Technical White Paper

Dell EMC PowerMax and VMAX All Flash: Data at Rest Encryption

Abstract

This document describes how Dell EMCÊ PowerMax and VMAXÊ All Flash Data at Rest Encryption (D@RE) protects data confidentiality by adding back-end encryption to the entire array.

September 2019

H13936.2

Revisions

Date	Description
February 2015	Initial release
May 2017	Content update
September 2019	Content update; new template

Acknowledgements

Author: Richard Pace

Table of contents

Executive summary

Securing sensitive data is one of the greatest challenges faced by many enterprises. Increasing regulatory and legislative demands and the constantly changing threat landscape have brought data security to the forefront of IT issues. Several of the most important data security threats are related to protection of the storage environment, where drive loss and theft are primary risk factors. Dell EMC™ PowerMax and VMAX™ All Flash Data at Rest Encryption (D@RE) protects data confidentiality by adding back-end encryption to the entire array.

D@RE provides hardware-based, on-array, back-end encryption for PowerMax and VMAX All Flash arrays with FIPS 140-2 validated back-end I/O modules that use the 256-bit AES-XTS encryption algorithm. These modules encrypt and decrypt data as it is being written to or read from physical drives, which protects information from unauthorized access even when physical drives are removed from the array.

Terminology

The following terms are used in this document:

Drive Array Enclosure (DAE): Storage module that contains fully redundant drives, link control cards (LCCs), power supplies, and cooling components.

PowerMaxOS: The PowerMax operating environment that runs on PowerMax and VMAX All Flash arrays.

Audit Log: An immutable audit log that tracks security events on a PowerMax or VMAX All Flash array. The audit log allows administrators to identify any breaches in the array and prove compliance with data-protection policies.

Management Module Control Station (MMCS): Component that monitors the array environment, provides remote notification and remote support capabilities, and allows Dell EMC personnel to access the array locally or remotely.

SymmWin Application: Graphics-based tool used by Dell EMC personnel for configuring and monitoring PowerMax and VMAX All Flash arrays.

Back-end I/O module: Component that contains a 256-bit AES-XTS encryption controller and provides connectivity to DAEs. The key encryption key is programmed into write-only, non-volatile memory in the I/O module.

AES-XTS algorithm: An XEX-based tweaked-codebook (TCB) mode with cipher-test stealing (XTS) disk encryption used for the encryption of sector-based storage devices.

Data encryption key (DEK): Key used by PowerMax and VMAX All Flash encryption algorithms to encrypt and decrypt data and apply confidentiality protection to information.

Key encryption key (KEK): Key that keeps DEKs secure during storage and transmission. The approved technique to protect DEKs is to use KEKs along with the AES Key Wrap algorithm.

RSA Embedded Data Protection Manager (eDPM): Manager that provides onboard set-and-forget data-at-rest encryption services.

Key Management Interoperability Protocol (KMIP) client: Client software that allows for separation of key management between PowerMax or VMAX All Flash arrays and an OASIS KMIP based key management server.

1 Data at Rest Encryption

Data at Rest Encryption (D@RE) provides hardware-based, on-array, back-end encryption for PowerMax and VMAX All Flash systems. Back-end encryption protects your information from unauthorized access when physical drives are removed from the system. D@RE provides encryption on the back-end using I/O modules that incorporate 256-bit AES-XTS data encryption.

These modules encrypt and decrypt data as it is being written to or read from a physical drive. All configured drives are encrypted, including both data and spare drives using a unique DEK per drive. In addition, all cached user data that gets stored during a vault is encrypted.

D@RE incorporates RSA Embedded Data Protection Manager (eDPM) for on-board, set-and-forget key management.

D@RE can also be deployed with an external key manager using KMIP, which provides external centralized key storage and management which simplifies key generation and recovery management for PowerMax and VMAX All Flash and other KMIP-compatible encryption solutions.

By securing data on PowerMax and VMAX All Flash systems, D@RE ensures that the potential exposure of sensitive data on discarded, misplaced, or stolen media is reduced or eliminated. As long as the key used to encrypt the data is secured, encrypted data cannot be read. In addition to protecting against threats related to physical removal of media, this also means that media can readily be repurposed by process of data cryptoshredding, which destroys the encryption key used for securing the data previously stored on that media.

