VAST FEDERAL

White Paper

VAST Data Platform Security Configuration Guide

Version 1.5

Executive Summary

The United States (U.S.) Federal Government is one of the largest purchasers of Information Technology (IT) products in the world with an estimated IT budget of over $250 billion for 2026. It is also one of the most rigorous enforcers of product security and compliance requirements since it is one of the most sought-after targets of highly valuable information. As the U.S. Government expands from utilizing strictly Government off the Shelf (GOTS) to a more cost-effective Commercial of the Shelf (COTS) environment, additional risks materialize with using commercial technology. To reduce taking on additional risk, the U.S. Government puts mandatory product security requirements prominently listed within its procurement regulations. These include the Federal Acquisition Regulations (FAR) and the Defense Federal Acquisition Regulations Supplement (DFARS). The requirements listed within each must be met in order for hardware and software products and services to be eligible for purchase by the U.S. Federal Government.

In order to be competitive in this customer market, VAST products and services must be compliant with all applicable federal and state procurement and operational requirements, regulations and laws. The steps detailed in this guide should be considered by customers intent on deploying a secure infrastructure. This Security Configuration Guide (SCG) details the security characteristics of the VAST Data Platform to demonstrate how it can effectively and securely operate within a customer's infrastructure.

Revision History

Name	Date	Changes	Version
Sabre Schnitzer	5/18/2025	Initial draft, content and structure	1.0
Sabre Schnitzer	5/20/2025	Network STIG Updates	1.1
Sabre Schnitzer	5/29/2025	Web and GPOS STIG Updates	1.2
Sabre Schnitzer	6/5/2025	VAST formatting update	1.3
Sabre Schnitzer	6/11/2025	STIG procedures update, FIPS additions	1.4
Sabre Schnitzer	7/7/2025	Significant STIG content expansion	1.5

Table of Contents

List of Figures

List of Tables

1.0 Document Objectives

This VAST Data Platform Security Configuration Guide (SCG) is the document that details the security characteristics of the product and how they can be utilized to secure the product's operation within a customer environment. VAST Data Federal is providing this white paper to our customers as a resource and a demonstration of the security features that VAST has engineered into the Data Platform product. This white paper and its associated white papers should be used when implementing the Data Platform in a secure manner to participate in a customer's infrastructure without raising the risk level.

1.1 Purpose

The purpose of this white paper is to detail the security characteristics of the VAST Data Platform product for customer education.

1.2 Scope

This SCG covers just the product discussed in this white paper. It does not address the other network and environment hardening steps that must be undertaken to ensure that the entire infrastructure is secure. To be utilized effectively, this SCG should be utilized on a VAST system that is incorporated into a hardened environment.

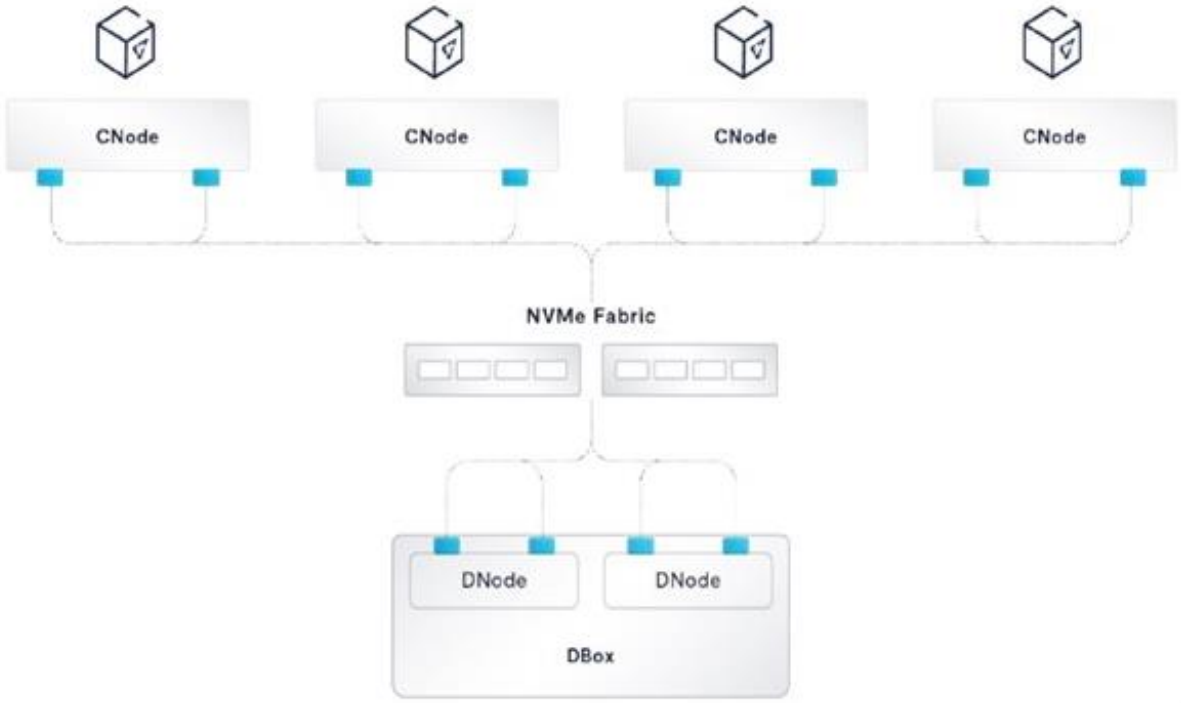

Figure 1. The VAST Federal Data Platform Product Design

1.3 Related Documents

The following documents should be utilized in conjunction with this SCP

- The VAST Data Platform NIST SP800-53 System Security Plan
- The VAST Data Platform Military Unique Deployment Guide
- The VAST Data Platform Product Hardening Procedures
- The VAST Data Platform Spillage Remediation Plan

1.4 Point of Contact and Feedback

Users of this document / procedure can submit comments, feedback, and request changes to the author of this paper:

Sabre Schnitzer
VAST Data Federal Compliance Officer
sabre@vastfederal.com

2.0 VAST Operating System Overview

The VAST Data Platform product is built as a STIG-hardened appliance. However, rather than hide behind an appliance claim, VAST provides customers with access to all areas of the product to demonstrate the product's security hardening posture and to enable a complete vulnerability scanning platform. Too many technology companies hide their inner working from vulnerability scans to hide insecure components. VAST determined very early on that we would provide customer access to all components in order to demonstrate unquestionable insight into our security posture.

Each component of the VAST architecture has been thoroughly examined and secured to comply with all applicable US Government information security and product security regulations, specifications and procurement requirements. The VAST Data Platform is listed on the Department of Defense Information Network (DoDIN) Approved Products List (APL) after passing its significant information security and interoperability audits.

The chapters below demonstrate VAST's commitment to secure operations.

3.0 Security Characteristics

The table below provides the security characteristics of the product that will be discussed in this white paper.

Table 1 – Security Categories

Security Category	Description
Access Control	Limiting access by end-user or by other entities to protect hardware, software, or specific product features.
Auditing	Managing the logging of events.
Communication Security	Securing product network communications.
Data security	Providing protection for product data.
Serviceability	Maintaining control of product service operations performed by the manufacturer or its service partners.
Alerting	Managing the alerts and notifications generated for security-related events.
Other Security Settings	Security settings that do not fall in one of the previous sections, such as physical security.

4.0 Access Control

The VAST Data Platform expands on the limitations of Role-Based Access Control (RBAC) and implements an Attribute-Based Access Control (ABAC) model to definitively control access to the product and its services. ABAC is a logical access control model that determines authorization to perform operations by evaluating attributes associated with the subject (requester), the object (resource to be accessed), requested operations, and, in some cases, environmental conditions. This evaluation is conducted against policies, rules, or relationships that describe the allowable operations for a given set of attributes.

The flexibility of ABAC allows for the creation of highly granular and precise access control policies that can respond in real time to the context of access requests. This level of detail and adaptability makes ABAC particularly well-suited for protecting against unauthorized data access and mitigating the risk of data exploits. As organizations continue to grapple with the challenges of securing their data, ABAC stands out as a next-generation approach that can provide the robust and flexible access control needed in today's complex security landscape.

The VAST Data Platform also implements a Zero Trust Architecture (ZTA) for its normal operation so that no action is inherently trusted. At no time will the product authorize an action to be taken without first evaluating whether the use or service is allowed to take that action. Additionally, all actions taken on the system, whether successful or unsuccessful, are recorded in an immutable audit log.

The paragraphs below detail the access control capabilities of the product.

4.1 Access Methods

The VAST Data Platform supports the following access methods:

Table 2 – Access Methods

Type	Description
Management Accounts	These accounts have privileges for performing management and monitoring tasks associated with the storage system and its storage resources. Passwords are created and managed through the storage system management interfaces and can be used to access either of the following management interfaces: • **VAST Management Console** (VMS): A Web-based graphical interface accessed via HTTPS that provides tools for configuring, managing, and monitoring storage system storage and system settings. • **VAST Command Line Interface (CLI):** The VAST CLI provides a command line interface for the same functionality available through VMS.
Service Accounts	This account performs specialized service and management functions on the appliance operating system. This account is designated as a backup emergency account and is not to be used for day-to-day operations. This account has full administrative control over the product.

4.2 Default Roles

Each account on the product must be assigned roles in order to be granted authorization to perform actions on the product. The following predefined roles are the default roles available to assign to users within the VAST Management System (VMS).

Table 3 – Default Roles

Type	Description
Administrators	This role grants comprehensive access to all realms and functions, allowing users to perform any action within the system. It's typically reserved for senior IT staff responsible for overall system management.
Read Only	This role provides view-only access across all realms, allowing users to monitor the system without making changes. It's ideal for junior administrators, auditors, or monitoring staff.
Configuration	This specialized role focuses on system configuration tasks, with appropriate permissions to set up and modify system parameters.
CSI	This role is designed specifically for Container Storage Interface operations, granting the necessary permissions for Kubernetes integration.
Debug Metrics	This technical role provides access to detailed system metrics for debugging purposes.

4.3 Roles and Realms

Once an account is assigned to its role/s, it needs to be added to a set of realms. This assignment will limit the account to only those areas of the product that requires its access.

Table 4 – Role Structure and Realms

Type	Description
Events Realm	This realm governs all event management functions, including: • Creating, viewing, and managing system alerts Setting up event triggers and responses
Hardware Realm	This realm controls access to physical component management: • Monitoring CNodes (compute nodes) status and performance • Managing DNodes (data nodes) configurations • Implementing hardware upgrades or replacements
Logical Realm	This critical realm manages the logical storage structure: • Creating and managing views • Setting quotas to control storage usage • Configuring network access settings such as virtual IPs and protocols
Monitoring Realm	This realm focuses on system health and performance: • Accessing real-time performance metrics

	• Viewing historical performance data • Setting up monitoring dashboards
Security Realm	This realm controls access to security functions: • Managing user authentication methods including external identity providers • Setting up encryption policies • Managing the RBAC system itself
Settings Realm	This realm handles general system configurations: • Setting system-wide parameters • Managing licensing information
Support Realm	This realm provides access to support functions: • Generating support bundles for troubleshooting • Accessing system logs and diagnostic information • Managing firmware and software updates • Configuring remote support access

4.4 Permission Types

The following permission types can be used to further lock down an account.

Table 5 – Permission Types

Type	Description
Create	This permission allows users to add new resources or configurations within a realm. For example, in the Logical realm, Create permission would allow adding new views or quotas.
View	This basic permission lets users see resources without modifying them. It's the foundation of read-only access and is often granted broadly for monitoring purposes.
Edit	This permission enables users to modify existing resources but not create new ones. For instance, Edit permission in the Hardware realm would allow reconfiguring existing nodes but not adding new ones.
Delete	This powerful permission allows users to remove resources from the system. It's typically restricted to prevent accidental data loss.

It is important to note how permissions can be combined to create precise access profiles:

- Some roles might have View-only access to sensitive realms like Security while having full permission in other areas.

- Other roles might have Create and Edit permissions but not Delete, limiting potential damage from accidental actions Observe how clicking on column or row headers can toggle all permissions in that column or row, simplifying role configuration.

4.5 Types of Users

The following table details the types of users that the product supports. Local users are the only default users on the product. All other types of users require that the product be joined to an external identity management solution.

Table 6 – Types of Users

Type	Description
Active Directory	Microsoft's enterprise directory services.
LDAP	Lightweight Directory Access Protocol services
NIS	Network Information Service
Local Users	Local users defined directly within the VAST product

4.6 Default Users

There is only one default user on the product when it is shipped from the factory. This user, the vastdata account, is the root administrator of the product. This account and password are handed to the customer at the time of installation. VAST recommended it be used for initial installation and configuration. Afterwards, the account should be restricted for use with a complex password and used only during emergency situations.

Table 7 – Default Users

Type	Description
vastdata	Local root administration account.

4.7 Single Sign On

The VAST Data Platform is designed to integrate seamlessly into an existing customer-managed identity management solution. Integrating the VAST Data Platform into an existing Identity Provider (IdP) ensures that the VAST product doesn't implement an additional stovepipe and the existing users can utilize the VAST product as a new service without having to be issued an additional account.

The following steps can be utilized to configure Single Sign On (SSO) and Multi-Factor Authentication (MFA).

