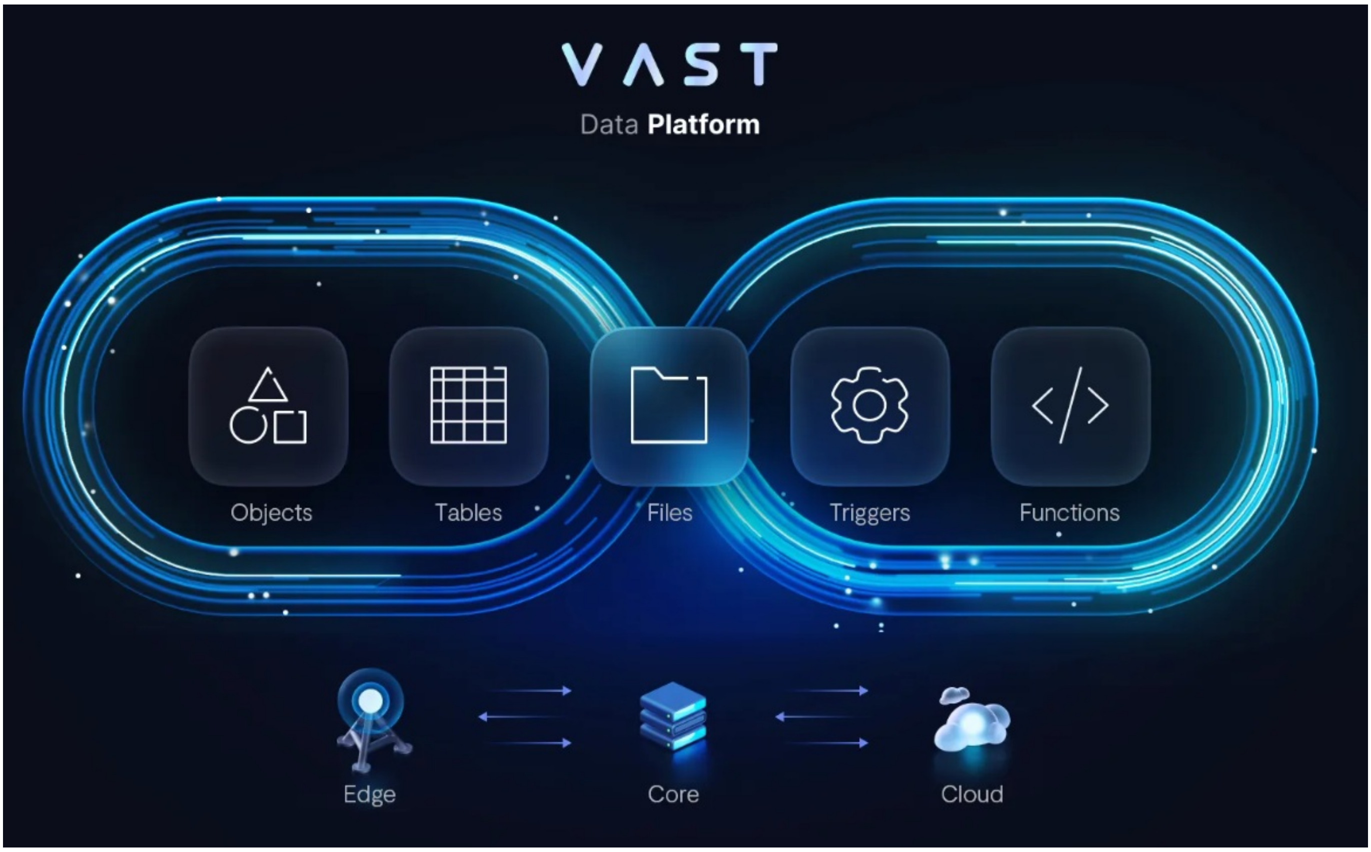
VAST Data Platform Software User Guide

VAST Data Platform Software Use



Contents

Introduction

In today's data-driven world, the confidentiality and security of unstructured data are paramount. Multi-Category Security (MCS) and secure tenancy features offer a robust framework to address these concerns. MCS, an access control mechanism in Security-Enhanced Linux (SELinux), enhances data confidentiality by assigning specific categories to files and processes. This ensures that only authorized users and processes can access sensitive information, providing an additional layer of protection for unstructured data such as documents, images, and videos.

Secure tenancy further strengthens data isolation by creating distinct environments for different groups, departments, or organizations within the same infrastructure. This approach ensures that each tenant's data is logically or physically separated, preventing unauthorized access and maintaining data privacy. Key aspects of secure tenancy include resource isolation, data segregation, network segmentation, and granular access controls.

The VAST Data Platform exemplifies these principles through its comprehensive suite of features, including VLAN tagging, role-based and attribute-based access controls, and robust encryption mechanisms. This document explores how integrating MCS with secure tenancy within the VAST Data Platform provides a comprehensive and secure solution for managing unstructured data, particularly for organizations with stringent data confidentiality requirements. This introduction is concise, focused, and provides a clear guide to the document's content, aligning with best practices for technical documentation.

