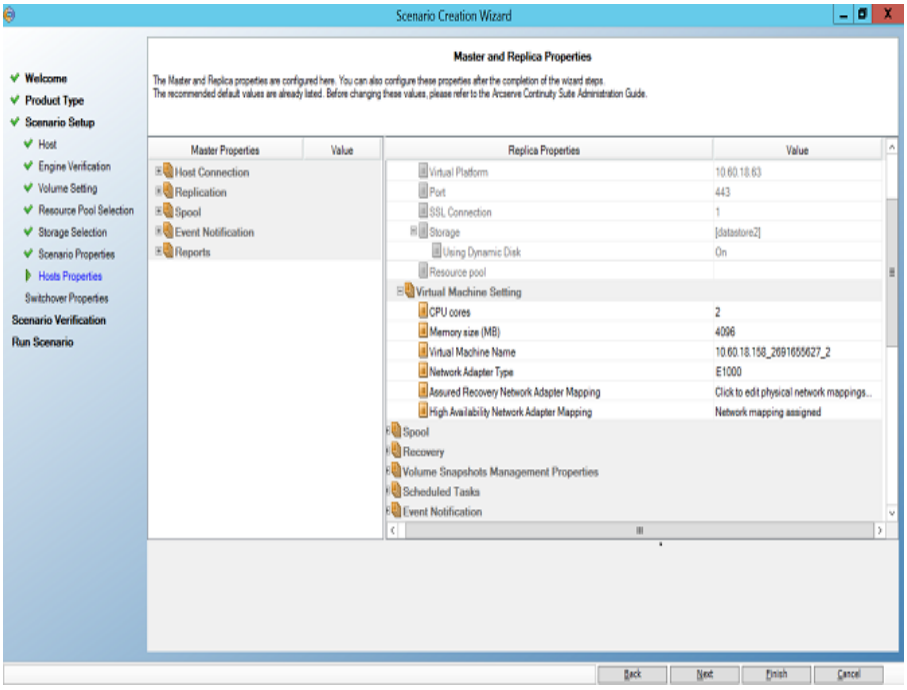


9. Specify where the virtual machine must be stored. Enable the option, Allocate and commit space on demand, if desired and then click **Next**.

   The Scenario Properties screen opens.

10. Change properties, as desired and click **Next**. For more information, see Arcserve Continuous Availability Administration Guide.

    The Master and Replica Properties screen opens.



11. Change properties, as desired, and then click **Next**.

The following information is acquired:

- CPU number
- Memory size on VM
- Adapter information on the physical Master
- Network Mapping List

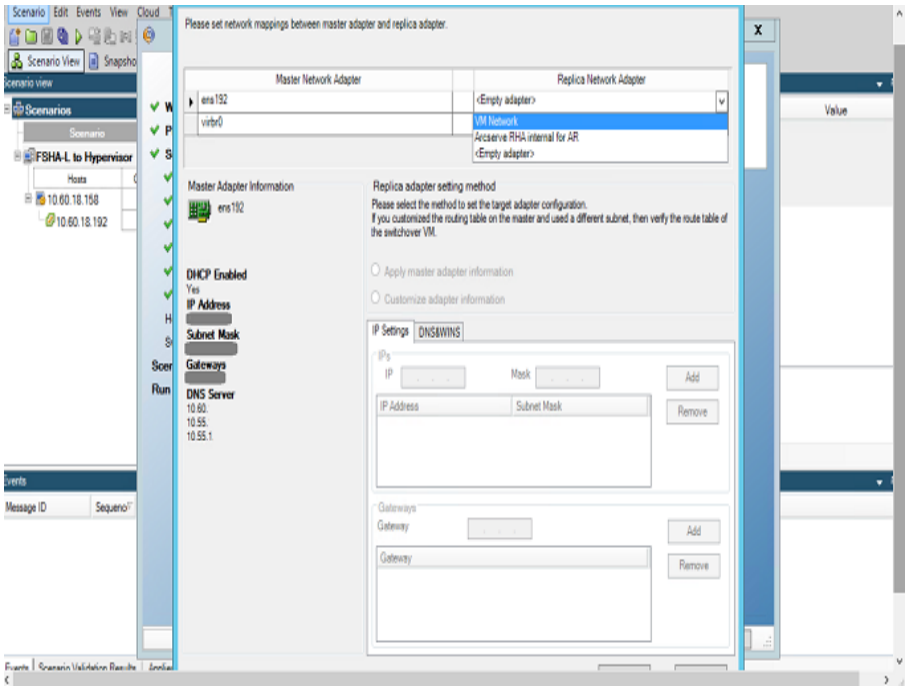
You may also change these settings outside of the scenario creation wizard. For more information, see Arcserve Continuous Availability Administration Guide.

Wait until Arcserve Continuity Suite retrieves Switchover Properties.

12. When the Switchover Properties screen opens, expand the Network Traffic Redirection properties. The Network Adapter Mapping dialog opens. On this dialog, modify the physical network mappings.

    Note: If there is only one virtual network adapter in both the Master and Replica servers, they are mapped automatically.

    a. Click the drop-down menu in the Replica Network Adapter column and select the adapter you wish to map to the adapter listed in the Master Network Adapter column.



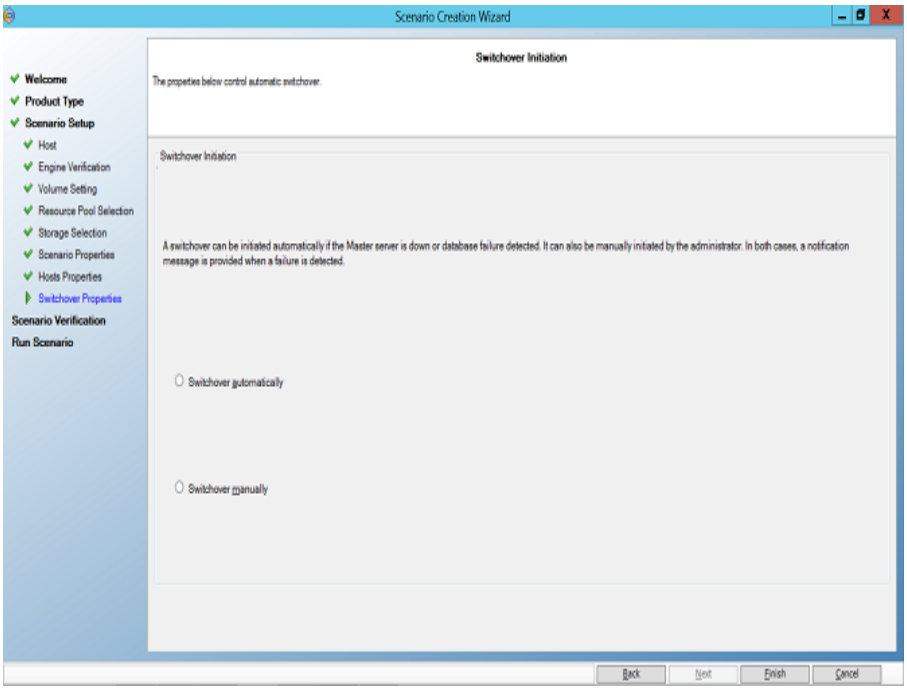
    b. For Replica adapter setting method, do the following:

        - **Apply master adapter information** - (default) Select this option if the Master Adapter is in DHCP mode.

- **Customize adapter information** - Select this option to enable the IP Settings and DNS&WINS tabs.
- **IP Settings** - You can add or remove IP Addresses, Subnet Masks and Gateways.
- **DNS&WINS** - You can add or remove DNS IP Addresses, Primary or Secondary WINS.

13. Click **OK** to close the Network Adapter Mappings dialog, and then click **Next** to continue.

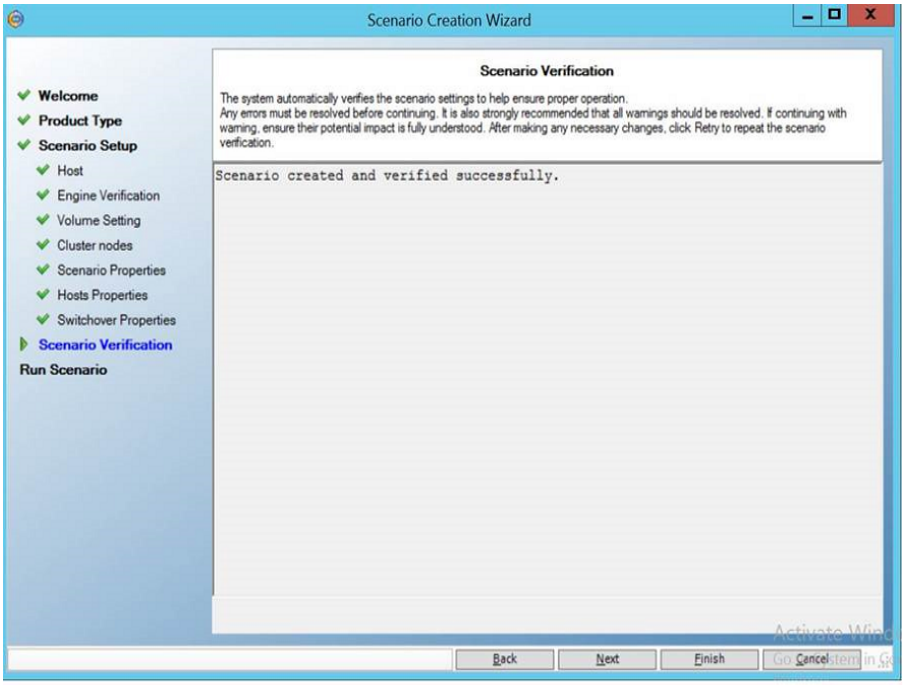
    The Switchover Initiation screen opens.



14. Specify if switchover must be started automatically or manually, and then click **Next**. Reverse Replication cannot be specified in this scenario.

    Note: If Scenario Verification lists any errors, you must resolve them to continue. If any warnings are listed, you should also resolve them to successfully continue. After making changes, click **Retry** to repeat verification.

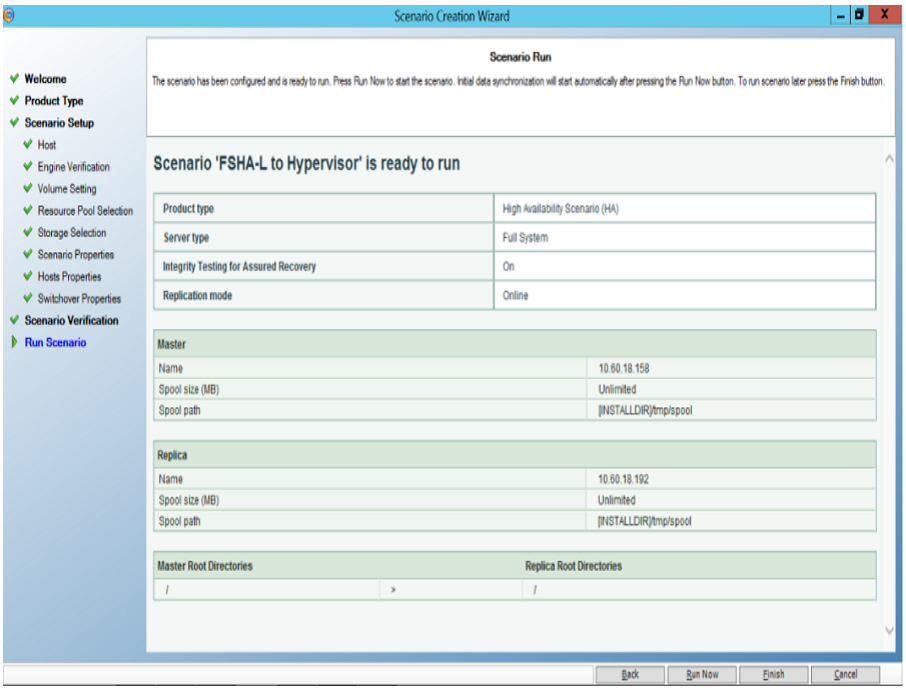
    The Scenario Verification screen opens.