Prerequisite: Trusted TLS communications need to be configured prior to configuring SSO and MFA

Procedure:

1. From a networked workstation, enter the IP address of the VAST Data Platform into a browser. The VAST Data Platform GUI will appear.
2. Authenticate to the VAST Data Platform with an authorized account. Upon successful authentication and authorization, the user will be granted into the system.
3. From the left navigation menu, navigate to the **Administrators** page, then select the **SAML** tab.
4. Click **Add** new identity.
5. In the **General** section, add these details for the Identity Provider:
    a. **IdP name.** The name of the Identify Provider (e.g. Okta)
    b. **IdP Entity ID.** The Entity ID for the Identity Provider, typically obtained from the metadata.
    c. **Force Authenticate.** Forces authentication with the IdP for each sign-on.
6. In the **Metadata** section, enter these details:
    a. **Metadata URL.** The URL to the metadata on the IdP, usually in the form of https://<idp-url/sso/saml/metadata where idp-url is the URL of the IdP.
    b. **Local Metadata.** Use metadata stored locally on VMS. This is an alternative to including a Metadata URL.
    c. Paste metadata text in the box.
7. In the Assertions and Certificates section you can optionally enable and configure encryption for SAML assertions and responses. If enabled, you must also provide or upload certificates.
8. To enable encryption of SAML assertions, toggle **Enable Assertion Encryption**.

    If enabled, follow these steps to configure a certificate and key.
    a. Click **Add Certificate**.
    b. Paste an X.509 certificate in the box or click **Upload**, and upload an X.509 certificate file.
    c. Click **Save** to save the certificate.
    d. Click **Add Key**.
    e. Paste an X.509 key in box or click **Upload**, and upload an X.509 key file.
    f. Click Save.
9. To enable signatures on SAML assertion responses, toggle Enable assertion response signing. If enabled, follow these steps to configure a certificate and key. This is enabled independently of the Enable assertion encryption option. The certificate and key used for this option can be different from the ones used for Assertion Encryption.

a. Click Add certificate.
b. Paste an X.509 certificate in the box or click **Upload** and upload an X.509 certificate file.
c. Click **Save** to save the certificate.
d. Click **Add Key**.
e. Paste an X.509 key in box or click **Upload** and upload an X.509 key file.
f. Click **Save**.

10. Click **Save**

Result: The VAST Data Platform will accept multifactor authentication for users.

4.8 Access Control Management

The VAST Data Platform complies with the access control management requirements of the applicable STIGs through the following features and characteristics:

- **SRG-APP-000317-NDM-000282**. The VAST Data Platform provides a mechanism to voluntarily log out of a network connection. Following logout, an explicit logout message is displayed for the user. The logout mechanism can be used at any time. Upon logging out of the system, the unique session ID is deleted so that reuse is impossible. This functionality is default and cannot be disabled by any user.

- **SRG-APP-000317-NDM-000282**. The VAST Data Platform terminates shared/group account credentials when members leave the group. Customer managed accounts located in a customer managed IDP will be managed by the VAST Data Platform in accordance with the customer's access management policies so that when a member is removed from a group, the product will forbid the former member of the group to authenticate to the product.

- **SRG-APP-000328-NDM-000286**. The VAST Data Platform uses discretionary access control to enforce organization-defined discretionary access control policies over defined subjects and objects. In conjunction with the product's ABAC services, the VAST Data platform offers comprehensive access control services. When joined to a customer managed IDP, the product will enforce the DAC policies as required by the customer's access control policies.

- **SRG-APP-000329-NDM-000287**. The VAST Data Platform uses role-based access control top enforce organization-defined role-based access control policies over defined subjects and objects. In conjunction with the product's ABAC services, the VAST Data platform offers comprehensive access control services. When joined to a customer managed IDP, the product will enforce the DAC policies as required by the customer's access control policies.

- **SRG-APP-000340-NDM-000288**. The VAST Data Platform prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. The product's ABAC services ensure that no non-privilege user is allowed to perform privileged actions. When joined to a customer managed IDP, the product will enforce the DAC policies as required by the customer's access control policies.

- **SRG-APP-000378-NDM-000302**. The VAST Data Platform prohibits installation of software without explicit privileged status. The product's ABAC services ensure that no non-privilege user is allowed to perform privileged actions. Any action that is taken by a non-administrative user will be disallowed by the product's ABAC service. The disallowed action will be recorded in the product's audit logs for after-the-fact analysis.

- **SRG-APP-000380-NDM-000304**. The VAST Data Platform enforces access restrictions associated with changes to device configuration. The product's ABAC services ensure that no non-privilege user is allowed to perform privileged actions. Any action that is taken by a non-administrative user will be disallowed by the product's ABAC service. The disallowed action will be recorded in the product's audit logs for after-the-fact analysis.

- **SRG-APP-000038-NDM-000213**. The VAST Data Platform enforces approved authorizations for controlling the flow of management information within the VAST Data Platform based on information flow control policies. In conjunction with the product's ABAC services, the VAST Data platform offers comprehensive access control services. The product's ABAC services ensure that no non-privilege user is allowed to perform privileged actions.

- **SRG-APP-000408-NDM-000314**. When performing maintenance functions, the VAST Data Platforms restrict use of these functions to authorized personnel only. The product's ABAC services ensure that no non-privilege user is allowed to perform privileged actions. Any action that is taken by a non-administrative user will be disallowed by the product's ABAC service. The disallowed action will be recorded in the product's audit logs for after-the-fact analysis.

- **SRG-APP-000516-NDM-000335**. The VAST Data Platform enforces access restrictions associated with changes to the system components. The product's ABAC services ensure that no non-privilege user is allowed to perform privileged actions. Any action that is taken by a non-administrative user will be disallowed by the product's ABAC service. The disallowed action will be recorded in the product's audit logs for after-the-fact analysis.

- **SRG-APP-000033-WSR-000169**. The product enforces approved authorizations for logical access to hosted applications and resources in accordance with applicable access control policies. Through the use of the product's ABAC system, every action attempted by a user or service is checked for proper permissions before being allowed. Any action that is taken by a non-administrative user will be disallowed by the product's ABAC service. The disallowed action will be recorded in the product's audit logs for after-the-fact analysis.

- **SRG-APP-000118-WSR-000068**. VAST Data Platform log files are accessible only by privileged users. Non-privileged users are not permitted to access the audit logs. The product's ABAC services ensure that no non-privilege user is allowed to perform privileged actions. Any action that is taken by a non-administrative user will be disallowed by the product's ABAC service. The disallowed action will be recorded in the product's audit logs for after-the-fact analysis.

- **SRG-APP-000119-WSR-000069**. The log information from the VAST Data Platform is protected from unauthorized modification. Non-privileged users are not permitted to access the audit logs. The product's ABAC services ensure that no non-privilege user is allowed to perform privileged actions. Any action that is taken by a non-administrative user will be disallowed by the product's ABAC service. The disallowed action will be recorded in the product's audit logs for after-the-fact analysis.

- **SRG-APP-000120-WSR-000070**. The log information from the VAST Data Platform is protected from unauthorized deletion. The log information from the VAST Data Platform is protected from unauthorized deletion. Non-privileged users are not permitted to access the audit logs. The product's ABAC services ensure that no non-privilege user is allowed to perform privileged actions. Any action that is taken by a non-administrative user will be disallowed by the product's ABAC service. The disallowed action will be recorded in the product's audit logs for after-the-fact analysis.

- **SRG-APP-000131-WSR-000051**. All VAST Data Platform files are verified for their integrity (e.g., checksums and hashes) before becoming part of the production VAST Data Platform instance. Software not signed by VAST is not permitted to be installed on the product.

- **SRG-APP-000131-WSR-000073**. Expansion modules, referred to as patches, have been fully reviewed, tested, and signed before they can exist on a production VAST Data Platform. Software not signed by VAST is not permitted to be installed on the product. This is a default feature of the product and cannot be disabled.

- **SRG-APP-000141-WSR-000078**. VAST Data Platform accounts not utilized by installed features (i.e., tools, utilities, specific services, etc.) are not created and have been deleted on the VAST Data Platform. The vastdata account is the only default account that exists on the product. The vastdata account is the account that is utilized during all code upgrades. This account will remain on the product following the code upgrade because the vastdata account is the backup emergency account for the product.

- **SRG-APP-000141-WSR-000081**. The VAST Data Platform has Multipurpose Internet Mail Extensions (MIME) that invoke OS shell programs disabled. MIME is not utilized on the product and does not exist in any library.

- **SRG-APP-000141-WSR-000083**. The VAST Data Platform has resource mappings set to disable the serving of certain file types. The only file types that are serviced are those that are required for the product to operate. Nonutilized files and protocols have been removed from the system in order to comply with U.S. Government regulations. An IMAP scan for the running protocols will demonstrate compliance with this requirement.

- **SRG-APP-000141-WSR-000086**. The VAST Data Platform protects system resources and privileged operations from unauthorized individuals. The VAST Data Platform does not host applications. The VAST ABAC system will prevent unauthorized individuals from performing any administrative function. Additionally, any action attempted by any product user will be audited and recorded in the product's audits log.

- **SRG-APP-000141-WSR-000087**. Users and scripts running on behalf of users are contained to the document root or home directory tree of the VAST Data Platform.

- **SRG-APP-000176-WSR-000096**. Only authenticated system administrators or the designated PKI Sponsor for the VAST Data Platform have access to the VAST Data Platforms private key. Only product administrators connecting via SSH have access to a user's private key.

- **SRG-APP-000211-WSR-000031**. Anonymous user access to the VAST Data Platform application directories is prohibited. All accounts are required to have password or MFA requirement to exist. The VAST ABAC system will prevent unauthorized individuals from performing any function on the product. Additionally, any action attempted by any product user will be audited and recorded in the product's audits log.

- **SRG-APP-000233-WSR-000146**. The VAST Data Platform does not utilize a document directory as documents are not offered on the product. The product is a purpose-built product for administering the Data Platform capabilities.

- **SRG-APP-000251-WSR-000157**. The VAST Data Platform limits the character set used for data entry. Password character limits are set to 128 characters.

- **SRG-APP-000316-WSR-000170**. The VAST Data Platform provides the capability to immediately disconnect or disable remote access to the hosted applications. The product does not host applications.

- **SRG-APP-000340-WSR-000029**. Non-privileged accounts on the hosting system only access VAST Data Platform security-relevant information and functions through a distinct administrative account. Non-privileged accounts do not have access to any privileged functions.

- **SRG-APP-000380-WSR-000072**. The VAST Data Platform application, libraries, and configuration files are only accessible to privileged users. Non-privileged users do not have access to the product. The product's ABAC services ensure that no non-privilege user is allowed to perform privileged actions. Any action that is taken by a non-administrative user will be disallowed by the product's ABAC service. The disallowed action will be recorded in the product's audit logs for after-the-fact analysis.

- **SRG-APP-000429-WSR-000113**. The VAST Data Platform encrypts user identifiers and passwords. All data at rest and data in flight are encryption with a FIPS-140-3 validated cryptography. For VASTOS version 5.2 and earlier utilize the FIPS 140-3 certificate number 4675 for all at-rest and in-flight encryption.

- **SRG-APP-000435-WSR-000147**. The VAST Data Platform is protected from being stopped by a non-privileged user. Non-privileged users have no rights on the product. The VAST Data Platform's ABAC access control system enforces proper authentications for each and every user and software service of the system. Each user, when properly authenticated to the system, is assigned only those authorized usage conditions and abilities appropriate to each user. For a standard, non-administrative user, security functionality will not be allowed or provisioned to that user. This includes stopping the product.

- **SRG-APP-000516-WSR-000079**. All accounts installed with the VAST Data Platform software and tools have passwords assigned and default passwords changed. There are no null passwords on the system. The password complexity policy for non-local accounts are managed by the customer's IDP and enforced by the VAST product. Local accounts have a password policy enforced by the VAST product. The password complexity requirements are

- **SRG-OS-000585**. The VAST Data Platform disables accounts when the accounts have expired. When a password expires, the associated account is disabled. The VAST Data Platform implements a least privilege and a least functionality architecture where accounts are only granted rights that are in line with the security policy currently in place. These rights are taken away immediately upon expiration of the account or password occurs. This is a default feature of the product.

- **SRG-OS-000590**. The VAST Data Platform disables accounts when the accounts are no longer associated with a user. The VAST Data Platform implements a least privilege and a least functionality architecture where accounts are only granted rights that are in line with the security policy currently in place. This is a default feature of the product.

- **SRG-OS-000109**. The VAST Data Platform requires users to be individually authenticated before granting access to the shared accounts or resources. All accounts on the product are individual accounts. Shared accounts are only available when LDAP support is enabled and supported through a customer managed environment.

- **SRG-OS-000002**. The VAST Data Platform automatically removes or disables temporary user accounts after 72 hours. Temporary accounts managed by the customer's IDP will be governed by the customer's account management policies. Temporary accounts managed by the VAST product will be governed by the local user management policy enforced by the product and set by the customer. This is a default feature of the product.

- **SRG-OS-000028**. The VAST Data Platform retains the session lock until the user reestablishes access using established identification and authentication procedures. This is a default feature of the product. Additionally, once the session is closed the session ID is deleted so that it cannot be utilized again. For each new session, a new and unique session ID will be used to establish the TLS link to the user.

- **SRG-OS-000031**. The VAST Data Platform conceals, via the session lock, information previously visible on the display with a publicly viewable image. This is a default feature of the product. At no time does the product display and discernable information to a user prior to the authentication attempt. This is a default feature of the product and cannot be disabled or changed in any manner.

- **SRG-OS-000073**. The VAST Data Platform, for password-based authentication, stores passwords using an approved salted key derivation function, preferably using a keyed hash. All hashes utilized on the product are created with a FIPS-140-3 validated cryptographic library.

