Commvault Systems Inc.

Security Target

Commvault Platform Release CPR2025E (11.42.41)
Evaluation Assurance Level (EAL): EAL2

TOE Reference:	Commvault Platform Release 2025E (11.42.41)
Version	v1.9
Date	2026-02-19
Classification:	PUBLIC

Version history

Version	Date	Author	Description
v1.0	2024-08-29	Commvault Systems Inc.	The first version of the Security Target.
v1.1	2025-02-05	Commvault Systems Inc.	Updates based on anomaly observation report.
v1.2	2025-06-03	Commvault Systems Inc.	Updates based on anomaly observation report.
v1.3	2025-08-18	Commvault Systems Inc.	Updates based on anomaly observation report.
v1.4	2025-10-14	Commvault Systems Inc.	Updates according to TOE version update.
v1.5	2025-11-17	Commvault Systems Inc.	Updating references.
v1.6	2025-11-26	Commvault Systems Inc	Minor updates.
v1.7	2025-12-04	Commvault Systems Inc	Updates based on anomaly observation report.
v1.8	2026-01-28	Commvault Systems Inc	Removing FCS related parts.
v1.9	2026-02-19	Commvault Systems Inc	Minor updates.

Table of Contents

1 Introduction

This is the Security Target of Commvault Platform Release CPR2025E (11.42.41) for Common Criteria Evaluation EAL2.

1.1 ST Reference

Table 1 – ST Reference

ST Title	Security Target Commvault Platform Release CPR2025E (11.42.41) Evaluation Assurance Level (EAL): EAL2
ST Version	v1.9
ST Creation Date	2026-02-19

1.2 TOE reference

Table 2 – TOE Reference

TOE Name	Commvault Platform Release CPR2025E (11.42)
TOE Reference	Commvault Platform Release CPR2025E (11.42.41)
TOE Short Name	CPR2025E
TOE Version	11.42.41

The referenced TOE version includes the following patches applied:

11.0.0B80-SP42-CU41_SP42-CU41-964, …965, 966, 967, 968, 971, 972, 973, 985, 986, 996, 997, 998, 999, 1002, 1009, 1010, 1012, 1013, 1014, 1015, 1016, 1017, 1018, 1019, 1020, 1021, 1022,1029, 1033,1036, 1037, 1038, 1039, 1040, 1041, 1042, 1043, 1044, 1045, 1046, 1047, 1048, 1049, 1056, 1058, 1062, 1063, 1064, 1066, 1067, 1068, 1069, 1070, 1071, 1073, 1074, 1075, 1076, 1077, 1078, 1079, 1082, 1083, 1087, 1090, 1091, 1096, 1100, 1101, 1104, 1106, 1107, 1108, 1109, 1110,1111, 1113, 1114, 1115, 1118, 1119, 1120, 1122, 1123, 1125, 1126, 1127, 1128, 1129, 1132, 1133, 1135, 1157, 1160, 1161, 1197, 1200, 1201, 1203, 1208, 1209, 1212, 1218, 1220, 1221, 1222, 1223, 1224, 1225, 1226, 1227, 1228, 1229, 1230, 1234, 1235, 1236, 1237, 1238, 1239, 1240, 1241, 1247, 1248, 1249, 1257, 1260

1.3 Product Overview

Commvault Cloud software implements the Intelligent Data Management features to backup different versions of the data, stores the data in a space efficient and encrypted format.

A Commvault Cloud software deployed environment (referred to as a CommCell) is the logical grouping of all software components that protect, move, store, and manage data and

information. A CommCell environment at a minimum contains one CommServe Server host, one or more MediaAgents, and many clients/servers whose data is protected.

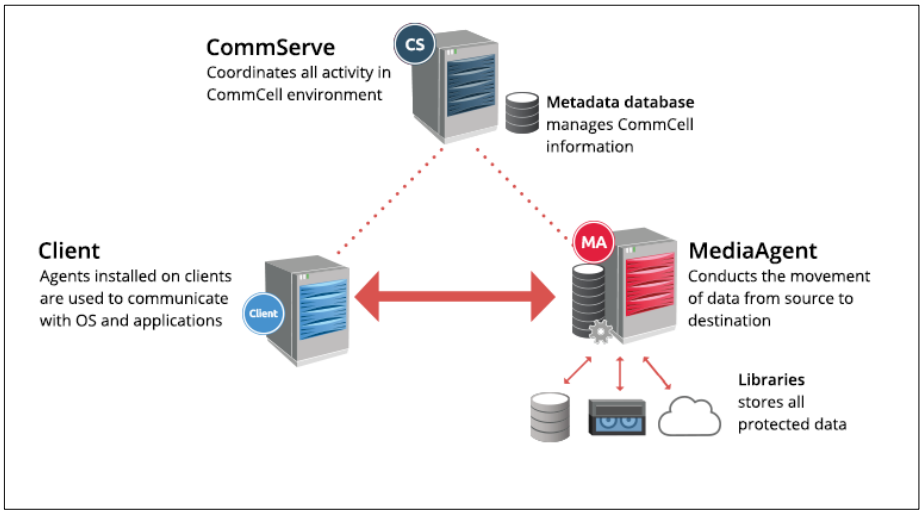


Figure 1

The CommCell components provide various features and services.

- CommServe Server
  - Central Catalog and the main server.
  - Application Configuration Management
  - User Management, Role based Security, External System Integration.
  - Identity Management, Credential Management
  - Software Install, upgrade, update management for all entities.
  - Storage Policies, Storage Pool Management, Data Retention Management.
  - Schedule Policies, Resource and Job Management
  - Orchestrates operations like Backup, Archiving, Restore, Replication, Content Indexing, Disaster Recovery, Data Migration, Multi-cloud format conversion, Intellisnap etc.
  - WebServer APIs, Command Lines, User Interfaces – CommCell Console and Command Center, Third party integration.
  - Audits and Alerts
  - Reporting – Metrics server, custom Reports
  - Automation and Workflows
  - Multi-commcell operations, Commcell migration, Federated IDP
  - Commserve LiveSync
  - Managing encryption keys
- MediaAgent
  - Metadata Indexing
  - Facilitates Data Storage – Common Interface – by an abstraction of MediaFileSystem – Disk, Object (Cloud) (Not in scope), Tape (not in scope)
  - Data Indexing (Content Indexing) (not in scope for attestation)
  - Bandwidth efficient Data Copies.
  - Provides open protocol interfaces like NFS, iSCSI, WebDAV etc.

