

TECHNICAL NOTES

Dell Technologies PowerStore Storage Replication Adapter (SRA)
Plugin for VMware Site Recovery Manager
Version 2.1

The Release Notes document contains information on these topics:

[Revision History](#) 2

[Product Description](#) 2

[Environment and System Requirements](#) 2

[Technical Notes](#) 3

[Documentation](#)..... 4

[Software Media](#) 5

[Installation](#)..... 5

[Configuring certificates for Photon OS](#) 8

[Configuring multi-site replication](#) 13

[Resetting the SRA Configuration to the Factory Defaults](#) 17

[Uninstalling the Dell PowerStore Storage Replication Adapter for Linux](#)..... 18

[Upgrading the Dell PowerStore Storage Replication Adapters](#) 18

[Getting Help](#) 18

Revision History

Revision	Date	Description
01	May 2020	Initial release of version 1.0
02	January 2022	Multisite support release 2.0
03	May 2023	Rebranded to Dell Technologies
04	July 2023	Multisite support release 2.1.

Product Description

Dell PowerStore Storage Replication Adapter for VMware Site Recovery Manager (SRA) allows VMware Site Recovery Manager (SRM) to implement disaster recovery for PowerStore clusters. Dell PowerStore Storage Replication Adapter supports SRM functions such as failing over, failing back, and failover testing using PowerStore as the replication engine.

- SRA version 2.1 is for Linux/Photon OS environments only.

Environment and System Requirements

Prerequisites

Before the Dell PowerStore SRA can be installed, the following prerequisites must be met:

- The VMware vCenter and Site Recovery Manager (SRM) must be installed and configured according to the VMware documentation.
- HTTPS TCP port 443 must be opened between the SRM server and PowerStore.

SRA Compatibility Matrix

The following table presents the Dell PowerStore SRA Compatibility Matrix; the latest versions are recommended:

vSphere	SRM
6.7	8.2 (Photon OS only) 8.3 (Photon OS only)
7.0	8.4 (Photon OS only) 8.5 (Photon OS only)
8.0	8.6 (Photon OS only) 8.7 (Photon OS only)

For the VMware Administration Guide, refer to VMware Documentation (<http://www.vmware.com/support/pubs>).

Setting Up the PowerStore Native Replication

To use the VMware Site Recovery Manager, the PowerStore clusters must be configured for native replication and metro replication. Refer to the *PowerStore Configuring Volumes Guide* for a detailed explanation of setting up the PowerStore clusters for native replication and the *PowerStore Protecting Your Data Guide* for instructions on setting up clusters for metro replication.

Technical Notes

This section contains important information about deploying Dell PowerStore SRA and VMware Site Recovery Manager.

Volume Groups and SRM Protection Groups

SRM protection group failover (during testing and actual failover) instructs the Dell PowerStore Storage Replication Adapter to operate on all the LUNs of all the virtual machines in a protection group. PowerStore uses a single volume or volume groups to define groups of LUNs that replicate together. If the SRM protection group LUNs upon which the Dell PowerStore Storage Replication Adapter operates differ from the PowerStore volume group LUNs, then the mismatch may result in unintended behavior or operation failure. The mismatch of LUNs could be the result of LUNs in the SRM protection group that are missing from the PowerStore volume groups, LUNs in the volume groups from another SRM protection group, or LUNs in the volume group from non-SRM protection groups. To avoid unintended behavior or operation failover, it is recommended that you take the following actions:

- Group all the virtual machine LUNs in an SRM protection group in one or more PowerStore volume groups or replicate them as a single volume. Ensure each of these contains only LUNs from that protection group and does not contain LUNs from any other protection group or other application. This ensures that all the SRM protection

group's LUNs are handled by SRM. This also ensures that SRM does not attempt to operate concurrently on the same volume group, which may result in SRM operations failing, or unintended behavior.

- Ensure PowerStore volume groups that contain SRM protection group LUNs do not contain non-SRM protection group LUNs. This ensures that SRM does not handle non-SRM protection group LUNs.
- In addition, it is a best practice to avoid concurrently performing operations on the same volume group using VMware SRM or PowerStore Manager as this may cause these operations to interfere with each other.
- Allowlist and Blocklist fields enable you to filter devices.

For further information about PowerStore volume groups and other objects, refer to the *PowerStore Configuring Volumes Guide*.

Note: Before you first launch SRA, verify that all the protected replicated volumes are mapped to hosts. SRA does not report to SRM protected replicated volumes that are unmapped to hosts. For more details about PowerStore native replication objects and settings, refer to the *PowerStore Configuring Volumes Guide*.

New Features

The following features have been added to this release:

- Support for PowerStore 3.5
- Support for metro volumes

Known issues

Summary	Description	Workaround
Device discovery fails for SRM array pairs if there is a broken PowerStore metro replication session.	When metro replication sessions exist are broken (probably due to array initialization or lost connections), attempts to discover PowerStore devices in SRM fail with the error "SRA command discoverDevices failed."	Delete all broken metro replication sessions or volume pairs and re-discover the devices in SRM.