- **SRG-OS-000121**. The VAST Data Platform uniquely identifies and authenticates nonorganizational users (or processes acting on behalf of nonorganizational users). The VAST Data Platform's ABAC access control system enforces proper authentications for each and every user and software service of the system. Each user, when properly authenticated to the system, is assigned only those authorized usage conditions and abilities appropriate to each user. For a standard, non-administrative user, security functionality will not be allowed or provisioned to that user.

- **SRG-OS-000132**. The VAST Data Platform separates user functionality (including user interface services) from VAST Data Platform management functionality. The VAST Data Platform's ABAC access control system enforces proper authentications for each and every user and software service of the system. Each user, when properly authenticated to the system, is assigned only those authorized usage conditions and abilities appropriate to each user. For a standard, non-administrative user, security functionality will not be allowed or provisioned to that user.

- **SRG-OS-000134**. The VAST Data Platform isolates security functions from nonsecurity functions. The VAST Data Platform's ABAC access control system enforces proper authentications for each and every user and software service of the system. Each user, when properly authenticated to the system, is assigned only those authorized usage conditions and abilities appropriate to each user. For a standard, non-administrative user, security functionality will not be allowed or provisioned to that user.

- **SRG-OS-000302**. The VAST Data Platform enforces organization defined circumstances and/or usage conditions for organization-defined accounts. The VAST Data Platform's ABAC access control system enforces proper authentications for each and every user and software service of the system. Each user, when properly authenticated to the system, is assigned only those authorized usage conditions and abilities appropriate to each user.

- **SRG-OS-000312**. The VAST Data Platform enforces organization-defined discretionary access control (DAC) policies over defined subjects and objects. The VAST Data Platform's ABAC access control system enforces proper authentications for each and every user and software service of the system. Each user, when properly authenticated to the system, is assigned only those authorized rights and abilities appropriate to each user. Users are not allowed to disable, circumvent or alter implemented security safeguards/countermeasures unless granted and authorized administrator permissions.

- **SRG-OS-000326**. The VAST Data Platform prevents nonprivileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. The VAST Data Platform's ABAC access control system enforces proper authentications for each and every user and software service of the

system. Each user, when properly authenticated to the system, is assigned only those authorized rights and abilities appropriate to each user. Users are not allowed to disable, circumvent or alter implemented security safeguards/countermeasures unless granted and authorized administrator permissions.

- **SRG-OS-000326**. The VAST Data Platform prevents organization-defined software from executing at higher privilege levels than users executing the software. The VAST Data Platform's ABAC access control system enforces proper authentications for each and every user and software service of the system. Each user, when properly authenticated to the system, is assigned only those authorized rights and abilities appropriate to each user. Additionally, any software executed by the user will be granted only the permissions assigned to that user. Software packages cannot execute at privileges higher than the user is authorized.

- **SRG-OS-000329**. The VAST Data Platform automatically locks the account until the locked account is released by an administrator when three unsuccessful login attempts in 15 minutes are exceeded. The VAST Data Platform can lock both local and customer managed accounts when three unsuccessful login attempts are recorded within a 15-minute window.

- **SRG-OS-000362**. The VAST Data Platform prohibits user installation of software without explicit privileged status. The VAST Data Platform prevents the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. All official VAST software is digitally signed by VAST before posting on public support sites for customer downloads. Any software that is not digitally signed by VAST will be rejected by the system and will prevent installation. Additionally, only authenticated and authorized VAST Data Platform administrators will be granted the ability to install software onto the product. Only when the software is properly signed by VAST and utilized by an authenticated administrator of the product will the system allow software to be installed on the product.

- **SRG-OS-000363**. The VAST Data Platform implements automated organization-defined security responses if baseline configurations are changed in an unauthorized manner. The VAST Data Platform utilizes a comprehensive audit mechanism. Each and every action attempted by every user of the system is audited in a manner that allows for forensic analysis after the fact. Additionally, the product's audit logs can be offloaded from the product with the use of syslog. Exporting the logs allows the product to participate in a customer managed audit examination service. Lastly, the product also supports real-time notifications to identified individuals when specific events occur.

- **SRG-OS-000364**. The VAST Data Platform enforces access restrictions through the use of a comprehensive ABAC service. The VAST Data Platform's ABAC access control system enforces proper authentications for each and every user of the system. Each user, when properly authenticated to the system, is assigned only those authorized rights and abilities appropriate to each user.

- **SRG-OS-000365**. The VAST Data Platform audits the enforcement actions used to restrict access associated with changes to the system. The VAST Data Platform utilizes a comprehensive audit mechanism. Each and every action attempted by every user of the system is audited in a manner that allows for forensic analysis after the fact. Additionally, the product's audit logs can be offloaded from the product with the use of syslog. Exporting the logs allows the product to participate in a customer managed audit examination service. Lastly, the product also supports real time notifications to identify individuals when specific events occur.

- **SRG-OS-000366**. The VAST Data Platform prevents the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. All official VAST software is digitally signed by VAST before posting on public support sites for customer downloads. Any software that is not digitally signed by VAST will be rejected by the system and will prevent installation.

- **SRG-OS-000368**. The VAST Data Platform prevents program execution in accordance with organization-defined policies regarding software program usage and restrictions and/or rules authorizing the terms and conditions of software program usage. The VAST Data Platform utilizes a comprehensive ABAC access control system to enforce only proper authentications to each and every user of the system. Each user, when properly authenticated to the system, is assigned only those authorized rights and abilities appropriate to each user.

- **SRG-OS-000370**. The VAST Data Platform employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs. The Data Platform firewall policy is one of the steps that are required in the VAST Data Platform Hardening Procedures. VAST recommends that the STIG hardening procedures be applied to the product before placing the product into a production environment.

- **SRG-OS-000383**. The VAST Data Platform prohibits the use of cached authenticators after an organization-defined time period. When connected to a customer's IDP, the product will enforce the cached authenticator requirements established by the IDP. If the customer's IDP is Active Directory with X.509-based Certificate Authorities (CA) and a CA is offline, the VAST Data Platform will utilize the IDP as the authoritative source of the user's authentication.

- **SRG-OS-000391**. VAST Data Platforms that perform maintenance functions restrict use of these functions to authorized personnel only. Only authenticated administrators of the product will be granted administrative functions on the product. The product's ABAC control system governs all actions on the platform

- **SRG-OS-000725**. The VAST Data Platform for password-based authentication allows user selection of long passwords and passphrases, including spaces and all printable characters. Users of the product are not restricted in any manner when selecting a new password. Uppercase, lowercase, numbers and special characters are all allowed for password use.

- **SRG-OS-000720**. The VAST Data Platform, for password-based authentication, requires immediate selection of a new password upon account recovery. A user with an account that has been recovered must select a new password prior to being given access to the system.

5.0 Auditing

The VAST Federal Data Platform provides a comprehensive audit service for data security and user accountability. Audit functionality provides an immutable, persistent record of the actions performed by any user and any service on the product. This record can be used to forensically analyze user or service behavior and to reconstruct a chain of events that led to a specific outcome or action. VAST products log all events in an internal database that is tightly restricted to only authorized personnel.

5.1 Auditing Details

The VAST product default audit configuration ensures that each audit log contains the information needed to determine:

- Who initiated the event:
- What type of event occurred;
- When the event occurred;
- Where the event occurred;
- The source of the event;
- The outcome of the event;
- and Identifiers associated with the event.

Each audit log contains the following fields:

- Date and time of event;
- Message (what type of event);
- Source of event;
- Source IP and/or hostname;
- Destination IP and/or hostname;
- Source port;
- Destination port;
- User ID or account (if applicable);
- Outcome or actions (success, failure, deny, drop, alert, alert/deny, alert/drop, etc.);
- Protocol type (such as TCP, ICMP);
- Path (if applicable);
- Account privilege type (if applicable);
- Account authentication type (if applicable).

Activity log messages describe the current state of tasks on the local VAST product and furnish information about every task that is started on the local VAST product over the past 90 days, including tasks that result in a notification. User events are logged in the VAST activity log, along with all other product activities. To reconstruct a set of user activities, filter the activity log to display user events.

The VAST product supports transmission of system activities to an external syslog server. VAST uses the standard syslog protocol for formatting and transmission of system notifications. The transport layer protocol and port can also be configured to use custom settings. When syslog support is enabled, the VAST product sends to the syslog server messages that are based on the events that also appear in the Audit Log.

The VAST Federal Data Platform's auditing capabilities are designed to provide a comprehensive and compliant framework that aligns with the NIST SP 800-53 Revision 5 Audit and Accountability (AU) controls. The platform employs a trio of auditing frameworks—Auditd, Admin, and Protocol Auditing to capture and log a wide range of audit events, ensuring that all system, protocol, and administrative activities are meticulously recorded.

The Auditd framework is responsible for monitoring and capturing system-level events, providing a detailed log of actions taken within the platform's operating environment. This includes tracking user logins, file accesses, and system changes, which are crucial for maintaining a secure and traceable record of operations.

The Admin Audit framework focuses on administrative activities, offering insights into the actions performed by system administrators. This includes changes to user permissions, system configurations, and policy updates. By auditing these activities, the platform ensures that any administrative action is accountable and can be reviewed for compliance and security purposes.

The Protocol Audit framework captures events related to the various communication protocols used within the platform. This includes data transfers, access requests, and protocol-specific interactions that occur during the operation of the platform. By auditing these events, the VAST Federal Data Platform can ensure the integrity and security of data in transit and provide a clear trail of protocol-based activities.

5.2 Auditing Configuration

Follow these steps to configure Auditing on the Data Platform.

Procedure:

1. From a networked workstation, enter the IP address of the VAST Data Platform into a browser. The VAST Data Platform GUI will appear.
2. Authenticate to the VAST Data Platform with an authorized account. Upon successful authentication and authorization, the user will be granted into the system.
3. Navigate to **Settings** → **Auditing**.
4. Add your user account to the RO view of the audit log – without this you will not be able to access audit logs.
5. Select the Enable Auditing slider.
6. You can optionally enable auditing globally for one or more protocols.
7. Click Save.

Result: The VAST Data Platform will enable comprehensive auditing.

Procedure: To enable client users to access audit files:

1. Give users read access permission to the audit directory. This is done by specifying users and groups in the **Read-access Users** and **Read-access Groups** fields in the global auditing settings configuration.
2. Ensure that there is a view on the audit directory or on the root directory. Users need to mount the view on their client operating system in order to access the files.

Audit File Location and Name

- The audit directory is located directly under the root directory of the Element Store. Audit records are written to files in different subdirectories for different CNodes. There are multiple active audit files for each CNode, identified by silo ID, which represent internal handlers. Each file may contain multiple audit records.
- Each subdirectory is named audit_env_#, where # is a data environment ID.

- The maximum size of an audit file is set by the **Max audit file size** field in the global auditing settings. Audit records roll over to a new file when the file reaches this size.
- Files are named audit_log_<silo ID>_<time and date stamp in UTC>. For example: audit_log_13_2022-07-25_10.06.22.971753164.

5.3 Auditing Control Management

The VAST Data Platform complies with the auditing management requirements of the applicable STIGs through the following features and characteristics:

- **SRG-OS-000055**. The VAST Data Platform uses internal system clocks to generate time stamps for audit records. The VAST product supports the use of two NTP services provided by the customer. This support ensures that all audit logs generated by the product are timestamped correctly.

- **SRG-OS-000057**. The VAST Data Platform protects audit information from unauthorized read access. The VAST Data Platform utilizes a comprehensive ABAC access control system to enforce only proper authentications to each and every user of the system. Each user, when properly authenticated to the system, is assigned only those authorized rights and abilities appropriate to each user. Therefore, even a verified user cannot read audit logs unless they are assigned a security role permission.

- **SRG-OS-000058**. The VAST Data Platform protects audit information from unauthorized modification. The VAST Data Platform utilizes a comprehensive ABAC access control system to enforce only proper authentications to each and every user of the system. Each user, when properly authenticated to the system, is assigned only those authorized rights and abilities appropriate to each user. The VAST Data Platform's audit logs are immutable. Therefore, even a verified administrator cannot modify audit logs.

- **SRG-OS-000059**. The VAST Data Platform protects audit information from unauthorized deletion. The VAST Data Platform utilizes a comprehensive ABAC access control system to enforce only proper authentications to each and every user of the system. Each user, when properly authenticated to the system, is assigned only those authorized rights and abilities appropriate to each user. The VAST Data Platform's audit logs are immutable. Therefore, even a verified administrator cannot delete audit logs.

- **SRG-OS-000358**. The VAST Data Platform records time stamps for audit records to a minimum granularity of one second. This is a default feature of the product. The VAST product supports the use of two NTP services provided by the customer. This support ensures that all audit logs generated by the product are timestamped correctly. The VAST product synchronizes time to one second of granularity.

- **SRG-APP-000745-WSR-000120**. The VAST Data Platform implements the capability to centrally review and analyze audit records from multiple components within the system. When configured for syslog, all audit records from all nodes of the product will be collected in a single repository for centralized review. Syslog services are recommended in the VAST STIG Hardening Guide as a security relevant configuration in order to support centralized audit log analysis.

