Microsoft SharePoint Server Operation Guide

Arcserve® Continuous Availability

arcserve®

Legal Notices

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

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

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

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

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

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

The manufacturer of this Documentation is Arcserve.

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

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

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 Continuous Availability 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 Continuous Availability 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 you can implement a Arcserve RHA solution for Microsoft SharePoint Server. It is essential that you have the appropriate resources and permissions to carry out each task.

Related Documentation

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

- Bookshelf
- Release Notes

Server Requirements

To implement Arcserve Continuous Availability, refer to the appropriate list of requirements, depending on the server type you selected. These components are licensed separately. If you do not have the license required to access support for a specific server type, contact Technical Support.

This section contains the following topics:

- Base Configuration
- Microsoft SharePoint Server Configuration Requirements
- Microsoft SharePoint Deployment Requirements
- Log On Account Conditions
- Register Arcserve RHA Licenses

Base Configuration

Base Configuration

- Two servers running supported Windows Server with the same level of service packs and hot fixes installed.

Note: For a complete list of supported operating systems and applications, see the Arcserve Continuous Availability Release Notes.

- All IP addresses are statically assigned (DHCP-assigned IP addresses on the Master or Replica server are not supported)

- The protected server is not a domain controller or DNS server.

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

Microsoft SharePoint Server Configuration Requirements

The system requirements Arcserve HA for Microsoft SharePoint Server 2007 Standalone or Farm deployment are as follows:

- You must have two servers (production server and stand-by server) with Microsoft SQL 2005 SP3 or Microsoft SQL 2008 SP2 or later required for some advanced features; installed on both servers.

- Both servers should have the same SQL version, service packs, and hot fixes installed.

- Both servers should hold identical SQL Server instances-default or named.

- Both servers must have the same SharePoint version, service packs, and hot fixes installed.

- The full path to the default system database of each instance should be identical on both servers. Drive letters containing database files should be identical on both servers.

- You must verify that the port defined in the Network Configuration TCP/IP properties of the SQL instances is assigned statically and is identical on both master and replica servers.

- If you are installing SharePoint with SQL Server 2005 Express Edition, you must enable TCP/IP protocol for that SQL instance (that is, OfficeServers) on both Master and Replica servers.

- Stop SQL DB on replica server before you run the scenario.

For a stand-alone SharePoint server, the Local Service account is configured by default with following accounts:

- Service Account for Office SharePoint Search Server

- Service Account and Content Database Account for Windows SharePoint Services Help Search

You should reconfigure the accounts on the Central Administration website with a domain user account before you create a SharePoint HA scenario.

Note: You should not configure these accounts with Network Service, as this may prevent the services from functioning properly after failover.

Microsoft SharePoint Deployment Requirements

At present the following typical SharePoint deployments are supported by Arcserve Continuous Availability for Microsoft SharePoint Server:

Standalone

- Installation type: Stand-alone

- All components (Web Front End, Application, database) are on a single server

- Cannot add another server to create a server farm

- The SharePoint 2007 database is local SQL Server 2005 Express Edition. The SharePoint 2010 database is local SQL Server 2008 Express Edition.

Note: Standalone deployment requires special Replica configuration. For more information, see the topic, Prepare the Replica Server for Standalone Deployment.

Server Farm (all-in-one)

- Installation type: Complete

- All components (Web Front End, Application, database) are on a single server

- Can add other servers to this server farm

- The SharePoint database is local SQL Server 2005/2008

Server Farm (distributed)

- SharePoint Server 2007 Installation type:

  – WFE server: Web Front End

  – Application server: Complete

- SharePoint Server 2010 Installation type:

  – Application Server: Complete

- Each component (Web Front End, Application or database) can have its own dedicated server (i.e., a typical medium farm includes two servers, one for WFE + Application roles and another for database role.)

- All the servers (Web Front End and Application) can be protected by SharePoint Replication or HA scenario.

- Can add other servers to this server farm

- The SharePoint database is local or remote SQL Server 2005/2008

Log On Account Conditions

The Arcserve Continuous Availability 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.

- If the account does not have built-in administrator permissions on all SQL Server instances, add appropriate permissions.

- The account must be able to modify the SQL Master and Replica DNS A-Record.

Important! For a SharePoint Farm deployment, the SharePoint server's Farm Admin account must employ the same log on account conditions.

Register Arcserve Continuous Availability Licenses

The Arcserve Continuous Availability 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 Continuous Availability 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 Continuous Availability 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 Continuous Availability 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 Continuous Availability Manager according to your license permissions.

Chapter 2: Managing Replication and High Availability Scenarios

This section describes how to create and use high availability scenarios.

This section contains the following topics:

Prepare the SharePoint Replica Server

Before running a scenario, you need to prepare the Replica server. Ensure the following are installed on the Replica server to ensure it meets the infrastructure requirements described in the previous chapter.

- Install SQL Server 2005/2008 on the Replica server if the production server is a SharePoint Farm all-in-one deployment.

Note: Do not install SQL Server if the production server is a SharePoint standalone or SharePoint Farm distributed deployment. For more information on SharePoint Server deployments, see Microsoft SharePoint Deployment Requirements.

- SharePoint Server 2007 SP2 or 2010, with identical configurations as the Master server.

Note: Do not configure SharePoint after installation.

- Arcserve Continuous Availability Engine

Next Steps:

If the production server is a SharePoint standalone deployment, there is additional configuration required. For more information, see Prepare the Replica for Standalone Deployment.

This section contains the following topics:

- Prepare the Replica for Standalone Deployment
- Third-Party Web Parts for SharePoint
- Arcserve RHA SharePoint COM+ Service

Prepare the Replica for Standalone Deployment

SharePoint Servers store **configuration** and **content** data. To protect both kinds of data, perform the Replica Server configuration procedure before you run any high availability scenarios in a SharePoint Server standalone deployment. The procedure ensures the Replica is configured identically to the Master.

Standalone deployments are not scalable and cannot join other SharePoint farms. The Replica server is completely independent from the Master. Arcserve Continuous Availability automatically synchronizes and replicates the content database on the Master. You must maintain and customize the configuration and administration content database on the Replica so that it is identical with the one on the Master before you run an HA scenario.
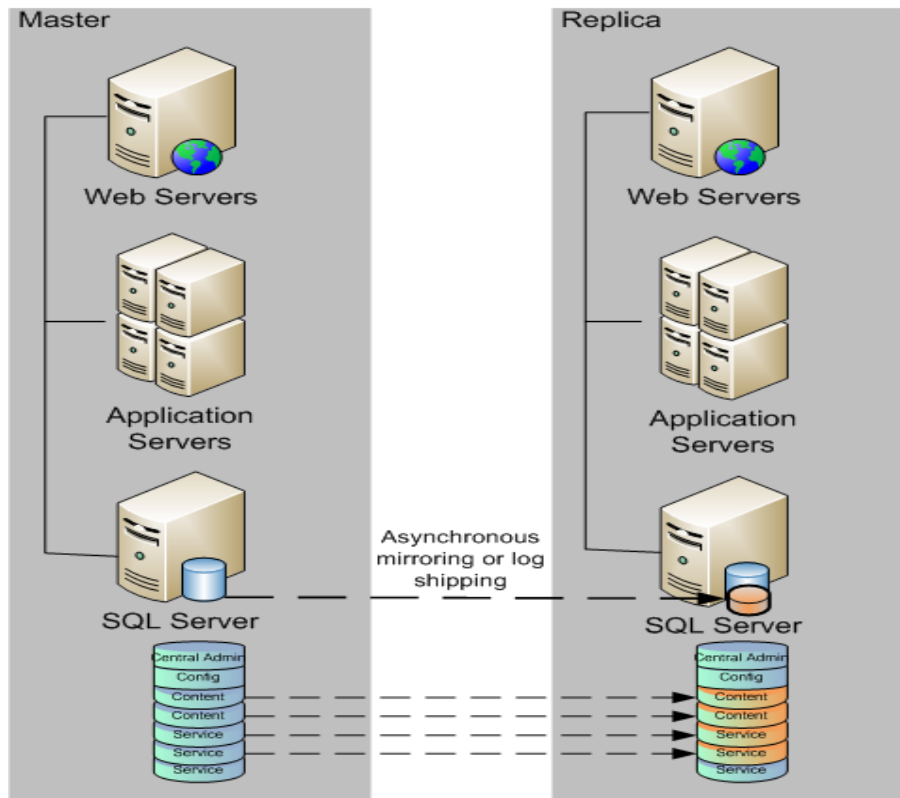
Note: The configuration and administration content databases are not displayed in Auto-Discovery when creating HA scenarios for SharePoint Server standalone deployment. Only existing web application databases can be discovered and replicated in Assured Recovery scenarios.