- Client
    - Local and Network File Systems
    - Databases like Oracle, SQL, Postgres etc.
    - NoSQL Databases
    - Bigdata sources
    - Applications like Exchange, Sharepoint, SAP
    - Cloud Applications like Office 365, Salesforce
    - Cloud infrastructure like AWS, Azure and GCP compute instances
    - Cloud Database infrastructure like Azure PaaS, AWS
    - Cloud Applications like Office 365
    - Virtual Servers like VMWare, HyperV, Nutanix
    - Hybrid Cloud – K8s, Openshift
    - Mainframe – iSeries, OpenVMS

The Command Center (Web Console) is used to manage the CommServe system through API calls.

There are three consumption/deployment options:

- Commvault Cloud Software– Software only deployment option, which is suitable for the cases where the customer deploys the software on the on-prem or cloud or hybrid environment with the infrastructure managed by the customer.
- Hyperscale – Infrastructure components embedded together with the software in easy consumable configurations. This is available in both Appliance mode where Hardware is supplied as part of the offering or as a Reference Architecture model where the customer brings in any of the certified reference hardware server infrastructure.
- Commvault Cloud SaaS –offering where the infrastructure and software components are completely managed by Commvault.

The CommCell provides high availability access to the stored data as well as the required services and should have ways to overcome single hardware failures like disk/machine failures. This is usually achieved by redundancy for hardware and software.

- High Availability of the Data storage
    - Data access is made highly available by utilizing multiple Datapaths (multiple MediaAgents and networks) to the storage. If any of the MediaAgents are down, other MediaAgents will be used for accessing the data, index data or Deduplication DB. This is based on the Gridstor feature in the software.
    - With the Hyperscale solution, both storage and compute are made highly available by using a set of Compute plus local storage nodes which acts together to provide the redundancy.
- High Availability of the Commserve
    - Commserve High Availability is achieved by the CS LiveSync feature. With this feature, the commserve metadata is replicated to a standby server in frequent

intervals so that if the active server goes down, the standby can take over as active.

- Scalability
    - The amount of workload that the software can process be increased by increasing the number of MediaAgents and the amount of available storage for managing the data. In each Commcell, these entities can be increased to achieve more and more scalability for the operations.

1.4 TOE Overview

The Target of Evaluation (TOE) is an enterprise data backup and recovery software. The CPR2025E implements the Intelligent Data Management features to backup different versions of the data, stores the data in a space efficient and encrypted format. The following features are scope of the evaluation:

- Data Transport from the source clients to the storage.
- Data Transport from the storage to the client
- Management interface (Command Center)
- Data Deduplication
- Indexing of the backup Metadata for easy search and browse
- Backup and Restore operation management.
- Disaster Recovery
- Network Topologies, Gateways, Throttling – limited

The data deduplication, indexing of the metadata and disaster recovery are running in the background, there are no operations required on a management interface for them.

TOE components:

- CommServe – Contains the central catalog and it is the main server. Users and configurations can be managed from here. Creating policies, jobs for backups and restore can be done on that component. The audit is generated on this component and can be reviewed as an authorized user.
- Virtual Server Agent (VSA) is a module that interacts with the hypervisor through the ESXI API to facilitate backup and recovery.
- MediaAgent – Behaves as data storage for the encrypted data. Physically it is the same virtual machine as the Commserve.

Critical non-TOE component:

- Client – Contains the customer data to be backed up. The Client, in this context is a virtual machine on an ESXI hypervisor environment. During the backup we can choose a single VM or a VM Group associated with the hypervisor environment. Choosing the VM Group will back up every VM associated to the group for the Hypervisor . The scope of the evaluation is backing up one virtual machine.

- Commvault Crypto Library 3.0 – Cryptographic module used for the cryptographic operations. TOE uses the Commvault Crypto Library[1] for all cryptographic operations. It is a FIPS validated library.

The TOE deployment architecture is the following:

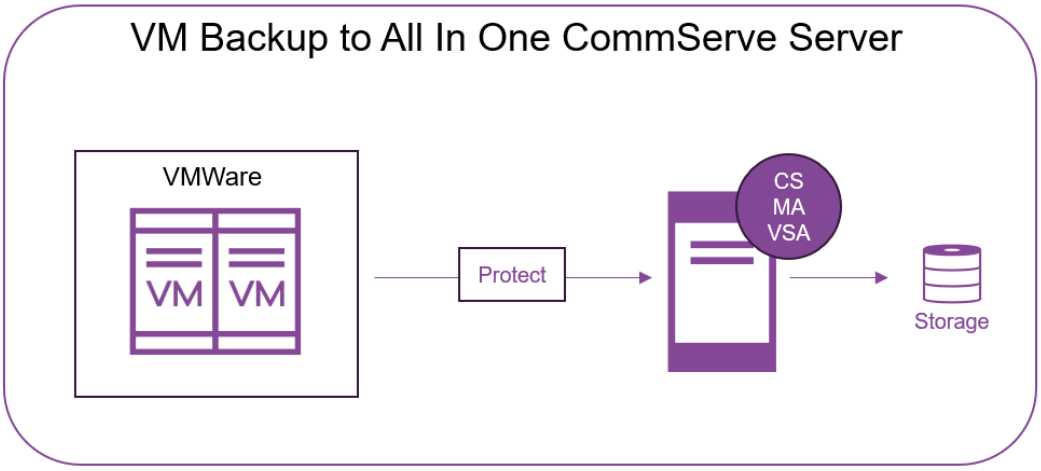


Figure 2 – TOE Deployment architecture

In the evaluated configuration there is one CommServe (CS) and one MediaAgent (MA) – these are installed on the same Windows Server; and one Windows Client hosted on an ESXI hypervisor. Virtual Server Agent (VSA) also installed on the same system as CommServe and Media Agent is the module that interacts with the hypervisor through the ESXI API.

During the backup the TOE uses the Application Admin's credentials to access the client on the ESXI hypervisor and create the backup.

1.4.1 TOE Boundary

The TOE is an IDM (Intelligent Data Management) backup/restore solution for a windows virtual machine (Client) where the Server (CommServe) and Media Agent are deployed on the same Windows Server machine. There are several services provided by the TOE (See the bullet point listing in section 1.4 above) and the TOE can be managed through the Command Center (Web Console). There are other interfaces, and a function provided by the product, but these are out of scope of the evaluation. These are also listed below. The client itself is not part of the TOE, only the VSA module which interacts with the hypervisor where the client is installed.

