Rubrik Inc.

Cloud Data Management

v8.1.0

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.0

Prepared for:

Rubrik Inc.
3495 Deer Creek Road
Palo Alto, CA 94304
United States of America

Phone: +1 844 478 2745
www.rubrik.com

Prepared by:

Corsec Security, Inc.
12600 Fair Lakes Drive, Suite 210
Fairfax, VA 22003
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Figures

List of Tables

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the Rubrik Inc. (Rubrik) Cloud Data Management and will hereafter be referred to as the TOE throughout this document.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs to which the TOE adheres.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the SFRs and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

The following table shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	*Rubrik Inc. Cloud Data Management v8.1.0 Security Target*
ST Version	Version 1.0
ST Author	Corsec Security, Inc.
ST Publication Date	2024-05-16
TOE Reference	Rubrik CDM[1] v8.1.0
Guidance Supplement	Rubrik CDM v8.1.0 Guidance Documentation Supplement Document Version: 1.0

[1] CDM – Cloud Data Management

1.3 TOE Overview

Rubrik Cloud Data Management is a software platform that distributes data, metadata, and task management across the cluster to deliver predictive scalability and eliminate performance bottlenecks. A Rubrik cluster is a collection of objects that includes sources from where data is getting backed up, targets where backups are stored, and security principals, or the users and service accounts, that manages the cluster.

Figure 1 –TOE Components

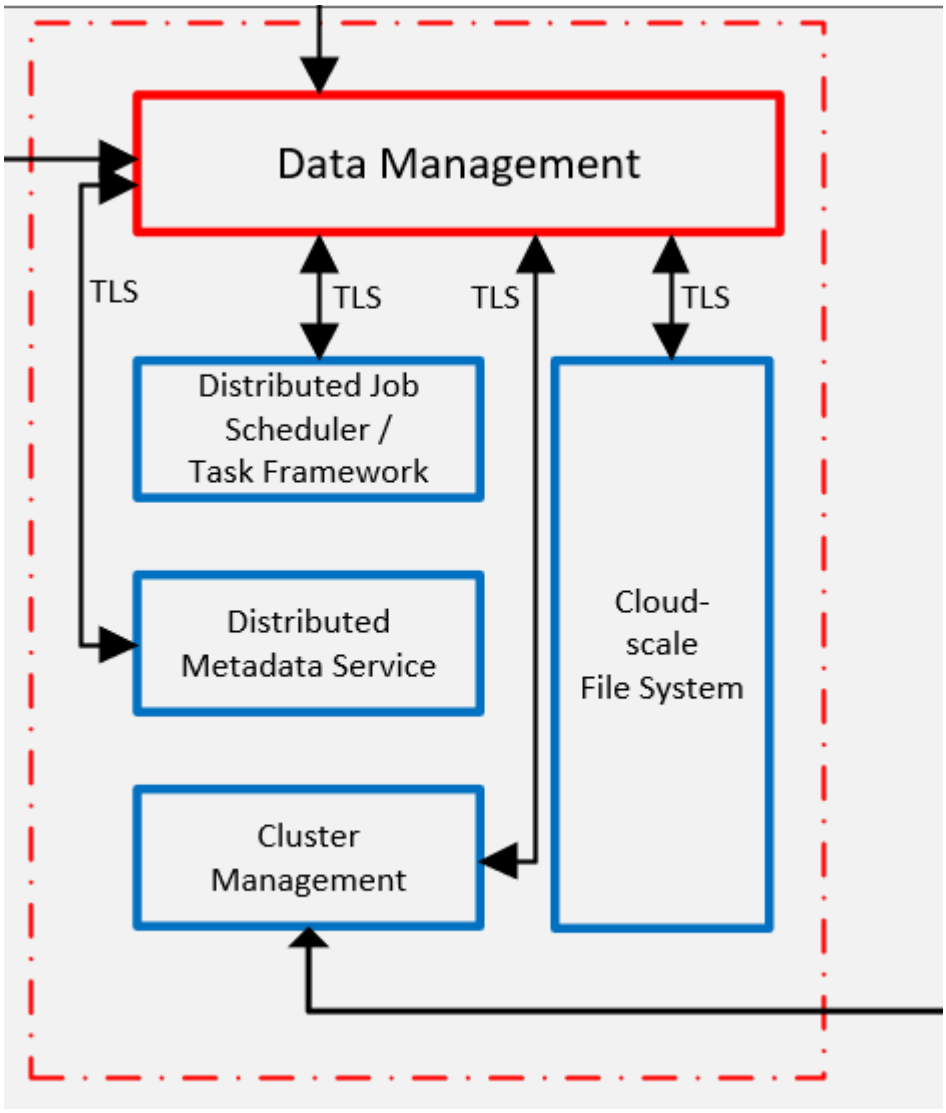

Table 2 – TOE Components

Component	Description
Core	comprised of the file system, metadata service, cluster management, and task framework
Data Management	• organizing, removing redundancy, and making data available for search • administrative interface

The usage and major security features of the TOE are described in detail within Section 1.6.2 and its consequent subsections.

1.3.1 Core

Rubrik Cloud-Scale File System
Rubrik Cloud-Scale File System is a distributed file system that stores and manages versioned data.

