Technical White Paper

# Dell EMC PowerProtect DD Series Appliances: Security


## Abstract

This document describes Dell EMC™ PowerProtect DD series appliance security options with the Dell EMC Data Domain™ Operating System (DDOS).



November 2020

# Revisions

| Date | Description |
|---|---|
| November 2020 | Updated for DDOS 7.3 release |
| | |

# Acknowledgments

Author: Vinod Kumar Kumaresan

# Table of contents

# Executive summary

Why Data Security?

Data Security is the most important consideration for any data protection environment providing protection against unauthorized access, modification, destruction, or disclosure and destruction including network security, physical security, and file security. Dell EMC understands the problems facing the modern data center and that it needs secured data management options.

This document provides an overview of key security features available with Dell EMC PowerProtect DD series appliance that ensures secure data protection and appropriate access control.

# Audience

This technical white paper is intended for Dell Technologies customers, partners, and employees. It describes the DD series security features, and details how they can be used to securely manage, protect, and recover data.

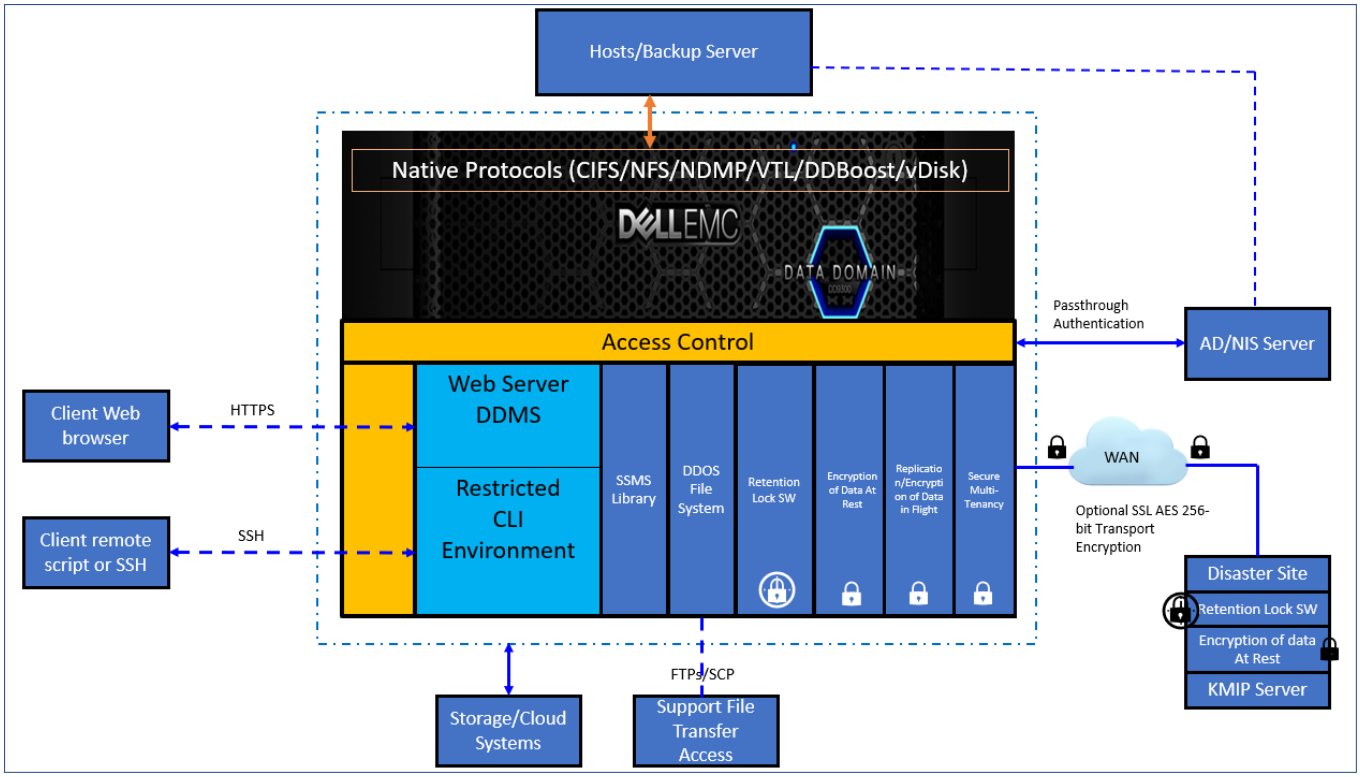
# 1 Introduction

**Dell EMC PowerProtect DD series appliances: Security**

DD series is an appliance that runs with embedded DDOS (Data Domain Operating System), additional software, or agents cannot be installed or executed within a system. This restriction ensures control, and consistency of DDOS releases and provides additional security over the system. DD series are purpose-built physical and virtual appliances with restricted access to their internal operation.

DD series as central repositories for both structured and unstructured backup data have many security capabilities and attributes to protect the data.

Hosts and backup applications interface with DD series appliance through one or more of the standard native server interface protocols: CIFS, NFS, NDMP, VTL and DD Boost. Access control and user authentication to the system is controlled by either local users, NIS environments, LDAP, or within a Microsoft Active Directory Domain environment.



# 2 Security Configuration Settings

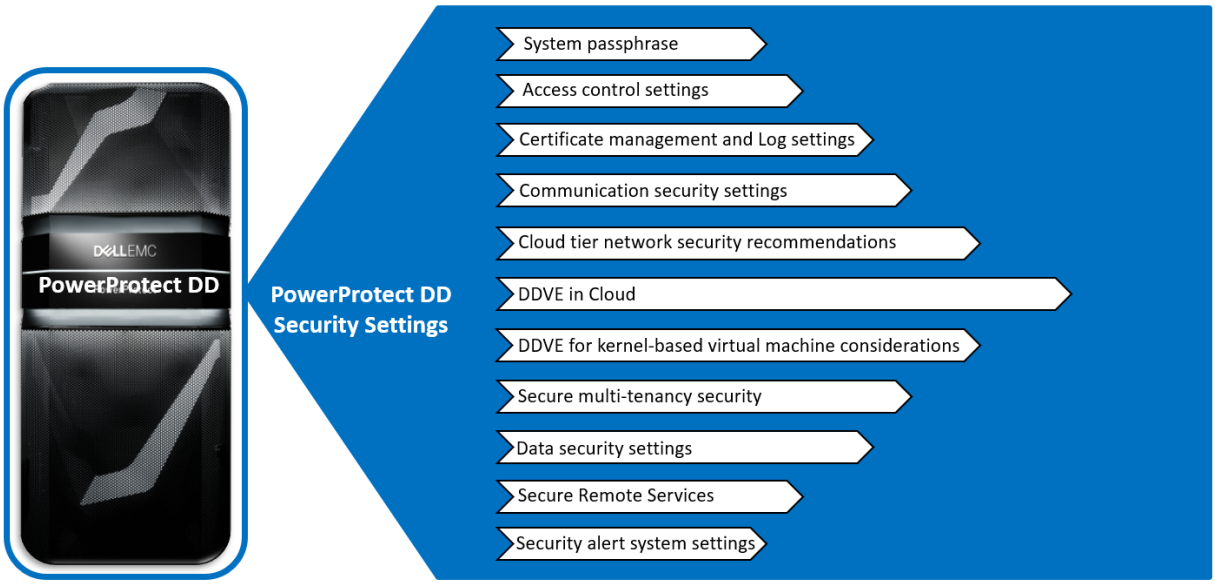



Figure 1 DD series security settings overview

## 2.1 System passphrase

The passphrase is used to encrypt the encryption keys, cloud access, secure keys, imported host certificate private keys, and DD Boost token keys. It enables a system to be transported with encryption keys on the system but without the passphrase being stored on it. The system uses the passphrase to encrypt imported host private keys and DD Boost token keys. If the system is stolen in transit, an attacker cannot easily recover the data, and at most, they can recover the encrypted user data and the encrypted keys.

