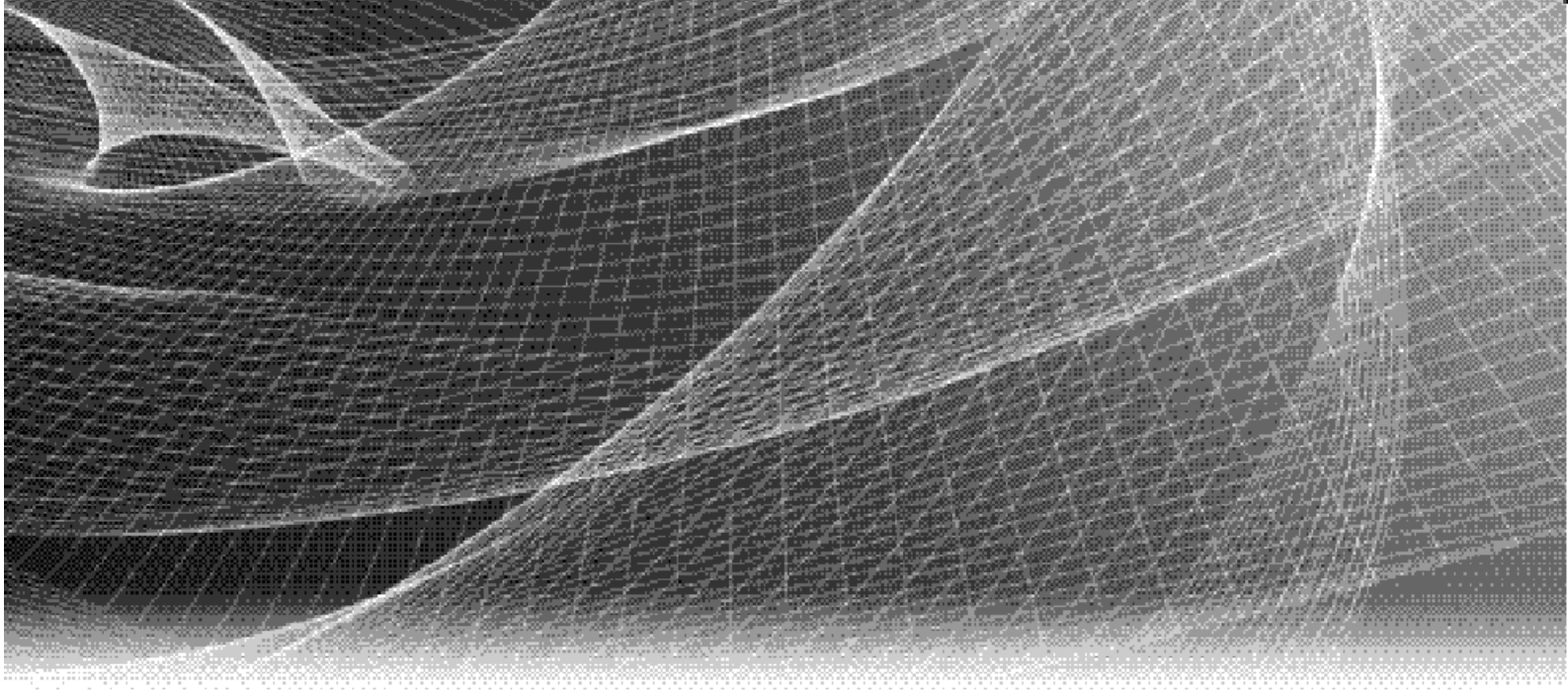

Secure Remote Services

Release 3.40

Technical Description

REV 01

Published October 2019

CONTENTS

PREFACE

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document.

Note: EMC Secure Remote Services (ESRS) is being rebranded to Secure Remote Services (SRS). This document was accurate at publication time. Go to Dell EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

This document provides a technical overview of Secure Remote Services (SRS).

Audience

This document is intended to provide information to network and storage administrators who are planning, installing, and administering Secure Remote Services at the customer site.

Related documentation

The following Dell EMC publications provide additional information:

- *Secure Remote Services Release Notes*
- *Secure Remote Services Site Planning Guide*
- *Secure Remote Services Pre-Site Checklist*
- *Secure Remote Services Port Requirements*
- *Secure Remote Services Installation Guide*
- *Secure Remote Services Operations Guide*
- *Secure Remote Services Policy Manager Release Notes*
- *Secure Remote Services Policy Manager Operations Guide*

Typographical conventions

Dell EMC uses the following type style conventions in this document:

Bold	Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Use for full titles of publications referenced in text and for variables in body text.
`Monospace`	Use for: • System output, such as an error message or script • System code • Pathnames, file names, prompts, and syntax • Commands and options
`Monospace italic`	Use for variables.
`Monospace bold`	Use for user input.
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

Dell EMC support, product, and licensing information can be obtained as follows:

Product information — For documentation, release notes, software updates, or information about Dell EMC products, go to Dell EMC Online Support at:

https://support.emc.com

Technical support — Go to Dell EMC Online Support and click Service Center. You will see several options for contacting Dell EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your Dell EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to:

techpubcomments@emc.com

CHAPTER 1
Secure Remote Services

This Secure Remote Services technical description contains information about the following topics:

Introduction

Dell EMC maintains a strong commitment to protecting your information infrastructure through the 24x7 availability of remote technical support resources and automated secure remote services solutions. Secure Remote Services (SRS) 3.40 delivers a secure, IP-based, distributed remote service support solution that provides command, control, and visibility of remote services access.

SRS Release 3.40 is the virtual edition of SRS, which expands and improves the Secure Remote Services portfolio with the following features:

Consolidation — SRS consolidates access points for Dell EMC support by providing a uniform, standards-based architecture for remote access across Dell EMC product lines. The benefits include reduced costs through the elimination of modems and phone lines, controlled authorization of access for remote services events, and consolidated logging of remote access for audit review.

Security — SRS fulfills requirements for authentication, authorization and auditing with the use of Policy Manager in a secure, highly scalable, fault-tolerant solution. This IP-based, firewall-friendly remote access architecture initiates all connections from your site. SRS security features include:

Comprehensive digital security — SRS security includes Transport Layer Security (TLS) data encryption, TLS v1.2 tunneling with Advanced Encryption Standard (AES) 256-bit data encryption SHA-2, entity authentication (private digital certificates), and remote access user authentication verified through Dell EMC network security.

Authorization controls — Policy controls enable customized authorization to accept, deny, or require dynamic approval for connections to your Dell EMC device infrastructure at the support application and device level, with the use of Policy Manager.

Secure remote access session tunnels — SRS establishes remote sessions using secure IP and application port assignment between source and target endpoints.

Licensing Usage Data Transfer — SRS Version 3 (SRSv3) REST APIs support transfer of licensing usage data to Dell EMC, from Dell EMC Products. Such Products must be managed by SRSv3, and be Usage Intelligence enabled in order to send usage data. Dell EMC processes usage data and provides Usage Intelligence reports, visible to Customers and Dell EMC, to better track product usage, and manage compliance.

