

Dell SRDF Adapter for VMware vCenter Site Recovery Manager 10.0.0 Release Notes

This document describes the new features, known issues, and limitations in the Dell SRDF Adapter for VMware vCenter Site Recovery Manager 10.0.0.

Current Release Version: 10.0.0

Release Type: Service (SR)

Topics:

- [Revision history](#)
- [Product description](#)
- [New features](#)
- [Support deprecation](#)
- [Resolved issues](#)
- [Known issues](#)
- [Limitations](#)
- [Environment and system requirements](#)
- [Installation and upgrade considerations](#)
- [Where to get help](#)

Revision history

Document revision history

Document Revision	Date	Description
001	July 2022	Initial release

Product description

Dell SRDF Adapter 10.0.0 is a Storage Replication Adapter (SRA) that extends the disaster restart management functionality of VMware vCenter Site Recovery Manager (SRM) to the Dell storage environment. It enables Site Recovery Manager to automate storage-based disaster restart operations on Dell arrays in an SRDF configuration.

New features

Dell SRDF Adapter 10.0.0 has the following new features:

- Support for 2K RDF Groups.

- Support for the mandatory creation of CG/DG for TestFailover operations.
- Support to perform TestFailover CleanUp for SnapVX without waiting for track definitions.

Support deprecation

The following lists the features that are deprecated in this release:

- Support for TimeFinder/VP Snap is deprecated.
- Support for TimeFinder/Mirror is deprecated.
- Support for TimeFinder/Snap is deprecated.
- Support for automated creation of CG/DG is deprecated in TestFailover.

This is the last release of Dell SRDF Adapter that supports VMware SRM Windows.

Resolved issues

This release of Dell SRDF Adapter resolves the issue that prohibited users from performing TestFailover CleanUp for SnapVX without waiting for track definitions.

Known issues

Table 1. Known issues in Dell SRDF Adapter 10.0.0

Functional Area	Description
TestFailoverForce	<ul style="list-style-type: none"> • SRA now ignores consistency disabled state when the Global option TestFailoverForce is enabled to support TestFailover workflow. SRA now uses a FORCE flag for SnapVX establish when the Global option TestFailoverForce is enabled to support TestFailover workflow. • Global option TestFailoverForce should be used with caution as usage might result in establishing the SnapVX session with a FORCE flag. Snapshots that are established with a FORCE flag cannot be guaranteed for data consistency and so should not be used for backups or for restoring production data.
TestFailover	<ul style="list-style-type: none"> • A TestFailover operation succeeds when SRDF consistency is disabled and the global option "TestFailoverForce" is set to Yes. • TestFailover fails for stretched devices when TestFailoverForce is enabled and SRDF pair state is not Activebias/ActiveActive. • TestFailover for stretched devices without snapshots is not supported. • TestFailover is not supported with SRDF/S configurations when the SRDF devices (part of the same recovery plan) belong to multiple SRDF groups and no composite group (CG) has been created. • TestFailover is not supported with the global option TestFailoverWithoutLocalSnapshots enabled when testing in a disconnected state. • When SRA uses TestFailoverWithoutLocalSnapshots to test a cascaded SRDF configuration (non-Star) to the Sync site, it does not suspend the hop2 link. This propagates all the changes that are made during the test of the sync devices to the third site removing any protection against failure. It is recommended not to use TestFailoverWithoutLocalSnapshots in this environment. • In Cascaded SRDF/Star environments that have been recovered to the Asynchronous target site, TestFailover, with or without TimeFinder ("without" means enabling the advanced setting TestFailoverWithoutLocalSnapshots) is not supported. Only full recovery back to the original workload site is supported with the SRDF Adapter.
SRDF/Metro	<ul style="list-style-type: none"> • TestFailover for stretched devices without snapshots is not supported. • SRDF/Metro 3-site cascaded setups are not supported in any configuration. Only SRDF/Metro 3-site concurrent setups are supported.

Table 1. Known issues in Dell SRDF Adapter 10.0.0 (continued)

Functional Area	Description
SRDF	<ul style="list-style-type: none"> Reprotect workflow is not supported for SRDF/Metro 3 site, Failover to Async configuration. Reprotect must be done manually which may include downtime. SRDF masking for R1 stretched devices is not supported. When disaster recovery is run with the protected site down, and the R1-R2 session is in a split state, the recovery returns with warnings. Attempt a second recovery after the protected site comes back up. If the R1-R2 session is still in a split state, SRDF write disables the R1 mirror before running the recovery for the second time. TestFailover and Recovery operations are not supported when a composite group contains SRDF devices from multiple storage systems. If SRDF consistency is enabled using SRDF group names at R11 and R21 in non-Star concurrent and cascaded configurations, SRA fails to perform reverse replication. In a 3-site concurrent Sync/Sync configuration, the SRDF pairs must be created in a specific order. The first SRDF pair that is created must always be the SRDF pair between the Site Recovery Manager protected site and the Site Recovery Manager recovery site. If not, SRA fails to discover the Sync/Sync concurrent configuration.
Reprotect	<ul style="list-style-type: none"> ReverseReplicationDuringRecovery is not supported for Star configurations. ReverseReplicationDuringRecovery is not supported for Disaster recovery scenarios. Ensure that this option is disabled before performing disaster recovery operations or it may result in undefined behavior. The SetReplicaTargetToReady option is not supported during the Reprotect operation in SRDF/Star configurations. During a reverse replication operation (reprotect) SRA continues despite failure to enable SRDF consistency after swapping the R1/R2 devices. If Star is not protected at the end of the Recovery operation and none of the sites are in disconnected state, manually protect or enable Star and then run Reprotect at the synchronous site. When disaster recovery is run with only compute resources down at the Site Recovery Manager protected site (that is, storage resources are not down), a Refresh operation must be performed from within the Site Recovery Manager Array Manager before performing a Reprotect operation.
SRDF/Star	<ul style="list-style-type: none"> In a disaster recovery operation, Site Recovery Manager may time out and the operation may fail when SRDF/Star configuration is in a halted state. The reason is the default timeout value is 300 s, which is too short for a disaster recovery operation when SRDF/Star configuration is in a halted state. Increase the parameter to at least 600 s in Site Recovery Manager. In an SRDF/Star with failover to the ASYNC target site environment, there are a few limitations to the Star operations. Once a Planned Migration or Disaster Recovery has run, the final state of Star is Unprotected. The first target site is Protected, and the second target site is Connected. If a Planned Migration or Disaster Recovery has to run again, it should be verified that the target sites are in the states that are previously mentioned. If the target sites are in a different state, you should manually get them to the required state outside of SRA.
GNS-enabled device groups	<ul style="list-style-type: none"> Goldcopy backup is not supported with devices that are contained in GNS-enabled device groups. <AutoTargetDevice> is not supported with devices that are contained in a GNS-enabled configuration.
Multi-extent datastore	Site Recovery Manager does not support the creation of protection group of a multi-extent datastore when the extents do not belong to a CG/DG.
TimeFinder/Clone	Devices that are used for testing a recovery plan using TimeFinder/Clone must be non-SRDF devices.