Documentation

For the most current VMware vCenter SRM documentation, refer to the VMware web site (<http://www.vmware.com/support/pubs>).

For the most current Dell SRA documentation, on the Dell Online Support Site (<https://dell.com/support>) go to PowerStore > Documentation > Release Notes or contact Dell Customer Support.

Use the release of any of the following documents, available in the Documentation Library on Dell Online Support Site, that matches your installed PowerStore version:

- *PowerStore Release Notes*
- *PowerStore Configuring Volumes Guide*
- *PowerStore Protecting Your Data Guide*

Software Media

Once you download the SRM software from the VMware web site and install it, the Dell PowerStore SRA may be downloaded and installed.

The Dell Online Support Site also has the most current Dell PowerStore SRA information.

Installation

This section contains important information about downloading, installing, updating, and uninstalling Dell PowerStore Site SRA Installers for Photon OS Linux operating system.

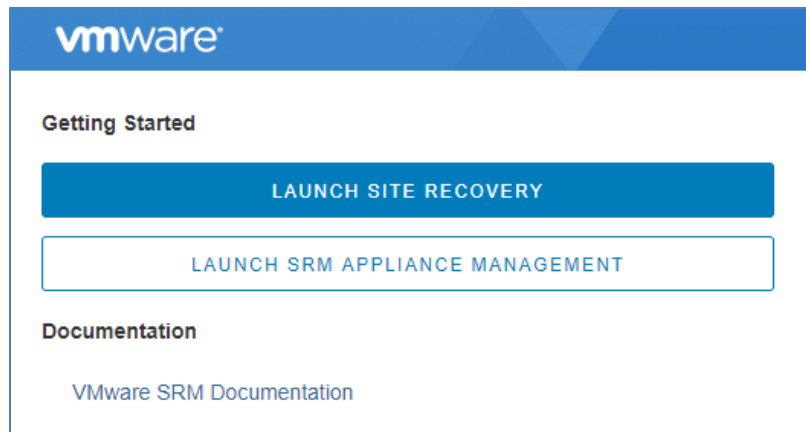
Downloading, Installing, Updating and Uninstalling Dell PowerStore SRA for Photon OS

Before installing the Dell PowerStore SRA for Linux, make sure that VMware SRM is installed on each Site Recovery Manager Server host. For more information on installing Site Recovery Manager, see the VMware vCenter Site Recovery Manager documentation (<https://pubs.vmware.com>).

To download and install Dell PowerStore SRA for Photon OS:

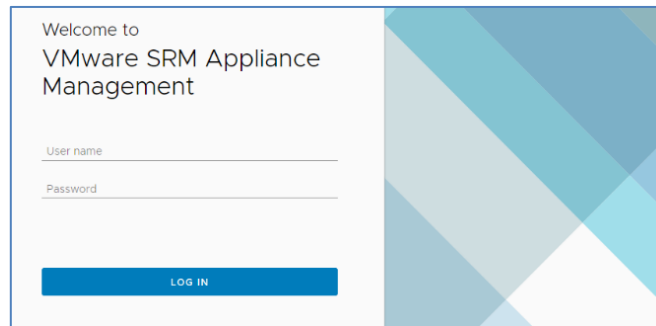
1. Verify that PowerStore clusters are configured to be fully operational, including remote systems, volume groups, and replication sessions.
2. Navigate to <https://my.vmware.com/web/vmware/downloads>.
3. Click VMware Site Recovery Manager > **Drivers & Tools**.
4. Click **Storage Replication Adapters > GO TO DOWNLOADS**.
5. Find the row for Dell PowerStore SRA for Photon OS and click **DOWNLOAD NOW** to download the installer file:
`Dell_EM_C_PowerStore_SRA_Linux_v.(release version).tar.gz`.
Optionally, you can download the signature file and then verify the downloaded file.

6. Go to the SRM WEB UI at [https:// <appliance IP address or FQDN>/](https://<appliance IP address or FQDN>/) and click **Launch SRM Appliance Management**.



VMware Getting Started dialog

The Welcome to VMware Appliance Management dialog box appears.

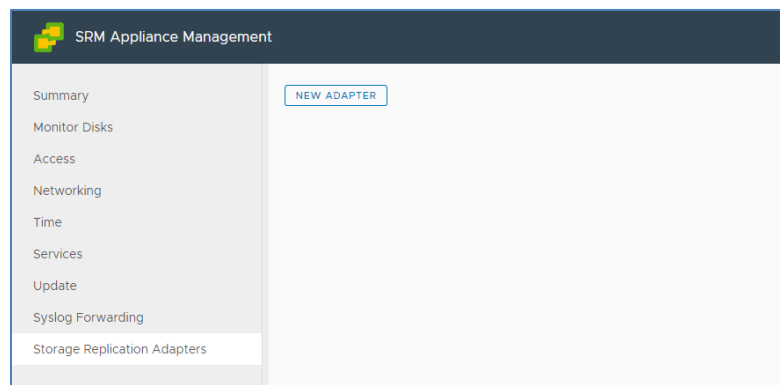


Welcome to VMware Appliance Management dialog

7. Enter your credentials (default administrator user is admin), and click **LOG IN**.

Note: Authenticate using SRM administrative user as configured during the SRM installation stage with administrative privileges. Verify that the replication sessions to be used with SRM are enabled and active.