Data at rest encryption keys are dependent on this passphrase, and therefore, the use of a stronger passphrase is mandatory.

DDOS supports passphrase up to 1024 characters.

DDMC only uses a passphrase for imported host certificate private keys

**Passphrase security**

The passphrase is encrypted and stored in a file on the head unit of the DD series. The encryption key that is used to encrypt the passphrase is hard coded.

## 2.2 Access control settings

Access control settings enable the protection of resources against unauthorized access.

**System access**

DD series operating environment provides secure administration through either the DD series System Manager by HTTPS or SSH for CLI. Either method enables locally defined users, Network Information Service (NIS) users, Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory (AD) domain users, and Single Sign-on (SSO).

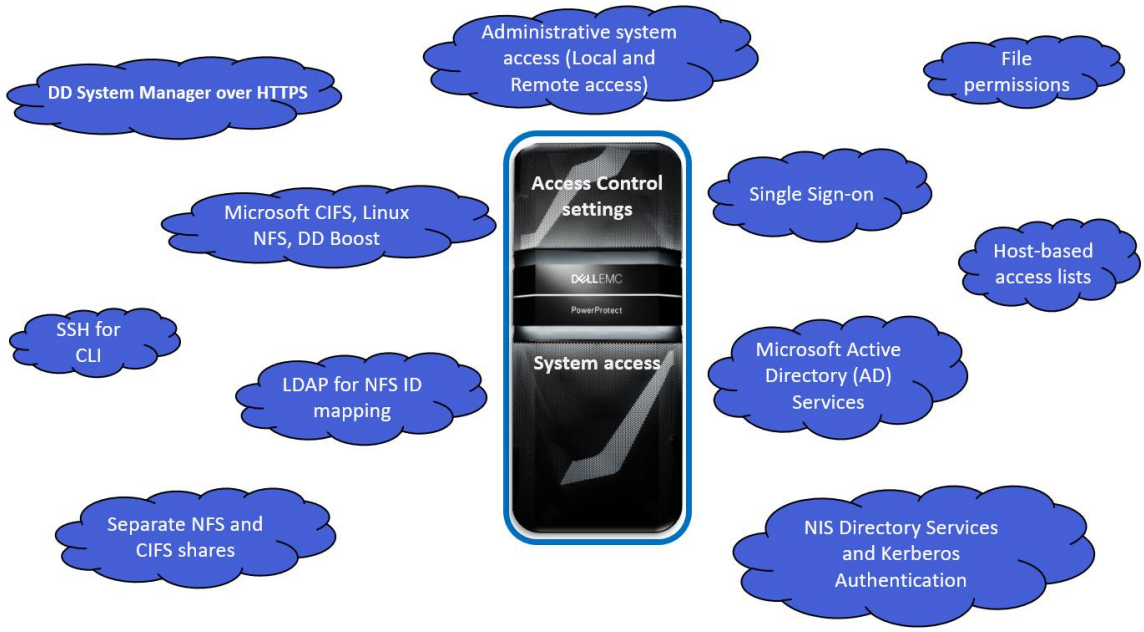



Figure 2 DD series – Access control settings

**User authentication**

User authentication settings control the process of verifying an identity claimed by the user for accessing the product.

**Default account** - The default user account is sysadmin. The account cannot be deleted or modified.

**Local users** - Additional accounts can be created after logging in as sysadmin, with admin-role or limited-admin user, user's role for an account, password, and account expiration parameters can be changed.

**Enabling, disabling, or deleting user accounts** - Local user accounts are enabled, disabled, or deleted by the system administrator

**Active Directory**

DD series systems can use Microsoft Active Directory pass-through authentication for the users.

**NIS**

DD series systems can use NIS Directory Authentication for the users in UNIX/LINUX environments for configuration management.

**LDAP**

DD series systems can use LDAP for user authentication. Users can also configure Secure LDAP with either LDAPS or Start_TLS method.

**Single Sign-on**

DD series systems can authenticate a user with a username and password from a supported Single Sign-on (SSO) provider. SSO feature must be enabled, and the system must be registered with an SSO provider.

**Login using certificates**

User certificate consisting of username is authenticated and authorized based on preexisting role mapping to login to DD System Manager from UI and REST.

**User authorization**

User authorization settings control rights or permissions that are granted to a user for accessing a resource that manages the product. Specific authorization levels are defined for each user account created using the Role-Base Access Control scheme listed below.

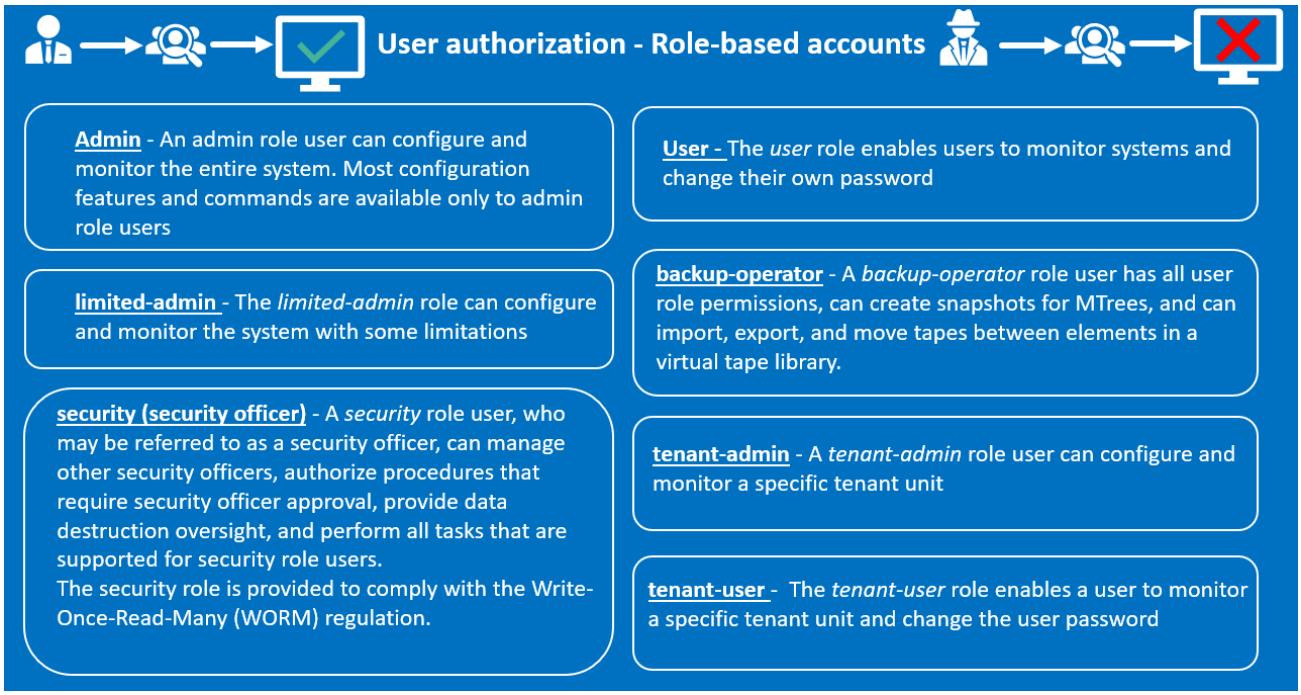



Figure 3 User authorization overview

## 2.3 Certificate management

DD series systems use certificates to securely communicate with following applications and protocols: HTTPS, external Key Manager (KMIP), DD Boost, LDAP server, Cloud tier (AWS, Azure, Alibaba Cloud, Google Cloud, ECS, AWS federal), and certificate-based user authentication and two factor authentication with a Common Access Card (CAC).