Next Steps

Use the SharePoint Products Configuration Wizard to Prepare the Replica

Use the SharePoint Products Configuration Wizard to Prepare the Replica

The following procedure is the recommended method for configuring the Replica server in SharePoint Server standalone deployments. The SharePoint Products Configuration wizard configures the services and service applications automatically on the Replica server and creates a default web application on port 80. Before you begin, go to Microsoft TechNet to read information about how to change the administrative site port. You should also obtain the following information:

- The alternate access mapping and administrative site port from the Master server

- The display names, headers and ports for all web applications created on the Master server

- The names of the content databases for all web applications created on the Master server

Note: Do not perform the "disconnect from farm" procedure to reconfigure SharePoint servers auto-configured as Replicas for use in new Arcserve Continuous Availability scenarios. Disconnecting an auto-configured Replica can also cause the Master server in the old scenario to disconnect from the farm. Instead, delete the following registry key:

- For SharePoint Server 2007: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\12.0\Secure\ConfigDB

- For SharePoint Server 2010: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\14.0\Secure\ConfigDB

After you delete the registry key, you may safely perform the disconnect from farm procedure using the Configuration Wizard.

To use the SharePoint Products Configuration Wizard to prepare the Replica

1. On the Replica server, launch the SharePoint Products Configuration Wizard from the Windows Start menu.

2. Complete the wizard screens. After configuration, use the PowerShell or STSADM tool to change the administrative site port on the Replica to match the one on the Master.

    For PowerShell, enter:

    set-SPCentralAdministration -Port <PortNumber>

    When you are prompted to confirm the action, press Y for yes.

Usually SharePoint uses high port numbers for central management. If you try to change the port to above 32767 then *set-SPCentralAdministration* fails to change the port and shows the "invalid port" error. For more information about this, see http://technet.microsoft.com/en-us/library/cc288247.aspx

The *stsadm* allows to change the port and then the choice is to use the *stsadm -o setadminport –port* command.

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\ADMINISTRATOR.MONSANTO> Add-PSSnapin microsoft.sharepoint.powershell
PS C:\Users\ADMINISTRATOR.MONSANTO> Set-SPCentralAdministration -port 8881

Confirm
Are you sure you want to perform this action?
Performing operation "Set-SPCentralAdministration" on Target "Microsoft.SharePoint.Administration.SPGlobalAdmin".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
PS C:\Users\ADMINISTRATOR.MONSANTO>
```

For STSADM, enter:

stsadm -o setadminport -port <PortNumber>

The command line interface returns the message, Operation completed successfully.

```
C:\>cd "Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\bin

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN>stsa
dm -o setadminport -port 8888

