Best Practices for Securing Dell Compellent Storage Center

A Dell Compellent best practices paper

Dell Storage Engineering
June 2014

Revisions

Date	Description
June 2014	Initial release

Table of contents

Acknowledgements

This best practice white paper was produced by the following members of the Dell Storage team:

Engineering: Clay Cooper and Darin Schmitz

Editing: Camille Daily

Additional contributors: Michael Kosacek, Richard Golasky, Adam Lysne, Mike Markovich, BJ Kowalski and Justin Braun

Feedback

We encourage readers of this publication to provide feedback on the quality and usefulness of this information by sending an email to SISfeedback@Dell.com.

SISfeedback@Dell.com

Executive summary

This paper explores the technologies available for building a secure Dell Compellent SAN with operational environment best practices and self-encrypting drives.

1 Introduction

The Dell Compellent Storage Center is a high performance, enterprise-level Storage Area Network (SAN) storage device that supports both Fibre Channel, Fibre Channel over Ethernet (FCoE) and iSCSI connections. It provides fast, network-based storage to corporate servers.

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 technical paper serves as a guide to deploying a secure Compellent Storage Center SAN to prevent unauthorized access to administrative interfaces and to protect data at rest using self-encrypting drives.

1.1 Audience

This technical white paper is for storage administrators, SAN system designers, storage consultants, network and security consultants, or anyone tasked with building a secure, production SAN using Compellent Storage Center. It is assumed that all readers have experience in designing and/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 IEEE (Institute of Electrical and Electronic Engineers) as well as TCP/IP (Transmission Control Protocol/Internet Protocol) and iSCSI standards as defined by the IETF (Internet Engineering Task Force).

2 Compellent Storage Center SAN

A Compellent Storage Center SAN consists of at least one Storage Center controller and disk enclosure interconnected with Serial Attached SCSI (SAS) or, in some older Storage Center systems, with Fibre Channel. For more advanced storage administration capabilities, the Enterprise Manager application may be used to administer multiple Storage Center instances. Enterprise Manager and the associated Data Collector service run on a separate server on the same management network as the Storage Centers they administer. Storage administrators use this management network to access and administer Enterprise Manager and each Storage Center.

In addition to the management network, each Storage Center is connected to a storage area network (SAN), which can be Fibre Channel, Fibre Channel over Ethernet (FCoE), or iSCSI protocol over Ethernet. The SAN consists of the Storage Center front-end adapters and the Fibre Channel, FCoE, or iSCSI initiators of the host servers.

