Technical White Paper: **August 2023**

VMware Tanzu

PCI best practices for containers and container orchestration

vmware®

Table of contents

Introduction

This document provides guidance for the secure use of containers and container orchestration tools in a payment environment with VMware Tanzu. It serves as a how-to guide for customers who need to follow vendor best practices outlined by the Payment Card Industry (PCI) Security Standards Council (SSC) 2022 Information Supplement: Guidance for Containers and Container Orchestration when using VMware offerings, including:

VMware Tanzu® Application Platform™

VMware Tanzu® Build Service™

VMware Application Catalog™

VMware Image Builder™

VMware Tanzu® Mission Control™

VMware Tanzu® Service Mesh™

VMware Tanzu® Kubernetes Grid™

VMware Tanzu® Application Service™

VMware Aria Operations™ for Applications

VMware Aria Automation™ for Secure Clouds

VMware Carbon Black Cloud™

Audience

This document provides VMware Tanzu customers, service providers and their qualified security assessors (QSA) with the information they need when running a cardholder data environment (CDE) that includes VMware technologies. Although this document was developed with the PCI Data Security Standard (DSS) Level 1 category in mind, it is valuable to all VMware Tanzu deployers and operators.

Merchants and service providers gain guidance on security considerations that apply to using VMware Tanzu products in a containerized payment environment.

Assessors can better understand security issues when assessing a payment environment that uses VMware Tanzu products.

Best practice scope

This document provides supplemental guidance and best practices, but it does not add, extend, replace or supersede requirements in any PCI SSC standard. As general software platforms, Tanzu Application Platform, Tanzu Build Service, Tanzu Kubernetes Grid and Tanzu Application Service cannot be assessed as being “compliant” or “not compliant” with PCI. Only an actual CDE—which might include these deployments, along with the related technology infrastructure and associated people and processes—can be assessed for compliance with PCI. VMware SaaS services, Tanzu Mission Control, Tanzu Service Mesh, Aria Operations for Applications, CBC and SS do not store, transmit nor process cardholder data but potentially could be scoped as dependent and connected systems and should be assessed as needed based on customer and QSA-defined CDE scope.

Demonstrating compliance

As with other audit and compliance standards, satisfying the PCI DSS standard is not simply a matter of installing and configuring the software. Compliance with PCI requires both technical and nontechnical controls to be in place. A generally recurring theme throughout the PCI standard is the need to demonstrate that the necessary technical controls exist within the CDE and that these controls are being properly managed as a normal part of doing business. The organization must show evidence that the necessary technical controls are active within the CDE. In addition, the organization must then show that the associated policies and management procedures are documented, in use and known to the people who are responsible for maintaining these controls within the CDE. The combination of these controls is often summarized with the phrase "People, Process and Technology." The scope of a PCI DSS audit covers all three.

Containers, container orchestration Tools, and VMware Tanzu

A containerized application can run without concern for the underlying host and be easily transferred between hosts.

Containers

A container is a lightweight, standalone package that encapsulates a complete runtime environment, including an application and its dependencies (libraries, binaries and any additional configuration files), increasing the application's portability, scalability, security and agility.

A container fully encapsulates a minimal operating system layer along with a layer with the application runtime, such as .Net, Node or Spring, and the code that is being run. Packaging an application with these components removes external dependencies, and keeps all internal dependencies running at versions required by the application.

Containers are popular with both developers and operators because they offer a straightforward way to deploy and manage applications regardless of the target environment. They facilitate DevOps and DevSecOps practices by improving handoffs between development and operations teams.

Containers consume resources efficiently, enabling high density and resource utilization. Although you can use a container with almost any application, they are frequently associated with microservices in which multiple containers run separate application components or services. The containers that make up an application are typically coordinated and managed using a container orchestration platform, such as Kubernetes.

Using a container to build an application accelerates the delivery of new functionality and encourages an environment of continuous innovation. The benefits include

- **Agility** – Improved developer agility increases productivity and speed. Containers streamline CI/CD pipelines and are ideal for DevOps teams and microservices deployments.
- **Scalability** – Using Kubernetes, you can automatically scale a container deployment up or down as workload requirements change.
- **Portability** – A container consumes fewer resources and is more lightweight than a virtual machine (VM). A containerized application is infrastructure-agnostic and operates the same regardless of where it is deployed.
- **Resilience** – A containerized application is isolated and abstracted from the OS and other containers, so one container can fail without impacting other running containers.

Container Orchestration Tools

Container orchestration helps manage the complexity of the container lifecycle, which is especially important for distributed applications with a large number of containers. The most common container orchestration tool used today is Kubernetes, which includes an ever-growing set of features for controlling containers, container networks, routing, scaling, logs, eventing and more.

Each feature configuration is completed with a series of YAML files that define the configuration, secrets and state. Figure 1 shows some of the configurations needed to get an application operating in Kubernetes container orchestration tools.

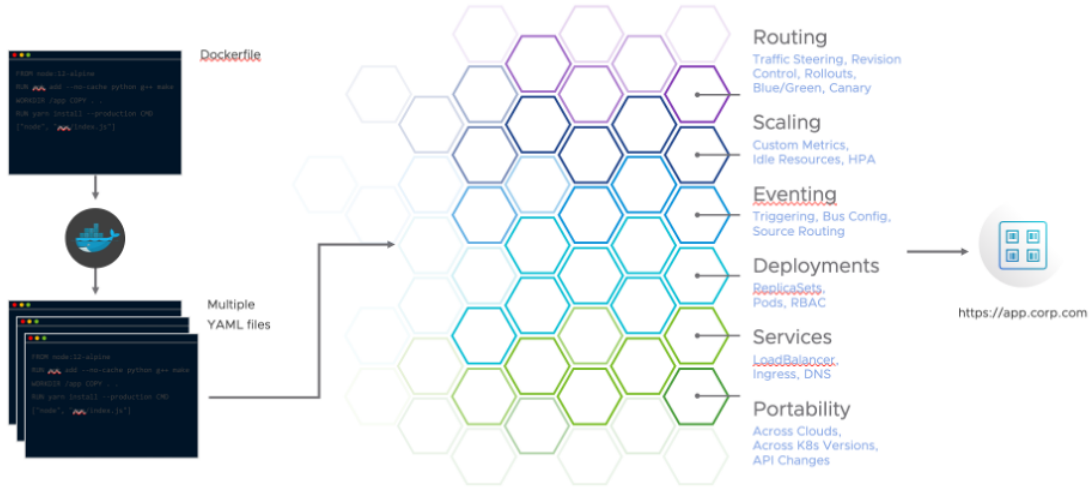

Figure 1: Kubernetes run application components.

There are three primary VMware Tanzu container orchestration platforms.

- **Tanzu Application Service** – Based on Cloud Foundry, Tanzu Application Service uses BOSH to orchestrate VM configuration, availability and scaling. The Cloud Foundry components provide application container building, registry, application deployment, scaling, routing, secrets, segmentation and service integration. For details, see the Tanzu Application Service PCI primer document.
- **Tanzu Application Platform** – Based on Backstage, Cartographer, Cloud Native Buildpacks and other CNCF and VMware tools, provides automated application container builds, registry, application deployment, scaling, routing, service integration and more. This document addresses Tanzu Application Platform best practices.
- **Tanzu for Kubernetes Operations** – Including capabilities to simplify Kubernetes operations like automated deployment, load balancing, resource allocation and security enforcement for containers via declarative configuration and automation. It keeps containerized applications running in their desired state, ensuring that they are scalable and resilient. An application deployed to Kubernetes requires more tools and processes than one using Cloud Foundry. Tanzu for Kubernetes Operations also supports compliant Kubernetes cluster management, service mesh and observability services. This document addresses Tanzu for Kubernetes Operations best practices.

There are many open-source projects to enable the full configuration of Kubernetes as an application and container orchestration tool. Figure 2 shows the most essential projects that are supported by the Cloud Native Computing Foundation (CNCF). VMware Tanzu offers products and product bundles that are built from many of these projects. VMware is also an active open-source contributor and committer to these essential CNCF projects.

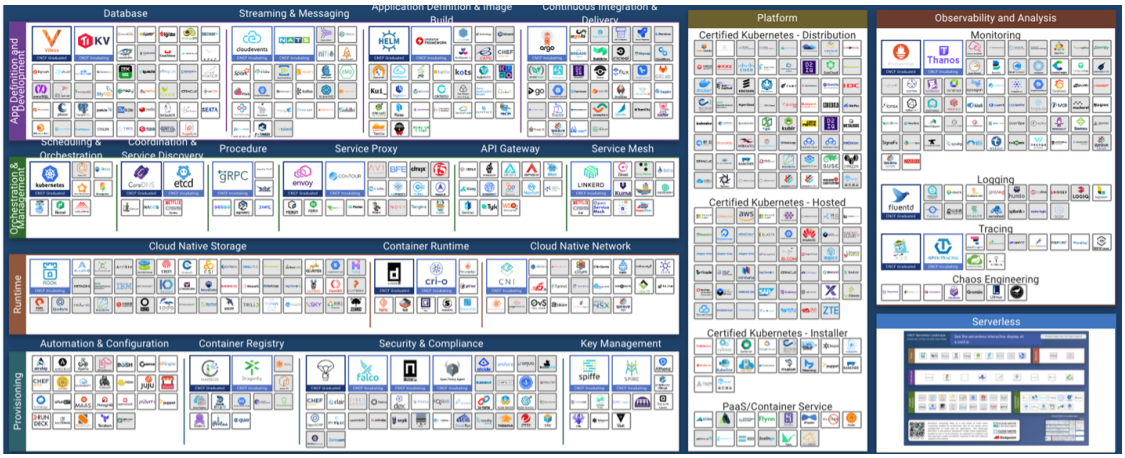

Figure 2: CNCF projects.

Tanzu Application Platform

To enable developers to rapidly develop applications and microservices, Tanzu Application Platform builds on Backstage, Cartographer and Cloud Native Buildpacks. Tanzu Application Platform provides the following functionality:

- Preapproved template accelerators to build business requirements
- Documentation and learning center for existing applications, APIs, programs and standards
- Up-to-date container buildpacks to build and continuously rebuild with the latest update application containers
- Container software bill of materials (SBOM) generation and security scanning
- Third-party security and tool integrations
- Gatekeeping automation that allows only preapproved paths to production
- Preapproved secure container deployment configurations based on application and Kubernetes or cloud requirements to deploy to Knative, Kubernetes, public cloud or edge
- Container signing and registry
- Managed deployment of applications in built, test and run clusters, such as Tanzu Kubernetes Grid or public cloud Kubernetes and Knative clusters

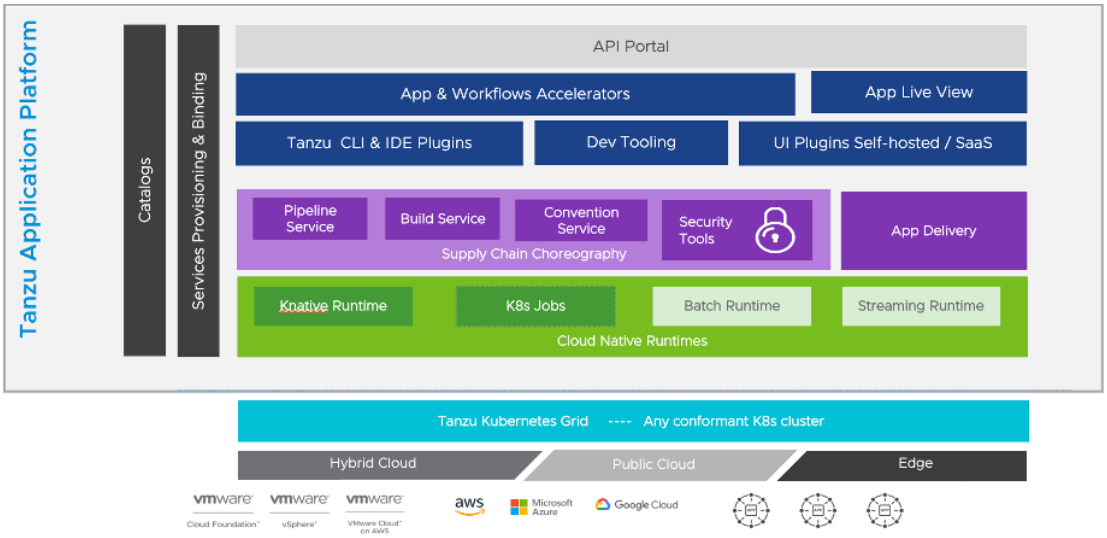

Figure 3: Tanzu Application Platform layered API and capabilities.

While it is possible to leverage Tanzu Application Platform for a payment application that the PCI Payment Application Data Security Standard (PA-DSS) could apply to, this PCI best practices document does not cover PA-DSS. The processes for building, signing, storing and then deploying to Kubernetes are addressed in the *Threats and best practices* section. A payment application managed and deployed by Tanzu Application Platform could also have Kubernetes run clusters that are within a PCI CDE, and the configuration generation and application deployment could be in scope for the PCI CDE.

VMware Application Catalog

VMware Application Catalog provides up-to-date and tested container images for the most common open-source applications, such as Nginx, RabbitMQ and MySQL. This catalog is based on Bitnami technology and provides the latest support and testing for all container layers, including a customizable base operating system and the application runtime. All applications are scanned for viruses, malware and vulnerabilities and are smoke-tested on Tanzu Kubernetes Grid and multiple public cloud platforms. All containers are signed, and metadata from all tests and scans is available with every Helm chart installer and application image.

Tanzu for Kubernetes Operations

Tanzu for Kubernetes Operations is a bundle of products that provide all the needed components and services for running and managing secure and compliant Kubernetes-based applications at scale. Tanzu for Kubernetes Operations provides container tools for managing Kubernetes clusters security, policies, services and configurations in addition to service mesh, backup, observability and authentication orchestration tools.

Tanzu for Kubernetes Operations consists of multiple VMware products providing custom and CNCF project integrations, including

- Tanzu Kubernetes Grid – Kubernetes runtime for any cloud
  - Antrea Container Network Interface (CNI) – Ingress/egress/network policies
  - Multus CNI – Allows multiple network interfaces to attach to pods
  - Contour – Kubernetes ingress service
  - Cert-Manager – Manage certificates used in Kubernetes
  - ExternalDNS – Publish DNS records to DNS servers
- Tanzu Mission Control – Kubernetes policies, cluster lifecycle, authentication, backups and catalog
  - Pinniped – Authentication
  - Harbor – Container image registry
  - Velero – Backups
  - Open Policy Agent – Kubernetes security admission policy controller
  - VMware Application Catalog, Service Mesh and Observability integration
  - Sonobuoy – CIS and conformance tests

- **Tanzu Service Mesh** – Service mesh
  - Global namespace (GNS) – Intra-cluster routable service mesh with full Tanzu Application Platform supply chain integration. GNS is designed for teams responsible for managing and maintaining applications and APIs in a multi-cloud and multi-namespace environment. It is also useful for teams that need to ensure high availability, security and resiliency for their applications
  - Enforce mTLS – Authenticate and enforce connectivity mesh
  - Istio service mesh with custom VMware extensions
  - API security, mapping and monitoring
  - Automates connectivity, resiliency and security policies for apps and APIs
  - Connects apps and APIs across one or multiple namespaces, clusters or clouds
  - PII/PHI tracking
  - SLO/SLA monitoring and enforcement
  - Provides a logical and physical view for better understanding and management of applications
  - Offers a wide range of services, including naming/DNS rules, discovery of app components, APIs, and data, certificate management, observability and insights, and policies/enforcement
  - Provides risk profiles as indicators of risk
  - Integrates with external tooling to get additional telemetry metrics
- **Aria Operations for Applications**
  - Prometheus – Kubernetes statistics and time-based event monitoring
  - Fluent Bit – Node and application log export and monitoring
- **NSX Advanced Load Balancer** – AVI
  - Global DNS load balancing
  - DDOS protection
  - Kubernetes ingress
  - Web Application Firewall (WAF) with OWASP protection

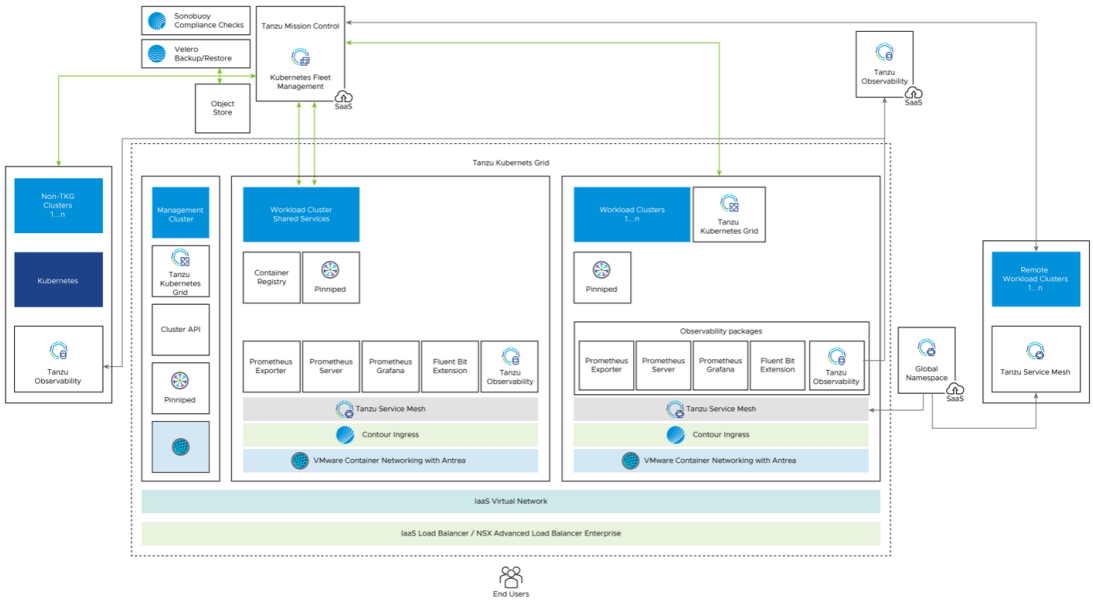

Figure 4: Tanzu for Kubernetes Operations.

Tanzu Mission Control, Tanzu Service Mesh, Aria Operations for Applications and VMware Application Catalog are all SaaS products. You can enroll or onboard CDE Kubernetes systems into the Tanzu Services, which will then manage controls for the onboarded CDE systems. The VMware SaaS services do not store, transmit nor process card data, but they might have the ability to manage authentication, segmentation or other security controls. Tanzu Kubernetes Grid, Antrea and other CNI, and the VMware NSX® advanced load balancer based on AVI could all be in scope if used to run cardholder applications where they could be part of CDE systems.

Tanzu Kubernetes Grid and Antrea CNI

Tanzu Kubernetes Grid provides organizations with a consistent, upstream-compatible Kubernetes container orchestration system that is ready for end-user workloads and ecosystem integrations. Tanzu Kubernetes Grid provides the Kubernetes runtime for Tanzu for Kubernetes Operations. Tanzu Kubernetes Grid runs natively with VMware vSphere® and VMware ESX® or on any public cloud, sovereign cloud or edge cluster deployment.

Antrea, a Kubernetes CNI, is a CNCF VMware project that provides the Kubernetes virtual network and includes network policy controls for ingress and egress controls for a container running within Kubernetes.

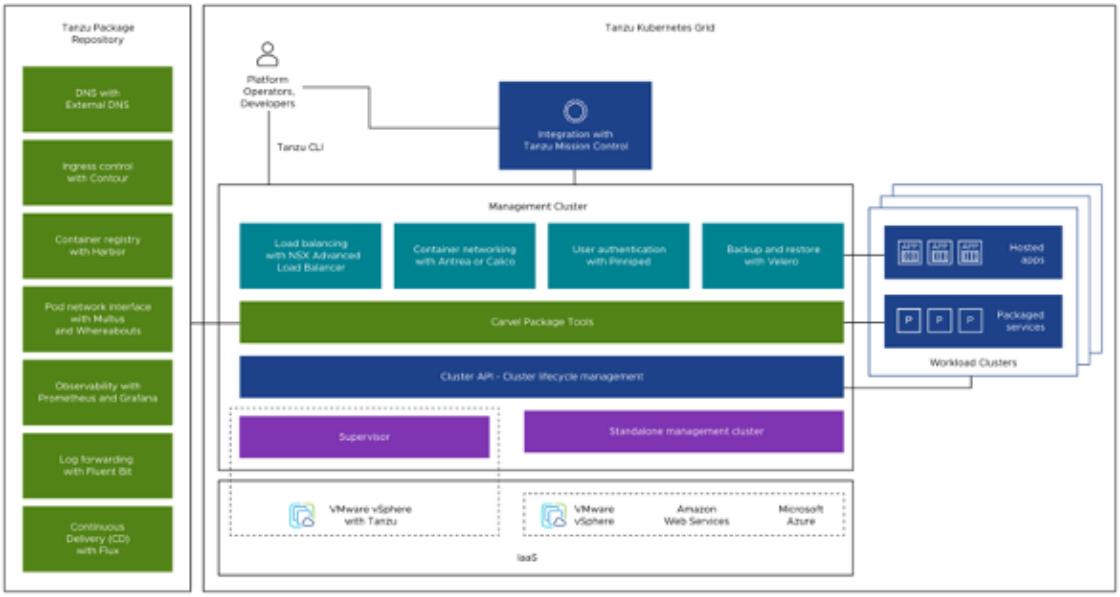

Figure 5: Tanzu Kubernetes Grid.

Kubernetes clusters can process and transmit cardholder data and can be in scope for the PCI CDE. Many best practices and PCI controls are highlighted in the following sections.

Tanzu Mission Control

Tanzu Mission Control is a platform for Kubernetes container orchestration management that provides a single control point to manage Kubernetes and operate containerized applications across multiple clouds and clusters.

Tanzu Mission Control provides instances of the service in regions around the world, including Australia, Canada, Ireland, Japan, United States, and most recently in Mumbai, India. There is also a non-SaaS version available for customers unable to use SaaS but who still need the container orchestration management features provided by Tanzu Mission Control.

Some of the Kubernetes cluster management capabilities of Tanzu Mission Control include

- **Lifecycle management** – Connect to a cloud provider account to create clusters, resize and upgrade them, and delete clusters that are no longer needed. For more information, see Cluster Lifecycle Management.
- **Observability and diagnostics** – See the health and resource usage for each Kubernetes cluster from a single console, and view cluster details, namespaces, nodes and workloads directly from the Tanzu Mission Control console. For more information, see Observation and Analysis of Cluster Health and Resources.
- **Inspections** – Run preconfigured inspections against Kubernetes clusters using Sonobuoy to ensure consistency over your fleet of clusters. For more information, see Cluster Inspections.
- **Data protection** – Back up and restore the data resources in Kubernetes clusters using Velero. For more information, see Data Protection.
- **Access control** – Use federated identity management and apply granular role-based access control to fine-tune security access requirements. For more information, see Access Control.
- **Policy management** – Create policies to consistently manage Kubernetes clusters, namespaces and workloads. For more information, see Policy-Driven Cluster Management.

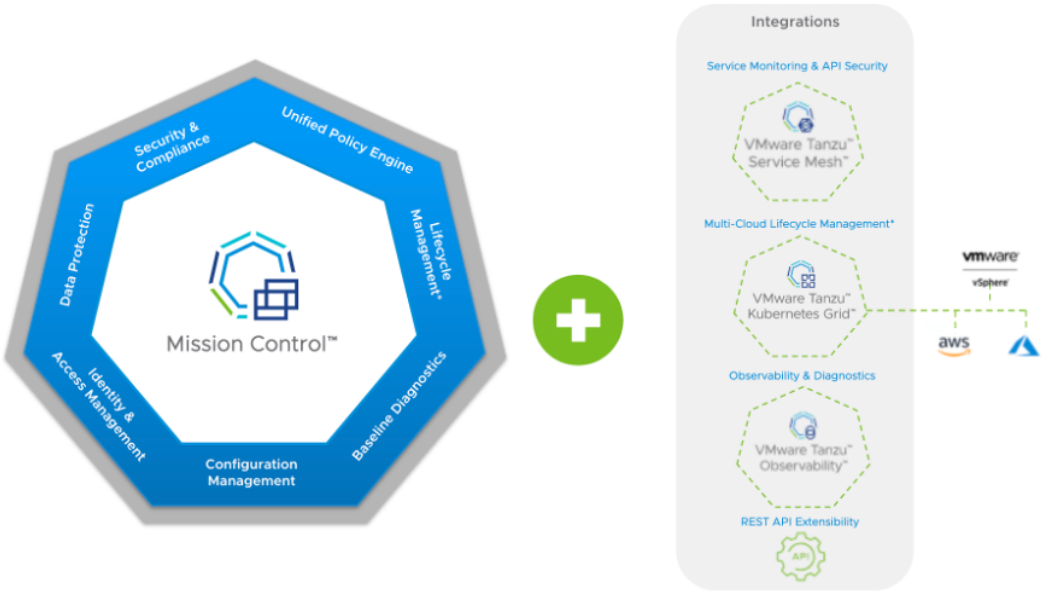

Figure 6: Tanzu Mission Control capabilities.

Tanzu Mission Control has both SaaS and non-SaaS product versions that can connect to CDE systems or manage controls for CDE systems. Tanzu Mission Control does not store, transmit or process card data. Because it can manage security, authentication and other controls for CDE systems, it potentially could be scoped as dependent and connected systems and should be assessed as needed based on the customer- and QSA-defined CDE scope.

Tanzu Service Mesh

Tanzu Service Mesh provides fine-grain traffic management policies that give control and visibility into how traffic, API calls and data flow between services and across clusters and clouds. It runs on multiple application platforms, public clouds and runtime environments, including Kubernetes clusters.

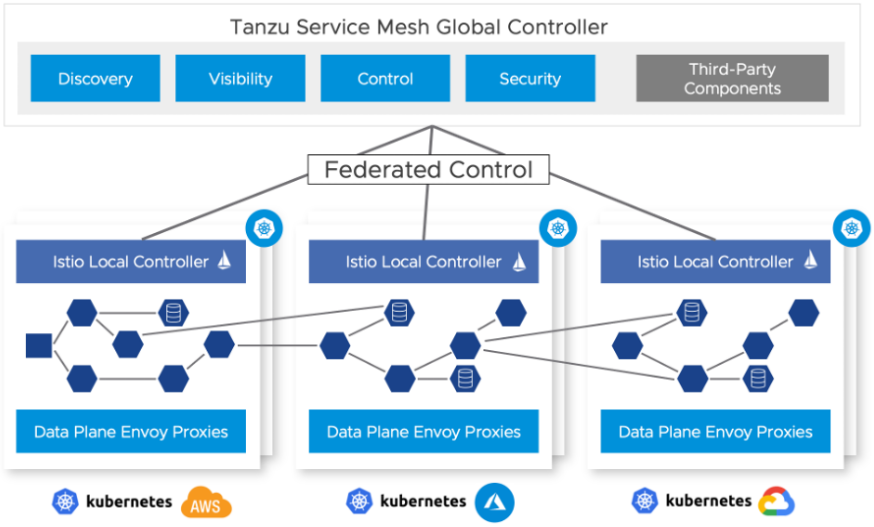

Figure 7: Tanzu Service Mesh.

Tanzu Service Mesh supports cross-cluster and cross-cloud use cases with global namespaces to enable traffic management policies across multiple clusters and locations, and security policies across cloud silos and boundaries, regardless of where the applications are running.

Tanzu Service Mesh can track complete transactions—from the point an application end user makes a request and continuing as that request flows through the service mesh—including services, APIs and data (PCI and PII data visibility and control). Tanzu Service Mesh enables application teams to implement business context-aware policies to ensure performant and secure transactions. In addition to rich transaction-level metrics and visualizations, Tanzu Service Mesh offers application and data-level security policies.

Tanzu Service Mesh is composed of a SaaS product that manages service mesh configuration and a local Kubernetes service that performs the service mesh connectivity. You can connect Tanzu Service Mesh to CDE systems providing service mesh configuration and managing connectivity between applications and services. The Kubernetes component can transmit cardholder data, but that data does not get communicated back to the Tanzu Service Mesh SaaS service. The SaaS side of Tanzu Service Mesh does not store, transmit or process card data, but potentially could be scoped as dependent and connected systems and should be assessed as needed based on the customer- and QSA-defined CDE scope.

Aria Operations for Applications

Aria Operations for Applications (formerly Tanzu Observability) is a high-performance streaming analytics platform that supports observability for metrics, counters, histograms, traces and spans. Aria Operations for Applications can collect data from many services and sources across your entire application stack and can look at details for data that was ingested earlier.

Some of the capabilities of Aria Operations for Applications include:

- **Charts and dashboards** – Visualize information using filters and functions to see exactly what is needed.

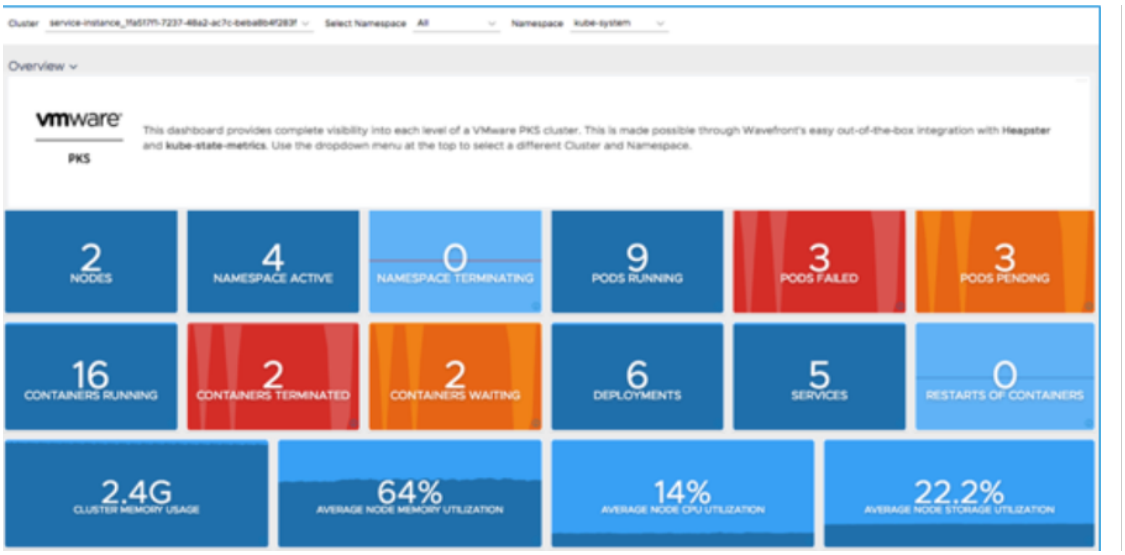

Figure 8: Aria Operations for Applications.

- **Alerts** – To detect problems, create alerts directly from charts, such as when the CPU reaches a certain threshold.
- **Distributed tracing** – In an application that consists of multiple services, an incoming request typically starts a chain of requests that are propagated from one service to the next. Distributed tracing gives end-to-end visibility into the chain across services, even when the services are running in different environments. This visibility can help find errors and performance problems in code. OpenTracing and OpenTelemetry are supported.

Aria Operations for Applications is a SaaS product. You can connect it to CDE systems providing observability for containers, clusters, applications and services, but the SaaS service does not store, transmit or process card data, although it potentially could be scoped as dependent and connected systems and should be assessed as needed based on customer- and QSA-defined CDE scope.

Also, depending on the developer configuration, a misconfigured or programmed application can potentially leak cardholder data that could make its way into Aria Operations for Applications. Aria Operations for Applications provides an egress proxy and filter function that can prevent leaking or transpose critical data to harmless data. Proxy configuration should be part of the scope and assessment for a business or service provider PCI validation.

VMware NSX Advanced Load Balancer

VMware NSX Advanced Load Balancer (formerly known as Avi Networks) makes it easy to apply load balancing, a web application firewall and a container ingress to any application in any data center and cloud.

VMware NSX Advanced Load Balancer offers these benefits:

- **Multi-cloud consistency** – Simplify administration with centralized policies and operational consistency.
- **Pervasive analytics** – Gain unprecedented insights with application performance monitoring and security.
- **Full lifecycle automation** – Free teams from manual tasks with application delivery automation.
- **Future proof** – Extend application services seamlessly to cloud native and containerized applications.

The VMware NSX Advanced Load Balancer architecture separates the data and control planes to deliver application services beyond load balancing, such as application analytics, predictive autoscaling, micro-segmentation and self-service for application owners in on-premises or cloud environments.

The platform provides a centrally managed, dynamic pool of load balancing resources on commodity x86 servers, VMs or containers to deliver granular services close to individual applications, so you can scale up network services without the added complexity of managing hundreds of disparate appliances.

The NSX Advanced Load Balancer consists of a control plane and data plane. Depending on the configuration, the control plane components might not be part of a CDE. The components do not store, transmit or process card data but do provide management and are connected to the data plane, which runs inside of and part of deployed applications, which can be within a CDE. The exact deployment should be assessed as needed based on the customer- and QSA-defined CDE scope.

Threats and best practices for container orchestration tools

When best practices are not applied, the use of containers and container orchestration tools can adversely affect the security of an environment. The correct application of industry best practices is critical for addressing plausible threats to the containers and container orchestration tools. The Tanzu PCI SSC *Best Practices for Containers and Container Orchestration Tools* includes sample threats to container or container orchestration tools, best practices and VMware Tanzu product-specific guidelines to interpret the potential controls needed when using Tanzu components within a container orchestration system.

The following tables present common threats to environments employing VMware Tanzu tools and possible best practices for addressing these threats. Many of the best practices are also applicable outside of a containerized environment and might be required in some PCI SSC standards. For more details, see the applicable PCI SSC standards.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
1. Authentication						
1.1 The container orchestration tool provides unauthenticated access to APIs, allowing unauthorized modification of workloads.	Configure all access to orchestration tool components and supporting services, for example, monitoring from users or other services, to require authentication and individual accountability.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service APIs require authentication and can be configured with federated authentication.	You can configure Tanzu Kubernetes Grid manually or with Tanzu Mission Control to use federated external authentication with strong access controls. Antrea is native to Kubernetes as a CNI and uses the Kubernetes API, which is secured using the above process.	Tanzu Mission Control uses VMware Cloud™ services and provides authenticated access.	Tanzu Service Mesh uses VMware Cloud services and provides authenticated access.	Aria Operations for Applications uses VMware Cloud services and provides authenticated access.
1.2 Generic administrator accounts are in place for container orchestration tool management. Using these accounts prevents the non-repudiation of individuals with administrator account access.	Tie all user credentials for authenticating to the orchestration to specific individuals. Do not use generic credentials. When a default account is present and cannot be deleted, changing the default password to a strong unique password and then disabling the account prevents malicious individuals from reenabling the account and gaining access with the default password.	Tanzu Application Platform and Tanzu Build Service include default service accounts that you can strongly configure as suggested. VMware Application Catalog does not provide nor use generic administrator accounts.	You can configure Tanzu Kubernetes Grid with generic or certificate-based accounts, which can be disabled when external authentication is enabled either manually or with Tanzu Mission Control integration. Antrea is native to Kubernetes as a CNI and uses the Kubernetes API, which is secured using the above process.	Tanzu Mission Control includes a default initial account that should not be used after initial configuration. Instead, configure Tanzu Mission Control to federate authentication through customer authentication systems.	Tanzu Service Mesh does not provide generic administration accounts.	Aria Operations for Applications does not provide generic administration accounts.

Threats and Best Practices table originally published in the Payment Card Industry (PCI) Security Standards Council (SSC) 2022. Information Supplement: Guidance for Containers and Container Orchestration

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
1. Authentication						
1.3 Credentials, such as client certificates, do not provide for revocation. Lost credentials present a risk of unauthorized access to cluster APIs.	Make sure that authentication mechanisms used by the orchestration system store credentials in a properly secured datastore.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service use Kubernetes credential and secret store.	Tanzu Kubernetes Grid supports a secure credential and secret store. Configure it to use external federated authentication configured either manually or through Tanzu Mission Control. Antrea is native to Kubernetes as a CNI and uses the Kubernetes API, which is secured using the above process.	Tanzu Mission Control provides a secure credential store. However, it is recommended to federate authentication to customer authentication system.	Tanzu Service Mesh provides a secure credential store. However, it is recommended to use federated authentication to customer authentication system.	Aria Operations for Applications provides a secure credential store. However, it is recommended to use federated authentication to customer authentication system.
1.4 Availability of automatic credentials for any workload running in the cluster. These credentials are susceptible to abuse, particularly if given excessive rights.	Provide credentials to services running in the cluster only when explicitly required. Configure service accounts for least privilege. The level of rights depends on how the cluster RBAC is configured.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service design specifically enables orchestration and automated building and deploying. Configure service accounts with least privilege.	Configure Tanzu Kubernetes Grid with minimal privileges for all service, system, supply chain and user accounts. You can configure this option manually or with Tanzu Mission Control. Antrea is native to Kubernetes as a CNI and uses the Kubernetes API, which is secured using the above process.	Tanzu Mission Control installs management services in each managed Kubernetes cluster with the privileges necessary to operate. The service is installed with service-level authorization and not managed by RBAC.	Tanzu Service Mesh installs management services in each managed Kubernetes cluster with the privileges necessary to operate. The service is installed with service-level authorization and not managed by RBAC.	Aria Operations for Applications installs management services in each managed Kubernetes cluster with the privileges necessary to operate. The service is installed with service-level authorization and not managed by RBAC.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
1. Authentication						
1.5 Static credentials (passwords) used by administrators or service accounts are susceptible to credential stuffing, phishing, keystroke logging, local discovery, extortion, password spray, and brute force attacks.	Grant access to orchestration systems for users or services based on least privilege. Do not use blanket administrative access.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service automate the build process and can leverage Kubernetes based secrets. VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service should also have restricted access limiting this risk.	Configure Tanzu Kubernetes Grid to use federated RBAC either manually or with Tanzu Mission Control. Configure this access for all orchestration, service accounts, clusters and user accounts. Do not use blanket administrative access. Antrea is native to Kubernetes as a CNI and uses the Kubernetes API, which is secured using the above process.	Tanzu Mission Control installs management services in each managed Kubernetes cluster. The Tanzu Mission Control service is granted least privilege access, which is not managed nor controllable by administrators or users.	Tanzu Service Mesh installs management services in each managed Kubernetes cluster. The Tanzu Service Mesh service is granted least privilege access, which is not managed or controllable by administrators or users.	Aria Operations for Applications installs management services in each managed Kubernetes cluster. Aria Operations for Applications is granted least privilege access, which is not managed or controllable by administrators or users.
2. Authorization						
2.1 Excessive access rights to the container orchestration API could allow users to modify workloads without authorization.	Grant access to orchestration systems for users or services based on least privilege. Do not use blanket administrative access.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service are automated systems that do not provide API access or users access into the system to modify workloads. Tanzu Application Platform accelerators and deployment code are predefined and approved by security and not modifiable by end users.	Configure Tanzu Kubernetes Grid to restrict access based on least privilege and enable customized role configuration. This configuration can be manual or done through Tanzu Mission Control. Antrea is native to Kubernetes as a CNI and uses the Kubernetes API, which is secured using the above process.	Tanzu Mission Control includes a default initial account which should not be used after initial configuration. Instead, configure Tanzu Mission Control to federate authentication through customer authentication systems. Tanzu Mission Control uses VMware Cloud services and provides authenticated access.	Tanzu Service Mesh uses VMware Cloud services and provides authenticated access.	Aria Operations for Applications uses VMware Cloud services and provides authenticated access.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
2. Authorization						
2.2 Hard-coded access groups provide excessive access rights to the container orchestration tools.	All access granted to an orchestration tool should be capable of modification. Do not hard-code access groups.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service access is granted through configurable options and does not contain hard-coded groups or rights.	Tanzu Kubernetes Grid access rights are configured through an extensive Kubernetes authorization system that you can manually configure or integrate with Tanzu Mission Control. Antrea is native to Kubernetes as a CNI and uses the Kubernetes API, which is secured using the above process.	Tanzu Mission Control uses VMware Cloud services and provides authenticated access that you can modify and does not contain hard-coded access groups.	Tanzu Service Mesh uses VMware Cloud services and provides authenticated access that you can modify and does not contain hard-coded access groups.	Aria Operations for Applications uses VMware Cloud services and provides authenticated access you can modify and does not contain hard-coded access groups.
2.3 Accounts accumulate permissions without documented approvals.	Use manual and automated means to regularly audit implemented permissions.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service are configured for automation, are not manually edited, and do not change permissions without following change management processes.	Configure Tanzu Kubernetes Grid to use an external federated identify provider that follows standard change control processes that require permission and approval for changes.	Configure Tanzu Mission Control to use an external federated identity provider that follows standard change control processes that require permission and approval for changes.	Configure Tanzu Service Mesh to use an external federated identity provider that follows standard change control processes that require permission and approval for changes.	Configure Aria Operations for Applications to use an external federated identity provider that follows standard change control processes that require permission and approval for changes.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
3. Workload security						
3.1 Access to shared resources on the underlying host permits container breakouts to occur, compromising the security of shared resources.	Configure workloads running in the orchestration system to prevent access to the underlying cluster nodes by default. Grant access to resources provided by the nodes based on least privilege, and avoid using "privileged" mode containers.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service configuration does not provide access to underlying host clusters or nodes.	You can configure Tanzu Kubernetes Grid to restrict access to the underlying host. Using Tanzu Mission Control, the Kubernetes policies can be automatically applied to prevent host and privileged access when running containers.	Tanzu Mission Control provides automated management of Kubernetes clusters, enabling policies that can disable host access and privileged access except where specifically required.	Tanzu Service Mesh does not provide access to the underlying host nor grant privileged access to any containers running. Tanzu Service Mesh can enable least privileged network access between containers and restrict and require mutual Transport Layer Security (TLS), enforcing nonprivileged access to running container applications.	Aria Operations for Applications does not enable or provide underlying host access or privileged access.
3.2 Using nonspecific versions of container images could facilitate a supply chain attack in which an attacker pushes a malicious version of the image to a registry.	Workload definitions and manifests should target specific known versions of container images using a reliable mechanism that checks an image's cryptographic signature. If signatures are not available, use message digests.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service generate secure application containers and use specific versions and signatures when deploying into clusters.	Tanzu Kubernetes Grid supports configuring a deployment with a specific version or tag mechanism. Tanzu Application Platform provides a secure supply chain to securely deploy updated versions based on the approved build completion.	Tanzu Mission Control does not provide container image version details but can provide policies that restrict namespaces and namespace groups (workspaces) to allow loading images only from authorized registries. Deployed Tanzu Mission Control agents are managed using a specific version hash to prevent supply chain attacks.	Tanzu Service Mesh does not provide container image versioning. Deployed Tanzu Service Mesh agents are managed using a specific version hash to prevent supply chain attacks.	Aria Operations for Applications does not provide container image versioning. Deployed Aria Operations for Applications agents are managed using a specific version hash to prevent supply chain attacks.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
3. Workload security						
3.3 Containers retrieved from untrusted sources can contain malware or exploitable vulnerabilities.	All container images running in the cluster should come from trusted sources.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service build secure images that are signed and pushed to approved supply chain registries and build from VMware-provided images that provide provenance and secure updates.	You can configure Tanzu Kubernetes Grid manually or through a Tanzu Mission Control policy to allow only authorized registries to supply images to namespaces.	Tanzu Mission Control policies can enforce namespace or groups of namespaces (workgroup) to provide images only from predefined and approved image registries. It is recommended to build images with Tanzu Application Platform or Tanzu Build Service using VMware provided, secured and signed images. Tanzu Mission Control service containers can be retrieved from a configurable registry option, enabling downloading from VMware registry or from an internal controlled registry.	Tanzu Service Mesh does not control Kubernetes source configuration. Tanzu Service Mesh service containers can be retrieved only from VMware registry.	Tanzu Service Mesh does not control Kubernetes source configuration. Aria Operations for Applications service containers can be downloaded only from VMware registry.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
4. Network security						
4.1 Container technologies with container networks that do not support network segmentation or restriction allow unauthorized network access between containers.	Configure container orchestration tool networks on a default deny basis with access explicitly required only for the operation of the applications in scope.	Tanzu Build Service does not use or configure network segmentation. You can integrate Tanzu Application Platform with secure supply chains into Tanzu Service Mesh or Tanzu Mission Control or directly into a Kubernetes deployment to deploy preapproved network segmentation controls using service mesh or native CNI network policies.	Tanzu Kubernetes Grid with Antrea or another CNI provides network policies to segment network access between containers. You can configure the network policies manually or with Tanzu Mission Control. When used with VMware NSX-T Data Center™, cluster and node-level distributed segmentation is possible with NSX distributed firewalls.	Tanzu Mission Control provides network policy management for managed Kubernetes clusters. Policies can be preconfigured and associated to clusters or cluster-groups, allowing new clusters to inherit a preconfigured network policy configuration.	Tanzu Service Mesh provides secure TLS and authenticated mTLS connections between containers, along with policies to enforce segmentation between containers not authorized to communicate.	Aria Operations for Applications does not provide segmentation services but can be used to observe events from segmentation technologies and observe or alert on connections not allowed or attempted.
4.2 Access from the container or other networks to the orchestration component and administrative APIs could allow privilege escalation attacks.	Restrict access to orchestration system components and other administrative APIs using an explicit allow-list of IP addresses.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service do not provide network segmentation controls. Tanzu Application Platform can enable Tanzu Service Mesh or network policies in a secure supply chain deployment that could prevent access to administrative APIs.	Tanzu Kubernetes Grid with Antrea or another CNI provides network policies to segment access to administrative APIs. If used with NSX-T, you can use NSX-T distributed firewalls to segment container access to administrative APIs.	Tanzu Mission Control provides network policy management for managed Kubernetes clusters to prevent access to administrative APIs. Policies can be preconfigured and associated to clusters or cluster-groups, allowing new clusters to inherit a preconfigured network policy configuration.	Tanzu Service Mesh provides secure TLS and authenticated mTLS connections between containers, along with policies to enforce segmentation between containers and administrative APIs.	Aria Operations for Applications does not provide segmentation services, but you can use it to observe events from segmentation technologies and observe or alert on connections not allowed or attempted.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
4. Network security						
4.3 Unencrypted traffic with management APIs is allowed as a default setting, allowing packet sniffing or spoofing attacks.	All traffic with orchestration system component APIs should be over encrypted connections, ensuring that encryption key rotation meets PCI key and secret requirements.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service provide encrypted APIs for managing VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service services.	All Tanzu Kubernetes Grid APIs are encrypted.	All Tanzu Mission Control management APIs are encrypted.	All Tanzu Service Mesh management APIs are encrypted.	All Aria Operations for Applications management APIs are encrypted.
5. PKI						
5.1 The inability of some container orchestration tool products to support revocation of certificates can lead to misuse of a stolen or lost certificate.	If revocation of certificates is not supported, use certificate-based authentication. Rotate certificates as required by PCI or customer policies or if a container is compromised.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service do not use certificate-based authentication.	Tanzu Kubernetes Grid supports certificate authentication, but best practice is to enable external federated authentication, which you can configure manually or through Tanzu Mission Control. If using Tanzu Kubernetes Grid certificates, there is a documented process for rotating certificates.	Tanzu Mission Control does not support certificate authentication.	Tanzu Service Mesh does not support certificate authentication.	Aria Operations for Applications does not support certificate authentication.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
5. PKI						
5.2 PKI and Certificate Authority services integrated within container orchestration tools might not provide sufficient security outside of the container orchestration tool environment, which could lead to exploitation of other services that attempt to use this chain of trust.	Do not trust certificates issued by orchestration tools outside of the container orchestrator environment because the container orchestrator's Certificate Authority (CA) private key can have weaker protection than other enterprise PKI trust chains.	When using certificates with Tanzu Build Service or Tanzu Application Platform, a CA integration establishes trust only with the certificate providers used.	When using certificates with Tanzu Kubernetes Grid, a CA integration establishes trust only with the certificate providers used.	Tanzu Mission Control does not use PKI.	Tanzu Service Mesh does not use PKI.	Aria Operations for Applications does not use PKI.
6. Secrets management						
6.1 Inappropriately stored secrets, including credentials, provided through the container orchestration tool could be leaked to unauthorized users or attackers with some level of access to the environment.	Hold all secrets needed for the operation of applications hosted on the orchestration platform in an encrypted dedicated secrets management system.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service leverage platform-native secrets tools for encryption.	Tanzu Kubernetes Grid supports encrypting the etcd secrets system for Kubernetes. The encryption can use a preconfigured secret or tie into a key management system.	Tanzu Mission Control has secrets used for service integration as well as secrets tied to backups running on managed clusters. All secrets are stored in an encrypted dedicated secrets management system.	Tanzu Service Mesh uses Kubernetes secrets, which can be encrypted and on dedicated secrets management system.	Aria Operations for Applications has an encrypted dedicated management system for platform secrets and for secrets used within managed clusters use Kubernetes secrets, which can be encrypted and on dedicated secrets management system.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
6. Secrets management						
6.2 Secrets stored without version control can lead to an outage if a compromise occurs and they need to be rotated quickly.	Apply version control for secrets so they are easy to refresh or revoke in case of a compromise.	N/A Tanzu Application Platform and Tanzu Build Service do not support version tracking for secrets.	N/A Tanzu Kubernetes Grid does not support version tracking for secrets.	N/A Tanzu Mission Control does not support version tracking for secrets.	N/A Tanzu Service Mesh does not support version tracking for secrets.	N/A Aria Operations for Applications does not support version tracking for secrets.
7. Container orchestration tool auditing						
7.1 Existing inventory management and logging solutions might not suffice due to the ephemeral nature of containers and container orchestration tools integration.	Audit and monitor the orchestration system APIs for indications of unauthorized access. Securely store audit logs on a centralized system.	Tanzu Application Platform and Tanzu Build Service logs are contained in the application logs available through cluster-connected log monitoring using fluent bit and monitoring from Security Information and Event Management (SIEM) or other log monitoring tools.	Tanzu Kubernetes Grid and AVI and Antrea logs are contained in the platform logs available through cluster-connected log monitoring using fluent bit and monitoring from SIEM or other log monitoring tools.	Tanzu Mission Control cluster service logs are contained in the platform logs available through cluster-connected log monitoring using fluent bit and monitoring from SIEM or other log monitoring tools. Tanzu Mission Control platform logs can be exported or streamed to SIEM or log monitoring tools.	Tanzu Service Mesh cluster service logs are contained in the platform logs available through cluster-connected log monitoring using fluent bit and monitoring from SIEM or other log monitoring tools. Tanzu Service Mesh platform logs are available only in the application interface where they can be reviewed regularly for unauthorized or suspicious access or usage.	Aria Operations for Applications cluster service logs are contained in the platform logs available through cluster-connected log monitoring using fluent bit and monitoring from SIEM or other log monitoring tools. The Aria Operations for Applications proxy is also a platform run service and logs similarly to the cluster service. You can export or stream the logs to SIEM or log monitoring tools.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
8. Container monitoring						
8.1 Local logging solutions do not allow for appropriate correlation of security events during which containers are regularly destroyed.	Implement centralized logging of container activity and allow events across instances of the same container to be correlated.	Tanzu Application Platform and Tanzu Build Service logs are contained in the application logs available through cluster-connected log monitoring using fluent bit and monitoring from Security Information and Event Management (SIEM) or other log monitoring tools.	Tanzu Kubernetes Grid + AVI + Antrea logs are contained in the platform logs available through cluster connected log monitoring using fluent bit and monitoring from SIEM or other log monitoring tools.	Tanzu Mission Control cluster service logs are contained in the platform logs available through cluster connected log monitoring using fluent bit and monitoring from SIEM or other log monitoring tools. Tanzu Mission Control platform logs are available to be exported or streamed to SIEM or log monitoring tools.	Tanzu Service Mesh cluster service logs are contained in the platform logs available through cluster connected log monitoring using fluent bit and monitoring from SIEM or other log monitoring tools. Tanzu Service Mesh platform logs are available only in the application interface where logs can be reviewed regularly for unauthorized or suspicious access or usage.	Aria Operations for Applications cluster service logs are contained in the platform logs available through cluster connected log monitoring using fluent bit and monitoring from SIEM or other log monitoring tools. The Aria Operations for Applications proxy is also a platform run service and logs similarly to the cluster service. You can export or stream the logs to SIEM or log monitoring tools.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
8. Container monitoring						
8.2 Without appropriate detection facilities, the ephemeral nature of containers can allow attacks to go unnoticed.	Implement controls to detect the addition and execution of new binaries and unauthorized modification of container files to running containers.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service provide secure supply chains to ensure that authorized containers are built, signed and deployed securely to run clusters. Tanzu Application Platform provides for image signing that can be enforced by the registry to use only authorized and signed images. Admission control policies can be configured to restrict loading images from unauthorized registries.	You can configure Tanzu Kubernetes Grid to restrict downloading unauthorized images through the admission controller. You can use Tanzu Mission Control to automate the configuration of authorized registries and image paths to specific namespaces and groups of namespaces (workspaces). Adding services like Carbon Black can also enforce running only authorized containers and also monitor for runtime network- or system-level suspicious activities.	You can use Tanzu Mission Control to automate the configuration of authorized registries and image paths to specific namespaces and groups of namespaces (workspaces).	N/A Tanzu Service Mesh does not implement controls for monitoring or controlling unauthorized modification of containers.	N/A Aria Operations for Applications does not implement controls for monitoring or controlling unauthorized modification of containers.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
9. Container runtime security						
9.1 The default security posture of Linux process-based containers provides a large attack surface using a shared Linux kernel. Without hardening, it can be susceptible to exploits that allow container escape.	Where high-risk workloads are identified, use either container runtimes that provide hypervisor-level isolation for the workload or dedicated security sandboxes.	N/A VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service are image build and secure supply chain deployment tools and do not provide sandbox or hypervisor-level isolation.	You can deploy Tanzu Kubernetes Grid on vSphere or a public cloud using hypervisor-level isolation of workloads or dedicated nodes that can be configured to isolate and sandbox workloads requiring high-risk considering.	N/A Tanzu Mission Control does not provide sandbox or hypervisor-level isolation.	N/A Tanzu Service Mesh does not provide sandbox or hypervisor-level isolation.	N/A Aria Operations for Applications does not provide sandbox or hypervisor-level isolation.
9.2 Windows process-based containers do not provide a security barrier (per Microsoft's guidance), allowing for possible container breakout.	Where Windows containers are used to run application containers, deploy Hyper-V isolation in line with Microsoft's security guidance	N/A VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service are image build and secure supply chain deployment tools and do not provide Windows containers.	You can deploy Tanzu Kubernetes Grid to support Windows containers, which can be configured to follow Microsoft's security guidance.	N/A Tanzu Mission Control does not provide Windows containers.	N/A Tanzu Service Mesh does not provide Windows containers.	N/A Aria Operations for Applications does not provide Windows containers.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
10. Patching						
10.1 Outdated container orchestration tool components are vulnerable to exploits that could potentially compromise installed clusters or workloads.	Use only supported container orchestration tools and apply security patches regularly, either from the core project or back-ported by the orchestration system vendor.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service provide up-to-date and regularly updated images and provide an automated secure supply chain to automatically rebuild images if there is an update to the rootfs, container runtime or custom application code, ensuring that the latest security patches are always available and can be immediately deployed.	Tanzu Kubernetes Grid, Avi and Antrea are updated with new images and containers on a regular basis. Through platform automation tools like Tanzu Mission Control and clusterapi, Tanzu Kubernetes Grid–deployed systems can be automatically updated as soon as new versions are available.	Tanzu Mission Control can provide automated or one-button-click upgrades of managed Kubernetes clusters. Tanzu Mission Control services are regularly updated and automatically updated on all registered clusters.	Tanzu Service Mesh services are regularly updated and automatically updated on all registered clusters.	Tanzu Service Mesh services are regularly updated and automatically updated on all registered clusters.
10.2 Vulnerabilities present on container orchestration tool hosts (commonly Linux VMs) allow container orchestration tools and other components to be compromised.	Patch and keep up to date the host operating system of all the nodes that are part of a cluster controlled by a container orchestration tool. With the ability to reschedule workloads dynamically, each node can be patched one at a time without a maintenance window.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service provide up-to-date and regularly updated images and provide an automated secure supply chain to automatically rebuild images if there is an update to the rootfs, container runtime or custom application code, ensuring that the latest security patches are always available and can be immediately deployed.	Tanzu Kubernetes Grid, Avi and Antrea are regularly updated with new releases, which include new host OS images and containers. Through platform automation tools like Tanzu Mission Control and clusterapi, Tanzu Kubernetes Grid–deployed systems can be automatically updated as soon as new versions are available.	Tanzu Mission Control can provide automated or one-button-click upgrades of managed Kubernetes clusters. Tanzu Mission Control services are regularly updated and automatically updated on all registered clusters.	Tanzu Service Mesh services are regularly updated and automatically updated on all registered clusters.	Tanzu Service Mesh services are regularly updated and automatically updated on all registered clusters.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
10. Patching						
10.3 Because container orchestration tools commonly run as containers in the clusters, any container with vulnerabilities can compromise container orchestration tools.	Regularly scan all container images used for applications running in the cluster for vulnerabilities. Apply patches regularly, and redeploy the patched images to the cluster.	Tanzu Application Platform provides integrated scanning using internal or third-party tools for all applications in secure supply chains. VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service provide up-to-date and constantly updated images and provide an automated secure supply chain to rebuild images if there is an update to the rootfs, container runtime or custom application code, ensuring that the latest security patches are always available and can be immediately deployed.	Tanzu Kubernetes Grid, Avi and Antrea are updated with new images and containers on a regular basis. Through platform automation tools like Tanzu Mission Control and clusterapi, Tanzu Kubernetes Grid–deployed systems can be automatically updated as soon as new versions are available. Tanzu Kubernetes Grid can integrate with Carbon Black and other runtime security tools to monitor for vulnerabilities in containers and nodes.	Tanzu Mission Control can provide automated or one-button-click upgrades of managed Kubernetes clusters. Tanzu Mission Control services are regularly updated and automatically updated on all registered clusters.	Tanzu Service Mesh services are regularly updated and automatically updated on all registered clusters.	Tanzu Service Mesh services are regularly updated and automatically updated on all registered clusters.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
11. Resource management						
11.1 A compromised container can disrupt the operation of applications due to excessive use of shared resources.	To reduce the risk of "noisy neighbors" causing availability issues with workloads in the same cluster, define the resource limits of all workloads running via a container orchestration system.	You can configure Tanzu Application Platform so the secure supply chain deployment enforces required resource limits.	You can configure Tanzu Kubernetes Grid to have defined resource limits and reduce the risk of noisy neighbors.	You can configure Tanzu Mission Control to have defined resource limits and reduce the risk of noisy neighbors for individual clusters or groups of clusters. When new clusters are joined to an existing group, established resource policies are automatically applied.	Tanzu Service Mesh provides for SLO, SLA and network resource usage and can assist in enforcing defined network resource constraints.	Aria Operations for Applications does not provide resource limit controls, but you can configure it to monitor resource usage for all deployed applications and alert on any impacts that applications are causing.
12. Container image building						
12.1 Container base images downloaded from an untrusted source or that contain unnecessary packages increase the risk of supply chain attacks.	Build application container images from trusted, up-to-date minimal base images.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service are secure supply chain image services. Images are built from the latest VMware-provided container buildpacks, scanned for vulnerabilities, SBOM and other metadata created, signed and stored in a registry so the registry can enforce that only trusted and signed images are downloaded.	You can configure Tanzu Kubernetes Grid through an admission controller or Tanzu Mission Control to allow images from only specific registries, ensuring that only trusted and authorized application images can run in Tanzu Kubernetes Grid clusters.	Tanzu Mission Control can configure registry policies for individual namespaces or groups of namespaces (workspaces) and enforce that only specific trusted registries that provide signed and authorized built images can be downloaded to run on the managed clusters. Tanzu Mission Control services are regularly updated and automatically updated on all registered clusters.	Tanzu Service Mesh services are regularly updated and automatically updated on all registered clusters.	Aria Operations for Applications services are regularly updated and automatically updated on all registered clusters.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
12. Container image building						
12.2 Base images downloaded from an external container image registry can introduce malware, backdoors and vulnerabilities.	Maintain a set of common base images in a container registry that is under the entity's control.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service build from VMware up-to-date base images and save in any registry, including the Tanzu Harbor registry deployed with every Tanzu deployment.	Tanzu Kubernetes Grid can deploy with the Tanzu Harbor Registry as well as provide integration with VMware Application Catalog. Tanzu Application Platform and Tanzu Build Service secure supply chain signed image builders that deploy to harbor or other customer registries. Harbor registry then restricts access to only authorized images through project security configuration.	Tanzu Mission Control builds all application images from a common base image that is produced and maintained by VMware.	Tanzu Service Mesh builds all application images from a common base image that is produced and maintained by VMware.	Aria Operations for Applications builds all application images from a common base image that is produced and maintained by VMware.
12.3 The default position of Linux containers, which is to run as root, can increase the risk of a container breakout.	Build container images to run as a standard (non-root) user.	You can configure Tanzu Build Service and Tanzu Application Platform built images to build without root user.	You can configure Tanzu Kubernetes Grid to enforce non-root or privileged container access.	Tanzu Mission Control can configure Tanzu Kubernetes Grid or any managed Kubernetes to not allow root or privileged containers.	N/A Tanzu Service Mesh does not build images.	N/A Aria Operations for Applications does not build images.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
12. Container image building						
12.4 Application secrets—cloud API credentials—embedded in container images can facilitate unauthorized access.	Never include secrets in application images. When secrets are required during image building—for example, to provide credentials for accessing source code—leverage container builder techniques to ensure that the secret is not present in the final image.	Tanzu Build Service and Tanzu Application Platform do not build images with secrets. Through integrations with Carbon Black and third-party tools, Tanzu Application Platform can scan for secrets in images being built. This custom configuration needs services support.	Tanzu Kubernetes Grid does not build images. Carbon Black and other Tanzu Kubernetes Grid security integrated products can scan images for secrets, but scanning and preventing at build time is recommended.	N/A Tanzu Mission Control does not build images.	N/A Tanzu Service Mesh does not build images.	N/A Aria Operations for Applications does not build images.
13. Registry						
13.1 Unauthorized modification of an organization's container images can allow an attacker to place malicious software into the production container environment.	Control access to container registries managed by the organization. Limit rights to modify or replace images to authorized individuals.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service are deployed with the Tanzu Harbor Registry or can use customer registries that are under control and managed by the organization. Tanzu Build Service and Tanzu Application Platform secure supply chain automates image build and release to registry and Kubernetes clusters and remove the need for individuals' access limiting authorized and unauthorized access to the registry.	Tanzu Kubernetes Grid is deployed with the Tanzu Harbor Registry, or it can use customer registries that are under control and managed by the organization. You can configure it to limit authorized individual functions.	N/A Tanzu Mission Control does not provide a registry.	N/A Tanzu Service Mesh does not provide a registry.	N/A Aria Operations for Applications does not provide a registry.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
13. Registry						
13.2 A lack of segregation between production and non-production container registries can result in insecure images deployed to the production environment.	Consider using two registries—one for production or business-critical workloads and one for development and test purposes—to help prevent image sprawl and the opportunity for an unmaintained or vulnerable image being accidentally pulled into a production cluster.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service can use multiple registries based on the organization configuration.	Tanzu Kubernetes Grid supports multiple registries and restricting which registries are authorized to be used through policies that can be manually configured or configured through Tanzu Mission Control.	N/A Tanzu Mission Control does not provide a registry.	N/A Tanzu Service Mesh does not provide a registry.	N/A Aria Operations for Applications does not provide a registry.
13.3 Base images, regardless of their source, can contain vulnerabilities due to misconfiguration or other methods.	If available, registries should regularly scan images and prevent vulnerable images from being deployed to container runtime environments.	Tanzu Application Platform and Tanzu Harbor Registry can regularly scan images.	Tanzu Kubernetes Grid does not provide image scanning capabilities, but it can be used with Carbon Black or other third-party tools to regularly scan images running in Tanzu Kubernetes Grid clusters.	N/A Tanzu Mission Control does not provide a registry.	N/A Tanzu Service Mesh does not provide a registry.	N/A Aria Operations for Applications does not provide a registry.
13.4 Known good images can be maliciously or inadvertently substituted or modified and deployed to container runtime environments.	Configure registries to integrate with the image build processes so only signed images from authorized build pipelines are available for deployment to container runtime environments.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service produce signed images that are recognized by the Tanzu Harbor Registry, which can enforce signature requirement before accessing and downloading.	You can configure Tanzu Kubernetes Grid manually or through Tanzu Mission Control to download only from authorized registries that enforce container signatures.	Tanzu Mission Control can configure managed clusters, namespaces or groups of namespaces (workspaces) to download images only from authorized registries that enforce signed images.	N/A Tanzu Service Mesh does not provide a registry.	N/A Aria Operations for Applications does not provide a registry.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
14. Version management						
14.1 Without proper control and versioning of container orchestration configuration files, an attacker could modify an environment's setup.	Use version control to manage all non-secret configuration files. Group related objects into a single file. Use labels to semantically identify objects.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service provide tools for container generation and deployment configuration using preconfigured version-controlled accelerators that manage all non-secret configurations, group all related deployment details into a single deployment, and use labels where needed or required.	Tanzu Kubernetes Grid configuration follows Kubernetes configuration and maintains a version history allowing for rolling back changes. It can be integrated into a DevOps/GitOps lifecycle with Tanzu Application Platform, Tanzu Mission Control or other tools to enforce authorized configurations and to prevent unauthorized modifications.	Tanzu Mission Control provides network policy management for managed Kubernetes clusters that enforces a preauthorized configuration. The Tanzu Mission Control configuration is not version controlled, but it does enforce the preconfigured state and prevents unauthorized modification. Policies can be preconfigured and associated to clusters or cluster groups to allow for new clusters to inherit the preconfigured network policy configuration.	Tanzu Service Mesh provides secure TLS and authenticated mTLS connections between containers along with policies that can be used to enforce segmentation between containers and administrative APIs. The Tanzu Service Mesh policies do not offer a version-controlled configuration; however, Tanzu Service Mesh enforces the defined configuration and prevents unauthorized modification of the configured service mesh state.	Aria Operations for Applications does not provide version management, but it can be used to track changes to cluster or service configuration monitoring and alerting on unauthorized modification of the environment's setup.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
15. Configuration management						
15.1 Container orchestration tools can be misconfigured and introduce security vulnerabilities.	Test all configurations and container images in a production-like environment prior to deployment. For all system components, including container orchestration tools, develop configuration standards that address all known security vulnerabilities and are consistent with industry-accepted hardening standards and vendor security guidance. Update configuration standards as new vulnerability issues are identified.	The Tanzu Application Platform and Tanzu Build Service function is to build secure pre-configured application supply chains and container build processes that remove end user configuration requirements. The Tanzu Application Platform and Tanzu Build Service provide central templates that standardize configurations and remove the potential for misconfiguration as they are defined once by security and platform architects and not by end users who only reuse and build from those templates. The VMware Application Catalog on a regular release cycle pre-builds common open-source application containers and deployment helm charts. By providing pre-configured and built services it prevents end users from mis-configuring or introducing security vulnerabilities. Tanzu Application Platform and Tanzu Build Service provide full lifecycle management of containers, enabling automated updates for known security vulnerabilities.	You can configure Tanzu Kubernetes Grid to meet PCI, business or vendor-recommended best practices. A VMware Tanzu Labs engagement that deploys Tanzu Application Platform or Tanzu for Kubernetes Operations includes a workshop to design the cluster, application and resource configuration requirements to meet all production requirements and then using automation, like CI/CD, Tanzu Application Platform or GitOps, to enable full standard compliance and production readiness while preventing unauthorized configuration changes. Tanzu Kubernetes Grid provides full lifecycle management of clusters, enabling automated updates for known security vulnerabilities using updated VMware node images.	Tanzu Mission Control is a container orchestration management tool designed to preconfigure cluster, namespace, resource and other production security and operational requirements. Tanzu Mission Control enforces this configuration and automatically applies it to new clusters added into Tanzu Mission Control management. Tanzu Mission Control provides full lifecycle management of clusters, allowing for automated updates for known security vulnerabilities.	Tanzu Service Mesh is a container service mesh management tool designed to preconfigure cluster connectivity with service mesh that meets production security and operational requirements. Tanzu Service Mesh enforces this configuration and automatically applies it to new clusters added into Tanzu Service Mesh management.	Aria Operations for Applications is an observability platform that does not provide specific production control to the cluster, but it can be used to monitor for nonstandard or non-hardened configurations. When used with Tanzu Application Platform and Tanzu Kubernetes Grid, it can identify scanned or known vulnerabilities if configured to monitor the meta store. The Aria Operations for Applications proxy needs to be configured for production usage with proper filters and controls to restrict production data from being used in Aria Operations for Applications.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
16. Segmentation						
16.1 Unless an orchestration system is designed for secure multitenancy, a shared mixed-security environment can allow attackers to move from a low-security to a high-security environment.	Where practical, place higher-security components on dedicated clusters. If this is not possible, maintain complete segregation between workloads with different security levels.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service segments the components used within the system into build, test and run clusters, separating workloads to different security levels.	Tanzu Kubernetes Grid supports the configuration and use of multiple clusters. When used with AVI or NSX-ALB, ingress can be configured using global DNS and routing based on the workload security level and segmented Tanzu Kubernetes Grid clusters.	Tanzu Mission Control is a multitenant system designed to provide a secure, multiuser segmented environment. Tanzu Mission Control managed clusters can use network policies to ensure complete segmentation between workloads and manage multiple clusters to support full cluster segmentation when necessary.	Tanzu Service Mesh is a multitenant system designed to provide a secure, multiuser segmented environment. Tanzu Service Mesh managed clusters can provide secure, preauthorized connectivity between containers and clusters and also allow for strong segregation and segmentation between containers and clusters not authorized to communicate.	Aria Operations for Applications is a multitenant system designed to provide a secure, multiuser segmented environment. Aria Operations for Applications provides no segmentation capabilities to observed Kubernetes and container-orchestrated environments, but through observability and event monitoring, it might be able to capture and alert for unauthorized access attempts.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
16. Segmentation						
16.2 Placing critical systems on the same nodes as general application containers allows attackers to disrupt the security of the cluster by using shared resources on the container cluster node.	Run critical systems on dedicated nodes in a container orchestration cluster.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service segments the components used within the system into build, test and run clusters, separating workloads to different security levels. You can configure components to run on dedicated nodes if the architecture requires it. If necessary, applications managed by Tanzu Application Platform can use secure supply chain deployment to configure PCI and other workloads to run on dedicated nodes.	Tanzu Kubernetes Grid supports the configuration and use of multiple clusters. When used with AVI or NSX-ALB, ingress can be configured using global DNS and routing based on the workload security level and segmented Tanzu Kubernetes Grid clusters. Kubernetes configurations can enable PCI and other workloads to run on dedicated clusters or dedicated nodes within clusters.	Tanzu Mission Control is a multitenant system designed to provide a secure, multiuser segmented environment. Tanzu Mission Control can manage existing or new clusters and provides the ability to add, remove or otherwise configure the cluster configuration. Tanzu Mission Control does not provide the ability to schedule container workloads on dedicated nodes, but the clusters managed by Tanzu Mission Control have that ability.	Tanzu Service Mesh is a multitenant system designed to provide a secure, multiuser segmented environment. Tanzu Service Mesh managed clusters can provide secure preauthorized connectivity between containers and clusters, but Tanzu Service Mesh cannot provide container scheduling on dedicated nodes.	Aria Operations for Applications is a multitenant system designed to provide a secure, multiuser segmented environment. Aria Operations for Applications provides no ability to configure containers on dedicated nodes. Instead, you can use it to observe where containers are running and, if configured, alert on PCI or other workloads that might not be running on dedicated nodes or wherever they are configured to run.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
16. Segmentation						
16.3 Placing workloads with different security requirements on the same cluster node allows attackers to gain unauthorized access to high-security environments via breakout to the underlying node.	Enforce split cluster node pools so that a user of low-security applications cannot schedule workloads to the high-security nodes.	VMware Application Catalog, Tanzu Application Platform and Tanzu Build Service segments the components used within the system into build, test and run clusters, separating workloads to different security levels. You can configure the components to run on dedicated nodes if the architecture requires it. If necessary, applications managed by Tanzu Application Platform can use secure supply chain deployment to configure PCI and other workloads to run on dedicated nodes.	Tanzu Kubernetes Grid supports the configuration and use of multiple clusters. When used with AVI or NSX-ALB, ingress can be configured using global DNS and routing based on the workload security level and segmented Tanzu Kubernetes Grid clusters. Kubernetes configurations can enable PCI and other workloads to run on dedicated clusters or dedicated nodes within clusters.	Tanzu Mission Control is a multitenant system designed to provide a secure, multiuser segmented environment. Tanzu Mission Control can manage existing or new clusters and provides the ability to add, remove or otherwise configure the cluster configuration. Tanzu Mission Control does not provide the ability to schedule container workloads on dedicated nodes, but the clusters managed by Tanzu Mission Control have that ability.	Tanzu Service Mesh is a multitenant system designed to provide a secure, multiuser segmented environment. Tanzu Service Mesh managed clusters can provide secure, preauthorized connectivity between containers and clusters, but Tanzu Service Mesh cannot provide container scheduling on dedicated nodes.	Aria Operations for Applications is a multitenant system designed to provide a secure, multiuser segmented environment. Aria Operations for Applications provides no ability to configure containers on dedicated nodes. Instead, you can use it to observe where containers are running and, if configured, alert on PCI or other workloads that might not be running on dedicated nodes or wherever they are configured to run.

Threat	Best Practices	Tanzu Application Platform + Tanzu Build Service + VMware Application Catalog	Tanzu Kubernetes Grid + NSX Advanced Load Balancer + Antrea	Tanzu Mission Control	Tanzu Service Mesh	Aria Operations for Applications
16. Segmentation						
16.4 Modification of shared cluster resources by users with access to individual applications could result in unauthorized access to sensitive shared resources.	Workloads and users who manage individual applications running under the orchestration system should not have the rights to modify shared cluster resources or any resources used by another application.	Tanzu Application Platform deploys secure supply chain built applications into shared or dedicated clusters based on preapproved configuration of resources. Tanzu Application Platform does not have the ability to enable users or individuals to change the shared cluster resources.	You can configure Tanzu Mission Control to require specific user or group authorization to change the configuration or resources used in the cluster. You can manually configure the cluster authorization settings, but it is recommended to use Tanzu Mission Control to automate all policy configurations.	Tanzu Mission Control can be used to configure the cluster configuration for resources, privileges and other resource or policy settings. Tanzu Mission Control enforces authorized modifications and prevents users, unauthorized users, applications or application owners from modifying the container policy configurations.	Tanzu Service Mesh is a multitenant system designed to provide a secure, multiuser segmented environment. Tanzu Service Mesh managed clusters can provide secure, preauthorized connectivity between containers and clusters, but Tanzu Service Mesh cannot provide container controls to modify existing cluster configuration as defined by the administrators or through Tanzu Application Platform, Tanzu Kubernetes Grid or Tanzu Mission Control.	Aria Operations for Applications is a multitenant system designed to provide a secure, multiuser segmented environment. Aria Operations for Applications provides no ability to configure resource configuration or utilization. Instead, you can use it to observe what current resource access and utilization is and alert based on unauthorized attempts to change resources used by other applications.

Glossary

Some of the terms used in this document are defined in the Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations, and Acronyms (https://www.pcisecuritystandards.org/pci_security/glossary).

(Auto-)Scaling	An (automatic) adjustment of the number of instances of running containers using the same definition, to address service demands and the availability of resources.
Clusters	A set of containers grouped together and running on nodes.
Container	A software package that includes all elements (application and dependencies) necessary to run on a container platform.
Container Engine	An application that generates an instance of a container from a container image. A physical or virtual device that hosts running container(s).
Container Host	A physical or virtual device that hosts running container(s).
Container Image	A read-only template from which containers are created by the container engine. Also referred to as a Container Engine.
Container Orchestration	A process that automates the deployment, management, scheduling, and scaling of containers.
Container Orchestration Tool	A set of software tools that provide container orchestration functions. Sometimes referred to as a Container Orchestrator.
Container Runtime	An application that generates an instance of a container from a container image. Also referred to as a Container Engine.
Control Plane	A set of services within the network that perform traffic management functions,
Image Registry	A collection of container images from which containers may be accessed by the container engine.
Master Node	A node that acts as a controller, acting as a front end to the cluster of one or more worker nodes, providing scheduling, scaling, implementing updates, and maintaining the state of the cluster.
Node	A physical or virtual machine that hosts a container and that may be defined as a worker node, manager, or master node.
OCI	The Open Container Initiative (OCI) is an open governance structure for creating open industry standards around container formats and runtimes.

Pod	A collection of one or more Kubernetes-coupled containers. A file server storing container images.
Registry Server	A node that executes the container(s) and applications, often as clusters.
Worker Node	An application running on or managed by the container orchestration system. A workload can be a single component or several that work together.
Workload	The Open Container Initiative (OCI) is an open governance structure for creating open industry standards around container formats and runtimes.

PCI SSC reference documents

These resources are available from the Document Library on the PCI Security Standards website.

- PCI DSS
- *Information Supplement: PCI SSC Cloud Computing Guidelines*
- *Information Supplement: PCI DSS Virtualization Guidelines*

Non-PCI SSC reference documents

- CIS Benchmarks
- CSA
- Docker
- Kubernetes
- NIST

Item No: FY24-7303-VMW-TANZU-BEST-PRACTICES-CONTAINERS-WP-USLET-WEB-20230804 8/23