Operation completed successfully.
```

3. Launch SharePoint 2010 Central Administration on the Replica. Click Configure Alternate Access Mappings and then click Edit Public URLs. Change the public URL on the Replica to match the one on the Master.

4. Create the web applications on the Replica using the same display names, headers, and ports as the Master.

    a. From SharePoint 2010 Central Administration, click Manage web applications.
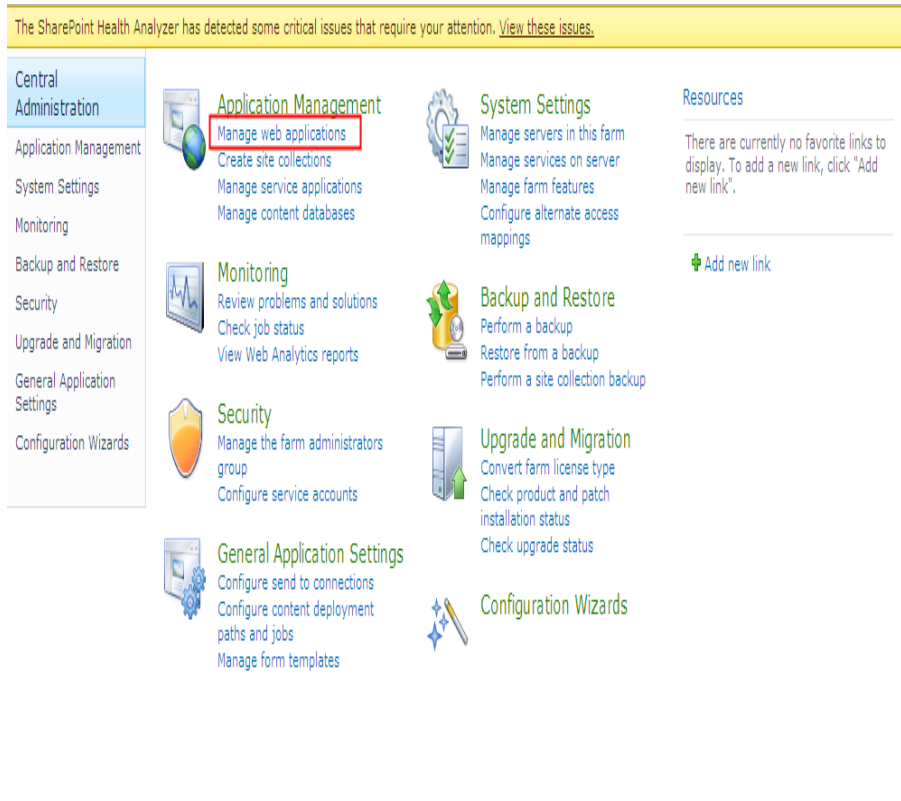
b. Click New.

c. Enter the same display names, headers, and ports used on the Master server to create web applications.

d. Click Manage content databases.

e. Click Add a content database.

   On replica, WSS_Content Database guides are different (at least it will be always different for the default web application on port 80 that was created by the SharePoint configuration wizard). You need to add a new database matching the master name and delete the existing database using SharePoint Web Application Management, Manage Content Database. For more information, see http://msdn.microsoft.com/en-us/library/cc668750(v=vs.100).aspx

   If you do not delete the old database, then the associated web application will have two databases and can have various implications. If you delete the database from SQL, SharePoint would not be aware of that and will still show the database as a web content DB. So, delete it using the instructions above.

f. Enter the same database name for each content database used on the Master server.

5. Create and run your HA scenarios to protect the standalone deployment.

Note: SharePoint stand-alone server uses SQL Express Edition that installs SQL instance with TCP/IP disabled. RHA scenario does not work if TCP/IP is disabled. You need to enable it on both master and replica.

Next Steps:

- Create a SharePoint Server Scenario for Standalone Deployments
- Create a SharePoint Server Scenario for Farm (All in One) Deployments
- Create Multiple Scenarios for Farm (Distributed) Deployments
- How to Run a Scenario or Group

Third-Party Web Parts for SharePoint

SharePoint websites support third-party web parts. To ensure that web parts on the Master server are available to the SharePoint website on the Replica server, you must import the web parts to the Replica server after failover is complete.

Arcserve Continuous Availability SharePoint COM+ Service

When the Arcserve Continuous Availability Engine is installed in a SharePoint environment that is joined to a SharePoint farm, the installation process installs Arcserve Continuous Availability SharePoint COM+ and registers the corresponding service, CAARCserveRHASPSCOMApp, for all SharePoint Scenarios. When you uninstall the Arcserve Continuous Availability Engine, the uninstallation process uninstalls and unregisters the corresponding components.

On Windows Server 2008 systems, the Microsoft Distributed Transaction Coordinator (MSDTC) service may prevent the SharePoint COM+ application from starting properly. This may prevent SharePoint HA scenarios from performing critical operations. For example, database Auto-Discovery, Run this scenario, Assured Recovery (AR) testing, and so on. To remedy this problem, restart the server where the problem occurred (Master or Replica).

For server farms, change the logon account of the Arcserve Continuous Availability SharePoint COM+ service on the Master server to Domain Administrator after the service is installed to prevent some SharePoint HA operations from failing. The service logon account on the Replica is changed during auto-configuration.

During Arcserve Continuous Availability Engine upgrade, the COM+ service is removed with the previous version of the Engine. After the upgrade is finished and the Engine is restarted, you can automatically install and start the COM+ service, but the start-up account may be set to Local System instead of Domain Administrator, as configured before upgrade. You must manually configure the service to be Domain admin before you start a scenario.

During scenario creation, you are prompted to enter the Domain Administrator's account credentials for Replica auto-configuration. If you enter the wrong account and passphrase (SharePoint Server 2010), auto-configuration fails. Click Back in the Scenario Creation Wizard to try again.

Note: Auto-configuration changes the logon account of the SharePoint services on the Replica to the account you specify. If the logon accounts of SharePoint services on the Master are different, you must change the Replica account manually.

Manage Services

As part of scenario creation or modification, you can specify the services to manage. During scenario creation, the services management screens are displayed in the Scenario Creation Wizard. For existing scenarios, you can also manage services from the Arcserve Continuous Availability Manager Root Directories tab.

Services discovered on the specified Master server are automatically shown on the Services Discovery Result screen in the Scenario Creation Wizard.

The following steps are for Custom Application scenarios.

To manage services
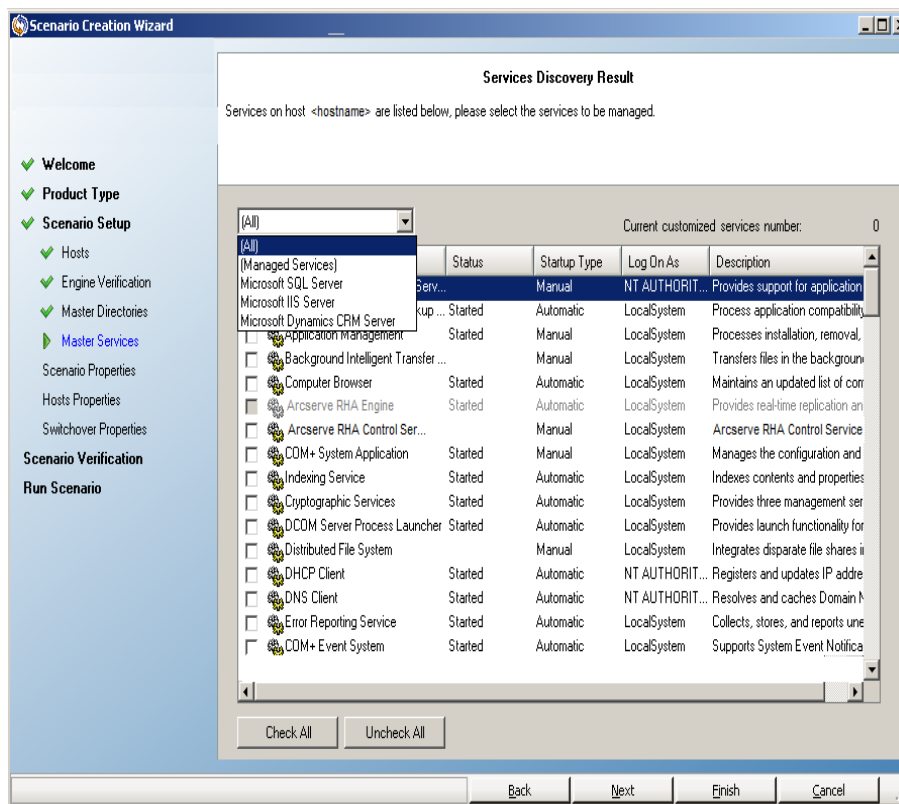
— **All** - lists all services discovered on the Master server

— **Managed Services** - lists only the checked services

— **Oracle Database** - lists Oracle-related services if the current host has Oracle installed

— **Microsoft SQL Server** - lists SQL Server-related services if the current host has SQL Server installed

— **Microsoft IIS Server** - lists IIS Server-related services if the current host has IIS Server installed

— **Microsoft SharePoint Server** - lists SharePoint Server-related services if the current host has SharePoint Server installed

— **VMware vCenter Server** - lists vCenter Server-related services if the current host has vCenter Server installed

— **Microsoft Exchange Server** - lists Microsoft Exchange Server-related services if the current host has Microsoft Exchange Server installed

— **Microsoft Dynamics CRM Server** - lists Microsoft Dynamics CRM Server-related services if the current host has Microsoft Dynamics CRM Server installed

1. Select a Service to Monitor. Click the box to the left of each service listed to select it for monitoring.

   Important! Do not use Services Management to monitor every service on the Master server in a single scenario. This scenario type is not designed to protect an entire server.

2. Click Next to proceed to the Services Setting screen.

Services Setting

Managed services are listed below, please set the properties for each service.

(Managed Services) ▼	Current customized services number:	4

Display Name	Start Order	Critical
Application Management	(Not Set)	☐
Computer Browser	(Not Set)	☐
Arcserve RHA Control Service	1	☑
Indexing Service	(Not Set) ▼	☑
	(Not Set)	
	1	
	2	
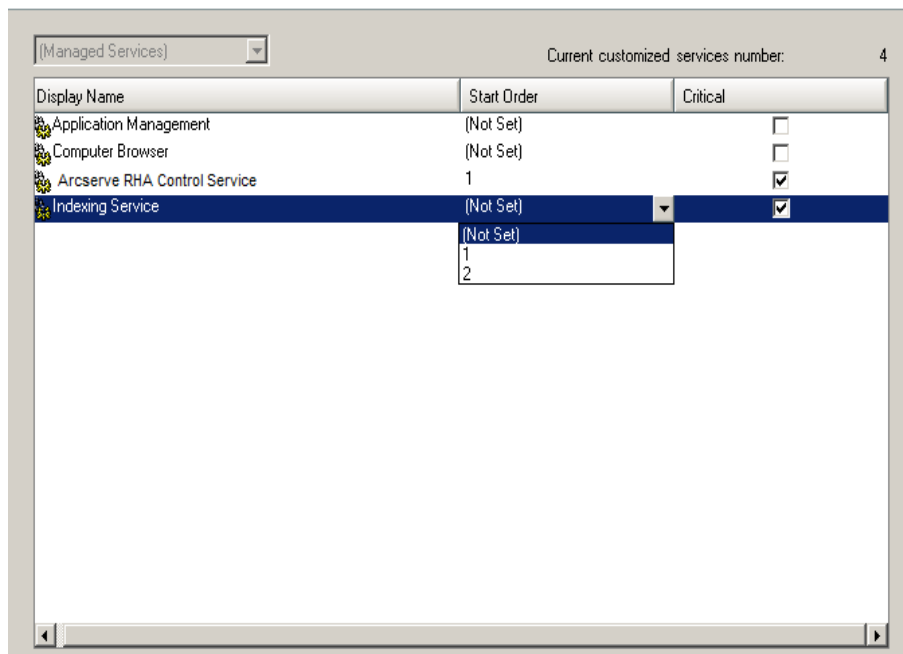
3. In the Start Order column for each service you chose, specify the numeric value representing start order. For services where order does not matter, use the default value, (Not Set). The options available in the drop down list update as you configure the value. The first service has only two options: Not Set and

1. The second service has three options: Not Set, 1 and 2, and so on. If you assign the same start order to two services, Arcserve Continuous Availability automatically reorders the selections you already made.

4. In Replication scenarios, the Critical column is disabled. In HA scenarios, use the Critical column to specify if a service should trigger switchover when it fails. By default, all services are marked Critical. Clear the box for any service whose failure does not require switchover to the stand-by server.

Create SharePoint Server Scenarios

Creating scenarios is covered in full detail in the *Arcserve Continuous Availability Administration Guide*. This section provides additional information specific to creating a Microsoft SharePoint Server scenario. The Scenario Creation Wizard guides you through the steps required to create a high availability scenario. When completed, you should run your scenario to start data synchronization. Synchronization could take a while, depending on database size and network bandwidth. After synchronization completes, your high availability scenario now maintains the Replica server so that it can take over for the Master the moment a failure is detected.

Notes:

- When the Arcserve Continuous Availability Engine is installed in a SharePoint environment that is joined to a SharePoint farm, the installation process installs Arcserve Continuous Availability SharePoint COM+ and registers the corresponding service, CAARCserveRHASPSCOMApp, for all SharePoint Scenarios. When you uninstall the Arcserve Continuous Availability Engine, the uninstallation process uninstalls and unregisters the corresponding components.

- On Windows Server 2008 systems, the Microsoft Distributed Transaction Coordinator (MSDTC) service may prevent the SharePoint COM+ application from starting properly. This may prevent SharePoint HA scenarios from performing critical operations. For example, database Auto-Discovery, Run this scenario, Assured Recovery (AR) testing, and so on. To remedy this problem, restart the server where the problem occurred (Master or Replica).

- For a high availability scenario, you must replicate the entire SharePoint Farm.

- For SharePoint Foundation 2010, you need two additional DLL files, Microsoft.Office.Server.dll and Microsoft.Office.Sever.Search.dll. You can copy these two files from the SharePoint 2010 full edition. Copy the two DLL files to the RHA engine folder and restart the CAARCserveRHASPSCOMAPP service.

This section contains the following topics:

- [Create a SharePoint Server Scenario for Standalone Deployments](#)
- [Create a SharePoint Server Scenario for Server Farm (all in one) Deployments](#)
- [Create Multiple Scenarios for SharePoint Server Farm (distributed deployments)](#)
- [Troubleshooting--Automatic AR failed for a SharePoint Scenario](#)

Create a SharePoint Server Scenario for Standalone Deployments

The following procedure applies to HA scenarios in SharePoint Server standalone deployments. It creates a single scenario to protect the SharePoint Server deployment.

To create a SharePoint High Availability scenario

1. From the Arcserve Continuous Availability Manager, select Scenario, New or click the New Scenario button.

2. When the Welcome dialog opens, select Create New Scenario and click Next.

3. When the Select Scenario Type dialog opens, select SharePoint, High Availability Scenario, and Replica Integrity Testing for Assured Recovery (optional). If you choose Assured Recovery, note that only existing web application databases can be discovered and replicated. For more information about Assured Recovery, see the *Arcserve Continuous Availability* Administration Guide.

4. When the Master and Replica hosts dialog opens, name your scenario and provide the hostname or IP address for the Master and Replica servers. Click Next. For more information, see Redirection Methods.

5. Wait for Engine Verification to complete and click Next. If needed, click Install to upgrade the Engine on one or both servers and then click Next.

   The Replica Configuration dialog opens, listing all auto-discovered results for the specified Master. By default, all databases are included.

   Note: For a high availability scenario, all data items (i.e. database, SharePoint data folder, and so on) are replicated and cannot be deselected.

6. On the Replica Configuration dialog, do one of the following:

   ◆ If the comparison results for the Replica and the Master are identical, click Next.