Automatic Software Updates — SRSv3 automatically checks for software updates, and notifies users via email as they become available. In addition, the SRS Web UI Dashboard displays the latest available updates when it becomes available. Users can apply updates as they choose from the SRSv3 Web UI.

Managed File Transfer (MFT) — MFT is a bidirectional file transfer mechanism that is provided as part of SRSv3. You can use MFT to send or receive large files, such as log files, microcode, firmware, scripts, or large installation files) between the product and Dell EMC. A distribution "locker" is used for bi-direction file staging.

Note: The SRSv3 does not support installing software not already included in the appliance. While the customer has full access to the appliance, loading additional software or updating software already installed may require redeployment.

Description

This section provides a detailed description of SRS.

Remote services benefits

The Dell EMC remote services strategy delivers immediate, secure response to product event reports such as error alerts, which can greatly increase the availability of your information infrastructure. When a support event occurs, Dell EMC provides rapid remote services through two phases: first, through automated recognition and notification from your site to Dell EMC (or recognition by Dell EMC, in the case of connectivity loss), and second, through interpretation and response from Dell EMC. In many cases this support can eliminate the need for an on-site support visit.

Dell EMC's immediate and interactive remote services provides:

- Improved service levels
- Increased protection of information
- Simplification of complex environments
- Reduced risk
- Improved time-to-repair

Solution security

SRS design acknowledges that the heart of any well-designed distributed system is security, and thus it incorporates the industry-recognized "3 A's": authentication, authorization, and audit logging. SRS employs multiple security layers to ensure that you and Dell EMC can use the system with confidence.

From an applications architecture perspective, SRS is an asynchronous messaging system in which all communications are initiated from your site. All communications between SRS at your site and the Dell EMC Enterprise servers use the HTTPS protocol with end-to-end TLS tunneling with strong encryption.

SRS uses a firewall-friendly, IP-based communication technology over TLS VPN tunnels. Customer-controlled SRS server(s) negotiate the secure exchange of information between Dell EMC devices behind your internal firewall and the Dell EMC Customer Support Center. All communication between your site and Dell EMC is initiated by an SRS server at your site. Using industry standard Transport Layer Security (TLS) encryption over the Internet, and Dell EMC-signed digital certificate authentication, your administrators need only enable outbound communication over TLS default ports 443 and 8443.

IMPORTANT

Port 8443 is not required for functionality, however without this port being opened, there will be a significant decrease in remote services performance, which will directly impact time to resolve issues on the end devices.

SRS is designed to be scalable and fault-tolerant, and to provide you with the authentication, authorization, and audit logging control you require to meet your security needs and to support your environment. SRS remote access to your Dell EMC devices is secured using a session-based IP port-mapping solution. Service notification file transfers from the managed devices are brokered through the SRS server to ensure secure encryption and audit logging.

SRS comprises a suite of software products that securely link your Dell EMC devices to the Dell EMC Global Services support application systems. This distributed system provides you with the commands and controls to authorize and log Dell EMC support actions such as remote access connections, file transfers, diagnostic script executions, and system updates.

The following security features are used in SRS:

- RSA SecurID 2 Factor Authentication of digital certificate request
- Dell EMC-issued RSA SecurID Authenticators for digital certificate registration
- Programatically X.509 digital certificates generation and installation
- SRS authentication based on digital certificate at Dell EMC
- Secure remote application path using IP and port-mapping
- Dynamic device-level customer authorization control using a Policy Manager (PM)
- Logging of Dell EMC-requested actions at the customer site
- All access restricted to authenticated and authorized Dell EMC personnel
- Dell EMC-issued RSA SecurID authentication for all users (required for access to the SRS ServiceLink application and use)

Licensing Usage Data

Dell EMC Products can now send licensing usage data to Dell EMC over a secure channel by calling SRSv3 REST APIs. Dell EMC stores this data for monitoring and reporting across all supported Dell EMC Products at all customer locations.

SRSv3 Updates

SRSv3 automatically detects availability of updates and notifies users via SRS Web UI and email when any new SRSv3 update is available.

SRS Control

You control all Dell EMC remote services access to the SRS-managed products through the SRS server/client and its associated Policy Manager software. Connections with Dell EMC devices and Dell EMC at the SRS-managed site originate from, and are managed, by SRS (or SRS embedded device clients) and the Policy Manager.

You set the policies of the Policy Manager, which controls SRS remote access for support events. The Policy Manager can be set to accept, ask for approval of, or deny remote services connection requests.

Note: The PM is optional but is strongly recommended. The PM is required to provide authentication, authorization, and audit logging.

At Dell EMC, a distributed Dell EMC Enterprise suite is the processing core of SRS. The Dell EMC Enterprise provides the mechanism for remote access activities from Dell EMC Global Services.

Architecture

The SRS application architecture is a secure, asynchronous messaging system designed to support the functions of secure encrypted file transfer, monitoring of device status, and remote execution of diagnostic activities. This distributed solution is designed to provide a scalable, fault-tolerant, and minimally intrusive extension to your system support environment. Figure 1 on page 11 illustrates the processing components and their interconnections.