- **SRG-OS-000650**. The VAST Data Platform alerts organization-defined personnel or roles upon detection of unauthorized access, modification, or deletion of audit information. When notifications are enabled, specific individuals can be notified when specific events occur. The notification configuration procedure is available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000004**. The VAST Data Platform automatically audits account creation. This is a default feature of the product. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000032**. The VAST Data Platform monitors remote access methods. This is a default feature of the product. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000255**. The VAST Data Platform produces audit records containing information to establish what type of events occurred. This is a default feature of the product. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the type of action attempted on the product. The audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000063**. The VAST Data Platform allows only the information system security manager (ISSM) (or individuals or roles appointed by the ISSM) to select which auditable events are to be audited. The VAST product maintains a comprehensive audit

logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the type of action attempted on the product. Only authorized administrators can configure the audit service on the VAST product. It is the customer's responsibility to ensure that only the ISSM can be assigned as VAST administrators.

- **SRG-OS-000348**. The VAST Data Platform provides an audit reduction capability that supports on-demand reporting requirements. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the type of action attempted on the product. The audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000180**. The VAST Data Platform identifies prohibited mobile code. The VAST Data Platform prevents the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. All official VAST software is digitally signed by VAST before posting on public support sites for customer downloads. Any software, including mobile code, that is not digitally signed by VAST will be rejected by the system and will prevent installation.

- **SRG-OS-000181**. The VAST Data Platform prevents the execution of prohibited mobile code. The VAST Data Platform prevents the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. All official VAST software is digitally signed by VAST before posting on public support sites for customer downloads. Any software, including mobile code, that is not digitally signed by VAST will be rejected by the system and will prevent installation.

- **SRG-OS-000182**. The VAST Data Platform prevents the download of prohibited mobile code. The VAST Data Platform prevents the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. All official VAST software is digitally signed by VAST before posting on public support sites for customer downloads. Any software, including mobile code, that is not digitally signed by VAST will be rejected by the system and will prevent installation.

- **SRG-OS-000184**. The VAST Data Platform fails to a secure state if system initialization fails, shutdown fails, or aborts fail. The VAST product operates in Docker architecture. Each customer facing node is a Docker virtualized, stateless node. If the product's

inspection service identifies a malfunctioning node, the audit logs are copied off of the node, the node is shut down and deleted, and a new node is established from a golden image stored on the product. Should a hardware node fail, the product fails to a secure state that prohibits reinitialization by anyone but the backup emergency account.

- **SRG-OS-000216**. The VAST Data Platform uses cryptographic mechanisms to protect the integrity of log information. All VAST audit logs are secured and encrypted with FIPS-140-3 validated cryptography. In versions up to 5.2, the certificate number is 4675. Additionally, the product's ABAC system ensures that only authenticated administrators are provided access to the audit logs of the system.

- **SRG-OS-000254**. The VAST Data Platform initiates session audits at system startup. This is a default feature of the product and cannot be disabled. The VAST product maintains a comprehensive audit logging capability that operates at all times the product is running. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action. The audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000255**. The VAST Data Platform produces audit records containing information to establish the identity of any individual or process associated with the event. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action. The audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000256**. The VAST Data Platform protects audit tools from unauthorized access. Through the VAST ABAC system, only authenticated administrators are provided access to the product's audit tools. Users not assigned with administrator roles will be prohibited from accessing the product's audit tools. Any attempt to access the product's audit tool from a non-administrator will be denied and audited. If the product is configured to notify individuals when an attempt to access the audit logs, when a user is denied access to the audit tools, the ISSO or ISSM can be immediately notified.

- **SRG-OS-000257**. The VAST Data Platform protects audit tools from unauthorized modification. Through the VAST ABAC system, only authenticated administrators are provided access to the product's audit tools. Users not assigned with administrator roles will be prohibited from accessing and/or modifying the product's audit tools. Any attempt to access or modify the product's audit tool from a non-administrator will be denied and

audited. If the product is configured to notify individuals when attempting to access or modify the audit logs, when a user is denied access to the audit tools, the ISSO or ISSM can be immediately notified.

- **SRG-OS-000258**. The VAST Data Platform protects audit tools from unauthorized deletion. Through the VAST ABAC system, only authenticated administrators are provided access to the product's audit tools. Users not assigned with administrator roles will be prohibited from accessing and/or deleting the product's audit tools. Any attempt to access or modify the product's audit tool from a non-administrator will be denied and audited. If the product is configured to notify individuals when attempting to access or delete the audit logs, when a user is denied access to the audit tools, the ISSO or ISSM can be immediately notified.

- **SRG-OS-000259**. The VAST Data Platform limits privileges to change software resident within software libraries. Through the VAST ABAC system, only authenticated administrators are provided access to change the software resident on the product. Users not assigned with administrator roles will be prohibited from accessing and/or deleting the product's audit tools. Any attempt to access or modify the product's audit tool from a non-administrator will be denied and audited. If the product is configured to notify individuals when attempting to access or delete the audit logs, when a user is denied access to the audit tools, the ISSO or ISSM can be immediately notified.

- **SRG-OS-000268**. The VAST Data Platform blocks, quarantines, and/or alerts administrators when prohibited mobile code is identified. The VAST Data Platform prevents the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. All official VAST software is digitally signed by VAST before posting on public support sites for customer downloads. Any software, including mobile code, that is not digitally signed by VAST will be rejected by the system and will prevent installation. Any attempt to install mobile code will be denied and an audit log will be generated identifying who and what was attempted. If the product is configured for notifications, the product will notify the ISSM and ISSO of the attempted action.

- **SRG-OS-000269**. In the event of a system failure, VAST Data Platforms preserves any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes. The VAST data platform is deployed with at least three physical nodes operating in a redundant cluster. On this physical cluster reside at least three virtual docker nodes configured as a cluster. This is the minimum configuration that VAST allows. Typical deployments incorporate dozens of physical nodes and hundreds of virtual nodes. Each physical node is able to take on the functions of another node should that node fail. The same is true for the virtual

docker nodes. Should a virtual docker node fail, another virtual docker node will pick up the failed nodes functions. The failure and cause of the failure will be detailed on the audit logs.

- **SRG-OS-000278**. The VAST Data Platform uses cryptographic mechanisms to protect the integrity of audit tools. All VAST audit tools are secured and encrypted with FIPS-140-3 validated cryptography. In versions up to 5.2, the certificate number is 4675. Additionally, the product's ABAC system ensures that only authenticated administrators are provided access to the audit tools of the system.

- **SRG-OS-000303**. The VAST Data Platform must automatically audit account enabling actions. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action to include account enabling actions. The audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000341**. The VAST Data Platform allocates audit record storage capacity in accordance with organization-defined audit record storage requirements. The VAST Data Platform is inherently an enterprise class storage product. Therefore, considerable storage capacity can be allocated to the audit logs. Additionally, all audit logs are overwritten locally after 30 days. Therefore, there is no opportunity for audit logs to be overwritten. The audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000342**. The VAST Data Platform offloads audit records onto a different system or media than the system being audited. The product's audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000343**. The VAST Data Platform provides an immediate warning to the system administrator (SA) and information system security officer (ISSO) (at a minimum) when allocated audit record storage volume reaches 75 percent of repository maximum audit record storage capacity. If the product is configured for notifications, the product will notify the ISSM and ISSO of the situation. However, the VAST Data Platform is inherently an enterprise class storage product. Therefore, considerable storage capacity can be allocated to the audit logs. Additionally, all audit logs are overwritten locally after 30 days. Therefore, there is no opportunity for audit logs to be overwritten. The audit

service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000344**. The VAST Data Platform provides an immediate real-time alert to the system administrator (SA) and information system security officer (ISSO), at a minimum, of all audit failure events requiring real-time alerts. The notification configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000344**. The VAST Data Platform provides an immediate real-time alert to the system administrator (SA) and information system security officer (ISSO), at a minimum, of all audit failure events requiring real-time alerts. The notification configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000346**. The VAST Data Platform provides the capability to search audit records for events of interest based on the content of organization-defined audit fields within audit records. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action to include account enabling actions. The audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000350**. The VAST Data Platform provides an audit reduction capability that supports on-demand audit review and analysis. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action to include account enabling actions. The audit logs on VAST are immutable. The audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000349**. The VAST Data Platform provides an audit reduction capability that supports after-the-fact investigations of security incidents. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action to include account enabling actions. With proper authorization, VAST administrators can perform searches of audit records for any definable content. Additionally, the audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection

service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000625**. The VAST Data Platform supports a report generation capability that supports on-demand audit review and analysis. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action to include account enabling actions. With proper authorization, VAST administrators can perform searches of audit records for any definable content and export these reports. Additionally, the audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000351**. The VAST Data Platform supports a report generation capability that supports on-demand reporting requirements. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action to include account enabling actions. With proper authorization, VAST administrators can conduct searches of audit records for any definable content and export these reports in an on-demand manner. Additionally, the audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000349**. The VAST Data Platform provides a report generation capability that supports after-the-fact investigations of security incidents. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action to include account enabling actions. With proper authorization, VAST administrators can conduct searches of audit records for any definable content and export these reports in an after-the fact investigation. Additionally, the audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000640**. The VAST Data Platform provides an audit reduction capability that must not alter original content or time ordering of audit records. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action to include account enabling actions. The audit logs on the product are immutable. Additionally,

the audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000355**. The VAST Data Platform compares the internal system clocks every 24 hours with an organization-defined authoritative time source. The VAST product supports the use of two NTP services provided by the customer. This support ensures that all audit logs generated by the product are timestamped correctly. The VAST product synchronizes time to one second of granularity on an hourly basis.

- **SRG-OS-000356**. The VAST Data Platform synchronizes the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period. The VAST product supports the use of two NTP services provided by the customer. This support ensures that all audit logs generated by the product are timestamped correctly. The VAST product synchronizes time to one second of granularity on an hourly basis.

- **SRG-OS-000358**. The VAST Data Platform records time stamps for audit records that meet a granularity of one second for a minimum degree of precision. The VAST product supports the use of two NTP services provided by the customer. This support ensures that all audit logs generated by the product are timestamped correctly. The VAST product synchronizes time to one second of granularity on an hourly basis.

- **SRG-OS-000359**. The VAST Data Platform records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). The VAST product supports the use of two NTP services provided by the customer. This support ensures that all audit logs generated by the product are timestamped correctly. The VAST product synchronizes time to one second of granularity on an hourly basis.

- **SRG-OS-000392**. VAST Data Platforms sessions audit non-local maintenance and diagnostic sessions organization-defined audit events. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful to include non-local maintenance sessions. The audit log records the identity of the user or service attempting the action to include account enabling actions. The audit logs on the product are immutable. Additionally, the audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

- **SRG-OS-000665**. The VAST Data Platform ensures risk monitoring is an integral part of the continuous monitoring strategy that includes change monitoring. VAST has incorporated risk management into the development processes of the Data Platform. VAST development practices follow NIST SP800-37 for each phase of the development process. Artifacts and policies speaking to internal VAST development processes are available upon request when an NDA is in place.

- **SRG-OS-000660**. The VAST Data Platform ensures risk monitoring is an integral part of the continuous monitoring strategy that includes compliance monitoring. VAST has incorporated risk management into the development processes of the Data Platform. VAST development practices follow NIST SP800-37 for each phase of the development process. Artifacts and policies speaking to internal VAST development processes are available upon request when an NDA is in place

- **SRG-OS-000655**. The VAST Data Platform ensures risk monitoring is an integral part of the continuous monitoring strategy that includes effectiveness monitoring. VAST has incorporated risk management into the development processes of the Data Platform. VAST development practices follow NIST SP800-37 for each phase of the development process. Artifacts and policies speaking to internal VAST development processes are available upon request when an NDA is in place.

- **SRG-OS-000680**. The VAST Data Platform automatically generates audit records of enforcement actions. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful to include all enforcement actions. The audit log records the identity of the user or service attempting the action to include account enabling actions. The audit logs on the product are immutable. Additionally, the audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

6.0 Communications Security

All communications to and from the VAST product are handled by FIPS-140-3 (4675) TLS encryption.

The paragraphs below detail the communications security capabilities of the product.

6.1 Communications Session Management

The VAST Data Platform manages sessions in compliance with all applicable DISA STIGs.

- **SRG-APP-000224-WSR-000135**. All session identifiers are created with the use of the FIPS validated random number generator and cipher. All session identifiers are invalidated and then deleted once the session is closed. The VAST Data Platform utilizes FIPS validated cryptography for all RNG. All session identifiers are created with the use of FIPS library certificate #4675.

- **SRG-APP-000296-NDM-000280.** The VAST Data Platform is built to provide a logout mechanism for administrator-initiated communication sessions. This is a default feature and cannot be disabled. A logout mechanism is provided on each page of the product's GUI.

- **SRG-APP-000297-NDM-000281**. The VAST Data Platform displays an explicit logout message to administrators indicating the reliable termination of authenticated communications sessions. This is a default feature and cannot be disabled.

- **SRG-APP-000223-NDM-000269**. The product only recognizes VAST generated session identifiers. The VAST Data Platform utilizes FIPS validated cryptography for all RNG. All session identifiers are created with the use of FIPS library certificate #4675. The VAST product only recognizes VAST created session identifiers created with the use of the FIPS validated RNG. Attempting to connect to the VAST product with a non-VAST generated session ID will result in refusal to establish the connection.

- **SRG-OS-000138**. VAST Data Platforms prevents unauthorized and unintended information transfer via shared system resources. As a network storage product, serving up storage for network attached hosts is the product primary mission. It is for this reason that the product's ABAC access control system enforces proper authentications for each and every user and software service of the system. Each user, when properly authenticated to the system, is assigned only those authorized usage conditions and abilities appropriate to each user. For a standard, non-administrative user, security functionality will not be allowed or provisioned to that user. The product's ABAC system is the primary mechanism to prevent unauthorized and unintentional information transfer.