8. In the SRM Appliance Management dialog box, click **Storage Replication Adapters**.



Creating a new adapter

9. Click **NEW ADAPTER**; the New Adapter dialog box appears.
10. Click **UPLOAD**, and in the resulting file browser, navigate to and select the `Dell_EMCPowerStore_SRA_Linux_v.(release version).tar.gz` file.
11. Click **CLOSE** when finished.

Verifying the digital signature on systems running Linux

If you do not already have Gnu Privacy Guard (GPG) installed on your system, you must install it to verify the Linux Dell GPG digital signature. The following steps describe the standard verification procedure:

1. Download the Dell Linux public GnuPG keys (GPG1 and GPG2), if you do not already have them.
You can download the keys by navigating to http://linux.dell.com/files/pgp_pubkeys/.
2. Import the public key to the GPG trust database by running the following command: `gpg --import <Public Key Filename>`
Note: You must import the GPG1 and GPG2 public keys:
 - GPG2 key: `0x756ba70b1019ced6.asc`
 - GPG1 key: `0xca77951d23b66a9d.asc`
3. Validate the public key by its fingerprint to avoid a distrusted key warning.
 - a. Enter the following command: `gpg --edit-key <key>`
 - b. In the GPG key editor, enter `fpr`.
A message like the following appears:

```
pub 2048D/1019CED6 2011-10-17 Dell Inc., PGRE 2011
(PG Release Engineering Build Group 2011)
PG Release Engineering@Dell.com. Primary key
fingerprint: 79A1 61F5 A83F 992C CB10 A544 756B A70B
1019 CED6.
```

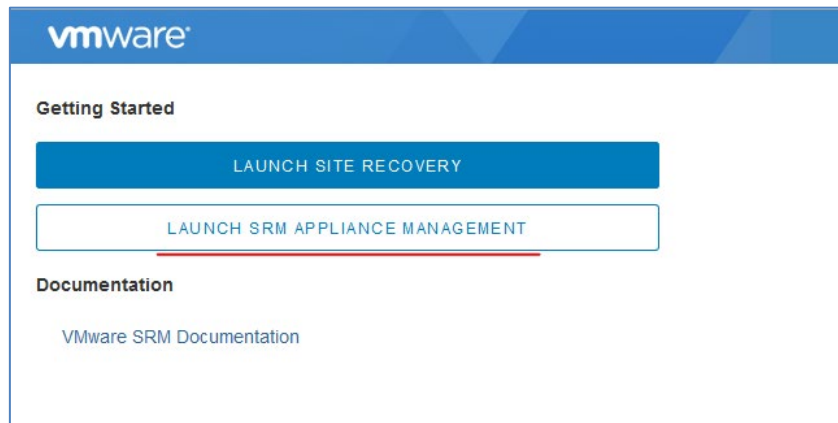
If the fingerprint of the imported key is the same as that of the key owner, you have a correct copy of the key. You can verify the key owner in person, over the phone, or by other means that guarantees that you are communicating with the true owner of the key.
 - c. Enter `sign` while you are still in the key editor.
 - d. Answer the list of trust validation questions that appear and create a passphrase to use as the secret key.
You import and validate the public key only once.
4. Enter the following command to verify the downloaded `Dell_EMCPowerStore_SRA_Linux_v.(release version).tar.gz` file:
`gpg --verify Dell_EMCPowerStore_SRA_Linux_v.(release version).tar.gz.sign`

Dell EMC PowerStore_SRA_Linux_v.(*release version*).tar.gz

Configuring certificates for Photon OS

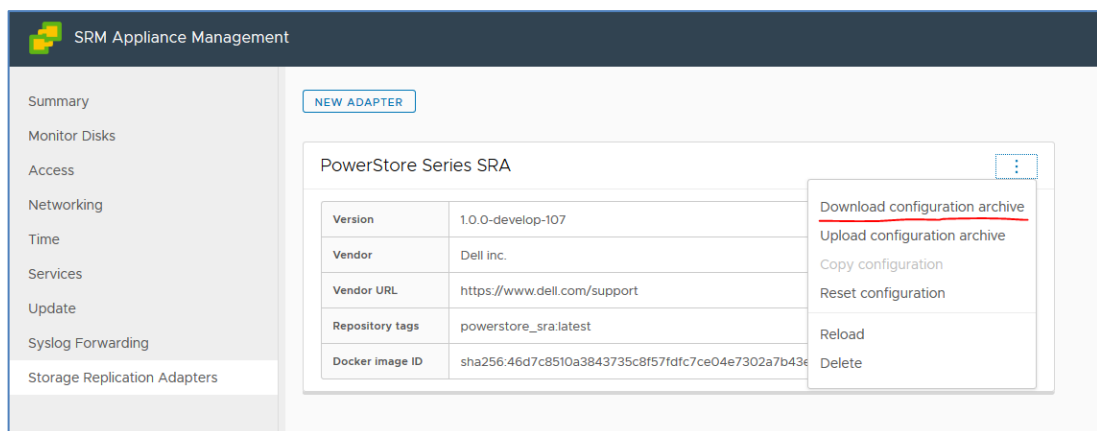
The following procedure describes configuring Dell PowerStore SRA certificates for Photon OS.