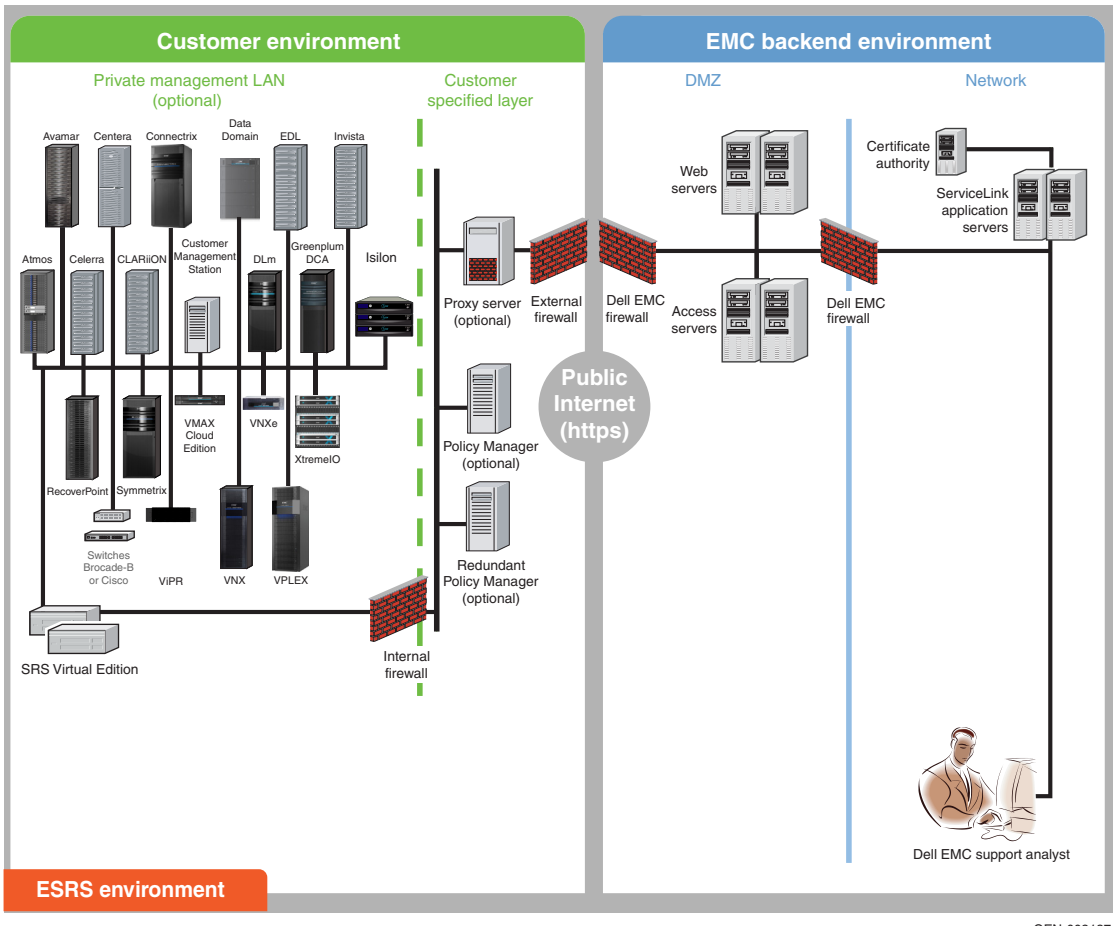

Figure 1 Secure Remote Services (SRS) architecture

Customer site components

This section describes the SRS components at the customer site: SRSv3, which can be SRS Virtual Edition (SRS VE) or SRS Docker Edition (SRS DE), and Policy Manager.

SRS VE

SRS software component can be installed on a customer-supplied VMware ESX or Microsoft Hyper-V instance. It can also be installed on multiple virtual infrastructure servers (two or more servers are preferred for high availability (HA). The servers act as the single point of entry and exit for all IP-based remote services activities and most Dell EMC connect home notifications. Note that in an HA configuration, the server(s) monitors the same devices but do not communicate with each other.

SRS functions as communications brokers between the managed devices, the Policy Manager, and the Dell EMC Enterprise. All communication with Dell EMC initiates from SRS on port 443 or 8443 outbound. The SRS servers are HTTP handlers. All messages are encoded using standard XML and SOAP application protocols. SRS message types include:

- Device state heartbeat polling
- Data file transfer (connect homes)
- Licensing Usage Data transfer (using MFT RESTful Webservices)
- User authentication requests
- Device management synchronization

Each SRS server acts as a proxy, carrying information to and from managed devices. SRS can also queue Connect Home events in the event of a temporary local network failure. The SRS servers have their own Web UI, which is run on the underlying OpenSUSE operating system (runs as Linux Service). All SRS actions are logged to a local runtime and audit files.

SRS polls the Policy Manager, receives the current policies, and caches them locally. During the periodic poll, SRS posts all requests and actions that have occurred. These are written to the Policy Manager database and the Policy Manager audit log files.

SRS DE

SRS can be installed on a Linux host using the Docker Engine. Before installing SRS on a Linux host, the following must already be installed:

- Docker supported Linux distribution (x64 bit)
- Docker Engine (Docker runtime)

Using the binary installer, SRS can be installed on the Linux distributions that support Docker. For a list of Linux distributions that are supported by Docker and for Docker installation instructions, refer to the following address:

https://docs.docker.com/engine/installation

For SRS installation instructions on a Linux host, refer to the Secure Remote Services Installation Guide.

Policy Manager

(Optional: Required for Access Control and Auditing) The Policy Manager enables you to set permissions for devices being managed by SRS. When the SRS server retrieves a remote access request from the Dell EMC Enterprise, the access is controlled by the policies configured on the Policy Manager and are enforced by the SRS server.

The Policy Manager software may be on a standalone server (preferred method) or on another application server, provided there are no software, ports, or resource conflicts.

Note: Policy Manager cannot be colocated on the SRS Version 3 (SRSv3) host server.

Note: Proxy server: Network traffic can be configured to route from the SRS server through proxy servers to the Internet. SRS supports basic authentication for HTTP and SOCKS proxy servers, with or without credentials based on the proxy setup.

Application installation

Customers can download and install SRSv3 software using their Dell EMC Single Sign On account. You will need to download an OVF/VHD template, which is used when importing the SRSv3 into the virtual infrastructure. The template is available for download from the Dell EMC Online Support Site (support.emc.com).

Note: SRS download, installation, and provisioning can be done by the customer, Dell EMC personnel, and partners.

Deployment and configuration

SRSv3 provides a Web UI that is used for:

- Initial configuration of SRSv3
- Upgrades
- Configuring and monitoring SRSv3 features and services
- Adding/removing of devices
- SRSv3 Logs review

Security enhancements

SRS provides the enhanced security practices and encryption technologies, including:

- Certificate protected by RSA Lockbox Technology
- Advanced Encryption Standard (AES), SHA-2, 256-bit encryption between the SRSv3 and Dell EMC
- Bilateral certificate authentication for all communication between the Client and Dell EMC
- Configurable security between SRS components
- Customer Multifactor Authentication during SRSv3 Provisioning

Specifications

For specifications for SRS VE and SRS DE, see the Secure Remote Services Installation Guide.

Table 1 on page 14 shows the minimum configuration of the required hardware and the application software for the Policy Manager that Dell EMC provides.

Table 1 **Policy Manager specifications**

Type	Requirements	Dell EMC provided software	Notes
Policy Manager server (optional)	**Processor** — One or more processors, each 2.1 GHz or better. **Free memory** — Random Access Memory (RAM) required: • Minimum 2 GB of RAM for 32-bit operating systems; 3 GB of RAM preferred • Minimum 4 GB of RAM for 64-bit operating systems **Note:** Policy Manager collocated on the SRSv3 is not supported. **Network Interface Cards (NIC)** — One 10/100 Ethernet adapter (NIC card) is recommended (1 GB preferred). You may choose to use a second NIC card for data backups. **Free Disk Space** — Minimum 2 GB available (preferably on a storage device of 80GB or larger) **Microsoft .NET Framework** Version 2.0 with SP1 (minimum) or Microsoft .NET Framework 3.5 is required if you are using the Customer Environment Check Tool (CECT) to validate that the PM server is setup correctly to install the PM software. NOTE: Microsoft.NET Framework 4.0 is not compatible at this time. **Operating Systems** — any of the following (U.S. English only): • Windows XP, SP2 or later (deprecated) • Windows Vista • Windows 7 • Windows 8 • Windows Server 2003 R1, 32-bit or 64-bit, SP1, SP2 or SP3 (to be deprecated) • Windows Server 2003 R2, 32-bit or 64-bit, SP1, SP2 or SP3 (to be • deprecated) • Windows Server 2008 R1, 6.0, 32-bit or 64-bit, SP1 or SP2 • Windows Server 2008 R2, 6.1, 64-bit only, SP1 or SP2 • Windows 2016 • Supported Japanese OS (Windows 2008 R1 and R2) with English language pack • Windows Server 2012 R1 Foundation 64-bit (GUI mode only) • Windows Server 2012 R1 Standard 64-bit (GUI mode only) • Red Hat 6.4 (32-bit and 64-bit) • Red Hat Enterprise Linux (RHEL) 7.5 • CentOS 6.4 (32-bit and 64-bit) • SUSE Linux Enterprise 11 SP3 (64-bit) **Note:** Policy Manager version 2.02.1-xxx software is currently only available for the Microsoft operating systems listed above. Policy Manager versions 6.6 and 6.8 are available for all of the operating systems listed above, for both 32- and 64-bit versions.	Policy Manager	A Policy Manager is optional, but highly recommended. Policy Manager requires a site-supplied server. Policy Manager supports up to three SRS servers or pairs. One Policy Manager server can support up to 750 devices. **Note:** Support for Policy Manager on Windows XP and Windows Server 2003 will be deprecated in the near future due to declaration of End of Life/End of Service Life by Microsoft.

