Installation Guide

Arcserve Replication and High Availability

Version 18.0

arcserve®

Legal Notices

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

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

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

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

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

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

The manufacturer of this Documentation is Arcserve.

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

Arcserve Product References

This document references the following Arcserve products:

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

Chapter 1: Arcserve High Availability Documentation

Arcserve Replication and High Availability documentation contains specific guides and release notes for all major releases and service packs. Click links below to access documentation.

- Arcserve High Availability 18 Release Notes
- Arcserve High Availability 18 Bookshelf

Contact Arcserve

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

https://www.arcserve.com/support

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.

You can access other helpful resources appropriate for your Arcserve product.

Providing Feedback About Product Documentation:

If you have comments or questions about product documentation, please contact us.

Contents

Chapter 1: Arcserve Replication and High Availability Components and Deployment

This section provides an overview of Arcserve Replication and High Availability 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

Arcserve RHA consists of the following components:

- Control Service
- Engine
- Management Center - consists of three components: Overview Page, Manager, and Report Center.
- PowerShell

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.

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 Arcserve RHA Control Service in separate scenarios. For more information, see Protecting the Control Service in the *Arcserve RHA Administration Guide*.

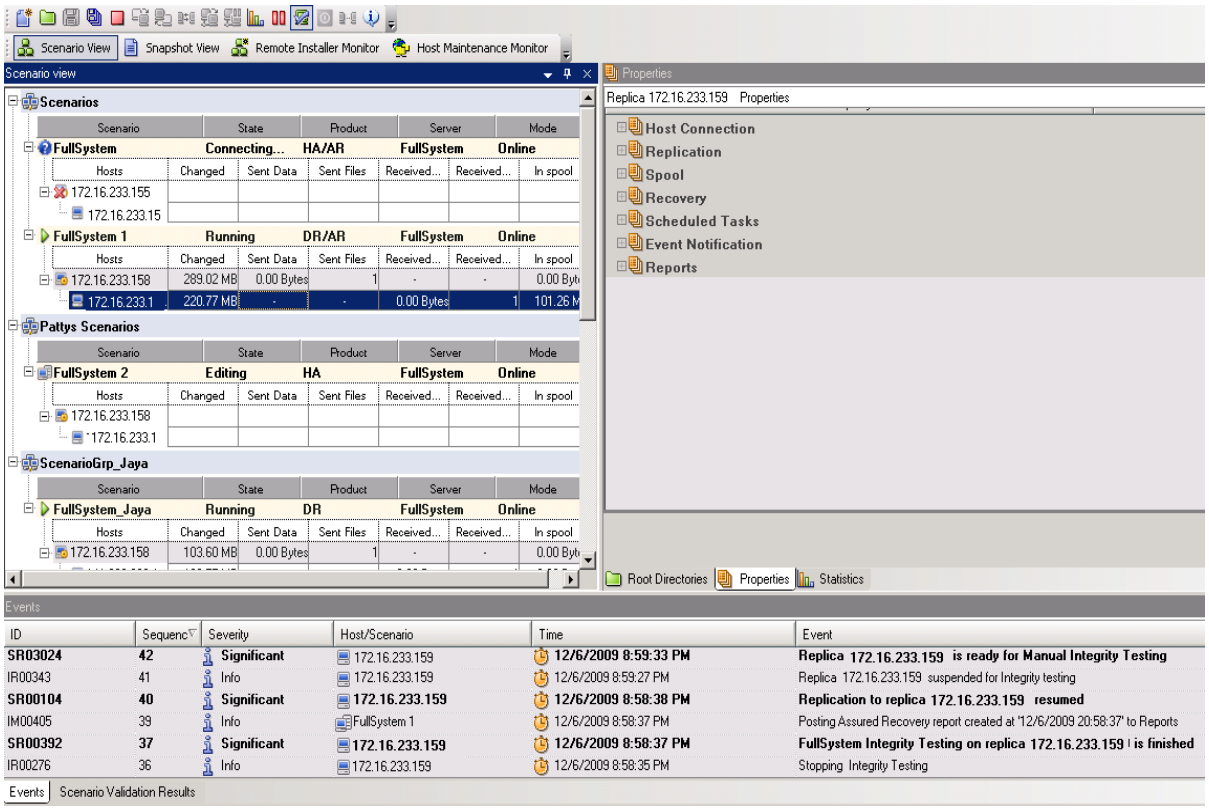
Engine

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.

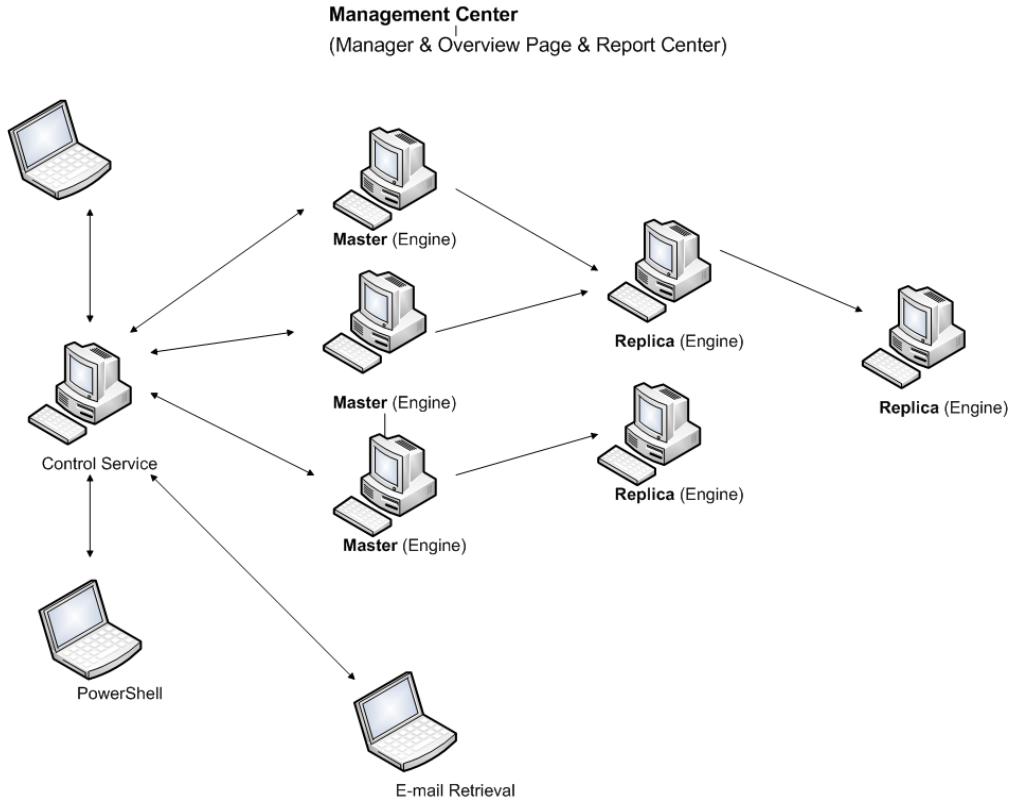
The PowerShell is a command-line shell and scripting environment that allows you to configure a replication scenario and control and monitor the replication process. All scenarios managed by the PowerShell look and operate exactly as the ones that are managed by the Manager, and they are automatically 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.