- Fault Tolerant: it is resilient to multiple node and disk failures, employing an intelligent replication scheme to distribute multiple copies of data throughout the cluster
- Storage Efficient: it utilizes zero-space clones to make multiple copies of data from one "golden image"
- Scale-out NAS server: it appears as a scale-out NAS[2] server to any host when a snapshot is mounted

Rubrik Distributed Metadata System
Rubrik Distributed Metadata System provides a high-speed index, continuous availability, linear scalability, and operational simplicity with no single point of failure in the cluster. It handles large amounts of data, distributes replicas of data across nodes, and provides low latency operations.

Rubrik Cluster Management
Rubrik Cluster Management manages the Rubrik system setup and ongoing system health. Its zero-configuration multicast DNS protocol automates appliance discovery – the cluster expands with minimal manual intervention with new nodes autodiscovering each other. Post system setup, it maintains the status of each node by performing health checks on individual nodes.

Rubrik Distributed Task Framework
Rubrik Distributed Task Framework is the engine that globally assigns and executes tasks across the cluster. Tasks are load balanced across the entire cluster, and are distributed to the nodes that house the impacted data. This engine runs on all nodes and incorporates a masterless architecture where all nodes cooperatively schedule and run tasks.

1.3.2 Data Management

Rubrik Data Management

- stores versions of data using full snapshots with forward incremental and reverse incremental copies
- ensures data integrity with multiple checks within the file system and data management layers
- applies content-aware global deduplication and compression

Admin GUI

- web interface for administrators

1.4 TOE Functionality

Auto-Configuration
Upon startup, the TOE invokes multicast DNS[3] protocols to automatically discover and self-configure each of the nodes within the cluster. The operator assigns IP addresses to each of the nodes and login credentials for the virtualized primary environment to be managed. The cluster size is expanded by assigning new IP[4] addresses through the management dashboard, and it is reduced by selecting nodes to be removed. Thereafter, the cluster automatically self-adjusts and re-balances to deliver fault tolerance against node and disk failures.

[2] NAS – Network Attached Storage
[3] DNS - Domain Name Service
[4] IP - Internet Protocol

Automated Data Discovery
Once the credentials for its virtualized environment are entered, the TOE auto-discovers details of the entire virtualized environment, such as hosts and applications. The TOE utilizes VMware APIs (vStorage APIs for Data Protection) to discover VMware environments.

Dynamic Policy Engine
From the list of discovered Virtual Machines (VMs), the operator selects which VMs to protect and what SLA[5] policies to apply for recovery. An SLA policy is made of 4 components:

- Frequency of backup
- Retention of backups
- Archival policy (when data is archived for long-term retention)
- Replication to another Rubrik cluster for Disaster Recovery restore purposes

SLA policies are pre-configured based on industry standards, so there is no configuration of individual jobs or tasks for scheduling or data movement between archival or replication targets.

New SLA domain policies are created by specifying the desired snapshot capture frequency and data retention policy.

High Speed Data Ingestion
The TOE is a high-speed data ingestion engine that handles large volumes of data, with a distributed workflow management system that maximizes the number of parallel data streams processed. As it is a web-scale system, performance increases at a linear pace as more nodes are added to the cluster.

For VMware environments, VMware's Changed Block Tracking is used to identify and copy only the changed blocks from the previous operation. Global deduplication and compression are applied before the data is stored in the file system. All metadata is stored in a flash tier for rapid access in a search pulldown. Data is distributed across multiple nodes to deliver a fault tolerant file system.

Fast Global File Search
As a query is entered, the TOE expedites the query by displaying suggested search results with auto-complete functionality, allowing for fast location of specific versions of files across all VMs.

Instant Recovery
Backup software and globally deduplicated backup storage are combined into a single software fabric that serves as a storage endpoint to recover as many VMs as needed. Post-recovery, users can put the VMDK[6] in the primary storage environment or continue using the TOE. Writes and reads are gathered on the flash tier to deliver performance required by the recovered application.

Live Storage for DevOps
The TOE provides multiple copies to developers from just one "golden image", using cloning capabilities to allow any number of mounts to be created without requiring additional storage capacity. Provisioning as many copies as needed without impacting storage capacity and within a sandbox environment to prevent any network conflicts. As the provisioned data set is altered, the TOE stores the deltas by forking to a new branch. The journaled Cloud-Scale File System accelerates and provisions the latest data for application development. The TOE allocates the flash tier for all writes and hot reads when utilizing Live Storage.

[5] SLA – Service Level Agreement
[6] VMDK – Virtual Machine Disk

Rubrik clusters access VM data through a connection with the VMware vCenter Server that manages the hypervisor running the VM. To successfully connect with a vCenter Server, Rubrik clusters require connection information for that vCenter Server.

1.5 TOE Environment

The TOE runs in a VMware VM provisioned by an ESXi hypervisor, with the following:

- 2 virtual CPUs[7] at 4GHz[8]
- 16 GB[9] RAM[10]
- Minimum 500GB hard drive

The VM that hosts the TOE must have an IPv4 address that is reachable on port 443 by Rubrik clusters that connect to the instance.

1.6 TOE Description

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

1.6.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE. The TOE components that are part of the physical scope are described in detail in sections 1.3.1 and 1.3.2.

