NetApp, Inc. ONTAP® 9.1

Security Target

Evaluation Assurance Level (EAL): EAL 2+
Document Version 1.3
14 March 2018

Prepared by:
NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
United States of America

Version	Date	Document Version History
0.1	2017-01-24	Initial draft. (Garrett Cooper)
0.2	2017-02-23	• Split FIA_SOS.1 into (a) and (b) • Add FIA_SOS.2 • Add KMIP interface to Figure 4 • Add FCS_COP.1 • Remove all FSC_CKM SFRs Reformat document for enhanced readability (Modified by: Garrett Cooper)
0.3	2017-03-01	Remove inappropriate references to FIPS 140-2 (Modified by: Garrett Cooper)
0.4	2017-03-09	• Added "Inadvertent data disclosure" to Section 3.1 Security Threats • Added and clarified T.INADVERTENT_DISCLOSURE as the security threat countered by O.PROTECT_DATA_AT_REST in Table 29 • Changed Table 30 column header from Tthreats" to "Assumptions" • Corrected assignment operation in FMT_MSA.1.1 • Corrected FCS_COP.1 assignment operation ("FIPS 140-2" changed to "FIPS 197") Added CAVP AES algorithm certificate numbers for SEDs used in the TOE (Modified by: Mike Scanlin)
0.5	2017-03-15	• Removed "Physical theft of hard disk drives" from Section 3.1 Security Threats • Added FCS_COP.1 to list of SFRs • Reformatted CAVP AES algorithm info using table format • Corrected assignment operation in FMT_MSA.1.1 • "Rename a directory" added as Write operation to Table 26 (UNIX-Style File Access Requests) and Table 27 (NTFS-Style File Access Requests) Updated rationale for FCS_COP.1.1 in Table 32 to ensure mapping / traceability for threat (T.INADVERTENT_DISCLOSURE) security objective (O.PROTECT_DATA_AT_REST) and supporting SFR (FCS_COP.1.1) (Modified by: Mike Scanlin)

Version	Date	Document Version History
0.6	2017-04-03	Re: ONTAP-ASE-INT-OR-6 • Changed reference from “Section 1.5.1.2” to “Table 6” • Table 4: Removed “or later” and specified single browser versions for testing • Section 1.6.1: References to ONTAP Select and Safenet KeySecure Manager as part of TOE environment removed (they are part of TOE) Re: ONTAP-ASE-INT-OR-7 • Table 4: Removed “or later” and specified single browser versions for testing Re: ONTAP-ASE-INT-OR-8 Removed references to TOE environment in Section 1.6 below Figure 4 (Modified by: Mike Scanlin)
0.7	2017-05-04	Removed cryptographic claims (Modified by: Teresa MacArthur)
0.8	2017-05-15	Re: ONTAP-ASE-OBJ-OR-3 • Removed reference to FDP_SDI_EXT in Section 8.1 Re: ONTAP-ASE-OBJ-OR-4 • Updated table of contents Updated template (Modified by: Teresa MacArthur)
0.9	2017-09-20	Removed FMT_MTD.1(b) (Modified by: Teresa MacArthur)
1.0	2017-10-02	Updated OnCommand Insight version from 7.2.5 to 7.3.1 (Modified by: Mike Scanlin)
1.1	2017-10-23	Updated Table 6 to reflect both General Availability (GA) models and End Of Availability (EOA) models that support ONTAP 9.1 (Modified by: Mike Scanlin)
1.2	2018-03-05	Updates ONTAP version to 9.1P10 and the ST version and publication date in section 1.3 (Security Target and TOE Reference)
1.3	2018-03-14	Moved EOA platforms from Table 6 (Supported ONTAP 9.1 models) to new Table 8 (Supported ONTAP 9.1 models excluded from the TOE). Updates version of CC standard in Section 8.1 (Conformance Claims Rationale) to CC v3.1. Release 4.

Preface

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), NetApp ONTAP 9.1.

This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the Information Technology (IT) Security Functions provided by the TOE which meet the set of requirements.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization.

1.1 TOE Components

The TOE, itself, contains several components. These are:

1.1.1 NetApp ONTAP 9.1

The NetApp ONTAP® 9.1 Operating System, and will hereafter be referred to as ONTAP throughout this document. The ONTAP includes the kernel operating system that supports the protection of the hardware appliances on which it runs, as well as multi-protocol services and advanced data management capabilities for consolidating and protecting user data used for enterprise applications. The ONTAP includes integrated management capabilities via CLI[1] and GUI[2] interfaces. These CLI and GUI interfaces are used to manage the ONTAP security functionality (TSF).

- The management CLI is accessible via a serial connection to the FAS or AFF controller console interface or an SSH session via the management network.
- The management GUI interface was formerly an external software-only component, but is still known as NetApp OnCommand System Manager (OCSM). This component has been integral to ONTAP since Clustered Data ONTAP version 8.3. The GUI is accessible through an HTTPS session via the management network using a supported web browser.

1.1.2 ONTAP Select 9.1

In addition, the TOE also includes a virtualized implementation of ONTAP 9.1 (ONTAP® Select 9.1) which runs as a VM on VMware ESXi. **ONTAP Select 9.1** offers a subset of features found on ONTAP 9.1 running on FAS[3] or AFF[4] appliances.

Note: Throughout this document, the security functionality of ONTAP 9.1 and ONTAP Select 9.1 will coincide unless otherwise noted.

1.1.3 OnCommand Insight 7.3.1 (OCI)

The TOE also includes a separate software-only NetApp OnCommand monitoring and diagnostic component. This component allows administrators to quickly identify and troubleshoot problems that arise in the monitored storage cluster. This component is hosted on a Microsoft Windows Server 2012 R2 platform (hardware or virtual based).

1.2 Purpose

This ST is divided into eight sections and one appendix, as follows:

---

[1] CLI - Command Line Interface
[2] GUI - Graphical User Interface
[3] FAS - Fabric Attached Storage
[4] AFF - All Flash FAS

- **Introduction (Section 1**) – Provides a summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TSF 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, and Evaluation Assurance Level (EAL) package conformance 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 met by the TOE.
- **TOE Security Specification (Section 7)** – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- **Rationale (Section 8)** – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- **Acronyms (Appendix A -)** – Defines the acronyms used within this ST.

1.3 Security Target and TOE Reference

Table 1 - ST and TOE References

ST Title	NetApp ONTAP 9.1 Security Target
ST Version	Version 1.2
ST Author	NetApp Inc.
Publication Date	2018-03-05
TOE Reference	NetApp ONTAP 9.1, including: • ONTAP 9.1P10 Software • FAS or AFF Appliance (as specified in Table 6) • NetApp ONTAP Select 9.1 NetApp OnCommand component: • OnCommand Insight 7.3.1

1.4 Product Overview

The Product Overview provides a high-level description of the product that is the subject of the evaluation.

ONTAP 9.1 is a proprietary operating system developed by NetApp, Inc. ONTAP 9.1 provides data management functions that include providing secure data storage and multi- protocol access.
ONTAP 9.1 is distributed with the following NetApp storage solution products:

- **FAS** - NetApp's FAS systems offer seamless access to a full range of enterprise data for users on a variety of platforms. FAS systems support NFS[5] and CIFS[6] for file access, as well as FC[7] and iSCSI[8] for block-storage access.
- **AFF** - NetApp's All Flash FAS systems offer seamless access to a full range of enterprise data for users on a variety of platforms. AFF systems support NFS and CIFS for file access, as well as FC and iSCSI for block-storage access.

As shown in Figure 1, a typical ONTAP 9.1 system consists of two or more individual NetApp storage controllers with attached disks. The storage controllers are also called nodes.
The basic building block is the High Availability (HA) pair. An HA pair consists of two identical controllers; each controller actively provides data services and has redundant cabled paths to the other controller's disk storage. If either controller is down for any planned or unplanned reason, it's HA partner can take over its storage and maintain access to the data. When the downed system rejoins the cluster, the partner will give back the storage resources. A single node cluster is a special implementation of a cluster running on a standalone node. In a single node cluster, the HA mode is set to standalone. This configuration does not require a cluster network, and enables you to use the cluster ports to serve data traffic. In this document, the HA pair is usually not shown, for clarity.
Multiple HA pairs are combined into a cluster to form a shared pool of physical resources available to applications, SAN hosts, and NAS clients. The shared pool appears as a single system image for management purposes. This means there is a single common point of management for the entire cluster, whether through the CLI or GUI tools. While the members of each HA pair must be the same controller type, the cluster can consist of heterogeneous HA pairs. Over time, as the cluster grows and new controllers are released, it is likely to evolve into a combination of several different node types. All cluster capabilities are supported, regardless of the underlying controllers in the cluster.
An ONTAP 9.1 system can scale from one to 24 nodes, supporting up to 172 PB[9] of raw drive capacity. A cluster hosts virtualized storage systems called Storage Virtual Machines (SVMs). SVMs provide SAN and NAS data access to hosts and clients. SVMs provide complete isolation from one another allowing the implementation of secure multi-tenancy within the same ONTAP cluster.
Figure 1 also shows the underlying network architecture of ONTAP. Three networks are shown:

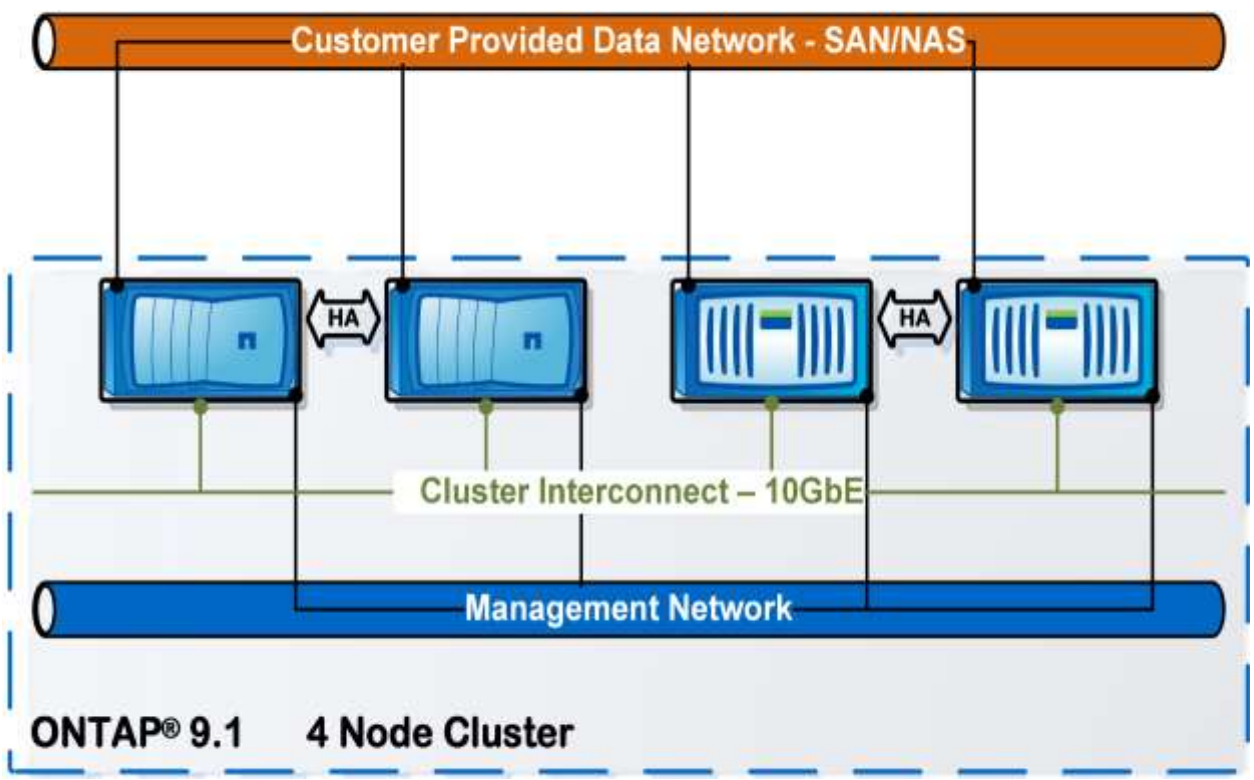
- **Cluster Interconnect** - A 10 Gb/S[10], private, dedicated, redundant, high-throughput network used for communication between the cluster nodes and for data motion within the cluster. The cluster interconnect infrastructure is provided with every ONTAP 9.1 configuration to support this network.

---

[5] NFS -Network File System
[6] CIFS - Common Internet File System
[7] FC - Fiber Channel Protocol
[8] iSCSI - Internet Small Computer System Interface
[9] PB - Petabyte – (1024 x 1024 gigabytes)
[10] Gb/S - Gigabits per second

- **Management Network** - All management traffic passes over this network. Management network switches can be included in a ONTAP 9.1 configuration, or customer- provided switches can be used. The integrated OnCommand System Manager (OCSM), built into the ONTAP, is available for management, and configuration of ONTAP systems. OCSM provides GUI management, including several easy-to-use wizards for common tasks. In addition, a CLI is available.
- **Data Networks** - Provide data access services over Ethernet or Fiber Channel to the SAN hosts and NAS clients. These networks are customer provided, per requirements, and could also include connections to other clusters acting as volume replication targets for data protection.

Figure 1 - ONTAP Overview



Storage controllers, while they can be of different types, are by default considered equivalently in the cluster configuration in that they are all presented and managed as cluster nodes. Individual disks are managed by defining them into aggregates: groups of disks of a type that are protected using NetApp's RAID-DP or RAID-TEC.
NICs[11], CNAs[12] and HBAs[13] provide physical ports (Ethernet and Fiber Channel) for connection to the management and data networks. The physical components are visible only to cluster administrators, and

---

[11] NIC - Network Interface Card
[12] CNA - Converged Network Adapter

not directly to the applications and hosts that are using the cluster. The physical components constitute a pool of resources from which are constructed the logical cluster resources.
Applications and hosts access data only through SVMs that contain data volumes and logical interfaces (LIFs).
The primary logical cluster component is the SVM. Clustered ONTAP supports from one to hundreds of SVMs in a single cluster. Each SVM is configured for the client and host access protocols it will support; any combination of SAN and NAS. Each SVM contains at least one volume and at least one logical interface. The administration of each SVM can also be delegated if desired, so that separate administrators could be responsible for provisioning volumes and other SVM-specific operations. This is particularly appropriate for multi-tenancy environments or where workload separation is desired.
For more information on NetApp Storage Controllers, see section 1.6.1.2. The products support both single controller and High Availability controller pairs as Storage Controller options on some models.

ONTAP 9.1 supports multiple authentication mechanisms:

- For CIFS sharing, ONTAP 9.1 can authenticate end users with Kerberos[14] or New Technology Local Area Network Manager (NTLM) against an Active Directory (AD) domain, with NTLM against a Windows NT-style domain, or locally using NT-style NTLM authentication against a local user database.
- For NFS sharing, the TOE can authenticate end users with Kerberos against both an Active Directory domain and a Network Information Service (NIS) domain, or locally against User Identifiers (UID) and passwords in local UNIX identity stores.
- For administration, the TOE authenticates administrators against a local user repository or a Microsoft Active Directory (AD) domain.

ONTAP Select 9.1 supports most of the features of ONTAP 9.1 running on a FAS or AFF appliance. ONTAP Select can be implemented as either a single node cluster or as a four (4) node cluster. Each virtualized node must be run on separate VMware ESXi servers. Physical storage is limited to the disks (HDD or SSD) local to the hardware server, itself. An integral hardware raid controller is required. As ONTAP Select 9.1 is a virtualized appliance, some physical attributes found on hardware FAS/AFF appliances do not apply. For ONTAP Select 9.1, there is no support for Fiber-Channel (FC) SAN.

OnCommand Insight 7.3.1 (OCI) is designed to simplify operational management of complex private cloud and virtual IT environments. OCI is a single solution to enable cross-domain, multi-vendor resource management and analysis across networks, storage, and servers in physical and virtual environments. OCI provides a "single pane of glass" for reporting on storage costs and provides the transparency needed to make decisions about performance and efficiency. Version 7.3.1 includes these key enhancements:

- Usability – New web-based user interface (UI) enables better visualization of the IT infrastructure relationships and provides simpler and easier installation, upgrade process, and product administration.
- Scalability – Scale across multiple data centers.
- Flexibility – New dashboard and improved asset search and navigation enable quicker troubleshooting.