Arcserve RHA Deployment

The deployment of 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 Arcserve RHA components.

The following illustration shows a typical deployment of Arcserve RHA components:



- **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.

- **Arcserve RHA Engine**

  The Engine must be installed on each Master and Replica server that participates in the defined scenarios.

- **Arcserve RHA Management Center**

  This component can be opened from any workstation that has a browser and network connectivity to the Control Service.

- **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 Arcserve RHA Components

This section provides information regarding the software and configuration requirements of each 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.

Important! If Arcserve Replication and High Availability components belong to different versions, the version of each component must follow the rule *RHA Manager GUI = RHA PowerShell >= Control Service >= Master Engine >= Replica Engine*.

This section contains the following topics:

Control Service Requirements

For the latest information regarding supported systems, see Compatibility Matrix.

Several required applications are installed automatically during the installation process if not already installed on your machine. These applications include:

- Microsoft .NET Framework 4.5 (if 4.0 or above is NOT already installed)

User Credentials

- A Windows user running the Arcserve RHA Control Service requires Read-Write permission to the installation directory.

Engine Requirements

For the latest information regarding supported systems, see Compatibility Matrix.

Important! For Exchange scenario to work correctly on Windows 2008 or 2008 R2, Microsoft .Net framework 4 or above must be installed on both master and replica server. For details, refer to the KB article.

Note: 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 link.

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 8, 9, 10, or 11.

  Note: Enable active scripting in your browser.

- Google Chrome version 76 or later
- Mozilla Firefox version 69 or later

  Note: The ClickOnce plug-in is required for Chrome and Firefox. For more information, see the ClickOnce Requirements section.

Log On Account

- To log into the Management Center, you must be a member of the Administrators Group on the Local machine where the Control Service is installed or corresponding ACL user group if ACL license is used.

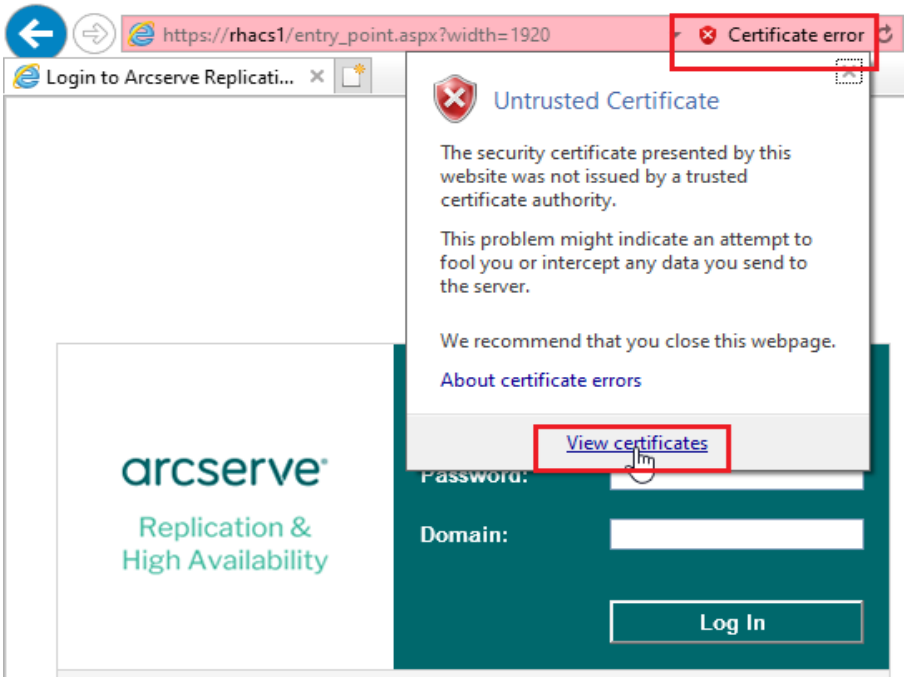
HTTPS Consideration

If Control Service is installed with https and self-signed certificate, the user may not be able to open Scenario Management Manager from a 3rd machine. This issue occurs because the self-signed certificate is not trusted by browser on the 3rd machine, and a trusted connection to Control Service cannot be established.
The user can use a certificate issued by a trusted certificate authority (CA) to install with Control Service to avoid this issue.
As a workaround with self-signed certificate, follow these steps:

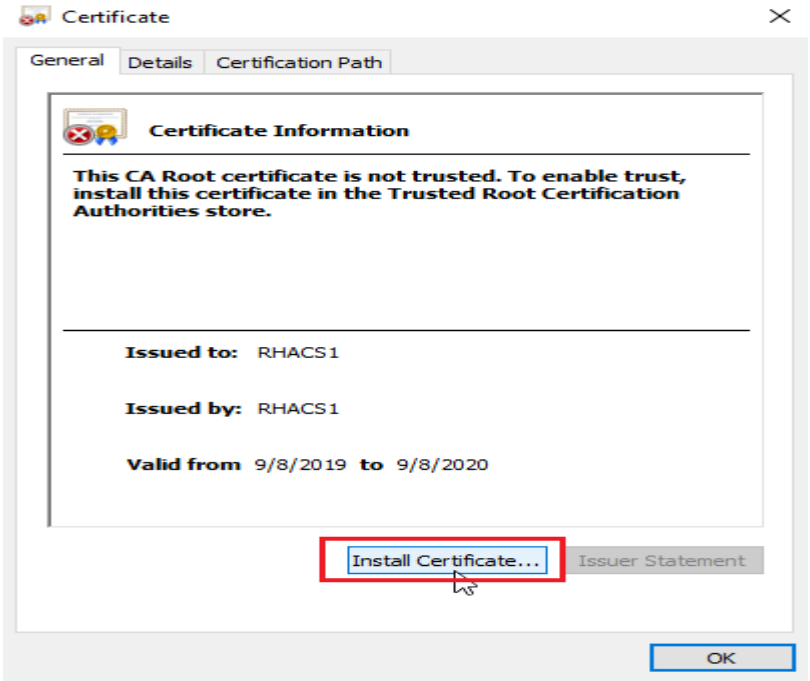
1. On the 3rd machine, open a browser and enter the URL of Control Service. The default URL is https://<cs-hostname>

   Note: You must use only the hostname for <cs-hostname> and not FQDN. This is because during the Control Service installation, a self-signed certificate is generated and issued to <cs-hostname>, and not its FQDN when it is in the domain environment.
   If https://<cs-hostname> cannot navigate to Control Service, make sure your DNS can solve <cs-hostname> correctly. As a simple workaround, add a line in c:\windows\system32\drivers\etc\hosts file.