   ◆ If the comparison results for the Replica and the Master are different you must re-configure SharePoint on the Replica.

7. Enter the domain administrator's account credentials. For SharePoint Server 2007, enter the user name, password and domain. For SharePoint Server 2010, enter the user name, password, domain, and farm pass phrase. The account you specify is applied as the logon account for the Arcserve Continuous Availability SharePoint COM+ service on the Replica to process auto-configuration. For more information, see Arcserve Continuous Availability SharePoint COM+ Service.

8. Wait for the auto-configuration to complete and click Next. For more information, see [Prepare the SharePoint Replica Server](#).

9. When the Scenario Properties dialog opens, configure additional properties, if needed. If you use NTFS ACLs with domain accounts for user access control, we recommend that you select the Replicate NTFS ACL option and click Next. For more information, see [Scenario Properties](#) or the *Arcserve Continuous Availability* Administration Guide.

   Note: The Synchronize Windows Shares option is set to On by default to ensure the query role in the server farm works correctly after failover.

   The Master and Replica Properties dialog opens.

10. Accept default settings or make the desired changes and click Next.

11. Wait for the Switchover Properties dialog to retrieve information. Configure the desired redirection properties and click Next. For more information, see [Switching Over and Switching Back](#).

12. From the Switchover and Reverse Replication Initiation dialog, select automatic or manual switchover, and automatic or manual reverse replication, as needed.

   You should not set both of these options to automatic. For more information, see [Scenario Properties](#) or the *Arcserve Continuous Availability* Administration Guide.

13. If you selected Integrity Testing for Assured Recovery, the dialog opens now. Set a schedule if desired. For more information, see the *Arcserve Continuous Availability* Administration Guide.

14. Click Next to initiate scenario verification. If errors are reported, you should resolve them before continuing. At successful verification, click Next to complete scenario creation.

   Note: If scenario verification reports an error about replicas still existing in the farm, this is due to a configuration problem. To resolve it, launch the SharePoint Wizard on the Replica to disconnect it from the Master's farm and then repeat auto-configuration.

15. Select Run Now or Finish. Run Now starts synchronization. Finish allows you to run the scenario later.

Create a SharePoint Server Scenario for Server Farm (all in one) Deployments

The following procedure applies to HA scenarios in SharePoint Server all-in-one deployments. It creates a single scenario to protect the SharePoint server deployment.

To create a SharePoint High Availability scenario

1. From the Arcserve Continuous Availability Manager, select Scenario, New or click the New Scenario button.

2. When the Welcome dialog opens, select Create New Scenario and click Next.

3. When the Select Scenario Type dialog opens, select SharePoint, High Availability Scenario, and Replica Integrity Testing for Assured Recovery (optional). For more information about Assured Recovery, see the *Arcserve Continuous Availability* Administration Guide.

4. When the Master and Replica hosts dialog opens, name your scenario and provide the hostname or IP address for the Master and Replica servers. Click Next. For more information, see Redirection Methods.

5. Wait for Engine Verification to complete and click Next. If needed, click Install to upgrade the Engine on one or both servers and then click Next.

   The Replica Configuration dialog opens, listing all auto-discovered results for the specified Master. By default, all databases are included.

   Note: For a high availability scenario, all data items (i.e. database, SharePoint data folder, and so on) are replicated and cannot be deselected.

6. On the Replica Configuration dialog, do one of the following:

   ◆ If the comparison results for the Replica and the Master are identical, click Next.

   ◆ If the comparison results for the Replica and the Master are different you must re-configure SharePoint on the Replica.

7. Enter the domain administrator's account credentials. For SharePoint Server 2007, enter the user name, password and domain. For SharePoint Server 2010, enter the user name, password, domain, and farm pass phrase. The account you specify is applied as the logon account for the Arcserve Continuous Availability SharePoint COM+ service on the Replica to process auto-configuration. For more information, see Arcserve Continuous Availability SharePoint COM+ Service.

8. Wait for the auto-configuration to complete and click Next. For more information, see Prepare the SharePoint Replica Server.

9. When the Scenario Properties dialog opens, configure additional properties, if needed. If you use NTFS ACLs with domain accounts for user access control, we recommend that you select the Replicate NTFS ACL option and click Next. For more information, see Scenario Properties or the *Arcserve Continuous Availability* Administration Guide.

   Note: The Synchronize Windows Shares option is set to On by default to ensure the query role in the server farm works correctly after failover.

   The Master and Replica Properties dialog opens.

10. Accept default settings or make the desired changes and click Next.

11. Wait for the Switchover Properties dialog to retrieve information. Configure the desired redirection properties and click Next. For more information, see Switching Over and Switching Back.

12. From the Switchover and Reverse Replication Initiation dialog, select automatic or manual switchover, and automatic or manual reverse replication, as needed.

   You should not set both of these options to automatic. For more information, see Scenario Properties or the *Arcserve Continuous Availability* Administration Guide.

13. If you selected Integrity Testing for Assured Recovery, the dialog opens now. Set a schedule if desired. For more information, see the *Arcserve Continuous Availability* Administration Guide.

14. Click Next to initiate scenario verification. If errors are reported, you should resolve them before continuing. At successful verification, click Next to complete scenario creation.

   Note: If scenario verification reports an error about replicas still existing in the farm, this is due to a configuration problem. To resolve it, launch the SharePoint Wizard on the Replica to disconnect it from the Master's farm and then repeat auto-configuration.

15. Select Run Now or Finish. Run Now starts synchronization. Finish allows you to run the scenario later.

Create Multiple Scenarios for SharePoint Server Farm (distributed deployments)

SharePoint deployments often include application, database, and load balancing web-front-end servers, each critical to the successful operation of the application. To protect distributed deployments like this, a separate scenario is required for each of the following:

- SQL scenario to protect the database server

- SharePoint scenario to protect the application server

- SharePoint scenario to protect the web front end server (For SharePoint Server 2007 only)

With this release, you can now create a single scenario group that configures the required individual scenarios needed to protect a distributed deployment, and lets you set switchover properties at the group level, so the entire farm can switch over when a failure is detected anywhere in the deployment. Arcserve Continuous Availability automatically discovers the farm topology and creates the required scenario for each discovered component.

Note: If you installed the SQL Server and SharePoint Server software on the same host, you need only one SharePoint HA scenario to protect it. The Farm Discovery panel does not appear if this host is the only server in the farm.

To create multiple SharePoint Server scenarios for a SharePoint Farm

1. From the Manager, click the New Scenario button to launch the Scenario Creation Wizard.

   The Welcome screen opens.

2. From the Welcome screen, do the following:

   a. Click Create a New Scenario.

   b. Enter a new Scenario Group name, which Arcserve Continuous Availability will create with the scenario.

   c. Click Next.

   The Select Server and Product Type screen opens.

3. From the Select Server and Product Type screen, do the following:

   a. Select MS SharePoint Server as the Server Type.

   b. Click High Availability Scenario as the Product Type.

    c. Click None for Tasks on Replica. For more information on performing Assured Recovery, see the *Arcserve Continuous Availability Administration Guide*.

    d. Click Next.

The Master and Replica Hosts screen opens.

4. Do the following:

    a. Enter a name for the scenario to add to the group.

    b. In the Master Hostname/IP field, enter the host name or IP address of your SharePoint web front end server. Arcserve Continuous Availability discovers all the SharePoint servers in your deployment.

    c. In the Replica Hostname/IP field, enter the host name or IP address of a server you wish to use as the stand-by server.

    d. For the Port numbers, accept the default value.

    e. Enable the option, Verify Arcserve Continuous Availability Engine on hosts.

    f. Click Next.

The Engine Verification screen opens.

5. Wait while verification completes. If needed, install the Engine on one or both servers and click Next.

The Configure the Master/Replica Host Mappings screen opens, showing a list of the discovered servers in your deployment.

6. On this screen, do the following:

    a. In the Host Mappings list, select the SharePoint servers you want to protect. The first Master is automatically listed from the information you provided on the Master and Replica Hosts screen.

    b. In the Replica Hostname column, enter the Replica hostname for each selected server.

    c. In the Scenario Name column, enter a unique scenario name for each selected server.

    d. Enable the option, Verify Arcserve Continuous Availability Engine on Hosts.

    e. Click Next.

The Engine Verification screen opens again, showing the status for each dis-
covered Master and assigned Replica server. The first server you specified is
excluded from this list because it was previously verified.

7. Install the Engine on any server, if needed, and click Next.

    The Database for Replication screen opens.

8. Enable the option, Replicate new databases in the selected root directories
    and click Next.

9. Wait while the server configuration on the Master and Replica servers is com-
    pared. Replicas are auto-configured to match Masters.

10. When the Replica Configuration screen opens, click Next if any Replica is not
    auto-configured. For server farms, enter the domain administrator's account
    credentials. For SharePoint Server 2007, enter the user name, password and
    domain. For SharePoint Server 2010, enter the user name, password, domain,
    and farm pass phrase. The account you specify is applied as the logon account
    for the Arcserve Continuous Availability SharePoint COM+ service on the Rep-
    lica to process auto-configuration. For more information, see Arcserve
    Continuous Availability SharePoint COM+ Service

    The Scenario Properties screen opens.

11. This screen displays properties with each scenario on its own tab. You may
    configure scenario properties independently for each scenario. Click Next