[7] CPU – Central Processing Unit
[8] GHz - Gigahertz
[9] GB - Gigabyte
[10] RAM – Random Access Memory

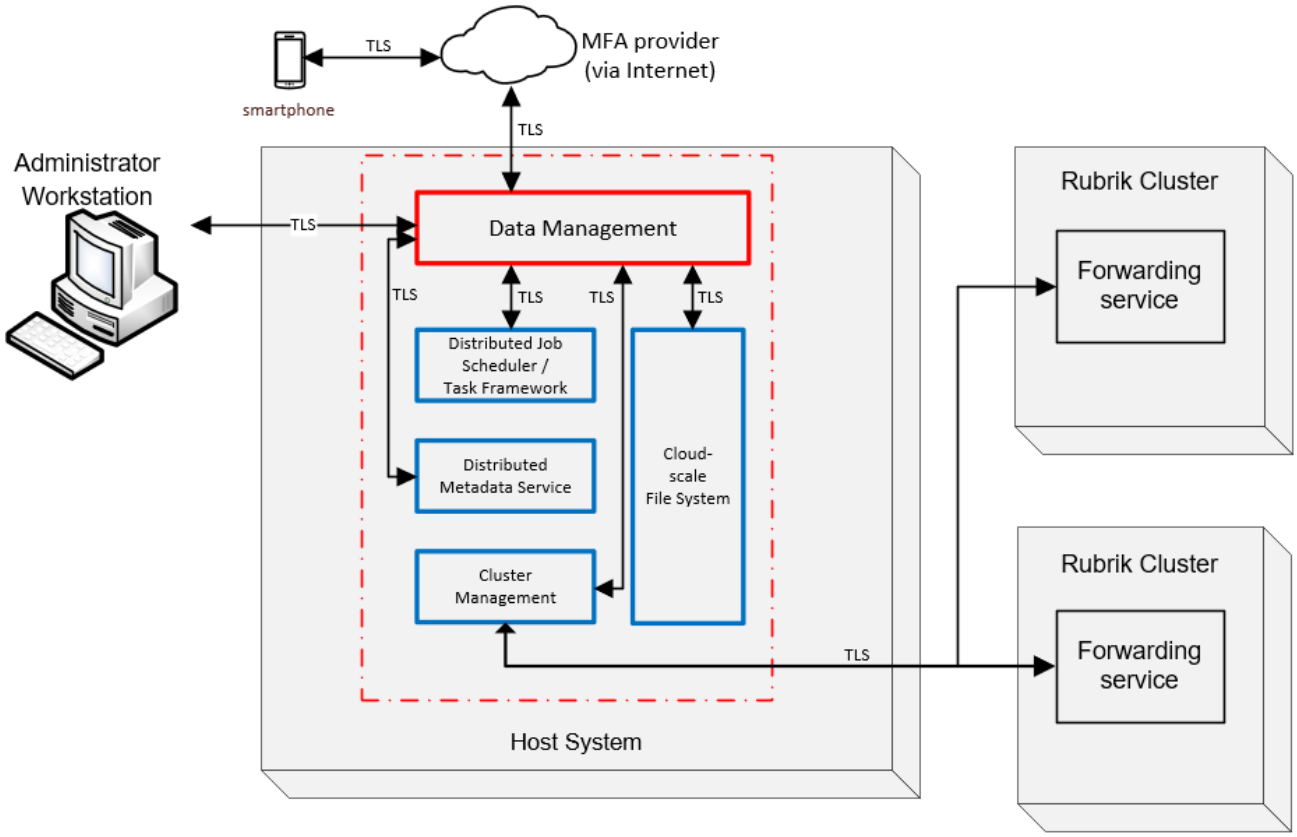

Figure 2 – Physical TOE Boundary

1.6.1.1 TOE Software

The TOE is a software-only TOE and is comprised of Rubrik Edge in an OVA[11] format installed in a VM.

1.6.1.2 Required Non-TOE Components

The TOE requires the following non-TOE components:

- VMware ESXi, which is the host server for Rubrik Edge running in a VM
- Rubrik Backup Connector, which is installed on each backup source, is required to do a backup of the physical infrastructure.

1.6.1.3 Guidance Documentation

The following PDF guide, available for download through the Rubrik website, is required reading and part of the TOE:

- *Rubrik CDM v8.1.0 Guidance Documentation Supplement Document Version: 1.0.pdf*

1.6.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The SFRs implemented by the TOE are usefully grouped under the following Security Function Classes:

[11] OVA – Open Virtual Appliance

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- User Data Protection

The internal components Cluster Management, Cloud-Scale File System, Data Management Layer and Distributed Job Scheduler, talk to other instances of the same component on other nodes using a Thrift RPC protocol. This protocol is implemented on top of an encrypted, TLS[12] based transport layer. To prevent man-in-the-middle attacks, all internode TLS connections are verified using a private key and a public key certificate shared by all nodes in the cluster (data in flight encryption), using both client and server certificate. The key (2048-bit RSA) and the certificate (self-signed including the clusters' UUID in the name) are generated when the customer first installs the Rubrik cluster ("bootstrapping"), and are known only by nodes within that cluster. In addition, the private key and the certificate are distributed to all nodes during bootstrap via a Thrift RPC[13]. Prior to and during bootstrap, this Thrift RPC uses a fixed TLS certificate and private key shipped with all nodes. After bootstrap, the new per-cluster certificate and private key are used.

1.6.2.1 Security Audit

The TOE provides extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, and the outcome of the event.

1.6.2.2 Cryptographic Support

The TOE provides cryptography in support of remote administrative management via TLS/HTTPS[14].

1.6.2.3 Identification and Authentication

The TOE provides authentication services for local and AD[15] administrative users wishing to connect to the TOE's Secure Web UI administrator interface.

