Best Practices for Securing Dell EMC SC Series Storage

Abstract

This paper explores the technologies available for building a secure Dell EMC™ SC Series storage area network (SAN) with operational environment best practices and self-encrypting drives.

October 2018

Revisions

Date	Description
June 2014	Initial release
April 2015	Minor updates
April 2016	Updates for SCOS7.0 and DSM 2016 R1
October 2018	Validated for SCOS 7.3 and DSM 2018; added CloudIQ and air-gapped sections

Acknowledgements

Updated by: David Glynn

Table of contents

1 Introduction

Data security is a primary concern in any IT environment. Business-critical or confidential information must be protected from unauthorized access and properly disposed of when required. Many organizations are compelled to implement data-protection technologies due to regulatory compliance.

This document provides best practices for deploying a secure Dell EMC™ SC Series SAN to prevent unauthorized access to administrative interfaces and to protect data at rest using self-encrypting drives.

1.1 Audience

This paper is intended for storage administrators, SAN system designers, storage consultants, network and security consultants, or anyone tasked with building a secure, production SAN using SC Series storage. It is assumed that all readers have experience in designing or administering a shared storage solution. Also, there are some assumptions made in terms of familiarity with all current Ethernet standards as defined by the Institute of Electrical and Electronic Engineers (IEEE) as well as TCP/IP and iSCSI standards as defined by the Internet Engineering Task Force (IETF).

2 SC Series SAN

The SC Series includes high performance, enterprise-level SAN devices that support Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), and iSCSI connections. They provide fast, network-based storage to servers.

An SC Series SAN consists of at least one controller and disk enclosure interconnected with SAS, or Fibre Channel in some legacy SC Series systems. For more advanced storage-administration capabilities, the Dell Storage Manager (DSM), formerly Enterprise Manager, application may be used to administer multiple SC Series SANs. DSM and the associated Data Collector service run on a separate server on the same management network as the SC Series storage. Storage administrators use this management network to access and administer DSM and each SC Series system.

In addition to the management network, each SC Series array is connected to a SAN consisting of the SC Series front-end adapters and the FC, FCoE, or iSCSI initiators of the host servers.