---

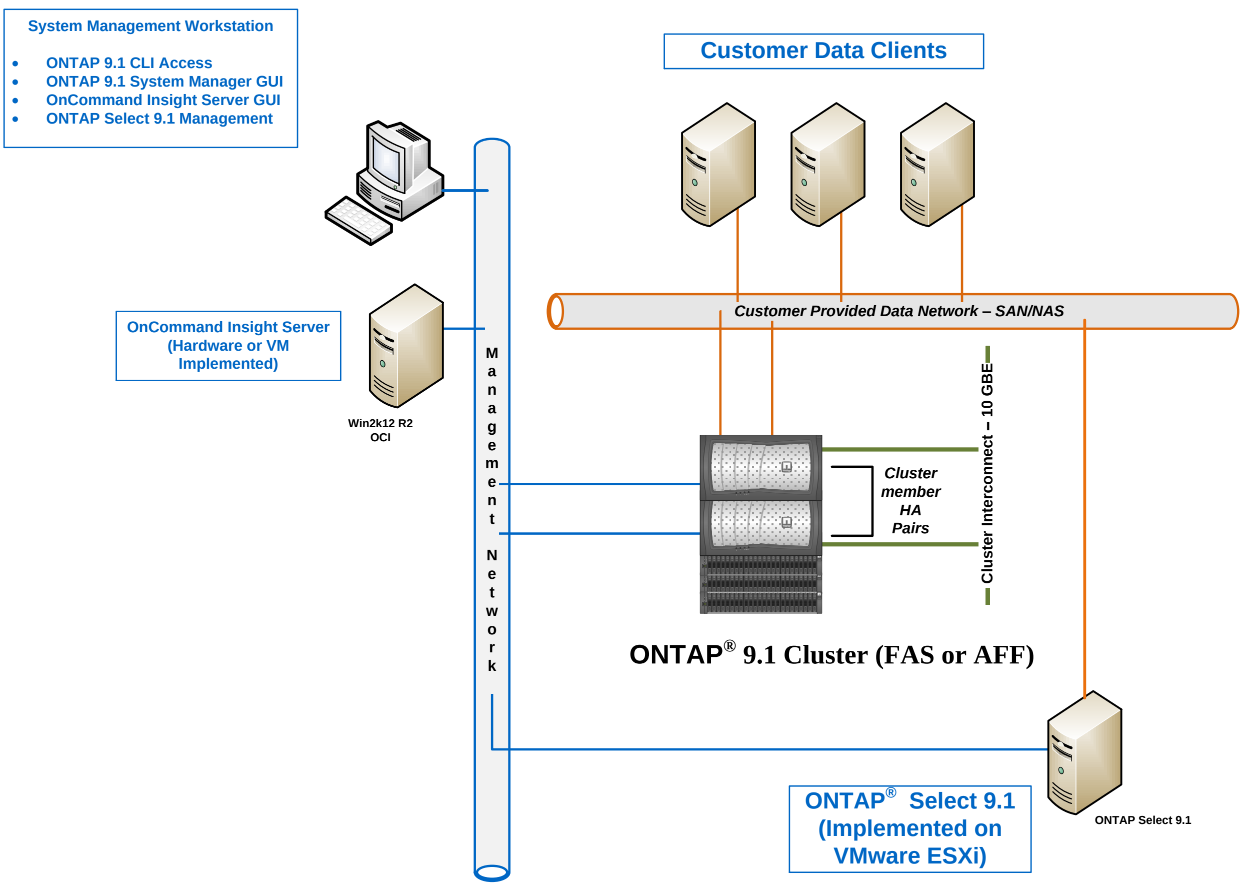
[13] HBA - Host Bus Adapter
[14] Off-box Identification and Authentication to a NIS or AD domain either NTLM or Kerberos is a functionality provided by the IT environment. Identification and Authentication of end-users is not a claimed security functionality of the TOE whether local or remote.

- Interoperability – Most comprehensive multi-vendor support in the industry, including enhanced NetApp ONTAP configuration and performance monitoring.
- OCI has three (3) components:
  - OnCommand Insight Server
  - OnCommand Data Warehouse and Reporting Server
  - OnCommand Remote Acquisition Server

Note:	Of the three (3) OCI components, only OnCommand Insight Server is evaluated and within the scope of this TOE.

Figure 2 shows a complete two-node (HA pair) cluster deployment with the OnCommand and SafeNet components.

Figure 2 - ONTAP Two Node (HA Pair) Cluster Deployment



1.5 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration. The TOE is a data storage system. It is a hardware and software TOE. Functionality included in the logical software components of the TOE boundary includes:

- **Secure Multi-Protocol Data Storage Access** – TOE Secure storage is provided by implementing strict access control rules to data managed on the TOE. By supporting both NFS and CIFS clients, as well as providing transparent access to data, Multi-Protocol access support is achieved.

- **Identification and Authentication** – The TOE supports on-box Identification and Authentication of administrators against a local user repository or off-box Authentication to a Microsoft Active Directory (AD) domain.
- **Domain Separation** – The TOE can function as a storage server for multiple groups of users within the TOE's control that must remain isolated from one another through the implementation of NetApp's Storage Virtual Machine (SVM) technology.
- **Management** – The Management functionality included in the TOE's logical boundary enables administrative users to modify TOE data and TSF security functional behavior.
- **Audit** – The Audit functionality provided by the TOE generates audit records for administrator logins and configuration changes.

1.5.1 Brief Description of the Components of the TOE

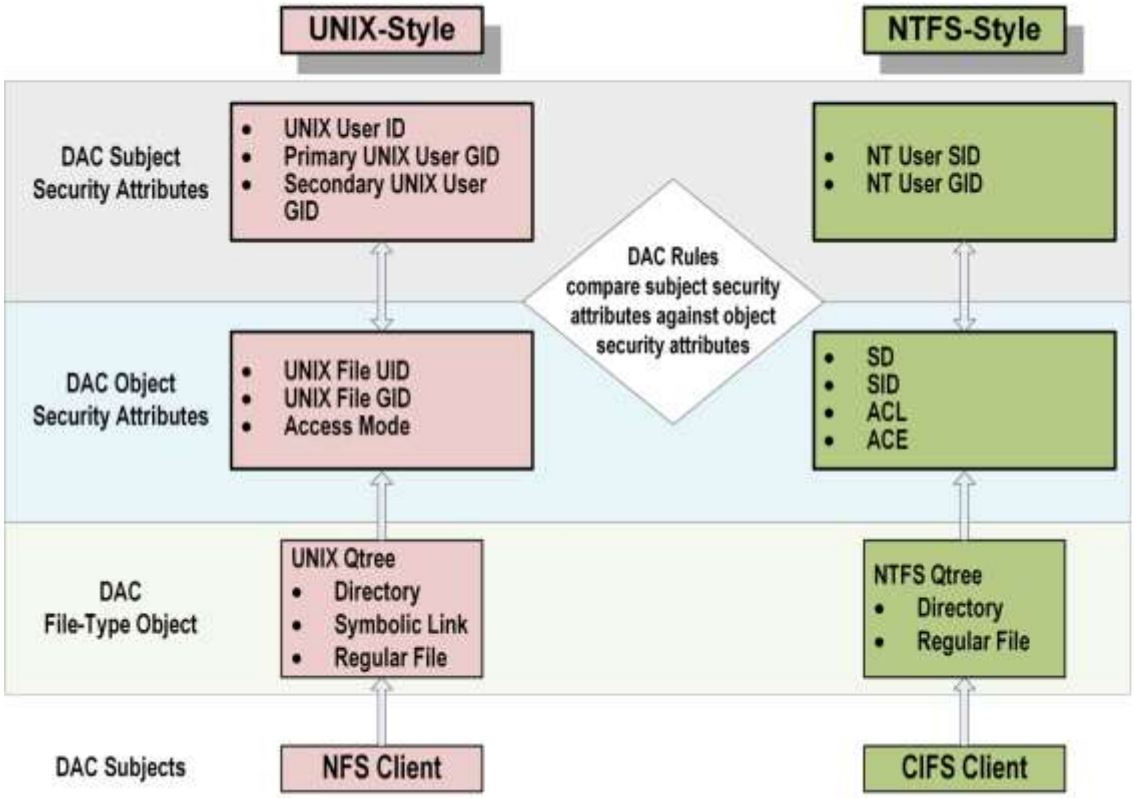
The software component of the TOE is divided into six primary components: Write Anywhere File Layout (WAFL), System Administration, the Operating System Kernel, the Management Host, and the OnCommand Insight (OCI). The six components are described below. Their relationship to the IT Environment-supplied components is depicted in Figure 4.

- **WAFL** - The TOE's WAFL component is responsible for implementing the TOE's Discretionary Access Control (DAC) Security Function Policy (SFP). The DAC SFP includes enforcing access rules to user data based on client type, client security attributes, file types, file security attributes and access request (create, read, write, execute, delete, change permission, and change owner).
- **System Administration** - The System Administration component provides an administrator with an interface supporting operator functions including enforcing identification and authentication, user roles, and providing the necessary user interface commands that enable an operator to support the TOE's security functionality. A user who has been granted the "admin role" performs the System Administration function. This functionality is available locally and remotely via a Command Line Interface (CLI), or remotely via one of several management interfaces detailed in section 7.1.4 System Administration functions are audited by default.
- **Operating System Kernel** - The Kernel facilitates communication between the components of the Operating System. The Kernel is a small portion of the operating system through which all references to information and all changes to authorizations must pass.
- **Management Host** - Host the management and services applications for the node. One of the functions of the Management Host (M-Host) is the Cluster Admin which is responsible for the CLI interface for the cluster and the Volume Location Data Base (VLDB) which locate the physical location of volumes in a node.
- **OnCommand Insight Server** (**OCI**) - The OnCommand Insight Server component is a versatile datacenter monitoring and management tool. Its use, in respect to ONTAP 9.1, is for monitoring only. Other functionality within OnCommand Insight Server is outside the scope of this TOE.

1.5.1.1 WAFL Functionality Detail

The TOE's WAFL Component protects User data. The TOE uses the subject, subject's security attributes, the object, the object's security attributes and the requested operation to determine if access is granted. The subjects are end users on remote systems that access the TOE via NFS or CIFS.

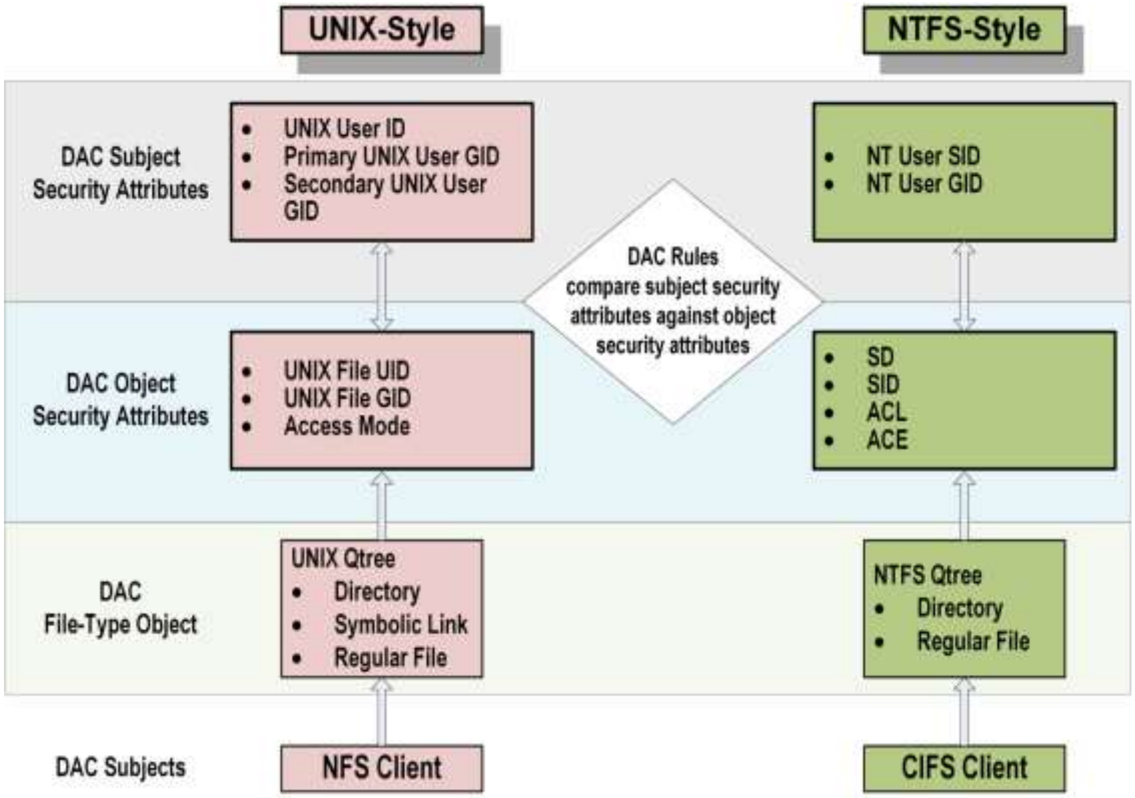
Figure 3 – WAFL Functionality Detail



depicts the WAFL functionality.

The following acronyms not yet defined appear in

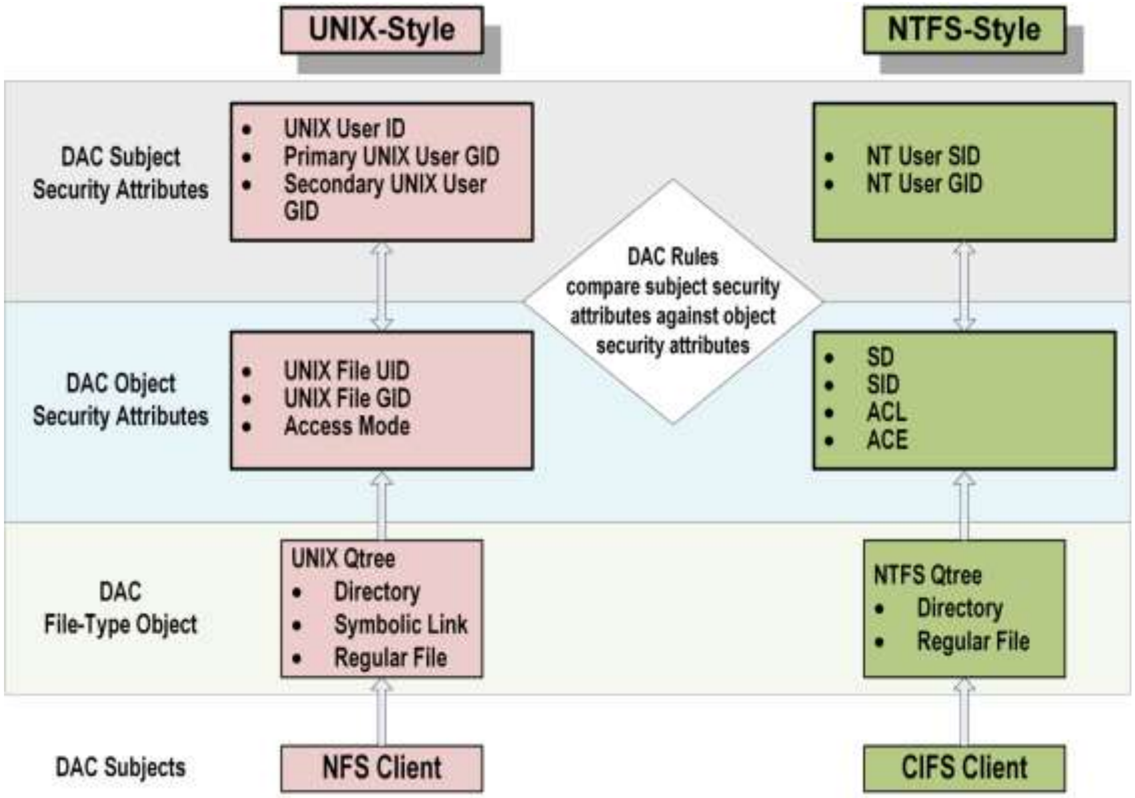
Figure 3 – WAFL Functionality Detail



below:

- ACL – Access Control List
- ACE – Access Control Entry
- GID – Group Identifier
- NTFS – New Technology File System
- SD – Security Descriptor
- SID – Security Identifier

Figure 3 – WAFL Functionality Detail



1.5.1.1.1 User Data

The User Data that is covered by the DAC SFP are the user files on:

- NetApp disks attached to a FAS or AFF appliance
- FlexArray SANs attached to a FAS appliance
- Local disks attached to an ESXi server hosting ONTAP Select

Each file maintained by the TOE has a file style associated with it. The TOE maintains three styles of files: NFSv3 UNIX-Style files, NFSv4 UNIX-Style files, and NTFS-Style files. NFSv3 UNIX-Style files have UNIX-Style security attributes, NFSv4 UNIX-Style files have NFSv4 security attributes, and NTFS-Style files have NTFS-Style security attributes.

In addition to a file style, each file has a file type. The file types may be directories, symbolic links, or regular files. UNIX-Style files may be a directory, a symbolic link, or a regular file. NTFS-Style files do not have symbolic links therefore the file type will be either a directory or a regular file.

A Qtree is a disk space partition. In addition to the file type, the TOE maintains three different storage types: UNIX Qtrees, NTFS Qtrees and Mixed Qtrees. UNIX Qtrees store UNIX-Style files with UNIX-Style security attributes. NTFS Qtrees store NTFS-Style files with NTFS Style security attributes. Mixed Qtrees store both styles of files. Files stored in Mixed Qtrees always have the security attributes associated with the client that was last used to change their access permissions or ownership. Mixed Qtrees are not part of the evaluated configuration.