Limitations

Table 2. Limitations in Dell SRDF Adapter 10.0.0

Functional Area	Description
Support	<p>Dell SRDF Adapter 10.0.0 does not support:</p> <ul style="list-style-type: none">• The use of Non-Disruptive Data Migration (NDM) on any devices that are configured in SRM. Any NDM sessions must be completed and removed from one or more devices before reconfiguring SRM for the new array. At that point, device discovery can be completed successfully.• The SRA does not support targetless snapshots with the GoldCopy option.• SRDF/Metro DR• HYPERMAX OS version lower than 5977.1125. As a result, all features associated with HYPERMAX OS lower than this version are not supported by Dell EMC SRDF Adapter 10.0.0.• Database files and auto provisioning backup files that were originally written by Solutions Enabler versions older than 9.0.0 are not supported.• Clients that are running Solutions Enabler 10.0.0 that attempt to connect to a Solutions Enabler server with versions older than 10.0.0 are rejected.• Servers running Solutions Enabler 10.0.0 reject connections from Solutions Enabler clients with versions newer than 10.0.0 or older than 9.0.0.• The SRA does not support failover in a partitioned state when Invalid tracks exist. A manual failover with the force flag is required prior to running failover in SRM.• SRDF SRA 10.0.0 cannot operate with versions lower than Solutions Enabler version 10.0.0.• The use of custom CA-signed certificates on the Dockers platform.
Solutions Enabler	<ul style="list-style-type: none">• The only arrays discovered by Solutions Enabler 10.0.0 are arrays running the minimum supported release of HYPERMAX OS 5977.1125 and higher. Arrays running an unsupported version of HYPERMAX OS cannot be found with the symcfg discover CLI.• If Solutions Enabler was upgraded from an older version and an SE database file contains arrays with unsupported versions of HYPERMAX OS, the older arrays are not removed from the database automatically. Information about these arrays is not updated as part of the DISCOVER or SYNC commands.
Non-Disruptive Data Migration	<p>SRA does not support the use of Non-Disruptive Data Migration (NDM) on any devices that are configured in SRM. Any NDM sessions must be completed and removed from one or more devices before reconfiguring SRM for the new array. At that point, device discovery can be completed successfully.</p>
Reprotect	<p>Reprotect fails when configuring Windows SRM 8.3 and above with SRDF/Metro devices, see the VMware SRM Release Notes for a workaround.</p>
SRDF/Metro	<p>In a three-site SRDF/Metro Concurrent configuration, when failover to SRDF/Metro after a reverse replication occurs, the protected R1 remains R1 and recovery R2 remains R2 as a result of the microcode behavior.</p>

Environment and system requirements

- The following requirements apply to VMAX 100K, VMAX 200K, VMAX 400K, VMAX 250F, VMAX 450F, VMAX 450FX, VMAX 850F, VMAX 850 FX, VMAX 950F, VMAX 950FX, PowerMax 2000, PowerMax 2500, PowerMax 8000, and PowerMax 8500 arrays:
- If the SYMAPI server is different from the server running VMware vCenter Site Recovery Manager, the SYMAPI server must be running Solutions Enabler 10.0.0 or higher.
 - The following operating environment requirements apply:
 - VMAX 100K, 200K, 400K, 250F, 450F, 450FX, 850F, 850 FX, 950F, and 950FX arrays must be running HYPERMAX OS 5977 or higher.
 - PowerMax 2000 and PowerMax 8000 arrays running PowerMaxOS 5978 or higher.
 - PowerMax 2500 and PowerMax 8500 array running PowerMaxOS 10 (6079).

VMware requirements

The table below lists the SRA 10.0 requirements.

Table 3. SRA 10.0.0 Compatibility and interoperability matrix

VMAX platform	VMAX Enginuity/ HYPERMAX operating system/PowerMaxOS (b)	Solutions Enabler (a)	VMware vCenter Site Recovery Manager (b) (c)
VMAX 100K, VMAX 200K, VMAX 400K	5977	10.0.0	8.3
VMAX 250F/FX, VMAX 450F/FX, VMAX 850F/FX, VMAX 950F/FX, PowerMax 2000, PowerMax 8000 PowerMax 2500 PowerMax 8500	5977 5978 10 (6079)		8.4 8.5

(a) SRA supports Solutions Enabler point releases beyond the initially supported release. For instance, if a patched version of 10.0.0 became available (10.0.x), it would be supported.

(b) For complete and detailed VMware supported platforms, see the VMware vCenter Site Recovery Manager Compatibility Matrix available on the VMware support website at: www.vmware.com/support/pubs/srm_pubs.html.

(c) SRA Supports VMware Site Recovery Manager Major Release and minor updates of beyond the initially supported major release. For example, if a updated version of 8.5 became available, it would be supported.

Installation and upgrade considerations

Installation on the Windows platform

This section explains how to install and configure the Dell SRDF Adapter.

The Dell SRDF Adapter software must be installed on both the protected and recovery servers.

Before you begin

Before you begin installing Dell SRDF Adapter, verify that the following prerequisites are met:

- The pair of PowerMax/VMAX arrays are running the appropriate version of PowerMaxOS/HYPERMAX OS, the VMware vCenter Site Recovery Manager servers are running the appropriate version of Solutions Enabler, and the SYMAPI servers (if any) are running the appropriate version of Solutions Enabler. For more information, see [Environment and system requirements](#).
- The PowerMax/VMAX arrays for each protected VMware vCenter data center are locally defined to one or more hosts, and that these hosts are configured with Solutions Enabler client/server.
- Consistency protection is enabled at the protection site. Do this by adding the SRDF devices to the device groups or composite groups. The corresponding remote devices must be added to a device group/composite group at the recovery site. Consistency groups are required even if there is only one device in the group.
- The SRDF/Star configuration is set up before installation.

Installing Dell SRDF Adapter

To install Dell SRDF Adapter:

1. Download the Dell SRDF Adapter zip file from the VMware website.
2. Unzip the file and run the .exe file.
3. In the **Welcome** dialog box, click **Next**.
4. In the **License Agreement** dialog box, click **I accept the terms in the license agreement** and then click **Next**.
5. In the **Ready to Install Program** dialog, click **Install**.
6. In the **Dell SRDF SRA Wizard Completed** dialog box, click **Finish**.

Upgrading Dell SRDF Adapter

Upgrading from SRA 5.6.x or higher

Before upgrading Dell SRDF Adapter to version 10.0.0, ensure that VMware vCenter Site Recovery Manager and vCenter have been upgraded to their respective versions. While installing Dell SRDF Adapter 10.0.0 select Upgrade and complete the installation.

