Virtualized Server Environments Operation Guide

Arcserve® Replication and High Availability

Version 18.0

arcserve®

Legal Notices

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

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

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

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

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

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

The manufacturer of this Documentation is Arcserve.

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

© 2019 [[[Undefined variable My Variables.CA]]], including its affiliates and subsidiaries. All rights reserved. Any third party trademarks or copyrights are the property of their respective owners.

Arcserve Product References

This document references the following Arcserve products:

- Arcserve® High Availability (HA)
- Arcserve® Replication
- Arcserve® Assured Recovery®
- Arcserve® Content Distribution

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 Replication and High Availability (Arcserve RHA) is a solution based on asynchronous real-time replication and automated application switchover and switchback to provide cost-effective business continuity for virtualized environments on Windows servers.

Arcserve RHA lets you replicate data to a local or remote server, making it possible to recover that data due to server crash or site disaster. You may switch your users to the replica server manually, or automatically, if you licensed High Availability. This Guide presents both Replication and High Availability concepts and procedures.

The procedures covered in this Guide should be followed as is. Customize the steps only if:

- You are familiar with Arcserve RHA and fully understand the potential impact of any changes you make.

- You have fully tested the steps in a lab environment before implementing in a production environment.

This section contains the following topics:

About This Guide

This document describes how to implement a Arcserve Replication and High Availability solution for virtualized environments. Please review each procedure before you begin. It is essential that you have the appropriate resources and permissions to carry out each task.

The Guide is organized into the following main sections:

- **Microsoft Windows Hyper-V** -- Full server replication and switchover for each individual guest machine
- **Full System High Availability (HA)** -- Transfers an entire physical system to a virtual machine hosted by a Hyper-V server

Related Documentation

Use this Guide with the *Arcserve RHA Installation Guide* and the *Arcserve RHA Administration Guide*. For links of Arcserve RHA 18.0 documentation, refer to the following:

- Bookshelf
- Release Notes

Log On Account Conditions

The Arcserve RHA Engine service must satisfy certain account conditions for successful communication with other components. If these requirements are not met, scenarios may not run. If you lack the permissions required, contact your local IS team.

- It is a member of the Domain Admins group. If the Domain Admins group is not a member of the built-in domain local group Administrators you must use an account that is.

- It is a member of the local computer 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. If you have used Redirect DNS redirection method in a HA scenario, then use the local administrator account.

  Note: In MS SQL server 2012, Local System (NT AUTHORITY\SYSTEM) is not automatically provisioned in the sysadmin server role. See Microsoft documents on how to provision the sysadmin server role to the NT AUTHORITY\SYSTEM account. Alternatively, use Administrator account to install and log in to the engine service.

- When your SQL servers are in a workgroup, enable "sa" account on Master and Replica server before you run the scenario.

Register Arcserve RHA Licenses

The Arcserve RHA licensing policy is based on a combination of several parameters which include the following:

- the operating systems involved

- the required solution

- the supported application and database servers

- the number of participating hosts

- additional modules (for example, Assured Recovery)

The license key that is generated for you is therefore tailored to your exact needs.

After logging in for the first time, or if your old license has expired, you must register the Arcserve RHA product using your license key. To register the product, you need to open the Manager, which does not depend on the existence of a valid registration key. After the Manager opens, a License Warning message appears, prompting you to register the product. A License Warning message also appears when your license is about to expire during the next 14 days.

When you are creating a scenario, some of the options might be disabled following the terms of your license. However, you can create any number of scenarios, since the validity of your license key is confirmed, before you try to run a specific scenario. Only when you click the Run button, the system checks whether you are allowed to run the selected scenario according to your license key. If the system determines that you do not have the required license for running this scenario, the scenario will not run and a message will appear on the Event pane informing you of the type of license you need.

To register Arcserve RHA using the license key

1. Open the Manager.

   The Welcome message appears, followed by a License Warning message informing you that your product is not registered. You are prompted to register it.

2. Click OK to close the message.

3. Open the Help menu and select the Register option.

   The Register Arcserve RHA dialog opens.

4. Complete the following fields:

   - Registration Key field - enter your registration key

- [Optional] In the Company Name field - enter your company name

5. Click the Register button to register the product and close the dialog.

   You can now start working with the Arcserve RHA Manager according to your license permissions.

Virtualization Considerations

In virtual machine environments, all disks are added to the first controller after switchover, until it is full (16 disks). When it is full, Arcserve RHA creates another SCSI controller. This means the switched over VM could have a different deployment than its master.

Chapter 2: Protecting Hyper-V Environments

This section contains the following topics:

Hyper-V Server Configuration Requirements

- Configure the same number and type of network connections on the Replica that exists on the Master.

- (In the Active Directory environment) Both Master and Replica servers should reside in the same Active Directory forest and should be members of the same domain or trusted domains.

- Make sure to change the default location of the virtual machine. You can change the location to any other custom location.

- For supported Hyper-V versions, see the Arcserve RHA Compatibility Matrix on Arcserve Support.

This section contains the following topics:

Considerations for Hyper-V scenarios across WAN

This section describes how to create a Hyper-V scenario and ensure a smooth fail-over across different subnets in WAN environment. First set up an additional IP address and then specify the details while creating the Hyper-V scenario.

1. Set up an additional NIC on the VM running on the master Hyper-V server. The IP address of this NIC will be used on Replica after the VM fails over.

   Note: Make sure that appropriate route table entries are added or updated to make both IP addresses and subnets work.

2. Create the Hyper-V scenario as usual. However, set the High Availability properties as described in the following steps:

   a. Expand Switchover and click Virtual Network mapping and choose the appropriate network mapping. Map the additional NIC/IP that you added. This IP address is used when the Replica server takes over.

   b. Enter the DNS server IP details.

      Note: Make sure DNS record can be updated by the RHA engine. See Log On Account Conditions.

   c. Expand Network Traffic Redirection and click Redirect DNS. Select On and enter the following details:

      Virtual Machine IPs on Master server in DNS

      IP Address

      Specifies the IP address of the virtual machine on the master server

      Virtual Machine IPs on Replica server in DNS

      IP Address

      Specifies the additional IP address that you specified in step 1.

Hyper-V VM Auto-Discovery

When you create a Hyper-V scenario, the Engine collects information about all virtual machines on the Hyper-V server and stores this data in a scenario configuration file. This is an .XML file. The following information is collected:

Virtual Machine Settings

These settings are stored in an XML file named <VM GUID>.XML, where VM GUID is the unique global identifier for the virtual machine. This file resides in the %ProgramData%\Microsoft\Windows\Hyper-V\Virtual Machines folder.

Virtual Machine Folder

There is a folder for each virtual machine and the name of the folder is <VM GUID>. This folder contains VSV and BIN files when a virtual machine is running.

Virtual Hard Disks (VHDs)

VHDs are hard disks associated with each VM. These files could be in different locations and have a .VHD extension.

Snapshots

All snapshots for a virtual machine are placed in the snapshot folder. All files inside a snapshot are considered for replication. Any VHD files in the snapshot have the extension, .AVHD. Multiple snapshots for a VM have multiple AVHD files. All files are discovered and replicated.

ACLs

In addition to files and folders, security data such as ACLs and owner information for each folder and file are replicated. This security information is needed to register and run the virtual machine on the Replica server.

Virtual Network Configuration

If a VM is connected to a virtual network, the network data setting is included in the XML configuration file.

Hyper-V Server Configuration

The following information applies only to Arcserve RHA High Availability. The default Hyper-V settings are usually sufficient when using Arcserve RHA but there are some default changes you should make to ensure virtual machines can easily and successfully be started on the Replica when the Master is unavailable:

- The Hyper-V CSV cluster and standalone server are supported. Master and Replica could be CSV cluster or standalone server.

- The Hyper-V server version should be the same, including service pack levels, for all Hyper-V servers.

- The RHA Engine service logon account should be in local Administrators group on each server, and in Domain Admins group if it's domain environment.

- For Hyper-V CSV cluster, the Virtual Switch name on all cluster nodes should be the same.

- Modify Hyper-V Manager -> Hyper-V Settings -> Virtual Hard Disks folder and Virtual Machines folder to non-default folders on both Master and Replica Hyper-V servers. For Hyper-V CSV cluster environment, set the folders to the CSV mount point on each cluster node.
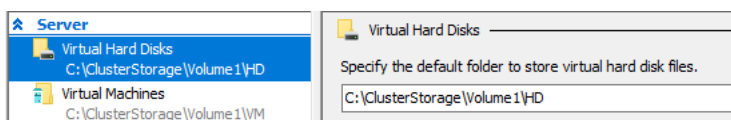
Hyper-V Replication and High Availability

The following replication and high availability tasks can be performed for Hyper-V:

- Hyper-V HA Properties
- Create a New Hyper-V High Availability Scenario

Create a Hyper-V Scenario

For Hyper-V, it is possible to perform switchover at the individual VM level, rather than the whole Hyper-V server, which means you need a separate HA scenario for every virtual machine in the Hyper-V environment. To make scenario creation easier, you can select multiple VMs from the Master that inherit the same scenario properties. This 'multiple VM' scenario is then split into sub-scenarios so you can manage each virtual machine independently.

To create a new Hyper-V HA Scenario

1. Start Manager. Select File, Create, New Scenario or click the New Scenario button.

   The Welcome dialog opens.

2. Click Create a New Scenario and type a Scenario Group Name, or select one from the list and then click Next.

   Note: If you do not assign a Scenario Group Name, all scenarios you create default to the Scenarios Group. This group becomes part of the scenario name and updates automatically to Hyper-V after the scenario wizard is completed.

   The Select Server and Product Type dialog opens.

3. Select Microsoft Hyper-V, and then select DR or HA scenario. If you need Integrity Testing for Assured Recovery (AR), select the checkbox, and then click **Next**.

   The Master and Replica Hosts dialog opens.

4. Type Hostname or IP, and Port number for both Master and Replica servers, then click **Next**.

   Note: For Hyper-V CSV clusters, you should enter the cluster name, and Arcserve Replication and High Availability inspects all nodes of the cluster automatically, and list all VMs on those nodes. If you enter a single node name of the cluster, Arcserve Replication and High Availability only lists VMs running on that node.

   If you enabled engine verification, the Engine Verification page appears. You may be prompted for user credentials. Enter the appropriate credentials and click **OK**.

5. Wait for verification to complete. Click **Install** to install the Engine on the specified hosts or click **Next**.

   The Database for Replication dialog opens, listing the auto-discovered virtual machines found on the Master server you specified. By default, all virtual machines are selected for replication. For HA, the entire VM with all related files must be selected.

6. Select or clear virtual machines for replication and click **Next**.

The Scenario Properties dialog opens.

7. Change properties, as desired, and then click **Next**. For more information, see the *Arcserve RHA Administration Guide*.
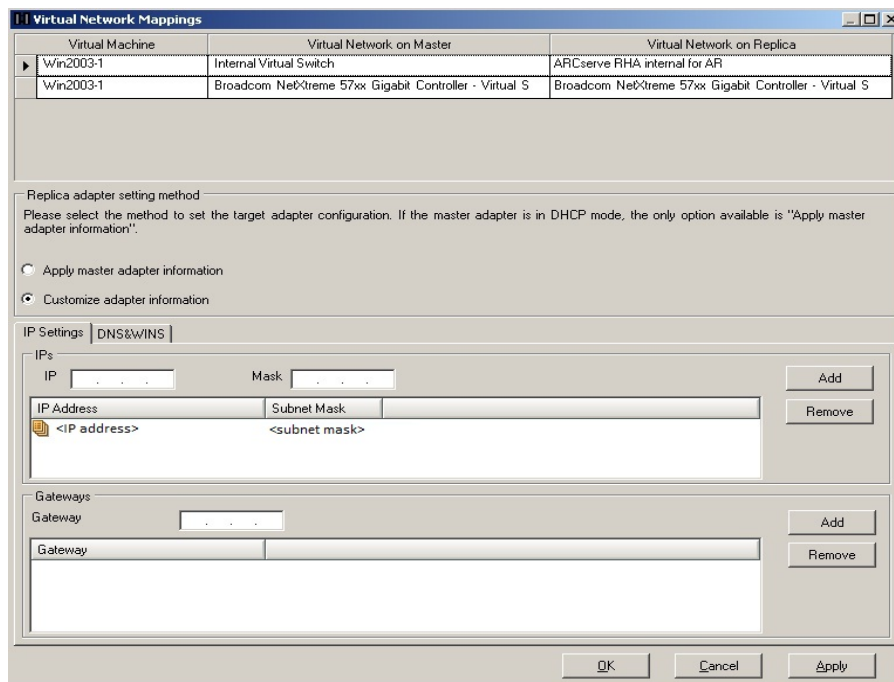
   The Master and Replica Properties dialog opens.

8. Modify properties, as desired, and then click **Next**.

   Wait while the Switchover Properties dialog retrieves information.

9. When Switchover-Properties opens, select **Click** to edit VN mappings.

   The Virtual Network Mappings dialog opens.

The Virtual Network Mapping dialog may pop up. When Replica Hyper-V has only one virtual switch, RHA automatically selects that virtual switch for Virtual Network on Replica, and does not pop up the mapping dialog.

Only if multiple virtual switches are available on Replica, Arcserve Replication and High Availability pops up the mapping dialog for user to choose for network mapping. You can click Switchover -> Virtual Network Mappings to view or change the mapping.

You may also receive an error dialog, "Fully Qualified Name could not be assigned automatically, please edit Fully Qualified Name".

Click **OK** and then click Hosts ->Click to edit fully qualified name property.

This error appears when Arcserve Replication and High Availability cannot get the host name of the guest OS of VMs, which could happen for Linux-based VMs. Fill in the host name if blank and then click **OK**.

10. Map the virtual machines listed to the desired virtual networks on the Replica and select the Replica adapter setting method.

    Apply master adapter information

    Specifies that the virtual machines on the replica use the same network adapter information as that of the master.

    Customize adapter information

    Specifies that you can manually enter the IP address, DNS, WINS, and Gateway information for the virtual machines.

    Note: For virtual machines having boot volume on a dynamic disk, sometimes the network information does not configure successfully after switchover. You may have to manually set the IP address after the virtual machine starts up.