1. Get the **root** certificate of the PowerStore instance; the certificate format should be .pem.
2. Go to the SRM configuration web user interface and click **Launch SRM Appliance Management**; the UI should be communicating with the PowerStore instance.



Getting started

3. Log in.
4. Go to **Storage Replication Adapters**.
5. Click the ellipses (...), and then click **Download configuration archive**.



Download the configuration archive

6. Extract the archive content.

<input type="checkbox"/> Name	Date modified	Type	Size
config.ini	12/4/2019 3:12 PM	Configuration sett...	1 KB
sra-configuration-version.txt	12/4/2019 3:11 PM	Text Document	1 KB

The config.ini file

7. Place the root SSL certificate beside the config.ini file.

<input type="checkbox"/> Name	Date modified	Type	Size
config.ini	12/4/2019 3:15 PM	Configuration sett...	1 KB
root_ca.pem	12/3/2019 3:01 PM	PEM File	2 KB
sra-configuration-version.txt	12/4/2019 3:11 PM	Text Document	1 KB

The root.ca.pem file with the config.ini file

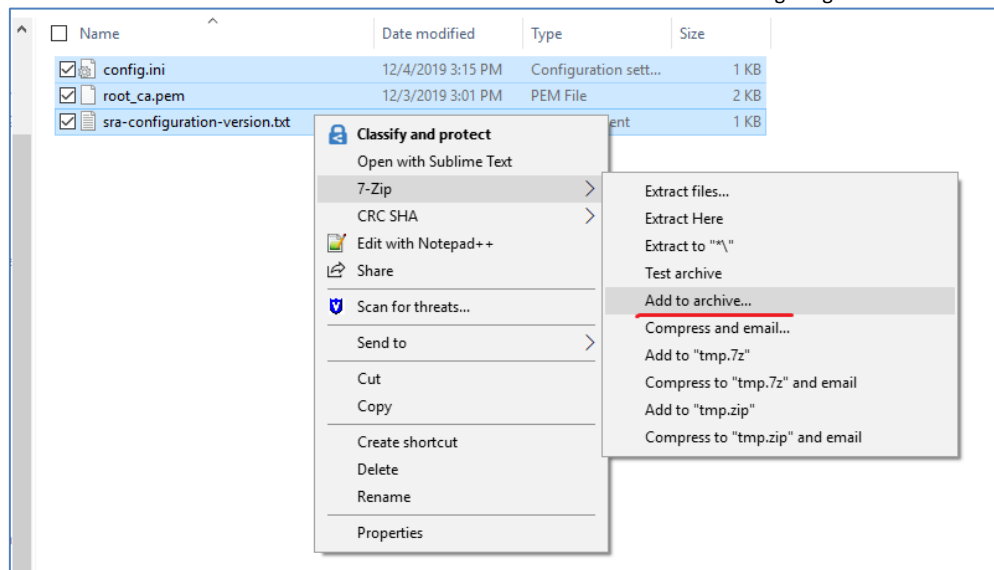
8. Open the config.ini file, specify the location for the root_ca.pem certificate, and then save the config.ini file.

```

1 ; Use only UTF-8 encoding for this file!
2
3 [client]
4 ; specify in seconds
5 connection_timeout = 20.0
6 connection_attempts = 3
7
8 [ssl]
9 verify = True
10 ca_path = root_ca.pem
11 ; if you're using a self-signed certificate you should install a root certificate to windows trust store.
12 protocols = tls1.2
13 ;         tls1.1 (deprecated)
14
15 [ssl:tls1.2]
16 ; the cipher list consists of one or more openssl cipher strings separated by colons.
17 ciphers = AESGCM:-ANULL:-DH:-kRSA:@STRENGTH
18
19 [ssl:tls1.1]
20 ; the cipher list consists of one or more openssl cipher strings separated by colons.
21 ciphers = AESGCM:-ANULL:-DH:-kRSA:@STRENGTH
22 ; to see detailed list use command: openssl ciphers -v "aesgcm:-anull:-dh:-krsa:@strength"
23
24 [polling]
25 ; specify in seconds
26 poll_delay = 3.0
27 poll_attempts = 10

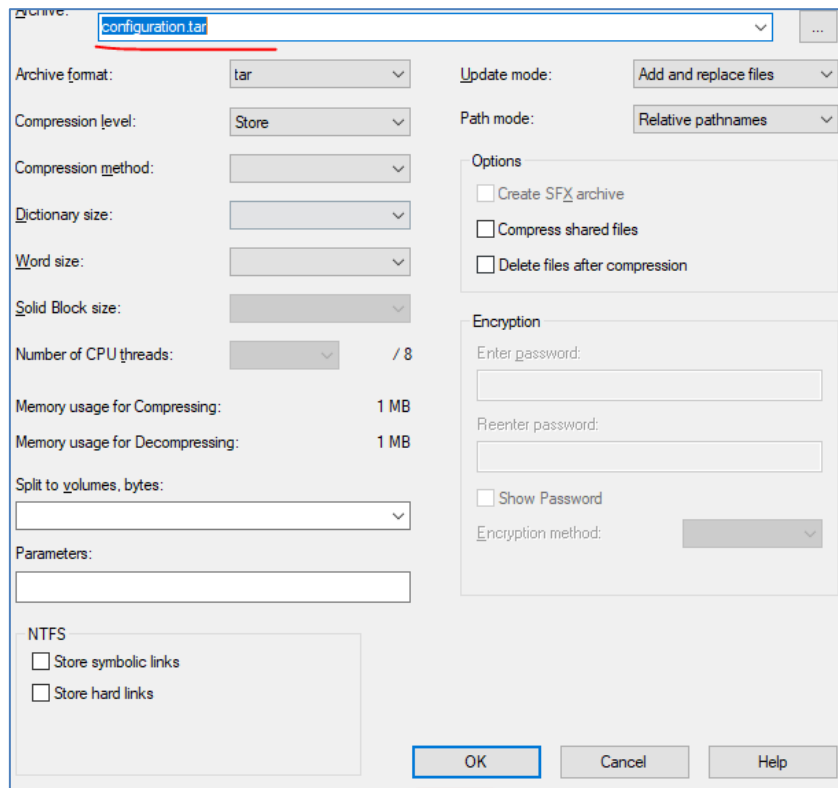
```