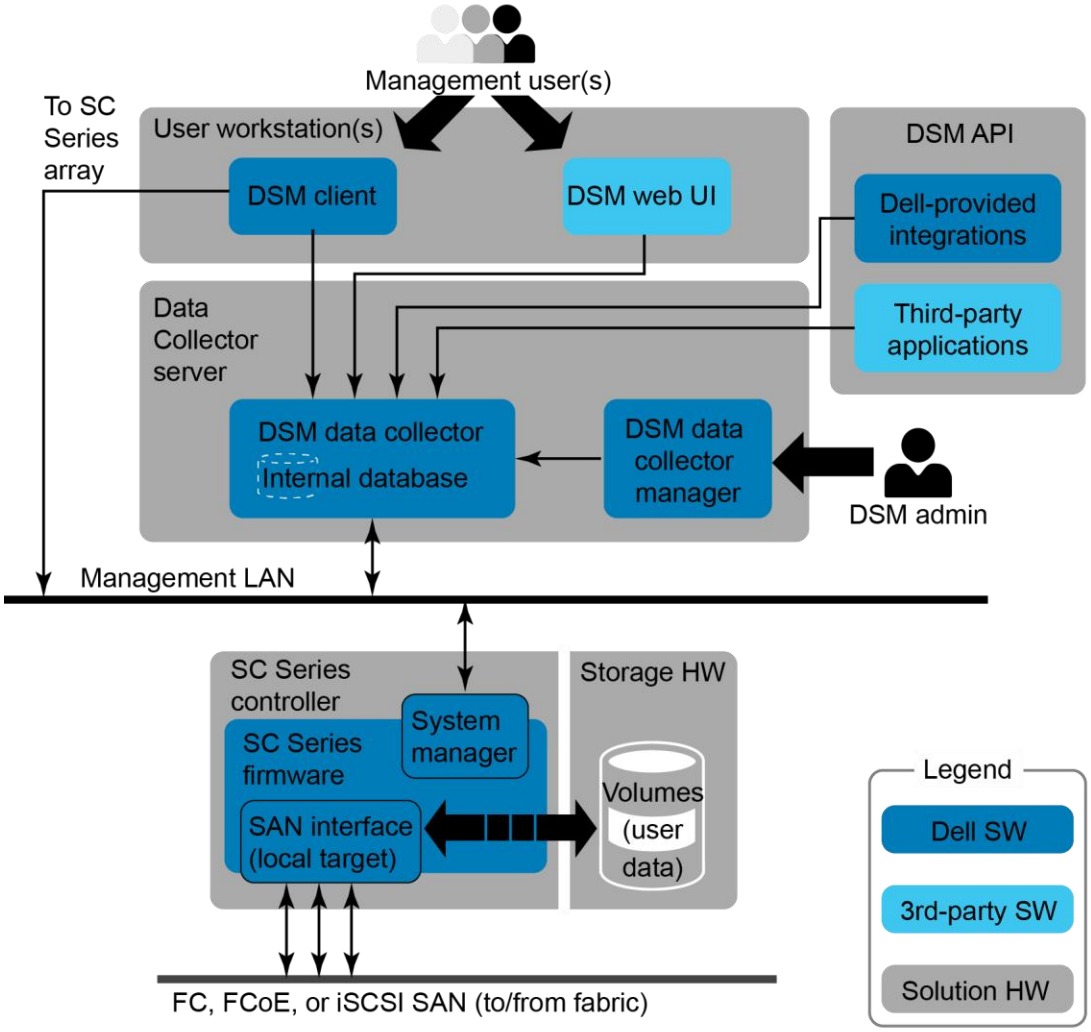

Figure 1 Functional block diagram of the SC Series SAN components

2.1 Basic security features

An SC Series SAN offers a variety of mechanisms for preventing unauthorized access to administrative access points or to storage volumes. In addition, self-encrypting drives (SEDs) are available to provide security for data at rest.

Note: Common Criteria (CC) for IT Security Evaluation certification of SC Series storage is in process at the time of this publication (certificate number: BSI-DSZ-CC-0847): https://www.bsi.bund.de/EN/Topics/Certification/incertification.html

The primary security features of an SC Series SAN include the following:

Event auditing: For administrative events at DSM or Dell™ Storage Center OS (SCOS), this records the controller, user identity and role, date, time, and outcome.

User identity and authentication: This ensures that users authenticate with proper credentials to access administrative functions or storage volumes. Management users require a password to authenticate, Fibre Channel initiators authenticate using their persistent WWN, and iSCSI initiators can be authenticated using unidirectional or bidirectional CHAP.

Data access control: This prevents unauthorized access to storage volumes by requiring an explicit volume mapping from each Fibre Channel or iSCSI initiator to each storage volume. By default, the SC Series system blocks access to all storage volumes, a behavior known as LUN masking. Fibre Channel environments also implement zoning for additional security.

Residual information protection: Whenever a new volume is created, SCOS does not allow a storage host to read from unwritten areas on the volume, and newly allocated pages are zeroed before host access.

Security role management and access: This allows users to have different levels of authorization. In addition to the administrator role for administering DSM and SCOS, there is also a restricted volume manager role that must be granted permission to volumes, storage hosts, or disk folders. A read-only reporter role can view all information but cannot make changes.

Reliable time stamps: Using an internal time source or an NTP server, time stamps within auditing and logs are synchronized.

Trusted channel communication: Management traffic to SCOS and DSM is encrypted using HTTPS over TCP port 443 and TCP port 3033.

2.2 Operational environment

Physical security is always the most basic form of protection for any business-critical infrastructure. To make sure an SC Series SAN operates in a physically secure environment that is accessible only to authorized administrators, use the following best practices:

- Ensure secondary services, such as DNS and NTP, originate from trustworthy sources.
- Physically secure and logically protect the SAN and the management network using firewalling or network isolation. From a physical security and performance standpoint, SAN traffic should be physically separate from the end-user application network. However, in environments with shared networking infrastructure, SCOS supports layer-2 VLAN partitioning to logically separate the iSCSI and LAN traffic on the same physical hardware. Although the SAN and LAN traffic is separated onto different VLAN networks, resource contention with shared hardware means that disproportionate LAN traffic has the potential to negatively affect storage performance.
- Be sure that password complexity is consistent with the authentication policy of the organization. The administrator must change the default password during initialization of the SC Series system. If the password is lost, the administrative password can be reset through physical access using a special procedure only available by contacting Dell Support.
- Apply firmware, security and anti-virus updates regularly to all systems having access to the SAN. In particular, keep web browsers used for remote administrative access up to date.