Dell SRDF Adapter 10.0.0 provides the following options files:

- EmcSrdfSraGlobalOptions.xml
- EmcSrdfSraTestFailoverConfig.xml
- EmcSrdfSraRecoverySiteGoldcopyConfig.xml
- EmcSrdfSraProtectionSiteGoldcopyConfig.xml
- EMCSrdfSraDeviceMaskingControl.xml

If any of the options files for Dell SRDF Adapter 5.6.x were modified either manually, using Storage Viewer, or Virtual Storage Integrator repopulate these files after the upgrade. The old options file, renamed as `EmcSrdfSraGlobalOptions.xml_bak` is available for reference in the new SRA data directory under the common application data folder with the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common AppData
```

After installation and upgrade, rescan SRAs on both sites and ensure that the SRA status is OK.

Upgrading from SRA 5.5.x, or lower versions

SRA 10.0.0 does not support upgrade from SRA 5.5.x or lower versions. If the previous SRA kit is already installed on the server, the installer enables you to back up the configuration files if the previous SRA kit is already installed on the server.

When upgrading from a 32-bit SRA (version lower than SRA 5.6) kit to a SRA 10.0.0 kit, the installer displays the following Dell SRDF Adapter warning message:

```
32 bit SRA kit already installed on this host and SRA 10.0(64 bit) does
not support upgrade. So please follow below instructions.
- Click YES to take backup of all Config files.
- Click NO to abort installation without backup of all config files.
- After above steps click Cancel or Finish to Abort installation.
- Uninstall previously installed SRA from host and then install SRA 10.0
kit.
```

Uninstall the existing version of SRA, and then install SRA 10.0.0.

 **NOTE:** The config files backup is saved to `ProgramData\EMC\EmcSrdfSra\Config\`.

Registry key

After you have successfully installed the adapter, the installation program creates the **Dell SRDF Adapter** registration key under `HKEY_LOCAL_MACHINE\SOFTWARE\EMC`.

The following values are under the **Dell SRDF Adapter** key:

- **InstallPath**: Refers to the location of `command.pl`.
- **Version**: Contains the version of the adapter that verifies the integrity of your installation.

To verify the integrity of your Dell SRDF Adapter installation, use the **md5sums** checksum utility:

1. Download and install the **md5sum.exe**. Remember to set up the PATH environment variable to point to the location of the executable, which can be found under: `SRM_install_dir\storage\sra\EMC Symmetrix`
The default path for `SRM_install_dir` is `C:\Program Files\VMware\VMware vCenter Site Recovery Manager`.
2. Open the Windows command prompt and change the directory to the Dell SRDF Adapter installation directory. Its default location is: `SRM_install_dir\storage\sra\EMC Symmetrix`
3. Type the following command: `md5sum EmcSrdfSra.exe`
The checksum of the indicated file is displayed.
4. Verify the output against the output included in the `md5checksums.txt` file in the installation directory.

Configuring Dell SRDF Adapter

This section provides the procedures for configuring Dell SRDF Adapter to work with Site Recovery Manager.

Configuring a locally attached PowerMax array

When configuring a PowerMax array that is locally attached to the server running VMware vCenter Site Recovery Manager, specify Local in the SYMAPI Server field in the Array Manager configuration wizard of VMware Site Recovery Manager.

Configuring for SYMAPI client/server support

Dell SRDF Adapter requires the use of `SYMAPI Server [:Port]` format in the Array Manager configuration wizard, where `SYMAPI Server` can be either an IP address, or the name of the host machine where the SYMAPI server is running.

To configure the SYMAPI server on a non-default port, the port number is specified in the below format. If a port number is not specified, the adapter uses the default port number 2707.

For example:

`SERVER.lss.emc.com:2708` or `192.168.10.1:2708` (non-default port)

or

`SERVER.lss.emc.com` or `192.168.10.1` (default port)

To change the security level of the SYMAPI server connection, use the Solutions Enabler options file located in the `C:\Program Files\EMC\SYMAPI\Config` directory. This option must be set before starting the adapter.

Additional configuration guidelines

Consider the following when configuring devices used by Dell EMC SRDF Adapter:

- The R1 devices being protected must be defined as ReadWrite, and the corresponding R2 devices must be defined as WriteDisabled, not NotReady, unless using SRDF/Metro.
- Devices must be defined as dynamic SRDF capable.
- Larger environments may need the storage timeout increased.

Cascaded and concurrent configurations

Follow the guidelines in the table below for cascaded and concurrent configurations.

Table 4. Concurrent and cascaded configurations

Three-site (initial configuration)		Three-site (after reprotect)		
R11 -> R2 (1st mirror)	R11 -> R2 (2nd mirror)	R1 -> R21 (1st mirror)	R21 -> R2 (2nd mirror)	vCenter Site Recovery Manager Recovery Site
Synchronous	Asynchronous	Synchronous	Asynchronous	Synchronous
Synchronous	Asynchronous	Adaptive Copy - DISK	Asynchronous	Asynchronous
Synchronous	Adaptive Copy - DISK	Synchronous	Adaptive Copy - DISK	Synchronous
Synchronous	Synchronous	Synchronous	Adaptive Copy - DISK	Synchronous
Asynchronous	Asynchronous	Asynchronous	Adaptive Copy - DISK	Asynchronous
Asynchronous	Adaptive Copy - DISK	Asynchronous	Adaptive Copy - DISK	Asynchronous
Active	Asynchronous	N/A	N/A	N/A
R1 -> R21 (1st mirror)	R21 -> R2 (2nd mirror)	R11 -> R2 (1st mirror)	R11 -> R2 (2nd mirror)	vCenter Site Recovery Manager Recovery Site
Synchronous	Asynchronous	Synchronous	Asynchronous	Synchronous
Synchronous	Adaptive Copy - DISK	Synchronous	Adaptive Copy - DISK	Synchronous
Asynchronous	Adaptive Copy - DISK	Asynchronous	Adaptive Copy - DISK	Asynchronous
R1 -> R21(1st mirror)	R21 -> R2 (2nd mirror)	R1 -> R21 (1st mirror)	R21 -> R2 (2nd mirror)	vCenter Site Recovery Manager Recovery Site
Synchronous	Asynchronous	N/A	N/A	Asynchronous (In this scenario, Reprotect is not supported. The user is required to manually fail back to the original site.)

Configuring SRDF/Star

SRDF/Star is a data-protection and failure-recovery solution that covers three geographically dispersed data centers in a triangular topology.

Consider the following when configuring SRDF/Star:

- Reconfiguration of the SRDF/Star topology from Concurrent to Cascaded, and from Cascaded to Concurrent, is not a supported workflow. If reconfiguration is needed, it has to be done outside SRA.
- The SRDF/Star commands in SRA might take multiple hours. It depends on the amount of replication data.
- SRA supports the following valid SRDF/Star states for device discovery:

Table 5. Valid SRDF/Star states for device discovery

SRDF/Star state	Sync target site state	Async target site state
Protected	Protected	Protected
Tripped	PathFailed	PathFailed
Tripped	PathFailed	Protected
Tripped	Protected	PathFailed

Table 5. Valid SRDF/Star states for device discovery (continued)

SRDF/Star state	Sync target site state	Async target site state
Unprotected	Disconnected	Protected
Unprotected	Connected	Protected
Unprotected	Protected	Protected
Unprotected	Halted	Halted
Unprotected	Isolated	Protected
Unprotected	Protected	Isolated
Unprotected	Isolated	Disconnected

- SRA supports the following SRDF/Star states for vCenter Site Recovery Manager operations, such as Recovery and Test Recovery:

Table 6. Valid SRDF/Star states for recovery and test recovery operations for sync target site

SRDF/Star state	Sync target site state	Async target site state
Protected	Protected	Protected
Tripped	PathFailed	PathFailed
Tripped	PathFailed	Protected
Tripped	Protected	PathFailed

- Only if site A is down, or partitioned from site B, can the mode of operation change from Cascaded Star to Concurrent Star. To return the configuration to its original Cascaded Star mode, a reconfiguration, outside of SRA, is required.

Table 7. Valid SRDF/Star states for recovery and test recovery operations for async target site

SRDF/Star State	1st Target site state	2nd Target site state
Protected	Protected	Protected
Tripped	PathFailed	PathFailed
Tripped	PathFailed	Protected
Tripped	Protected	PathFailed
Unprotected	Protected	Connected

- Only if Site B is down, can the mode of operation change from Cascaded Star to Concurrent Star. To return the configuration to its original Cascaded Star mode, a reconfiguration, outside of SRA, is required.

Uninstalling Dell SRDF Adapter

To uninstall Dell SRDF Adapter:

1. From the Windows **Start** menu, select **Settings > Control Panel > Add/Remove Programs**.
2. In the **Add/Remove Programs** dialog box, select **Dell SRDF Adapter**, and click **Remove**.