DD series systems use self-signed certificates to build mutual trust between another system for secure data replication. It supports two different secure configurations using certificate that is one-way and two-way authentication.

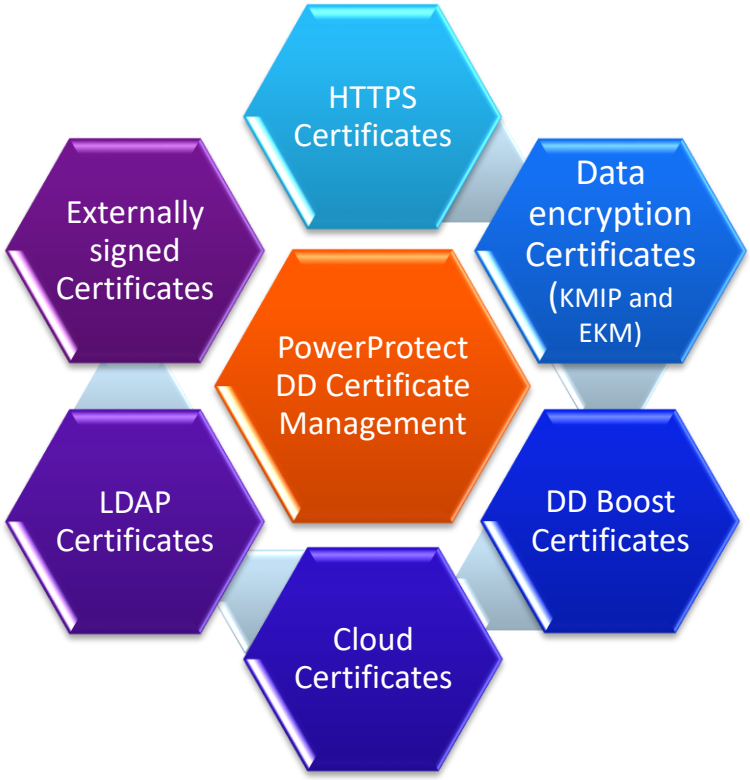



Figure 4 DD series certificate management overview

Managing DD series system with DDMC

To manage a DD series system, a trust needs to be established between DDMC and the system. A self-signed certificate is used to establish the trust.

**Cloud certificates**

To verify the identity of a cloud provider before backing up data from a system, the cloud providers have a host certificate that is issued by a CA. Import the CA certificate and any applicable CRLs before backing up any data to the cloud.

Certificate revocation list - Certificate revocation list (CRL) is PEM formatted file which is issued by a CA lists the revoked user certificate. Once this CRL file is imported to Data Domain System Manager, the revoked certificates are not enabled to log in. Online Certificate Status Protocol (OCSP) is not supported.

**DD Boost certificates**

DD Boost protocol can be used with or without externally signed certificates for encryption of data and authentication and was introduced to offer a more secure data transport capability.

In-flight encryption enables applications to encrypt in-flight backup or restore data over LAN from the system. When configured, the client can use TLS to encrypt the session between the client and the system. If TLS with certificates is used, then the specific suites that are used are DHE-RSA-AES128-SHA and DHE-RSA-AES256-SHA for medium and high encryption, respectively

**HTTPS certificates**

The system can use an imported certificate to establish a trusted connection to manage the system over SSL. If a certificate is not provided, the system can use its self-signed identity certificate.

**Data encryption certificates**

External CA and host certificates are required to set up SafeNet KeySecure Key Manager (KMIP). If encryption is enabled on Cloud Tier, only the DD series Embedded Key Manager (EKM) is supported.

**LDAP certificates**

LDAP for NFS ID mapping for folder and file permissions support secure LDAP using certificates.

**High Availability**

In a High Availability (HA) configuration, there are two controllers, where only one at a time is active, and are logically considered as a single file system.

- Both systems have the same Root Certificate Authority
- To establish mutual trust with the HA system, trust is required to be established with the active node ONLY
- Mutual trust, certificate signing request, and all the imported certificates on the active node are mirrored to the standby node
- Host certificate is generated per Active and Standby node and is used for HTTPS application. CA for secure support bundle upload is also kept per node

**Externally signed certificates**

Certificate authority (CA) is in public certificate (PEM) format to establish a trusted connection between the external entity and each system.

If the system or Cloud Tier uses the SafeNet KeySecure external key manager, it requires a PKCS12 host certificate and CA certificate in PEM (public key) format to establish a trusted connection between the SafeNet KeySecure Key Manager Server and each system that it manages.

The certificate signing requires PKCS10 format. The public certificate key can have either PKCS12 (public plus a private key) or PEM format. The host certificate PEM format is used only with the Certificate Signing Request (CSR) feature.

Individual host certificates can be imported for HTTPS and communication with SafeNet KeySecure Key Manager (KMIP). Importing the host certificate in PKCS12 format is supported. If there is a CSR on the system, host certificate can be imported in PEM format after the CSR is signed by a Certificate Authority.

On a FIPS enabled DD system, PKCS12 file must be FIPS-compliant. While encrypting PKCS12 file, compatible encryption algorithms must be used. We recommend using "PBE-SHA1-3DES" for encrypting key and certificate in PKCS12 file.

## 2.4 Log settings

A log is a chronological record of system activities that is necessary to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation,

procedure, or event from inception to results. All system logs (system, space, errors, access related) are stored on the root file system partition, and not accessible directly except through these services:

- Logs can be configured to send to a remote syslog server
- Authorized service personnel can copy logs to another system using FTP or SCP
- Some logs can be accessed using successful login using the CLI or the System Manager

The system log file entries contain messages from the alerts feature, auto support reports, and general system messages. The log directory is /ddvar/log.

### 2.4.1 Log descriptions

Log files can be bundled and sent to Dell EMC Support to provide the detailed system information that aids in troubleshooting any system issues that may arise. The DD series system logfile entries contain information from the alerts feature, auto support reports, bash scripts, and general system messages. Audit and secure logs are searchable by multiple parameters, such as username, string, authentication failure/successes, including tenant units.

