

# Tanzu Mission Control

**KUBERNETES A ÚSKALÍ JEHO PROVOZU V PRAXI**

12.4.2023

**Jan Cipra & Ondřej Palkovský**



# Tanzu Mission Control

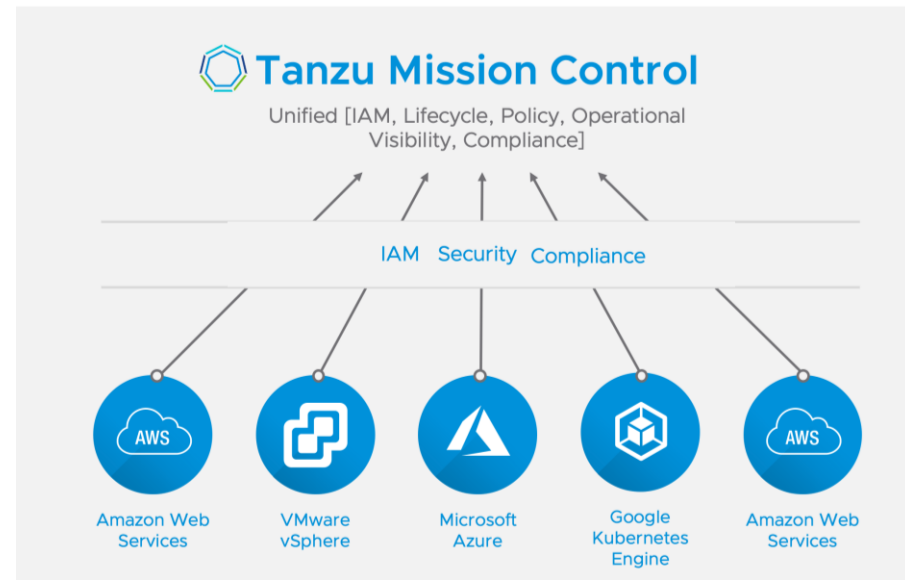


## Management portál pro správu Kubernetes clusterů

- SaaS služba (oznámena byla i on-premise varianta)
- TANZU Kubernetes Grid, AWS EKS, Azure, Google ...

## V přehledném webovém rozhraní umožňuje správu Kubernetes infrastruktury

- Lifecycle management
- Operations
- Access management
- Policy management
- Observability
- Inspection, conformance



# Lifecycle management



## LM operace nad Tanzu Kubernetes Grid clustery a AWS EKS

- Create
- Update
- Upgrade
- Delete

The screenshot displays the 'Create cluster' interface in the Tanzu Mission Control console. The left sidebar contains navigation options: Launchpad, Cluster groups, Clusters, Workspaces, Namespaces, Workloads, Catalog, Access, Policies, Inspections, Events, Administration, Automation center, and Audit logs. The main content area shows a five-step process:

- 1. Choose provisioner**: Choose your cluster's provisioner. The management cluster is 'gapp-test' and the provisioner is 'testns1'. A 'NEXT' button is visible.
- 2. Name and assign**: Choose your cluster's name and assign it to a cluster group.
- 3. Configure**: Select your kubernetes version, network and storage options.
- 4. Select control plane**: Choose between a single node or highly available control plane.
- 5. Edit and add node pools**: Customize and optionally add more node pools.

At the bottom of the main content area, there is a 'CREATE CLUSTER' button.



- **Přehled o jednotlivých clusterech**
  - Zdraví jednotlivých komponent
  - Základní přehled o využití zdrojů
  - Úprava konfigurace clusteru konfigurace clusteru
  - Konfigurace integrací – Observability a Service Mesh
- **Data protection**
  - Zálohování clusterů pomocí Velero

The screenshot displays the 'test2' cluster overview in the Tanzu Kubernetes Grid console. The cluster is in a 'Healthy' state, last updated 6 minutes ago. The overview includes a navigation menu, a metadata table, and several health and resource usage panels.