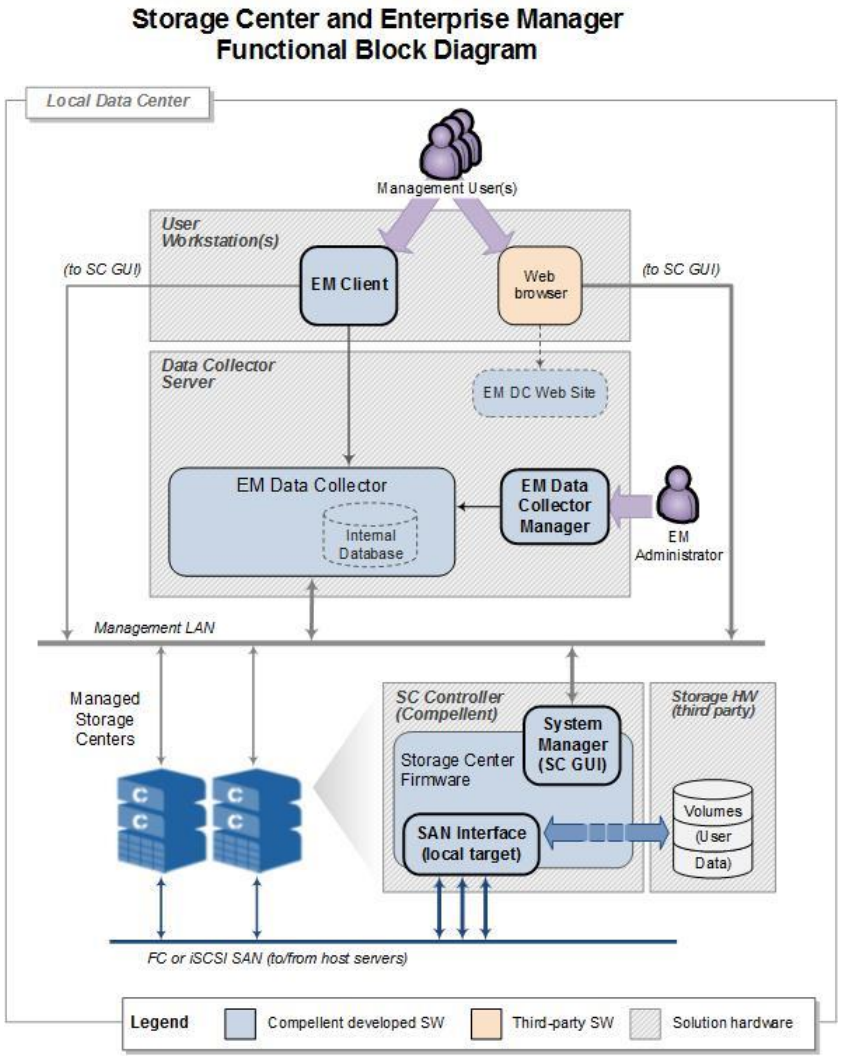

Figure 1 Functional block diagram of Compellent SAN components

2.1 Basic security features

A Compellent Storage Center SAN offers a variety of mechanisms for preventing unauthorized access to administrative access points or to storage volumes.

In addition, self-encrypting drives are available to provide security for data at rest.

Common Criteria for IT Security Evaluation (CC) certification of Compellent Storage Center 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 a Compellent Storage Center SAN are:

- **Event auditing:** For administrative events at Enterprise Manager or Storage Center, the controller, the user identity and role, the date, time and outcome are recorded.
- **User identity and authentication:** 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 World Wide Name (WWN), and iSCSI initiators authenticate using CHAP (Challenge-Handshake Authentication Protocol).
- **Data access control:** 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, Storage Center 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, Storage Center 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:** Allows users to have different levels of authorization. There are roles for administering Enterprise Manager or Storage Center or for volume management. In addition, a read-only Reporter role can view all information but cannot make changes. Access can further be limited to certain sets of volumes, storage hosts, or Storage Center disk folders.
- **Reliable time stamps:** Using an internal time source or an NTP (Network Time Protocol) server, time stamps within auditing and logs are synchronized.
- **Trusted channel communication:** Management traffic to Storage Center and Enterprise Manager is encrypted using Hypertext Transport Protocol Secure (HTTPS) over TCP port 443.

2.2 Operational environment

Physical security is always the most basic form of protection for any business critical infrastructure. A Compellent Storage Center SAN is designed to operate in a physically secure environment that is accessible only to authorized administrators.

Ensure secondary services, such as DNS (Domain Name System) 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, Storage Center supports layer-2 VLAN partitioning to logically separate the iSCSI and LAN traffic on the same physical hardware. It is important to keep in mind that 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 Storage Center system. If the password is lost, the administrative password can be reset through physical access using a special procedure only available by contacting Dell Storage 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.

CVE-2014-0160, also known as the "Heartbleed bug" is a serious vulnerability in the popular OpenSSL cryptographic software library. For more information on this vulnerability, see http://heartbleed.com. For a status of Dell products, workarounds and updates, see the Dell Heartbleed bug remediation page at http://www.dell.com/learn/us/en/04/campaigns/heartbleed-remediation.

2.3 Administrative access points

Each Storage Center 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 Storage Support for advanced troubleshooting, and is not intended to be used for daily administrative tasks.

The System Manager GUI is available through the management Ethernet port using a standard web browser. Initially a java application will be downloaded using the web browser over TCP port 80 or port 443. Once downloaded, the java application will securely connect to the Storage Center using the administrative credentials set during system initialization. The traffic will be encrypted using Transport Layer Security (TLS).