    Limitation: If Hyper-v scenario protected VM sys volume is dynamic disk, some net-work mapping settings can't apply to the replica VM during Swithcover process. RHA doesn't support network mapping for this type virtual machine.

11. Set any other switchover properties, as desired, and click **Next**.

    The Switchover and Reverse Replication Initiation dialog opens. We recommend set-ting Switchover to Automatic and Reverse Replication to Manual.

12. Choose the desired method for initiating switchover and reverse replication and click **Next**.

    Wait while the Scenario Verification process completes.

    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.

13. Click **Next**.

    The Scenario Run dialog opens.

14. Click **Run Now** to start synchronization and activate the scenario.

15. Click **Finish** to run the scenario later.

Hyper-V Scenario Properties

If you wish to change a scenario configured through the Wizard or configure additional settings, you can use the Properties pane to modify the scenario.

The Properties pane and its tabs are context-sensitive and change whenever you select a different node from a scenario folder. You must stop a scenario before configuring its properties. Certain values cannot be modified once set; they are noted. For full details on configuring scenario properties and their descriptions, see the *Arcserve RHA Administration Guide*.

Properties are organized into tabs on the Manager Framework pane. The tabs displayed are based upon server type, Arcserve RHA solution, and scenario status. Select the scenario for which you wish to change properties, and then select the appropriate tab. The following screen shows an example:

Settings on the Root Directories tab

- Select a Master Server from the Scenario Pane. Double-click its Directories folder to add or remove Master Root Directories. You cannot directly update the Hyper-V root directory. Double-clicking it launches Auto Discovery, which lists all virtual machines on the Master.

- Select a Replica Server from the Scenario Pane. For each Master Root directory, you must specify a Replica Root directory. Double-click the Directories folder for the Replica server.

Settings on the Properties Tab

Scenario Properties

These settings establish default behavior for the entire scenario.

- General properties -- cannot be changed once created

- Replication properties -- choose the replication mode (Online or Scheduled), synchronization values (File or Block, Ignore Files of Same Size/Type) and optional settings (Replicate NTFS Compress Attribute, Replicate NTFS ACL, Synchronize Windows Shares, Prevent Automatic Re-sync upon Error)

- Event notification properties -- specify a script to run or choose email notification and write results to the event log

- Report Handling -- specify report settings, email distribution or script execution

Master and Replica Properties

These settings establish server properties on both Master and Replica. Some settings vary by server type.

- ◆ Host connection properties -- Enter the IP address, Port number and Fully Qualified Name of the Master and Replica.

- ◆ Replication properties -- Enable Hyper-V scheduled bookmarks for master. These properties differ for Master and Replica. See the *Arcserve RHA Administration Guide* for more information.

- ◆ Spool properties -- Set the size, minimum disk free size and directory path. See Spool Directory Settings for more information.

- ◆ Event notification properties -- specify a script to run or choose email notification and write results to the event log.

- ◆ Report properties -- choose synchronization or replication reports, specify distribution or script execution.

- ◆ (Replica) Recovery properties -- set delay or data rewind properties. Data rewind is On by default.

Settings on the Scenario Properties Tab

These settings control how switchover and switchback are performed.

- ▪ Switchover properties -- choose automatic or manual switchover, provide switchover hostname, virtual network mappings, and reverse replication settings

- ▪ Hosts properties -- specify the Master and Replica Fully Qualified Name

- ▪ Is Alive properties -- set the heartbeat frequency and check method

- ▪ Action upon Success properties -- defines custom scripts and arguments for use

Switching Over and Switching Back

Switchover and *Switchback* is the process in which active and passive roles are exchanged between the Master and Replica servers, so that if the Master is currently active, it changes to passive after Switchover passes the active role to the Replica. If the Replica is active, it changes to passive after Switchover passes the active role to the Master. Switchover can be triggered at the push of a button or automatically by Arcserve RHA when it detects that the Master is unavailable, if you enabled the Perform Switchover Automatically option from the Switchover and Reverse Initiation dialog. When this option is Off, the system notifies you that the Master server is down so you can manually initiate switchover from the Arcserve RHA Manager.

This section contains the following topics:

- How Switchover and Switchback Work
- Initiate Switchover
- Initiate Switchback
- Switchover Considerations
- Run a Scenario from Outside the Wizard
- Stop a Scenario
- View a Report

How Switchover and Switchback Work

After the HA scenario starts running and the synchronization process is completed, the Replica checks the Master on a regular basis, by default every 30 seconds, to see if it is alive. The following types of monitoring checks are available:

- **Ping** -- a request sent to the VM on the Master to verify that the VM is up and responding. If the Is Alive check returns false, the Replica brings up the VM automatically.

- **User-defined check** -- a custom request you can tailor to monitor specific applications.

- **Connect to database** -- a request sent to the Master to verify that the appropriate services are running, and the VM is active and responding to pings.

These checks are performed sequentially (if enabled). If an error occurs with any part of the set, the entire check is considered to have failed. If all checks fail throughout a configured timeout period (by default, 5 minutes), the VM on the Master server is considered to be down. Then, depending on the HA scenario configuration, Arcserve RHA sends you an alert or automatically initiates a switchover.

When you created an HA scenario, you defined how you want the switchover to be initiated.

- If you selected the Initiate Switchover manually option from the Switchover and Reverse Replication Initiation page, perform a manual switchover. For more information, refer to the topic, Initiate Switchover.

- If you 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 you want to use the Replica server to continue the application service while some form of maintenance is performed on the Master server. Triggered (automatic) switchover is in all ways identical to manual switchover performed by the administrator, except it is triggered by a resource failure on the master server rather than by an administrator manually initiating the switchover by clicking the Perform Switchover button. Server ping response, application service status, and VM connectivity are monitored. The timeout parameters are configurable and are more extensively covered in the *Arcserve RHA Administration Guide.*

When you created an HA scenario, you defined how you want the reverse scenario to be initiated.

- If you selected the Initiate Reverse Replication automatically option from the Switchover and Reverse Replication Initiation page, replication in the reverse direction (from Replica to Master) automatically begins after a switchover, one the original Master server becomes available again.

- If you selected the Initiate Reverse Replication manually option, you need to perform switchback manually. If you select the manual option and do not initiate a manual switchback, you must resynchronize data from Replica to Master, even after testing a clean switchover without a Master failure.

When the Reverse Replication feature is off, to start reverse replication after a switchover has occurred, click the Run button. The benefit to this feature is resynchronization in the reverse direction is not required, if both the master and replica servers were online and connected during switchover. Resynchronization involves comparing the data on the master and replica servers to determine which changes to transfer before real-time replication starts; this can take some time. If automatic reverse replication is turned on, and both servers were online during switchover, replication is reversed without the need for resynchronization. This is the one situation in which resynchronization is not required.

Initiate Switchover

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

To initiate manual switchover

1. Open the Manager and select the desired scenario from the Scenario pane. Verify it is running.

2. Click on the **Perform Switchover** button, or select from the **Tools** menu then **Perform Switchover** option:

   A confirmation message appears.

3. Click **OK** on the **Perform Switchover** confirmation message. This procedure initiates a switchover from the Master server to the Replica server:

   Detailed information about the switchover processes is located in the Events pane during switchover.

4. After the switchover is completed the scenario stops:

   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 Master becomes passive and the Replica becomes active.

Initiate Switchback

After a switchover is initiated, whether manually or automatically, at some point, you will want to reverse the server roles and make the original Master the active server and the Replica the standby server. Before you switch back the roles between servers, decide if you want the data on the original Replica server to over-write the data on the original Master. If yes, you must first perform a reverse scenario, called a backward scenario.

Note: The following steps are the same regardless of server type.

To initiate manual switchback

1. Ensure that both Master and Replica servers are available on the network and that the Engine is running.

2. Open the Manager and select the desired scenario from the Scenario pane.

3. Perform one of the following:

   ◆ If the scenario is already running, skip directly to Step 4

   ◆ If the scenario is not running, perform these steps and then go to Step 4:

      a. Click Run on the toolbar to start the scenario.

         Arcserve RHA detects that a switchover has occurred and verifies its state and configuration. After verification completes, the Verification Results dialog appears, listing existing errors and warnings if detected, and prompting you to approve the running of the backward scenario. If desired, click the Advanced button to open an additional pane with detailed information about the hosts that participate in the scenario.

      b. Select a synchronization method from the Run dialog and click OK to start resynchronization.

         Note: See the Arcserve RHA Administration Guide for more inform-ation on Synchronization Methods.

   ◆ After resynchronization completes, you receive a message in the Event pane: All modifications during synchronization period are replicated. Now, rep-lication from the active server to the standby server begins.

      Note: You are now ready to reverse the roles between the Master and Rep-lica servers.

4. Click Perform Switchover on the toolbar while the scenario is running to reverse the server roles. A confirmation message appears.

5. Click Yes to clear the message and start the switchback process.

After the switchback is completed, the server roles are reversed back and the scenario automatically stops.

Note: The scenario will continue to run after the switchback when the Reverse Replication Initiation option is defined as Start Automatically.

You may now run the scenario again in its original (forward) state.

Switchover Considerations

To prevent overwriting data, the best practice is to set *either* the Switchover or the Reverse Replication Initiation property to Automatic. If a server fails while both properties are set to Automatic, Arcserve RHA triggers Switchover without administrative involvement and could start Reverse Replication before you have investigated the cause of the failure. During Reverse Replication, Arcserve RHA overwrites data on your production server.

If a crash or outage occurs during switchover, you may need to perform the Recover Active Server procedure.

Run a Scenario from Outside the Wizard

After you create a scenario, you need to run it to start the replication process. Normally, before changes to data on the Master can be replicated on the Replica, the Master and the Replica need to be synchronized. Therefore, the first step in initiating a replication is synchronizing the Master and Replica servers. After the servers have been synchronized, online replication starts automatically, continuously updating the Replica with all of the changes that occur on the Master.

Note: In order for the replication process to succeed, verify that the user under which the Engine is running has Read permission on the Master, and Read and Write permissions on each replication root directory and included files, and on all participating Replica hosts.

To start a scenario:

1. From the Scenario pane, select the scenario you want to run.

2. To run the scenario, click the **Run** ▷ button on the Standard toolbar.

   Arcserve RHA verifies the scenario before running it.

   If the scenario was not set up correctly or problems occurred in the participating hosts, errors are reported on the Event pane.

   Notes:

   ◆ If any errors are displayed, you cannot run the scenario. These errors must be corrected before you can start the replication process.

   ◆ Replication of mount points will succeed only if those were added to the Master before the Engine was started. If you included the mount points in the Master root directories when the Engine was already running, no error is reported but the replication does not start. In this case, you need to restart the Engine on the Master before initiating replication.

   When no error is reported, the **Run** dialog appears.

3. From the Run screen, select the following and then click OK:

   ◆ **Synchronization Method** -- For database and virtual machine applications, Block Synchronization is usually best but for File Servers or other applications with large numbers of small files, choose File Synchronization. See the *Arcserve RHA Administration Guide* for more information.

   ◆ **Ignore same size/time files** -- Disable this option for database applications. Enable this option for File Server applications to speed up the comparison pro-

cess and reduce overall synchronization time. See the *Arcserve RHA Admin-istration Guide* for more information.

◆ **Skip Synchronization** -- Select this option only if you are certain that the data in the Master and Replica root directories is identical.

The Manager indicates that the scenario is running with a green play symbol to the left of the scenario, and with the scenario's state, which turns into **Running**:

Once a scenario is running, a Statistics tab appears at the bottom of the Framework pane, displaying a graphical view of the replication.

By default, once synchronization occurs, a Synchronization Report is generated. To view the report, refer to the topic, View a Report.

Note: You can also generate a Replication Report on a regular basis to monitor the replication process on each participating server. For more information, see *Arcserve RHA Administration Guide.*

Stop a Scenario

To stop a scenario

1. From the Scenario pane, select the scenario you want to stop.

2. To stop the scenario, click the Stop ⬜ button on the Standard toolbar.

   A confirmation message appears prompting you to approve the scenario stopping.

3. Click Yes in the confirmation message. The scenario stops.

   After stopping the scenario, the Manager no longer shows the green play symbol to the left of the scenario, the scenario state turns to Stopped by user and the Statistics tab is no longer available on the Framework pane.

View a Report

Arcserve RHA can generate reports on the replication and synchronization processes. These reports can be stored on your desired location, opened for view from the Report Center, sent by email to a specified address, or they can trigger script execution.

The default storage directory of the generated reports is: *[ProgramFilesFolder]\CA\XOsoft\Manager\reports*

To view a report

1. To view a report, first you need to open the Report Center. There are two ways to open it:

   ◆ On the Overview Page, click the **Report Center** link on the **Quick Start** pane on the left.

   ◆ From the **Tools** menu, select the **Reports** option and then **Show Scenario Reports**.

   The Report Center opens in a new window.

   The Report Center consists of two tables:

   ◆ The upper table - **Available Reportsper Scenario** - contains a list of all scenarios that have reports, along with the type and number of available reports for each scenario.

   ◆ The lower table - **Reports** - contains a list of all the reports that are available for the scenario selected in the upper table.

2. To view a specific report, select from the **Available Reportsper Scenario** table the scenario that this report represents. Then, from the **Reports** table below, click the report you want to open:

   Note: Depending on your settings, for Synchronization and Replication reports a **Detailed** report can be generated in addition to the **Summary** report. Both reports represent the same process, but the **Detailed** report also provides a list of the files that participated in the process.

   The report you selected appears in a new window.

The Data Recovery Process

When an event causes loss of Master data, the data can be restored from any Replica. The recovery process is in fact a synchronization process in the reverse direction - from a Replica to the Master. You can recover lost data from the Replica to the master -- this option is a synchronization process in the reverse direction and requires you to stop the scenario. Or, you can recover lost data from a certain event or point in time (Data Rewind) -- This option uses a process of stamped checkpoints and user-defined bookmarks to roll corrupt data on the Master back to a time before corruption occurred.

Important! You must stop replication in order to initiate recovery.

This section contains the following topics:

- Setting Bookmarks
- How to Restore Data on Hyper-V Machines

Setting Bookmarks

A *bookmark* is a checkpoint that is manually set to mark a state that you may want to rewind back to. We recommend setting a bookmark just before any activity that may cause data to become unstable. Bookmarks are set in real-time, and not for past events.

