CA ARCserve® Replication and High Availability and CA ARCserve® D2D

Integrated Solutions Guide for Offsite Data Protection

r16.5

Contents

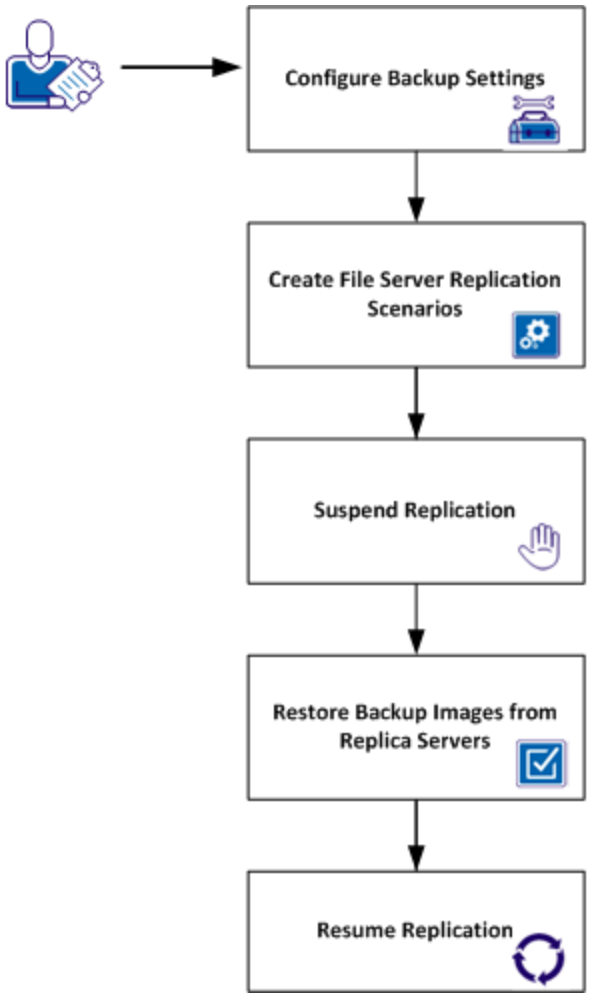
Chapter 1: CA ARCserve Replication and High Availability and CA ARCserve D2D – Working Together as an Integrated Solution

This section contains the following topics:

Introduction

Welcome to the CA ARCserve Replication and High Availability and CA ARCserve D2D Integrated Solutions Guide. This guide describes how to protect offsite backup images of CA ARCserve D2D (and CA ARCserve Central Host-Based VM Backup) data using CA ARCserve Replication and High Availability.

CA ARCserve Replication and High Availability and CA ARCserve D2D are designed to work together to allow a user to replicate CA ARCserve D2D backups to an offsite location for additional security and recoverability. These CA ARCserve D2D backups can then be restored from either the local backup or from the remote replica copy.



Be aware of the following:

- This solution can also be used to replicate CA ARCserve Central Host-Based VM Backup sessions to an offsite location.
- This document is not meant to describe all the options for CA ARCserve Replication and High Availability, CA ARCserve D2D, and CA ARCserve Central Host-Based VM Backup. See the official documentation for each product for more comprehensive information about the proper installation and use of each product.
- Configure Backup Settings (see page 7) and Create File Server Replication Scenarios (see page 8) describe how to utilize the ARCserve D2D option when creating a CA ARCserve Replication scenario.
- Restore a Recovery Point from a Replica (see page 19) describes how to restore CA ARCserve D2D backup data from the replica copy.

Configure Backup Settings

Before using CA ARCserve Replication and High Availability to replicate CA ARCserve D2D backup sessions, you specify the backup settings to be applied to the backup jobs. These settings let you specify behaviors such as the backup source and destination, the schedule for each type of backup, the advanced settings for your backup jobs, and any pre or post backup operations. These settings can be modified at any time from the CA ARCserve D2D home page.

To manage the backup settings, click the Settings link on the CA ARCserve D2D home page to display the Backup Settings dialogs and the subordinate tab options.

When configuring your backup settings, it is important to consider the following best practices:

- Verify that you have configured the CA ARCserve D2D destination before creating the CA ARCserve Replication and High Availability replication scenario. This approach lets CA ARCserve Replication and High Availability detect the backup destination (automatically) and other related information, and then use this information to help create the scenario.
- Verify that your compression and encryption settings are correct. When you change the encryption settings or the compression level (from No Compression to any other compression level) after you create the replication scenario, CA ARCserve D2D performs full backup operations. The full backup operation creates large backups that consume more time and bandwidth to replicate.
- Do not schedule periodic full backups for replicated CA ARCserve D2D backups. Scheduled full backups consume more time and bandwidth to replicate.

Note: Similarly, to replicate CA ARCserve Central Host-Based VM Backup sessions, you define a backup policy. For more information, see the CA ARCserve Central Host-Based VM Backup User Guide.

Create File Server Replication Scenarios

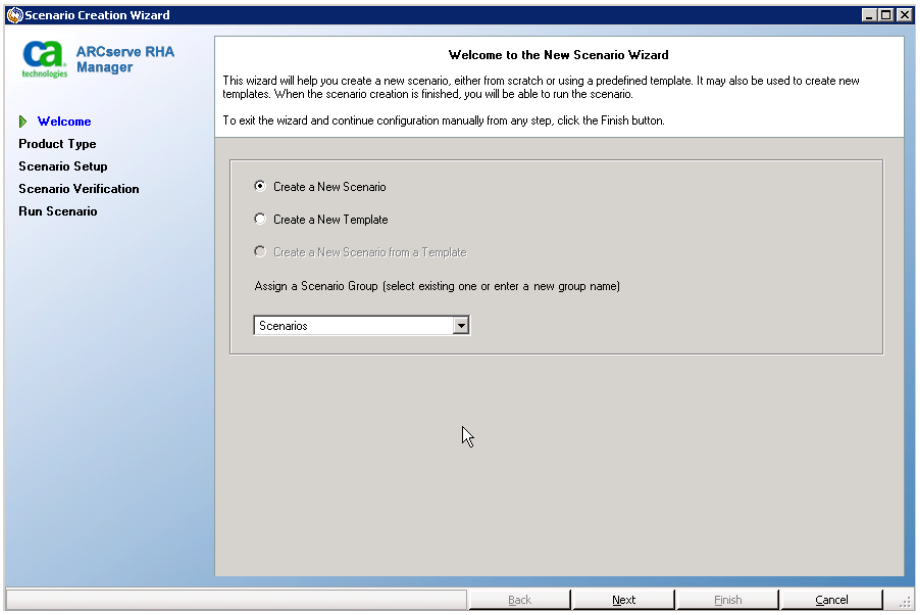
The following procedure demonstrates the creation of a File Server Replication scenario for a CA ARCserve D2D Backup.