Setting ca_path to root_ca.pem

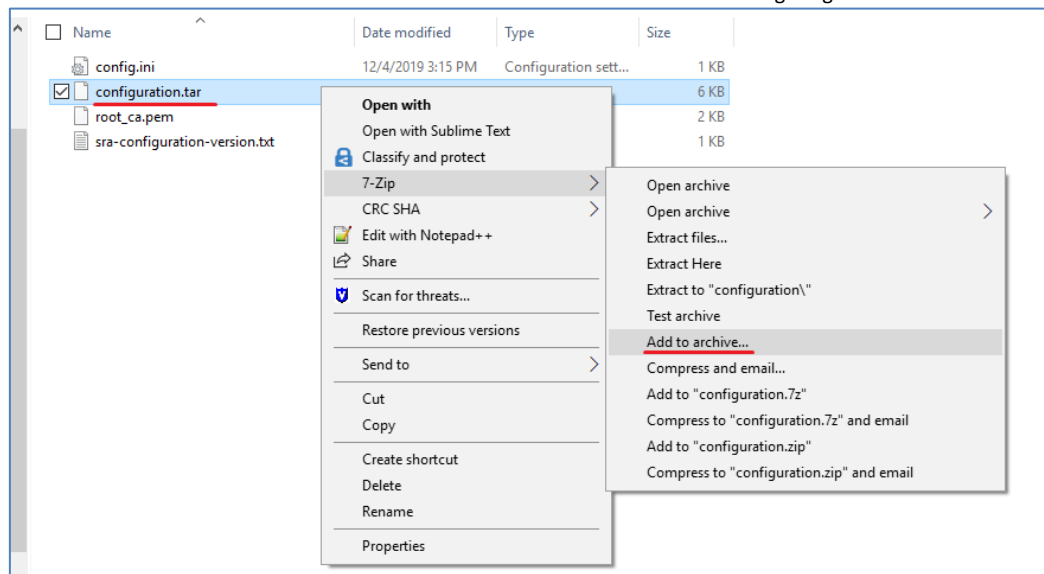


Ready to pack the configuration

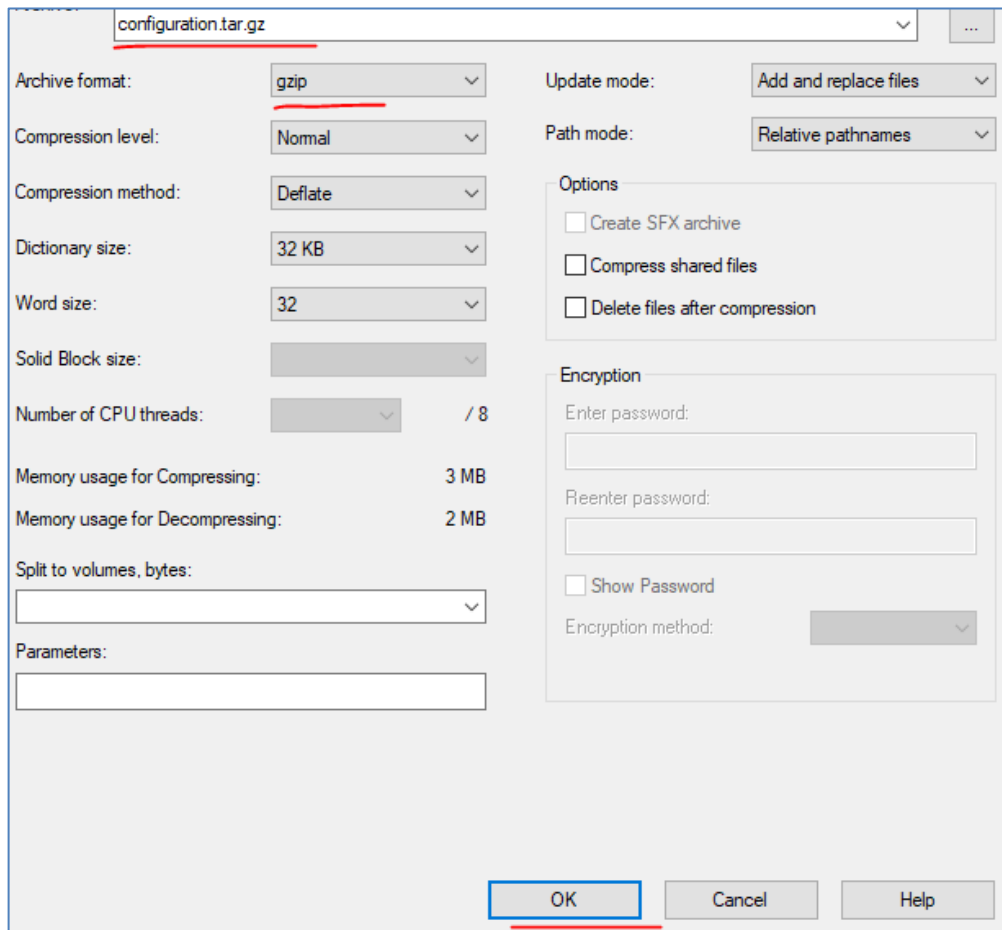
9. Pack the configuration to a new gzipped tarball.