Notes:

- You can use this option only if you set the **Recovery - Data Rewind** option to **On,** in the Replica Properties list.

- You cannot set bookmarks during the synchronization process.

- Hyper-V HA allows you to schedule bookmarks.

To set a bookmark

1. When the required scenario is running, select the Replica host from which you want to rewind data.

2. From the menu, select **Tools, Set Rewind Bookmark**.

    The **Rewind bookmark** dialog appears:

    The text that appears in the **Rewind bookmark** dialog will appear in the **Rewind Points Selection** dialog as the bookmark's name. The default name includes date and time.

3. Accept the default name, or enter a new name for the bookmark. It is recommended to give a meaningful name that will later help you recognize the required bookmark. Then, click OK.

    The bookmark is set.

How to Restore Data on Hyper-V Machines

The process of restoring data from a Hyper-V virtual machine is much like restoring data in any other scenario with the following conditions:

- **Stop the VM** -- Arcserve RHA automatically powers off the VM before recovery so that the existing VM can be overwritten. After restore completes, you need to restart the VM manually.

- **Select a bookmark** -- You must roll data back to a specific point in time called a bookmark, or rewind point. The default frequency is 1 hour, but bookmarks can be set at frequencies you define. When you create the Hyper-V scenario, ensure the Enable Hyper-V Scheduled Bookmarks setting is set to On from the Master and Replica Properties screen. For existing scenarios, you can edit this property manually.

- **Synchronize data** -- Use File or Block synchronization.

This section contains the following topics:

- Recover Hyper-V Data with Rewind Points
- How to Start a Hyper-V VM on the Replica Server

Recover Hyper-V Data with Rewind Points

For Hyper-V scenarios, the Data Rewind recovery method also applies.

To recover lost data using rewind points in a Hyper-V Server HA scenario

1. From the Manager, select the desired scenario and stop it.

2. From the Manager, select the Replica host to enable Restore Data options.

3. From the Tools menu, select Restore Data, or click the Restore Data button to open the Recovery Method dialog.

4. Choose the desired Rewind Data method, depending on whether you want the rewind data synchronized back to the Master or left on the Replica only. When you choose a Rewind Data option, a Recovery Scenario is automatically created. This Recovery Scenario runs until the end of the rewind process. Click Next to continue.

5. Wait while the Rewind Point Selection dialog retrieves information. When the Select Rewind Point button is enabled, click it to continue.

6. The Select Rewind Point dialog for Hyper-V opens.

   This dialog displays information specific to Hyper-V scenarios. You can choose to display rewind points by file name or start time. Select the desired rewind point and click OK to return to the Rewind Point Selection dialog, which now displays the rewind point you selected.

7. Click Next to open the Synchronization Method dialog.

8. Choose Block Synchronization and then click Finish.

   Arcserve RHA rewinds the data to the point you selected. After the rewind process ends, the following message is displayed in the Event Pane: Rewind process is completed successfully.

   If you chose to replace the data on the Master with the data on the Replica, Arcserve RHA starts a synchronization process from the Replica to the Master. Once completed, the temporary Recovery Scenario is stopped and then deleted. If you wish, you can view the Synchronization Report that is generated by default. At this time, Replication can restart on the original scenario.

How to Start a Hyper-V VM on the Replica Server

When a virtual machine fails over to the Replica server, Arcserve RHA starts the virtual machine on the Replica automatically.

Additional Information and Tips

This section provides you with helpful information concerning the application.

- By default, the spool is located in the Arcserve RHA installation /tmp directory. You can change the default location by modifying the pathname for spool directory. It is best to configure the spool on a non-SQL database or log file drive. Using a dedicated volume for the spool folder can increase performance under high load. If you do change the spool location, please remember to remove the new path from the anti-virus scans, both scheduled and real-time.

- Arcserve RHA supports bandwidth limitation and bandwidth limitation scheduling. If you require such features, please consult the *Arcserve RHA Administration Guide*.

This section contains the following topics:

- Troubleshooting Hyper-V
- Spool Directory Settings

Troubleshooting Hyper-V

The following information is provided to help you resolve certain problems:

CV01378 Hyper-V HA scenario has unassigned virtual network mapping

Reason:

The scenario you created discovered more than one virtual network on the Replica. You must map additional virtual networks manually.

Action:

From High Availability Properties, expand Switchover properties and click "Click to edit virtual network mapping" to map virtual networks manually.

Could not edit virtual network mappings

Reason:

This is an internal error.

Action:

1. Restart the Control Service.

2. Re-create the scenario.

3. Collect log messages and the scenario .xmc file.

4. Contact Support.

Could not retrieve list of virtual networks from replica

Reason:

This is an internal communication error, but the scenario is likely correctly configured.

Action:

1. Collect log messages and the scenario .xmc file.

2. Contact Support.

The Replica Server has no virtual networks defined. This could mean the Replica has no Hyper-V role enabled or no virtual networks were configured.

Reason:

The Replica Server has no virtual networks defined. This could mean the Replica has no Hyper-V role enabled or no virtual networks were configured.

Action:

Ensure the Hyper-V role is enabled on the Replica server. Ensure at least one virtual network is defined.

Editing error

Reason:

You left a required field blank or provided an invalid entry.

Action:

Ensure all fields are completed and entries are valid.

Spool Directory Settings

The Arcserve RHA spool is a folder on disk where data to be replicated is backed up (spooled) if bandwidth is not sufficient to transfer the amount of changes in real-time. Data can spool due to temporary network disconnections, network congestion, or simply because the network bandwidth is not sufficient to transfer the amount of data changing over on the server. In addition to storing changes waiting on available bandwidth, spool space is also used as part of the normal synchronization process. Thus, some spool build up during synchronization is normal.

Place the spool folder on a drive with relatively low use such as a dedicated volume or boot/system volume. Do not place the spool folder on a volume containing frequently accessed system (OS), user, or application data. Examples include volumes containing databases, shared files, or the system pagefile. By default, the spool folder is located in the tmp folder under the Arcserve RHA installation directory. The spool parameters, located in the properties tab (on both master and replica) or set with the New Scenario Wizard, determines how much disk space is available for the spool. In most cases the default values are sufficient. However, if you change this value, it should be at least 10% of the total dataset size. For example, if you are replicating 50 GB of data on a server you should ensure that at least 5 GB of space is available for spool.

Important! If you change the spool location, remember to remove the new path from file level antivirus scans: both scheduled and real time.

Note: The Spool Directory is not a pre-allocated space folder and will be used only if needed.

Chapter 3: Protecting Full System to Virtualization Platforms and Cloud

Full System scenarios let you protect or move a physical system to a virtual machine. With Full System scenarios, you can switch a physical machine over to a virtual server manually or automatically, perform assured recovery testing, or set bookmarks that can be used as restore points to either the original machine, or to a new machine.

Arcserve RHA supports dynamic disks including Simple, Striped, Mirrored, Spanned, and RAID-5 volumes. You can have both master and replica as dynamic disks. Dynamic disks let you create volumes that span multiple disks.

Note: When you create a bookmark, RHA engine calls the application VSS writer to create an application consistent snapshot on the master. RHA has four parameters (EnableVSSWriters, ExcludedWriterList, IncludedWriterList, StartWriterServicesList) in the ws_rep.cfg file to customize how the RHA engine calls the application VSS writer to create the snapshot.

Full System Scenario Limitations:

- Arcserve Replication and High Availability Full System scenario is not supported if the master server is FAT32 system volume or partition from non-UEFI (legacy) system.

- Arcserve Replication and High Availability Full System scenario is not supported if the master server is Windows 2008 R2 UEFI system and the replica/appliance is Hyper-V.

  For more information, see link.

This section contains the following topics:

Full System Requirements and Configurations

This section contains the following topics:

How Full System Scenarios Work

Use Full System scenarios to protect any server, regardless of application type. Replication, High Availability and Assured Recovery are supported. Full System scenarios are application-independent and let you transfer an entire physical machine (Master), including all system status information, to a virtualized Replica that supports the guest operating system of the active server.

The following virtualized environments are supported as the Replica server in Full System scenarios:

- Amazon EC2 Cloud

- Microsoft Azure Cloud

- Microsoft Hyper-V

- Citrix Hypervisor / XenServer

    Note: Review XenServer Configuration Limitations before using XenServer on www.citrix.com.

- VMware vCenter/ESXi

- KVM

- Oracle VirtualBox (Experimental. Not supported)

Note:

Data from a physical Master is replicated *not* to a physical Replica, as it is in typical Arcserve RHA scenarios, but to a virtual hard drive file stored on a VM. This virtual machine, called an *appliance[1]* in Full System scenarios, runs on a virtual platform host and is configured with the Arcserve RHA Engine. At switchover, the physical Master is disabled, a new virtual machine is created on the virtual platform host and the virtual disk file is mounted as a disk. The new VM is booted and integration services are deployed.

Note: You cannot run two Full System scenarios that protect the same physical Master.

---

[1]The appliance is a virtual machine running on the virtual platform host specified in a Full System scenario. Install the Arcserve RHA Engine on this VM and specify it as the Replica server in these scenarios. However, if Hyper-V is the virtual platform, the Appliance field does not apply.
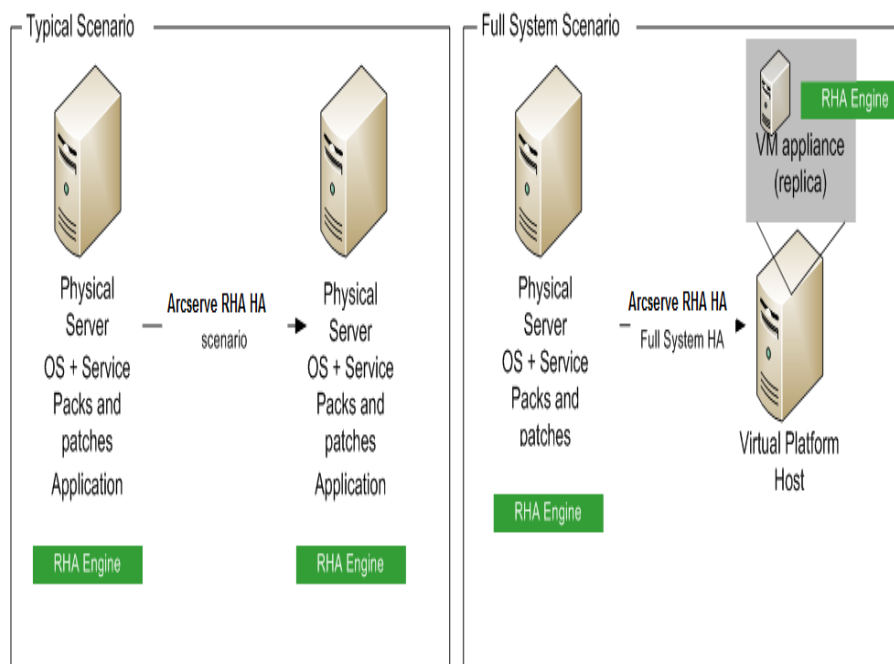
The following list highlights how primary Arcserve RHA operations work with Full System scenarios.

Scenario Creation -- Create a Full System scenario that identifies a physical machine as the Master server and a virtual machine as the Appliance (Replica) and the virtual platform that hosts this Appliance VM. Specify information unique to Full System scenarios, depending upon the virtual platform type:

- Volume List -- You can select which volumes on the Master to include in the scenario. The system and boot volumes must be protected and are always selected by default.

- Root Directory List -- Since there is no root directory concept in Full System scenarios, this list is used to guide which data is replicated to virtual disk.

- Local Directory on VM -- This is the location of the virtual disk stored on the virtual machine server. All virtual disks are stored here. It also stores the virtual disk volume mount point. Arcserve RHA replicates data from the source directory on the physical Master to the mount point on the virtual Replica.

- Network Adapter List -- This stores all network adapter information (adapter name, adapter ID, IP address, MAC address, and so on) on the physical machine. This information is used to create network mapping lists between the physical machine's adapter and the virtual machine's adapter.

- Network Mapping List -- When the virtual machine is created, the network adapter on the VM is set according to the information in this list.

- CPU/Memory Value -- When the virtual machine is created, Arcserve RHA sets the CPU number and memory size of the VM according to configuration properties defined in the scenario.

- Resource Pool -- For vCenter or ESXi platforms, choose a resource pool that specifies the shared resources for the VM.

- Datastore -- For vCenter or ESXi platforms, choose a datastore that specifies where the VM files are to be saved.

Scenario Start -- Arcserve RHA validates the stored scenario to verify no errors exist that could prevent a successful switchover, if needed.

Synchronization -- The physical Master creates and transfers the virtual disk file to the local directory on the virtual Replica. After transfer, the virtual disk file is stored in the directory you specified on the Root Replica Directory dialog during scenario creation.

Replication -- The physical Master replicates any data changes to the virtual disk file stored on the Replica in real time mode. The virtual disk file is mounted as a directory on the Hyper-V server file system.

Switchover -- If the physical Master is unavailable, Arcserve RHA initiates switchover according to the properties set during scenario creation. Arcserve RHA stops the Full System scenario and disables the physical machine network. The virtual machine is created on the server using the same name as the physical Master. The virtual disk is mounted and the network adapter for the virtual machine is added according to the network mapping list defined in the stored scenario. Finally, the virtual machine is booted. For end users accessing the failed physical Master, switchover takes several minutes.

Data Recovery -- Launch the Data Recovery Wizard and select a restore point. You can select the volumes to be restored and the target to which these volumes should be restored. Arcserve RHA creates and starts the restore scenario.

Assured Recovery -- You can perform manual or automatic assured recovery. Select the virtual Replica and click Replica Integration Testing, select the type of Assured Recovery and continue. Arcserve RHA stops applying journal changes, starts the AR process by creating a virtual machine with the specified virtual disks and then starts the VM. Arcserve RHAresumes applying journal changes when AR is stopped.

Full System Scenario System Requirements

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

For supported Operating Systems and platforms, refer to Arcserve Replication and High Availability 18.0 Compatibility Matrix.