A file's security attributes are determined when the file is created. The TOE will create UNIX-Style security attributes for a file stored in a UNIX Qtree. The TOE will create NTFS-Style security attributes for a file stored in an NTFS Qtree. These security attributes are outlined in Table 2.

Table 2 - TSF User Data Security Attribute Descriptions

Security Attribute	Description
Access Control Entry	A data structure associated with NTFS-Style files. Each ACE explicitly allows or denies access to a user or group for a specific NTFS-Style supported operation.
	A data structure associated with NFSv4-Style and NFSv4.1-Style files. Each ACE explicitly allows or denies access to a user or group for a specific NFSv4.x-Style supported operation.
Access Control List	A data structure associated with NTFS-Style files. Each ACL includes one or more ACEs.
	A data structure associated with NFSv4-Style and NFSv4.1-Style files. Each ACL includes one or more ACEs.
Access Mode	A data structure associated with a UNIX-Style Files. An access mode string is the last nine characters of a UNIX-Style File Permission string (drwxrwxrwx). The nine characters represent the access mode for the file in three sets of rwx triplets. The first triplet specifies the permission for the file's owner (UID). The next triplet specifies the permissions for the group associated with the file (UNIX file GID). The last three characters specify the permission for the users who are neither the owner nor members of the file's group (other). The rwx triplet identifies the permission for that set (owner, group, other). The three characters represent read, write, or execute privileges. If the character is a dash, the set does not have permissions to perform the specific action.
File Permission String	A data structure associated with a UNIX-Style file. The file permission string is represented in ten characters common to all UNIX files (e.g. drwxrwxrwx). The first character contains one of three characters that identify the file type: d for directory, l for a symbolic link, or a dash (-) indicates the file is a regular file. The following 9 characters represent the access mode for the file in three sets of rwx triplets.
Security Descriptor	A data structure associated with NTFS-Style files. An SD contains a SID and an ACL.
Security Identifier	The CIFS User SID of the file's owner.
Group Identifier	A UNIX File GID identifies the groups associated with the UNIX-Style file.
User Identifier	The UNIX User UID of the file's owner.

1.5.1.1.2 TOE Clients

End-user access to TSF data is possible using either the NFS or CIFS client protocol. In a typical deployment as depicted in Figure 2, end user workstations or the file, web, mail, or application servers of the IT Environment connect to the TOE that hosts the TSF data residing on the storage arrays. The TOE is positioned between these workstations and servers, and the storage arrays, facilitating seamless NFS or CIFS connectivity between them while adding increased performance, efficiency, manageability, scalability, security, redundancy, and fault tolerance.

End-system workstations and the file, web, mail, or application servers authenticate with the TOE per the operating procedures of the organization and IT Environment. Typical scenarios include the file, web, mail, or application servers prompting end users for credentials as they attempt to access a web page, e-mail system, or standalone application or the TOE prompting end users for credentials as they attempt to access shared network directories (NFS or CIFS). The TOE facilitates server and end-user authentication of the end users attempting to access the TSF data via NFS or CIFS.

To determine if file access is allowed, the TOE compares a client's security attributes with the file's security attributes, listed in Table 3. The type of client security attributes (UNIX-Style or NTFS-Style) required by the TOE depends on the type of security attributes maintained by the file and the operation requested. The file or operation will require UNIX-Style subject security attributes (NFSv3 or NFSv4), NTFS-Style subject security attributes or both. If the file or operation requires UNIX-Style security attributes for a client, the TOE will attempt to obtain the client's UNIX User UID and UNIX User GID. If the file or operation requires NTFS-Style subject security attributes, the TOE will attempt to acquire the client's Windows User SID and a Windows User GID. Because of the native operating systems of the two clients, NFS clients are associated with UNIX-Style security attributes and CIFS Clients are associated with NTFS-Style security attributes.

In the TOE, the resolution of client security attributes is processed differently for each type of client because the two protocols are different. NTFS-Style security attributes for a CIFS client are resolved when the CIFS client logs into the remote system and joins the Windows domain (of which the TOE is a member). Therefore, NTFS-Style security attributes for a CIFS client is completed before the TOE receives a CIFS request. Alternatively, NFS client security attributes are resolved per NFS request. The UNIX User UID is passed in each NFS request and this UID is used to resolve the required client security attributes.

Table 3 - TOE Client Security Attribute Descriptions

Security Attribute	Description
Windows User SID	The Windows user ID number. Each user in a Windows system is assigned a unique Windows User SID.
Windows User GID	The Windows group ID number. Each user in a Windows system is assigned to a group and that group is assigned a unique GID.
UNIX User UID	The UNIX user ID number. Each user in a UNIX system is assigned a unique UNIX User UID.
UNIX User GID	The UNIX group ID number. Each user in an UNIX system is assigned to a group and that group is assigned a unique GID.

1.5.2 TOE Environment Hardware

The IT environment requires the following hardware:

- Mandatory:
  - Storage Array FAS or AFF controllers
  - A server with adequate raid-controlled disks capable of running VMware ESXi (ONTAP Select)
- **Optional** (if management workstation or OCI is not deployed in an ESXi environment):
  - Server capable of running Microsoft Windows Server 2008 or later to host the OnCommand Insight Server
  - Server or workstation, used for management purposes, capable of running a supported web browser and an SSH client

The OnCommand Insight Server has the following minimum hardware requirements when hosted on a physical server or the functional equivalent if hosted on an ESXi or Microsoft Hyper-V virtual machine (VM):

- Architecture capable of supporting 64 bit Microsoft Windows Server 2008 and later
- 2 or more or more CPU cores
- 8 or more GB RAM
- 100 GB available free hard disk space

Note: Larger environments may require larger values. See appropriate product installation documentation for specifics.

1.5.3 TOE Environment Software

Note: Web browser software and the SSH capable terminal emulator, although used to manage the TOE, are not under evaluation.

Before an authorized administrator begins the software setup process, he must ensure that the network and storage environment for the new storage system has been prepared per the Guidance Documentation. Once the proper configuration has been met, the administrator must gather the appropriate configuration items from the network and storage environment and keep them handy for proper installation of the TOE.

1.5.3.1 System Requirements for a Workstation used to Access and Manage the TOE Components (as evaluated)

- Microsoft Windows 10

1.5.3.2 User Interface Requirements for use of OnCommand Insight, OnCommand System manager, and CLI Access

Table 4 lists the web browser and terminal emulation software requirements for administrative communication to the various TOE components:

Table 4 - Web Browser and Terminal Emulation Compatibility Matrix

TOE Component	Internet Explorer Version	Google Chrome Version	Terminal Emulator (SSHv2 capable)
ONTAP CLI	n/a	n/a	PuTTY or equivalent
OnCommand System Manager	10	42	n/a
OnCommand Insight Server	10	42	n/a

1.6 TOE Description

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

1.6.1 Physical Scope

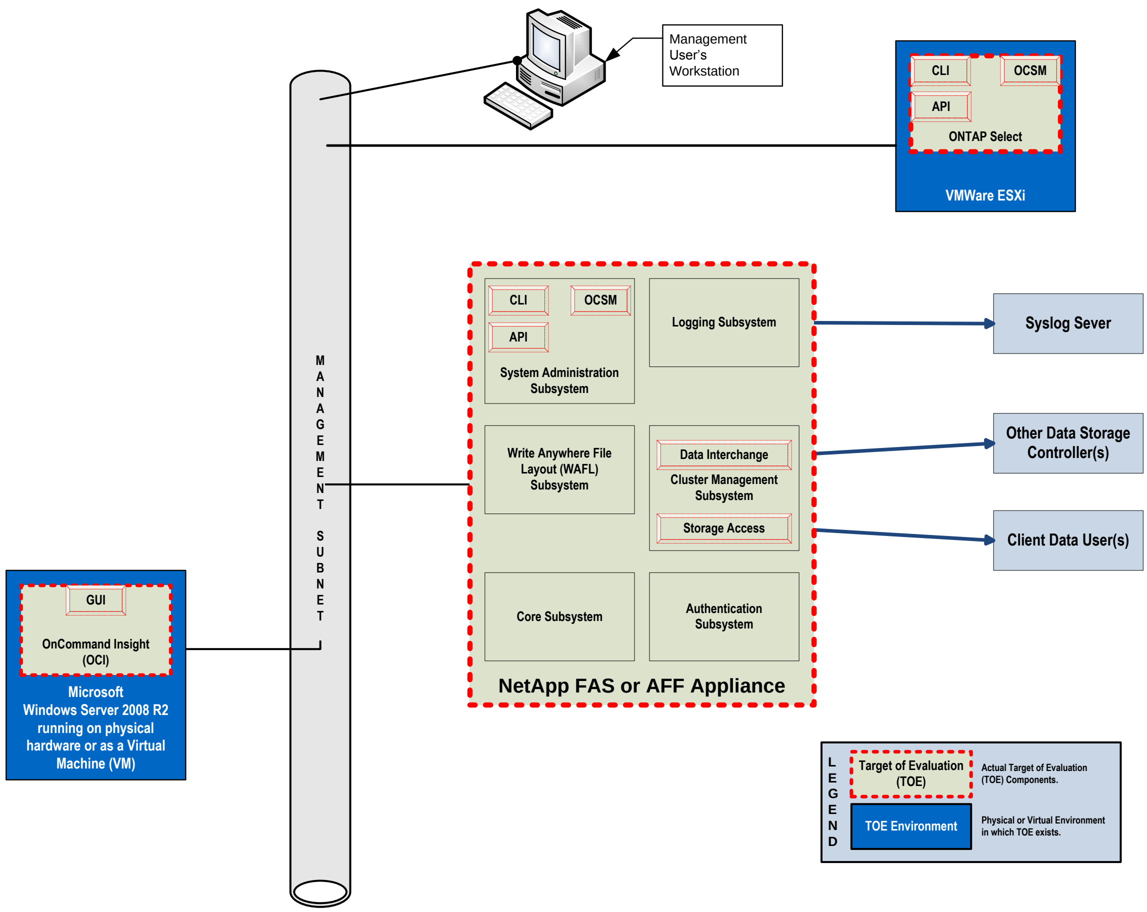
Figure 4 illustrates the physical scope and the physical boundary of the overall solution, its deployment in a networked environment, and ties together all the components of the TOE and the constituents of the TOE Environment. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- The **ONTAP 9.1** operating system on the NetApp Appliance Hardware or as **ONTAP Select**. The ONTAP 9.1 operating system consists of:
  - **WAFL** – TOE's WAFL component is responsible for implementing the TOE's DAC SFP.
  - **System Administration** – Service supporting management of the node.
  - **Operating System Kernel** – Provides messaging between individual components of ONTAP
  - **Management Host** – An administrator may directly communicate to the Cluster through a connection to the Management Host. When commands are directed to a node on another storage controller, the request is forwarded to the specific node's System Administration service through the Management Network shown in Figure 4.

- **OnCommand Insight Server Component** – The OnCommand Insight Server component provides an authorized administrator with a web-based GUI, and an exposed API. Together, these interfaces provide an authorized administrator the ability to view the status for capacity, availability, performance, and protection relationships of the monitored systems in the storage cluster.

The TOE components are depicted in Figure 4.

Figure 4 - Physical TOE Boundary



1.6.1.1 TOE Software

The ONTAP portion of the TOE software is a kernel operating system which runs on a subset of NetApp's proprietary 64-bit x86- based storage controller platforms listed in section 1.6.1.2 or virtualized as ONTAP Select.

1.6.1.1.1 Administration Users

Cluster administrators are registered locally, and identified by user-account names on the ONTAP cluster. Each user-account may have one (1) or more login method(s) defined. Each method determines how the admin-user will access the cluster (-application) and which type of account authentication (-authentication-method) is appropriate for that access. Table 5 lists the valid access applications and relevant authentication methods.

Table 5 - Access Methods and Relevant Authentication Methods

Access Method (Application)	Relevant Authentication Methods	Comments
console	password	Must authenticate to a local account.
http	password, domain, nsswitch, cert	"domain" refers to MS Active Directory domain and requires CIFS service running on an SVM. For cluster access, a domain-tunnel must be defined linking a CIFS SVM. "nsswitch" refers to NIS/LDAP running in an SVM. "nsswitch" cannot be used to authenticate cluster administrators.
ontapi	password, domain, nsswitch, cert	"domain" refers to MS Active Directory domain and requires CIFS service running on an SVM. For cluster access, a domain-tunnel must be defined linking a CIFS SVM. "nsswitch" refers to NIS/LDAP running in an SVM. "nsswitch" cannot be used to authenticate cluster administrators.
rsh	password	By default, is disabled. Do not use as rsh is not secure.
snmp	community, usm	
service-processor	password	Access is only available by serial console and/or SSH to FAS controller management interface.
ssh	password, publickey, domain, nsswitch	"domain" refers to MS Active Directory domain and requires CIFS service running on an SVM. For cluster access, a domain-tunnel must be defined linking a CIFS SVM. "nsswitch" refers to NIS/LDAP running in an SVM. "nsswitch" cannot be used to authenticate cluster administrators.
telnet	password	By default, is disabled. Do not use as telnet is not secure.

Once an admin-user has been identified and authenticated, then the specific role assigned to that admin-user account will determine the actual functionality authorized for that user account.

1.6.1.1.2 Administrative Command Auditing

By default, auditing of any CLI or ONTAPI commands which modify the ONTAP portion of the TOE is active. This cannot be disabled.
Optionally, the CLI command "security audit modify" is used to enable administrative command auditing of any CLI or ONTAPI commands which read/display status or configurations on the ONTAP portion of the TOE. At least one of the following parameters should be provided with this command:

- **-cliget {on | off}** — sets the auditing state for any CLI commands that query any current configuration values. If set to on, may overinflate auditing (log) files if CLI command activity level is high. (Recommended to be set to **off**. Set to **off** for this TOE evaluation)
- **-ontapiget {on | off}** — sets the auditing state for any API commands that query any current configuration values. If set to on, may overinflate auditing (log) files if API command activity level is high. (Recommended to be set to **off**. Set to **off** for this TOE evaluation)

1.6.1.1.3 NFS Configuration for TOE's Evaluation

The following commands set the TOE's evaluated NFS configuration on any SVM exporting NFS data:

- **set -privilege advanced** - This privilege level is required to set the -chown-mode option for a SVM's NFS configuration.
- The **vserver nfs modify –chown-mode** option for the evaluated configuration is set to "*unrestricted*". When set to "*restricted*", only a "superuser" has permission to change the owner of a file. When set to "*unrestricted*", the vserver nfs modify –chown-mode option enables the "*owner*" of a file or a "*superuser*" to change ownership of a file.

1.6.1.2 TOE Hardware

The ONTAP 9.1 portion of the TOE runs on the NetApp's storage appliances listed in Table 6 below. The primary differences between the listed models are:

- Chassis/Controller size
- Number of network interface connections points
- Performance

The ONTAP 9.1 portion of the TOE supports the hardware appliance models in Table 6. Each appliance runs one instance of the ONTAP 9.1 TOE software.

Table 6 - Supported ONTAP 9.1 Models

FAS, All Flash FAS (AFF), and ONTAP Select			
FAS2240-2	FAS2650	FAS8200	AFF A700s
FAS2520	FAS8020	FAS9000	AFF8040
FAS2552	FAS8040	AFF A200	AFF8080 EX
FAS2554	FAS8060	AFF A300	ONTAP Select
FAS2620	FAS8080 EX	AFF A700	

For a complete list of NetApp Storage Controllers on which the TOE operates, refer to the "New and changed platform and hardware support" section of the release notes for ONTAP 9.1.

1.6.1.3 Guidance Documentation

The following guides are required reading and part of the TOE:

- ONTAP® 9 Software Setup Guide
- ONTAP 9.1 Guidance Documentation Supplement
- ONTAP® 9 Commands: Manual Page Reference (Updated for ONTAP 9.1)
- ONTAP® 9 System Administration Reference
- ONTAP® 9 Cluster Management Workflows for OnCommand® System Manager
- ONTAP® 9 Cluster Management Using OnCommand® System Manager (Updated for 9.1)
- ONTAP® 9 High-Availability Configuration Guide
- ONTAP® 9 Disks and Aggregates Power Guide (Updated for 9.1)
- ONTAP® 9 Network Management Guide
- ONTAP® 9 Logical Storage Management Guide
- ONTAP® 9 Data Protection Tape Backup and Recovery Guide
- ONTAP® 9 NFS Reference
- ONTAP® 9 NFS Configuration Power Guide
- ONTAP® 9 NFS Configuration Express
- ONTAP® 9 CIFS Reference
- ONTAP® 9 CIFS/SMB Configuration Express Guide
- ONTAP® 9.1 Release Notes

- ONTAP® Select 9 Installation and Cluster Deployment Guide (Updated for ONTAP Select 9.1)
- ONTAP® Select 9 Quick Start Guide: Deploying an Evaluation Single-Node Cluster (Updated for 9.1)
- ONTAP® Select 9 Quick Start Guide: Deploying an Evaluation Four-Node Cluster (Updated for 9.1)
- ONTAP® Select 9.1 Release Notes
- OnCommand® Insight 7.3.1 Installation Guide for Microsoft Windows®
- OnCommand® Insight 7.3.1 Configuration and Administration Guide

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 security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

1.6.2.1 Security Audit

The TOE keeps track of auditable events through the "mgwd.log" files, stored in /etc/log/mlog/ on each cluster node. An audit log is a record of "get" and "set" commands executed at the console or a secure shell (SSH) via the cluster management CLI. Administrative Secure Hypertext Transfer Protocol (HTTPS) "ontapi" operations, such as those resulting from the use of OnCommand System Manager, are also logged. All login attempts to access the storage system, with success or failure, are also logged. In addition, there are "command-history.log" files in the same /etc/log/mlog/ location on each cluster node. For commands executed through the console, an SSH shell, or the HTTPS "ontapi", the audit log shows the following information:

- What commands were executed
- Source of the executed the commands
- When the commands were executed (Time stamp)

The TOE ensures that rotating log files protect the audit-trail storage as they reach an administrator-configurable maximum size, and overwriting the oldest log file when the audit trail reaches an administrator - configurable maximum size. In addition, the log files are accessible for viewing by an authorized administrator via NFS, CIFS, or HTTPS.
The node audit files are available for read-access or download via the Service Processor Infrastructure (SPI). Access is accomplished via HTTPS by pointing a supported browser to the following URL:
https://<cluster-management-ip-address>/spi.
where the *cluster-management-ip-address* is an IP address assigned to the cluster's management LIF. For more information on the Security Audit functionality of the TOE, see section 7.1.1.