The scenario verification runs automatically, and the configurations are now complete.

15. Click **Next**.

    The Scenario Run screen opens.



16. Click **Run Now** if you wish to start synchronization immediately and activate the scenario. Click **Finish** to save current settings and run the scenario later.

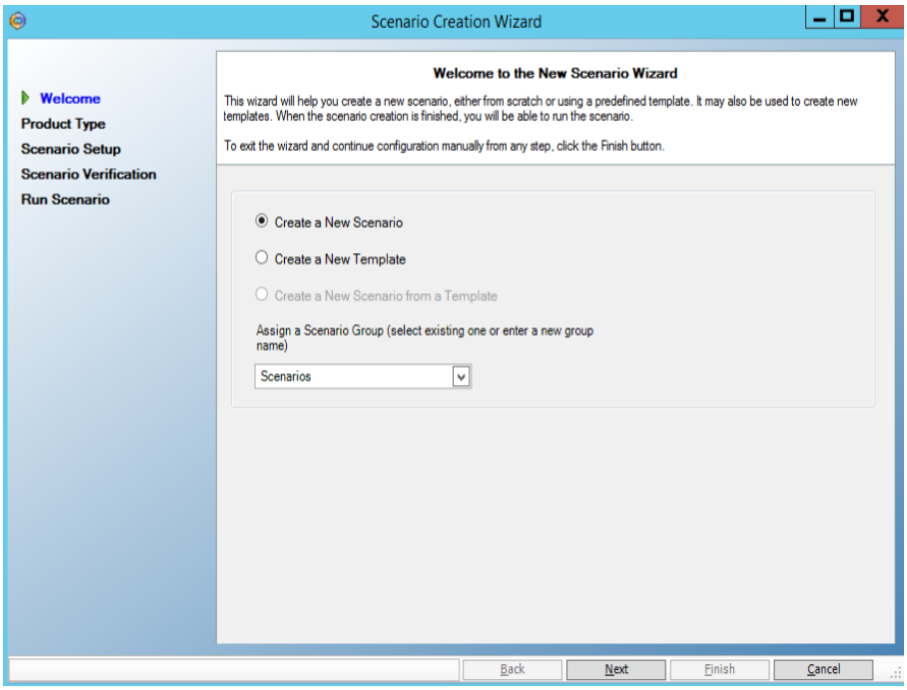
Migrating FSHA to Microsoft Azure

This section provides instructions on how to migrate FSHA to Azure. Before you begin, make sure to register and create an account in Azure.

To migrate FSHA to Microsoft Azure, follow these steps:

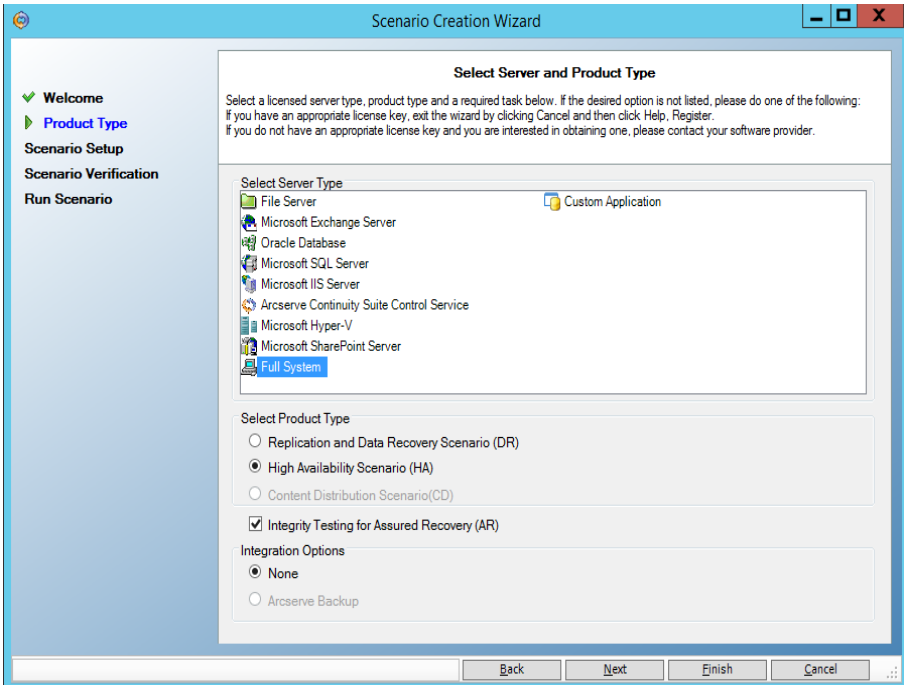
1. Open the Manager, select Scenario, **New** or click the **New Scenario** button to launch the wizard.

   The Welcome screen opens.



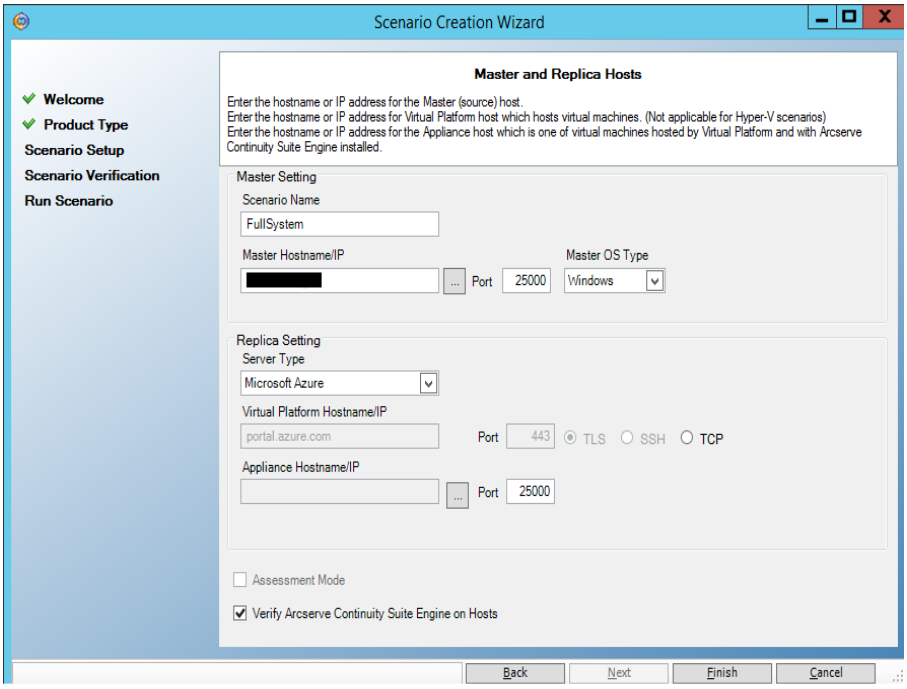
2. Select **Create a New Scenario**, select a Group from the list, and then click **Next**.

   The Select Server and Product Type screen opens.



3. Select Full System, High Availability Scenario (HA), and desired tasks on Replica, and then click **Next**.

   The Master and Replica Hosts screen opens.



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

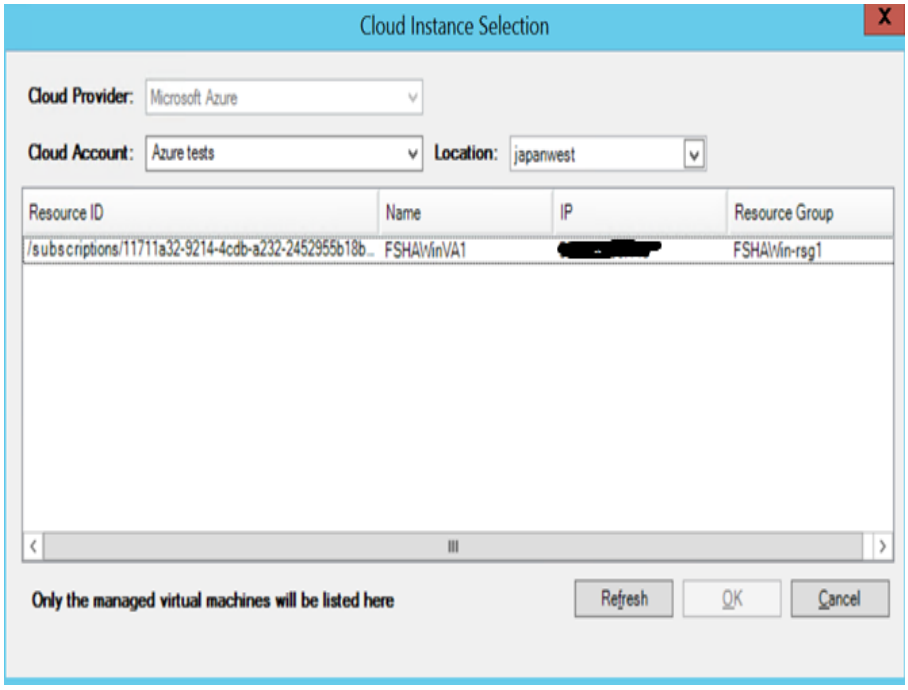
   - **Scenario Name:** Type a Scenario Name. The default value is the scenario type, for example, Full System.

- **Master Hostname/IP and Port:** Specify the physical machine you wish to protect or browse to select Master server.
- **Master OS Type:** Specify Windows or Linux as the Master OS Type.

  Note: For Windows, enter IP address or hostname of the Windows server to be migrated.
- **Server Type:** Specify Microsoft Azure as the Replica server.
- **Appliance Hostname/IP and Port:** Specify the virtual machine hostname or IP address of the VM to act as the Replica server in this scenario.

  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 the verification, clear the check box.