Note: For information about how to configure scenarios to replicate CA ARCserve Central Host-Based VM Backup sessions, see the CA ARCserve Replication and High Availability Administration Guide.

Follow these steps:

1. From CA ARCserve Replication and High Availability, open the Manager, access the Scenario menu, and click New (or click the New on the Standard toolbar).

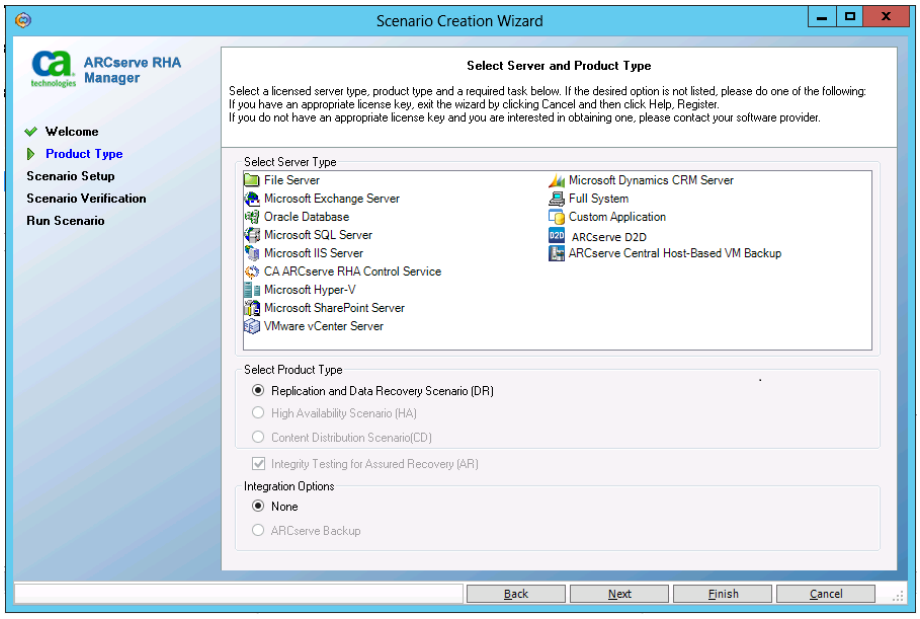
   The Welcome screen of the Scenario Creation Wizard is displayed.



   Note: To access other Manager features while you are creating a scenario, minimize the Scenario Creation Wizard. The Scenario Creation Wizard is bound to the Scenario View. If you switch views, the wizard is automatically minimized.

2. Select Create a New Scenario and Click Next.

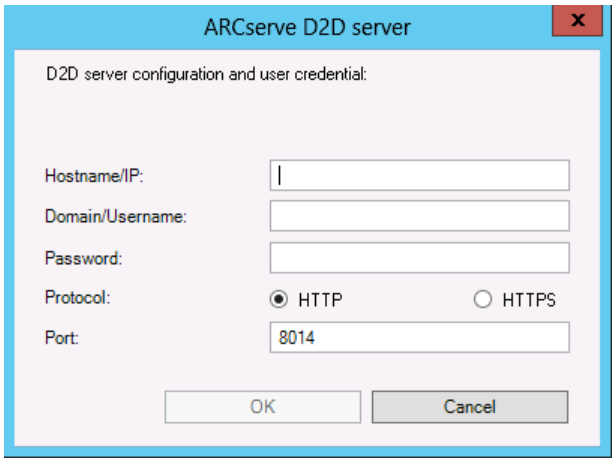
   The Select Server and Product Type screen opens.



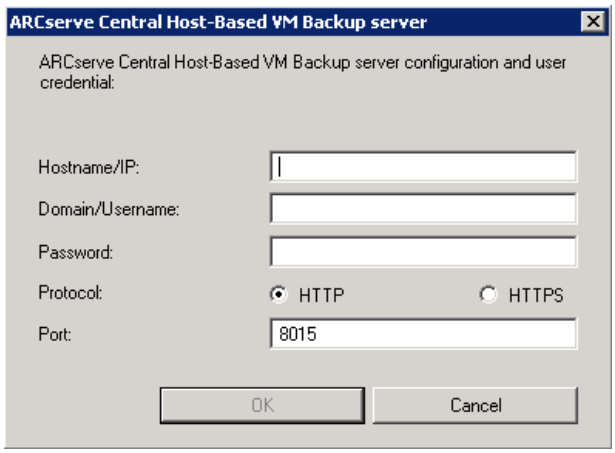
3. Select the required Server, Product Type, and Integration options. Then, from the Select Server Type list, click ARCserve D2D.

   Note: To replicate CA ARCserve Central Host-Based VM Backup sessions, click ARCserve Central Host-Based VM Backup.

   The ARCserve D2D Server dialog opens.



Note: When you click CA ARCserve Central Host-Based VM Backup, the ARCserve Central Host-Based Backup server credentials dialog opens, as illustrated by the following dialog.