1.6.2.2 User Data Protection

User data protection defines how clients (users) connecting to the TOE can perform operations on objects.

User access to objects controlled by the TOE is governed by the enforcement of the DAC SFP. Access to NTFS-Style files via a CIFS share is authorized locally by file ACEs. Access to NFSv3 UNIX-Style files via an NFSv3 export is authorized locally by file/directory ownership and UNIX-Style security attributes. Access to NFSv4 UNIX-Style files via an NFSv4 export is authorized locally by file ACEs.
The TOE provides authorized administrators with several management interfaces outlined in section 1.6.2.4 to configure end-user network access. The management interfaces provide for the creation of rules that define actions the TOE is to take are based on a set of conditions. The conditions and actions

affect either the allowed access to user data by end-users (DAC SFP), or the way administrators interact with the TOE.

For more information on the User Data Protection functionality of the TOE, see section 7.1.2.

1.6.2.3 Identification and Authentication

The Identification and Authentication (I&A) functionality of the TOE forces human administrators to identify and authenticate themselves to the TOE before allowing any modifications to any TOE managed TSF Data. All TOE components maintain Authentication identification credentials in a local registry. All TOE components also support local authentication using locally stored passwords, if so configured. All TOE components are also capable of authenticating administrators via external means (i.e.: LDAP or Microsoft Active Directory).

The ONTAP and ONTAP Select components of the TOE enforce minimum password strength requirements, when authenticating locally. The security login role config create, and modify commands offer parameters to specify the minimum number of alphabetic characters, a mix of alphabetic with numeric, and the number of special characters that a password must contain. Passwords must have a length of at least 8 characters and contain at least one numeric character and at least one alphabetic character. Special characters are optional.
The TOE will lock out an administrator account if the user fails to enter the proper credentials after reaching the "–max- failed-login-attempts" limit, set by the "security login role config modify" or "security login role create" command.
For more information on the I&A functionality of the TOE, see section 7.1.3.

1.6.2.4 Security Management

The TSF management functionality provides the necessary functions to allow an administrator to manage and support the TSF. Included in this functionality are the rules enforced by the TOE that define access to TOE-maintained TSF Data and its corresponding security attributes, and functions.
The security attributes include authentication data (used to authenticate end users), roles, security attribute data (used for DAC SFP enforcement) and other TSF data (used for DAC SFP subject security attribute resolution).

Table 7 - TOE Built-In (Default) Administrative Roles

ONTAP or ONTAP Select		OnCommand Insight
Cluster	SVM	
admin	vsadmin	admin
autosupport	vsadmin-volume	guest
backup	vsadmin-protocol	user
readonly	vsadmin-backup	
none	vsadmin-readonly	

An "ONTAP or OCI Administrator" is defined to be any human user who is assigned any of the administrative roles (except for ONTAP "none") listed above.
The TSF Functions are managed using the following capabilities (which are defined in detail in Table 25):

- Command Directory Access
- Access
- Query

For more information on the TSF management functionality, see section 7.1.4.

1.6.2.5 Protection of TOE Security Functionality

The TOE protects the TSF via the implementation of domain separation made possible by Secure Multi-Tenancy (SMT) functionality.
For more information on domain separation and Protection of the TSF, see section 7.1.5.

1.6.2.6 TOE Access

The TOE mitigates unauthorized administrator access by automatically terminating administrator sessions after 30 minutes of inactivity at the CLI.
For more information on the TOE Access functionality of the TOE, see section 7.1.6.

1.6.3 Product Physical Features, Logical Features, and Functionality Not Included in the TOE

Physical Features that are not part of the evaluated configuration of the TOE are:

- Physical hardware (servers and/or workstations) and installed Operating Systems on which the OnCommand Insight server component is hosted
- Physical hardware (servers and/or workstations) and installed Operating Systems on which the SafeNet KeySecure Key Manager virtual appliance is hosted
- Physical hardware (servers and/or workstations) and installed Operating Systems on which management access web browsers and SSH terminal emulators are hosted

Table 8 - Supported ONTAP 9.1 models excluded from the TOE

FAS / AFF Model						
FAS2220	FAS2240-4	FAS3220	FAS3250	FAS3270	FAS6210	FAS6220
FAS6240	FAS6250	FAS6280	FAS6290	AFF8020	AFF8060	

Logical Features and Functionality that are **not** part of the evaluated configuration of the TOE are:

- Management access using insecure protocols (i.e.: Telnet[15], RSH[16], HTTP[17], FTP[18])
- Remote resolution of authentication data via UNIX LDAP
- Cross-protocol support (NFS access to NTFS-Style files, CIFS access to UNIX-Style files)
- Mixed security style models on user data volumes and qtrees
- Share level ACLs
- Bypass traverse checking option
- Microsoft Windows Group Policy Objects
- ONTAP - ONTAP not configured to run in a FIPS compliant manner
- ONTAP - API interface
- ONTAP - Data Interchange Interface
- ONTAP - On-board Key Manager
- ONTAP - Administrative user supplied “passphrases” for SED operation
- SafeNet KeySecure key manager not configured to operate in a FIPS compliant manner

[15] Telnet - Protocol for network connection
[16] RSH - Remote Shell
[17] HTTP - Hyper Text Transport Protocol
[18] FTP - File Transfer Protocol

- Self-Encrypting Drives - the NetApp FAS and AFF appliances support the use of Self-Encrypting Drives as part of the storage array

Other Features and Functionality not evaluated:

- Supported workstation operating systems:
  - Microsoft Windows versions prior to Windows 10
  - Linux desktop systems
  - Macintosh OS X 10.x
- Web browsers:
  - Any Web Browsers other than Microsoft Internet Explorer or Google Chrome

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (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 9 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM[19] as of 06/14/2013 were reviewed, and no interpretations apply to the claims made in this ST
PP Identification	None
Evaluation Assurance Level	EAL2+ (Augmented with Flaw Remediation (ALC_FLR.3))

[19] 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 way 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
- All organizational security policies with which the TOE must comply
- All assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets where the TOE requires protection, or by the security environment. The threat agents are divided into four categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters, and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)
- Agents or processes working either on behalf of attackers or autonomously: They may or may not have knowledge of the public or proprietary TOE configuration. These agents and processes can take many forms, such as bots or botnets designed to exploit common vulnerabilities or deny others access to IT products and services.

These threats are assumed to have a low level of motivation. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 10 - Threats

Name	Description
T.MASQUERADE	A TOE user or process may masquerade as another entity to gain unauthorized access to data or TOE resources.
T.TAMPER	A TOE user or process may be able to bypass the TOE’s security mechanisms by tampering with the TOE or TOE environment.
T.UNAUTH	A TOE user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE SFP.
T.DATALOSS	Threat agents may attempt to remove or destroy data collected and produced by the TOE.
T.NO_AUDIT	Threat agents may perform security-relevant operations on the TOE without being held accountable for it.
T.IA	Threat agents may attempt to compromise the TOE or network resources controlled by the TOE by attempting actions that it is not authorized to perform on the TOE or network resources.

3.2 Organizational Security Policies

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. No OSPs are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

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. The specific conditions in Table 11Table 11 are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 11 - Assumptions

Name	Description
A.PEER	Any other systems with which the TOE communicates are assumed to be under the same management control and use a consistent representation for specific user and group identifiers.
A.NETWORK	Security Management shall be provided to protect the Confidentiality and Integrity of transactions on the network.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NO_EVIL_ADM	The system administrative personnel are not hostile and will follow and abide by the instructions provided by the administrator documentation.
A.COOP	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
A.PROTECT	The processing resources of the TOE critical to the SFP enforcement will be protected from unauthorized physical modification by potentially hostile outsiders.
A.ADMIN_ACCESS	Administrative functionality shall be restricted to authorized administrators.
A.NTP	The IT Environment will be configured to provide the TOE to retrieve reliable time stamps by implementing the Network Time Protocol (NTP).
A.PHYSICAL	Physical security of the TOE and network, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

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 as follows:

Table 12 - Security Objectives for the TOE

Name	Description
O.ADMIN_ROLES	The TOE will provide administrative roles to isolate administrative actions.
O.AUDIT	The TOE will audit all administrator authentication attempts, whether successful or unsuccessful, as well as TOE user account configuration changes.
O.DAC_ACC	TOE users will be granted access only to user data for which they have been authorized based on their user identity and group membership.
O.ENFORCE	The TOE is designed and implemented in a manner that ensures the SFPs can't be bypassed or interfered with via mechanisms within the TOE's control.
O.IA	The TOE will require users to identify and authenticate themselves.
O.MANAGE	The TSF will provide functions and facilities necessary to support the authorized administrators that are responsible for the management of TOE security.
O.STRONG_PWD	The TOE must ensure that all passwords will be at least 8 characters in length and will consist of at least one number and at least one alphabetic character. Special characters are optional. Password construction will be complex enough to avoid use of passwords that are easily guessed or otherwise left vulnerable, e.g. names, dictionary words, phone numbers, birthdays, etc. should not be used.
O.INACTIVE	The TOE will terminate an inactive management session after a configurable interval of time.
O.TIME STAMP	The TOE will provide a reliable time stamp for use by the TOE.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 13 - IT Security Objectives

Name	Description
OE.ACCESS	The IT Environment will ensure that users gain only authorized access to the data the IT Environment manages.
OE.ADMIN_ROLES	The IT Environment will provide administrative roles to isolate administrative actions.
OE.ENFORCE	The IT Environment will support the TOE by providing mechanisms to ensure the TOE is neither bypassed nor interfered with via mechanisms outside the TOE's control.
OE.IA	The IT Environment must require authorized CIFS and NFS Clients to successfully I&A before allowing access to the TOE.
OE.NETWORK	The network path between the TOE components is a trusted channel. The network path between the CLI client and the TOE is a trusted channel.
OE.NTP	The IT Environment will enable the TOE to provide reliable time stamps by implementing NTP.
OE.SUBJECTDATA	The IT Environment will provide the TOE with the appropriate subject security attributes.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 14 - Non-IT Security Objectives

Name	Description
ON.CREDEN	Those responsible for the TOE must ensure that all access credentials, such as passwords, are protected by the users in a manner that maintains IT security objectives.
ON.INSTALL	Those responsible for the TOE and hardware required by the TOE must ensure that the TOE is delivered, installed, configured, managed, and operated in a manner which maintains IT security objectives.
ON.PHYSICAL	Those responsible for the TOE and the network on which it resides must ensure that those parts of the TOE and the IT Environment critical to SFP are protected from any physical attack that might compromise the IT security objectives.
ON.TRAINED	Those responsible for the TOE will be properly trained and provided the necessary information that ensures secure management of the TOE and the IT Environment.

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

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 15 identifies all extended SFRs implemented by the TOE

Table 15 - Extended TOE Security Functional Requirements

Name	Description
FPT_SEP_EXT.1	TSF domain separation for software TOEs

5.1.1 Class FPT: Extended Protection of the TSF

Families in this class address the requirements for functions to implement domain separation functionality as defined in CC Part 2

5.1.1.1 Family FPT_SEP_EXT: TSF Domain Separation for Software TOEs

5.1.1.1.1 Family Behavior

Component Leveling

Figure 5 - TSF Domain Separation for Software TOE's family decomposition

Note: The extended FPT_SEP_EXT.1 a component is part of the FPT_SEP_EXT family.

FPT_SEP_EXT.1:	**TSF Domain Separation for Software TOEs**
	Provides the capability of the TOE to maintain a separate security domain to protect it from untrusted objects under the TOE's control. The extended family "FPT_SEP_EXT" was modeled after other Class FPT SFRs.
Management:	The following actions could be considered for the management functions in FPT_SEP_EXT.1: • Physical storage system administrators performing maintenance (deletion, modification, addition) of SVM (Storage Virtual Machine) units, volumes, users, and groups of users, and their assignment to various SVMs within the TOE's control. • SVM (security domain) administrators performing maintenance (deletion, modification, addition) of volumes, users, and groups of users within the SVM unit.

Audit:	The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST: • Maintenance (deletion, modification, addition) of SVM units, users, and groups of users, and their assignment to various security domains within the TOE's control.
Hierarchical to:	No other components
Dependencies:	No Dependencies
FPT_SEP_EXT.1.1	The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TOE's control.
FPT_SEP_EXT.1.2	The TSF shall enforce separation between the security domains of subjects in the TOE's control.

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components 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 Security Target. 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. 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 selection statements are identified using [<u>underlined text within brackets</u>].
- Completed assignment statements are identified using [*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 end 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 16 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 16 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_GEN.2	User Identity Association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FAU_STG.1	Protected audit trail storage	✓			
FAU_STG.4	Prevention of audit data loss	✓	✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_ATD.1	User attribute definition		✓		
FIA_SOS.1	Verification of secrets		✓		✓
FIA_UAU.2	User authentication before any action			✓	
FIA_UID.2	User identification before any action			✓	
FMT_MOF.1	Management of security function behavior	✓	✓	✓	
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialization	✓	✓		

Name	Description	S	A	R	I
FMT_MTD.1	Management of TSF data	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_SEP_EXT.1	TSF domain separation for software TOEs				
FPT_STM.1	Reliable time stamps				
FTA_SSL.3	TSF-initiated termination		✓		

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

6.2.1 Class FAU: Security Audit

Note: The TSF Security Audit requirements do not apply to the OCI application component. This application does not audit TSF data.

FAU_GEN.1	**Audit Data Generation**
Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events, for the [not specified] level of audit; and c) [The events specified in Table 17].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*the additional event information specified in Table 17*].

Table 17 - FAU_GEN.1.2 Audit Generation Details

SFR Addressed	Auditable Events	Additional Event Information
FIA_UAU.2 FIA_UID.2	Successful local logon	User identity, security domain
FIA_UAU.2 FIA_UID.2	Unsuccessful local logon	User identity supplied, security domain
FMT_SMF.1	Local User created	User ID[20] created, User ID of the administrator performing the action, security domain
FMT_SMF.1	Local User deleted	User ID deleted, User ID of the administrator performing the action, security domain
FMT_SMF.1	Active Directory User or Group created	Group created, User ID of the administrator performing the action, security domain
FMT_SMF.1	Active Directory User or Group deleted	Group deleted, User ID of the administrator performing the action, security domain

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.

FAU_SAR.1	**Audit review**
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide [*authorized administrators*] with the capability to read [all audit information] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

[20] ID - Identifier

FAU_SAR.2	Restricted audit review
Hierarchical to:	No other components.
Dependencies:	FAU_SAR.1 Audit review
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access

FAU_STG.1	Protected audit trail storage
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4	Prevention of audit data loss
Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.

6.2.2 Class FDP: User Data Protection

Note: The User Data Protection requirements do not apply to the OCI. This application does not access user data. It only monitors the storage array resources used to contain that data.

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 [DAC SFP] on [the subjects, objects, and operations among subjects and objects listed in Table 18].

Table 18 - FDP_ACC.1.1 Detail

Subject	Object (Files on the Storage Appliance)			Operation among Subject and Object covered by the DAC SFP
	File Style	File Type	Qtree Type	
NFSv3 Client	NFSv3 UNIX-Style File	Directory, Symbolic Link, Regular File	UNIX Qtree	Create, read, write, execute, delete, change permissions, change ownership
NFSv4 Client	NFSv4 Unix-Style File	Directory, Symbolic Link, Regular File	UNIX Qtree	Create, read, write, execute, delete, change permissions, change ownership
CIFS Client	NTFS-Style File	Directory, Regular File	NTFS Qtree	Create, read, write, execute, delete, change permissions, change ownership

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 initialization
FDP_ACF.1.1	The TSF shall enforce the [DAC SFP] to objects based on the following: [the subjects, objects, operations, and associated security attributes listed in Table 19].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*access is granted if one of the following conditions listed in Table 20 is true*].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*access is granted if the object is a UNIX-style file and the subject is root*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rule: [*access is denied if the subject does not have an Administrative Role*].