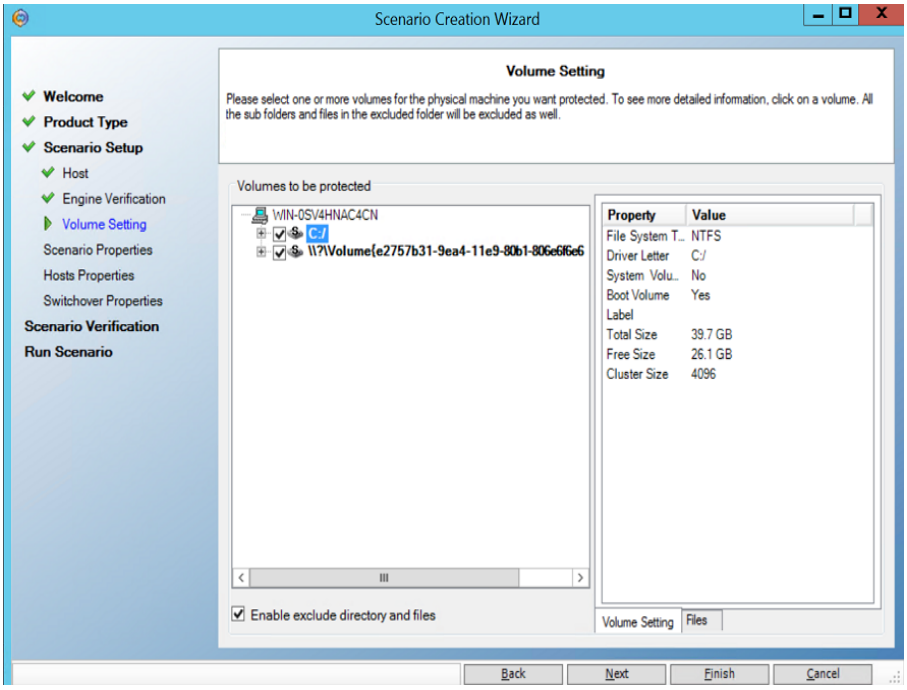
  The Cloud Instance Selection dialog opens.



- Select the Azure account, cloud replica, and location, and then click **OK**.

5. Wait for Engine Verification to complete and click **Next**. If required, click **Install** to upgrade the Engine on one or both servers and Verify Again.

   The Volume Setting screen opens.



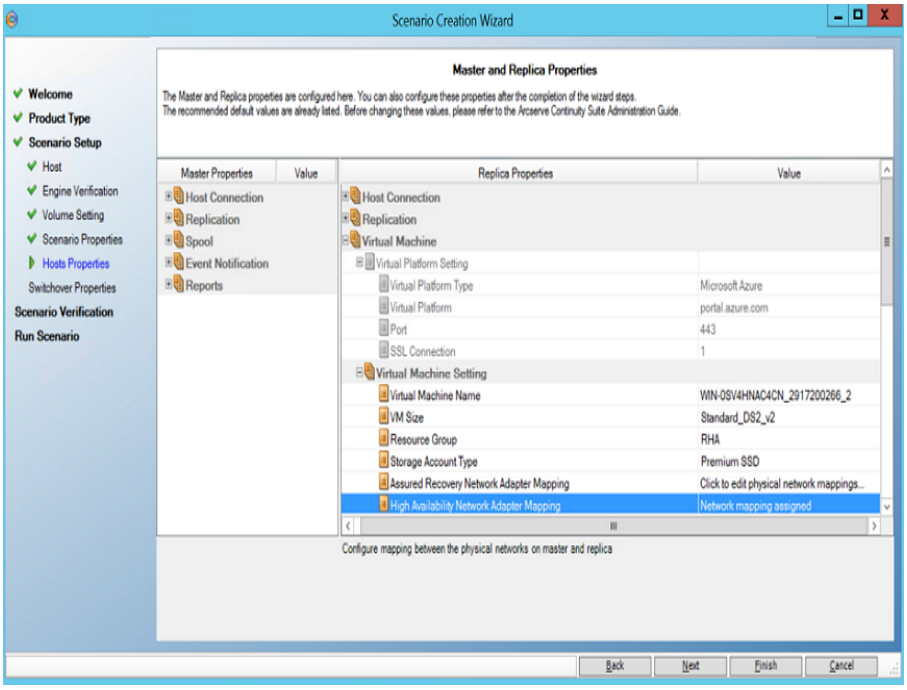
6. Select one or more volumes for the physical machine you want to protect and click **Next**.

   The Scenario Properties screen opens.

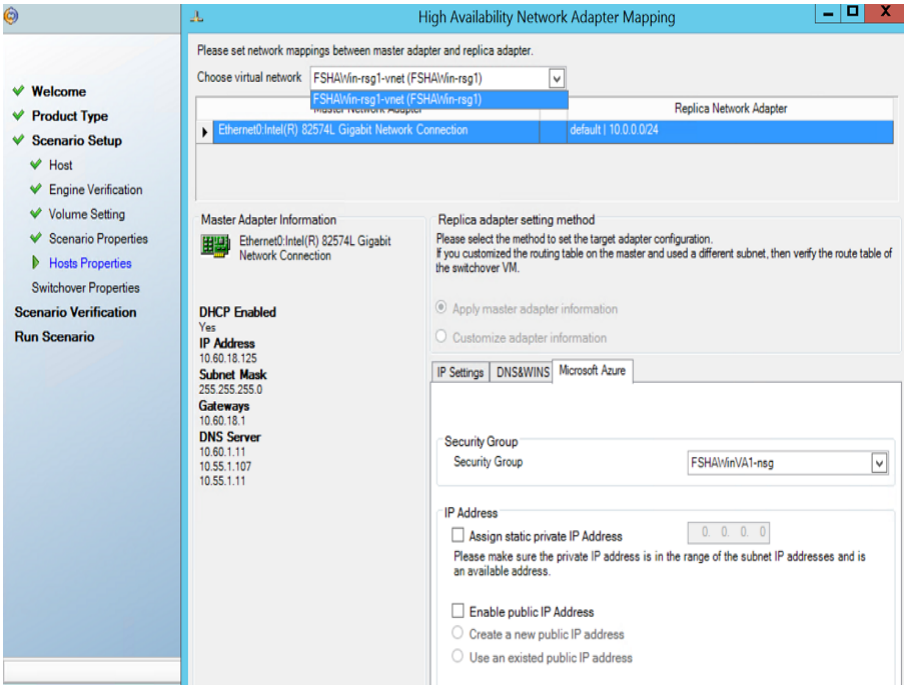
7. Accept the default values or set new values as required and click **Next**.

   Note: Scenario properties control the entire scenario. These properties can also be configured outside of the Wizard. For more information, see Configure Scenario Properties.

   The Master and Replica Properties screen opens.



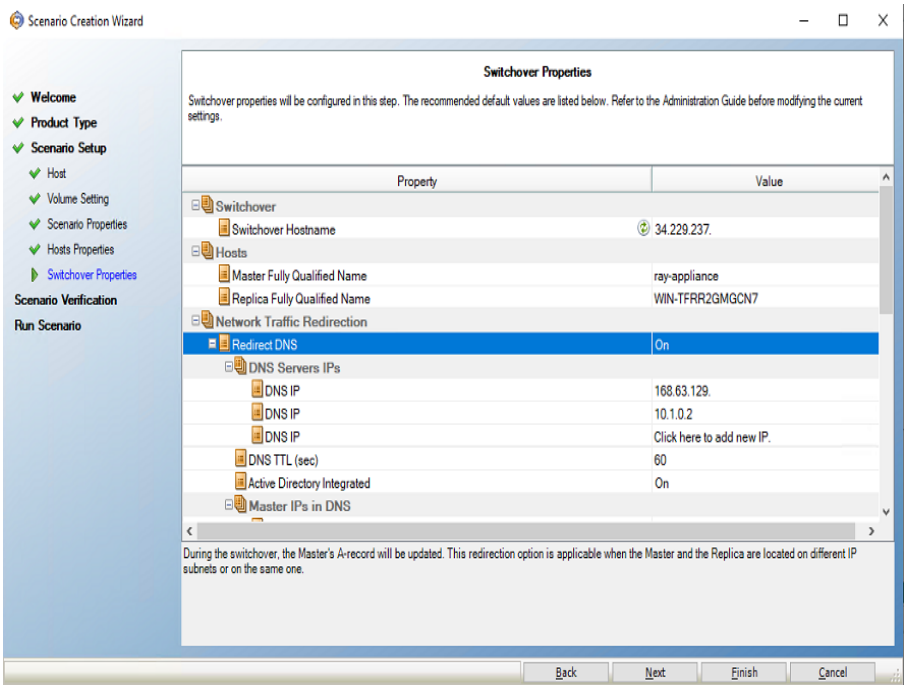
8. In the network mapping dialog launched automatically from Master and Replica properties screen, set the mapping between the Master's NICs and subnets on Microsoft Azure, security groups, and IP addresses and then click **OK** to save and close the network mapping dialog.



Master and Replica properties apply only to host servers.

9. Accept the default values or modify values and click **Next**.

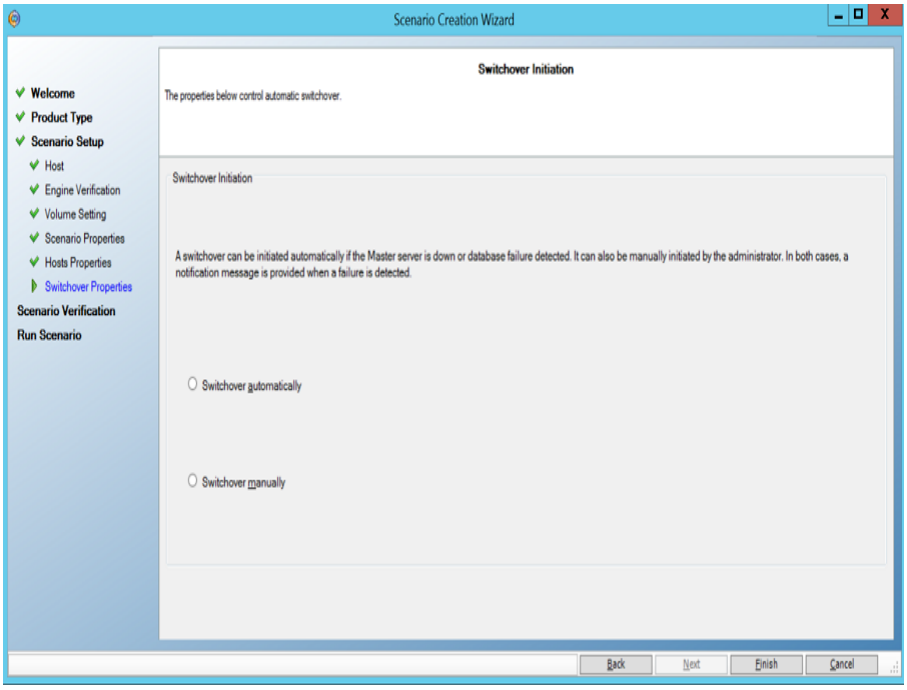
   The Switchover Properties screen opens.



10. Expand the *Switchover* property and enter the Switchover Hostname.
11. Expand the *Hosts* property and enter the Master Fully Qualified Name and Replica Fully Qualified Name.
12. Expand the *Network Traffic Redirection* property and specify redirection options, including Redirect DNS, DNS Servers IPs, and Master IPs in DNS.