    when done.

    The Master and Replica Properties screen opens.

12. This screen also features a tab for each scenario so you can set properties
    independently. Click Next when done.

    The Switchover Properties screen opens after Arcserve Continuous Availability
    retrieves default settings for all scenarios in the group.

13. Set properties on each tab and click Next when done.

    The Switchover and Reverse Replication Initiation screen opens.

14. All scenarios share the same settings on this screen. Select either Switchover
    or Reverse Replication and set to automatic, but not both. Click Next.

    The Group Properties screen opens.

15. This screen lets you specify the group switchover settings. Do the following:

    a. Expand the Switchover Settings properties group.

    b. If you want the whole group to switchover as a single entity, turn on the
        Switchover as a Group property.

c. Expand the Failure Triggers Group Switchover property. All scenarios in your group are listed. Set the value to On for any scenario that should trigger whole group switchover if it fails.

d. If Arcserve Continuous Availability is unable to switch over the whole group, you can set the Actions When Unable to Switchover as a Group option to On.

e. Click Next.

Wait while Arcserve Continuous Availability performs Group Verification.

16. The verification process actually verifies every scenario in the group and lists any errors or warnings found. You must resolve errors and should fix warnings before continuing. Finally, click Next.

    Note: If scenario verification reports an error about replicas still existing in the farm, this is due to a configuration error. Launch the SharePoint configuration wizard from the Windows Start menu on the Replica server to disconnect it from the Master's farm and then repeat auto-configuration.

17. The scenario group is ready. Do one of the following:

    ◆ Click Finish to save the scenario group. You can add additional scenarios, if desired. For more information, see the topic Create a SharePoint Server Scenario, or view the Operation Guides for instructions on creating other scenario types. You can run the group later.

    ◆ Click Run Now to run the scenario group immediately.

Troubleshooting--Automatic AR failed for a SharePoint Scenario

[[[Undefined variable Variables.sy]]]

The following error is displayed when performing automatic Assured Recovery testing for a SharePoint scenario:

Unable to check SharePoint state: Unknown
Automatic SharePoint testing on replica hostname is unsuccessful

[[[Undefined variable Variables.so]]]

These errors are related to the SQL account security. If SQL is a local account, set Replicate ACL OFF to solve the issue.

[[[Undefined variable Variables.fts]]]

1. Navigate to Scenario Properties.

2. Click Replication and then click Optional Settings.

3. Set Replicate ACL to OFF.

4. Save the properties.

Set Scenario Properties

You can change a scenario configured using the Wizard or configure additional settings, or modify the scenario, using the Properties pane.

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 Continuous Availability Administration Guide.*

Properties are organized into tabs on the Arcserve Continuous Availability Manager Framework pane. The tabs displayed are based upon server type, Arcserve Continuous Availability solution, and scenario status. Select the scenario for which you want to change properties, and then select the appropriate tab.

Settings on the Root Directories tab

Do the following:

1. Select a Master Server from the Scenario Pane. Double-click its Directories folder to add or remove Master Root Directories. Select or clear checkboxes next to folders, as desired, to include or exclude them. You may also edit directory names.

2. 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. Select or clear checkboxes next to folders, as desired, to hold the corresponding Master directory.

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 -- select 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, select email notification, or write to 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 -- These properties differ for Master and Replica. See the *Arcserve Continuous Availability 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, select email notification, or write to event log.

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

- (Replica) Scheduled Tasks -- set or suspend tasks, including Replica Integrity Testing for Assured Recovery. For more details, see the *Arcserve Continuous Availability Administration Guide*.

- (Replica) Recovery properties -- set delay, data rewind properties, or scheduled task for replica.

Settings on the HA Properties Tab

These settings control how switchover and switchback are performed.

- Switchover properties -- select automatic or manual switchover, provide switchover hostname, and reverse replication settings.

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

- Network Traffic Redirection properties -- select Move IP, Redirect DNS, Switch Computer Name or User-defined scripts.

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

- DB Management properties (does not apply to File Server scenarios) -- instructs Arcserve Continuous Availability to manage shares or services on a database server.

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

Prepare the Distributed Group for Protecting SharePoint Farm

A *distributed group* is a SharePoint Server farm with several servers where multiple scenarios are created to protect them. These scenarios must be centrally managed as single logical unit, as they are part of the same farm. Unlike the default group and the regular group, the distributed group has central management functionalities. Some of the central management functionalities include:

- Group Run/Stop: You can start/stop all the scenarios in the group together.

- Group Switchover: You can initiate manual switchover on all the scenarios once, and configure them to be switched over together automatically in case any of them is failed.

- Group Recover Active Server: You can resolve the split-farm problem (some SharePoint server Masters are active while other Replicas are active). It can easily recover active servers of all scenarios to either Master or Replica.

Create Distributed Groups

You can create distributed groups from available regular groups using Central Scenario Management.

To create a distributed group using the Scenario Creation Wizard

1. Open the Scenario Creation Wizard.

2. Specify a new group name in the scenario creation wizard when creating scenarios for SharePoint farm.

A new distributed group is created.

To convert a regular group to a distributed group

1. Create a Regular Group.

2. Select the Regular group on the Manager and right-click to select the Enable Central Management Option.

The regular group is converted to Distributed Group.

Note: You can easily convert a Distributed Group to Regular Group by disabling the Scenario Group Management option.

Group Properties

You can configure the group properties using the Scenario Creation Wizard, while creating a scenario.

The group properties include:

Scenario Dependencies

Manages the interdependencies between scenarios. Usually a distributed application has multiple components/roles/servers which are interdependent. Any scenario can be configured to depend on one or more scenarios or multiple scenarios can depend on a single scenario. These services can be handled by the Scenario Dependencies property.

Switchover Settings

Manages the switchover setting in a distributed group. Some of the switchover setting options include:

- Switchover as a Group : If this option is set to On, the whole group (all the scenarios) will be automatically switched over together in case one of the scenarios is failed and ready to take switchover.

- Failure Triggers Group Switchover: A single failure can trigger a group switchover. By default, all scenarios can trigger group switchover, and you can configure some light-weight scenarios to be set to Off.

- Execute Scenario Switchover Settings: This option decides whether the scenario should execute its own switchover settings.

Scenario Availability Sets

A distributed application might configure two or more servers to provide same services to improve availability or performance. When one server is down, the other servers are still working and can still provide the services. Scenario Availability Set will be used when Arcserve Continuous Availability manages these servers/scenarios of that distributed application.

If two scenarios are configured in the same Scenario Availability Set, the group switchover is initiated only when both scenarios fail. This function is not invoked when one of the options fail.

Note: The same group can have one or more Scenario Availability Sets, but one scenario cannot be configured in two different sets.

If there are Load-Balancing WFE servers configured in the SharePoint farm, it is recommended that you configure the scenarios protecting WFE servers to be in same scenario availability set.

Event Notification

Lets you configure the policies for the group event. Some of the policies include:

- Notify by email: Send an email to specified recipients.

- Execute script: Execute some pre-defined script.

- Write system event log: Write a log to Windows system events.

How to Run a Scenario or a Group

After you create a scenario, you need to run it to start the replication process. Typically, before data changes on the Master are replicated to 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: For the replication process to succeed, verify that the user under which the Arcserve Continuous Availability 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.

This section contains the following topics:

- Run a Scenario
- Run a Group

Run a Scenario

You can run a single scenario using the following procedure:

To run the scenario

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

2. Click Run ▷ on the Standard toolbar.

   Before initiating synchronization and replication, Arcserve Continuous Availability verifies your scenario configuration. When verification completes successfully, the Manager displays the message: *Are you sure you want to run scenario "scenario_name?"* If problems are discovered, the top pane displays any warning and error messages resulting from verification.

   Note: Scenario Verification checks many different parameters between the Master and Replica servers to ensure a successful switchover. If any errors or warnings are reported you should not continue until they are resolved.

3. Correct errors before you continue. Errors are reported on the Event pane.

   Note: Replication of mount points succeeds 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 and contains synchronization options.

   Note: Do not use **Skip Synchronization** for any scenarios replicating a database.

4. If you have a large number of small files, select File Synchronization. If you have large files, select Block Synchronization. If you have low bandwidth, select Offline Synchronization to transfer data to an external device, then perform synchronization from that device. Select the Ignore same size/time files to skip the comparison of files with the same path, name, size and modification time, which are generally identical, to reduce synchronization time. You should enable the Skip Synchronization option only when you are certain the files on both Master and Replica are identical. (The default selections are File Synchronization and Ignore same size/time files option enabled).