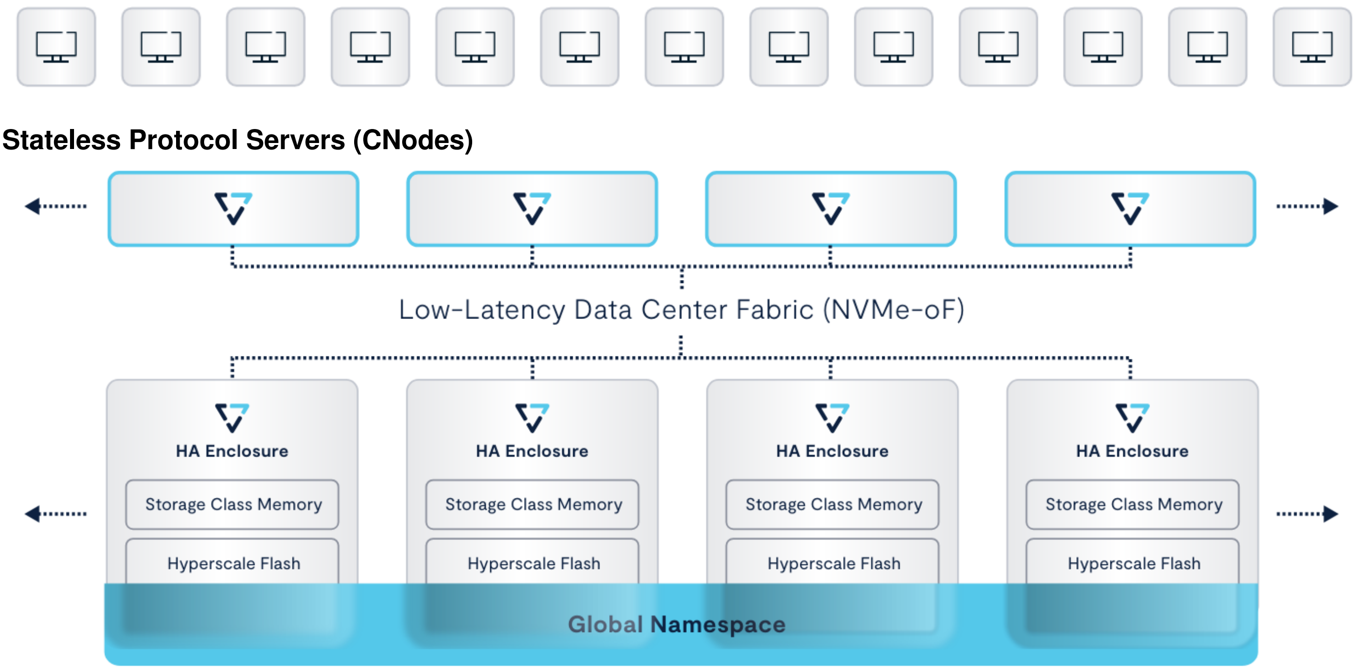
What is the VAST Data Platform

The VAST Data Platform is a comprehensive solution for handling unstructured data, particularly for AI and deep learning applications. It integrates various capabilities to capture, catalog, label, enrich, and preserve data, providing seamless data access from edge to cloud.

Disaggregated and Shared-Everything (DASE) Architecture

This architecture decouples compute logic from system state, allowing for independent scaling of capacity by adding Data Nodes (DNodes) and performance by adding Compute Nodes (CNodes). It combines shared and transactional data structures to overcome the limitations of traditional distributed systems.

Supported Clients: NFS, NFSoRDMA Server Message Block (SMB), Amazon S3, and Containers (CSI)


Stateless Protocol Servers (CNodes)
Low-Latency Data Center Fabric (NVMe-oF)
HA Enclosure
Storage Class Memory
Hyperscale Flash
Global Namespace

VAST Disaggregated, Shared-Everything (DASE) architecture

VAST DataStore

Introduced in 2019, the DataStore is designed for storing and serving unstructured data. It breaks the tradeoff between performance and capacity, making it suitable for enterprise AI-ready unstructured data storage.

VAST DataBase

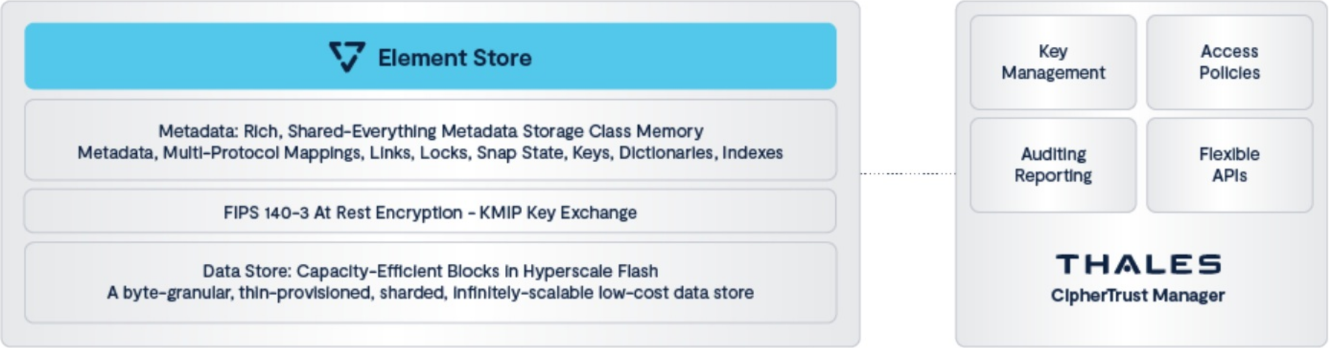
This component delivers the transactional performance of a database, the analytical performance of a data warehouse, and the scale and affordability of a data lake. It supports both row and columnar data storage.

VAST DataSpace

Launched in 2023, DataSpace provides global data access from edge to cloud, balancing strict consistency with local performance. It enables computation on data from any public, private, or edge cloud platform.

The platform unifies structured and unstructured data, database analytics, and provides a global namespace. It supports various protocols like NFS, SMB, S3, SQL, and embeds Apache Spark for data transformation and consumption from messaging systems.

The platform is built to power AI and enterprise applications, providing real-time deep data analysis and deep learning capabilities. It captures and processes data in real-time, enabling AI inference, metadata enrichment, and model retraining.