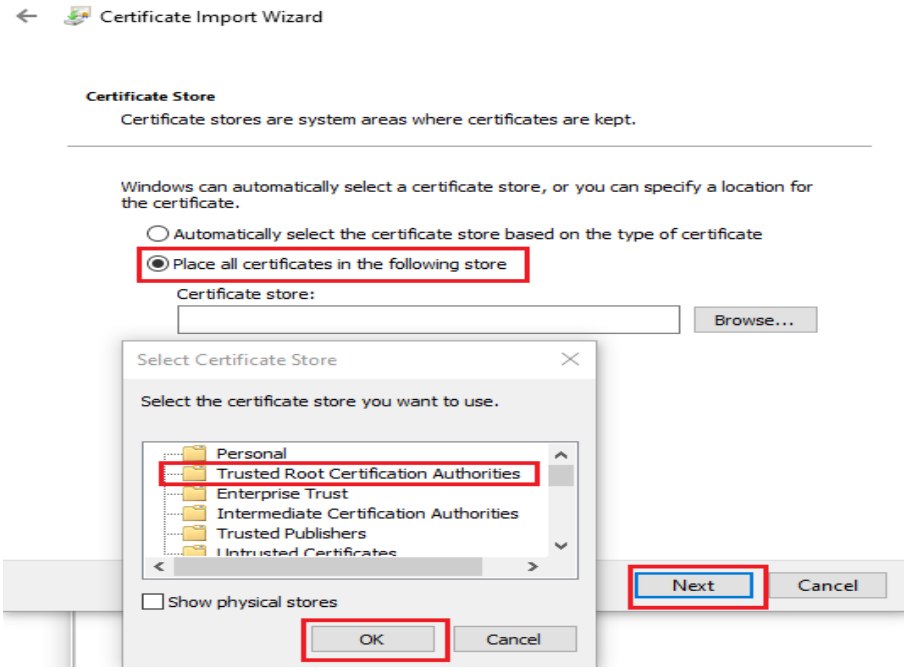
2. Open the Login page. The login page displays the Certificate Error in address bar.



3. Install the certificate of Control Service on the 3rd machine.



4. Select Local Machine, and then click **Next**.
5. Select **Place all certificates in the following store**, and from the Select Certificate Store box, select **Trusted Root Certificate Authorities**.



6. Click **OK**, and then Next.
7. Click **Finish**. A message dialog pops up indicating that the installation of certificate is successful. To close the dialog box, click **OK** twice.
8. Close all browser instances and pages, and then reopen Control Service Login page.

   The Certificate Error icon disappears, and the login page opens successfully.

ClickOnce Requirements

Arcserve RHA product lines use the ClickOnce technology for deploying and running management UI component. For best experience and seamless support for the ClickOnce technology, we recommend installation of browser plug-ins of Chrome and/or Firefox.

The Chrome and Firefox browsers offer multiple third-party plugins, and you can install these plug-ins from Chrome Web Store and/or Firefox Extensions page as needed.

Note: Arcserve does not endorse any particular plug-in and provides the below links only for reference and example.

- **Edge:** By default, ClickOnce is enabled in Microsoft Edge 87, which reduces the barriers for enterprises to deploy software and better align with the Microsoft Edge Legacy browser behavior. Initiated in Microsoft Edge 87, the

ClickOnceEnabled policy's "Not configured" state reflects the new default ClickOnce state of *Enabled* as compared to the previous default state of *Disabled*. To enable the Edge browser for Trusted sites, see the Troubleshooting the Edge Related section.

To enable ClickOnce on an older version of Edge, follow these steps:

1. On the Edge browser, open the following URL:

   edge://flags/#edge-click-once

2. From the ClickOnce Support drop-down list, select **Enabled**.

   ClickOnce is enabled successfully.

- **Chrome:** If you are using the Chrome browser, you may use one of the following ClickOnce plug-ins:
  - **Meta4 ClickOnce Launcher:** https://-chrome.google.com/webstore/detail/meta4-clickonce-launcher/jkncabbipkgbconhaajbapbhokpbgkdc
  - **ClickOnce for Google Chrome:**https://-chrome.google.com/webstore/detail/clickonce-for-google-chro/kekahkplibinaibelipdcikofmedafmb
- **Firefox:** If you are using the Firefox browser, you may use one of the following the ClickOnce plug-ins:
  - **Meta4 ClickOnce Launcher:** https://addons.mozilla.org/en-US/firefox/addon/meta4clickoncelauncher/
  - **Breez ClickOnce:**https://addons.mozilla.org/en-US/firefox/addon/breez-clickonce/

PowerShell Requirements

For the latest information regarding supported systems, see Compatibility Matrix.

.Net Framework

- Microsoft .NET Framework 4.0 or above

You need the .Net Framework for the Windows PowerShell installation. You can download and install it from the Microsoft Download Center if already not installed in the system.

Chapter 3: Install, Upgrade and Uninstall Arcserve Arcserve RHA

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

Register Windows Installer

The Microsoft Windows Installer service must be properly installed and registered to install 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 Arcserve RHA.

Initial Arcserve RHA Installation

Installing Arcserve RHA components for the first time is very straightforward. The installation package, which is downloaded from the 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 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 Arcserve RHA service runs.
- If you are running High Availability (HA) scenarios, the account under which the Arcserve RHA> service runs may require privileges in addition to those of the local system account. (See the appropriate Arcserve HA Operations Guide for more information.)
- A Windows user account running the Arcserve RHA Control Service requires Read-Write permission to the installation directory.
- The service logon account for the Arcserve RHA Engine requires Read-Write permission to the installation directory.

Installation Considerations

Important! The Arcserve Replication and High Availability download image exceeds the amount of free disk space available on a standard compact disk (CD). To copy the download image to media, you must use a DVD or a flash drive.

Consider the following:

- Ensure your screen resolution is set to 1024 x 768 or higher. Lower resolutions may result in cropped screens.
- On Japanese environments, the Launching Application dialog may appear in English. To avoid this problem, apply .NET Framework Japanese Language Pack.
- To avoid firewall issues, install or update the Arcserve Replication and High Availability Engine on Windows Server 2008 Master and Replica servers by running setup.exe **locally**, and then disable **the Verify Arcserve RHA Engine on Hosts** option during scenario creation. If you must **remotely** install the Arcserve Replication and High Availability Engine on these machines, enable WMI traffic through the Windows Server 2008 Firewall, and then configure port 25000 on all Master and Replica machines. In addition, if you are creating Hyper-V scenarios, also enable ICMP echo messages on all Master, Replica, and Hyper-V guest machines so that Arcserve RHA can successfully ping guest operating systems.

