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 CA 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 CA. This Documentation is confidential and proprietary information of CA 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 CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

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 CA 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 CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA 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 CA 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 CA 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 CA.

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.

Copyright © 2012 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.
Product References

This document references the following CA Technologies products:

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

Throughout this Guide, the term, CA ARCserve RHA, is used to represent the entire product family, which was previously sold as CA XOsoft Replication (WANsync) and CA XOsoft High Availability (WANsyncHA).

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At arcserve.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.
Documentation Changes for the CA ARCserve RHA Installation Guide

The following documentation updates have been made since the last release of this documentation:

- Updated to include user feedback, enhancements, corrections, and other minor changes to help improve the usability and understanding of the product or the documentation itself.
## Contents

### Chapter 1: CA ARCserve RHA Components and Deployment

Replication and High Availability Components ................................................................. 9
  - Control Service .............................................................................................................. 9
  - Engine .......................................................................................................................... 10
  - Management Center ................................................................................................. 11
  - PowerShell .................................................................................................................. 11
  - CA ARCserve RHA for Microsoft Failover Cluster ...................................................... 12
CA ARCserve RHA Deployment .......................................................................................... 13

### Chapter 2: Requirements and Configurations of CA ARCserve RHA Components

Control Service Requirements ........................................................................................... 16
Engine Requirements ........................................................................................................ 17
Management Center Requirements .................................................................................. 17
PowerShell Requirements ............................................................................................... 18
Cluster System Requirements .......................................................................................... 18

### Chapter 3: Requirements of Supported Applications and Databases

Supported Application and Database Servers ...................................................................... 20
File Server Replication and High Availability ................................................................. 20
  - File Server Requirements .......................................................................................... 21
  - File Server Log On Account ...................................................................................... 21
  - File Servers Operating in a Workgroup ...................................................................... 21
Microsoft Exchange Server Replication and High Availability .......................................... 21
  - Exchange Server Replication .................................................................................... 22
  - High Availability for Exchange Server ....................................................................... 23
Microsoft SQL Server Replication and High Availability ................................................... 24
  - SQL Server Replication ............................................................................................. 24
  - High Availability for SQL Server ............................................................................... 25
IIS Server High Availability .............................................................................................. 27
  - IIS HA Configurations ............................................................................................... 27
  - IIS HA Log On Account ............................................................................................. 29
Oracle Server High Availability ........................................................................................ 29
  - Oracle HA Configurations ......................................................................................... 29
  - Oracle HA Log On Account ....................................................................................... 30
Oracle Servers Operating in a Workgroup ......................................................................... 30
Microsoft Hyper-V Server Replication and High Availability ......................................................... 30
Hyper-V Server Replication ........................................................................................................... 30
High Availability for Hyper-V ....................................................................................................... 30
Microsoft SharePoint Server Replication and High Availability .................................................. 32
Replication for SharePoint Server .................................................................................................. 32
High Availability for SharePoint Server ......................................................................................... 33
vCenter Server Replication and High Availability ........................................................................ 41
vCenter Server Replication.............................................................................................................. 41
High Availability for vCenter Server .............................................................................................. 42
Microsoft Dynamics CRM Replication and High Availability ....................................................... 43
CA ARCserve RHA Configuration for Dynamics CRM ................................................................. 43
UNIX/Linux Configuration .............................................................................................................. 44
Full System High Availability ........................................................................................................ 45
Configure BlackBerry for CA ARCserve RHA ............................................................................... 46
Additional CA ARCserve RHA Installation and Configuration Information for BlackBerry .......... 47
Control Service High Availability ................................................................................................ 47
Control Service HA Configuration ................................................................................................. 47
Control Service HA Log On Account ............................................................................................ 48

**Appendix A: Install, Upgrade and Uninstall CA ARCserve RHA**

Register Windows Installer ........................................................................................................... 50
Initial CA ARCserve RHA Installation ......................................................................................... 50
Component Installation Workflow ................................................................................................. 51
Install CA ARCserve RHA for Microsoft Failover Cluster ......................................................... 52
Upgrade an Installation ................................................................................................................ 52
Upgrade in Phases ........................................................................................................................ 54
XONET Proxy Application ............................................................................................................ 54
InstallShield Package .................................................................................................................... 55
Uninstall v4 and Proxy Applications ............................................................................................ 56
Troubleshooting XONET Proxy .................................................................................................... 57
Install the CA ARCserve RHA Control Service .......................................................................... 57
Control Service Installation Considerations .................................................................................. 58
Install a Control Service for a Standard Operation ....................................................................... 58
Install two Control Services for Control Service Role Switching ............................................. 61
Install the Control Service using the CLI ...................................................................................... 63
How to Install the CA ARCserve RHA Engine .......................................................................... 64
Install the Engine Using the Setup.exe Installation File ............................................................... 65
Install the Engine Using the Scenario Creation Wizard ............................................................... 66
Install Engine Using the Remote Installer ................................................................................... 68
Install the Engine using the CLI ................................................................................................... 70
Install and Open the Management Center and Manager ............................................................. 71
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the CA ARCserve RHA PowerShell</td>
</tr>
<tr>
<td>Uninstall CA ARCserve RHA</td>
</tr>
<tr>
<td>Uninstall CA ARCserve RHA for Microsoft Failover Cluster</td>
</tr>
<tr>
<td>Troubleshooting CAVSSSoftProv Error</td>
</tr>
<tr>
<td>Troubleshooting RHA Engine Verification Issue</td>
</tr>
<tr>
<td>Appendix B: Install IIS 6.0 Management Compatibility for IIS 7.0/7.5</td>
</tr>
<tr>
<td>Appendix C: Installing SSL Self-Signed Certificate</td>
</tr>
<tr>
<td>Appendix D: Renewing an Expired SSL Certificate</td>
</tr>
<tr>
<td>Appendix E: Installing Oracle Client for Supporting 32-bit Oracle on 64-bit OS</td>
</tr>
<tr>
<td>Appendix F: Acknowledgements</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acknowledgement</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC bind 9.3.2</td>
<td>87</td>
</tr>
<tr>
<td>CAPICOM 2.1.0.1</td>
<td>88</td>
</tr>
<tr>
<td>Zlib 1.2.3</td>
<td>93</td>
</tr>
<tr>
<td>OpenSSL 1.0.0d</td>
<td>94</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
</tr>
</tbody>
</table>
Chapter 1: CA ARCserve RHA Components and Deployment

This section provides an overview of CA ARCserve RHA components, and guidelines for an efficient deployment of these components on the Microsoft Windows platform.

This section contains the following topics:

- Replication and High Availability Components (see page 9)
- CA ARCserve RHA Deployment (see page 13)

Replication and High Availability Components

CA ARCserve RHA consists of the following components:

- **Control Service** (see page 9)
- **Engine** (see page 10)
- **Management Center** (see page 11) - consists of three components: Overview Page, Manager, and Report Center.
- **PowerShell** (see page 11)
- **CA ARCserve RHA for Microsoft Failover Cluster** (see page 12)

Control Service

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

The Control Service receives requests from the Managers, processes them, converts them to particular commands, and passes them on to the Engines. Then, the Control Service receives up-to-date data and events from the Engines, and sends back information and statistics about the scenario's state to the Manager.

The Control Service is also responsible for the authentication and authorization of users. It can also serve as a central point for report handling and storage. The information and statistics that are accumulated by the Control Service can be presented to the user through the Overview Page, Manager, Report Center and PowerShell.
Replication and High Availability Components

All the scenario files are kept on the server that runs the Control Service. If the Control Service is down, the scenario functioning will not be affected. However, for receiving information about the scenario's state, the Control Service must be active. For best results, install the Control Service on a standalone host. If this is not possible, you can install the Control Service on either the Master or Replica servers. However, if the server is down, the connection with the Control Service is lost and scenarios will be unmanageable.

You may protect the CA ARCserve RHA Control Service in separate scenarios. For more information, see Protecting the Control Service in the CA ARCserve RHA Administration Guide.

Engine

The Engine is a service that must be running before any scenario can start. It is installed on every server participating in any given scenario, meaning the Master (source) and Replica (target) hosts. Each Engine supports both Master and Replica functionality, for both Replication and High Availability scenarios. It may participate in multiple scenarios and serve in a different role in each scenario. Engines can be installed either locally on each host at a time, or through a remote installer on numerous hosts at once, and can be installed during scenario creation, if needed.
Management Center

The Management Center consists of three components, none of which requires any manual installation:

- **Overview Page** - a statistical overview of the Replication and High Availability scenario state.
- **Manager** - a User Interface that lets you create, configure, manage and monitor scenarios. This is a GUI application that is activated from the Overview Page by clicking the Scenario Management link.

- **Report Center** - an interface that gathers all existing reports, along with information about the available reports per scenario. You can decide where these reports will be stored, and for how long they will be displayed and saved in the Report Center.

PowerShell

The PowerShell is offered as an alternative if you do not want to manage the replication process using the Manager graphic user interface. It enlarges and facilitates the capabilities of the CLI provided in previous versions, and it supports both replication and HA operations.
The PowerShell is a command-line shell and scripting environment that allows you to configure a replication scenario and control and monitor the replication process. All scenarios managed by the PowerShell look and operate exactly as the ones that are managed by the Manager, and they are automatically saved in the same default location: INSTALL_DIR/ws_scenarios.

The PowerShell is based on the standard Windows PowerShell™, which comes with a large set of built-in commands with a consistent interface. The PowerShell component adds a number of scenario-related commands, called snap-ins, which facilitate scenario management.

**CA ARCserve RHA for Microsoft Failover Cluster**

CA ARCserve RHA for Microsoft Failover Cluster includes a virtual disk resource plug-in and a lightweight interface installed on every node in the cluster.

Though high availability is built in to Microsoft cluster environments, shared storage could still be a single point of failure. CA ARCserve RHA protects cluster storage, allowing you to replicate data to a disk resource on or off-premises.
CA ARCserve RHA Deployment

The deployment of CA ARCserve RHA components depends on the size of your IT enterprise network and your replication and HA needs. However, there are certain guidelines that you should follow when designing your Replication and High Availability environment and deploying the different components on a Windows platform. The following section provides information regarding an efficient deployment of CA ARCserve RHA components.

The following illustration shows a typical deployment of CA ARCserve RHA components:

- **CA ARCserve RHA Control Service**
  The Control Service must be able to connect to all Master and Switchover Replica servers. It is not mandatory that the Control Service have a direct connection to each non-Switchover Replica server in the scenarios.

  We recommend installing the Control Service on a separate server. If you are working with High Availability scenarios, do not install the Control Service on either the Master or the Replica hosts.

  You can install the Control Service on your local workstation. However, you should be aware that if this workstation is disabled or offline, you will not be able to monitor or manage your scenarios.

- **CA ARCserve RHA Engine**
  The Engine must be installed on each Master and Replica server that participates in the defined scenarios.

- **CA ARCserve RHA Management Center**
This component can be opened from any workstation that has a browser and network connectivity to the Control Service.

- **CA ARCserve RHA PowerShell**
  This component can be opened from any workstation that has Windows PowerShell and network connectivity to the Control Service.
Chapter 2: Requirements and Configurations of CA ARCserve RHA Components

This section provides information regarding the software and configuration requirements of each CA ARCserve RHA component.

**Note:** For the most current list of supported operating systems, see the Release Notes document or go to the website at [arcserve.com](http://arcserve.com).

This section contains the following topics:

- Control Service Requirements (see page 16)
- Engine Requirements (see page 17)
- Management Center Requirements (see page 17)
- PowerShell Requirements (see page 18)
- Cluster System Requirements (see page 18)
Control Service Requirements

Operating Systems

- Windows Server 2003 (32-bit, 64-bit)
- Windows Server 2003 R2 (32-bit, 64-bit)
- Windows Server 2008 (32-bit, 64-bit)
- Windows Server 2008 R2

**Note:** To avoid Microsoft configuration errors, install the Control Service on Windows Server 2003 and Windows Server 2008 R2 systems using the administrator account if you plan to deploy the engine on local hosts using the remote installer.