The TOE requires authorized administrators to authenticate prior to being granted access to any of the management functionality. After successful authentication, the TOE determines the permitted level of access for a user based on the local authorization setting for that user and provides role-based access.

When a Rubrik node joins a new AD domain, it temporarily obtains domain admin credentials to create a TOE service account in AD. The domain admin credentials are never stored on disk (but temporarily stored in memory) on the TOE.

1.6.2.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs through a secure TLS/HTTPS session, or via a local console connection. The TOE supports an Administrator role.

There are two primary use cases that shape the default TOE RBAC[16] roles: Administrator, and End User.

[12] TLS – Transport Layer Security
[13] RPC – Remote Procedure Call
[14] HTTPS – Hypertext Transport Protocol - Secure
[15] AD – Active Directory
[16] RBAC – Role Based Access Control

1.6.2.5 Protection of the TSF

The TOE provides timestamps for local audit log entries, in addition to the date/time information provided by audit log and event log entries forwarded to it by Rubrik clusters.

1.6.2.6 User Data Protection

The TOE limits the execution of commands and the ability to change usernames and passwords to authorized administrators only.

1.6.3 Product Physical/Logical Features and Functionality not included in the TOE

Features and/or Functionality that are not part of the evaluated configuration of the TOE include:

- Command Line Interface

2. Conformance Claims

This section and Table 3 provide the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM[17] were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented (Augmented with Flaw Remediation (ALC_FLR.1))

[17] CEM – Common Evaluation Methodology

3. Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies to which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel, and connectivity aspects

3.1 Threats to Security

Table 4 – Assets

Name	Description
A.DATA	Sensitive or security functional data contained in TOE backups, both locally and archived across all mediums supported by the TOE.
A.KEY	Cryptographic keys contained in the TOE, for encryption of 'data in flight'.

Table 5 – Threat Agents

Name	Description
T.ADMIN	Authorized person/process that performs installation and configuration/setup of the TOE to ensure that the TOE operates according to the needs of the enterprise/organization.
T.ATTACKER	A person/company or process with skills and resources to mislead the system in any way necessary to reveal/divulge/misuse data and prevent the system from intended operations.

Table 6 – Threats to the TOE

Name	Threat Agent	Asset	Description
TT.ADMIN_ERROR	T.ADMIN	A.DATA	During operation, the administrator unintentionally configures the TOE incorrectly, making the TOE inoperable or resulting in ineffective security mechanisms.
TT.ADMIN_EXPLOIT	T.ATTACKER	A.DATA	A person/company uses hacking methods to exploit missing, weak or incorrectly implemented access control in the TOE.
TT.CRYPTO_COMPROMISE	T.ATTACKER	A.DATA and A.KEY	An attacker cause key or data associated with the cryptographic functionality to be inappropriately accessed (viewed/modified/deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
TT.HACK_ACCESS	T.ATTACKER	A.DATA	A person/company uses hacking methods to exploit missing, weak or incorrectly implemented access control in the TOE.
TT.MALFUNCTION	T.ATTACKER	A.DATA and A.KEY	A malfunction in the TOE implies unauthorized access to TOE resources.

Table 7 – Threats to the TOE Environment

Name	Threat Agent	Asset	Description
TE. EAVESDROPPING	T.ATTACKER	A.DATA	An unauthorized person with no physical access to TOE is eavesdropping on the communication between Rubrik nodes to intercept information.

3.2 Organizational Security Policies

Table 8 – OSPs

Name	Description
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHIC	The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 9 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 9 – Assumptions

Name	Description
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A. TRUSTED_ADMIN	The administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.

4. Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 10 below.

Table 10 – Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.
O.AUDIT	The TOE shall record and maintain security-related events to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.
O.CRYPTOGRAPHY	The TOE shall provide cryptographic functions to maintain the confidentiality of 'data in flight'.
O.MANAGE	The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.
O.PROTECTION	The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 Non-IT Security Objectives

Table 11 – Non-IT Security Objectives

Name	Description
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines as indicated by Rubrik and any additional trusted parties in which an agreement has been entered.

5. Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

The following extended component has been included in this Security Target because the Common Criteria components were found to be insufficient as stated.

Table 12 –Extended Security Functional Component

Explicit Component	Identifier	Description
FAU_GEN_EXT.1	Audit data generation	The TOE enables auditing during cluster initialization, and auditing remains operational for the entire period of time that the TOE is operating.

5.1.1 Family FAU_GEN_EXT: Audit Data Generation

5.1.1.1 Audit Data Generation (FAU_GEN_EXT.1)

Family Behavior

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

Component Leveling

Figure 3 – FAU_GEN_EXT.1: Audit Data Generation Component Levelling

FAU_GEN_EXT.1 The TOE enables auditing during cluster initialization, and auditing remains operational for the entire period of time that the TOE is operating.

Management: FAU_GEN_EXT.1
The following actions could be considered for the management functions in FMT:

- There are no management activities foreseen.

Audit: FAU_GEN_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

- there are no auditable events foreseen.