Element Store
Metadata: Rich, Shared-Everything Metadata Storage Class Memory
Metadata, Multi-Protocol Mappings, Links, Locks, Snap State, Keys, Dictionaries, Indexes
FIPS 140-3 At Rest Encryption - KMIP Key Exchange
Data Store: Capacity-Efficient Blocks in Hyperscale Flash
A byte-granular, thin-provisioned, sharded, infinitely-scalable low-cost data store
Key Management
Access Policies
Auditing Reporting
Flexible APIs
THALES
CipherTrust Manager

VAST Data Platform & Thales Cipher Trust

Network and Node Segmentation

The VAST Data Platform includes several features related to management efficiency and network segmentation, including CNode grouping functionality, as well as the ability to bind CNodes to VLANs. Here are the detailed descriptions of these features, along with the relevant sections from the VAST Cluster 5.1 Documentation:

CNode Grouping and Pooling

Server (CNode) Pooling: Storage protocols are served from the Compute Nodes (CNodes). The VAST Data Platform allows for the grouping of CNodes into distinct server pools. Each server pool has an assigned set of Virtual IP Addresses (VIPs) that are distributed across the CNodes in the pool. This provides a mechanism for Quality of Service (QoS) by controlling the number of servers assigned to each pool. When a CNode goes offline, the VIPs it was serving are non-disruptively redistributed across the remaining CNodes in the pool. This ensures load balancing and high availability.

- Section: VAST Cluster Documentation, “Managing Virtual IP Pools” [p. 593]

VLAN Tagging and Binding

VLAN Tagging: VLAN tagging allows administrators to control which Virtual IPs are exposed to which VLANs on the network. This feature ensures that network traffic is isolated between different VLANs, preventing unauthorized access and data leakage between tenants. VLAN tagging is configured by creating Virtual IP pools within VLANs in the VAST platform, providing secure network segmentation and isolation.

- Section: VAST Cluster Documentation, “Tagging Virtual IP Pools with VLANs” [p. 147]
- Section: Network Access and Storage Provisioning (v5.1) [p. 141]

Network Segmentation

Control Access to Views and Protocols: A VAST View is a multi-protocol representation of a network storage share, export, or bucket. The platform allows administrators to control which VLANs have access to specific Views and which protocols are allowed to be used when accessing the VIPs on those VLANs. This feature enhances security by ensuring that only authorized VLANs can access certain data and services. It is configured by using View Policies, which can specify access permissions based on VLANs.

- Section: VAST Cluster Documentation, “Creating View Policies” [p. 628]

Logical Tenancy

The VAST Data Platform offers several features related to multi-tenancy that enable secure isolation and management of tenants. Here are the key tenancy features along with detailed descriptions and the relevant sections from the VAST Cluster 5.1 Documentation:

Tenants

Description: Tenants in the VAST Data Platform define isolated data paths and can have their own authentication sources such as Active Directory (AD), LDAP, or NIS. Each tenant can also manage its own encryption keys, ensuring that data remains securely isolated from other tenants. This feature is crucial for multi-tenant environments where different organizations or departments need to maintain strict data separation.

- Section: Tenants (v5.1) [p. 251]

View Policies

Description: View Policies define access permissions, protocols, and security settings for Views assigned to tenants. These policies allow administrators to control who can access the data, what actions they can perform, and which protocols they can use. This granular control is essential for maintaining security and compliance in multi-tenant environments.

- Section: Managing Views and View Policies (v5.1) [p. 260]

VLAN Isolation

Description: VLANs can be bound to a specific tenant to further isolate traffic between tenants, preventing cross routing or broadcast traffic from occurring across the L2 boundary.

- Section: Tagging Virtual IP Pools with VLANs [p. 147]

Quality of Service (QoS)

Description: QoS policies provide granular performance controls for bandwidth and IOPs (input/output operations per second) for Views assigned to tenants. These policies ensure predictable performance and prevent resource contention issues, which is particularly important in multi-tenant environments where different tenants may have varying performance requirements. In addition to QoS maximum thresholds which help prevent performance exhaustion, QoS minimum thresholds are also available, to help prevent the noisy-neighbor problem of multi-tenancy.

- Section: Quality of Service (v5.1) [p. 323]

Quotas

Description: Quotas allow administrators to set capacity limits on Views and directories for tenant isolation. This feature ensures that no single tenant can consume more than their allocated share of resources, helping to prevent unexpected system capacity resource exhaustion.

- Section: Managing Quotas (v5.1) [p. 314]

Authorization and Identity Management

Tenant and Identity Management

Description: Tenants in the VAST Data Platform define isolated data paths and can have their own authentication sources such as Active Directory (AD), LDAP, or NIS. The platform supports up to eight unique identity providers that can be configured for use at the tenant level.

- Section: Tenants (v5.1) [p. 251]

Views

Description: Views are multi-protocol shares, exports, or buckets that belong to specific tenants. They provide securely isolated data access, ensuring that each tenant can only access their own data. Views can be configured with specific access permissions and protocols, making them versatile for different use cases.

- Section: Managing Views and View Policies (v5.1) [p. 260]

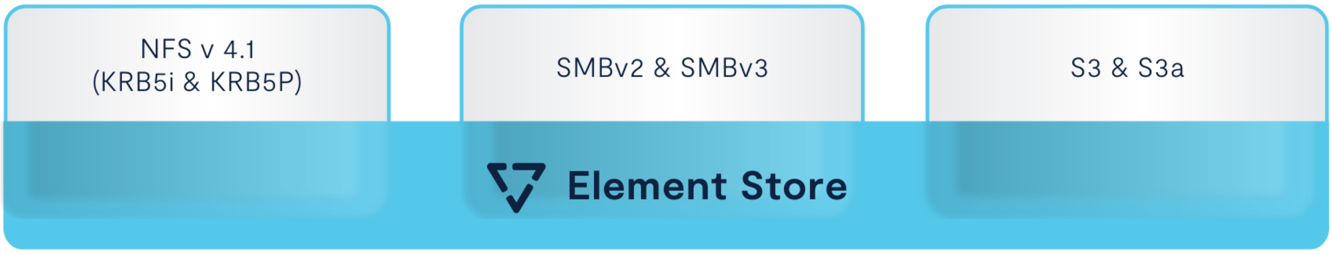
View Policies

Description: View Policies define access permissions, protocols, and security settings for views assigned to tenants. These policies allow administrators to control who can access the data, what actions they can perform, and which protocols they can use. This granular control is essential for maintaining security and compliance in multi-tenant environments.