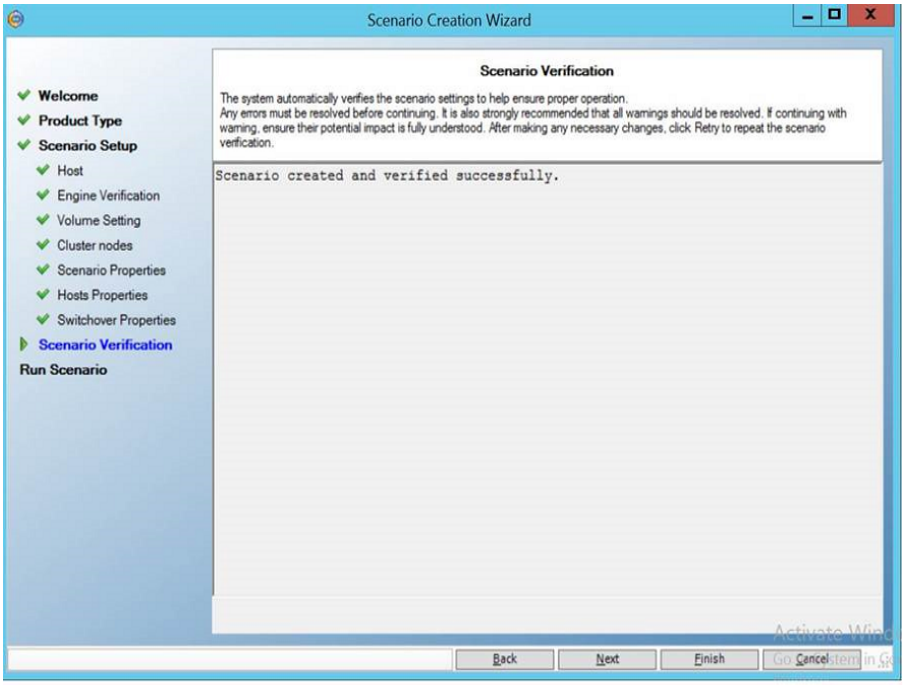
    Note: When you set the Redirect DNS option to *Off*, you can also specify a value for the Virtual Machine IPs on Replica server in DNS option. If the Redirect DNS property value is *On*, then the Virtual Machine IPs on Replica server in DNS option will not display in the list.
13. Set the switchover properties and click **Next**.

    The Switchover Initiation screen opens.



14. Specify if switchover must be started automatically or manually, and then click **Next**.

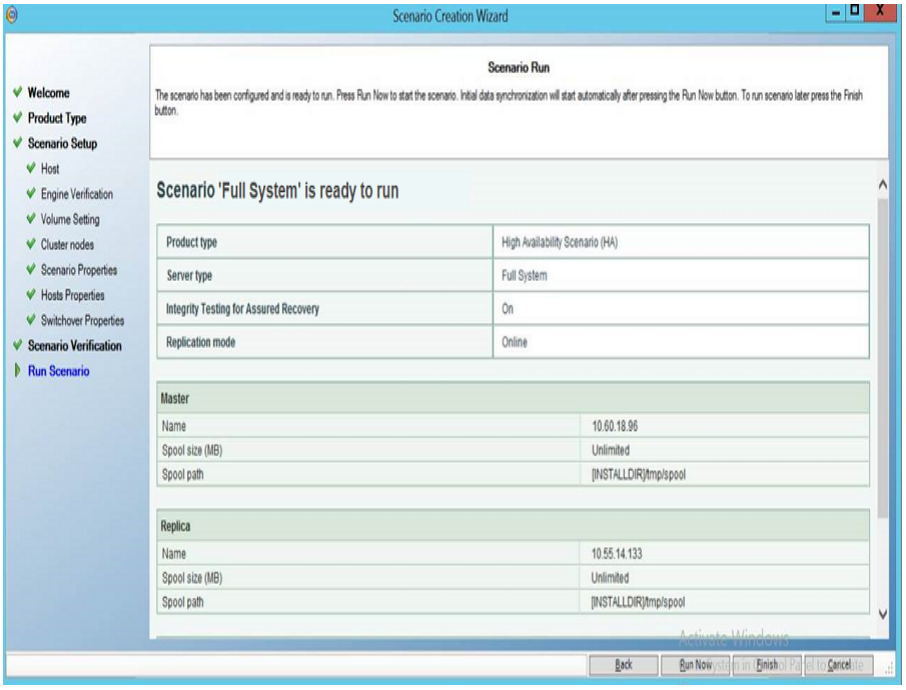
    The Scenario Verification screen opens.



    The scenario verification runs automatically, and the configurations are now complete.

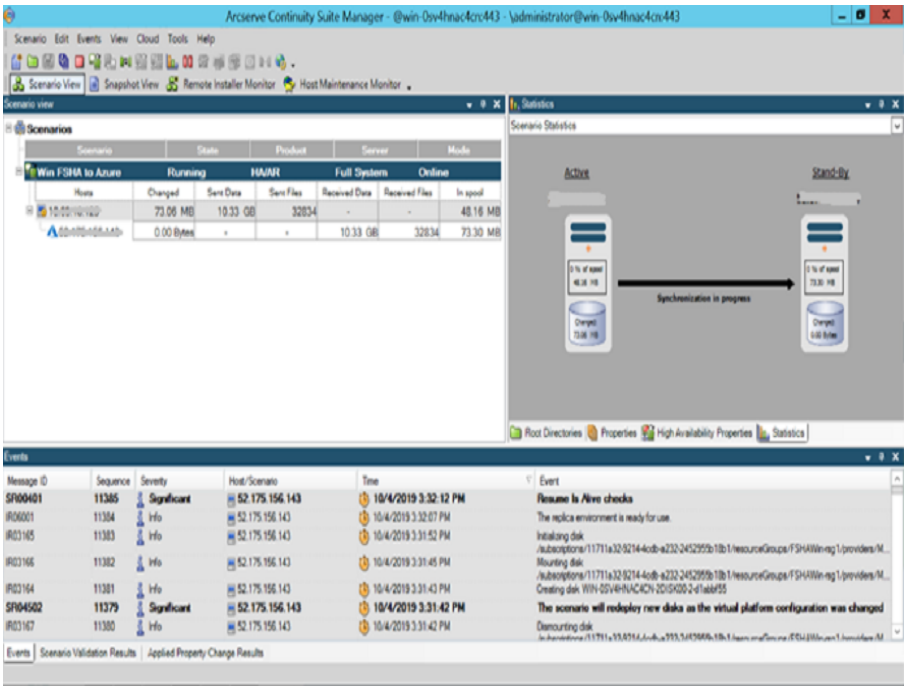
15. Click **Next**.

    The Scenario Run dialog opens.



16. Click **Run Now** if you wish to start synchronization immediately and activate the scenario. Click **Finish** to save and run the scenario later.

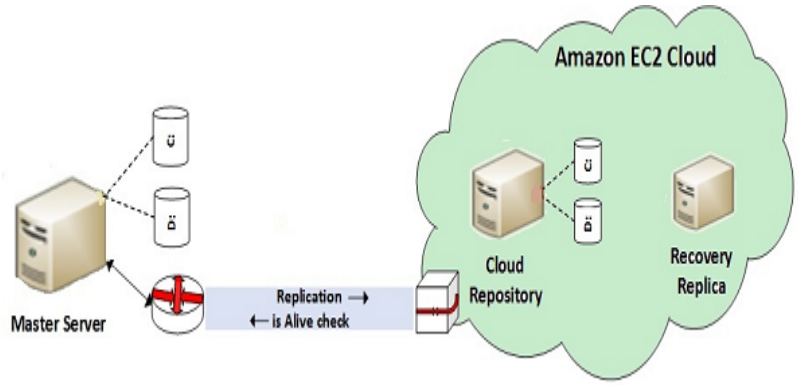
    Note: If you click Run Now, when the software is readying your cutover, the message *Synchronization in progress* appears.



When the Azure instance is successfully created, the switchover completes. The Azure instance is now ready for use.

Migrating FSHA to Amazon EC2

This section provides instructions on how to migrate FSHA to Amazon EC2.



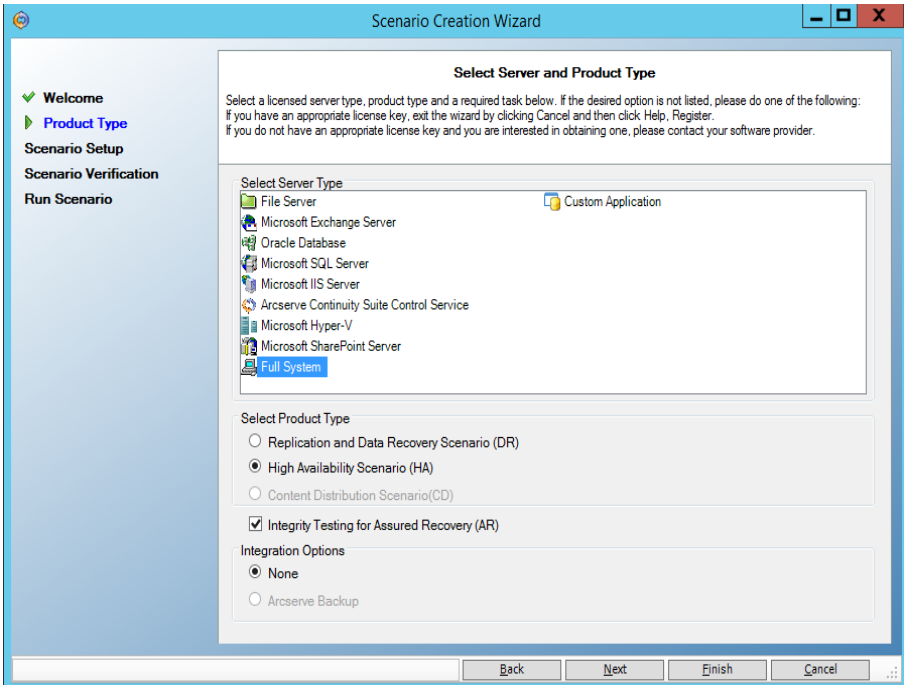
To migrate FSHA to Amazon EC2, follow these steps:

1. Open the Manager, select Scenario, **New** or click the **New Scenario** button to launch the wizard.

   The Welcome screen opens.

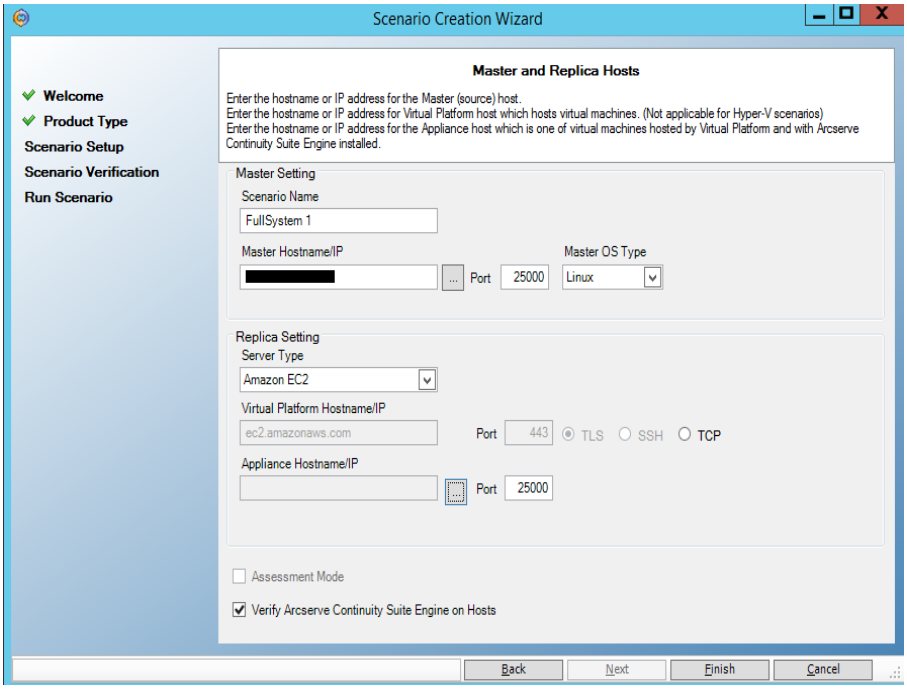
2. Select **Create a New Scenario**, select a Group from the list, and then click **Next**.