  Note: We recommend using the Windows Firewall with Advanced Security MMC snap-in. For more information about using the Windows Firewall with Advanced Security MMC snap-in, refer to the Microsoft website.

  Before remotely installing the Arcserve Replication and High Availability Engine, enable WMI traffic through the firewall:

  1. From the Control Panel, open Security settings and then click **Windows Firewall**.

     The Windows Firewall Settings dialog opens.

  2. Click **Change Settings** and then click the **Exceptions** tab.

     A list of programs and ports is displayed.

  3. Select Windows Management Instrumentation (WMI) to enable WMI traffic through the firewall.

  4. Click **OK** to exit firewall settings.

5. Install the Engine as usual.
6. After you install the Engine, configure port 25000 on each Master and Replica machine using the New Inbound Rule Wizard from the Windows Firewall with Advanced Security MMC snap-in.

   Ensure TCP is selected and add port 25000 to the Specific local ports list. Allow the connection and apply to the applicable profile (for example, Private).

   Note: Port 25000 is the default. You may change this port. For more information about completing the wizard, refer to the Microsoft website.
7. (For Hyper-V scenarios) Enable ICMP echo messages on all Master, Replica and Hyper-V guest machines so that Arcserve RHA can successfully ping Hyper-V guest operating systems.

   Use the New Inbound Rule wizard to create a custom rule that enables Specific ICMP Echo Requests for any IP address and allows the connection.

   Note: For more information, refer to the Microsoft website.

- Installing the Arcserve Replication and High Availability Control Service with ACL-based authentication on domain controllers is not supported.

Component Installation Workflow

Installing 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 **Arcserve RHA Control Service** option, and following the wizard's instructions.
2. Installing the Manager - open the Arcserve RHA Overview Page. By clicking the **Scenario Management** link on this page, the system automatically installs the 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 Arcserve RHA for Microsoft Failover Cluster

This section contains the following topics:

Installation Prerequisites

Before you install Arcserve RHA for Microsoft Failover Cluster, verify that your environment meets the following minimum requirements for Microsoft Failover Cluster.

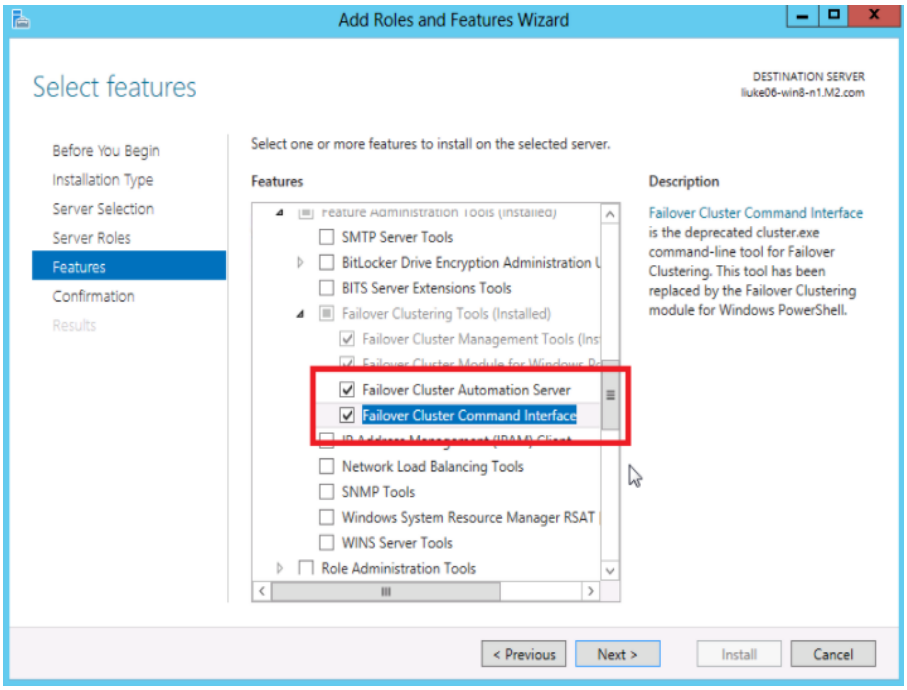
- Ensure that the Arcserve RHA Engine has been installed on all nodes in the cluster. For more information about installing the Engine, see How to Install the Arcserve RHA Engine.
- Ensure Microsoft .NET Framework 3.5 has been installed on all nodes in the cluster.
- Ensure that you have installed the Windows Server Failover Cluster feature and created a failover cluster.

Now you can launch the Install Shield wizard.

Considerations for Microsoft Windows Server 2012

If you are installing Arcserve RHA on Microsoft Windows Server 2012, consider the following points:

- Microsoft Clusters: Microsoft deprecated the cluster.exe command-line tool for Failover Clustering and replaced the tool with the Failover Clustering module for Windows PowerShell. While installing Windows Server 2012 features, make sure you install Failover Cluster Command Interface under the Failover Clustering Tools feature.



- Install .NET Framework 3.5 from Microsoft.com.

Install Arcserve RHA for Microsoft Failover Cluster

On each node in your cluster environment, run the 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 Arcserve RHA Disk Resource for Microsoft Failover Cluster and the Arcserve RHA Disk Cluster Manager MMC Snap-in.

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

- **Complete:** Installs all program components
- **Custom Setup:** Installs the components you specify

Note: After installation, you should restart the 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 Arcserve RHA for Microsoft Failover Cluster processes as exceptions to ensure proper communication between MMC and the Arcserve RHA Engine.

Upgrade an Installation

Although 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. You can import existing scenarios and reuse them through the Arcserve RHA Manager.

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

Note: The scenarios that were created in the previous version were saved by default in *INSTALLDIR:\Program Files\CA\<ca> RHA\ws_scenarios*. For more information about the import process, see *Arcserve RHA Administration Guide*.

For a successful upgrade, the only component you need to remove is the previous Arcserve RHA Engine. Therefore, you need to uninstall 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 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 Arcserve RHA Installation wizard appears.
2. Click the **Install** option. The **Install Components** page appears.
3. Click the **Install Arcserve RHA Engine** option. Click the **Install 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 Arcserve RHA Engine.

   Note: All existing bookmarks and rewind points are lost after the upgrade.

Upgrade in Phases

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

To run 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 simultaneously, make sure you upgrade the Master server first and then the Replica server. Backward replication is not supported until both servers are upgraded.
- For HA scenarios, you must upgrade Master and Replica servers simultaneously.