- Section: Managing Views and View Policies (v5.1) [p. 260]

Access Control

The VAST Data Platform offers a comprehensive suite of features for authorization and identity management. Here are the detailed descriptions of each feature along with the relevant sections and page numbers from the VAST Cluster 5.1 Documentation:



VAST Element Store

Role-Based Access Control (RBAC)

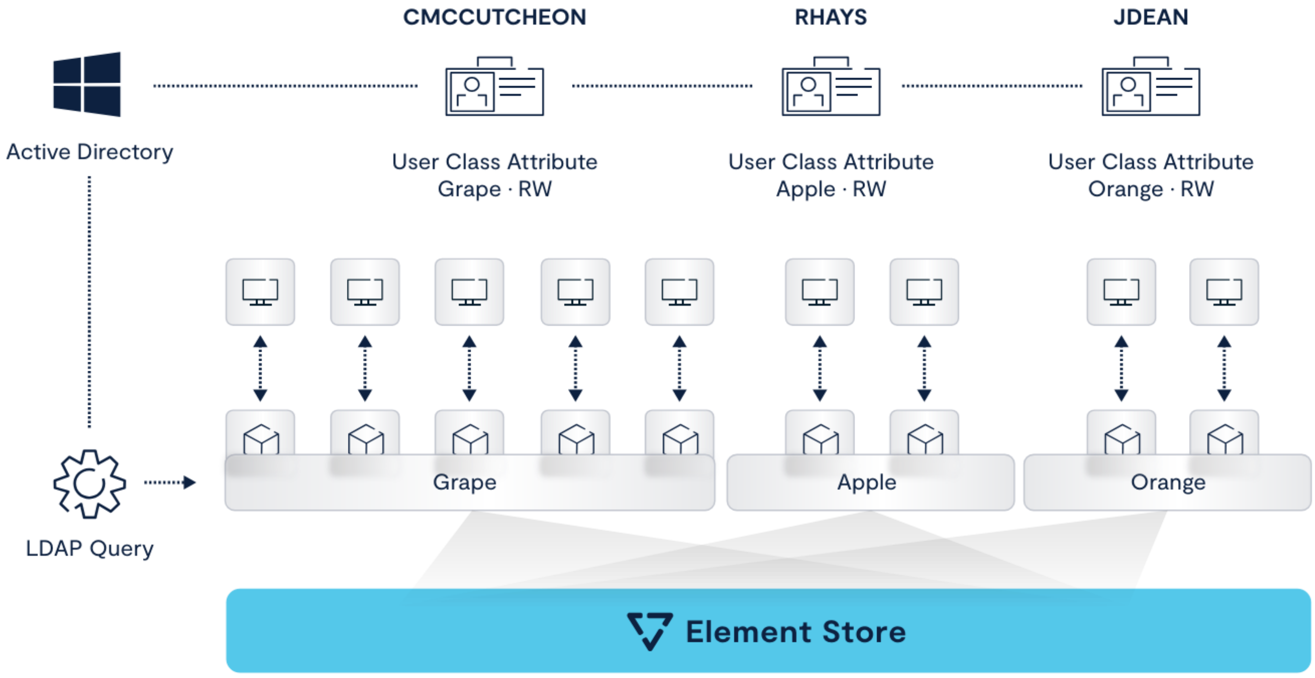
Description: VAST Cluster employs a Role-Based Access Control (RBAC) system for managing access to the VAST Management System (VMS). RBAC allows administrators to define roles with specific permissions and assign these roles to users. This ensures that users have access only to the resources and actions necessary for their roles, enhancing security and simplifying management.

- Section: Authorizing VMS Access and Permissions [p. 82]

Attribute-Based Access Control (ABAC)

Description: Attribute-Based Access Control (ABAC) is supported on views accessed via NFSv4.1 with Kerberos authentication or via SMB with Kerberos or NTLM authentication. ABAC allows access to a view if the user's account in Active Directory has an associated ABAC attribute that matches the ABAC tag assigned to the view. This provides fine-grained access control based on user attributes.

- Section: Attribute-Based Access Control (ABAC) [p. 269]



Hybrid ABAC + RBAC illustrated with example, tenants

Single Sign-On (SSO) Authentication

Description: VAST VMS supports Single Sign-On (SSO) authentication using SAML-based Identity Providers (IdP). This allows VMS managers to sign in to a VAST Cluster using their credentials from an IdP such as Okta, which can additionally provide multi-factor authentication (MFA) capabilities. SSO simplifies the login process and enhances security by centralizing authentication.

- Section: Configure SSO authentication in VMS [p. 90]

Active Directory Integration

Description: VAST Cluster supports integration with Active Directory (AD) for both VMS and data protocol user authentication and authorization. This allows organizations to leverage their existing AD infrastructure to manage user access to VAST Cluster resources. AD integration supports features such as SID History for groups and users, ensuring seamless access control.

- Section: Connecting to Active Directory (v5.1) [p. 347]

LDAP Integration

Description: The platform supports integration with LDAP servers for both VMS and data protocol user authentication and authorization. This allows organizations to use their existing LDAP directories to manage access to VAST Cluster resources, providing a flexible and scalable authentication solution.