2.3 Administrative access points

Each SC Series system can be accessed administratively using either the management Ethernet port, or the controller serial port. The controller serial port is only to be used under the direction of Dell Support for advanced troubleshooting and is not intended to be used for daily administrative tasks.

The SC Series array can be configured to allow third-party monitoring tools to access the array controllers using SNMP. An SC Series system can also be configured to send email alerts to an SMTP server or to send system events to a syslog server. SNMP access and syslog logging are disabled by default, whereas SMTP email alerts are set up during initial SC Series configuration or afterwards.

SC Series systems can also be accessed using one of two scripting utilities. Scripts can be created with Microsoft® PowerShell®, or the Dell Storage REST API. With these utilities, administrative commands issued to the array are encrypted over HTTPS and must be authenticated with SCOS credentials.

In addition, there are other software integration components from Dell EMC and from third parties, such as Dell Foglight for Storage Management, the VMware® vRealize® Operations™ plug-in, and the CommVault® Simpana® plug-in, which access SCOS or DSM to provide additional management or reporting capabilities. For more information, refer to the corresponding software product documentation.

Each SC Series controller also includes an iDRAC out-of-band management controller that can be used for administrative tasks, such as remotely power cycling the controller chassis. The iDRAC interface is also used by the SC Series system to apply firmware updates to controller hardware during upgrades. An IP address should be assigned to the iDRAC to make it accessible using a web browser or the remote CLI utility RACADM. Since iDRAC functionality is required for upgrades, firewalls should be used to secure the environment and communications should be limited to only from the SC Series management IP addresses.

2.4 SupportAssist and Secure Console

SC Series includes two features that enhance the enterprise support that Dell provides:

Dell SupportAssist (formerly known as Phone Home) is a service that allows SCOS to automatically send diagnostic logs and alerts to and download firmware updates from Dell.

Secure Console is a service that allows Dell Support engineers to access the SCOS console using Secure Shell (SSH).

SupportAssist is enabled by default but can be disabled in the SCOS settings. Secure Console services are disabled by default. Neither SupportAssist nor Secure Console requires inbound ports to be open at the network firewall while running. Each service, when enabled, makes an outbound connection to a Dell EMC internet server when needed. In the case of Secure Console, this outbound connection allows Dell Support engineers to connect to SCOS using SSH tunneling.

SupportAssist requires outbound TCP port 443 to be open and Secure Console requires outbound TCP port 22 and 8443 to be open.

2.5 SupportAssist at air-gapped sites

There are occasions when configuring the SC Series capabilities for SupportAssist is not an option, such as an air-gapped site configuration. For such occasions, SupportAssist data can be manually exported from SC Series storage and sent to Dell Support.

For instruction on how to perform this task, see the *Saving SupportAssist Data to a USB Flash Drive Tech Note* available on Dell.com/Support.

2.6 CloudIQ data sources

CloudIQ provides centralized monitoring for numerous Dell EMC products across multiple sites. It enables proactive serviceability that informs customers about issues before there is impact to their environment. All of this is provided through a dashboard that aggregates key information such as system health scores, performance metrics, and current capacity and trends.

CloudIQ leverages the existing SC Series SupportAssist data, so there are no additional ports or protocols used for transferring the information from the customer site.

3 Protect data at rest with self-encrypting drives

Data at rest is the data that resides on the physical hard drives within the SC Series enclosure. Though difficult, it is possible that bits of data could be extracted from a conventional hard drive if physical security is breached and the hard drive is removed from an enclosure.

Self-encrypting drives (SEDs) guard against this threat by encrypting data as it is written to the disk and decrypting data as it is read. Starting in version 6.5, SCOS implements this technology in a licensed feature called Secure Data which is transparent to the storage user. Since the encryption is offloaded to the SED, performance impact is negligible.