Communication to Dell EMC

All communication between the customer's site and Dell EMC is initiated outbound from the customer's site by SRS. Using industry-standard Transport Layer Security (TLS) encryption over the Internet and Dell EMC-signed digital certificate authentication, SRS creates a secure communication tunnel.

SRS use industry-accepted bilateral authentication for the Dell EMC servers and the SRSv3. Each SRSv3 server has a unique digital certificate, which is programatically generated and installed during the SRSv3 installation and activation, and is verified by Dell EMC whenever the SRSv3 makes a connection attempt. The SRSv3 then verifies Dell EMC's server certificate. Only when the mutual TLS authentication passes does the SRSv3 transmit messages to Dell EMC, securing the connection against spoofing and man-in-the-middle attacks.

The SRS server uses the TLS tunnel to Dell EMC to perform the following functions:

- Heartbeat polling
- Remote notification
- Remote access

Each function relies on the TLS tunnel. However, communication processes and protocols within the tunnel vary by function. Each function is described in the following sections.

Heartbeat polling

Heartbeat polling is described in the following sections:

- Heartbeat to Dell EMC by the SRSv3
- Heartbeat to Dell EMC devices managed by the SRSv3

Heartbeat to Dell EMC by the SRSv3

The Heartbeat is a regular communication, at a default interval of 30 seconds, from the SRSv3 to the Dell EMC Enterprise. Each heartbeat contains a small amount of data that identifies the SRS server and provides the Dell EMC Support Center with Connectivity status information on the Dell EMC devices and the SRS server. The heartbeat can also be used for transporting Device Connect-home files to Dell EMC.

Note: This is a non-persistent connection and is established for each heartbeat to Dell EMC.

Dell EMC servers receive the data in XML format and acknowledge the receipt of data using SOAP (Simple Object Access Protocol) commands. The SRSv3 terminates the connection once it receives the acknowledgment response.

Figure 2 on page 16 provides an illustration of the heartbeat communication paths.

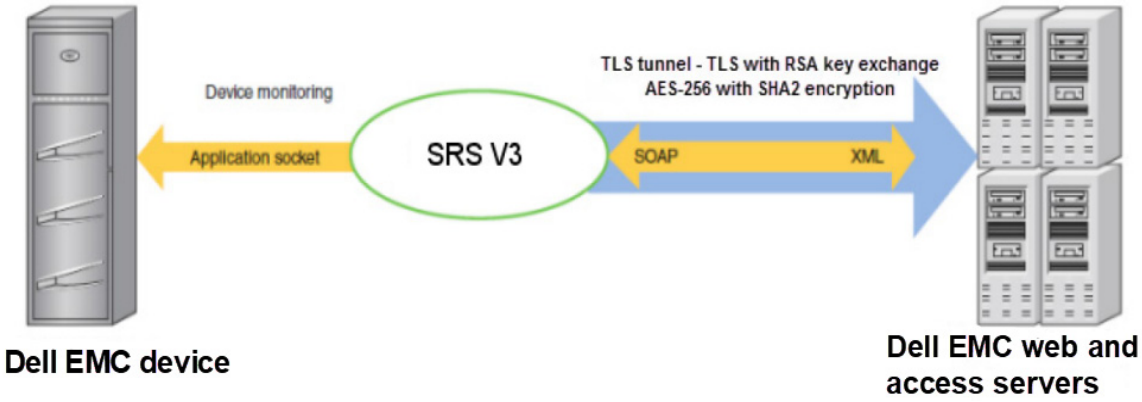

Figure 2 Heartbeat communication

Connectivity checking to Dell EMC devices managed by the SRSv3

SRSv3 regularly checks each managed device for responsiveness on the primary support applications ports (for details, see the Secure Remote Services Port Requirements document). The information is recorded by the SRSv3. If a change in status is detected, then the SRSv3 notifies Dell EMC using the next heartbeat. The status can be verified in the Dell EMC infrastructure, and is fed into the customers' GUI, as well as into support.emc.com -> MyService360.

Remote notification (Connect Home)

The SRSv3 serves as a conduit for Dell EMC products to send remote notification event files to Dell EMC. Dell EMC hardware platforms use remote notification for several purposes. Errors, warning conditions, health reports, configuration data, and script execution statuses may be sent to Dell EMC. Figure 3 on page 17 provides an illustration of the remote notification communication paths.

When an alert condition occurs, the Dell EMC device generates an event message file. this file is sent by ConnectEMC to the SRSv3, where it is received by one of the following local listener services:

- HTTPS
- SMTP (e-mail)
- SRS REST Client
- Passive FTP

When an event file is received, the SRSv3 compresses the file, opens the TLS tunnel to the Dell EMC Enterprise, posts the data file to Dell EMC ServiceLink, and deletes the file(s) from the SRS listener directory. At Dell EMC, the file is decompressed and forwarded to the Customer Relationship Management (CRM) systems.

Transport from the SRSv3 to Dell EMC can be done through either REST (primary protocol for SRS 3.24 and up) or SRS heartbeat (primary protocol for SRS versions prior to 3.24 and failover protocol for SRS 3.24 and up). SRSv3 can also be configured to use failover channels FTPS or encrypted e-mail (using Customer E-mail server) if the primary is unavailable. This might require additional Network and/or Mail Server configuration.