Note: For more information about the upgrade of Arcserve Continuous Availability to Arcserve RHA, see Upgrade from Arcserve Continuous Availability to Arcserve RHA.

Install the Arcserve RHA Control Service

This section describes how to install the Arcserve RHA Control Service.

This section contains the following topics:

Control Service Installation Considerations

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

- For standard Arcserve RHA Replication and HA operations, you only need to install one Control Service. This Control Service will function as the single-point-of-control for all 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 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. 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 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 Arcserve RHA before creating a scenario for the Control Service.
  - For more information about creating Replication and HA Control Service scenarios, refer to the *Arcserve RHA* Administration Guide.

Install a Control Service for a Standard Operation

To install Arcserve RHA Control Service

1. Double-click the **Setup.exe** installation file. The Arcserve RHA Installation wizard appears.
2. Click the **Install** option. The **Install Components** page appears.
3. Click the **Install 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 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.

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, 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 Installthe 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 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.
- To use SSL self-signed certificate, refer to Installing SSL Self-Signed Certificate.

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/User-name.

    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 Installthe Program** page appears.

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

13. Click the **Install** button to install the Arcserve RHA Control Service. The **Installing 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 Arcserve RHA Engine on the destination servers of both Control Services.

Install the Control Service using the CLI

You can install the Arcserve RHAControl Service using the Command Line Interface.

To install Arcserve RHA Control Service using the CLI

- Open the CLI and enter the following:

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

Parameters

RHAManager.exe

The setup file of the Arcserve 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. If you don't enter the Log On Account details, the default is Local System.

Language

Select the 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

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

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

How to Install the Arcserve RHA Engine

This section describes how to install the Arcserve RHA Engine.

The following are three ways to install the 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 Arcserve RHAControl 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 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
4. Install the Microsoft Visual C++ 2005 Redistributable Package (x64). Download the Redistributable Package from www.microsoft.com.

This section contains the following topics:

Install the Engine Using the Setup.exe Installation File

To install Arcserve RHA Engine using the Setup.exe file

1. Double-click the **Setup.exe** installation file. The Arcserve RHA Installation wizard appears.

   Important! On Windows 2003 and 2008, you may get digital signature error during installation and then the installation rolls back. You need to update the Windows root certificate to avoid this error. Download and install the update from the Microsoft website.

2. Click the **Install** option. The **Install Components** page appears.
3. Click the **Install Arcserve 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 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 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 *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 *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.

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

To install Engine using the Remote Installer

1. On the Arcserve RHA Manager, from the **Tools** menu, select **Launch Remote Installer**.

   The Remote Installer view opens, and the **Remote InstallationWizard** 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 all 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.
   - If you log in using the non-admin local account or domain account without the admin rights, the default setting will change from the Current User to The Following user.

6. Click **Next**. The **Preinstall Verification** page appears.

   The Remote Installer automatically checks the existence, connectivity and configuration of the servers you 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.

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

   Local System Account

   Specifies to use Windows Local system account.

   Current User

   Specifies to use the user account you logged in with.

This Account

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

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

9. Click **Next**. The **Ready to Install** page appears.
10. Verify that all desired servers are listed. Then, click the **Install** button to install the Engine on these servers. A confirmation message appears.
11. Click **Yes** to install the Engine. The **Remote Installer** status pane appears. Wait until the **Server Status** is reported as **Installed.**
12. Close the **Remote Installer** status pane. On the Remote Installer view, the installation status is reported as **Installation complete.**

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

Install the Engine using the CLI

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

To install Arcserve RHA Engine using the CLI

For local system service registration, open the CLI, and then run the following command:

- Without domain credentials

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

- With domain credentials

  E:\Install>RHAEngine64.exe /S "/v/qn XOLOGIN="domain\Administrator" XOPASSWORD="xxxxx" XOPORT="25000" XOLANG="1033" LOCALACCOUNT=No ServiceUserName="domain\Administrator" ServicePassword="*****"

Parameters

RHAEngine.exe

The setup file of the 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. 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

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

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

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 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 Arcserve RHA PowerShell

This section describes the installation of the Arcserve RHA PowerShell.

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

Important! The Arcserve RHA PowerShell and the Arcserve RHA Control Service to which it is connected must have the same version.

To install Arcserve RHA PowerShell:

1. Double-click the **Setup.exe** installation file. The **Arcserve RHA Installation** wizard appears.
2. Click the **Install** option. The **Install Components** page appears
3. Click the **Install Arcserve RHA PowerShell** 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.

   To install Arcserve RHA PowerShell in silent mode, run the following command:

   RHAPowerShell.exe /S "/v/qn"

Uninstall Arcserve RHA

Uninstalling 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 Arcserve RHA component separately.

- The un-install does not remove the default directory storing the user generated .xmc scenario files that have been set up by the Arcserve RHA Manager. The directories are:
  - CA_INSTALL_LOG
  - INSTALLDIR\ws_co
  - INSTALLDIR\ws_root
  - INSTALLDIR\reports
  - INSTALLDIR\ws_events
  - INSTALLDIR\ws_help
  - INSTALLDIR\ws_scenarios
  - INSTALLDIR\ws_template
- There are two additional methods to uninstall the Arcserve RHA Engine. These methods are best suited for uninstalling previous Engine versions:
  - Using the Remote InstallerUsing the Setup.exe file
- The following folders are not removed after Arcserve RHA engine uninstallation:
  - INSTALLDIR
  - INSTALLDIR\vm

Uninstall Arcserve RHA for Microsoft Failover Cluster

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

To uninstall completely

1. Delete the Arcserve RHA disk resource from storage
2. Use the cluster command to delete the resource type while the cluster is running.

   cluster.exe restype "Arcserve Disk" /delete

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

Troubleshooting the Edge Browser Related Issue

Symptom

When you install the RHA Manager using an older version of the Edge Browser such as 86.0.622.38, the RHA Manager installation fails, and the following error occurs:

Deployment and application do not have matching security zones.