Note: Before deploying Arcserve Replication and High Availability scenarios, refer to Limitations section in *Release Notes*.

Full System Scenario System Configuration

Arcserve Replication and High Availability supports both Windows and Linux for Full System scenario. If Master is Windows, then the Virtual Appliance (VA) must be Windows. If Master if Linux, then the VA must be Linux as well. For supported Operating Systems and platforms, refer to Arcserve Replication and High Availability 18.0 Compatibility Matrix.

Full system scenarios require three hosts instead of two, typical for other Arcserve Replication and High Availability scenarios:

- Master server - is the host that you want to protect. This host can be physical or virtual.

- Appliance - is a VM where you installed the Arcserve RHA Engine.

- Virtual Platform Host - is the server where the Appliance VM is running.

Consider the following when planning Full System scenario:

- **Engine Service Account:** For Windows, Local System account is recommended for RHA 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 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, RHA Engine runs with root account after installation, and cannot be changed.

- **Engine package dependencies on Linux:** RHA 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 RHA engine, run the following command to get the list of required packages:

  rpm -qpR arcserverha_rhel7_x86_64.rpm

This section contains the following topics:

Configure Master Server

For Full System scenarios, the Master can be any Windows machine, physical or virtual, supported as both a guest OS in the virtual environment and by the Arcserve RHA Engine. For a complete list of supported operating systems, see the Arcserve RHA Release Notes.

Install RHA Engine on Master. Usually, no additional configuration is required. For more information, refer to Instalation Guide.

Configure Virtual Appliance (VA) Server

The RHA Virtual Appliance (VA) is a VM running on the virtualization platform or cloud where you want to replicate Master servers. The VA act sas Replica in a RHA 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: 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.

Next Topics:

- Hardware Configuration for VA
- Considerations for VA Running on Cloud
- RHA Engine for Virtual Appliance (VA) Installation

Hardware Configuration for Virtual Appliance (VA)

Following are minimal hardware configuration 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 RHA spool directory is set, depending upon 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.

Next Topics:

- Considerations for VA Running on Cloud
- RHA Engine for Virtual Appliance (VA) Installation

Considerations for VA Running on 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.

Note the following 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 ESX and vCenter platforms, install VMware Tools on the Appliance VM.

- Install the Arcserve RHA 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: In Disks configuration screen, select **Use managed disks**. Arcserve Replication and High Availability does not support unmanaged disks on Azure.

- RHA 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 RHA Engine is installed on VA, verify that RHA 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 RHA Engine version information.

Next Topic:

- [RHA Engine for Virtual Appliance (VA) Installation](#)

RHA Engine for Virtual Appliance (VA) Installation

Configure RHA Engine on Windows and Linux.

OS	Plaforms 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

For details, view Arcserve Replication and High Availability Compatibility Matrix.

Next Steps:

- Configure RHA Engine on Linux
- Configure RHA Engine on Windows

Configure RHA Engine for Virtual Appliance (VA) Installation in Linux

Configure RHA Engine on Linux. Check Software Compatibility Matrix for updated information.

Following platforms are supported as VA.

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

Follow these steps to install:

1. Transfer RHA engine to VA, then extract and then change directory to extracted directory:

   tar xzf arcserverha-xxxx.rhel7.tgz

   cd arcserverha

2. 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 and then use the installation wizard.

▪ **Silent mode**: Run the following command to install RHA engine and VA module silently:

./install.sh -y -v y

3. RHA engine and VA packages are installed properly:

4. Run the following command:

yum list installed arcserverha libvir

Sample Installation Package as output

arcserverha.x86_64	18.0-0.5311	@arcserve-install
libvirt.x86_64	4.9.0-7.arcserve.el7.centos	@arcserve-install

Configure RHA Engine for Virtual Appliance (VA) Installation in Linux

Configure RHA Engine on Windows. For details, view Arcserve Replication and High Availability Compatibility Matrix.

To install Engine component on virtual apliance, refer to Installation Guide. Usually no additional configuration is required.

Following platforms are supported as VA:

▪ Windows 2012 R2

▪ Windows 2016

▪ Windows 2019

Configure Virtualization Platform and Cloud

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

- ESXi
- Hyper-V
- XenServer
- KVM
- Amazon EC2
- Microsoft Azure

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

An output as shown below indicates successful configuration.

Name	State	Autostart
RHA_datastore1	active	yes

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

   An output as shown below indicates successful configuration.

Name	State	Autostart
F:\HyperVVM\	active	yes

Configure XenServer

No special configuration is needed on XenServer.

Configure KVM

Arcserve Replication and High Availability supports three protocols for VA to communicate with the KVM server: SSH, SSL, and None. Following is an example procedure for configuring SSH protocol. You can refer to the corresponding KVM documentation for configuring other protocols.

To use the SSH protocol, you can configure for Arcserve Replication and High Availability on Linux VA server using the *root* account.

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

    You are asked to enter password to continue.

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

    Ssh root@kvm-server

4. Run the following command in shell:

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

    An output as shown below indicates successful configuration.

Name	State	Autostart
Default	active	yes
kvm-datastore1	active	yes

Configure Amazon EC2

Arcserve Replication and High Availability VA virtual machine resides in VPC, and Master servers are replicated to that VPC.

Note: Refer to 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:

- 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 RHA Scenario, you can pick one public IP from existing Elastic IP addresses for the DR VM.

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 RHA 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 RHA Manager.

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 from the right pane click **App registrations**.

   c. Click **New application registration**.

   d. Enter a name and sign-on URL for the application.

   The application is a Web app/API. Note that sign-on URL can be any address as it is not called in RHA.

   e. After setting the values, click **Create**.

   Now, you need to assign Contributor role to the application through Subscription Access Control (IAM).

   f. Navigate to Select Subscriptions -> Click your Subscription -> Select Access control (IAM) and click **Add**.

   g. From the respective drop-down lists of **Add permissions** on the right pane, select the Contributor role, select 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:

   a. From the left navigation panel 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 RHA Manager.

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

   a. From the left pane of Azure portal, click Azure Active Directory.

   b. From the Azure Active Directory Properties screen, copy the Directory ID o use while adding the account in RHA Manager.

4. Perform the following steps to get the Application ID:

   a. From App registrations in Azure Active Directory, select the application.

   b. Copy the Application ID to use while adding the account in RHA Manager.

5. Perform the following steps to generate an authentication key and get the Client Key[2]:

   a. Select the application, and navigate to **Settings** to select Keys.

   b. Enter the description, duration, value of the key, and then click **Save**.

      The value of saved key is displayed. The saved value of the key is referred as the Client Key.

   c. Copy this value to use while adding the account in RHA Manager.

      Note: Copy the key as you cannot retrieve later.

   Preparation of Azure Cloud Account is complete. Now, add details in RHA Manager.

Add an Azure Cloud Account in RHA Manager

---
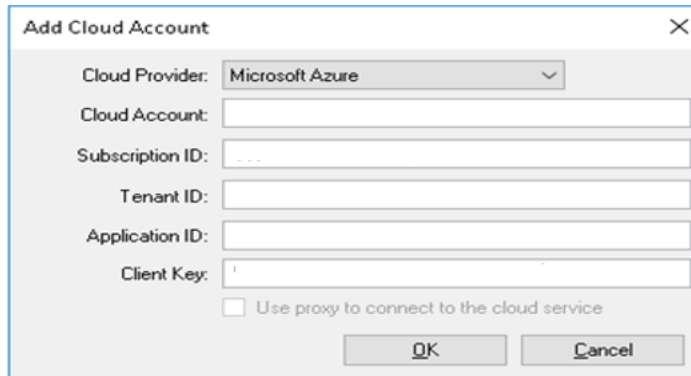
[1]Tenant ID refers to the ID of the Azure Active Directory where you created the application registration. Tenant ID is called Directory ID inside Azure Active Directory Properties.
[2]Client Key is referred as authentication Key in Azure.

1. From the RHA Manager, navigate to Cloud -> Manage Cloud Accounts and click **Add**.

   Add Cloud Account screen is displayed.

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

Arcserve Replication and High Availability is configured for Microsoft Azure.

Creating Full System Scenarios

Full System scenarios create virtual disks from a physical Master server and store them on a virtual platform host. In the event of a switchover or failover, the virtual disk is used to create a virtual machine on the virtual platform host.

Full System scenarios are supported on the following virtual platforms:

- Amazon EC2

- Microsoft Azure Cloud

- VMware vCenter/ESXi

- Microsoft Hyper-V

- KVM

- Citrix Hypervisor / XenServer

Note: Refer to the Arcserve RHA Release Notes or the Compatibility Matrix for supported versions.

While most Arcserve RHA scenarios require that you specify two hosts (a Master and a Replica), Full System scenarios require three:

- **Master** - this is the physical machine you wish to protect.

- **Appliance** - this is a virtual machine that acts as the Replica server (the Arcserve RHA Engine should be installed here). If you are using a Hyper-V virtual platform, this field does not apply and is not available (appears dim).

  Notes:

  - If the Master is Windows 2008 or a later version, we recommend using Windows 2008 R2 as the appliance.

  - If you are using Hyper-V as the destination platform, we recommend using Windows 2008 R2 as the appliance.

- **Virtual Platform Host** - this is the machine that hosts the Appliance VM acting as Replica server.

This section contains the following topics:

How to Manage Cloud Account
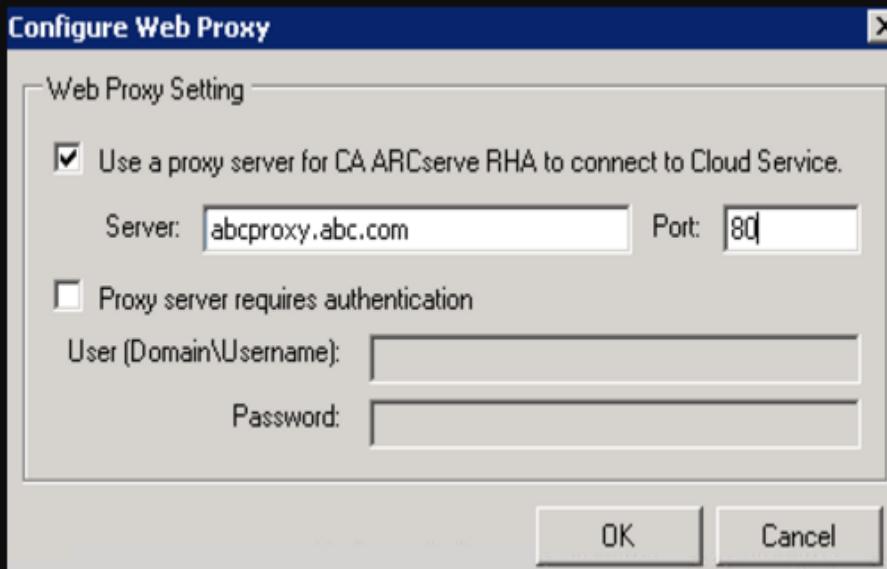
This section contains the following topics:

Configure the Web Proxy to Connect to the Cloud Service

If you want to use the Use proxy to connect to the cloud service option in the Add Cloud Account dialog, you must first configure the Web proxy that you want to use to manage EC2 resources.

To configure the Web proxy, click the Configure Web Proxy click the configure web proxy 🌐 toolbar button to configure Amazon web services server toolbar button in the Cloud View panel and enter web proxy setting information (such as server, port, and user credentials). A test request is sent to the server to verify the proxy setting. Once verified, the proxy setting is saved in the AWS account.

Add a New Cloud Account

To see and manage EC2 instances in the Cloud View panel, you must first add a new cloud account using your AWS credentials.

To add a new Cloud Account

1. Click the Add Cloud Account button click the add cloud account toolbar button on the toolbar.

   The Add Cloud Account dialog opens.

2. Enter information in the following fields:

   Cloud Provider

   Specifies the name of the cloud provider service.

   Cloud Account

   Specifies the cloud account; typically this is the email address you used to register your AWS account.

   Access Key ID

   Lets you enter the access key ID for your AWS account.\

   Secret Access Key

   Lets you enter the secret access key provided by your AWS account.

   (Optional) Use proxy to connect to the cloud service

   Lets you specify whether to use a Web proxy to communicate with the AWS web services server. If you select this check box to enable this option, ensure that you have first configured this proxy.

Note: The information required for these fields can be obtained from your AWS account home page using the Security Credentials tab, as shown here:

Access Credentials

There are three types of access credentials used to authenticate your requests to AWS services: (a) access keys, (b) X.509 certificates, and (c) key pairs. Each access credential type is explained below.

| Access Keys | X.509 Certificates | Key Pairs |

Use access keys to make secure REST or Query protocol requests to any AWS service API. We create one for you when your account is created — see your access key below.

Your Access Keys

Created	Access Key ID	Secret Access Key	Status
January 27, 2009	003KNR20D32SJNAQ5ET2	Show	Active (Make Inactive)
October 11, 2010	A5ETY8A6DJS2A92NSKA6	Show	Active (Make Inactive)

View Your Deleted Access Keys

For your protection, you should never share your secret access keys with anyone. In addition, industry best practice recommends frequent key rotation.

Learn more about Access Keys

3. Click OK.

   The Add Cloud Account dialog closes. The cloud account displays in the Cloud View panel as a registered cloud account, and it displays all of the EC2 instances that belong to that account.

Update Cloud Account Information

aYou can update the credentials for a previously configured cloud account. For example, if the Access Key ID and Secret Access Key were changed (a new pair was generated and the previous pair was deactivated) using the Amazon Management Console, the AWS account credentials must be manually updated. To update cloud account credential information, select the cloud account in the Cloud View panel that you want to update and click the Update Cloud Account button click the update cloud account toolbar button on the toolbar. Enter the new credentials and click OK. The cloud account information is updated in the Cloud View pane.

Delete a Cloud Account

You can delete a cloud account that you no longer use. To delete a cloud account, select the cloud account in the Cloud View panel that you want to delete and click the Delete Cloud Account button click the delete cloud account toolbar button 🗑 on the toolbar. The cloud account is removed from the list in the Cloud View panel.

Create Full System Scenarios for Hypervisors

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

To create full system scenarios for all platforms except Hyper-V

1. Start Arcserve RHA Manager. Select File, Create, New Scenario or click the New Scenario button on the toolbar.

   The Welcome dialog opens.