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

6. Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Completed assignment statements within a selection statement are identified using [*underlined and italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 13 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 13 – TOE Security Functional Requirements

Functional Class	Name	Description	S	A	R	I
FAU: Security audit	FAU_GEN_EXT.1	Audit data generation	✓	✓		
	FAU_GEN.2	User identity association				
	FAU_SAR.1	Audit Review		✓		
FCS: Cryptographic support	FCS_CKM.1	Cryptographic key generation		✓		
	FCS_CKM.4	Cryptographic key destruction		✓		
	FCS_COP.1	Cryptographic operation		✓		
FDP: User data protection	FDP_ACC.1	Subset Access Control		✓		
	FDP_ACF.1	Security attribute based access control		✓		
FIA: Identification and authentication	FIA_ATD.1	User attribute definition		✓		
	FIA_UAU.1	Timing of authentication		✓		
	FIA_UID.1	Timing of identification		✓		

Functional Class	Name	Description	S	A	R	I
FMT: Security management	FMT_MTD.1	Management of TSF[18] data	✓	✓		
	FMT_SMF.1	Specification of Management Functions		✓		
	FMT_SMR.2	Restrictions on security roles		✓		
	FMT_MSA.1	Management of security attributes	✓	✓		
	FMT_MSA.3	Static attribute initialization	✓	✓		
FPT: Protection of the TSF	FPT_STM.1	Reliable time stamps				

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

6.2.1 Class FAU: Security Audit

FAU_GEN_EXT.1 Audit data generation

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN_EXT.1.1

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

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

b) [**All administrative actions and the following security events:**

- **Resuming all protection activity,**
- **Pausing all protection activity**].

FAU_ GEN_EXT.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, [**None**].

FAU_GEN.2 User identity association

Dependencies: FAU_GEN_EXT.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.

FAU_SAR.1 Audit review

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [*authorized users*] with the capability to read [*all audit and event 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.

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

[18] TSF – TOE Security Function

Dependencies: 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 [*AES Counter_DRBG*] and specified cryptographic key sizes [*128 bits*] that meet the following: [*NIST[19] SP[20] 800-90A*].

FCS_CKM.4 Cryptographic key destruction

Dependencies: 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 [*overwrite with 0s and 1s*] that meets the following: [*standard industry practice*].

FCS_COP.1 Cryptographic operation

Dependencies: FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1

The TSF shall perform [*cryptographic operations in Table 14*] in accordance with a specified cryptographic algorithm [*see Table 14*] and cryptographic key sizes [*see Table 14*] that meet the following: [*see Table 14*].

Table 14 – Cryptographic Operations

Operation	Algorithm	Key size(s)	Standard
Encryption / decryption	AES[21]	128, 256	FIPS[22] PUB[23] 197
Encryption / decryption	RSA[24]	2048	
Hashing	SHA[25]-1, SHA-256, SHA-384, SHA-512		FIPS PUB 180-4
HMAC[26]	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512		FIPS PUB 198-1
Key agreement	EC[27] Diffie-Hellman	256, 384, 512	

6.2.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1

The TSF shall enforce the [*Administrator Access Control SFP[28]*] on [*subjects: authorized administrator, objects: commands, operations: execute*].

FDP_ACF.1 Security attribute based access control

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1

[19] National Institute of Standards and Technology
[20] SP – Special Publication
[21] AES – Advanced Encryption Standard
[22] FIPS - Federal Information Processing Standard
[23] PUB - Publication
[24] RSA – Rivest Shamir Adelman
[25] SHA – Simple Hashing Algorithm
[26] HMAC – Keyed Message Authentication Code
[27] EC – Elliptic Curve
[28] SFP – Security Function Policy

The TSF shall enforce the [*Administrator Access Control SFP*] to objects based on the following: [*subjects: authorized administrator; subject attributes: user name, password; object: commands; object attributes: none*].

6.2.4 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [
a) *User identity:* ***user name****;*
b) *Local authentication data:* ***password****;*
c) *Authorizations:* ***access rights***; and
d) ***Email address***].

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1

The TSF shall allow [*entry of username and corresponding password*] 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.

FIA_UID.1 Timing of identification

FIA_UID.1.1

The TSF shall allow [*entry of username and corresponding password*] 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.

6.2.5 Class FMT: Security Management

FMT_MTD.1 Management of TSF data

Dependencies: FMT_SMR.2 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1

The TSF shall restrict the ability to [*manage*] the [*TSF data*] to [*authorized administrators*].

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*administer the TOE remotely*].

FMT_SMR.2 Restrictions on security roles

Dependencies: FIA_UAU.1 Timing of authentication

FMT_SMR.2.1

The TSF shall maintain the roles: [*Administrator, End User*].

FMT_SMR.2.2

The TSF shall be able to associate users with roles.

FMT_SMR.2.3

The TSF shall ensure that the conditions [*only the authorized administrator shall administer the TOE remotely*] are satisfied.

FMT_MSA.1 Management of security attributes

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.2 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1

The TSF shall enforce the [*Administrator Access Control SFP*] to restrict the ability to [modify] the security attributes [*in Administrator Access Control SFP*] to [*authorized administrators*].

FMT_MSA.3 Static attribute initialization

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.2 Security roles

FMT_MSA.3.1

The TSF shall enforce the [*Administrator Access Control SFP*] to provide [no] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*authorized administrator*] to specify alternative initial values to override the default values when an object or information is created.

6.2.6 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2+ augmented with ALC_FLR.1. Table 15 summarizes these requirements.