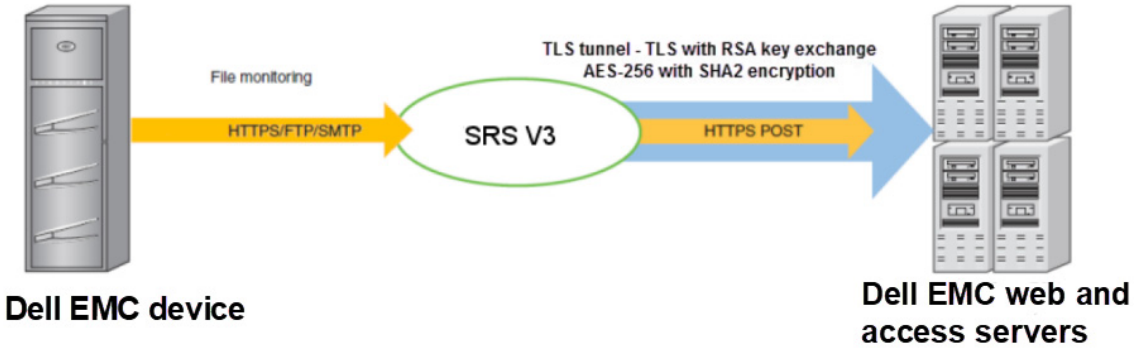

Figure 3 Remote notification communication

Remote access

To establish an Dell EMC Global Services remote access session, SRS uses asynchronous messaging to ensure that all communication is initiated from the customer's site.

After being properly authenticated at Dell EMC, a Dell EMC Global Services professional makes a request to access a managed device. The remote access session request includes a unique identifier for the user, the serial number of the managed device, the name of the remote application to be run on the managed device, and the service request number if available. The remote access request is queued at Dell EMC until an SRSv3 that manages the device in question sends a heartbeat to Dell EMC and retrieves the work request.

In response to the Heartbeat XML message, the Dell EMC Enterprise sends a special status in the SOAP response. This response contains the request information as well as the address of the Global Access Server and a unique session ID that the SRSv3 would use to connect. The SRSv3 uses its local repository to determine the local IP address of the managed device. It then checks with the cached policy from Policy Manager to see if the connection is permitted. If there is no cached policy, then the SRSv3 checks with the Policy Manager. If the connection is permitted, then the SRSv3 establishes a separate persistent TLS connection to the Global Access Server of the preferred port 8443 for the specific remote access session.

This secure session enables IP traffic from the Dell EMC Global Services professional to be routed through the SRSv3 to the managed device. IP socket traffic received by the Global Access Server for this session is established, wrapped in a message, and sent to the SRSv3. The SRS unwraps the SOAP object and forwards the traffic to the IP address and port of the end device for which the session was established. SOAP communication flows between the SRSv3 and the Global Access Server through this tunnel until it is terminated or times out after a period of inactivity. Figure 4 on page 18 provides an illustration of the remote access communication paths.

As the result of an application remote access session request, the SRSv3 forwards traffic to the specific ports at the IP address that is associated with the registered serial number of the device at time of deployment.

If a Policy Manager is configured, then these actions and requests are sent to the Policy Manager as audits, which are viewable in the Policy Manager WebUI on the Audit tab and in the flat text Policy Manager audit logs.

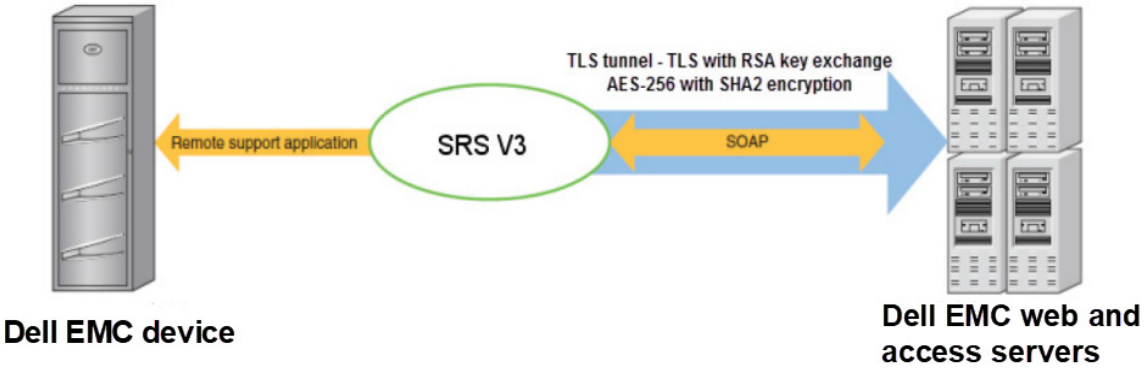

Figure 4 Remote access communication

Product use of SRS

Table 2 on page 18 shows the products that use the remote notification and remote access features of SRS.

Table 2 **Product use of SRS (page 1 of 3)**

Product	Dell EMC remote access to device through SRS	Remote notification to Dell EMC through SRS
AppSync	Yes	Yes
Atmos®	Yes	Yes
Avamar®	Yes	Yes
Celerra®	Yes	Yes
Centera®	Yes	Yes
CLARiiON®	Yes	Yes
CloudArray	Yes	Yes
CloudBoostAppliance	Yes	Yes
CloudIQ-CLTR	Yes	Yes
Connectrix	Yes	Yes
Customer Management Station	Yes	Device does not send Connect Homes through the SRS
Data Domain®	Yes	Yes
DCA	Yes	Yes
DellEMCSymphony	Yes	Yes
DL3D	Yes	Device does not send Connect Homes through the SRS
DLm	Yes	Yes
DPAppliance	Yes	Yes
Data Protection Advisor (DPA)	Yes	Yes

Table 2 **Product use of SRS (page 2 of 3)**

Product	Dell EMC remote access to device through SRS	Remote notification to Dell EMC through SRS
DPC CloudBoost	Yes	Yes
DSSD	Yes	Yes
Elastic Cloud Storage (ECS)	Yes	Yes
EDL	Yes	Yes
Embedded NAS (eNAS)	Yes	Device does not send Connect Homes through the SRS
Enterprise Copy Data Management (eCDM)	Yes	Yes
Greenplum® Data Computing Appliance (DCA)	Yes	Yes
Integrated Data Protection Appliance (IDPA)	Yes	Yes
Insight360	Yes	Yes
Invista®	Yes	Yes
Isilon®	Yes	Yes
NetWorker	Yes	Remote notification but no remote access on NetWorker.
PowerPath®	Yes	Device does not send Connect Homes through the SRS
PowerProtectAppliance	Yes	Yes
PowerProtectDataManager	Yes	Yes
RecoverPoint	Yes	Yes
ScaleIO	Yes	Yes
SRM	Yes	Yes
Switch-Brocade-B	Yes	Yes[1]
Switch-Cisco	Yes	Yes[2]
UCC	Yes	Yes
Unity/ UnityVSA™	Yes	Yes
VCE Vision™	Yes	Yes
ViPR®	Yes	Yes
ViPR SRM®	Yes	Yes
VMAX[3]	Yes	Yes
VNX®	Yes	Yes
VNXe®	Yes	Yes
VPLEX®	Yes	Yes

Table 2 **Product use of SRS (page 3 of 3)**

Product	Dell EMC remote access to device through SRS	Remote notification to Dell EMC through SRS
VxFlex OS	Yes	Yes
VxRack Flex	Yes	Yes
VxRack SDDC	Yes	Yes
VxRail (VSPEX BLUE®)	Yes	Yes
XtremIO®	Yes	Yes

1. By Connectrix Manager, Connectrix Manager Data Center Edition, or Connectrix Manager Converged Network Edition.
2. By Fabric Manager or Cisco Data Center Network Manager.