- **SRG-OS-000279**. The VAST Data Platform automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect. The VAST Data Platform is configured to terminate a user session after 15 minutes of inactivity. This time limit is configurable by the customer.

- **SRG-OS-000280**. VAST Data Platform provides a logout capability for user-initiated communications sessions. The VAST product offers a logout capability on all areas of

the product's GUI. A user can execute a voluntary logout at any time when connected to the product's GUI. This is a default capability of the product and cannot be changed.

- **SRG-OS-000281**. The VAST Data Platform displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions. The VAST product offers a logout capability on all areas of the product's GUI. A user can execute a voluntary logout at any time when connected to the product's GUI. Upon successful logout, an explicit logout message is displayed to the user. This is a default capability and cannot be changed.

- **SRG-OS-000297**. The VAST Data Platform controls remote access methods. Being a networked storage product, all access to the VAST Data Platform is performed via remote access. The product's ABAC access control system enforces proper authentications for each and every user and software service of the system. Each user, when properly authenticated to the system, is assigned only those authorized usage conditions and abilities appropriate to each user. Each access attempt is logged and recorded in the product's audit logs.

- **SRG-OS-000298**. The VAST Data Platform provides the capability to immediately disconnect or disable remote access to the information system. A VAST administrator can disconnect any user or service connected to the system at any time. This is the default capability of the product.

- **SRG-OS-000299**. The VAST Data Platform does not support wireless communications. The product only communicates via ethernet connections. No wireless protocols are supported by the product.

- **SRG-OS-000379**. Before establishing a local, remote, and/or network connection with any endpoint device, the VAST Data Platform uses a bidirectional authentication mechanism configured with a FIPS-validated Advanced Encryption Standard (AES) cipher block algorithm to authenticate with the device. The product utilizes FIPS certificate number 4675 to perform all authentication services. The product's ABAC access control system enforces proper authentications for each and every user and software service of the system. Each user, when properly authenticated to the system, is assigned only those authorized usage conditions and abilities appropriate to each user. Each access attempt is logged and recorded in the product's audit logs.

- **SRG-OS-000394**. The VAST Data Platform configures web management tools with FIPS-validated Advanced Encryption Standard (AES) cipher block algorithm to protect the confidentiality of maintenance and diagnostic communications for non-local maintenance sessions. The VAST product utilizes FIPS validated encryption, certificate

#4675, to establish and protect all remote connections. The product utilizes TLS 1.3 to protect the integrity and security of all remote connections.

- **SRG-OS-000267**. VAST Data Platforms used for non-local maintenance sessions verifies remote disconnection at the termination of non-local maintenance and diagnostic sessions. When any remote connection to the VAST product is terminated, the product immediately deletes the session ID so that the session cannot be reestablished. The VAST product utilizes FIPS validated encryption, certificate #4675, to establish and protect all remote connections. The product utilizes TLS 1.3 to protect the integrity and security of all remote connections.

- **SRG-OS-000403**. The VAST Data Platform only allows the use of DOD PKI-established certificate authorities for authentication in the establishment of protected sessions to the VAST Data Platform. The VAST product can be configured to utilize DoD certificate authorities as the authentication source for all non-local accounts. Once configured, the product will only accept digital user certificates from the DoD certificate authority.

- **SRG-OS-000404**. The VAST Data Platform implements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components. The VAST product utilizes FIPS validated encryption, certificate #4675, to establish and protect all remote connections and data at rest. All data stored on the VAST product is encrypted at rest and in flight by a FIPS validated cryptographic library.

- **SRG-OS-000405**. The VAST Data Platform implements cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components. The VAST product utilizes FIPS validated encryption, certificate #4675, to establish and protect all remote connections and data at rest. All data stored on the VAST product is encrypted at rest and in flight by a FIPS validated cryptographic library.

6.2 Communications Security Management

The product performs the following communications security functions.

- **SRG-APP-000172-WSR-000104**. The VAST Data Platform encrypts passwords during transmission through the use of TLS 1.3. The VAST product utilizes FIPS validated encryption, certificate #4675, to establish and protect all remote connections and data at rest. All data stored on the VAST product is encrypted at rest and in flight by a FIPS validated cryptographic library.

- **SRG-APP-000179-WSR-000110**. The VAST Data Platform uses cryptographic modules that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance when encrypting stored data. The VAST product utilizes FIPS validated encryption, certificate #4675, to establish and protect all remote connections and data at rest. All data stored on the VAST product is encrypted at rest and in flight by a FIPS validated cryptographic library.

- **SRG-APP-000179-WSR-000111**. The VAST Data Platform uses cryptographic modules that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. The VAST product utilizes only FIPS 140-3 validated encryption, certificate #4675, to establish and protect all remote connections and data at rest. All data stored and transmitted on and by the VAST product is encrypted at rest and in flight by a FIPS validated cryptographic library.

- **SRG-APP-000206-WSR-000128**. The VAST Data Platform does not utilize mobile code. No mobile code is allowed on the system. Any attempt to load or execute mobile code on the product will be disallowed.

- **SRG-APP-000211-WSR-000030**. VAST Data Platform accounts accessing the directory tree, the shell, or other operating system functions and utilities are only administrative accounts. The product's ABAC access control system enforces proper authentications for each and every user and software service of the system. Each user, when properly authenticated to the system, is assigned only those authorized usage conditions and abilities appropriate to each user. Each access attempt is logged and recorded in the product's audit logs. Accessing any filesystem on the

- **SRG-APP-000211-WSR-000129**. The VAST Data Platform does not host applications. The VAST product is a purpose-built storage platform. The product's web server's only functionality is to make the VAST management GUI available for access. The product does not host any other application functionality, nor does it have the ability to do so.

- **SRG-APP-000220-WSR-000201**. The VAST Data Platform invalidates session identifiers upon hosted application user logout or other session termination. The VAST product utilizes FIPS validated encryption, certificate #4675, to establish and protect all remote connections. The product utilizes TLS 1.3 to protect the integrity and security of all remote connections. Once a connection is terminated, the product immediately deletes the session ID so that the session cannot be reestablished. If the same user requires reconnection to the product, a new session ID will be issued by the product.

- **SRG-APP-000223-WSR-000011**. Cookies exchanged between the VAST Data Platform and client, such as session cookies, have security settings that disallow cookie access outside the originating VAST Data Platform and hosted application. The VAST product has cookie properties securely set. The VAST product has cookie security properties set to “samesite” and “strict”. Setting the cookie properties to samesite restricts the cookie from being used outside of the VAST architecture.

- **SRG-APP-000223-WSR-000145**. The VAST Data Platform accepts only system-generated session identifiers. The VAST product utilizes only FIPS 140-3 validated encryption, certificate #4675, to establish and protect all remote connections and data at rest. All data stored and transmitted on and by the VAST product is encrypted at rest and in flight by a FIPS validated cryptographic library. The product utilizes a FIPS validated RNG engine to generate session identifiers for use across all remote connections. Attempts to connect to the VAST product when using a session identifier not generated by VAST will be denied. This is a default feature of the product and cannot be disabled or changed.

- **SRG-APP-000224-WSR-000135**. The VAST Data Platform generates a unique session identifier for each session using a FIPS 140-2 approved random number generator. The VAST product utilizes only FIPS 140-3 validated encryption, certificate #4675, to establish and protect all remote connections and data at rest. All data stored and transmitted on and by the VAST product is encrypted at rest and in flight by a FIPS validated cryptographic library. The product utilizes a FIPS validated RNG engine to generate session identifiers for use across all remote connections.

- **SRG-APP-000224-WSR-000136.** The VAST Data Platform generates unique session identifiers that cannot be reliably reproduced. The VAST product utilizes FIPS validated encryption, certificate #4675, to establish and protect all remote connections via a FIPS validated random number generator. This RNG ensures that all session identifiers are unique. The product utilizes TLS 1.3 to protect the integrity and security of all remote connections. Once a connection is terminated, the product immediately deletes the session ID so that the session cannot be reestablished. If the same user requires reconnection to the product, a new session ID will be issued by the product.

- **SRG-APP-000224-WSR-000137**. The VAST Data Platform generates a session ID long enough that it cannot be guessed through brute force. The VAST product utilizes FIPS validated encryption, certificate #4675, to establish and protect all remote connections via a FIPS validated random number generator. This RNG ensures that all session identifiers are unique and long enough to present brute force guessing. The product utilizes TLS 1.3 to protect the integrity and security of all remote connections. Once a connection is terminated, the product immediately deletes the session ID so that the

session cannot be reestablished. If the same user requires reconnection to the product, a new session ID will be issued by the product.

- **SRG-APP-000224-WSR-000138**. The VAST Data Platform generates a session ID using as much of the character set as possible to reduce the risk of brute force. The VAST product utilizes FIPS validated encryption, certificate #4675, to establish and protect all remote connections via a FIPS validated random number generator. This RNG ensures that all session identifiers are unique and long enough to present brute force guessing by using a full character set to include characters, numbers symbols and special characters. The product utilizes TLS 1.3 to protect the integrity and security of all remote connections. Once a connection is terminated, the product immediately deletes the session ID so that the session cannot be reestablished. If the same user requires reconnection to the product, a new session ID will be issued by the product.

- **SRG-APP-000224-WSR-000139**. The VAST Data Platform generates unique session identifiers with definable entropy. The VAST product utilizes FIPS validated encryption and entropy, certificate #4675, to establish and protect all remote connections via a FIPS validated random number generator. This RNG ensures that all session identifiers are unique and long enough to present brute force guessing by using a full character set to include characters, numbers, symbols and special characters. The product utilizes TLS 1.3 to protect the integrity and security of all remote connections. Once a connection is terminated, the product immediately deletes the session ID so that the session cannot be reestablished. If the same user requires reconnection to the product, a new session ID will be issued by the product.

- **SRG-APP-000231-WSR-000144**. Information at rest is encrypted using a DOD-accepted algorithm (FIPS-140-2 Certificate #4675) to protect the confidentiality and integrity of the information. All information is encrypted on the VAST product when at-rest and when in-flight by default. There is no way to disable this configuration.

- **SRG-APP-000246-WSR-000149**. The VAST Data Platform restricts the ability of users to launch Denial of Service (DoS) attacks against other information systems or networks. The VAST data platform is deployed with at least three physical nodes operating in a redundant cluster. On this physical cluster reside at least three virtual docker nodes configured as a cluster. This is the minimum configuration that VAST allows. Typical deployments incorporate dozens of physical nodes and hundreds of virtual nodes. Each physical node is able to take on the functions of another node should that node fail. The same is true for the virtual docker nodes. Should a virtual docker node fail, another virtual docker node will pick up the failed nodes functions. This highly available architecture will prohibit DoS attacks from impacting the product's functionality.

- **SRG-APP-000266-WSR-000142**. The VAST Data Platform displays a default hosted application web page, not a directory listing, when a requested web page cannot be found. The VAST Data platform will display a generic web page whenever a web page cannot be displayed. A directory listing is never presented under any circumstances. This is a default feature of the product and cannot be changed or disabled.

- **SRG-APP-000266-WSR-000159**. Warning and error messages displayed to clients are modified to minimize the identity of the VAST Data Platform, patches, loaded modules, and directory paths. While the VAST product's audit logs contain all information necessary to answer who, what, where, when and how the error occurred, messages displayed to users have reduced information in order to minimize the information shared with a potential individual with questionable motivations. This is a default feature of the product and cannot be changed or disabled.

- **SRG-APP-000266-WSR-000160**. Debugging and trace information used to diagnose the VAST Data Platform is disabled. The VAST OS kernel has both dynamic debugging and kernel tracing disabled systemwide. The verification steps are located in the Military Unique Deployment Guide.

- **SRG-APP-000315-WSR-000003**. Remote access to the VAST Data Platform follows access policy or work in conjunction with enterprise tools designed to enforce policy requirements. The VAST product utilizes FIPS validated encryption, certificate #4675, to establish and protect all remote connections via a FIPS validated random number generator. This RNG ensures that all session identifiers are unique and long enough to present brute force guessing by using a full character set to include characters, numbers symbols and special characters. The product utilizes TLS 1.3 to protect the integrity and security of all remote connections. Additionally, the VAST Data Platform's ABAC access control system enforces proper authentications for each and every user and software service of the system. Each user, when properly authenticated to the system, is assigned only those authorized usage conditions and abilities appropriate to each user. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action to include account enabling actions. The audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide. It is between these features that all remote access to the product is audited and required to follow the applicable access control policy.

- **SRG-APP-000315-WSR-000004**. The VAST Data Platform restricts inbound connections from nonsecure zones through the use of iptables. The VAST Data Platform's firewall is based on the use of iptables to perform whitelisting and blacklisting.

The VAST STIG Hardening Procedures provide the VAST firewall script that automates the installation of the firewall on the Data Platform. Additionally, the script can be provided by contacting the POC of this white paper. Changes to the VAST firewall script is allowed after contacting the POC of this paper.

- **SRG-APP-000383-WSR-000175**. The VAST Data Platform prohibits or restricts the use of nonsecure or unnecessary ports, protocols, modules, and/or services. The VAST product has removed all unnecessary ports, protocols, modules and services that are not required for any required feature of the product to function. The Power, Protocols and Services table is available in chapter 6.3 of this white paper.