The following points provide further information about Secure Data behavior:

- An SED will not encrypt or decrypt data if Secure Data is unlicensed.
- Secure Data requires an external key management server, such as Gemalto™ SafeNet KeySecure™.
- A secure data folder can only contain disks identified by SCOS as FIPS-140-2 certified.
- When an SED is assigned to a secure data folder, the existing media encryption key (MEK) on the disk is destroyed and a new MEK is created, rendering all previous data unreadable. This process is known as a cryptographic erase.
- A cryptographic erase is also performed when an SED is removed from a secure data folder. If user data is present on the SED, SCOS will issue a warning prior to un-assigning the drives and destroying and recreating the MEK. This cryptographic erase obviates the need for time-consuming hard-drive data wiping prior to recommissioning.
- When an SED assigned to a secure data folder is physically removed from an enclosure, it locks on reset and can only be unlocked using authority credentials stored on the key management server.
- An SED will lock on reset after a loss of power to the controller and enclosure simultaneously or in the event of a controller flash card failure. After the next SCOS boot, the startup wizard will prompt the administrator to confirm the key management server configuration before unlocking the SED. If a flash card fails, Dell Support can assist with replacing the flash card and unlocking the SED.
- Replicating a secure data folder to an unsecure folder is permitted, but the data on the drives in the unsecure folder will not be encrypted.

Note: For more information on the Dell EMC implementation of SED technology, see the *Dell Compellent Storage Center System Manager Administrator's Guide* on the Knowledge Center at the SC Series Customer Portal, as well as the document, Using Self-Encrypting Drives (SEDs) with Dell EMC SC Series Storage.

4 Protect data in flight

Data in flight is data as it is transmitted over the network within packets. These network packets contain unencrypted data payloads that can be read if the packet is captured in transit.

SC Series storage relies on the physical security of storage and networking hardware and the logical or physical isolation of the SAN and management networks from external networks. It does not support IPsec network-layer security or Fibre Channel encryption.

It is recommended to secure WAN replication traffic with a virtual private network (VPN) using a WAN optimizer or router.

5 Security scanning

No security analysis would be complete without a review of open IP network protocol ports for a given system. Nmap, the open source network discovery and security-auditing tool, was used for this purpose. The following tables list all TCP and UDP ports and services for SCOS and DSM. Not all services are enabled by default. For each port, the protocol is listed as well as the actual port usage.

In order for SCOS and its associated services to function as expected, these ports must remain open through any firewalls or switch access control lists that reside in between the SC Series system and storage initiators, DSM, or secondary services such as NTP. In the case of the Secure Console and SupportAssist services, the external firewall must accept outbound connections through TCP ports 22 and 443 for SCOS to establish connections with Dell EMC internet servers.

5.1 SCOS port list

Table 1 and Table 2 list the TCP and UDP ports and services associated with SC Series storage.

Table 1 SCOS TCP ports and services

TCP port	Protocol	Purpose	Direction
22	SSH	Secure Console service	Outbound
25	SMTP	Sending email notifications	Outbound
80	HTTP	Automatic redirect to HTTPS port	Inbound
88	Kerberos	Secure communication with KDC	Outbound
389	LDAP	Directory access	Outbound
443	HTTPS	Communicating with SC Series applications SupportAssist	Inbound and outbound
636	LDAPS	Using LDAP over SSL	Outbound
3033	HTTPS	Dell API	Inbound and outbound
3205	iSNS	Communication with network servers	Outbound
3260	iSCSI	iSCSI initiator (server or replication source)	Inbound and outbound
8080	HTTP	Automatic redirect to HTTPS port	Inbound
8443	HTTPS	Communicating with SC Series applications SupportAssist	Inbound and outbound

Table 2 SCOS UDP ports and services

UDP port	Protocol	Purpose	Direction
69	TFTP	SupportAssist access to configuration and boot files	Inbound
123	NTP	Network Time Protocol	Inbound and outbound
161	SNMP	Communication from network manager	Inbound
162	SNMP trap	Sending alerts	Inbound and outbound
514	syslog	Forwarding SCOS logs to syslog server	Outbound
5000-5010	Dell EMC IPC	IPC traffic for communicating with SCOS components	Inbound and outbound
20000	Dell EMC IPC	IPC traffic for communicating with SCOS components	Inbound and outbound

5.2 DSM port list

Table 3 and Table 4 list the TCP and UDP ports and services associated with DSM.