Table 15 – 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 a CM system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.1 Basic Flaw Remediation
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

7. TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 16 lists the security functionality and their associated SFRs.

Table 16 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN_EXT.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of identification
Security Management	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.2	Restrictions on security roles
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
Protection of TOE Security Functionality	FPT_STM.1	Reliable time stamps
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control

7.1.1 Security Audit

The TOE generates a comprehensive set of audit logs that identify specific TOE operations whenever an auditable event occurs. Potentially time-sensitive notifications and completed replication tasks are recorded.
FAU_GEN_EXT.1

The TOE ensures that each auditable event is associated with the user that triggered the event. For an IT entity or device, the VM name of the endpoint is included in the audit record.
FAU_GEN.2

The TOE provides a source of date and time information used in audit event timestamps.
FPT_STM.1

The administrators are allowed to read the audit records, but they have no other access privileges to the buffer containing the audit log.

The TOE receives audit log and event log entries from the connected Rubrik clusters.
FAU_SAR.1

7.1.2 Cryptographic Support

The TOE uses TLS to protect administrative communications using the Web GUI. TLS is also used to protect communications between the components of the TOE, and the TOE's communication with clusters that it remotely administers. For TLS session keys, the TOE uses symmetric AES keys to encrypt and decrypt data.

The TOE utilizes the Rubrik Cryptographic Library (CMVP[29] #2658) for all cryptographic functions.

Keys are generated via the use of the Counter_DRBG to provide random keying material.
FCS_CKM.1

The TOE provides zeroization techniques that meets the FIPS 140-2 zeroization requirement for all plaintext secret and private keys. TLS session keys reside in volatile memory only and are never stored persistently.
FCS_CKM.4

The TOE provides cryptographic capabilities to support the operations listed in Table 14.
FCS_COP.1

7.1.3 Identification and Authentication

User account information is stored in the TOE and contains the following attributes for local users:

- User name – The logon name of the user.
- Email address – The valid email address for the user.
- Password – The user must use a strong password.
- Access rights - By default, the TOE sets all new local user accounts to the Administrator authorization level.

FIA_ATD.1

Each individual must be successfully identified and authenticated with a username and password by the TSF before access is allowed to the TOE.

No actions are allowed, other than entry of identification and authentication data, until successful identification and authentication.
FIA_UAU.2, FIA_UID.2

7.1.4 Security Management

The TOE provides permissive default values for security attributes.
FMT_MSA.3

The TOE permits an authorized administrator to specify alternative initial values.

[29] CMVP – Cryptographic Module Validation Program

FMT_MSA.3

The ability to modify the security attributes is restricted to authorized administrators.
FMT_MSA.1

The TOE restrict management activities to authorized administrators.
FMT_SMF.1

The TOE supports the following roles:

- Administrator –operator with full access to all functionality that is available through the Web UI
- End User –operator with access only to assigned objects

FMT_SMR.2

7.1.5 Protection of the TSF

The TOE provides timestamps for local audit log entries, in addition to the date/time information provided by audit log and event log entries forwarded to it by Rubrik clusters.
FPT_STM.1.

7.1.6 User Data Protection

The ability to execute commands is restricted to authorized administrators.
FDP_ACC.1

The ability to change usernames and passwords is restricted to authorized administrators.
FDP_ACF.1

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 5.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat and assumption that compose the Security Target. Sections 8.2.1 and 8.2.2 demonstrate the mappings between the threats and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 17 below provides a mapping of the objectives to the threats they counter.

Table 17 – Threats: Objectives Mapping

Threats	Objectives	Rationale
TT.ADMIN_ERROR An administrator unintentionally configures the TOE incorrectly, making the TOE inoperable or resulting in ineffective security mechanisms.	O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	The objective O.MANAGE provides administrators the capability to view and manage configuration settings.
	OE.TRUSTED_ADMIN The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines as indicated by Rubrik and any additional trusted parties in which an agreement has been entered.	The objective OE.TRUSTED_ADMIN ensures that the administrators are non-hostile and are trained to appropriately manage and administer the TOE.
TT.ADMIN_EXPLOIT A person/company uses hacking methods to exploit missing, weak or incorrectly implemented access control in the TOE.	O.ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	The objective O.ACCESS includes mechanisms to authenticate TOE administrators and place controls on administrator sessions.
	O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	The objective O.MANAGE restricts access to administrative functions and management of TSF data to the administrator.
	OE.TRUSTED_ADMIN The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines as indicated by Rubrik and any additional trusted parties in which an agreement has been entered.	The objective OE.TRUSTED_ADMIN ensures that the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.

Threats	Objectives	Rationale
TT.CRYPTO_COMPROMISE An attacker causes key or data associated with the cryptographic functionality to be inappropriately accessed (viewed/modified/deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.	O.PROTECTION The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.	The objective O.PROTECTION ensures that the TOE will have adequate protection from external sources and that all TOE Security Policy functions are invoked.
TT.HACK_ACCESS A person/company uses hacking methods to exploit missing, weak or incorrectly implemented access control in the TOE.	O.AUDIT The TOE shall record and maintain security-related events to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.	The objective O.AUDIT provides the TOE the capability to detect and create records of security-relevant events associated with users.
	O.ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	The objective O.ACCESS includes mechanisms to authenticate TOE administrators and place controls on administrator sessions.
	O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	The objective O.MANAGE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the administrator. These objectives ensure that no other user can modify the information flow policy to bypass the intended TOE security policy.
	O.PROTECTION The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.	The objective O.PROTECTION ensures that the TOE will have adequate protection from external sources and that all TOE Security Policy functions are invoked.
	OE.TRUSTED_ADMIN The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines as indicated by Rubrik and any additional trusted parties in which an agreement has been entered.	The objective OE.TRUSTED_ADMIN ensures that the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.
TT.MALFUNCTION A malfunction in the TOE implies unauthorized access to TOE resources.	O.AUDIT The TOE shall record and maintain security-related events to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.	The objective O.AUDIT provides the TOE the capability to detect and create records of security-relevant events associated with users.
	O.ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	The objective O.ACCESS includes mechanisms to authenticate TOE administrators and place controls on administrator sessions.
	O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality of 'data in flight'.	The objective O.CRYPTOGRAPHY requires the TOE to implement cryptographic services to provide confidentiality protection of data in flight.
	O.PROTECTION The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.	The objective O.PROTECTION ensures that the TOE will have adequate protection from external sources and that all TOE Security Policy functions are invoked.