The Storage Center array can be configured to allow third party monitoring tools to access the array controllers using SNMP (Simple Network Management Protocol). A Storage Center system can also be configured to send email alerts to an SMTP (Simple Mail Transfer Protocol) server or to send system events to a syslog server. SNMP access and syslog logging are disabled by default whereas SMTP email alerts are setup during initial Storage Center configuration.

Storage Center systems can also be accessed via one of two scripting utilities. Scripts can be created with Microsoft PowerShell for Windows based scripts, or a Java based utility called the Compellent Command Utility (CompCU) can be used for platform agnostic scripting needs. With these utilities, administrative commands issued to the array are encrypted over HTTPS, and must be authenticated with Storage Center credentials.

In addition, there are other software integration components from Dell and from third parties, such as Dell Forlight for Storage, the VMware vCOPS plug-in, and the CommVault Simpana plug-in, which access Storage Center to provide additional management or reporting capabilities. For more information, refer to the corresponding software product documentation.

Each Storage Center 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 IP address of the iDRAC can be assigned using the LCD panel on the front of the chassis and the iDRAC can then be accessed using a web browser or the remote CLI utility RACADM. The default password of the administrative account should be changed immediately. If iDRAC functionality is not required, then the iDRAC Ethernet port should not be connected to the network.

2.4 Phone Home and Secure Console

Compellent Storage Center includes two features that enhance the enterprise support that Dell is able to provide.

- Phone Home is a service that allows Storage Center to automatically send diagnostic logs and alerts to and download firmware updates from Dell Compellent Phone Home Servers.
- Secure Console is a service that allows Dell Storage Support engineers to access the Storage Center console using Secure Shell (SSH).

Phone Home is always enabled but can be effectively disabled by blocking outbound TCP port 443. Secure Console services are disabled by default. Neither Phone Home nor Secure Console requires inbound port to be open at the network firewall while running. Each service, when enabled, makes an outbound connection to a Dell internet server when needed. In the case of Secure Console, this outbound connection allows Dell Storage Support engineers to connect to the Storage Center using SSH tunneling.

Phone Home requires outbound TCP port 443 to be open and Secure Console requires outbound TCP port 22 to be open.

3 Protecting data at rest with self-encrypting drives

Data at rest is the data that resides on the physical hard drives within the Storage Center 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 (SED) 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, Compellent Storage Center 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 Compellent Secure Data behavior:

- An SED will not encrypt/decrypt data if Secure Data is unlicensed.
- Secure Data requires an external key management server.
- A Secure Data folder can only contain disks identified by Storage Center 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 crypto erase.
- A crypto erase is also performed when an SED is removed from a Secure Data folder. If user data is present on the SED, Storage Center will issue a warning prior to un-assigning the drives and destroying and recreating the MEK. This crypto erase obviates the need for time-consuming hard drive data wiping prior to re-commissioning.
- 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.
- SED may 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 Storage Center boot, the Startup Wizard will prompt the administrator to confirm the key management server configuration before unlocking the SED. If a flash card fails, contact Dell Storage Support for assistance 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.

For more on the Compellent implementation of SED technology, see the *Dell Compellent Storage Center System Manager 6.5 Administrator's Guide* at http://kc.compellent.com.

4 Protecting data in flight

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

Compellent Storage Center 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 tables below list all TCP and UDP ports and services for Compellent Storage Center and Enterprise Manager. Not all services are enabled by default. For each port, the protocol is listed as well as the actual port usage.

In order for Storage Center 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 Storage Center and storage initiators, Enterprise Manager, administrator web clients or secondary services such as NTP. In the case of the Secure Console and Phone Home services, the external firewall must accept outbound connections through TCP ports 22 and 443 for Storage Center to establish connections with Dell Compellent internet servers.

5.1 Storage Center port list

Table 1 and Table 2 list the TCP and UDP ports and services associated with Storage Center.

