VMware Tanzu Observability
Security and Privacy
Table of contents
Introduction .......................................................... 3
About this white paper .............................................. 3
Tanzu Observability architecture: secure by design .......... 4
Certifications .......................................................... 4
Architecture ............................................................ 4
Data isolation .......................................................... 6
How Tanzu Observability protects customers from unauthorized access ........................................... 7
Authentication ......................................................... 8
Authorization with roles and permissions ..................... 9
Authorization with access control lists ......................... 9
Authorization with policies (under development) .......... 9
How Tanzu Observability protects customer data .......... 10
Customer data protection in transit ............................ 10
Customer data protection at rest ................................... 10
Data replication and backup ....................................... 11
Capacity management .............................................. 11
Data retention and data deletion .................................. 11
How Tanzu Observability tests and secures its own environments ...................................................... 12
VMware secure development cycle .............................. 12
Operating procedures .............................................. 12
Tanzu Observability internal access control .................. 13
Physical Security ..................................................... 13
Management of technical vulnerabilities ...................... 14
Networking security practices .................................... 14
Introduction

VMware Tanzu™ Observability™ by Wavefront® is a platform designed for the ingestion, analysis, and visualization of enormous amounts of time-series streaming data, histograms, and traces for digital enterprises. DevOps, SRE and developer teams use Tanzu Observability to proactively alert on, rapidly troubleshoot, and optimize the performance of their modern applications running on the enterprise multi-cloud or on Kubernetes.

Tanzu Observability security features include authentication, authorization, and data protection. Customer data is protected in transit and at rest. Customers can take additional steps to segment who can see who is using our access control solution. Most importantly, as part of VMware for several years, Tanzu Observability follows the VMware Secure Software Development Lifecycle guidelines and takes advantage of both the expertise of the original Tanzu Observability ops and dev teams and the broader knowledge and processes of the VMware security team.

About this white paper

The scope of this white paper is intentionally broad. It discusses not only the security of the product but also secure, auditable processes within Tanzu Observability. Some sections of the white paper are product-specific (e.g., a discussion of authentication and authorization or explanation of how Tanzu Observability protects customer data). Other sections are company-specific (e.g., an overview of processes to guarantee physical security, and a discussion of how VMware limits access to source code using least-privilege principles).

For additional details, see the Cloud Security Alliance PDF about Wavefront by VMware.
Tanzu Observability architecture: secure by design
All levels of the product are protected:

- **Encryption.** All data is encrypted at rest and in transit.
- **Secure Transit.** All network connections use TLS 1.2 or later.
- **Data Protection.** Data at rest is managed by AWS S3 (protected by KMS) or AWS NVME (protected by Amazon's very strict security measures).
- **Penetration Testing.** VMware Tanzu Observability by Wavefront has contracted with outside vendors to perform regular penetration testing.
- **Intrusion Detection & Response.** Intrusion detection mechanisms are in place and updated frequently. If issues are detected, alerts notify Tanzu Observability staff, who will take corrective action (24x7).

**Certifications**
As this white paper is going to publication, Tanzu Observability has already successfully completed all requirements for the following certifications and reports:

- ISO 27001/27017/27018
- SOC 2 Type 1
- CSA STAR Level 1

As Tanzu Observability receives additional certifications, the [list of certifications](#) is updated.

**Architecture**
Each instance of the Tanzu Observability service runs on a cluster on AWS. The cluster uses a three-layer architecture with:

- A distributed high availability (HA) traffic load-balancing layer;
- A mirrored hot/hot application layer; and
- A clustered database layer.

The Tanzu Observability service runs in a shared-nothing mode across two mirrors. The mirrors are in separate AWS regions or availability zones within a Virtual Private Cloud (VPC). Mirroring across AWS regions is a special Tanzu Observability offering for customers seeking real-time disaster recovery. The HA layer is distributed between three or more regions or availability zones, depending on the configuration.
The architecture has these benefits:

- **Isolation of Customer Data.** Tanzu Observability customers can have dedicated or shared tenancy on a cluster. In the case of a shared tenancy, Tanzu Observability guarantees complete isolation of customer data.
- **Data Protection.** All customer data are protected at rest and in transit (discussed in detail below).
- **Replication.** Incoming metrics (telemetry, tracing, histograms, etc.) are kept in sync between mirrors via standard pub-sub services.
- **Authentication.** Tanzu Observability customers can restrict and manage access to the service by customizing authentication with SSO integrations. In addition, Tanzu Observability offers service accounts for API-only access.
- **Authorization.** Role-based access control (RBAC) supports global permissions. In addition, access control lists provide fine-grained control for individual dashboards, alerts, and metrics.
- **Management.** Roles and groups, available from the UI or REST API, facilitate administration and automation of identity and access management.
Data isolation

Each Tanzu Observability cluster is deployed to a new VPC that is completely separate and isolated from other customer workloads. The management VPC, which is used internally to monitor system health, is the only central VPC that has network connectivity to customer VPCs. The networks for Tanzu Observability clusters are managed in code and monitored by a variety of tools to ensure the security, stability, and performance of the environment. The standard is the code, and its definition evolves with the system. Tanzu Observability customers send data from cloud services, Kubernetes containers, virtual or physical hosts, and more, to the Tanzu Observability service.

• For cloud services, Tanzu Observability pulls the data from your cloud provider (after minimal setup). All major cloud providers are supported.

• For containers and on-premises telemetry, most customers send data to a Tanzu Observability proxy (dev) or load-balanced team of proxies (production) that run at the customer site. The Tanzu Observability proxy buffers and manages data traffic—in case of connectivity problems, customers do not lose data points. In addition, the proxy sends all traffic to the Tanzu Observability service using TLS 1.2 or above. The Tanzu Observability service also supports a direct ingestion mode over HTTPS.
How Tanzu Observability protects customers from unauthorized access

In addition to the network isolation practices discussed above, customer data are protected through authentication and authorization. VMware Tanzu Observability by Wavefront supports authentication and authorizations, with different levels of security available.

- **Authentication.** Tanzu Observability clusters support several authentication solutions to prevent unauthorized access. Administrators at a customer site can create and delete accounts managed within Tanzu Observability or utilize LDAP or cloud identity providers to manage authentication and transmit authentication to Tanzu Observability via SAML.

- **Authorization.** Different levels of authorization support fine-grained control over who can view or modify what:
  - RBAC limits access at a global level.
  - Access control lists limit access to individual objects (e.g., dashboards, alerts).
  - Per-metric access control (forthcoming) is unique to Tanzu Observability and supports hiding or revealing confidential data at a fine-grained level.

**FIGURE 2. Tanzu Observability Authorization Model Workflow**
Authentication

Authentication is the cornerstone of any access control solution. Tanzu Observability customers can use the credential-based authentication provided by Tanzu Observability or elect to use any identity provider that supports SAML authentication, which includes Okta, AzureAD, and Google ID. Administrators at each customer site select their preferred solution. Tanzu Observability authentication integrations use SAML and fully support two-factor authentication (managed by individual identity providers).

Tanzu Observability limits access, so only accounts that are explicitly invited or set up by privileged administrators at the customer site can authenticate. An authenticated user can log in and view or modify components of the service based on permissions and, optionally, access control settings. For automated tasks, administrators can create service accounts with revocable tokens that have only permissions explicitly assigned to the account.

- **User Account Authentication.** For user accounts, an administrator at the customer site invites a user and may assign the user roles or add the user to groups at the same time to grant permissions. The user can then log in to the cluster with username and password or use a two-factor authentication solution such as Okta.
- **Service Account Authentication.** Service accounts are used to automate certain management tasks. Administrators generate (and revoke) authentication tokens for the service account. It’s also possible to deactivate a service account completely.

![Tanzu Observability Authentication Model Workflow](https://customer.wavefront.com)

**FIGURE 3.** Tanzu Observability Authentication Model Workflow
Authorization with roles and permissions
The Tanzu Observability role-based access control implementation uses permissions to enable groups or accounts (user accounts or service accounts) to perform tasks.

User Account Authorization. User accounts have some system-defined, read-only permissions. Administrators can grant additional permissions through roles.
- Any user who can authenticate to a Tanzu Observability instance can view a basic set of UI elements such as dashboards, charts, and alerts.
- Administrators (i.e., users with Accounts and Roles permission) can grant additional permissions to each user. For example, a user with Dashboards permission can both view and modify all dashboards.
- Administrators can create roles that are sets of permissions, and then assign the role to one or more users.

Service Account Authorization. Service accounts have no permissions by default. Administrators at customer sites explicitly grant each service account only the permission required for the task that’s being automated (least required privilege). That ensures that permissions for service accounts are always very limited. Service accounts do not have the view permissions that user accounts have by default.

Authorization for Groups. To make authorization management easier, roles can be assigned to groups. Administrators create groups and give all members of the group a set of permissions by assigning a role.

Authorization with access control lists
In some situations, roles and permissions are not enough. For example, imagine a customer that wants to limit access to two confidential dashboards to the Finance team. Because permissions always apply to all dashboards, it’s not possible to use them to limit access to confidential dashboards. In those situations, administrators and dashboard creators can control access on a per-dashboard basis. In contrast to permissions, which apply to all objects of a type (e.g., to all dashboards), access control applies to individual objects via Access Control Lists (ACLs).
- For each dashboard or alert, privileged users (including the object creator) can limit who can view and who can modify that object. That might mean that certain users can view a dashboard but not make changes to it.
- A global setting allows the administrator to require that users who create a new dashboard grant access explicitly. Once this setting is selected, only the owner of the dashboard and the Super Admin user can view and modify the dashboard.
- ACLs and permissions work together. For example, assume user Bob has Dashboards permission and can view and manage all dashboards. Now user Alice creates a new dashboard, and grants View & Modify access only to user Zhang. Bob cannot access that dashboard at all.

Authorization with policies (under development)
Tanzu Observability allows you to define policies to secure access (patent pending) or secure ingestion (patent pending) to different types of time-series data (metrics, spans, etc.) based on roles, groups, or individual accounts within the same cluster. These unique, first-of-its-kind capabilities support limiting access to or ingestion of time-series data on a need-to-know basis while preserving the ability to correlate different sources of information within a single cluster.

Tanzu Observability is unique in this ability. Competitors typically address the requirement to secure access or ingestion of time-series data through a new cluster, which creates data silos and impacts the ability to correlate information.
How Tanzu Observability protects customer data

VMware Tanzu Observability by Wavefront protects customer data at rest and in transit. Table 1 lists common questions and answers, followed by details on each bullet point.

<table>
<thead>
<tr>
<th>Is data encrypted at rest?</th>
<th>Yes. Data at rest is managed by AWS S3 (protected by KMS) or AWS NVME (protected by Amazon’s strict security measures).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is data encrypted in transit?</td>
<td>Yes, TLS 1.2 or later secures all data in transit. See “Networking Security” below for details.</td>
</tr>
<tr>
<td>We expect to send large amounts of data. How do you protect against data loss?</td>
<td>The Tanzu Observability proxy performs queuing and data management for you. Capacity management practices guarantee that the Tanzu Observability service can take the data. In addition, all data sent to Tanzu Observability are backed up upon receipt.</td>
</tr>
</tbody>
</table>

TABLE 1. Frequently Asked Questions About Customer Data Protection in Tanzu Observability

Customer data protection in transit

Customer data and information in transit are protected at all times, as follows:

- **Customer Metrics.** These include time series, histograms, traces and span. All telemetry data are protected in transit (TLS 1.2 and later). Data are sent via the Tanzu Observability proxy (installed at the customer site) or directly (direct ingestion).
- **Electronic Messaging.** In communications with customers, Tanzu Observability uses settings that guarantee maximum security and privacy.
- **Protection of Log Information.** Tanzu Observability monitors the performance of customer clusters using Tanzu Observability. However, some of the monitoring tools collect log information. All logging facilities and log information are protected against tampering and authorized access.

Customer data protection at rest

All Tanzu Observability clusters run on AWS. Data are stored following Amazon’s strict security measures.

- For Amazon S3 cloud storage, “The security and compliance of Amazon S3 are assessed by third-party auditors as part of multiple AWS compliance programs.”
- Tanzu Observability uses the KMS to protect those data at rest.
- For Amazon EBS NVME, data are encrypted at rest and protected by Amazon security measures.

Algolia is used for some Tanzu Observability internal processing. Algolia has strict security in place.
Data replication and backup
Tanzu Observability tiered architecture replicates all shared state twice on the High Availability tier, which stores user information, dashboards, alerts and more. Telemetry is replicated up to four times because the architecture has two replicas per mirror, with no shared state between the replicas. The data is streamed from the serving side to the nonserving side and replicated in isolation; there is no “read replica” concept.

The High Availability tier is backed up nightly to S3 while the telemetry database is streamed into S3 via SNS replication channels. This makes it possible for us to restore or play back any telemetry with any level of granularity required into a customer’s infrastructure.

Capacity management
Capacity management practices guarantee that the Tanzu Observability service doesn’t run out of space. Resources at each tier of the Tanzu Observability architecture can scale horizontally using an automated or manual process. The infrastructure is defined as code, allowing for required changes to be made rapidly. The configurations for these components are managed with industry-standard tools.

- **Automated Instances.** Capacity management for automated instances leverage AWS autoscaling and monitor CPU usage to execute scaling decisions dynamically. The configuration includes HA ingest and query service.

- **Manually Managed Instances.** Capacity management for manually managed instances is tracked with a ticketing system.

Data retention and data deletion
The retention period for customer data is 18 months by default. Customers can request a longer retention period. The data shifts between storage tiers depending on usage patterns and the age of data.

Tanzu Observability continuously scans for data that is older than 18 months and removes that data. Some customers have SLAs that guarantee a different time for data retention.
**How Tanzu Observability tests and secures its own environments**

Securing the VMware Tanzu Observability by Wavefront service and making sure that customers are protected at all times is only part of the puzzle. Tanzu Observability also takes special care that internal procedures don’t expose customers.

- Operating procedures are secure.
- Internal systems are protected by access control.
- Physical security is guaranteed.
- Processes for vulnerability detection and remediation are in place. Regular penetration testing by third parties is part of this process.
- Networking security is in place at all levels.

**VMware secure development cycle**

VMware uses an industry-leading *Security Development Lifecycle process* and has a VMware Cloud Services Security organization that focuses on ensuring that VMware cloud services implement industry-standard operational and security controls. As part of the process, all VMware employees participate in Security and Privacy Compliance Training. This training program is customized based on the role of the employee. All employees must take an initial set of courses, and refresher modules are required annually. Additional modules are required for certain locales.

**Operating procedures**

Tanzu Observability operating procedures are secure from the ground up. To achieve that, everything is documented clearly, then implemented and tracked.

- **Process Documentation.** Operations procedure documentation addresses all aspects of both internal and customer environments. That includes installation, configuration, information handling, backup and recovery, job scheduling, error handling, support contacts, disaster recovery, audit trails and system monitoring.
- **Changes.** All modifications to the Tanzu Observability system must be the result of a ticket with approval at the required level.
- **Error Handling.** The Ops team uses automated runbooks to remedy problems such as a hardware failure. Other common Ops error remediation processes are documented in runbooks.
- **Audit Logs.** Audit logs are available for each code system Logs to allow filtering to reveal logs of interest. Tanzu Observability logs activities such as user access provisioning, login/logout, check-in/check-out of code, and so on.
- **Monitoring.** The Ops team uses Tanzu Observability to monitor the Tanzu Observability service. See *Monitor Wavefront Service Documentation* for more details.
- **Information Security Compliance Management.** Tanzu Observability contracts an external vendor to evaluate control objectives at regular intervals.
Tanzu Observability internal access control
Access control mechanisms are in place for all Tanzu Observability employees and contractors.

- **Source Code Access.** The Tanzu Observability Engineering, ESO, and Operations teams store source code in repositories with strict access control. Access is granted only after a Jira ticket has been filed. VPN connections protected by two-factor authentication and SSH connections are required. Logs of all access are retained.

- **Passwords and Two-Factor Authentication.** VMware employs strict password rules. All employees must choose strong passwords of sufficient length. In addition, Tanzu Observability employees have to authenticate to a VPN before access to sensitive information, such as development clusters and other confidential material, is possible. Access to this VPN requires two-factor authentication.

- **Least-Privilege Access.** Tanzu Observability employees are granted access following the least-privilege principles. A manager-approved Jira ticket is required before access is granted.

- **Access Revocation.** Processes for access revocation are in place and followed, for example, when an employee leaves.

- **Access Review and Remediation.** Access rights for all internal systems are reviewed at least monthly. Log reviews for each of the tools in use help identify problems. A user account can be revoked temporarily until the problem has been resolved.

**Physical Security**
VMware takes physical security seriously. Most Tanzu Observability developers work at VMware offices and can take advantage of VMware physical security.

- **Processes.** In-place processes include, but are not limited to, the following:
  - Access to buildings and offices is controlled through badging. Security personnel performs continuous walk-throughs of the VMware campus.
  - Additional access control for server rooms and other confidential areas is in place.
  - Tanzu Observability deploys only to cloud providers that have obtained industry-standard certifications that attest to the governance and risk management best practices.

- **External and Environmental Threats.** VMware Security has processes in place that protect the VMware offices against physical threats. Disaster recovery procedures help mitigate in case of a physical emergency such as an earthquake. Both customer clusters and development clusters are hosted in an environment that either spans availability zones or regions.

Additional processes, such as two-factor authentication and a Tanzu Observability internal VPN, are in place for Tanzu Observability employees (both onsite and remote).
Management of technical vulnerabilities
Tanzu Observability continuously monitors all systems for vulnerabilities, evaluates potential exposure, and takes appropriate measures to address the associated risks. Identification of vulnerabilities is based in part on:

- monitoring relevant security feeds (e.g., CERT and Ubuntu security releases)
- performing internal and external scans to detect issues

Tanzu Observability performs timely patching of all systems to ensure security updates are in place. In addition, processes for deploying emergency patches at any level of the architecture are in place. Intrusion detection mechanisms continually monitor the environment, and Tanzu Observability Ops staff responds to any issues 24x7.

Networking security practices
Networking practices ensure that data access is strictly controlled.

- **Strict Segregation of Development, Testing, and Customer Environments.** Network segmentation for groups of system components is based on services provided and applicable security controls such as DMZ, databases, and internal zones. In addition, access to the network and network services is available only for users that have been explicitly authorized to use those networks. Tickets track who is granted access to which network, and two-factor authentication is in place.

- **Security of Network Services.** Tanzu Observability continually updates security mechanisms, service levels, and management requirements of all network services (both in-house and outsourced services). Service level agreements for cloud provider network services are in place.

- **Application Services Transactions.** Network security standards that address requirements for new network connections and secure transmission protocols. Tanzu Observability protects the transactions themselves through configuration management and monitoring for deviations. All events are reviewed daily for suspicious activity. Remediation processes are in place and applied to all potentially affected environments immediately.