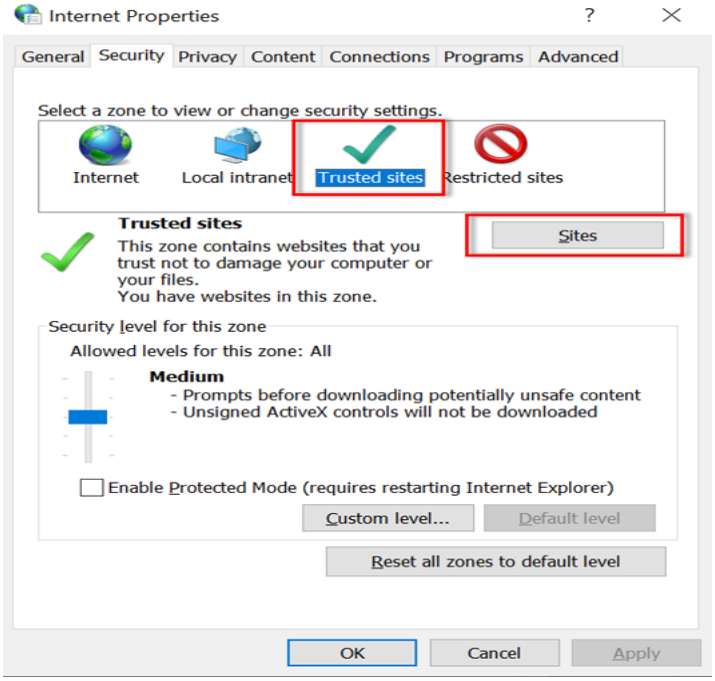
Solution

Add the RHA web portal URL as a trusted site.

To add the RHA web portal URL to the Trusted sites list, follow these steps:

1. Open the Control Panel.
2. Navigate to **Network and Internet** > **Internet Options**.

   The Internet Properties dialog appears.
3. On the Internet Properties dialog, under the Security tab, select the **Trusted sites** icon, and then click **Sites**.

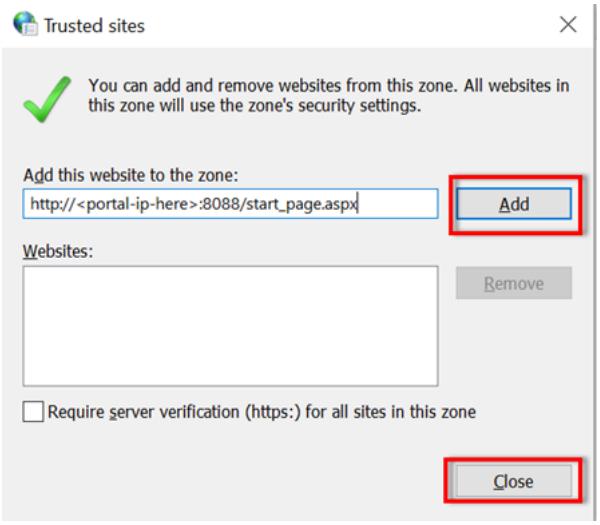


The Trusted sites dialog appears.

4. On the Trusted sites dialog, enter the RHA web portal URL in the Add this website to the zone text field, and then click **Add**.

   Notes:

   - When you add a non-secure URL (starts with *http* rather than *https*), then you must clear the **Require server verification (https:) for all sites in this zone** check box before you click the **Add** button.
   - If you are using an older version of Edge browser, enable the ClickOnce feature. For more information, see ClickOnce Requirements.



5. Click **Close** to close the Trusted sites dialog.

6. Click **OK** on the Internet Properties dialog.

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 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 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.

Troubleshooting Verification Failure when Using the Remote Installer

Symptom:

I get the verification failure error while deploying the Arcserve RHA engine using the Remote Installer.

Solution:

In some setups, the remote WMI requests are disabled and you get the verification failure error. To resolve this error, perform the following steps:

Enable Remote WMI Request

1. On the target server, navigate to Administrative Tools, Computer Management.
2. Expand Services and Applications.
3. Right-click the WMI Control properties.
4. Select the Security tab and click Security.
5. Add the monitoring user (if needed), and then click Remote Enable for the user or group that requests WMI data.
6. Restart the machine or the “Windows Management Instrumentation” service.

If required, perform the following step to allow WMI through firewall.

Allow WMI through Windows firewall

All users (including non-administrators) are able to query WMI data on the local computer. For reading WMI data on a remote server, establish a connection from your management computer to the target server. When the target server is running Windows Firewall (Internet Connection Firewall) like what is shipped with Windows XP and Windows 2003, then you need to tell the firewall to let remote WMI requests to go through. Run the following command on the target computer if it is running a Windows firewall:

```
netsh firewall set service RemoteAdmin enable
```

If you still get the “Access is denied.” error, then grant DCOM remote launch and activation permission to the user or group.

Follow these steps:

1. Click Start, Run, and type DCOMCNFG. Click OK.
2. In the Component Services dialog box, expand Component Services, Computers. Right-click My Computer and click Properties.
3. The My Computer Properties dialog box opens.
4. Click the COM Security tab.
5. From the Launch and Activation Permissions section, click Edit Limits.
6. The Launch and Activation Permission dialog opens.
7. Add your name or group in the Groups or user names list if your name or group does not appear.
8. From the Launch Permission dialog box, select your user and group in the Group or user names box.
9. From the Allow column, Permissions for User/Group, select Remote Launch and select Remote Activation. Click OK.

Chapter 4: 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.

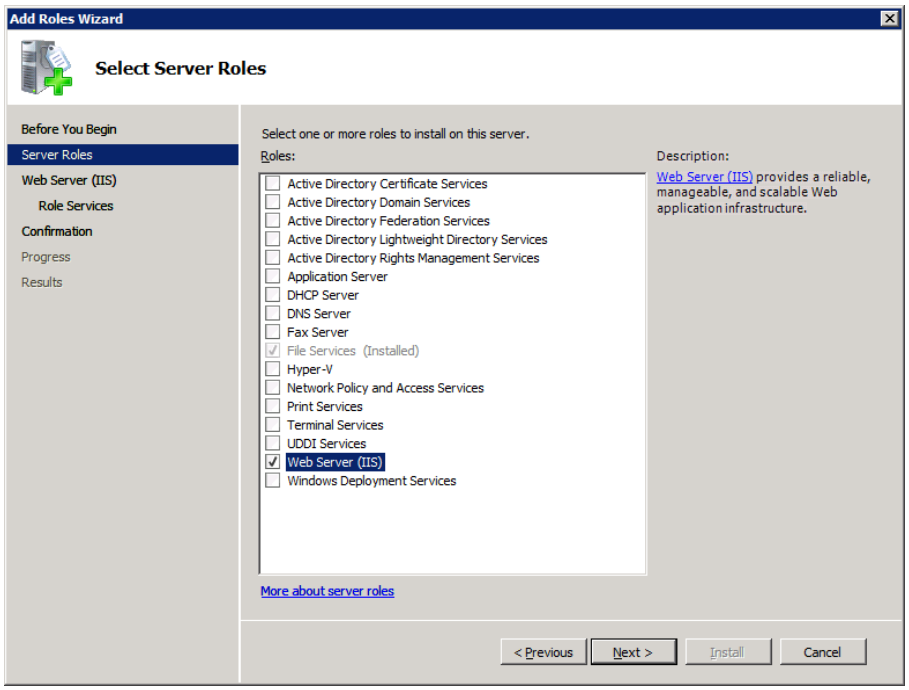
Note: If you intend to create an HA scenario for IIS 7.0/7.5, you need to repeat this process on both the Master and the Replica hosts.