D@RE is compatible with all PowerMax and VMAX All Flash system features, allows for encryption of any supported drive type or volume emulation, and delivers powerful encryption without performance degradation or disruption to existing applications or infrastructure.

2 Key management

Because encryption offers protection for the data itself rather than for a device or host, it is a powerful tool for enforcing security policies. However, the data security provided by encryption is only as good as the generation, protection, and management of the keys used in the encryption process. Encryption keys must be available when they are needed, but at the same time access to the keys during decryption activities must be preserved for the lifetime of the data. This is especially important for the enterprise storage environments where encrypted data is kept for many years. D@RE offers flexible key management options with both embedded and external key managers.

2.1 Embedded key manager

Because of the critical importance of key management in encryption solutions, D@RE was designed to be integrated with RSA Embedded Data Protection Manager (eDPM). RSA eDPM provides enterprise key management for a broad range of encryption environments, establishing a pervasive and secure infrastructure for this essential component of data security. All key generation, distribution, and management capabilities required for D@RE are provided by eDPM, according to the best practices defined by industry standards such as NIST 800-57 and ISO 11770.

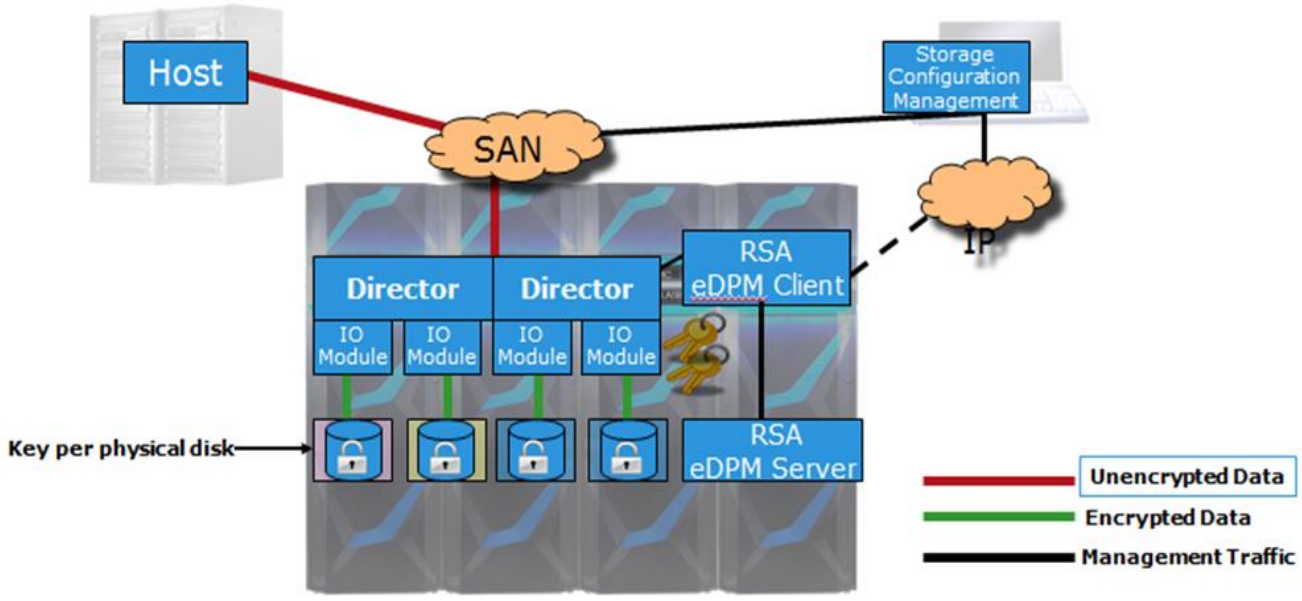

Figure 1 Embedded key manager architecture

2.2 External key manager

D@RE can also be deployed with external key managers using the OASIS Key Management Interoperability Protocol (KMIP) which allows for a separation of key management from PowerMax and VMAX All Flash arrays. KMIP is an industry standard that defines message formats for the manipulation of cryptographic keys on a key management server. External key managers provide support for consolidated key management and allows integration between PowerMax and VMAX All Flash arrays with an existing key management infrastructure. They also provide the ability to non-disruptively migrate keys from an embedded key manager. External key management can cluster multiple key server appliances and separate key ownership and management individually while providing a centralized audit log. Depending on the specific capabilities of the

external key manager, hardware security module (HSM) integration can provide FIPS 140-2 Level 3 compliance.