   The Select Server and Product Type screen opens.



3. Select Full System, High Availability Scenario (HA), and desired tasks on Replica, and then click **Next**.

The Master and Replica Hosts screen opens.

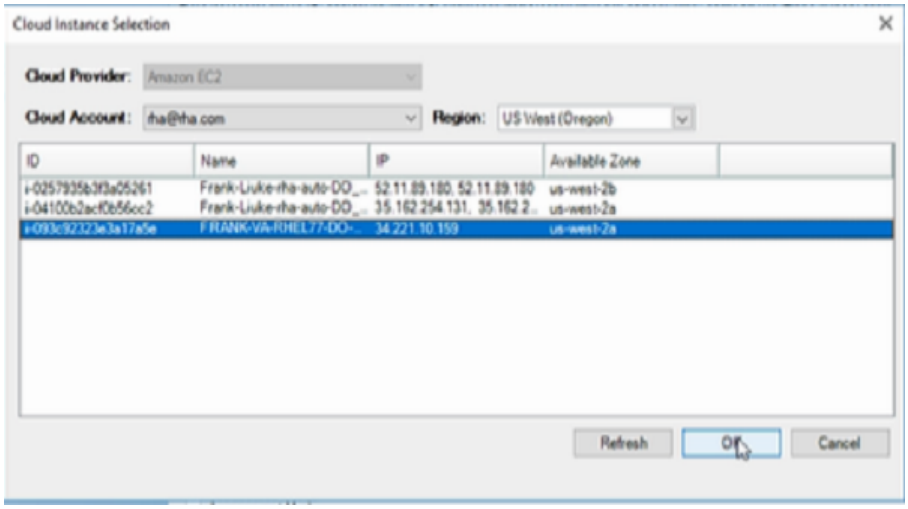


4. On the **Master and Replica Hosts** screen, do the following, and then click **Next**:

   - **Scenario Name:** Type a Scenario Name. The default value is the scenario type, for example, Full System.
   - **Master Hostname/IP and Port:** Specify the physical machine you wish to protect or browse to select the Master server.
   - **Master OS Type:** Specify Linux as the Master OS Type.
   - **Server Type:** Specify Amazon EC2 as the Replica server.
   - **Appliance Hostname/IP and Port:** Specify the virtual machine hostname or IP address of the VM to act as the Replica server in this scenario.

     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 the verification, clear the check box.

     The Cloud Instance Selection dialog opens.



- Select the AWS account, cloud replica (appliance), and region and then click **OK**.

5. Wait for Engine Verification to complete and click **Next**. If required, click Install to upgrade the Engine on one or both servers and Verify Again.

   The Volume Setting screen opens.

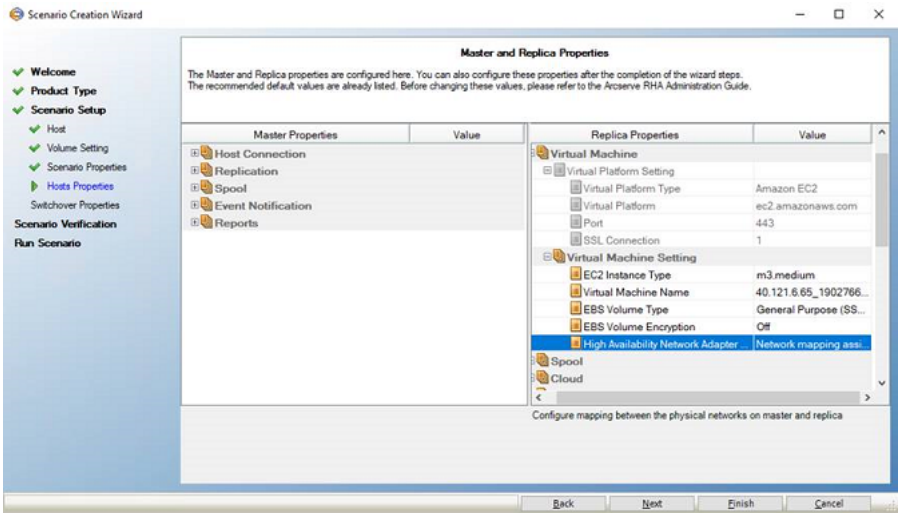
6. Select one or more volumes for the physical machine you want to protect, and then click **Next**.

   The Scenario Properties screen opens.

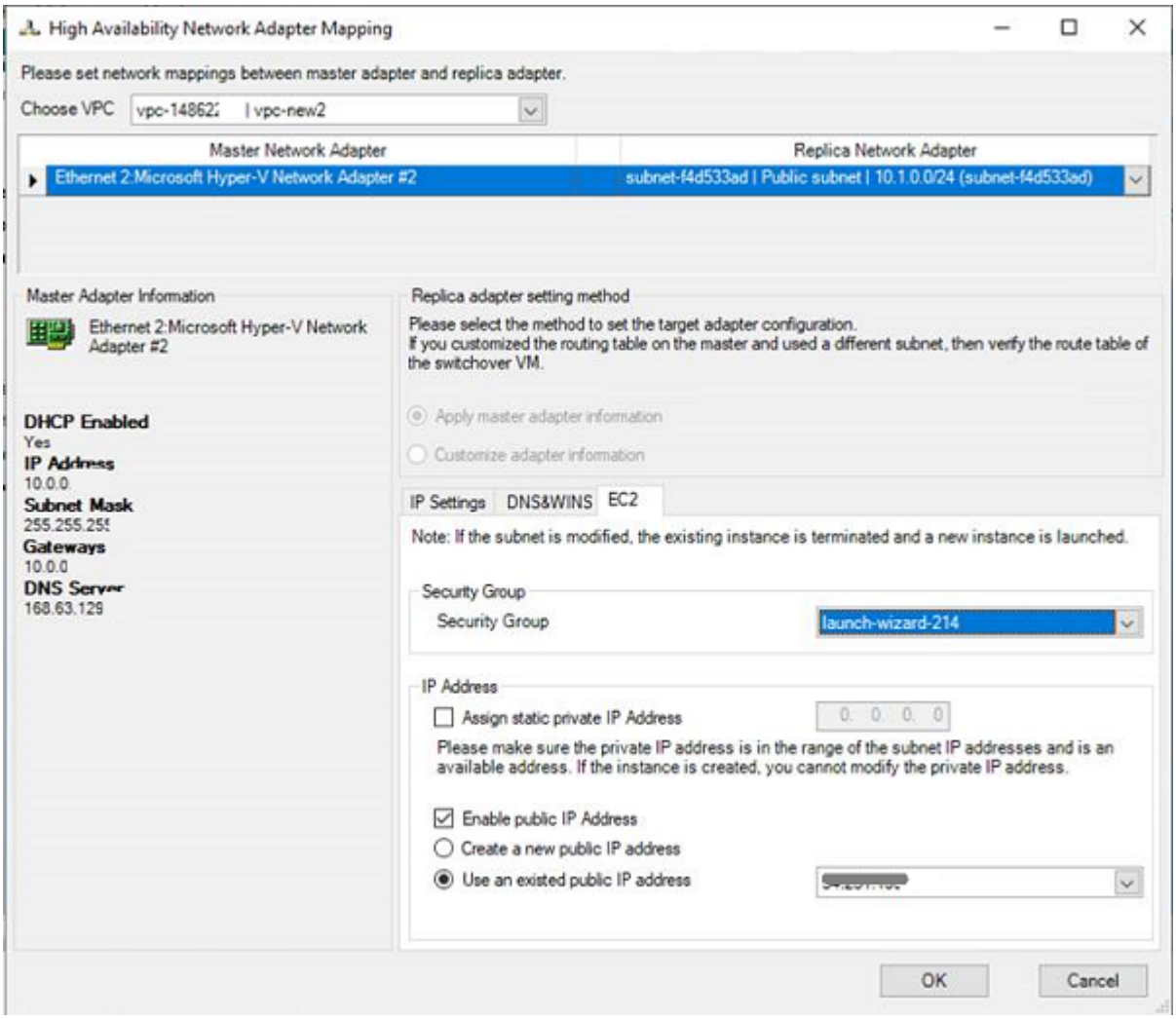
7. Accept the default values or set new values as required and click **Next**.

   Note: Scenario properties control the entire scenario. These properties can also be configured outside of the Wizard.

   The Master and Replica Properties screen opens.



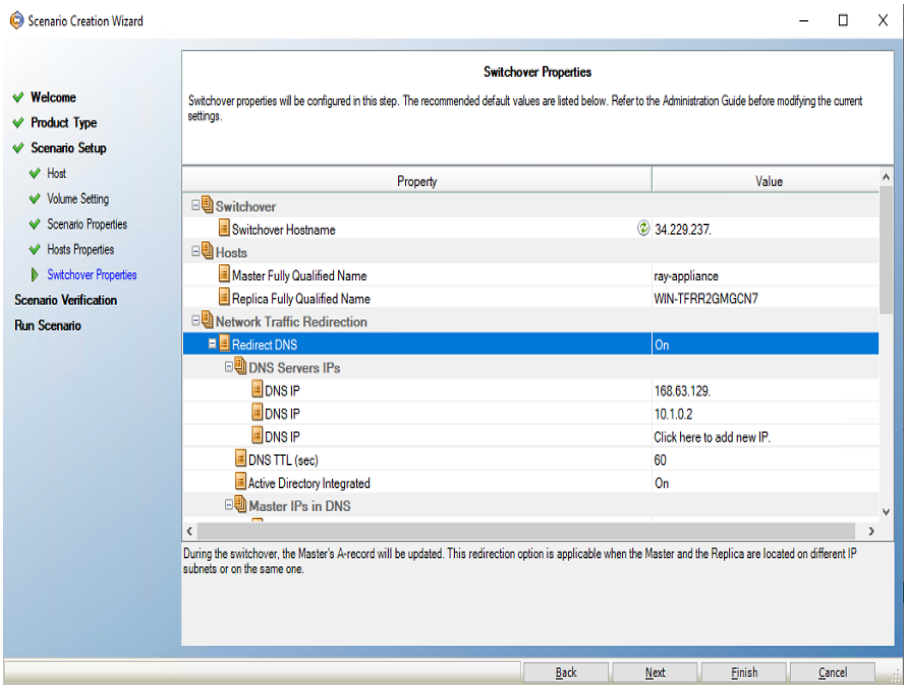
8. In the network mapping dialog launched automatically from Master and Replica properties screen, set the mapping between the Master's NICs and subnets on AWS, security groups, and IP addresses and then click **OK** to save and close the network mapping dialog.



Master and Replica properties apply only to host servers.