Packing the configuration

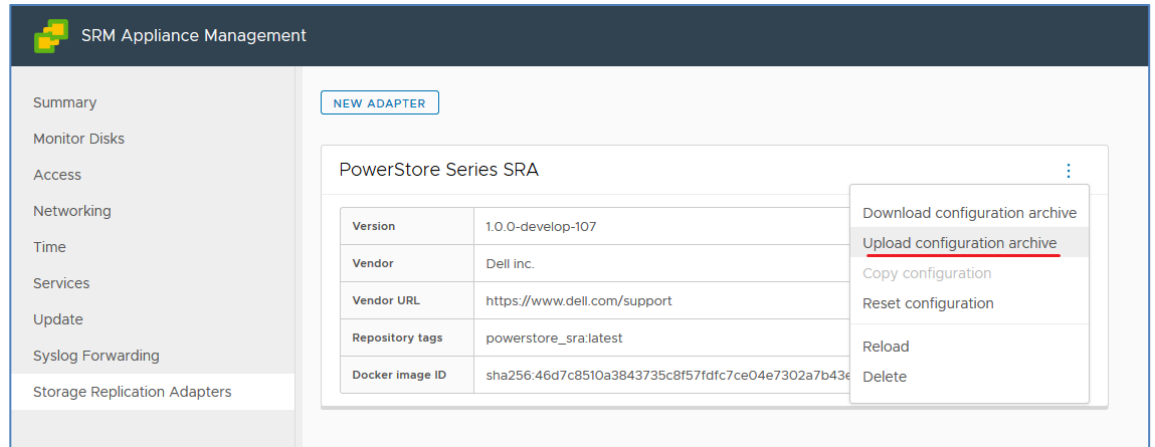


Adding the configuration to the archive

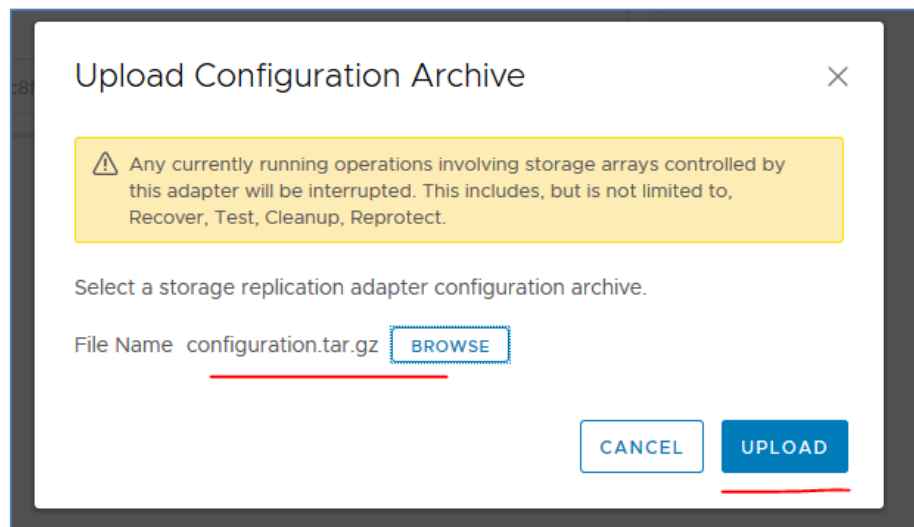


Putting the configuration into a gzipped tarball

10. Go back to SRM and upload the new configuration (configuration.tar.gz).

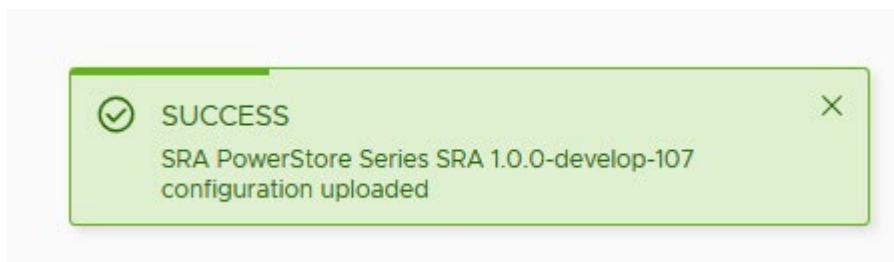


Preparing to upload the configuration



Uploading the configuration.tar.gz file.

The configuration is complete. SRA should be using a secure connection.



Configuration complete

Configuring multi-site replication

You can configure multi-site replication for SRA for PowerStore. As you add more site pairs, the topology of SRA grows more complex, although each SRM supports one site pair only.

SRA is isolated within the site pair scope. Because of this isolation, each SRA cannot know which storage elements are related to its site pair. By default, SRA shows all replicated storage elements. If you want to filter these elements, specify the Preferred local and remote PowerStore Manager IPs when you create each array pair in the Add Array Pair wizard.

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

Local array manager

Array managers allow Site Recovery Manager to communicate with array based replication storage systems.

Enter a name for the array manager on "vc0.sra.lab.emc.com":
RT-DO105

PowerStore Manager

Connection and limiting discovery parameters for current PowerStore Manager.

PowerStore Manager Address
10.230.24.94

IP address or Fully Qualified Domain Name (FQDN).

Preferred Remote PowerStore Manager IPs Allowed list
10.230.24.136

Enter comma separated remote PowerStore management IPs if you want to filter discovered arrays. (Optional)

Volume Name Prefixes Blocked list

Enter disallowed comma separated volume name prefixes if you want to filter discovered volumes/groups. (Optional)

Volume Name Prefixes Allowed list
sra-

Enter allowed comma separated volume name prefixes if you want to filter discovered volumes/groups. (Optional)

Username
admin

Enter username for PowerStore Manager.

Password
.....

Enter password for PowerStore Manager.

CANCEL
BACK
NEXT

Specify the local array manager

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

Remote array manager

☐ Do not create a remote array manager now.

Enter a name for the array manager on "vc1.sra.ple.lab.emc.com":

PowerStore Manager

Connection and limiting discovery parameters for current PowerStore Manager.

PowerStore Manager Address

IP address or Fully Qualified Domain Name (FQDN).

Preferred Remote PowerStore Manager IPs Allowed list