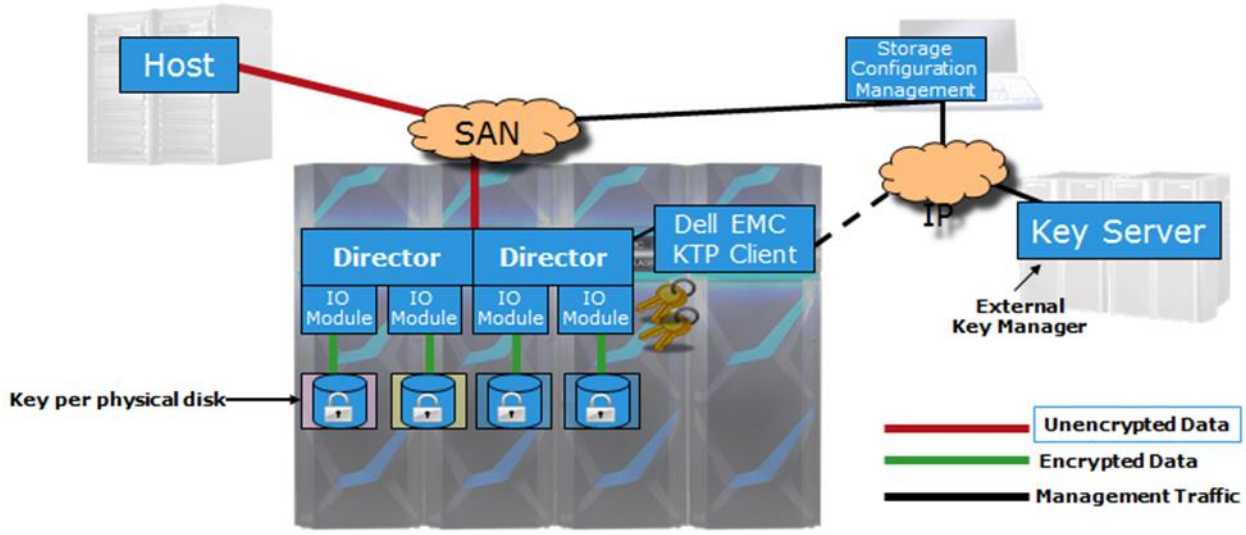

Figure 2 External key manager architecture

3 Key manager components

This section describes the components for both embedded and external key managers.

3.1 Embedded key management components

Embedded key management utilizes the following RSA software, which resides on the primary Management Module Control Station (MMCS):

- eDPM server: Embedded key manager which provides encryption key management capabilities such as secure key generation, storage, distribution, and audit
- eDPM client: Client software that handles communication with the eDPM server
- RSA BSAFE® Cryptographic Libraries: Provides foundational security functionality for the eDPM server and client
- Common Security Toolkit (CST) Secure Lockbox: An encrypted repository that securely stores passwords and other sensitive key manager configuration information

3.2 External key management components

External key management utilizes the following components:

- Key Trust Platform (KTP) client: Client software that runs securely on the MMCS and facilitates communication between the external key manager and PowerMax or VMAX All Flash system
- RSA BSAFE® Cryptographic Libraries: Provides foundational security functionality for the external key management server and KTP client
- Common Security Toolkit (CST) Secure Lockbox: An encrypted repository that securely stores passwords and other sensitive key manager configuration information

PowerMax and VMAX All Flash systems can interoperate with the following external key manager platforms:

- Gemalto® (SafeNet) KeySecure™
- IBM® Secure Key Lifecycle Manager

Note: The above external key managers are offered as of the publication date of this document. Check with Dell EMC to confirm support for any additional external key managers.

3.3 Data encryption key protection

The following ensures the protection of data encryption keys (DEKs):

- For embedded D@RE, the local key repository is encrypted with 256-bit AES using a random-generated password which is saved in the secure lockbox.
- The lockbox is protected by PKCS#12 using primary MMCS-specific stable system values (SSVs).
  - Removal of an MMCS will not allow file access without valid SSC credentials.
  - Copying lockbox repository files will fail SSV tests.