5. Click the OK button. Synchronization may take a while, depending on database size and network bandwidth between the Master and Replica. You will receive the following message in the event window when the synchronization is complete: *All modifications during synchronization are replicated.*

At this point, the scenario is operational and active. By default, a Synchronization Report is generated when synchronization finishes. To view the report, refer to the topic, View a Report. You can also generate regular Replication Reports to monitor the replication process on each participating server. For more information, see the *Arcserve Continuous Availability Administration Guide*.

Run a Group

You can run multiple scenarios in a group using the following procedure.

To run the group

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

2. Click Run ▷ on the Standard toolbar.

   Before initiating synchronization and replication, Arcserve Continuous Availability verifies your group configuration. When verification completes successfully, the Manager displays the message: Are you sure you want to run group ' group_name' ?

   Note: If problems are discovered, the top pane displays any warning and error messages resulting from verification.

   Group Verification checks many different parameters between the Master and Replica servers to ensure a successful switchover. If any errors or warnings are reported you should not continue until they are resolved.

   If scenario verification reports an error that replicas still exist in the farm, this is due to a configuration error. Launch the SharePoint configuration wizard from the Windows Start menu on the Replica server to disconnect it from the Master's farm and then repeat auto-configuration.

3. Correct errors before you continue. Errors are reported on the Event pane.

   Note: Replication of mount points succeeds 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 and contains synchronization options.

   Note: Do not use **Skip Synchronization** for any scenarios replicating a database.

4. If you have a large number of small files, select File Synchronization. If you have large files, select Block Synchronization and if you have a different default synchronization method and run a group, then select Use default 'Synchronization Method' for each scenario in this group and then perform synchronization from that device. Select the Ignore same size/time files to skip the comparison of files with the same path, name, size and modification time, which are generally identical, to reduce synchronization time. You should

enable the Skip Synchronization option only when you are certain the files on both Master and Replica are identical. (The default selections are File Synchronization and Ignore same size/time files option enabled).

5. Click the OK button. Synchronization may take a while, depending on database size and network bandwidth between the Master and Replica. You will receive the following message in the event window when the synchronization is complete: *All modifications during synchronization are replicated.*

At this point, the group is operational and active. By default, a Synchronization Report is generated when synchronization finishes. To view the report, refer to the topic, View a Report. You can also generate regular Replication Reports to monitor the replication process on each participating server. For more information, see the *Arcserve Continuous Availability Administration Guide*.

How to Stop a Scenario or a Group

This section contains the following topics:

- [Stop a Scenario](#)
- [Stop a Group](#)

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.

Stop a Group

To stop a scenario

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

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

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

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

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

How Arcserve Replication and High Availability Supports Load Balanced SharePoint WFE

SharePoint WFE (Web Front End) servers can be deployed in a load balanced system to improve WFE performance. In many-to-many configuration mode, each WFE server is protected in a scenario with a dedicated standby for failover. In many-to-one configuration mode all WFE servers are consolidated into single standby server and the scenarios are in a single group to ensure group failover. Since the whole group of load balanced servers is protected as one, only when the last active server is down, the standby is going to be active.

Arcserve Replication and High Availability provides high availability for these servers in many-to-many and many-to-one configuration methods. Considering that you can choose different kinds of load balance systems (hardware solution or software based solution such as DNS round robin or Microsoft NLB), Arcserve Replication and High Availability will not handle load balance related logic during switchover such as workload distribution. The load balance system must ensure that your requests can be sent to a new server node and no further service requests are distributed to a removed node.

If you have used Microsoft NLB as WFE load balanced solution, it is easier to redirect the network flow to standby after failover. Consider the following scenarios:

- If you have configured a scenario with redirection-DNS or switchover-hostname property, Arcserve Replication and High Availability lets you dynamically start or stop NLB based on the scenario status. You can do this by specifying start-db and stop-db scripts.

- If you have configured a scenario with move-IP as network resource, the IP address you specify can be the private IP address of the server or the IP of the NLB cluster (virtual IP).

- For many-to-many configurations, if you want to move the virtual IP from the active server to a standby, you must first make all standby servers part of NLB, and then dynamically start or stop NLB in addition to moving virtual IP to standby. The reason for this is to avoid IP confliction when you are sharing the same IP among several non-NLB standbys.

- For many-to-one configurations, you must move the virtual IP from active to standby and then the standby will host the virtual IP address to respond to user requests.

View a Report

Arcserve Continuous Availability can generate reports on the replication and syn-chronization 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\ArcserveRHA\Manager\reports*

To view reports

Note: Though an Exchange report is shown for illustrative purposes, the steps and screens are similar regardless of the type of scenario.

1. To view reports, locate the Tools menu, click Reports, and then select Show Scenario Reports.

   The Report Center opens in a new window.

The Report Center consists of two tables:

- ◆ The upper table - Available Reports per Scenario - contains a list of all scenarios that have reports, 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 Reports per 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.

SYNCHRONIZATION REPORT

Synchronization mode	BlockSynchronization (include files with the same size and modification time)
Scenario	Exchange 1
Master host	192.168.50.2(1)
Replica host	192.168.50.12(2)
Scenario start time	12/22/2009 06:37:52
Report start time	12/22/2009 06:38:07
Report finish time	12/22/2009 06:39:15

EVENT	BYTES	TIME STAMP	FILE NAME

View Events

To view the events of a scenario, open the Manager, and select a scenario in the scenario view.

Note: Select the group in the scenario view to see the group events.

The events of the scenario are displayed at the bottom of the Manager window (by default).

View Statistics

Arcserve Continuous Availability provides statistics on the replication and synchronization processes. You can display these statistics on the Manager.

To view statistics

1. Select the scenario or the group in the scenario view.

2. Click the Statistics tab.

    The Statistics pane appears.

Chapter 3: Redirection Methods

This section contains the following topics:

How Redirection Works

Each server type supported by Arcserve RHA can be configured to use one or more redirection methods. You should enable redirection methods based on your environonment and business needs. The following sections describe the supported redirection methods for Microsoft SharePoint Server.

Note: For Microsoft Exchange Server 2010, by default, only Move IP is available for the redirection method. In addition, Exchange Server 2010 HA scenario works fine even if all redirection methods are set to off.

DNS Redirection

DNS Redirection changes the DNS "A" Record of the Master server to resolve to IP address of the Replica server. Upon failure of the Master, the Replica server modifies the appropriate DNS record so that references to the Master server resolve to the Replica's IP address rather than the Master's IP address. This redirection method requires no network reconfiguration and works in LAN and WAN network configurations.

DNS redirection works only with A (host) type records and cannot update CNAME (Alias) records directly. However, if the CNAME record points to the modified A record, it is indirectly redirected.

Using the record that has the Master server's name is the default, however you can configure Arcserve Continuous Availability to redirect any DNS A (host) record via the *Master's name in DNS* setting in the switchover properties tab.

Move IP Redirection

Move IP redirection involves moving the Master server IP address to the Replica server.

This redirection method is preferred for Virtual Machine scenarios and is usable only in a LAN configuration in which the Master and Replica servers reside in the same network segment. In this configuration, switchover of the Master server causes the Replica to take over one or more of the IP addresses assigned to the Master server.

Important! Use this method only when both servers are on the same IP subnet.

When using Move IP as the redirection method, you must first add IP addresses to the Master host. For more information, refer to the topic, Add IP on the Master Server.

Add IP on the Master Server

You need to add an additional IP address to the Master host, (which is denoted as *Arcserve-IP* in the following steps) to use Move IP redirection in your HA scenarios. This new IP address is used for Arcserve Continuous Availability internal communication and replication. This is necessary because once switchover occurs, the current production IP address is no longer available on the Master -- it switches to the Replica server.

Important! Perform the following only if you are using the Move IP redirection method.

To add IP Address to Master Server

1. Open the Control Panel and select Network Connections.

2. Right-click Local Area Network and select Properties.

3. Click Internet Protocol (TCP/IP) and then click the Properties button.

4. Click Advanced.

5. Click Add and enter an additional IP address (Arcserve-IP).

    In the following screenshot, the Arcserve-IP IP address is 192.168.220.23 and the current production server IP address is 192.168.220.111.

6. Click Add.

7. Click OK.

8. Click OK to exit the LAN settings.

After you add the IP to the Master, you must add the Arcserve-IP to your HA scenarios. There are two ways to add the Arcserve-IP address to an HA scenario:

-   For new scenarios, from directly in the Wizard

-   For existing scenarios, by modifying the master host name

The procedures for both ways follow.