Enter comma separated remote PowerStore management IPs if you want to filter discovered arrays. (Optional)

Volume Name Prefixes Blocked list

Enter disallowed comma separated volume name prefixes if you want to filter discovered volumes/groups. (Optional)

Volume Name Prefixes Allowed list

Enter allowed comma separated volume name prefixes if you want to filter discovered volumes/groups. (Optional)

Username

Enter username for PowerStore Manager.

Password

Enter password for PowerStore Manager.

CANCEL
BACK
NEXT

Specify the remote array manager

Advanced Configuration

The following table shows the advanced configuration parameters for PowerStore:

Section	Parameter	Default Value	Description
client	connection_timeout	20 seconds	The <code>connection_timeout</code> parameter determines how long SRA attempts to connect before a timeout error occurs. In addition, the parameter determines how long SRA waits before making another attempt if the connection is interrupted. This parameter is measured in seconds. You can adjust this parameter according to your network configuration.
	connection_attempts	3 attempts	The <code>max_attempts</code> parameter determines the maximum number of attempts SRA performs if the connection times out.

Section	Parameter	Default Value	Description
			You can adjust this parameter according to your network configuration.
polling	<code>poll_delay</code>	3 seconds	The <code>poll_delay</code> parameter determines how long SRA waits until a job or a replication session becomes the expected state. This parameter is measured in seconds.
	<code>poll_attempts</code>	10 attempts	The <code>poll_attempts</code> parameter determines the maximum number of attempts SRA performs if a replication session does not achieve the expected state.
ssl	<code>verify</code>	False	The <code>verify</code> parameter determines whether SRA validates a server SSL certificate. If the parameter set to <code>True</code> , SRA performs the validation. If the parameter is set to <code>False</code> , SRA does not perform the validation. NOTE: You must adjust this parameter if you want a secure connection.
	<code>ca_path</code>	N/A	The <code>ca_path</code> parameter specifies a path to a root certificate. If <code>verify</code> is enabled and you are using a self-signed certificate, you should export the root certificate from the storage host, place it beside the downloaded config file and set <code>ca_path</code> to the certificate name if you are using the Linux version. For the Windows version of the SRA, do not set the <code>ca_path</code> parameter. You must import the certificate