- For D@RE with external key management, the secure lockbox contains the PKCS#12 password that protects the PowerMax or VMAX All Flash client's Transport Layer Security (TLS) authentication private key.
- All persistent key storage locations either contain wrapped or encrypted keys.
- There are no backdoor keys or passwords to bypass security.

3.4 Data encryption key recovery

The following information applies to recovery of encryption keys:

- External key managers only need to be available during initial installation, back-end maintenance or upgrades, or in an unlikely system-recovery event.
- The array can come online without the MMCS being available, using keys persistently cached on the array itself.
- MMCS key management components can restore the D@RE configuration and keys directly from the array, in most cases.

3.5 Data encryption key integrity

The following features ensure the integrity of the DEKs:

- Data keys exported to the array include a unique keytag identity alias along with the key metadata, which is appended to key data during the keywrap process along with an AES-key-wrap-required constant initial value (IV).
- During encryption I/O, the expected keytag associated with the drive is separately supplied along with the wrapped key.
- During key unwrap (prior to starting an I/O), the encryption hardware checks for both a valid IV and matching keytag to ensure the correct key is being used to protect data on a specific drive.
- Arrays with data encryption enabled have a special physical information block (PHIB) located in a reserved system area at the beginning of each drive. Before the drive is made available for normal I/O operation, the PHIB contents are used to validate that the key being used to encrypt the drive matches the last known key in use by the array.

3.6 Data at Rest Encryption certificate management

With the PowerMaxOS Q3 2019 release and Dell EMC Unisphere™ 9.1 release, customers have the ability to enter or update existing D@RE external public key certificates. The certificates, along with other sensitive information such as the key server's IP address and authentication information, can be entered to deploy or update an external key manager without having to share sensitive information with anyone outside of the organization. Once the information is entered into Unisphere, it is sent to the array MMCS in an encrypted file where the D@RE external key manager migration or certificate update script will be run by Dell EMC personnel. The script then verifies the information entered and proceeds with the process. Loading certificates and authentication information can be performed in advance before scheduling any script activity from Dell EMC.