2. Click **Create a New Scenario**, type a Scenario Group name or select one from the list and then click **Next**.

   The Select Server and Product Type dialog opens.

3. Select Full System, choose HA or DR and the desired Tasks on Replica. For more information about Tasks on Replica, see Assured Recovery. Click **Next**.

   The Master and Replica Hosts dialog opens.

4. Enter description in the screen as given below and click **Next** when done:

   - **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 one. Enter its port number.

- **Server Type:** Select the virtual platform of the machine that will host the VM, for example, ESX Server.

- **Virtual Platform Hostname/IP and Port:** Specify the physical machine running the virtual machine platform you selected in Server Type or browse to select one. Enter its port number.

- **(Optional) SSL Connection:** Click this option if you wish to specify an SSL port number instead. You may do so for all virtual platform types except Hyper-V.

- **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 RHA 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 while verification completes. If desired, you may install the Arcserve RHA Engine on any server. If errors occur, try resolving them by clicking Verify Again. Contact your security administrator if any RPC Services errors occur.

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

The Volume Setting dialog opens. Arcserve RHA auto-discovers the volumes on the specified Master server.
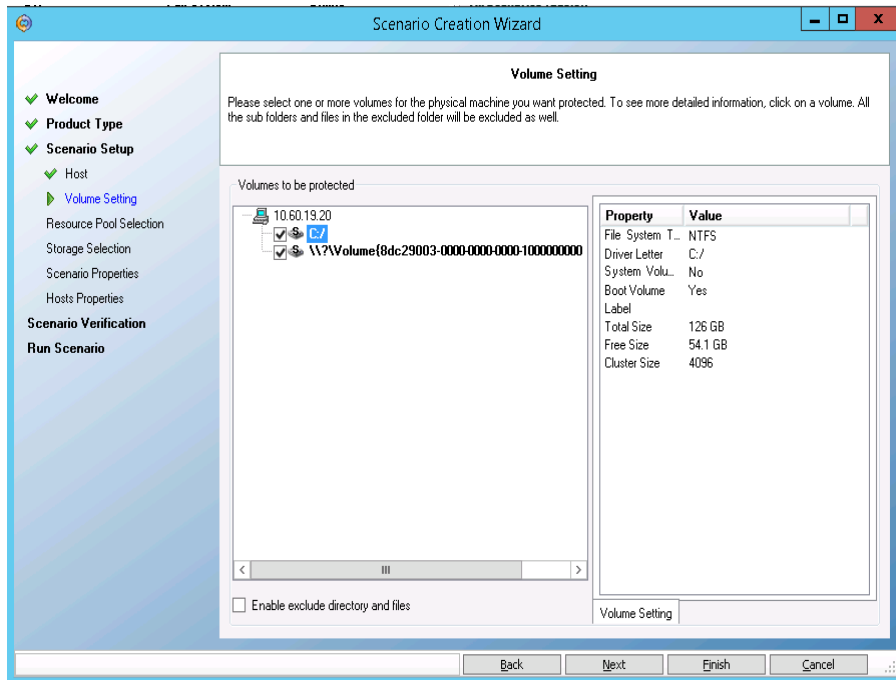
6. Specify the volumes you wish to protect. (Optional) Enable the option, Enable Exclude Directory and Files. This option filters pagefile.sys, hiberfil.sys, System Volume Information, Recycler, and Recycled files and folders by default.

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 should be stored. Enable the option, Allocate and commit space on demand, if desired and click **Next**.

    The Scenario Properties dialog opens.

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

    The Master and Replica Properties dialog opens.

11. Change properties, as desired, and click **Next**. The following information is acquired: CPU number, memory size on VM, adapter information on the physical Master, and the Network Mapping List. You may also change these settings outside of the scenario creation wizard. For more information, see the Arcserve RHA Administration Guide.

    Wait while Arcserve RHA retrieves Switchover Properties.

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

    – Select **Click** to edit physical network mappings.

    The Network Adapter Mapping dialog opens. If there is only one virtual network adapter in both the Master and Replica servers, they are mapped automatically. Click the drop-down in the Replica Network Adapter column and choose the adapter you wish to map to the adapter listed in the Master Network Adapter column.

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

    Customize adapter information -- Choose 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 click Next to continue.

    The Switchover and Reverse Replication Initiation dialog opens.

14. Specify if switchover should be started automatically or manually. Reverse Replication cannot be specified in this scenario.

15. Click **Next**.

    Wait while the Scenario Verification process completes.

    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.

16. Click **Next**.

    The Scenario Run dialog opens.

17. Click **Run Now** if you wish to start synchronization and activate the scenario. For full system scenarios, choose Volume Synchronization. Click Finish to save current settings and run the scenario later.

Next Steps:

■ For Full System-to-ESX server scenarios, you must manually enter the IP
address or your scenarios will fail. For more information, see Create Full Sys-
tem Scenario for Cloud.

■ For Hyper-V, see Use Hyper-V CSV for Full System Scenario.

Use Hyper-V CSV for Full System Scenario

Arcserve Replication and High Availability supports Hyper-V CSV cluster as des-
tination hypervisor for Full System scenario.

Follow these steps:

1. From the Master and Replica Hosts page of the Scenario Creation wizard,
   select **Hyper-V** as **Server Type**.

2. Specify the Hyper-V cluster virtual server name or IP as **Cluster/Hyper-V
   HostName/IP**.

3. From the Storage Selection page, select a CSV mount point for the VM that is
   created for Integrity Testing or Switchover.

4. Follow the wizard and specify the values as required and click **Finish**.
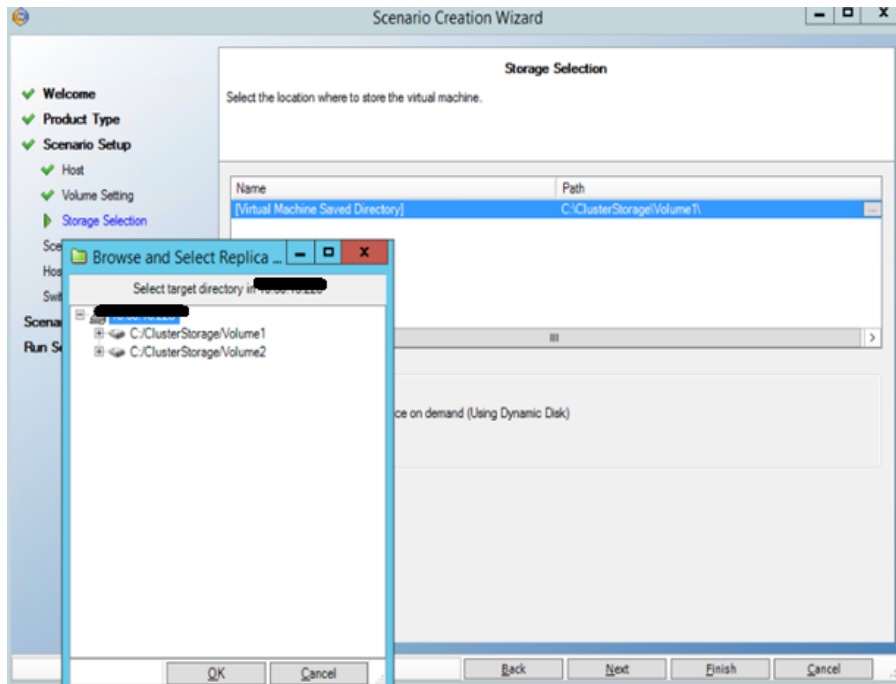
Create Full System Scenario for Cloud

You can create a Full System EC2 High Availability scenario and replicate an entire on-premises Windows system into offline EBS-backed Windows AMIs that will be brought online should the master server fail. This procedure launches a Wizard that guides you through the steps required for High Availability scenario creation. However, properties can also be configured outside of the wizard.
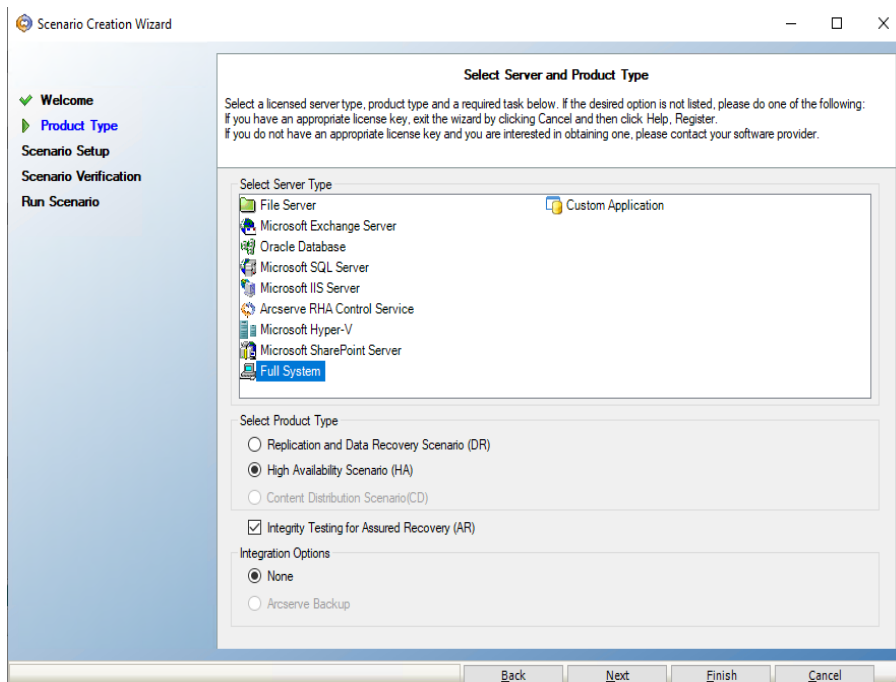
To create a new full system EC2 High Availability Scenario

1. Open the Manager and choose Scenario, New or click the New Scenario button to launch the wizard.

   The Welcome screen opens.

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

   The Select Server and Product Type screen opens.

3. Choose Full System, High Availability Scenario (HA) and then click **Next**.

   The Master and Replica Hosts screen opens.

4. Do the following in the Master and Replica Hosts screen:

   a. Type a Scenario Name and enter the Hostname or IP Address and Port number for the Master server.

   b. Specify Amazon EC2 as the Replica server.

   c. Specify the EC2 replica instance (appliance). Click the [···] button to browse for and select the AWS account and EC2 replica instance (appliance).

   The Cloud Instance Selection dialog opens.

   d. Select the AWS account, cloud replica (appliance), and region and click OK.

   e. Select or clear the Use Control Service DNS check box as needed. Selecting this check box applies the DNS settings from the Control Service server to the EC2 replica instance (appliance) host.

   f. Ensure the Verify Arcserve RHA Engine on Hosts option is enabled (default) and click Next.

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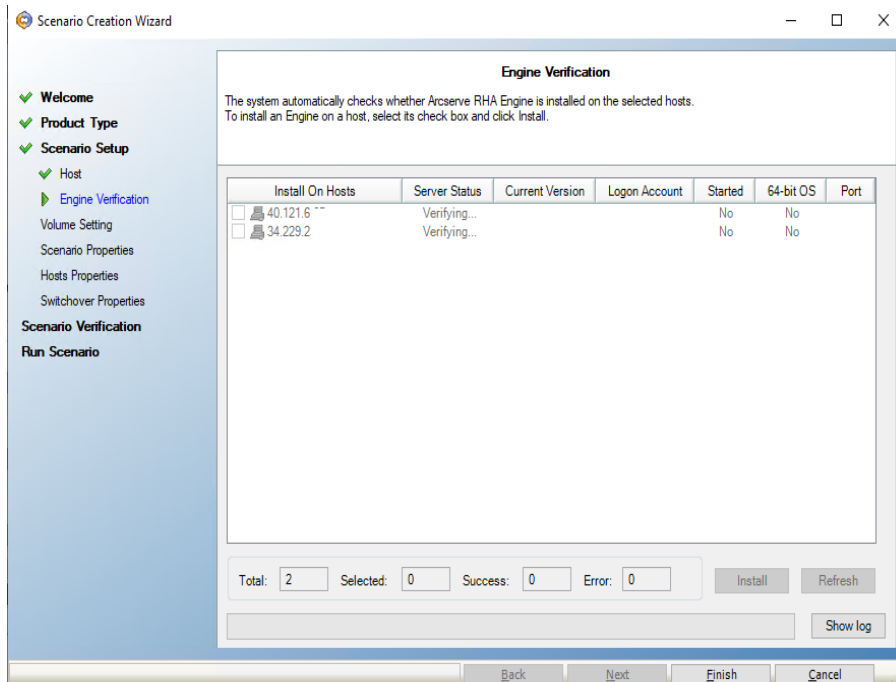
5. Wait for Engine Verification to complete and click **Next**. If required, click Install to upgrade the Engine on one or both servers and Verify Again.

   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 Configuring Scenario Properties.