9. Accept the default values or modify values, and then click **Next**.

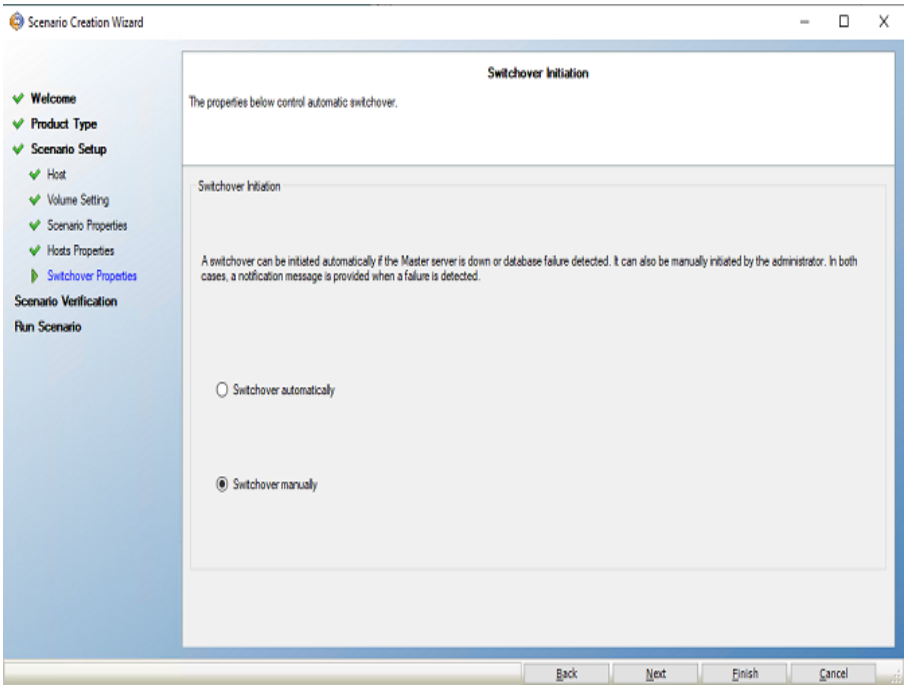
   The Switchover Properties screen opens.



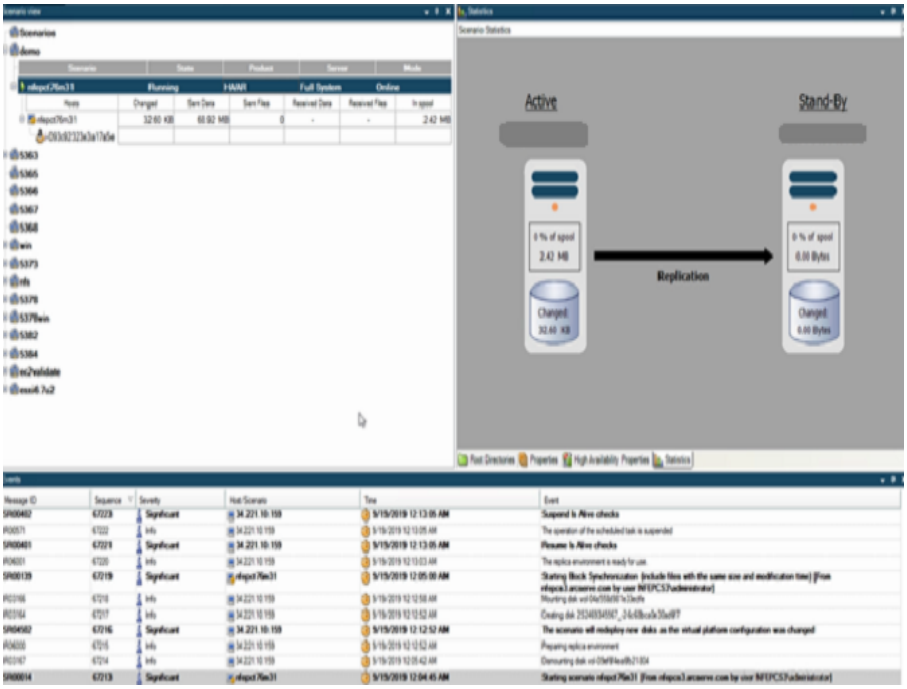
10. Expand the *Switchover* property and enter the Switchover Hostname.
11. Expand the *Hosts* property and enter the Master Fully Qualified Name and Replica Fully Qualified Name.
12. Expand the *Network Traffic Redirection* property and specify redirection options, including Redirect DNS, DNS Servers IPs, and Master IPs in DNS.

    Note: When you set the Redirect DNS option to *Off*, you can also specify a value for the Virtual Machine IPs on Replica server in DNS option. If the Redirect DNS property value is *On*, then the Virtual Machine IPs on Replica server in DNS option will not display in the list.
13. Set the switchover properties and click **Next**.

    The Switchover Initiation screen opens.

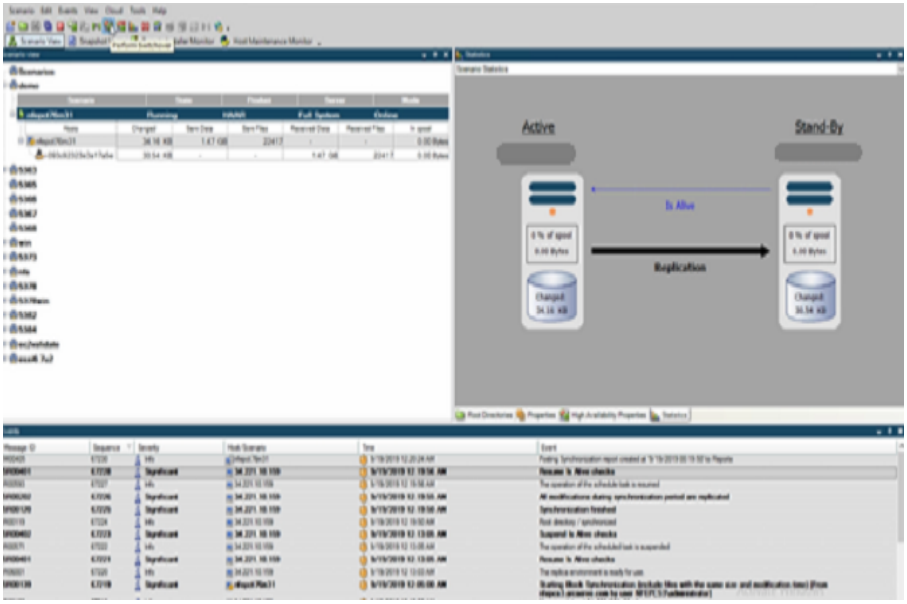


14. Specify if switchover must be started automatically or manually, and then click **Next**.
15. Scenario verification runs automatically, and configurations are now complete.
16. Configure NAT. For more information, see Configuring the Continuous Availability NAT Utility for Various Network Setups.
17. Create a New EC2 Data Replication Scenario. For more information, see Create a New EC2 Data Replication Scenario.
18. Run the scenario and monitor events in the management center.

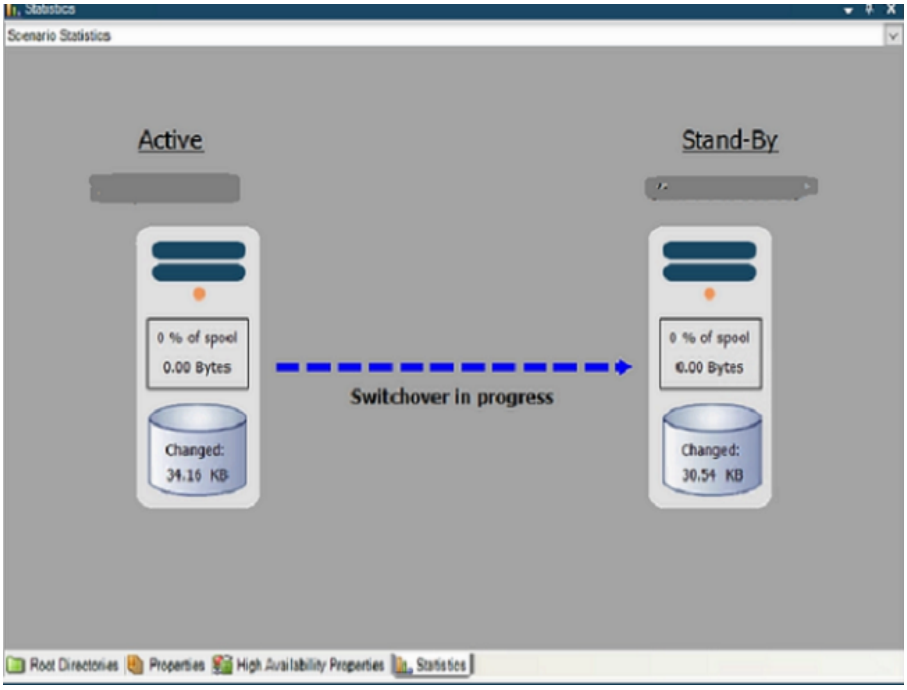


19. After replication of the data, check if the switchover is complete. On successful switchover, the following message is displayed:

    The replica environment is ready for use.



20. When the software is readying your cutover, it displays the "Starting switchover procedure..." message.



When the EC2 instance is successfully created, the switchover completes. The EC2 instance is now ready for use.

Run Scenario and Wait for Full Sync

When you start a Full System scenario, Arcserve Replication and High Availability first validates the scenario configuration with a verification check. During synchronization, the data in protected volumes on the Master is replicated to a virtual disk file on the Replica. During replication, the software replicates all file system changes that occur on the Master to the Replica and applies those changes to the data on the virtual disk.

Consider the following when running a Full System scenario:

- For Linux Full System scenario, Volume and Offline synchronization methods are not supported.
- Selecting Windows as Choosing synchronization method:
  - For initial synchronization, the Volume synchronization is recommended because it usually gives better synchronization performance over LAN or WAN.
  - For subsequent synchronizations, the File or Block level synchronization is recommended since they offer a significant load reduction. File or Block synchronization compares data on the Master and Replica and sends only the difference, while the Volume synchronization sends all data from the Master to the Replica. For resynchronization, Block synchronization is used by default.
- Selecting Linux as Choosing synchronization method:
  - For initial synchronization, the File synchronization is recommended because it takes less time to complete data comparison and start sending data. Make sure to select the check box of **Ignore same size/time files**.
  - For subsequent synchronizations, make sure to clear the check box of **Ignore same size/time files** to ensure data integrity.
- If data transfer happens across WAN, use Multiple Streams to improve synchronization/replication performance. Select scenario -> Replication -> Optional Settings -> Number of Streams, test 5 or 10 which works better for your network environment.

Perform Assured Recovery Testing

This section describes about Assured Recovery testing, and how to do the following:

- How to create AR scenario
- How to perform AR test in a scheduled and non-scheduled mode
- How to configure the AR properties
- How to set up VSS snapshot creation
- How to manage snapshots

About Assured Recovery

The Assured Recovery option enables you to perform a full transparent test of the recoverability of your data on the Replica server. The Replica server is the one that takes over the production server if it gets down. The Assured Recovery option is a true test of the actual server, applications and actions that are required when the Replica server needs to switch, become the Active server, and carry out its functions.

This Assured Recovery test is executed by starting up database services and performing the operations required to verify the integrity of the data. All this is done without performing the resynchronization, and without impacting the availability of the production server, or the safety that the Replication and HA systems are designed to provide.