Table 19 - FDP_ACF.1.1 Detail

Operation	Subject	Object (File)	Subject		Object (File) Security Attribute	Other Objects and Security Attributes used for DAC SFP
			Security Attribute	Other TSF Data		
Create	NFSv3 Client	NFSv3 UNIX-Style File	UNIX User UID, UNIX User GID	UNIX Username	N/A	UNIX Parent Directory UID, UNIX Parent Directory GID and access mode
	NFSv4 Client	NFSv4 UNIX-Style file	UNIX User UID, UNIX User GID	UNIX Username	N/A	UNIX Parent Directory UID, UNIX Parent Directory ACEs
	CIFS Client	NTFS-Style File	Windows User SID, Windows User GID	Windows Username	N/A	Qtree type, Parent directory's SID and ACEs
Read, Write, Execute	NFSv3 Client	NFSv3 UNIX-Style File	UNIX User UID, UNIX User GID	None	UNIX file UID, UNIX file GID, access mode	None
	NFSv4 Client	NFSv4 UNIX-Style file	UNIX User UID, UNIX User GID	None	UNIX User UID, ACEs	None
	CIFS Client	NTFS-Style File	Windows User SID, Windows User GID	Windows Username	SID and ACEs	None
Delete	NFSv3 Client	NFSv3 UNIX-Style File	UNIX User UID, UNIX User GID	UNIX Username	None	UNIX Parent Directory UID, UNIX Parent Directory GID and access mode
	NFSv4 Client	NFSv4 UNIX-Style file	UNIX User UID, UNIX User GID	None	UNIX User UID, ACEs	UNIX Parent Directory UID, UNIX Parent Directory ACEs
	CIFS Client	NTFS-Style File	Windows User SID, Windows User GID	Windows Username	SID and ACEs	Parent directory's SID and ACEs

Operation	Subject	Object (File)	Subject Security Attribute	Subject Other TSF Data	Object (File) Security Attribute	Other Objects and Security Attributes used for DAC SFP
Change Permission	NFSv3 Client	NFSv3 UNIX-Style File	UNIX User UID, UNIX User GID	UNIX Username	None	UNIX Parent Directory UID, UNIX Parent Directory GID and access mode
	NFSv4 Client	NFSv4 UNIX-Style file	UNIX User UID, UNIX User GID	None	UNIX User UID, ACEs	UNIX Parent Directory UID, UNIX Parent Directory ACEs
	CIFS Client	NTFS-Style File	Windows User SID, Windows User GID	Windows Username	SID and ACEs	Parent directory's SID and ACEs
Change Owner	NFSv3 Client	NFSv3 UNIX-Style File	UNIX User UID	None	UNIX User UID	None
	NFSv4 Client	NFSv4 UNIX-Style file	UNIX User UID	None	UNIX User UID	None
	CIFS Client	NTFS-Style File	Windows User SID, Windows User GID	None	SID and ACEs	None

Table 20 - FDP_ACF.1.2 Detail

Operation	Subject	Object (File)	Rule #	= DAC Rule
Create	NFSv3 Client	NFSv3 UNIX-Style File	1	The subject is the owner of the parent directory and the owner has been granted Write and Execute access (UNIX-Style security attributes).
			2	The subject is not the owner of the parent directory but is a member of the parent directory's group and the group has Write and Execute access (UNIX-Style security attributes).
			3	The subject is neither the owner of the parent directory nor a member of the parent directory's group but Write and Execute access has been granted to all subjects (UNIX-Style security attributes).
	NFSv4 Client	NFSv4 UNIX-Style File	4	The subject is the owner of the parent directory and the owner has been granted Write and Execute access (UNIX-Style security attributes).
			5	There is no parent directory ACE that denies Write or Execute access to the subject and parent directory ACEs exist that grant Write and Execute permission to the subject (NFSv4-Style security attributes).

Operation	Subject	Object (File)	Rule #	= DAC Rule
			6	There is no parent directory ACE that denies Write or Execute access to any group that the subject is a member of and parent directory ACEs exist that grant Write and Execute permission to any group the subject is a member of (NFSv4-Style security attributes).
	CIFS Client	NTFS-Style File	7	There is no parent directory ACE that denies Write or Execute access to the subject and parent directory ACEs exist that grant Write and Execute permission to the subject (NTFS-Style security attributes).
			8	There is no parent directory ACE that denies Write or Execute access to any group that the subject is a member of and parent directory ACEs exist that grant Write and Execute permission to any group the subject is a member of (NTFS-Style security attributes).
Read, Write, Execute	NFSv3 Client	NFSv3 UNIX-Style File	9	The subject is the owner of the file and the owner has been granted access for the specific operation (UNIX-Style security attributes).
			10	The subject is not the owner of the file but is a member of the object's group and the object's group has access for the specific operation (UNIX-Style security attributes).
			11	The subject is neither the owner of the file nor a member of the object's group but the specific access request has been granted to all subjects (UNIX-Style security attributes)
	NFSv4 Client	NFSv4 UNIX-Style File	12	The subject is the owner of the file and the owner has been granted access for the specific operation (UNIX-Style security attributes).
Read, Write, Execute	NFSv4 Client		13	There is no ACE that denies access to the subject for the specific operation and an ACE exists that grants permission to the subject for the specific operation (NFSv4-Style security attributes).
			14	There is no ACE that denies access for the specific operation to any group that the subject is a member of and an ACE exists that grants permission to any group the subject is a member of for the specific operation (NFSv4-Style security attributes).
	CIFS Client	NTFS-Style File	15	There is no ACE that denies access to the subject for the specific operation and an ACE exists that grants permission to the subject for the specific operation (NTFS-Style security attributes).
			16	There is no ACE that denies access for the specific operation to any group that the subject is a member of and an ACE exists that grants permission to any group the subject is a member of for the specific operation (NTFS-Style security attributes).
Delete	NFSv3 Client	NFSv3 UNIX-Style File	17	Rule 1, 2 or 3 above is true (subject has Write and Execute UNIX-Style permission for parent directory).
	NFSv4 Client	NFSv4 UNIX-Style File	18	Rule 12, 13, or 14 above is true (subject has Delete NFSv4-style permission or is UNIX owner for parent directory)

Operation	Subject	Object (File)	Rule #	= DAC Rule
	CIFS Client	NTFS-Style File	19	Rule 15 or 16 above is true for Delete operation (subject has Delete NTFS-Style permission for object).
			20	The subject is not the owner and Rule 21 or 22 below are true (subject has Delete Child NTFS-Style permission for parent directory)
			21	There is no parent directory ACE that denies Delete Child access to the subject and a parent directory ACE exists that grants Delete Child permission to the subject (NTFS-Style security attribute).
			22	There is no parent directory ACE that denies Delete Child access to any group that the subject is a member of and an object ACE exists that grants Delete Child permission to a group the subject is a member of (NTFS-Style security attribute).
Change Permission	NFSv3 Client	NFSv3 UNIX-Style File	23	Rule 1, 2 or 3 above is true (subject has Write and Execute UNIX-Style permission for parent directory) and rule 9, 10 or 11 above is true for Write operation (UNIX-Style permission for object).
	NFSv4 Client	NFSv4 UNIX-Style File	24	Rule 4, 5, or 6 above is true (subject has Write and Execute NFSv4-Style permission for parent directory) and rule 12, 13, or 14 above is true for Change Permission operation (UNIX and NFSv4 Style permission for object)
	CIFS Client	NTFS-Style File	25	Rule 7 or 8 above is true (subject has Write and Execute NTFS-Style permission for parent directory) and rule 15 or 16 above is true for Change Permission operation (NTFS-Style permission for object).
Change Owner	NFSv3 Client	NFSv3 UNIX-Style File	26	If the UNIX UID is root, or the owner of the file, the operation is allowed.
	NFSv4 Client	NFSv4 UNIX-Style File	27	Rule 12, 13, or 14 above is true for Change Ownership operation (subject has Change Owner NFSv4-Style permission or is UNIX-Style owner for object)
	CIFS Client	NTFS-Style File	28	Rule 15 or 16 above is true for Change Ownership operation (subject has Change Owner NTFS-Style permission for object).

6.2.3 Class FIA: Identification and Authentication

Note: The Identification and Authentication requirements of FIA_AFL.1, FIA_ATD.1, FIA_SOS.1(a), and FIA_SOS.1(b) do not apply to the OCI.

FIA_AFL.1	**Authentication failure handling**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication

FIA_AFL.1.1	The TSF shall detect when an administrator configurable positive integer within [*6*] unsuccessful authentication attempts occur related to [login attempts].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock the user, except for the root account, out of the system*].

FIA_ATD.1	**User attribute definition**
Hierarchical to:	No other components.
Dependencies:	No dependencies
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [*TOE username, password, group membership, UNIX User UID and GID; Windows User SID and GID*].

FIA_SOS.1	**Verification of secrets**
Hierarchical to:	No other components.
Dependencies:	No dependencies
FIA_SOS.1(a).1	The TSF shall provide a mechanism to verify that secrets meet [the following criteria: at least 8 characters in length and consist of at least one number and at least one alphabetic character].

FIA_UAU.2	**User authentication before any action**
Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each ~~user~~ **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.

FIA_UID.2	**User identification before any action**
Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies

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

6.2.4 Class FMT: Security Management

FMT_MOF.1	**User identification before any action**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MOF.1.1	The TSF shall restrict the ability to [~~determine the behavior of, disable, enable, modify the administration of~~ **perform**] the functions [Default command access in Table 21, Table 22, and Table 23] to [the roles listed in the previously mentioned tables.]

Table 21 - ONTAP Cluster Administrator Roles Maintained by the TOE

Cluster Administrator Role	Level of access…	to command directory or directories
admin	all	All command directories (DEFAULT)
autosupport	all	• set • system node autosupport
backup	all	• security login password • set • vserver services ndmp
	readonly	• volume
readonly	readonly	All command directories (DEFAULT)
none	none	All command directories (DEFAULT)

Table 22 - ONTAP SVM Administrator Roles Maintained by the TOE

SVM Administrator Role	Level of access…
vsadmin	This role is the super user role for a Vserver and is assigned by default. A Vserver administrator with this role has the following capabilities: • Managing own user account local password and key information • Managing volumes, quotas, qtrees, Snapshot copies, and files. • Managing LUNs • Configuring protocols: NFS, CIFS, iSCSI, and FC (FCoE included) • Configuring services: DNS, LDAP, and NIS • Monitoring jobs • Monitoring network connections and network interface • Monitoring the health of a Vserver
vsadmin-volume	A Vserver administrator with this role has the following capabilities: • Managing own user account local password and key information • Managing volumes, quotas, qtrees, Snapshot copies, and files. • Managing LUNs • Configuring protocols: NFS, CIFS, iSCSI, and FC (FCoE included) • Configuring services: DNS, LDAP, and NIS • Monitoring network interface • Monitoring the health of a Vserver
vsadmin-protocol	A Vserver administrator with this role has the following capabilities: • Managing own user account local password and key information • Configuring protocols: NFS, CIFS, iSCSI, and FC (FCoE included) • Configuring services: DNS, LDAP, and NIS • Managing LUNs • Monitoring network interface • Monitoring the health of a Vserver

SVM Administrator Role	Level of access…
vsadmin-readonly	A Vserver administrator with this role has the following capabilities: • Managing own user account local password and key information • Monitoring the health of a Vserver • Monitoring network interface • Viewing volumes and LUNs • Viewing services and protocols
vsadmin-backup	A Vserver administrator with this role has the following capabilities: • Managing NDMP operations • Making a restored volume as read-write • Viewing volumes and LUNs **Note**: A Vserver administrator with vsadmin-backup role cannot manage own user account local password and key information

Table 23 - OnCommand Insight (OCI) Roles Maintained by the TOE

Roles applicable to OCI	Level of access…
guest	Guest permits you to log into Insight and to view the various pages. If your user account is defined to the OnCommand Insight local user database (and not through LDAP), you can also modify your own password. This account type does not allow you to perform actions such as identifying generic devices and defining the policies in the Java UI.
user	User permits all guest-level privileges, as well as access to Insight operations such as defining policy and identifying generic devices. The User account type does not allow you to perform data source operations, nor to add or edit any user accounts other than your own.
administrator	Administrator permissions vary depending on whether you use LDAP: • If you authenticate and authorize users through LDAP, this level of permission allows you manage data sources. • If you use only the local database to manage users, this level of permission allows you perform any operation, including adding new users and managing data sources.

FMT_MSA.1	**Management of Security Attributes**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MSA.1.1	The TSF shall enforce the [*DAC SFP*] to restrict the ability to [<u>modify, delete, *add*</u>] the security attributes [*TOE User UID and TOE User Primary GID maintained locally by the TOE and described in* 7.1.2.1.1] to [*an authorized administrator*].

FMT_MSA.3	Static Attribute Initialization
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 [*DAC SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [*no authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1	Management of TSF data
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MTD.1.1	The TSF shall restrict the ability to [query, modify, delete] the [local user account repository] to [authorized administrators with the Admin or OnCommand administrator role].

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: [management of security functions behavior, management of security attributes, and management of TSF data].

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 [as identified in Tables 20 - 22].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.2.5 Class FPT: Protection of the TSF

Note: The Protection of the TSF requirements do not apply to the OCI.

FPT_SEP_EXT.1	**TSF Domain Separation for Software TOEs**
Hierarchical to:	No other components.
Dependencies:	No dependencies
FPT_SEP_EXT.1.1	The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TOE's control.
FPT_SEP_EXT.1.2	The TSF shall enforce separation between the security domains of subjects in the TOE's control.

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.

6.2.6 Class FTA: TOE Access

FTA_SSL.3	**TSF-initiated termination**
Hierarchical to:	No other components.
Dependencies:	No dependencies
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [configurable time interval of user inactivity at the CLI, defaulting to 30 minutes].

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.3. Table 24 summarizes the requirements.

Table 24 - Assurance Requirements

Class	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

Class	Assurance Requirements
	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.3 Systematic 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 Security 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 25 lists the security functionality and their associated SFRs.

Table 25 - Mapping of TOE Security Functionality Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security function behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_SEP_EXT.1	TSF domain separation software TOEs
	FPT_STM.1	Reliable time stamps
TOE Access	FTA_SSL.3	TSF-initiated termination

7.1.1 Security Audit

In the ONTAP portion of the TOE, two (2) types of security auditing occurs:

- Cluster administrative command auditing
- NAS event auditing for user data file access

7.1.1.1 Cluster Administrative Command Audit

ONTAP captures every administratively issued command which changes the configuration of the storage array. These changes are:

- Object or attribute creation/addition
- Object or attribute modification/assignment
- Object or attribute removal/deletion

The source of the command may be from the CLI interface, the OnCommand System Manager GUI interface, or by other means via the API interface. The administrator cannot suppress the generation of these audit events.

Optionally, the ONTAP may be configured to also record any read-only event of configuration data. By default, auditing of read-only events is suppressed.
ONTAP may be configured to forward the “command-history” audit data to one or more designated SYSLOG server destinations, or the data may be retrieved via read-only browser access to the Service Processor Infrastructure (SPI) web interface (as shown):

https://<ip-address-of-cluster-admin-interface>/spi

(You will be required to authenticate as a valid administrative user to access this data).

7.1.1.2 NAS Event Audit for User Data File Access

NAS event auditing is accomplished using staging files contained within staging volumes.

Staging files
The intermediate binary files on individual nodes where audit records are stored prior to consolidation and conversion. Staging files are contained in staging volumes.

Staging volume
A dedicated volume created by ONTAP to store staging files. There is one staging volume per aggregate. Staging volumes are shared by all audit-enabled Storage Virtual Machines (SVMs) to store audit records of data access for data volumes in that aggregate. Each SVM's audit records are stored in a separate directory within the staging volume.
Cluster administrators can view information about staging volumes, but most other volume operations are not permitted. Only ONTAP can create staging volumes. ONTAP automatically assigns a name to staging volumes. All staging volume names begin with “MDV_aud_” followed by the UUID of the aggregate containing that staging volume (for example: MDV_aud_1d0131843d4811e296fc123478563412.)
System volumes
A FlexVol volume that contains special metadata, such as metadata for file services audit logs. The admin SVM owns system volumes, which are visible across the cluster. Staging volumes are a type of system volume.

Consolidation task
A task that gets created when auditing is enabled. This long-running task on each SVM takes the audit records from staging files across the member nodes of the SVM. This task merges the audit records in sorted chronological order, and then converts them to a user-readable event log format specified in the auditing configuration - either the EVTX or XML file format. The converted event logs are stored in the audit event log directory that is specified in the SVM auditing configuration.

About the ONTAP auditing process
The ONTAP auditing process is different than the Microsoft auditing process.

Audit records are initially stored in binary staging files on individual nodes. If auditing is enabled on an SVM, every member node maintains staging files for that SVM. Periodically, they are consolidated and converted to user-readable event logs, which are stored in the audit event log directory for the SVM.