[1] https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4989

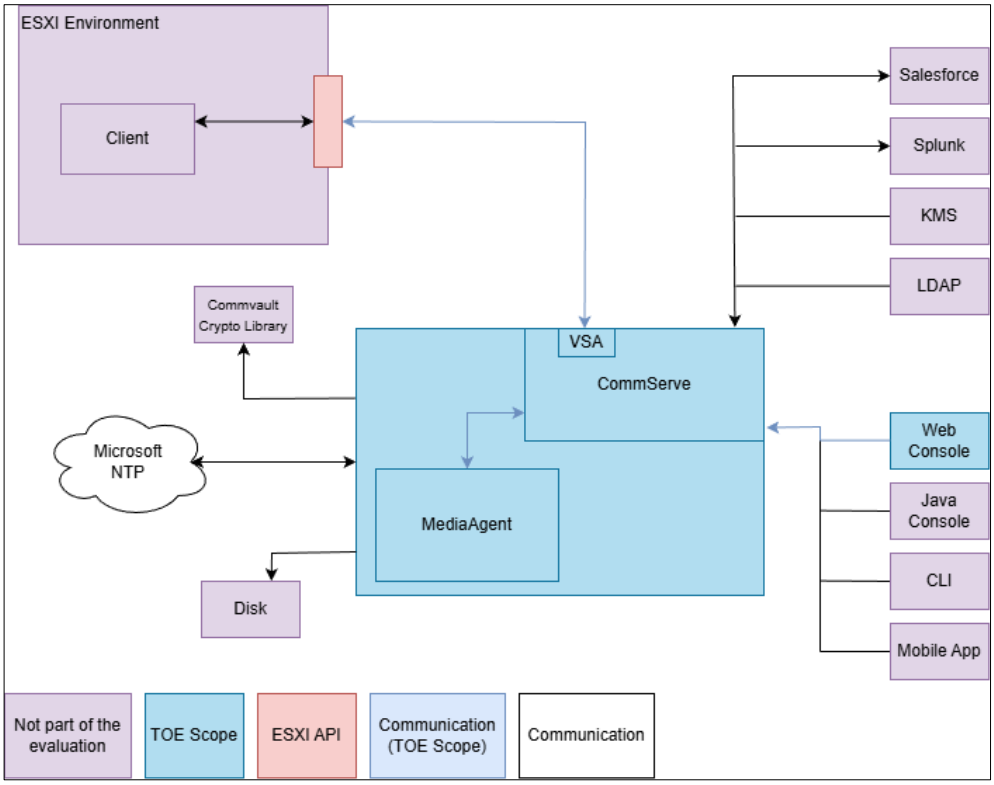


Figure 3 – TOE Environment

The scope of the evaluation is the following:

- CommServe Server where the management functions are available through the Command Center (Web Console)
- One MediaAgent where the backup is saved on a virtual disk – physically the MediaAgent is the same as the CommServe server.
- The communication path between the components.
- VSA module which interacts with the ESXI API.

Critical non-TOE component:

- Client – A guest Windows Virtual machine running on ESX Server, that can be protected through the ESXI API.
- Commvault Crypto Library 3.0 – Cryptographic module used for the cryptographic operations.

1.4.2 TOE Type

CPR2025E is an enterprise data backup and recovery product which implements the Intelligent Data Management features (Data Deduplication, Data Encryption, Disaster recovery, etc.) to backup different versions of the data, stores the data in a space efficient and encrypted format.

1.4.3 TOE Usage and Major Security Features

The TOE's major security features are the following:

- Data Transport from the source client to the storage facilitated by means of VSA – Backup operation.
- Data Transport from the storage to the client facilitated by means of VSA – Restore operation.
- Data Deduplication – DDBs (Deduplication database) may be defined as Deduplication Engines that achieves reduction of data across many different dependent Copies. (MediaAgent)
- Indexing of the Metadata for easy search and browse. - When in the backup phase the stream reaches the MediaAgent, the data is indexed and stored on the MediaAgent.
- Management interface - The Command Center (Web Console)
- Backup and Restore operation management (CommServe)
- System Disaster Recovery - By default, the CommServe software runs Disaster Recovery (DR) backup jobs to protect the CommServe production database. The DR backups include the CommServe database and other databases (if installed with the CommServe software). In this method, the CommServe configurations and data are backed up to a disk media and periodically moved (if configured) to a network share, Metallic cloud, cloud library, or tape media. In the event of an actual disaster, you can use these backed up database dumps from the remote media and recover the CommServe database on the same or new host.
- Network Topologies, Gateways, Throttling – Set up an encrypted path between the TOE components on a specific tunnelling port.

All backup and restore operations can be initiated on the Command Center.

The backup and restore operations can be divided in the following subsections:

- Backup phase
    - In the backup phase, the client backup process (VSA) reads the binary data from the ESXI and sends the data across to the MediaAgent over pipeline. When this stream reaches MediaAgent, indexing of the data is performed and the index is stored on the MediaAgent. Data is then written down on the storage target (library).
- Restore Phase
    - During the restore phase the administrator initiates the restore function where the MediaAgent performs the Index browse to find the data to be restored.
    - The data is sent from the MediaAgent through the Access Node component VSA agent, then it is sent to the ESXI to restore the client using the ESXI API.
    - When the restore is finished the Backup Admin is notified. The data is sent in an encrypted way and is decrypted on the Access Node, then sent to the ESXI over an encrypted communication pipe.

1.4.4 TOE Hardware requirements

The following hardware requirements are needed for secure use of the TOE:

- Windows Server 2019 x64 - https://learn.microsoft.com/en-us/windows-server/get-started/hardware-requirements?tabs=cpu
- CPU with at least 16 cores
- 32GB RAM
- 2 TB of working space for the CommServe database, the deduplication database (DDB), index and job results (SSD is recommended)

1.4.5 Non-TOE Software/Firmware/Hardware/Functions

The following non-TOE requirements are needed for the TOE:

- **CommServe/MediaAgent**
  - Windows 2019 Server OS
  - MSSQL Server Database 2022
  - Internet browser, Preferably Microsoft Edge
  - Commvault Crypto Library 3.0 (Installed along with the TOE)
- **Client**
  - An ESXI hypervisor environment where a Client VM (Windows Server 2019) is installed with the following requirements:
    - General system requirements for Windows Server 2019 x64: https://learn.microsoft.com/en-us/windows-server/get-started/hardware-requirements?tabs=cpu
  - The following versions are supported for vSphere, vCenter, vCenter Server Appliance, and ESX/ESXi: 4.1 or later, 5.0.x, 5.1.x, 5.5, 5.5.1, 5.5.2, 5.5.3, 5.5.6, 6.0, 6.0.1, 6.0.2, 6.0.3, 6.5, 6.7, 6.7.1, 6.7.2, 6.7.3, 7.x (all minor updates), 8.x (all minor updates)
  - For any ESXi servers, the VADP is not available in the free version of ESXi. The Essentials licensing level or higher is required.