4. Enter the CA ARCserve D2D configuration and user credentials. Click OK.

   When providing the CA ARCserve D2D server configuration details, if any of this information is not correct or does not match, you cannot continue with the scenario creation process and an error message displays.

   For example:

   - By default, CA ARCserve Replication and High Availability displays the protocol as http. If CA ARCserve D2D is installed with https protocol, then the web URL should be changed to:

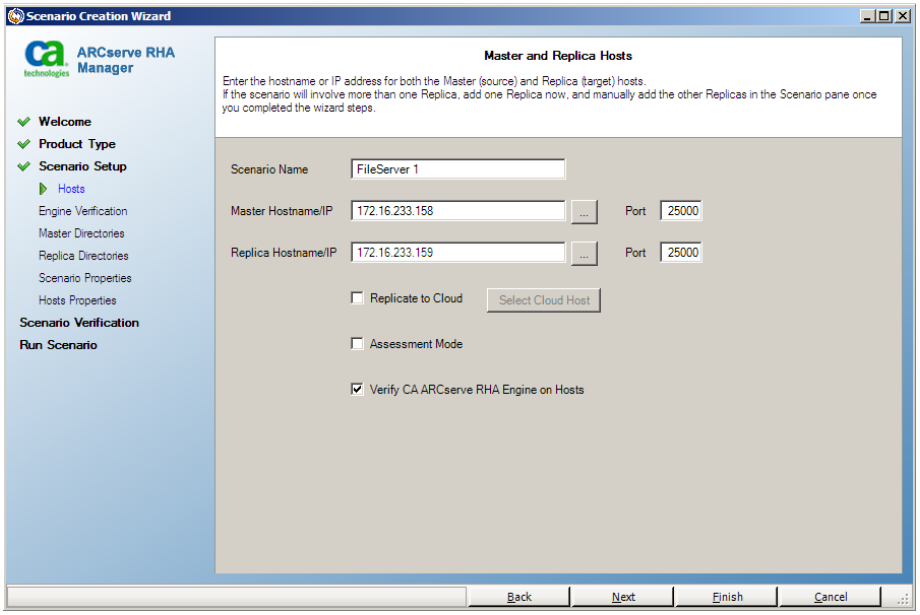
     `https://<<D2D server name>>:<<port number>>`

   - By default the port number is displayed as 8014. If you installed CA ARCserve D2D using a different port number, then the correct port number should be provided in the web URL.

   - Verify that you have configured the CA ARCserve D2D destination before creating the CA ARCserve Replication and High Availability replication scenario. This approach lets CA ARCserve Replication and High Availability detect the backup destination (automatically) and other related information, and then use this information to help create the scenario.

5. Click Next.

   The Master and Replica Hosts screen opens.



6. On this screen, specify the Master (source host to protect) and the Replica (target host that holds the replicated data), as follows:

   Note: For more information about these settings, see the CA ARCserve Replication and High Availability Administration Guide.

   a. In the Scenario Name field, accept the default name or enter a unique name.

   b. In the Master Hostname/IP field, the host name or IP address of the Master server is automatically populated.

   c. In the Replica Hostname/IP field, enter the host name or IP address of the Replica server.

      This server is the target server. Use the Browse button to find one. If you want to include more Replicas in your scenario, enter the details for the first or most upstream server here. When you have finished the Wizard to create the scenario, you can manually enter the other Replica servers.

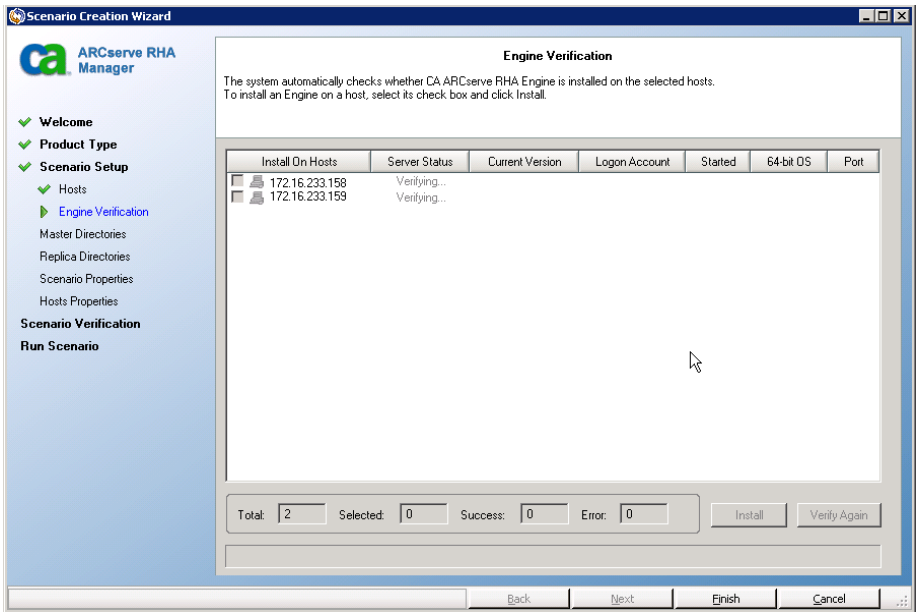
   d. In the Port fields, accept the default port number (25000) or enter new port numbers for the Master and Replica.

   e. (Optional) Enable Verify CA ARCserve Replication and High Availability Engine on Hosts to verify whether the Engines are installed and running on the specified Master and Replica hosts. If Engines are not installed on the hosts you specified, you can use this option to install the Engines on one or both hosts remotely.

f. Click Next.

If you enabled the Verify CA ARCserve Replication and High Availability Engine on Hosts option, the Hosts Verification screen opens. The software verifies the existence and connectivity of the Master and Replica hosts specified on the previous screen.

After the connections are verified, the software checks whether an Engine is installed on each host. If you log in to the Manager with different user credentials than remote hosts, the Server Status is reported as Not Connected. You are then prompted to enter User Credentials for each selected host. Verification repeats after you do so.