This section contains the following topics:

-   Add Arcserve-IP to Existing Scenarios-sharepoint

-   Add Arcserve-IP to New Scenarios

-   Switch Computer Name Redirection

Add Arcserve-IP to Existing Scenarios-sharepoint

Perform this procedure only if you are using the Move IP redirection method.

To add the Arcserve-IP to existing scenarios:

1. On the Scenario pane, select the required Master host:
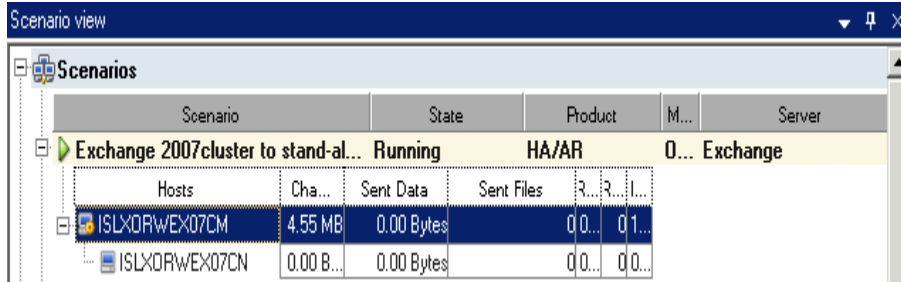
2. Right-click the Master and select **Rename** from the pop-up menu. Then, enter the Arcserve-IP address.

3. On the Framework pane, select the **Switchover** tab and then select the Replica server as the switchover host.

4. Set the **Move IP** option to On. Ensure that the IP address under **Move IP**, **IP/Mask** matches the production server IP address: this is the IP address that will switch-over. If you are moving more than one IP address you can add multiple production IP addresses by selecting **Click here to add new IP/Mask**:
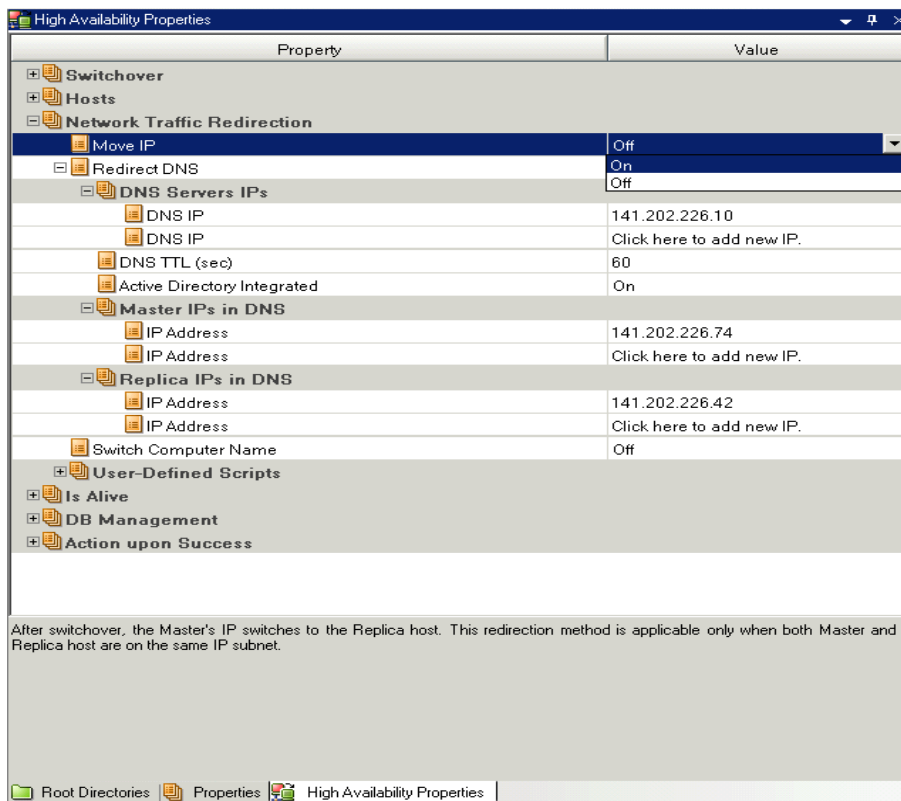
Add Arcserve-IP to New Scenarios

Note: Perform this procedure only if you are using the Move IP redirection method.

During the initial run of the Scenario Creation Wizard, enter the Arcserve-IP and Replica IP addresses in the Master Hostname/IP and Replica Hostname/IP boxes, instead of the server names.

Switch Computer Name Redirection

If you are redirecting File Shares, in which clients connect via the Master server name, enable Switch Computer Name. For example, if the Master server name is fs01 and clients connect to \\fs01\sharename or \\fs01.domain.com\sharename, using the Switch Computer Name method redirects clients to the failover server. To use Switch Computer Name Redirection in the Active Directory environment, both Master and Replica must belong to the same domain.

It is also recommended to enable one other method. The most common method is to use both DNS Redirection and Switch Computer Name. Arcserve Continuous Availability makes the required computer name switch by assigning a temporary name to the Master server and taking over its computer name for use with the Replica server.

Arcserve Continuous Availability updates records directly and does not generally require a reboot. If, however, you encounter any problems after switchover, consider setting the reboot option to On and testing again.

Note: For Windows Server 2008 systems, you must reboot the computer after a switchover occurs when the switch computer name method is used. To do so, enable the property, Reboot after switchover. However, for Windows 2008 Cluster systems, reboot will not occur even if this property is enabled. You must reboot manually and ensure the SQL Server service is running.

Scripts Redirection

Arcserve Continuous Availability can trigger custom scripts or batch files to perform the user redirection or any additional steps not covered by built-in methods. If the above methods are not appropriate or do not fully meet all requirements, see the *Arcserve Continuous Availability Administration Guide* for details on scripted redirection methods.

Chapter 4: Switching Over and Switching Back

(missing or bad snippet)

This section contains the following topics:

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. There are three types of monitoring checks:

- **Ping** -- a request sent to the Master to verify that the Master is up and responding

- **Database check** -- a request that verifies the appropriate services are running and all databases are mounted and SharePoint websites are started.

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

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 Master server is considered to be down. Then, depending on the HA scenario configuration, Arcserve HA 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 database connectivity are monitored. The timeout parameters are configurable and are more extensively covered in the *Arcserve Continuous Availability 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, if both the master and replica servers were online and connected during switchover, resynchronization in the reverse direction is not required. 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.

Note: Though the following steps show Exchange scenario screens as examples, the procedure is similar for all server types.

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 the **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 Switchover for a Group

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

To initiate switchover for a group

1. Open the Manager and select the group from the Scenario pane. Verify if it is running.

2. Click Perform Switchover.

   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. The operation stops when the switchover completes.

   Detailed information about the switchover process is located in the Events pane during switchover. A message appears in the Event pane, informing you that the switchover is completed, and that the scenarios in the group have 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 scen-ario, 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 Continuous Availability 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 but-ton 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, replication from the active server to the standby server begins.

        Note: You are now ready to reverse the roles between the Master and Replica 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.

Initiate Switchback for a Group

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 again the Replica the standby server. Before you switch back the roles between servers, decide if you want to the data on the original Replica server to overwrite the data on the original Master. If yes, you must first perform a reverse scenario, a backward scenario.

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

To initiate switchback for a group

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

2. Open the Manager and select the desired group 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 group.

        Arcserve Continuous Availability 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 group. If desired, click the Advanced button to open an additional pane with detailed information about the hosts that participate in the group.

     b. Select Block synchronization method from the Run dialog and click OK.

        Resynchronization starts. After resynchronization completes, the message, "All modifications during synchronization period are replicated. Now, replication from the active server to the standby server begins" appears in the Event pane. You can now reverse the roles between the Master and Replica 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.

Recover Active Server

In certain circumstances, it may be necessary to forcibly make the Master or Replica server the active server without completing the data synchronization process.

For example, if switchover occurred but no data was changed on the Replica server. In this case you may even have newer data on the Master server making it undesirable to synchronize data from the Replica to the Master server. Arcserve Continuous Availability allows Recover Active Server process, to use this option. You must ensure that the scenario is stopped, and select *Recover Active* Server from the Tools menu.

Important! While this option is the right choice in many situations, use it with caution. If used improperly data loss can occur. Usually, Arcserve Continuous Availability will not allow switchover from one host to another until all data is synchronized. It is designed this way so users are not redirected to an out of date data set that then overwrites what may be a more current data set. When using Recover Active Server, Arcserve Continuous Availability 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, you must manually ensure 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.

Select either *Make Master Active* or *Make Replica Active* depending onto which server you want to force the active role.

Important! If a legitimate switchover in a disaster situation occurs and users are redirected to the Replica server for any period of time, it is important to replicate all changes on the Replica back to the Master before making the Master server active. Using *Recover Active Server* in such a situation results in loss of data.

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 Continuous Availability triggers Switchover without administrative involvement and could start Reverse Replication before you have investigated the cause of the failure. During Reverse Replication, Arcserve Continuous Availability overwrites data on your production server.

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

Recover Active Server for a Distributed Group

You can also forcibly make the Master or Replica server the active server without completing the data synchronization process for a group. This recovery process id used to resolve the split-farm problem. For more information about split farm, see Microsoft documentation.

To recover the Active Server for a Distributed Group

1. Ensure all scenarios are stopped.

2. Select the group node in the Manager and select Recover Active Server from the Tools menu.

   The group node performs verification, and lists the results of each scenario in a row.

   Note: You must consider the different types of scenarios before performing the recovery process. For all scenarios running on the server to be recovered, note which servers are active. Decide which servers you wish to force into the active role.

3. Select either Make Master Active or Make Replica Active depending onto which server you want to force the active role.

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

Chapter 5: Recovering Data

This section contains the following topics:

The Data Recovery Process

When an event causes loss of Master data, the data can be restored from any Replica. The recovery process is a synchronization process in the reverse direction - from a Replica to the Master.

Arcserve Continuous Availability enables you to recover data in two ways:

- **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. (This option is not recommended for Oracle, SQL or Exchange scenarios.)

- **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 to initiate recovery.

Recover Lost Data from Replica

To recover all lost data from a Replica

1. On the Manager, from the Scenario pane select the desired scenario and stop it.

2. [For database applications only] stop the database services on the Master host.

3. On the Manager, from the scenario folder select the Replica host:

   Note: If multiple Replica servers participate in the required scenario, select the Replica from which you want to recover data.

   The **Restore Data** option is enabled.

4. From the **Tools** menu, select **Restore Data**, or click the **Restore Data** button on the Standard toolbar.

   The **Recovery Method** page of the Restore Data wizard appears.

   Note: If the **Data Rewind** property is set to On, another **Restore Data** dialog will appear. In this case, select the first option - Replace all data on Master with the data on Replica.

5. Click Next. The Synchronization Method page appears.

6. Make sure that the **Block Synchronization** method is selected, and click **Finish**.

   Once you finished initiating the recovery process, Arcserve Continuous Availability builds a temporary reverse tree using the selected Replica as the root, and the Master as the terminating node. After the Master recovery process ends, the temporary scenario is deleted, and you receive the following message in the Event pane: **Synchronization finished**.