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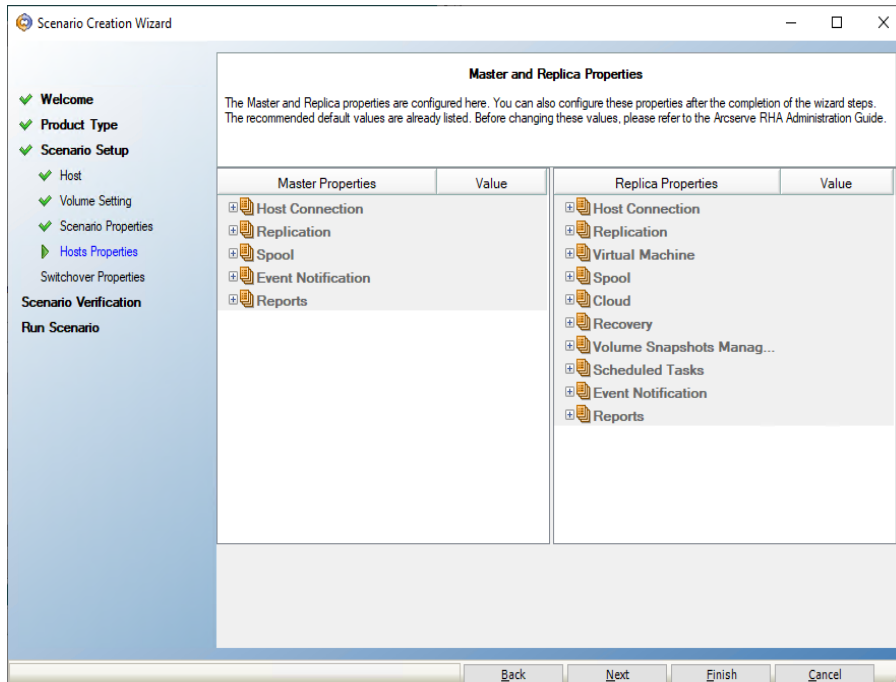
8. In the network mapping dialog launched automatically from Master and Replica properties screen, set the mapping between the Master's NICs and subnets on AWS, security groups, and IP addresses and then click **OK** to save and close the network mapping dialog.
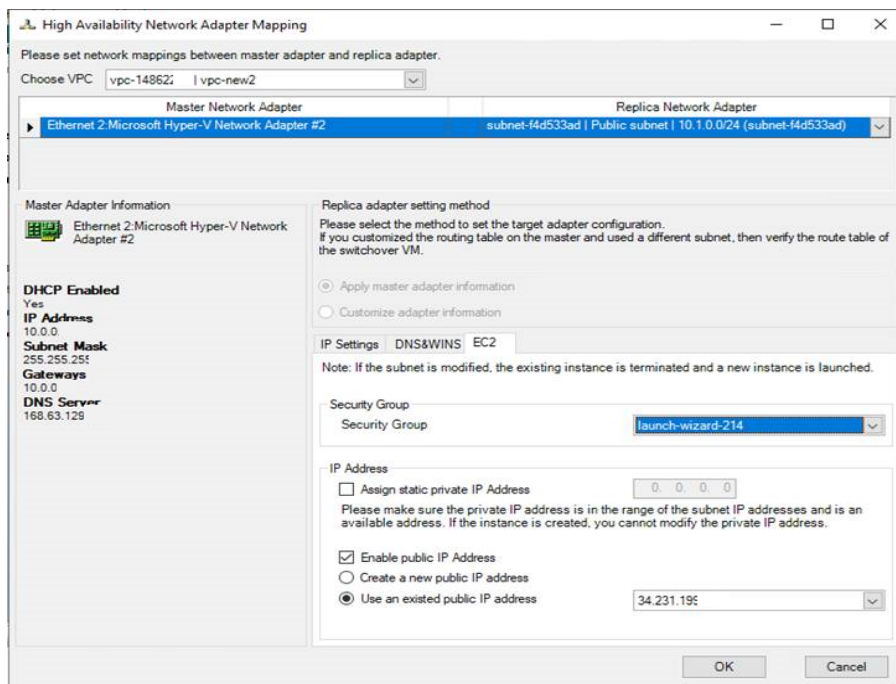
Master and Replica properties apply only to host servers.

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

The Switchover Properties screen opens.
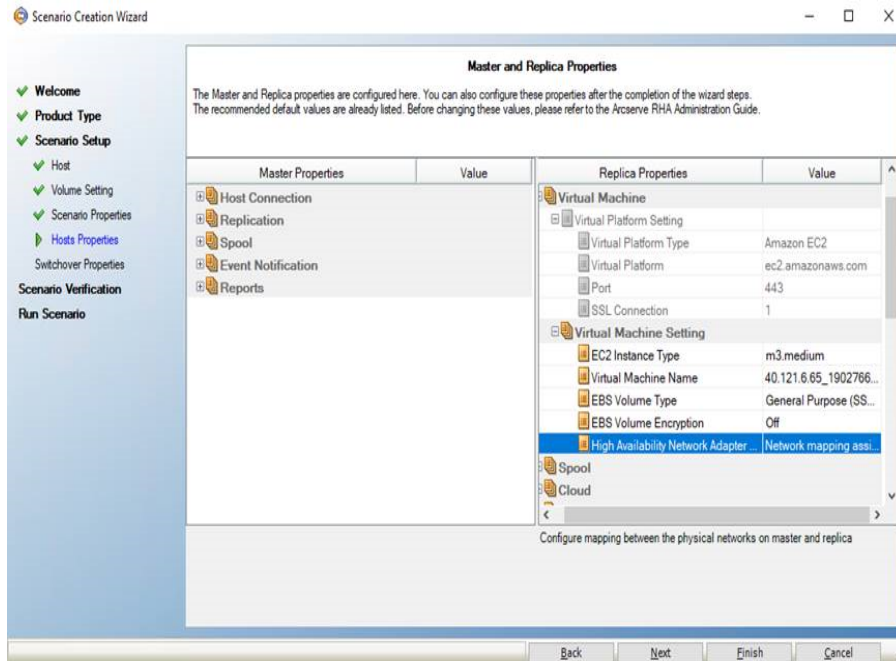
10. Expand the *Switchover* property and enter the Switchover Hostname.

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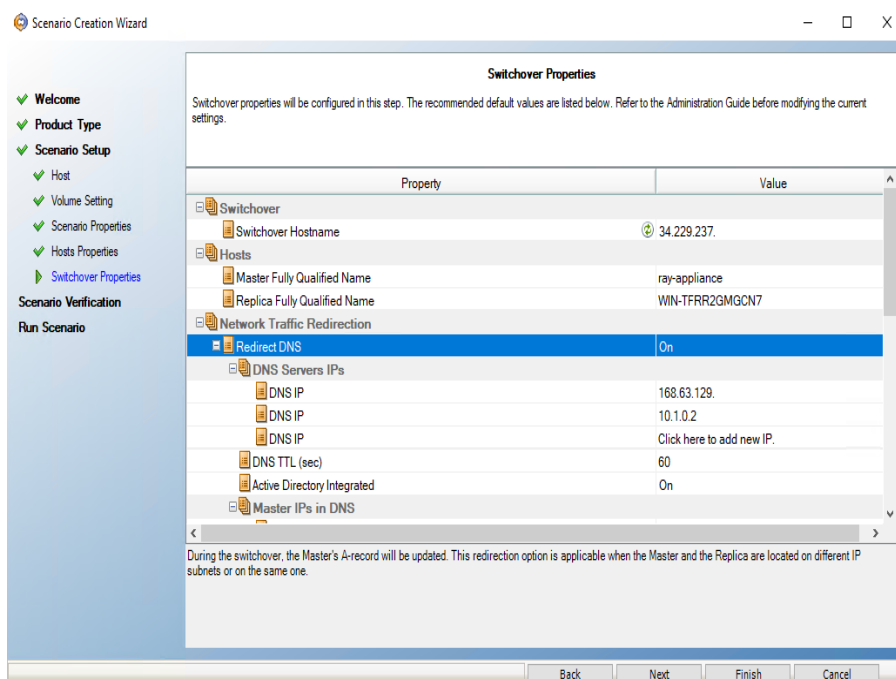
12. Expand the *Network Traffic Redirection* property and specify redirection options, including Redirect DNS, DNS Servers IPs, and Master IPs in DNS.

    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 **OK**.

The Switchover Initiation screen opens.
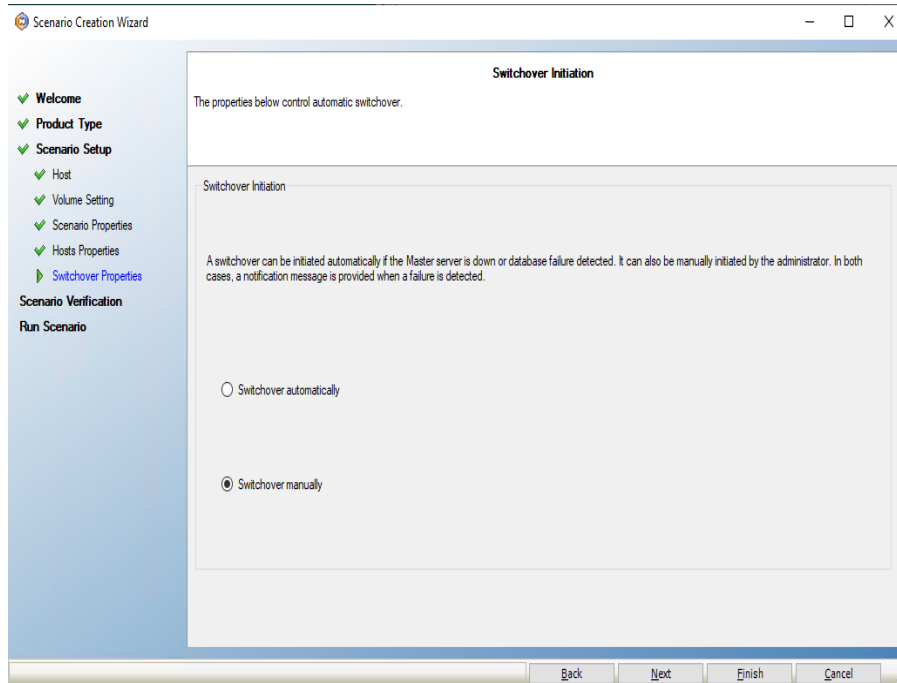
14. Select a switchover option and click **Next**.

Automatic is not recommended. For more information, see Switchover.

Wait for Scenario Verification to complete.

15. If errors or warnings are listed, resolve them before continuing. When ready,
click **Next**.

The Scenario Run screen opens.

16. Click **Run Now** to start synchronization and activate the scenario, or click **Fin-
ish** to run the scenario later.

Redirection Methods

This section contains the following topics:

Redirection Methods for Full System Scenarios

For Full System HA scenarios, Switch computer name and IP redirection are not supported; you may optionally choose DNS redirection. You can also customize the network resource to be used on the virtual machine. Specify the IP, gateway DNS and WINS address on the mapped NIC, if it uses static IP.

During Auto-Discovery, the software obtains only the Master server IP address on the DNS server. If you set Redirect DNS to On, you must manually enter the IP address of the virtual machine on the Replica server or switchover will fail.

To manually enter the virtual machine IP Address on Replica server in DNS

1. Create the full system scenario, as usual or modify an existing scenario from the Arcserve RHA Manager.

2. On the Switchover Properties screen, expand the Network Traffic Redirection properties group.

3. Expand Redirect DNS properties.

4. Expand Virtual Machine IPs on Replica server in DNS.

5. For the IP Address property, click the Value column ("Click here to add new IP").

6. Specify the IP address.

7. Save modified scenario or click Next to continue creating it.

DNS Redirection using the Update DNS Tool

Use this tool to change the DNS A record of the master server to resolve to the IP address of the replica. You use this tool after you start or stop the VM using the Start/Stop VM feature. This redirection is applicable when the master and replica are on the same or different subnets. You can use this tool by running the update_ dns.exe file in the RHA engine installation folder.

Syntax:

```
Update_dns.exe -dns –hostname -hostip –ttl -user-
name -password -keyfile
```

Example: Update the master server address, master.rha.com (199.100.5.1) to that of the DNS server (199.200.2.1).

```
Update_dns.exe -dns 199.100.5.1 –hostname master.rha.com –
hostip 199.200.2.1 -username test -password test
```

Example: Update the local server address to that of DNS servers 199.100.4.1 and 199.100.6.1.

```
Update_dns.exe -dns 199.100.4.1,199.100.6.1
```

Additional Properties for Full System Scenarios

You can manually change the following properties after the scenario creation process is complete:

Virtual Machine Local Directory (Scenario Properties tab)

> In the Replica Root Directory list, double-click the virtual machine local directory to browse and select a new location. Click OK and then click the disk icon to save the modified scenario.

CPU Core (Replica Properties tab)

> On the High Availability Properties tab, expand Virtual Machine settings. Click CPU Core to modify the number.

Memory Size (Replica Properties tab)

> Click Memory Size to modify the value.

Virtual Network Mappings (Scenario Properties tab)

> Besides the Virtual Network Mappings setting, click the entry, "Click to edit Virtual Network Mappings" to display the Physical Network Mapping dialog.

Virtual Machine Name (Replica Properties tab)

> You may change the Virtual Machine Name, if desired. By default, the Master hostname is used.

Save the modified scenario when you are done modifying these settings.

Configure Additional Properties in Full System-to-ESX Scenarios

When configuring full system scenarios on ESX servers, you must manually enter an IP address on the Replica server to prevent scenarios from failing to run.

To manually enter a virtual machine IP address on the Replica server

1. Configure the scenario as described in the Create Full System Scenarios topic.

2. When you reach the Switchover Properties screen, expand the Network Traffic Redirection properties.

3. Set the following property to On: Redirect DNS.

4. Enter the DNS IP address.

5. Expand Master IPs in DNS. Click the value column and enter the IP address for the Master host.

6. Expand Virtual Machine IPs on Replica server in DNS.

7. Select Click here to add new IP and specify the IP address of the virtual machine on the Replica server to be used in case a switchover or failover is triggered.

Configure Additional Properties in Full System Cloud Scenarios

For full system Cloud scenarios, you can specify additional properties for Cloud and Virtual Machine as required for your environment.

To configure additional full system Cloud properties, configure the scenario as described in Create a New Full System Cloud High Availability Scenario. When you reach the Master and Replica Properties screen, expand the Cloud and Virtual Machine properties and work with the following options:

Cloud Properties:

Cloud Provider

Identifies the name of the cloud service running the selected cloud instance. This is a read-only property.

Cloud Account ID

Identifies the account ID of the AWS account. This is a read-only property.

Cloud Region

Identifies the VPC region of the AWS account. This is a read-only property.

Cloud Instance ID

Identifies the ID of the cloud instance. This is a read-only property.

Cleanup Cloud Resources When Remove Scenario

Lets you specify whether to clean up cloud resources when a scenario is removed. For Full System EC2 Data Replication or High Availability scenarios, several cloud resources can be used such as the cloud instance used for failover, volumes, and snapshots. If these cloud resources are useless after a scenario is removed, you can enable this option to clean up these resources. This option is disabled by default.

Shutdown Instance on scenario stop

Lets you specify whether to shut down the replica instance automatically on scenario stop. This option is disabled by default, which means that the replica instance will not be automatically stopped if the scenario is stopped.