7. From the Hosts Verification screen, check whether an Engine is installed on the selected hosts using the Current Version column.

Complete on of the following steps:

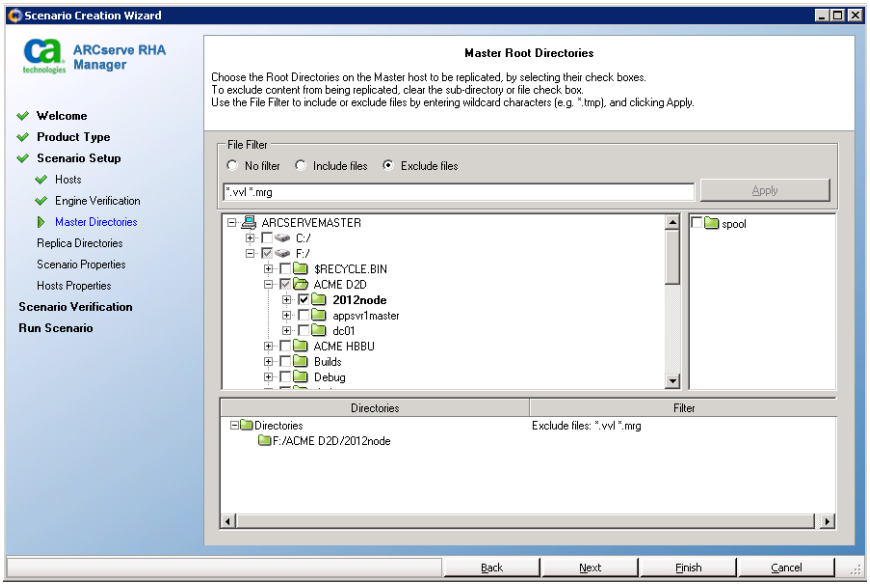
- If an Installed indication displays in the Server Status column in both rows, click Next to browse to the next page.
- If an Installed indication displays, but the version is different from the version of the Control Service you are using, install the current version.
- If a Not Installed indication is displayed, install the Engine. Click Install to install the Engine on the selected host. You can install the Engine on both hosts at the same time. Click each server and click Install.

  After you click Install, you are prompted to enter the CA ARCserve Replication and High Availability Engine service account credentials. For Replication scenarios, it is sufficient to be a Local Administrator (Local System).

  After the installation completes, the Engine version number is displayed in the Current Version column.

8. Click Next to open one of the following screens.

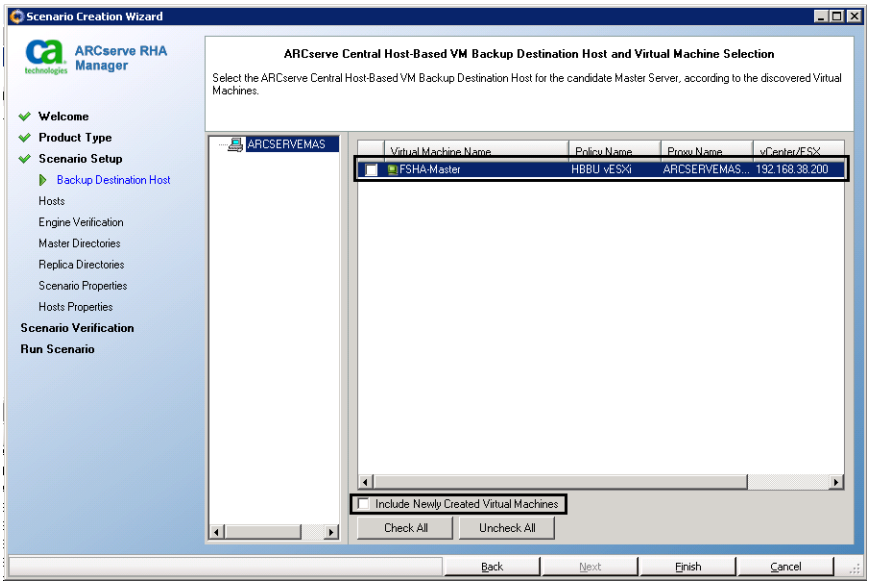
   - For CA ARCserve D2D scenarios, the Master Root Directories screen opens, as illustrated by the following screen:



   By default, this screen displays the directories and files in the CA ARCserve D2D backup folder on the Master server. This folder is the backup folder that is specified by CA ARCserve D2D. These directories and files contain the data to be replicated and protected.

   Note: Continue to the next step.

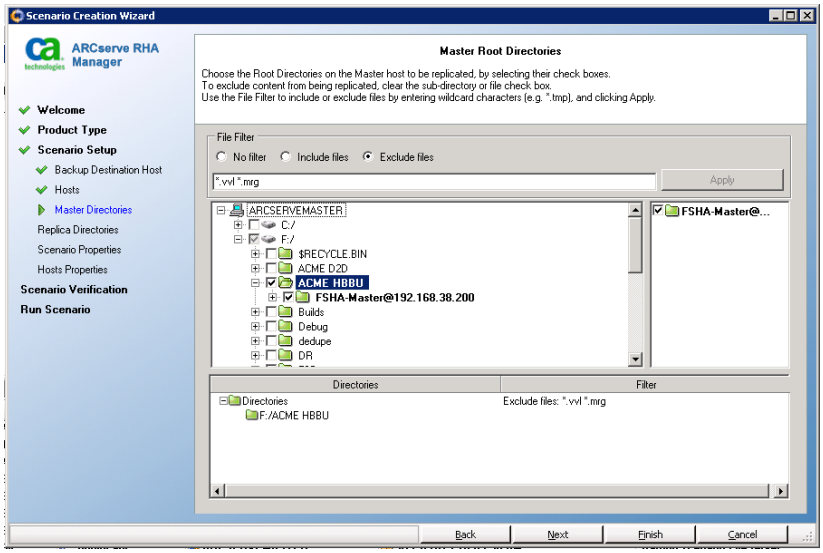
- For Host-Based VM Backup scenarios, the The ARCserve Central Host-Based VM Backup Destination Host and Virtual Machine Selection screen opens to list the systems that are protected by CA ARCserve Host-Based VM Backup