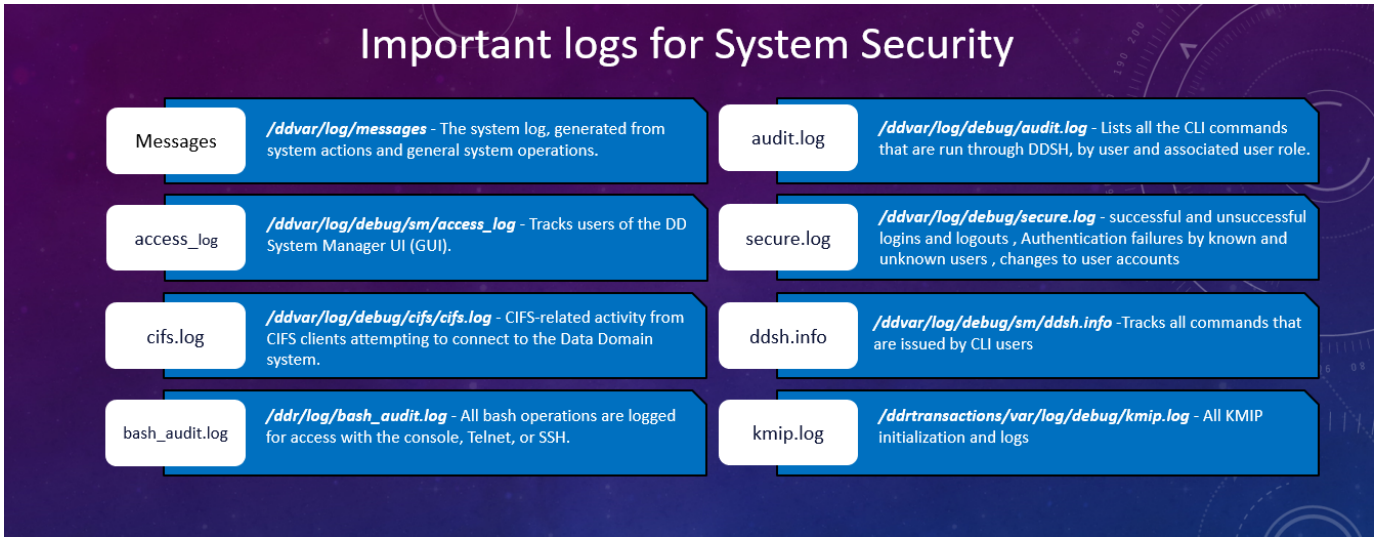



Figure 5 Important logs for system security

## 2.5 Communication security settings

Communication security settings enable the establishment of secure communication channels between the product components and between product components and external systems or components.

### 2.5.1 TCP and UDP ports

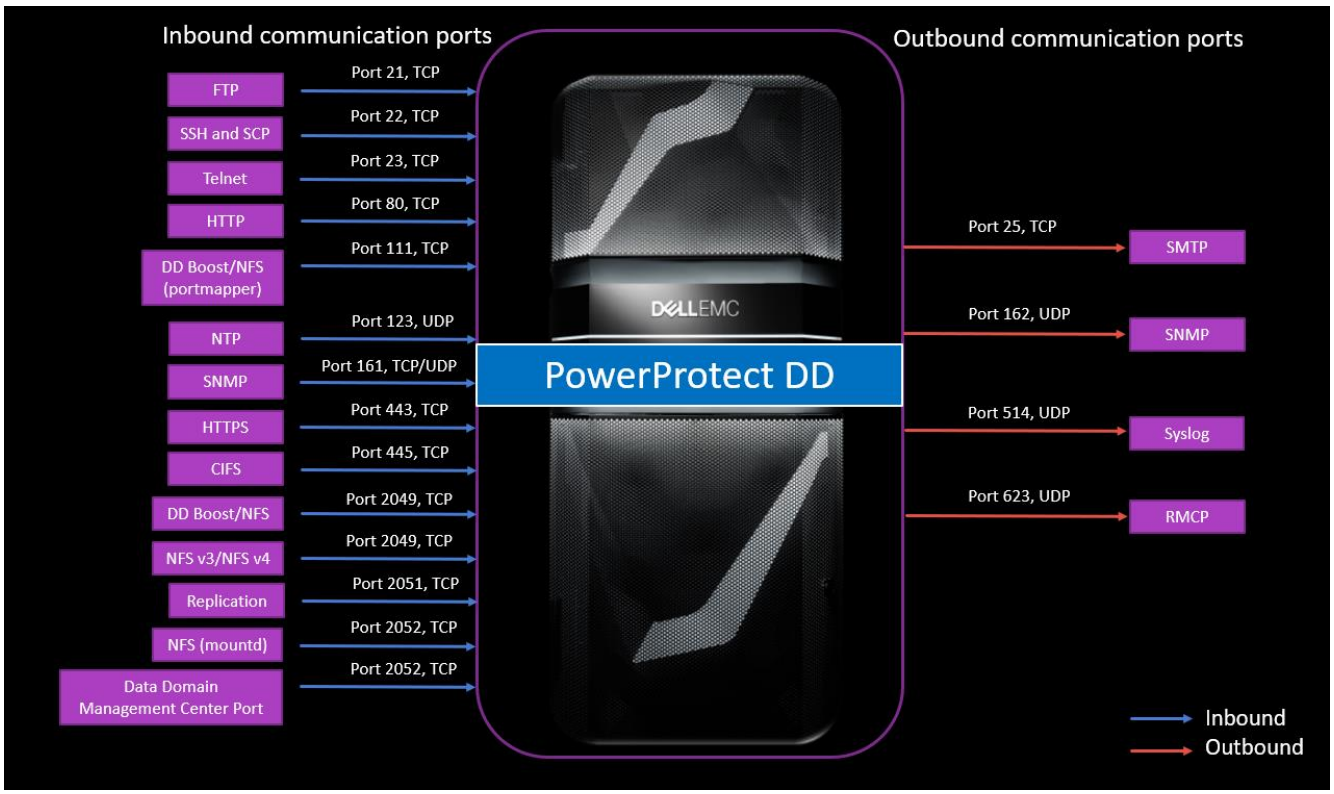



Figure 6 TCP and UDP ports overview

### 2.5.2 Active Directory ports

| Port | Protocol | Port configurable | Description |
|---|---|---|---|
| 53 | TCP/UDP | Open | DNS (if AD is the DNS as well) |
| 88 | TCP/UDP | Open | Kerberos |
| 139 | TCP | Open | Netbios/Netlogon |
| 389 | TCP/UDP | Open | LDAP |
| 445[1] | TCP/UDP | No | User authentication and other communication with AD |
| 3268 | TCP | Open | Global Catalog Queries |

## 2.6 Cloud tier network security recommendations

To verify the identity of a cloud provider before backing up data from DD series system, the cloud providers have a host certificate issued by a certificate authority (CA).

Kindly see Dell EMC PowerProtect DD – Security Configuration Guide for the recommended settings on securely connecting to cloud tier storage.

For enhanced security, the Cloud Tier feature uses:

- Signature Version 2 for Alibaba Cloud and Google Cloud requests
- Signature Version 4 for all AWS requests. AWS V4 signing is enabled by default

### 2.6.1 Certificates for cloud providers

Certificate authority (CA) certificates must be imported before adding cloud units for Alibaba Cloud, Amazon Web Services S3 (AWS), Azure, Elastic Cloud Storage (ECS), and Google Cloud Platform (GCP),

DD series system uses secure transport in all its communications with the public cloud providers and verifies the identity of the cloud provider. Each cloud provider has a host certificate that identifies the cloud provider and is issued by a CA.