Virtual Machine Properties:

Virtual Platform Setting

Lets you review the settings for the following read-only properties:

Virtual Platform Type

Identifies the virtual platform type of the cloud account.

Virtual Platform

Identifies the virtual platform server of the cloud account.

Port

Identifies the port number used to connect to the virtual machine.

SSL Connection

Identifies whether the SSL (secure socket layer) connection is on or off.

Virtual Machine Setting

Lets you define the following properties:

EC2 Instance Type

Lets you specify the size assigned to the EC2 instance on the virtual machine. You can specify the appropriate instance type based on the operating system of the master and the requirements of your environment. Instance type options include:

- Small Instance

- Large Instance

- Extra Large Instance

- High-Memory Extra Large Instance

- High-Memory Double Extra Large Instance

- High-Memory Quadruple Extra Large Instance

- High-CPU Medium Instance

- High-CPU Extra Large Instance

Available options are related to the master's platform. If the master is a 32-bit operating system, only the Small Instance and High-CPU Medium Instance are available. If the master is a 64-bit operating system, then all of the other types are available.

Virtual Machine Name

Specifies the name of the virtual machine managed on the virtual platform server.

Virtualization Hypervisor Login Setting Tool

Use this tool to set up the login credential information for a specific virtualization hypervisor on an existing full system scenario. Each login credential record is uniquely identified by its hostname/IP and the port. To use this tool, run the ws_p2v_log_in_setting.exe file from the RHA engine installation folder on the appliance server and follow the instructions.

Managing Full System Scenarios

This section contains the following topics:

Running a Full System Scenario

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, 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 Master and Replica and send only difference, while Volume synchronization sends all data from Master to Replica. For resynchronization, Block synchronization is used by default.

- Selecting Linux as Choosing synchronization method:

    - For initial synchronization, recommend File synchronization, and select checkbox of **Ignore same size/time files**. This method uses least time to complete data comparison and start sending data.

    - For subsequent synchronizations, make sure to clear checkbox 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.

Operations on a Virtual Machine

You can use available operations to manage a virtual machine. These operations lets you start, stop, and delete all VM resources.

This section contains the following topics:

- [Start or Stop a Virtual Machine](#)
- [Delete Virtual Machine Resources](#)

Start or Stop a Virtual Machine

Use this operation to start or stop a virtual machine from its latest system status or from a bookmark. You can start or stop a virtual machine after you create a scenario and synchronize the master and replica. Use this feature when the scenario is not running. This feature is available for Full System DR and HA scenarios. The Start/Stop is a toggle menu item.

Follow these steps:

1. Click Tools, Start/Stop VM.

   The Set up the virtual machine dialog opens.

2. Select a bookmark and an option to set the network for the newly created virtual machine.

   Consider the following points before you use this operation:

   - If you perform any of these functions: Switchover, Failover, Start VM, Recover Active Replica server, or BMR Restore, RHA automatically creates a bookmark, "bookmark for last state of the scenario". This bookmark is to keep the last data state of the scenario before the scenario stopped or performed switchover. This bookmark is internally deleted when you run the forward scenario next time.

     You can go back to the last scenario state any time.

   - RHA keeps the latest system status before you performed the Start VM operation. When you start the VM again, you can find a bookmark, "Latest System Status of bookmark [bookmark name]" in the bookmark list.

   - When you select any other bookmark to start the VM after the VM is stopped, all data changes in latest system status is lost.

This operation creates and starts a new virtual machine on the appliance. Depending on the platform, virtual machine tools such as VMware tools, Integration Service, or XenServer tools are also installed on the virtual machine. Log in and check if data is accurate and various services are working.

Important: After the VM is started, do not use virtualization platform management tools (such as VMware vSphere Client, Hyper-V Manager, or XenCenter) to create a VM snapshot. This results in an unexpected error.

Delete Virtual Machine Resources

When you run a full system scenario, some temporary resources are created such as disk files, snapshots, and other files. This operation lets you delete these resources and is available when the scenario is not running.

Follow these steps:

1. Click Tools, Delete all VM Resources.

   A warning appears that all protected data will be deleted.

2. Select Yes to clean up all VM resources.

   Note: If the VM is already running, the operation shuts down the VM first and then removes all VM resources.

All created image as well as disk files and snapshots are deleted.

Perform Full System Assured Recovery Testing

You can perform Assured Recovery Testing for Full System HA scenarios manually or automatically.

During AR Testing, the software suspends journal application, creates a VM with the virtual hard disk file and a snapshot to save possible changes, then starts the VM. If you chose automatic AR testing, VMware tools are installed. Wait for the software to stop the test. If you chose manual, you'll need to stop the AR test manually.

Once stopped, the software resumes applying journal changes.

For more information, see the section, Testing Assured Recovery and Managing VSS Snapshots, in the Arcserve RHA Administration Guide.

Recover Active Server for Full System Scenarios

The Recover Active Server process lets you forcibly make the Master or Replica server the active server without completing the data synchronization process. This action is necessary in cases where you do not want to synchronize data. For example, if switchover occurred but no data was changed on the Replica server. In this case, you can even have newer data on the Master server making it undesirable to synchronize data from the Replica to the Master server.

To use this option, make sure that the scenario is stopped, and select Recover Active Server from the Tools menu. Select either Make Master Active or Make Replica Active depending on which server you want to make active. If you make the Master active, the process stops and unregisters the virtual machine (that the appliance created). If you make the Replica active, the appliance registers and starts the virtual machine.

Note: When the platform is Amazon EC2, the appliance would stop the VM without unregistering. Register or unregister the VM separately.

Important! While this option is the right choice in many situations, use it with caution. When used improperly data loss can occur. Usually, RHA does not allow switching from one host to another until all data is synchronized. When using Recover Active Server, RHA is forcing users to one server or the other with no regard as to which server has the correct data set. Thus, as an administrator, manually make sure that the server you are making active has the most up-to-date data set.

If the Recover Active Server method does not solve the problem, you can manually recover a server. For more information, refer to the section, Recovering Servers.

The following scenarios are some examples where you can use the recover active server process.

Scenario 1: Making the Master server active after a switchover or failover

After switchover or failover, the Master server becomes the standby server, and the Replica (virtual machine the appliance created) the active server. Now if you do not want to make the Replica as the active server, then you can use this feature and can make the master active.

Follow these steps:

1. Click Tools, Recover Active Server.

    The Recover Active Server dialog opens.

2. Click Make Master Active.

3. The appliance unregisters the virtual machine.

You can run the forward scenario again.

Scenario 2: Making the Replica server active after synchronization

You created a scenario and just synchronized the Master and Replica. In this case, the master is active and the replica is inactive. In some cases, you want to make the replica active, for example, if you want to check whether the replica (virtual machine) is available and working as expected.

Follow these steps:

1. Click Tools, Recover Active Server.

    The Recover Active Server dialog opens.

2. Click Make Replica Active.

   The appliance registers and starts the virtual machine.

Restoring Full Systems

This section contains the following topics:

Restore Files and Directories

As an Administrator, you are responsible for ensuring that data is replicated and failover happens in case the Master server fails. On a failover or switchover, you can recover the entire data to an active server from the Replica.

The following diagram illustrates how the recovery process restores data to an active server.
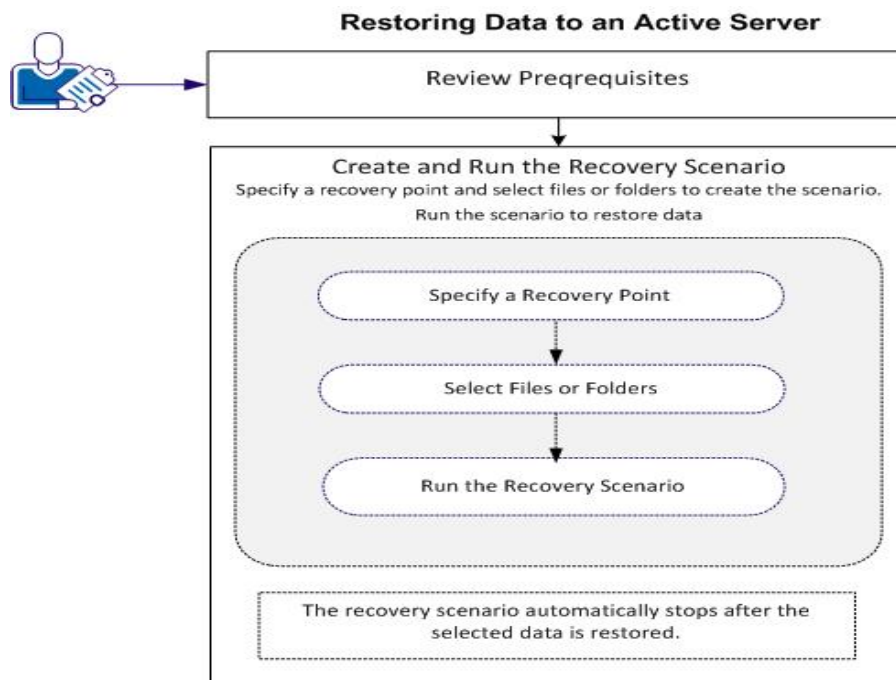
Perform the following tasks to restore data:

- Review Prerequisites
- Create and Run the Recovery Scenario

Review Prerequisites

Before you can restore data to an active server, consider the following points:

- Start recovery only when the full system scenario is stopped or a switchover-/failover is triggered.

- Restore data to a similar machine. Install the same version of the operating system and applications as much as possible.

- Build the new Master first and then launch the recovery process.

- For an FSP scenario, do not manually stop the virtual machine that performed a switchover or failover before you start the Master.

- Stop critical services before launching the recovery process, such as Database services and Exchange server services. When the services are running, some applications lock their files and cannot be opened during the recovery process. Start these services again after the recovery.

Create and Run the Recovery Scenario

Review the prerequisites carefully before you launch the recovery. Use the Data Recovery wizard to restore data from the Replica.

Follow these steps:

1. Log into Arcserve RHA as an Administrator.

2. From the Quick Start pane, click Scenario Management to open the Arcserve RHA Manager.

3. Launch the Data Recovery Wizard from the Manager screen.

4. Enter the credentials, when prompted.

5. Select a recovery point on the Recovery Point Selection screen. For example, click Latest System Status and then click **Next**.

   The virtual machine shuts down.

6. On the Master Root Directories screen, expand the source host and then, click or clear check boxes to include or exclude folders from the list. If you wish, you can apply a file filter. Click **Next**.

   Important: Do not select the C:\Windows folder as it can lead to certain conflicts later, especially if the operating system versions are different. If you do select the folder, then system registry files such as Sam, Security, Software, and Default are not restored.

   Note: We recommend skipping the RHA Engine folder (C:\Program Files\CA\ARCserve RHA\Engine) when you are not sure about the engine versions.
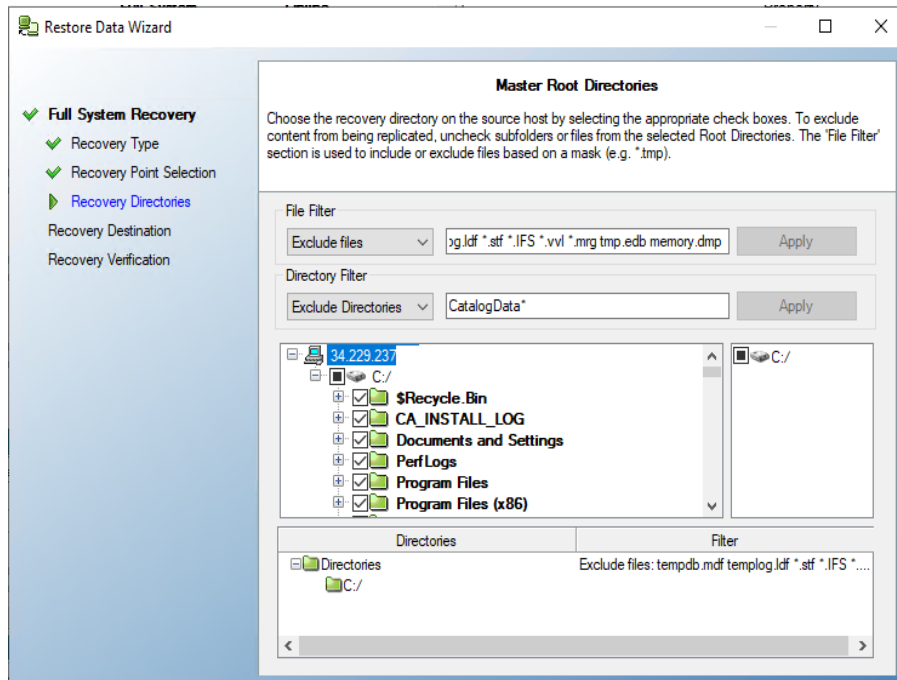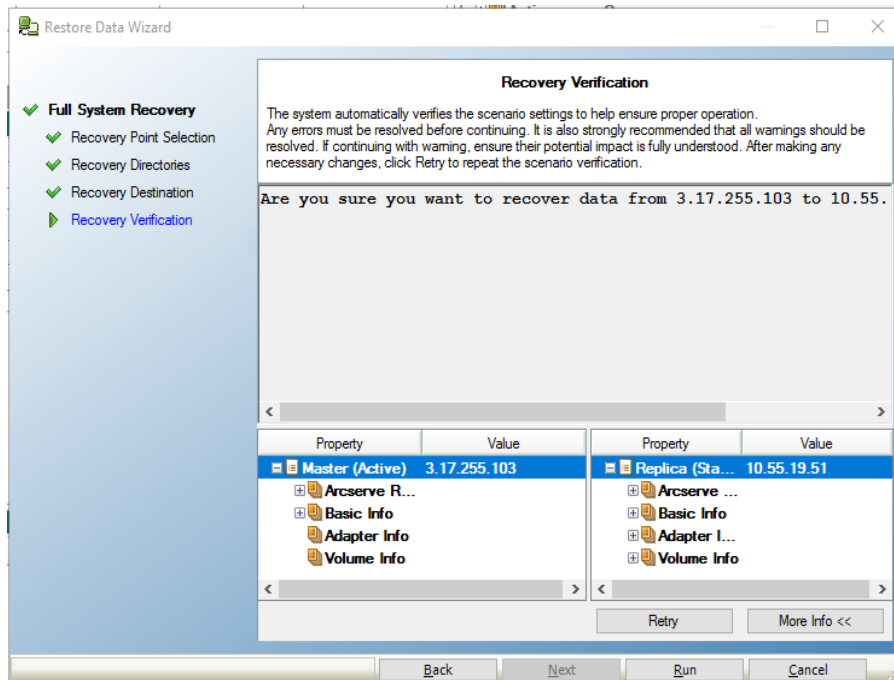
7. On the **Recovery Destination** screen, enter the required credentials.
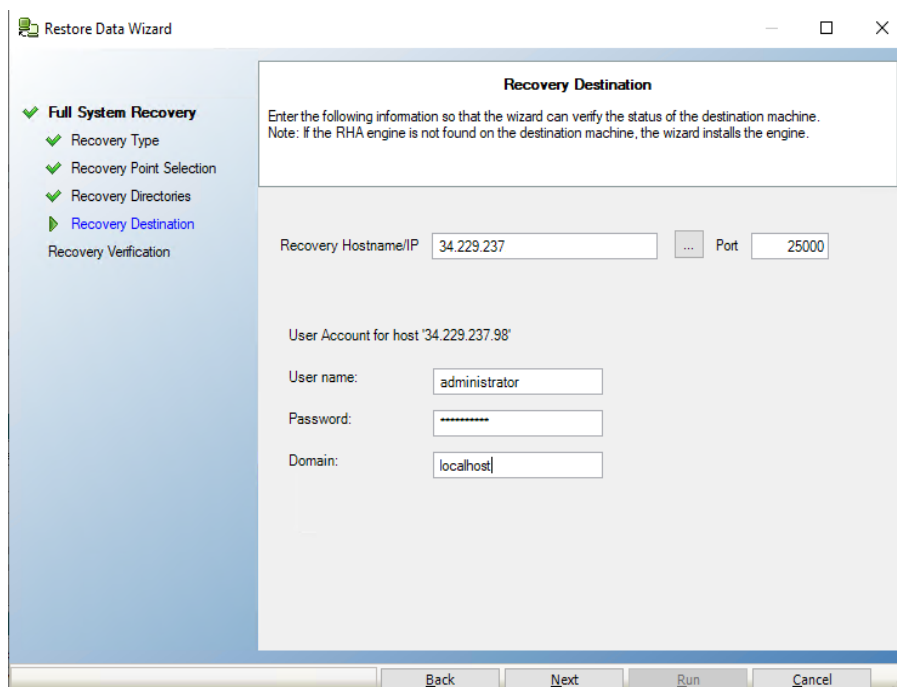
8. Click **Run**.