Note: CommServe and MediaAgent are considered part of the TOE, except for their environmental requirements. The Client and its environmental requirements are considered non-TOE components. The list structure is intended to clearly distinguish the environmental requirements associated with the different components.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

1.5.1 Physical Scope of the TOE

The physical scope of the TOE consists of the TOE installers and of the guidance documents.

The TOE binary can be downloaded from the Commvault Store (https://store.commvault.com/webconsole/softwarestore/store.do#!/)

After downloading the TOE, the customer has to check the digital signature of the installer and the checksum.

The installer of the certified TOE is the following:

- Platform: Windows
- File Name: Commvault_Media_11_32.exe
    - SHA-256 checksum: *16cc8c1043d3e83455c5b1ae585a78c083ca6f32425905cb23dd8f8215d4c0c1*

The product's documentation and the [AGD] document is sent to the customer via e-mail when receiving the license.

The documents can be verified as follows:

- Guidance document
    - Name: "Commvault Systems Inc. Guidance document Commvault Platform Release CPR2025E (11.42.41) Evaluation Assurance Level (EAL): EAL2.pdf"
    - Version: v1.9
    - Release date: 2026-02-19
    - SHA-256: 6b9a0763a356096012499dfde7eddb3ceedb177c8fe3153ef5ac2540bc97f2c9
- Product documentation ([CPR2023E])
    - Name: "11.32_offlinedocs.zip"
    - SHA-256: 33a3355f140144a6bc79c5384b5f8481dd27923965247b9b0dd413973aac9cde
- Product documentation ([CPR2025E])
    - Name: "11.42_offlinedocs.zip"
    - SHA-256: 2e54444fce28b16a6818ee4328cdc0afa96c1834e5c91d1d767dedf882cc762c

1.5.2 Logical Scope of the TOE

The TOE provides the following security functions:

- Security Audit
- User Data Protection
- Identification and authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels

1.5.3 Security Audit

The TOE generates audit records for events associated with TSF-mediated actions, TOE startup, and TOE shutdown. These records contain relevant information such as the identity of the initiating TOE user. Authorized TOE users have the capability to review these audit entries.

1.5.4 User Data Protection

The TOE offers backup (offering DDB[2]) and restore capabilities to Backup Admin, managed through Plans. These Plans are access-controlled by the TOE, ensuring that only authorized TOE users can query, create, modify, or delete them. Access to the Plans is determined by the security attributes of the TOE user's account and the backup plan itself.

1.5.5 Identification and authentication

The TOE guarantees that access to TSF-mediated actions is restricted to authenticated and identified TOE users. Before identification, three public endpoints are available.

1.5.6 Security Management

The TOE offers management functionalities such as audit reviewing, encryption policy and key rotation policy management, backup plan management, backup data restoration, and local account management. When accessing the TOE to oversee these functions, the TOE will assign TOE users to the roles it maintains. This ensures that TOE users are confined to the TOE areas accessible by their assigned roles. Specifically, when managing backup plans or local accounts, the TOE imposes access control on which roles can handle the security attributes associated with these plans and accounts.

1.5.7 Protection of the TSF

To ensure that the audit records have the correct time, the TOE is configured to synchronize with the Microsoft NTP servers and the system time is used as a reliable timestamp. Systems are configured to have NTP sync with Microsoft NTP servers and system time is used to record audit logs. The TOE stores temporary timestamps and when the sync goes off the TOE stops working, and a warning message appears.

1.5.8 Trusted Path/Channels

Communication between the Command Center and CommServe is encrypted and trusted using TLSv1.2 compliant communication protocol. Communication between CommServe/MediaAgent is established using a certificate-based encryption mechanism. Communication between CommServe and VSA is done using TLS 1.2 and between VSA and Client (in this case, ESX Server) is done using NBD SSL encryption.

2 Conformance Claims

Table 3 – Conformance Claims

Common Criteria Conformance	Common Criteria for Information Technology Security Evaluation, CC Part 1 [CC_P1], CC Part 2 extended [CC_P2], CC Part 3 conformant [CC_P3], CC Part 4 [CC_P4], CC Part 5 [CC_P5]
Common Criteria version	CC:2022 Revision 1, November 2022

[2] Data deduplication is the process of removing duplicate copies of datasets to optimize storage resources and enhance their performance. By eliminating redundant information, the system frees storage space and reduces the size of datasets.

PP Conformance	This security target does not claim conformance to any protection profile.
Evaluation Assurance Level	EAL2

3 Security Problem Definition

This section defines the security problem to be addressed by the TOE and its operational environment and includes the following:

- Assets
- Secure Usage Assumptions,
- Threats, and
- Organisational Security Policies (OSPs).

3.1 Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Table 4 - OSPs

Name	Description
P.ACCOUNT	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.BACKUP	The TOE shall backup specified client data and make it available for restore operations

3.2 Assets

The IT assets requiring protection are the following:

- Backup Data - All the backup data of the clients.
- TSF Data – All the configuration data and parameters which affect the functionality of the TOE (Encrypted KEK, DEK, Master Key)

3.3 Assumptions

Table 5 - Assumptions

Assumption	Description
A.MANAGE	It is assumed that there are one or more competent individuals assigned to manage the TOE. These users are not careless, wilfully negligent, or hostile. They are appropriately trained and will follow the instructions provided by the TOE documentation.
A.NETWORK	It is assumed that the TOE components and their hosts are installed on an internal network which protects the data from disclosure and modification by untrusted systems or users.

A.PROTECT	It is assumed that the hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical access.

3.4 Threats

Table 6 - Threats

Threat	Threat agent	Asset	Adverse action
T.UNAUTH	Unauthorized user	Backup data	An unauthorized user may attempt to access backup data which could result in the loss of sensitive information.
T.PRIVILEGE	Unauthorized user	TSF data	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.IMPCON	Unauthorized user	TSF data	An unauthorized user may inappropriately change the configuration of the TOE causing potential unauthorized data accesses to go undetected.
T.SNIFF	Unauthorized user	Backup data	An unauthorized user may intercept the traffic between the TOE components it to gain information of the backup data.

4 Security Objectives

The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

Table 7 - Security Objectives for the TOE

Objective	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.ADMIN	The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE and restrict these functions from unauthorized use.

O.AUDIT	The TOE must generate audit records for security related events.
O.BACKUP	The TOE shall backup specified client data and make it available for restore operations.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.PROTECT	The TOE must ensure the integrity of all TSF data, including audit records, by protecting itself from unauthorized access.
O.TIME	The TOE must provide reliable timestamps.
O.TRAFFIC	The TOE must ensure that the internal traffic and the traffic between the management interface and the TOE user is secured.