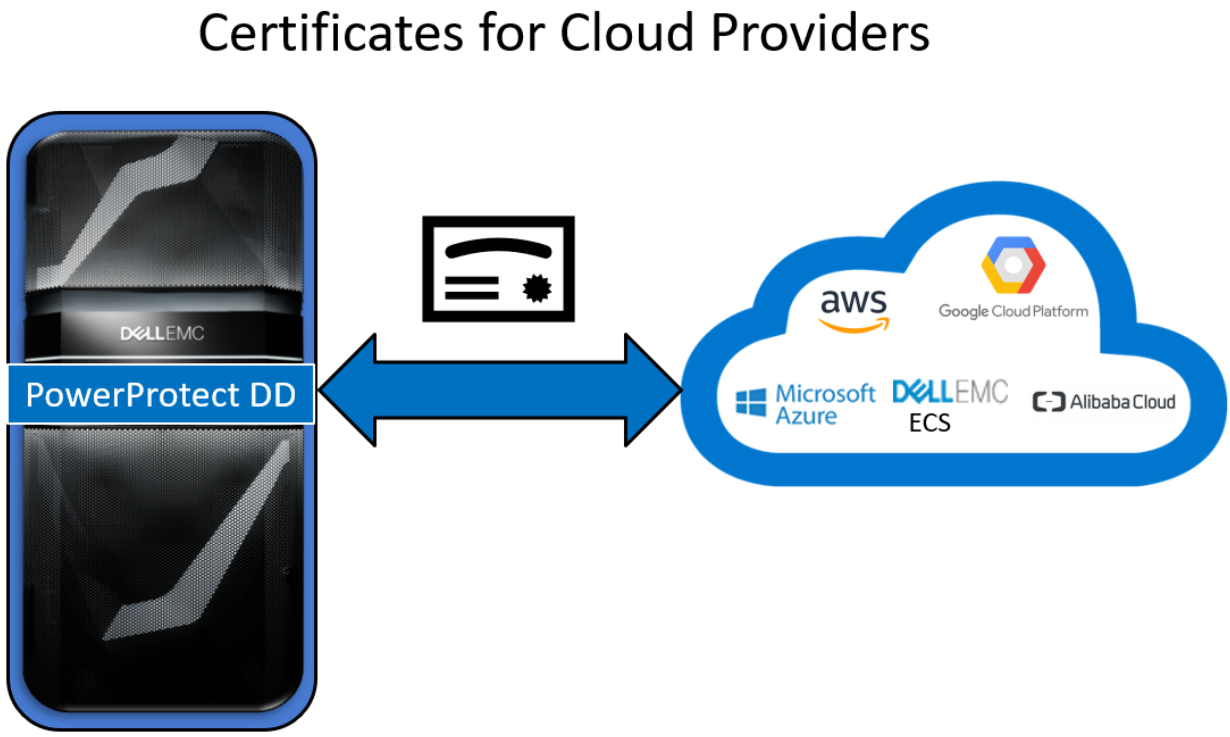



Figure 7 Certificates for Cloud Providers

Kindly see *Dell EMC PowerProtect DD – Security Configuration Guide* for the steps on how to download and import the CA certificate to the system.

## 2.7 DDVE in Cloud

The object store bucket or container that is created particularly for DDVE must not be shared with any other appliance or application. Sharing the bucket or container with other application or other DDVE could cause data loss and/or corruption.

### 2.7.1 Network security

DDVE in cloud solution is a backend service. DDVE must be deployed in a private subnet and must not be exposed using public IP address. Most of the public IP address spaces are under continuous attacks by hackers.

Appropriate security groups network access lists shall be configured to enable only intended traffic to DDVE. Open only the required ports. A complete list of DDVE ports and their usage can be found in the applicable DDVE Installation and Administration Guide.

## 2.8 DDVE for kernel-based virtual machine considerations

Security recommendations for DDVE running on Kernel-based Virtual Machine (KVM).

- Do not provide access to non-admin users for the DDVE deployed and related files or storage on the host
- The DDVE clock and the hypervisor host clocks must be synchronized with each other to ensure that the timestamps match

## 2.9 Secure multitenancy security

DD OS provides multiple security enhancements to enhance security for tenant administrators and tenant users.

**Unique tenant-unit hostnames**

A hostname that is configured for a tenant-unit cannot resolve to an IP address associated with another tenant-unit.

**Data access isolation**

Data access through the local IP addresses that are registered to a tenant-unit is restricted to the storage resources associated with that tenant unit. The following constraints apply to data access isolation:

- The local IP address for data access must exist on the system
- Existing IP addresses cannot be shared by multiple tenant-units
- IP ranges are not supported
- DHCP-assigned IP addresses are not supported

**Network firewall**

The system can restrict access from specific remote IP addresses to provide those clients with access to specific tenant-unit IP addresses.

The following constraints apply to the network firewall:

- Remote data-access IP addresses cannot be shared between multiple tenants
- Tenant exclusion checks are not performed for subnets or IP ranges

**Unique default gateways**

The system can route data from different tenants through different routers or gateways, with separate default gateways that are configured for each tenant-unit, and the tenant-unit IP addresses mapped to the gateways for their associated tenant-unit.

The following constraints apply to unique default gateways:

- Targeted default gateways, which are assigned to a specific interface, are supported with secure multitenancy (SMT)
- Static, added, or DHCP gateways are not supported with SMT
- A single default gateway cannot be shared between multiple tenants
- Unique gateways that are assigned to a tenant cannot be used by non-SMT entities on the system

## 2.10 Data security settings

Data security settings including data encryption enable controls that prevent data permanently stored by the product from being disclosed in an unauthorized manner.

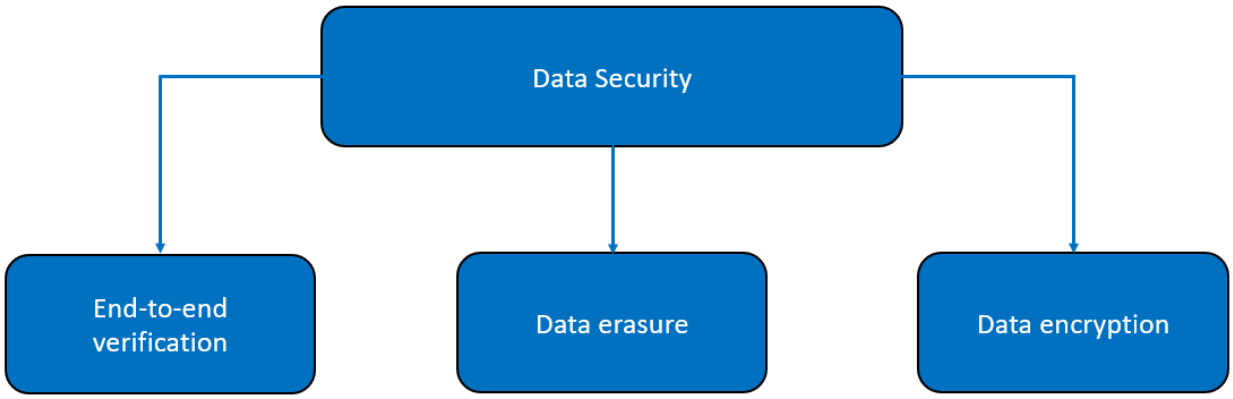



Figure 8 Data Security settings overview

### 2.10.1 Dell EMC DD Retention Lock software

DD Retention Lock software provides immutable file locking and secure data retention capabilities for customers to meet both corporate governance and compliance standards.