   Wait while the verification completes.

9. When the Recovery Verification screen opens, review the information or click More Info to see more details. Click Finish.

   A new scenario, Recovery_<Scenario Name>, is added to the list on the Manager screen. View the statistics for progress. The new scenario automatically stops once the selected data is recovered. The system reboots if necessary.

# Restoring Data to a Bare Metal from a Bookmark

As an Administrator, you are responsible for ensuring that data is restored in case the Master server fails.

Arcserve RHA lets you restore data to a bare metal machine. This feature not only restores data but also builds the bare metal machine by installing the operating system, applications, and other necessary components. After you complete the process, the bare metal machine is ready to take over as the Master server.

A bare metal recovery provides the following benefits:

- Builds a machine exactly similar to the Master including operating system, applications, and data

- Eliminates manual setting up of a machine

- Recovers data to a dissimilar hardware

The following diagram illustrates how you can build and restore data to a bare metal machine from the Replica.
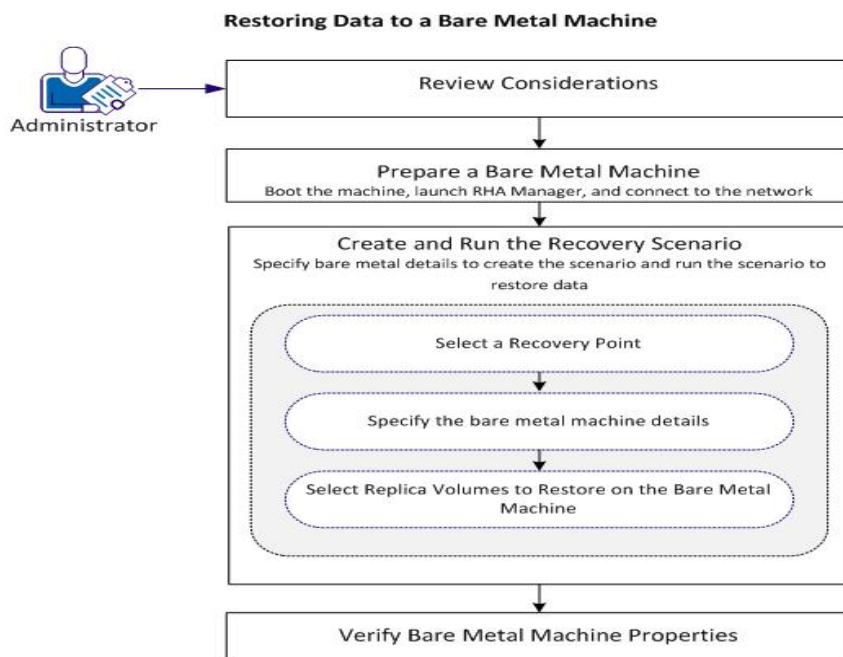
Perform the following tasks to restore data:

- Review Prerequisites

- Prepare a Bare Metal Machine

- Create and Run the Recovery Scenario

- Verify Bare Metal Machine Properties

Review Prerequisites

Before you restore data to a bare metal machine, consider the following points:

- Applies only to Full System Scenarios

- Supports only basic disks, no support for dynamic disks.

- Upgrade considerations: If you upgrade the RHA engine from previous releases to Service Pack 16.0.02, you must synchronize the Master and Replica at least once to complete the upgrade.

Prepare a Bare Metal Machine

Before you create a recovery scenario, prepare a bare metal machine on which you want to restore data. In this process, boot the machine with the RHA BMR CD to start the machine and launch the RHA engine. An IP address is assigned to the machine. Specify this IP address while creating the recovery scenario.

Follow these steps:

1. Insert the RHA BMR CD and boot the computer.

2. Select Arcserve RHA BMR to boot the system.

3. Select the language of your choice and click Next.

   The RHA CD detects network adapters and disks on the bare metal machine.

4. (Optional) If the RHA CD is unable to detect network adapters and disks, click appropriate links on the left panel to install them.

The RHA engine is launched and the machine is assigned an IP address.

Create and Run the Recovery Scenario

After you prepare the bare metal machine, create a recovery scenario with the bare metal machine as the Replica. Creating this scenario lets you specify the Master and Replica (bare metal machine) details and configuration properties. When you run the scenario, data is restored to the bare metal machine.

Specify the following details on Restore Data Wizard screens to create the scenario:

- IP address of the bare metal machine.

- Volumes--Select the volumes on the Master that you want to restore. You can also manually resize the volume to a different size on the bare metal machine.

    Note: You can exclude volumes that you do not want to restore.

When you run this scenario, data is restored to the bare metal machine.

Follow these steps

1. Log in to Arcserve RHA as an Administrator.

2. From the Quick Start pane, click Scenario Management to open the Arcserve RHA Manager.

3. Select the full system scenario and click Restore Data.

    The Restore Data Wizard opens.

4. Follow the instructions on wizard screens to create and run the recovery scenario.

Data is restored to the bare metal machine.

Verify Bare Metal Machine Properties

After the data is restored, the bare metal machine is rebooted. Now this machine has the same name, operating system, applications, and data components as that of the original Master server. Verify these details by checking operating systems and other application properties.

Note: When the machine is rebooted, some drivers could be missing. Manually install and reconfigure these drivers to work for any hardware changes.

Restoring Data to a Bare Metal from the Running DR VM after Switchover

As a System Administrator you are responsible for ensuring that data is replicated and failover happens when a Master server does not respond. In such a case, you create a recovery scenario to restore data from its Replica. You have the option of restoring data to a bare metal machine. The bare metal recovery feature not only restores data but also builds the bare metal machine by installing the operating system, applications, and other necessary components.

A bare metal recovery provides the following benefits:

- Builds a machine exactly similar to the Master before restoring data

- Recovers data even to a dissimilar hardware

- Recovers data on a volume level

The following diagram illustrates restoring data to a bare metal machine using Reverse Replication.
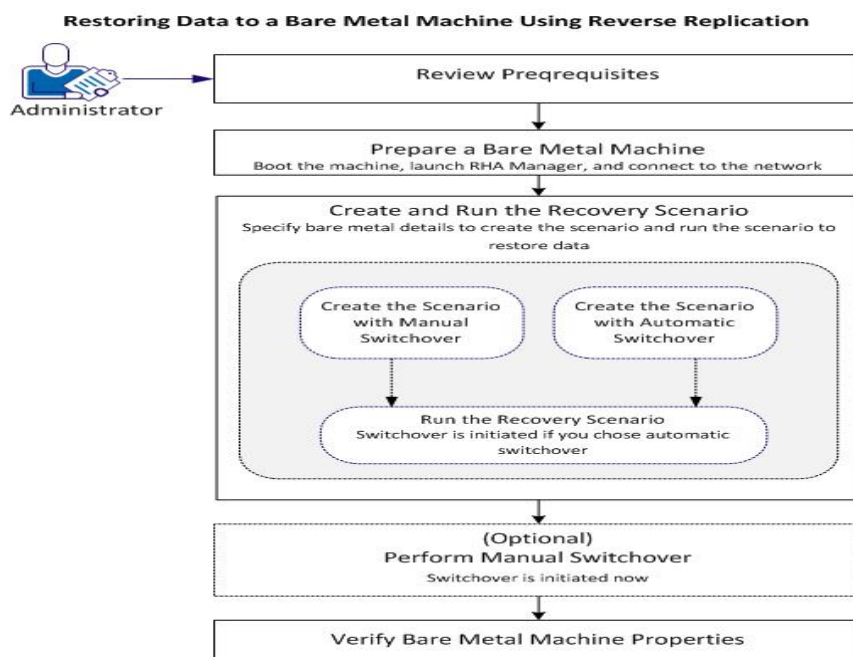
Perform the following tasks to restore data:

- Review Prerequisites

- Prepare a Bare Metal Machine

- Create and Run the Recovery Scenario

- ▪ [(Optional) Perform a Manual Switchover](#)
- ▪ [Verify the Bare Metal Machine Properties](#)

Review Prerequisites

Before you restore data to a bare metal machine, consider the following points:

- Applies only to full system scenarios that have performed a failover or switchover.

- Supports basic disks and does not support dynamic disks.

- Upgrade considerations: If you upgrade the RHA engine from previous releases to Service Pack 16.0.02, you must synchronize the Master and Replica at least once to complete the upgrade.

Prepare a Bare Metal Machine

Before you create a recovery scenario, prepare a bare metal machine on which you want to restore data. Boot the machine with the RHA BMR CD to start the machine and launch the RHA engine. An IP address is assigned to the machine. Specify this IP address while creating the recovery scenario.

Follow these steps:

1. Insert the RHA BMR CD and boot the computer.

2. Select Arcserve RHA BMR to boot the system.

3. Select the language of your choice and click Next.

   The RHA CD detects network adapters and disks on the bare metal machine.

4. (Optional) If the RHA CD is unable to detect network adapters and disks, click appropriate links on the left panel to install them.

The RHA engine starts and an IP address is assigned to the machine.

Create and Run the Recovery Scenario

Now the bare metal machine is in the network with a unique IP address. To restore data, create a recovery scenario with this bare metal machine as the Replica. This way, you can restore data from the virtual machine to the bare metal machine.

Specify the following details on Restore Data Wizard screens to create the scenario:

- IP address of the bare metal machine.

- Volumes--Select the volumes on the Master that you want to restore. You can also manually resize the volume to a different size on the bare metal machine.

  Note: You can exclude volumes that you do not want to restore.

- Network Adapters—Select the Replica network adapter that you want to map to the Master network adapter. For servers in a workgroup, use Redirect DNS. To use Redirect DNS, specify domain administrator credentials.

- Switchover type--Automatic or Manual.

When you run this scenario, data is restored to the bare metal machine. Depending on the switchover type, either the switchover process is automatically triggered or you manually initiate the process.

Follow these steps

1. Log in to Arcserve RHA as an Administrator.

2. From the Quick Start pane, click Scenario Management to open the Arcserve RHA Manager.

3. Select the full system scenario that performed switchover or failover and click Run.

   The Restore Data Wizard opens.

4. Follow the instructions on wizard screens to create and run the recovery scenario.

   Data is restored to the bare metal machine. If you selected automatic switchover, the switchover process is initiated and the bare metal machine is ready to take over as the Master server.

   Note: If you selected the manual switchover, manually initiate the switchover process. See (Optional) Perform a Manual Switchover.

The switchover process performs the following tasks:

- Moves the resources like IPs, DNS from the Master server to the bare metal machine.

- Performs driver injection on the bare metal machine.

- Shuts down the Master.

- Reboots the bare metal machine.

  Note: If you stop a scenario, then above tasks are not executed and bare metal machine is not recovered completely.

(Optional) Perform a Manual Switchover

If you chose manual switchover, data is synchronized after you run the recovery scenario. To perform the switchover, select the scenario and manually initiate the switchover process.

Follow these steps

1. Open Arcserve RHA Manager and select the recovery scenario from the Scenario pane. Verify that the scenario is running.

2. Click Perform Switchover.

   A confirmation message appears.

3. Click Yes.

   A switchover process is initiated and the Master server is disconnected. The bare metal machine is rebooted.

Now, the bare metal machine is ready to take over as the Master server.

Verify Bare Metal Machine Properties

After the switchover process is complete, verify that the machine name, operating system, applications, and data components are same as that of the original Master server.

Note: When the machine is rebooted, some drivers may be missing. Manually install these drivers.

Now if you want to run the original forward scenario, perform the Recovering Active Server process to set the recovered Master as the Active Server. See Recover Active Server.