Table 8 - Security Objectives for the Operational Environment

Objective	Description
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
OE.NETWORK	The operational environment will provide a segregated, internal network that protects the traffic that passes between the TOE components from disclosure and modification by untrusted systems or users.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

4.1 Security Objectives Rationale

This section demonstrates that the stated security objectives counter all identified threats, enforce policies, and uphold assumptions.

The following tables provide a mapping of security objectives for the TOE and security objectives for the operational environment of the TOE to the defined threats, policies, and assumptions, illustrating that each security objective covers at least one threat, enforces a policy or upholds an assumption and that each threat, policy or assumption is covered by at least one security objective.

The tables below provide information regarding:

- the identified security objectives providing effective countermeasures for the threats;
- the identified security objectives providing complete coverage of each organizational security policy;
- the identified security objectives upholding each assumption.

4.1.1 Security Objectives Rationale related to Threats

The security objectives rationale shall trace each security objective for the TOE and security objectives for the operational environment back to threats countered by that security objective and OSPs enforced by that security objective.

Table 9 – Rationale for threats and security objectives for the TOE and for the operational environment

Threats	Objectives	Rationale
T.UNAUTH An unauthorized user may attempt to access backup data which could result in the loss of sensitive information.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective permits only authorized access to TOE data.
	O.AUDIT The TOE must generate audit records for security related events.	The O.AUDIT objective supports O.ACCESS by requiring the TOE to record audit data for security related events such as unauthorized access attempts.
T.PRIVILEGE An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDENTAUTH objective by permitting only authorized users to access TOE functions.
	O.IDENTAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDENTAUTH objective requires authentication of users prior to allowing access to TOE functions.
	O.PROTECT The TOE must ensure the integrity of all TSF data, including audit records, by protecting itself from unauthorized access.	The O.PROTECT objective addresses the threat by providing self-protection for the TOE.
T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDENTAUTH objective by only permitting authorized users to access TOE functions.

potential unauthorized data accesses to go undetected.	O.ADMIN The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE and restrict these functions from unauthorized use.	The O.ADMIN objective ensures the TOE has all the necessary administrative functions to manage the product.
	OE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.	The OE.INSTALL objective states the authorized administrators will configure the TOE properly.
	O.AUDIT The TOE must generate audit records for security related events.	The O.AUDIT objective supports O.ACCESS by requiring the TOE to record audit data for security related events such as unauthorized access.
	O.IDENTAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDENTAUTH objective requires authentication of users prior to allowing access to TOE functions.
T.SNIFF	OE.NETWORK The operational environment will provide a segregated, internal network that protects the traffic that passes between the TOE components from disclosure and modification by untrusted systems or users.	The OE.NETWORK ensures that the no attacker can access data on the TOE network.
	O.TRAFFIC The TOE must ensure that the internal traffic and the traffic between the management interface and the TOE user is secured.	The O.TRAFFIC ensures that the communication between the TOE components are encrypted and cannot be sniffed.

4.1.2 Security Objectives Rationale relating to Assumptions

The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

Table 10 – Rationale for assumptions and security objective for the operational environment

Assumptions	Objectives	Rationale
A.MANAGE	OE.INSTALL	The OE.INSTALL objective ensures that the TOE is properly installed and operated.
	OE.PERSON	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
	OE.PHYSICAL	The OE.PHYSICAL objective provides for physical protection of the TOE.
A.NETWORK	OE.NETWORK	The OE.NETWORK objective ensures that the management traffic will be protected on an internal network.
A.PROTECT	OE.PHYSICAL	The OE.PHYSICAL objective provides for the physical protection of the TOE hardware and software components, and the hardware and software components that support the TOE implementation.

4.1.3 Security Objectives Rationale relating to OSPs

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. The table below provides a mapping of the OSPs to the Security Objectives.

Table 11 – Security Objectives Rationale relating to OSP

OSPs	Objectives	Rationale
P.ACCOUNT	O.TIME	The O.TIME objective supports this policy by providing a time stamp for insertion into the resulting audit records.
P.BACKUP	O.BACKUP	The O.BACKUP objective requires the TOE to backup specified client data, and requires the TOE to make the data available for restore operations.

5 Extended Components Definition

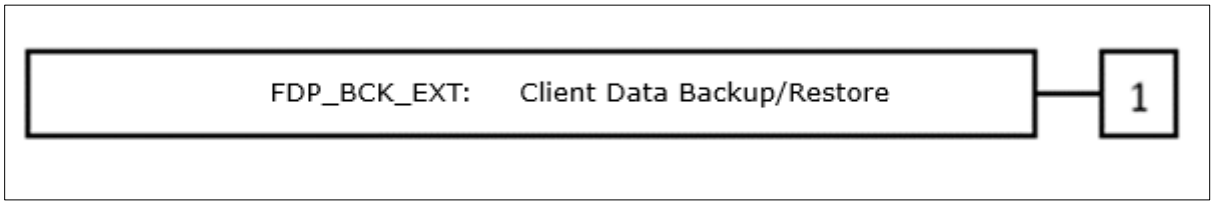
5.1 Family FDP_BCK_EXT: Client Data Backup/Restore

Client data Backup/Restore provides for the functionality to perform backup and restore operations as directed by administrators. The Client Data Backup/Restore family was modelled after FDP_ACC: Access Control Policy. The Client Data Backup/Restore SFR was loosely modelled after FDP_ACC.1: Subset access control.

Family behaviour

This family defines the requirements for the TOE to provide backup and restore services for IT systems in the operational environment.

Component levelling:



Management: FDP_BCK_EXT.1

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

- Configuration of the backup and restore operations to be performed.

Audit: FDP_BCK_EXT.1

There are no auditable events foreseen.

FDP_BCK_EXT.1	*Client data backup/restore*
Hierarchical to:	No other components.
Dependencies:	No dependencies

FDP_BCK_EXT.1.1 The TSF shall provide a capability to backup data and systems in accordance with the backup plan configured by authorized administrators.

FDP_BCK_EXT.1.2 The TSF shall provide a capability for authorized administrators to restore files to systems from previously created backups.

6 Security Requirements

This section defines the SFRs, and SARs met by the TOE.

This section defines whether the SFRs and SARs are clear, unambiguous, and well-defined, whether they are internally consistent, and whether the SFRs meet the security objectives of the TOE.

6.1 Conventions

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Completed assignments statements within a selection statement are identified using [*underlined and italicized test within brackets*]

6.2 Subjects, Objects and Operations

All subjects, objects, operations, used in the SFRs and the SARs are defined.

Table 12 - Subjects

Subject	Description
TOE users	*TOE users for management through the Command Center (Web Console).*

Table 13 – Objects

Object	Description
Backup plans	*Defines where backups will go, and when they will be backed up*

Table 14 - Subjects, Objects and Operations

Subject	Operation	Object	Description
TOE users	*query, create, modify, delete*	*Backup plans*	*The TSF restrict the ability for specific TOE users to query, create, modify or delete backup plans.*

6.3 TOE Security Functional Requirements

List of the SFRs along with their description and the operations performed on them.