Table 3 DSM TCP ports and services

TCP port	Protocol	Purpose	Direction
22	SSH V2	Access to console (DSM virtual appliance only)	Inbound
25	SMTP	Send email notifications	Outbound
389	LDAP	Communicating with Active Directory Domain Controllers or OpenLDAP servers	Outbound
443	HTTPS	Communicating with managed SC Series Sending diagnostic data with SupportAssist Activating licenses	Inbound and outbound
636	LDAPS	Communicating with Active Directory Domain Controllers or OpenLDAP servers	Outbound
1433	Microsoft SQL Server®	Connecting to an external Microsoft SQL Server database	Outbound
3003	OCP	Communicating with managed Dell PS Series groups	Outbound
3033	HTTPS	Communication from all clients, including the DSM client and Dell Storage Replication Adapter (SRA) Alerts from Dell FluidFS clusters Alerts from Fluid Cache clusters Communicating with managed SC Series SANs	Inbound and outbound

TCP port	Protocol	Purpose	Direction
3034	HTTPS	VASA 1.0 and 2.0 provided with DSM 2016 R1, supports communications from VMware vCenter® and ESXi®	Inbound
3306	MySQL	Connecting to an external MySQL database	Outbound
5988	SMI-S over HTTP	Receiving unencrypted SMI-S communication	Inbound
5989	SMI-S over HTTPS	Receiving encrypted SMI-S communication	Inbound
7342	Legacy Client Listener Port	Communicating with the remote data collector Providing automatic upgrade functionality for previous versions of the DSM client	Inbound and outbound
8080	HTTP	Communication from Storage Manager Server Agents Alerts forwarded from SC Series arrays Communicating with VMware servers	Inbound and outbound
27355	Server Agent Socket Listening Port	Communicating with Server Agents	Outbound
27555	APM Agent Listening port	Communicating with Application Protection Manager agents	Outbound
35451	FluidFS	Communicating with managed FluidFS clusters	Outbound
44421	FluidFS diagnostics	Retrieving diagnostics from managed FluidFS clusters	Outbound

Table 4 DSM UDP ports and services

UDP port	Protocol	Purpose	Direction
22	SSH V2	Access to console (DSM virtual appliance only)	Inbound
514	Syslog	Receiving logs forwarded from SC Series arrays Forwarding SCOS logs to syslog servers	Inbound and outbound
8514 (VA only	Syslog	Alternative port for syslog messages	Inbound and outbound

5.3 DSM client port list

Table 5 list the TCP ports and services associated with DSM client. No UDP ports are used.

Table 5 DSM client TCP ports and services

TCP port	Protocol	Purpose	Direction
3033	HTTP	Communicating with the DSM server Direct communication with managed or unmanaged SC Series SAN	Outbound

5.4 DSM Server Agent port list

Table 6 list the TCP ports and services associated with DSM Server Agent. No UDP ports are used.

Table 6 DSM Client TCP ports and services

TCP port	Protocol	Purpose	Direction
8080	HTTP	Communicating with the DSM server	Outbound
27355	Server Agent Socket Listening Port	Receiving communication from the DSM server	Inbound

6 Conclusion

An SC Series SAN offers a variety of mechanisms for preventing unauthorized access to administrative access points or to storage volumes.

The following actions are recommended to ensure the security of SC Series storage:

- Restrict physical access to the SAN hardware and to the DSM server.
- Ensure password complexity is consistent with the organizational security policy.
- Logically isolate and firewall the SAN and management networks.
- Ensure all host systems and applications on the SAN are kept up to date with firmware and software updates, particularly web browsers used for administrative access.
- Ensure secondary services such as DNS and NTP are trustworthy.
- License the Secure Data feature and use SEDs to ensure that no data is lost in the event of a physical security breach.
- Use a VPN to secure replication traffic.
- Change the default password of the iDRAC administrative account.

A Additional resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage Solutions Technical Documents provide expertise that helps to ensure customer success on Dell EMC storage platforms.

A.1 Related resources

See the following referenced or recommended Dell EMC publications and resources. Access to the SC Series Customer Portal requires a login.

- *Dell Storage Center System Manager Administrator's Guide* on the SC Series Knowledge Center
- *Dell Storage Manager Administrator's Guide* on the SC Series Knowledge Center
- Common Criteria certifications in process