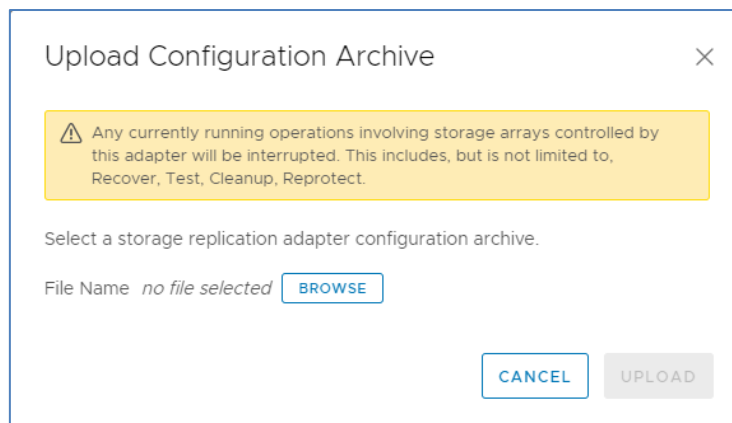
Section	Parameter	Default Value	Description
			through the Windows Trust Store. NOTE: You must adjust this parameter if you want a secure connection.
	protocols	tls1.2	The protocols parameter specifies a list of SSL protocols that SRA can use. SRA uses the first protocol in which a connection succeeded, from first to last through the list. You can use TLS1.2 and TLS1.1, although TLS1.1 is deprecated. Setting the value to TLSv1.0 means 1.0, 1.1, and 1.2 are all supported. However, you can enable TLS1.1 by changing settings in the <code>config.ini</code> file if you need to allow traffic through TLS1.1. Enabling TLS1.1 might be helpful if you are migrating data from older systems.
ssl:tls.1.2	ciphers	AESGCM:-aNULL:-DH:-kRSA:@STRENGTH	For each protocol, you can set a cipher list consisting of one or more OpenSSL cipher strings separated by colons. It specifies in the cipher's parameter in each protocol section. CAUTION: Adjusting these parameters without consulting Dell technical support is not recommended.
ssl:tls1.1			

Configuring SRA parameters:

1. In the SRM Appliance Management dialog box, select **Storage Replication Adapters**.
2. From the Dell PowerStore Storage Replication Adapter menu, select **Download configuration archive**.

The archive file contains the following files:

- `sra.configuration.version`
 - `config.ini`
3. Modify the configuration parameters in the `config.ini` file.
 4. From the Dell PowerStore Storage Replication Adaptor menu, select **Upload Configuration Archive**.



Upload Configuration Archive dialog box

5. Click **Browse** and navigate to the original archive location.
6. Click **Open**; the Success window appears, confirming a successful upload.

Resetting the SRA Configuration to the Factory Defaults

1. In the SRM Appliance Management dialog box, select **Storage Replication Adapters**.
2. From the Dell PowerStore Storage Replication Adaptor menu, select **Reset configuration**.

The Reset Adapter Configuration dialog box opens.

3. Click **Reset**; the Success window appears, confirming a successful reset.

Uninstalling the Dell PowerStore Storage Replication Adapter for Linux

1. In the SRM Appliance Management dialog box, select **Storage Replication Adapters**.
2. Locate the relevant SRA, and from the Dell PowerStore Storage Replication Adaptor menu, select **Delete**.

The Delete Adapter dialog box appears.

3. Select the checkboxes and click **DELETE**; the selected SRA is uninstalled.

Upgrading the Dell PowerStore Storage Replication Adapters

To upgrade the SRA, follow the instructions for installing the SRA (“[Downloading, Installing, Updating and Uninstalling Dell PowerStore SRA for Linux](#)”). The newer version is installed. Deletion of the old SRA is done through the web interface.

Getting Help

As part of an improvement effort, revisions of the software and hardware are periodically released. Some functions that are described in this document are not supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features. Contact your technical support professional if a product does not function properly or does not function as described in this document.

Where to get help

Support, product, and licensing information can be obtained as follows:

- Product information

For product and feature documentation or release notes, go to the product documentation page at <https://dell.com/support>.

- Troubleshooting

For information about products, software updates, licensing, and service, go to <https://dell.com/support> and locate the appropriate product support page.

- Technical support

For technical support and service requests, go <https://dell.com/support> and locate the Service Requests page. To open a service request, you must have a valid support agreement. Contact your Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

Copyright © 2023 Dell Inc. or its subsidiaries. All rights reserved. Published in the USA.

Published July 24, 2023.

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. Dell makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any Dell software described in this publication requires an applicable software license.

Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to Dell Online Support (<https://dell.com/support>).