Threats	Objectives	Rationale
TE.EAVESDROPPING	O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality of 'data in flight'.	The objective O.CRYPTOGRAPHY requires the TOE to implement cryptographic services to provide confidentiality protection of data in flight.
	O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	The objective O.MANAGE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the administrator.

This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Assumptions

Table 18 provides a mapping of assumptions and the environmental objectives that uphold them.

Table 18 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.PHYSICAL The TOE is installed on the appropriate, dedicated hardware and operating system.	OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	The objective OE.PHYSICAL ensures that the environment provides physical security, commensurate with the value of the TOE and the data it contains.
A. TRUSTED_ADMIN The IT environment provides the TOE with the necessary reliable timestamps.	OE.TRUSTED_ADMIN The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines as indicated by Rubrik and any additional trusted parties in which an agreement has been entered.	The objective OE.TRUSTED_ADMIN ensures that the administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.

This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.2.3 Security Objectives Rationale Relating to Organizational Security Policies

Table 19 provides a mapping of policies effectively addressed by the security objectives.

Table 19 – Policies: Objectives Mapping

Assumptions	Objectives	Rationale
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	The objective O.ACCESS requires the TOE to identify and authenticate users prior to allowing any TOE access or any TOE mediated access on behalf of those users
	O.AUDIT The TOE shall record and maintain security-related events to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.	The objective O.AUDIT provides the administrator with the capability of recording the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the administrator's user identifier is recorded when any security relevant change is made to the TOE (e.g., modifying TSF data).

	OE.TRUSTED_ADMIN The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines as indicated by Rubrik and any additional trusted parties in which an agreement has been entered.	The objective OE.TRUSTED_ADMIN ensures that the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.
P.CRYPTOGRAPHIC The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.	O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality of 'data in flight'.	The objective O.CRYPTOGRAPHY requires the TOE to implement cryptographic services to provide confidentiality protection of the TOE.

8.3 Rationale for Extended Security Functional Requirements

Table 20 – Rationale for Extended Component

Explicit Component	Identifier	Description
FAU_GEN_EXT.1	Audit data generation	This extended component is necessary to describe that the TOE enables the audit functions during cluster initialization, and that the audit functions cannot be turned on or off while the TOE is operational.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs defined for this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 21 – Mapping of SFRs to Security Objectives

Objective	SFR																
	FAU_GEN_EXT.1	FAU_GEN.2	FAU_SAR.1	FDP_ACC.1	FDP_ACF.1	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.2	FMT_MSA.1	FMT_MSA.3	FPT_STM.1
O.ACCESS				X	X				X	X	X				X	X	
O.AUDIT	X	X	X														X
O.CRYPTOGRAPHY						X	X	X									
O.MANAGE			X									X	X	X	X	X	
O.PROTECTION				X	X							X	X	X	X		
OE.PHYSICAL																	

Objective	SFR																
	FAU_GEN_EXT.1	FAU_GEN.2	FAU_SAR.1	FDP_ACC.1	FDP_ACF.1	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.2	FMT_MSA.1	FMT_MSA.3	FPT_STM.1
OE.TRUSTED_ADMIN																	

Table 22 provides a mapping of the objectives and the SFRs that support them.

Table 22 – Objectives: SFRs Mapping

Objective	SFR	Rationale
O.ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	FIA_ATD.1 User attribute definition	FIA_ATD.1 defines the attributes of users, including a user identifier that is used by the TOE to determine a user's identity and enforce what type of access the user has to the TOE, and ensures that untrusted users cannot be associated with a role and reduces the possibility of a user obtaining administrative privileges.
	FIA_UAU.1 Timing of authentication	FIA_UAU.1 ensures that users are authenticated before they are provided access to the TOE or its services. In order to control logical access to the TOE an authentication mechanism is required. The local user authentication mechanism is necessary to ensure that an administrator has the ability to login to the TOE regardless of network connectivity (e.g., it would be unacceptable if an administrator could not login to the TOE because the authentication server was down, or that the network path to the authentication server was unavailable).
	FIA_UID.1 Timing of identification	FIA_UID.1 ensures that every user is identified before the TOE performs any mediated functions.
	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 defines static attribute initialization for the Administrator Access Control SFP. FMT_MSA.1 specifies which roles can access security attributes.
	FDP_ACC.1 Subset Access Control	FDP_ACC.1 requires the TOE to enforce Access Control SFP.
	FDP_ACF.1 Security attribute based access control	FDP_ACF.1 specifies the attributes used to enforce Access Control SFP.
O.AUDIT The TOE shall record and maintain security-related events to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.	FAU_GEN_EXT.1 Audit data generation	FAU_GEN_EXT.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant event that takes place in the TOE.
	FAU_GEN.2 User identity association	FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID.
	FAU_SAR.1 Audit review	FAU_SAR.1 provides administrators the capability to read the audit records.
	FPT_STM.1 Reliable time stamps	FPT_STM.1 supports the audit functionality by ensuring that the TOE is capable of obtaining a time stamp for use in recording audit events.
O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality of 'data in flight'.	FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 ensures that the TOE is capable of generating cryptographic keys.
	FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 provides the functionality for ensuring that keys and key material is zeroized.

