VAST Cluster 5.3 Release Notes

22 April 2025

Always check support.vastdata.com for the latest

Contents

VAST Cluster 5.3.0 Release Notes

VAST Cluster 5.3.0 is released to General Availability as of April 2025.

To access this release, contact the VAST Customer Success team via a support ticket, Slack, or by sending an email to support@vastdata.com.

Upgrade to VAST Cluster 5.3.0 is supported from VAST Cluster 5.2.0 to 5.2.0-SP20. Direct upgrade from pre-5.2 versions is not supported. To upgrade from a pre-5.2 version, begin by upgrading to VAST Cluster 5.2, and then upgrade to VAST Cluster 5.3.0.

For scale related information, see *VAST Cluster Scale Guidelines*.

New Features in 5.3.0

- NETWORKING
  - Support for Layer 3 Networking
- PROTOCOLS
  - Block Storage Support
  - S3 Indestructible Object Mode
- MULTI-TENANCY
  - Storage Administration by VAST Tenants
  - Tenant Capacity Limits
  - Tenant Client Metrics
- QUALITY OF SERVICE
  - Workload Prioritization
- VAST DATA ENGINE
  - VAST Data Broker
- VAST DATABASE
  - Support for Database Views
- GLOBAL ACCESS
  - Global Access to S3 Buckets

- AUTHENTICATION & AUTHORIZATION
  - Multiple Local Auth Providers
  - User Impersonation
- VMS
  - VMS Token-Based Authentication
- PLATFORM & CONTROL
  - Conversion to Write Buffer RAID
- VAST DRIVERS
  - New VAST Drivers to Enable Block Storage Access

Support for Layer 3 Networking

VAST Cluster 5.3 supports Layer 3 networking for its data network, allowing cluster nodes to be directly connected to a switch with L3 routing capabilities. The CNodes act as BGP (Border Gateway Protocol) peers belonging to a VAST Autonomous System (AS) that is connected to an upstream AS.

L3 access can be enabled or disabled per virtual IP pool.

The following user controls have been added for this feature:

- In VAST Web UI:
  - The Network Access -> BGP Configurations page where you can set up BGP for the cluster
  - The Network Access -> BGP Connections page that lists all cluster's BGP connections with their status and details
  - Options to enable L3 access and select a BGP configuration in virtual IP pool settings (Network Access -> Virtual IP Pools -> choose to create or edit a pool -> Advanced tab), as well as in DNS settings (Network Access -> DNS -> choose to create or edit DNS)
- In VAST CLI:
  - The `--enable-l3` and `--disable-l3` options on the `vippool create` command
  - The `--vast-asn`, `--peer-asn` options on the `vippool create` and `vippool modify` commands

The following limitations apply:

- After enabling L3 access for a virtual IP pool, it cannot be disabled.
- L3 access is not supported on virtual IP pools for which CNode Port Affinity is configured.
- L3 networking is not supported on IB clusters.
- L3 networking is not available for VAST on Cloud.
- MD5 authentication is not supported.
- Numbered BGP is not supported.

For more information about this feature, see *VAST Cluster Administrator's Guide*.

Block Storage Support

VAST Cluster 5.3.0 adds support for block storage devices based on NVMe/TCP.

To expose a block device, create a new Element Store view and enable the new *Block* access protocol for it. The view acts as an NVMe subsystem. You can create volumes (NVMe namespaces) on that view and associate (map) them with hosts that you define.

The following user controls have been added for this feature:

- In VAST Web UI:
  - Option to enable the Block access protocol in the Protocols field of view settings (Element Store -> Views -> choose to create a view -> General tab)
  - The new Block tab in view settings to manage block protocol configuration
  - New grid pages to view and manage volumes (Element Store -> Volumes) and hosts (Element Store -> Hosts)
- In VAST CLI:
  - A new BLOCK value for the `--protocols` option on the `view create` command
  - Volume management commands: `volume create`, `volume modify`, `volume delete`, `volume list`, `volume show`, `volume get_snapshots`, `volume fetch-capacity`
  - Host management commands: `blockhost create`, `blockhost modify`, `blockhost delete`, `blockhost list`, `blockhost show`
  - Commands to associate block volumes with host: `blockmapping show`, `blockmapping list`, `blockmapping map_host_to_volumes`, `blockmapping unmap_host_volumes`, `blockmapping map_volume_to_hosts`, `blockmapping unmap_volume_hosts`, `blockmapping map_volume_path`, `blockmapping unmap_volume_path`
  - The `--set-is-default-subsystem` and `--reset-is-default-subsystem` options on the `view create` and `view modify` commands
  - The `--nqn` filter on the `view list` command to list block-enabled views

The following requirements and limitations apply:

- For Rocky Linux-based clients, VAST recommends that the client uses Rocky Linux 9.4 or later.
- If a host defined on the VAST cluster does not have any volumes mapped to it, NVMe auto-discovery does not show this subsystem.
- A view that is used to expose block storage cannot have other storage protocols enabled.
- You cannot enable or disable block storage support on an existing view. Block storage support can only be enabled for a view during view creation and cannot be disabled afterwards.
- Block devices can be created on empty directories only.
- Nesting of a block view inside an existing block view is not allowed.
- The host NQN cannot be modified. To change the NQN, you need to remove the host and then add and map it anew.
- When using the VAST Web UI or CLI options to bulk create volumes or hosts, the number of items to be created cannot

exceed 256. When mapping hosts to volumes, up to 256 items can be mapped at a time.

- The following VAST capabilities are not available with block views:
  - Access control features (such as ABE, ABAC, WORM)
  - VAST Audit Log
  - Replication to a remote peer
  - Global Access
  - Remote Global Snapshot Clones
- Snapshots on local protected paths are allowed but replication on non-local protected paths is not supported.
- An attempt to remove a volume that has snapshots may cause errors for volume objects of snapshots of that volume, if they exist.
- The maximum IO block size is limited to 1MB (4GB for unmap).

Known issues include:

- ORION-245989: Bulk operations on volumes performed by a cluster admin, cannot be tracked by a tenant admin in the Activities page of VAST Web UI.
- ORION-237444: An attempt to create a block view with the same name as a previously deleted block view fails with a `CreateDirResultCode.ALREADY_EXISTS` error.

For more information about this feature, see *VAST Cluster Administrator's Guide*.

S3 Indestructible Object Mode

Indestructible Object Mode protects objects in an S3 bucket from being altered (including any change in the object's metadata) or removed during a specified period of time.

After this capability has been enabled for the cluster, Indestructible Object Mode can be enabled per view. To disable indestructible object configuration or modify its effective period, the cluster needs to be unlocked.

The following user controls have been added for this feature:

- In VAST CLI, the the `--enable-indestructible-object` and `--indestructible-object-duration` options on the `cluster modify` command
- In VAST Web UI, a new pane in view settings, Indestructible Object Mode, where you can enable the mode for the view and set the mode effective period (Element Store -> Views -> choose to create or edit a view)
- In VAST CLI, the `--enable-indestructible-object` and `--indestructible-object-duration` options on the `view create` and/or `view modify` commands.

The following limitations apply:

- An S3 Bucket view with Indestructible Object Mode cannot have other protocols enabled.
- Indestructible Object Mode cannot be set for a view that points to / (root directory).
- It is not allowed to have views under the view in Indestructible Object Mode, or at the same path as the Indestructible Object Mode view.

- Indestructible Object Mode cannot be used together with S3 Object Locking or S3 Object Versioning.
- Indestructible Object Mode cannot be set for a view that exposes the protocol audit log directory.
- Views in Indestructible Object Mode are not subject to replication or Global Access.

For more information about this feature, see the *VAST Cluster Administrator's Guide*.

Storage Administration by VAST Tenants

VAST Cluster 5.3 offers a new level of multi-tenancy support. Each VAST tenant is provided with an ability to monitor and manage their storage resources through the cluster's VMS. The tenant admin capabilities include:

- Monitor tenant storage using VAST capacity reports, Top Actors analytics, and Data Flow visualizations
- Manage users that belong to the tenant and monitor their activities
- Manage protected path and protection policies
- Set up and run replication and Global Access (based on cluster peer configuration created by the cluster admin)
- Manage the tenant's VAST Databases
- Manage tenant's VAST Catalog and VAST Protocol Audit logs

Note

Managing the cluster hardware is not included in tenant admin capabilities.

To access the new self-manage capabilities, the tenant admin needs to log in to the VMS using their own credentials, which can be set up by the cluster admin.

The cluster admin manages the cluster as a whole, including the following:

- Create and manage cluster tenants
- Set capacity and performance quotas for the tenants
- Configure cluster networking (virtual IP pools, DNS)
- Set up replication peers for the cluster and map tenants between clusters

The following user controls have been added for the cluster admin to manage cluster and tenant admins and their permissions:

- To designate Active Directory or LDAP user groups as groups of cluster admins:
  - In VAST Web UI, the Cluster admin groups option in the provider settings (User Management -> Active Directory or LDAP -> choose to create or edit a provider -> Advanced tab)
  - In VAST CLI, the `--super-admin-groups` option on the `activedirectory create`, `activedirectory modify`, `ldap create`, `ldap modify` commands
- To designate an Active Directory or LDAP user group as a group of tenant admins for a specific tenant:

    - In VAST Web UI, the Admins group field in tenant settings (Element Store -> Tenants -> choose to create or edit a tenant -> VMS Login tab)
    - In VAST CLI, the `--tenant-admins-group-name` option on the `tenant create` and `tenant modify` commands.
- To designate a VMS user as a cluster or tenant admin:
    - In VAST Web UI, the Cluster Admin and Tenant Admin options in manager settings (Administrators -> Managers -> choose to create a manager)
    - In VAST CLI, the `--user-type` option on the `manager create` and `manager delete` command.
- To associate a role with an admin type and a tenant:
    - In VAST Web UI, the Cluster Admin and Tenant Admin options and the User Type field in role settings (Administrators -> Roles -> choose to create a role)
    - In VAST CLI, the `--tenant-id` option on the `role create` command.
- To associate a realm with a tenant:
    - In VAST Web UI, the Tenant field in realm settings (Administrators -> Realms -> choose to create a realm)
    - In VAST CLI, the `--tenant-id` option on the `realm create` command.
- To set Tenant Privacy mode, in which cluster admins cannot view details (views, users, data protection configurations, and so on) about any tenants, except for the default tenant:
    - In VAST Web UI, the Enable tenant privacy option in VMS settings (Settings -> VMS -> General -> Tenant Privacy pane).

Tenant Capacity Limits

You can limit storage capacity available for a tenant by specifying soft and hard capacity limits, expressed in capacity units of measure such as GB or TB, and also by setting a limit on the number or files and directories that can be created for this tenant.

The following user controls have been added for this feature:

- In VAST Web UI, capacity limits can be set in the Capacity rules pane of the new Tenant Limits tab in tenant settings (Element Store -> Tenants -> choose to create or edit a tenant).
- In VAST CLI, the `--capacity-rules` option on the `tenant create` and `tenant modify` commands.

Collection of Tenant Client Metrics

VAST Cluster can collect statistics on tenant's NFS client operations based on user-defined metadata and present the collected data for analysis. The information is collected by the VAST NFS Collector that is deployed on the client. Collected data is stored in a VAST Database table and can be analyzed as a graph in VAST Web UI or by querying the table directly.

This feature can be enabled or disabled per tenant.

The following user controls have been added for this feature:

- In VAST Web UI, the new Client Metrics page (Analytics -> Client Metrics) where you can enable the feature for one or more tenants, set up the metrics to be collected, and view the metrics graph(s).

- In VAST CLI, the `tenant show-client-metrics` and `tenant update-client-metrics` commands

The following limitations apply:

- NFSv3 and NFSv4 are the only access protocols supported.

For more information about this feature, see *VAST Cluster Administrator's Guide*.

Workload Prioritization

VAST Cluster provides options that help prioritize workloads and eliminate unexpected performance degradation among views controlled with QoS policies:

- You can define a cluster-wide maximum write bandwidth to help prevent situations where workloads do not achieve the expected QoS because of extensive media consumption by other workloads.

  The recommended cluster-wide maximum is 70% of the cluster's total write bandwidth.

  To define a cluster-wide maximum write bandwidth:

  - In VAST Web UI, go to the Global Write BW Limit pane in cluster settings (Settings -> Cluster -> General Cluster Setup and Actions tab). Select Set Manually and enter the write bandwidth limit in the provided fields.
  - In VAST CLI, run the `cluster modify` command with the `--max-cluster-write-bw-mb` option specified.

- You can set the prioritization flag for a view QoS policy in order to prioritize the workloads in contention for both CPU and memory resources beyond the limits defined for the tenant and/or for the cluster.

  To set the prioritization flag for a QoS policy:

  - In VAST Web UI, enable the Prioritize policy over cluster or tenant limitations option in QoS policy settings (Element Store -> QoS Policies -> choose to create or edit a QoS policy -> View tab).
  - In VAST CLI, run the `qospolicy create` or `qospolicy modify` command with the `--is-gold` option specified.

Tip

Since prioritized workloads are not restricted by the tenant or cluster-wide limits, it is recommended to set a maximum limit for such workloads within the QoS policy.

The following limitations apply:

- The prioritization flag is supported for view QoS policies. It cannot be set for user QoS policies.
- S3 (including Kafka and VAST Database) and block storage I/Os are not calculated as part of the cluster-wide maximum write bandwidth limit.
- Some high-priority optimizations are applied to NFSv3 only.
- When the cluster-wide maximum write bandwidth is set, the actual performance may be ±15% of the expected performance.
- Use of QoS with RDMA is not supported.

For more information about QoS and workload prioritization, see *VAST Cluster Administrator's Guide*.

VAST Event Broker

In addition to publishing events to third-party event brokers such as Apache Kafka, VAST Cluster now features its own broker implementation, the VAST Event Broker.

VAST Event Broker is based on the VAST Database, which allows for querying Kafka topics via various database APIs.

The VAST implementation of the Kafka protocol supports a basic subset of the Kafka APIs to allow clients to publish and consume events from the VAST Event Broker:

- Producer API
- Consumer API
- Consumer groups
- Database queries on topics
- Admin API (create topics, delete topics and consumer groups)

You set up Kafka per view. Each Kafka-enabled view has to have one virtual IP pool assigned to it. The virtual IP pool must have enough virtual IPs so that there is at least one virtual IP per CNode.

The following user controls have been added for this feature:

- In VAST Web UI, in view settings (Element Store -> Views -> choose to create a view):
  - The Kafka protocol can now be selected for a view (General tab -> Protocols field).
  - The new Kafka tab lets you assign a virtual IP pool to the view.
- In VAST CLI:
  - The `KAFKA` keyword for the `--protocols` option on the `view create` command
  - The `--kafka-vip-pools` option on the `view create` command
  - New commands to manage event topics: `topic create`, `topic modify`, `topic delete`, `topic list`, `topic show`.

The following limitations apply:

- Producer API:
  - Messages are limited to 1MB.
  - In the event record, the key is limited to 126KB and the value is limited to 126KB.
  - Access to topics by UUID is not supported.
  - Idempotent producing is not supported.
  - Automatic creation of topics is not supported.
- Consumer API:
  - No more than 256 consumer groups per view (broker)
  - The following is not supported:

        - Consumer group stickiness parameters (such as `group.instance.id`)
        - READ UNCOMMITTED isolation level
        - Cooperative rebalancing
        - Client rack awareness
        - Fetch sessions (only full fetch will be applied), delayed fetch parameters
        - Seek by time
- Admin API:
    - Supported APIs include the APIs to create topics, delete topics, and to delete groups.
    - Only the following topic parameters are supported:
        - Number of partitions
        - Topic retention period
- The following Kafka capabilities are not supported:
    - Over-the-wire compression of messages

      

      Tip

      VAST compression of data is supported.
    - Topic compaction
    - Automatic creation of topics
    - Authentication and authorization
    - SSL
    - Transactions
- Only one virtual IP pool can be associated with a Kafka-enabled view, providing at least one virtual IP per CNode. Once the view has been created, the virtual IP pool cannot be replaced by another one (but it can be modified if needed).
- A topic can have up to 1000 partitions. The number of partitions in a topic cannot be changed after the topic has been created.
- Event queries based on the topic partition are not supported.
- When listing consumer groups, the response is limited to 256 groups per Kafka-enabled view.
- VAST replication of consumer groups is not supported.
- Event publishing and consuming operations, as well as topic management operations are not subject to VAST Protocol Auditing or Quality of Service (QoS).

For more information about VAST Event Broker, see *VAST Cluster Administrator's Guide*.

Support for Database Views

VAST Cluster 5.3 supports creation and management of database views (stored results of queries that present part of the database and can be queried). Clients connecting to a VAST Database can now create database views, list views in the database, get details of a view, redefine a view (Spark only), query a view, and rename a view. Permissions for database view operations are managed through identity policies.

The following limitations apply:

- View properties are not supported.
- Queries to a view must include full table names.
- Redefining a view is supported for Spark clients only.
- User-defined column names and comments are lost if the schema of the query changes when redefining a view.
- Nested data types are not supported.

For more information about this feature, see *VAST Cluster Administrator's Guide*.

Global Access for S3 Buckets

VAST Cluster 5.3 adds support for the S3 protocol in Global Access, subject to the following rules and limitations:

- Identity policies must be enabled at the cluster to which they get replicated.
- The following VAST capabilities are not supported on destination buckets:
  - S3 event notifications
  - S3 Indestructible Object Mode
  - Lifecycle policies
  - Write Once Ready Many (WORM)
- Bucket logging is only supported if both the source and destination buckets are in the same protected path.
- Bucket replication between two clusters is only supported when the bucket is associated with the default S3 view policy.
- S3 endpoints are not replicated.

Note

Before configuring Global Access for S3, it is recommended to enable bucket replication on both origin and satellite clusters (Settings -> S3 -> enable Bucket Replication). Note that once enabled, bucket replication cannot be disabled.

For more information about this feature, see *VAST Cluster Administrator's Guide*.

Multiple Local Authentication Providers

Local providers let you manage users and groups on the VAST cluster without the need to connect an external authentication and authorization provider, such as Active Directory or LDAP. VAST Cluster 5.3 offers an ability to create multiple local providers and associate each provider with one or more tenants.

During upgrade to VAST Cluster 5.3, a default local provider is automatically created to include all local users and groups that existed prior to the upgrade. All new local users and groups must be associated with a local provider when they are created. When a new tenant is created, VAST Cluster automatically creates a local provider associated with it.

To manage local providers:

- In VAST Web UI, choose User Management -> Local Providers to open the Local Providers page where you can view, create and modify local providers, and also view users and groups associated with a provider.
- In VAST CLI, use the `localprovider create`, `localprovider modify`, `localprovider delete`, `localprovider list` and `localprovider show` commands.

To associate a local provider with a tenant, select Vast Provider in tenant settings in VAST Web UI (Element Store -> Tenants -> choose to create or edit a tenant -> Providers tab), or run the VAST CLI `tenant create` or `tenant modify` command with the `--local-provider-id` option specified.

To associate a user or group with a local provider, select a provider in the new Local provider field in user or group settings in VAST Web UI (User Management -> Users or Groups -> choose to create a user or a group), or run the `user create` , `user modify`, `group create` or `group modify` command with the `--local-provider-id` option specified.

To copy user accounts from one local provider to another, use the VAST CLI `user copy` command or the VAST REST API endpoint `/users/copy/`.

For more information about this feature, see *VAST Cluster Administrator's Guide*.

User Impersonation

User impersonation lets you handle client users' requests against an NFS export or SMB share using with a preconfigured impersonator user account. When a client user creates or accesses a file or directory stored on the VAST cluster, the operation is handled as though it is performed by the impersonator.

The following user controls have been added for this feature:

- In VAST Web UI, the User Impersonation tab in view settings (Element Store -> Views -> choose to create or modify a view)
- In VAST CLI, the following options on the `view create` and `view modify` commands:
  - `--enable-user-impersonation` and `--disable-user-impersonation`
  - `--user-impersonation-username`, `--user-impersonation-identifier` and `--user-impersonation-identifier-type`

The following limitation applies:

- ORION-216379: When VAST protocol auditing is enabled on a user-impersonated view, only UID of the original user is included in the log. The user's login name and SID are not included.

For more information about this feature, see *VAST Cluster Administrator's Guide*.

VMS API Token-Based Authentication

VAST Cluster 5.3 supports token-based authentication for VMS manager users accessing the VMS API. With token-based authentication, requests are authenticated with a unique token included in the HTTP Authorization header as `Api-Token`.

VMS provides an ability to create, modify and revoke authentication tokens, as well as to display effective and archived tokens. Token-related activities can be tracked using VAST Audit logs.

API tokens can be managed using the following VAST CLI commands: `apitoken create`, `apitoken modify`, `apitoken revoke`, `apitoken list`, `apitoken show`. To set a maximum number of tokens per VMS manager user, use the `vms set_max_api_tokens_per_user` VAST CLI command.

The following limitation applies:

- ORION-212118: If a wrong VMS authentication token is passed, the cluster responds with `403 FORBIDDEN` but not with `401 UNAUTHORIZED`.

For more information about this feature, see *VAST Cluster Administrator's Guide*.

Conversion to Write Buffer RAID

For clusters upgrading from a pre-5.1 release, VAST Cluster 5.3 offers an option to convert DBox write buffers from mirrored layout (an older layout used on pre-5.1 clusters) to RAID-6, which provides increased write performance and storage efficiency.

The conversion is a one-time activity that does not interfere with normal cluster operation. Once started, the conversion cannot be stopped and is irreversible. It may take several hours, depending on the number of DBoxes.

Before starting the process, ensure that the cluster is not busy with any rewrite operations (such as encryption or similarity-based reduction), cluster expansion, DBox migration or replacement activities, or cluster upgrades.

The following user controls have been added for this feature:

- In VAST Web UI, the Activate Write Buffer RAID option in cluster settings (Settings -> Cluster -> Data Management)
- In VAST CLI, the `--enable-write-buffer-raid` and `--disable-write-buffer-raid` options on the `cluster create` and `cluster modify` commands
- In VAST CLI, the `--force-wbr-rewrite` flag on the `cluster create` command to forcefully run the rewrite process even when there are failed devices.

The following limitations apply:

- Conversion from VAST releases prior to 3.4 is not supported.
- This capability is not supported for clusters with TLC drives, and also for VAST on Cloud clusters.
- The cluster must include the following minimum number of DBoxes:

DBox Type	DBox HA enabled	DBox HA disabled
Ceres	11	4

DBox Type	DBox HA enabled	DBox HA disabled
Mavericks	13	4

For more information about this feature, see *VAST Cluster Administrator's Guide*.

New VAST Drivers to Enable Block Storage Access

VAST Block CSI Driver

When used with VAST Cluster 5.3 or later, VAST CSI Driver lets you dynamically provision block storage for your Kubernetes pods. This functionality is referred to as the **VAST Block CSI Driver**.

To let your applications use block storage on a VAST cluster, you define a block storage class and reference it in the PVC. Based on the storage class definition, the driver provisions a block volume for the PVC using a preconfigured view on the VAST cluster.

For deployment and usage guidelines, see the *VAST Block CSI Driver Administrator's Guide*.

VAST Driver for Cinder

With this release, VAST provides an implementation of the VAST driver for the OpenStack Block Storage service (Cinder). VAST Driver for Cinder enables you to use VAST NVMe storage as a backend for data volumes managed through Cinder.

For deployment and usage guidelines, see *VAST Driver for Cinder documentation*.

Enhancements in 5.3.0

VAST Cluster 5.3 enhancement highlights:

- Cluster deployment checkpointing
- Import/export VAST cluster installation utility fields to JSON
- Support for Fortanix and HashiCorp EKM providers
- Support of SMB with S3 security flavor
- Support for S3 conditional writes and trailing checksums
- VAST Database analytics
- Support for Spark 3.5.1 with Thrift and Connect

Install & Upgrade

- VAST Cluster 5.3 features a checkpoint mechanism for the cluster deployment procedure. Checkpointing splits the procedure into a series of discrete steps. If one of the steps fails, the process can be resumed from the failed step, without the need to rerun the steps that have already completed.

- ORION-177163: Added an ability to import and export VAST Cluster Install field values from/to a JSON configuration file. To do so, use the new Export Config and Import Config buttons in the VAST cluster installation utility.
- ORION-235299: Added an ability to determine whether to run automatic upgrade of firmware on non-active drives as part of the cluster upgrade procedure. The following user controls have been added for this purpose to VAST CLI:
  - The `--auto-drive-fw-upgrade` option on the cluster upgrade command
  - The new `cluster set-drive-fw-upgrade` command

Cluster Expansion

- The cluster expansion procedure includes an additional validation step to verify the setup. If you do not want to wait for the validation to complete, you can skip this step by choosing Skip Validation.

Networking

- ORION-241635: Support of InfiniBand *Connected* mode has been deprecated.
- ORION-207871: Added an ability to configure the cluster so that one VAST DNS name can be used for multiple VLANs (virtual IP pools with VLAN tags). If you want clients to be able to connect to any of virtual IPs from any of the VLANs behind a single VAST DNS name, contact VAST Support to turn this feature on.
- ORION-187391: Added indication of cluster nodes' IP addresses and hostnames to the `/etc/hosts` file on each node.
- ORION-195238: The non-disruptive network reconfiguration feature (Settings -> Configure Network) is now available for support and root users only.

Multi-Tenancy

- ORION-236542: VAST Web UI features a new dashboard, the Tenants Dashboard, that lets you monitor performance (capacity, bandwidth and latency) per tenant. To access the new dashboard, choose Dashboard in the left navigational menu and then switch to the Tenants Dashboard tab.
- You can optionally set a domain name that will be used to build the cluster login URL for the tenant. (If a domain name is not specified, the tenant name is used instead.)

  To specify a tenant domain name:

  - In VAST Web UI, enter the domain name in the Domain field in tenant settings (Element Store -> Tenants -> choose to create or edit a tenant).
  - In VAST CLI, use the `--domain-name` option on the `tenant create` and `tenant modify` command.

  In addition, VAST Web UI lets you preview the resulting login URL in the same dialog.
- ORION-194717: Increased the maximum allowed number of tenants per cluster from 1000 to 2048.
- Added predefined analytics to visualize bandwidth, capacity, IOPS and latency per tenant. To access the analytics, select the Tenant category in Analytics -> Analytics -> Predefined Analytics.
- ORION-238567: If you're deleting a tenant in VAST Web UI (Element Store -> Tenants -> right-click a tenant and select Remove), the confirmation box does not provide an option to force the deletion despite that the tenant directory contains data. The deletion is performed regardless of the presence of tenant data.

- The `--vippool_ids` option on the `tenant create` command has been deprecated.

Encryption of Data at Rest

- Added support for the following EKM providers:
  - Fortanix Data Security Manager (DSM)
  - HashiCorp Vault Enterprise
- ORION-197339, ORION-206540: With VAST Cluster 5.3, the Revoke action has been updated to revoke the encryption key or group on the EKM server. To revoke on the VAST cluster only, use the new Deactivate action. A deactivated key can be reinstated on the VAST cluster using the Reinstate action.

  In VAST Web UI, both actions are available in the right-click menu for an encrypted path (Element Store -> Encrypted Paths) or a tenant (Element Store -> Tenants).

  VAST CLI features a new command to deactivate an encryption group, `encryptiongroup deactivate-encryption-group`, and also a new `--deactivate` option on the `tenant alter-encryption-group-state` command.

  

  Note

  The Revoke operation cannot be undone.

Quotas

- Extended the list of units of measure that can be selected when setting a quota in VAST Web UI to include terabytes (TB), petabytes (PB), exabytes (EB), zettabytes (ZB), and yottabytes (YB).
- ORION-157643: The VAST CLI `userquota list` command features new filters to display group rules, user and group accounting information, as well as default user or group rules.

Quality of Service (QoS)

- The settings to define minimum QoS have been deprecated.
- ORION-207047: You can now set QoS static limits for the entire cluster. To do so in VAST CLI, use the `--static-limits` option on the `cluster modify` command.

Protocols

- The S3 security flavor now supports the SMB protocol. This lets you implement policy-based access control for SMB sessions. You can use identity and/or bucket policies to control SMB client access to views associated with a view policy that enforces the S3 Native security flavor.

  For more information about how access checks are performed with the S3 Native security flavor, see *VAST Cluster Administrator's Guide*.
- ORION-115966: Added an ability to control the way VAST Cluster sets the owning group when creating files on a view

controlled with SMB and Mixed Last Wins security flavor.

By default (which is the same as in previous versions), the owning group is determined based on the access protocol: from the user's `primaryGroupID` for SMB and from the user's POSIX GID for NFS. You can change this behavior to set the owning group based on the POSIX GID of the user for both SMB and NFS. The setting is made per tenant.

To set the behavior, run the `tenant create` or `tenant modify` command with the `--preferred-owning-group PROTOCOL_BASED` or `--preferred-owning-group POSIX_GID` option specified.

- ORION-66805: Added support for applying identity or bucket policies to NFS requests for S3 Bucket views created in a parent NFSv3 view controlled with S3 Native security flavor. In other words, access to `object` in `/nfs_view/bucket_view/object` can now be authorized based on S3 policies set for `bucket_view`.

NFS

- ORION-212662: Added user controls to determine whether POSIX mode bits are inherited from the parent directory when using a view policy with NFS security flavor:
  - In VAST Web UI, the Inherit ACL from parent in NFS Flavor option in the Default POSIX modebits tab of view policy settings (Element Store -> View policies -> choose to create or edit a policy).
  - In VAST CLI, the `--enable-inherit-parent-mode-bits` and `--disable-inherit-parent-mode-bits` options on the `viewpolicy create` and `viewpolicy modify` commands.
- ORION-179496: Added support for NFS aliases to the VAST implementation of Remote Quota Protocol (rquota).

SMB

- ORION-223116: Added an ability to configure the way the cluster handles SMB compound requests beginning with a CREATE request when the starting CREATE request gets a STATUS_PENDING response.

  By default, the cluster sends STATUS_PENDING responses to all remaining requests in the compound, which may not be expected by the client.

  You can alter this behavior so that the cluster will first respond with STATUS_PENDING only to the starting CREATE request (skipping the rest of the responses). After the entire compound is executed, responses to all requests in the compound will be sent. To alter the cluster behavior, contact VAST Support.

- ORION-130460: The following limitation has been removed:

  VAST Cluster does not show any previous versions for a directory that has the same name as a directory that has been deleted.

S3

- ORION-198542: Added support for S3 conditional writes. If the PutObject or CompleteMultipartUpload request contains the `If-None-Match` header and the value is '*', the object is uploaded only if there is no existing object with the same key name in the bucket. Conditional writes are not supported for versioned buckets.
- ORION-191255: Optimized performance when processing S3 PutObject requests for objects with the size of less than 1MiB. The optimization works with S3 Native security flavor only.
- ORION-187569: Added support for S3 trailing checksums, including the following S3 request headers:

- x-amz-checksum-crc32
- x-amz-checksum-crc32c
- x-amz-checksum-sha1
- x-amz-checksum-sha256

VAST Cluster now recognizes that an S3 request includes a checksum and handles the checksum separately from the uploaded content. Note that VAST Cluster does not perform checksum verification.

- ORION-159797: Added support for bucket object delimiters other than a forward slash (/).

ABAC

- ORION-204606: Added support for replication or Global Access where the destination directory has ABAC tags.
- ORION-204605: Added support for replication and Global Access on a directory that has ABAC tags where the parent directory also has ABAC tags.

Protocol Auditing

- ORION-222769: Expanded protocol auditing to log the following VAST Database transaction-related operations when protocol auditing is enabled and configured to log session create and close operations:
  - BEGIN_TRANSACTION
  - ROLLBACK_TRANSACTION
  - COMMIT_TRANSACTION
  - START_QUERY
  - QUERY_STATUS
  - FINISH_QUERY
  - LIST_QUERIES
  - GET_DATA
  - FINISH_DATA

Event Publishing

- ORION-212929: Added an ability to set up event notifications for the events of adding a tag to an object (`PutObjectTagging`) and removing a tag from an object (`DeleteObjectTagging`).

  The following user controls have been added for this purpose:

  - In VAST Web UI, the Object Tagging tab in the Trigger pane of view's event notification settings (Element Store -> Views -> choose to create or edit a view -> go to Event Notifications tag)
  - In VAST CLI, the `S3_OBJECT_TAGGING_PUT`, `S3_OBJECT_TAGGING_DELETE` and `S3_OBJECT_TAGGING_ALL` keywords for the `--triggers` option on the `eventnotification create` and `eventnotification delete` command.

VAST Database

- ORION-215020: Added support for Trino 462.
- ORION-206485: Added an ability to set user-defined row IDs in VAST Web UI and VAST CLI. Prior to this change, user-defined row IDs could be set through the VAST Connector only.
- ORION-205367: Added an ability to delete a database from the DataBase -> VAST Database page in VAST Web UI.
- ORION-194120: VAST Database metrics are now included in Analytics -> Top Actors visualizations.
- ORION-183605: Added an ability to associate a VAST Database with a non-default tenant. Prior to this change, all VAST databases were associated with the default tenant.

  To supply a tenant when creating or managing databases:

  - In VAST Web UI, use the Tenant selection field in the VAST Database page (DataBase -> VAST Database).
  - In VAST CLI, specify the `--tenant-id` option on the command.
- ORION-174344: Added an ability to monitor VAST Database operations in the Analytics -> Data Flow page. To do so, open the page and select Database in the Protocol field.

VAST Data Engine

- Added support for Spark 3.5.1 with the Spark Thrift server and Spark Connect. You can select the new Spark 3.5.1 with Thrift image tag when adding a managed application in VAST Web UI (Data Engine -> Managed Applications -> choose to create an application).

  If the Spark cluster includes Spark Connect, select the Thrift and Connect checkbox. This checkbox enables support for Spark clusters with TLS encryption. You can upload the SSL certificate and keys using the new Configuration & Security tab in managed application settings (Data Engine -> Managed Applications -> choose to create or edit an application).
- When running Spark as a managed application, you can upload Spark configuration files (`spark-defaults.conf`, `core-site.xml`, `hive-site.xml`, `hdfs-site.xml`), SSL certificates and keys in VAST Web UI using the new Configuration & Security tab in managed application settings (Data Engine -> Managed Applications -> choose to create or edit an application). You can also make use of sample configuration files that can be downloaded from this tab.
- ORION-218020: Added an ability to specify ranges of worker IP addresses when adding a managed application (Data Engine -> Managed Applications -> choose to create an application -> Network tab -> Worker Details).
- ORION-210269: Added indication of the CNode IP when displaying the CNode state for a running managed application (Data Engine -> Applications -> right-click a running application and choose View CNode State to open the CNode State dialog).

Data Protection

- ORION-214687: Increased the maximum allowed number of snapshots per protection policy and per protected path from 980 to 1500.
- ORION-213277: Added an ability to associate a protection policy with a VAST tenant, as follows:
  - In VAST Web UI, use the Tenant and Remote tenant fields in protection policy settings (Data Protection -> Protection Policies -> choose to create a protection policy)

- In VAST CLI, use the `--tenant-id` and `-remote-tenant-name` options on the `protectionpolicy create` command.

Replication

- ORION-210450: Added an ability to automatically create configuration for the replicated VAST Database bucket on the destination replication peer:
  - In VAST Web UI, the Bucket DB replication toggle in the cluster's S3 settings (Settings -> S3)
  - In VAST CLI, the `--enable-bucket-db-replication` option on the `cluster modify` command
  - In VAST REST API, the `enable_bucket_db_replication` parameter for the `/clusters/{id}/` endpoint

  Once enabled, this capability cannot be disabled.
- ORION-115311: Added the ability to move files and directories from or to a protected path that is a replication source or replication target. This includes both moving a file or directory from a protected path to a non-protected path and vice versa, and also moving a file or directory from one protected path to another protected path.

Global Access

- Added an ability to configure a Global Access protected path and an asynchronous replication remote protected path on the same source path. The configuration requires that all participating clusters run VAST Cluster 5.3 or later and that the destination paths for asynchronous replication and Global Access are be on different replication peers (different clusters).

VAST Dataspace

- ORION-190960: Enhanced validations run when creating or modifying a replication peer to ensure that the remote cluster has a replication virtual IP pool that is enabled and can be used for replication.

VAST on Cloud

- You can deploy a VAST on Cloud (VoC) cluster on Google Cloud Platform (GCP).

  VoC deployment in GCP is done through Terraform using a set of Terraform configuration files provided by VAST. For a complete installation procedure, see *VAST Cluster Administrator's Guide*.

  The following limitation applies:
  - Encryption is not supported with VoC on GCP.
- ORION-205091: Updated the VoC on GCP cluster removal routines to automatically clean up all static routes created by the cluster.

Authentication & Authorization

- ORION-175702: Added an ability to set the type of periodic health check that VAST Cluster performs for an Active Directory or LDAP provider configured for the cluster: by pinging the provider or by binding to it.

  The following user controls have been added for this feature:

- In VAST Web UI, the Ping check and Bind check options in the Periodic health check type pane of advanced provider settings (User Management -> Active Directory or LDAP -> choose to create or edit a provider -> Advanced tab)
- In VAST CLI, the `--monitor-action` action on the `activedirectory create`, `activedirectory modify`, `ldap create` and `ldap modify` commands
- In VAST REST API, the `monitor_action` parameter for the `activedirectory` endpoint.

VMS

- ORION-231659: VAST Prometheus Exporter lets you export various NIC-related metrics that help monitor physical packet transmission and reception rates. The new metrics can be exported with the `/prometheusmetrics/nics` and `/prometheusmetrics/all` endpoints.
- ORION-225096: Added an ability to modify the VMS virtual IP, subnet mask and port via VAST CLI. To do so, use the `--mgmt-data-vip`, `--mgmt-data-netmask` and `--mgmt-data-interface` options on the `vms modify` command.
- ORION-219419, ORION-208085: Added an ability to set ranges of IP addresses from which users are allowed to log in to the VMS. The settings can be made for the entire cluster and/or per tenant:
  - For the entire cluster:
    - In VAST Web UI, use the new tab named Client Source Address in VMS settings (Settings -> VMS).
    - In VAST CLI, run the `cluster modify` command with the `--access-ip-ranges` option specified.
  - Per tenant:
    - In VAST Web UI, use the Source IP Address for Tenant Admin to VMS pane in the **VMS Login** tab of tenant settings (Element Store -> Tenants -> choose to create or edit a tenant).
    - In VAST CLI, run the `tenant create` or `tenant modify` command with the `--access-ip-ranges` option specified.
- ORION-216027: Added an indication of the virtual IP pool name to CNode metrics that can be exported with VAST Prometheus Exporter.
- ORION-196210: Added the DBox state as a metric that can be exported with the VAST Prometheus Exporter.
- ORION-172950: VMS can monitor the amount of packets pruned or discarded due to TCP socket buffer overruns. The following VMS alerts will be raised when the packet rates get high enough to indicate a potential cable issue:
  - `CNode - Hardware,component=node,packets_pruned_socket_buffer_overrun`
  - `CNode - Hardware,component=node,packets_dropped_socket_buffer_overrun`
- ORION-168916: Fine-tuned the `dbox configuration does not match the pci switch type configuration` alarm so that it is skipped from alarm listings if the same alarm has already occurred within the day.

VAST Web UI

- Improved the identity policy visual editor (User Management -> Identity Policies -> choose to create or edit an identity policy) to include:
  - Predefined sets of statements that you can use as building blocks when creating your identity policy from scratch

    - Fields to define conditions under which policy statements take effect.

- ORION-234678: The right-click menu for a VMS manager entry in the Administrators -> Managers page includes a new option, Clone and Edit, that lets you create a copy of an existing manager account and open it for editing in VAST Web UI.
- ORION-182749: Added an ability to select and deselect all CNodes when creating or modifying a virtual IP pool (Network Access -> Virtual IP Pools -> choose to create or modify a pool -> Resource Selection tab).
- ORION-186882: Enhanced the Access Mask column in the File Handles And Byte-Range Locks On A File dialog to provide a user-friendly list of access masks.
- ORION-110630: Enhanced the Settings -> Certificates page to display certificate expiration dates.

VAST CLI

- ORION-229365: Added the `--tenant-id` option that lets you specify the tenant when using the `user modify` command to update user's S3 permissions. In addition, the `user show` command now features the `--tenant-id` option to filter the displayed S3 permissions per tenant.
- ORION-204569: The output of the `identitypolicy list` and `identitypolicy show` commands now includes the Enabled field (shows whether the policy is currently in effect) and the Replicated field (indicates whether the policy is replicated from a peer cluster).
- The `tenant create` and `tenant modify` commands now feature a new option, `--identity-provider-name`, that you can use to specify an authentication provider to authorize access when logging in to VMS.
- When creating a view in VAST CLI, you can give it a name by specifying the new `--name` option on the `view create` command.

VAST REST API

- ORION-200936: VAST API documentation includes a change log that lists API changes introduced in version 5.3.

Platform & Control

- ORION-241820: The `ebox replace` command features a new option, `--host-sn`, that lets you update the EBox serial number. This option is helpful when troubleshooting EBox discovery issues.
- ORION-225992: The VAST CLI `ebox modify` command features a new option, `--immediate-phaseout`, to power off an EBox without waiting for the drives to finish phasing out.
- ORION-223443: Root permissions are no longer required when establishing an SSH connection by node name.

Resolved Issues in 5.3.0

Cluster Expansion

- ORION-184301: Updated the logic behind the CBox add wizard to ensure that the option to skip external NICs is honored as appropriate.

Networking

- ORION-217557: Resolved an issue where during cluster networking configuration, incorrect IP addresses could be assigned to the management ports on a cluster where only IPv6 addressing was used.
- ORION-209079: Updated the cluster networking configuration script (`configure_network.py`) so that it supports use of VLANs for application CNodes. Prior to this change, VLANs could be assigned to application CNodes in VAST Web UI or VAST CLI, but the resulting configuration could be incorrect.
- ORION-203289: Improved port status checks to eliminate a flow where some hosts could encounter NFS connectivity issues following a switch replacement.
- ORION-202575: Added a validation to ensure that IP addresses entered as arguments to the cluster networking configuration script (`configure_network.py`) do not include hyphens or dashes.
- ORION-193428: Improved handling of SSL sockets to eliminate a flow where CNode containers could restart with the `msg=release_ips` or `msg=assign_vips_from_bucket` errors following modification of the CNodes' virtual IP pool.

Element Store

- ORION-234379: Improved lock management routines to resolve an issue that could cause multiple CNode containers to restart with the `assertion failed: (did_lock)` error.

Encryption of Data at Rest

- ORION-196475: Introduced updates to ensure that upon deletion of a tenant, the EKM keys associated with the tenant get deleted from the EKM server.

Protocols

- ORION-216774: Resolved an issue that could cause incorrect setting of the directory owner for child directories of a parent that had no default ACL on views with the SMB and S3 protocols enabled and the Mixed Last Wins or SMB security flavor set.
- ORION-204972: Made updates to prevent propagation of the SGID POSIX modebit to files/objects created in a directory that has the bit set, on a multi-protocol view controlled with the NFS security flavor.

NFS

- ORION-205404: Resolved an issue where high read latency could be observed on one of the cluster's CNodes when processing a specific NFS workload.
- ORION-187096: Resolved an issue that could occasionally cause NFS3ERR_STALE errors when attempting to mount an NFSv3 share after a seamless failover.

SMB

- ORION-173200: Resolved an issue that could cause a permission error when attempting to access an SMB share if the user had only *Traverse* and *List Folder* permissions.

- ORION-144020: Resolved an issue where after enabling use of Kerberos/NTLM authentication to authorize SMB users from non-trusting domains, a Windows client would let you add a new ACE only by searching for a specific user in the list of trusted forest users, instead of locating the user through the list of domains.

S3

- ORION-217661: Removed a restriction that caused VAST Cluster to reject zero-sized parts in a multipart upload with a 400 Bad Request error.
- ORION-217396: Optimized processing of S3 listing requests to avoid increased read latency at the time when the cluster is busy handling multiple listing requests with a very large number of items.
- ORION-213741: Resolved an issue where after toggling the Enable bucket logging option off, the feature state changed to Disabled for a short time and then went back to Enabled.
- ORION-204296: Introduced updates to improve performance when processing S3 workloads.
- ORION-198606: Improved the logic used to wait for completion of an S3 multi-part upload so that it does not cause an `IO is stuck - should close` alert on the cluster.
- ORION-182790: VAST Cluster now returns the `UnresolvableGrantByEmailAddress` S3 error code on attempts to put an object or bucket ACL based on a non-existing user email address. Prior to this change, the `MalformedACLError` error code was returned.
- ORION-136153: Improved the way VAST Cluster handles multi-part uploads that include an extremely large number of objects to avoid performance degradation.

Protocol Auditing

- ORION-206735: Optimized VAST Database performance to eliminate an issue where logging of protocol operations after having enabled the feature to save protocol audit results to a VAST Database table (Settings -> Auditing -> General tab -> the Save audit logs to VAST DB toggle) could impact performance of subsequent VAST Database queries.
- ORION-203287: Made updates to ensure VAST Cluster creates an audit log entry for an SMB CLOSE operation when the operation involves file deletion.

Replication

- ORION-204141: Added validations to prevent changing or deleting of replication peers on the replication destination cluster.

Global Access

- ORION-164710: Improved capacity estimations to prevent skewing in cases where local and remote capacity figures differ significantly and the remote capacity amounts to a significant portion of the overall capacity.

VAST on Cloud

- ORION-193259: Resolved an issue that could prevent creation of a VAST on Cloud (AWS) instance in a region different from the one used for Multi-Cluster Manager.

Authentication & Authorization

- ORION-210990: Updated the tooltip for the Bind DN field in the Active Directory provider settings (User Management -> Active Directory -> choose to create or edit an Active Directory provider) so that it does not imply that the bind DN must be a superuser.

VMS

- ORION-235592: Resolved an issue that could cause an error when attempting to establish an SSH connection through SSO to a cluster with a management virtual IP being an IPv6 address.
- ORION-216977: Updated the message that VMS issues to report the beginning of a bulk permission update to state that the second path in the message is a subpath on the view: `Bulk permission update on tenant <tenant>, view <view path> subpath / started`.

VAST Web UI

- ORION-206747: Updated the filter in the Replicated column in the Identity Policies page (User Management -> Identity Policies) to filter entries by the Replicated status as appropriate.
- ORION-205879: Updated the Encryption Group field in tenant settings (Element Store -> Tenants -> choose to view or edit a tenant) to display the currently assigned encryption group. Prior to this change, the group was not shown, although it was displayed when viewing the tenant in the Tenants page.

VAST CLI

- ORION-198847: Made updates to avoid triggering the SSH `REMOTE HOST IDENTIFICATION HAS CHANGED!` warning when logging into VAST CLI from a CNode that does not run VMS.

VAST REST API

- ORION-214067: Made updates to eliminate discrepancies between VAST REST API documentation and actual API parameters.

Platform & Control

- ORION-214371: Eliminated a flow that could cause temporary service disruption due to an internal race condition.
- ORION-193956: Resolved an issue that could cause a `leader hogging for <number> us` alert message to occasionally appear in VAST logs when using IceLake (HPE) CBoxes.
- ORION-158539: Updated the Hardware Layout for the CERES DBox so that the the back view shows each data port in the left or right position as appropriate.

Limitations in 5.3.0

Install & Upgrade

- ORION-242658: BMC firmware upgrades are not supported for Supermicro Genoa CNodes.
- ORION-232732: VAST Cluster 5.3 does not support Broadwell CNodes. Running VAST Cluster 5.3 on a cluster with Broadwell CNodes may entail severe performance issues.
- ORION-222648: NDU that includes automatic adjustment of CNode CPU isolation settings (`isolcpus`) is not supported for EBoxes.
- ORION-214559: A BMC upgrade cannot be performed with an inactive CNode that has been powered off.

Networking

- ORION-242967: The cluster networking configuration script (`configure_network.py`) does not support configuring CNode Port Affinity for HPE Genoa CNodes.
- ORION-241708: The cluster networking configuration script (`configure_network.py`) does not support configuring CNode Port Affinity for Supermicro Gen5 CNodes.

Encryption of Data at Rest

- ORION-208004: Enabling VAST OS boot drive encryption requires that the node is inactive. Enabling the encryption on an active node may cause a long reboot sequence.

Quotas

- Quotas are not enforced on replication destination directories under a protected path. For example, if the protected path is `/ppath`, a quota on `/ppath/yourdir` is not enforced.

NFS

- ORION-115336: If one creates an NFSv4.1-only view and mounts it, and then creates its parent view with NFSv3 only, IO operations on the NFSv4.1-only view succeed but mounts are not allowed.

NFSv3

- In rare cases with large numbers of files and directories, the existence of a view with *Global Synchronization* enabled under a protected path can block the removal of the protected path.

SMB

- ORION-169707: When the Hyper-V management tool tries to list VAST Hyper-V SMB shares on an SMB server, the `The RPC server is not available` error can occur if the SMB server is specified using its FQDN. To avoid this error, specify the IP address of the SMB server instead of the FQDN.

- ORION-160323: After updating permissions for an SMB share in Windows Explorer, a duplicate SMB share can be displayed. The duplicate SMB share disappears upon a refresh (F5).
- ORION-134730: An attempt to restore a file can fail if after the restore has started, a quota is set on the path where the file resides.

S3

- An object to be uploaded via a S3 presigned POST request must have only ASCII characters in its name.
- A POST policy (used for S3 presigned POST requests) can be up to 4800 bytes.
- S3 with proxy clients is not supported.
- ORION-197281: VAST Cluster disables bucket logging set on a bucket from which data is synchronously replicated to another bucket once you set up bucket logging on the replication destination bucket and configure it to use a different logging destination bucket.
- ORION-190674: Once created, an S3 bucket cannot be renamed or moved to a different path. Thus, for example, if you try to change the bucket's path when modifying a view in VAST Web UI, the change does not take effect and the view will still be listed with the old path.

Protocol Auditing

- ORION-211474: The *Create* permissions for the *Logical* realm are required to access the VAST Audit Log (DataBase -> VAST Audit Log).

Attribute-Based Access Control (ABAC)

- ABAC is supported on views controlled with *SMB*, *S3 Native* and *Mixed Last Wins* security flavors. ABAC is not supported with *NFS* flavor.
- ABAC is not supported with NFSv3.
- ABAC tags cannot be set on the cluster's root directory (/).
- Once assigned, you cannot edit or remove the ABAC tags of a view. Assigning new ABAC tags to an existing view or directory (storage path) is not allowed.
- After a child view inherits ABAC tags from the parent view, you cannot update or remove the ABAC tags on the child view.
- If you create a view for a directory that already exists, ABAC tags from the existing directory are assigned to the newly created view. In this case, there can be a delay between the view creation time and the time when the view's ABAC tags can be displayed.
- If a user does not have any ABAC permissions, the user still can mount an NFSv4 export or map a SMB share to a local drive, but the user is not allowed to perform any operations on the files or directories.
- ORION-163697: When an SMB user accesses a file for which the user has ABAC set to read-only, a lock is placed on the file although the user does not have read/write permissions for the file.

The following features and capabilities cannot be used together with ABAC-tagged views:

- If a tenant has ABAC-tagged views, you cannot change or remove the Active Directory provider configured for the tenant.

- When using NFSv4, it is not allowed to create hardlinks in views that have ABAC tags.
- When using S3:
  - ABAC cannot be used with anonymous S3 access. You cannot set ABAC tags for views that have anonymous S3 access enabled.
  - It is not allowed to set ABAC tags on a view that is a target for S3 bucket logging.
  - Requests from S3 superusers are handled in the same way as for regular users. This means that an S3 superuser is not granted access if the ABAC access check denies access for this user.
- A directory under which an ABAC-tagged view exists, cannot be moved to the Trash folder.
- Bulk permission updates are not available for ABAC-tagged views.
- Lifecycle rules cannot be set for files or directories with ABAC tags.

VAST Catalog

- The maximum path length supported by VAST Catalog is 1024 characters.
- When VAST Catalog is enabled, replication is limited to two peers (group replication is not supported with VAST Catalog).
- VAST Catalog must be disabled before a protected path can be deleted.
- ORION-197741: VAST Catalog cannot be enabled on a cluster that uses encryption keys managed through EKM, including per-tenant and per-path encryption keys.

Replication

- ORION-208123: Local user accounts are not subject to replication.
- The following limitation applies to VAST Database asynchronous replication:
  - ORION-179909: VAST Database asynchronous replication cannot be used together with Global Access or synchronous replication on the same path.
- The following limitations apply to synchronous replication for S3:
  - Synchronous replication is supported for S3 buckets only.
  - It is not allowed to configure local snapshots, asynchronous replication or Global Access on the protected path for which syncronous replication is configured.
  - Up to 250 replication streams are supported.
  - S3 lifecycle rules are not replicated.
  - S3 keys are replicated asynchronously.
  - Synchronously replicated directories are not subject to bulk permission updates.

Global Access

- NFSv3, SMB and S3 access protocols are supported. NFSv4 is not supported.

If a view is configured with both NFSv4 and SMB, it must be controlled with the NFS security flavor.

- VAST Database is not supported.
- Lease expiration time can only be set when creating a global access protected path. You cannot change lease expiration time when you modify a global access path.
- VAST Catalog does not provide information on the cached data on the remote cluster.
- ORION-194805: Applications that use SMB2 Byte Range Locks are not supported when the SMB client is connected via a remote Global Access protected path. Examples of such applications are Microsoft Office suite on macOS, Microsoft Hyper-V, AutoDesk 3ds Max and some Adobe Premiere plugins.
- ORION-194613: If some files have additional hardlinks, the amount of bytes reported as prefetched can be higher than the actual amount prefetched.

VAST on Cloud

- ORION-145141: Creating a tenant with EKM encryption is not supported on VoC clusters.
- ORION-113036: After you reregister the same VoC cluster in Uplink, information about the previously registered instance of this cluster is no longer available in Uplink.

VAST DataSpace

- VAST DataSpace requires that each cluster participating in the inter-connection is running VAST Cluster 5.0 or later.
- ORION-135966: The inter-connecting clusters must have connectivity to each other through the clusters' management networks.
- ORION-132073: When you remove a VoC cluster from a Multi-Cluster Manager cloud service instance (using the removal button on the cluster's card ()), the VoC cluster is terminated. There is no option to remove a VoC cluster from Multi-Cluster Manager without also terminating it. (In the VAST DataSpace page in the VAST Web UI, the button removes the VoC cluster from VAST DataSpace and does not terminate it.)

Authentication & Authorization

- ORION-202335: If the cluster has Active Directory domain auto-discovery enabled, the discovered domains are kept in cache for quite a long time. If you modify an existing provider's configuration while auto-discovery is on, VMS may still report the old cached entries. To avoid this, rerun auto-discovery or remove and re-add the provider.
- ORION-195524: Following a cluster recovery and while the Active Directory provider is still inaccessible, VAST Cluster can resume IO of provider users if they use NFSv3 or NFSv.4.1 with NTLM authentication. IO of provider users accessing through SMB or NFSv4.1 with Kerberos authentication is not resumed during this period.
- ORION-187136: Identity policies are replicated as disabled to the destination peer, where if needed, they can be enabled manually.
- ORION-187936: Joining/leaving an Active Directory domain may take longer compared to previous versions.
- ORION-152475: An access denied error is returned for NFSv3 or NFSv4 requests if they are checked against an identity or bucket policy with an `s3:ExistingObjectTag` condition statement in it.
- ORION-143944: When using Kerberos/NTLM Authentication to authorize SMB users from non-trusting domains, the *DOMAIN\username* format cannot be used to specify users of remote domains. The *username@domain* format must be

used instead.

- ORION-134299: When the tenant is set to use Kerberos/NTLM authentication to authorize SMB users from non-trusting domains, both NFS and SMB must use the native SMB authentication (Kerberos), and not Unix-style UID/GIDs.
- ORION-141763: Before enabling or disabling NTLM authentication, you need to leave the cluster's joined Active Directory domain. After NTLM authentication is enabled or disabled, rejoin the domain.
- The following limitations apply to Multi-Forest Authentication:
  - VAST Cluster does not allow adding two different Active Directory configuration records with the same domain name but different settings for multi-forest authentication and/or auto-discovery.
  - Names of users' domains are not displayed in data flow analytics.
  - If a trusted domain becomes unavailable and then recovers, SMB clients can use it to connect to the VAST cluster only after a period of time, but not immediately upon domain recovery.
  - Clients cannot establish SMB sessions immediately after a trusted domain recovers from a domain failure.
  - If a group exists on an Active Directory domain in a trusted forest and the group scope is defined as *DomainLocal*, VAST Cluster does not retrieve such a group when querying Active Directory, so members of such a group are denied access despite any share-level ACLs that can rule otherwise.
  - If TLS is enabled, the SSL certificate has to be a CA-signed certificate that is valid for all of the domain controllers in all trusted forests. If the certificate is not valid for a domain controller, this domain controller is not recognized.
  - ORION-156168: In a multi-forest environment, after migrating a group account from the forest of the cluster’s joined domain to another forest, information about historical group membership is not kept, so users in the migrated group might not be able to access resources to which they used to have access prior to the migration.

VMS

- ORION-131386: When there is a parent directory that has a very large number of child directories, a total of children’s capacity values displayed in the Capacity page can exceed the capacity value shown for the parent directory.

Platform & Control

- ORION-201807: P5316 QLC SSDs running a firmware version of ACV10200 may cause performance degradation if used together with the Flash Write Buffers functionality. To avoid performance impact, upgrade the firmware to version ACV10203.
- ORION-169078: VMS does not provide an indication of the link state of the external management port on a CERES DTray.
- The following limitations apply to EBoxes:
  - ORION-193794: Power cycling of an EBox where the leader was running may result in significant IOPS degradation until the EBox is up again. Contact VAST Support for a workaround.
  - DBox migration is not available for EBoxes.

Call Home & Support

- When creating a support bundle with the METADATA preset, only one CNode can be selected for the bundle. Selecting any DNode(s) or multiple CNodes together with the METADATA preset results in an error.

Known Issues in 5.3.0

Install & Upgrade

- ORION-242331: VAST Web UI lets you set the BMC Firmware and Force options for an upgrade at the same time, although forced BMC upgrades are not allowed. If the Force flag is set, BMC upgrade is not performed.
- ORION-145815: In some cases, VAST Cluster does not raise an alert on a wrong NIC firmware version during a cluster upgrade.

Cluster Expansion

- ORION-220738: In some cases, VMS does not provide any alerts or other status indication when a drive gets disabled while the newly added DBox is being initialized.
- ORION-175762: In some cases, a DBox expansion procedure run on a cluster with similarity-based data reduction enabled can take longer than expected.
- ORION-173816: VAST Cluster does not block expansion from CERES 15TB to CERES 60TB, although such expansion is not supported.

Networking

- ORION-228412: When running the cluster networking configuration script (`configure_network.py`) with both `auto_ports_ext_iface=northband` and `auto_ports_skip_nic=ext` options specified, no error is raised although this combination of options may result in incorrect network configuration.
- ORION-155530: Sometimes after you run the cluster networking configuration script (`configure_network.py`) and then rebooted the CNode, the `eb1` interface can still be down with the `Device ib1 has different MAC address than expected, ignoring` error. In this case, rerun the script after the reboot to bring the interface up.

Quality of Service (QoS)

- ORION-243368: Prioritization of workloads based on the QoS policy prioritization flag is not supported if the policy also has burst and/or total limits defined.
- ORION-236122: Intense read workloads may impact performance on views controlled with a QoS policy with the prioritization flag set.
- ORION-231253: When the cluster-wide write bandwidth limit is set, the actual performance can be up to 10% off from the limit specified. For example, if the limit is set to 7.5GB, the actual performance would be about 6.6GB.
- ORION-139913: When applying a QoS policy to NFSv3 access, both data and metadata are taken into account in QoS limit calculations, while with NFSv4.1, only data are considered.
- ORION-137986: Enabling a QoS policy for a view on which a mixed (read and write) workload runs, can result in decreased performance for the workload.

NFSv4

- ORION-238708: In some cases, an NFSv4.1 client attempting to move files to the trash folder may get a Permission denied

error due to an issue that may cause the trash folder to use a more restricting policy than expected.

SMB

- ORION-142968: If a quota is exceeded during the process of coping a file to the VAST cluster, the copying process is stopped with a misleading error message: `A device attached to the system is not functioning.`

S3

- ORION-189731: When creating an S3 Bucket view with the ACLs disabled option selected, the view is created with ACLs enabled instead, and after a short period of time after saving the changes VMS reports the view as ACLs enabled.

  This issue does not occur when modifying an existing view. If you encounter this issue after the view has been created, open the Update View dialog for the view (Element Store -> Views -> choose to edit a view) and set it to ACLs disabled again.

ABAC

- ORION-196170: When a parent and child NFSv4.1 view both have same ABAC tags on them, an attempt to mount the child view may result in a Permission denied error. If this occurs, try setting the ABAC tags for the machine account that the client uses to mount the view.

VAST Database

- ORION-163038: When importing data into a VAST Database table and there is a type mismatch between the column and the data being imported, VAST Cluster produces an ambiguous error message (`Failed to get column`) instead of pointing to the expected data type.

Replication

- ORION-246796: In some cases where you have a source VAST cluster with release 5.2 replicating to a destination VAST cluster running release 5.3, an attempt to delete a replication peer on a source cluster may succeed on the source cluster but result in COMMUNICATION_ERROR state reported on the destination cluster, with the destination cluster being unable to clear the replication relationship. If you encounter this issue, contact VAST Support for a workaround.
- ORION-233749: VAST Cluster does not automatically delete access keys associated with a replication destination tenant which has been deleted.
- ORION-140894: When attempting to delete a protected path from the destination peer after an ungraceful failover, a `Failed to delete following streams` or a similar error occurs. The workaround is to manually change the destination peer's role to STANDALONE and retry the deletion.

Global Access

- ORION-154973: There can be a performance impact when deleting a very large number of files from the origin cluster. To avoid it, delete the protection policy associated with the path on the origin cluster prior to deletion.
- ORION-145307: Bulk permission updates are not supported for files and directories on satellite clusters.

Authentication & Authorization

- ORION-25479: Latin characters are not supported with LDAP. If you attempt to pass, for example, a username encoded with a Latin character set, the 'LDAP sanity check res: Invalid credentials' error is returned.

VMS

- ORION-238083: The VMS option to power off an EBox does not work as expected. In some cases, the power off task can be reported as complete although the box is inactive but not powered off.
- ORION-225432: Some metrics listed under Analytics -> Predefined Analytics in VAST Web UI may be unavailable for EBoxes.
- ORION-175334: When creating a managed application (Data Engine -> Applications -> choose to create an application), VMS does not block attempts to set port membership for CNodes on a cluster that does not support CNode Port Affinity.
- ORION-143717: On a cluster with CNode Port Affinity configured, there is no way to expose the VAST DNS IP on a specific port (left or right).
- ORION-131386: When there is a parent directory that has a very large number of child directories, a total of children's capacity values displayed in the Capacity page can exceed the capacity value shown for the parent directory.
- ORION-89570: In some cases, capacity analytics for subdirectories cannot be reported due to an internal timeout. This issue occurs when there is an extremely large number of subdirectories to be estimated.

VAST Web UI

- ORION-234835: Some VAST Web UI pages might not allow for proper filtering or sorting by column where value presentation differs from that in the VAST internal database.
- ORION-207301: When you open an existing lifecycle rule for viewing or editing (Element Store -> Lifecycle Rules -> choose to view or edit a rule), the field for setting the unit of measure for the Minimum object size and Maximum object size filters may show *KB* although the values supplied and used are in bytes.
- ORION-203737: The value filter in the Box column in the Infrastructure -> CNodes and DNodes pages does not work as expected.
- ORION-203189: The External Netmask field in cluster networking settings (Settings -> Configure Network) does not accept alphabetic characters.
- ORION-175189: When querying a local user using the *Aggregated* context, the Leading GID and Primary group SID fields in the User Details dialog have a value of -1 instead of an empty string.
- ORION-174128: The tooltip for the Include all CNodes option in the Resource Selection tab of the Add New Application dialog (Data Engine -> Applications -> choose to create an application) claims that the option is mandatory, although it is not.

VAST REST API

- ORION-234256: The description for the `tenant_id` parameter of a virtual IP pool (used when creating a pool by `POST /vippools/` or modifying a pool by `/PATCH /vippools/<pool id>`) must read as follows: *Tenant ID. If a tenant is supplied, only this tenant is able to access the virtual IP pool. If no tenant is supplied, the pool can be accessed by any tenant*.

- ORION-178569: The `/users/names` endpoint always returns only the first 50 entries, regardless of the page size parameter or the total amount of entries to be returned.

Platform & Control

- ORION-232944: When clicking the Power off option in the CNode page of VAST Web UI (Infrastructure -> CNodes -> right-click a node), the node gets deactivated but not powered off. To power it off, click Power off one more time.
- ORION-173461: Slot numbers displayed in the Slot column of the Infrastructure -> SCMs page in VAST Web UI are not aligned with slot numbers displayed in the Hardware Layout page.

Call Home & Support

- ORION-239170: When obfuscating a support bundle, the CNode hostname may not get obfuscated in some of the logs included in the bundle.
- ORION-238168: If you try to delete a support bundle that is still in the process of being created, the creation process does not stop and the bundle does not get deleted immediately.


VAST