DD Retention Lock provides the capability for administrators to apply retention policies at an individual file level. This software enables customers to use their existing systems for backup and archive data. DD Retention Lock ensures that archive data is retained long term with data integrity and secure data retention.

DD Retention Lock Governance edition and DD Retention Lock Compliance edition can co-exist on the same system to enable different retention periods for different classes of archive data. DD Retention Lock software is compatible with industry-standard, NAS-based (CIFS, NFS) Write-Once-Read-Many (WORM) protocols and is qualified with leading archive applications such as EMC SourceOne, EMC DiskXtender, and Veritas Enterprise Vault.

**Dual sign-on requirement**

When DD Retention Lock Compliance is enabled, additional administrative security is provided in the form of “dual” sign-on. This requirement involves a sign-on by the system administrator and a sign-on by a second authorized authority (the “Security Officer”). The dual sign-on mechanism of the DD Retention Lock Compliance edition acts as a safeguard against any actions that could potentially compromise the integrity of locked files before the expiration of the retention period.

**Secure system clock**

DD Retention Lock Compliance implements an internal security clock to prevent malicious tampering with the system clock. The security clock closely monitors and records the system clock. If there is an accumulated two-week skew within a year between the security clock and the system clock, the file system is disabled and can be resumed only by a security officer.

On Retention Lock Compliant DD systems, system time can be modified only within certain restrictions set by date-change-limit and date-change-frequency.

### 2.10.2 Data integrity

- The DD OS Data Invulnerability Architecture™ protects against data loss from hardware and software failures
- When writing to disk, the DD OS creates and stores checksums and self-describing metadata for all data received. After writing the data to disk, the DD OS then recomputes and verifies the checksums and metadata
- An append-only write policy guards against overwriting valid data
- After a backup completes, a validation process examines what was written to disk and verifies that all file segments are logically correct within the file system and that the data is identical before and after writing to disk
- In the background, the online verification operation continuously checks that data on the disks is correct and unchanged since the earlier validation process

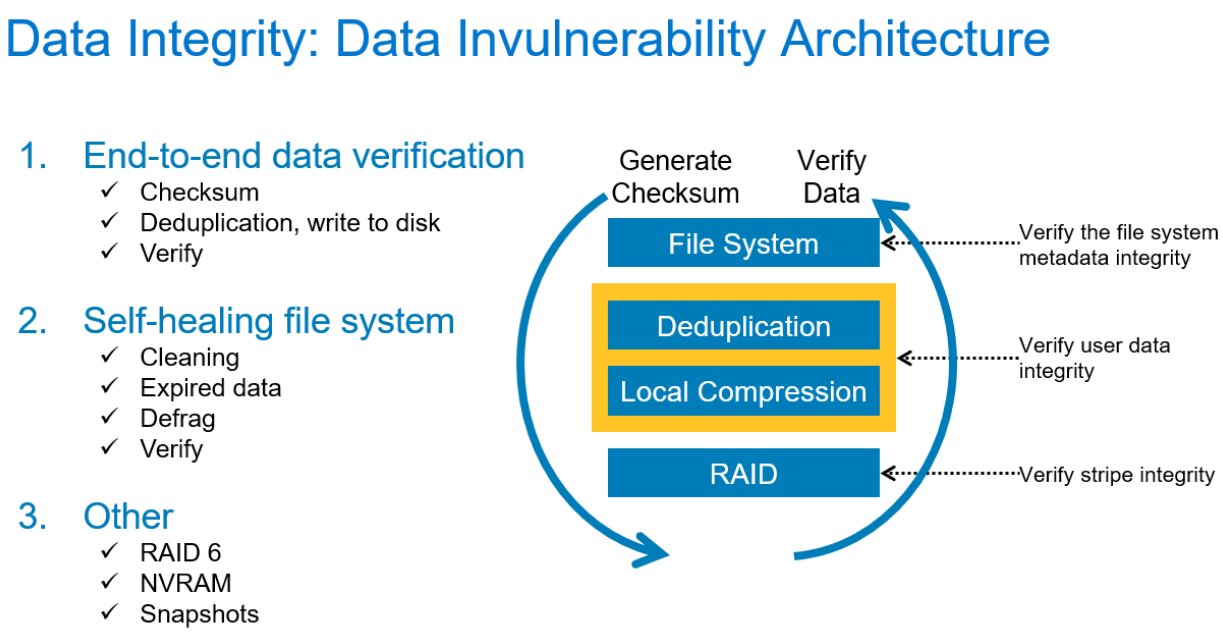



Figure 9 Data Invulnerability Architecture overview

Storage in most systems is set up in a double-parity RAID 6 configuration (two parity drives). Also, most configurations include a hot spare in each enclosure, except in certain low-end series systems, which have eight or fewer disks. Each parity stripe has block checksums to ensure that data is correct. Checksums are constantly used during the online verification operation and while data is read from the system. With double parity, the system can fix simultaneous errors on as many as two disks.

To keep data synchronized during a hardware or power failure, the system uses NVRAM (nonvolatile RAM) to track outstanding I/O operations. An NVRAM card with fully charged batteries (the typical state) can retain data for hours, which is determined by the hardware in use. When reading data back on a restore operation, the DD OS uses multiple layers of consistency checks to verify that restored data is correct.

DD series systems support SNMP V2C and/or SNMP V3. SNMP V3 provides a greater degree of security than V2C by replacing cleartext community strings as a means of authentication with user-based authentication using MD5, SHA1, or SHA-256.

Multiple layers of data verification are performed by the DD OS file system on data that is received from backup applications to ensure that data is written correctly to the system disks. This process ensures that the data can be retrieved without error. The DD OS is purpose-built for data protection, and it is architecturally designed for data invulnerability. There are four critical areas of focus, described in the following sections: end-to-end verification, data erasure, system sanitization, and data encryption.

**End-to-End verification**

End-to-end checks protect all file system data and metadata.

As data comes into the system, a strong checksum is computed. The data is deduplicated and stored in the file system. After all data is flushed to disk, it is read back, and re-check summed. The checksums are compared to verify that both the data and the file system metadata are stored correctly.

### 2.10.3 Data erasure

The filesys destroy command deletes all data in the file system. The file system can be destroyed using the DD System Manager.

**System sanitization**

System sanitization was designed to remove all traces of deleted files and restore the system to the previous state. The primary use of the sanitize command is to resolve Classified Message Incidents (CMIs) that occur when classified data is copied inadvertently onto a non-secure system. System sanitization is typically required in government installations. Sanitization is not supported with SSD cache tier. Use the storage remove and storage add commands to remove the logical to physical mapping. This action ensures that physical pages not to return previous written data. However, the previously written data may still be on SSD.

### 2.10.4 Data encryption

There are three types of encryption offered with DD series systems.

They are:

- Inline Encryption of data at rest using the DD Encryption software option
- Encryption of data in flight using DD Replicator software, which is used for replicating data between sites over the WAN
- Encryption of data in flight using DD Boost software, using Transport Layer Security (TLS)

### 2.10.4.1 Inline Encryption of data at rest using the DD Encryption Software option

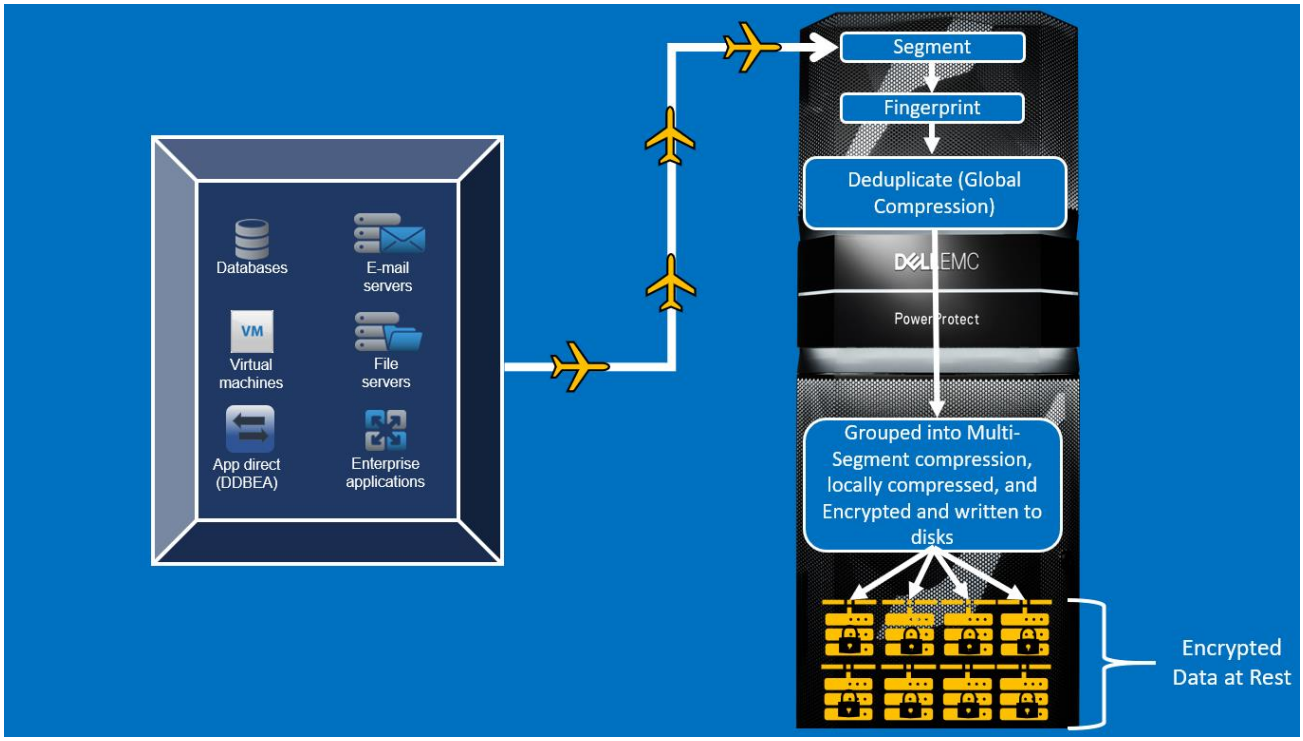



Figure 10 Inline Encryption overview

### 2.10.4.2 Encryption of data in flight using DD Replicator software

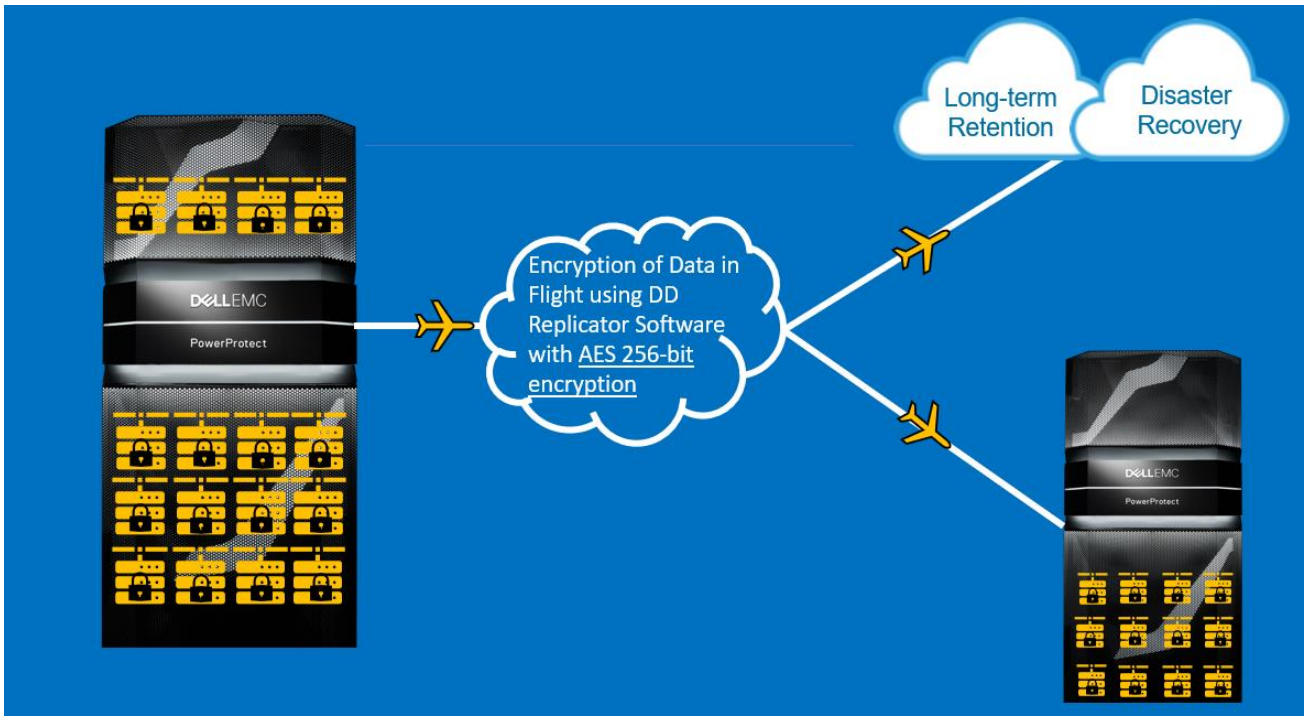



Figure 11 Encryption of data in flight using DD Replicator overview

### 2.10.4.3 Encryption of data in flight through DD Boost

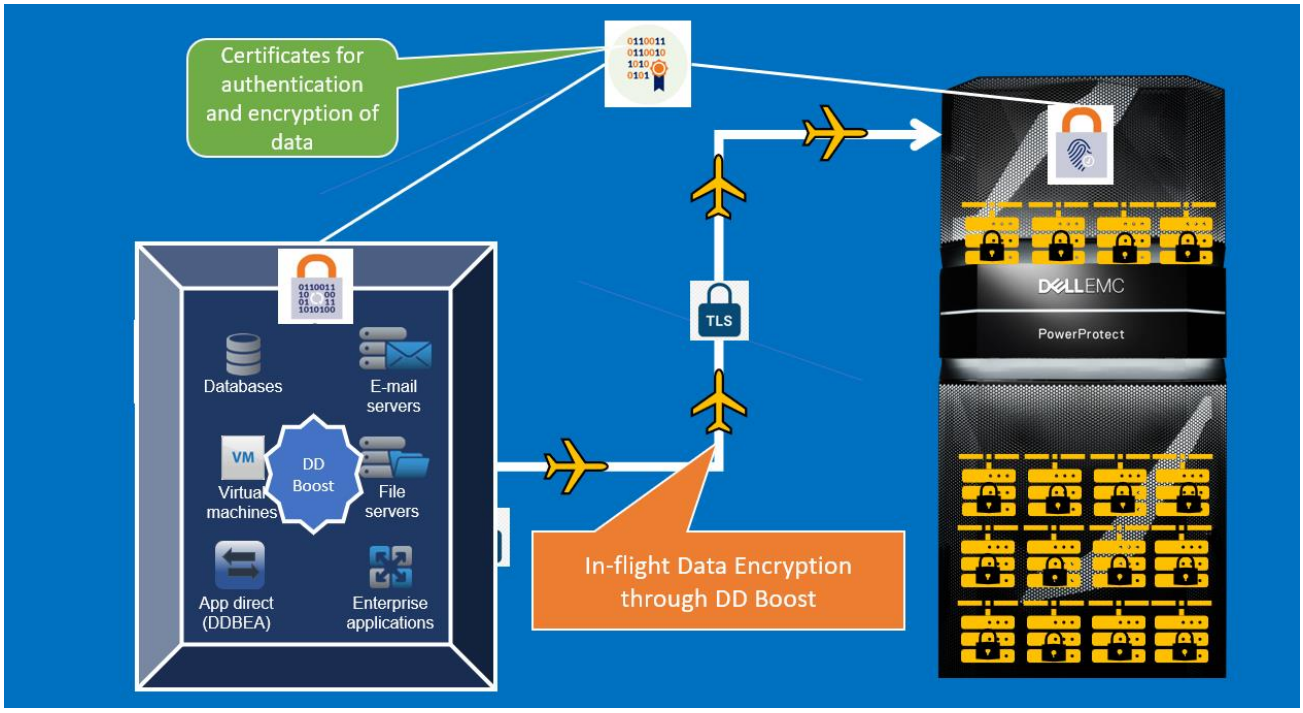



Figure 12 Encryption of data in flight through DD Boost

## 2.11 Secure Remote Services

Secure Remote Services is an IP-based automated connect home and remote support solution and creates both a unified architecture and a common point of access for remote support activities that are performed on the product. The Secure Remote Services IP Solution does the following:

- Provides continuous monitoring, diagnosis, and repair of minor hardware issues
- Uses the most advanced encryption, authentication, audit, and authorization for ultra-high security remote support
- Addresses compliance with corporate and governmental regulations by providing logs of all access events
- Provides easy integration and configuration with the storage management network and firewalls
- Provides maximum information infrastructure protection. IP-based sessions enable fast information transfer and resolution
- Consolidates remote support for the information with the Secure Remote Services Gateway Client
- Provides remote access to the disaster recovery site and makes recovery from unplanned events seamless
- Protects information in motion or at rest. AES 256 encryption during information transfer protects the information
- Reduces costs and data center clutter and accelerates time to resolution. The elimination of modem/phone line costs translates to lower costs

## 2.12 Security alert system settings

System operation can be monitored with a variety of DD System Manager tools: reporting tools that automatically send emails containing status and alerts, log files that contain a record of important system events, and SNMP monitoring using third-party SNMP managers.

Automatic logging and reporting tools that provide system status to Dell EMC Support and designated email recipients are important in monitoring system operation. Their setup and use are described in this chapter.

Alerts are also sent as SNMP traps. See the DD OS MIB Quick Reference for the full list of traps.

**Securing data in flight**

Data can be vulnerable to man-in-the-middle (MITM) attacks when the attacker can impersonate an endpoint. DD series use self-signed certificates to build mutual trust between another system for secure data replication. It supports two different secure configurations using certificate that is one-way and two-way authentication.

DD OS supports one-way and two-way authentication between the replication source and destination to provide additional security for replication operations.