Process when auditing is enabled on an SVM

Auditing can only be enabled on SVMs with FlexVol volumes. When the storage administrator enables auditing on the SVM, the auditing subsystem checks whether staging volumes are present. A staging volume must exist for each aggregate that contains data volumes owned by the SVM. The auditing subsystem creates any needed staging volumes if they do not exist. The auditing subsystem also completes other prerequisite tasks before auditing is enabled:

- The auditing subsystem verifies that the log directory path is available and does not contain symlinks.
  The log directory must already exist. The auditing subsystem does not assign a default log file location. If the log directory path specified in the auditing configuration is not a valid path, auditing configuration creation fails with the following error:

  The specified path "/<path>" does not exist in the namespace belonging to Vserver “<vserver_name>"

  Configuration creation fails if the directory exists but contains symlinks.
- Auditing schedules the consolidation task.

After this task is scheduled, auditing is enabled. The SVM auditing configuration and the log files persist across a reboot or if the NFS or CIFS servers are stopped or restarted.

Event log consolidation

Log consolidation is a scheduled task that runs on a routine basis until auditing is disabled. When auditing is disabled, the consolidation task ensures that all the remaining logs are consolidated.

Guaranteed auditing

By default, auditing is guaranteed. Data ONTAP guarantees that all auditable file access events (as specified by configured audit policy ACLs) are recorded, even if a node is unavailable. A requested file operation cannot be completed until the audit record for that operation is saved to the staging volume on persistent storage. If audit records cannot be committed to the disk in the staging files, either because of insufficient space or because of other issues, client operations are denied.

Consolidation process when a node is unavailable

If a node containing volumes belonging to an SVM with auditing enabled is unavailable, the behavior of the auditing consolidation task depends on whether the node's SFO partner (or the HA partner in the case of a two-node cluster) is available.

- If the staging volume is available through the SFO partner, the staging volumes last reported from the node are scanned, and consolidation proceeds normally.
- If the SFO partner is not available, the task creates a partial log file. When a node is not reachable, the consolidation task consolidates the audit records from the other available nodes of that SVM. To identify that it is not complete, the task adds the suffix .partial to the consolidated file name.
- After the unavailable node is available, the audit records in that node are consolidated with the audit records from the other nodes at that point of time.
- All audit records are preserved.

Event log rotation
Audit event log files are rotated when they reach a configured threshold log size or on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file.

Process when auditing is disabled on the SVM
When auditing is disabled on the SVM, the consolidation task is triggered one final time. All outstanding, recorded audit records are logged in user-readable format. Existing event logs stored in the event log directory are not deleted when auditing is disabled on the SVM and are available for viewing.
After all existing staging files for that SVM are consolidated, the consolidation task is removed from the schedule. Disabling the auditing configuration for the SVM does not remove the auditing configuration. A storage administrator can reenable auditing at any time.
The auditing consolidation job, which gets created when auditing is enabled, monitors the consolidation task, and re-creates it if the consolidation task exits because of an error. Previously, users could delete the auditing consolidation job by using job manager commands such as job delete. Users are no longer allowed to delete the auditing consolidation job.

Viewing audit event logs
You can view and process audit event logs saved in the EVTX or XML file formats. Viewing is accomplished by exporting the audit log directory (NFS) or sharing via SMB (CIFS) and using the appropriate applications on the host where viewing is to occur.

- **EVTX file format**
  You can open the converted EVTX audit event logs as saved files using Microsoft Event Viewer.
  There are two options that you can use when viewing event logs using Event Viewer:
  - General view
    Information that is common to all events is displayed for the event record. In this version of ONTAP, the event-specific data for the event record is not displayed. You can use the detailed view to display event-specific data.
  - Detailed view
    A friendly view and a XML view are available. The friendly view and the XML view display both the information that is common to all events and the event-specific data for the event record.
- **XML file format**
  You can view and process XML audit event logs on third-party applications that support the XML file format. XML viewing tools can be used to view the audit logs provided you have the XML schema and information about definitions for the XML fields. For more information about obtaining the XML schema and documents related to XML definitions, contact NetApp technical support.

Note: See the ONTAP 9 CIFS and NFS Auditing Guide for additional details.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4

7.1.2 User Data Protection

The TSF mediates access of subjects and objects. The subjects covered by the DAC SFP are NFS Clients and CIFS Clients. The objects covered by the DAC SFP are files (user data). The TOE maintains files with either NTFS-Style security attributes or UNIX-Style security attributes. The access modes covered by the DAC SFP are: create, read, write, execute, delete, change permission and change owner. The DAC SFP is detailed below:

7.1.2.1 Discretionary Access Control Security Function Policy

The DAC SFP protects user data (FDP_ACC.1). The DAC SFP uses the subject type, subject's security attributes, the object, the object's security attributes and the access mode (operation) to determine if access is granted. For some operations, the security attributes of the object's parent directory are also used. The following sections describe the DAC SFP and provide the Security Functional Requirements that meet the Security Function.

7.1.2.1.1 DAC SFP Object Security Attributes

The User Data that is covered by the DAC SFP are files (objects). Each file maintained by the TOE has a file style associated with it. The type of security attributes associated with the file defines a file style. The TOE maintains two styles of files: UNIX-Style files and NTFS-Style files. UNIX-Style files have UNIX-Style security attributes and NTFS-Style files have NTFS-Style security. Each file style is assigned different security attributes that are used by the DAC SFP to determine if access is granted for a subject.
In addition to a file style, each file has a file type. The file types may be directories, symbolic links, or regular files. UNIX-Style files may be a directory, a symbolic link, or a regular file (FDP_ACC.1). NTFS-Style files do not have symbolic links; therefore, the file type will be either directory or regular file (FDP_ACC.1).

In addition to the file type, the TOE maintains three different storage types: UNIX Qtrees, NTFS Qtrees or mixed Qtrees. A Qtree is a disk space partition. UNIX Qtrees store UNIX-Style files with UNIX-Style security attributes. NTFS Qtrees store NTFS-Style files with NTFS-Style security attributes. Mixed Qtrees store both styles of files. Any file may have either UNIX-Style security attributes or NTFS-Style security attributes associated with them. Mixed Qtrees will not be part of the evaluated configuration. The following sections describe the security attributes associated with the objects.

NFSv3 UNIX-Style File Security Attribute Description
A UNIX-Style file managed by the TOE has twelve security attributes that are used to determine file access. The security attributes include a UNIX File UID, a UNIX file GID, a file type character, and a nine-character access mode string. The UNIX File UID is the UID of the file's owner. The UNIX file GID is the GID associated with the file. The access mode is a subset of characters within the file's file permission string. The file permission string is represented in ten characters common to all UNIX files (e.g. drwxrwxrwx). The first character contains one of three characters that identify the file type: d for directory, l for a symbolic link, or a dash (-) indicates the file is a regular file. The following 9 characters represent the access mode for the file in three sets of rwx triplets. The first triplet specifies the permission for the file's owner (UID). The next triplet specifies the permissions for the group associated with the file (UNIX file GID). The last three characters specify the permission for the users who are neither the owner nor members of the file's group (other). The rwx triplet identifies the permission for that set (owner, group, other). The three characters represent read, write, or execute privileges. If the character is a dash, the set does not have permissions to perform the specific action (FDP_ACF.1). A directory's permission string may also contain a "sticky bit" represented at the end of the nine-character access mode string by a "T" (e.g. drwxrwxrwxT). A sticky bit-enabled directory signifies that files or folders created within this directory can only be deleted by the file owner.

To determine if a client user has read, write, or execute permission for a UNIX-Style file, the TOE first compares the client's UNIX User UID with the file's UID. The UNIX User UID is a unique positive integer assigned by the UNIX system administrator to each user. If a match occurs (the client is the owner) and the file's access mode specifies permission for the specific access request (rwx), the request is allowed. If the owner does not have permission to perform the request, the request is denied. If the client is not the file's owner, the TOE determines if the client is a member of the file's group by comparing the client's UNIX User's Primary Group ID (GID) to the file's GID. The UNIX administrator assigns each User a unique Primary GID during account creation or modification. If the client is a member of the file's group and the access mode specifies permission for the specific access request, the request is allowed. If the group does not have permission to perform the request, the request is denied. If the client user is not the file's owner or a member of the file's group, the TOE then determines if all others (the last triplet) have permission to perform the request. If all others have permission, the request is honored. Otherwise the request is denied (FDP_ACF.1).

For the remainder of this document, when the DAC SFP rules state that the TOE determines if a client, using UNIX-Style security attributes, has access, the above steps are what the TOE performs: the TOE walks through the owner, group, and other attributes to determine access.

NFSv4 UNIX-Style File Security Attribute Description

The TOE's NFSv4 UNIX-Style file security attributes are NFSv4 ACLs. Each file has a data structure associated with it containing the file owner's UID and an ACL. Each ACL consists of one or more ACE(s). Each ACE explicitly allows or denies access to a single user or group. Access is allowed if there is no ACE that denies access to the user or any group that the user is a member of and if an ACE exists that grants permission to the user or any group the user is a member of.

This determination is made by consulting the ownership, permissions, and ACEs on the file or directory and comparing against the UID and GID of the requesting user. The group memberships (and possibly username to UID number mapping) are obtained from local files or a directory service, while the file permissions and ACLs are stored in the file system.

For the remainder of this document, when the DAC SFP rules state that the TOE determines if a client, using NFSv4 UNIX-Style security attributes, has access, the above steps are what the TOE performs to determine access.

NTFS-Style File Security Attributes Description

The TOE's NTFS-Style file security attributes are standard Windows file security attributes. Each file has a data structure associated with an SD. This SD contains the file owner's SID, group's SID, DACL[21], and SACL[22]. Each ACL consists of one or more ACEs. Each ACE explicitly allows or denies access to a single user or group. Access is allowed if there is no ACE that denies access to the user or any group that the user is a member of and if an ACE exists that grants permission to the user or any group the user is a member of.

For the remainder of this document, when the DAC SFP rules state that the TOE determines if a client, using NTFS-Style security attributes, has access, the above steps are what the TOE performs to determine access.

7.1.2.1.2 DAC SFP Access Requests

Access requests define what operation a subject has requested to perform on an object. The TOE's DAC SFP addresses seven access requests: create, read, write, execute, delete, change permissions, and change owner (FDP_ACC.1). The following sections define the operations.

---

[21] DACL - Discretionary ACL; Used to determine permissions.

[22] SACL - System ACL; Used for auditing purposes.

UNIX-Style Access Requests

The following Table 26 identifies the operations of subjects on UNIX-Style files (objects) covered by the DAC SFP and explains what each of the file access request means.

Table 26 - UNIX-Style File Access Requests

DAC SFP Operation	UNIX-Style File Types		
	Directory	Symbolic Link	Normal File
Create	Create a directory.	Create a symbolic link.	Create a file.
Read	Get info about the directory or its contents.	Read the file the symbolic link contains the name of.	Read the file.
Write	• Add a file in the directory • Rename a directory	Write to the file the symbolic link contains the name of.	Append/write/truncate the file.
Execute	Traverse the directory; change the working directory or access a file or subdirectory in the directory.	Execute the file the symbolic link contains the name of.	Execute the file.
Delete	Delete the directory.	Delete the symbolic link.	Delete the file.
Change Permission	Change the permission of the directory.	Change the permission of the symbolic link.	Change the permission of the file.
Change Owner	No effect.	Become the symbolic link's owner.	Become the file's owner.

NTFS-Style File Access Requests

The NTFS-Style file security attributes define more access modes than UNIX does. There are, however, no symbolic links in NTFS-Style files. The following Table 27 identifies the operations of subjects on NTFS-Style files (objects) covered by the DAC SFP and explains what each of the basic file access request means.

Table 27 - NTFS-Style File Access Requests

DAC SFP Operation	NTFS-Style File Types	
	Directory	Normal File
Create	Create a directory	Create a file.
Read	Get info about the directory or its contents	Read the file.
Write	• Add a file in the directory • Rename a directory	Truncate, append, or overwrite the file.
Execute	No effect	If the file has an extension of .exe or .com, attempt to execute it as a native binary. If it has an extension of .bat or .cmd, attempt to execute it as a batch or command file using the command interpreter.

DAC SFP Operation	NTFS-Style File Types	
	Directory	Normal File
Delete	Delete the directory. Delete privilege must be explicitly granted on the contained files and subdirectories before they can be deleted. A directory may not be deleted unless it is empty.	Delete the file.
Change Permission	Change the permissions on the directory (change the directory's ACL)	Change the file's ACL.
Change Owner	Become the directory's owner	Become the file's owner.

7.1.2.1.3 DAC Operations and Rules

In general, the TOE supports access to all objects from all subjects. However, the following exceptions apply:

- Client – The DAC SFP supports client protocol-specific support for create, read, write, execute, delete, change permission and change owner operations.
- File Style – The file style (UNIX-Style or NTFS-Style) is considered in the TOE's DAC SFP Rules because the type of security attributes maintained by the object aids in determining the type of security attributes required by the client.
- File Type – The file type (directory, symbolic link, or regular file) is considered when determining if object access is allowed for a subject. The CIFS protocol does not know about symbolic links. Therefore, CIFS Clients will not request an operation for a symbolic link; the only operations for objects with file type of symbolic link applicable to the DAC SFP are NFS Client operations for UNIX-Style files.
- Additional Data – As well as client security attributes and object security attributes, certain operations require the TOE to examine the security attributes of other objects to determine if access is allowed, specifically, the object's parent directory. The TOE examines the security attributes of an object's parent directory for create, delete and change permission operations.
- Operation – The operations supported by the DAC are: Create, Read, Write, Execute, Delete, Change Permissions, and Change Owner. The execute command is treated differently for the different file styles and file types. Executing an NTFS directory has no effect. Executing a UNIX- Style directory means to traverse the directory, change the working directory, or access a file or subdirectory in the directory.

7.1.2.1.4 DAC SFP Subject Security Attributes

The subjects that apply to the DAC SFP are subjects with or without administrative roles; they access the TOE as NFS Clients and CIFS Clients (FDP_ACC.1). To determine if access is permitted for an object, the TOE requires the security attributes associated with the client. These security attributes may be resolved by the TOE or the IT Environment.

The subject security attributes required by the DAC SFP depend on the type of security attributes maintained by the object; the object will require either UNIX-Style subject security attributes or NTFS-Style subject security attributes to determine if access is permitted. Based on the native systems, NFS clients are typically associated with UNIX-Style security attributes and CIFS Clients are associated with NTFS-Style security attributes. The following sections describe the TOE's subject security attribute resolution used to enforce the DAC SFP.

Derivation of UNIX-Style Client Subject Security Attributes
If the TOE determines that NFSv3 UNIX-Style security attributes should be used to determine access for an object, the TOE requires a client's (subject's) UNIX User UID and UNIX User GID (FDP_ACF.1).

If the TOE determines that the NFSv4 UNIX-Style security attributes should be used to determine access for an object, the TOE requires a client's (subject's) UNIX User UID and GID with permission matching the file's ACL (FDP_ACF.1).

If the access request is initiated by an NFS Client, the TOE received the NFS Client's UNIX User UID in the NFS request (IT Environment). The TOE then searches the IT Environment to get the UNIX User GID and UNIX username (FDP_ACF.1).

Derivation of NTFS-Style Client Subject Security Attributes
If the TOE determines that NTFS-Style security attributes should be used to determine access for an object, the TOE requires two subject security attributes: a Windows User SID and a Windows User GID.

If the access request is initiated by a CIFS Client, the TOE obtained the CIFS Client's username (Windows username) when the client logged onto the remote system and joined the Windows Domain. In addition to this, the IT Environment queried the domain controller to obtain the Windows User SID and the Windows User GID.

DAC SFP Rules
The DAC SFP rules that apply depend on the subject, the operation, and the object. In addition, the objects file type (directory, symbolic link and regular) is used to determine access and the type of Qtree the file is stored in. The five access modes under the control of the TOE DAC SFP are described below.

CREATE ACCESS REQUEST
To determine if a client has permissions to create a file, the TOE first looks at the parent directory's security attributes.

If the parent directory is **NTFS-Style**, the TOE uses NTFS-Style security attributes for both subject and object to determine if access is permitted. If the client does not have write and execute privileges to the parent directory, the request is denied. If the client has write and execute privileges for the parent directory, the file is created (FDP_ACF.1). In an NTFS Qtree, the new file inherits the NTFS-Style security attributes from the parent directory (FMT_MSA.3).

If the parent directory is **NFSv3 UNIX-Style**, the TOE uses NFSv3 UNIX-Style security attributes for both subject and object to determine access. If the client does not have write and execute privileges to the parent directory, the request is denied. If the client has write and execute privileges for the parent directory, the file is created (FDP_ACF.1). In a UNIX Qtree, the new file's NFSv3 UNIX-Style security attributes are determined by the file mode creation mask, also known as the User Mask (umask) of the user-owned process creating the file (FMT_MSA.3).