**Important!** During the Control Service installation, when you enter Service Logon Information, you can either use Administrator Account or define a new account. If you define a new account, the startup state of the OS Computer Browser Service must be enabled, and the Service must be running. On Windows Server 2003, the Computer Browser Service is enabled by default, but on Windows Server 2008, the startup state of the Computer Browser Service is *Disabled* by default. Therefore, if you want to install the Control Service on Windows 2008 and define a new system account for it, before you start the installation you need to change the startup state of the Computer Browser Service to *Automatic*, and start the Service. Because the Computer Browser Service relies on file and printer sharing, you will also need to turn to *On File and Printer Sharing* in the Network and Sharing Center. For more information about enabling the startup state of the Computer Browser Service, see: [http://technet.microsoft.com/en-us/library/bb726965.aspx](http://technet.microsoft.com/en-us/library/bb726965.aspx)

After the installation is complete, you can stop the Computer Browser Service and return its startup state to *Disabled*.

There are several required applications that will be installed automatically during the installation process if they are not already installed on your machine. These applications include:

- Microsoft .NET Framework Version 2.0
- Microsoft ASP.NET 2.0 AJAX Extensions 1.0
- Microsoft Core XML Services 6.0

**User Credentials**

- A Windows user running the CA ARCserve RHA Control Service requires Read-Write permission to the installation directory.
Engine Requirements

The Engine component runs on the following Operating Systems:

- Windows Server 2003 (32-bit, 64-bit)
- Windows Server 2003 R2 (32-bit, 64-bit)
- Windows Server 2008 (32-bit, 64-bit)
- Windows Server 2008 R2 including Server Core Installation
- AIX
- Solaris
- Red Hat Linux
- SuSE Linux
- CentOS

**Important!** During the Engine installation, when you enter Service Logon Information, you can either use Local System Account or define a new account. If you define a new account, the startup state of the OS Computer Browser Service must be enabled, and the Service must be running. On Windows Server 2003, the Computer Browser Service is enabled by default, but on Windows Server 2008, the startup state of the Computer Browser Service is **Disabled** by default. Therefore, if you want to install the Engine on Windows Server 2008 and define a new system account for it, before you start the installation, you need to change the startup state of the Computer Browser Service to **Automatic**, and start the Service. Because the Computer Browser Service relies on file and printer sharing, you will also need to turn to **On File and Printer Sharing** in the Network and Sharing Center. For more information about enabling the startup state of the Computer Browser Service, see: [http://technet.microsoft.com/en-us/library/bb726965.aspx](http://technet.microsoft.com/en-us/library/bb726965.aspx)

After the installation is complete, you can stop the Computer Browser Service and return its startup state to **Disabled**.

Management Center Requirements

Web Browser

- Internet Explorer version 6, 7, 8, or 9.

  **Note:** Enable active scripting in your browser.

Log On Account

- To log in to the Management Center, you must be a member of the Administrators Group on the Local machine where the Control Service is installed.
PowerShell Requirements

Operating Systems

- Windows Server 2003 (32-bit, 64-bit)
- Windows Server 2003 R2 (32-bit, 64-bit)
- Windows Server 2008 (32-bit, 64-bit)
- Windows Server 2008 R2
- Windows Server 2008 32-bit and 64-bit
- Windows Vista
- Windows XP

.NET Framework

- Microsoft .NET Framework 2.0 (build 50727)

You need the .Net Framework for the Windows PowerShell installation. You can download and install it from the Microsoft Download Center.

Microsoft PowerShell

- Microsoft PowerShell version 1.0

Windows Vista SP1 contains PowerShell as a built-in application. If you are using Windows XP or 2003, you can download and install it directly from Microsoft.

Cluster System Requirements

Verify Microsoft Windows 2003, 2008, 2008 R2 is installed on all computers in the cluster. Typical clusters consist of five (5) machines:

- Windows Server 2008 R2 Failover Cluster (x64) as a domain controller and DNS server.
- Several virtual machines running Windows 2008 R2 (x64), joined to the same domain controlled by the first server.
- A fifth machine running FreeNAS.
- Microsoft .NET Framework 3.5 (or later) on all cluster nodes.

Important! Application data and logs must reside on the same volume.

For more information, refer to the Microsoft documentation to make sure your cluster environment is correctly configured.
Chapter 3: Requirements of Supported Applications and Databases

This section provides information about the configurations and log on account requirements of each supported application and database server and for each replication solution.

**Note:** The configurations and requirements of a File Server are described in Installing the CA ARCserve RHA Engine (see page 64).

This section contains the following topics:

- Supported Application and Database Servers (see page 20)
- File Server Replication and High Availability (see page 20)
- Microsoft Exchange Server Replication and High Availability (see page 21)
- Microsoft SQL Server Replication and High Availability (see page 24)
- IIS Server High Availability (see page 27)
- Oracle Server High Availability (see page 29)
- Microsoft Hyper-V Server Replication and High Availability (see page 30)
- Microsoft SharePoint Server Replication and High Availability (see page 32)
- vCenter Server Replication and High Availability (see page 41)
- Microsoft Dynamics CRM Replication and High Availability (see page 43)
- UNIX/Linux Configuration (see page 44)
- Full System High Availability (see page 45)
- Configure BlackBerry for CA ARCserve RHA (see page 46)
- Control Service High Availability (see page 47)
Supported Application and Database Servers

The Replication and High Availability solutions are custom-tailored for the following application and database servers, for both 32-bit and 64-bit Windows:

- File Server
- Microsoft Exchange
- Microsoft SQL
- Microsoft IIS
- Oracle
- Microsoft SharePoint
- Microsoft Hyper-V
- VMware vCenter Server
- CA ARCserve RHA Control Service
- Microsoft Dynamics CRM

CA ARCserve RHA can also transfer full systems to virtual machines. For an up-to-date list of supported platforms and applications, see the CA ARCserve RHA Supported Configurations document at the CA Support website.

Important! For all supported servers, you must statically assign all IP addresses (DHCP-assigned IP addresses on the Master or Replica server are not supported).

File Server Replication and High Availability

This section describes the requirements for running CA ARCserve RHA for File Server.
File Server Requirements

To implement High Availability procedures for File Server, you need to have the following configurations:

- 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 CA ARCserve RHA Release Notes.

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

- Statically assign all IP addresses (DHCP-assigned IP addresses on the Master or Replica server are not supported).

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

File Server Log On Account

The CA ARCserve HA service log on account must satisfy all of the following account conditions:

- 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 machine Administrators Group. If the Domain Admins group is not a member, add the account manually.

File Servers Operating in a Workgroup

For servers in a workgroup, set the CA ARCserve RHA Engine service account to Local System (unless you have added any custom scripts that require higher level permissions). Servers in a workgroup can use Redirect DNS only with DNS servers that allow non-secure updates. You can use Move IP, Switch Computer Name, and custom redirection scripts normally.

Microsoft Exchange Server Replication and High Availability

This section describes the CA ARCserve RHA configuration requirements for Microsoft Exchange Server.
Exchange Server Replication

This section describes the requirements for running CA ARCserve RHA for Exchange Server.

Exchange Replication Configuration

To implement Replication for Exchange Server, you need to have the following configurations:

- 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 CA ARCserve RHA Release Notes.

- Exchange Server installed on both Master and Replica servers, with the same edition, version, service packs and hot fixes installed on each.

- Exchange Server installed with the same login credentials on Master and Replica servers.

- Both servers should have the Mailbox and CAS roles installed. If the Master server is the only server in the Exchange organization that holds the CAS And HUB transfer roles, than the Replica server should have the identical Exchange Server roles installed.

- Both servers should have the identical version of PowerShell installed.

- Both servers should have the same Exchange Administrative Group.

  **Note:** Exchange Server 2010 does not permit you to create two databases with the same name on Master and Replica servers, even if the database is dismounted. Use a name for the Replica database that is less than 64 characters long and follows this convention:

  `<ReplicaName>=<MasterName>_xxxx`

  Where `xxx` = random number.

Exchange Replication Log On Account

The CA ARCserve RHA Engine service log on account must meet all of the following conditions:

- Must be an Exchange View Only Administrator.

- Must be a member of the Administrators Group on the local machine.

  **Note:** If your company's security policy requires even more granular permissions than described, contact CA technical support to receive detailed instructions on permissions required.
Exchange Replication Clusters

With CA ARCserve RHA, working with clusters is nearly identical to working with stand-alone servers. Simply enter the "Exchange Virtual Server Name" as the Master or Replica server name where appropriate.

On Exchange 2007, CA ARCserve RHA supports LCR deployments. No additional configurations are required.

Note: On Exchange 2007, CCR deployments are not supported.

High Availability for Exchange Server

This section describes the requirements for running CA ARCserve HA for Exchange Server.

Exchange HA Configuration

To implement Replication for Exchange Server, you need to have the following configurations:

- 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 CA ARCserve RHA Release Notes.

- Exchange Server installed on both Master and Replica servers, with the same edition, version, service packs and hot fixes installed on each.

- Exchange Server installed with the same login credentials on Master and Replica servers.

- Both servers should have the Mailbox and CAS roles installed. If the Master server is the only server in the Exchange organization that holds the CAS And HUB transfer roles, than the Replica server should have the identical Exchange Server roles installed.

- Both servers should have the identical version of PowerShell installed.

- Both servers should have the same Exchange Administrative Group.

Note: Exchange Server 2010 does not permit you to create two databases with the same name on Master and Replica servers, even if the database is dismounted. Use a name for the Replica database that is less than 64 characters long and follows this convention:

<ReplicaName>=<MasterName>_<xxxx

Where xxx = random number.
Exchange HA Log On Account

The CA ARCserve HA Engine service log on account must meet all of the following conditions:

- Must be a member of the Domain Admins group.
- Must be an Exchange Administrator.
- Must be a member of the Administrators Group on the Local machine.

Note: If your company's security policy requires more granular permissions than described, contact CA ARCserve RHA technical support to receive detailed instructions on the permissions required.

Exchange HA Clusters

With CA ARCserve HA, working with clusters is nearly identical to working with stand-alone servers. Simply enter the "Exchange Virtual Server Name" as the Master or Replica server name where appropriate.

On Exchange 2007, CA ARCserve HA supports LCR deployments. No additional configurations are required.

Note: On Exchange 2007, CCR deployments are not supported.

Microsoft SQL Server Replication and High Availability

This section describes the CA ARCserve RHA requirements for Microsoft SQL Server.

SQL Server Replication

This section describes the requirements for running CA ARCserve RHA for SQL Server.
SQL Replication Configuration

To implement Replication for SQL Server, you need to have the following configurations:

- 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 CA ARCserve RHA Release Notes.

- An instance of SQL Server installed on the Master.

To use the Replication solution with the Assured Recovery option for SQL Server, you need to have the following configurations:

- The same version of Microsoft SQL Server installed on both Master and Replica servers.

- SQL Server installed with the same login credentials on Master and Replica servers.

Also, you must stop the SQL Server service on a Replica host when replication is active.

**Note:** If the SQL Master Database is not replicated, you can detach the replicated databases on the Replica server without stopping the Engine service.

SQL Replication Log On Account

The CA ARCserve RHA Engine service log on account must meet all of the following conditions:

- For stand-alone servers (i.e., non-clustered), use the default of Local System.

- For cluster nodes, use a service account that is a Local Administrator on all cluster nodes.

High Availability for SQL Server

This section describes the requirements for running CA ARCserve HA for SQL Server.
SQL HA Configuration

To implement High Availability procedures for SQL Server, you need to have the following configurations:

■ 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 CA ARCserve RHA Release Notes.

■ One or more instances of Microsoft SQL Server installed on each server:
  - Both servers should have the same SQL version, service packs, and hot fixes installed.
  - Both servers should hold identical SQL Server instances, i.e., default or named.
  - Drive letters containing database files should be identical on both servers.
  - The full path to the default system database of each instance should be identical on both servers.
  - (In the Active Directory environment) Both Master and Replica servers should reside in the same Active Directory forest and be members of the same domain or trusted domains.

