MOAQ (Mother Of All Questions)

Table of contents

MOAQ (Mother Of All Questions)

Section 1.1 Infrastructure – Cloud

1. Please describe lightweight methods for isolating running containers, such as sandbox runtime environments or MicroVMs.

vSphere Pods enable the creation of fully sandboxed container runtime environments directly on the hypervisor. Each vSphere Pod is implemented as a micro virtual machine in vSphere, which provides strong security and resource isolation for the container environment. Each vSphere Pod is sized precisely for the workload that it accommodates and has explicit resource reservations for that workload. It allocates the exact amount of storage, memory, and CPU resources required for the workload to run. One of the key benefits of vSphere Pods is their simplicity and ease of use. They can be deployed quickly and easily using a declarative YAML configuration file and can be managed using standard Kubernetes tools and APIs. This makes it easy to manage multiple vSphere Pods across a large vSphere infrastructure, and to scale up or down the number of Pods as needed to meet changing workload demands.

2. Please describe how you support preemptible compute instances to be used for running containers.

We allow the deployment of clusters in any topology and configuration that is supported by the underlying managed Kubernetes provider such as Amazon EKS. We allow the selection of the desired compute instance type such as preemptible compute instances for worker nodes when creating clusters on Amazon EKS. Cluster configuration and instance type selection is managed via a declarative API.

3. Please describe how you support load balancing for container-based services at Layer 7 (application layer).

At VMware, we understand that load balancing is a critical component of delivering highly available and scalable container-based services. Tanzu provides Layer 7 (L7) features such as content-based routing, URL-based routing, and header-based routing. It also provides advanced features such as HTTP/2, WebSocket, and TLS/SSL termination and HTTP/2 Push alongside request routing, rate limiting, and authentication. Our load balancing solutions are designed to enable seamless connectivity for containerized applications across any environment, with the flexibility to choose the ingress solution that best meets the customer's needs. Additionally, Tanzu's service mesh provides consistent, policy-driven communication across services and clouds, ensuring that load balancing is seamlessly integrated into the overall service mesh architecture. These capabilities enable customers to deliver secure, performant, and scalable containerized applications, regardless of the underlying infrastructure.

For clusters that are managed by Tanzu, a default Loadbalancing service is automatically deployed at the time of cluster creation, This service helps provision a Layer 7 Loadbalancer that understands how to work with container networks within the cluster.

Tanzu also installs ingress controllers like Contour out of the box, that work with the load balancing services like NSX ALB for on-prem deployments and public cloud load balancing services. The ingress controllers help implement layer 7 traffic routing policies between containers within a cluster that get forwarded via the load balancing service.

Also, Tanzu supports multi-cloud service mesh and a global ingress controller that can work with any conformant Kubernetes cluster across on-prem, cloud and edge. This helps customers execute more complex use-cases like SLO based application scaling, cloud-bursting workloads from on-prem to cloud etc.

4. Please describe how you support load balancing traffic directly to containers (i.e., without going through an intermediary proxy).

We support load balancing traffic directly to containers by utilizing the NSX Advanced Load Balancer as an ingress controller with the Antrea CNI:

- Externally routable - pods have routable IPs so the load balancer can direct route to the pods removing the need for kubeproxy and routing through the node IP
- Node port local - pods expose a unique port on the node that the LB can route to so no need for kubeproxy
- ClusterIP - Enables routing directly to Pod network. Traffic is routed direct to the cluster IP removing the need for kubeproxy

If Contour is used as the load balancing and ingress solution, the Node port local configuration would need to be utilized to route traffic directly to containers bypassing kubeproxy.

One of our customers is a large billing provider for Telecom companies and utilizes Node port local as their routing method on the clusters that serve their backend billing system. This system is used by Telecom companies to process customer payments.

5. Please describe how you support full virtual network connectivity for containers (i.e,. without network address translation [NAT]).

We support full virtual network connectivity for containers in use cases where NAT is not desired by offering support for the following configuration scenarios with the Antrea or Calico CNI:

- Externally routable – With Antrea and Calico, pods can have routable IPs so the load balancer can direct route to the pods removing the need for kubeproxy and routing through the node IP

This setup can be achieved by enabling the Antrea or Calico feature flag for external routing and providing the desired CIDR block to use. Customers can also utilize their desired CNI of choice to support routable pods without NAT.

6. Please describe your support for gRPC remote procedure calls with containers.

We support gRPC in both our load balancing solutions (Contour and NSX Advanced Load Balancer) and in our service mesh. Contour's Envoy proxy and NSX Advanced Load Balancer provide support for gRPC and are capable of routing gRPC traffic to the appropriate backend services and containers. Additionally, they provide L7 features such as HTTP/2, TLS/SSL termination, and HTTP/2 Push, which are also useful for handling gRPC traffic.

VMware Tanzu's service mesh supports gRPC security via mTLS both within and cross-clusters/cross-cloud. Tanzu's service mesh capability can auto scale services up and down that leverage gRPC by collecting gRPC requests and latency between services.

Additionally, Tanzu uses the standard Container Runtime Interface (CRI) framework to manage containers within clusters via Containerd. Containerd by default uses gRPC calls to interact with various nodes within a cluster via Kubelet.

7. Please describe how you support HTTP/2 networking with containers.

We support HTTP/2 networking via Contour, NSX Advanced Load Balancer and native Public Cloud's Load balancing services.

Also, Tanzu's service mesh supports HTTP/2 connections between services on the same cluster or across clusters / clouds that participate in a Global Namespace. Tanzu supports HTTP/2 in-bound (public services) connectivity and out-bound HTTP/2 connections to external systems. Tanzu collects and reports on HTTP/2 requests per second (RPS) and latency between services on the same cluster, or across clusters / clouds that participate in a Global Namespace. We also support HTTP/2 Push, which are also useful for handling gRPC traffic.

8. Please describe how you support block storage service for containers.

Tanzu supports block storage devices by utilizing the native CSI drivers when creating a cluster in a public cloud. As a result, we can leverage several types of block storage types surfaced through the infrastructure/cloud provider and attach them to containers automatically. For example, when deploying clusters on Amazon AWS, the Amazon EBS CSI driver is supported. When deploying Tanzu clusters on the VMware on AWS solution, the vSphere CSI driver is used.

Tanzu supports the AccessMode that the underlying block storage supports, which in many cases is RWO.

9. Please describe any data management services that you provide for containers (i.e., backup and disaster recovery).

Tanzu provides a convenient GUI, API, and CLI for utilizing out-of-the-box data protection, migration, and disaster recovery for Kubernetes clusters based on the open source Velero project (for which VMware is a founder and lead contributor). These are the key features we support for cluster/container data management services:

- Backup and restore Kubernetes cluster resources and persistent volumes to the same Cloud or a different Cloud.
- Customers can schedule or create on-demand backups of the entire cluster, specific namespaces, objects matching label selectors, or by including/excluding specific

Kubernetes resources/volumes.
- Persistent volumes can be backed up using volumes snapshots, including CSI-backed volumes using the Kubernetes CSI snapshot.
- We offer flexibility for using AWS S3, S3 compatible, and Azure Blob Storage as storage locations. This allows our customers to have a much greater degree of control over data locality and egress costs.
- We support Recovery point objectives (RPO) and Recovery Time Objectives (RTO) in minutes as snapshot data backup can be captured much more frequently depending on the size of the volume data.

This flexibility helps provide business continuity and application portability without the need for additional products. This helps customers increase crisis preparedness using sandbox environment for testing with the ability to restore backup to new infrastructure; meet regulatory requirements for app availability and recover from disasters due to human error, hardware failures, or security breaches.

10. Please state the maximum number of clusters per account supported.

Tanzu doesn't have a theoretical maximum number of clusters connected to one customer account; this is a result of building our product to horizontally scale to meet the needs of our customers. In our labs we routinely scale test to 5000 clusters.

11. Please describe any ability to automatically repair failing nodes in a cluster.

We implement default health checks for nodes of a cluster that it's managing. We detect issues within a node by constantly determining heartbeats from the cluster nodes using ClusterAPI. If an issue is detected, a new node is automatically instantiated and added to the cluster. It then cordons or drains the failing node to move any workloads to other nodes and deletes the faulty node from the cluster's config. This is applicable for both control pane nodes and data plane nodes.

12. Please describe how you support control plane fault isolation.

We support control plane fault isolation by constantly detecting the state of control nodes via Node Health Check in ClusterAPI, automatically deploying new control nodes when nodes fail. In addition, Tanzu provides the ability to deploy control planes across AZs in public clouds to provide infrastructure fault tolerance. By default, we recommend deploying clusters with 3 control planes, striped across fault lines to enable redundancy of the etcd data and Kubernetes processes. This redundancy and stripping prevent downtime for the majority of IaaS failures.

13. Please describe how you support worker node fault isolation.

We support worker node fault isolation by constantly detecting the state of worker nodes via Node Health Check in ClusterAPI, automatically deploying new worker nodes when nodes fail. Similar to the control planes, Tanzu enables customers to deploy worker nodes across multiple AZs to mitigate the risk of infrastructure failure. We support deploying clusters with multiple instances of worker nodes balanced across multiple node pools in different availability zones. This redundancy enables customer workloads and applications to continue to run in the event of underlying infrastructure failures.

14. Please describe how you support serverless cluster control planes.

Tanzu provides serverless control planes across public cloud and on-prem environments. Azure Spring Apps, our first-party Azure application platform developed and sold with Microsoft, provides a native public cloud serverless experience catering to Spring developers. This platform abstracts away the infrastructure layer from developers and allows them to focus on their Spring application code while all infra management, deployment, networking, and scaling are handled by the platform. The service recently announced true consumption pay-go pricing model that leverages scale to zero functionality to allow users to only pay for what they use while their app is running.

Additionally, Tanzu comes with serverless functionality out of the box with Cloud Native Runtimes serving as the default runtime for the platform. This serverless runtime is based on the OSS Knative project and allows developers to leverage the serverless platform abstraction in on-prem environments. This allows them to experience similar outcomes on-prem that they would with native public cloud serverless offerings.

15. Please describe how you support automatic upgrades of cluster control planes.

Tanzu supports automating cluster rolling upgrades using CLI, GUI, Terraform, or REST APIs. The standard Kubernetes practice of repaving is used, where an updated version of the control plane nodes is deployed, and the previous version is destroyed when the updated version becomes available. The control plane upgrades are performed as rolling upgrades with no downtime.

16. Please describe how you support serverless data planes (automatic provisioning and upgrade of worker nodes).

With the Azure Spring Apps service existing as a first-party fully managed service on Azure, all infra provisioning and cluster management is automatically handled for customers by the platform itself. The user can define app availability and auto-scaling settings that the platform adheres to, but all instance provisioning, systems upgrades, and system operations are handled by the platform itself, ultimately decreasing the operational burden of running Spring applications at scale in the public cloud.

17. Please describe how you provide Terraform IaC support for cloud container services.

Our approach to capability development is API first; anything we expose in our UI or CLI is fully backed by our declarative API. All Tanzu capabilities are backed by a declarative API that enables customers to manage their container platform following GitOps and infrastructure as code best practices. The Tanzu Terraform provider is supported across all of our APIs.

18. Please describe how you support cluster autoscaling.

We enable users to use a cluster-autoscaling feature when provisioning a cluster. The auto-scale configs enable users to define min. and max. nodes that a cluster can be scaled to and back. Once a cluster is provisioned, the control plane nodes periodically check for workloads and node sizes and will automatically add or delete nodes as needed based on the overall load within the cluster.

19. Please describe your support for automatically updating the host OS running containers.

We support automating cluster upgrades using our CLI, Terraform, or REST APIs. The upgrades themselves are applied in a rolling fashion automatically. A new cluster node with the latest host OS patch/version is brought in and the node with the older Host OS is cordoned and drained to ensure continuity of workloads.

20. Please describe how you enable IAM credentials to be assigned to individual pods or services based in clusters.

We create and assign custom roles and permissions at multiple levels of an organization and clusters within. Permissions applied at the organization level will cascade to all other objects within; any permissions applied at lower levels of the resource tree will override the inherited permissions. Custom permissions can even be configured and scoped to any Kubernetes API object within the cluster such as specific pods or services from within our container management portal. Kubernetes service accounts can also be assigned IAM permissions through the container management portal.

21. Please describe how you support ARM worker node instances.

We currently do not offer support for ARM worker nodes due to lack of customer demand. We are always monitoring customer needs and making investments in these areas based on the opportunity.

22. Please describe your North American geography coverage for container services.

Tanzu can be used to manage a container service in any public and private cloud in any geography.

The Tanzu service itself is hosted in US West (N. California), in Canada, and in US West (Oregon) regions within North America. Additionally, we can enable other regions based on customer demand and input.

Please reference this link for coverage: https://www.vmware.com/global-infrastructure.html

23. Please describe your APAC geography coverage for container services.

Tanzu can be used to manage a container service in any public and private cloud in any geography.

The Tanzu service itself is available in AWS regions of Tokyo, and Mumbai. Additionally, we can enable other regions based on customer demand and Input.

Please reference this link for coverage: https://www.vmware.com/global-infrastructure.html

24. Please describe your European geography coverage for container services.

Tanzu can be used to manage a container service in any public and private cloud in any geography

Tanzu service itself is available in AWS region Ireland. Additionally, we can enable other regions based on customer demand and Input.

Please reference this link for coverage: https://www.vmware.com/global-infrastructure.html

25. Please describe your geography coverage for container services in the rest of the world.

Tanzu can be used to manage a container service in any public and private cloud in any geography as long as there is egress from the container service back to Tanzu. Additionally, we can create more regions based on customer demand and Input.

Please reference this link for coverage: https://www.vmware.com/global-infrastructure.html

26. Please describe whether all regions offer full functional consistency for container services.

We provide full functional consistency for container services across all regions they are available.

27. Please describe how you support cross-region service mesh functionality.

We support cross-region, cross-cloud service mesh functionality. Organizations can enable this functionality through a single click or an API request on an individual cluster or fleet of clusters. The service mesh on clusters is accomplished by enabling sidecar-based service mesh locally on individual clusters (on-prem, cloud, or edge). This enables organizations to visualize all the clusters and services across their organization's cluster footprint.

A big differentiator for us is the ability to achieve cross cluster / cloud / provider / region connectivity using a construct called the Global Namespace (GNS) that logically abstracts each cluster's K8s namespace that participates in the GNS. This is a design that we pioneered and added on top of the standard Istio offering to achieve additional value for our customers. A global ingress control plane is used that works with local clusters to create a cross region service mesh that routes communication between services across cloud clusters. Each cluster has a curated Istio installation that is lifecycle managed by Tanzu. We deploy a local control plane on each cluster (data plane) and have a global control plane delivered via SaaS and hosted by VMware.

28. Please use this space to provide any further information on capabilities related to container services on cloud infrastructure.

We support attaching any CNCF-conformant clusters to our platform, no matter where they are running, and manage them centrally. Organizations can manage a fleet of Kubernetes clusters located on-prem, across clouds, and at the edge and provide common identity and access controls. Tanzu also helps enable central monitoring and observability from a single place. Cross-cluster services can become part of a globally load-balanced ingress controller with all communications secured and encrypted with mTLS. Tanzu supports centralized policy management and governance at scale with the ability to group clusters into Cluster Groups, and by using Workspaces to group namespaces together across multiple clusters. We enforce IAM, image registry, network, backup, and pod security policies. Through our Cluster Group concept, we enable platform teams to define which packages and configurations should be automatically installed on clusters in each group, enabling them to optimize their fleet management and easily introduce configuration changes.

Teams can use our default package catalog – which provides a set of Carvel packages and the Bitnami application catalog – or bring their own Git repo to consistently install, configure, and upgrade software running on the clusters. With Flux Continuous Delivery enabled on Cluster Groups, each member of the group will inherit the same configuration and synchronize against the defined Git repos. Any valid Kubernetes YAML object is ingested, so if there are Helm deployments or Carvel packages defined,

they will be automatically installed, and their configurations continually reconciled against the Git repository. We have customers utilizing this functionality to automatically deploy their desired container security tools, ingress controllers, certificate managers, and more.

29. What load balancing, segmentation, or other networking features are supported?
We provide service load balancing for application workloads, automation of multi-cluster networking, and secure north-south/east-west communication between Kubernetes nodes/clusters. We enable logical network abstraction across multiple clusters, externally routable pods, NodePortLocal, GSLB, gRPC & HTTP/2 networking. Layer 7 ingress including traffic splitting via Load balancing (multiple modes such as Round Robin, weighted, header hash), TLS termination & passthrough, HTTP -> HTTPs automatic redirection, mTLS protection, session affinity, rate limiting and more are supported.

30. Are all networking features available for all supported deployment options (if applicable)?
The networking features we make available vary depending on the specific platform and deployment capabilities. With public cloud for example, we utilize underlying public cloud networking for infrastructure and enhance the Kubernetes cluster connectivity with our capabilities where possible.

31. What are the maximum cluster scaling options supported by Tanzu, including nodes per cluster, pods per node, and containers per cluster?
Tanzu's scaling capabilities are robust and align with Kubernetes best practices. Regarding nodes per cluster, the platform doesn't impose a theoretical maximum, while adhering to the recommended limit of 5000 nodes per cluster. In terms of pods per cluster, Tanzu follows Kubernetes best practices and supports up to 5000 pods per cluster. Furthermore, there isn't a theoretical maximum number of clusters connected to a customer account, and in testing environments, the platform routinely scales to 5000 clusters, showcasing its scalability and adaptability.

32. How do you support container networking in multicluster, multi-zone, or hybrid cloud environments, especially in terms of service mesh functionality across various regions and providers?
We offer a global multicluster service which can be activated across different clusters, clouds, and regions, allowing for a consistent implementation of policies, security measures, visibility, and service discovery across various environments. This is achieved by employing the concept of a Global Namespace (GNS) that logically abstracts each participating cluster's Kubernetes namespace. Tanzu bolsters this with its cross-region and cross-cloud service mesh capabilities. This design ensures applications can be deployed consistently regardless of the cloud, Kubernetes provider, or geographical location. It also offers the adaptability for applications to be hosted across a multitude of clouds, regions, or providers, facilitating the usage of local services or broadening their reach. At the core of this multicluster functionality is Tanzu's service mesh which utilizes the GNS to logically represent each cluster. This is complemented by a global ingress control plane that collaborates with local clusters to form a cross-regional service mesh, directing communication between services spread across various cloud clusters. Additionally, Tanzu sets up a local control plane on every cluster (data plane) and integrates it with a Global Control Plane delivered via SaaS, maintained by VMware.

Section 1.2: Infrastructure - On Premises

33. Please describe how you support deployment of containers on bare-metal infrastructure without hyper-visors.

Tanzu supports managing any existing CNCF-conformant Kubernetes cluster, including those provisioned on bare-metal. As it does with other managed clusters, Tanzu enables users to exercise control over container deployments to these clusters via centrally managed governance policies. It can also streamline and accelerate container deployments to bare metal servers using GitOps-based container deployment automation. Tanzu allows platform operators to manage governance policies, provide access control, and enable developers with automatic Flux CD deployment to clusters.

34. Please describe how you support deployment and operations of containers on air-gapped infrastructure with limited or no connectivity to public internet.

Tanzu supports deploying clusters in internet-restricted environments by providing the ability to configure Kubernetes cluster network proxies, as well as the ability to install Tanzu agents from locally hosted image registries. Tanzu further provides simple support for installation and configuration in entirely air-gapped scenarios. Tanzu's management cluster serves as a central point of configuration and lifecycle management in such an air-gapped scenario. For customers that require a cross-site service mesh, Tanzu supports connectivity to the central control plane through a single proxy service. All connections from the Kubernetes clusters (data plane) are established outbound to Tanzu's central portal listening on Port 443 using TLS security. For installing local service mesh components, Tanzu's local Harbor registry can be used to deploy components.

35. Please describe how you support integration with VMware virtual infrastructure.

One of Tanzu's key differentiators is seamless integration with the VMware environment. By leveraging existing infrastructure and tools provided by vSphere, organizations can quickly and easily deploy and manage containerized applications with minimal additional overhead. This comprehensive integration extends to authentication, security, storage, networking, and compute. In addition to all the usual K8s-native tools, Tanzu K8s clusters can be managed using vCenter and the vSphere client, including cluster creation, resource quotas (memory, CPU, & storage), and monitoring of K8s resources such as control plane VMs, & network and storage resource usage. On the networking front, Tanzu integrates with VMware's NSX-T and NSX Advanced Load Balancer, allowing centralized control and management of load balancers, IP subnets, etc. Each cluster created in vSphere has default drivers installed that enable clusters to consume vSphere resources such as VM Disks and/or vSAN for storage and vSphere Distributed Switches and/or NSX for networking of containers. Additionally, Tanzu's service mesh capabilities can be configured on any vSphere-based Kubernetes cluster to establish cross-site or on-prem to cloud services management.

Furthermore, vSphere has native capabilities that extend ESXi nodes as cluster nodes for running containerized workloads alongside VM based workloads. This feature is called vSphere Pods and it is managed by the Supervisor Cluster. The supervisor cluster provides a more isolated container environment which proxies direct access to vCenter resources.

Combined this results in a unified platform that caters to both modern and traditional apps with reduced cognitive load for those looking to modernize their infrastructure.

36. Please describe how you can manage VMs with the same control plane used to manage containers.

Tanzu has been embedded in vSphere since vSphere version 7.0. The same vSphere UI and kubectl CLI can be used to deploy and manage VMs as well as containers. vSphere with Tanzu creates a Kubernetes control plane directly on the hypervisor layer. This allows customers to run traditional VMs alongside modern types of workloads, optionally with enhanced isolation with vSphere Pods running containers directly in kernel-isolated mode on the hypervisor. This control plane can also be used for life-cycle management of Tanzu Kubernetes clusters.

Additionally, VMs created declaratively through the VM Service can be managed as Kubernetes objects through CRDs allowing for VMs to be deployed, managed, and linked to K8s workloads through the same control plane as an organization's modern apps. This exposes K8s primitives such as front–end load balancing, idempotency and configuration as code for VMs just as it would be for native K8s workloads – opening the door to modern management practices such as GitOps for more traditional workload types.

This common platform also allows customers to deploy applications combining different workload types, such as a VM for a database backend and K8s frontend deployments running in a Tanzu Kubernetes cluster. The platform capabilities can be further extended using Supervisor Services which allow customers to deploy platform managed services, such as an L7 ingress controller, an OCI image registry, or certificate management that can be utilized by the previously deployed

37. Please describe your support for a container-optimized OS designed to work in an edge environment.

Tanzu provides Photon OS images. Photon OS is a Linux container host optimized for vSphere. Photon OS images are optimized for Kubernetes and cloud-native environments, reducing the attack surface and resource usage with a small footprint. Unnecessary packages and features have further been removed to make the Photon OS runtime suitable for edge environments. Of course, Photon OS supports the most common container formats and is lightweight, extensible, and optimized for cloud computing and applications, with fast boot and run times.

38. Please describe whether you support single-node clusters.

Tanzu supports the provisioning and management of single-node clusters in cloud, edge, and on-premises environments.

39. Please use this space to provide any further information on capabilities related to on-premises infrastructure.

For over 25 years, VMware has led the industry in helping customers embrace a software-defined infrastructure, providing solutions to abstract away the underlying physical hardware components and create greater agility in operations. VMware vSphere is the industry-leading virtualization platform used by organizations worldwide in their on-premises environments, and now also available as a consumption-based service on all the major public clouds. It has enabled greater efficiency in resource utilization, greater availability and resiliency of mission-critical workloads, and consistent management and control of underlying infrastructure resources.

Building on this robust foundation, VMware Tanzu is integrated into vSphere, providing seamless management of VMs and containers side by side for unparalleled consistency for infrastructure and platform teams. When using Tanzu in vSphere, platform teams can leverage existing virtual networking and storage, as well as consistently apply placement, storage, and availability policies, while automating provisioning and lifecycle management of Kubernetes clusters. Together, vSphere and Tanzu provide the unique ability to run any application or workload, whether monolithic or microservice-based side by side in the same environment.

VMware solutions offer consistent automation, monitoring, and observability of the entire software-defined stack as well as underlying hardware infrastructure. Customers can automate and monitor the underlying hardware infrastructure, through the virtual infrastructure, to the VM, Kubernetes cluster, node, pod & container. We offer capabilities like dashboards, alerts, reports, rightsizing, reclamation, capacity projections, troubleshooting workbench, synthetic monitoring, workload placement & optimization, compliance, remediation, automation central, log analytics, and more. Storage polices, networks, compute, and workloads can be managed via polices and tags for dynamic placement and governance.

40. Does the service mesh service support both container-based and virtual machine-based workloads?
Yes, we developed a VM integration framework using Global Namespaces, which allows our service mesh to support workloads running on VMs alongside K8s-based workloads.

41. What container and virtual machine (VM) runtimes (e.g., CRI-compliant container runtime, OCI-compliant container runtime, OCI-compliant VM runtime, and non-OCI standard VM runtimes) does the product support?
Tanzu supports containerd Photon OS and Ubuntu on vSphere. Amazon Linux, Bottlerocket Linux, and custom AMIs on EKS and can manage any CNCF-conformant distribution

42. Is KubeVirt supported? If so, what is differentiating about the implementation?
While Kubevirt is not supported, we can deploy VM and Kubernetes based workloads in vSphere namespaces using Kubernetes CRD's.

43. What edge-optimized Kubernetes distributions does the vendor support (e.g., K0s, K3s, MicroK8s, MicroShift)?
Tanzu can manage our own Kubernetes runtime as well as any third party CNCF conformant Kubernetes distribution at the edge. Tanzu provides minimized Photon OS and Ubuntu images for reducing the compute footprint at edge locations. Both distributions have been optimized for edge deployments by containing only the necessary packages. Tanzu can also deploy standard Kubernetes clusters with control plane and data plane nodes or single node clusters where the control plane and data plane run in a single virtual machine instance, further reducing compute footprint.

44. How does your platform support container-native storage services, particularly in terms of the types of

container storage (e.g., static/dynamic volumes, local/NAS/SAN storage, file/block/object for persistent storage, etc.)?
Tanzu employs the CNCF's standard for container storage, the Container Storage Interface (CSI) driver. Through this driver, we facilitate the provisioning and management of a wide range of container storage types, such as persistent volume claims, storage classes, and ephemeral storage. If the platform is hosted on vSphere, additional native S3 storage solutions become accessible through the vSAN Data Persistence Platform. This includes offerings provided by Minio, Cloudian, or Dell Object Scale.

45. How does your platform support file storage services for containers, especially in multicluster, hybrid cloud, or multicloud environments?
Tanzu establishes CNCF upstream compliant Kubernetes clusters. Integral to these clusters, Tanzu integrates a Container Storage Interface (CSI) framework to regulate container access to storage. The CSI can interface with various storage types provided by the infrastructure or cloud service, facilitating their automatic attachment to containers. Tanzu uses this CSI framework to support diverse volume types. Clusters orchestrated by Tanzu come with the storage CSI driver pre-deployed, allowing for the definition of multiple storage classes, with one potentially configured as the cluster default. This CSI driver, particularly the vSphere variant, can handle both backend block and file-based storage, presenting these as assorted file systems and modes (like RWO, RWM, ROM) contingent on the storage class leveraged for the persistent volume creation.

For multicloud, multicluster, and hybrid setups, Tanzu supports provisioning that can employ any endorsed storage backend, facilitating VMware storage partners to seamlessly integrate their unique features. With Tanzu deployments, the storage CSI driver is automatically launched, enabling the definition of diverse storage classes tailored to specific application needs.

Section 1.3: Infrastructure & Operations – General

46. Please describe whether you offer a Linux OS optimized for running containers.

We support Photon OS, a minimalistic Linux Operating System designed to implement containerized workloads. Photon OS is a Linux container host optimized for vSphere and cloud-computing platforms such as Amazon Elastic Compute and Google Compute Engine. As a lightweight and extensible operating system, Photon OS works with most common container formats. With a small footprint and fast boot and run times, Photon OS is optimized for cloud computing and cloud applications. We also support Ubuntu OS as an optimized container host OS that has been optimized for cloud native applications.

47. Please describe your support for Windows Server containers.

We support provisioning of Windows Server containers on Tanzu deployed on vSphere. Customers can run their Linux and Windows containers on the same cluster by deploying multi-OS, or hybrid clusters (these clusters contain a mix of Linux and Windows worker nodes). Today, Tanzu supports Windows Server 2019. We continue to evaluate the market demand for Windows containers, but thus far have not seen significant interest from the market.

48. Please describe how you provide specialized hardware such as function accelerator cards (FACs; aka SmartNICS) and graphics processing units (GPUs).

To provide specialized hardware such as function accelerator cards (FACs) and graphics processing units (GPUs), we provide two options. The first is native hardware passthrough capabilities from vSphere called DirectPath I/O. This allows a virtual machine in Tanzu to directly access and utilize the specialized hardware in a single physical host. The second is through virtual devices such as vGPUs. This allows specialized hardware to be shared amongst many instances in a particular cluster while preserving vMotion capabilities. Tanzu supports all x86 CNCF clusters, including instances with specialized hardware. To utilize the specific hardware, the necessary operators and packages need to be deployed. Tanzu is built on upstream Kubernetes, which means it benefits from the extensive development and testing of the Kubernetes community.

49. Please describe how you support multicluster networking.

Tanzu supports multi-cluster networking in a few different ways. We offer a choice of container network interface by choosing Antrea, Calico, or your CNI of choice. Customers can choose their own Layer 1-3 network overlay, whether hardware or software on-premises, or utilizing their infrastructure provider networking (VPC, VNET, etc.) in a public cloud platform of choice. Customers may also choose to utilize a network virtualization solution such as NSX to automate multi-cluster networking as well as secure north-south/east-west communication between Kubernetes nodes and clusters.

Tanzu can also provision a global service mesh that can be implemented multi-region and multi-cloud, enabling applications to be deployed on any cloud, K8s provider, and region. This flexibility enables applications to be deployed consistently with the same policies, security, visibility, and service discovery. Tanzu uses a construct called the Global Namespace (GNS) that logically abstracts each cluster's K8s namespace that participates in the GNS. A global ingress control plane is used that works with local clusters to create a cross region service mesh that routes communication between services across cloud clusters.

We also offer Global Server Load Balancing (GSLB) capabilities that provide a multi-cluster ingress operator that facilitates load-balancing for globally distributed applications/workloads and efficient traffic distribution. To achieve global load balancing, an operator is deployed across all Kubernetes clusters and acts as the default ingress controller to facilitate the creation and management of Virtual Services, VIP, FQDN, etc. and utilize API calls to create new GSLB services that are synchronized across all clusters automatically.

50. Please describe your integration of native service mesh functions.

Tanzu can deploy native service meshes into individual clusters and can also operate cross cloud, region, cluster service meshes via a global control plane. The native service meshes implemented based on Istio are integrated into clusters via side cars for individual containers/pods running.

Each cluster has a curated Istio installation that is lifecycle managed by our service mesh implementation.

51. Please use this space to provide any further information on capabilities related to general infrastructure and

operations.

Organizations worldwide have been consuming VMware solutions for over two decades. VMware vSphere has enabled them to standardize enterprise virtualization operations across infrastructure and cloud platforms. For these organizations now modernizing applications and evaluating container management solutions, VMware Tanzu provides container management and services that are integrated into established vSphere infrastructure, while enabling greater consistency in management of clusters and services from public clouds at-scale. This unique approach does not stop at the on-premises or customer-managed infrastructure, enabling organizations to more consistently manage multiple clusters across a multi-cloud estate that they consume.

Building on VMware's strong legacy of operational tooling and insights, customers can unify applications, infrastructure, and services across private, hybrid and public clouds in a single cloud management platform with a common data model. This approach provides customers full-stack observability and automation for their on-premises environments (including underlying compute, storage, network, virtualization, Kubernetes layer, pods and containers), but also into cloud platforms and services they're consuming across a multi-cloud landscape. We offer capabilities like dashboards, alerts, reports, rightsizing, reclamation, capacity projections, troubleshooting workbench, synthetic monitoring, workload placement & optimization, compliance, remediation, automation central, log analytics, and more. Using a unified cloud management platform that provides a sole source of truth across their cloud estate provides more detailed and actionable insights, provides the ability to control spend, manage risk, and maximize efficiency of the platforms and services they consume.

Section 1.4: Fleet Management

52. Please describe how you support managing the life cycle of multiple distributed clusters (deploy, start/stop, monitor health, upgrade).

Tanzu offers a centralized multi-cluster lifecycle management solution that provides automated provisioning and lifecycle management of Kubernetes clusters across Tanzu Kubernetes Grid and Amazon EKS. Today, Tanzu supports provisioning, scaling, upgrading, and deleting Amazon EKS clusters and Tanzu Kubernetes Grid clusters on vSphere, VMware Cloud Foundation, and VMware Cloud on AWS. For Tanzu Kubernetes Grid clusters, additional deployment targets are Azure VMware Solution, Google Cloud VMware Engine, and Oracle Cloud VMware Solution.

Organizations can also attach any CNCF-conformant Kubernetes cluster for identity, access, and policy management. Tanzu reduces the operational burden by providing a central place for automation, monitoring and observability.

For Tanzu Kubernetes Grid clusters, Tanzu uses the opensource ClusterAPI framework to simplify and automate cluster management. Tanzu CLI/UI/Ansible can be used to create, scale, and upgrade clusters. Tanzu changes the declarative configs triggering an automation process that deploys, starts, stops, and upgrades the cluster based on user input.

53. Please describe how you support centrally managing clusters deployed in different cloud services.

Tanzu can centrally manage and deploy clusters in on-prem and cloud environments, giving teams one place to view, manage and automate, no matter where their clusters are deployed. Tanzu supports the creation, upgrade, and deletion of Tanzu Kubernetes Grid or AWS EKS clusters. Tanzu also allows the attachment of any CNCF-conformant cluster created outside of the platform so these can take advantage of the full breadth of functionality Tanzu provides:

- Cluster Grouping: Tanzu allows you to group clusters based on criteria such as environment, region, or application. This enables teams to manage their clusters at scale across different cloud services.
- Policy management: Tanzu provides a policy engine that allows you to define and enforce policies across multiple clusters. You can set policies for security, compliance, and resource usage, and apply them to individual clusters or Cluster Groups.
- Data Protection: Enables organizations to manage backup and restore of clusters and namespaces, across their fleet.
- Centralized logging and monitoring: Tanzu provides a centralized dashboard for monitoring and logging across multiple clusters. You can monitor cluster health and performance, track application metrics, and troubleshoot issues.
- Connectivity: We provide full-stack application connectivity services that enable application mobility and migration, application high availability and failover, and automated application rollouts and upgrades. Tanzu controls north-south traffic from end-users at the application edge, through mesh ingress and egress, and east-west traffic between application workloads, APIs, and data. Fine-grained edge and ingress gateways load balance and route application traffic across clusters and clouds, while sidecar proxies route and load balance communications between microservices.

54. Please describe how you help to manage the infrastructure needed to deploy multiple clusters deployed on-premises.

VMware vSphere provides the infrastructure layer for on-premises Kubernetes clusters, enabling organizations to deploy, manage, and scale multiple clusters across their infrastructure. With vSphere, users can leverage existing infrastructure investments and optimize their resources through efficient allocation and utilization of compute, storage, and networking resources. vSphere also provides features like High Availability (HA), Distributed Resource Scheduler (DRS), and vMotion, which ensure the availability, performance, and scalability of the underlying infrastructure for Kubernetes clusters.

vSphere with Tanzu is an enterprise-grade Kubernetes runtime that can be deployed on top of vSphere. Tanzu simplifies the deployment and management of Kubernetes clusters, and provides a consistent experience across different environments, including datacenter, telco, and edge. Tanzu can leverage the virtual resources managed by vSphere, to provide the compute, networking and storage for the Kubernetes clusters.

Organizations call also leverage Aria to monitor the infrastructure from the physical layer (host, storage array, network switch, etc.) to the virtual infrastructure, to the VM, to the K8s cluster, node, pod, and container. Aria has many features that cover on-premises infrastructure like vSphere or physical server monitoring covering alerts and remediation, AI powered Troubleshooting Workbench, AI powered capacity management, reclamation of unused resource, rightsizing, what-if planning, compliance, cost management for showback reporting, pricing for chargeback, automation central to automate various actions, and more. Aria also has the ability to collect and visualize logs from all data sources from the physical to virtual to K8s that sends logs using syslog or with an agent.

55. Please describe how you support centralized policy management for multiple clusters in your container management products.

Tanzu has the capability to apply out-of-the-box polices to a fleet of clusters with centralized management. It allows organizations to view and manage their entire Kubernetes footprint across public and private clouds. Organizations can manage these clusters by grouping them into logical groupings. Policies can be applied to clusters at multiple levels: Organization, Cluster groups, Clusters, Workspaces (groups of namespaces), and Namespaces. Within Clusters we can combine namespaces into Workspaces. Policies applied at the top of the org structure can trickle down to all levels. Once a policy has been applied, any new clusters added to the group or org automatically get the policies applied to them. Tanzu has default out-of-the-box policies around access control, security policies, image registry management, quota, etc. These policies can be easily scoped to namespaces with labels. For organizations who want to define their own policies, Tanzu provides a way to define custom roles and policies in the portal using Open Policy Agent (OPA) Gatekeeper

Tanzu also enables applications to be deployed consistently with the same policies, security, visibility, and service discovery. Tanzu uses a construct called the Global Namespace (GNS) that logically abstracts each cluster's K8s namespace that participates in the GNS. Policies and security definitions can be deployed (full lifecycle) on a GNS which ensures consistency across all participating K8s cluster namespaces. As participating namespaces (regardless of cluster / cloud / region) are added (or removed) to the GNS, the policy and security definitions are applied consistently, and configuration sync is maintained. Consistent policies & security ensure that no matter where an application is deployed – even if the app spans multiple clusters / clouds / providers / regions - the security posture and configuration remain the same.

56. Please use this space to provide any further information on capabilities related to fleet management.

Beyond helping organizations operate their entire fleet of clusters, no matter where they are deployed, VMware helps organizations optimize their environment by giving the right feedback to continuously tune cost, performance, and security. We enable platform teams to control the cost and performance of their environment by providing resource quota polices, as well as cluster sizing recommendations. This includes providing the ability to segment Kubernetes cluster for visibility and optimization by task, namespace, label, deployment, and cluster. The segmentation provides a comprehensive solution for monitoring container usage, optimizing resource allocation and spend. This enables platform teams to not only optimize their cloud spend, but also enables showback/chargeback to downstream consumers.

Tanzu also provides advanced, end-to-end connectivity, security, and insights for modern applications—across application end-users, microservices, APIs, and data—enabling compliance with Service Level Objectives (SLOs) and data protection and privacy regulations.

Beyond Tanzu, organizations can leverage Aria to provision vSphere with Tanzu Kubernetes deployments and manage Tanzu Kubernetes clusters, providing an infrastructure-agnostic layer for provisioning and management of virtual infrastructure. Aria can also be leveraged https://blogs.vmware.com/management/2021/11/on-demand-workload-clusters-on-vsphere-with-tanzu-using-cloud-assembly.htmlto monitor K8s clusters, nodes, pods, and containers down to the cloud provider services (including AWS, Azure, GCP, and on-prem). K8s management benefits from AI powered Troubleshooting Workbench, AI powered capacity management, reclamation of unused resource, rightsizing, what-if planning, compliance, cost management for showback reporting, pricing for chargeback, automation central to automate various actions, and more. Aria also has the ability to collect and visualize logs from all data sources from the physical to virtual to k8s that sends logs using syslog or with an agent.
https://blogs.vmware.com/management/2021/11/on-demand-workload-clusters-on-vsphere-with-tanzu-using-cloud-assembly.html

57. What features are included to improve observability and service discovery in multi-cluster and hybrid cloud (public, hosted, on-premises and edge) environments (if applicable)?
Our service mesh gathers telemetry from multiple sources, including Istio and Kubernetes, and correlates the infrastructure and application-layer telemetry. We also offer advanced telemetry and topology maps such as detection and flow mapping of sensitive

data (e.g., PII and PCI) and detection of requests from outside geofences. Our service mesh excels at service and API discovery across multiple clusters residing on-premises, in the cloud, or at the far-edge. "

58. What runtime enhancements does the vendor offer for edge and other resource-constraint scenarios, including security?
Tanzu provides an edge-optimized runtime, minimal footprint deployments, resource quota by subscription, and automated security and governance policies that can be pushed to thousands of edge locations.

59. What differentiating Day 2 operations control plane features are provided (e.g., rolling or zero downtime upgrades)?
Teams can manage access, policies, and configurations at scale across any cluster type. Both rolling and zero downtime upgrades are supported for clusters and workloads. Tanzu enables customers to deploy service mesh across clusters and clouds, to enable active / active deployments. VMware also offers Aria Operations for Applications, which provides a unified multi-cloud observability solution with contextualized information across logs, metrics, and traces.

60. What configuration and cluster lifecycle operations features for multicluster and hybrid cloud (public, hosted, on-premises and edge) environments are provided?
Cluster lifecycle mgmt & ops are built with a multi-cluster first approach in Tanzu to support easy fleet management & scalability. We support the lifecycle management of Tanzu Kubernetes Grid on vSphere & Amazon EKS clusters. We also support config of Tanzu Kubernetes Grid on vSphere, Amazon EKS & all other CNCF-conformant Kubernetes distros through the use of FluxCD & various policies that can be applied to clusters.

61. What differentiating security features are available?
By enabling policy management as a fleet, Tanzu helps customers ensure consistent security is enforced on all clusters that are managed by the platform. Tanzu also provides a rich set of API security capabilities, like API vulnerability detection and mitigation, PII segmentation, and API security visibility.

62. What differentiating features are provided for intelligent edge computing scenarios and remote management of Kubernetes clusters at the edge?
Tanzu supports the automated provisioning and management of thousands of clusters at edge environments that can be visualized and managed through the UI. Tanzu provides flexible architectures to meet the needs of single node or highly available deployments depending on the requirements. Tanzu natively integrates with vSphere allowing the direct use of hardware such as GPUs at the edge.

63. How does the platform enable storage replication, failover, and disaster recovery operations?
Tanzu has native multi-AZ support through vSphere Zones that allow mgmt & workload components to be spread across multiple locations. For vSAN based infrastructure, vSAN datastores replicate data across hosts & vSAN based clusters providing protection & data mobility across clusters. Tanzu provides out-of-the-box backup, recovery & cross-cluster restore functionality based on Velero. Backups can be restored to different clusters to ensure business continuity and application portability without the need for additional products.

64. How do you support backup, disaster recovery, high availability, and restore functionalities for clusters, ensuring business continuity and application portability?
Tanzu provides comprehensive backup, recovery, cross-cluster, and cross-cloud restore functionalities based on Velero. We enable the backup and restoration of both the underlying etcd and application data. Backups can be restored to different clusters, bolstering business continuity and application portability without necessitating additional products. This system enhances crisis preparedness, allowing users to test restorations to new infrastructure in a sandbox environment. It also aids in meeting regulatory requirements for app availability, recovering from diverse disasters such as human errors, hardware failures, or security breaches. Tanzu supports AWS S3 and Azure Blob Storage as target locations and provides the flexibility to switch between backup locations. Snapshots can be taken as frequently as every minute, depending on the data volume, ensuring limited downtime. Tanzu oversees the installation, configuration, and upgrades of Velero on each cluster through its APIs, reducing the manual workload and YAML configurations for the end user.

65. What capabilities does your platform provide for monitoring usage, analyzing costs, and optimizing resource utilization in container management?

We offer a robust set of tools through Aria Cost for detailed monitoring and optimization. Our platform reports on the historical usage of CPU and Memory for Kubernetes and Amazon ECS workloads, capturing details like requests, limits, and overall cluster capacity. Aria Cost reallocates shared compute and memory costs for Kubernetes and ECS across various criteria like namespaces, containers, and custom business groupings. Using past usage patterns and current requests, Aria Cost gives rightsizing recommendations for Kubernetes, aiming for optimal CPU and Memory usage balance. Users also have the ability to set up dashboards in Aria to monitor cloud resource usage and receive alerts. Additionally, with Aria Operations for Applications, we offer insights into cluster resource utilization, recommending appropriate sizing based on application requirements. This comprehensive approach aids in efficient resource use and cost management.

66. How does your platform accommodate resource-constrained edge computing scenarios, such as lightweight components, automation for remote applications, optimization for varied edge hardware infrastructure, security, and deployment of containers on edge hardware?
Tanzu extensively supports deploying and centrally managing Kubernetes clusters at the edge. It offers both an edge-optimized runtime and caters to minimal footprint deployments, which includes configurations like single-host clusters and lightweight images. The automation of these deployments is handled by the upstream Kubernetes Cluster API, which can be navigated through the Tanzu CLI, UI, or gitops workflows. Furthermore, Tanzu's multi-cluster approach ensures efficient fleet management of Edge clusters. This is achieved by harnessing ClusterAPI and other upstream-aligned mechanisms to dictate cluster lifecycle and policy for a vast array of edge clusters. Once a Kubernetes cluster is established at an edge location, containers and packages can be deployed through various means. This can be done directly using kubectl to the cluster, via the Tanzu Catalog which contains Tanzu-specific packages, or through the use of helm charts from the extensive Bitnami portfolio or customized helm charts created by users.

67. How do you automate and simplify ongoing "Day 2" cluster operations, especially in terms of multicluster, federated cluster management, support for complex application stacks, and centralizing the state management of multiple clusters?
Tanzu streamlines "Day 2" operations through the use of ClusterAPI with TKG, EKS APIs, and automation facilitated by REST APIs & Terraform. For efficient multicluster management, Tanzu organizes clusters into logical groupings named Cluster Groups. These Cluster Groups enable centralized handling of monitoring, upgrades, policies, and backup targets across the entire fleet. Additionally, FluxCD can be enabled for these Cluster Groups, allowing continuous delivery of container application management at the fleet scale. This ensures that platform teams can apply Kustomizations uniformly on both current and subsequent clusters added to the Cluster Group, guaranteeing the replicated definition of applications and policies across all clusters.

68. How do you facilitate quota governance, cost forecasting, optimization, planning, and remediation, particularly in the context of optimizing resource usage for containerized workloads?
VMware Aria provides a comprehensive suite of tools designed for quota governance, resource optimization, and cost management:

- Usage Monitoring: Users can create dashboards to monitor cloud resource consumption, offering detailed insights by segmenting resource usage into categories like namespaces within your Kubernetes cluster.
- Alerts and Dashboards: These tools offer real-time notifications and deep insights into resource utilization, assisting users in understanding and optimizing resource consumption.
- Historical Analysis: Aria analyzes and reports on historical CPU and Memory usage patterns for Kubernetes and Amazon ECS workloads. It also provides insights into requests, limits, and the overall available capacity for clusters.
- Rightsizing Recommendations: Aria Cost offers intelligent recommendations for Kubernetes requests grounded on historical usage trends, current requests, and user-specified parameters for CPU and Memory. This optimization leads to improved resource utilization and cost efficiency.
- AI-Powered Projections: Leveraging AI, Aria presents capacity forecasts and rightsizing suggestions for infrastructure components, encompassing clusters and VMs.
- Resource Reclamation: The platform identifies and suggests the reallocation of unused resources, freeing up capacity for newer workloads.
- What-if Planning: Users can model potential operational changes in a risk-free

environment before actual implementation.
- Cost Reporting and Management: Aria delivers functionalities like showback reporting and chargeback pricing, shaping user behaviors in alignment with cost optimization goals.
- Automation Central: This central hub automates optimization suggestions, streamlining the resource management process.

69. Does the VMware Aria platform provide any tools or suggestions for optimizing costs and rightsizing recommendations for container and microservice services, including considerations for waste, length of commitment, and performance metrics such as CPU and Memory usage?

VMware Aria offers a comprehensive suite of tools to optimize usage, cost, and performance for Kubernetes and Amazon ECS workloads. The platform collects and reports on historical CPU and Memory usage, maps them against requests, limits, and total available cluster capacity. Based on this data, Aria delivers rightsizing recommendations for Kubernetes container requests, focusing on historical usage patterns, current needs, and desired parameters for CPU and Memory. Aria Cost also re-allocates shared Kubernetes and ECS compute and memory costs to various organizational units like namespaces, containers, clusters, account IDs, and custom business groupings such as line of business, application, or department. These data and recommendations can be shared on the platform, emailed to stakeholders, used for chargeback, or shown back to engineers in a context relevant to them. Additionally, Aria provides rightsizing recommendations and cost-saving options for vSphere VMs, which may be running Kubernetes and native vSphere Pods in the Workload Management capability. Showback reports can also display the cost for these VMs and vSphere Pods.

Section 1.5: Observability

70. Please describe the native monitoring capabilities of your container management products.

We have a central monitoring portal that shows default capacity and workload metrics like CPU/Memory usage, workloads deployed, control plane health for all the clusters that are brought under its management. Apart from these base metrics, organizations can enable the collection of metrics on clusters into a central portal. The central monitoring system allows real-time collection of data and presentation, visualization, and alerting. We can also help parse Kubernetes logs and alert customers on anomalies in their container environment. We also allow organizations to plug metrics and visualize data through Prometheus and Grafana or forward metrics and logs to their own APM systems. All information collected can be accessed via API.

In addition to our central monitoring portal, Tanzu Service Mesh collects the requests per second (RPS), latency, unique API counts, L7 API security violations, OWASP top-10 attacks, and transaction counts containing PII between each Service deployed on a Global Name Space (GNS) as well as public services exposed by an ingress gateway. Service Level Objectives (SLOs) are monitored along with violations. Autoscaler predictions and scaling actions are monitored.

71. Please describe the native logging capabilities of your container management products.

We provision log management components like Fluent-bit in every Cluster that is deployed. Organizations can configure Fluent-bit to forward logs to our central monitoring portal, or they can configure it to forward logs to their log management software of choice. For existing/brown-field clusters, Tanzu's central monitoring portal supports multi-agent logging via Fluentd, Fluent-Bit, or our own logging agent. Logs and events are collected from each container node, aggregated, tagged, and ingested for retention for up to 30 days. Fields can also be extracted from logs to provide custom query and reporting capabilities. Logs that are ingested that be viewed alongside metrics for a seamless unified observability experience bringing metrics, events, logs and traces together.

Our central portal integrates natively with clusters provisioned by Tanzu. This allows metrics, traces and logs to be correlated under a single pane of glass for faster resolution of critical down states in the container environment.

72. Please describe the native tracing capabilities of your container management products.

Our central monitoring allows Real-time collection of data and presentation, visualization, and alerting. For clusters that are brought under our management, distributed tracing can be enabled. Distributed tracing can capture every single transaction between service-to-service communications and calls to external services. Users have full flexibility to control the sampling granularity. They can setup explicit sampling policies via the proxy or instrumentation for rate based/duration based/mixed

In addition to our central monitoring, Tanzu Service Mesh collects the requests per second (RPS), latency, unique API counts, L7 API security violations, OWASP top-10 attacks, and transaction counts containing PII between each Service deployed on a Global Name Space (GNS) as well as public services exposed by an ingress gateway. The service-to-service communication metrics are collected within and across clusters with participating namespaces in the GNS. This enables the tracing of transactions in a fully distributed application that may have services on multiple clusters / clouds / providers / regions.

73. Please describe the interface you provide for centralizing observability of multiple clusters.

We can present default capacity and workload metrics like CPU/Memory usage, workloads deployed, for all the clusters that are brought under its management. Apart from these base metrics, organizations can enable collection of various data such as metrics, logs, traces, and events from each cluster to be collected and sent via proxy, ingested, and stored in our central monitoring portal. This data from multiple clusters is then available to view, query, and alert on.

Our central monitoring allows Real-time collection of data and presentation, visualization, and alerting of multiple clusters, platforms and even infrastructure to co-relate and debug issues. We can also help parse Kubernetes logs and alert on anomalies in your container environment. We also allow organizations to collect distributed tracing of multiple clusters into a single portal.

74. Please describe how you support monitoring applications running in containers.

Our central monitoring portal supports many out-of-the-box applications including RabbitMQ, GemFire, MySQL, REDIS, nginx, Apache, Spring etc. Tanzu's central portal supports alerting of critical states via log integration for Kubernetes and supports out-of-the-box metrics from applications as well as custom metrics.

In addition to our central monitoring portal, Tanzu Service Mesh collects the requests per second (RPS), latency, unique API counts, L7 API security violations, OWASP top-10 attacks, and transaction counts containing PII between each Service deployed on a Global Name Space (GNS) as well as public services exposed by an ingress gateway. The service-to-service communication metrics are collected within and across clusters with participating namespaces in the GNS. This enables tracing of transactions in a fully distributed application that may have services on multiple clusters / clouds / providers / regions.

If a customer is utilizing the Tanzu runtime, Prometheus, Grafana, and Fluent-bit Tanzu packages are provided and supported by VMware.

75. Please describe how you support alerting in the container environment.

Our central portal for Container management provides alerting capabilities for events around cluster management. Apart from this, our Central Monitoring portal provides a mechanism to collect and store container data in a central location. This data can then be queried, and alerts can be created based on this data. We do include out of the box alerts such as for the container control plane, pods, nodes. Alerts can be sent to external systems for notification and ticketing. Alerting of critical states via log integration for Kubernetes is also supported.

76. Please describe how you support integration of tracing into integrated development environments (IDEs).

Using IDE's such as VS Code, Visual Studio, IntelliJ, developers can instrument their code using open telemetry libraries to collect span and trace data.

With our central monitoring solution, we support Ingesting these spans and trace data using the OTEL format. RED metrics and ApDex scores are computed from this data, application maps are presented to visualize the communication and trace data is integrated with metrics and logs.

Our for tracing includes OpenTracing libraries (Zipkin/Jaeger) and OpenTelemetry libraries (Zipkin/Jaeger). Spans and traces can be visualized, and alerting performed on data such as RED metrics.

77. Please describe how you integrate logging in cluster control planes.

Tanzu provisions log management component like Fluentbit in every Cluster that it deploys. Organizations can configure Fluentbit to forward logs to Tanzu's central monitoring portal, or they can configure it forwards logs to their log management software of choice. For existing/brown-field clusters, Tanzu's central monitoring portal supports multi-agent logging via Fluentd, FluentBit, or our own logging agent. Logs and events are collected from each container node (including cluster control nodes), aggregated, tagged, and ingested for retention for up to 30 days. Fields can also be extracted from logs to provide custom query and reporting capabilities. Organizations have the choice to include/exclude control pane nodes

Tanzu's central portal integrates natively with clusters provisioned by Tanzu. This allows metrics, traces and logs to be correlated under a single pane of glass for quicker time to recovery of critical down states in the container environment.

78. Please describe how you integrate logging in cluster data planes (worker nodes).

The solution is identical to cluster control planes.

79. Please describe your Prometheus compatibility.

Tanzu includes monitoring components like Prometheus, Grafana, and Fluent-bit which are VMware supported applications with dashboards included on deployment of clusters. Tanzu's central portal can be used to manage Prometheus deployments on clusters or groups of clusters. This can be achieved using the Tanzu package or Helm chart and can be done automatically at the cluster or cluster group level. Prometheus metrics can be forwarded to Tanzu's central monitoring portal or to customer choice of APM software.

80. Please describe your compatibility with third-party observability tools.

Our central monitoring system can be used to deploy any third-party Kubernetes-native observability tools. Prometheus, Grafana, and Fluent-bit are included in Tanzu packages and the Bitnami Helm repository. Prometheus metrics from within the cluster can be scraped and sent to any third part APM Management software a customer uses, along with sending cluster logs. As you'd expect

from VMware and our broad ecosystem, we also have specific integrations with Datadog, Sysdig, New Relic, and others.

81. Please use this space to provide any further information on capabilities related to monitoring and observability.

Our Central Monitoring Portal provides a comprehensive solution for monitoring Kubernetes using the Kubernetes Operator to collect detailed metrics from Kubernetes clusters. It brings together metrics, events, traces, and log management in a unified platform to deliver full-stack observability for Kubernetes environments.

The solution collects real-time metrics from all layers of a Kubernetes environment (clusters, nodes, pods, containers and the Kubernetes control plane), including support for plugins such as Prometheus, Telegraf and Systemd. Capabilities such as auto-discovery of pods and services, daemonset mode for scalability, and auto reload of configuration changes are supported. The solution includes internal metrics for tracking collector health and sources of K8s metrics along with installing dashboards for health status, infrastructure, workloads, clusters, control plane, and more.

Our portal provides content packs for Kubernetes and TKG that allow end users to visualize and start making decisions based on their log data immediately without having to build their own charts and queries. This allows for quicker time to value and the ability to immediately troubleshoot issues in the environment with minimal configuration needed.

In addition, Aria Operations for Networks supports TKGI, OpenShift and Kubernetes from both a network monitoring and security planning standpoint on NSX-T networks.

82. What serverless, machine learning and observability metrics definition capabilities does the vendor provide to simplify day-2 operations?

We provide basic Kubernetes metrics within the Tanzu console. For those looking for enterprise-grade cloud monitoring & analytics, customers use our robust Unified Observability platform, which a multi-cloud solution providing single-source-of-truth visibility and
contextualized information across logs, metrics, and traces for greater business agility while maintaining SLAs.

83. What logging and tracing features are available (proprietary and/or open source components such as Prometheus, Grafana, OpenTracing, OpenTelemetry, and EFK)?

We offer a massively scalable, unified observability platform that supports analytics for metrics, distributed traces (DT), logs (beta), and histograms. DT is supported using our SDKs or OpenTelmetry to send Traces, Spans and Span logs. To forward logs, an agent is provisioned in every K8s cluster that is deployed. In the case of DT and logs, the metrics, such as RED metrics are automatically derived and made available for faster MTTD. Metrics, traces and logs can be viewed alongside each other for a seamless troubleshooting experience. We also support sending data to Prometheus, Grafana, or other proprietary tools.

84. How are metrics customized, queried, and analyzed for multidimensional analysis and decision-making?

Our SDKs allow ingestion of custom data. Our platform supports around a hundred mathematical and TSDB functions for correlating, manipulating and analyzing our data. Using PromQL or our query language customers are able to further analyze data, build dashboards and create alerts.

85. What platform security options are available, e.g., user authentication (MFA, adaptive), RBAC (fine-grained prebuilt roles, role customization, AD/LDAP integration); observability (distributed logging & monitoring) support, alerting, and auditing for risks and compliance; integration security (big data, AI/ML, IoT, etc.); third party security tool integration (WAF, DDoS, ZTNA, etc.); security policies (Security-as-Code), including comprehensive and configurable policy definition (pod-to-pod traffic restriction, isolation by nodes, clusters, tenants, and region); and automated policy enforcement?

Access to Kubernetes resources for users, groups, and service accounts can be configured with AD/LDAP integrations. Real-time data collection, presentation, visualization, and alerting are available. Our service mesh collects the RPS, latency, service metrics, unique API counts, L7 API security violations, OWASP top attacks, transaction counts containing PII, and public services exposed by ingress gateways.

Section 1.6: Kubernetes Features

86. If there is any supporting information, you can provide a link or upload a document.

https://tanzu.vmware.com/kubernetes-grid

87. Please describe which Kubernetes distributions you support.

Tanzu supports attaching and managing any CNCF-conformant Kubernetes cluster. including EKS, AKS, GKE, and OpenShift. We provide deeper integrations today for lifecycle management of EKS and our native Kubernetes runtime, with AKS support slated for delivery this year on our roadmap.

88. Please describe how long it takes to support new versions of upstream Kubernetes code in container management products.

Tanzu's Kubernetes distribution and management stack is approximately 8 months behind open source releases of Kubernetes. Our plan by the end of this fiscal year is to reduce this gap to 3 months. While staying up to date on Kubernetes releases is important, providing enterprise customers with the latest innovations in LCM such as upstream Cluster-API ClusterClass, and advanced cluster addons are key needs for these customers. VMware prioritizes these needs along with stability and reliability in our enterprise-grade solutions over these updates. Before integrating new Kubernetes releases into Tanzu, VMware needs to thoroughly test and validate them to ensure they work well with the other components in the Tanzu platform and meet their quality standards. This can take time, which can result in a lag between open source releases and supported releases in Tanzu. VMware prioritizes providing a stable and reliable solution that can meet the needs of enterprise customers over providing the latest features and updates immediately.

89. Please describe your approach to long-term or extended support of upstream Kubernetes code.

VMware offers support for the current and the two previous releases (n-1 and n-2) of Tanzu software, which typically include the two most recent stable upstream Kubernetes releases. Our extended support offering is specifically designed for use cases that require stability, security, and predictability for their production environments. Extended support provides support for specific VMware software releases beyond their standard support periods, typically for one additional year. While initially targeting telco use cases, we have a roadmap item to bring extended support to our standard customer base.

VMware employs a combination of upstream community resources and internal engineering expertise. This approach allows us to extend the support of specific Kubernetes releases in Tanzu software while maintaining compatibility with upstream open source Kubernetes. It provides a release cadence and lifecycle for Kubernetes clusters that aligns with the upstream Kubernetes release cycle. Tanzu ensures that all upstream Kubernetes patches and security updates are integrated into the Tanzu releases. Additionally, Tanzu provides customers with a roadmap for upcoming Tanzu releases, giving them visibility into the planned support for Kubernetes releases.

90. Please describe your ability to configure private and public access to the Kubernetes API servers.

Tanzu supports configuring public and private access to the Kubernetes API in multiple layers. The container management platform uses Pinniped, which is an authentication proxy installed on the cluster that maps Kubernetes RBAC roles to the users and groups that have been assigned permissions. Users can configure access by creating policies for cluster groups or workspaces which allow them to apply access settings to multiple clusters at once.

Tanzu supports configuring a Web Application Firewall (WAF) and micro-segmentation policies to control access to Kubernetes clusters that are running in public clouds, such as Amazon EKS, Azure AKS, and Google GKE, as well as on-premises environments containing modern and legacy services.

91. Please describe how you support multicluster ingress.

Tanzu integrates with NSX Advanced Load Balancer (NSX ALB) to support multicluster ingress. NSX ALB provides a feature called Avi Multi-Cluster Kubernetes Operator (AMKO) which is an operator for Kubernetes that facilitates application delivery across multiple clusters. AMKO runs as a pod in the Tanzu Kubernetes clusters and works in conjunction with AKO to facilitate multi-cluster application deployment, mapping the same application deployed on multiple clusters to a single GSLB service, extending

application ingresses across multi-region and multi-availability-zone deployments. Moreover, the Global Server Load Balancing (GSLB) function of NSX ALB enables load-balancing for globally distributed applications/workloads. GSLB offers efficient traffic distribution across scattered application servers. This enables an organization to run several sites in either Active-Active (load balancing and disaster recovery) or Active-Standby (DR) mode.

Tanzu can also provide a global multicluster service ingress that can be enabled across clusters, clouds, and regions to logically group services within these clusters together. This enables applications to be deployed on any cloud, K8s provider, and region with consistency using the same policies, security, visibility, and service discovery. Tanzu service mesh uses a construct called the Global Namespace (GNS) that logically abstracts each cluster's K8s namespace that participates in the GNS. A global ingress control plane is used that works with local clusters to create a cross-region service mesh that routes communication between services across cloud clusters. Each Cluster has a curated Istio installation that is lifecycle managed by Tanzu's Service Mesh. Tanzu's service mesh deploys a local control plane on each cluster (data plane) and has a Global Control Plane delivered via SaaS and hosted by VMware. Enablement of the service mesh can be done automatically via CLI, UI, API, and Terraform.

92. Please describe how you support vertical pod autoscaling (VPA).

Tanzu uses native Kubernetes deployment and pod specs where the Vertical Pod Autoscaler will right size resource requests. Users can implement changes via the CLI, API or UI.

The Vertical Pod Autoscaler consists of three distinct components that run in the cluster and uses two custom resources. It relies on Metrics Server to provide CPU and memory usage metrics.

There are different modes the VPA can run in which Tanzu supports

- Off: The dry-run mode. Recommendations are calculated and can be queried using kubectl describe for the VPA resource in question but are never applied.
- Initial: The safe mode. Recommendations are calculated and can be queried. They are applied when new pods are created, but running pods are never evicted in order to update them.
- Recreate: The active mode. Recommendations are calculated and are applied when they differ significantly from the current requested resources. The recommendations are applied by evicting the running pods so that the new pod gets the recommendations. Only use this mode if your pods can safely be evicted and restarted when the VPA determines they should be updated. If using this mode, and when availability is important, you should also apply a PodDisruptionBudget to ensure all of your pods are not evicted at once.
- Auto: Is currently (in v1) equivalent to Recreate. May take advantage of restart-free updates in future.

93. Please describe how you support managing cloud resources using Kubernetes custom resource definitions (CRDs).

Tanzu makes it simple to dynamically provision and manage multi-cloud resources and services using a native integration with the Crossplane framework. This eases consumption of services for developers of multi-cloud via APIs, simplifies deployments with dynamic provisioning for platform engineers across infrastructure from multiple cloud providers, and scales control planes along with growth in Kubernetes clusters, reducing complexity. A sample of resources/services that can be dynamically provisioned include AWS services such as Amazon RDS, Amazon Kinesis, Amazon ElasticCache for Redis, also services from Bitnami and VMware Application Catalog including MySQL, PostgreSQL, RabbitMQ, and Redis.

Tanzu's native runtime leverages Kubernetes Cluster-API which leverages CRD's to define the configuration of a cluster itself. Separately, our native runtime's method of package management leverages CRD's to validate package installation and dependency management.

94. Please describe how you use Kubernetes Operators.

Tanzu supports the use of Kubernetes Operators by a user but also leverages Operators internally for various components in the platform. Operators are used for critical services in the Tanzu platform such as load balancing, providing telemetry data, and monitoring the availability of all running clusters. Tanzu uses the optimal Kubernetes service dependent on the capability and needed outcome for a running service.

95. Please describe your support for a hyperconverged infrastructure solution built around Kubernetes.

VMware has a rich history of software-defined data center solutions. It has led the industry with hyperconverged software solutions that bring compute, network, and storage together into tightly integrated unified software infrastructure rather than purpose-built hardware. Tanzu is supported for deployment on hyper-converged infrastructure solutions, including VMware vSAN where it can take advantage of vSphere and vSAN cloud native storage (CNS) capabilities that automate the provisioning and scaling of persistent volumes for stateful applications. Using Tanzu with vSAN, platform teams can gain greater visibility and unified storage management for both VMs and containers with consistent storage policy-based management. Tanzu is deployed on vSAN when customers consume Tanzu services on VMware Cloud on AWS, Azure VMware Solution, Google Cloud VMware Engine, or Oracle Cloud VMware Solution. Additionally, VMware and DellEMC have a jointly validated reference architecture for Tanzu on VxRail.

96. Please describe your support for lightweight Kubernetes clusters.

Tanzu allows users to install single node clusters with small footprints for environments that can be deployed at the edge, on cloud or on–prem.

97. Please describe how you help with the configuration of Kubernetes RBAC.

Tanzu helps simplify the process of assigning Kubernetes RBAC roles and permissions by providing an easy-to-use GUI to manage them. In addition, the CLI/API/Terraform module can also be used to manage these roles. Because we ingest the various RBAC configs that can be applied to a Kubernetes cluster, we are able to surface and bind these RBAC policies to users and groups federated through your desired authentication backend. When a cluster is managed by Tanzu, the Pinniped authentication service is automatically deployed and configured to provide passthrough authentication support and role mapping on the clusters. As users and groups are assigned various roles, they get automatically mapped to corresponding Kubernetes cluster roles by Pinniped.

Tanzu offers custom OOTB roles that can be utilized immediately such as ‘clustergroup.admin’ or ‘namespace.admin’ to make adoption quick and easy. Custom roles can also be created and scoped all the way down to individual Kubernetes API objects, such as configMaps or services.

98. Please describe how you integrate Kubernetes RBAC with native IAM credentials in the cloud.

Tanzu helps organizations to integrate Kubernetes RBAC with the native IAM credentials of cloud providers by automatically configuring and deploying Pinniped to clusters being managed by Tanzu Mission Control.

Users on the Tanzu portal can be authenticated using their LDAP/ OAUTH identity provider. Tanzu authenticates users against the identity service provider and authenticates them against their assigned role. Tanzu deploys Pinniped which enables LDAP and OAUTH integration

99. Please use this space to provide any further information on capabilities related to Kubernetes features.

Tanzu adds to Kubernetes by providing consistent Kubernetes everywhere, validated integrated services, several security controls and best practices, including system audit logging, log forwarding, monitoring, automated and customizable multi-cluster operations, deep integration with vSphere, enterprise-wide management, and 24x7 production support from VMware Global Support Services.

100. How are multiple levels of developer account role structures created, changed, and updated for multiple teams, organizations, and projects, including project management features?
Tanzu supports authentication via OpenID Connect (OIDC) and uses K8s role-based access control model to create granular permissions. The platform includes out of box roles mapping users to permission scopes for app building, operating, service management, and platform operation. OIDC integrations coupled with the K8s API allow mapping multiple teams or organizations to roles based on attributes taken from the enterprise identity provider

101. How are release management and upstream compatibility handled?
When integrating new K8s releases into Tanzu, VMware thoroughly tests & validates the release to ensure they work well with the

other components in the Tanzu platform & meet their quality standards. We follow upstream K8s, validating each release against our portfolio before declaring support.

102. Q: Could you provide information about the service-level agreements (SLAs) applicable to container and cloud services offered within Tanzu SaaS?

Tanzu SaaS services adhere to a minimum SLA of 99.5%. However, the precise SLA may be contingent upon the specific underlying container management planes they are linked to. These encompass diverse combinations, such as managed Kubernetes on public cloud platforms, Tanzu Kubernetes Grid deployments on vSphere, and even customer-managed native Kubernetes instances.

For in-depth insight into SLAs associated with individual Tanzu components, you can review the following resources:

- Tanzu Mission Control
- Tanzu Service Mesh
- Aria Operations for Applications
- NSX Advanced Load Balancer

Furthermore, this commitment to SLAs extends to pertinent cloud services within the Tanzu portfolio, guaranteeing robust reliability and availability for users.

Section 1.7: Governance

103. Please describe how you support cluster policy management.

We have the capability to apply either a set of out-of-the-box or customer policies to a fleet of clusters via the Tanzu API, CLI, terraform provider, or UI. We allow organizations to view and manage their entire Kubernetes footprint centrally across clouds. Organizations can manage these clusters by grouping them into logical groups. Policies can be applied to clusters at multiple levels: Organization, Cluster groups, Clusters, Workspaces, and Namespaces. Within Clusters, we can combine namespaces into Workspaces. Policies applied at the top of the org structure can trickle down to all levels. Once a policy has been applied, any new clusters added to the group or org automatically get the policies applied to them. Tanzu has default out-of-the-box policies around access control, security policies, image registry management, quota, etc. Also, for organizations who want to define their own policies, Tanzu provides a way to define custom policies in the portal that are implemented in the backend by Open Policy Agent (OPA)

104. Please describe how you support network policy with containerized workloads.

Tanzu has the capability to apply out of the box polices to a fleet of clusters via Tanzu API, CLI, terraform provider, or UI. We allow organizations to view and manage their entire Kubernetes footprint centrally across clouds. One of the policies Organizations can apply out of the box is around Network policy, for Egress/Ingress of namespace and pod level traffic Management. Tanzu supports configuring Kubernetes CNI network policies at the cluster namespace, and pod level. Namespace and pod level policies can be enforced using label selectors.

The Tanzu Default CNI Antrea supports standard Kubernetes Network Policies and extends it with global policies bound to workloads across multiple namespaces, priority (i.e. evaluation order), tiers (using RBAC) and additional actions (DENY). In a vSphere/NSX environment the Antrea (Cluster) Network Policies can be centrally managed with NSX (the NSX tiers always have higher priority than the Antrea tiers).

Additionally, Tanzu enables platform teams to define policies around network traffic such as data geofencing, autoscaling, and SLO based policies.

105. Please describe what notification you provide when deprecating software components.

We notify users by providing in-product notification banners. We also send monthly product newsletters to customers. Depending on the severity or level of use, a direct email campaign to notify affected customers is sent out. Customer Success Managers will also reach out to ensure customers are notified in a timely manner. We also announce deprecation of version during new product version releases.

106. Please describe what notification you provide when product changes result in incompatibility.

We leverage a combination of release notes and in-product notifications to alert customers to any changes that may impact incompatibility.

107. Please describe how you enable management of service quotas.

Customers can define namespace quotas within clusters leveraging the Tanzu policy framework using the Tanzu API, CLI, terraform provider, or UI. These quotas define how much CPU and Memory can be requested or consumed. These policies can be easily applied across a fleet of clusters by logically grouping together namespaces in a construct called “Workspaces”. Once created, the Quota policies will automatically be applied to existing namespaces and any new ones that get added to the Workspace in the future. These policies can be applied to both clusters created by Tanzu or any existing/brownfield clusters brought under Tanzu’s management.

108. Please describe how you enable enforcement of trusted container image policies.

Customers can set policies that limit which registries clusters can use for pulling image using the Tanzu API, CLI, terraform provider, or UI. Tanzu has the capability to apply polices on allowed or denied image registries across a fleet of clusters. One of the out of the box policies that organizations can use is around Image Registry. With an Image registry policy, organizations can define what container images are allowed to be pulled into running containers. Organizations can also choose to block containers that

would be deployed from non-verified image registries.

109. Please describe how you support Open Policy Agent (OPA) support for managing container management policies.

Tanzu has the capability to help organizations to view and manage their entire Kubernetes footprint centrally across clouds. Apply out of the box OPA polices to a fleet of clusters via its central portal. The policy types that utilize OPA are:

- Security – Admission & Mutating
- Image
- Custom Rego policies

The OOTB OPA security templates are:

- Baseline
- Strict
- Custom

The security policies also support the 'warn' and 'dry-run' modes of gatekeeper, allowing you to determine workloads that might break if you enabled a security policy. Policy violations are surfaced under the insights view. Policies can also be scoped to namespace labels for greater flexibility.

The policies applied to clusters are continually reconciled to ensure any attempts to modify a policy are reverted.

110. Please use this space to provide any further information on capabilities related to governance.

Tanzu provides governance capabilities to ensure that applications are deployed in a secure and compliant manner. These capabilities include pre-configured templates to enable cloud native patterns. We support governance rules via an API-first approach that spans dev tooling and debugging processes, default secure software supply chains, customizable components with quick and actionable visibility and remediation steps via a central control plane. These capabilities help ensure that applications are deployed in a secure and compliant manner, and that the development process is streamlined and efficient.

We enable platform teams to apply several types of policies today, including Access, Network, Image Registry, Quota, Security out of the box as well as giving teams the ability to leverage their own custom policies. Custom policies can include additional business rules, built on user-defined templates to enforce policies that are not already addressed using the other built-in policy types as well as support for mutating policies.

Teams can achieve consistent and automatic cluster configurations synced with Git repositories by enabling and configuring FluxCD on cluster groups or individual clusters. Clusters will then continuously reconcile their state against the desired YAML objects. A common use case is to ensure clusters have all the base tooling required by an organization such as Pod runtime security agents such as Carbon Black Container or Falco. Logging and Analytics such as fluent-bit or Prometheus or Ingress controllers such as Contour.

Tanzu enables you to run inspections on your clusters for potential configuration and security risks against industry standards. For example, you can run cluster conformance inspection leveraging the built-in, open source Sonobuoy project to make sure your clusters are configured in conformance with the CNCF standards and run Center for Internet Security (CIS) Benchmark Inspection for any potential security risks.

111. How intuitive, simple, and efficient is the experience of the operator using the platform to provision, monitor, update, expand, and secure container clusters?

Operators can easily manage and scale their clusters from our container management platform across multiple Kubernetes distributions. We provide a consistent way to upgrade clusters across our runtime as well as EKS. Platform team can define rules for scaling services based on performance or efficiency needs. Clusters can be grouped into 'cluster groups' to simplify management. Identity & Access Mgmt, OPA security admission/mutation policies, network, quota and custom OPA policies can then be applied to cluster groups. Policies can be configured to target namespaces by label, negating the tedious process of manually configuring policies at multiple levels. FluxCD and Helm charts can be defined at the cluster group level so that clusters within the group automatically inherit the desired configurations and package deployments.

Section 1.8: Security

112. Please describe how you support application-level secret encryption.

We offer a comprehensive approach to support application-level secret encryption, ensuring secure and compliant operations across all levels of the application. Here are the key features collectively enhancing the security posture:

- Securing secrets during continuous delivery: Tanzu supports Secrets Operations (SOPS), sealed secrets, and key vault. Tanzu generates and manages secrets, supporting certificates, passwords, RSA keys, and SSH keys.
- Secret management for application transport layer: Tanzu provides end-to-end encryption for in-flight traffic across multiple clusters, clouds, and service meshes. With a top-level certificate authority (CA) and mutual transport layer security (mTLS) encryption, Tanzu ensures authorized services communicate securely, safeguarding sensitive data. CA integrations include Enterprise CAs, such as Venafi.
- Managing cluster secrets: Tanzu facilitates image registry secret creation and management, allowing the export of secrets to other namespaces without copying. We leverage secretgen-controller to handle secrets effectively across the Kubernetes cluster.
- Sensitive information: We offer secret properties for encrypting sensitive information, such as access keys and credentials. Once created, secret property values are encrypted and cannot be unencrypted or read.
- Cloud credentials: We store sensitive information like cloud account credentials as secrets. Access to secrets is restricted to users included in the project they are created in, ensuring proper isolation.

These features demonstrate VMware's commitment to providing a secure and compliant environment for container management across various levels of the application and it's lifecycle. By offering robust application-level secret encryption capabilities we ensure the protection of sensitive data and adherence to regulatory requirements, enabling organizations to focus on their core business objectives.

113. Please describe how you support automatic image rescanning.

To implement a comprehensive automatic image rescanning solution, we support capabilities that include scanning at the container image registry, scanning as part of the software supply chain, and pre-packaged apps and components.

- Container image registry: We use Harbor to store and scan container images at rest and restrict deployments based on rules defined by an organization. Harbor supports Trivy and Clair for container image scanning. Clair is an open source project for the static analysis of vulnerabilities in application containers and Trivy is an open source project that does comprehensive and versatile security scanning. Harbor rescans images for vulnerabilities periodically. Organizations can view hosted container Images alongside the CVE's detected in them.
- Container security: VMware Carbon Black provides automatic image scanning throughout the entire development lifecycle, including runtime image scanning. Our scanners automatically scan to detect vulnerabilities, misconfigurations, and malware.
- Software supply chain: Customers can use their own scanner as a plug-in, scan source code repositories and images for known CVEs before deploying to a cluster, while analyzing scan results against user-defined policies by using Open Policy Agent.
- Pre-packaged apps and components: For apps and components available in VMware's Application Catalog, VMware automatically monitors the source and dependencies of all images and automatically builds, tests and publishes updated versions of the images to provide the latest versions and security patches. All images are consistently hardened based on a published set of secure container best practices.

114. Please describe what CIS benchmarks are available for your container management products.

We provide integrated conformance scanning to verify that a cluster conforms to CNCF Kubernetes specifications and whether Kubernetes is deployed according to security best practices as defined in the CIS Kubernetes Benchmark. Customers can run preconfigured cluster inspections using Sonobuoy, an open source community standard. The CIS benchmarks available are based on the specific Kubernetes version configured.

VMware can also evaluate container platforms using the following CIS benchmarks:

- CIS Amazon Elastic Kubernetes Service (EKS) Benchmark 1.0.1
- CIS Azure Kubernetes Service (AKS) Benchmark 1.0.0
- CIS Google Kubernetes Engine (GKE) Benchmark 1.0.0, 1.1.0
- CIS Kubernetes Benchmark v1.2, v1.23

Benchmark definitions are regularly updated and released to customers.

115. Please describe how you support confidential computing for running containers.

We support confidential containers in public cloud using the native public cloud capabilities and in vSphere pods on AMD with secure encrypted virtualization – encrypted state (AMD SEV-ES) functionality from AMD. We also support all the capabilities of the native public clouds Kubernetes services like EKS, AKS, and GKE.

116. Please describe how you support egress to access native cloud services from clusters.

We support egress capabilities in any native cloud service along with external cloud-based services and policies to provide visibility and secure communications.

- Service-level: We support use of public or private VPCs, and proxies for cluster egress to native cloud services. Egress policies can be configured to restrict or ensure access to services over specific native cloud service networks.
- Policies: Customers can define service-layer policies which allow or deny egress traffic as necessary. It also automates the creation of routing rules, destination rules, and gateway configuration for external services.
- External services: Customers can also secure egress traffic to other external cloud-based services, virtual machines, external databases, etc. by external services connectivity configured in a Global Namespace. This includes native cloud services and can be accessed over TCP, TLS, HTTP, or HTTPS.
- Network-level: Egress (SNAT) IPs can be specified for the traffic from selected pods (in a namespace) to the external network that should be used. When a selected pod accesses the external network, the egress traffic will be tunneled to the node that hosts the egress IP if it's different from the node that the pod runs on and will be SNATed to the egress IP when leaving that node. When using multiple availability zones different egress IP pools can be attached to the zones to achieve failover capabilities.

117. Please describe how you support content trust for container images.

Content trust is supported through our image registry and in our prepackaged applications and components, all incorporated in the secure supply chain.

- We leverage Harbor, an open source container registry, to store and scan container images at rest and restrict deployments based on rules defined by an organization. Harbor can be configured to enable content trust, the ability to verify that container images pushed to the registry came from a trusted source. Harbor uses Notary to digitally sign images using keys that allow enterprises to securely publish and verify content. Organizations can define a policy in Harbor to disable any container images to be

downloaded that are not signed by a content trust.
- Tanzu also includes functionality to build containers as part of a secure supply chain. This process includes the ability to sign images using notary and include that signature in registries like Harbor. Other artifacts produced by the secure supply chain include other attestations for container trust and provide Supply-chain Levels for Software Artifacts (SLSA) trust and conformance capabilities.
- Third-part applications, as well as open source applications such as message queues and databases, that include signed images can be validated through a CLI tool. This enables trusted validation during the CD process of a secure supply chain when binding those applications to business logic application containers.
- For apps and components available in VMware's Application Catalog, we automatically monitor the source and dependencies of all images and automatically build, test and publish updated versions of the images to provide the latest versions and security patches. All images are consistently hardened based on a published set of secure container best practices.

118. Please describe how you support a software bill of materials (SBOM) for container images.

As part of the supply chain steps, we export an SBOM file for the source/image step and pass it to our VMware Carbon Black scanner, or alternatively to the customer's 3rd party scanner of choice with integrations to Grype, Snyk, Trivy, and Prisma. The output of this source/image scan is visible under a security analysis dashboard that presents the CVE's and mitigation plans. The SBOM can be exported in a standard format (XML) based on CycloneDX or SPDX formats.

For pre-packaged apps and components available in our Application Catalog, we generate a build time SBOM in JSON SPDX format for each container and Virtual Machine managed by the catalog. The SBOM contains Version, Source and Software License information for the application and all its required dependencies.

119. Please describe how you support key/secret rotation.

We primarily rely on integrations with 3rd party providers for key/secret rotation.

At a high-level, the key recommendations are:

- To support secrets, encryption should be active at the application, transport, and filesystem levels.
- Prefer external secret management solutions, such as Vault over using Kubernetes as a secret store.
- While Vault is the most mature, weigh it against what you're most familiar with.
- If using Kubernetes as a secret store, prefer using a Key Management Service (KMS)-plugin to achieve envelope encryption.
- KMS-plugins are largely immature, unless using a managed offering.
- If using Kubernetes as a secret store and a KMS-plugin is a non-option, configure encryption at rest using a static key.
- If storing secrets declaratively is desired (e.g., in git) use sealed-secrets.
- Expose secrets in volumes; not environment variables.
- Keep applications unaware of secret providers (Vault, Kubernetes, or otherwise).

We have several recommendations around key rotation based on the encryption layer found in our Securing Kubernetes Guide: https://tanzu.vmware.com/developer/guides/platform-security-secret-management/

120. Please describe if logging functions are enabled by default.

Customers who follow our best practices guidelines will have logging capabilities in every cluster being managed. Organizations can forward logs to our log management service or to 3rd party log management software. For existing/brownfield clusters, we support multi-agent logging with our own logging agents. Logs and events are collected from each container node (including

cluster control nodes), aggregated, tagged, and ingested for retention for up to 30 days. Fields can also be extracted from logs to provide custom query and reporting capabilities. Organizations have the choice to include/exclude control plane nodes.

The bedrock of security monitoring is logging. Customers can capture application logs, host-level logs, Kubernetes API audit logs, and cloud-provider logs (if applicable). We support well-established patterns for implementing log aggregation on common cluster configurations.

121. Please describe how you help with the integration of managed certificates into your container management products.

We support our customers' use of managed certificates for containerized services in two ways:

- Managed Service: Enterprises can upload their managed certs from a certificate authority (CA) to our managed service, which provides a centralized view of all the services across multi-cloud and on-prem environments. We provide integration with the Venafi Trust Protection platform to import trusted CA certs directly from a public CA for ease of use. Certficates uploaded to the central repository can be applied to any container image in any cloud/hybrid/on-prem environment. When building a public/external service, a platform operator can easily assign a pre-uploaded certificate to a service, and we automatically manage the cert allocation for that service.
- Self-Managed: We provide a catalog of services that users can download and install on their containers. From that catalog, users can deploy Cert-Management software with the click of a button. Users can then pass managed CA certs to the local Cert-Manager deployment.
- Transport/Network layer certificates: Integrations with 3rd parties like Venafi can also be used for mTLS at the service mesh and with advanced load balancing solutions, like NSX Advanced Load Balancer.

122. Please describe if monitoring functions are enabled by default.

By default, we enable monitoring of Kubernetes cluster capacity, workload utilization and service connectivity. We also default to capture platform and application time-based metrics and logs. Users can disable this feature and use 3rd party monitoring solutions using provided integration hooks.

123. Please describe how you support secret management via a native KMS.

We provide native secret management to protect credentials that clusters use to access cloud infrastructure APIs and resources, client certificates that internal cluster components use to authenticate requests, Certificate Authority (CA) certificates that clusters use to access private container registries, and credentials that clusters use to access authenticated private container registries.

Our comprehensive approach to secret management helps ensure secure and compliant operations. Here are the key features provided, collectively enhancing the security posture:

- During continuous delivery: We support Secrets Operations (SOPS), sealed secrets, and key vault providers for securing secrets when using Continuous Delivery functionality. The secretgen-controller component generates and manages secrets, supporting certificates, passwords, RSA keys, and SSH keys.
- Cluster management: We facilitate image registry secret creation and management, allowing the export of secrets to other namespaces without copying. We leverage secretgen-controller to handle secrets effectively across the Kubernetes cluster.
- Workload identities: We provide a native certificate authority that provisions, rotates, and revokes keys and certificates used for authentication and authorization for secure communications between workloads

These features demonstrate our commitment to providing a secure and compliant environment for container secret management.

By offering robust secret encryption capabilities, we help our customers ensure the protection of their sensitive data and adherence to regulatory requirements, enabling them to focus on their core business objectives leveraging native KMS functionality where possible.

We publish a Securing Kubernetes Guide that walks customers through various KMS options:
https://tanzu.vmware.com/developer/topics/securing-kubernetes/

124. Please describe how you support third-party key management.

We support the External Secrets Operator to simplify Kubernetes secret life cycle management. The External Secrets Operator is a Kubertnetes operator that integrates with external secret management systems such as Google Secrets Manager and Hashicorp Vault. It reads information form external APIs and automatically injects the values into a Kubernetes secret.

125. Which of the following security certifications has your container management products received?

FedRAMP Moderate HIPAA

PCI DSS Level 1

All Tanzu SaaS services have SOC2 Type 2, Cloud Security Aliance, GDPR, and ISO27001 at a minimum. Our global load balancing solution covers OWASP CRS protection, support for compliance regulations such as PCI DSS, HIPAA, and GDPR, positive security model, and signature-based detection.

Tanzu can be configured to meet PCI DSS, HIPAA, and NIST 800 standards. It supports a broad set of trust programs, including NIST 800-53, FISMA Moderate Mappings, and CIS Hardening. Tanzu also has an ATO and offers a managed service for Classified US Government customers on an air-gapped network. Tanzu is deployed in 4 of the big 5 Intelligence Community clients.

126. Please use this space to provide any further information on capabilities related to security.

We provide almost complete coverage of Supply chain Levels for Software Artifacts (SLSA) and Cloud Native Application Protection Platform (CNAPP). Tanzu provides an attestable golden path to production for applications that ensures SLSA 1 and 2 are met out of the box, and depending on customer configuration higher levels of SLSA can be achieved. Aria takes a pre-defined cloud and container cluster configuration definition and ensures that it operates across multiple cloud configurations, offering full Cloud Security Posture Management (CSPM). Tanzu provides full container cluster security and operational policy configuration and network ingress and service mesh configuration providing Cloud Security - Network Security (CSNS) and Kubernetes Security Posture Management (KSPM). The operational side of Aria provides protections in a Cloud Workload Protection Platform (CWPP) that is more fully realized with the runtime protections provided by Carbon Black that includes full runtime workload protections.

Upcoming features in Carbon Black around Cloud Native Detection and Response will provide context and unified visibility into endpoints, workloads, containers, and Kubernetes environments and will model an application's behavior and any deviations from that model. Users will see where a specific alert came from and what possible actions the adversary took to get there, facilitating faster remediation. Behavior modeling will detect drift and anomaly-based threats to help reduce the noise and number of alerts for security teams.

A full container management platform is only secured when evaluated as a whole application stack. VMware provides for full application and platform modernization allowing for a holistic approach from application design to developer enablement and development to a secure golden path to production that provides for secure container build, release, deployment and management of operating application containers at massive scale globally.

127. What infrastructure security options are available, including container image security (image scanning, image signing), container runtime and Kubernetes security (binary authorization, runtime inspection on containers/hosts/K8s/network/OS, intrusion detection, sandboxed/enclave-aware containers)?
We offer integrations with security scanners like VMware Carbon Black, Grype, Snyk, Prisma and Trivy. SBOM files can be exported to the scanner of choice for visualization. Our runtime security continuously scans images for vulnerabilities, malware, and misconfigurations & restricts deployments based on rules. We harden images based on best practices and automatically build/test/publish based on code changes.

Section 1.9: Application Platform Functions, including Developer Experience

128. Please describe how you provide debugging tools, including multilanguage support.

We provide a comprehensive set of debugging tools that enable developers and operators to troubleshoot and optimize their applications across multiple languages and platforms. Some of the key features include:

- Tanzu Developer Tools are IDE extensions that integrate with popular IDEs such as VS Code, Visual Studio, and IntelliJ. These tools enable developers to rapidly iterate on their code including live debugging without the need to build, push, pull a new container for each code change, and all without the need to leave their IDE.
- After an application is deployed to the platform, the application can be debugged, and metrics garnered through the App Live View feature, which allows deep introspection into the app as it is running on the cluster. Metrics include CPU and Memory consumption, threading, logging levels (including live changing of log levels), HTTP requests, latencies, success rates and many more. This is twofold – it can be viewed real-time by the developer for direct debugging, or for longer-term trends and analysis by ops teams.
- Tanzu supports all popular languages such as Java, Spring Boot, .NET Core, Steeltoe, Golang, Python, NodeJS, Ruby, and PHP using Cloud Native Buildpacks. These buildpacks automatically detect and configure the language runtime, dependencies, and security patches for the applications, reducing the complexity and risk of debugging.
- Tanzu allows operators to automatically deploy debugging tooling such as Jaeger tracing and Prometheus monitoring to all clusters within a cluster group, ensuring consistent observability and diagnostics across environments.

With Tanzu, developers and application operators can focus on creating high-quality applications while leveraging the power and flexibility of Kubernetes and multi-cloud environments.

129. Please describe how you support developer environment integrations with IDEs.

VMware Tanzu is a modular, cloud native application platform that accelerates development, delivery, and operations across multiple clouds. One of the key features of Tanzu is its support for developer environment integrations with IDEs.

Tanzu provides IDE extensions, known as Tanzu Developer Tools, for the most popular IDEs such as VS Code, Visual Studio, and IntelliJ. These tools enable developers to rapidly iterate on their code including live debugging without the need to build, push, pull a new container for each code change. Developers can deploy, delete, debug, and monitor their code progressing along the path to production all without leaving their IDE.

Tanzu Developer Tools also provide access to a curated catalog of application templates, or scaffolds, known as Application Accelerators from within the IDE. These accelerators are templates that codify best practices and ensure that important configurations and structures are in place. Developers can bootstrap their applications and get started with feature development right away.

With Tanzu Developer Tools, developers can enjoy a consistent, secure, and productive developer experience on any cloud or Kubernetes distribution. They can focus on creating great apps while Tanzu takes care of the rest.

130. Please describe how you support developer environment integrations with CI/CD workflow.

The Tanzu Developer Tools for VS Code, Visual Studio and IntelliJ offer direct visibility over the supply chain (our opinionated view of CI/CD) from within the developer's IDE. The developer has access to information such as which applications have been deployed in their namespace, their state (are they actively being updated, or debugged), and their point in the supply chain.

To get developers up and running quickly without having to worry about configuration for specific tools, the IDE plugins for Tanzu offer Application Accelerators (templated code repositories) that are known good starting points, pre-configured with the organization's language and frameworks of choice, as well as tooling like test frameworks and configurations for deep integration into the Tanzu Platform like API schema imports, documentation and metric scraping from live apps.

Additionally, should an application fail any policy gate, the developer will get information as to what stage it is stuck at, including debug information to help them resolve the issue. As an example: an application is pushed that has a Critical level CVE (Common

Vulnerabilities and Exposures) included, the security policy on the supply chain is set up to block any code containing High or above level CVEs – and so the deployment is blocked. The developer will see in their IDE that the workload has failed the deployment and will be given the results of the CVE scan so they can remediate and re-push the application successfully.

If more information is required to debug an issue, the Tanzu CLI can be used to query the pipeline run that is failing, allowing users to pull back detailed trace information as to what has broken, and any logs associated. It should be noted that developers are not responsible for the pipeline – that responsibility belongs to the platform team, who can use GitOps or directly update the pipeline – this leaves developers free to work on business logic instead of troubleshooting the path to prod.

131. Please describe how you support developer environment integrations with VCS.

To not disrupt the standard development flow of writing code, and then push to a VCS (Version Control System) such as GitHub, GitLab etc, Tanzu is designed to harness this well understood development paradigm by using git commits as triggers to kick off deployments and application builds. As such, a developer does not need to have knowledge of the platform used for build and delivery because it fits into the natural flow of software development, with the git source code repository acting as the source of truth and provenance for the code in the application.

If a new application is being deployed, Tanzu can automatically create a git repository and push templated code (that we call Application Accelerators) to this repo, so a development team can instantly start collaborating on a project with no waiting on language and framework setup to be done and pushed by a team member.

Additionally, GitOps is utilized to support platform installation, operations, upgrades, as well as gating and delivery of apps to destination environments. For example, an application can either be allowed to proceed directly to production or can be gated behind a PR (Privileges Required) approval flow in your Git system of choice, meaning that practices requiring two sets of eyes to push an app to production can be enforced.

With all teams involved in the development and delivery of applications all using git as their source of truth, this allows easier and more effective communication and collaboration across development and ops teams. As an example, code provenance is provided through the hash of the git commit in the platform, so an ops team debugging an issue will be made aware of exactly what commit caused the issue and the code changed as part of it, allowing them to communicate directly with the dev team, and honing in on the problem without back and forth.

132. Please describe how you support command line interface (CLI) or a plug-in to platform CLI.

VMware Tanzu offers a powerful and versatile command line interface (CLI) called Tanzu CLI. This tool is designed to provide an integrated and unified command-line access to the Tanzu platform, enhancing the developer experience. Key features and benefits of Tanzu CLI include:

- Plugin Architecture: Tanzu CLI is built upon a flexible plugin mechanism, allowing it to be extended with independently developed plugin binaries. This architecture enables seamless integration with various Tanzu platform components.
- Command Groups and Targets: CLI commands are organized into command groups, offering developers easy navigation and exploration of available commands. Tanzu CLI supports multiple targets, such as Kubernetes (k8s) and Tanzu Mission Control (TMC), enabling users to interact with different control planes within the Tanzu ecosystem.
- Plugin Discovery and Lifecycle Management: Tanzu CLI offers robust plugin lifecycle management capabilities, including secure installation and updates. Users can discover new plugins through the default plugin repository and easily manage them using CLI commands such as tanzu plugin search, tanzu plugin install, and tanzu plugin update.
- Context Management: Tanzu CLI maintains a list of contexts, allowing developers to switch between different user and server identities seamlessly. This feature simplifies interactions with multiple endpoints within the Tanzu ecosystem.
- CLI Configuration: Tanzu CLI configuration is stored in a centralized location, making it easy for developers to customize their CLI environment. Users can set global and plugin-specific configuration options or feature flags using commands like tanzu config set and tanzu config unset.

By incorporating the Tanzu CLI into the VMware Tanzu platform, we provide developers, app operators, and platform engineers

with a comprehensive and user-friendly command-line experience, ultimately supporting greater productivity and more efficient workflows.

133. Please describe how you support fully remote developer environments.

The Tanzu platform is unopinionated about users interacting with it either locally through tooling on their laptop, or via a remote hosted IDE, given that all builds, scans, and policy is applied on the platform itself. There is an obvious advantage to using local tooling as it provides a shorter debug time and iteration loop due to the local nature; however, should an organization choose a hosted IDE, there is nothing stopping those environments from interacting with the platform.

If a developer requires a dedicated namespace for development with discrete tooling, that can be requested in a self-service manner, and the tooling will automatically be provisioned into said namespace, providing an isolated, identical environment to production for an individual or team to test within.

The Tanzu platform also offers a Learning Center environment for new developers to be onboarded through. It includes live tutorials that can be customized by the organization to teach lessons like custom libraries or frameworks, and it uses built-in browser-based tools like VS Code and sandboxed environments, including all setup and tooling needed to get started quickly.

Once a developer is comfortable with deploying apps and using the tooling, they can choose to either deploy it locally on their laptop, or if the organization is using tooling like GitPod or JupyterLab for development, the tools can be deployed into those environments and pre-wired to communicate with no user setup or intervention needed. It provides low latency, fast access to workloads, wherever the developer is located.

134. Please describe how you support templating and application scaffolding tooling.

We offer a comprehensive solution for templating and application scaffolding tooling with Application Accelerators. These accelerators provide key benefits for developers and organizations:

- Preconfigured Cloud Native Pattern Templates: Application Accelerators are based on best practices and enable organizations to bootstrap application development and deployment in a discoverable and repeatable way.
- Authoring and Publishing: Enterprise Architects can create and publish accelerator projects, offering developers and operators ready-made, conforming code and configurations that align with their organization's requirements.
- Git Repository Integration: Published accelerator projects are maintained in Git repositories, ensuring version control and collaboration capabilities. Application Accelerator allows for the creation of new projects based on existing accelerator projects.
- Ease of Access: Accelerators are available through both the Tanzu Developer Tools in developers' IDEs and the Tanzu Portal, making it simple for developers to access and utilize these resources.
- Flexible and Customizable: The Application Accelerator architecture allows for the creation of customized accelerators, which can then be easily shared across teams and integrated into the development workflow.

By leveraging the powerful features of Application Accelerators, we support organizations in creating robust and efficient application scaffolding and templating solutions that streamline development and enhance developer experience.

135. Please describe how you support certified container images for common programming languages and frameworks.Tanzu offers comprehensive support for certified container images across common programming languages and frameworks, ensuring a seamless development and deployment experience. We cater to diverse use cases, providing access to ready-to-use images, customizable images, and flexible buildpacks for cloud-native applications:

- Bitnami Application Catalog: Delivers free container images for languages such as PHP, Ruby, JRuby, Python 3, NodeJS, Golang, Java, ASP .NET Core, and ASP.NET SDK. Bitnami Secure Container best practices guarantee consistently hardened and updated images.
- VMware Application Catalog: Allows customization of container images from the Bitnami

Application Catalog. Users can modify configuration files, libraries, dependencies, and scripts, then deliver customized images to private registries. Discover and consume certified container images from VMware and third-party vendors.

- Tanzu Build Service & Cloud Native Buildpacks (CNB): Employs CNB to build certified container images from source code without writing Dockerfiles or managing dependencies manually. CNB detects application language and dependencies, applies curated buildpacks, packages the application into a layered container image, and adds metadata. CNB exports the image to a registry of your choice, with optional image signing using cosign.
- Tanzu Application Platform: A cloud-native platform that leverages supply chains to automate application delivery from source code to production guarantees the produced container images are certified by generating software bills of materials, scanning images for vulnerabilities, signing images digitally, and storing images in trusted registries.

VMware's comprehensive approach to certified container images caters to the diverse needs of enterprises, while maintaining security and compliance. Our flexible, secure, and up-to-date container images empower organizations to focus on innovation and accelerate app development and deployment.

136. Please describe how you support automatic container rebuilds and redeployment.

The Tanzu platform is at its core a git commit-driven platform, in that every commit made to a repository or targeted branch will kick off a build and delivery through the supply chain for that application. Every commit then — if all tests, CVE scans, and other policies are met – will rebuild and redeploy the container to production if desired.

Rebuilding images can also be initiated not only by the developer committing code – but also by operators adjusting policy – assume that an application is blocked from building because a CVE scan finds a critical vulnerability – it is reviewed by the SecOps team and deemed a false positive, so the policy is updated to ignore that CVE and the build is then automatically kicked off on the policy update.

Another way in which Ops can control builds is by updating the base images containers are built from, if new Buildpacks are pulled into the environment it can automatically kick off rebuilds of every application sourced from that image to ensure they are up to date.

A final note on rebuilds is that they take time – in dev/test environments this can cause unnecessary time to be spent on waiting for builds in between debugging changes – as such, if permitted by policy, code can be live updated and debugged in a running container, through Tilt which is integrated in the Tanzu Developer Tools meaning that the loop from changing code, to testing and debugging in a prod-like environment takes seconds, not minutes.

137. Please describe how you support build automation policies.

The Tanzu platform, through supply chains, implicitly requires a policy for each step in the path to production, whether it is pass/fail for things like unit tests, or more comprehensive policies like code coverage percentage, CVE severity levels accepted in production, etc. These policies act as gates for every step along the supply chain such that all must be passed in order for source code to make it from the developer’s laptop into production.

In addition to the custom policies that can be enforced through supply chains, when a container image is built through the platform the basis of that image is always known, vetted and approved as base images (Buildpacks) are included with the platform – therefore all images transiting the pipeline can only be built through these images making the standard implicit and trusted.

Finally, before an application can run in production, its image signature is verified through the included supply chain security tools on the destination cluster – if the artifact doesn’t match the signature generated during the container build it will not be allowed to start, providing assurance that what is running in production could only have passed through the entirety of the secure software supply chain.

138. Please describe how you support build automation tools.

By default, Tanzu comes with a comprehensive build system called Tanzu Build Service (TBS) coupled with Cloud Native Buildpacks for providing automatic, robust, and trusted container builds and images for a wide array of languages and frameworks, while not

requiring the creation, maintenance, and ongoing updating of Dockerfiles.

That said, many organizations have already invested in Docker and are happy with the stack they have created with Dockerfiles. To that end the platform allows organizations to swap out components, including the build service to a tool like Kaniko, so organizations that are either happy with their current stack, or are in a transitionary period and are migrating to TBS and Buildpacks can continue operations and builds as they always have while still benefitting from the other capabilities included in the platform.

139. Please describe how you support CI/CD customization.

Tanzu offers the concept of Supply Chains, providing a way to codify all the steps in your path to production, or what most organizations know as CI/CD. Supply Chains, however, are distinct from traditional CI/CD in that they can be used generically across applications and even languages – whereas CI/CD pipelines are generally coupled one-to-one with an application, or at least a specific language and version.

Supply Chains are offered with some out of the box default examples of known good paths to production, including unit and feature testing, source and image scanning and image building and storage. However, we realize that organizations that will be adopting these tools will have opinions about what tools are used at each stage and so we allow and provide guidance on how to swap out components.

For example: you use Jenkins for testing and have existing pipelines you'd like to integrate there – you can swap out the default Tekton for your existing Jenkins pipelines – or you prefer to use Trivy or Snyk instead of the default Grype scanner – they can be easily swapped in. You may even want to add an arbitrary step to the Supply Chain to update a Jira task or send a Slack notification, these are all possible and simple using the Supply Chain concept.

With all that customization it would be easy for Supply Chain sprawl to become a major maintenance issue, as such – Supply Chains are built to be dynamic and allow automatic swapping of steps to suit the application, language, framework, or version used as well as other arbitrarily defined parameters. It is feasible and common for customers to have one or two Supply Chains in their entire organization, even using different languages across apps as steps will be swapped (for example, testing) to suit the tooling needed for the language in use.

140. Please describe how you support CI/CD policy management.

Through Supply Chains, policy management is an integral part of the path to production – every step in a Supply Chain is gated with success or failure criteria, be that successfully run tests, CVE severities, build status, or even arbitrary conditions for custom steps.

Critically, when it comes to security in particular, policy can be done per scan type (either source code, or image scans) and per workload if desired, although it is generally better practice to have a consistent policy for security scans across all workloads. This compliance can be set to allow certain CVE IDs or gate based on severity, e.g.: Critical, High, Medium, etc.

Workloads are then permitted or blocked from reaching production based on these policy gates and are reported within the UI to the platform operator teams giving them comprehensive information on why a particular step was failed, why the app was blocked as well as overall compliance from a security perspective in a dedicated dashboard so larger scale trends can be viewed.

Additionally, before an application will be allowed to run on a destination environment, the signature for that application must be verified against the signature stored in the platform from when the application was built – this signature generation and verification guarantees that what is running in production is what was built by the platform, providing assurance that all gates and policies were met and not circumvented in any way.

141. Please describe how you support third-party container registry integration.

Tanzu comes with a Harbor, a Container registry that can be deployed on-prem or in a cloud environment. Harbor provides users with the ability to sign and scan their container images, ensuring that they are secure and compliant with industry standards. However, Tanzu can integrate with any Docker compliant third-party registry. Organizations can authenticate against a third-party registry from within a Tanzu provisioned cluster by installing the image registry's pull secrets within the Kubernetes Cluster. This allows organizations to use any third-party container registry to pull/push Container Images.

142. Please describe how you support preintegrated container registry.

VMware Tanzu provides pre-integrated container registry through Harbor. Harbor is an open source container image registry that provides secure storage, management, and deployment of container images. It allows users to store, sign, and scan container images for vulnerabilities, and provides a secure way to deploy and manage container images across multiple clusters. Harbor also provides a user-friendly interface for managing and deploying container images, making it easy for users to quickly deploy and manage their container images.

143. Please describe how you provide container registry with geo replication support.

Tanzu comes with a Harbor, a Container registry that can be deployed on-prem or in a cloud environment One of the key features of Harbor is its geo-replication capability, which enables users to replicate container images across multiple geographically distributed Harbor instances. Harbor's geo-replication feature works by setting up a primary Harbor instance (the "source") and one or more secondary Harbor instances (the "targets") located in different geographic locations. The primary instance is responsible for hosting the "master" copy of the container images, while the secondary instances host "replica" copies of the same images.

When a user pushes a container image to the primary Harbor instance, the image is automatically replicated to all of the secondary instances. Similarly, when a user pulls an image from a secondary instance, the request is automatically routed to the closest available instance that hosts a replica copy of the image, improving performance and reducing latency.

144. Please describe how you provide container registry with helm chart support.

Tanzu comes with a Harbor, a Container registry that can be deployed on-prem or in a cloud environment. Harbor supports storing and distributing Docker images and Helm charts, packages of pre-configured Kubernetes resources that can be used to deploy and manage applications on a Kubernetes cluster. Harbor's Helm support enables users to store, manage, and distribute Helm charts alongside Docker images within the same registry.

145. Please describe how you support GitOps.

The Tanzu platform can be deployed, operated and life cycle managed entirely through GitOps. This goes all the way from Day-0 of platform deployment to the management, scaling and onboarding of new projects, developers, and developer environments into the platform.

With cluster-groups, arbitrary applications or Helm charts can be deployed via policy to any number of K8s clusters allowing easy customization and extension of the platform.

In fact, the platform can scale to n-nodes because of GitOps decoupling the build of applications from the delivery of that application on to the clusters that are destined to run those applications. This allows for use cases such as large-scale retail deployments where minor changes may need to be deployed to hundreds or thousands of locations.

Additionally, because the Supply Chains are entirely code based and store their state in Git, all information relating to the provenance of that application as well as version deployed to production can be traced back to a given source code commit.

For continuous integration and delivery (CI/CD), NSX ALB provide graceful Blue-Green or canary deployment based on policy-based orchestration that automates the entire process.

146. Please describe how you manage deployment automation strategies.

Tanzu, through the baseline of supply chains, can facilitate deployment strategies, such as version replacement, blue/green, canary, or feature-flag deployments through integrations with tools such as Flagger. Prior to deployment, steps are also included by default for gating those deployments via testing, security scanning, etc., requiring an app to pass all steps before it can be made available for deployment.

Supply chains provide the basis that allow us to change out the deployment mechanism based on the application type, language, destination environment or other parameters that are configurable by the organization – this allows for great flexibility when it comes to either onboarding old apps to modernize them with a straight up replacement, or in using more modern apps with traffic steering deployment strategies such as blue/green or user-agent targeting.

Additionally, the supply chain can be sourced from severaluts such as application source code, DockDocker filesnkins jobs, Maven artifacts or even existing container images allowing for complete flexibility over not just deployment, but the source of that application build.

147. Please describe how you support certified packages/add-ons for common cluster functions.

We offer out of the box certified and supported packages for baseline functionality in K8s clusters, by default users can choose to bring their own, or use our packaged solutions for ingress, certificate management, GitOps, object store, external DNS integration, metrics and logging.

Naturally, the applications we distribute are opinionated – but customers are free to choose or swap out components if they have preferences they would prefer or have standardized on for particular functions.

This can be extended beyond basic cluster-level functions to more complex and app-level packages through our VMware Application Catalog product which provides trusted pre-packaged application components that are continuously maintained and verifiably tested for use in production environments.

148. Please describe how you support installing applications from marketplaces.

The VMware Marketplace has a wide variety of vetted applications available from VMware and our Partners. Customers can use this marketplace to consume applications in the form of VMs or containers on a range of infrastructure.

Some solutions are offered by partners, while a large number of them are built, secured, and maintained by VMware directly. A wide range of these are open source solutions, either in the form of VMs, container images or helm charts. These applications can be consumed through config-as-code methods like GitOps, or through a GUI-driven experience should the organization prefer, for testing out new applications for their stack.

A platform team can choose to build a curated catalog of applications that the organization wishes to use and support internally and make those available to the consumers of the K8s platform, this allows organizations to embrace open source software to the fullest while not getting stuck with sprawl, disparate apps for the same purpose or analysis paralysis.

149. Please describe how you support on-premises marketplace access.

We support both SaaS based and on-premises application marketplaces. VMware builds its software with portability in mind. To that end, the SaaS based application catalog offering mirrors very closely its on-premises counterpart.

VMware provides the ability to curate packages/applications for your organization and serve this curated catalog to developers from the cloud, across clouds, or on-premises. The solution also supports highly popular templating frameworks like Helm, Carvel, and consumption frameworks like Crossplane allowing for better standardization, aligned with the community. Organizations in highly regulated industries can use this solution to meet compliance for control of packages/applications and meet strict on-prem or geolocation requirements including the solution being completely air-gapped.

150. Please use this space to provide any further information on capabilities related to cloud infrastructure.

Tanzu offers pre-configured templates for cloud native patterns to save developers time when bootstrapping new applications. This approach simplifies API discovery and integration for developers. Tooling and live debugging are available to developers, allowing for rapid iteration and testing. OOTB or customizable secure software supply chains automate application deployment from development to production with baked-in security and compliance. A centralized GUI delivers a unified user experience with consistent visibility into workloads and applications across application teams.

Tanzu can offer automated cluster operations to Platform teams and help DevOps and AppOps teams speed up time to deployments. Being an API first platform, you can integrate the Tanzu container management toolsets with existing pipelines and leverage familiar toolsets like Terraform and FluxCD to further automate cluster and security operations. We provide tools to ensure that your development environments are consistent with production environments so that you can avoid costly mistakes for deployments while securing your Kubernetes infrastructure.

This automation can be further extended to the NSX Advanced Load Balancer, as it is based on 100% REST APIs enabling cloud-native automation. Developers can use self-service provisioning in minutes instead of waiting for an IT ticket request. The data plane is elastic and scalable, to easily scale-out or scale-in service engines to support the ephemeral container workloads. The application service fabric has resilience and high availability built-in to ensure minimal service exhaustion or disruption. We provide end-to-end observability into application and network, allowing DevOps teams to easily troubleshoot and identify issues. For continuous integration and delivery (CI/CD), NSX ALB provides graceful Blue-Green or canary deployment based on policy-based orchestration that automates the entire process.

151. How intuitive, simple, and efficient is the developer experience (e.g., using automation and abstractions) when using the platform to build, deploy, modify, and scale applications?
Tanzu provides an intuitive developer experience that enables developers to create new apps in minutes. Developers leverage codified best practices for various cloud native patterns to get apps running with their IDE of choice. With Tanzu, developers can focus on application logic as the platform abstracts the testing, building, scanning and generating deployment artifacts automatically via secure software supply chains; shipped with preconfigured tools, but fully customizable with preferred choice of tools.

152. What low-code features does the platform have for cloud-native app development?
Tanzu Application Accelerators allow developers to create projects with pre-configured best practices for various application architecture patterns to get a skeleton running app from zero in minutes.

153. How rich and accessible are the training materials and documentation for developers? Please provide links to these resources and documentation.
Our online developer guides (https://via.vmw.com/tap15-dev-guide) offer a comprehensive set of instructions for creating and deploying applications, IDE integrations, etc.

154. What accelerators for functional/horizontal and industry/vertical scenarios are available, such as a range of artifacts (templates, data models, preconfigured workflows, etc.)?
Tanzu Developer Portal (based on Backstage) allows enterprise development teams to create, discover, and manage applications from a single interface. From the portal, Application Accelerators (preconfigured templates & workflows) enable developers to start new projects quickly. Application templates, technical documentation, and API specs are cataloged, indexed, and viewed in one place. Hands-on labs (learning centers) help developers to strengthen their knowledge or practice new skills in a safe environment.

155. How rich and accessible are the training materials and documentation for operators? Please provide links to these resources and documentation.
VMware provides a rich and accessible variety of material for operators such as our technical resource center, documentation, hands on labs as well as online training. Links are listed in the next column.

156. Does the platform provide native service/application catalogs, and does the catalog support third-party cloud-native application components? If so, which?
Tanzu Mission Control Catalog is prepopulated with Helm Charts from the Bitnami Application Catalog and Carvel packages from the Tanzu Standard repository. Customers can also bring their own private registries. Tanzu Standard repository is a set of open-source components that are supported by VMware, such as Harbor, Fluent Bit, cert-manager. Customers can additionally purchase the subscription of VMware Application Catalog (the enterprise version of Bitnami Application Catalog) which allows customization of container images, while providing support and enables customers to have a secure OSS supply chain. With VMware Application Catalog, you get continuous monitoring of upstream code changes that automatically trigger image rebuild, testing and artifacts getting pushed to the registry. Customers can also leverage the VMware Marketplace to discover and consume certified container images from VMware and third-party vendor apps such as Snyk Container, F5 Container Ingress, HashiCorp Vault, etc.

157. What prebuilt, customizable, and manageable application templates are included out of the box (e.g., Helm charts, operators, etc.) and can they be deployed across multiple heterogeneous clusters ?
Packages from Tanzu Standard repository and Bitnami Application Catalog are both included. Bitnami Application Catalog contains over 180 popular open source Helm charts. These packages can be easily deployed across multiple heterogeneous clusters using different methods such as FluxCD, or the Tanzu Mission Control Catalog. Irrespective of the deployment method used, they can be managed using the Cluster Group, to simplify deployment across all participating clusters.

158. What open source web frameworks (e.g., Spring Boot/Spring Cloud, .NET Core, Node.js Express, Dubbo, Flask, Django, and WildFly) are supported out of the box for microservice development, including microservices apps for different form factors (e.g., mobile, tablet, and PC) including features to improve code quality and dependency management?
Tanzu supports many open-source frameworks and libraries including Spring Boot, Java, .Net Core, Node.js, Python, GoLang, Ruby, Express, Django, Flask. Supported packaging and dependency management choices include Maven, Gradle, PipEnv, NPM, NuGet,

and more.
Applications built with these OSS frameworks support apps running on smartphones, tablets, and desktops or as background 'worker' tasks.
Unlike many traditional software build systems, the platform's secure software supply chain prevents compromised microservices from reaching critical runtime environments. The Security Analysis dashboard lists all vulnerabilities, simplifying triage and mitigation

159. What open source frameworks (e.g., Dapr, Orleans, and Akka) and/or features does the platform support for microservice packaging, deployment and management?
Tanzu uses Carvel packaging that enables application artifacts, e.g. images and configuration to be self contained supporting version management and continuous reconciliation.

160. What low-code features does the platform have for business-oriented developers?
Business-oriented developers wishing to integrate with enterprise apps appreciate the easy access to software catalogs, technical documentation, and API specifications offered by the Tanzu Developer Portal.

161. What microservice features are offered to modernize traditional VM-based applications on the vendor's platform into cloud-native apps on the vendor platform as well as migrate applications or infrastructure from on-premises or other cloud platforms into the vendor's platform (if applicable)?
Customers looking to migrate and modernize their application portfolio appreciate the platform's compatibility with popular Spring Cloud "12-factor" features such as externalized application configuration. Service bindings provide easy, self service access to enterprise data stores. Building and running existing Docker containers is also supported. Finally, we have Tanzu Labs consultancy services, our practical modernization experts.

162. Are FaaS services using open source (e.g., Knative), and what value-added enhancements are provided (e.g., multiple event types, complex workflow features for function chaining, and data storage options)?
Tanzu features serverless functionality based on Knative and supports Knative Functions (Beta) with buildpacks for Java, Node.js and Python. Buildpacks give developers the ability to quickly build and deploy a Function. Functions can be invoked by either CloudEvents or HTTP events from a variety of sources (including AWS, Azure, and GCP) and also leverage RabbitMQ's durable message routing functionality. Azure Spring Apps, developed and sold with Microsoft, also provides an additional native public cloud serverless experience for Spring developers.

163. What serverless container and autoscaling features does the platform provide?
Cloud Native Runtimes, built on Knative Serving, provides autoscaling for applications to match incoming demand provided by default by using the Knative Pod Autoscaler (KPA). Replicas are scaled up/down to meet demand as traffic to the application changes with support for rolling and blue/green deployments.

164. What features are available to accelerate serverless application development (e.g., features to improve code quality and productivity)?
Tanzu offers Functions buildpacks (Knative Function templates) to create Functions with multiple languages. Tanzu's Application Accelerators allow users to build and deploy Functions to a public facing URL with scale-to-zero, autoscaling, rolling updates, ingress controller (Contour), automatic HTTPS and URL provisioning.

165. What programming languages are supported in GA?
Knative Serving and Eventing are language and framework agnostic. Knative Functions feature templates for Node.js, Python, Go, Quarkus, Rust, Spring Boot and TypeScript. Users can extend the Knative Function Language Packs to create their own custom starter templates using any language.

166. What CI/CD and CDRA features are included in the platform (e.g., prebuilt or integrated third party CI/CD toolchains)?
Tanzu provides a modern CI/CD and CDRA experience that takes the best of open-source; integrates, validates and extends it to provide out-of-the-box Secure Software Supply Chains that can be fully customized. The Secure Software Supply Chain pulls source code (from
compatible repositories, inc. Git), and tests, scans, builds, containerizes, stores, audits, and deploys all the way to production via

automated GitOps workflow.

167. How are container registries integrated into development pipelines and workflows?
Tanzu software supply chains integrate with multiple OCI-compliant container registries including VMware Harbor. New images are published to the registry automatically to alleviate developers from manually interacting with it.

168. Are GitOps-style deployments supported?
Tanzu uses GitOps-style deployments. When a developer pushes code to a repository, a GitOps workflow is triggered which delivers their code through the supply chain for that application. The resulting OCI image is automatically deployed to clusters by FluxCD. The platform itself can also be deployed, managed and upgraded through GitOps

169. What automation features are available for build, testing, and deployment?
Tanzu is a git commit-driven platform. Every commit made to a targeted branch in a repository will kick off a build and delivery through the supply chain for that application. All code is tested, scanned, built into a container, scanned again, and stored in a registry. These supply chains can be customized and extended. K8s manifests are auto-generated and can be deployed to multiple runtime clusters through GitOps.

170. Which IDE plug-ins and extensions are available out of the box?
Tanzu provides extensions for VS Code, Visual Studio & IntelliJ, enabling developers to create projects using Application Accelerators (templates) and rapidly iterate on their code, debug remote apps, update code "live" & avoid the toil of build, push, pull, and apply without leaving their IDE.

171. What APIs and software development kits (SDKs) does the vendor provide beyond the Kubernetes APIs?
Tanzu offers API, CLI & Terraform for managing all aspects of Platform Engineering needs, e.g. creating clusters, deploying packages, defining policy etc. Our Workload API (a K8s abstraction layer) allows developers to focus on application logic & worry less about infrastructure. ServiceClaim API seamlessly connects apps to backend services e.g. databases & messaging. Supply Chain API enables platform engineers to create customized secure software supply chains.

172. What programming languages are supported?
Tanzu's Buildpacks (CNCF) bring out of box support for popular programming languages, frameworks e.g. Java, Spring Boot, .Net Core, Node.js, Python, GoLang & Ruby. Dockerfile support broadens this list to nearly any programming language that supports Linux containers.

173. What support does the vendor have for integrations, including operators and any domain-specific integrations (e.g., database, big data, machine learning, AI, IoT, and blockchain)?
We offer commercially supported Kubernetes operators for GemFire, RabbitMQ, MySQL & Postgres. VMware Application Catalog provides a customizable selection of trusted, pre-packaged app components that are continuously maintained and verifiably tested for use in production environments.

174. What integrations with middleware (e.g., WebSphere, JBoss, WebLogic, Kafka, and message queue) are available?
We have RabbitMQ and VMware RabbitMQ integrations. These are treated as 1st class citizens as the main backing services for Knative & Cloud Native Runtime eventing amongst others. RabbitMQ easily integrates with other messaging & streaming services.

175. What prebuilt integration support does the vendor provide for enterprise application (e.g., SAP) hosting?
We enable partners and customers to use Service Bindings to build integrations with SaaS services. Having others build integrations is a more scalable way to create a growing ecosystem of 3rd party solutions.

176. What private image registry features are available (e.g., an integrated registry, pre-integrated third-party registries, built-in operators, image scanning, image building, and CI/CD integrations)?
VMware Harbor offers a private image registry with integrated features such as third-party registry mirroring and pushing, image scanning, image signing, and robot accounts for CI/CD integrations.

177. What public image marketplace features are available (e.g., community image support, content sourcing, distribution, and federation)?
Tanzu customers get access to the public Bitnami Application Catalog, which has over 180 popular open source software applications. These are community supported images, but customers have the option to purchase VMware Application Catalog, the enterprise version of Bitnami Application Catalog, to get add on support. Customers can also make use of VMware Marketplace to access validated first-party and third-party applications.

178. What automation features are available for image management?
Tanzu leverages Cloud Native Buildpacks (CNB) to a build container image from source code without a Dockerfile. Additionally, once the image is built, CNB enables our customers to update the base image easily through image layer rebasing. For enterprises with thousands of applications deployed, this drastically reduces the efforts required to update all the applications when patching a CVE. Without buildpacks they would need to rebuild each application fully, but with image layer rebase option they can quickly update all apps with one change.

179. What differentiated image and application lifecycle management features are available? "
Application built with Tanzu automatically leverages CNB and include a software bill of materials by default. They can be seamlessly and automatically updated using the image rebase option, and are easily reproducible. All of these differentiators ensure a secure and easy-to-manage application lifecycle.

180. What platform provisioning and configuration templates (like Helm charts), automations or prebuilt offerings are included out of the box to configure Kubernetes components, including declarative configuration?
Tanzu Standard package repository and the Bitnami App Catalog are both available by default. The Tanzu repository contains: cert-manager, Contour, external-dns, Grafana, fluent-bit, Harbor, multus-cni, Prometheus & whereabouts. The Bitnami App Catalog contains 180+ Helm-based open source apps. Deployment & config can be entirely automated using Tanzu's declarative APIs, CLIs or terraform.

181. How are monitors and alerts created?
With over 200 built-in integrations we are able to ingest data from numerous sources and support the most popular open standards like Telegraf, OpenTracing, OpenCensus and OpenTelemetry. Each integration ships with dashboards and alerts built following best practices and these can be updated or customized per the users' needs.

182. What analysis features and dashboards are included? What features for multicluster and hybrid cloud (public, hosted, on-premises and edge) environments are provided? Are integrations with third-party infrastructure, application performance management, or AIOps tools available? Is eBPF supported? What differentiating logging and monitoring features are available?
Built-in dashboards or by using PromQL or our query language customers are able to further analyze data, build dashboards and create alerts.

183. Does the platform have the ability to inform at time of provisioning about optimal container size selection, and/or to query at time of launch about the best size as part of the deployment process?
VMware Aria can inform on usage data at time of provisioning for AKS and GKE workloads. For native Kubernetes, Aria can inform after time of provisioning

184. What AI services or integrations are available (e.g., search, natural language processing, machine learning and deep learning, automated ML, model explanability, speech and text analytics, computer vision, and image, video recognition and responsible AI)?
VMware Greenplum. A comprehensive range of integrations, including full-text search, natural language processing, ML, deep learning, geospatial analytics, graph analytics, and more. The integrations provide tools to process and analyze large data sets with speed and efficiency.
VMware GemFire: Leverages Spring Boot, Spring Data Flow, and other Spring technologies fully integrated with ML frameworks. It integrates seamlessly with native public cloud AI/ML or specifics like JPMML or MLFlow.

185. Which ML frameworks or integrations are available, and does the vendor offer model operation tools and features, prebuilt ML models, customizable prebuilt ML models, and/or data sets?

VMware Greenplum: Integration with Apache Madlib provides access to 10+ supervised ML models including Logistic Regression, Support Vector Machines, and Radom Forest. It also provides access to unsupervised learning via k-Means Clustering, Principal Component Analysis, and other algorithms.

186. What sources are available to access prebuilt models (e.g., ML marketplace, community, etc.)?
VMware Greenplum: Integration with Apache Madlib offers a library of 40+ algorithms specifically for data science and analytics. The algorithms cover a wide range of apps with diverse data challenges. Integration with Java and Python allows importing popular libraries such as NLTK, TensorFlow, PyTorch, and others. This allows the use of preferred tools to perform advanced analytics tasks. Apache Madlib is Open Source.

187. What advanced in-stream operations (e.g., externally created ML models, in-streaming training, imported math models, and/or other external code) does the platform support?
VMware Greenplum: PL/Python integrations give ML users access to a variety of models and libraries which can be used to score the data in Greenplum. Greenplum supports PMML which can be used to import/export via a streaming server.

188. Which services and/or integrations does the platform provide for business reporting and analytics (e.g., BI tools, data warehousing, data lake analytics, streaming/real-time data analytics, interactive analytics, geospatial analysis, and visualization), and which of the vendor's analytics services can the customer apply to data stored outside of the vendor's platform?
Our streaming server offer real-time and streaming analytics capabilities. It integrates with a variety of BI tools, like Power BI, Tableau and many others, which provides flexibility in analyzing and visualizing data.

189. Does the platform support data warehousing and data lake services, and if so, are they automatically provisioned and scaled?
We offer robust data warehousing services that can be seamlessly provisioned and scaled using VMware vSphere, providing a powerful and flexible infrastructure.

190. What are the platform's capabilities to ingest and analyze big data, including raw unmodeled data that has not been modeled for BI?
We offer a high-performance, massively parallel processing database designed for data warehousing and data analytics. It allows you to efficiently store, manage, and analyze large volumes of structured and unstructured data.

191. What data connectors for data ingestion are available?
VMware Greenplum: Data is ingested natively with gpload, Greenplum Streaming Server or with connections to Apache Kafka, RabbitMQ, Talend, Informatica, and IBM Data Stage.
VMware RabbitMQ: Natively supports MQTT, AMQP, STOMP, and HTTP.
VMware GemFire: Via integrations with Spring Cloud Data Flow, the following adapters are available to ingest datRabbitMQ, Kafka, Kafka Streams, Amazon Kinesis, Google Pub/Sub, Solace PubSub+, Azure Event Hubs, Databases to leverage CDC ingestion from well-known DB technologies. Also, there is a native Greenplum GemFire adapter.

192. What features do the data connectors have to handle large volumes, real-time/near-time updates, and content types?
VMware Greenplum: With its MPP architecture, petabytes of data can be ingested in batch or near real-time.
VMware RabbitMQ: Supports both point-to-point and pub/sub with high rates of data ingestion and multiple content types.
VMware GemFire: Supports real-time analytics for use cases such as fraud detection, risk management, or purchase recommendations. GemFire Search enables geospatial applications.

193. How does the vendor provide data preparation, data integration, and data fabric/virtualization, catalog and pipeline services and data quality?
VMware Greenplum: The Platform Extension Framework (PXF) or GPSS is used to import data. Either built-in or custom transform functions can clean/transform the data before inserting it into VMware Greenplum. The adapter for Apache Nifi enables users to connect to data pipelines and make VMware Greenplum the data sink.

194. What tools, services, and resources are available to support DataOps, data governance, data quality, and data

catalog?
VMware RabbitMQ: Provides an audit logging capability that shows user actions down to the individual resource level, supporting DataOps and data governance use cases.

195. Are all persistent storage features available for all supported deployment options, including formal partnerships for enterprise container storage?
All persistent storage features are available for all supported deployment patterns per cloud endpoint.

196. How does this vision impact the direction of this and/or adjacent markets?
VMware has been a pioneer in shaping the market and helping customers adopt a platform-as-a-product approach. It has led critical market trends (e.g. OSS frameworks, developer portals, continuous automation) which are now being adopted by other vendors.

197. What are the conversion rates from freemium to paid subscription?
VMware Tanzu does not currently have a freemium offering. Our free trial to paid conversion rate is about 15-20% depending on the offering.

198. What container network interface (CNI) drivers or plugins, both native and third party, do you support for container-to-container, container-to-host communications, and when deployed on public clouds?
We support native CNI plugins like AWS's VPC CNI and Azure CNI when deployed on a public cloud. For container-to-container and container-to-host communications, Tanzu supports Antrea and Calico. Additionally, we support third-party plugins such as Multus-cni and Whereabouts. While other CNIs can be used, maintenance, upgrades, and interoperability are the responsibility of the customer.

199. How do you manage updates and patches for the Kubernetes platform components, especially regarding automatic security updates for the OS hosting containers?
For every new software or patch release, we supply updated OS images that encompass security improvements. Users can easily modify the OS base images utilized for containers. When there's an available update, the cluster displays a notification in the portal. These updates can be manually initiated with a simple click or set to be applied automatically via a CI/CD pipeline using tools like Terraform, CLI, or APIs. To ensure uninterrupted service, nodes undergo updates in a rolling fashion.

200. What security features and controls does the vendor offer for both container images and container runtime?
Our security offerings span across the container management stack:

- OS Level for the VM: We maintain a hardened OS stack, proactively removing unwanted software, and consistently monitor for CVE’s, patches, and updates.
- Container Runtime: By default, containers are safeguarded with settings that prevent them from running in privileged mode, sharing the host namespace, or executing as root. However, these policies can be adjusted globally, affecting all containers across diverse environments. These modifications are made via global controls that impact every container Host OS. In addition, default security templates are available for deviations from these standard settings.
- Platform Layer: We facilitate secure access by mapping authorized users from trusted identity providers, such as Active Directory, to the container runtime's RBAC system. This offers granular permissions to Kubernetes resources for distinct users, groups, and service accounts at both the pod and service levels. Furthermore, mutating security policies automatically incorporate desired state security configurations to incoming workloads. For instance, if a deployment YAML omits the 'runAsUser' value, our system can autonomously incorporate it, ensuring the workload is accepted rather than denied and re-submitted.
- Connectivity: Our system implements east/west OWASP checks at the API layer, designed to halt detected attacks. This includes monitoring for connection anomalies and data protection, such as PII and PCI. Customizable API/App access control policies further

enhance security.
- Application Edge: We provide robust defense against ingress attacks through OWASP and other monitoring tools, adding runtime application controls for traffic directed to the container runtime.
- Deployment Templates: Users benefit from pre-defined templates that dictate runtime behavior. These templates can confine and regulate aspects like service binding, connectivity, policies, and runtime controls for every application deployment.
- Runtime Image Scanning: We proactively identify vulnerabilities and misconfigurations within images during runtime, ensuring a robust defense layer.

201. How do you support application security across the lifecycle, including options like code/API/artifact scanning, vulnerability detection in container images, configuration scanning for misconfigurations, automated testing for security compliance, CI/CD integration, pipeline security support, and the management of pre-packaged apps and components?

We offer comprehensive application security throughout the container lifecycle, from build to operate:

- Build: Tanzu incorporates security scanning with VMware Carbon Black, in addition to offering integrations with third-party security scanners like Grype, Snyk, Prisma, and Trivy. During the supply chain process, Tanzu produces an SBOM file, passing it to the selected scanner. The outcomes of this source image scan are accessible in a dedicated security analysis dashboard, showcasing detected CVEs and recommended mitigation measures.
- Run: Leveraging Carbon Black, we ensure runtime security, executing continuous scans on images to identify vulnerabilities, malware, and configuration oversights within production environments.
- Image Registry: Tanzu capitalizes on Harbor, a robust open-source container registry, to store and scrutinize container images. This facilitates the scanning of container images when at rest and the enforcement of deployment restrictions based on organizationally-defined parameters. Harbor introduces the concept of interrogation services, permitting the direct connection of security scanners to the registry, enabling image scans upon push or when manually initiated. Supported interrogation services include Carbon Black, Trivy, and Clair. With Carbon Black, our capability spans the entirety of the container lifecycle, from the initiation within the CI/CD pipeline to the final cluster scanning in live production.
- Pre-packaged Apps and Components: For the apps and components contained within VMware's Application Catalog, VMware systematically reviews the sources and dependencies of every image. We then automatically construct, test, and distribute the latest versions, ensuring the most recent security patches are in place. Every image undergoes rigorous hardening, conforming to established secure container best practices.

202. What analytics and data management services are available for containerized applications, either directly or through integrations, including support for analytics, batch processing, and machine learning?

We offer a modernized, comprehensive data platform designed to store, move, process, analyze, and query complex datasets in real-time and at a massive scale. This platform is optimized for containerized services and applications, and provides a suite of commonly used backing services, which include:

- A distributed key-value database optimized for a microservices architecture, offering a scalable, low-latency, and high-performance cache that handles frequently accessed data at single-digit millisecond performance.
- A massively parallel database designed for large-scale data processing and analytics tasks, featuring advanced data analytics and machine learning capabilities. This includes the execution of user-defined functions via PL/Container language extensions.
- A message broker that enables non-blocking, asynchronous messaging and event

streaming among loosely coupled services.
- A highly available and scalable SQL database suitable for both OLTP and OLAP workloads, providing a reliable persistence layer.
  These services offer flexible data management options for containerized applications and can handle tasks ranging from basic data storage to complex analytics and machine learning operations.

Section 2: Overall Viability

203. Please provide the revenue for your container management services for the last three fiscal years.

VMware does not report or provide revenue by product.

204. Please provide the number of customers for your container management services for the last three fiscal years.

We don't report on customer count by product. However, we have 1000+ customers using our container management solution.

205. Please indicate the number of personnel you have in each of the following areas.

In addition to the VMware sales team, we have over 300 dedicated sales specialists and 1000's of engineers in R&D globally.

206. Have you had any major container management product or service changes over the last three years?

The Tanzu portfolio was first introduced to market in early 2020 with Tanzu Mission Control and Tanzu Kubernetes Grid as the first components, followed by expansions into other areas that are critical to customers such as Service Mesh, Application Platform, and Observability. The Aria portfolio was launched in late 2022 with a focus on operations, guardrails, and cost.

While the fundamental principles of our product offerings remain unchanged (one being choice and meeting customers where they are in their journey) we partner daily with customers and partners to adjust our roadmap and execution to meet changing market conditions.

One foundational change has been a shift in focus from point products to cohesive end-to-end solutions that enable customers to address critical business needs without having to "assemble the Lego pieces" themselves, resulting in a faster time to value.

The Tanzu + Aria portfolio revolves around a major outcome: accelerating application delivery and, as a portfolio, we focus on three pillars of capability: deliver, operate, and optimize. We offer our customers all they need for their unique internal development & container management platform needs, with the right level of choice and customization. We also enable our customers to start small and grow into the rest of the solution and we assure them that they can bring their tools of choice across many layers of the solution (from observability to scanners to their Kubernetes distribution of choice).

207. What is the attrition/retention rates for this product?
VMware does not report externally on retention rates.

208. What is the revenue for multicloud container platforms (NOT the overall company) for the last four completed fiscal quarters?
VMware corporate policy prevents us from providing product level revenue to any 3rd party, even under NDA, other than publicly available information.

209. How many individual customer logos are there for the multicloud container platform?
VMware corporate policy prevents us from providing product level customer count to any 3rd party, even under NDA, other than publicly available information. However, we have acknowledged in public forums that we have over 1000 customers using our container management solution.

Section 3: Sales Execution/Pricing

210. Please describe any container management wins you have had in the past 12 months, highlighting the sales and solution architect aspects.

Our core and specialist teams work with the customer to ensure the correct solution is being selected for the right use cases and that they are implemented correctly to accelerate the achievement of the customer's business goals. Most Tanzu container management wins over the last year cite simplified and faster Kubernetes adoption using vSphere with Tanzu as a key factor in decision criteria. Using Tanzu has eased the management burden on IT Operations teams where multi-cloud and multi-cluster requirements for Sandbox, Pre-Prod, Prod & DR environments were present. In multiple retail, manufacturing and edge wins, the SaaS-delivered container management and observability components of Tanzu enabled a smaller footprint than incumbent solutions, with greater and more consistent management at scale.

In many wins, VMware Tanzu Labs has helped customers with the activation of Tanzu products and services, as well as providing guidance and enablement in their application transformation. Tanzu Labs' agnostic approach and differentiated service engagements have built trust with customers that often will lead to additional sales of products and services. Tanzu Labs consultants work with our customers to create a unique multi-tiered plan for implementation, accelerating platform adoption, and enabling them to help scale it over time. Through unique programs like Rapid Portfolio Modernization, we also work with our customers to understand their entire portfolio of applications, develop a plan to migrate to containers in a current or new Kubernetes platform.

211. What is the typical size of your container management wins?

Container Management Services are a portion of bigger VMware Enterprise License Agreement deals and are typically between $140K to $200K (FY23), and can range as high as >$1M USD

212. Please describe details on any discounting that applies.

VMware offers customers commitment-based discounts that increase as the customer's committed contract length and deal size grow. Discounting for Tanzu products is in line with VMware average ELA discounts.

Section 4: Market Responsiveness/Record

213. Please provide a link to your container management product announcements for each of the last three years.

See list of links for container management product announcements here: VMware_ContainerManagementMQ_Q142 announcement links

In addition to these major news announcements, we have communicated many more updates and enhancements through a series of blog announcements.

214. How many Cloud Native Computing Foundation (CNCF) projects do you support?

VMware has a strong commitment to open source, evidenced by its support for CNCF open source projects and its investment in community health through collaboration with developers and product management. VMware has dedicated teams that manage VMware-initiated CNCF projects, working daily to ensure their success and vitality. This involves fostering collaboration among contributors, supporting project users, and ensuring the project's health.

Over the past five years, VMware has contributed to 78 CNCF projects with the help of 676 contributors.

VMware actively participates in community and VMware-initiated CNCF projects such as Harbor, Kubernetes Cluster-API, Contour, and Pinniped, which are integrated into our products. For example, VMware-initiated CNCF projects Carvel and Cloud Native Buildpacks and the community-led projects, Knative, Backstage, and the K8s Service Binding Spec are all core pieces of our Tanzu Application Platform developer offering.

215. What is the length of time, in months, it takes for you to support new K8s versions?

Tanzu's Kubernetes distribution and management stack is approximately 7 months behind open source releases of Kubernetes. Our plan by the end of this fiscal year is to reduce this gap to 3 months. While staying up to date on Kubernetes releases is important, providing enterprise customers with the latest innovations in LCM such as upstream Cluster-API ClusterClass, and advanced cluster addons are key needs for these customers. VMware prioritizes these needs along with stability and reliability in our enterprise-grade solutions over these updates. Before integrating new Kubernetes releases into Tanzu, VMware needs to thoroughly test and validate them to ensure they work well with the other components in the Tanzu platform and meet their quality standards. This can take time, which can result in a lag between open source releases and supported releases in Tanzu. VMware prioritizes providing a stable and reliable solution that can meet the needs of enterprise customers over providing the latest features and updates immediately.

216. How does the vendor maintain the community strategy, and how does that allow customers to connect with peers?

VMware has dedicated OSS community management, engineering, and developer advocacy teams who work daily to ensure project success. This work includes contributing code, fostering collaboration among other contributors & supporting customers & project users. Additionally, the developer advocacy team builds content, speaks at conferences & holds customer training events to drive awareness, adoption & expertise around VMware & open source technologies.

217. What key contributions has the vendor made to upstream open source projects?

VMware initiated and/or is the main contributor to many open source projects such as Spring, Greenplum, Salt, RabbitMQ, Cartographer, Velero, Pinniped, Sonobuoy, Steeltoe, Idem & Reactor. VMware also donated numerous projects to open source foundations including Harbor, Contour, Carvel, Cloud Foundry & Antrea. VMware actively participates in projects such as Kubernetes, Cluster API, Istio, PostgreSQL, Tomcat & projects that have become key technologies within Tanzu Application Platform, such as Backstage, Cloud Native Buildpacks, Knative, Carvel, Cartographer and Flux.

Section 5: Marketing Execution

218. Please provide an overview of marketing campaigns for container management executed in 2021 or 2022.

In 2022 (VMware's FY23) Tanzu ran a global campaign for container management called Scale Kubernetes Platform Operations. The goal of this campaign was new customer acquisition.

VMware's strategy is to market to all audiences that can see benefit from VMware Tanzu.

- Primary Target Audience: platform engineering team as the primary decision maker.
- Buyers: we find platform owners also require buy in of a multi-disciplinary leadership team (CIO, VP of Apps, VP of Cloud, VP of Apps, Line of Business App owner)
- Influencers/ End Users: (developers, SRE, etc.). Our VMware Tanzu platforms answer the needs of end users because it abstracts the complexity away from the end user.

Summary of key objectives and activities

OBJECTIVE 1 **Awareness & Aircover**	**OBJECTIVE 2** **Primary Persona Acquisition**	**OBJECTIVE 3** **Executive and Account Engagement**
Key Results		
• Priority Keyword Share of Voice • Activation of targeted Partners	• New Exec Persona Contact Acquisition • New DM Persona Contact Acquisition	• CXO/C-1 Engagement • Target Account Engagement
Strategies to Achieve Key Results (The How)		
• Attract and engage executive personas through paid and earned media • Align customers journey from brand to demand campaign	• Attract and engage target personas through paid and earned media • Strategic Accounts Account Based Marketing (Global, E1, E2, C1) to influence big deals	• CXO & Executive engagement to drive pipeline acceleration • Engage with target accounts through Field events and bottom-funnel digital programs to drive pipeline creation and acceleration
Tactics Programs to Drive Strategies (The To-Do's)		
• Thought Leadership Content • Partner Demand Center Campaign • Partner Enablement Materials	• Digital Advertising Channels (Content Syndication, Paid Social, Paid Search) • Tanzu Webinars Series • Tanzu Kubernetes Connect Workshop • 3rd Party Events • VMware Explore	• Marquee Executive Events Program: • Executive Summit at VMware Explore (5) • Lead/Forward Regional Executive Events • Programmatic Digital Account Based Marketing.

Additional Resources: Gartner_Marketing Execution_Tanzu Campaigns.docx

Section 6: Customer Experience

219. Please describe how enterprises begin a relationship with you for container management offerings.

Enterprises often begin their relationship with us via our onboarding team, which helps them activate and onboard our solutions, and connects them to customer support, online resources, and training. Strategic customers also engage with a customer success manager who helps guide them through their journey.

From a solutions standpoint, enterprises often begin their journey with Tanzu for Kubernetes Operations, paired with expert guidance provided by VMware Tanzu Labs.

- Platform: TKO is a curated platform of Tanzu capabilities that provides the foundation for building a modern Kubernetes-based container infrastructure at scale across all clouds. TKO simplifies container management with tools, automation, and data-driven insights that boost developer productivity, secure applications and data, and optimize infrastructure performance across all clouds.
- Desired Outcome: How customers start with TKO will depend on the desired outcomes they want to achieve. Do they want to modernize existing applications? Provide a platform for building new custom applications? Deliver a self-service platform for developers?
- Learn the Platform: We direct customers to start with a simple use case, such as automating deployment and management of the containerized application and establishing observability of the infrastructure and application.
- Continuous Compliance: Many applications rely on Tanzu for use cases such as application resiliency and auto-scaling for compliance with SLAs, and zero trust security for compliance with data protection and data privacy regulations.
- VMware Tanzu Labs: VMware offers a portfolio of proven services and methodologies to help customers accelerate the delivery of software and modernize legacy apps, while reducing operating costs and risk.

220. Please describe the container management activities that can be performed via your portal.

As a Platform Engineer, you can perform a wide range of container management activities using VMware product interfaces. Some of the key outcomes of our solution that enhance the customer experience include:

- Simplify Security Governance & Compliance: Apply consistent policies to all clusters, namespaces, and applications across different clouds and environments. Built-in security policies and cluster inspection capabilities ensure secure and compliant multi-cloud Kubernetes deployments, OOTB policies and OPA integration.
- /Restore/Migrate: Tanzu enables easy backup and restore of clusters, namespaces and groups of resources with cross-cloud backups and restores. Tanzu also simplified migration of Kubernetes resources from one cluster to another.
- Cluster Lifecycle Management: Provision, update, and delete Tanzu Kubernetes and Amazon EKS clusters across public clouds and vSphere, ensuring consistent governance and streamlined operations.
- Cluster Health and Diagnostics: Global health insights for clusters and workloads across environments. Visualize health status and troubleshoot issues, with expanded insights through Aria Operations for Applications.
- Cluster Configuration Management: Automate cluster configuration and workload deployment using Flux CD for consistency in GitOps toolchain. Attach Git repositories to clusters and sync artifacts
- Identity and Access Management: Centralized authentication and authorization with federated identity from sources like AD, LDAP, and SAML enabling granular access management to clusters, namespaces, and even specific Kubernetes API resources.
- Extendable through APIs: Future-proof and adaptable, Tanzu offers integrations and

package deployments for monitoring and analytics, Kubernetes runtimes, BYO-Repo, and a REST API Endpoints

VMware delivers a comprehensive container management solution for modern enterprises requiring scalable, secure, and compliant Kubernetes deployments across multi-cloud and on-premises environments.

221. Please describe your contracting process for container management products/services.

1. VMware Enterprise Order is a simple, streamlined order form. It sets out the commercial terms of the deal, including a list of the products and services, start and end dates, quantities, and pricing (as applicable).
2. VMware General Terms is a single, unified set of terms that applies to all purchases of VMware software and services.
3. Exhibits to the VMware General Terms lay out the terms applicable to software, cloud services, professional services, and VMware's processing of a customer's personal data, as well as terms for public sector entities and international purchases.
4. Offering-Specific Terms apply only to specific offerings. These terms become part of the VMware General Terms agreement based on the offerings a customer buys.

Section 7: Operations

222. Please identify any outages with your container management products (e.g., bugs) or services over the last 12 months.

In the past 12 months, we have had one critical outage that caused ~30 minutes of downtime.

223. How do you handle problems with your container management products/services?

We proactively monitor our availability from external monitors that probe critical functionality, as well as tracking internal metrics that indicate the services health. In the event of a service issue, alerts page engineers with the ability to rollback recent changes or push fixes to alleviate the issue. We have dedicated SRE teams that provide incident command during these incidents, to ensure that the issue is worked to completion and that post-incident activities such as retrospectives and product fixes are discussed and prioritized.

Section 8: Market Understanding

224. Please describe your understanding of container management requirements for new application development.

For container management for new application development, organizations rely on platform engineering teams to accelerate app delivery by addressing developer needs while conforming to mandated security, resiliency, and compliance directives.

We also see Internal Developer Platforms trending upwards and bringing needed tooling to developers, removing toil/choice complexity. Organizations are seeking faster developer onboarding, a decrease in inefficient manual tickets, and automated day 2 operations of containers. Platform teams are relying on container management solutions to provide these capabilities and abstract complexity from developers.

To accomplish these outcomes new apps are expected to have serverless operational models, secure APIs, component scalability, resiliency, cloud-portable design, fault tolerance, and performance optimization which lead to the following requirements:

- Support for all types of apps regardless of underlying infra, including hybrid VM and container mixed apps
- Support for any K8s runtime on any clouds across multiple clusters, to support LoB choice
- Automated security and compliance tracked through the lifecycle of the application development.
- Ability to quickly provision dev/test environments and automate A/B testing and blue/green deployments
- Visibility into performance, security, and cost for the optimization of apps
- Curated dependencies and catalog management for apps
- Integration with existing ecosystem and open source tools and services, with the ability to expand those integrations to support developer needs
- Ability to connect to on-prem and off-prem data stores, data services, and other PaaS services, expanding to new geo locations and environments, and networking changes (e.g., encrypted requests and API discovery off-platform) all delivered through self-service.

VMware's app-centric container management services provide a platform to reliably develop, operate, and optimize any type of app on any cloud across the entire app lifecycle.

225. Please describe your understanding of container management requirements for the modernization of legacy applications.

Enterprises must carefully weigh the costs versus benefits of application modernization to ensure ROI. They must understand:

- Functional needs & infrastructure topology
- Cost, performance, & security requirements
- Non-functional requirements (resiliency, HA, geo location)

From there, they can assess effort and decide how to pursue modernization by understanding the effort to:

- Decompose an app into microservices
- Package images & code components and align to CI/CD
- Comply with data locality & governance needs
- Align people & processes around modern app models

These result in a few approaches for modernization:

- A static app may be best served by lifting & shifting into a container for use of cloud resources & more effective pooling.
- A large app may be rewritten with a combination of lift-and-shift and modern DevOps practices for better resiliency.
- An app that is suited for refactoring can be decomposed into microservices, with deployment based on GitOps.

- An app that is suited for rewriting can be re-designed with modern templates and components.

A robust container management system must provide support for that entire spectrum, including discovery of existing apps, inspection of app components and recommended modernization path. We also optimize for both app and cloud migration costs, understand performance, and security requirements

First, Tanzu Labs provides the people/process evolution that is often required to support the technology shift. For 1 & 2, Tanzu provides a shared management plane between VMs and containers on the same infrastructure and supports the DevOps model through baked-in capabilities to improve security, efficiency, and cost. For 3 & 4, Tanzu provides an entire software supply chain model. Apps that are refactored into microservices can slot into pre-defined (or user-created) “golden paths” to production. And apps written from scratch can use a set of pre-defined templates and services to streamline the path to production.

226. Please describe your understanding of container management requirements for lift-and-shift application requirements.

Lift-and-shift is important for customers who have identified apps to be rehosted, and want to leave the data centers, leverage pooling of infrastructure on K8s container management platform, reduce cost and use DevOps practices.

For such applications, the container platform’s benefits must be realized from:

- Reduced infrastructure usage due to higher workload density
- Simplification in workload image versioning and management
- Enabling cost management tooling to provide better recommendations

A lift-and-shift should also enable gradual modernization by adding the 12 factors over time as the potential ROI evolves.

Container management solutions must help organizations achieve consistent management across heterogeneous application form factors. Organizations are looking to automate their operations in a consistent way across whatever environment they choose, to streamline the operation of all applications — inclusive of lifted-and-shifted apps.

Therefore, container management solutions must support these requirements:

- Providing a set of common data services
- Providing workload placement automation (based on cost, policy, and resource usage, for example)
- Providing a set of common configuration tools, along with enabling best practices for image immutability
- Integrating modern security tools to ensure assumptions made in initial development still apply after lift-and-shift.
- Enabling modern observability tools to work with existing applications.
- Container management needs to provide brownfield apps discovery and migration path

With Tanzu and the rest of the VMware portfolio, we not only provide the container platform but also all the surround capabilities to enable these requirements starting with discovery of apps to be modernized, ensuring the realization of benefits from containerization without a complete application rewrite.

227. Please describe your understanding of container management requirements for infrastructure modernization.

Platform Engineers must manage infrastructure cost, security, resiliency, and upgrades to support diverse needs of an app portfolio. It is critical to have a common operating model and tooling that unifies security and configuration across a diverse infrastructure footprint in support of hybrid and multi-cloud, multi-K8s deployments.

Container management solutions must meet customer needs across existing infrastructure, in any cloud, and any K8s environment, with consistent tooling for cost, performance, and security across containers and non-container environments. It is necessary to provide prescriptive templates and infrastructure as code to rapidly provision/de-provision complete environments that include the containerized apps and the underlying infrastructure. Consistent management experience of configuration, security, and observability is also key.

Container management solutions require infrastructure to support:

- Multi-cloud, multi-region, multi-AZ deployment patterns
- Network traffic connectivity and observation in a configurable and composable way in-line with GSLB and underlay connectivity requirements, isolating environments for multi-tenancy
- Automated and seamless secure connectivity to external resources, either in the same cloud, or across clouds for container and non-container apps
- Guardrails and policies on new infrastructure resources, including container runtime
- End-to-end cost, security, and performance optimization from app to infrastructure, with the ability to isolate metrics across shared container infrastructure
- Automated infrastructure landing zones, along with policies and accounts

VMware enables organizations to manage hybrid infrastructure using a common control plane across VMs and containers. We focus on a composable, extensible approach to infrastructure modernization that allows customers to leverage existing tooling, while taking advantage of new capabilities that deliver security, resiliency, and cost optimization.

228. What is the vision for the offering?

VMware's vision centers around an application-first approach that helps organizations develop, operate & optimize apps at scale across public and private clouds, on-prem and at the edge. Our customers have choice and flexibility in runtimes, clouds and data services with common management and governance that provides consistency, simplification of Day 2 operations and superior DevEx across complex enterprise environments. Our vision is to enable higher-order services that abstract across various runtimes, separating app concerns from the underlying infrastructure.

229. How well articulated and differentiated is the vision?

VMware's vision has been articulated extensively & publicly at tradeshows and industry events. We are differentiated by our comprehensive yet modular approach that includes: 1) a federated data platform that integrates with customers' existing tools to provide a near real time state-of-environment and apps, enabling collaboration across teams 2) a common control plane across clouds and runtimes with centralized control and policies enabling continuous management of cost, performance and security 3) an integrated DevEx that curates best practices for development & deployment via app accelerators addressing the entire app development & delivery lifecycle.

230. How relevant and well defined are planned enhancements?

Our FY24 roadmap focuses on enabling customers to accelerate app delivery across clouds by helping them develop, operate, and optimize apps.

Develop:

- Speed time to production with secure Golden Paths that capture app knowledge/best practices & with OOB OSS content
- Simplify developer experience with LLM based assists, shift-left of operational metrics, and by leveraging AI/ML to abstract infra & app runtime configurations

Operate:

- Simplify Day 2 Operations to manage and scale apps seamlessly even as underlying infrastructure is updated & optimized.
- Automatically maintain the desired level of security, HA, resilience, (defined by intent) by integrating into cloud services and dynamically configuring it to meet "intent" on an ongoing basis.

Optimize:

- Unify app and infra governance with continuous refinement for cost, performance and security of running apps
- Meet customers where they are with a rich set of ISV and tool integrations, ensuring customers can easily leverage existing tools

231. How effectively do they address changing customer requirements?

We use customer value around software agility as the primary metric to prioritize R&D. Customers want simplicity of operations, ability to leverage existing investments, choice of runtimes, clouds & services, continuous enforcement of governance, rapid onramp to new techniques such as AI/ML, rapid startup with OOB best practices. Our roadmap addresses these requirements.

Section 9: Marketing Strategy

232. Please describe how you market container management services for net new development.

Overview

Tanzu provides the foundation for building a modern container infrastructure at scale, across all clouds. Our marketing strategy for container management is to provide a holistic solution that incorporates platforms, tools and people, and processes. We are passionate about meeting customer needs and focus on outcomes-based solution selling in our marketing strategy.

Product Positioning:

For net new development, Tanzu provides products and services that accelerate application development and delivery while complying with corporate standards for security, allowing fast iteration and feedback, and enabling developers with pre-curated templates complying with industry and security standards for app development.

Messaging:

Currently, we are also focused on addressing challenging macro-economic trends. Our thematic focus highlights how we address customer needs to optimize, increase efficiency and productivity, increase resiliency, increase revenue and help our customers remain competitive during these challenging times. We share this message with three target audiences – App Owners (Buyer), App Platform owners (Decision Maker) and Developers (End Users). See question 145 for more information on VMware Tanzu Campaigns.

Services Marketing Approach:

We market technology solutions and consulting engagements to customers needing operational readiness and skills transformation. Our platform services engagements help customers build a modern platform to centralize, provide guard rails, and increase developer efficiency by providing learning, accelerators, supply chains, and tooling. Our application services engagements tune developer practices via short iterations and extreme/test-driven development. We offer packaged service engagements which help stand up a modern app platform and get an app running on it while enabling platform engineers and developers to use the new platform optimally and confidently.

233. Please describe how you market container management services for legacy modernization.

Overview:

VMware Tanzu takes a holistic approach across people, technology, tools and practices to rapidly achieve customer outcomes, maximizing value, even with legacy systems of various maturity levels.

Messaging:

We market to customers focusing on app delivery transformation with a goal of speeding time to value. This includes code modernization, focus on value, and full stack insights (code, infrastructure, resource utilization, data). We share this message with three target audiences – App Owners (Buyer), App Platform owners (Decision Maker) and Developers (End Users). See question 218 for more information on VMware Tanzu Campaigns.

Product Positioning:

We use a top-down design approach, leveraging lean concepts to learn user needs & position products around them. Together, VMware Cloud, VMware Tanzu, Aria Migration, and Tanzu Labs engagements help customer discover apps and modernize them with minimal disruption, including app and data modernization, and cost savings by migrating or containerizing apps. Tanzu & Aria tooling provides portfolio analysis before we build a cloud-agnostic modernization framework and business case for refactoring or developing new, cloud native apps, while identifying risks to execution.

Services Marketing Approach:

The assessment and migration cost of legacy applications can be high if approached individually as it requires time and a large amount of application knowledge. We use advanced tools to rapidly collect data from various sources and create a model of the portfolio. We identify patterns and archetypes within the environment and then use them to identify groups of applications with common technical features and/or technical debt and build out a golden path. Modernization solutions can then be created for representative applications within the archetypical groups. These solutions are leveraged to the other applications within the group to achieve scale, reduce duplication of effort across the portfolio, and modernize efficiently & cost-effectively.

234. Please describe how you market container management services for lift-and-shift scenarios

Overview:

We focus on matching the needs of enterprises and apps to the best cloud environment and provide consistent container management across clouds. Because of VMware's consistent infrastructure deployed to every hyperscale cloud and thousands of clouds worldwide, our customers have a unique opportunity to move production enterprise apps to any cloud and between clouds without the cost, complexity and risk of refactoring. This is done with minimal downtime, significantly accelerating cloud migration initiatives. VMware provides consistent management and operations for any type of app, whether running in a VM or a container.

Product Positioning:

VMware container management solutions give our customers the best of both worlds with the ability to manage both on-premises and cloud deployments. With full end-to-end monitoring and visibility built-in, and continuous optimization for cost, capacity, and performance, they can operate containers on a familiar VMware vSphere tool stack to drive agility and productivity.

Messaging:

Our container management services allow developers to focus on consumption and motoring applications at the application layer, while I/O teams focus on monitoring VM and containers at the infra layer, extending existing investments in VMware software stack and providing full visibility into business applications for both VM and container-based workloads while minimizing staff retraining and complexity.

Services Marketing Approach:Tanzu Labs provides proven practices, and automated tools to reduce risk and accelerate impactful, measured outcomes that go beyond tactical solutions. Through a services engagement, Tanzu Labs confirms the app inventory, applies a first-pass filter, and initiates a technical discovery to determine app components and dependencies. Next, we strategically prioritize app modernization candidates based on business impact and goals and rank them before initiating modernization, helping customers start small and scale fast.

235. Please describe how you market container management services for infrastructure modernization.

Overview:

Because VMware Tanzu's products work well with on-premises, hybrid cloud, multi-cloud and at the edge, VMware is able to extend our marketing strategy to complement infrastructure modernization initiatives at our customers. VMware has a large and loyal vSphere installed base so these customers understand a cloud-like experience which is a natural precursor to public cloud. Our marketing strategy for customers who are utilizing vSphere is to focus on augmenting and unifying their infrastructure management through VMware Tanzu and VMware Aria.

Product Positioning:

VMware Tanzu provides a unifying runtime that can increase operational efficiency and consistent management because it runs on any infrastructure type. It can therefore be leveraged as part of a foundational and enabling technology for infrastructure modernization.

Messaging:

VMware Tanzu offers an enterprise-ready runtime for quickly delivering workloads, addressing macroeconomic pressures to provide value quickly, and increasing security threats with automated spin-up of security-hardened dependencies. We share these messages with three target audiences – App Owners (Buyer), App Platform owners (Decision Maker) and Developers (End Users). Please see question 145 for more information on VMware Tanzu Campaigns.

Services Marketing Approach:

Tanzu Labs modernizes infrastructure with container management services, Kubernetes deployment, rationalizing and analyzing workloads, and tooling to manage and observe the architecture. This helps organizations reach 90% operational efficiency. We find that our customers get most value out of an initial product activation service engagement and a portfolio modernization service engagement that set them on the path to effectively operationalizing Kubernetes that rationalizes their workload modernization, followed by custom services engagements to refine and mature their platform engineering practices in service of developers and lines of business.

236. What advanced wireless communication (including but not limited to 5G) support is available?

We modernize our customer's existing telco clouds in preparation for 5G deployments. Our Telco Cloud Platform improves innovation by enabling telcos to deliver new applications and services, reduces operational complexities & helps our customers

realize substantial cost savings, further accelerating their cloud modernization journey to 5G. With VMware's telco cloud solution, companies can operate cloud-native telco clouds with speed & agility while maintaining carrier-grade performance, resiliency & service quality. Modernized clouds enable our customers to scale network functions up & down dynamically in an automated manner—providing them with the ability to introduce core, edge & far edge innovations quickly.

237. What features or services are offered to migrate applications or infrastructure from on-premises or other cloud platforms into the vendor's multicloud container platform (MCP) in multicloud environments?
VMware offers Tanzu Labs professional services to work side-by-side with customers to build a cloud native platform & modernize their app portfolio through our Rapid Portfolio Modernization program: we leverage in-house tooling including Cloud Suitability Analyzer & vRealize Network Insights to aid in the discovery, analysis, containerization& migration of apps. We can also help backup & restore workloads to any CNCF-conformant cluster running on any cloud.

238. How does this approach anticipate and exhibit a commitment to innovation relevant to customer needs?
We anticipate customers' needs by engaging enterprise customers in design partner programs, trials & advisory boards, having broad engagement with & participation in OSS communities and incorporating continuous feedback from close strategic partnerships & services engagements.

Section 10: Sales Strategy

239. Please describe how you sell container management services to high-touch buyers.

For VMware's strategic customers, the VMware Tanzu field team leads with a solution-oriented approach by consulting with customer personas like Application Leader or Platform Engineering leader. This helps the VMware Tanzu field team to clearly understand the customer's current pains with their application path to production on any landing zone, as well as understanding the skillset and tools they currently employ. The field team can then show them a future state of how their current pains can be resolved with the tools within VMware Tanzu and VMware Aria with TCO metrics.

The VMware Tanzu field team then aligns our Customer Success teams with the customer stakeholders to ensure they get value out of their purchase. They do this by executing with the customer against a proven customer solution journey, continually showing metrics of improvement, and then expand the use cases within a customer. In short, VMware Tanzu field teams start with their desired business outcomes, then partner with them to create a compelling value proposition. This helps the customer realize benefits around costs, innovation, and speed to market, and mitigate risks, depending on what opportunities represent their highest priorities. Our collaborative approach includes technical, process, and team-focused workshops, path-to-production exercises, value stream mapping, automated analysis of workloads, and developer-centric platform design sessions. From these exercises the field team builds a strategic vision that emphasizes our partnership with the customer and shows a way forward through the operational and technical challenges of modernization and containerization.

The products and services of the solution the field team puts forward are designed to enable the customer to build, refine, and mature a secure, performant, efficient, and reliable platform that self-sustains by creating a streamlined developer experience.

240. Please describe how you sell container management services to users not needing "white glove" service.

VMware's vSphere platform has a feature to enable Tanzu Kubernetes Grid as part of its workload management feature. For existing experienced vSphere users, this offers a turnkey approach for them to provide a Kubernetes dial-tone to their end users. A lot of VMware's customers buy this feature along with their purchase of vSphere.

In addition, VMware has a program known as Subscription Purchase Program (SPP) where customers can purchase SPP tokens up front and self-service redeem them for any product in the SPP marketplace. Tanzu products are available via the SPP program for customers to easily purchase, and many of our Tanzu container management products are also available on the public cloud marketplaces.

241. Please describe how you use MSPs in selling container management services.

We launched our MSP program this past year, so our initial focus has been building up our foundational ecosystem. We have seen a growing need for managed service providers due to a large skills gap in Dev/Sec/Ops and Platform Ops within our customers across every segment. Our strategic MSP partners are very excited about the opportunity to deliver customer outcomes, business value, in an end-to-end offering that customers can consume with monthly payments. We are seeing asset-heavy and asset-light partners emerge in our ecosystem.

The Tanzu MSP business model is critical to drive growth in net-new customers and to fully realize the solution outcomes for customers that already own Tanzu licenses. Our Tanzu sales teams are driving joint GTM with our MSP partners and our MSP partners are leading full customer lifecycle on their own as well.

242. Please identify the top 10 most strategic MSPs that you work with.

1. Capstone
2. CDI
3. ITQ
4. TeraSky
5. evoila
6. Telecom Italia
7. SVA
8. Rackspace
9. Lumen
10. ATEA

243. Please describe your approach to solution selling in the context of your container management offering.

VMware Tanzu goes to market with a customer outcome-centric messaging and packaging. Our portfolio is organized and packaged to achieve two key customers outcomes which are:

- Faster, more secure paths to production
- Automate Kubernetes platform operations.

We work with the customer to understand their current path to production and operational readiness regarding tooling and skills and provide a solution aligned to the above outcomes that will be delivered by either one or a few products in the VMware Tanzu and VMware Aria portfolio. Our direct and channel customers also have the benefit of modularity so they can choose the right components that work for their needs.

244. Will the company's approach to innovation for maintaining or obtaining a leadership position in this market?
Our approach combines the strong understanding of customer's IT & business drivers with a deep investment in technical expertise to deliver innovative solutions. By exposing R&D to customer needs & enabling direct customer interaction, we tap into innovative ideas across a much larger team. For e.g., this approach has allowed us to incorporate graph tech from media companies to deliver infra/app visibility, AI to do continuous policy/SLA enforcement, and LLMs to create remediation code on the fly.

245. How does the vendor communicate the roadmap to customers?
Our roadmap is shared at industry events, through our release notes and in private customer meetings.

246. What is the approach to developing and maintaining partnerships relevant to this market?
VMware has an ecosystem of GTM alliances which includes CSP, MSPs, GSIs, strategic alliances and resellers. In the large enterprise segment, VMware works with CSP, GSIs and Strategic partners to jointly drive customer value and broad based adoption of use cases. In SMB segment, VMware works with MSPs and VARs to drive sales and adoption services. Our sales and services partnerships are critical to ensuring net new customer acquisition and adoption within existing customers through services.

247. How does the vendor enable MCP adoption to maximize product use (starter kits, prebuilt offerings)?
We enable adoption in several ways:

- We ensure that use cases are understood during sales cycle.
- Post sales, Tanzu Customer Onboarding Specialists and/or Customer Success Managers (CSM) guide customers through onboarding.
- Tanzu Academy Learning Paths guide customers through self-paced videos & hands-on labs, and some products include an integrated get-started guide.
- Finally, we offer an extensive set of design, activation, acceleration and scale-out services to support adoption of industry best practices leveraging our solutions.

248. What customer success models are available to facilitate/enable MCP adoption, including in multicloud and/or hybrid environments?
Customer success is included with all Tanzu product sales. CSM help customers achieve faster, secure paths to production, automate Kubernetes platform ops, & optimize for app cost, security & performance.

The success model outlines steps and success metrics to design, activate, accelerate, and scale adoption. These services help customers build, deploy and configure platforms, while also training them on modern operating techniques. This involves setting up the platform across multiple clouds, advising & helping with modernizing and moving workloads across clouds, guiding DevOps teams, and helping to build Developer Experience functionality. We train partners on the same techniques so they can create their own centers of excellence.

249. What additional products or services are offered to support or enhance customers' investment in their MCPs other than those described in Current Offerings above?
VMware Tanzu Labs, the professional consulting services branch of VMware Tanzu, helps customers get started using their Tanzu

MCP products through packaged professional services offerings called Tanzu Activation Services. Tanzu Activation Services are custom scoped services to deploy the new container platform into a customer's current cloud environment and then get an application running on it to realize the value of the platform immediately.

We ensure a smooth transition from installation to operation with Customer Success solutions including Tanzu Technical Account Managers who work with customers to adopt, use and procure our Tanzu products while optimizing their multicloud environment; Tanzu Academy, our online 24/7 learning platform for Tanzu products that allows customers to get started using and maintaining Tanzu products in their multicloud environments; and our Customer Success Managers who provide ongoing support for our Tanzu multicloud products.

VMware Tanzu Labs also offers custom professional services to accelerate adoption of multicloud container platforms at scale including application migration and modernization, platform health checks, secure software supply chain engagements, building automation, training in site reliability engineering and platform engineering best practices. We work side by side with our customers to enable them to run, maintain and manage their platforms independently after our services engagements have ended.

Section 11: Offering (Product) Strategy

250. Please describe your container management product roadmap for the next 12 to 18 months.

Over the next 12-18 months, we will focus on enabling customers to accelerate app delivery to any cloud by expanding the capabilities to develop, operate, and optimize applications at the right cost, performance, and security. The VMware portfolio is uniquely positioned to deliver an end-to-end solution with flexible customer entry points to use the products they choose and gain exponential value with each additional solution.

Develop:

Our focus is capabilities to enable platform teams to manage self-service access for developers around resources like clusters or namespaces as a service, provisioned with guardrails to ensure organizational security, networking, cost and compliance needs are met. With these capabilities developers experience fewer delays in their day-to-day work, a faster time to market, and a proactive approach to managing vulnerabilities early in the cycle, rather than after deployment.

Operate:

Our App Runtime will decouple the logical representation of an application from the physical deployment and connectivity; it includes capabilities like aggregated observability, one command deployment, and standardized secure images and will enable platform engineers to enforce consistent cluster configurations and usage, making the infrastructure complexity invisible to the developer. Additionally, we'll enhance multi-cloud container management capabilities including advanced options for upgrading, patching and simplifying zero downtime operations.

Optimize:

We will further integrate Tanzu and Aria to continuously improve application cost, performance, and security from the container management solution including providing Developers easy visibility into the cost, performance, and security data for each of their applications directly in the app platform to help make better, informed decisions.

251. Please describe your container management product roadmap for the next three to five years.

As Kubernetes gains adoption over the next three to five years, VMware's early investment in managing clusters at scale will help accelerate our ability to meet the needs of enterprise customers. As the basic building blocks for container-based application development and operations become commoditized, we are focusing on building higher level solutions and ways to help customers optimize.

Develop: Provide golden paths to production to capture app knowledge and practices.

We will speed up the ways teams develop, by automatically creating app runtimes based on app traits and characteristics, further abstracting Kubernetes complexity from developers. The app requirements, such as security, will be autoconfigured based on app characteristics and AI/ML recommendation engine.

Operate: Deploy, manage and scale apps seamlessly even as underlying infrastructure is updated.

More customers will be operating clusters in more locations, like the edge, so we will be investing in ways to optimize the distribution and management of applications across edge sites. To simplify service dependencies, we will provide a deeper integration into cloud services, further abstracting the complexity from developers and simplifying how teams operate the platform. For example, developers shouldn't need to care where the app or database is running, they should just know that it will run, and a database will be there.

Optimize: Continuously tune cost, performance and security of apps at runtime.

Additionally, we will provide more integrations with ISV partnerships to help customers optimize their platform, via our Application Runtime, ensuring that customers can easily use their tools of choice. This will give customers the flexibility to choose the right tool for their business needs.

252. What is the innovation strategy, including R&D budget?

Our innovation strategy is focused on delivering a comprehensive yet modular, capability-rich yet simple solution that accelerates app delivery by simplifying how our customers develop, operate & optimize apps. We prioritize capabilities that help customers achieve business outcomes. We have 1000s of developers across 4+ geolocated centers providing 24x7 development & innovation.

253. How well positioned is the strategy to execute on innovation given the history of innovation investments?
VMware's top priority is to accelerate customer's modern app transformation. We have deep domain & market expertise with Pivotal, Heptio, Bitnami, Wavefront & Spring OSS heritage. We make pioneering contributions in many open source communities and maintain cutting edge innovation across OSS & commercial offerings.

Section 12: Business Model

254. Is your container management product/service offered as a stand-alone service or as part of additional/complementary services?

VMware Tanzu is a fully modular portfolio of container management products that fits any scenario. It is sold as standalone products or as full technology solutions depending on the customer's need. VMware Tanzu is differentiated in that we can provide an opinionated and integrated stack of products, or we offer individual products that can work with the end customers' existing tooling. Customers can pick what they want and ensure that they do not have to rip and replace existing technology investments. Our VMware Tanzu solutions work alongside, and in some cases integrate with, other vendor's products.

We also offer certain components of VMWare Tanzu as part of vSphere + entitlements.

X Offered as a stand-alone service

X Offered as part of additional/complementary services

Section 13: Vertical/Industry Strategy

255. Please describe the approach to offering your container management offering for regulated workloads.

Regulated industries that need to comply with regional data security, residency requirements, while innovating for greater value, can experience the benefits of VMware Tanzu in a compliant environment.

No Internet connection dependency

For those customers that operate in sensitive industries, Tanzu is now available without a dependency on internet access (“air gap”) for deployment. VMware Tanzu, when on sovereign clouds enables organizations to operate a non-SaaS service so that they can maintain independence from any web connectivity. This on-premises offering maintains the sovereignty of the data, environment, and personnel in which it runs.

Sovereign-Ready Solutions

VMware Tanzu solution on sovereign cloud includes a hosted and/or managed offering that can be operated as a fully disconnected version of VMware Tanzu products, including the tools and open- source technologies that organizations need to deploy and consistently operate a scalable Kubernetes environment.

256. Please describe the approach to offering your container management offering for specific industries.

VMware Tanzu is used by some of the world’s largest organizations across several industries including insurance, healthcare, retail, banking, financial services, automotive, energy and telecommunications among others. The Tanzu family of products and services is particularly well-suited for the needs of highly regulated industries.

For example, VMware Tanzu today meets over 80% of Federal Authority to Operate (ATO) requirements, out of the box. It also enables compliance with numerous Federal security standards so government agencies can spend less time juggling compliance requirements and more time building software that delivers real outcomes.

VMware Tanzu is a critical component of VMware Telco Cloud Platform, providing Containers as a Service (CaaS) functionality for cloud native network functions to help telco operators transform their networks to support high speed low latency 5G services.

Meanwhile, with Tanzu Labs’s expertise in these sectors we offer consulting and training that is tailored to our customers unique regulatory and industry needs with a high concentration of expertise in financial services, federal government, healthcare, insurance, retail, automotive and energy.

Section 14: Innovation

257. Please describe the investments made in the last 12 months to enhance your container management technical capabilities.

VMware delivers solutions that integrate the end-to-end app lifecycle. We help customers develop apps with golden paths, operate and manage containers at scale across any cloud, and optimize ongoing cost, security & performance:

Develop:

Our app platform investments have focused on improving the developer experience with deeper integrations, enhancements, and extensions of the Backstage dev portal technology; expanding our catalog of curated app patterns; broadly distributing and enhancing our large catalog of secure and compliant open source packages; monitoring and productizing industry best practices into out-of-the-box capabilities for development and deployment; end-to-end security; and metrics like DORA and SLSA.

Operate:

Our core platform investments for container management have focused on capabilities such as a near real-time configuration graph of applications and dependencies to improve troubleshooting, optimize day2 operations, and automate scale-in and scale-out; a powerful AI/ML data platform for auto-remediations and business insights; an app-aware platform that auto-adapts to app needs and org best practices; enhancing enterprise reliability with built-in data protection, backup and restore capabilities. We're investing in GitOps with FluxCD for Tanzu managed clusters and our Istio based service mesh and deepening the integration between the service mesh and container management.

Optimize:

Our investments to optimize container management have been focused on integrations with our Aria platform to enable governance and continuously improve the cost, security, and performance of applications, container management environments, and underlying infrastructure.

258. Please describe the investments made in the last 12 months to enhance your container management business capabilities (e.g., ecosystem expansion).

We have enhanced our business through new pricing and packaging that simplifies the customer buying experience, expansion of our alliances and partner programs to a wide array of partner types and routes to market.

- Pricing and Packaging – We introduced the Tanzu for Kubernetes Operations sku to package together simplify the go to market messaging and customer buying experience for container management solutions from individual capabilities to an inclusive suite.
- Managed Services Provider program – We launched an MSP program specifically for container management partners. Program details are provided in the answer to question 162.
- VMware Cloud Provider program (vSphere partners) - We continue to invest in our robust ecosystem of vSphere partners by providing VMware Tanzu products in both a rental and managed service context. In 2022, we expanded our VMware Tanzu offerings to Sovereign Cloud providers.
- Alliances Expansion
    - Microsoft Azure Spring Apps was introduced in 2019 as a managed service with a basic revenue sharing model. In 2022 we launched Azure Spring Apps Enterprise – also a managed service, which is developed, promoted and sold in collaboration with Microsoft. The partnership on Azure Spring Apps Enterprise is unique in that VMware controls the pricing of the Tanzu components and as such does not require revenue sharing.
    - Dell: Tanzu for Kubernetes Operations on VxRail provides a curated hyperconverged infrastructure that establishes a foundation for building and managing a modern container platform built for enterprise scale.
    - Native Public Cloud: VMware Tanzu continues to tightly integrate our VMware Tanzu container management offerings with Microsoft and Amazon. VMware Tanzu has

been available for customers through the Amazon Marketplace and Azure Marketplaces and is co-sold with Amazon and Microsoft sellers.

259. How much has been invested in the last 12 months to enhance your container management technical capabilities and business capabilities?

VMware is a publicly traded $13B revenue company and does not report at this level of detail in our financial statements

260. Are service mesh services using open source (e.g., Istio/Envoy) or homegrown components included in the platform out of the box?

Our service mesh is built on an Istio base and extends the capabilities of Istio/Envoy in multiple ways. It delivers a fully managed OSS Istio experience while incorporating unique, value-added capabilities from VMware - such as advanced SLOs, API Security, Data Security, and Access Control Policies. We do not modify Istio, which allows customers to benefit from open-source features and compatibility with the broader Istio ecosystem.

261. If the component is open source, what value-added enhancements are provided, if any?

We enhance Istio by:

- Adding Envoy filters/WASM plugins to provide a new level of visibility and security at the API and data level.
- Controlling multiple service meshes from a federated control plane delivered as SaaS.
- Using our unique Global Namespace abstraction to deliver strong isolation, multi-tenancy, and simplified operational models for DevSecOps across single and multi-cloud environments.

262. Does the vendor offer consistent versions of its platform for both on-premises and public cloud/multicloud deployments and allow integration directly with the public cloud providers' managed Kubernetes control plane, including in multicloud scenarios?

We are consistent across our Tanzu self managed & SaaS solutions. Most Aria products are available in self-managed or SaaS. A self-managed version of our container mgmt solution Tanzu Mission Control will launch imminently. SaaS-based Tanzu solutions are continually being evaluated and integrated into our self managed offerings to provide a consistent experience & those that are already released as Self Managed provide consistency across both deployment models and public & private cloud.

263. What types of deployment models are available (installable software suites, self-managed on converged infrastructure, vendor-managed converged infrastructure, SaaS, multicloud, etc.)?

SaaS, self-managed, self-managed on converged infrastructure, self-managed multi-cloud, vendor-managed on converged infrastructure, vendor-managed and partner-managed multi-cloud are available today.

264. What formal partnerships does the vendor have with public cloud providers and data center equipment providers, including managed services and multicloud environments?

We have formal cloud partnerships with AWS, Azure, Google, Oracle, IBM Cloud & Alibaba Cloud. We have OEM partnerships with Dell, HPE, Lenovo, Rackspace, Deloitte, Accenture, Wipro, Cognizant, Atos, Cloudian, Fortanix, Caveonix & Veeam. Our VMware Cloud Partner program has 4000+ partners for customers to choose from.

265. What alliances/awards does the vendor have?

We have strong strategic alliances with CSPs (Microsoft Azure, AWS, GCP, Oracle), Dell, and other VMware Cloud Provider Partners (VCPP) such as Rackspace, ATOS etc. We have joint offerings with the hyperscalers and VMware Tanzu is also available through public cloud marketplaces.

266. How does the vendor leverage partnerships to drive differentiated work in this market?

We have several differentiated offerings with our partners. a) We introduced Azure Spring Apps Enterprise which is jointly developed, promoted & sold in collaboration with Microsoft. b) With Dell, we introduced Tanzu on VxRail, a curated hyperconverged infrastructure foundation for containerized apps. c) With our VCPP partners such as Swisscom - we have industry

specific solutions. d) With the VMware Technology Alliance Program we offer hundreds of curated vendor-supported, VMware tested/validated integrations & community contributed content: ~65 validated Tanzu Application Service integrations; ~25 validated Tanzu Kubernetes Grid integrations; 180+ Helm Charts & Containers with 1B+ downloads.

Section 15: Geographic Strategy

267. In what regions of the world are your container management products/services offered?

- North America
- Western Europe
- Eastern Europe
- Middle East
- Africa
- Asia/Pacific (excluding China)
- Latin America

Customers can consume Tanzu Services worldwide, in any region or geography, except where regulatory requirements may require localized regions. This applies to our SaaS based solutions

Please reference this link for coverage: https://www.vmware.com/global-infrastructure.html

268. What type of support is offered for your container management products/services in each one of these regions?

North America 24x7 Support

Western Europe 24x7 Support

Eastern Europe 24x7 Support

Middle East 24x7 Support

Africa 24x7 Support

Asia/Pacific (excluding China) 24x7 Support

Latin America 24x7 Support

269. Do you offer local language support?

Yes, we offer local language support in some regions in which we offer support

Technical support in local language is available for the following countries on a limited set of VMware products: France (French), Germany (German), Poland (Polish), Latin America (Spanish), Saudi Arabia (Arabic), United Arab Emirates (Arabic), Turkey (Turkish), Japan (Japanese), and China (Chinese).

Note: Local Language support is not available for Basic Support Entitlement users.

Commercial support for both Tanzu for Kubernetes Operations and Tanzu Application Platform solutions is provided in English, Japanese, and Chinese.

VMware product documentation website has navigation that is localized using regional browser settings. The products are not localized into multiple languages.

270. Please identify the top 10 certified MSP partners that support your container management products/services for each region.

	Certified MSP Partners
North America	Capstone IT, CDI, TeraSky, Rackspace, Lumen, Infinite Ranges
Western Europe	TietoEvery, OVH, Telecom Italia, Swisscom, CGI Sweden, Aruba, ATEA, SVA, evoila, ITQ, Xtravirt, TeraSky, Tieto
Eastern Europe	
Middle East	TeraSky, TurkCell, DU
Africa	
China	
Asia/Pacific (excluding China)	CloudHM, IIJ, AVM Cloud, AIS, AU cloud and Datacom
Latin America	AmericaMovil
Other; please use the additional info box to specify