Table 1 Storage Center TCP ports and services

TCP Port	Protocol	Purpose
22	SSH	Secure Console service
25	SMTP	Sending email notifications
80	HTTP	Automatic redirect to HTTPS port
389	LDAP	Directory access
443	HTTPS	Storage Center GUI access, Phone Home service
636	LDAPS	Directory access using SSL
3033	HTTPS	Dell Compellent API (for internal Storage Center communication only)
3205	iSNS	Internet Storage Name Service
3260	iSCSI	iSCSI initiator access
8080	HTTP	Automatic redirect to HTTPS port
8443	HTTPS	Storage Center GUI access, Phone Home service

Table 2 Storage Center UDP ports and services

UDP Port	Protocol	Purpose
69	TFTP	Configuration and boot files
123	NTP	Network Time Protocol
161	SNMP	Communication with Enterprise Manager
162	SNMP trap	Sending alerts
514	syslog	Forwarding logs to Syslog server
3478	STUN	Session Traversal Utilities for NAT
5000-5010	Compellent IPC	IPC traffic for communicating with Storage Center components
20000	Compellent IPC	IPC traffic for communicating with Storage Center components

5.2 Enterprise Manager port list

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

Table 3 Enterprise Manager TCP ports and services

TCP Port	Protocol	Purpose
25	SMTP	Sending email notifications
443	HTTPS	Communicating with managed Storage Centers and managed zNAS servers Sending Phone Home data Activating the license
1433	Microsoft SQL Server	Connecting to an external Microsoft SQL Server database
3033	HTTP	Communication from all clients, including the Enterprise Manager Client and Storage Replication Adapter (SRA) 6.2.2 Alerts from FluidFS clusters Alerts from Fluid Cache clusters
3306	MySQL	Connecting to an external MySQL database
5988	SMI-S over HTTP	Receiving unencrypted SMI-S communication
5989	SMI-S over HTTPS	Receiving encrypted SMI-S communication
6774	Fluid Cache	Communicating with Fluid Cache servers

7342	Legacy Client Listener Port	Communicating with the remote Data Collector Providing automatic upgrade functionality for previous versions of the Enterprise Manager Client
8080	HTTP (legacy)	Communication from Server Agents Alerts forwarded from Storage Centers
27355	Server Agent Socket Listening Port	Communicating with Server Agents
35451	FluidFS	Communicating with managed FluidFS clusters
44421	FluidFS diagnostics	Retrieving diagnostics from managed FluidFS clusters

Table 4 Enterprise Manager UDP ports and services

UDP Port	Protocol	Purpose
514	Syslog	Receiving logs forwarded from Storage Centers Forwarding Storage Center logs to syslog servers

6 Conclusion

A Dell Compellent Storage Center 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 Storage Center:

- Restrict physical access to the SAN hardware and to the Enterprise Manager 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 self-encrypting drives (SED) to ensure that no data is lost in the event of a physical security breach.
- Use a VPN to secure replication traffic.
- The default password of the iDRAC administrative account should be changed immediately. If iDRAC functionality is not required, then the iDRAC Ethernet port should not be connected to the network.

A Test configuration details

Hardware	Description
SAN storage	(2) Dell Compellent SC8000 — Firmware version: 6.5 • (1) Two port 10GbE iSCSI Adapter • (1) Four port 8 Gbps Fibre Channel Adapter • (1) Four port 6 Gbps SAS Adapter (1) SC-220 Disk Drive Enclosure • (24) 15k Disk Drives
Management Software	(1) Dell Compellent Enterprise Manager Data Collector — Version: 2014 R2

Additional resources

Support.dell.com is focused on meeting your needs with proven services and support.

DellTechCenter.com is an IT Community where you can connect with Dell customers and Dell employees for the purpose of sharing knowledge, best practices, and information about Dell products and your installations.

Referenced or recommended Dell publications:

- Dell Compellent Storage Center System Manager Version 6.5 Administrator's Guide
  - Site requires login: http://kc.compellent.com
  - To acquire a login visit: http://customer.compellent.com

- Dell Compellent Enterprise Manager 2014 R2 Administrator's Guide
  - Site requires login: http://kc.compellent.com
  - To acquire a login visit: http://customer.compellent.com

Common Criteria certifications in process:

- https://www.bsi.bund.de/EN/Topics/Certification/incertification.html