If the parent directory is **NFSv4 UNIX-Style**, the TOE uses NFSv4-Style ACL security attributes for the object, and UNIX user UID and GID for the subject. If the client has write and execute privileges for the parent directory, the file is created (FDP_ACF.1). In an NFSv4 UNIX-Style Qtree, the new file inherits the NFSv4 UNIX-Style security attributes from the parent directory (FMT_MSA.3).

READ, WRITE, EXECUTE ACCESS REQUESTS
To determine if a client has permission to read, write or execute a file, the TOE first examines the client type. If a client requests access to a file with NFSv3 UNIX-style security attributes, the TOE uses NFSv3 UNIX- Style security attributes for both subject and object to determine if read, write, or execute access request is permitted. If the client has read, write, or execute permission for the file, access is permitted (FDP_ACF.1). If the client does not have access, the request is denied.

Otherwise, the TOE uses the file's ACL to determine if read, write, or execute permission is allowed. The TOE uses NFSv4 or NTFS-Style security attributes for both subject and object to determine access. The TOE determines if the file's ACEs allow permission for the specific request. If they do, access is granted (FDP_ACF.1). If the ACEs do not grant permission, access is denied.

CLIENT DELETE ACCESS REQUEST
To determine if a client has permission to delete a file, the TOE looks at the styles of the file and parent directory.

NFSv3 UNIX-Style File stored in a UNIX-Style Parent Directory
The TOE, using NFSv3 UNIX-Style security attributes for both subject and object, determines if the client has write and execute access for the file's parent directory. If the client does, the delete access is permitted (FDP_ACF.1). Otherwise, access is denied.

NFSv4 and NTFS-Style File stored in an NTFS-Style Parent Directory
The TOE, using NFSv4 and NTFS-Style security attributes for both subject and object, first determines if the file's ACL grants the client delete access to the file. If so, access is granted (FDP_ACF.1). If the file's ACEs do not grant delete permission for the client, the TOE determines if the parent directory has a DC (Delete Child) ACE that grants access for the subject. If the parent does, delete access is permitted (FDP_ACF.1). Otherwise, access is denied.

CHANGE PERMISSION ACCESS REQUESTS
To determine if a client has permission to change the permissions of a file, the TOE looks at the styles of the file and parent directory.

NFSv3 UNIX-Style File stored in a UNIX-Style Parent Directory
The TOE, using NFSv3 UNIX-Style security attributes for both subject and object, determines if the client has write and execute access for the file's parent directory. If the client does, and the client also has write access for the file, the change permission access is permitted (FDP_ACF.1). Otherwise, access is denied.

NFSv4 and NTFS-Style File stored in an NTFS-Style Parent Directory
The TOE, using NFSv4 and NTFS-Style security attributes for both subject and object, determines if the file's ACL grants the client change permission access to the file. If so, the TOE determines if the parent directory's ACL grants write and execute access for the subject. If so, change permission access is permitted (FDP_ACF.1). Otherwise, access is denied.

CHANGE OWNER ACCESS REQUESTS
The DAC SFP distinguishes between the NFS Client Change Owner (chown) UNIX command and the CIFS Client Change Owner (Change Ownership) command.
NFSv3 Clients

If an NFSv3 Client requests a Change Owner request (chown) for an NTFS-Style file, the request is denied (FDP_ACF.1). If an NFS Client sends a Change Owner request (chown) for an NFSv3 UNIX-Style directory, the request is denied. For other UNIX-Style file types, the TOE determines if the client is root (UNIX User UID is root UID) or the file owner. If the client is root or the file owner, access is allowed (FDP_ACF.1) and the TOE changes the object's owner to the owner specified in the chown request. If the object had an ACL, the TOE removes the ACL.

NFSv4 Clients
If an NFSv4 Client requests a Change Owner request for an NTFS-Style file, the request is denied (FDP_ACF.1). If the file is an NFSv4 UNIX-Style file, the TOE determines if the client has Change Owner

ACE privileges for the file. If the client does, access is allowed (FDP_ACF.1). The TOE will replace the existing owner ACE with the new ACE sent in the command. If the NFSv4 Client does not have Change Owner privileges, the request is denied.

CIFS Clients
If a CIFS Client requests a Change Owner request for a UNIX-Style file, the request is denied (FDP_ACF.1). If the file is an NTFS-Style file, the TOE determines if the client has Change Owner ACE privileges for the file. If the client does, access is allowed (FDP_ACF.1). The TOE will replace the existing owner ACE with the new ACE sent in the command. If the CIFS Client does not have Change Owner privileges, the request is denied.

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

7.1.3 Identification and Authentication

The TOE's I&A functionality enforces human administrators to identify and authenticate themselves to the TOE before allowing any modifications to TOE managed TSF Data (FIA_UID.2, FIA_UAU.2). Administrators authentication credentials are maintained by the TOE in a local registry. The file contains the username, password, full name, password aging, role, and other similar characteristics for each administrator. Authentication credentials are maintained by the TOE in a local registry. Several roles exist for administrator authentication: admin, autosupport, backup, readonly, and none.
The ONTAP portion of the TOE enforces minimum password strength requirements. Passwords must have a length of at least 8 characters and contain at least one numeric character and at least one alphabetic character (FIA_SOS.1(a)). The TOE also maintains the following attributes for administrative accounts: TOE username, password, group membership, UNIX User UID and GID, and Windows User SID and GID (FIA_ATD.1).

The TOE enforces minimum password strength requirements. The ***security login role config create***, and ***security login role modify*** commands offer parameters to specify the minimum number of alphabetic characters, a mix of alphabetic with numeric, and the number of special characters that a password must contain. The parameters setting password requirements are:

- **-passwd-minlength** – This specifies the required minimum length of a password. Possible values range from 3 to 64 characters. The default setting is 8 characters.
- **-passwd-alphanum** – This specifies whether a mix of alphabetic and numeric characters is required in the password. If this parameter is enabled, a password must contain at least one letter and one number. This needs to be enabled.
- **-passwd-min-special-chars** – This specifies the minimum number of special characters required in a password. Possible values range from 0 to 64 special characters.

The TOE will lock out an administrator account if the user fails to enter the proper credentials. Lockout occurs after **–max- failed-login-attempts** ***failed login attempts*** set by the ***security login role config modify*** or ***create*** command. (FIA_AFL.1). Recommended value for this attribute is **6**.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2

7.1.4 Security Management

The Administrative Security Function provides the necessary functions, or capabilities, to allow ONTAP 9.1 cluster and Vserver administrators to manage and support the TSF within the ONTAP 9.1 and the ONTAP Select portions of the TOE. Included in this functionality are the rules enforced by the TOE that define access to TOE-maintained TSF Data and TSF Functions. The TSF Functions are categorized into the groups of capabilities listed in Table 28:

Table 28 - Security Function Capabilities

Role Configurable Capability	Capabilities
Command Directory Access	Grants the specified role specific command capabilities. This specifies the command or command directory to which the role has access. This includes permission for all variations of the security command.
Access	The possible access level settings are none, read-only, and all. The default setting is all.
Query	This optionally specifies the object that the role can access. The query object must be applicable to the command or directory name specified by the –cmddirname parameter. The query object must be enclosed in double quotation marks (“”), and it must be a valid field name.

Only administrative users associated with the specific roles as outlined in Table 20 for a Cluster Administrator may modify the association between users, groups, and any of the above capabilities.
For OnCommand Insight, the management functionality available to a user is dependent on the assigned role; the assigned role may be administrator, user, or guest. Each role has access to a set of functionality appropriate for that role.

The TOE provides several interfaces for administrators to use to manage the behavior of the TSFs. The various management interfaces available to administrators are outlined below:

CLI (ONTAP 9.1)
Local CLI available via a serial terminal connected to the console port of the appliance. Remote CLI available via a secure shell program, such as SSH, OpenSSH, PuTTY, etc.

(See section 1.6.3 for a list of other methods of accessing the CLI which are not included in the evaluated configuration of the TOE).

CLI (ONTAP Select 9.1)
Remote CLI available via a secure shell program, such as SSH, OpenSSH, PuTTY, etc.

(See section 1.6.3 for a list of other methods of accessing the CLI which are not included in the evaluated configuration of the TOE).

OnCommand System Manager GUI
The OnCommand System Manager GUI is integral to ONTAP 9.1 and ONTAP Select. The OnCommand System Manager GUI makes API calls to the System Administration TOE component for management of the TOE security functions.

OCI Web Interfaces and API
The OnCommand component (OCI) is an application installed on a separate management application server (standalone or VM). The external interfaces of OCI provide diagnostics based on storage availability, capacity, performance, and protection and allow for operators, storage administrators, and OnCommand administrators to analyze collected data and take corrective or preventative actions if necessary.

7.1.4.1 Management of Security Attributes

The TOE protects TSF data via the implementation of the DAC SFP as described in section 7.1.2.1 above. The security attributes upon which the DAC SFP relies for access control are configurable only by users who are owners of the object or users who are assigned the admin role.

The management of security attributes is performed by editing the attributes of individual objects such as the SD of NTFS-style files, the ACL of NFSv4 UNIX-style files, or the nine-character access mode string of NFSv3 UNIX-style files, by editing the file's group membership, or by editing a user's membership in a group. For more information on the security attributes of TSF data, see section 7.1.2.1.1 and its subsections above.

7.1.4.2 Management of TSF Data

The ONTAP 9.1 and ONTAP Select portion of the TOE's Administration Security Function includes TSF Data Management. The TSF Data Management includes management of both authentication data and security attributes. The TOE manages the following data:

- TOE Username Management.
- Deny unauthorized administrative login attempts via ONTAP 9.1 and ONTAP Select.
- Implement a "Sleep Mode" function call to ONTAP 9.1 and ONTAP Select to deny access and initiate a time out period for further login attempts, to counter brute force password guessing.

The ONTAP 9.1 and ONTAP Select portions of the TOE maintain authentication data locally that is used to authenticate the ONTAP administrators. This authentication database can only be accessed through the security command. The OnCommand Insight also maintains authentication data locally to authenticate administrators.

7.1.4.3 Management of Roles

Within ONTAP 9.1 and ONTAP Select, the TOE maintains the following roles for users: admin, autosupport, backup, readonly, none, vsadmin, vsadmin-volume, vsadmin-protocol, vsadmin-backup, and vsadmin-readonly. The admin role has the default capability to administratively access the TOE and modify security attributes. The other administrative roles have varying functionality as defined in Tables 20 and 21.

Within OnCommand Insight, the TOE maintains the following roles for users: guest, user, and administrator. The administrator role has the capability to administer users and perform the generic maintenance tasks required for TOE operation of the OnCommand Insight component. The other roles have varying functionality as defined in Table 22.

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

7.1.5 Protection of the TSF

The TOE protects the TSF via the implementation of SMT (i.e., domain separation) made possible by SVM functionality.

Secure Multi-Tenancy is the use of secure virtual partitions within a shared physical storage environment for sharing the physical environment among multiple distinct tenants. SMT allows the consolidation of tenants into shared resources, at the same time providing assurance that tenants cannot access resources not explicitly assigned to them.

ONTAP is an inherently multi-tenant storage operating system and is architect to provide data access through secure virtual storage partitions. A cluster can be a single partition representing the resources of the entire cluster, or can be divided into multiple partitions, each representing specific subset of cluster resources. These secure virtual storage partitions are called Storage Virtual Machines (SVMs).

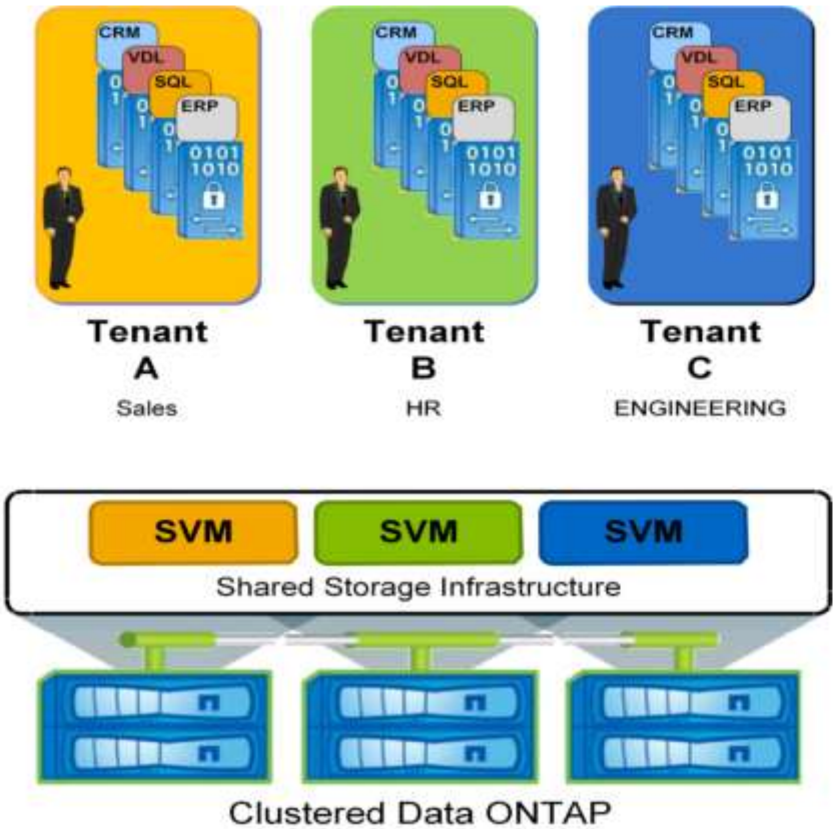
A cluster serves data through one of more SVMs. An SVM provides logical abstraction that represents a set of physical resources on the cluster. Data volumes and network logical interfaces (LIFs) are created and assigned to an SVM and may reside on any node in the cluster to which the SVM has been given access. An SVM may own resources on multiple nodes concurrently, and those resources can be moved from one node to another without disruption.

An SVM can support multiple protocols concurrently. Volumes within the SVM can be appended together to form a single NAS namespace, which makes all an SVM's data available through a single share or mount point to NFS and CIFS clients. SVMs also support block-based protocols, and LUNs can be created and exported using iSCSI, Fiber Channel, or Fiber Channel over Ethernet. Any of these data protocols may be configured for use within a given SVM.

SVM, being a secure entity, is only aware of the resources that have been assigned to it and has no knowledge of other SVMs and their respective resources. Each SVM operates as a separate and distinct entity with its own security domain. Tenants manage resources allocated to them through a delegated SVM administration account. Each SVM connects to unique authentication zones such as Active Directory, LDAP, or NIS. An SVM is effectively isolated from other SVMs that share the same physical hardware.

As illustrated in Figure 6, an SVM's configuration allows it to store and retrieve data in the correct context in its storage units. This information also allows the SVM to correctly interpret the access control and security-related meta-information embedded in its storage.

Figure 6 – Storage Virtual Machines enable Secure Multi-tenancy for Shared Storage Implementations



For more information on SVM and its components including LIFs, Flexible Volumes, Namespace, and Infinite Volume, please refer to NetApp document "Secure Multi-Tenancy in ONTAP – Overview and Design Considerations, April 2013".

The system clock is set at boot via the Network Time Protocol and provides reliable time stamps for use by the TOE.

TOE Security Functional Requirements Satisfied: FPT_SEP_EXT.1, FPT_STM.1

7.1.6 TOE Access

The TOE mitigates unauthorized administrator access by automatically terminating administrator sessions after a configurable time interval of inactivity at the CLI, defaulting to 30 minutes. Administrators configure the time interval using the system timeout modify -timeout command.
TOE Security Functional Requirements Satisfied: FTA_SSL.3.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target extends Part 2 and conforms to Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1, Release 4. The extended SFR contained within this ST is:

- FPT_SEP_EXT.1

There are no protection profile claims for this Security Target.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, OSP statement, and assumptions 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. There are no OSPs presumed for the TOE as mentioned previously in Section 3.2.

8.2.1 Security Objectives Rationale Relating to Threats

Table 29 - Threats: Objectives Mapping

Threats	Objectives	Rationale
T.MASQUERADE A TOE user or process may masquerade as another entity to gain unauthorized access to data or TOE resources.	**O.ADMIN_ROLES** The TOE will provide administrative roles to isolate administrative actions.	Access to the TOE or network resources controlled by the TOE will only be granted to user accounts associated with the root, admin, power, backup, compliance, or audit role. This prevents threat agents from gaining unauthorized access to the TOE or network resources.
	O.DAC_ACC TOE users will be granted access only to user data for which they have been authorized based on their user identity and group membership.	The TOE will prevent access to TSF data by users masquerading as other entities by implementing discretionary access control. Users shall be granted access only to data for which they have been authorized based on their user identity and group membership.
T.TAMPER A TOE user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	**O.ADMIN_ROLES** The TOE will provide administrative roles to isolate administrative actions.	The TOE will monitor attempts to access configuration data or other trusted data that could result in system failure resulting in unauthorized access to trusted data. Authorized roles are required for users to perform administrative procedures, thus isolating the amount of damage a user can perform.