Configuration

This section provides details on the configurations of SRSv3.

Server Client configuration

SRSv3 servers can be implemented in one of several configurations to meet your network and security requirements. See Figure 1 on page 11 for a sample configuration.

Dell EMC recommends that the operating systems of your Policy Manager servers be hardened before installing the Policy Manager software. The preparation and hardening of servers is the customer's responsibility.

There are no technical restrictions on the network location of the SRSv3 server. It must connect to your devices, to Policy Manager, and to the Dell EMC Enterprise. Dell EMC strongly recommends that you use a firewall to block network ports not required by SRSv3.

High Availability SRS Cluster configuration

To enable maximum remote access availability, Dell EMC recommends deployment of a High Availability SRS Cluster server configuration to eliminate single point of failure. An SRS Cluster refers to the relationship created on the Dell EMC SRS infrastructure between two or more SRS servers.

Synchronization of SRS clusters

SRS server device management is synchronized by the Dell EMC Enterprise servers during polling cycles so that changes to the configuration on one SRSv3 in the cluster are automatically propagated to the other(s). When there is an addition, removal, or edit of a device on the managed devices list for any SRSv3 in a High Availability Cluster configuration, the Dell EMC Enterprise sends a synchronization message to all clustered SRS servers.

When the other SRSv3(s) in the cluster receives the device management transaction information, it updates its list of managed devices. If that SRS server is not currently available during a synchronization attempt, the Dell EMC Enterprise queues the transaction. Synchronization of the SRS Cluster occurs upon the next successful poll message received from the previously unavailable SRSv3.

Installing a High Availability SRS Cluster

To implement a High Availability Cluster configuration, your Dell EMC Global Services professional will create the cluster relationship from within the Dell EMC infrastructure.

When a cluster is created, a cluster name must be assigned. The default name is the organization name followed by "HA." Other names can be assigned, but no two clusters can have the same name.

The High Availability Cluster will take on the devices managed by the *first* SRSv3 enrolled into the cluster. When additional SRSv3(s) are added to the cluster, they will begin managing the cluster's devices.

Note: The first SRSv3 used to create a High Availability Cluster may have managed devices. Any additional SRSv3 enrolled in a High Availability Cluster must not be managing devices at the time of enrollment. An error message will result if the additional SRSv3 are managing devices.

Web UI Configuration

For information on the Web UI configuration, see the Web UI configuration sections for Device Management and Policy Manager in the *Secure Remote Services Operations Guide*.

Security features

This section details the security features of SRSv3.

Policy Manager

Using the Policy Manager, you control the authorization requirements for remote access connections, diagnostic script executions, and other SRS-related activities. The Policy Manager enables you to set access permissions for devices being managed by SRS. The SRSv3 regularly polls Policy Manager for changes to the permissions and caches the permissions locally. All requests and actions are recorded in the Policy Manager database and local audit log files. When a request for remote access or any other action arrives at the SRSv3, it enforces the policy received from the Policy Manager even if the Policy Manager is unavailable.

Policy Manager permissions can be assigned in a hierarchical system, establishing policies based on model and product groups.

More information on Policy Manager functions, configuration, control, and audit logging can be found in the SRS Policy Manager Operations Guide.

When you set an authorization rule to Ask for Approval, the Policy Manager sends an e-mail message to your designated address upon each action request, per transaction. This e-mail message contains the action request itself and the user ID of the Dell EMC Global Services representative.

The e-mail message requests your permission to perform the action. You use the Policy Manager interface to accept or deny the requested action. You also have the option of creating filters to set further restrictions on authorization and actions.

As with SRSv3 and Dell EMC Enterprise communication behavior, the Policy Manager only responds to requests from the SRS server. Since the Policy Manager's permission rules are cached at startup, the SRSv3 must poll the Policy Manager for configuration updates. In this way, any changes are captured to the Policy Manager rule set after its last polling cycle. The Policy Manager is an HTTPS listener, which must be configured to receive messages on an agreed-upon port. The default port is 8443, but if necessary, you can specify a different port during your Policy Manager installation.

The Policy Manager uses the Apache Tomcat engine and a 100 percent compliant local JDBC relational database to provide a secure web-based user interface for permission management.

Logging

The Policy Manager records all remote services events, remote access connections, diagnostic script executions, and support file transfer operations and stores them in the Policy Manager database and flat text audit log files. The Policy Manager also audits access to the Policy Manager, policy changes, and all authorization or denial of access activity. The audits are viewed through the Policy Manager interface and cannot be edited. The audits are also streamed to local flat text files which can be read with any text editor and are not tamper proof. Audit logs can also be configured to stream to a syslog server in your environment. See Figure 5 on page 23 for a Policy Manager interface example.