7. By default, once a data recovery occurs a Synchronization Report is generated.

   Now, the replication process can restart following the original scenario.

Setting Bookmarks

A *bookmark* is a checkpoint that is manually set to mark a state back to which you can revert. We recommend setting a bookmark just before any activity that can 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* (default setting is *Off*).

- You cannot set bookmarks during the synchronization process.

- You can insert manual bookmarks for Full System HA scenarios.

To set a bookmark

1. Select the Replica host on the Scenario pane from which you want to rewind data when the required scenario is running.

2. Select the Set Rewind Bookmark option on the Tools menu.

   The Rewind Bookmark dialog opens.

   The text that appears in the Rewind Bookmark dialog appears 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, and click OK.

   Note: It is recommended that you provide a meaningful name that will later help you recognize the required bookmark.

   The bookmark is set.

Note: In some scenarios, such as Full System HA, applying journal changes is suspended until the bookmark is created and then resumed.

Data Rewind

The Data Rewind recovery method allows you to rewind data to a point in time before it was corrupted. The rewind process takes place on the Replica server before the reverse synchronization process starts. The Data Rewind method uses rewind points or bookmarks that enable you to reset the current data back to a previous state.

You can use this option only if you set the **Recovery - Data Rewind** option to **On.**

If this option is set to Off, the system will not register data rewind points. For more information about Data Rewind parameters (Retention Period, Max Disk Size), see the *Arcserve Continuous Availability* Administration Guide.

Important! The data rewind process operates in one way only - there is no replay forward. After rewind, all data subsequent to the rewind point will be lost, since data after the rewind point will be overwritten with new data.

Note: The automatic registration of the rewind points starts only after the synchronization process is completed, and the message **All modifications during synchronization period are replicated** appears on the Event pane. Similarly, you cannot manually set bookmarks during synchronization.

To recover lost data using rewind points

1. On the Manager, from the Scenario pane select the desired scenario and stop it.

2. [For database applications only] stop the database services on the Master host.

3. On the Manager, from the scenario folder select the Replica host:

   Note: If multiple Replica servers participate in the required scenario, select the Replica from which you want to recover data.

4. From the **Tools** menu, select **Restore Data**, or click the **Restore Data** button.

   The **Recovery Method** page of the Restore Data Wizard opens.

5. Select one of the Rewind data options, depending on whether you want the rewind data synchronized back to the Master (option 2) or left on the Replica only (option 3).

   After you select a Rewind data option, a Recovery scenario is automatically created. This Recovery scenario will run until the end of the rewind process.

6. Click **Next**. The **Rewind Point Selection** page is displayed.

7. Wait until the **Select Rewind Point** button is enabled, and click it to view the existing rewind points.

   The **Select Rewind Point** dialog opens.

   The **Select Rewind Point** dialog displays a list of all rewind points appropriate to the application you are protecting. These include modifications of folders and SQL checkpoints that were automatically registered by the system and user-defined bookmarks.

   The list can be filtered according to the rewind point type or other criteria, using the **Filter Rewind Points** pane on the left.

8. Select the required rewind point, and click **OK.**

   Note: If you want to use a Bookmark as the rewind point, it is best practice to select the closest rewind point that indicates an actual event.

   You return to the **Rewind Point Selection** page, now displaying information about the rewind point you selected.

9. Click **Next**. The **Synchronization Method** page is displayed.

10. Select the **Block Synchronization** method and click **Finish**.

    Arcserve Continuous Availability rewinds the data to the point you selected. After the rewind process ends, you receive the following message 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, Arc-serve Continuous Availability starts a synchronization process from the Replica to the Master. Once the process ends, the temporary Recovery scenario is stopped and then deleted.

11. By default, once a data recovery occurs a Synchronization Report is generated.

    Now, the Replication process can restart on the original scenario.

Chapter 6: Additional Information and Tips

This section contains the following topics:

Spool Directory Settings

The Arcserve Continuous Availability 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 Continuous Availability 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.

New Web Application Creation

After a SharePoint HA scenario failover, do not create any web applications on the Replica before you run a backwards scenario. Creating new web applications makes the configuration between Master and Replica different, which prevents you from running a backwards scenario.

If you want to create a new web application after a SharePoint HA scenario failover, you must set the load balancing URL for the new application as http://WFEMaster:Port after running the backwards scenario, instead of the default value, http://WFERplica:Port.

Back up Farm Data After Failover

After failover, do not process a whole farm backup on the Replica (Active server).

Reconfigure Scenarios Created in Previous Versions

Due to the auto-configuration, SharePoint HA scenarios created with previous versions of Arcserve Continuous Availability must be reconfigured. Launch the SharePoint configuration wizard from the Windows Start menu on the Replica to disconnect it from the Master's farm. Repeat the auto-configuration process.

Recovering Servers

Arcserve Continuous Availability can detect when a Replica server is active and run the recovery process automatically. If recovery does not complete correctly for some reason, do the following:

- Perform the Recover Active Server procedure. For more information, see Recover Active Server.

- If the Recover Active Server procedure does not resolve the issue, try one or more of the following manual tasks appropriate to the redirection method you use:

  - If IP Redirection is used, manually remove the IP. You cannot use this method for scenarios that do not support Move IP redirection (Hyper-V HA, CS HA). For more information, see [Manually Recover a Failed Server-Move IP Address.](#)

  - If Switch Computer Name Redirection is used, manually switch the names. You cannot use this method for scenarios that do not support Switch Computer Name Redirection (Hyper-V HA, Exchange HA, vCenter HA if local Oracle is used). For more information, see [Manually Recover a Failed Server-Switch Computer Name](#).

  - If both IP and Switch Computer Name Redirection methods are used, manually remove the IP and switch the computer names. You cannot use this method for scenarios that do not support Move IP and Switch Computer Name redirection (Exchange, CS HA). For more information, refer to the topic, [Manually Recover a Failed Server-IP and Switch Computer Name](#).

Manually Recover a Failed Server-Move IP Address

If IP Redirection is used, you must remove the IP address manually. You cannot use this method for scenarios that do not support Move IP redirection (Hyper-V HA, CS HA).

To recover a failed server using Move IP Address redirection method

1. Boot the Master server without a network connection, to avoid IP conflicts.

2. From the TCP/IP properties dialog, remove the additional IP address.

3. Reboot the server and reconnect to the network.

4. If it is not already running, start the scenario from the Manager. If automatic reverse replication was set to On, the scenario runs in backward mode so that the Replica server is now active and the Master server is on standby.

5. Wait for synchronization to complete.

6. Perform a manual switchover to return the active role to the Master server. It is recommended that you do so outside of normal business hours.

Manually Recover a Failed Server-Switch Computer Name

If Switch Computer Name Redirection is used, you must switch the names manually. You cannot use this method for scenarios that do not support Switch Computer Name Redirection (Hyper-V HA, Exchange HA, vCenter HA if local Oracle is used).

To manually recover a failed server using the Switch Computer Name redirection method

1. Boot the Master server without a network connection, to avoid duplicate network names.

2. Rename the server to <NewServerName>-RHA and move it to a temporary workgroup.

   For example, if the server is "Server1", rename it to "Server1-RHA". You will be required to reboot this computer. After the reboot completes, the following error appears: "At least one Service could not be started." Ignore this, it is normal under these circumstances because the Arcserve Continuous Availability Engine usually runs in a domain account.

3. Connect to the network.

4. Rejoin the domain, make sure that you use the -RHA name assigned in step 2.

5. Reboot the computer.

6. If it is not already running, start the scenario from the Manager. (If automatic reverse replication was set to On, the scenario runs in backward mode so that the Replica server is now active and the Master server is now standby.)

7. Wait for synchronization to complete. Perform a manual switchover to make the Master server active. It is recommended that you do so outside of normal business hours.

Manually Recover Failed Server-IP and Switch Computer Name

If both IP and Switch Computer Name Redirection methods are used, you must remove the IP address and switch the computer names manually. You cannot use this method for scenarios that do not support Move IP Address and Switch Computer Name redirection (Exchange, CS HA).

To manually recover a failed server using both IP and Switch Computer Name redirection methods

1. Repair any hardware problems that could have caused the switchover, if any.

2. Reboot the server without a network connection to prevent IP conflicts.

3. From the TCP/IP properties dialog, remove the additional IP address.

4. From the System Properties, Computer Name dialog, change the Computer Name to <ServerName>-RHA. For example, if your server is called Server 3, rename it to Server 3-RHA.

5. Assign the server to a temporary workgroup.

6. Restart the computer to enable your changes to take effect. When rebooting completes, reconnect to the network now. Ignore the message, "At least one service failed during system startup." This is normal because the Engine runs in a domain, which is not currently available.

7. Rejoin the domain, making sure you use the -RHA name, and reboot again.

8. The reverse scenario begins and the Replica server assumes the active role. Wait while synchronization completes.

9. Perform a manual switchover by clicking the Perform Switchover button from the toolbar, to return the active role to the Master server.