Software media, organization, and files

The Dell SRDF Adapter version 10.0.0 software and these release notes can be downloaded from the VMware website: <https://my.vmware.com/web/vmware/downloads>

The Dell SRDF Adapter is distributed as a zip file, which contains two files: These release notes and the software installer.

Installation on the Dockers platform

This section explains how to install and configure the Dell SRDF Adapter with the VMware SRM Appliance (SRM VA). The Dell SRDF Adapter software must be installed on both the protected and recovery servers.

Before you begin

Before you begin installing Dell SRDF Adapter, verify that the following prerequisites are met:

- Complete deployment of the VMware SRM VA.
- SRA Dockers only supports the Client and Server model, therefore configure SYMAPI servers for both Protected and Recovery site.

Installing Dell SRDF Adapter on the Dockers platform

To install Dell SRDF Adapter on the Dockers platform:

1. Download the Dell SRDF Adapter Dockers .zip file from the VMware website.
2. Unzip the file. The files `EMCSRDFSRADockers_X.X.X.X.tar` and `enableAutoSSLCertGen.sh` appear.
3. Login to the VMware SRM appliance management: `https://FQDN>:5480/configure`.
4. Select **Storage Replication Adapters>New Adapter** and upload the `EMCSRDFSRADockers_X.X.X.X.tar` file.
5. SRM automatically installs and starts the docker image.
6. Copy the `enableAutoSSLCertGen.sh` file to the `/home/admin` directory on the SRM host.
7. SSH to the SRM host using admin credentials.
8. Change to root user, su to root or use sudo, and run the `enableAutoSSLCertGen.sh` script as root user.
 - a. Usage: `./enableAutoSSLCertGen.sh <REPOSITORY>:<TAG>`
 - b. Example: `./enableAutoSSLCertGen.sh sradocker:10.0.0.0`
9. If needed, provide vCenter authorization details and input all required details.
10. **Rescan Adapter** through SRM GUI.

NOTE:

- Allowed values for "Do you wish to provide vCenter authorization details? (y/n)" during the script performance are [Y/y/YES/yes/Yes]. Any other input is considered as 'No'.
- Running `enableAutoSSLCertGen.sh` script, the hostname file and vCenter authorization details is persisted across SRM host reboot or container reload.
- SRM hostname modified - this requires a script re-run, followed by reload container.
- vCenter authorization details modified/incorrect - this requires a script re-run. This overwrites previous credentials.
- The authorization details provided through the script work with the **FilterNonVMwareDevices** flag enabled in the SRA Global Options file. To opt out from the filtering of devices, disable the **FilterNonVMwareDevices** flag.

Configuring Dell SRDF Adapter

This section provides the procedures for configuring Dell SRDF Adapter to work with SRM VA.

Configuring for SYMAPI client/server support

Dell SRDF Adapter requires the use of `SYMAPI Server [:Port]` format in the Array Manager configuration wizard, where `SYMAPI Server` can be either an IP address, or the name of the host machine where the SYMAPI server is running.

To configure the SYMAPI server on a non-default port, the port number is specified in the below format. If a port number is not specified, the adapter uses the default port number 2707.

For example:

`SERVER.lss.emc.com:2709` or `192.168.10.1:2709` (non-default port)

Or

SERVER.lss.emc.com or 192.168.10.1 (default port)

NOTE: You are required to configure the default SYMAPI server details to run SYMCLI commands in the SRM container.

The file is available at `sradocker_latest\symapi\config` after selecting **Menu (three dots) > Download Configuration Archive**.

If accessing the Docker container directly to run Solutions Enabler commands, it is necessary to modify the `netcnfg` file with the SYMAPI server details.

Change the security level of the SYMAPI server connection as follows:

Updating SYMAPI files and SRA options files

Download the configuration files:

1. Log in to the **VMware SRM Appliance Management Interface**.
2. Go to **Storage Replication Adapters > Dell EMC SRDF Adapter**.
3. Select **Menu (three dots) > Download Configuration Archive**.
4. The downloaded file has the filename format `<buildname>_<buildTAG>.tar.gz`.
5. Extract the file and verify the `sra-configuration-version.txt` exists.

Modify the configuration files:

1. Download the configuration archive.
2. Copy the file ('.tar.gz' file) to a UNIX machine using an FTP tool.
3. Run Gunzip on the file to extract the .tar output.
4. Untar the file, `tar -xvf <target file>`, ensure that the current directory does not have any previous configuration files.
5. Edit the file as necessary.
6. Tar and Gunzip all the files at once by specifying the filename with '.tar.gz' extension. `tar czvf final_file.tar.gz *.xml symapi sra-configuration.txt`.

NOTE: Tar and Gunzip must be done as a single command. Refrain from adding or moving the files to any directory.

7. Copy the file back to windows machine using FTP.

Upload the configuration files:

1. Go to the SRM App User Interface.
2. Log in to the **VMware SRM Appliance Management Interface**.
3. Go to **Storage Replication Adapters > Dell SRDF Adapter**.
4. Select **Menu (three dots) > Upload Configuration Archive**.

If SYMAPI config files are modified, it is necessary to perform a Storage Replication Adapters **Reload** using the SRM Appliance Management followed by a **Rescan Adapter/Discover Devices** using the SRM User Interface .

NOTE:

- Do not modify any SRA or Solutions Enabler configuration files from inside the container. Any configuration changes must be made using the Appliance Management Interface to ensure the changes persist.
- It is necessary to run a reload operation on the Appliance Management after a SYMAPI config change. These details persist on host reboot.
- Do not modify the files on a Windows box as unsupported formatting is included and the configuration files can fail to load properly.

Downloading SRA logs from the GUI

SRA logs and the SRM Support bundle are downloaded by using the SRM DR link or the SRM Appliance Management.

- Connect to SRM DR:
 1. Select **Summary > Site Recovery Manager**.
 2. Expand the name that is listed and select **server-name and dropdown ACTIONS**.
 3. Select Export logs.
- Connect to SRM Appliance Management, select **Summary > Download Support Bundle**.

Upgrading Dell SRDF Adapter in VMware SRM VA

Upgrading to Dell SRDF Adapter 10.0.0 from the previous version installed, provides the following below steps:

1. **Upload** the new SRA 10.0.0 image through Appliance Management.
2. Perform **Copy Configuration** in Appliance Management from old SRA x.x.x.x to new SRA 10.0.0 (to persist the customized configuration).
3. Perform **Reset Configuration** followed by **Delete** in Appliance Management for old SRA x.x.x.x.
4. Run the **enableAutoSSLCertGen.sh** script as per installation procedure.
5. **Rescan Adapter** through SRM GUI.

Uninstalling Dell SRDF Adapter in VMware SRM VA

This section explains how to uninstall the Dell SRDF Adapter in VMware SRM VA. Before proceeding take a backup of necessary SRA options files.

1. Log in to the **VMware SRM Appliance Management Interface**.
2. Go to **Storage Replication Adapters > Dell SRDF Adapter**.
3. Select **Menu (three dots) > Reset configuration > Reset**.
4. Select **Menu (three dots) > Delete**.
A window appears, select both check boxes and click **Delete**.

NOTE:

- The **Reset Configuration** option on the Appliance Management Interface deletes all the mounts and volumes that are associated with the image, deleting all the persisted data and the running containers. Configuration data can be downloaded from the Appliance before a reset is initiated.
- A **Reset Configuration** should be initiated before deleting an image.
- A **Delete** operation on the Appliance Management Interface without a prior **Reset Configuration** deletes the image and its containers without deleting the volumes that are associated with the image causing ineffective space utilization.

Where to get help

The Dell Technologies Support site (<https://www.dell.com/support>) contains important information about products and services including drivers, installation packages, product documentation, knowledge base articles, and advisories.

A valid support contract and account might be required to access all the available information about a specific Dell Technologies product or service.

Technical notes

This section provides technical information on the SRDF Adapter.

Setting log levels

To set the log levels for SRDF Adapter in the VMware vCenter Site Recovery Manager environment, the following XML tags should be added to the `vmware-dr.xml`:

```
<level id="Storage">
<logName>Storage</logName>
<logLevel>verbose</logLevel>
</level>
<level id="SraCommand">
<logName>SraCommand</logName>
```

```
<logLevel>verbose</logLevel>
</level>
```

Restart the Site Recovery Manager service for these settings to take effect.

SYMAPI debug log

In Solutions Enabler, the variable `permit_symapi_debug` is available for getting the SYMAPI logs.

- To collect the SYMAPI debug logs from client, set the variable `permit_symapi_debug` to `CLIENT` at the SYMAPI server.
- To collect the SYMAPI debug logs from Server, set the variable `permit_symapi_debug` to `SERVER` at the SYMAPI server (default value).

The debug logs are generated in the following folder: `SYMAPI\logs\debug`. SRA tries to create the SYMAPI debug log at the SYMAPI server being used. If you want to collect the SYMAPI debug logs with Solutions Enabler, first set the variable `permit_symapi_debug` to `CLIENT` at the SYMAPI server. For more information, see the *Solutions Enabler Command Reference Guide*.

EmcSrdfSra command

This section presents the syntactical form with argument and option descriptions for the `EmcSrdfSra` command.

Syntax

```
EmcSrdfSra [-env | -version]
```

Description

This command provides the application interface to SRDF Adapter. Its compound actions perform the necessary commands, in the proper order, enabling Site Recovery Manager to manage the recovery environment for PowerMax arrays. Site Recovery Manager normally invokes this command.

Arguments

STDIN

Site Recovery Manager uses the normal command options passing method scheme.

Options

`-env`

Displays the option settings from the options files. If the options are not specified in the options files, the adapter displays the default options.

`-version`

Returns the installed `EmcSrdfSra` version.

Options files

SRDF Adapter provides the following options files under the folder `ProgramData\EMC\EmcSrdfSra\Config`:

- `EmcSrdfSraGlobalOptions.xml`
- `EmcSrdfSraTestFailoverConfig.xml`
- `EmcSrdfSraProtectionSiteGoldCopyConfig.xml`
- `EmcSrdfSraRecoverySiteGoldCopyConfig.xml`
- `EmcSrdfSraDeviceMaskingControl.xml`

The options files are XML based. The options can be set to control some of the adapter features. A Document Type Definition (DTD) is a set of instructions that states which tags are usable and which actions or reactions are created.

The following DTDs provide the definitions of all options files.

EmcSrdfSraGlobalOptions.xml

EmcSrdfSraGlobalOptions.xml comes pre-filled with default values. In most cases, these values do not need to be changed. However, if you need to change any of the default values, Dell recommends that you understand the consequence of those changes before proceeding.

The following DTD describes EmcSrdfSraGlobalOptions.xml:

```
<!ELEMENT EmcSrdfSraGlobalOptions (Version?, SymapiDebug,
TestFailoverForce, TestFailoverWithoutLocalSnapshots, TerminateCopySessions,
FailoverIfGoldCopyFails, IgnoreActivatedSnapshots, FilterNonVmwareDevices,
CheckForVirtualDisks, FailoverToAsyncSite, SetReplicaTargetToReady,
TestReplicaMaskingControl, RdfDeviceMaskingControl, ReverseReplicationDuringRecovery)>
<!ELEMENT Version (#PCDATA)>
<!ELEMENT SymapiDebug (#PCDATA)>
<!ELEMENT TestFailoverForce (#PCDATA)>
<!ELEMENT TestFailoverWithoutLocalSnapshots (#PCDATA)>
<!ELEMENT TerminateCopySessions (#PCDATA)>
<!ELEMENT FailoverIfGoldCopyFails (#PCDATA)>
<!ELEMENT IgnoreActivatedSnapshots (#PCDATA)>
<!ELEMENT FilterNonVmwareDevices (#PCDATA)>
<!ELEMENT CheckForVirtualDisks (#PCDATA)>
<!ELEMENT SetReplicaTargetToReady (#PCDATA)>
<!ELEMENT TestReplicaMaskingControl (#PCDATA)>
<!ELEMENT RdfDeviceMaskingControl (#PCDATA)>
<!ELEMENT ReverseReplicationDuringRecovery (#PCDATA)>
<!ELEMENT FailoverToAsyncSite (#PCDATA)>
<!ELEMENT IgnoreDisconnectedStar (#PCDATA)>
<!ELEMENT AutoTargetDevice (#PCDATA)>
<!ELEMENT AutoTargetDeviceReuse (#PCDATA)>
<!ELEMENT AutoTargetDeviceFreeTracks (#PCDATA)>
<!ELEMENT ViClientIgnoreSecurityException (#PCDATA)>
```

The following is an example of EmcSrdfSraGlobalOptions.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<EmcSrdfSraGlobalOptions>
  <Version>9.2</Version>
  <SymapiDebug>0</SymapiDebug>
  <TestFailoverForce>No</TestFailoverForce>
  <TerminateCopySessions>No</TerminateCopySessions>
  <TestFailoverWithoutLocalSnapshots>No</TestFailoverWithoutLocalSnapshots>
  <FailoverIfGoldCopyFails>Yes</FailoverIfGoldCopyFails>
  <IgnoreActivatedSnapshots>No</IgnoreActivatedSnapshots>
  <FilterNonVmwareDevices>Yes</FilterNonVmwareDevices>
  <CheckForVirtualDisks>No</CheckForVirtualDisks>
  <FailoverToAsyncSite>No</FailoverToAsyncSite>
  <SetReplicaTargetToReady>No</SetReplicaTargetToReady>
  <TestReplicaMaskingControl>No</TestReplicaMaskingControl>
  <RdfDeviceMaskingControl>No</RdfDeviceMaskingControl>
  <ReverseReplicationDuringRecovery>No</ReverseReplicationDuringRecovery>
  <IgnoreDisconnectedStar>No</IgnoreDisconnectedStar>
  <AutoTargetDevice>No</AutoTargetDevice>
  <AutoTargetDeviceReuse>Yes</AutoTargetDeviceReuse>
  <AutoTargetDeviceFreeTracks>No</AutoTargetDeviceFreeTracks>
  <ViClientIgnoreSecurityException>Yes</ViClientIgnoreSecurityException>
</EmcSrdfSraGlobalOptions>
```

The following section describes the options in EmcSrdfSraGlobalOptions.xml.