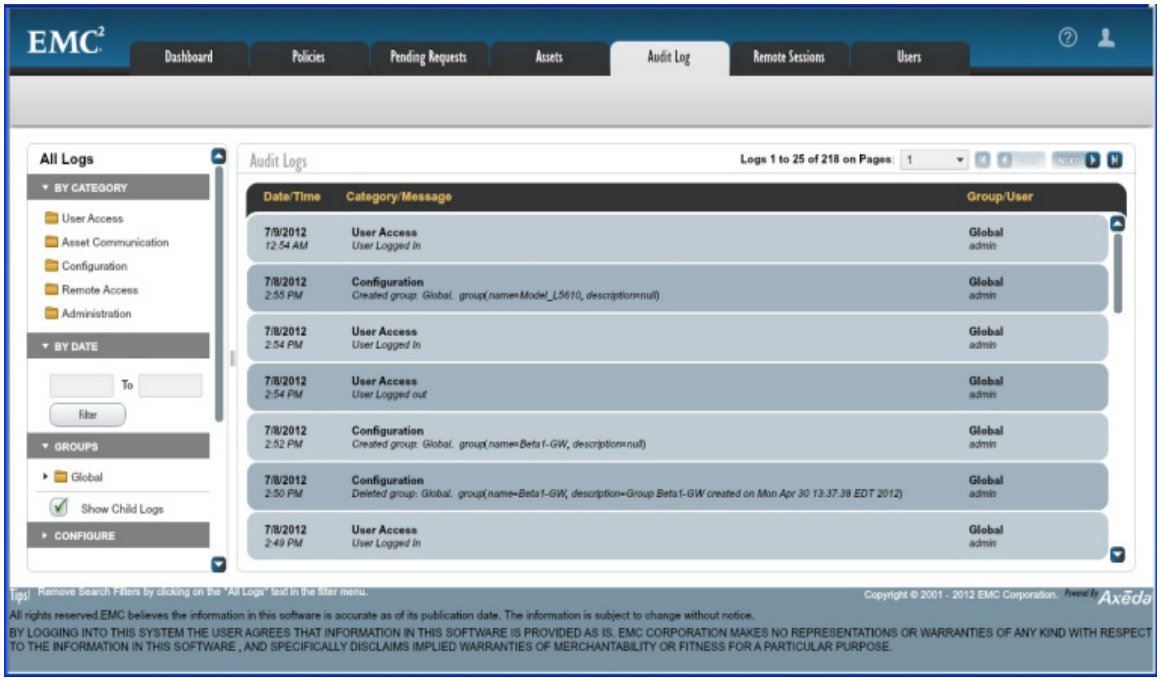

Figure 5 Audit log example

Device control

SRS Enterprise proactively monitors and notifies Dell EMC Global Services if the SRSv3 or any managed device fails to regularly communicate back to Dell EMC. Dell EMC alerts you of potential failures or issues that may affect Dell EMC's ability to provide timely support. As a Dell EMC customer, you have complete control over which devices are managed by your SRS solution. You can group them in by product line, network location, or any other criteria you desire. Dell EMC provides applications and tools to assist you with the addition of new devices for management by the SRSv3. All device management operations are logged and must be Approved on the Dell EMC enterprise by authorized Dell EMC Global Services professionals.

Digital Certificate Management

During the SRS installation, digital certificates are installed on the SRSv3. All certificate usage is protected by unique password encryption. Any message received by the SRSv3, whether pre- or post-registration, requires entity-validation authentication.

Digital Certificate Management automates SRS digital certificate enrollment by taking advantage of Dell EMC's existing network authentication systems, which use the RSA SecurID Authenticator and the Dell EMC's private certificate authority (CA). Working with Dell EMC systems and data sources, Digital Certificate Management aids in programmatically generating and authenticating each certificate request, as well as issuing and installing each certificate on the SRSv3.

The SRS Digital Certificate provides proof-of-identity for your SRSv3. This digital document binds the identity of the SRS server to a key pair that is used to encrypt and authenticate communication back to Dell EMC. Because of its role in creating these certificates, the Dell EMC Certificate Authority is the central repository for the Secure Remote Services key infrastructure.

Before the certificate authority issues a certificate for the SRSv3, it requires full authentication of a certificate requester by verifying that the Dell EMC Global Services professional making the request is properly authenticated using the Dell EMC RSA SecurID, and belongs to a Dell EMC Global Services group that is permitted to request a certificate for the customer site or by a customer with a valid Dell EMC support account. The certificate authority then verifies that the information contained in the certificate request is accurate and generates the Certificate and returns the certificate to the requestor. The process is as follows:

Once authentication is completed by the customer, Dell EMC personnel, or partner, the SRSv3 installation program gathers all the information required for requesting certificates and generates a certificate request, a private key, and a random password for the private key. The SRSv3 installation program then writes the certificate request information to a request file, ensuring accuracy and completeness of the information.

The installation program then submits the request over a TLS tunnel. After the certificate is issued and returned over the TLS tunnel the installation program automatically installs the certificate to the SRS server.

Note: Due to Dell EMC's use of RSA Lockbox technology, a certificate cannot be copied and used on another machine.

Device configuration access control caution

Once your devices are configured for SRS management, you must ensure that the configuration of the managed devices are carefully controlled and monitored. For example, changing the configured IP address of the SRSv3 will disable the storage device connect home capabilities; or changing the IP address of the storage device will disable Dell EMC's ability to perform remote service on that device. After changes to the SRSv3 or devices configuration are made, these changes MUST be reconfigured on the other affected portions of the Solution. Each device modification is tracked in the Policy Manager and the Dell EMC enterprise audit logs.

Note: For REST devices, you will need to read the product documentation on how to update the SRSv3 IP information.

Dell EMC Enterprise access control

Several robust security features are incorporated into the Dell EMC enterprise. To access the SRS Enterprise Solution, Dell EMC Global Services professionals or authorized service providers must log in using RSA SecurID two-factor authentication technology. Only authorized Dell EMC personnel or authorized service providers can access the Dell EMC's SRS Enterprise Solution.

Supported products

The products supported by SRS are listed in Table 3 on page 25.

Note: All of the following listed products are supported on the SRSv3. The code supported is **only** for the SRSv3.

Table 3 **Product and application releases supported by SRSv3 (page 1 of 2)**

Product	Environment/application releases	Minimum SRSv3 Code Supported
AppSync	Contact your Dell EMC representative	3.22
Atmos	Atmos 1.4 or later	3.02
Avamar	Avamar 6.0 or later	3.02
Celerra	NAS Code 5.4 or later	3.02
Centera	CentraStar® 2.4 or later [b]	3.02
CLARiiON CX, CX3, CX4, and AX4-5 Series storage systems (distributed or Enterprise environments)	FLARE® Operating Environment 2.19 or later Navisphere® Manager 6.19 or later The AX-100/AX-150 are not supported as they do not support the required CLARalert. **Note:** AX4-5 series are supported only if the Navisphere Full license (with CLARalert) is purchased and installed on the storage system.	3.02
CloudArray	Contact your Dell EMC representative	3.08
CloudBoost Appliance	Contact your Dell EMC representative	3.06
CloudIQ-CLTR	Contact your Dell EMC representative	3.30
Connectrix	Contact your Dell EMC representative	3.30
Customer Management Station	Contact your Dell EMC representative	2.24
Data Domain	DD OS version 4.8 or higher	3.02
Data Protection Advisor (DPA)	Contact your Dell EMC representative	3.04
DellEMCSymphony	Contact your Dell EMC representative	3.20
DCA	Contact your Dell EMC representative	3.30
DL3D	Contact your Dell EMC representative	2.02
Disk Library for mainframe (DLm), Gen2	DLm 4020, DLm 4080, release 1.2 and later	3.02
Disk Library for mainframe (DLm), Gen3	DLm 8000 3.4.0 & 3.4.1	3.02
	DLm 6000 All releases	3.02
	Dlm 2000 All releases	3.02
	Dlm 1000 3.5	3.02
Disk Library for mainframe (DLm), Gen4	DLm® 8100, DLm 2100 with VNX, DLm 2100 with DD	3.02
DPA	Contact your Dell EMC representative	3.02
DPAppliance	Contact your Dell EMC representative	3.18
DPC CloudBoost	Contact your Dell EMC representative	TBA
DSSD	Contact your Dell EMC representative	3.12
Disk Library (EDL)	• DL-5100 and 5200 series • DL-4000 series—DL-4100, DL-4106, DL-4200, DL-4206, DL-4400A/B, DL-4406A/B • DL-700 Series—DL-710, DL-720, DL-740 • DL-310 • DL3D 1500, 3000, 4000—Release 1.01 and later	3.02
Elastic Cloud Storage (ECS)	Contact your Dell EMC representative	3.02
Embedded NAS (eNAS)	Contact your Dell EMC representative	3.12