Table 15 - SFRs

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	x	x		
FAU_GEN.2	User identity Association				
FAU_SAR.1	Audit review		x		
FDP_ACC.1	Subset access control		x		
FDP_ACF.1	Security attribute-based access control		x		
FDP_BCK_EXT.1	Client data Backup/Restore				
FIA_UAU.1	Timing of authentication		x		
FIA_UID.1	Timing of identification		x		
FMT_MSA.1	Management of security attributes	x	x		
FMT_MSA.3	Static attribute initialisation	x	x		
FMT_SMF.1	Specification of management functions		x		
FMT_SMR.1	Security roles		x		
FPT_STM.1	Reliable time stamps				
FTP_TRP.1	Trusted Path	x	x		

Note: S = Selection, A = Assignment, R = Refinement, I = Iteration

6.3.1 Security Audit

6.3.1.1 Audit data generation (FAU_GEN.1)

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][3] level of audit; and

[3] [selection, choose one of: minimum, basic, detailed, not specified]

c) [*Backup and Restore events)*][4].

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;

b) For each audit event type, based on the auditable event definitions of the functional components included in in the PP, PP-Module, functional package or ST,, [*the audit events will include the relevant information listed in Table 16*][5].

Table 16 – Audit Record Contents

Column	Content	Notes
Process ID	ID of the process	Event log (Backup and Restore events)
Thread ID	ID of the thread	
Timestamp	Formatted timestamp	
Job ID	ID of the job	
Event Description	Description of the event which is logged.	

6.3.1.2 User identity association (FAU_GEN.2)

FAU_GEN.2	*User identity association*

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.3.1.3 Audit review (FAU_SAR.1)

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 [*Backup Admin, Auditor*][6] with the capability to read [*job related audit information*][7] from the audit records.

[4] [assignment: *other specifically defined auditable events*]
[5] [assignment: *other audit relevant information*]
[6] [assignment: *authorised users*]
[7] [assignment: *list of audit information*]

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

6.3.2 User Data Protection

6.3.2.1 Subset access control (FDP_ACC.1)

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 [*Role Based Access Control SFP*][8] on [

- *Subjects: TOE users*
- *Objects: Backup plans*
- *Operations: query, create, modify, delete*][9].

6.3.2.2 Security attribute-based access control (FDP_ACF.1)

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

FDP_ACF.1.1 The TSF shall enforce the [*Role Based Access Control SFP*][10] to objects based on the following: [

- *Subject security attributes for TOE users – Role*
- *Object security attributes for backup plans – Plan name, Backup Destination, RPO*][11].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*TOE users assigned a role with the appropriate privileges are able to query, create, modify, or delete backup plans*][12].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*no additional rules*][13].

---

[8] [assignment: *access control SFP*]
[9] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[10] [assignment: *access control SFP*]
[11] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[12] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[13] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*][14].

6.3.2.3 Client Data Backup/Restore (FDP_BCK_EXT.1)

FDP_BCK_EXT.1	*Client data backup/restore*

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_BCK_EXT.1.1 The TSF shall provide a capability to backup data and systems in accordance with the backup plan configured by authorized administrators.

FDP_BCK_EXT.1.2 The TSF shall provide a capability for authorized administrators to restore files to systems from previously created backups.

6.3.3 Identification and authentication

6.3.3.1 Timing of authentication (FIA_UAU.1)

FIA_UAU.1	*Timing of authentication*

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*accessing the public endpoints listed in 7.3 Identification and authentication*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.3.3.2 Timing of identification (FIA_UID.1)

FIA_UID.1	*Timing of identification*

Hierarchical to: No other components

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [*accessing the public endpoints listed in 7.3 Identification and authentication*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[14] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

6.3.4 Security Management

6.3.4.1 Management of security attributes (FMT_MSA.1)

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 [*Role Based Access Control SFP*][15] to restrict the ability to [query, modify, delete, [*create*]][16] the security attributes [*role, Plan name, Backup Destination, RPO*][17] to [*Backup Admin*][18].

6.3.4.2 Static attribute initialisation (FMT_MSA.3)

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 [*Role Based Access Control SFP*][19] to provide [restrictive][20] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*Backup Admin*][21] to specify alternative initial values to override the default values when an object or information is created.

6.3.4.3 Specification of Management Functions (FMT_SMF.1)

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: [

[15] [assignment: *access control SFP(s), information flow control SFP(s)*]
[16] [selection: change_default, query, modify, delete, [assignment: *other operations*]]
[17] [assignment: *list of security attributes*]
[18] [assignment: *the authorised identified roles*]
[19] [assignment: *access control SFP, information flow control SFP*]
[20] [selection, choose one of: restrictive, permissive, [assignment: *other property*]]
[21] [assignment: *the authorised identified roles*]

- *Manage encryption policy*
- *Manage backup plan*
- *Backup client*
- *Restore data from backups*
- *Manage local accounts*
- *Manage key rotation policy*][22].

6.3.4.4 Security roles (FMT_SMR.1)

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 [*Backup Admin, Auditor*][23].

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

6.3.5 Protection of the TSF

6.3.5.1 Reliable time stamps (FPT_STM.1)

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.

6.3.6 Trusted Path/Channels

6.3.6.1 Trusted Path (FTP_TRP.1)

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][24] users that is logically distinct from other communication paths and provides assured identification of its end points and

[22] [assignment: *list of management functions to be provided by the TSF*]
[23] [assignment: *the authorised identified roles*]
[24] [selection: remote, local]

protection of the communicated data from [modification, disclosure][25].

FTP_TRP.1.2 The TSF shall permit [remote users][26] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [*Accessing the Command Center, Communicate with the ESXI API, Communication between the CS and MediaAgent*][27].

[25] [selection: modification, disclosure, [assignment: *other types of integrity or confidentiality violation*]]
[26] [selection: the TSF, local users, remote users]
[27] [selection: initial user authentication, [assignment: *other services for which trusted path is required*]]

6.4 TOE Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 5 and are EAL2.

Table 17 – Assurance Requirements

Assurance Requirements		
Class ASE: 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
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Class ALC: Life Cycle Support	ALC_CMC.2	Use of the CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Class ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Class AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Class ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

6.5 Security Requirements Rationale

6.5.1 Security Requirements Coverage

The Table below provides a mapping between the Security Functional Requirements and the Security Objectives, illustrating that each Security Functional Requirement covers at least one Objective and that each Objective is covered by at least one Security Functional Requirement.