- **SRG-APP-000439-WSR-000153**. VAST Data Platform cookies, such as session cookies, sent to the client using SSL/TLS are not compressed. The VAST Data Platform utilizes TLS 1.3 for all remote network connections established via a FIPS-140-3 validated cryptographic library. A FIPS validated RNG is used to establish the session IDs utilized within the TLS 1.3 tunnel. Utilizing a TLS 1.3 tunnel prevents compression of the contents.

- **SRG-APP-000439-WSR-000154**. Cookies exchanged between the VAST Data Platform and the client, such as session cookies, have cookie properties set to prohibit client-side scripts from reading the cookie data. The VAST Data Platform has cookie properties set to “secure” which requires all cookies to be encrypted when in use. Additionally, the VAST Data Platform utilizes TLS 1.3 for all remote network connections established via a FIPS-140-3 validated cryptographic library. A FIPS validated RNG is used to establish the session IDs utilized within the TLS 1.3 tunnel.

- **SRG-APP-000439-WSR-000155**. Cookies exchanged between the VAST Data Platform and the client, such as session cookies, have cookie properties set to force the encryption of cookies. The VAST Data Platform has cookie properties set to “secure” which requires all cookies to be encrypted when in use. Additionally, the VAST Data Platform utilizes TLS 1.3 for all remote network connections established via a FIPS-140-3 validated cryptographic library. A FIPS validated RNG is used to establish the session IDs utilized within the TLS 1.3 tunnel.

- **SRG-APP-000439-WSR-000188**. The VAST Data Platform removes all export ciphers to protect the confidentiality and integrity of transmitted information. The VAST Data Platform utilizes FIPS-140-3 validated library #4675 for all at-rest, in-flight, hashing and RNG. All encryption functions of the product are performed by the same FIPS validated library. None of the cryptographic libraries are configured as an export cipher as no cipher are configured with EXPORT or EXPORT40 in their name or configuration.

- **SRG-OS-000297**. The VAST Data Platform implements required cryptographic protection using cryptographic modules complying with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance when encrypting data that must be compartmentalized. The VAST Data Platform utilizes FIPS-140-3 validated library #4675 for all at-rest, in-flight, hashing and RNG. All encryption functions of the product are performed by the same FIPS validated library.

- **SRG-OS-000079**. The VAST Data Platform obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. All password fields are obscured with no option to disable the obscurity. This is a default feature of the product and cannot be disabled.

- **SRG-OS-000080**. The VAST Data Platform enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. The VAST Data Platform's ABAC access control system enforces proper authentication for each and every user and service of the system. Each user, when properly authenticated to the system, is assigned only those authorized rights and abilities appropriate to each user. Users are not allowed to disable, circumvent or alter implemented security safeguards/countermeasures unless granted and authorized administrator permissions.

- **SRG-OS-000095**. The VAST Data Platform is configured to disable nonessential capabilities. The VAST Data Platform is a purpose-built enterprise class storage appliance. Non-essential capabilities have either been removed from the CIQ Rocky operating system or not built into the application code. There are no nonessential capabilities on the appliance.

- **SRG-OS-000096**. The VAST Data Platform is configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the PPSM CAL and vulnerability assessments. The VAST data platform is a universal storage system. To support various applications and services, the product must support many protocols. To ensure that protocols are not enabled, customers are requested not to enable services that are not required. For example, if NFS services are not required, then NFS storage should not be provisioned. Following this recommendation will ensure that the product only utilizes the minimum number of ports, protocols, and services. All ports and protocols are listed on the PPSM CAL as registered and recognized ports and protocols allowed across the DoDIN. The ports, protocols and services in use are listed in chapter 6.3 of this white paper.

- **SRG-OS-000141**. The VAST Data Platform restricts the ability of individuals to use information systems to launch organization-defined denial-of-service (DoS) attacks

against other information systems. The VAST data platform is deployed with at least three physical nodes operating in a redundant cluster. On this physical cluster reside at least three virtual docker nodes configured as a cluster. This is the minimum configuration that VAST allows. Typical deployments incorporate dozens of physical nodes and hundreds of virtual nodes. Each physical node is able to take on the functions of another node should that node fail. The same is true for the virtual docker nodes. Should a virtual docker node fail, another virtual docker node will pick up the failed nodes functions. This highly available architecture will prohibit DoS attacks from impacting on the product's functionality.

- **SRG-OS-000175**. The VAST Data Platform prohibits remote activation of collaborative computing devices. The VAST Data Platform is a purpose-built enterprise storage appliance. It is not a collaborative computing device. Collaborative computing services are not present or installable on the product.

- **SRG-OS-000398**. The VAST Data Platform associates organization-defined security attributes with information exchanged between information systems. The VAST Data Platform utilizes TLS 1.3 for all remote network connections established via a FIPS-140-3 validated cryptographic library. A FIPS validated RNG is used to establish the session IDs utilized within the TLS 1.3 tunnel. This double layer of encryption ensures that all remote network connections are kept separate and secure from other connections. The product's ABAC services ensure that all access to the product is allowed to only authenticated users and services. The ABAC system also ensures that no unauthorized user or service is allowed to access the system. These two capabilities of the product ensure that information is only sent to another system via an approved information security policy defined by the end customer.

- **SRG-OS-000178**. The VAST Data Platform validates the integrity of transmitted security attributes. The VAST Data Platform utilizes TLS 1.3 for all remote network connections established via a FIPS-140-3 validated cryptographic library. A FIPS validated RNG is used to establish the session IDs utilized within the TLS 1.3 tunnel. This double layer of encryption ensures that all remote network connections are kept separate and secure from other connections. The product's ABAC services ensure that all access to the product is allowed to only authenticated users and services. The ABAC system also ensures that no unauthorized user or service is allowed to access the system. These two capabilities of the product ensure that information is only sent to another system via an approved information security policy defined by the end customer.

- **SRG-OS-000203**. The VAST Data Platform checks the validity of all data inputs except those specifically identified by the organization. The VAST Data Platform checks the validity of all inputs without exception when discussing access to the system and

resources. The only inputs are the storage volumes presented to hosts. The storage volume validates inputs but only from a consistency and integrity perspective.

- **SRG-OS-000205**. The VAST Data Platform generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action to include account enabling actions. The audit logs on the product are immutable. The information recorded in the audit logs are the who, what, where, when and how the action occurred. The audit logs contain just the minimum information in order to tell who and when and what the action occurred. Additionally, the audit logs are rigidly protected from access by anyone not an authorized security administrator.

- **SRG-OS-000221**. The VAST Data Platform enforces approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies. The VAST Data Platform utilizes TLS 1.3 for all remote network connections established via a FIPS-140-3 validated cryptographic library. A FIPS validated RNG is used to establish the session IDs utilized within the TLS 1.3 tunnel. This double layer of encryption ensures that all remote network connections are kept separate and secure from other connections. The product's ABAC services ensure that all access to the product is allowed to only authenticated users and services. The ABAC system also ensures that no unauthorized user or service is allowed to access the system. These two capabilities of the product ensure that information is only sent to another system via an approved information security policy defined by the end customer.

- **SRG-OS-000242**. The VAST Data Platform enforces approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies. The VAST Data Platform utilizes TLS 1.3 established via a FIPS-140-3 validated cryptographic library. A FIPS validated RNG is used to establish the session IDs utilized within the TLS 1.3 tunnel. This double layer of encryption ensures that all remote network connections are kept separate and secure from other connections. The product's ABAC services ensure that all access to the product is allowed to only authenticated users and services. The ABAC system also ensures that no unauthorized user or service is allowed to access the system. These two capabilities of the product ensure that information is only sent to another system via an approved information security policy.

- **SRG-OS-000267**. VAST Data Platforms used for non-local maintenance sessions protects non-local maintenance sessions by separating the maintenance session from other network sessions by using logically separated communications paths based upon

encryption. The VAST Data Platform utilizes TLS 1.3 established via a FIPS-140-3 validated cryptographic library. A FIPS validated RNG is used to establish the session IDs utilized within the TLS 1.3 tunnel. This double layer of encryption ensures that all remote network connections are kept separate and secure from other connections.

- **SRG-OS-000417**. The VAST Data Platform has organization-defined connection ports or input/output devices either physically disabled or removed. The VAST data platform is a universal storage system. To support various applications and services, the product must support many protocols. To ensure that protocols are not enabled, customers are requested not to enable services that are not required. For example, if NFS services are not required, then NFS storage should not be provisioned. Following this recommendation will ensure that the product only utilizes the minimum number of ports, protocols, and services.

- **SRG-OS-000745**. The VAST Data Platform accepts only external credentials that are NIST-compliant. VAST recommends that the local administration account be utilized as only a backup, emergency account. All day-to-day user and administrator accounts should be customer managed accounts. VAST recommends that all customer accounts be multi-factor accounts that are based on NIST-compliant supported certificate authorities. Should both of these recommendations be followed, the VAST product will only accept NIST-compliant accounts.

6.3 VAST Federal Data Platform All Port and Protocol Usage

The tables below list all the Ports, Protocols, and Services that can be enabled on the system when using all available features.

Table 8 – Data Platform Appliance Ports, Protocols, and Services

Source	Access Direction	Destination	Port / Protocol	Service
VAST	Outgoing	VAST	0	Redis
VAST	Outgoing	Mail Svr	7 / Echo	Echo Protocols MGT/IPMI Network
VAST	Outgoing	Clients	22 SSH	Secure Shell
VAST	Outgoing	Mail Svr	25 SMTP	SMTP
VAST	Outgoing	DNS Svr	53 / DNS	VAST DNS
Client	Incoming	VAST	66 / IPMI	IPMI Network
Client	Incoming	VAST	80 / HTTP	VMS/Web UI
Client	Incoming	VAST	111 / Portmapper	NFSv3 / NIS RPC services

Source	Access Direction	Destination	Port / Protocol	Service
Client	Incoming	VAST	389 / LDAP	Lightweight Directory Access Protocol
Client	Incoming	VAST	443 / HTTPS	VMS/Web UI SSL
Client	Incoming	VAST	444 / NetBIOS	NetBIOS
VAST	Outgoing	KMIP Svr	443 / KMIP	Thales
VAST	Outgoing	DNS Svr	445 / SMB	Microsoft AD/SMB
Client	Incoming	VAST	623 / IPMI	IPMI Network
VAST	Outgoing	LDAP Svr	636 / LDAPS	LDAP S
VAST	Outgoing	VAST	2049	NFS Comms/Mount
VAST	Outgoing	VAST	3128	Proxy
VAST	Outgoing	VAST	3268	Active Directory Global Catalog
VAST	Outgoing	VAST	4000	RDMA
VAST	Outgoing	VAST	4001	TCP
VAST	Outgoing	VAST	5000 / Docker	Docker Registry
VAST	Outgoing	VAST	5001 / Replicate	Data + Native Replication
VAST	Outgoing	VAST	5432 / Postgres	Postgres Local
VAST	Outgoing	VAST	5433 / Postgres	Postgres Cluster
VAST	Outgoing	Clients	5551 / VMS	VMS Install
VAST	Outgoing	KMIP Svr	5696 / KMIP	Fornetix, Fortanix, Vault Enterprise
Client	Incoming	VAST	5902 / IPMI	IPMI Network
VAST	Outgoing	VAST	6000	DEFAULT_LEADER_RDMA_PORT
VAST	Outgoing	VAST	6001	Native Replication DEFAULT_LEADER_TCP_PORT
Client	Incoming	VAST	6126	Management Network
VAST	Outgoing	VAST	6379	Redis
VAST	Outgoing	VAST	7000	Remote Direct Memory Access
VAST	Outgoing	VAST	7777	Leadership Election
VAST	Outgoing	VAST	8000	VMS Debug
VAST	Outgoing	VAST	9090	Loopback
VAST	Outgoing	VAST	9091	Secure Loopback

Source	Access Direction	Destination	Port / Protocol	Service
VAST	Outgoing	VAST	20048	NFS Comms/Mount
VAST	Outgoing	VAST	20049	NFS/RDMA
VAST	Outgoing	VAST	20106 / NLM	NFS Comms/Mount
VAST	Outgoing	VAST	20107 / NLM	NFS Comms/Mount
VAST	Outgoing	VAST	49001 / Replication Initialization	VAST Cluster-Cluster Replication non-TLS
VAST	Outgoing	VAST	49002 / Replication Peer Initialization	VAST Cluster to Cluster Replication TLS

6.4 VAST Federal Data Platform Services

The below table lists **all** the Services that **can** be enabled on the system when using all available.

Table 9 – VAST Federal Data Platform Running Services

Service / Daemon Name	Definition
atop.service monitor	Atop advanced performance
auditd.service	Security Auditing Service
chronyd.service	NTP client/server
containerd.service	containerd container
crond.service	Command Scheduler
dbus.service	D-Bus System Message Bus
docker.service	Docker Application
getty@tty1.service	Getty on tty1
gssproxy.service	GSSAPI Proxy Daemon
irqbalance.service	irqbalance daemon
polkit.service	Authorization Manager

rngd.service	Hardware RNG Entropy
rpcbind.service	RPC Bind
rsyslog.service	System Logging Service
serial-getty@ttyS0.service	Getty on ttyS0
smartd.service	Self-Monitoring and Reporting Technology (SMART)
sshd.service	OpenSSH server daemon
systemd-journald.service	Journal Service
systemd-logind.service	Login Service
systemd-udevd.service	Kernel Device Manager
tuned.service	Dynamic System Tuning
user@1000.service	User Manager for UID 1000

7.0 Data Security

As required by many regulated industries, VAST Cluster features the ability to encrypt the data that is saved on the cluster's storage media (data 'at rest') to protect data from unauthorized usage. When encryption is enabled, all data on each of the cluster's tenants is encrypted and decrypted transparently using 256-bit AES-XTS FIPS-140-3 (4675) encryption. VAST Cluster generates a random unique 256-bit key at cluster initialization. Keys can be managed internally, or they can be managed by an external key manager (EKM). The key is unique to the cluster with the internal key management option.