- Section: Connecting to an LDAP Server (v5.1) [p. 342]

NIS Integration

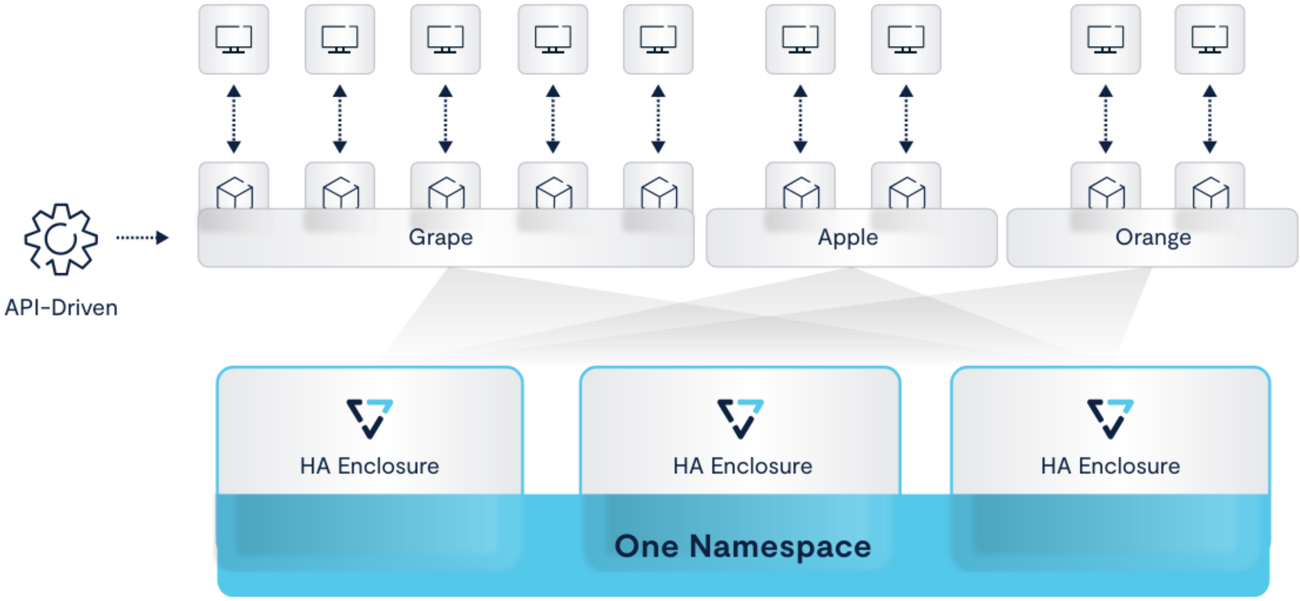
Description: VAST Cluster supports integration with Network Information Service (NIS) for data protocol user authentication. Thisfeature is useful for environments that rely on NIS for managing user information and access control.

- Section: Connecting to NIS (v5.1) [p. 358]

Local Users and Groups

Description: Administrators can manage local users and groups directly within the VAST Cluster. This includes creating, modifying, and deleting local user accounts and groups, as well as assigning permissions and roles to these accounts.

- Section: Managing Local Users (v5.1) [p. 335]
- Section: Managing Local Groups (v5.1) [p. 337]



VAST supports securely isolated tenants with QoS capabilities

Protocol ACLs and SELinux Labels

The VAST Data Platform supports various protocol ACLs and SELinux label features, ensuring robust access control and security. Here are the detailed descriptions of each feature along with the relevant sections and page numbers from the VAST Cluster 5.1 Documentation:

POSIX Access Control Lists (ACLs)

Description: VAST systems support POSIX ACLs, allowing administrators to define detailed permissions for files and folders beyond the simple Unix/Linux model. POSIX ACLs enable the assignment of permissions to multiple users and groups, providing flexible and granular access control.

- Section: NFS File Sharing Protocol (v5.1) [p. 154]

NFSv4 ACLs

Description: NFSv4 is a stateful protocol with secure authentication via Kerberos that supports detailed ACLs. These ACLs are similar in granularity to those available in SMB and NTFS, allowing for robust access control. NFSv4 ACLs can be managed using standard Linux tools over the NFS protocol.

- Section: NFS File Sharing Protocol (v5.1) [p. 154]

SMB ACLs

Description: SMB ACLs are managed in the same manner as Windows shares, allowing users to set fine-grained Windows ACLs through PowerShell scripts and Windows File Explorer over SMB. These ACLs, including deny list entries, can be enforced on users accessing via both SMB and NFS protocols simultaneously.

- Section: SMB File Sharing Protocol on VAST Cluster (v5.1) [p. 171]

S3 Identity Policies

Description: The S3 Native Security Flavor allows for the use of S3 Identity Policies to control access and the ability to set and change ACLs according to S3 rules. This feature provides granular access control for S3 buckets and objects.

- Section: S3 Object Storage Protocol (v5.1) [p. 182]

Multi-Protocol ACLs

Description: VAST supports multi-protocol ACLs, providing a unified permission model for accessing data across different protocols. This ensures consistent access control and security regardless of the protocol used to access the data.

- Section: Multi-Protocol Access (v5.1) [p. 151]

SELinux Label Features

1. NFSv4.2 Security Labels

Description: VAST Cluster 5.1 supports NFSv4.2 labeling in Limited Server Mode. In this mode, the VAST Cluster can store and return security labels of files and directories on NFS views of NFSv4.2-enabled tenants, but the Cluster does not enforce label-based access decision-making. Label assignment and validation are performed by NFSv4.2 clients.

- Section: NFSv4.2 Security Labels (v5.1) [p. 169]

Certificate Management and Encryption

The VAST Data Platform offers a comprehensive suite of features for encryption and certificate management. Here are the detailed descriptions of each feature along with the relevant sections and page numbers from the VAST Cluster 5.1 Documentation:

Data Encryption at Rest

Description: VAST Data Platform supports encryption of data at rest using external key management solutions. This feature ensures that data stored on the platform is securely encrypted with keys kept external to the VAST Cluster, protecting data from unauthorized access. The platform supports Thales CipherTrust Data Security Platform and Fornetix Vault Core for external key management. Each cluster has a unique master key, and encryption can be enabled during the initial setup of the cluster.

- Section: Data Encryption (v5.1) [p. 128]

FIPS 140-3 Level 1 Validation

The VAST Data Platform embeds the OpenSSL 1.1.1 Cryptographic Module, which is FIPS 140-3 Level 1 validated. The certificate number for this validation is #4675. All encryption for data in flight and at rest is linked to the FIPS validated OpenSSL 1.1.1 Cryptographic Module. The platform utilizes TLS 1.3 for secure data transmission and 256-bit AES-XTS encryption for data at rest, ensuring robust security and compliance with industry standards. Enhancing Data Security and Management with Multi-Category Security and Secure Tenancy 14

- Source: Cryptographic Module Validation Program (CMVP)

TLS Certificate Management

Description: The platform supports the installation and management of TLS certificates for securing communications
with the VAST Management System (VMS). Administrators can install TLS certificates to ensure that data transmitted
between clients and the VMS is encrypted and secure.

• Section: Installing an SSL Certificate for VMS (v5.1) [p. 78]

mTLS Authentication for VMS Clients

Description: The platform supports mutual TLS (mTLS) authentication for VMS GUI and API clients. When mTLS is enabled, VMS requires that the client present a certificate signed by a specific Certificate Authority. This adds a layer of mutual authentication, in which both the client and server authenticate each other, providing an additional layer of security for communications with the VMS to optionally support PIV/CAC Cards.

- Section: Enabling mTLS Authentication for VMS Clients (v5.1) [p. 78]

Securing Active Directory Communication

The VAST Data Platform provides robust security measures for Active Directory (AD) authentication by allowing administrators to disable NTLM v1 and v2 protocols. NTLM (NT LAN Manager) is an older authentication protocol that has known vulnerabilities, making it less secure compared to more modern protocols like Kerberos.

- Section: Connecting to Active Directory (v5.1) [p. 347]

Securing S3 Access

The VAST Data Platform enhances the security of S3 access by allowing you to disable Signature Version 2 (SigV2) signing, ensuring that all S3 interactions are conducted using the more secure Signature Version 4 (SigV4). Additionally, the platform enforces the use of TLS 1.3 for S3 communications, leveraging FIPS 140-3 validated ciphers.

- Section: S3 Object Storage Protocol (v5.1) [p. 182]

Crypto Erase

Description: Crypto erase is a method to remove a tenant’s data from a VAST system. This is done by revoking or deleting the tenant’s keys using either the VAST system or the External Key Manager. The VAST system will purge the Data Encryption Keys (DEKs) and Key Encryption Keys (KEKs) from system RAM, thereby immediately removing access to all data written using those keys. The VAST system can then erase the encrypted data. This feature provides a method to securely delete data in case of data spillage or when a tenant leaves the platform.

Section: Data Encryption (v5.1) [p. 128]

Catalog and Audit

The VAST Data Platform offers a comprehensive suite of features for auditing and cataloging, ensuring robust data management and compliance. Here are the detailed descriptions of each feature along with the relevant sections and page numbers from the VAST Cluster 5.1 Documentation:

Protocol Auditing

Description: Protocol auditing in the VAST Data Platform logs operations that create, delete, or modify files, directories, objects, and metadata. It also logs read operations and session activities. This feature helps in tracking user activities and ensuring compliance with security policies. Administrators can configure global auditing settings and view audit logs through the VAST Web UI or CLI.

- Section: Protocol Auditing Overview [p. 243]
- Section: Configuring Global Auditing Settings [p. 243]
- Section: Configuring Auditing with View Policies [p. 245]
- Section: Audited Protocol Operations [p. 245]
- Section: Viewing Protocol Audit Logs [p. 248]

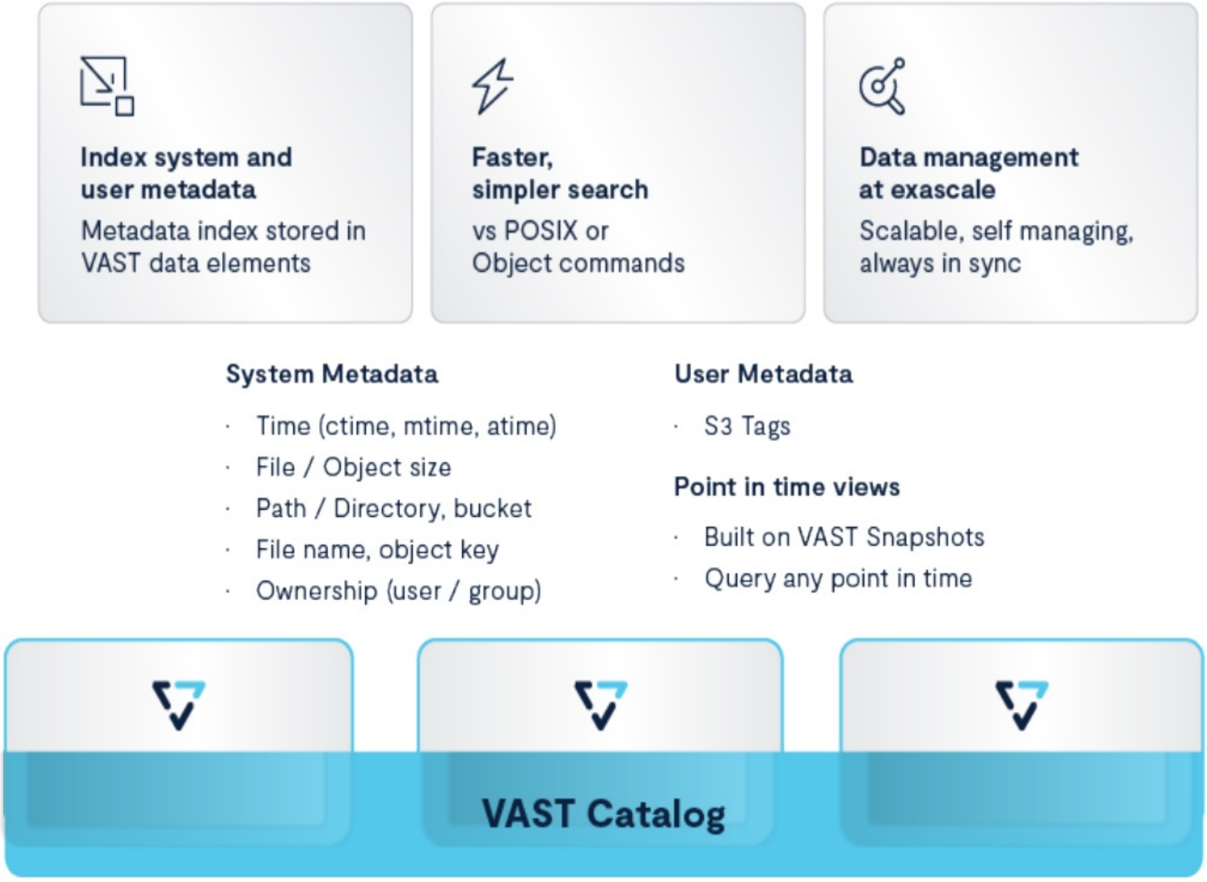
Storing Protocol Audit Logs in VAST Database Tables