6.5.2 Security Functional Requirements Related to Security Objectives

The following table should give a rationale that all Security Objectives are covered by at least one SFR.

Table 18 – Security Functional Requirements Related to Security Objectives

Objective	Functional Requirement	Rationale
O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	FIA_UAU.1 – Timing of authentication	FIA_UAU.1 requires users to be authenticated in most cases prior to gaining access to TOE functions. This ensures that only authorized users gain access to TOE functions and data.
	FIA_UID.1 -Timing of identification	FIA_UID.1 requires users to be identified in most cases prior to gaining access to TOE functions. This ensures that only authorized users gain access to TOE functions and data.
	FMT_MSA.1 - Management of security attributes	FMT_MSA.1 defines which user roles have permissions to read and modify user roles for other users.
	FMT_SMR.1 - Security roles	FMT_SMR.1 ensures the TOE supports multiple roles so that appropriate data access can be provided to users with varied responsibilities.
O.ADMIN The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE and restrict these functions from unauthorized use.	FMT_MSA.1 - Management of security attributes	FMT_MSA.1 defines the access permissions to the security attributes of the SFP.
	FMT_MSA.3 - Static attribute initialisation	FMT_MSA.3 defines the access permissions to the initial values for security attributes.
	FMT_SMF.1 - Specification of management functions	FMT_SMF.1 specifies the management functionality required for effective management of the TOE.
	FMT_SMR.1 - Security roles	FMT_SMR.1 defines the roles required to provide effective management capabilities for users with different responsibilities.
O.AUDIT	FAU_GEN.1 - Audit Data Generation	FAU_GEN.1 requires audit record to be generated for security related events within the TOE.

The TOE must generate audit records for security related events.	FAU_GEN.2 - User Identity Association	FAU_GEN.2 requires audit records to contain the username of the account initiating the action.
	FAU_SAR.1 - Audit review	FAU_SAR.1 requires that audit records be available to authorized users for review.
	FPT_STM.1 – Reliable time stamps	FPT_STM.1 requires reliable time stamps to be available for the audit records.
O.BACKUP The TOE shall backup specified client data and make it available for restore operations.	FDP_ACC.1 – Subset access control	FDP_ACC.1 ensure that the backup data is created as directed and is available to be restored as required
	FDP_ACF.1 – Security attribute-based access control	FDP_ACF.1 ensure that the backup data is created as directed and is available to be restored as required.
	FDP_BCK_EXT.1 – Client Data Backup/Restore	FDP_BCK_EXT.1 ensure that the TOE supports backup and restore operations
	FMT_MSA.1 – Management of security attributes	FMT_MSA.1 ensures that appropriate security attributes are maintained for subjects and objects.
	FMT_MSA.3 – Static attribute initialisation	FMT_MSA.3 ensures that default attributes are restrictive in nature.
O.IDENTAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	FIA_UID.1 – Timing of identification	FIA_UID.1 ensures that users are identified before every security relevant action, thus ensuring that only authorized users have access to the TOE.
	FIA_UAU.1 – Timing of authentication	FIA_UAU.1 ensures that users are authenticated before performing any security relevant action, thus ensuring that only authorized users have access to the TOE.
O.PROTECT The TOE must ensure the integrity of all TSF data, including audit records, by protecting itself from unauthorized access.	FDP_ACC.1 - Subset access control	FDP_ACC.1 defines the subject, objects, and operations applicable to the access control policy.
	FDP_ACF.1 - Security attribute based access control	FDP_ACF.1 defines the security attributes and rules to the access control policy that determines access to TSF data.
	FIA_UAU.1 – Timing of authentication	FIA_UAU.1 ensures that users must be authenticated prior to access to TSF data, thereby preventing unauthorized access.
	FIA_UID.1 -Timing of identification	FIA_UID.1 ensure that users must be identified prior to access to TSF data, thereby preventing unauthorized access.

	FMT_MSA.1 - Management of security attributes	FMT_MSA.1 provides the functionality that determines the attributes used by the access control policy.
	FMT_MSA.3 - Static attribute initialisation	FMT_MSA.3 provide the functionality that determines the attributes used by the access control policy.
	FMT_SMR.1 - Security roles	FMT_SMR.1 provides the roles that are used to restrict access to TSF data.
O.TIME The TOE must provide reliable timestamps.	FPT_STM.1 - Reliable time stamps	FPT_STM.1 requires the provision of accurate time stamps.
O.TRAFFIC The TOE must ensure that the internal traffic and the traffic between the management interface and the TOE user is secured.	FTP_TRP.1 – Trusted Path	FTP_TRP.1 requires that the communication path must be trusted.

6.5.3 Security Assurance Requirements Rationale

EAL2 was chosen since it is best suited to address the stated security objectives of the TOE. EAL2 provides a fundamental level of assurance by requiring independent testing and a review of the product's security features. This level ensures that the product meets a basic standard of security without demanding extensive formal design documentation. It allows vendors to demonstrate that their product's security measures are effective while benefiting from the Common Criteria Recognition Agreement, recognized internationally. The chosen assurance level offers an ideal balance between security and cost-effectiveness, making it a practical choice for achieving security assurance

6.6 Requirements Dependency Rationale

6.6.1 Rationale Showing that Dependencies are Satisfied

The SFRs in this ST satisfy all the required dependencies listed in the Common Criteria. The table in this section lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As it is indicated by the table, all dependencies are fulfilled.

6.6.2 Security Functional Requirements Dependencies

The following table provides a summary of the SFRs and their dependencies.

Table 19 - Summary of Security Functional Requirements Dependencies

Component	Dependency	Which is:
FAU_GEN.1	FPT_STM.1	Included
FAU_GEN.2	FAU_GEN.1	Included
	FIA_UID.1	included

FAU_SAR.1	FAU_GEN.1	Included
FDP_ACC.1	FDP_ACF.1	Included
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Included
FDP_BCK_EXT.1	No dependencies	-
FIA_UAU.1	FIA_UID.1	Included
FIA_UID.1	No dependencies	-
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 Included FMT_SMR.1 Included FMT_SMF.1 Included
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Included
FMT_SMF.1	No dependencies	-
FMT_SMR.1	FIA_UID.1	Included
FPT_STM.1	No dependencies	-
FTP_TRP.1	No dependencies	-

7 TOE Summary Specification

Each of the security requirements and the associated descriptions correspond to a security functionality. In this section each security functionality is described by how it specifically satisfies each of its related requirements.