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.

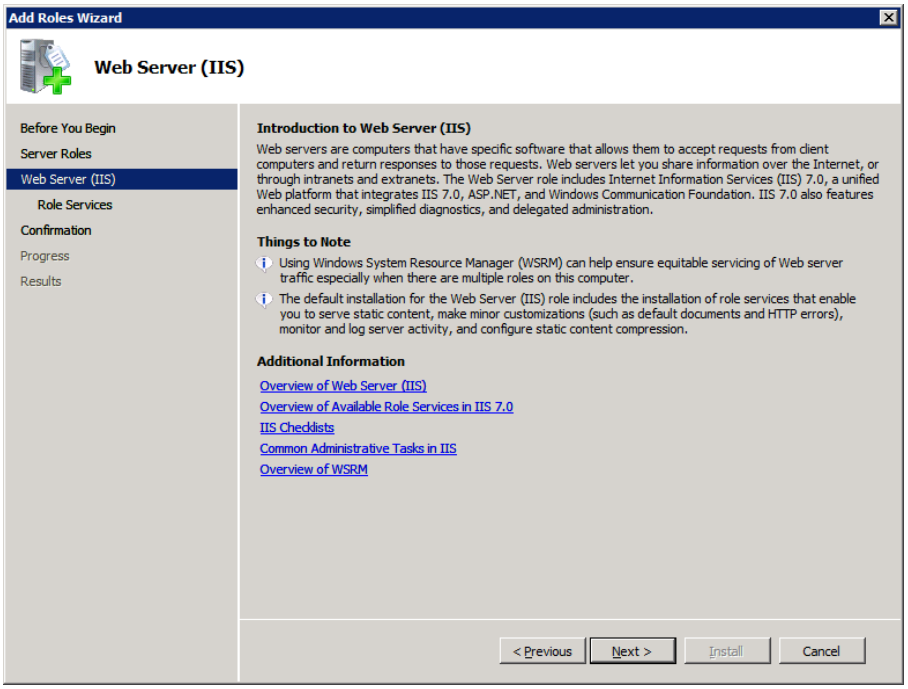
   A pop-up message appears, asking you whether to add features required for Web Server (IIS).

4. Click Add Required Features.

   The Select Server Roles window appears.

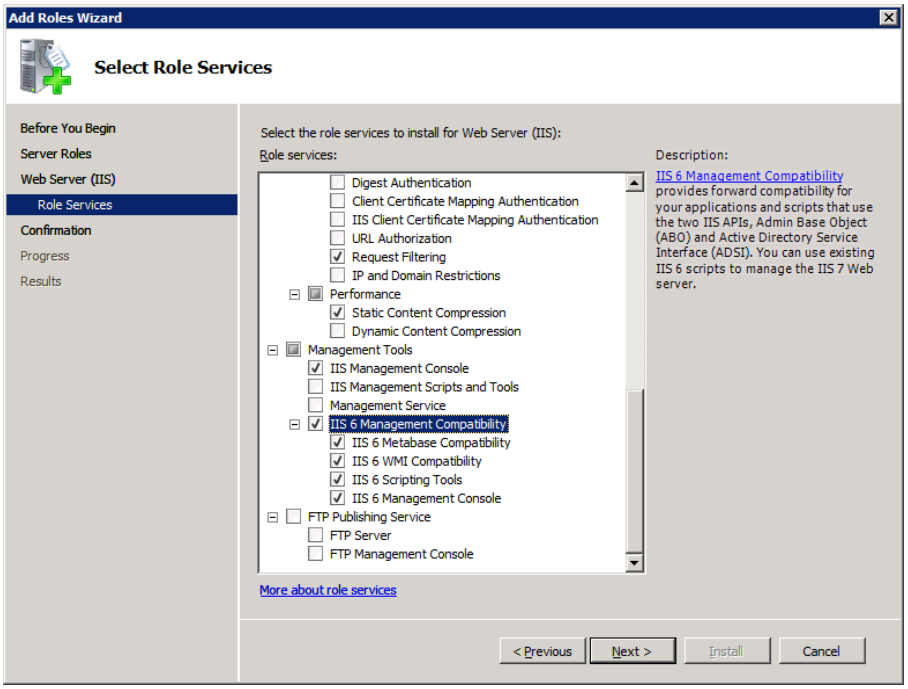
5. Click Next.

   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.

Chapter 5: 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

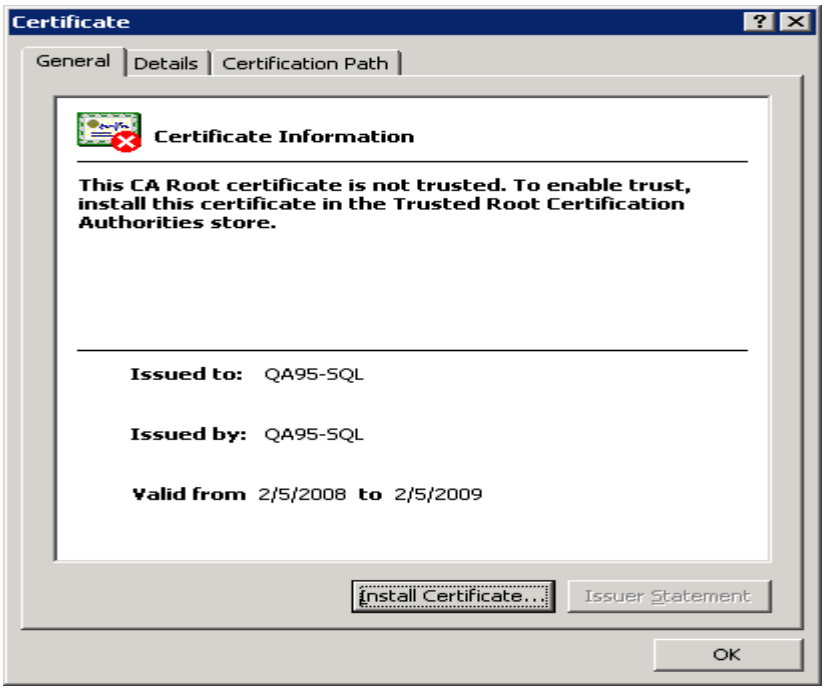
1. On the remote machine, open Internet Explorer. On the **Address** box, enter the Control Service Host Name and Port No. as follows: https://host_name:port_no/start_page.aspx

   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.