Click the check boxes next to the host names of the virtual machines that you want to protect (as illustrated by the previous screen), and then complete one of the following steps:

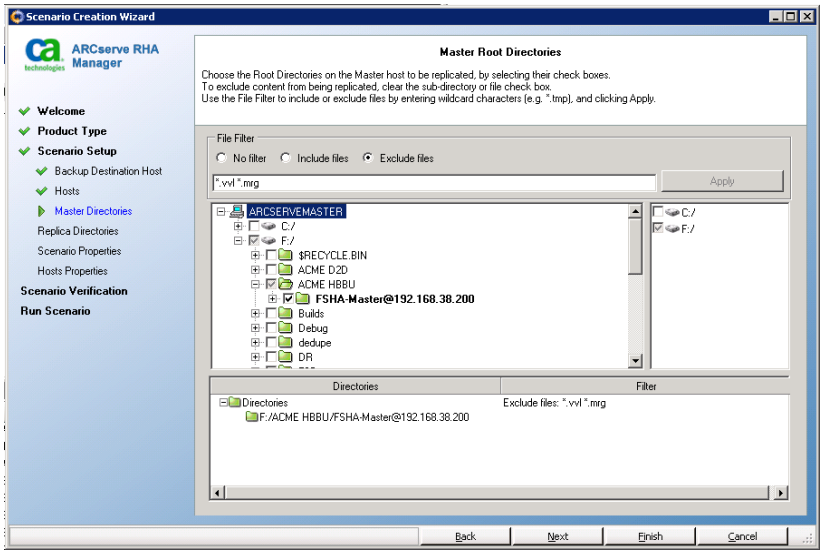
- To include all newly created virtual machines in the scenario, click the check box next to Include Newly Created Virtual Machines, and then click Next to open the Master Root Directories screen.

  Note: The Include Newly Created Virtual Machines option lets you include all virtual machines that are associated with the backup proxy system in all subsequent scenarios without having to stop, reconfigure, and restart the scenario.



- When you do not want to include all newly created virtual machines in the scenario, do not click the check box next to Include Newly Created Virtual Machines and then click Next to open the Master Root Directories screen.

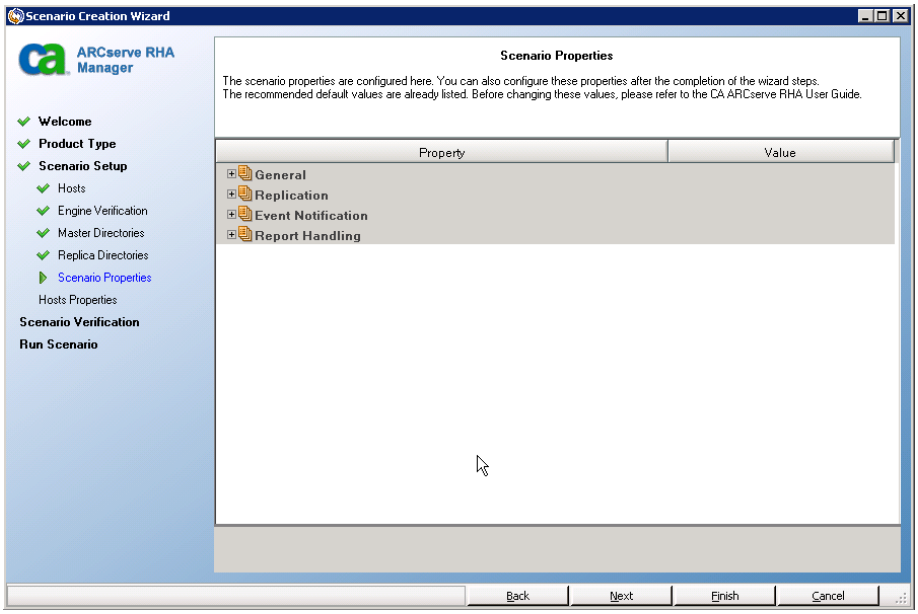
  Note: This approach does not let you include newly created virtual machines. When you add virtual machines using this approach, you stop the scenario, select the virtual machines, and then restart the scenario.



9. Click Next to open the Replica Root Directories screen opens. Accept the default or type a new directory name.

10. Click Next.

    The Scenario Properties screen opens.

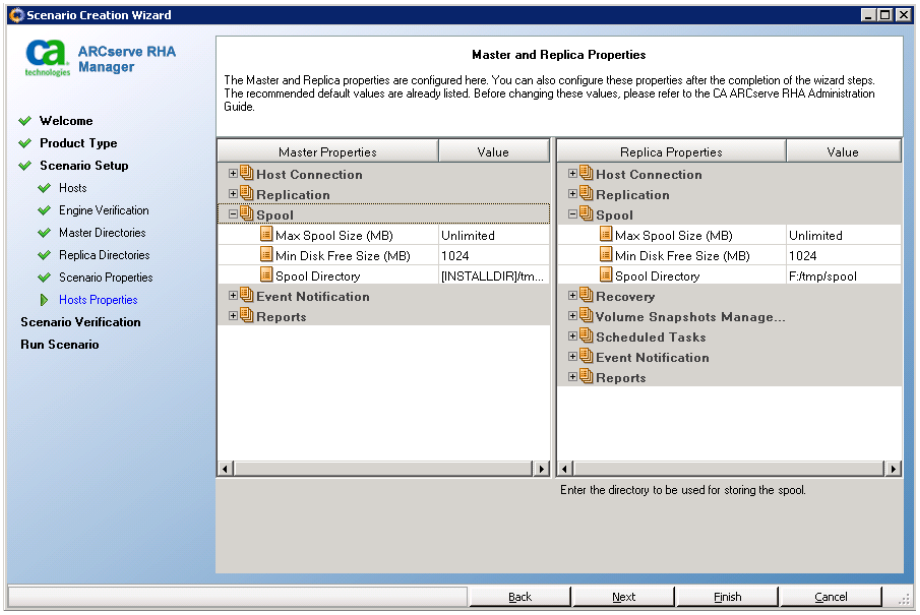


11. From the Scenario Properties screen, configure the properties that affect the entire scenario.

    For CA ARCserve D2D, accept all default values.