Table 3 **Product and application releases supported by SRSv3 (page 2 of 2)**

Product	Environment/application releases	Minimum SRSv3 Code Supported
Enterprise Copy Data Management (eCDM)	Contact your Dell EMC representative	3.12
Greenplum Data Computing Appliance (DCA)	Greenplum 4.0	3.02
Integrated Data Protection Appliance (IDPA)	Contact your Dell EMC representative	TBA
Insight360	Contact your Dell EMC representative	3.30
Invista	Invista 2.2 or later	3.02
Isilon	OneFS 7.1	3.02
NetWorker	Contact your Dell EMC representative	3.20
PowerPath	Contact your Dell EMC representative	3.08
PowerProtectAppliance	Contact your Dell EMC representative	3.34
PowerProtectDataManager	Contact your Dell EMC representative	3.36
RecoverPoint	RecoverPoint 3.1, 3.2, 3.3, 3.4 and later [a]	3.02
ScaleIO	Contact your Dell EMC representative	3.08
SRM	Contact your Dell EMC representative	3.32
Symmetrix Device Client	Enginuity 5670, 5671, 5771, 5772, 5773, 5874, 5875	3.02
UCC	Contact your Dell EMC representative	3.30
Unity/UnityVSA	Contact your Dell EMC representative	3.12
VCE Vision	Contact your Dell EMC representative	3.08
ViPR	Contact your Dell EMC representative	3.02
ViPR SRM	Contact your Dell EMC representative	3.02
VMAX[3]	Enginuity 5977	3.02
VNX	VNX Operating Environment (OE) for Block 05.31.000.5.006 or greater VNX Operating Environment (OE) for File 7.0.12.0 or greater	3.02
VNX Control Station Device Client	VNX Operating Environment (OE) for Block 05.31.000.5.006 or greater VNX Operating Environment (OE) for File 7.1.44 or greater	3.02
VNXe	VNXe 2.0.x	3.02
VNXe Device Client	VNXe 2.0.x	3.02
VPLEX	GeoSynchrony 4.0.0.00.00.11 or later	3.02
VxFlex OS	Contact your Dell EMC representative	3.36
VxRack Flex	Contact your Dell EMC representative	3.26
VxRack SDDC	Contact your Dell EMC representative	3.22
VxRail (VSPEX BLUE)	Contact your Dell EMC representative	3.04
XtremIO	XtremIO 2.2.x and greater	3.02
XtremIO Device Client	XtremIO 2.2.x and greater	3.02
Switch - Fabric Manager managing Brocade B-series	Brocade B-series switches running Fabric OS 5.0.1b through 6.1.0x only, with Fabric Manager 5.2.0b or later [bdeg]	3.02
Switch - Cisco	Cisco MDS switches running SAN-OS 3.1(2) or later, NX-OS 4.1(1b) or later. [b] Nexus switches running NX-OS 4.2(1)N1(1) or later. [bh] MDS switches require Fabric Manager or Cisco Data Center Network Manager (DCNM) to be the same version or higher than the highest switch firmware version. Nexus requires Fabric Manager 5.0(1a) or higher.	3.02

a. RecoverPoint 3.1 and 3.2 utilize SRS for remote services access only. RecoverPoint 3.3 and later add the connect home feature. RecoverPoint Management GUI (RPMGUI) is supported on SRS 2.20 and above.

b. For remote services access only, not for connect home through SRS.

c. These part numbers designate Service Processor that is running Windows NT SP6. xx70 code only supports ftp for connect home.

d. Fabric Manager does not support FOS 6.1.1 or higher. CM or CMDCE is required. Please refer to the appropriate FOS Release Notes.
e. CM does not support FOS 6.3.x or higher. cmdce is required. Please refer to the appropriate FOS Release Notes.
f. CMDCE is required to support FOS 6.3.x or higher. Please refer to the appropriate FOS Release Notes.
g. Connect home via CM, CMDCE, or CMCNE, otherwise no connect home through SRS.
h. Connect home via Cisco Fabric Manager or Cisco Data Center Network Manager, otherwise no connect home through SRS.

Port requirements

For port requirements, refer to the *Secure Remote Services Port Requirements* document.

Summary

SRSv3 provides increased security and functionality to the Secure Remote Services portfolio.

Site architecture

You set up SRS at your site, with the assistance of Dell EMC Global Service professionals. SRS has the following capabilities:

- **SRSv3** — This TLS HTTPS handler is the broker that directs communication between your Dell EMC-installed products and Dell EMC Global Services, handling user authentication, service notification data file transfer, remote access session regulation, and device management—all the tasks required for remote services.
- **Configurations** —You can choose from a variety of configurations. If you choose a High Availability Cluster server configuration, you will use two or more SRS servers to eliminate single point of failure and help ensure that your system is available for remote services of your Dell EMC products.
- **Policy Manager** — This application lets you specify the access authorization criteria for remote access operations on each device or group of devices that you manage using SRS.

Security features

SRS protects customer confidentiality and integrity through the industry-recognized "3 A" security practices—authentication, authorization, and audit logging—with full customer control over remote communications and policy management: All connections are initiated from your site:

- **Device Control** — Your Dell EMC devices are protected with 24/7 heartbeat monitoring and rapid alert response to system events.
- **Policy Management** — You can specify authorization rules within a wide range of possible configurations and behaviors.
- **Digital Certificate Management** — Digital Certificate Management automates the SRS digital certificate enrollment by taking advantage of Dell EMC's existing authentication system.
- **Access Control** — You have complete control over the configuration and management of Dell EMC's strict IP and port-mapping secure connection solution. Dell EMC Global Services professionals are granted access to your system only under your approval, in addition to their required authorization using Dell EMC's strict centralized access controls.

Glossary

authenticate Confirm or deny the identity of a system user candidate.

authorize Confirm or deny the level of access or editing privileges for a system user.

Client The SRS application that acts as the single point of entry and exit for all IP-based Dell EMC remote services activity.

Dell EMC Enterprise The Dell EMC SRS back-end infrastructure, which includes a Graphical User Interface used by authorized Dell EMC Global Services professionals.

demilitarized zone (DMZ) A computer or subnetwork that sits between a trusted internal network, such as a corporate private Local Area Network (LAN), and an untrusted external network, such as the public Internet.

device See managed device.

embedded client An Embedded SRS Device Client is integrated on some Dell EMC Products, and utilizes the same technology as the SRSv3. If using a Policy Manager, it enforces the policy and audits just like an SRSv3, but only on that specific device.

event An error or otherwise notable activity reported from the managed device.

managed device A Dell EMC information infrastructure product (such as Celerra, Centera, CLARiiON, Symmetrix) installed at a customer site and "managed" by an SRSv3.

Network Address Translation (NAT) An Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

RSA RSA, the Security Division of Dell EMC, makers of security servers and SecurID Authenticators used in SRS authentication procedures.

Documentation

SRS documentation is available from Dell EMC Online Support:

https://support.emc.com

INDEX