During the test, the data changes that continue to take place on the Master are sent to the Replica, but they are not immediately applied. Instead, these changes are accumulated and stored in a spool, and only when the testing is completed, they are applied to the Replica data. Since the spooling occurs on the Replica, if something happens to the Master during the testing process, none of the accumulated changes are lost.

Once the testing is finished, the Assured Recovery option stops the application services it started on the Replica. Then, the Replica server automatically rewinds back to the state that existed when the replication was paused and the test has started. This way, the accumulated changes in the spool can be applied as if no testing has occurred. From this point on, the Replication or HA scenario continues normally. In case of an HA scenario, if the Master server fails during the testing, the switchover begins.

The Assured Recovery test can be fully automated and performed on a scheduled basis as often as needed. Upon completion, appropriate personnel can be alerted with the status of the test, and additional actions can be triggered on success, for example, taking a VSS snapshot of the Replica data or creating a backup. You can also perform AR testing in a non-scheduled mode.

The Assured Recovery testing is tailored to all supported application and database servers. However, since the Assured Recovery option tests database services, it is less applicable for File and IIS Servers. You can still use the Assured Recovery option with these servers for special tasks. For example, you can automatically suspend replication on a regular basis during several hours each day, week or month, and run scripts in this interval, or you can use this suspension to take VSS snapshots on the Replica. Since there is no *application* per se, testing of the data with File and IIS Servers scenarios requires additional custom scripts.

The Assured Recovery option supports both Replication and HA scenarios, except for Control Service scenarios. However, it is best suited for HA scenarios since in this case, the Replica server contains the actual database servers, on which the test is performed, and not only data.

Note: The Assured Recovery option is not available for Control Service scenarios.

If you are using AR test as a part of Replication scenario, you must verify that the root directories path is the same on the Master and the Replica. In addition, the Replica must have database application installed, or share files if you test a File Server, and they need to be configured on the Master and the Replica in the same way. Otherwise, the AR test does not produce meaningful results.

Creating Assured Recovery Testing Scenarios

The Assured Recovery testing feature must be enabled during the creation of the scenario. For this reason, you cannot perform testing within a Replication or HA scenario that is already running, and was not configured to use the Assured Recovery option. To use Assured Recovery, it is necessary to create a new scenario with the **Integrity Testing for Assured Recovery** option turned to On.

Note: This section demonstrates the creation of an Assured Recovery testing scenario for Exchange Server HA. The procedure is similar for all application types.

To set Assured Recovery testing scenario, follow these steps:

1. Open the Manager, select from the Scenario menu the **New** option, or click the **New** button on the Standard toolbar.

   The Scenario Creation Wizard opens.

2. Select the required scenario options as follows:

   - Select **Create a New Scenario** option.
   - Select from the Group drop-down list, the group to which you want to assign the new scenario, or enter a name for a new scenario group.

3. Click **Next**.

   The Select Server and Product Type screen opens.

4. A list of available applications and scenario types is presented.

   Note: The list of available applications depends on the licenses applied.

   Select the required scenario options, as follows:

   - Select Server Type - select the type of server for which you want to create the AR scenario.
   - Select Product Type - select either Replication and Disaster Recovery or High Availability Scenario.

     Note: The Assured Recovery test is best suited for HA scenarios. If you select the Replication option, you must verify that the root directories path is the same on the Master and the Replica. In addition, the Replica must have database application installed, or share files if you test a File Server. Otherwise, the AR test does NOT give meaningful results.

   - Select the **Integrity Testing for Assured Recovery** option.

5. Click **Next**.

   The Master and Replica Hosts screen opens.

6. Enter the following information:

   - In the Scenario Name box - accept the default name or enter a new name for the scenario.
   - In the Master and Replica Hostname/IP boxes - enter the hostname or IP address of the Master (active) and Replica (standby) servers, or use the Browse buttons to find the Master and Replica Servers.

   Important! Only one Replica can be configured for AR testing in a single scenario. If you add more than one Replica to the scenario and try to configure it for the AR test, the following message appears: **Only one scheduled task per scenario can be set. Replica integrity testing for Assured Recovery for host [Replica_name] is already switched on. Do you want to turn this option off now?** To switch the test to the second Replica, click **Yes**.

   Note: If either server is a MSCS cluster, enter the Virtual Server Name or IP address as the Master and/or Replica name (instead of name/IP of the physical node).

   - In the Port boxes: accept the default port no. (25000) or enter a new port number for the Master and Replica.
   - The Verify Engine on Hosts option - select this check box if you want the system to verify whether Engines are installed and running on the Master and Replica hosts you specified in this screen. If Engines are not installed on the selected hosts, use this option to remotely install the Engines on one or both hosts.

7. After you have entered or selected the desired options, click **Next**.

   The Databases for Replication screen opens.

   The auto-discovery component automatically displays the Exchange databases that are on the Master server. These are the databases that can be replicated and protected.

8. By default, all the discovered databases are selected and get replicated. Clear the check boxes to exclude any of these storage groups from the replication, and then click **Next**.

   The Replica Configuration screen opens.

9. The auto-configuration component verifies that the Exchange Server configuration on the Master and Replica servers is identical during the replication procedure. This means that if there are discrepancies, the Arcserve Replication and High Availability performs the required actions, such as, deletes the storage groups, public folders or mailbox stores from the Replica,

creates new ones and makes modifications to the existing ones. The actions that are performed during the configuration process are indicated in the Action column on the right.

10. Review the changes that occur during the automatic configuration on the Replica server, and make sure that you want them to be performed.

    Note: If a Remove action is indicated, make sure that you are ready to delete the specified storage item from the Replica server, since it does not have an automatic backup. If you want to save it in a different location before you delete, click the Finish button to exit the wizard.

    Important! You cannot use UNC paths as root directories on the Replica host for Assured Recovery scenario.

11. Click **Next** to start the Replica configuration process.

    The Scenario Properties screen opens.

    The **Scenario Properties** screen enables you to configure the scenario properties that affect the entire scenario. Typically, the default values are sufficient.

    If you want to configure the scenario properties at this stage, see Understanding Scenario Properties. To configure the scenario properties at a later stage, see Configuring Scenario Properties.

12. Click **Next**.

    The Master and Replica Properties screen opens.

    The Master and Replica Properties screen enables you to configure the properties that are related to the Master or the Replica host. Typically, the default values are sufficient.

13. To verify that the Assured Recovery option is active, under the Replica Properties list on the right, open the Scheduled Tasks group and ensure that the Replica Integrity Testing for Assured Recovery property is set to On. You can leave the default values of the other related properties and change them later if needed. For more information about AR properties, see Specify Assured Recovery Properties.

    If you want to configure the Master and Replica properties at this stage, see Setting Master and Replica Properties. To configure the Master and Replica properties at a later stage, see Configuring Master or Replica Server Properties.

Note: You can modify all the settings in this pane after the scenario is created. However, before changing any Spool properties (which can be configured here), review the Spool information for configuration details.

14. Click **Next**. If you have selected HA, the Switchover Properties screen opens.
15. From this stage, set up the scenario as you would normally following the instructions in the usual manner. For more information, see the appropriate Operation Guide. After the scenario creation is completed, run the scenario.

    Once the initial synchronization is completed and the replication process is active, the AR test can be performed.

Configure Assured Recovery Properties

To configure Assured Recovery properties, the scenario must be stopped.

Note: The Properties pane and its tabs (Root Directories, Properties, Statistics) are context sensitive, and change whenever you select a different node from a scenario folder.

To set Assured Recovery scenario properties, follow these steps:

1. On the Scenario pane, select the Replica that you want to test and whose properties you want to configure.
2. On the Framework pane, select the **Properties** tab.

   The Replica Properties list opens.

   Note: A running scenario has a gray background, and scenarios that are not running have a white background.
3. If the scenario is running, click the **Stop** button on the toolbar. The scenario stops.
4. On the Replica Properties list, open the Scheduled Tasks group to display the Replica Integrity testing for Assured Recovery properties.
5. From the list, select the required property, and select or enter the appropriate values. Some values can be selected from a combo box while other values can be manually entered in an edit box field.
6. Click the **Save** button on the Standard toolbar to save and apply your changes.

Specify Assured Recovery Properties

This section lists the Assured Recovery properties, corresponding values, and provides an explanation of each property.

Note: On Windows x64 systems, you cannot run scripts that activate applications with a graphical user interface.

Scheduler

The Scheduler enables you to automatically run Assured Recovery tests according to a pre-defined schedule, for example, every few hours, once in a day, or several times a month. To set the scheduler, see Performing Assured Recovery Test in a Scheduled Mode.

Start DB

This property defines the first step in the AR test: starting the database services on the Replica.

Automatic

By default, this property is set to On. To use script to replace the automatic initiation of database services, set this option to Off.

User-Defined Script

You can specify a script to augment or replace the standard step to start the database services.

To replace the standard step, set **Automatic** to Off and set **User-Defined Script** to On. Then, specify the full path name of the script to be executed in the **Script Name** box.

To execute the script following the standard step, leave **Automatic** set to On.

Script Name (full path)

Enter the name and full path of the script that is invoked following the starting of database services or instead of it.

Arguments

Additional arguments to be passed to the script are specified in the previous property. Arguments entered here are static values.

DB Testing of Replica

This property defines the second step in the Assured Recovery test: verifying that all application services have started properly and that all databases or information stores have mounted successfully and are in a valid state.

Automatic

By default, this property is set to On. To use script to replace the automatic actions performed during this database validation stage, set this option to Off.

User-Defined Script

You can specify a script to augment or replace the actions performed during this database validation stage.

To replace the standard step, set **Automatic** to Off and set **User-Defined Script** to On. Then, specify the full path name of the script to be executed in the Script Name box.

To execute the script following the standard step, leave Automatic set to On.

Script Name (full path) -- Enter the name and full path of the script that is invoked following the database validation step or instead of it.

Arguments -- Additional arguments to be passed to the script are specified in the previous property. Arguments entered here are static values.

Actions upon Successful Test (DB Online)

After the Replica is successfully tested, the application data is in a known, valid state. You may want to make use of this fact, for example, to ensure that a backup is performed at this point on validated data. If the action you want to perform requires that the application is running and the databases or information stores are mounted, then the action must be registered through a script. To register the actions, specify the script details in the User-Defined Script boxes. This section has no default actions.

User-Defined Script

Script Name (full path) -- Enter the name and full path of the script that is invoked when the application is still running, and the databases or information stores are mounted.

Arguments -- Additional arguments to be passed to the script are specified in the previous property. Arguments entered here are static values.

Stop DB

This property defines the third and final step in a standard AR test: stopping the database services once the testing is complete.

Automatic

By default, this property is set to On. To use a script to replace the automatic stopping of database services, set this option to Off.

User-Defined Script

To stop the database services, specify a script to augment or replace the standard step.

To replace the standard step, set **Automatic** to Off and set **User-Defined Script** to On. Then, specify the full path name of the script to be executed in the **Script Name** box.

To execute the script following the standard step, leave **Automatic** set to On.

Script Name (full path) -- Enter the name and full path of the script that is invoked following the stopping of database services or instead of it.

Arguments -- Additional arguments to be passed to the script are specified in the previous property. Arguments entered here are static values.