12. Click Next.

    The Master and Replica Properties screen opens.



13. From the Master and Replica Properties screen, configure the properties that are related to either the Master or Replica hosts.

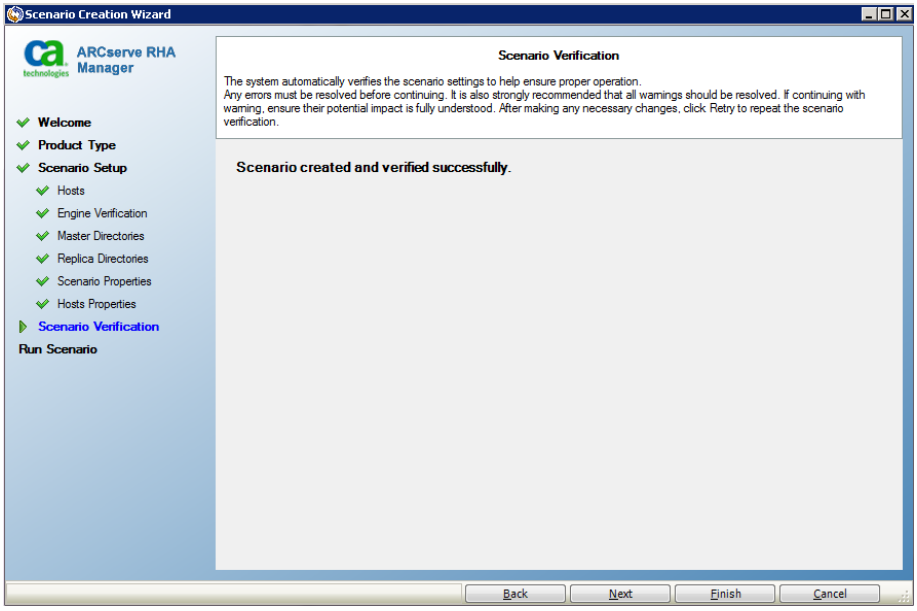
    For CA ARCserve D2D, accept all default values.

    Be aware of the following limitations:

    - Due to the manner in which CA ARCserve Replication and High Availability transfers CA ARCserve D2D replication data, verify that the overall capacity of the Spool Directories on the Master server and Replica server can contain the data for at least one full backup.
    - By default, the Spool Directories are configured to reside in the CA ARCserve D2D installation directory. The volume that contains the installation directory is typically the C:\ drive. To help ensure there is sufficient free disk space within the volume that contains the Spool Directory, specify an alternative volume to contain the Spool Directory (for example, F:\).

14. Click Next.

    The Scenario Verification screen opens.



15. The software validates the new scenario and verifies the parameters for a successful replication. After the verification completes, the screen opens, displaying any problems and warnings. The software lets you continue even if warnings are displayed. Resolve any warnings for a proper software operation.

    Click Next when all errors and warnings are resolved. The Scenario Run screen opens.

16. Running the scenario initiates the data synchronization process. Select Run Now to start synchronization immediately or Finish, which saves the scenario configuration and allows you to initiate synchronization later.

    Important! Do not initiate data synchronization if CA ARCserve D2D is currently performing a Verify Backup. When the synchronization process starts at this time, the operation can result in excessive data being sent to the Replica. To avoid this behavior, wait until the Verify Backup finishes before starting the data synchronization process.

    Note: Synchronization takes a while, depending upon your data size and network bandwidth.

    If you select Run Now, the software notifies you when synchronization completes. Now the real-time replication is operational and the replication scenario is active.

    A synchronization report is generated.

Restore a Recovery Point from a Replica

Each time CA ARCserve D2D performs a successful backup, a point-in-time snapshot image of your backup is also created. This collection of recovery points allows you to locate and specify exactly which backup image you want to restore.

Important! Do not attempt to restore a backup from a Replica during synchronization. When CA ARCserve Replication and High Availability initiates the synchronization process, the data on the Replica is not guaranteed to be in a consistent state. Therefore, any CA ARCserve D2D backup cannot be restored from the Replica until the synchronization has successfully completed.

Follow these steps:

1. From the CA ARCserve Replication and High Availability Manager, select the Replica you want to suspend, then click the Suspend button (or select the Suspend Replication option from the Tools menu).

   A confirmation message appears, informing you that any change of the Replica root directories content during suspension requires manual resynchronization.

   When you suspend replication on the Replica, changes continue to be recorded for the suspended Replica, but are not actually transferred until replication is resumed.

   Important! Do not suspend replication during synchronization.

2. Click Yes to suspend the replication.

   After the Replica is suspended, a red icon appears next to the Replica on the Scenario pane.