Table 20 - TSF

TOE Security Functionality	SFR	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit Review
User Data Protection	FDP_ACC.1	Complete access control
	FDP_ACF.1	Security attribute based access control
	FDP_BCK_EXT.1	Client data Backup/Restore
Identification and authentication	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing identification
Security Management	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
Protection of the TSF	FPT_STM.1	Reliable time stamps
Trusted Path/Channels	FPT_TRP.1	Trusted path

7.1 Security Audit

The Backup Admin and Auditor has access to the audit records through the Command Center. The Audit Trail feature allows you to track the operations of users who have access to the TOE. This security functionality is used when you want to determine the source of a detrimental operation that was performed in the TOE. Information about audited operations is saved in the CommServe database. Data is kept according to the data retention settings for Audit Trail. The TOE records audit records for the events and actions listed in Table 16 – Audit Record Contents, the startup and shutdown of audit functions and all auditable events at the not specified level of audit. Audit information can be viewed on the Audit Trail report within Command Center.

The startup/shutdown of the TOE is logged on the filesystem.

Each job (backup or restore operation) contains a standalone log file which can be reviewed one by one in the Command Center. This is the event log.

The TSF also associate each auditable event with the identity of the user that caused the event.

The Backup and Restore events are logged and that the audit record contains the Date and time of the event, type of event, subject identity (if applicable) and the outcome of the event.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1

7.2 User Data Protection

The Role Based Access Control SFP is used to maintain access to the backup plans. The SFP determines for each TOE users the available operations in the Command Center. With appropriate privileges the TOE users are able to query, create, modify or delete backup plans.

Backups occur on schedule based on the plan configuration or by manually initiating the backup. In the backup phase, the client backup process reads the binary data from the ESXI and sends the data across to the MediaAgent over pipeline. When this stream reaches MediaAgent, indexing of the data is performed and the index is stored on the MediaAgent. Data is then written down on the storage target (library). During the Restore phase the administrator initiates the restore function where the MediaAgent performs the Index browse to find the data to be restored. The data is sent from the MediaAgent through the Access Node

component, then it is sent to the ESXI client using the ESXI API. When the restore is finished the administrators is notified. The data is sent in an encrypted way and is decrypted on the Access Node, then sent to the ESXI over an encrypted communication pipe.

The client's data is compressed, and deduplication by capturing signatures on the chunk of data. This is sent to the deduplication database and it if the signature is not already contained within the databases, the new signature, and block of data will be sent to the database and storage respectively. The deduplication saving can be reviewed by navigating to the general information of the specific storage.

The Backup Admin can initiate backup and restore operations.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_BCK_EXT.1

7.3 Identification and authentication

The TOE identifies and authenticates all TOE users before allowing access to any TSF-mediating functionality (except for the publicly accessible endpoints). The authentication functionality is used to verify the credentials typed by the user. All TOE users must enter their credentials (password) into the Command Center's Login Page to be authenticated, and the authentication is performed by the Command Center. Furthermore, CA-based authentication is required on the Command Center.

There are three publicly accessible endpoints on the TOE:

- (*<TOE_IP>/commandcenter/webServiceStatus.do)* for web service status
- (*<TOE_IP>/downloads/sqlscripts/*) for end user scripts
- (*<TOE_IP/publicdownloads/sqlscripts/*) for end user scripts

TOE Security Functional Requirements Satisfied: FIA_UAU.1, FIA_UID.1

7.4 Security Management

The TOE maintains the following roles: Backup Admin, Auditor

The Application Admin's credentials have to be used when logged in to the Command Center as Backup Admin to communicate with the ESXI API through the VSA interface.

The Backup Admin has access to all management functions, backup and restore client data, manage and review jobs, creating/managing users and associate them with roles, review audit records and manage the encryption policy. This role can also manage the key rotation policy to rotate the cryptographic keys.

The Auditor has read only access to audit logs and other TOE data such as plans, users, encryption policy, disks; but does not have permission to view or modify the key rotation policy. The Auditor is also only able to modify its own parameters.

TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1

7.5 Protection of the TSF

The TOE is configured to synchronize with the Microsoft NTP server which provides the time stamps used to record audit logs. The TOE uses the following method to ensure that the timestamp is reliable:

Commvault automatically tracks the system time and detects clock resets and time changes on the CommServe server. When a time skew is detected, the system temporarily stops data aging operations. The system then asks the user to confirm the time change via email, or via an alert when restarting CommServe services in the event of a reboot operation.

TOE Security Functional Requirements Satisfied: FPT_STM.1

7.6 Trusted path/channels

The Command Center can be reached through an encrypted TLSv1.2 communication protocol in the browser. The communication between the TOE components is protected with certificate-based encryption mechanism. To set up the encryption policy between the TOE components we can create network topologies through the Command Center where we can specify the tunnel port where the encrypted communication will flow. The communication is secured between the CS/MediaAgent with RSA 3072-bit algorithm and AES-256 encryption. Between the VSA/MediaAgent TLSv1.2 using RSA 3072-bit algorithm and AES-256 encryption is used.

TOE Security Functional Requirements Satisfied: FTP_TRP.1

8 Acronyms

Table 21 - Acronyms

Acronym	Meaning
IT	Information Technology
CC	Common Criteria
OSP	Organizational Security Policy
SA	Security Association
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

DDB	Deduplication Database
IDM	Intelligent Data Management
CS	CommServe
MA	MediaAgent
VSA	Virtual Server Agent
VM	Virtual Machine
NTP	Network Time Protocol
RPO	Recovery Point Objective
RSA	Rivest–Shamir–Adleman (cryptography)
TLS	Transport Layer Security
AES-CBC	Advanced Encryption Standard-Cipher Block Chaining
AES-GCM	Advanced Encryption Standard-Galois/Counter Mode
SSL	Secure Sockets Layer
NBD	Network Block Device

9 Bibliography

[CC_P1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version CC:2022, November 2022, CCMB-2022-11-001

[CC_P2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation Part 2: Security Functional components, Version CC:2022, November 2022, CCMB-2022-11-002

[CC_P3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version CC:2022, November 2022, CCMB-2022-11-003

[CC_P4] Common Criteria, Part 4: Common Criteria for Information Technology Security Evaluation Part 4: Framework for the specification of evaluation methods and activities, Version CC:2022, November 2022, CCMB-2022-11-004

[CC_P5] Common Criteria, Part 5: Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, Version CC:2022, November 2022, CCMB-2022-11-005

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version CC:2022, November 2022, CCMB-2022-11-006

[AGD] A Commvault Systems Inc. Guidance document, Commvault Platform Release CPR2025E (11.42.41) Evaluation Assurance Level (EAL): EAL2, Version: 1.9, 19 February 2026

[CPR2023E] Offline product documentation, “11.32_offlinedocs.zip”, v1.0

[CPR_2025E] Offline product documentation, “11.42_offlinedocs.zip”, v1.0