Actions upon Successful Test (DB Off-line)

As noted in Actions upon Successful Test (DB Online), the application is in a known valid state at this stage. You may want to copy it or perform a backup or take a snapshot at this time. If the action does not require the application to be running, register this through a script here, by specifying the full path name of a script in the User-Defined Script field.

Note: On Windows Server 2008 and later systems, you can generate VSS snapshots automatically. For more information, see Create VSS Snapshots Automatically.

User-Defined Script

Script Name (full path) -- Enter the name and full path of the script that is invoked after the Assured Recovery test is successfully completed.

Arguments -- Additional arguments to be passed to the script are specified in the Script Name property. Arguments entered here are static values.

Assured Recovery Testing Limitations

When performing Assured Recovery Testing with Oracle or SQL Server databases, the software does not verify whether the database is mounted. It verifies only that the service is running. Create a custom script to verify that both the services are running and the databases are mounted. Enable the appropriate user-defined script property. For more information, see Understanding Assured Recovery Properties.

Perform an Assured Recovery Test

The Assured Recovery test can be fully automated and performed on a scheduled basis as often as needed. Upon completion, appropriate personnel can be alerted with the status of the test, and additional actions can be triggered on success, for example, taking a VSS snapshot of the data or running a backup. Alternatively, you can perform AR testing in a non-scheduled mode, by automatically or manually initiating the test whenever required.

In both modes, the AR test is performed in steps, according to the AR configuration settings. Some of the steps are transparent and are executed automatically whenever an AR test is performed. Other steps are visible and can be configured as to whether and how they get performed.

The standard steps are as follows:

1. Initiate Assured Recovery test - to initiate the AR test in a scheduled or non-scheduled mode, click **Replica Integrity Testing** on the toolbar.
2. Suspend application of data changes on the tested Replica - this step is performed automatically at the beginning of each AR test.
3. Initiate a rewind component on the tested Replica - this step is performed automatically. It is required to capture all the changes that are made to the Replica data during the test, so that they can be later rewind back to the point when the replication was suspended.
4. Start the database services - by default, this step is performed automatically. However, it can be switched off, replaced, or followed by a user-defined script.
5. Test the database - by default, the databases are verified using the same tests that are used to monitor the database in HA. These tests include verifying that all the services have correctly started and that all the databases have been successfully mounted. These tests can be switched off, replaced, or followed by a user-defined script.
6. Perform actions upon successful test while the database services are running - a user-defined script may be registered at this point to perform actions that are desired on a successful test, which also requires that the application must be running.
7. Stop the database services - by default, this step is performed automatically. However, it can be switched off, replaced, or followed by a user-defined script.
8. Perform additional actions upon successful test while the database services are stopped - this step is optional, and may be used to perform actions that take advant-

age of the fact that the application passed validation tests and that it was stopped in a systematic order.

9. Rewind AR Replica data and resuming replication - this step is performed automatically at the end of each AR test, that restores the Replica data to the state it was before the test begun using the rewind technology and then resumes the replication.

Performing Assured Recovery Test in a Scheduled Mode

When you set the AR test to run in a scheduled mode, it means that an AR test is performed automatically on a regular basis. After you select this option, the following flexible scheduling capabilities are offered:

- Testing on selected days of the week and for specific hours in a 24-hour cycle.
- Testing over selected periods (e.g., once every 36 hours) in a 7-day cycle.
- Exclusion of specific dates.

The AR test schedule can be set when the scenario is created or at a later stage.

Note: You can define only one scheduled task per scenario. If you attempt to configure AR testing when you already have a scheduled Suspend operation configured, the following message appears:

Only one scheduled task per scenario can be set. Suspend for host [Replica_name] is already switched on. Do you want to turn this option off now?

To switch the schedule option to the AR test, click **Yes**.

To schedule the AR test, follow these steps:

1. On the Scenario pane, select the Replica you want to test.
2. On the Framework pane on the left, select the properties tab.

   The Replica Properties list appears.

2. If the scenario is running, click the **Stop** button on the Standard toolbar to stop the scenario.
3. On the Replica properties list, open the Scheduled Tasks group. Under the **Replica Integrity Testing for Assured Recovery** group, select the Scheduler property, and then click the Not Set value.

   The Assured Recovery hours dialog appears.

   The Assured Recovery hours dialog is like the Schedule Setting dialog, which is used for scheduling automatic synchronization.
4. Set the schedule for automatic AR testing in the Assured Recovery hours dialog, and then click **OK** to save your schedule and close the dialog.
5. To activate the scheduler, click the **Save** button on the Standard toolbar and start the AR scenario.

   The Replica you have selected for testing is tested on a regular basis according to the schedule you set.

Performing Assured Recovery Test in a Non-Scheduled Mode

In a non-scheduled mode, you can test Assured Recovery either automatically or manually. When you are using the automatic method, initiate the AR test by a click of a button. The Arcserve Replication and High Availability automatically performs all the test steps according to the AR configuration setting. After the test is complete, the regular replication is resumed. The only difference between scheduled mode and a non-scheduled mode is, in a non-scheduled automatic mode, you can initiate the test whenever you need, without using the Scheduler.

When you are using the manual method, you also need to initiate the AR test by a click of a button. However, unlike the automatic method, the Arcserve Replication and High Availability suspends the test after the first standard step - starting the database service. This occurs even when all the standard steps are configured as Automatic.

Note: If the Start DB property is set to Off, and there is no user-defined script that replaces it, the Arcserve Replication and High Availability suspends the application of changes to the Replica in preparation for the manual AR test.

After the replication is suspended, you can perform tests or actions directly on the Replica without resynchronizing the Master and Replica. You can use this option for manually testing applications or data on the Replica, or for performing tasks on the Replica instead of the Master, such as report generation, to reduce the Master workload.

When you finish the manual testing or operation, you need to manually stop the AR test suspension. This is done again by a click of a button. If other steps and actions were configured in the AR test, such as stopping the database services, they get performed after you click the button for stopping the test, and before the test gets declared as finished. When the test is considered finished, the replication resumes automatically.

Perform Assured Recovery Test Automatically

To perform Assured Recovery test automatically, follow these steps:

1. On the Manager, verify that the AR scenario is running.
2. To start the AR testing, on the Scenario pane select the Replica you want to test. Click the **Replica Integrity Testing** button on the Standard toolbar, or right-click Replica and select **Replica Integrity Testing** from the shortcut menu.

   The Replica Integrity Testing for Assured Recovery dialog opens, displaying the configuration you set for the AR test.
3. To start the automatic AR test using the existing configuration, click **OK**.

   Note: To change the test configuration before running the test, click **Cancel**. For more information, see Configure Assured Recovery Properties.
4. After you initiate the AR testing, the Replica Integrity Testing for Assured dialog gets closed. Before the test begins to run, Arcserve Live Migration verifies that no synchronization, AR test or replication suspension tasks are currently in progress on any of the hosts that participate in the current scenario.
5. After the verification completes, the AR test begins.

   The steps of the test are displayed as messages in the Event pane.
6. After the test is finished, the Replica is automatically restored to the same state it was when the replication was suspended, using the underlying rewind technology. Then, the changes that were accumulated in the spool gets applied, and the replication resumes and continues normally.
7. 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 Assured Recovery Test Manually

You can manually perform the AR testing without using the Scheduler.

To perform Assured Recovery test manually, follow these steps:

1. On the Manager, verify that the AR scenario is running.
2. To start the AR testing, on the Scenario pane select the Replica you want to test. Click the **Replica Integrity Testing** button on the Standard toolbar, or right-click the Replica and select **Replica Integrity Testing** from the pop-up menu.

   The **Replica Integrity Testing for Assured** dialog opens, displaying the configuration you set for the AR test.
3. To start the manual AR testing using the existing configuration, select the **Manual testing** check box. Once this check box is selected, the dialog changes to reflect only the actions that are performed in a manual mode.

   Notes:

   - To change the test configuration before running the test, click **Cancel**. For more information, see Configure Assured Recovery Properties.
   - If Manual Testing is NOT selected, the VM still gets started, and stops automatically after the testing is successful.
4. Click **OK** to close the dialog and start the manual testing.
5. From this stage, the only automatic action that Arcserve Live Migration performs, unless other actions are configured as Automatic, is suspension of updates on the Replica.
6. After the replication is suspended, the message *"Replica is ready for Manual Integrity Testing"* appears in the Event pane.

   Now, you can start performing any test you want directly on the Replica host, including making changes to the database.

   Note: The changes made cannot be saved once the AR test is finished, due to the rewind process.

   Important! Do not restart the tested Replica at this stage. If you do, all the changes that accumulated on the spool gets lost.
7. After you finish testing the Replica host, click again the **Replica Integrity Testing** button to resume replication.

Important! If you do not click the Replica Integrity Testing button a second time at the end of the test, the changes continue to spool up on the Replica host. Eventually, the spool on the Replica host overflows and the scenario is stopped.

A confirmation message opens.

8. Click **Yes** to stop the AR test. If other steps and actions were configured in the AR test, such as stopping the database services, they get performed before the test gets finished. When the test is finished, the replication resumes automatically.
9. After the test is finished, the Replica is automatically restored to the same state it was when the replication was suspended. Then, the changes that were accumulated in the spool gets applied, and the replication resumes and continues normally.
10. By default, after the AR test is performed, an Assured Recovery Report is generated.

Perform Cut off/Switchover

This section contains the following topics:

The Switchover Workflow

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.

During the creation of HA scenario, you define how you want the switchover to be initiated. If you have selected in the **Switchover and Reverse Replication Initiation** page, the **Initiate Switchover manually** option, you need to perform a manual switchover. However, if you have selected the **Initiate Switchover automatically** option, you can still perform a manual switchover, even if the Master is alive. You can initiate switchover when you want to test your system or use the Replica server to continue the application service while some form of maintenance is performed on the Master server.

If you have selected to initiate switchover automatically, after the Master is considered to be down, the Arcserve Live Migration automatically tries to restore the services and databases on it to their active state. First, the Arcserve Live Migration tries to restart services that it previously checked to be managed. If the services are running, it then tries to mount the databases. If all attempts fail, the Arcserve Live Migration initiates failover. These attempts to restore the services and databases are not performed if the switchover is initiated manually.

Once triggered, whether manually or automatically, the switchover process itself is fully automated.

Initiate Switchover

To initiate a switchover, follow these steps:

1. Open the Manager and select the desired scenario from the Scenario pane. Verify if it is running.
2. Click the **Perform Switchover** button, or select from the **Tools** menu the **Perform Switchover** option.

   A confirmation message appears.
3. [Optional] Select the check box **Do not wait until all journals are applied** 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. Depending on your scenario configuration, the **Run a Reverse Replication Scenario after the Switchover** check box is either selected or cleared. Select or clear the check box to change the default configuration only for the switchover you are about to perform.
5. Click **Yes** on the **Perform a Switchover** confirmation message. This procedure initiates a switchover from the Master server to the Replica server.

   During switchover, the **Events** pane gives detailed information about the switchover process.
6. 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**.

   In the Event pane a message appears, informing you that **Switchover completed**, and then that the **Scenario has stopped**.

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

Important! If the Master server crashes or is rebooted during a switchover, the process stops. If this happens, you may need to recover the active server.