SymapiDebug

Specifies whether SYMAPI debug logging is enabled. This option can be set either to 1 or 0. When set to 1, SYMAPI debug logging is enabled. By default this option is disabled. The name of the SYMAPI debug logfile is SYMAPI_debug_<YYYYMMDD>.log.

For example:

```
<SymapiDebug>1</SymapiDebug>
```

TestFailoverForce

Forces the test failover operation to proceed regardless of the state of the SRDF link (the only exception is Transmit Idle). The possible values for this option are YES and NO. By default, the value is set to NO.

For example:

```
<TestFailoverForce>NO</TestFailoverForce>
```

TestFailoverWithoutLocalSnapshots

Performs a test failover operation directly using R2 devices without a need to use local TimeFinder replica devices. In case of SRDF/Star, the target site is Isolated when this option is enabled. During Cleanup, the Isolated site is connected back. The possible values are YES and NO. By default, the value is set to NO.

For example:

```
<TestFailoverWithoutLocalSnapshots>NO</TestFailoverWithoutLocalSnapshots>
```

TerminateCopySessions

Forces the test failover operation to terminate the clone snap and VP Snap sessions when the test failover operation resets storage. When this option is enabled, SRA removes the devices from the device group or composite group during cleanup. The possible values are YES and NO. By default, the value is set to NO.

For example:

```
<TerminateCopySessions>NO</TerminateCopySessions>
```

FailoverIfGoldCopyFails

When the goldcopy backup operation fails prior to failover, this option can be set or unset if failover of the LUNs is required. The possible values for this option are YES and NO. By default, the value is set to YES.

For example:

```
<FailoverIfGoldCopyFails>YES</FailoverIfGoldCopyFails>
```

IgnoreActivatedSnapshots

Ignores activated TimeFinder Snap snapshot, TimeFinder clone, or TimeFinder VP snap sessions and enables the test failover operation to complete successfully. In the case of SRDF/Star, Isolated target site is ignored when this option is enabled. The possible values are YES and NO. By default, the value is NO.

For example:

```
<IgnoreActivatedSnapshots>NO</IgnoreActivatedSnapshots>
```

FilterNonVmwareDevices

Filters out all the SRDF devices that are not visible to VMware environment. This must be set to the same value at both sites. The possible values are YES and NO. By default, the value is set to Yes.

For example:


```
<FilterNonVmwareDevices>YES</FilterNonVmwareDevices>
```

CheckForVirtualDisks

Checks if the target TimeFinder devices for test failover or goldcopy are already used VMware environment as virtual disks (Raw device mappings or Flat virtual disks). The possible values are YES and NO. By default, the value is set to No.

For example:

```
<CheckForVirtualDisks>NO</CheckForVirtualDisks>
```

 **NOTE:** FilterNonVmwareDevices and CheckForVirtualDisks options require VMware vCenter user credentials that are configured in the local Solutions Enabler authorization table. Make sure that you have the right credentials configured using SYMCLI. For instructions on this process, see *Using SRDF Adapter for VMware Site Recovery Manager* which is available on <https://support.EMC.com>.

FailoverToAsyncSite

Performs recovery operations between the sites connected with SRDF/A link. This option is applicable only when SRDF/Star and 3 site configurations are used in the Site Recovery Manager environment. The possible values are YES and NO. By default, the value is set to No. This option requires the same value set at both sites.

For example:

```
<FailoverToAsyncSite>No</FailoverToAsyncSite>
```

SetReplicaTargetToReady

Tries to set the target SRDF device to Ready state. For `TestFailoverWithoutLocalSnapshots`, the target SRDF device is set back to Not Ready during cleanup. For the Recovery operation, the source device is set to Not Ready after the Reprotect. The possible values are YES and NO. By default, the value is set to No.

For example:

```
<SetReplicaTargetToReady>No</SetReplicaTargetToReady>
```

ReverseReplicationDuringRecovery

When enabled SRA tries to reverse the replication direction at the end of the recovery operation. This is supported only in planned migration recovery. This option should be disabled for Disaster recovery. Also this is not supported in Star configurations. The possible values are YES and NO. By default, the value is set to NO.

For example:

```
<ReverseReplicationDuringRecovery>Yes</ReverseReplicationDuringRecovery>
```

RdfDeviceMaskingControl

When enabled:

1. During a planned recovery operation, RDF1 devices are masked to the protected site and RDF2 devices are unmasked (made visible) to the recovery site.
2. During a disaster recovery operation, RDF1 devices may or may not be masked to the protected site, based on the availability of Site Recovery Manager server, and RDF2 devices are unmasked (made visible) to the recovery site.

This option uses the masking view information provided in `EmcSrdfSraDeviceMaskingControl.xml` file. Possible values are YES and NO. By default, the value is set to No.

For example:

```
<RdfDeviceMaskingControl>No</RdfDeviceMaskingControl>
```

TestReplicaMaskingControl

When enabled, SRA tries to mask or unmask the TimeFinder devices and RDF2 devices (if `TestFailoverWithoutLocalSnapshots` is enabled) to the recovery site. This option is only applicable to test recovery operations. Possible values are YES and NO. By default, the value is set to No.

For example:

```
<TestReplicaMaskingControl>No</TestReplicaMaskingControl>
```

IgnoreDisconnectedStar

When enabled (set to YES), SRA does not try to bring up any Star configuration (even the ones protected by Site Recovery Manager) irrespective of the state of the Star. By default, this option is set to NO, which means that SRA tries to bring up the Star during discover devices.

For example:

```
<IgnoreDisconnectedStar>No</IgnoreDisconnectedStar>
```

AutoTargetDevice

When this option is enabled, SRA creates target devices dynamically to link snapshots during a Test operation. By default, these devices present to the same hosts to which corresponding R2 devices are visible. To present these dynamically created target devices to a different host, set the corresponding R2 device as a placeholder in `EmcSrdfSraMaskingControl.xml` file under `SrcDeviceList` tag.

For example:

```
<MaskView>
  <ArrayId> ArrayID </ArrayId>
  <StorageGroup> Storage Group</StorageGroup>
  <SrcDeviceList>
    <Device>R2 devices set as placeholder for dynamically created target device</
Device>
  </SrcDeviceList>
</MaskView>
```

Also when this option is enabled, these target devices would be unrepresented from hosts as well as deleted during a Cleanup operation (if the `AutoTargetDeviceReuse` global option is not set).