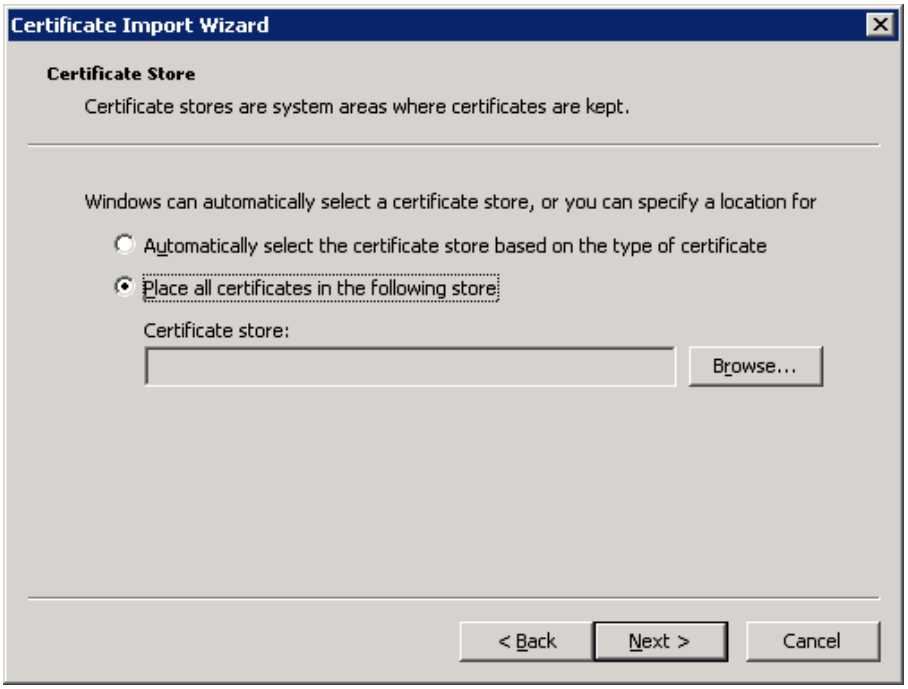
   The **Certificate** dialog appears:



3. To locally install the certificate, click the **Install Certificate** button.

   The **Certificate Import Wizard** appears:

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

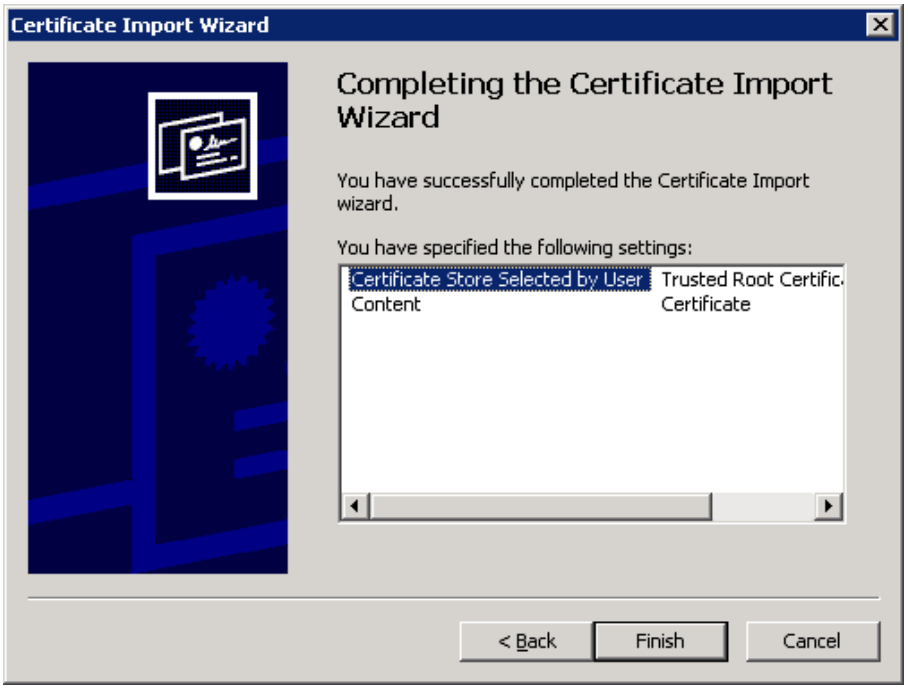


5. Select the **Place all certificates in the following store** option button, and click the **Browse** button.

   The **Select Certificate Store** dialog appears:

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

   The **Completing the Certificate ImportWizard** 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:

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.

Chapter 6: 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.

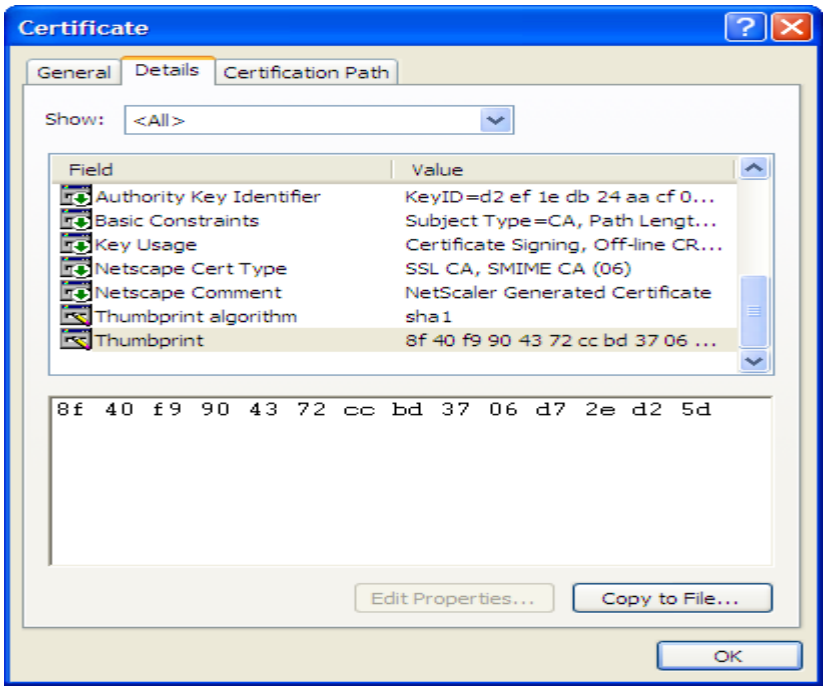
   The command result should not return any error. The end of the message should be:

   …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:



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.

Chapter 7: 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:

   http://www.oracle.com/technology/software/tech/oci/instantclient/htdocs/winx64soft.html

2. Install the **Instant Client Package - Basic** in the current installation directory of the Engine, or in one of the OS default PATH.

Index

A

C

D

E

H

I

M

O

P

R

S

U

W