Description: VAST Data Platform allows the configuration of VMS to store protocol audit logs in a VAST Database table. Log entries are stored as JSON records, which can be viewed directly from the VAST Web UI in the VAST Audit Log page. This feature enhances the ability to perform detailed audits and analyses of user activities.
Section: Storing Protocol Audit Logs in VAST Database Tables [p. 25]

VAST Catalog

Description: The VAST Catalog is a built-in metadata index that allows users to search and find data quickly. It treats the file system like a database, enabling next-generation AI and ML applications to use it as a self-referential feature store. The catalog supports SQL-style queries and provides an intuitive WebUI, a rich CLI, and APIs for interaction.

- Section: VAST Catalog Overview [p. 489]
- Section: Configuring VAST Catalog [p. 491]
- Section: Querying VAST Catalog from the VAST Web UI [p. 492]
- Section: Providing Client Access to VAST Catalog CLI [p. 493]



VAST Catalog metadata index is fully integrated into the VAST Data Platform

VAST DataBase

Description: The VAST DataBase extends the capabilities of the VAST Catalog by storing more complex content in a fully featured database. It supports high-speed and massive data queries, storing data in an efficient columnar format similar to Apache Parquet. The database is designed for real-time, fine-grained queries into vast reserves of tabular data and cataloged metadata.

- Section: VAST DataBase Overview [p. 495]
- Section: Configuring the VAST Cluster for Database Access [p. 499]
- Section: VAST Database CLI Quick Start Guide [p. 494]

Audit Log Record Fields

Description: The audit log record fields provide detailed information about each logged event, including the type of operation, user details, timestamps, and affected resources. This detailed logging is crucial for compliance and forensic analysis.

- Section: Audit Log Record Fields [p. 250]

Viewing Protocol Audit Logs

Description: Administrators can view protocol audit logs through the VAST Web UI or CLI. The logs provide insights into user activities and system operations, helping to ensure compliance and detect any unauthorized actions.

- Section: Viewing Protocol Audit Logs [p. 248]

Maintained and Secured Operating System

The VAST Data Platform employs a comprehensive approach to securing its operating system, ensuring robust protection and compliance with industry standards. Here are the key aspects of the operating system and the security measures implemented:

Maintained Operating System

Description: VAST Data Platform uses a maintained operating system provided by CIQ, specifically Enterprise Rocky 8, which is a RHEL binary-compatible operating system image. CIQ’s Mountain Platform delivers a secure, authoritative, and highly scalable image, package, and container delivery solution available on both public cloud and on-premises.

Regular Patching and Vulnerability Management

Description: VAST ensures the operating system is regularly patched and updated by staying informed about the latest security vulnerabilities, applying necessary patches, and implementing appropriate mitigations in a timely manner. This proactive approach helps maintain the security posture of the operating system.

Continuous Monitoring

Description: Continuous monitoring practices are implemented to maintain the security posture of the operating system. This includes regular assessments, audits, and reviews of the system’s security controls and configurations, as well as enabling logging for suspicious activities and potential security incidents.

DISA STIG Compliance

Description: The VAST Data Platform supports the DISA STIG (Security Technical Implementation Guide) for RedHat Linux 8, MAC 1 Profile – Mission Critical Classified. This compliance ensures that the operating system adheres to rigorous security standards required by customers in regulated environments.

Configuration Management

Description: The platform maintains a baseline configuration for RHEL 8 systems, including settings for system components, file permissions, and software installation. It also implements change control processes to track, review, and approve changes to the system configuration, ensuring that systems adhere to a secure and standardized configuration.

Least Functionality

Description: The principle of least functionality is emphasized by recommending the removal or disabling of unnecessary software, services, and system components. This reduces potential vulnerabilities and attack vectors.

System and Information Integrity

Description: The platform's encryption and key management features, as well as its integration with SIEM systems, help ensure the integrity of data and information. This includes regular security assessments, penetration testing, and vulnerability management to ensure up-to-date security patches, configurations, and best practices.

Secure Software Supply Chain

Ensuring a secure software supply chain is critical for compliance with regulations such as the Trade Agreements Act (TAA), Federal Acquisition Regulation (FAR), and ISO standards. The VAST Data Platform implements comprehensive measures to secure its software supply chain, ensuring that software is developed correctly and meets stringent security requirements.

Secure Software Development Framework (SSDF)

The VAST Data Platform adopts the NIST Secure Software Development Framework (SSDF), which provides guidelines for secure software development. This framework helps protect software supply chains against risks by outlining practices for secure coding, vulnerability management, and continuous monitoring.

Software Composition Analysis (SCA)

Tools like GitLab are utilized for Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) to analyze both proprietary and open-source code for vulnerabilities. This is crucial for identifying security weaknesses before deployment.

Software Bill of Materials (SBOM)

The platform generates and manages SBOMs to track components used in software development. GitLab and Artifactory are leveraged in the pipeline to enhance transparency and compliance with Executive Order 14028.

Continuous Integration and Continuous Deployment (CI/CD) Pipeline

A CI/CD pipeline incorporates security testing, code review, and compliance checks. The pipeline is hosted on a U.S.- based cloud platform to meet TAA/FAR requirements, ensuring that all operations are performed within the U.S. and managed by U.S. entities.

Container and Package Signing

Digital signing of containers and packages is implemented to ensure integrity and authenticity. Docker Content Trust and RPM signing are recommended practices for securing containerized applications and package distributions.