With the EKM option, the key is by default unique per encryption group, which can be per cluster, per tenant or per group of tenants.

From VAST Cluster 5.2 and newer releases, customers can encrypt any new path with its own dedicated, individually manageable, encryption key. This is done by creating the path as an encrypted path before creating a view that makes the path accessible to client access. A default key per tenant encrypts all other paths on the tenant.

This feature supports the following EKM solutions:

- Thales Group CipherTrust Data Security Platform, versions 2.11, 2.14 and 2.4
- Fornitex VaultCore, verson 2.6

Encryption is disabled by default. It can be enabled at cluster creation when installing a new cluster. Encryption with internal management of encryption keys can also be enabled on a running cluster. If encryption is enabled on a running cluster, after installation, a rewrite is automatically triggered. The rewrite process rewrites all data on the cluster with encryption, scrubs the drives from any old unencrypted data and restripes the data across the drives.

7.1 Enabling Encryption via VAST Web UI

Encryption can be enabled with the VAST Web UI Easy Install utility with internal key management or with EKM. EKM with the Fornetix CoreVault provider can be enabled only with the VAST CLI.

7.2 Enabling Encryption via VAST CLI

When creating a new cluster using the cluster create CLI command, include the following command line options in the command line.

- --enable-encryption. Enables encryption.
- --encryption-type INTERNAL|CIPHER_TRUST_KMIP|FORNETIX_KMIP. Specifies the type of key management:
    - INTERNAL = internally managed keys. CIPHER_TRUST_KMIP= Keys stored on a Thales Group CipherTrust Data Security Platform. FORNETIX_
    - KMIP= Keys stored on Fornetix CoreVault.

- If --encryption-type is CIPHER_TRUST_KMIP or FORNETIX_KMIP:
    - --ekm-servers EKM_ADDRESS1[:PORT1][,EKM_ADDRESS2[:PORT2][,EKM_ADDRESS3[:PORT3][,EKM_ADDRESS4[:PORT4]]]]. Specifies the IP addresses or DNS names and port numbers for up to four EKM servers. Valid port range: 1024 - 65535. Default: 5696.

    - Either of the following:
        - --ekm-certificate CERTIFICATE. Specifies the SSL certificate for the connection to the EKM servers. Enter the certificate content encapsulated in quotation marks (""). Include the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines from the certificate file content.

        - --ekm-certificate-file CERTIFICATE_FILE. Specifies the SSL certificate file for the connection to the EKM servers. Place the file on the CNode

host from which you are running the VAST CLI under /vast/bundles. Specify the file path in quotation marks as CERTIFICATE_FILE relative to /vast/bundles. For example: --ekm-certificate_file "/vast/bundles/cert.pem".

- Either of the following:
  - --ekm-private_key PRIVATE_KEY. Specifies the private key of the SSL certificate for connecting to the EKM servers. Enter the private key content encapsulated in quotation marks (""). Include the "-----BEGIN EC PRIVATE KEY-----" and "-----END EC PRIVATE KEY-----" lines from the private key file content.
  - --ekm-private_key-file PRIVATE_KEY_FILE. Specifies the private key file of the SSL certificate for connecting to the EKM servers. Place the private key file on the CNode host from which you are running the VAST CLIunder /vast/bundles. Specify the file path relative to /vast/bundles in quotation marks as PRIVATE_KEY_FILE. For example: --ekm-private_key_file "/vast/ bundles/tmp/cert.key".

- For Fornetix only, either of the following:
  - --ekm-ca-certificate CA_CERTIFICATE. Specifies the CA certificate file content for the connection to the EKM servers. Enter the CA certificate file content encapsulated in quotation marks (""). Include the ""-----BEGIN CA CERTIFICATE-----" and "-----END CA CERTIFICATE-----" lines from the CA certificate file content.
  - --ekm-ca-certificate_file CA_CERTIFICATE_FILE. Specifies the CA certificate file for the connection to the EKM servers. Place the file on the CNode host from which you are running the VAST CLIunder /vast/bundles. Specify the file path relative to / vast/bundles in quotation marks as CA_CERTIFICATE_FILE. For example: --ekm-ca-certificate_file "/vast/bundles/cacert.pem"
- If you need to bypass certificate validation: --ekm-bypass-validation

This example enables encryption with internal key management:

- vcli: admin> cluster create --cnode-ips 192.0.2.0,192.0.2.1,192.0.2.2,192.0.2.3 --dnode-ips 192.0.2.4,192.0.2.5 --name mycluster

7.3 Data Security Management

The following services are delivered via the FIPS validated library within the product:

- **SRG-APP-000395-NDM-000310**. The VAST Data Platform is configured to authenticate SNMP messages using a FIPS-validated Keyed-Hash Message Authentication Code

(HMAC) via certificate #4675. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing and RNG are all accomplished by a FIPS validated library.

- **SRG-APP-000400-NDM-000313**. The VAST Data Platform can be configured to prohibit cached authenticators after an organization-defined time period. When connected to a customer's IDP, the product will enforce the cached authenticator requirements established by the IDP. If the customer's IDP is Active Directory with X.509-based Certificate Authorities (CA) and a CA is offline, the VAST Data Platform will utilize the IDP as the authoritative source of the user's authentication.

- **SRG-APP-000411-NDM-000330**. The VAST Data Platforms uses FIPS-validated, certificate #4675, Keyed-Hash Message Authentication Code (HMAC) to protect the integrity of non-local maintenance and diagnostic communications. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing and RNG are all accomplished by a FIPS validated library.

- **SRG-APP-000412-NDM-000331**. The VAST Data Platform is configured to implement cryptographic mechanisms using a FIPS 140-2, certificate #4675, approved algorithm to protect the confidentiality of remote maintenance sessions. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing and RNG are all accomplished by a FIPS validated library.

- **SRG-APP-000915-NDM-000310**. The VAST Data Platform is configured to provide protected storage for cryptographic keys with organization-defined safeguards and/or hardware protected key store. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library. Additionally, the VAST Data Platform utilizes a comprehensive ABAC access control system to enforce only proper authentications to each and every user of the system. Each user, when properly authenticated to the system, is assigned only those authorized rights and abilities appropriate to each user. The VAST product's ABAC service coupled with its at-rest encryption ensures that only properly authorized individual have access to the product's protected key store.

- **SRG-APP-000251-WSR-000195**. The VAST Data Platform terminates the connection if server-level exceptions are triggered when handling requests to prevent HTTP request smuggling attacks. The VAST Data Platform requires that all remote communications be done over HTTPS. HTTP connections are redirected to HTTPS connections. Clients that utilize only HTTP connections will be refused. The VAST product utilizes TLS 1.3

established via a FIPS-140-3 validated cryptographic libraries for all remote connections. A FIPS validated RNG is used to establish the session IDs utilized within the TLS 1.3 tunnel. This double layer of encryption ensures that all remote network connections are kept separate and secure from other connections. The VAST Data Platform validates certificates used for TLS functions by performing RFC 5280-compliant certification path validation.

- **SRG-APP-000439-WSR-000196**. The VAST Data Platform does not utilize a forward proxy. Proxies are not utilized anywhere within the product.

- **SRG-OS-000033**. The VAST Data Platform implements DOD-approved encryption to protect the confidentiality of remote access sessions. The VAST product utilizes a FIPS-140-3 validated cryptographic library (certificate number 4675) to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library.

- **SRG-OS-000120**. The VAST Data Platform uses FIPS-validated SHA-2 or higher hash function to protect the integrity of hash message authentication code (HMAC), Key Derivation Functions (KDFs), Random Bit Generation, hash-only applications, and digital signature verification. The VAST product utilizes a FIPS-140-3 validated cryptographic library (certificate number 4675) to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library.

- **SRG-OS-000185**. The VAST Data Platform uses FIPS-validated encryption and hashing algorithms to protect the confidentiality and integrity of VAST Data Platform configuration and user-generated data stored on the host. The VAST product utilizes a FIPS-140-3 validated cryptographic library (certificate number 4675) to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library.

- **SRG-OS-000250**. The VAST Data Platform providing remote access services uses FIPS-validated digital signatures, in conjunction with an approved hash function to protect the integrity of remote access sessions. The VAST product utilizes a FIPS-140-3 validated cryptographic library (certificate number 4675) to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library.

- **SRG-OS-000294**. The VAST Data Platform associates organization-defined types of security attributes having organization-defined security attribute values with information in storage, process or in transmission.

- **SRG-OS-000404**. The VAST Data Platform implements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components. The VAST Data Platform utilizes FIPS-140-3 certificate #4675 for all data at rest and data in flight encryption.

- **SRG-OS-000405**. The VAST Data Platform implements cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components. The VAST Data Platform utilizes FIPS-140-3 certificate #4675 for all data at rest and data in flight encryption.

- **SRG-OS-000408**. The VAST Data Platform maintains a separate execution domain for each executing process. This is a default feature of the product and cannot be changed. Each significant component of the product runs within its own Docker instance. These Docker instances can be deleted or started based on the dynamic scaling capabilities of the product. Each of these instances run in their own separate execution domain.

- **SRG-OS-000432**. The VAST Data Platform behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received. The VAST Data Platform utilizes a comprehensive ABAC access control system to enforce only proper authentications to each and every user of the system. Each user, when properly authenticated to the system, is assigned only those authorized rights and abilities appropriate to each user. The ABAC system also protects the product from all unauthorized access. It is this system that will reject improper or invalid inputs. The ABAC system requires that only properly formatted authentications are accepted. Any invalid authentication attempts will be discarded and ignored. Each attempt will be audited for after-the-fact analysis.

- **SRG-OS-000433**. The VAST Data Platform implements organization-defined security safeguards to protect its memory from unauthorized code execution. The VAST Data Platform utilizes a comprehensive ABAC access control system to enforce only proper authentications to each and every user of the system. Each user, when properly authenticated to the system, is assigned only those authorized rights and abilities appropriate to each user. The ABAC system also protects the product from all unauthorized access.

- **SRG-OS-000437**. The VAST Data Platform removes organization-defined software components after updated versions have been installed. Following each update, the VAST product removes unnecessary software that has been superseded. Following an update, no legacy software exists on the system. This is a default feature of the product and cannot be disabled.

- **SRG-OS-000438**. The VAST Data Platform removes organization-defined firmware components after updated versions have been installed. Following each update, the VAST product removes unnecessary software to include firmware releases that have been superseded. This is a default feature of the product and cannot be disabled.

- **SRG-OS-000478**. The VAST Data Platform uses a FIPS-validated cryptographic module to generate cryptographic hashes. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library.

- **SRG-OS-000780**. The VAST Data Platform provides protected storage for cryptographic keys with organization-defined safeguards and/or hardware protected key store. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library.

- **SRG-OS-000267**. The VAST Data Platform protects non-local maintenance sessions by separating the maintenance session from other network sessions with the system by logically separated communications paths. The VAST Data Platform utilizes TLS 1.3 established via a FIPS-140-3 validated cryptographic library. A FIPS validated RNG is used to establish the session IDs utilized within the TLS 1.3 tunnel. This double layer of encryption ensures that all remote network connections are kept separate and secure from other connections.

- **SRG-OS-000555**. The VAST Data Platform services use FIPS-validated cryptographic module to implement encryption services for unclassified information requiring confidentiality. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library.

- **SRG-OS-000550**. The VAST Data Platform uses a FIPS-validated cryptographic module to provision digital signatures. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library.

- **SRG-OS-000540**. The VAST Data Platform uses a FIPS-validated block cipher mode to protect the confidentiality of maintenance and diagnostic communications for nonlocal maintenance sessions. The VAST product utilizes a FIPS-140-3 validated cryptographic

library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library.

- **SRG-OS-000535**. The VAST Data Platform configures SNMPv3 to use FIPS-validated AES cipher block algorithms to protect the confidentiality of maintenance and diagnostic communications for non-local maintenance sessions. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library. SMNPv3 protocols are generated using a FIPS validated cryptographic library.

- **SRG-OS-000120**. The VAST Data Platform uses FIPS-validated SHA-2 or higher hash function for digital signature generation and verification (nonlegacy use). The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library

- **SRG-OS-000525**. The VAST Data Platform validates certificates used for TLS functions by performing RFC 5280-compliant certification path validation. The VAST Data Platform utilizes TLS 1.3 established via a FIPS-140-3 validated cryptographic library. A FIPS validated RNG is used to establish the session IDs utilized within the TLS 1.3 tunnel. This double layer of encryption ensures that all remote network connections are kept separate and secure from other connections. The VAST Data Platform validates certificates used for TLS functions by performing RFC 5280-compliant certification path validation.

- **SRG-OS-000520**. The VAST Data Platform uses FIPS-validated SHA-2 or higher hash function to protect the integrity of HMAC, Key Derivation Functions (KDFs), Random Bit Generation, and hash-only applications. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library.

- **SRG-OS-000510**. The VAST Data Platform prohibits or restricts the use of protocols that transmit unencrypted authentication information or use flawed cryptographic algorithm implementations for transmission. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library. There are no uncovered, non-encrypted protocols or in-flight communications on the product. This is a default feature of the product and cannot be disabled.