This release supports ONLY SnapVX copy type for the dynamic target devices. By default copy mode is NOCOPY when no valid CopyInfoBlock is found in the EmcSrdfSraTestFailoverConfig.xml file. To use copy mode as COPY, EmcSrdfSraTestFailoverConfig.xml should be filled with valid CopyInfoBlock, leaving Target tags empty in DevicePairs.

For example:

```
<AutoTargetDevice>No</AutoTargetDevice>
```

AutoTargetDeviceReuse

When enabled along with AutoTargetDevice, SRA retains dynamically created target devices and adds the source to target mapping in the EmcSrdfSraTestFailoverConfig.xml file. SRA reuses these devices in subsequent operations until a Cleanup operation is called with disabled AutoTargetDeviceReuse which also removes mapping from the EmcSrdfSraTestFailoverConfig.xml file. Whenever SRA modifies EMCSrdfSraTestFailoverConfig.xml content, the original file content is preserved by adding the suffix ".EMCSRDFSRA.bak_YYMMDDhhmmssuuu" to the original file where year is YY, month is MM, date is DD, hour is hh, minutes are mm, seconds are ss and microseconds are uuu.

For example:

```
<AutoTargetDeviceReuse>Yes</AutoTargetDeviceReuse>
```

Notes on using AutoTargetDevice and AutoTargetDeviceReuse:

- Enabling AutoTargetDevice can cause a conflict when both TerminateCopySession and AutoTargetDeviceReuse are disabled. This is due to a disabled TerminateCopySession preserve session between a snapshot and a target device that makes dynamic target devices undeletable and AutoTargetDeviceReuse disabled tried to delete these devices when Cleanup is called. To resolve this, either TerminateCopySession must be enabled to ensure dynamically created devices can be deleted in Cleanup or else turn on AutoTargetDeviceReuse enable so that a Cleanup operation does not delete target devices.

Note: For manually created device: <TerminateCopySession> flag, if enabled, unlinks the SnapVX. For Auto Target Device: <TerminateCopySession> flag is not considered anymore. If the <AutoTargetDeviceReuse> flag is disabled, unlink operation is done followed by device delete operation.

- SRA fails when AutoTargetDeviceReuse is enabled but AutoTargetDevice is disabled as an invalid configuration. To fix this, AutoTargetDevice must be enabled to create target devices first and then enabled AutoTargetDeviceReuse is a valid configuration to retain those target devices.
- The creation and deletion of devices is an expensive operation in terms of time and may lead to SRM timeout. This can be fixed by adjusting the SRM timeout to a suitable value.
- SRA fails on Test and Cleanup operations when the CopyInfoBlock of the EmcSrdfSraTestFailoverConfig.xml file contains partially-filled Target tags. Either all Target tags should be empty or all should be filled (by SRA when Test successful completed and AutoTargetDeviceReuse is enabled). To avoid this issue, the EmcSrdfSraTestFailoverConfig.xml file can be deleted or renamed.
- SRA fails on Test and Cleanup operations when the CopyInfoBlock of the EmcSrdfSraTestFailoverConfig.xml file contains non-empty Targets (filled manually) and AutoTargetDevice is enabled. To fix this, the EmcSrdfSraTestFailoverConfig.xml file should be move/renamed to use the AutoTargetDevice feature.
- If devices in the SRM replication plan are a subset of the CopyInfoBlock device list, then target devices would be created for all R2 devices present in CopyInfoBlock. These devices are deleted when a Cleanup operation is called with AutoTargetDeviceReuse disabled.

ViClientIgnoreSecurityException

SRA uses ViClient to connect with VCenter Server. This flag is used to Ignore Security Exceptions while establishing a secure connection. Enable this flag to establish a secure connection by using existing user verified truststore certificates, the value options are YES and NO. By default, the value is set to Yes.

For example:

```
<ViClientIgnoreSecurityException>Yes</ViClientIgnoreSecurityException>
```

AutoTargetDeviceFreeTracks

When enabled along with AutoTargetDevice and AutoTargetDeviceReuse flags, SRA will free all tracks of the re-used auto target device in a Cleanup operation.

For example:

```
<AutoTargetDeviceFreeTracks>No</AutoTargetDeviceFreeTracks>
```

NOTE:

- While operating with this flag, all prerequisite of using the flag AutoTargetDeviceReuse must to be met.
- While the free tracks operation is in progress as part of the Cleanup operation, the re-used auto TDEVs are not present in the applicable storage groups. Once the Cleanup operation completes, the devices are present in the applicable storage groups.

EmcSrdfSraTestFailoverConfig.xml

This file is used to specify device pairs for test failover operations.

The following Document Type Definition (DTD) describes EmcSrdfSraTestFailoverConfig.xml:

```
<!ELEMENT TestFailoverInfo (Version?, CopyInfo+)>
<!ELEMENT Version (#PCDATA)>
<!ELEMENT CopyInfo (ArrayId?, CopyType?, SavePoolName?, DeviceList?, CopyMode?)>
<!ELEMENT ArrayId (#PCDATA)>
<!ELEMENT CopyType (#PCDATA)>
<!ELEMENT CopyMode (#PCDATA)>
<!ELEMENT SavePoolName (#PCDATA)>
<!ELEMENT DeviceList (DevicePair+)>
<!ELEMENT DevicePair (Source, Target)>
<!ELEMENT Source (#PCDATA)>
<!ELEMENT Target (#PCDATA)>
```

The following is an example of EmcSrdfSraTestFailoverConfig.xml:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<TestFailoverInfo>
  <Version>9.2</Version>
  <CopyInfo>
    <ArrayId>000190300186</ArrayId>
    <CopyType>SNAP</CopyType>
    <CopyMode>NOCOPY</CopyMode>
  <SavePoolName>SRA</SavePoolName>
  <DeviceList>
    <DevicePair>
      <Source>4D8</Source>
      <Target>4DE</Target>
    </DevicePair>
    <DevicePair>
      <Source>4D9</Source>
      <Target>4DF</Target>
    </DevicePair>
  </DeviceList>
</CopyInfo>
</TestFailoverInfo>
```

The following section describes the options in EmcSrdfSraTestFailoverConfig.xml.

TestFailoverInfo

Contains all of the elements for the test failover operations.

CopyInfo

The CopyInfo element defines device pairs for a specific copy type on a PowerMax array.

ArrayId

You can specify multiple CopyInfo blocks within TestFailoverInfo or GoldCopyInfo with different array IDs.

For example:

```
<ArrayId>000190300186</ArrayId>
```

CopyType

Specifies the type of replication technology for the test failover or goldcopy operation. The possible values are VSE (TimeFinder/VP Snap), clone, and SnapVx.

For example:

```
<CopyType>CLONE</CopyType>
```

CopyMode

Specifies the type of the data copy used in the TimeFinder SnapVX replication. This is applicable only to the TimeFinder SnapVX replication technologies. The possible values are COPY and NOCOPY.

For example:

```
<CopyMode>COPY</CopyMode>
```

DeviceList

Specifies the device pair information. This is necessary to perform the test failover operation. Each device pair represents source and target device pairs. For all copy types, the source device is the R2 device on the recovery site. For VSE type, the targets are TDEV devices. For clone types, the target devices are the clone targets, and for snap types, the target devices are the VDEVs. For SnapVX types, the target devices are TDEV devices.

For example:

```
<DeviceList>
  <DevicePair>
    <Source>4D8</Source>
    <Target>4DC</Target>
  </DevicePair>
  <DevicePair>
    <Source>4D9</Source>
    <Target>4DD</Target>
  </DevicePair>
</DeviceList>
```

EmcSrdfSraProtectionSiteGoldcopyConfig.xml

This file is used to specify device pairs for protection site goldcopy backup operations.

The following DTD describes EmcSrdfSraProtectionSiteGoldcopyConfig.xml:

```
<!ELEMENT ProtectionSiteGoldcopyInfo (Version?, CopyInfo+)>
<!ELEMENT Version (#PCDATA)>
<!ELEMENT CopyInfo (ArrayId?, CopyType?, SavePoolName?, DeviceList?, CopyMode?)>
<!ELEMENT ArrayId (#PCDATA)>
<!ELEMENT CopyType (#PCDATA)>
<!ELEMENT CopyMode (#PCDATA)>
<!ELEMENT SavePoolName (#PCDATA)>
<!ELEMENT DeviceList (DevicePair+)>
<!ELEMENT DevicePair (Source, Target)>
<!ELEMENT Source (#PCDATA)>
<!ELEMENT Target (#PCDATA)>
```

The following is an example of EmcSrdfSraProtectionSiteGoldcopyConfig.xml:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<ProtectionSiteGoldcopyInfo>
  <Version>9.2</Version>
  <CopyInfo>
    <ArrayId>000190300186</ArrayId>
    <CopyType>CLONE</CopyType>
    <CopyMode>NOCOPY</CopyMode>
    <SavePoolName></SavePoolName>
    <DeviceList>
      <DevicePair>
        <Source>4D8</Source>
        <Target>4DC</Target>
      </DevicePair>
      <DevicePair>
        <Source>4D9</Source>
        <Target>4DD</Target>
      </DevicePair>
    </DeviceList>
  </CopyInfo>
</ProtectionSiteGoldCopyInfo>
```

The options in EmcSrdfSraProtectionSiteGoldCopyConfig.xml are the same as those for EmcSrdfSraTestFailoverConfig.xml.

EmcSrdfSraRecoverySiteGoldcopyConfig.xml

This file is used to specify device pairs for recovery site goldcopy backup operations.

The following DTD describes EmcSrdfSraRecoverySiteGoldcopyConfig.xml:

```
<!ELEMENT RecoverySiteGoldcopyInfo (Version?, CopyInfo+)>
<!ELEMENT Version (#PCDATA)>
<!ELEMENT CopyInfo (ArrayId?, CopyType?, SavePoolName?, DeviceList?, CopyMode?)>
<!ELEMENT ArrayId (#PCDATA)>
<!ELEMENT CopyType (#PCDATA)>
<!ELEMENT CopyMode (#PCDATA)>
<!ELEMENT SavePoolName (#PCDATA)>
<!ELEMENT DeviceList (DevicePair+)>
<!ELEMENT DevicePair (Source, Target)>
<!ELEMENT Source (#PCDATA)>
<!ELEMENT Target (#PCDATA)>
```

The following is an example of EmcSrdfSraRecoverySiteGoldcopyConfig.xml:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<RecoverySiteGoldcopyInfo>
  <Version>9.2</Version>
  <CopyInfo>
    <ArrayId>000190300186</ArrayId>
    <CopyType>CLONE</CopyType>
    <CopyMode>NOCOPY</CopyMode>
    <SavePoolName></SavePoolName>
    <DeviceList>
      <DevicePair>
        <Source>4D8</Source>
        <Target>4DC</Target>
      </DevicePair>
      <DevicePair>
        <Source>4D9</Source>
        <Target>4DD</Target>
      </DevicePair>
    </DeviceList>
  </CopyInfo>
</RecoverySiteGoldCopyInfo>
```

The options in EmcSrdfSraRecoverySiteGoldCopyConfig.xml are the same as those for EmcSrdfSraTestFailoverConfig.xml.

EmcSrdfSraDeviceMaskingControl.xml

This file is used to specify PowerMax device masking details for SRDF and TimeFinder devices.

The following DTD describes EmcSrdfSraDeviceMaskingControl.xml:

EmcSrdfSraDeviceMaskingControl.xml

```
<!ELEMENT DeviceMaskingInfo (Version?, MaskViewList?)>
<!ELEMENT Version (#PCDATA)>
<!ELEMENT MaskViewList (MaskView+)>
<!ELEMENT MaskView (ArrayId?, StorageGroup?, DeviceList?)>
<!ELEMENT ArrayId (#PCDATA)>
<!ELEMENT StorageGroup (#PCDATA)>
<!ELEMENT DeviceList (Device+)>
<!ELEMENT SrcDeviceList (Device+)>
<!ELEMENT DevicePair (#PCDATA)>
```

The following is an example of EmcSrdfSraDeviceMaskingControl.xml:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<DeviceMaskingInfo>
  <Version>9.2</Version>
  <MaskViewList>
    <MaskView>
      <ArrayId>000194900390</ArrayId>
      <StorageGroup>spea219_390</StorageGroup>
      <DeviceList>
        <Device>0422c</Device>
        <Device>044b6</Device>
      </DeviceList>
    </MaskView>
  </MaskViewList>
</DeviceMaskingInfo>
```

```

    </DeviceList>
    <SrcDeviceList>
      <Device>0422d</Device>
      <Device>044b7</Device>
    </SrcDeviceList>
  </MaskView>
</MaskViewList>
</DeviceMaskingInfo>

```

The following section describes the options in `EmcSrdfSraDeviceMaskingControl.xml`:

MaskViewList

A list of MaskViews. Multiple MaskView blocks can be used for different array IDs.

MaskView

The MaskView information for a specific array ID.

ArrayId

The array ID for which device masking information is provided.

StorageGroup

A container of a storage devices. A masking view includes a storage group, a port group, and an initiator group. When a masking view is created, the devices in the storage group become visible to the host. This option takes the name of the storage group to which a set of devices should be added or removed.

DeviceList

A list of devices to be added or removed from storage group.

SrcDeviceList

A list of R2 devices as placeholder for dynamically created target devices. This tag is effective when `AutoTargetDevice` and `TestReplicaMaskingControl` both are enabled in `EmcSrdfSraGlobalOptions.xml`.

Device


The ID of a PowerMax device that needs to be added or removed from a storage group. A device can be either an SRDF device or a TimeFinder device.

SRA does not check for duplicate Device IDs. The first MaskView under which a Device ID is found is used in the device masking operation.

Dockers platform

- **enableAutoSSLCertGen.sh**: The **enableAutoSSLCertGen.sh** script ensures that a valid client certificate is generated with the correct hostname to ensure a smooth client/server communication for SYMCLI or other commands.
- **Reload**: A Reload operation using the Appliance Management Interface kills the existing running container and spawns a new container upon any operation in the SRM.
- **Reset Configuration**: A reset operation on the Appliance Management Interface deletes all the mounts and volumes that are associated with the image and deletes the data.

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.