Threats	Objectives	Rationale
	O.IA The TOE will require users to identify and authenticate themselves.	The TOE will monitor attempts to access configuration data or other trusted data that could result in system failure resulting in unauthorized access to trusted data. Users are required to identify and authenticate themselves to the TOE before attempting to modify TSF data or administrative functions.
	O.MANAGE The TSF will provide functions and facilities necessary to support the authorized administrators that are responsible for the management of TOE security.	The TOE will have defined methods and permissions for modification of configuration data.
	O.STRONG_PWD The TOE must ensure that all passwords will be at least 8 characters in length and will consist of at least one number and at least one alphabetic character. Special characters are optional. Password construction will be complex enough to avoid use of passwords that are easily guessed or otherwise left vulnerable, e.g. names, dictionary words, phone numbers, birthdays, etc. should not be used.	The TOE will have defined password rules that require strong passwords. The default password rules require passwords that are at least 8 characters in length and consist of at least one numeric and at least one alphabetic characters.
	OE.ACCESS The IT Environment will ensure that users gain only authorized access to the data the IT Environment manages.	The IT Environment will monitor attempts to access configuration data or other trusted data that could result in system failure resulting in unauthorized access to trusted data.
	OE.ADMIN_ROLES The IT Environment will provide administrative roles to isolate administrative actions.	The IT Environment will monitor attempts to access configuration data or other trusted data that could result in system failure resulting in unauthorized access to trusted data. Authorized roles are required for users to perform administrative procedures, thus isolating the amount of damage a user can perform.
T.UNAUTH A TOE user may gain access to security data on the TOE, even though the user is not	**O.ADMIN_ROLES** The IT Environment will provide administrative roles to isolate administrative actions.	The TOE will require authorized roles for users to perform administrative procedures therefore, isolating the amount of damage a user can perform.

Threats	Objectives	Rationale
authorized in accordance with the TOE SFP.	**O.ENFORCE** The TOE is designed and implemented in a manner the ensures that it can't be bypassed or interfered with via mechanisms within the TOE's control.	The TOE will ensure the SFP enforcement of the TOE is invoked and not interfered with inside the TOE.
	O.IA The TOE will require users to identify and authenticate themselves.	The TOE will require users to identify and authenticate themselves before attempting to modify TSF data or security attributes.
	O.MANAGE The TSF will provide functions and facilities necessary to support the authorized administrators that are responsible for the management of TOE security.	The TOE will have defined methods and permissions for modification of configuration data.
	O.INACTIVE The TOE will terminate an inactive management session after a configurable interval of time.	The TOE will prevent users from gaining access to security data on the TOE, even though the user is not authorized in accordance with the TOE SFP, by terminating an inactive management session after a configurable interval of time.
	OE.ACCESS The IT Environment will ensure that users gain only authorized access to the data the IT Environment manages.	The IT Environment will enforce restrictive access and modification rules for security attributes and TSF Data managed by the IT Environment and used by the TOE to enforce the DAC SFP.
	OE.ADMIN_ROLES The IT Environment will provide administrative roles to isolate administrative actions.	The IT Environment will require authorized roles for users to perform administrative procedures thus, isolating the amount of damage a user can perform.
	OE.ENFORCE The IT Environment will support the TOE by providing mechanisms to ensure the TOE is neither bypassed nor interfered with via mechanisms outside the TOE's control.	The IT Environment will ensure the SFP enforcement of the TOE is invoked and not interfered with outside the TOE.
T.DATALOSS Threat agents may attempt to remove or destroy data collected and produced by the TOE.	**O.IA** The TOE will require users to identify and authenticate themselves.	The TOE will mitigate unauthorized attempts to remove or destroy data collected and produced by the TOE by requiring that access to subject data is granted only after a user has been identified and authenticated.

Threats	Objectives	Rationale
T.NO_AUDIT Threat agents may perform security-relevant operations on the TOE without being held accountable for it.	**O.AUDIT** The TOE will audit all administrator authentication attempts, whether successful or unsuccessful, as well as TOE user account configuration changes.	The TOE will prevent a threat agent from performing a security- related action without being held accountable by auditing all security-related activity on the TOE and associating users with those activities.
	O.TIME STAMP The TOE will provide a reliable time stamp for use by the TOE.	The TOE will prevent a threat agent from performing a security- related action without being held accountable by auditing all security-related activity on the TOE and recording the time those activities were performed.
	OE.NTP The IT Environment will enable the TOE to provide reliable time stamps by implementing NTP.	The IT Environment will ensure that the TOE can perform reliable auditing by ensuring that the time stamp is reliable through the implementation of the Network Time Protocol.
T.IA Threat agents may attempt to compromise the TOE or network resources controlled by the TOE by attempting actions that it is not authorized to perform on the TOE or network resources.	**O.ADMIN_ROLES** The TOE will provide administrative roles to isolate administrative actions.	The TOE will prevent attempts to compromise the TOE or network resources controlled by the TOE by threat agents attempting actions that they are not authorized to perform by providing an administrator role and restricting access to the resources to users associated with that role.
	O.DAC_ACC TOE users will be granted access only to user data for which they have been authorized based on their user identity and group membership.	The TOE will prevent attempts to compromise the TOE or network resources controlled by the TOE by threat agents attempting actions that they are not authorized to perform by only granting users access to user data for which they have been authorized based on the identity of users and groups of users.
	O.IA The TOE will require users to identify and authenticate themselves.	The TOE will prevent attempts to compromise the TOE or network resources controlled by the TOE by threat agents attempting actions that they are not authorized to perform by requiring users to identify and authenticate themselves.
	OE.IA The IT Environment must require authorized CIFS and NFS Clients to successfully I&A before allowing access to the TOE.	The IT Environment will prevent attempts to compromise the TOE or network resources controlled by the TOE by threat agents attempting actions that they are not authorized to perform by requiring users to identify and authenticate themselves.

Every Threat is mapped to one or more Objectives in Table 30. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Assumptions

Table 30 - Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.PEER Any other systems with which the TOE communicates are assumed to be under the same management control and use a consistent representation for specific user and group identifiers.	**OE.SUBJECTDATA** The IT Environment will provide the TOE with the appropriate subject security attributes.	The security attributes provided by the IT Environment will be meaningful because the representations between the TOE and IT Environment systems are consistent.
A.NETWORK Security Management shall be provided to protect the Confidentiality and Integrity of transactions on the network.	**OE.NETWORK** The network path between the TOEs is a trusted channel. The network path between the CLI client and the TOE is a trusted channel.	The channel between the TOEs which are partners in an HA pair, and the channel between the TOE and the CLI client are trusted channels.
A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	**ON.INSTALL** Those responsible for the TOE and hardware required by the TOE must ensure that the TOE is delivered, installed, configured, managed, and operated in a manner which maintains IT security objectives.	One or more competent individuals will appropriately manage the TOE.
	ON.TRAINED Those responsible for the TOE will be properly trained and provided the necessary information that ensures secure management of the TOE and the IT Environment.	Those responsible for the TOE will be properly trained and provided the necessary information that ensures secure management of the TOE and the IT Environment.
A.NO_EVIL_ADM The system administrative personnel are not hostile and will follow and abide by the instructions provided by the administrator documentation.	**ON.INSTALL** Those responsible for the TOE and hardware required by the TOE must ensure that the TOE is delivered, installed, configured, managed, and operated in a manner which maintains IT security objectives.	The TOE will be delivered, installed, managed, and operated by a non- hostile administrator in a manner which maintains IT security objectives.
A.COOP Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.	**ON.CREDEN** Those responsible for the TOE must ensure that all access credentials, such as passwords, are protected by the users in a manner that maintains IT security objectives.	Authorized users will provide for the physical protection of the TOE's access credentials.

Assumptions	Objectives	Rationale
A.PROTECT The processing resources of the TOE critical to the SFP enforcement will be protected from unauthorized physical modification by potentially hostile outsiders.	**ON.PHYSICAL** Those responsible for the TOE and the network on which it resides must ensure that those parts of the TOE and the IT Environment critical to SFP are protected from any physical attack that might compromise the IT security objectives.	The security critical components of the TOE are protected from physical attacks by ensuring that the TOE is protected from unauthorized physical modification by hostile outsiders.
A.ADMIN_ACCESS Administrative functionality shall be restricted to authorized administrators.	**OE.ACCESS** The IT Environment will ensure that users gain only authorized access to the data the IT Environment manages.	Only authorized users will have access to administrative functionality.
	OE.ADMIN_ROLES The IT Environment will provide administrative roles to isolate administrative actions.	Authorized administrators will be restricted to administrative functionality based on their assigned role(s).
A.NTP The IT Environment will be configured to provide the TOE to retrieve reliable time stamps by implementing the Network Time Protocol (NTP).	**OE.NTP** The IT Environment will enable the TOE to provide reliable time stamps by implementing NTP.	The IT Environment will provide the TOE to synchronize a reliable time stamp through NTP.
A.PHYSICAL Physical security of the TOE and network, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.	**ON.PHYSICAL** Those responsible for the TOE and the network on which it resides must ensure that those parts of the TOE and the IT Environment critical to SFP are protected from any physical attack that might compromise the IT security objectives.	The TOE and the network on which it resides are protected from physical attacks commensurate with the value of the TOE and the data it protects such that physical attacks are mitigated.

8.3 Rationale for Extended Security Functional Requirements

The TOE contains the following explicitly stated security functional requirement:

- FPT_SEP_EXT.1

FPT_SEP_EXT.1 is an explicitly-stated functional requirement. The SFR family “TSF Domain Separation for Software TOEs” was created to specifically address the separation of virtual storage from each other when running within the TOE, as opposed to separation of the TOE’s domain of execution from outside entities. The SFR in this family has no dependencies since the stated requirement embodies all necessary security functions. This requirement exhibits functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

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 31 - Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN_ROLES The TOE will provide administrative roles to isolate administrative actions.	**FMT_SMR.1** Security roles	Defines the user roles implemented by the DAC SFP requiring authorized roles for NetApp Administrators to perform administrative procedures.
O.AUDIT The TOE will audit all administrator authentication attempts, whether successful or unsuccessful, as well as TOE user account configuration changes.	**FAU_GEN.**1 Audit data generation	Requires the TOE to generate audit event records for administrator logons and configuration changes, and defines the information saved in these records.
	FAU_GEN.2 User Identity Association	Requires the TOE to associate a specific user with the audit event records.
	FAU_SAR.1 Audit review	Requires the TOE to allow users to review audit event records.
	FAU_SAR.2 Restricted audit review	Requires the TOE to only allow administrators to review audit event records.
	FAU_STG.1 Protected audit trail storage	Requires the TOE to restrict the ability to modify or delete the audit trail to administrators, and to detect any such behavior by auditing all management operations.
	FAU_STG.4 Prevention of audit data loss	The TOE will continue to audit management activity if the audit trail is full by backing up the current audit trail, deleting the oldest audit trail file, and creating a new audit trail file.
O.DAC_ACC TOE users will be granted access only to user data for which they have been authorized based on their user identity and group membership.	**FDP_ACC.1** Subset access control	Identifies the subjects, objects, and operation of subjects on objects covered by the DAC SFP.
	FDP_ACF.1 Security attribute base access control	Identifies the subject and object security attributes used to enforce the DAC SFP, and defines the DAC rules enforced by the TOE that define access rules for TOE managed user data.
	FMT_MSA.3 Static attribute initialization	Ensures restrictive default values are defined for the TOE's object security attributes used to enforce the DAC SFP.

Objective	Requirements Addressing the Objective	Rationale
O.ENFORCE The TOE is designed and implemented in a manner the ensures the SFPs can't be bypassed or interfered with via mechanisms within the TOE's control.	**FPT_SEP_EXT.1** TSF domain separation software TOEs	The TOE tracks user sessions individually and enforces the SFPs appropriately for each session. User sessions cannot interfere with one another within the TOE. Without this assurance, there would not be assurance that the TOE could not be interfered with.
O.IA The TOE will require users to identify and authenticate themselves.	**FIA_AFL.1** Authentication failure handling	Protects the TOE from malicious brute-force and dictionary password attacks by locking out accounts after a configurable number of failed login attempts.
	FIA_UAU.2 User authentication before any action	Ensures that users must authenticate themselves before any TSF mediated access to the TOE functions or TSF data is allowed.
	FIA_UID.2 User identification before any action	Ensures that users must identify themselves before any TSF mediated access to the TOE functions or TSF data is allowed.
O.MANAGE The TSF will provide functions and facilities necessary to support the authorized administrators that are responsible for the management of TOE security.	**FIA_ATD.1** User attribute definition	Identifies the TOE maintained subject security attributes of TOE maintained objects.
	FMT_MOF.1 Management of security function behavior	Defines the restrictions enforced by the DAC SFP to modify roles associated with administrators managed by the TOE and used to enforce the DAC SFP.
	FMT_MSA.1 Management of security attributes	Only authorized NetApp Administrators responsible for the management of TOE security may modify, delete, or add the security attributes maintained locally by the TOE and used to enforce the DAC SFP.
	FMT_MTD.1 Management of TSF data	Defines the restrictions enforced by the DAC SFP to modify user accounts and roles managed by the TOE and used to enforce the DAC SFP.
	FMT_SMF.1 Specification of management functions	Defines the TSF management functions provided by the TOE that ensures the TOE's SFPs can be enforced.

Objective	Requirements Addressing the Objective	Rationale
O.STRONG_PWD The TOE must ensure that all passwords will be at least 8 characters in length and will consist of at least one number and at least one alphabetic character. Special characters are optional. Password construction will be complex enough to avoid use of passwords that are easily guessed or otherwise left vulnerable, e.g. names, dictionary words, phone numbers, birthdays, etc. should not be used.	**FIA_SOS.1** Verification of secrets	The TOE ensures that all passwords will be at least 8 characters in length and will consist of at least one number and at least one alphabetic character. Special characters are optional. This applies to passwords (secrets) assigned to administrative users for use in interactive management logins.
O.INACTIVE The TOE will terminate an inactive management session after a configurable interval of time.	**FTA_SSL.3** TSF-initiated termination	The TOE will terminate an administrator's session after a configurable interval of time.
O.TIME STAMP The TOE will provide a reliable time stamp for use by the TOE.	**FPT_STM.1** Reliable time stamps	The Operating System Kernel will provide a reliable time stamp for use by the TOE.

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. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended 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.3 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 32 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the Table 32 indicates, all dependencies have been met.

Table 32 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.2	✓	Although FAU_GEN.2 is dependent on FIA_UID.1 which is not claimed, the dependency SFR is substituted by FIA_UID.2 which is hierarchical to FIA_UID.1 and claimed because the TOE does not permit any TSF-mediated actions before users are identified.

SFR ID	Dependencies	Dependency Met	Rationale
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FIA_AFL.1	FIA_UAU.2	✓	Although FIA_AFL.1 is dependent on FIA_UAU.1 which is not claimed, the dependency SFR is substituted by FIA_UAU.2 which is hierarchical to FIA_UAU.1 and claimed because the TOE does not permit any TSF-mediated actions before users are authenticated.
FIA_ATD.1	No dependencies		
FIA_SOS.1	No dependencies		
FIA_UAU.2	FIA_UID.2	✓	Although FIA_UAU.2 is dependent on FIA_UID.1 which is not claimed, the dependency SFR is substituted by FIA_UID.2 which is hierarchical to FIA_UID.1 and claimed because the TOE does not permit any TSF-mediated actions before users are identified.
FIA_UID.2	No dependencies		
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies		
FMT_SMR.1	FIA_UID.2	✓	Although FMT_SMR.1 is dependent on FIA_UID.1 which is not claimed, the dependency SFR is substituted by FIA_UID.2 which is hierarchical to FIA_UID.1 and claimed because the TOE does not permit any TSF-mediated actions before users are identified.
FPT_SEP_EXT.1	No dependencies		
FPT_STM.1	No dependencies		
FTA_SSL.3	No dependencies		

Appendix A - Acronyms

Table 33 - Acronyms Defined

Acronym	Description
ACE	Access Control Entry
ACL	Access Control List
AK	Authentication key
API	Application Programming Interface
CC	Common Criteria
CIFS	Common Internet File System
CLI	Command Line Interface
CM	Configuration Management
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
EVT	Microsoft Windows Event Viewer format
FAS	Fabric Attached Storage
FC	Fiber Channel
GID	Group ID
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
ID	Identifier
IP	Internet Protocol
iSCSI	Internet Small Computer System Interface
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LIF	Logical Interface
LUN	Logical Unit Number
NFS	Network File System
NIS	Network Information Service
NTFS	New Technology File System
NTLM	New Technology Local Area Network Manager
NTP	Network Time Protocol
OS	Operating System
RAID	Redundant Array of Independent Disks
RSH	Remote Shell
SAN	Storage Area Network
SAR	Security Assurance Requirement
SD	Security Descriptor
SED	Self-Encrypting Drive
SFP	Security Function Policy
SFR	Security Functional Requirement

Acronym	Description
SID	Security Identifier
SMT	Secure Multi-Tenancy
SSH	Secure Shell
SVM	Storage Virtual Machine
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UID	User ID
UMASK	User Mask
VLDB	Volume Location Data Base
WAFL	Write Anywhere File Layout

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp