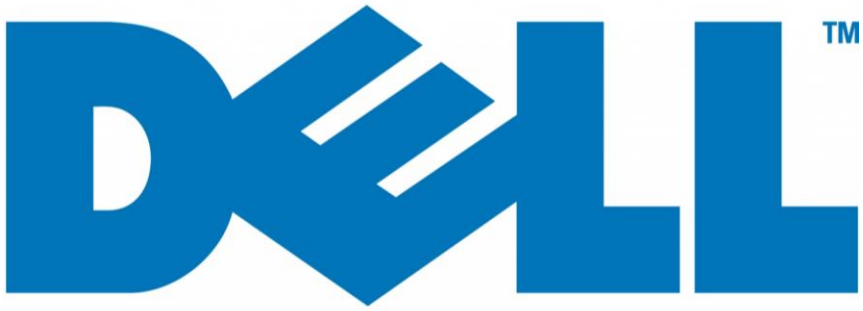

ECS v3.8.0.3

Security Target

Version 1.4

November 2023

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Description
0.1	9 June 2022	Initial draft
0.2	25 July 2022	Incorporated developer comments. Initial draft issued for evaluation.
0.3	11 October 2022	Addressed evaluator ORs.
0.4	18 October 2022	Addressed evaluator ORs.
1.0	15 March 2023	Addressed CB ORs. Updated TOE version and guidance references.
1.1	01 May 2023	Address CB OR
1.2	16 October 2023	Addressed evaluator ORs.
1.3	6 November 2023	Addressed CB ORs.
1.4	14 November 2023	Updated AGD version.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Dell ECS v3.8.0.3 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The Dell ECS v3.8.0.3 is a software-defined storage platform that supports the storage, manipulation, and analysis of unstructured data on commodity hardware. ECS is specifically designed to support mobile, big data, and social networking applications. It is deployed as a turnkey storage appliance using qualified commodity servers and disks. ECS provides object and file user access to stored data.

3 At a high level ECS is composed of the following main components:

a) ECS Portal and Provisioning Services – provides a Web-based portal that allows self-service, automation, reporting and management of ECS nodes. It also handles licensing, authentication, and provisioning services.

b) Data Services – provides services, tools and Application Programming Interfaces (APIs) to support Object and Network File System (NFS) version 3.

c) Storage Engine – responsible for storing and retrieving data, managing transactions, and protecting and replicating data.

d) Fabric – provides clustering, health, software, and configuration management as well as upgrade capabilities and alerting.

e) Infrastructure – uses SUSE Linux Enterprise Server (SLES) 12 SP4 as the base operating system.

f) Hardware – the hardware is provided as a turnkey appliance made up of industry standard hardware components.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Dell ECS v3.8.0.3.138685.3a0a9b6bf3a running on the EX500 Hardware
Security Target	Dell ECS v3.8.0.3 Security Target, v1.4

1.3 Conformance Claims

4 This ST supports the following conformance claims:

- CC version 3.1 Release 5
- CC Part 2 extended
- CC Part 3 conformant
- EAL2+ ALC_FLR.2

1.4 Terminology

Table 2: Terminology

Term	Definition
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
ARM	Advanced Retention Management
CAVP	Cryptographic Algorithm Validation Program
CAS	Content Addressed Storage
CC	Common Criteria
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
D@RE	Data at Rest Encryption
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
HDFS	Hadoop Distributed File System
OSP	Organizational Security Policy
PEA	Pool Entry Authorization
PP	Protection Profile
SFR	Security Functional Requirement
SLES	SUSE Linux Enterprise Server
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VDC	Virtual Data Centre

2 TOE Description

2.1 Type

5 The TOE is a software and hardware TOE.

2.2 Deployment

6 The building blocks of the TOE deployment include:

7 **Virtual Data Centre (VDC)**. A VDC is a geographical location defined as a single ECS deployment within a site.

8 **Storage Pool**. A storage pool can be thought of as a subset of nodes and its associated storage belonging to a VDC. An ECS node can belong to only one storage pool; a storage pool can have any number of nodes with the recommended minimum being five. A storage pool can be used as a tool for physically separating data belonging to different applications.

9 **Replication Group**. Replication groups define where storage pool content is protected and locations from which data can be read or written. Local replication groups protect objects within the same VDC against disk or node failures.

10 **Namespace** - A namespace, which is conceptually the same as a “tenant,” is a logical construct. The key characteristic of a namespace is that users from one namespace cannot access objects belonging to another namespace. Namespaces can represent a department within an organization or a group within a department.

11 **Buckets**. Buckets are containers for object data. Buckets are created in a namespace to give applications access to data stored within ECS. In S3, these containers are called “buckets” and this term has been adopted by ECS. In Atmos, the equivalent of a bucket is a “subtenant”, and for Content Addressed Storage (CAS), a bucket is a “CAS pool”. Buckets are global resources in ECS. In a single site, storage pools are defined, then the VDC is created with namespaces and buckets.

12 The TOE deployment is shown in Figure 1.

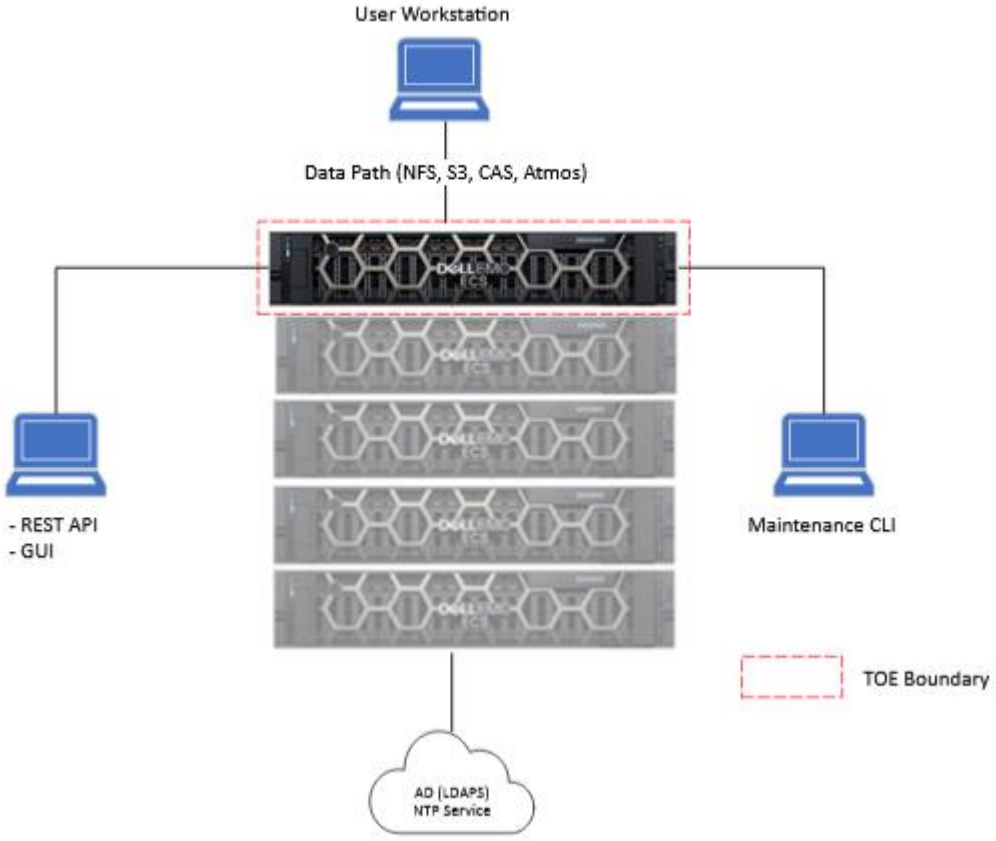

Figure 1: TOE Deployment

2.3 Logical Scope

13 The logical scope of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 5. Table 3 summarizes the logical scope of the TOE.

Table 3: Logical Scope of the TOE

Functional Class	Description
Security Audit	Audit entries are generated for security related events. The audit logs may be filtered and reviewed by authorized administrators. Failure events are monitored, and an alert is presented to the administrator where human intervention may be required.
Cryptographic Support	Cryptographic key generation and key destruction functionality and cryptographic operation support Data at Rest (D@RE) encryption of stored user information. ECS uses the RSA BSAFE® Crypto-J JSAFE and JCE Software Module (Software Version: 6.2.5) module, Cryptographic Module Validation Program (CMVP) certificate number 3819. The vendor affirms that no source code

Functional Class	Description
	changes were made to the cryptographic module prior to recompilation into the TOE software.
User Data Protection	User authentication and access control list (ACL) information associated with data is evaluated to determine if a user is permitted to access requested data. The TOE ensures the integrity of stored data. A retention period can be associated with data objects. Data may not be deleted until the retention period expires.
Identification and Authentication	Both Data path users and Management path/maintenance users must identify and authenticate prior to gaining TOE access.
Security Management	The TOE provides management capabilities via a REST API and a web-based GUI. Management functions allow the administrators to review audit records, configure storage options, and configure users and roles.
Protection of the TSF	The TOE protects user data against disk and node failure. Reliable time stamps are provided for audit records.
Resource Utilization	Read and write access is maintained in the case of limited failures.
TOE Access	Management path users may initiate logout, or will be logged out automatically after a configurable period of inactivity.
Trusted path/channels	Communications between the TOE and remote administrators, and between the TOE and an external LDAP server are protected using TLSv1.2.

2.4 Physical Scope

14 The physical boundary of the TOE is the Dell ECS v3.8.0.3 software running on the EX500 hardware appliance.

2.4.1 TOE Delivery

15 The component parts of an ECS node are assembled, loaded with the operating system, and placed in a rack. The rack is then packaged and delivered to the customer site using a trusted courier service.

16 Once the hardware has been received, an ECS professional services representative assembles the hardware in the rack, and then downloads, installs, and configures the TOE software at the customer site.

2.4.2 TOE Guidance

17 The following guidance documentation is provided to customers online in Portable Document Format (PDF):

- ECS 3.8 Administration Guide, April 2023

  https://dl.dell.com/content/manual52394679-ecs-3-8-administration-guide.pdf?language=en-us&ps=true

- ECS 3.8 Security Configuration and Hardening Guide, June 2023

  https://dl.dell.com/content/manual26095053-ecs-3-8-security-configuration-and-hardening-guide.pdf?language=en-us&ps=true

- ECS 3.8 Data Access Guide, April 2023

  https://dl.dell.com/content/manual53094723-ecs-3-8-data-access-guide.pdf?language=en-us&ps=true

- ECS EX Series Hardware Guide, April 2023

  https://dl.dell.com/content/manual51504581-ecs-3-7-ex-series-hardware-guide.pdf?language=en-us&ps=true

- EMC Centera SDK Version 3.3, API Reference Guide, July 2012

  https://dl.dell.com/content/docu41502_centera-sdk-3-3-api-reference-guide.pdf?language=en-us

18 The following guidance is downloaded as a ZIP file and accessed by customers in HTML format (web browser):

- Dell Technologies ECS REST API v3.8.0.2.138627.f5f4887, 2022

  https://dl.dell.com/downloads/9PKFR_ECS_3.8_REST_API-Reference.zip

19 The TOE also includes the following Common Criteria Guide, provide as a PDF, and available to customers upon request:

- Dell_ECS_EAL2_AGD_1.3.pdf

20 **Note**: Any guidance referencing an older version of the TOE (i.e. ECS 3.8.0.2) is applicable to the claimed TOE version, Dell ECS 3.8.0.3.

2.4.3 Non-TOE Components

21 The TOE operates with the following components in the environment.

Table 4: Non-TOE Components

Component	Software	Hardware
Management Path	Windows 10 This machine supports the applications required to support the Management path options: • Management REST API – PuTTy • Management Graphical User Interface (GUI) – Chrome Browser	General purpose computer hardware
Maintenance	Windows 10 This machine supports an SSH Client to access the Command Line Interface (CLI) for TOE installation	
Data Path Access (User Workstation)	SLES 12 SP4 This machine supports all of the applications required to exercise the Data path options: • NFS Client • S3 – S3Curl • Atmos – AtmosCurl • CAS – CenteraExerciser	
Domain Controller	Windows Server 2019 with Active Directory This server supports LDAP authentication for Management path users	
NTP Server	Provides the NTP service for the TOE to leverage for producing reliable time stamps on audit records and determining retention expiry dates	

2.4.4 Excluded Functionality

22 The following features are excluded from this evaluation:

a) Hadoop Distributed File System (HDFS) user access to stored data

b) Transfer of audit records to a syslog server

c) Advanced Retention Management (ARM)

d) Geo-Federation and Geo-Replication (Multi-site deployment)

23 The CLI is used only during installation in the evaluated configuration and then locked by ECS professional services.

3 Security Problem Definition

3.1 Threats

Table 5: Threats

Identifier	Description
T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.LOSS	A network or hardware failure could result in temporary or permanent loss of user data.
T.UNAUTH	A hostile/unauthorized user could gain access to stored data by bypassing the protection mechanisms of the TOE.
T.UNDETECT	Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.

3.2 Assumptions

Table 6: Assumptions

Identifier	Description
A.AUTH	The operational environment provides authentication services to the TOE in support of access control decisions.
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical and logical access.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

3.3 Organizational Security Policies

Table 7: Organizational Security Policies

Identifier	Description
P.CRYPTO	The TOE shall incorporate cryptographic mechanisms to protect against potential disclosure of the data it has been entrusted to store.
P.RETAIN	The TOE shall provide a means to identify a retention period before which data is not to be deleted, and prevent data from being deleted prior to the expiry of the retention period.

4 Security Objectives

4.1 Objectives for the TOE

Table 8: Security Objectives

Identifier	Description
O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions and must ensure that only authorized administrators are able to access such functionality.
O.AUDIT	The TOE must provide a means of logging security related events, and a means of filtering and viewing those events. The TOE must alert administrators to failure events that could compromise the availability of data to users.
O.CRYPTO	The TOE must provide cryptographic functions to support encryption of data at rest.
O.IDAUTH	The TOE must ensure that users are identified and authenticated prior to allowing access to data or administrative functions.
O.INTEGRITY	The TOE must protect the data that it has been entrusted to store from integrity errors due to node or disk failure.
O.PROTCOMMS	The TOE shall provide protected communication channels for remote administrators and management user authentication requests.
O.PROTECT	The TOE must protect the data that it has been entrusted to store from unauthorized access.
O.RETAIN	The TOE must prevent the deletion of data prior to expiry of the assigned retention period.
O.TIME	The TOE must provide reliable time stamps.

4.2 Objectives for the operational environment

Table 9: Objectives for the operational environment

Identifier	Description
OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to the enforcement of security are protected from any physical and logical attack.
OE.SERVICE	The operational environment shall provide an Active Directory server to provide authentication services.

5 Security Requirements

5.1 Conventions

24 This document uses the following font conventions to identify the operations defined by the CC:

- **Assignment.** Indicated with italicized text.
- **Refinement.** Indicated with bold text or strikethroughs.
- **Selection.** Indicated with underlined text.
- **Assignment within a Selection:** Indicated with italicized and underlined text.
- **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

5.2 Extended Components Definition

25 Table 10 identifies the extended components which are incorporated into this ST.

Table 10: Extended Components

Component	Title	Rationale
FDP_RET_EXT.1	Retention of data	No existing CC Part 2 SFRs addresses retention requirements for stored data. A new family was created within the User Data Protection (FDP) class to address the retention of data.

5.2.1 Retention of data (FDP_RET_EXT.1)

5.2.1.1 Family Behavior

26 This family provides requirements that address retention of user data while it is stored within containers controlled by the TOE Security Functionality (TSF).

5.2.1.2 Component Leveling

5.2.1.3 Management: FDP_RET_EXT.1

27 The following actions could be considered for the management functions in FMT:

- Setting the retention period.

5.2.1.4 Audit: FDP_RET_EXT.1

28 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: changes to the retention period.

FDP_RET_EXT.1 Retention of data

Hierarchical to: No other components.

Dependencies: FPT_STM.1

FDP_RET_EXT.1.1 The TSF shall allow a retention period to be assigned to user data.

FDP_RET_EXT.1.2 Where a retention period has been assigned to data, the TSF shall deny requests to delete the data until the retention period has expired, or has been removed.

5.3 Functional Requirements

Table 11: Summary of SFRs

Requirement	Title
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_SAA.1	Potential violation analysis
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FCS_CKM.1	Cryptographic key generation

Requirement	Title
FCS_CKM.4	Cryptographic key Destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_SDI.2	Stored data integrity monitoring and action
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_STM.1	Reliable time stamps
FRU_FLT.1	Degraded fault tolerance
FTA_SSL.3	TSF-initiated termination
FTA_SSL.4	User-initiated termination
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path

5.3.1 Security Audit (FAU)

FAU_ARP.1 Security Alarm

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall ~~take~~ **indicate** [*an alert in the GUI*] upon detection of a potential security violation.

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*no other specifically defined auditable events*]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*]

FAU_SAA.1 Potential Violations Analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*failure events*] known to indicate a potential security violation;

b) [*no other rules*]

FAU_SAR.1 Audit Review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*authorized management users*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*filtering*] of audit data based on [*date time range, and namespace*].

5.3.2 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Deterministic Random Bit Generator*] and specified cryptographic key sizes [*256 bits*] that meet the following: [*SP800-90A*].

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2*].

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES-XTS*] and cryptographic key sizes [*256 bits*] that meet the following: [*FIPS 197*].

5.3.3 User Data Protection (FDP)

FDP_ACC.1 Subset Access Control

Hierarchical to: No other components.

Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the [*Object Storage Access Control SFP*] on [*Subjects: Users accessing storage; Objects: Storage objects; Operations: Read, Write, Execute*].

FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF shall enforce the [*Object Storage Access Control SFP*] to objects based on the following: [*Subjects: Users accessing storage* *Security Attributes:* • *Username* • *Authentication status (success or failure)* *Objects: Storage objects* *Security Attributes:* • *ACLs for each object*]
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*A successfully authenticated subject of the TOE is allowed to perform an operation if the content of the Access Control List (containing permissions) for the object authorizes the Subject to perform the desired operation*].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all objects, based on the following attributes: [*checksum*].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [*rebuild the data*].

FDP_RET_EXT.1 Retention of data

Hierarchical to:	No other components.

Dependencies: FPT_STM.1 Reliable time stamp

FDP_RET_EXT.1.1 The TSF shall allow a retention period to be assigned to user data.

FDP_RET_EXT.1.2 Where a retention period has been assigned to data, the TSF shall deny requests to delete the data until the retention period has expired, or has been removed.

5.3.4 Identification and Authentication (FIA)

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.3.5 Security Management (FMT)

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [*Object Storage Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*username, object ACLs*] to [*authorized administrators assigned the appropriate role*].

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*Object Storage Access Control SFP*] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*authorized administrators assigned the appropriate role*] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*storage configuration, viewing of audit records, management of Management path users, management of Data path users and Data path user access, enabling/disabling of D@RE, management of retention periods and policies*].

FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*System Admin, System Monitor, Namespace Admin*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.3.6 Protection of the TSF (FPT)

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*disk failures, node failures*].

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.3.7 Resource Utilization (FRU)

FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.1.1 The TSF shall ensure the operation of [*read and write operations*] when the following failures occur: [*loss of one node and one disk*].

5.3.8 TOE Access (FTA)

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*configurable period of time of user inactivity*].

FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall allow user-initiated termination of the user's own interactive session.

5.3.9 Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*communications with external authentication servers*].

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [[*remote administration*]]

5.4 Assurance Requirements

29 The TOE security assurance requirements are summarized in Table 12 commensurate with EAL2+ (ALC_FLR.2).

Table 12: Assurance Requirements

Assurance Class	Components	Description
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements

Assurance Class	Components	Description
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent Testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6 TOE Summary Specification

6.1 Security Function

30 This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

Table 13: Security Function SFRs

SFR	Fulfilment
FAU_ARP.1 FAU_GEN.1 FAU_SAA.1 FAU_SAR.1 FAU_SAR.3	Audit logs capture security management functions resulting from use of the Management path interfaces. The management GUI allows only authorized management users to read audit records. The audit records may be filtered based on a time and date range and the namespace for which they were generated. When disk and node failure events indicate errors that require human intervention to correct, an alert is generated. This alert appears in a widget in the management GUI and would also be seen in the management REST API by a user that polls for alerts. For all disk and node failures that cannot be remedied, users should contact Dell Customer Support at: https://www.dell.com/support/incidents-online/en-us/contactsupport.
FCS_CKM.1 FCS_CKM.4 FCS_COP.1	ECS uses the RSA BSAFE® Crypto-J JSAFE and JCE Software Module (Software Version: 6.2.5) module (CMVP certificate number 3819) in support of the Data at Rest Encryption (D@RE) functionality. AES-XTS-256 is the only supported algorithm. The module employs a FIPS-approved HMAC Deterministic Random Bit Generator (HMAC DRBG SP 800-90A) for generating symmetric keys used in AES. Key destruction is performed on keys held in memory after their use using the BSAFE clearSensitiveData function. Stored keys are not destroyed. New keys are created for each object and are encrypted using a Key Encryption Key (KEK). KEKs are encrypted with a master key, which itself is stored encrypted. The KEKs and master key are never stored on the same drive.

SFR	Fulfilment
FDP_ACC.1 FDP_ACF.1 FDP_SDI.2	**Object Storage Access Control SFP** Each object within the storage space has an associated Access Control List (ACL), which is enforced in accordance with the rules of the protocol. The ACLs associated with an object are defined by the owner. Users must be authenticated before the ACL will be evaluated. Authentication occurs locally, or ECS verifies that the user has been authenticated, depending upon the data access protocol being used. **Amazon S3 Authentication** For Amazon S3, each user is assigned a secret key. The user presents the ECS user ID (which maps to the AWS Access key ID in Amazon S3 terminology) and a signature created using the secret key. Once successful authentication is confirmed, ECS verifies that the user has permission based on the contents of the associated ACL. Then, the user will be granted access to the object. **Atmos Authentication** Atmos users are authenticated locally by username and password. 7.3.1.4 Content Addressable Storage (CAS) Authentication CAS features are assigned to the user profile to allow object access via the CAS protocol. Information added through the ECS management interface is used to make up the elements of a CAS profile. This creates a PEA (Pool Entry Authorization) file for use in CAS applications. For CAS, ACLs allowing access to data objects are also configured through the ECS management interface. **NFSv3 Authentication** File based storage may be accessed using an NFS client and local authentication. **Data Integrity** Data integrity is a key security function of ECS. The integrity of data is protected in three ways: Triple-mirroring, Erasure Coding and Checksums. Checksums are used to verify integrity. Erasure coding ensures that the data can be rebuilt in the case of disk or node loss. Triple-mirroring protects data before erasure coding is complete.

SFR	Fulfilment
	Checksums During write operations, the checksum is calculated in memory and then written to disk. On reads, data is read along with the checksum, and then the checksum is calculated in memory from the data read and compared with the checksum stored in disk to determine data integrity. The storage engine runs a consistency checker in the background which performs checksum verification over the entire data set. **Triple-mirroring** All types of information relating to objects, such as data, metadata, and index are written to chunks. At ingest, the chunks are triple mirrored to three different nodes within the ECS system. This technique of triple mirroring allows for data protection of the data in case of a node or disk failure. Data in chunks is triple mirrored until the chunk is full. After that, the data is erasure-coded to provide the same integrity using less storage space. **Erasure Coding** When erasure coding is applied, a chunk is broken into 12 data fragments and 4 coding (parity) fragments, with a Cold Storage option for 10+2 as well. The resulting 16 fragments are dispersed across the nodes. The storage engine can reconstruct a chunk from any 12 of the 16 fragments. All data in ECS is erasure coded except the index and system metadata. The index provides location to objects and chunks and is frequently accessed; hence, it is always kept in triple-mirrored chunks for protection. When a chunk is full (128MB), or after a set period of time, it is sealed, and erasure coded. Erasure coding is conducted as a background process. After erasure coding completes, the mirrored copies are discarded, and a single erasure coded copy persists. **Data Reconstruction** If a disk or node fails, the data is reconstructed. If a request is made to read an object that has become unavailable, the object is reconstructed. If a disk or node fails, the hardware is replaced and the data that had been held by those resources may be reconstructed.

SFR	Fulfilment
FDP_RET_EXT.1.	ECS implements policy-based record retention to prevent data being modified or deleted within a specified retention period. Retention periods and retention policies can be defined in metadata associated with objects and is checked each time a request to modify an object is made. There are two ways of defining retention: retention periods and retention policies. **Retention Periods** Retention periods are assigned at the object and/or bucket level. Each time an attempt is made to modify or delete an object, an expiration time is calculated, where the object expiration time is equal to the object creation time plus the retention period. Where a retention period is assigned to a bucket, the retention period for the bucket is checked and the expiration time calculated based on the retention period set on the object and the value set on the bucket, whichever is the longest. Applying a retention period to a bucket means that the retention period for all objects in a bucket can be changed at any time, and can override the value written to the object by an object client by setting it to a longer period. It is possible to specify that an object is retained indefinitely. **Retention Policies** A retention policy may be applied to a set of data objects within a namespace to apply a retention period on those objects. This allows flexibility to change the period associated with a policy and, in doing so, automatically change the retention period that applies to any objects that have been assigned that policy. By applying a retention policy to a number of objects, rather than applying a retention period directly, a change to the retention policy will cause the retention period to be changed for the complete set of objects to which the policy has been applied. A request to modify an object that falls before the expiration of the retention period will be disallowed. For example, a retention policy can be created for email and this policy may have a one year retention period. All email is then assigned this policy. If it is decided that all email should be held for two years, the policy is changed. All email assigned to this policy now has a two year retention period.
FIA_UAU.2 FIA_UID.2	For the Management path interfaces, LDAP authentication using Active Directory is used in the evaluated configuration. Users must be identified and authenticated before any access to TOE functions is granted through the management REST API or management GUI. Authentication for Data path access depends upon the protocol being used. In the evaluated configuration, local authentication is used for S3, Atmos and CAS access.

SFR	Fulfilment
FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1	ECS provides a management REST API and a management GUI to administer the TOE. The Management GUI is a graphical representation of the functionality provided through the REST API. Through the management REST API and Management GUI, authorized Management path users can: • Configure storage • View audit records • Perform user and role administration of Management path users • Perform user administration of Data path users • Administer authentication and access for Data path users • Enable and disable D@RE • Manage retention periods and policies Access to data is controlled based on username, authentication status and the ACLs for the requested object. Username and ACLs (in some cases) may be managed through the management REST API and GUI. Default values for username and object ACLs are permissive, in that they may be set outside of the TOE. The roles and privileges available in ECS are as follows: **System Admin** - Management users in the System Admin role can configure storage, perform namespace administration, and configure user permissions. **System Monitor** - Users in the System Monitor role can view all ECS Portal data but cannot make any changes. **Namespace Admin** - Users in the Namespace Admin role can assign local users as object users for the namespace and create and manage buckets within the namespace. A root user account, which is assigned to the System Admin role, is provided for initial access. Note that this root account is not related to node-level Linux accounts. As indicated in the administrative guidance, users are directed to change the password for all pre-provisioned accounts on initial access. One or more System Admin accounts should be created, and the root account should no longer be used.
FPT_FLS.1 FPT_STM.1	The ability to rebuild objects from erasure coded data ensures that data is not lost due to the failure of disks or nodes. The number of disks and nodes that can be lost without loss of data is dependent upon the number of nodes implemented. In the evaluated configuration, there are 5 nodes. This configuration will maintain a secure state (i.e. no loss of data) in the case of losses up to and including the simultaneous loss of one node and one disk. ECS requires that a Network Time Protocol (NTP) service be available. Time from the NTP service is maintained by the TOE and provided as reliable time stamps on audit records and is used when determining retention expiry dates.

SFR	Fulfilment
FRU_FLT.1	The number of disks and nodes that can be lost while still maintaining read and write functionality is dependent upon the number of nodes implemented. In the evaluated configuration, there are five nodes. This configuration can tolerate the simultaneous loss of one node and one disk.
FTA_SSL.3 FTA_SSL.4	Interactive sessions with the Management GUI or the management REST API are terminated after a configurable period of inactivity. Once authenticated, users are provided with a token. This token is presented with subsequent requests. After the specified period of user inactivity, the token expires, and the user must log in again. This period of inactivity is set to 15 minutes by default and may be configured via the GUI. Users may log out of the GUI at any time.
FTP_ITC.1	Communications with an external LDAP server used for remote management authentication are protected using TLSv1.2. The following cipher suites are supported: • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
FTP_TRP.1	All communications with remote administrators via the Web GUI and REST API are protected using TLSv1.2. The following cipher suites are supported in the evaluated configuration: • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

7 Rationale

7.1 Security Objectives Rationale

31 Table 14 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 14: Security Objectives Mapping

	T.ACCOUNT	T.EAVES	T.LOSS	T.UNAUTH	T.UNDETECT	P.CRYPTO	P.RETAIN	A.AUTH	A.LOCATE	A.NOEVIL
O.ADMIN	X			X	X					
O.AUDIT			X		X					
O.CRYPTO						X				
O.IDAUTH	X			X	X					
O.INTEGRITY			X							
O.PROTCOMMS		X								
O.PROTECT				X						
O.RETAIN							X			
O.TIME					X		X			
OE.ADMIN										X
OE.PHYSICAL									X	
OE.SERVICE								X		

32

33 Table 15 provides the justification to show that the security objectives are suitable to address the security problem.

Table 15: Suitability of Security Objectives

Element	Justification
T.ACCOUNT	**O.ADMIN** mitigates this threat by ensuring that access to the security management functions of the TOE are restricted to authorized administrators. **O.IDAUTH** mitigates this threat by ensuring that all authorized administrators are identified and authenticated prior to gaining access to the TOE security management functions, and that all users are identified and authenticated prior to being granted access to data.
T.EAVES	**O.PROTCOMMS** mitigates this threat as it requires the TOE to encrypt communications with remote administrators and with external user authentication servers
T.LOSS	**O.AUDIT** mitigates this threat by alerting administrators to failure events that require human intervention for correction. **O.INTEGRITY** mitigates this threat by ensuring that the TOE provides the ability to protect data in the case of node or disk failure
T.UNAUTH	**O.ADMIN** mitigates this threat by providing authorized administrators the ability to manage TOE security functions. **O.IDAUTH** mitigates this threat by ensuring that all users are identified and authenticated prior to gaining access to the TOE security management functions and data. O.PROTECT mitigates this threat by ensuring that only authorized users have access to stored data.
T.UNDETECT	**O.ADMIN** mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized administrators. **O.AUDIT** counters this threat by ensuring that the TOE tracks all management actions taken against the TOE, and by providing a means to review these records. **O.IDAUTH** mitigates this threat by ensuring that all authorized administrators are identified and authenticated prior to gaining access to the TOE security management functions. **O.TIME** supports this policy by providing reliable time stamps in support of audit records.
P.CRYPTO	**O.RETAIN** supports this policy by ensuring that the TOE prevents deletion of data prior to expiry of the assigned retention period. **O.TIME** supports this policy by providing reliable time stamps in support the functions that determine whether or not the retention period has expired.

Element	Justification
P.RETAIN	**O.RETAIN** supports this policy by ensuring that the TOE prevents deletion of data prior to expiry of the assigned retention period. **O.TIME** supports this policy by providing reliable time stamps in support the functions that determine whether or not the retention period has expired.
A.AUTH	**OE.SERVICE** supports this assumption by providing Active Directory authentication services for use in access control decisions.
A.LOCATE	**OE.PHYSICAL** supports this assumption by protecting the physical resources of the TOE from attack.
A.NOEVIL	**OE.ADMIN** supports this assumption by ensuring that the administrators managing the TOE have been specifically chosen to be careful, attentive and non-hostile.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

34 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices with the addition of ALC_FLR.2 to provide assurance that any identified security flaws will be addressed.

7.2.2 SFR Rationale

Table 16: Security Requirements Mapping

	O.ADMIN	O.AUDIT	O.CRYPTO	O.IDAUTH	O.INTEGRITY	O.PROTCOMMS	O.PROTECT	O.RETAIN	O.TIME
FAU_ARP.1		X							
FAU_GEN.1		X							
FAU_SAA.1		X							
FAU_SAR.1		X							
FAU_SAR.3		X							
FCS_CKM.1			X						

	O.ADMIN	O.AUDIT	O.CRYPTO	O.IDAUTH	O.INTEGRITY	O.PROTCOMMS	O.PROTECT	O.RETAIN	O.TIME
FCS_CKM.4			X						
FCS_COP.1			X						
FDP_ACC.1							X		
FDP_ACF.1							X		
FDP_SDI.2					X				
FDP_RET_EXT.1								X	
FIA_UAU.2	X			X					
FIA_UID.2	X			X					
FMT_MSA.1	X								
FMT_MSA.3	X								
FMT_SMF.1	X								
FMT_SMR.1	X								
FPT_FLS.1					X				
FPT_STM.1									X
FRU_FLT.1					X				
FTA_SSL.3	X								
FTA_SSL.4	X								
FTP_ITC.1						X			
FTP_TRP.1						X			

Table 17: Suitability of SFRs

Objectives	SFRs
O.ADMIN	FIA_UID.2 and FIA_UAU.2 ensure that users are identified and authenticated prior to being allowed access to manage TOE security functions. FMT_MSA.1 ensures that access to the security attributes supporting access control functions is restricted to authorized Management path users. FMT_MSA.3 ensures that default values for the security attributes that make up that TSF data are permissive. FMT_SMF.1 provides security management functionality to support storage configuration, viewing of audit records, user management, access control, enabling/disabling D@RE and retention period and policy management. FMT_SMR.1 provides the security roles for Management path users. FTA_SSL.3 and FTA_SSL.4 protects the security management functionality from unauthorized access by allowing a user to terminate the user's own interactive GUI session, or by terminating the session after a configurable period of inactivity
O.AUDIT	FAU_GEN.1 outlines what data must be included in audit records and what events must be audited. FAU_SAR.1 provides functionality to review audit records. FAU_SAR.3 allows the Management path user to filter those records for more convenient viewing. FAU_SAA.1 provides the functionality to monitor the audited events for failures that may require human intervention. FAU_ARP.1 indicates an alert when such an event is detected.
O.CRYPTO	FCS_CKM.1 provides the key generation, FCS_CKM.4 provides the key destruction and FCS_COP.1 provides the cryptographic operation that supports the data at rest encryption functionality provided by the TOE.
O.IDAUTH	FIA_UID.2 ensures that the TOE verifies that the user has been identified before being allowed to access data or security management functions. FIA_UAU.2 ensures that the TOE verifies that the user has been authenticated before being allowed to access data or security management functions.
O.INTEGRITY	FDP_SDI.2 monitors the stored data for integrity errors and rebuilds the data if an error is detected. FPT_FLS.1 preserves the integrity of the data in the case of disk or node failure. FRU_FLT.1 ensures that read and write operations continue to be processed in the case of disk and node failure.

Objectives	SFRs
O.PROTCOMMS	FTP_ITC.1 requires encrypted communications with remote authentication servers. FTP_TRP.1 requires encrypted communications for remote administration.
O.PROTECT	FDP_ACC.1 and FDP_ACF.1 details the Object Storage Access Control SFP which ensures that only authorized users are able to access data resources protected by the TOE.
O.RETAIN	FDP_RET_EXT.1 ensures that data is not deleted prior to the expiry of the retention period.
O.TIME	FPT_STM.1 provides reliable time stamps for use on audit records and the enforcement of retention periods.

Table 18: Dependency Rationale

SFR	Dependency	Rationale
FAU_ARP.1	FAU_SAA.1	Met
FAU_GEN.1	FPT_STM.1	Met
FAU_SAA.1	FAU_GEN.1	Met
FAU_SAR.1	FAU_GEN.1	Met
FAU_SAR.3	FAU_SAR.1	Met
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	Met by FCS_COP.1.
	FCS_CKM.4	Met
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Met by FCS_CKM.1.
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Met by FCS_ITC.1 and FCS_CKM.1.
	FCS_CKM.4	Met
FDP_ACC.1	FDP_ACF.1	Met

SFR	Dependency	Rationale
FDP_ACF.1	FDP_ACC.1	Met
	FMT_MSA.3	Met
FDP_SDI.2	None	-
FDP_RET_EXT.1	FPT_STM.1	Met
FIA_UAU.2	FIA_UID.1	Met, FIA_UID.2 is hierarchical to FIA_UID.1.
FIA_UID.2	None	-
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Met by FDP_ACC.1
	FMT_SMR.1	Met
	FMT_SMF.1	Met
FMT_MSA.3	FMT_MSA.1	Met
	FMT_SMR.1	Met
FMT_SMF.1	None	-
FMT_SMR.1	FIA_UID.1	Met, FIA_UID.2 is hierarchical to FIA_UID.1.
FPT_FLS.1	None	-
FPT_STM.1	None	-
FRU_FLT.1	FPT_FLS.1	Met
FTA_SSL.1	None	-
FTA_SSL.4	None	-
FTP_ITC.1	None	-
FTP_TRP.1	None	-