■ Verify that the port defined in the Network Configuration TCP/IP properties of the SQL instance(s) is assigned statically and is identical on both Master and Replica.

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

SQL HA Log On Account

The CA ARCserve HA Engine service log on account must satisfy all of the following conditions:

■ 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 machine Administrators Group. If the Domain Admins group is not a member, add the account manually.

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

  **Note:** If your company’s security policy requires more granular permissions than described, contact technical support to receive detailed instructions. For servers in a workgroup, leave the log on user as Local System.
SQL Servers Operating in a Workgroup

For servers in a workgroup, set the CA ARCserve HA Engine service account to a user that is a member of the Local Administrators group. Servers in a workgroup can use Redirect DNS only with DNS servers that allow non-secure updates. You can use Move IP, Switch Computer Name, and custom redirection scripts normally.

When Switch Computer Name is used, you may use the System Account or the Local Administrators group as long as the account was added to the Microsoft SQL logins.

SQL HA Clusters

To install on a cluster, enter the SQL Server's Virtual Server Name as the Master or Replica name.

The only configuration that requires some preparation is the use of IP Move in conjunction with a cluster. For detailed instructions on how to use Move IP with clusters, see the CA ARCserve RHA Microsoft SQL Operation Guide.

IIS Server High Availability

This section describes the requirements for running CA ARCserve HA for Microsoft IIS server.

IIS HA Configurations

To implement High Availability procedures using CA ARCserve HA IIS server, you need to have the following configurations:

- 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 CA ARCserve RHA Release Notes.
  
  - Both servers should have the same level of service packs and hot fixes installed.
  
  - (In the Active Directory environment) Both Master and Replica servers should reside in the same Active Directory forest and be members of the same domain or trusted domains.

- An instance of Microsoft IIS Server 6.0 or 7.0/7.5 installed on each server:
  
  - Both servers should have the same IIS services installed: WWW, SMTP, etc.
  
  - Both servers should have identical web service extensions installed.
  
  - Full paths containing site files should be identical on both servers.

- The standby server should hold a clean installation of IIS with the default sites only.
Sites on the Master server should not use URL redirection or UNC path redirection.

If anonymous access is enabled and used, configure the following:

In order to keep permissions synchronized between the two servers, both IIS processes should use the same user account for anonymous user access. Create a new Domain user account and configure both IIS servers to use it. The following documents describe how to do this:


**Note**: Although the documents do not specify it, you need to edit the Local (or Domain) group policy to allow the user account the following privileges: Allow log on locally, Allow log on as a batch job, and Access this computer from the network. Also, make sure to duplicate any permission changes made to the file system for the original anonymous user account to the newly assigned domain account as well.

In IIS 6.0 and 7.0/7.5, if you define any new application pools on the Master server, you should also define them on the Replica server.

If you are using SSL encryption, see the following MS documents concerning copying the proper certificate:

- For IIS 6.0: How to load balance a Web server farm by using one SSL certificate in Internet Information Services version 6.0 in [http://support.microsoft.com/kb/313299](http://support.microsoft.com/kb/313299)

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

If you are using IIS 7.0/7.5, you need to have IIS 6.0 Management Compatibility installed. Since the IIS 6.0 Management Compatibility is disabled by default when installing IIS 7.0/7.5, you need to enable this option during the IIS 7.0/7.5 installation process (see page 75).
IIS HA Log On Account

The CA ARCserve HA Engine service log on account must satisfy all of the following account conditions:

- 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 machine Administrators Group. If the Domain Admins group is not a member, add the account manually.
- For servers in a work group, use the Local System account.

Note: If your company’s security policy requires more granular permissions than described, contact technical support to receive detailed instructions. Special considerations apply to IIS servers operating workgroups: see the Operation Guide for more information.

Oracle Server High Availability

This section describes the requirements for running CA ARCserve HA for Oracle Server.

Oracle HA Configurations

To implement High Availability procedures using CA ARCserve HA Oracle Server, you need to have the following configurations:

- 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 CA ARCserve RHA Release Notes.
  - Both servers should have the same level of service packs and hot fixes installed.
- Both servers should have the same Oracle version, service packs and hot fixes installed.
- (In the Active Directory environment) Both Master and Replica servers should reside in the same Active Directory forest and be members of the same domain or trusted domains.
- The Oracle SID must match between the Master and Replica servers.
- On both servers, ensure that all Oracle Services normally started at boot have been successfully started and are set to Automatic Startup.
- The path to ORACLE_HOME directory and the path to the database files on the Master and Replica servers must be identical.
To minimize replication traffic, Oracle temporary tablespace(s) are excluded from replication (make sure that the Oracle database on the Replica server is configured with the same temporary tablespace names and path as is used on the Master server).

On both servers, configure Oracle to mount the database automatically on service startup (oradim -edit -sid ORACLE_SID -startmode auto).

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

On UNIX/Linux systems, CA ARCserve RHA requires the 32-bit Oracle Instant Client to support Oracle databases. If you do not already have this client installed, abort CA ARCserve RHA installation, download the Oracle Instant Client from the Oracle website and restart CA ARCserve RHA installation. If the instant client is already installed, you must manually provide the full installation path.

Oracle HA Log On Account

The CA ARCserve HA Engine service log on account must satisfy all of the following conditions:

- 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 machine Administrators Group. If the Domain Admins group is not a member, add the account manually.

Note: If your company’s security policy requires more granular permissions than described, contact technical support to receive detailed instructions.

Oracle Servers Operating in a Workgroup

For servers in a workgroup, set the Engine service account to a user that is a member of the Local Administrators group. Servers in a workgroup can use Redirect DNS only with DNS servers that allow non-secure updates. You can use Move IP, Switch Computer Name, and custom redirection scripts normally.

Microsoft Hyper-V Server Replication and High Availability

Hyper-V Server Replication

This section describes the requirements for running CA ARCserve RHA for Hyper-V Server.
Hyper-V Replication Configuration

To implement Replication for Hyper-V Server, you need to have the following configurations:

- The Master running on Windows Server.
- The Replica running on Windows Server.
- An instance of Hyper-V Server installed on the Master.

**Note:** For a complete list of supported operating systems and applications, see the CA ARCserve RHA Release Notes.

Hyper-V Replication Log On Account

The CA ARCserve RHA Engine service log on account must meet all of the following conditions:

- For stand-alone servers (i.e., non-clustered), use the default of Local System.
- For cluster nodes, use a service account that is a Local Administrator on all cluster nodes.

High Availability for Hyper-V

This section describes the requirements for running CA ARCserve HA for Hyper-V Server.
Hyper-V HA Configuration

To implement High Availability procedures for Hyper-V Server, you need to have the following configurations:

■ 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 CA ARCserve RHA Release Notes.

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

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

■ Statically assign all IP addresses (DHCP-assigned IP addresses on the Master or Replica server are not supported).

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

Do not use the default Hyper-V installation path. Instead, create a new folder, such as c:\vm\ on both Master and Replica. CA ARCserve RHA cannot access the default virtual machine installation path during auto-discovery.

Hyper-V HA Log On Account

The CA ARCserve HA Engine service log on account must satisfy all of the following account conditions:

■ 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 machine Administrators Group. If the Domain Admins group is not a member, add the account manually.

■ For servers in a workgroup, use the Local System account.

Microsoft SharePoint Server Replication and High Availability

Replication for SharePoint Server

This section describes the requirements for running CA ARCserve RHA for SharePoint Server.
SharePoint Replication Configuration

To implement Replication for SharePoint Server, you need to have the following configurations:

- 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 CA ARCserve RHA Release Notes.

- An instance of SharePoint Server installed on the Master.

To use the Replication solution with the Assured Recovery option for SharePoint Server, you need to have the following configurations:

- The same version of SharePoint Server installed on both Master and Replica servers.

- SharePoint Server installed with the same login credentials on Master and Replica servers.

SharePoint Replication Log On Account

The CA ARCserve RHA Engine service log on account must meet all of the following conditions:

- For stand-alone servers (i.e., non-clustered), use the default of Local System.

- For cluster nodes, use a service account that is a Local Administrator on all cluster nodes.

High Availability for SharePoint Server

This section describes the requirements for running CA ARCserve HA for SharePoint Server.
SharePoint HA Configuration

To implement High Availability procedures for SharePoint Server, you need to have the following configurations:

- 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 CA ARCServe RHA Release Notes.

- An instance of a SharePoint Server installed on each server:
  - Both servers should have the same identical service packs and hot fixes.
  - Both servers should reside in the same Active Directory forest, and be members of the same domain or trusted domains.
  - Both servers should use the same port.
  - Both servers should have the same SQL version, service packs, and hot fixes installed.
  - Both servers should hold identical SQL Server instances, i.e., default or named.
  - Drive letters containing database files should be identical on both servers.
  - The full path to the default system database of each instance should be identical on both servers.

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

- Verify that the port defined in the Network Configuration TCP/IP properties of the SQL instance(s) is assigned statically and is identical on both Master and Replica.

- No participating server can be a domain controller or DNS server.

- Master and Replica servers must reside in the same Active Directory forest.
SharePoint HA Log On Account

The CA ARCserve HA Engine service log on account must satisfy all of the following conditions:

■ 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 machine Administrators Group. If the Domain Admins group is not a member, add the account manually.

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

Notes:

■ You should not use a Network Service account. This may prevent the services from functioning properly after a switchover.

■ If your company’s security policy requires more granular permissions than described, contact technical support to receive detailed instructions. For servers in a workgroup, leave the log on user as Local System.
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. CA ARCserve RHA 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 (see page 37)
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 CA ARCServe RHA 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.

   ```
   Windows PowerShell
   Copyright (c) 2009 Microsoft Corporation. All rights reserved.
   PS C:\Users\<USERNAME>\Documents> & set-SPCentralAdministration -Port 8088
   Read me
   How sure you want to perform this action?
   (Y)es, I want to perform this action.  (N)o, I do not want to perform this action.  (Q)uit
   [?] Help (default is "Y")? y
   ```

   For STSADM, enter:
   ```
   stsadm -o setadminport -port <PortNumber>
   ```
The command line interface returns the message, Operation completed successfully.

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\bin

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN\tsadmin.exe -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.

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.

**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
Manually Prepare the Replica for Standalone Deployment

Before you manually prepare the Replica for standalone deployment, collect the following information and read all steps before proceeding:

- The names of the SharePoint Server configuration database and central administration database on the Master server
- The display names, ports, headers, alternate access mapping and content database names for all web applications created on the Master server
- (For SharePoint Server 2007 standalone deployment) The Shared Services Provider name on the Master

You should also view the following Microsoft TechNet documents:

- **Psconfig command-line reference** (SharePoint Server 2010) (cc263093)
- **Command-line reference for the SharePoint Products and Technologies Configuration Wizard** (Office SharePoint Server) (for SharePoint Server 2007)
- **STSADM.exe command line reference**

**Important**! CA ARCserve RHA changes the setting of a Microsoft loopback check to ensure successful high availability scenarios on SharePoint standalone deployments. For more information, see the following Microsoft support information:

- [http://support.microsoft.com/kb/887993](http://support.microsoft.com/kb/887993)
- [http://support.microsoft.com/kb/926642](http://support.microsoft.com/kb/926642)

**To manually prepare the Replica for standalone deployment**

1. Gather the information listed.
2. Read the Microsoft TechNet documents.
   - **Note**: The value of the following parameters should be identical to the ones on the Master: sp_cfdDB, CenAdmContDB, CentralAdminPort.
3. Open a command line session and enter the following commands.

   psconfig.exe -cmd configdb -create -server hostname\inst -database sp_cfdDB -admincontentdatabase CenAdmContDB
   psconfig.exe -cmd installfeatures
   psconfig.exe -cmd secureresources
   psconfig.exe -cmd services -install
   psconfig.exe -cmd services -provision (Valid only for SP2010)
   psconfig.exe -cmd adminvs -provision -port centralAdminPort
4. Create the web applications on the Replica via the Central Administrative site or STSADM tool so all display names, headers, alternate access mapping, content database names and ports are identical to those on the Master. Use the Master hostname with the port as the load balance URL when creating web applications on the Replica. You do not need to create site collections because sub-sites and site collections are stored in the Content Database, which is replicated in CA ARCserve RHA scenarios.

5. Start the services and create Share Services Provider (SharePoint Server 2007) or create the service applications on the Replica so that they are identical to those on the Master using the Central Administrative site.

   **Important!** Do not use the SharePoint products configuration wizard to configure the Replica before you run an HA scenario.

---

vCenter Server Replication and High Availability

vCenter Server Replication

This section describes the requirements for running CA ARCserve RHA for vCenter Server.

vCenter Replication Configuration

To implement Replication for vCenter Server, you need to have the following configurations:

- An instance of vCenter Server installed on the Master.
- 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 CA ARCserve RHA Release Notes.

To use the Replication solution with the Assured Recovery option for vCenter Server, you need to have the following configurations:

- The same version of vCenter Server installed on both Master and Replica servers.
- The vCenter Server installed with the same login credentials on Master and Replica servers.
vCenter Replication Log On Account

The CA ARCserve RHA Engine service log on account must meet all of the following conditions:

- For stand-alone servers (i.e., non-clustered), use the default of Local System.
- For cluster nodes, use a service account that is a Local Administrator on all cluster nodes.

High Availability for vCenter Server

This section describes the requirements for running CA ARCserve HA for vCenter Server.

vCenter Server HA Configuration

To implement High Availability procedures for vCenter Server, you need to have the following configurations:

- 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 CA ARCserve RHA Release Notes.
- Both servers should have the same vCenter version, service packs and hot fixes installed.
- (In the Active Directory environment) Both Master and Replica servers should reside in the same Active Directory forest and be members of the same domain or trusted domains.
- Statically assign all IP addresses (DHCP-assigned IP addresses on the Master or Replica server are not supported).
- No participating server can be a domain controller or DNS server.
- If Database Server is installed locally or remotely to Master, configure Replica to connect to same Database Server.
- If License Server is installed locally to Master, install another instance of the License Server on the Replica and configure the Replica to connect to it.
- If License Server is installed remotely to Master, configure the Replica to connect to this instance.
vCenter HA Log On Account

The CA ARCserve HA Engine service log on account must satisfy all of the following account conditions:

- 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 machine Administrators Group. If the Domain Admins group is not a member, add the account manually.
- For servers in a work group, use the Local System account.

Microsoft Dynamics CRM Replication and High Availability

CA ARCserve RHA Configuration for Dynamics CRM

Microsoft Dynamics CRM is comprised of various server roles that have been combined into two server role groups:

- Application Server Role Group—This group contains the CRM core services, web front end, and help.
- Platform Server Role Group—This group contains the asynchronous processing service, discovery service, and reporting service.
Both server role groups use the SQL reporting service, which can be installed on a separate computer. You can install server role groups on the same computer, or on separate computers.

CA ARCserve RHA for Dynamics CRM can be configured in two ways:

**UNIX/Linux Configuration**

On AIX servers, the hostname is always set to be FQDN. When retrieving FQDN, only DNS is supported. NIS or NIS+ naming service are not supported.

If DNS redirection is used, set the lookup order to order bind, hosts in `/etc/host.conf`.

A bind package is required for DNS redirection:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Package Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>bind-utils-*</td>
</tr>
<tr>
<td>Solaris</td>
<td>SUNWbind</td>
</tr>
<tr>
<td>AIX</td>
<td>bos.rte.bind_cmds</td>
</tr>
</tbody>
</table>
For Oracle on UNIX/Linux systems, only the File System storage option for database instance datafiles is supported.

Full System High Availability

Full System HA can be configured as follows:

Master server
This server can be any Windows server supported by the Engine. The Master can be a physical or virtual server.

Replica server
The following virtualized environments are supported as the Replica server in Full System scenarios:
- Microsoft Hyper-V
- Citrix XenServer (Xen)
- ESX
- vCenter Server
- Amazon EC2

Note: For Hyper-V 1.0, ensure all patches are installed, particularly KB950050. Go to the Microsoft website for more information. Do not use the default installation path when creating Hyper-V virtual machines. CA ARCserve RHA cannot access the default virtual machine installation path during auto-discovery. Create a new folder such as C:\VM on Master and Replica. During Full System HA scenario creation, specify this folder on the Volume Setting screen.
Configure BlackBerry for CA ARCserve RHA

As most BlackBerry administrators are well aware, configuration information regarding BES is stored almost entirely in the configuration database. This information is critical for proper BES operation, and is also relied upon by CA ARCserve RHA for a successful switchover. The configuration database could be installed on the same machine as BES or on a different machine, depending on the needs of your environment.

Local or same machine installation creates a dependency between SQL and BES, establishing a platform that is tied together and, in regards to high availability, managed together with CA ARCserve RHA for Applications. For this reason, we refer to this solution as All in One Configuration.

If the SQL database is installed on a different machine (distributed configuration), you can combine multiple HA scenarios to decide how much protection to implement:

- **Front-End Configuration**—Create File Server HA scenarios modified to use the provided BlackBerry HA script to protect BES in environments where the separate SQL database is already protected.
- **Back-End Configuration**—Create standard SQL Server HA scenarios to protect the SQL server separately from BES. See the CA ARCserve RHA SQL Operation Guide for more information.

In an environment with two production BES servers and one separate SQL server, you would be required to create three HA scenarios to protect all six servers participating in the scenarios.
Additional CA ARCserve RHA Installation and Configuration Information for BlackBerry

Protecting your BlackBerry Enterprise Server environment with CA ARCserve RHA requires specific configuration and set-up steps. Install BES on the Master and Replica servers, configure the servers for high availability and then connect the database to the scenario.

Complete installation and configuration procedures are explained in detail in the CA ARCserve RHA BlackBerry Enterprise Server Operation Guide.

Control Service High Availability

This section describes the requirements for running HA solution for CA ARCserve RHA Control Service.

Important! The HA solution for Control Service is applicable only from CA ARCserve RHA r12.5 and up.

Control Service HA Configuration

To implement High Availability procedures for CA ARCserve RHA Control Service, you need to have the following configurations:

- 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 CA ARCserve RHA Release Notes.

- An instance of a Control Service installed on each server. Both instances should have the same Control Service version.

- Both servers should have identical service packs and hot fixes.

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

- Both servers should use the same port.

- No participating server can be a domain controller or DNS server.
Control Service HA Log On Account

The CA ARCserve HA Engine service log on account must satisfy all of the following conditions:

- 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 machine Administrators Group. If the Domain Admins group is not a member, add the account manually.
- For servers in a work group, use the Local System account.

Note: If your company's security policy requires more granular permissions than described, contact technical support to receive detailed instructions.
Appendix A: Install, Upgrade and Uninstall CA ARCserve RHA

This section provides instructions on the CA ARCserve RHA Installation process, and describes how to perform an upgrade.

This section contains the following topics:

- Register Windows Installer (see page 50)
- Initial CA ARCserve RHA Installation (see page 50)
- Component Installation Workflow (see page 51)
- Install CA ARCserve RHA for Microsoft Failover Cluster (see page 52)
- Upgrade an Installation (see page 52)
- XONET Proxy Application (see page 54)
- Install the CA ARCserve RHA Control Service (see page 57)
- How to Install the CA ARCserve RHA Engine (see page 64)
- Install and Open the Management Center and Manager (see page 71)
- Install the CA ARCserve RHA PowerShell (see page 72)
- Uninstall CA ARCserve RHA (see page 73)
- Uninstall CA ARCserve RHA for Microsoft Failover Cluster (see page 73)
- Troubleshooting CAVSSSoftProv Error (see page 74)
- Troubleshooting RHA Engine Verification Issue (see page 74)
Register Windows Installer

The Microsoft Windows Installer service must be properly installed and registered to install CA ARCserve RHA. If this service is stopped or damaged, the following error occurs when you install or uninstall certain applications:

Windows Installer Error 1720/1722

There are two ways to avoid this error:
■ Re-register the current Windows Installer service version
■ Download the latest Windows Installer service version

To re-register the current version, click Start, Run and type the following commands:

Msiexec/unregister
Msiexec/regserver

To install the latest Windows Installer service version
1. Go to the Microsoft website and download the latest Windows Installer.
2. Follow Microsoft’s instructions to install the service according to your system requirements.
3. Restart your computer after installation completes.
4. Verify the service is running. Click Start, Run and type the following command:

services.msc

If you are running Vista, type the command in the Start Search box.

The Services screen opens. Look for the Windows Installer service and verify the status is Started. Change the startup type to Automatic, if needed and start the service manually if it is not running.

After Windows Installer is installed and verified, you can install CA ARCserve RHA.

Initial CA ARCserve RHA Installation

Installing CA ARCserve RHA components for the first time is very straightforward. The installation package, which is downloaded from the CA ARCserve RHA Web site, contains an installation file called Setup.exe. This Setup.exe runs a standard installation wizard that guides you through the installation.

■ This installation does not require a reboot or application shutdown.
■ The required level of the Windows Installer (INSTMSI.EXE) is 3.0. Unless otherwise indicated, all supported Operating Systems contain Windows Installer 3.0 as a built-in application.
Standard prompts facilitate the installation. Your only major decision is on which servers to install the different components:

- Install Control Service on a computer that is used to monitor and manage all scenarios.
- Install Engine on both the Master and Replica servers.
- The user who installs CA ARCserve RHA components must have Local Administrative privileges or be a member of Local Administrators Group.

The default installation directory is: 
\[INSTALLDIR\Program Files\CA\ARCServe RHA\component_names.\]

- During the installation process, you are prompted to enter the service account under which the CA ARCserve RHA service runs.
- If you are running High Availability (HA) scenarios, the account under which the CA ARCserve RHA service runs may require privileges in addition to those of the local system account. (See the appropriate CA ARCserve HA Operations Guide for more information.)
- A Windows user account running the CA ARCserve RHA Control Service requires Read-Write permission to the installation directory.
- The service logon account for the CA ARCserve RHA Engine requires Read-Write permission to the installation directory.

## Component Installation Workflow

Installing CA ARCserve RHA basic components consists of several simple steps:

1. Installing the Control Service - install the Control Service on a stand-alone Microsoft server by using the Setup.exe file, selecting the CA ARCserve RHA Control Service option, and following the wizard's instructions.

2. Installing the Manager - open the CA ARCserve RHA Overview Page. By clicking the Scenario Management link on this page, the system automatically installs the CA ARCserve RHA Manager on your local computer.

3. Installing the Engines - open the Manager, and create a new scenario using the Scenario Creation Wizard. During the scenario creation, the system allows you to install the Engine on the Master and Replica hosts that participate in the scenario. You can also install an Engine locally by using the Setup.exe file, or install numerous Engines at once by using the Remote Installer.
Install CA ARCserve RHA for Microsoft Failover Cluster

On each node in your cluster environment, run the CA ARCserve RHA MSFC plug-in called CAARCserveRHAforMSFC.exe or CAARCserveRHAforMSFC64.exe (64-bit version) to launch the InstallShield wizard, which guides you through the process of installing the CA ARCserve RHA Disk Resource for Microsoft Failover Cluster and the CA ARCserve RHA Disk Cluster Manager MMC Snap-in.

Complete the wizard screens to install the CA ARCserve RHA for Microsoft Failover Cluster. You may choose Complete or Custom Setup.

- **Complete** -- installs all program components
- **Custom** -- installs the components you specify

**Note:** After installation, you should restart the CA ARCserve RHA Engine before you create a disk resource. Microsoft .NET Framework 3.5 is required. If the software does not detect it, you are prompted to install it and then retry installation.

During installation, the required processes are added to the Windows Firewall as exceptions. If you are using another firewall product or have manually configured one, you must remember to add the CA ARCserve RHA for Microsoft Failover Cluster processes as exceptions to ensure proper communication between MMC and the CA ARCserve RHA Engine.

Upgrade an Installation

Although CA ARCserve RHA is different from the previous version in many respects, there is no major difference between a new installation and an update to an existing one. The system automatically detects previous components, and the MSI wizard carries out all the required tasks to upgrade the application. Most of the components from a previous version can stay on your network, and you can import existing scenarios and reuse them through the CA ARCserve RHA Manager.

**Important!** Full System scenario must be re-run at least once after you upgrade to r16.0 SP2 from a previous release.

**Note:** The scenarios that were created in the previous version were saved by default in INSTALLDIR:\Program Files\CA/ARCserve RHA\ws_scenarios. For more information about the import process, see CA ARCserve RHA Administration Guide.
For a successful upgrade, the only component you need to remove is the previous CA ARCserve RHA Engine. Therefore, you need to uninstall CA ARCserve RHA from each Master and Replica server. You can either use the Setup.exe file to automate this procedure or you can do it manually before you start the new installation.

**Note:** If you are trying to install the Control Service on a machine that contains a GUI from a previous version, you will get the following message:

A previous version of CA ARCserve RHA has been detected. You don’t need to remove it in order to install the new version.

Click OK, and continue the installation.

**To remove a former Engine using the setup.exe file:**

1. Double-click the Setup.exe installation file. The CA ARCserve RHA Installation wizard appears.
2. Click the Install option. The Install Components page appears.
3. Click the Install CA ARCserve RHA Engine option. Click the Install CA ARCserve RHA Engine option.
   The Choose Setup Language dialog appears.
4. Select from the drop-down list the Installation wizard language you prefer, and click OK.
   A progress bar appears.
5. Once the initial process is completed, the Welcome page appears.
6. Click Next. The system detects that an old Engine exists on your server, and the Information about previous version page appears.
7. To automatically remove the older Engine, click Next. A progress bar appears.
8. Once the removal process is completed, the License Agreement page appears.
9. Follow the wizard’s instructions until the installation is complete, as described on Installing the CA ARCserve RHA Engine (see page 64).

**Note:** All existing bookmarks and rewind points are lost after the upgrade.
Upgrade in Phases

This release of CA ARCserve RHA is backwards compatible with the previous version, so you can upgrade over time.

To run CA ARCserve RHA in a mixed environment, consider the following:

- Upgrade the Control Service first.
- If you are not planning to upgrade the Master and Replica servers at once, make sure you upgrade the Master before the Replica. Backward replication is not supported until both servers are upgraded.
- For HA scenarios, you must upgrade Master and Replica servers at once.
- You cannot create new File Server or application scenarios when the running an older version of the Engine, but may create new CD scenarios.

XONET Proxy Application

The XONET Proxy Application is a TCP/IP-based service that enables prior and current versions of CA ARCserve RHA Engines to exist on the same network port. Use it when you wish to gradually upgrade a large Content Distribution installation base. See the topic, Uninstall v4 and Proxy Applications, when you are ready to remove the previous version.

XONET configuration is automatically performed during the upgrade process. When you install the upgrade to another port, XONET monitors port 25000 and analyzes incoming connections. All v4 connections are routed to port 24000 (default) and all connections for the current version are routed to port 26000 (default).

For more information, see the topic, Installation Program Enhancements.

Note: XONET Proxy supports Windows platforms only.
InstallShield Package

The InstallShield package for CA ARCserve RHA has been enhanced with a new Preserve v4 option to support a phased upgrade plan. Enable this option to retain prior installations when installing the current CA ARCserve RHA version. The installation program modifies the existing port setting stored in the v4 ws_rep.cfg file to 24000 and installs a new ws_rep.cfg file with the port setting of 26000.

The remote installer also supports installations that preserve v4. During scenario verification, the remote installer discovers the versions of all CA ARCserve RHA products installed on the target machine. When v4 is discovered, the Installation Settings dialog contains an additional option, "Uninstall Engine of version 4 before upgrade." This option is enabled by default. If you wish to preserve v4, clear the checkbox to display additional fields. Your v4 scenarios are automatically imported and converted.

**Important!** If you install the XONET Proxy on a Microsoft Cluster, you must also install hot fix T5LT025 or the proxy will not work. To obtain the fix, contact Support to request it.

**Version 4 port**

This is the port number to which the v4 Engine will be moved. The default value, 24000, should not be changed.

**Proxy port**

This is the port number on which the XONET Proxy application listens. The default value, 25000, should not be changed.

**Port number**

This is the port number where the Engine for the current version listens. The default value, 26000, should not be changed.

The installation program also does the following:

- Migrates all v4 Delegated security users into Delegated Security groups corresponding to the current version
- Imports and converts scenarios created in prior version to current version
- Lets you uninstall v4 and proxy applications at will

**Note:** Proxy installation is automatically performed during upgrade; no separate executable exists.
Uninstall v4 and Proxy Applications

You can uninstall v4 and proxy applications manually, on a per-server basis.

To uninstall v4 and Proxy Application

1. Stop the XONET proxy service via Services applet.
2. Run the XONET proxy service with the -uninstall switch to remove the service.
3. Remove the XONET proxy application from the disk, if desired.
4. Uninstall v4 WANsync using the Add/Remove programs option in Windows Control Panel.
5. Edit the Port setting in the ws_rep.cfg file for the current version to 25000.
6. Restart the Engine via Services applet.
Troubleshooting XONET Proxy

**Symptom:**
I cannot access the Engine from the user interface (it is displayed as disconnected).

**Solution:**
Do the following:
1. Verify that the Engine service is up and running (go to the services applet and check the status of the Engine).
2. Verify that proxy service is up and running (go to the services applet and check the status of CAXOProxy service)
3. Verify that the Engine ports for both the v4 and current versions correlate with proxy service ports configuration. Default proxy ports configuration (go to services applet and double-click proxy service entry. Verify parameters in the Path to executable field).
   a. Main proxy port 25000.
   b. v4 proxy port 24000 (v4 Engine port should listen on this port; check v4 ws_rep.cfg).
   c. current version proxy port 26000 (Engine should listen on this port; check ws_rep.cfg).
4. Verify that scenarios for both v4 and the current version refer to the main proxy port (in Scenario, Engine options, the Engine port should be set to the main proxy port default value (25000)).

Install the CA ARCserve RHA Control Service

This section describes how to install the CA ARCserve RHA Control Service.
Control Service Installation Considerations

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

- For standard CA ARCserve RHA Replication and HA operations, you only need to install one Control Service (see page 58). This Control Service will function as the single-point-of-control for all CA ARCserve RHA operations. If you want to replicate the Control Service data WITHOUT performing switchover between two Control Services, you can also install only one Control Service.

  **Note:** To replicate the Control Service data, you will need to create Replication Control Service scenario using the Manager, after you finished installing all CA ARCserve RHA components is completed.

- For replicating the Control Service data and switching roles between the original Control Service and a standby Control Service, you need to install two Control Services (see page 61). One of the installed Control Service will function as the active Control Service, while the other will function as the standby Control Service. For installing two Control Services, you need to repeat the installation process twice, since you can only install one Control Service at a time.

  **Notes:**
  - To apply HA solution on the Control Service, you will need to create HA Control Service scenario using the Manager, after the installation of all CA ARCserve RHA components is completed.
  - You do NOT need an HA license to apply HA solution on the Control Service. However, you do need to register CA ARCserve RHA before creating a scenario for the Control Service.
  - For more information about creating Replication and HA Control Service scenarios, refer to the *CA ARCserve RHA Administration Guide*.

Install a Control Service for a Standard Operation

**To install CA ARCserve RHA Control Service**

1. Double-click the **Setup.exe** installation file. The CA ARCserve RHA Installation wizard appears.
2. Click the **Install** option. The **Install Components** page appears.
3. Click the **Install CA ARCserve RHA Control Service** option. The **Choose Setup Language** dialog appears.
4. Select from the drop-down list the Installation wizard language you prefer, and click **OK**.

   A progress bar appears. Once the initial process is completed, the **Welcome** page appears.
5. Click Next. The License Agreement page appears.

6. Select the I accept check box, and click Next. The Customer Information page appears.

7. Verify that the details in the fields are correct, or change them accordingly. Then, click Next. The Destination Folder page appears.

8. Choose the Control Service installation location by using the Change button, or leave it at the default location. Then, click Next.

   Note: The default installation directory is: \Program Files\CA\ARCserve RHA\component_name. All executables, DLLs and configuration files are located within the INSTALLDIR.

   The SSL Configuration page appears.

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

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

   If you want to use SSL configuration, select the Use SSL Configuration check box. In this case, the communication with the Control Service will be over HTTPS. After you select this option, you need to enter a port number in the SSL Port box, and to enter a certificate file in one of the available certificate type boxes.

Notes:

- When selecting the SSL Configuration option, by default the SSL Port number is 443. However, if this port number is in use in your IT environment, use a different port.

- If you selected the SSL Configuration option, when you open the Overview Page, you need to use the hostname of the Control Service machine (instead of its IP Address). Enter the Control Service Host Name and Port No. as follows: https://host_name:port_no/start_page.aspx

- The .CER and .PEX certificates are Internet security files provided by a third party certificate authorities. These certificates are installed on a Web server, to authenticate the validity of a certain Web site hosted on the server. They are represented by a lock icon near the edge of a browser window when accessing a secure site (beginning with "https://"). After you enter the path and name of a .CER of .PEX certificate in the SSL Configuration page, the CA ARCserve RHA Control Service - InstallShield Wizard installs the certificate and adds SSL certificate meta-information to the Web server. Such meta-information is maintained by the HTTP API in a metastore, and is used to locate certificates for certificate exchange in HTTPS sessions.
If at present you do not have an authorized SSL certificate, you can use the **Self-signed Certificate**. After you select the **Self-signed Certificate** option button, when you try to access the Overview page from a remote machine, you need to install the certificate. For more information, refer to **Installing SSL Self-Signed Certificate** (see page 79).

10. Click **Next**. The **Service Logon Information** page appears.

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

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

12. Click **Next**. The **Control Service Role** page appears.

   **Note**: Only if you want to install two Control Services for role switching (see page 61), select the **Allow the Control Service** check box and define whether the currently installed Control Service will assume the role of the **Active** or **Standby** Control Service.

13. For a typical Control Service installation click **Next**. The **Ready to Install the Program** page appears.

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

14. Click the **Install** button to install the Control Service. The **Installing Control Service** page appears.

15. Once the installation is completed, click **Next**. The following page appears.

16. Click **Finish** to close the wizard. The Control Service is now installed on your selected location.
Install two Control Services for Control Service Role Switching

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

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

To install Control Service for role switching:

1. Double-click the Setup.exe installation file. The CA ARCserve RHA Installation wizard appears.
2. Click the Install option. The Install Components page appears.
3. Click the Install Control Service option. The Choose Setup Language dialog appears.
4. Select from the drop-down list the Installation wizard language you prefer, and click OK.
   A progress bar appears. Once the initial process is completed, the Welcome page appears.
5. Click Next. The License Agreement page appears.
6. Select the I accept check box, and click Next. The Customer Information page appears.
7. Verify that the details in the fields are correct, or change them accordingly. Then, click Next. The Destination Folder page appears.
8. Choose the Control Service installation location by using the Change button, or leave it at the default location. Then, click Next.
   Note: The default installation directory (INSTALLDIR) is: \Program Files\CA\ARCserveRHA\component_name. All executables, DLLs and configuration files are located within the INSTALLDIR.
   The SSL Configuration page appears.
9. The SSL Configuration page allows you to use SSL certificate to secure communication with the Control Service.
   - To use the SSL Configuration option, refer to Installation a Control Service for a Standard Operation (see page 58).
   - To use SSL self-signed certificate, refer to Installing SSL Self-Signed Certificate (see page 79).
10. After you selected the communication configuration, Click Next. The Service Logon Information page appears.
    Select and enter the required information. You can either use Local System Account privileges or provide a user name and a password in the form of Domain/Username.
Install the CA ARCserve RHA Control Service

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

11. Click Next. The Control Service Role page appears.
   To install the Control Service for role switching, select the Allow the Control Service check box. Then, define whether the currently installed Control Service will assume the role of the Active or Standby Control Service.

12. Click Next. The Ready to Install the Program page appears.
   Note: Click the Back button to return to the previous pages and change your configuration.

13. Click the Install button to install the CA ARCserve RHA Control Service. The Installing CA ARCserve RHA Control Service page appears, showing you the progress of the installation.

14. Once the installation is completed, click Next. The InstallShield Wizard completed page appears.

15. Click Finish to close the wizard. The Control Service is now installed on your selected location.

16. Repeat this installation process for the second (Active or Standby) Control service.

17. Install the CA ARCserve RHA Engine (see page 64) on the destination servers of both Control Services.
Install the Control Service using the CLI

You can install the CA ARCserve RHA Control Service using the Command Line Interface.

To install CA ARCserve RHA Control Service using the CLI

- Open the CLI and enter the following:

  CAARCserveRHAManager.exe /S "/v/qn XOLOGIN="[Domain/UserName]" XOPASSWORD="[Password]" XOLANG="[Language]"

Parameters

CAARCserveRHAManager.exe
The setup file of the CA ARCserve RHA Control Service

S, V, QN
Silent installation parameters

Domain/UserName, Password
Enter the required information according to the platform you use and the solution you implement, as described in the Requirements of Supported Applications and Databases chapter (see page 19). If you don't enter the Log On Account details, the default is Local System.

Language
Select the CA ARCserve RHA language, by using one of the following language codes:

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

Note: You cannot use SSL in the Control Service silent installation.

Example: Install the Control Service using the CLI

CAARCserveRHAManager.exe /S "/v/qn XOLOGIN="domain/administrator" XOPASSWORD="abcd" XOLANG="1033"
How to Install the CA ARCserve RHA Engine

This section describes how to install the CA ARCserve RHA Engine.

The following are three ways to install the CA ARCserve RHA Engine:

■ Using the Setup.exe file - install the Engine on one host at a time. This installation method automatically detects an Engine from a previous version, and enables you to remove it during the installation of the new Engine. The installation steps are similar to the Control Service installation steps, as described on Installing the CA ARCserve RHA Control Service.

■ Using the Scenario Creation Wizard - remotely install the Engine on the Master and Replica hosts, during the creation of a new scenario.

■ Using the Remote Installer - remotely install the Engine on one or more hosts at once, by using the Remote Installer wizard.

Installing the CA ARCserve RHA Engine on a Windows Server 2008 R2 Server Core

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

Follow these steps:

1. Navigate to the %programfiles%\Internet Explorer folder on a Windows Server 2008 R2 (non Server Core installation).
2. Locate the ieproxy.dll file and copy it to the following location on the Server Core:
   %systemRoot%\system32
3. To register, enter the following command at the command prompt:
   regsvr32 %systemRoot%\system32\ieproxy.dll
Install the Engine Using the Setup.exe Installation File

To install CA ARCserve RHA Engine using the Setup.exe file

1. Double-click the Setup.exe installation file. The CA ARCserve RHA Installation wizard appears.

2. Click the Install option. The Install Components page appears.

3. Click the Install CA ARCserve RHA Engine option. The Choose Setup Language dialog appears.

4. Select from the drop-down list the Installation wizard language you prefer, and click OK.
   A progress bar appears. Once the initial process is completed, the Welcome page appears.

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

6. On the License Agreement page select the I accept check box, and click Next. The Destination Folder page appears.

7. Verify that the details in the fields are correct, or change them accordingly. Then, click Next. The Custom Setup page appears.
   
   Note: When the Engine option is selected, the Space button is enabled. Clicking this button enables you to see the disk space required for the installation of the selected feature.

8. Click Next. The Service Logon Information page appears.

9. Enter the required information according to the platform you use and the solution you implement, as described in the Requirements of Supported Applications and Databases chapter.
   
   ■ For File Server use the following guidelines:
     ■ For Replication scenarios - it is sufficient to use the Local System Account.
     ■ For clusters (Replication scenarios) - you need to run under the same account as the Cluster Service or under equivalent permissions.
     ■ For High Availability scenarios (including clusters) -
       – You need to run under an account with the Domain Administrative privileges. If the Domain Admins group is not a member of the built-in domain local group Administrators, you must use an account that is.
       – The account also needs to be a member of the local machine Administrators Group. If the Domain Admins group is not a member, add the account manually. For servers in a workgroup, use the Local System account.
10. Click Next. The Ready to Install the Program page is displayed.
11. Click Install. The Installing CA ARCserve RHA Engine page appears.
12. Once the installation is completed, click Next. The InstallShield Wizard Completed page appears.
13. Click Finish to finish the installation.

Install the Engine Using the Scenario Creation Wizard

To install the Engine using the Scenario Creation Wizard

1. On the CA ARCserve RHA Manager, select from the Scenario menu the New option.
   The Scenario Creation Wizard appears.
2. Select the required scenario options, as follows:
   ■ Select the Create a New Scenario option button.
   ■ From the Group drop-down list, select the group to which you want to assign the new scenario, or enter a name for a new group.
3. Click Next. The Select Server and Product Type page appears.
4. Select the required scenario options, as follows:
   ■ From the Select Server Type list, select the type of server that is used in the scenario.
   ■ From the Select Product Type options, select Replication or High Availability Scenario according to your license.
   ■ Note: For using the Tasks on Replica options, refer to the CA ARCserve RHA Administration Guide.
5. Click Next. The Master and Replica Hosts page appears.
6. Enter the following information:
   ■ Scenario Name - accept the default scenario name or enter a new name for the scenario.
   ■ Master Hostname/IP and Replica Hostname/IP - enter the name or IP of the Master and Replica hosts, or use the Browse button to find them.
     Note: When creating an HA scenario we recommend to enter the host IP address (and not the hostname).
   ■ User credentials for hosts verification - enter user credentials that will enable you to access the remote hosts on which the Engines will be installed.
7. Click Next. The Engine Verification page appears.
   Note: If the User credentials for hosts verification dialog appears, enter user credentials that will enable you to access the remote hosts on which the Engines will be installed.
8. The system verifies the connectivity of the Master and Replica hosts you selected in the previous page. Once the connections are verified, the system checks whether an Engine is installed on each host.

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

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

- If all the hosts have an **Installed** version, you can move to the next page.

- If any of the hosts have **Not Installed** under the Current Version column, then you need to install the Engine on these hosts.

  **Note**: If an Engine is not installed on one or both hosts, and you click the **Next** button, the following message appears.

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

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

   **Note**: you can install the Engine on both hosts at once. To perform this, select the check boxes of the two hosts, and then click the **Install** button.

10. Wait until the installation is complete, and the Engine's version no. appears in the **Current Version** column.

11. Click **Next**. The **Master Root Directories** appears.

   Complete the scenario creation by following the wizard's instructions. (For more information about the creation of a new scenario, see **CA ARCserve RHA Administration Guide**.)
Install Engine Using the Remote Installer

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

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

To install Engine using the Remote Installer

1. On the CA ARCserve RHA Manager, from the Tools menu, select Launch Remote Installer.

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

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

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

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

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

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

   Note: To remove hosts from the Selected Hosts pane, select the host and click the Remove button.
4. Once you are satisfied with the host selection, click Next. The User Credentials page appears.

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

   Notes:
   - You must enter exactly the same User Credentials you used for logging into the remote host.
   - If you do not need to provide a Domain value to the selected host, leave the Domain field empty, and enter ".\" before the User name.

6. Click Next. The Preinstall Verification page appears.

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

   Note: If a server's status is reported as an Error, and you verified that the server exists and is properly connected, you can select it and click the Verify Again button. The Remote Installer will repeat the verification process.

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

   Note: If an older Engine version is reported as Installed, you can uninstall it by clicking the Uninstall button. Once the uninstall process ends, click Next.

   The Installation Settings page appears.

   On the Service Logon Information section, select This Account and enter Domain\Username and Password to set the Log On account for the CA ARCserve RHA Engine service.

   Note: Select the Keep the service log on account for existing installations check box, if you want to upgrade an existing Engine and you want CA ARCserve RHA to use the log on account details under which the Engine is installed.

8. Click Next. The Ready to Install page appears.

9. Verify that all desired servers are listed. Then, click the Install button to install the Engine on these servers. A confirmation message appears.

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

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

   The Engine is now installed on all selected servers or cluster nodes.
Install the Engine using the CLI

You can install the CA ARCServe RHA Engine on the Master and Replica servers using the Command Line Interface.

To install CA ARCServe RHA Engine using the CLI

- Open the CLI and enter the following:

  CAARCserveRHAEngine.exe /S "/v/qn XOLOGIN=[Domain\UserName]" XOPASSWORD=[Password]" XOPORT=[Port]" XOLANG=[Language]"

Parameters

CAARCserveRHAEngine.exe

The setup file of the CA ARCServe RHA Engine

S, V, QN

Silent installation parameters

Domain/UserName, Password

Enter the required information according to the platform you use and the solution you implement, as described in the Requirements of Supported Applications and Databases chapter (see page 19). If you don't enter the Log On Account details, the default is Local System.

Port

Enter the port no. The default is 25000.

Language

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

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

Example: Install the Engine using the CLI

CAARCserveRHAEngine.exe /S "/v/qn XOLOGIN=domain\administrator" XOPASSWORD="abcd" XOPORT="25000" XOLANG="1033"
Install and Open the Management Center and Manager

The Management Center and Manager do not require any component or application installed in advance. It is based on a one-click-installation procedure that can be performed from any workstation that has a network connection and a Web browser.

To install the Manager:

1. Open Internet Explorer. On the Address box, enter the Control Service Host Name/IP Address and Port No. as follows:
   http://host_name:port_no/start_page.aspx

   Note: If you selected the SSL Configuration option during the installation of the Control Service, when you open the Overview page, you need to use the hostname of the Control Service machine (instead of its IP Address). Enter the Control Service Host Name and Port No. as follows: https://host_name:port_no/start_page.aspx

   The Login dialog appears.

2. Enter your User Name, Password and Domain and click Log In.

3. The Overview Page appears.

4. On the Quick Start tool bar, click the Scenario Management option.

   A progress bar appears, indicating that the Manager component is currently installed on the local machine.

5. Once the Manager installation is completed, the Manager appears.

   Important! Multiple administrators can simultaneously access CA ARCserve RHA Manager, and they can make any changes anytime they need, depending on their privileges. The last update will be effective as the latest state of the scenario. Therefore, when multiple administrators are working with the Manager on the same time, it is important to be aware that one administrator can unintentionally overwrite the changes another administrator just did. We recommend taking internal measures to prevent the occurrence of this event.
Install the CA ARCserve RHA PowerShepl

This section describes the installation of the CA ARCserve RHA PowerShepl.

To use the CA ARCserve RHA PowerShepl, first you need first to install Windows PowerShepl. Then, install CA ARCserve RHA PowerShepl to add CA ARCserve RHA snap-ins to the PowerShell set of commands.

Important! The CA ARCserve RHA PowerShepl and the CA ARCserve RHA Control Service to which it is connected must have the same version.

To install CA ARCserve RHA PowerShepl:

1. Double-click the Setup.exe installation file. The CA ARCserve RHA Installation wizard appears.
2. Click the Install option. The Install Components page appears.
3. Click the Install CA ARCserve RHA PowerShepl option. The Choose Setup Language dialog appears.
4. Select from the drop-down list the Installation wizard language you prefer, and click OK.
   A progress bar appears. Once the initial process is completed, the Welcome page appears.
5. Click Next. The License Agreement page appears.
6. Select the I accept check box, and click Next. The Destination Folder page appears.
7. Verify that the details in the fields are correct, or change them accordingly. Then, click Next. The Ready to Install the Program page is displayed.
8. Click Install. A progress bar appears.
9. Once the installation is completed, click Finish to finish the installation.
Uninstall CA ARCserve RHA

Uninstalling CA ARCserve RHA components is performed by a simple and standard activity through the Operating System’s Add/Remove Programs in the Control Panel list. You need to uninstall each CA ARCserve RHA component separately.

- The uninstall does not remove the default directory storing the user generated .xmc scenario files that have been set up by the CA ARCserve RHA Manager. The directory is: INSTALLDIR\ws_scenarios.

- There are two additional methods to uninstall the CA ARCserve RHA Engine. These methods are best suited for uninstalling previous Engine versions:
  - Using the Remote Installer (see page 68)
  - Using the Setup.exe file (see page 65)

Uninstall CA ARCserve RHA for Microsoft Failover Cluster

Uninstalling CA ARCserve RHA does not delete the CA ARCserve RHA disk resource and resource type that stores your configuration.

To uninstall completely
1. Delete the CA ARCserve RHA disk resource from storage
2. Use the cluster command to delete the resource type while the cluster is running.

   cluster.exe retype "ARCserve Disk" /delete

You may also delete the resource type from the Microsoft Failover Cluster Manager.
Troubleshooting CAVSSSoftProv Error

**Symptom:**
I get the following error while installing or uninstalling the RHA engine:

Error 27508. Error installing COM+ application CAVSSSoftProv

**Solution:**
Do the following:
1. Restart the operating system.
2. Stop the CA ARCserve RHA Engine service.
3. Run install_engine.bat from the engine root path.
4. Run uninstall_engine.bat from the engine root path.
5. Remove the engine from add/remove programs.
6. Remove COM+ application CAVSSSoftProv application.
7. Reinstall CA ARCServe RHA Engine.

Troubleshooting RHA Engine Verification Issue

**Symptom:**
In windows 2008 workgroup server, when the server login user is a local account in the Administrator group, I get the Verification Failed error. I get this error while verifying the RHA engine.

**Solution:**
To resolve this issue, disable UAC or set the registry entry, LocalAccountTokenFilterPolicy, to 1.

For more information, see article 951016 on microsoft.com.
Appendix B: Install IIS 6.0 Management Compatibility for IIS 7.0/7.5

This section describes the necessary steps for installing IIS 6.0 Management Compatibility for IIS 7.0/7.5. This procedure is required if you want to create an HA scenario for IIS 7.0/7.5.

**Note:** If you intend to create an HA scenario for IIS 7.0/7.5, you need to repeat this process on both the Master and the Replica hosts.

**To install IIS 6.0 Management Compatibility**

1. On the Master or Replica host, open the Server Manager and select the Roles option. Then, click the Add Roles button. The first page of the Add Roles Wizard appears.

2. Click Next. The Select Server Roles window appears.

3. Select the Web Server (IIS) check box, and then click Next. A pop-up message appears, asking you whether to add features required for Web Server (IIS).

4. Click Add Required Features. The Select Server Roles window appears.
5. Click Next.

The Web Server (IIS) window appears.

6. Click Next.

The Select Role Service window appears.
7. On the Role Services list, select the IIS 6 Management Capability check box.

8. Click Next, and follow the Wizard instructions until the completion of the installation.
Appendix C: Installing SSL Self-Signed Certificate

This section describes the necessary steps for installing SSL self-signed certificate. This procedure is required when you are using Self-signed Certificate to secure your communication, and you try to connect to the Control Service from a remote machine in order to open the Overview page.

Installing self-signed certificate

1. On the remote machine, open Internet Explorer. On the Address box, enter the Control Service Host Name and Port No. as follows:
   https://host_name:port_no/start_page.aspx
   
   **Note:** You can not use here the IP address of the Control Service.
   
   A Security Alert appears, asking you whether you want to view the certificate.

2. Click the **View Certificate** button.
   
   The **Certificate** dialog appears:

   ![Certificate Dialog]

3. To locally install the certificate, click the **Install Certificate** button.
The **Certificate Import Wizard** appears:

![Certificate Import Wizard](image)

4. **Click Next.** The **Certificate Store** page appears:

![Certificate Store](image)
5. Select the **Place all certificates in the following store** option button, and click the **Browse** button.

The **Select Certificate Store** dialog appears:

6. Select the **Trusted Root Certification Authorities** store, and click **OK**.

The **Completing the Certificate Import Wizard** page appears:

7. Click **Finish** to complete the certificate import.

A confirmation message appears asking you to confirm the certificate installation.
8. Click **Yes**. A message appears, informing you of the import success:

![Certificate Import Wizard](image)

The import was successful.

9. Click **OK** to close the message. Then, on the **Certificate** dialog click **OK** to close it.

You can now connect to the Control Service machine and open the Overview page.
Appendix D: Renewing an Expired SSL Certificate

This section describes the necessary steps for renewing an expired SSL certificate, either authorized or self-signed. This procedure is required when you are already using SSL Certificate to secure your communication, your current certificate has expired, and you want install a new certificate.

**Note:** You do NOT have to stop the Control Service during the renewal process.

**To renew an expired SSL certificate**

1. Obtain a new certificate, and install it on the machine where the Control Service is running.
2. To remove the old certificate binding, run the following command:
   
   ```
   httpcfg.exe delete ssl -i 0.0.0.0:(CS SSL Port Number)
   ```

   **Note:** The **CS SSL Port Number** parameter is the port number you entered during the Control Service installation. You can find it in the `ws_man.exe.config` file, under the **"ws_port"** value.

   The command result should not return any error. The end of the message should be:

   ```
   ...completed with 0.
   ```

3. To bind the new certificate to the Control Service SSL port, run the following command:

   ```
   httpcfg.exe set ssl -i 0.0.0.0:(CS SSL Port Number) -h (New Certificate SslHash)
   ```
Notes:

- The `httpcfg.exe` parameter is a standard utility for Windows Servers, and you can find it in the Control Service installation directory.

- You can find the `New Certificate SslHash` parameter in the Certificate dialog, on the Details tab, under the Thumbprint value:

![Certificate dialog]

Remember to enter the Thumbprint value WITHOUT the spaces between the characters, like this: 8f40f9904372ccbd3706d72ed25d.

The command result should not return any error. The end of the message should be:

```
...completed with 0.
```

The SSL certificate is now renewed.
Appendix E: Installing Oracle Client for Supporting 32-bit Oracle on 64-bit OS

If you are using 32-bit Oracle on 64-bit OS, you need to install Oracle Client 11.x or up on the Oracle machine, to successfully run Oracle scenario.

To install Oracle Client 11.x

1. Download Oracle Client 11.x from the following location:
2. Install the Instant Client Package - Basic in the current installation directory of the Engine, or in one of the OS default PATH.
Portions of this product include software developed by third-party software providers. The following section provides information regarding this third-party software.

This section contains the following topics:

- ISC bind 9.3.2 Acknowledgement (see page 87)
- CAPICOM 2.1.0.1 Acknowledgement (see page 88)
- Zlib 1.2.3 Acknowledgement (see page 93)
- OpenSSL 1.0.0d Acknowledgement (see page 94)

**ISC bind 9.3.2 Acknowledgement**

Bind 9.3.2 copyright message Copyright (C) 2004, 2005 Internet Systems Consortium, Inc. ("ISC") Copyright (C) 1996-2003 Internet Software Consortium.

This product includes software developed by ISC. The ISC software is distributed in accordance with the following license agreement:

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
CAPICOM 2.1.0.1 Acknowledgement

This product contains a copy of Microsoft CAPICOM 2.1.0.1. All title, rights and interests therein is retained by Microsoft Corporation.

END-USER LICENSE AGREEMENT MICROSOFT PLATFORM SOFTWARE DEVELOPMENT KIT

IMPORTANT READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Microsoft Corporation for the Microsoft software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). An amendment or addendum to this EULA may accompany the SOFTWARE PRODUCT. YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE PRODUCT. IF YOU DO NOT AGREE, DO NOT INSTALL OR USE THE SOFTWARE PRODUCT; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE FOR A FULL REFUND.

1. GRANT OF LICENSE. Microsoft grants you the following rights provided you comply with all terms and conditions of this EULA:

* SOFTWARE PRODUCT. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT on computers, including workstations, terminals or other digital electronic devices residing on your premises ("Computers") to design, develop, and test your software application(s) ("Application") for use with any version or edition of Microsoft Windows 95, Windows 98, Windows NT 4.0, Windows 2000 operating system products and/or any version or edition of any Microsoft operating system product that is a successor to the foregoing and/or any Microsoft product suite that contains any of the foregoing (each a "Microsoft Operating System Product").

* Sample Code. You may modify the sample source code located in the SOFTWARE PRODUCT's "samples" directories ("Sample Code") to design, develop, and test your Application solely for use with a Microsoft Operating System Product. You may also reproduce and distribute the Sample Code in object code form along with any modifications you make to the Sample Code, provided that you comply with the Distribution Terms described below. For purposes of this section, "modifications" shall mean enhancements to the functionality of the Sample Code.

* Redistributable Code. Portions of the SOFTWARE PRODUCT are designated as "Redistributable Code." The text file, LICENSE\REDIST.TXT, lists the Redistributable code and describes distribution rights associated with the Redistributable Code, subject further to the Distribution Terms specified below.
* Distribution Terms. You may reproduce and distribute an unlimited number of copies of the Sample Code and/or Redistributable Code (collectively "Redistributable Components") as described above in object code form, provided that (a) you distribute the Redistributable Components only in conjunction with and as a part of your Application solely for use with a Microsoft Operating System Product; (b) your Application adds significant and primary functionality to the Redistributable Components; (c) you distribute your Application containing the Redistributable Components pursuant to an End-User License Agreement (which may be "break-the-seal", "click-wrap" or signed), with terms no less protective than those contained herein; (d) you do not permit further redistribution of the Redistributable Components by your end-user customers; (e) you do not use Microsoft's name, logo, or trademarks to market your Application; (f) you include a valid copyright notice on your Application; and (g) you agree to indemnify, hold harmless, and defend Microsoft from and against any claims or lawsuits, including attorneys' fees, that arise or result from the use or distribution of your Application. Contact Microsoft for the applicable licensing terms for all other uses and/or distribution of the Redistributable Components.

* Reservation of Rights. Microsoft reserves all rights not expressly granted to you in this EULA.

* Pre-release code. The SOFTWARE PRODUCT may contain prerelease code that is not at the level of performance and compatibility of the final, generally available, product offering. These portions of the SOFTWARE PRODUCT may not operate correctly and may be substantially modified prior to first commercial shipment. Microsoft is not obligated to make this or any later version of the SOFTWARE PRODUCT commercially available. Microsoft grants you the right to distribute test version of your Application created using the PRERELEASE CODE provided you comply with the Distribution Requirements described in Section 1 and the following additional provisions: (a) you must mark the test version of your Application "BETA" and (b) you are solely responsible for updating your customers with versions of your Application that operate satisfactorily with the final commercial release of the PRERELEASE CODE.

2. CONFIDENTIALITY OF PRERELEASE CODE. The PRERELEASE CODE, including its features, is proprietary and confidential information to Microsoft and its suppliers. you agree not to disclose or provide the PRERELEASE CODE, documentation, or any information relating to the PRERELEASE CODE (including features or the results of use or testing) to any third party except as expressly provided herein without Microsoft's express written permission. However, you may disclose confidential information in accordance with judicial or other governmental order, provided you shall give Microsoft reasonable notice prior to such disclosure and shall comply with any applicable protective order or equivalent. You shall not be liable to Microsoft for such information which you can prove (1) is already known to you; (2) becomes publicly known through no wrongful act of you; (3) is rightfully received from a third party without similar restriction and without breach of this Agreement; or (4) is independently developed by you. This provision shall survive the termination or expiration of this Agreement.
3. TRANSFER Internal. You may move the SOFTWARE PRODUCT to a different Computer. Transfer to Third Party. The initial user of the SOFTWARE PRODUCT may make a one-time transfer of the SOFTWARE PRODUCT to another end user. The transfer has to include all component parts, media, printed materials, this EULA, and if applicable, the Certificate of Authenticity. The transfer may not be an indirect transfer, such as a consignment. Prior to the transfer, the end user receiving the transferred SOFTWARE PRODUCT must agree to all the EULA terms. No Rental. You may not rent, lease, or lend the SOFTWARE PRODUCT.