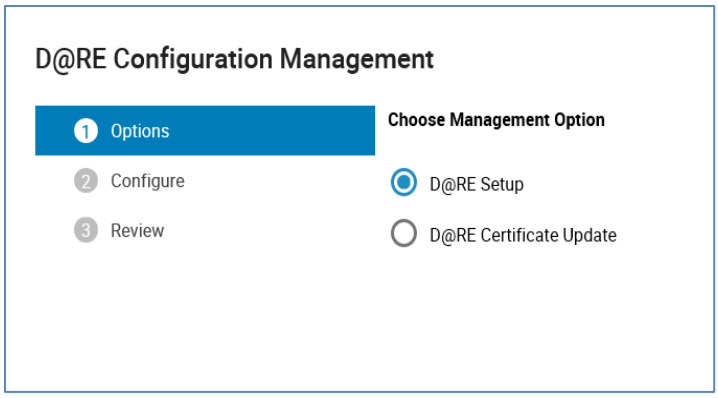

Figure 3 Unisphere D@RE Configuration Management wizard

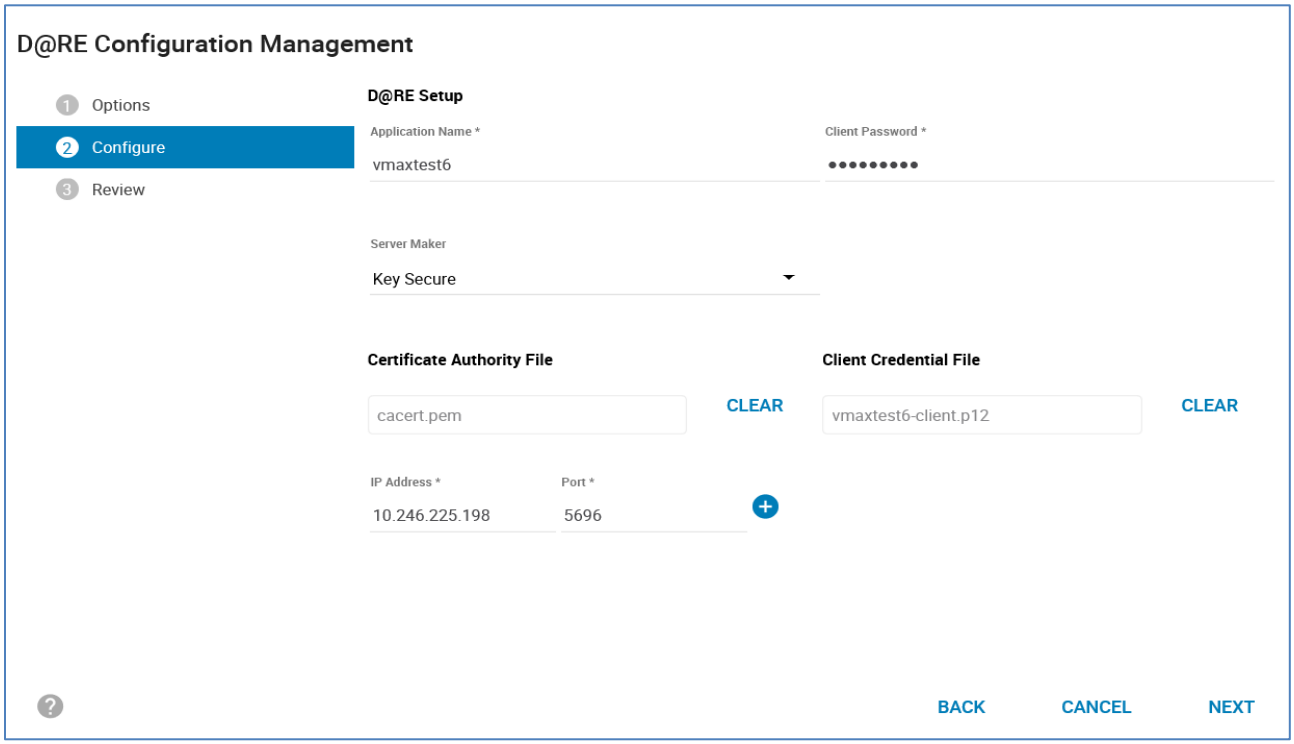

Figure 4 Unisphere D@RE external key manager setup

4 Operational examples

This section describes how Data at Rest Encryption works during common PowerMax and VMAX All Flash operations.

4.1 Installing a PowerMax and VMAX All Flash system

Once the PowerMax or VMAX All Flash system has been properly sized, D@RE can be enabled in the BIN file from Dell EMC Manufacturing or onsite prior to installation:

Note: If upgrading a currently installed system, work with your Dell EMC account team to submit a Request for Product Qualification (RPQ).

4.1.1 Installation with embedded key manager

1. Once the PowerMax or VMAX All Flash is at the site, Dell EMC field personnel begins the installation process.
2. The installation script automatically installs the RSA software on the primary MMCS.
3. The RSA Embedded Key Manager Server generates DEKs for each drive that is installed in the system and a KEK that is unique to that system.
4. PowerMaxOS generates an entry in the VMAX audit log for every key-generation event.
5. The RSA eDPM encrypts the keys and stores them in the local key repository file (lockbox) as non-volatile copies.
6. The RSA eDPM client wraps each DEK with the KEK, and PowerMaxOS stores all the keys on the system as encrypted, persistent backup copies.
7. PowerMaxOS initializes volumes using DEKs and writes any incoming host data to the drives as encrypted data.

4.1.2 Installation with external key manager

1. Once the PowerMax or VMAX All Flash is at the site, Dell EMC field personnel begins the installation process.
2. The Enterprise Key Server option is selected during the installation script.
3. The IP address, port number, certificate authentication information, and application registration name are provided either by Dell EMC field personnel or by the customer using the D@RE configuration management feature.
4. The script performs the following:

    a. Verifies the supplied server configuration information
    b. Verifies that the external key manager is correctly configured
    c. Asks the key manager to generate a KEK for the array and HMAC key
    d. Asks the key manager to generate a DEK for each drive
    e. Initializes the VMAX array with the D@RE objects and performs the rest of the generic initial configuration steps such as cable verification and VTOC
    f. Backs up the KTP client configuration details to the array for use during an MMCS replacement or during a PowerMaxOS non-disruptive upgrade

4.1.3 Migrating to external key manager

Existing D@RE-enabled arrays can migrate from embedded key management to an external key manager. However, an array running with an external key manager cannot be migrated back to embedded key management.

1. Dell EMC personnel begins the key migration script.
2. The IP address, port number, certificate authentication information, and application registration name are provided either by Dell EMC field personnel or by the customer using the D@RE configuration management feature.
3. The script performs the following:

    a. Verifies the supplied server configuration information
    b. Verifies that the external key manager is correctly configured
    c. Asks the key manager to generate a KEK for the array and HMAC key
    d. Asks the key manager to generate a DEK for each drive
    e. Backs up the KTP client configuration details to the array for use during an MMCS replacement or during a PowerMaxOS non-disruptive upgrade
    f. Populates the VMAX Audit Log with D@RE security events pertaining to this installation

4.2 Replacing a drive

In the event of a failed drive, the drive-replacement procedure completes as follows:

1. Dell EMC field personnel removes the failed drive from the system.
2. Once the drive has been removed from the array, the RSA eDPM server securely deletes the key from the key repository on the MMCS. If using an external key manager, the KTP client requests the KMIP server to securely delete the key.
3. After Dell EMC field personnel installs the new drive and PowerMaxOS verifies that the new drive is functional, the RSA eDPM server generates a new DEK for the drive and wraps the DEK using the KEK. For external key-manager configurations, the KMIP server generates a new DEK and returns it to the array to be wrapped with the KEK by the KTP client.
4. PowerMaxOS generates an entry in the audit log for the deletion of the old DEK and the creation of the new DEK.
5. PowerMaxOS caches the new DEK, which replaces the previous DEK.
6. PowerMaxOS rebuilds the drive data using the new DEK.

4.3 Vaulting with Data at Rest Encryption

PowerMax and VMAX All Flash arrays can encrypt data in cache during the vault process in the event the system is powered down. The vault image is encrypted and saved on the flash I/O modules. The back-end I/O modules running in loopback mode provide services to encrypt/decrypt the Power Vault image during vault operations. There is a unique DEK for each director board's set of flash I/O modules in the system, and flash DEKs are managed similar to normal drive DEKs.

Note: For more information on vaulting in PowerMax and VMAX All Flash arrays, see the Vaulting section of the Dell EMC PowerMax Reliability, Availability, and Serviceability Technical White Paper.

4.4 Decommissioning a PowerMax and VMAX All Flash system

This section describes how a PowerMax or VMAX All Flash array is decommissioned by a Dell EMC field personnel.

4.4.1 Decommission with embedded key manager

1. Dell EMC field personnel start the D@RE array decommission script.
2. The RSA eDPM server securely deletes all persistent copies of the keys in the key repository.
3. PowerMaxOS securely deletes the cached keys that are stored within the system, making the audit log irretrievable.
4. A certificate file is produced detailing the deletion of all keys during the decommissioning of the system.

4.4.2 Decommission with external key manager

1. Dell EMC field personnel start the D@RE array decommission script.
2. The KTP client instructs the KMIP external key manager server to securely delete each of the array's keys.
3. The system is taken offline.
4. All keys and authentication credentials are zeroed within the array.
5. A certificate file detailing the decommission results is produced on the MMCS.

5 Data at Rest Encryption considerations

The following options apply to D@RE for PowerMax and VMAX All Flash systems:

- Because D@RE can only be configured during initial install, the system needs to be properly sized and the D@RE flag set when the array is initialized at Dell EMC Manufacturing.
- Once the D@RE flag has been set, it cannot be disabled without the PowerMax or VMAX All Flash system being initialized again which will erase all data on the system.
- Mixing encrypted and unencrypted data on the system is not supported.

6 Summary

Data at Rest Encryption is an easy-to-use solution that keeps sensitive data safe from drive theft or loss by providing back-end encryption for the entire system. PowerMax and VMAX All Flash systems can utilize either the RSA Embedded Data Protection Manager or external key management using the standard OASIS KMIP protocol. Embedded key management allows the system to self-manage encryption keys, while external key management allows the end user to manage keys on an external management server for centralized key storage.

D@RE incorporates other important key management components such as Embedded Data Protection Manager, RSA BSAFE Cryptographic Libraries, and CST Secure Lockbox. PowerMax and VMAX All Flash also offer encryption during a vaulting operation in the event of a system power down, securing all data in cache to flash I/O modules. Through these components, D@RE offers Data Encryption Key protection, recovery and integrity to ensure all sensitive data is secure.

A Technical support and resources

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

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell EMC storage platforms.