Vulnerability and Compliance Scanning

Tools such as Tenable and Qualys are used for scanning operating systems and build packages, as well as for virus and malware detection. These tools are incorporated into the pipeline to identify and mitigate potential threats in the software environment.

Third-Party Software Management

All third-party software, whether open-source or proprietary, is sourced from U.S. locations to comply with TAA/FAR regulations. This software is included in the SAST and DAST scanning processes to ensure security.

Documentation and Audit Trails

Comprehensive documentation of the entire process from code check-in to the downloadable package used by customers is maintained. This documentation is accessible under NDA for audits and validations by customers, as required by leadership.

Employee and Asset Management

The process is managed by employees of the U.S. entity (Vast Federal), and all assets used in the software development and deployment process are owned by this entity. This compliance is crucial for meeting federal acquisition regulations.

Secure Development Environment

The software is developed and built in secure environments, with measures such as multi-factor authentication, conditional access, and encryption of sensitive data. Regular logging, monitoring, and auditing of trust relationships are enforced.

Trusted Source Code Supply Chains

Automated tools or comparable processes are used to validate the security of internal code and third-party components, managing related vulnerabilities effectively.

Security Vulnerability Checks

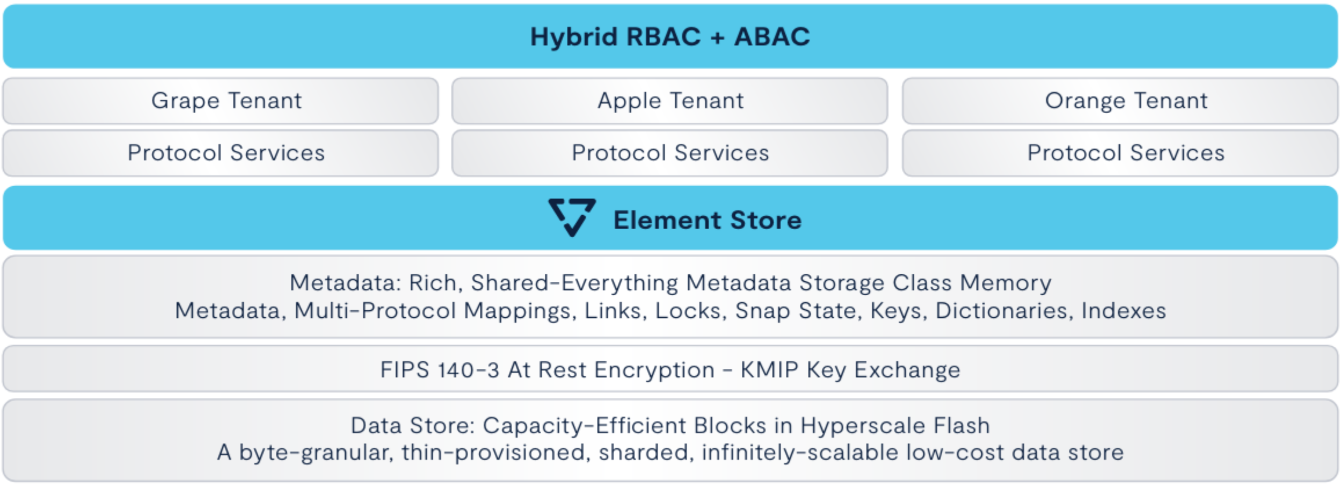
Ongoing vulnerability checks are conducted before releasing new products, versions, or updates. A vulnerability disclosure program is maintained to assess and address disclosed software vulnerabilities promptly.

Conclusion

The integration of Multi-Category Security (MCS) with secure tenancy features provides a robust framework for enhancing the confidentiality and security of unstructured data. By leveraging MCS, organizations can assign specific categories to files, ensuring that only authorized processes and users can access sensitive information. This additional layer of security is crucial for protecting unstructured data such as documents, images, and videos.

Secure tenancy further strengthens data isolation by creating distinct environments for different groups, departments, or organizations within the same infrastructure. Key aspects such as resource isolation, data segregation, network segmentation, and granular access controls ensure that each tenant’s data remains private and secure. The VAST Data Platform exemplifies these principles through its comprehensive suite of features, including VLAN tagging, role-based and attribute-based access controls, and robust encryption mechanisms.

In summary, the VAST Data Platform, with its integration of MCS and secure tenancy, provides a comprehensive and secure solution for managing unstructured data. This approach is essential for organizations with stringent data confidentiality requirements, such as government agencies, financial institutions, and healthcare providers. By implementing these advanced security measures, organizations can confidently protect their sensitive data while enabling efficient and scalable data management. This conclusion maintains the key points while ensuring clarity and conciseness.



Hybrid RBAC + ABAC

Grape Tenant	Apple Tenant	Orange Tenant
Protocol Services	Protocol Services	Protocol Services

Element Store

Metadata: Rich, Shared-Everything Metadata Storage Class Memory
Metadata, Multi-Protocol Mappings, Links, Locks, Snap State, Keys, Dictionaries, Indexes

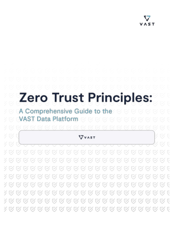
FIPS 140-3 At Rest Encryption - KMIP Key Exchange

Data Store: Capacity-Efficient Blocks in Hyperscale Flash
A byte-granular, thin-provisioned, sharded, infinitely-scalable low-cost data store

The VAST Data Platform architecture facilities MCS deployments

For more information on the VAST Data Platform and how it can help you solve your application problems, reach out to us at hello@vastdata.com.

Documents / Resources

 Enhancing Data Security and Management with Multi-Category Security and Secure Tenancy: A Comprehensive Guide to the VAST Data Platform	VAST Data Platform Software [pdf] User Guide Data Platform Software, Platform Software, Software
 Zero Trust Principles: A Comprehensive Guide to the VAST Data Platform	VAST Data Platform Software [pdf] User Guide Data Platform Software, Platform Software, Software

References

- User Manual