Objective	SFR	Rationale
	FCS_COP.1 Cryptographic operation	FCS_COP.1 requires that for data decryption and encryption an approved algorithm is used, and that the algorithm meets the standard.
O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	FAU_SAR.1 Audit Review	FAU_SAR.1 provides the administrators the capability to read all information from the audit records.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 specifies which roles can access security attributes.
	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 defines static attribute initialization for the Administrator Access Control SFP.
	FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of Management Functions FMT_SMR.2 Restrictions on security roles	FMT_MTD.1, FMT_SMF.1 and FMT_SMR.2 ensure that only the Administrator role can manage the entire TOE, and that the TOE supports both local administration and remote administration.
O.PROTECTION The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.	FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of Management Functions FMT_SMR.2 Restrictions on security roles	FMT_MTD.1, FMT_SMF.1 and FMT_SMR.2 ensure that only authorized administrators of the TOE may manage the TOE and TSF data.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 specifies which roles can access security attributes.
	FDP_ACC.1 Subset Access Control	FDP_ACC.1 requires the TOE to enforce Access Control SFP.
	FDP_ACF.1 Security attribute based access control	FDP_ACF.1 specifies the attributes used to enforce Access Control SFP.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. The following table lists each SFR to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 23 – SFR Dependencies and Rationales

SFR	Dependency	Rationale
FAU_GEN_EXT.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included
FAU_GEN.2 User identity association	FAU_GEN_EXT.1 Audit data generation FIA_UID.1 Timing of identification	Included

SFR	Dependency	Rationale
FAU_SAR.1 Audit review	FAU_GEN_EXT.1 Audit data generation	Included
FDP_ACC.1 Subset Access Control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	Included
FCS_CKM.1 Cryptographic key generation	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	Included
FCS_CKM.4 Cryptographic key destruction	[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]	Included
FCS_COP.1 Cryptographic Operation	[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	Included
FIA_ATD.1 User attribute definition	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	
FMT_MTD.1 Management of TSF data	FMT_SMR.2 Security roles FMT_SMF.1 Specification of Management Functions	Included[30]
FMT_SMF.1 Specification of Management Functions	None	
FMT_SMR.2 Restrictions on security roles	FIA_UID.1 Timing of identification	Included
FMT_MSA.1 Management of security attributes	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.2 Security roles FMT_SMF.1 Specification of Management Functions	Included[31]
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 Management of security attributes FMT_SMR.2 Security roles	Included[5]
FPT_STM.1 Reliable time stamps	None	

[30] FMT_MTD.1 has a dependency to FMT_SMR.2 which is covered by FMT_SMR.2.

[31] FMT_MSA.1 and FMT_MSA.3 have a dependency to FMT_SMR.2 which is covered by FMT_SMR.2.

9. Acronyms and Terms

Table 24 defines the acronyms and terms used throughout this document.

Table 24 – Acronyms and Terms

Acronym / Term	Definition
AD	Active Directory Microsoft Windows directory service that facilitates working with interconnected, complex and different network resources in a unified manner
AES	Advanced Encryption Standard
API	Application Programming Interface Set of routines, protocols, and tools for building software and applications
CC	Common Criteria
CDM	Cloud Data Management A system that distributes data, metadata, and task management across the cluster in order to deliver predictive scalability and eliminate performance bottlenecks.
CEM	Common Evaluation Methodology
CM	Configuration Management
CPU	Central Processing Unit
Data deduplication	Specialized data compression technique for eliminating duplicate copies of repeating data
DNS	Domain Name Service
EAL	Evaluation Assurance Level
EC	Elliptic Curve
FIPS	Federal Information Processing Standard
GB	Gigabyte
GHz	Gigahertz
HMAC	Keyed Message Authentication Code
Hypervisor	Hypervisor (or VM monitor) is a piece of computer software, firmware or hardware that creates and runs VMs
HTTPS	Hypertext Transport Protocol - Secure
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol An open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network
NIST	National Institute of Standards and Technology
OS	Operating System
OVA	Open Virtual Appliance
PP	Protection Profile
PUB	Publication
RAM	Random Access Memory
RBAC	Role Based Access Control Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file.

Acronym / Term	Definition
RPC	Remote Procedure Call Client/Server system in which a computer program causes a subroutine or procedure to execute in another address space without the programmer explicitly coding the details for this remote interaction
RSA	Rivest Shamir Adelman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Simple Hashing Algorithm
SLA	Service Level Agreement
Snapshot	Backup copy of a virtual machine. Each snapshot is a file. The first snapshot is a full copy of the virtual machine. Each subsequent snapshot is an incremental delta from the previous file. Every snapshot is a fully functional, point-in-time copy of the source VM.
SP	Special Publication
SSH	Secure Shell A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels
ST	Security Target
TLS	Transport Layer Security A protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
VM	Virtual Machine
VMDK	Virtual Machine Disk File format that describes containers for virtual hard disk drives to be used in virtual machines like VMware Workstation or VirtualBox (hypervisor)

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Drive, Suite 210
Fairfax, VA 22003
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com