- **SRG-OS-000505**. The VAST Data Platform uses TLS 1.2, at a minimum, to protect the confidentiality of sensitive data during electronic dissemination using remote access. The VAST Data Platform utilizes TLS 1.3 established via a FIPS-140-3 validated cryptographic library. A FIPS validated RNG is used to establish the session IDs utilized within the TLS 1.3 tunnel. This double layer of encryption ensures that all remote network connections are kept separate and secure from other connections. The VAST Data Platform validates certificates used for TLS functions by performing RFC 5280-compliant certification path validation.

8.0 Serviceability

The VAST Data Platform has the ability to both phone home and be serviced remotely. However, VAST Data Federal recommends that all phone home and remote service be disabled on all U.S. Government installations. VAST Data Federal maintains a roster of fully cleared support personnel available to support all U.S. Government installations regardless of level of clearance.

U.S. Government customers should follow the steps provided in Chapter 3.6 to ensure the Data Platform sends appropriate notifications to specific individuals whenever relevant events occur. These individuals can then decide if a VAST support ticket should be opened for onsite support.

8.1 Serviceability Management

The following serviceability features are available on the product.

- **SRG-APP-000225-WSR-000074**. The VAST Data Platform augments re-creation to a stable and known baseline. The VAST product operates in Docker architecture. Each customer facing node is a Docker virtualized, stateless node. If the product's inspection service identifies a malfunctioning node, the audit logs are copied off of the node, the node is shut down and deleted, and a new node is established from a golden image stored on the product. Should a hardware node fail, the product fails to a secure state that prohibits reinitialization by anyone but the backup emergency account.

- **SRG-APP-000225-WSR-000140**. The VAST Data Platform is built to fail to a known safe state if system initialization fails, shutdown fails, or aborts fail. The VAST data platform is deployed with at least three physical nodes operating in a redundant cluster. On this physical cluster reside at least three virtual docker nodes configured as a cluster. This is the minimum configuration that VAST allows. Typical deployments incorporate dozens of physical nodes and hundreds of virtual nodes. Each physical node is able to take on the functions of another node should that node fail. The same is true for the virtual docker nodes. Should a virtual docker node fail, another virtual docker node will pick up the failed nodes functions.

- **SRG-APP-000225-WSR-000141**. The VAST Data Platform provides clustering capability. The VAST data platform is deployed with at least three physical nodes operating in a redundant cluster. On this physical cluster reside at least three virtual docker nodes configured as a cluster. This is the minimum configuration that VAST allows. Typical deployments incorporate dozens of physical nodes and hundreds of virtual nodes. Each physical node is able to take on the functions of another node should that node fail. The same is true for the virtual docker nodes. Should a virtual docker node fail, another virtual docker node will pick up the failed nodes functions.

- **SRG-APP-000435-WSR-000148**. The VAST Data Platform is tuned to handle the operational requirements of the hosted application. The VAST Data Platform is a purpose-built enterprise class storage appliance. All aspects and components of the product have been tuned to best service the product's features to customers. There are no unnecessary or irrelevant services on the VAST product.

- **SRG-OS-000439**. The VAST Data Platform installs security-relevant software updates within the time period directed by an authoritative source (e.g., IAVM, CTOs, DTMs, and STIGs) when the owning Unit deems it appropriate. VAST has established a comprehensive federal compliance program whose purpose is to comply with all U.S. Government requirements. This program reviews all IAVMs, CTOs, DTMs and STIGs for applicability to the VAST product. When an applicable change is

- **SRG-OS-000445**. The VAST Data Platform verifies the correct operation of organization-defined security functions. The VAST product performs continuous inspection of components and services. The VAST product's auditing system is inspecting each and every action taken on the platform by any user or service. This continuous monitoring allows for inspection of all components of the system. When an anomaly is identified, the component is removed, if possible, an audit log is created, and a notification is sent if notifications have been enabled.

- **SRG-OS-000446**. The VAST Data Platform performs verification of the correct operation of security functions: Upon system startup and/or restart; upon command by a user with privileged access; and/or every 30 days. The VAST product performs continuous inspection of components and services. The VAST product's auditing system is inspecting each and every action taken on the platform by any user or service. This continuous monitoring allows for inspection of all components of the system. When an anomaly is identified, the component is removed, if possible, an audit log is created, and a notification is sent if notifications have been enabled.

- **SRG-OS-000447**. The VAST Data Platform shuts down the information system, restarts the information system, and/or notify the system administrator when anomalies in the

operation of the organization-defined security functions are discovered. The VAST Data Platform is deployed with at least three physical nodes operating in a redundant cluster. On this physical cluster reside at least three virtual docker nodes configured as a cluster. This is the minimum configuration that VAST allows. Typical deployments incorporate dozens of physical nodes and hundreds of virtual nodes. Each physical node is able to take on the functions of another node should that node fail. The same is true for the virtual docker nodes. Should a virtual docker node fail, another virtual docker node will pick up the failed nodes functions. The VAST product performs continuous inspection of operating components and nodes. When an anomaly is discovered on a stateless node, the node is removed and replaced with a golden image copy. This is a default feature of the product and cannot be disabled.

- **SRG-OS-000448**. The VAST Data Platform implements organization-defined security safeguards to protect the integrity of boot firmware in organization-defined devices. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library. When the product recognizes an invalid digital signature or incorrect component hash, the software is removed from the system and an audit log is generated.

- **SRG-OS-000449**. The VAST Data Platform implements cryptographic mechanisms to authenticate organization-defined software or firmware components prior to installation. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library. When the product recognizes an invalid digital signature or incorrect component hash, the software is removed from the system and an audit log is generated.

- **SRG-OS-000450**. The VAST Data Platform verifies the integrity of the boot process of organization-defined devices. The VAST product performs continuous inspection of components and services. The VAST product's auditing system is inspecting each and every action taken on the platform by any user or service. This continuous monitoring allows for inspection of all components of the system. When an anomaly is identified, the component is removed, if possible, an audit log is created, and a notification is sent if notifications have been enabled.

- **SRG-OS-000760**. The VAST Data Platform inspects the maintenance tools to ensure the latest software updates and patches are installed. The VAST product utilizes a FIPS-140-3 validated cryptographic library to perform all encryption functions on the product. At-rest, in-flight, hashing, digital signature generation, and RNG are all accomplished by a FIPS validated library. When a current maintenance contract is in place, VAST will notify the customer with any available updates or product patches. The

customer is responsible for applying the patch or update to the product. VAST does not perform online, automated updates of products.

- **SRG-OS-000755**. The VAST Data Platform monitors the use of maintenance tools that execute with increased privilege. The VAST product maintains a comprehensive audit logging capability. The auditing service of the product audits all actions attempted on the system whether successful or unsuccessful. The audit log records the identity of the user or service attempting the action to include account enabling actions. With proper authorization, VAST administrators can conduct searches of audit records for any definable content, to include all use of maintenance tools and export these reports in an on-demand manner. Additionally, the audit service can be configured to offload all audit logs via syslog to a customer managed audit log collection service. The syslog configuration procedures are available in the VAST Military Unique Deployment Guide.

9.0 Alerting

The VAST Data Platform has the ability audit each and every action taken on the system by either a user or a service. This comprehensive auditing capability is the foundation from which all notifications are built. The product has the ability to perform a notification for any type or collection of events that may occur on the product. Customers should fully understand what auditing events requires notifications and configure the product to support this requirement.

9.1 Notification Management

The paragraphs below detail the notification enablement.

Procedure:

1. From a networked workstation and SSH client, authenticate to the VAST Data Platform with an administrative account.
2. From the left navigation menu, select **Settings** and then **Notifications**.
3. To configure SMTP for sending email notifications, select **SMTP Setup** and complete the fields:
    a. **SMTP Host** - The host name of the SMTP server.
    For example: mail.company.com.
    b. **SMTP Port** - The port used by the SMTP server to send outgoing emails. The most commonly used port for SMTP is port 25, although some IPs deny its use in order to block spam. SMTP servers often support alternative ports, including port 587.
    c. **SMTP User** - User for SMTP host authentication.
    d. **SMTP Password** - The password for the SMTP user.
    e. **Use TLS** - Enable this setting to send emails over a TLS connection.

4. To set up email message properties and recipients, select **Email Setup** and complete the fields:

    a. **Email Sender** - The sender email address that is included in outgoing emails. This setting applies to all alarm notification emails.
    Example: do_not_reply@company.com

    b. **Email Subject** - The email subject to be included in outgoing emails. This optional setting applies to all alarm notification emails.

    Example: VAST Alarm If you want VAST Cluster to include the alarm description as the email subject, leave this field blank.

    c. **Email Recipients** - Default email recipients. These recipients receive notifications of all alarms except those triggered by events that have a different list of email recipients specified in the event definition or for which default notification actions are disabled. Enter as a comma-separated list of email addresses (no spaces).

    Example: storage_admin@company.com, bsmith@company.com,

5. To specify a webhook for sending alarms to an external application (optional), select **Webhook Setup** and enter the details for the default webhook. This webhook is triggered by all events except those for this a custom webhook is defined or for which notification actions are disabled.

    a. **Webhook URL** - The URL of the API endpoint of an external application, including parameters.

    b. **Webhook Data** - The payload, if required, for the endpoint. You can use the $event variable to include the event message.

    c. **Webhook Method** - Select the HTTP method you want to invoke with the trigger:

        i. POST

        ii. GET

        iii. PUT

        iv. PATCH

        v. DELETE

6. To configure sending alarm information to a syslog server, select **Syslog Setup** and complete the fields:

    a. **Syslog Host** - Specify the syslog server's IP address.

    b. **Syslog Port** - Specify the port number that the server listens on for syslog requests. Default: 514

    c. **Syslog Protocol** - Specify either of the protocols for communicating with the remote syslog server:

        i. TCP

ii. UDP (default)

d. The protocol you choose must be enabled on the syslog server.

e. Enable VMS Audit - Toggle on (default) or off to enable or disable auditing of VMS operations.

f. Enable Shell Audit - Toggle on or off (default) to enable or disable auditing of CNode and DNode shell commands.

g. Enable IPMI Audit - Toggle on or off (default) to enable or disable auditing of CNode and DNode IPMI commands.

h. Audit Logs Retention Enter the number of days to store audit logs on the syslog server.

7. Click Save.

Result: The VAST Data Platform will notify specified individuals when specific events occur.

10.0 FIPS-140-3

The VAST Data Platform has provided FIPS validated libraries in our product for many years. Depending on the version of VAST code in use will determine what FIPS certificate numbers are in use.

1. Versions 5.2 and prior – CMVP Certificate Number 4675
2. Versions 5.2.2 and newer:
    a. CMVP Certificate Numbers E205, E210, E219
    b. CAVP Certificate Numbers A6740, A6749, A6747, A6748, A6738, A6743, A6741, A6742, A6739, A6746, A6744, A6745, A6763, A6762, A6758, A6754, A6752, A6750, A6756, A6760, A6759, A6755, A6753, A6751, A6757, A6761, A6520, A6464, A6470, A6465, A6466, A6475, A6474, A6473, A6472, A6467, A6469, A6468, A6471, A6421, A6419, A6420, A6415, A6413, A6414, A6418, A6416, A6417, A6435, A6434, A6430, A6426, A6424, A6422, A6428, A6432, A6431, A6427, A6425, A6423, A6429, A6433, A6114, A6113, A6117, A6118, A6116, A6115, A5993, A5991, A5992, A5990, A5917, A5918, A5915, A5916, A5919, A5914, A5813, A5816, A5823, A5824, A5807, A5810, A5815, A5818, A5809, A5812, A5821, A5814, A5817, A5808, A5811, A5820, A5822, A5819, A5453, A5386, A5387, A3950, A3951, A3952, A3953, A3955, A3954, A3956, A3957

11.0 Other Security Settings

The following paragraphs provide additional security relevant topics that customers should take into account when undergoing a VAST Data Platform installation and subsequent operation.

11.1 Monitor VAST Security Advisories

The VAST security team creates and publishes advisories for security-related issues in VAST products. These advisories are posted on the VAST support portal located at https://support.vastdata.com/s/ In order to maintain a secure data management service, all customers need to be aware of the VAST security advisories so that patches can be applied before exploits become widely available.

For critical vulnerabilities, VAST provides patches as soon as feasible. The patches will be available for download from the support portal and can be applied through the VAST CLI. Each patch comes with release notes, which explains the vulnerability and the appropriate information about fixes.

11.2 Centralized Authentication

The VAST Data Platform supports both local authentication and Lightweight Directory Access Protocol (LDAP) authentication. Local authentication must be used only as a fallback mechanism to access the Data Platform product when LDAP services are unreachable.

11.3 Secure Communications

In order to secure and trust all communications to the product, customers should install a trusted server certification to enable trusted TLS communications to the product.

11.4 STIG Hardening Steps

The steps provided in the VAST Data Platform Product Hardening Guide are provided to our customers as a means to configure the product to be in compliance with all applicable DISA STIGs and SRGs. The following STIGs and SRGs are determined applicable to the VAST Data Platform:

- Application Security and Development STIG
- Application Server SRG
- Container SRG
- Database SRG
- Docker STIG
- Network Device SRG
- Red Hat Enterprise Linux 8 SRG
- Web Server SRG

If a hardening step is repeated due to the step resolving more than one STIG control, then the step is only provided once in this document.

12.0 Summary

This SCG is a living document and will be updated as the product and its security capabilities further mature. VAST is committed to delivering a secure product to our customers and will continue to provide documentation detailing the security characteristics of the product in order to support any certification and accreditation requirements.