DD Boost also supports two-way authentication using pre-shared keys (PSK), which does not require certificates. Various applications may support one or more methods of two-way authentication depending on the application and the protocol (such as DD Boost).

**FIPS configuration**

The DD file system, SMS, Apache HTTP service, LDAP client, and SSH Daemon use FIPS 140-2 compliant algorithms when FIPS is enabled.

DD OS uses FIPS certified libraries including Dell OpenSSL Cryptographic Library, BSafe, Crypto J, Cert-J, and SSL-K.

**System hardening and best practices**

The hardening process is twofold. Traditionally, customers that are looking to harden a system are doing so because they are either under mandate or are practicing secure computing practices.

Kindly see Dell EMC DD OS Version 7.3 Security Configuration Guide for the hardening procedures and the mitigation steps that comply with federal Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) on the device.

# 3 Physical Security Controls

**Physical controls**

Physical security controls enable the protection of resources against unauthorized physical access and physical tampering.

The DS60 has a disk drive locking mechanism that prevents the removal of a disk drive without the appropriate tool, which is a T10 Torx screwdriver. The bezel on the ES30, ES40, FS15, and FS25 has a lock and key that prevents access to the drives.

DD3300, DD6300, DD6800, DD6900, DD9300, DD9400, and DD9900 systems have ES30-style bezels.

DD9800 systems have a lock and a key, which prevents access to the drives

**Baseboard management controller and basic input/ output system recommendations**

Recommended baseboard management controller (BMC) and basic input/output system (BIOS) security practices.

- Always flash the latest BMC and BIOS images as they are released even if the release notes do not explicitly state a security fix.
- Use the Administrator Password in BIOS setup.
- Use strong passwords for IPMI user accounts and BIOS administrator password.
- Set up an isolated network for manageability and never expose that network to the internet.
- If using onboard NICs for manageability is required, configure VLANs to isolate it from the host network

**General USB security best practices**

1. Prohibit booting from USB (or any device other than the hard disks) in BIOS
2. Disable the USB ports completely in BIOS (if possible)
3. Setting a password in BIOS

**General operations for disabling USB and password setup in BIOS**

1. Disabling USB in BIOS
2. Setting BIOS password
3. Clearing BIOS password

**Securing Integrated Dell Remote Access Controller 9 (iDRAC)**

**iDRAC features**

**iDRAC provides user with the following features:**

- Monitors server health
- Remotely power on, off, or cycle system
- Provides view of system inventory

Kindly see chapter 4 - Physical Security Controls in Dell EMC DD OS Version 7.3 Security Configuration Guide for more details on iDRAC hardening.

# A Technical support and resources

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

Storage and data protection technical white papers and videos provide expertise that helps to ensure customer success with Dell EMC storage and data protection products.

## A.1 Related resources

- Dell EMC PowerProtect DDOS Admin Guide
- Dell EMC DD OS Version 7.3 Administration Guide
- Dell EMC PowerProtect DDOS Admin Guide
- Dell EMC DD OS Version 7.3 Security Configuration Guide