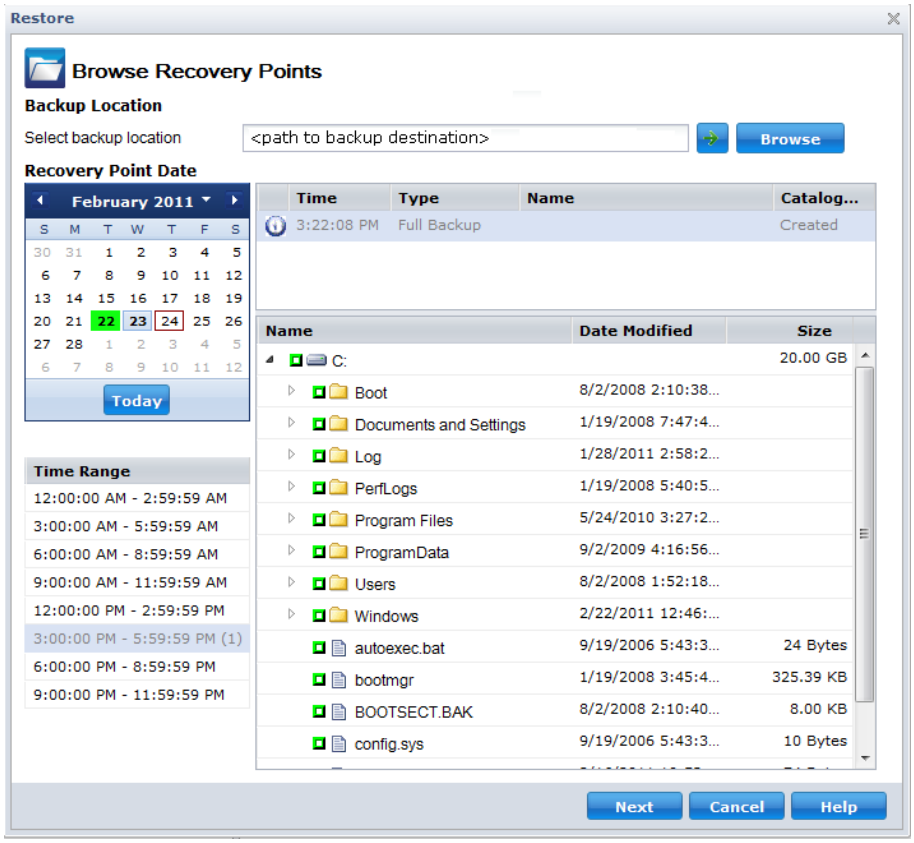
3. From the CA ARCserve D2D home page, select Restore.

   The restore methods selection dialog opens.

   Note: Steps 3 - 13 of this procedure details the Restore from a Recovery Point option of CA ARCserve D2D. However, a backup image can be restored from a Replica using any of the other available CA ARCserve D2D restore options, while observing the same replication considerations.

4. Click the Browse Recovery Points option.

   The Browse Recovery Points dialog opens.



5. Specify the backup source. You can either specify a location or browse to the location where your backup images are stored. If necessary, enter the User name and Password credentials to gain access to that location. You can click green arrow validate icon to verify proper access to the source location.

   The calendar view highlights (in green) all dates during the displayed time period that contain recovery points for that backup source.

6. Specify the information to restore.

   a. Select the calendar date for the backup image you want to restore.

      The corresponding recovery points for that date are displayed, with the time of the backup, the type of backup that was performed, and the name of the backup.

   b. Select a recovery point that you want to restore.

      The corresponding backup content (including any applications) for that recovery point is displayed.

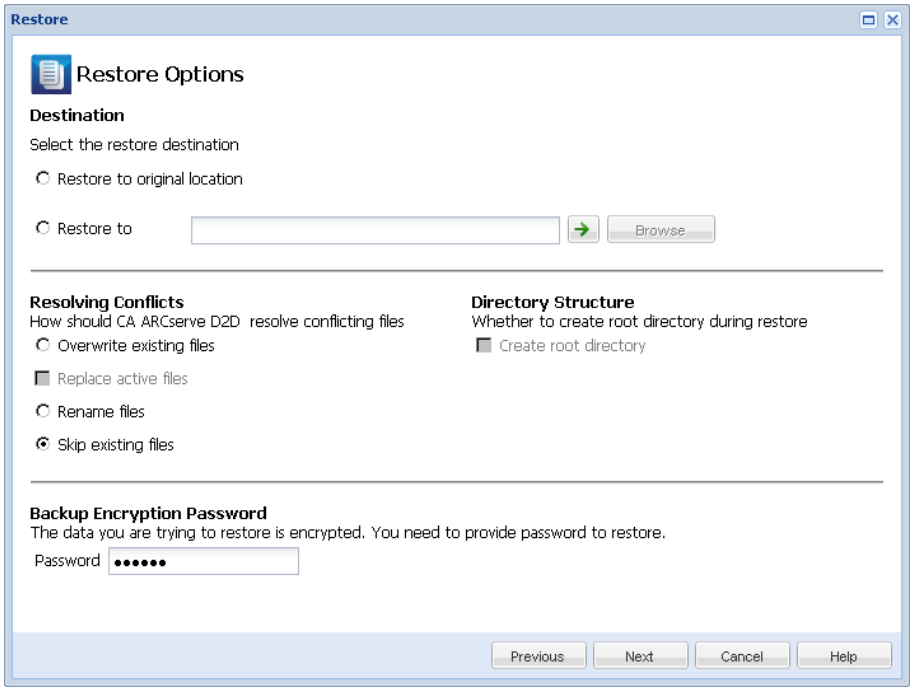
      Note: A clock icon with a lock symbol indicates the recovery point contains encrypted information and may require a password for restore.

   c. Select the content to be restored.

      - For a volume-level restore, you can specify to restore the entire volume or selected files/folders within the volume.
      - For an application-level restore, you can specify to restore the entire application or selected components, databases, instances, and so on, within the application.

7. When the backup information to be restored is specified, click Next.

   The Restore Options dialog is displayed.



8. Select the destination for the restore.

   The available options are to restore to the original location of the backup or restore to a different location.

   Restore to Original Location

   Restores to the original location from where the backup image was captured.

   Restore to:

   You can either specify a location or browse to the location where your backup images will be restored. You can click the green arrow icon button to verify the connection to the specified location.

   If necessary, you may need to enter the User Name and Password credentials to gain access to that location.

9. Select what CA ARCserve D2D will do to resolve any conflicts that are encountered during the restore process.

   The available options are to whether or not to overwrite the existing files and whether or not to replace any active files.

   Overwrite existing files

   Overwrites (replaces) any existing files that are located at the restore destination. All objects are restored from the backup files regardless of their current presence on your machine.