4. LIMITATION ON REVERSE ENGINEERING, DECOMPILATION, AND DISASSEMBLY. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that it is expressly permitted by applicable law notwithstanding this limitation.

5. TERMINATION. Without prejudice to any other rights, Microsoft may cancel this EULA if you do not abide by the terms and conditions of this EULA, in which case you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

6. CONSENT TO USE OF DATA. You agree that Microsoft and its affiliates may collect and use technical information you provide as a part of support services related to the SOFTWARE PRODUCT. Microsoft agrees not to use this information in a form that personally identifies you.

7. NOT FOR RESALE SOFTWARE. SOFTWARE PRODUCT identified as "Not for Resale" or "NFR," may not be resold, transferred or used for any purpose other than demonstration, test or evaluation.

8. ACADEMIC EDITION SOFTWARE. To use SOFTWARE PRODUCT identified as "Academic Edition" or "AE," you must be a "Qualified Educational User." For qualification-related questions, please contact the Microsoft Sales Information Center/One Microsoft Way/Redmond, WA 98052-6399 or the Microsoft subsidiary serving your country.

9. EXPORT RESTRICTIONS. You acknowledge that the SOFTWARE PRODUCT is of U.S. origin. You agree to comply with all applicable international and national laws that apply to the SOFTWARE PRODUCT, including the U.S. Export Administration Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments. For additional information, see .
10. DISCLAIMER OF WARRANTIES. To the maximum extent permitted by applicable law, Microsoft and its suppliers provide to you the SOFTWARE PRODUCT, and any (if any) support services relating to the SOFTWARE PRODUCT ("Support Services") AS IS AND WITH ALL FAULTS; and Microsoft and its suppliers hereby disclaim with respect to the SOFTWARE PRODUCT and Support Services all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) warranties, duties or conditions of or related to: merchantability, fitness for a particular purpose, lack of viruses, accuracy or completeness of responses, results, workmanlike effort and lack of negligence. ALSO THERE IS NO WARRANTY, DUTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE PRODUCT AND ANY SUPPORT SERVICES REMAINS WITH YOU.

11. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL MICROSOFT OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR: LOSS OF PROFITS, LOSS OF CONFIDENTIAL OR OTHER INFORMATION, BUSINESS INTERRUPTION, PERSONAL INJURY, LOSS OF PRIVACY, FAILURE TO MEET ANY DUTY (INCLUDING OF GOOD FAITH OR OF REASONABLE CARE), NEGLIGENCE, AND ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE SUPPORT SERVICES, OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS EULA, EVEN IF MICROSOFT OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

12. LIMITATION OF LIABILITY AND REMEDIES. Notwithstanding any damages that you might incur for any reason whatsoever (including, without limitation, all damages referenced above and all direct or general damages), the entire liability of Microsoft and any of its suppliers under any provision of this EULA and your exclusive remedy for all of the foregoing shall be limited to the greater of the amount actually paid by you for the SOFTWARE PRODUCT or U.S.$5.00. The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails its essential purpose.

13. NOTE ON JAVA SUPPORT. THE SOFTWARE PRODUCT MAY CONTAIN SUPPORT FOR PROGRAMS WRITTEN IN JAVA. JAVA TECHNOLOGY IS NOT FAULT TOLERANT AND IS NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE OR RESALE AS ONLINE CONTROL EQUIPMENT IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, DIRECT LIFE SUPPORT MACHINES, OR WEAPONS SYSTEMS, IN WHICH THE FAILURE OF JAVA TECHNOLOGY COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE. Sun Microsystems, Inc. has contractually obligated Microsoft to make this disclaimer.
14. U.S. GOVERNMENT LICENSE RIGHTS. All SOFTWARE PRODUCT provided to the U.S. Government pursuant to solicitations issued on or after December 1, 1995 is provided with the commercial license rights and restrictions described elsewhere herein. All SOFTWARE PRODUCT provided to the U.S. Government pursuant to solicitations issued prior to December 1, 1995 is provided with "Restricted Rights" as provided for in FAR, 48 CFR 52.227-14 (JUNE 1987) or DFAR, 48 CFR 252.227-7013 (OCT 1988), as applicable.

15. APPLICABLE LAW. If you acquired this SOFTWARE PRODUCT in the United States, this EULA is governed by the laws of the State of Washington. If you acquired this SOFTWARE PRODUCT in Canada, unless expressly prohibited by local law, this EULA is governed by the laws in force in the Province of Ontario, Canada; and, in respect of any dispute which may arise hereunder, you consent to the jurisdiction of the federal and provincial courts sitting in Toronto, Ontario. If this SOFTWARE PRODUCT was acquired outside the United States, then local law may apply.

16. ENTIRE AGREEMENT. This EULA (including any addendum or amendment to this EULA which is included with the SOFTWARE PRODUCT) are the entire agreement between you and Microsoft relating to the SOFTWARE PRODUCT and the support services (if any) and they supersede all prior or contemporaneous oral or written communications, proposals and representations with respect to the SOFTWARE PRODUCT or any other subject matter covered by this EULA. To the extent the terms of any Microsoft policies or programs for support services conflict with the terms of this EULA, the terms of this EULA shall control.

17. The SOFTWARE PRODUCT is protected by copyright and other intellectual property laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is licensed, not sold.

All copyright and other notices contained in CAPICOM must remain in their entirety with such component.
Zlib 1.2.3 Acknowledgement

/* zlib.h -- interface of the 'zlib' general purpose compression library version 1.1.4, March 11th, 2002

Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution. Acknowledgement

Jean-loup Gailly  jloup@gzip.org

Mark Adler  madler@alumni.caltech.edu
OpenSSL 1.0.0d Acknowledgement

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/) and distributed in accordance with the following licensing terms:

LICENSE ISSUES

==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

-------------

/* ====================================================================
   * Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.
   *
   * Redistributions of source code must retain the above copyright
   * notice, this list of conditions and the following disclaimer. 
   * Redistribution and use in source and binary forms, with or without
   * modification, are permitted provided that the following conditions
   * are met:
   * 1. Redistributions of source code must retain the above copyright
   *    notice, this list of conditions and the following disclaimer. 
   * 2. Redistributions in binary form must reproduce the above copyright
   */
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.

*============================================================================*

* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).

*/

Original SSLeay License

-----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscapes SSL.

* This library is free for commercial and non-commercial use as long as
* the following conditions are heared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).

* Copyright remains Eric Young’s, and as such any Copyright notices in
* the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.

* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:

* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:

   * "This product includes cryptographic software written by
     Eric Young (eay@cryptsoft.com)"

   * The word 'cryptographic' can be left out if the routines from the library
     being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from
   the apps directory (application code) you must include an acknowledgement:

   * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
  ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
  IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
  PURPOSE

  * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
    FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
    DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
    GOODS

    * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

    * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
      STRICT

    * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY

    * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

    * SUCH DAMAGE.

* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
Index

A
Acknowledgements • 87
Application and database supported • 20

C
CA ARCserve RHA
  CA ARCserve RHA components, overview • 9
  CA ARCserve RHA, deployment • 13
  CA ARCserve RHA, installing • 49
  CA ARCserve RHA, uninstalling • 73
  CA ARCserve RHA, upgrading • 52
CCR deployments
  Exchange DR • 23
  Exchange HA • 24
Certificate • See SSL
Clusters
  Exchange Server DR • 23
  Exchange Server HA • 24
  installing Engine on, using the Remote Installer • 68
  SQL Server HA • 27
Configuration • See Requirements
Configuring SSL
  for Control Service • 57
Control Service
  defined • 9
  deployment • 13
  HA configuration • 47
  HA Log on account • 48
  installing one for standard operation • 57
  installing two for role switching • 61
  installing using the CLI • 63
  requirements • 16
  SSL configuration • 57
  upgrading • 52

D
Database servers supported • 20
Deployment, CA ARCserve RHA components • 13

E
Engine
  defined • 10
  deployment • 13
  installing • 64
  installing using the Remote Installer • 68
  installing using the Scenario Creation Wizard • 66
  installing using the Setup.exe file • 65
  removing • 52
  requirements • 17
  uninstall using the Remote Installer • 68
  upgrading using the Remote Installer • 68
  upgrading using the Setup.exe file • 52
Exchange Server DR
  CCR deployments • 23
  clusters • 23
  configuration • 22
  LCR deployments • 23
  Log on account • 22
Exchange Server HA
  CCR deployments • 24
  clusters • 24
  configuration • 23
  LCR deployments • 24
  Log on account • 24
Exchange Virtual Server Name • 23, 24

F
File server, log on account • 65

H
Host selection for Engine installation • 68
Hyper-V Server DR
  configuration • 31
  Log on account • 31
Hyper-V Server HA
  configuration • 32
  Log on account • 32

I
IIS Server HA
  configuration • 27
  installing IIS 6.0 Management Compatibility for IIS 7.0 • 75
  Log on account • 29
Installing
  Control Service • 57
  default directory • 57
Engine • 64
Engine, using the Remote Installer • 68
Engine, using the Scenario Creation Wizard • 66
Engine, using the Setup.exe file • 65
IIS 6.0 Management Compatibility for IIS 7.0 • 75
Installing, CA ARCserve RHA • 49
Management Center • 71
Manager • 71
Oracle Client for Supporting 32-bit Oracle on 64-bit OS • 85
PowerShell • 72
SSL self-signed certificate • 73
with Remote Installer • 68

L

LCR deployments
Exchange DR • 23
Exchange HA • 24
Log on account
Exchange DR • 22
Exchange HA • 24
File server • 65
IIS HA • 29
Oracle HA • 30
SQL Server DR • 25
SQL Server HA • 26

M

Management Center
defined • 11
deployment • 13
installing • 71
Manager • 11
Overview Page • 11
Report Center • 11
requirements • 17
Manager
defined • 11
installing • 71

O

Oracle Server HA
configuration • 29
installing Oracle Client for Supporting 32-bit Oracle on 64-bit OS • 85
Log on account • 30
Workgroup • 49
Overview Page • 11

P

PowerShell
defined • 11
deployment • 13
installing • 72
requirements • 18

R

Remote Installer • 68
Removing Engine • 52
Report Center, overview • 11
Requirements • 19
  Control Service • 16
  Engine • 17
  Exchange DR • 22
  Exchange HA • 23
  Hyper-V DR • 31
  Hyper-V HA • 32
  IIS HA • 27
  Management Center • 17
  Oracle HA • 29
  PowerShell • 18
  SharePoint DR • 33
  SharePoint HA • 34
  SQL Server DR • 25
  SQL Server HA • 26
  Supported applications and databases • 19
vCenter DR • 41
vCenter HA • 42

S

Scenario Creation Wizard, installing Engine using • 66
Scenarios, installation directory • 52
Self-signed certificate
installing • 79
selecting • 57
SharePoint Server DR
configuration • 33
Log on account • 33
SharePoint Server HA
configuration • 34
Log on account • 35
SQL Server DR
configuration • 25
Log on account • 25
SQL Server HA
clusters • 27
configuration • 26
Log on account • 26
Workgroup • 27
SSL • 79
configuring for Control Service • 57
installing self-signed certificate • 79
opening the Overview page using • 71
Supported application and database servers • 20

U
Uninstalling CA ARCserve RHA • 73
Upgrading
Control Service • 52
Engine, using the Remote Installer • 68
Engine, using the Setup.exe file • 52
installation • 52
Upgrading, CA ARCserve RHA • 52

V
vCenter Server DR
configuration • 41
Log on account • 42
vCenter Server HA
configuration • 42
Log on account • 43

W
WANSync, upgrading • 52
Workgroup
Oracle Server • 49
SQL Server HA • 27