   Replace active files

   Replaces any active files upon reboot. If during the restore attempt CA ARCserve D2D discovers that the existing file is currently in use or being accessed, it will not immediately replace that file, but instead to avoid any problems will delay the replacement of the active files until the next time the machine is rebooted. (The restore occurs immediately, but the replacement of any active files is done during the next reboot).

   Note: If this option is not selected any active file is skipped from the restore.

   Rename files

   Creates a new file if the file name already exists. Selecting this option copies the source file to the destination with the same filename but a different extension. Data is then restored to the new file.

   Skip existing files

   Skips over and not overwrite (replace) any existing files that are located at the restore destination. Only objects that are not currently existing on your machine are restored from the backup files.

   By default, this option is selected.

10. Select what CA ARCserve D2D will or will not do with the directory structure during the restore process.

    Create root directory

    If selected, specifies that if a root directory structure exists in the captured backup image, CA ARCserve D2D recreates that same root directory structure on the restore destination path.

    When the Create Root Directory option is not selected (unchecked), the file/folder to be restored is restored directly to the destination folder.

    For example, if during the backup you captured the files "C:\Folder1\SubFolder2\A.txt" and "C:\Folder1\SubFolder2\B.txt" and during the restore you specified to the restore destination as "D:\Restore".

    - If you select to restore the "A.txt" and "B.txt" files individually, the destination for the restored files will be "D:\Restore\A.txt" and "D:\Restore\B.txt" (the root directory above the specified file level will not be recreated).
    - If you select to restore from the "SubFolder2" level, the destination for the restored files will be "D:\Restore\SubFolder2\A.txt" and "D:\Restore\SubFolder2\B.txt" (the root directory above the specified folder level will not be recreated).

    When the Create Root Directory option is selected (checked), the entire root directory path for the files/folders (including the volume name) is recreated to the destination folder. If the files/folders to be restored are from the same volume name, then the destination root directory path does not include that volume name. However, if the files/folders to be restored are from different volume names, then the destination root directory path does include the volume name.

    For example, if during the backup you captured the files "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", and also E:\Folder3\SubFolder4\C.txt" and during the restore you specified to the restore destination as "D:\Restore."

    - If you select to restore just the "A.txt" file, the destination for the restored file will be "D:\Restore\ Folder1\SubFolder2\A.txt" (the entire root directory *without* the volume name will be recreated).
    - If you select to restore both the "A.txt" and "C.txt" files, the destination for the restored files will be "D:\Restore\C\Folder1\SubFolder2\A.txt" and "D:\Restore\E\Folder3\SubFolder4\C.txt" (the entire root directory *with* the volume name will be recreated)

11. If the recovery point data you are trying to restore is encrypted, you may need to provide the encryption password.

    A password is not required if you are attempting to restore to the same machine from where the encrypted backup was performed. However, if you are attempting to restore to a different machine, a password is required.

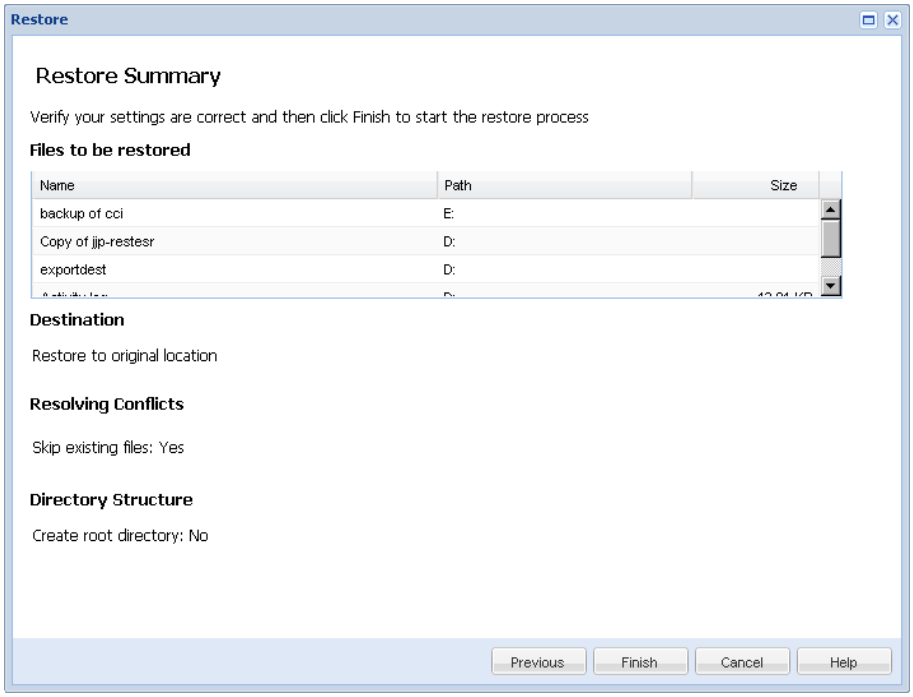
    Note: A clock icon with a lock symbol indicates the recovery point contains encrypted information and may require a password for restore.

    
    Non-encrypted recovery point (clock icon)

    
    Encrypted recovery point (clock icon with lock)

12. When the restore options are selected, click Next.

    The Restore Summary dialog is displayed.



13. Review the displayed information to verify that all the restore options and settings are correct.

    - If the summary information is not correct, click Previous and go back to the applicable dialog to change the incorrect setting.
    - If the summary information is correct, click Finish to launch the restore process.

14. When the restore is complete and you are ready to resume the replication, return to the CA ARCserve Replication and High Availability Manager and click the Resume Replication button (or select the Resume Replication option from the Tools menu).

    A confirmation message appears.

15. Click Yes to resume replication.

    After replication is resumed, the red icon disappears from the Replica on the Scenario pane.

    Any changes that occurred while in the suspended state and were accumulated are now transferred and applied to the Replica without the need to perform a full resynchronization of the data.