Cluster group	gapp	Provider	vSphere	Node count	3	Pod CIDR	10.51.0.0/20
Management cluster	gapp-test	Type	Tanzu Kubernetes Grid Service	Total memory	19.60 GB	Service CIDR	10.50.0.0/20
Provisioner	testns1	Kubernetes version	v1.23.8+vmware.3-tkg.1	Total cores	6 CPUs	Created	Tuesday, April 11, 2023, 09:38pm

**Requested/Allocatable CPU:** 93% (5.55 CPUs / 6 CPUs)

**Requested/Allocatable memory:** 28% (5.41 GB / 19.60 GB)

**Component health:** controller-manager, etcd-0, kube-apiserver, scheduler (all healthy)

**Worker nodes:** 2 nodes healthy

**Agent and extensions health:** agent-updater, cluster-auth-pinniped, cluster-config, cluster-health-extension, cluster-secret, data-protection, extension-manager, extension-updater, gatekeeper-operator, helm-deployment, inspection, intent-agent, package-deployment, policy-insight-extension, policy-sync-extension, sync-agent, tmc-observer, wavefront-extension (all healthy)

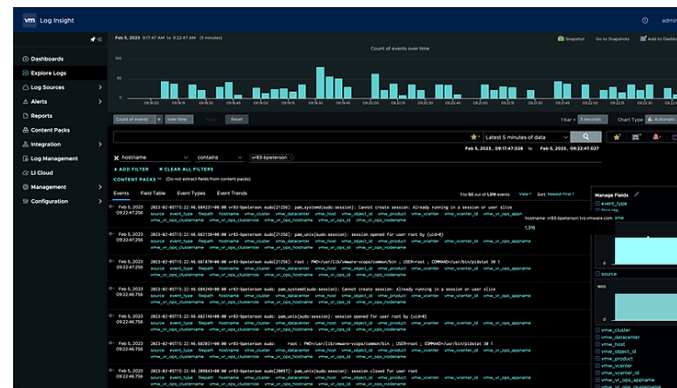
**Integrations:** Tanzu Observability (TMC Adapter: OK, Integration Workload: OK)



## Sběr a vizualizace metrik prostřednictvím integrace s VMware Aria Operations for Applications (Tanzu Observability)



## Sběr a vizualizace logů prostřednictvím VMware Aria Operations for Logs (vRealize Log Insight)



# Access management



- **Správa uživatelů a skupin**
  - Integrace na AD ...
- **RBAC přístup na jednotlivé zdroje**
  - Infrastructure view – Cluster, Cluster groups
  - Application view – Namespace, Workspace
- **Předdefinované a Custom role**

Role	organization	cluster group / cluster / workspace	namespace	Notes
<code>.admin</code>	x	x	x	Grants full root-level access to the object, including permission to see and edit access policies.
<code>.edit</code>	x	x	x	Grants permission to view the object, and create and delete child objects.
<code>.view</code>	x	x	x	Grants permission to see the object and its resources and child objects.
<code>.create</code>			x	Applicable only on the workspace, grants permission to create a namespace. Identities with this role are assigned the <code>.admin</code> role on the namespace that they create.
<code>.credential.admin</code>	x			Grants permission to create and edit credentials for data protection, connections to cloud provider accounts, and other features.
<code>.credential.view</code>	x			Grants permission to see and use credentials for data protection, connections to cloud provider accounts, and other features.



# Policy management a Inspection

## Policy management

- Access policy
- Image registry policy
- Network policy
- Quota policy
- Security policy
- Custom policy

The screenshot shows the 'Policies' management page in a Kubernetes dashboard. The 'Network' tab is active, displaying 'Network policies' for workspace 'app1'. It includes a sidebar with a workspace tree, a main panel with explanatory text and a 'Do not show this again' checkbox, and a section for 'Direct Network policies' with a form to create a new policy named 'custom-ingress'.

## Inspection

- Conformance
- CIS benchmark

The screenshot displays the 'CIS benchmark inspection' results for cluster 'rovmug'. The inspection was performed on March 02, 2023, at 08:43am. The results show 85 tests in total, with 75 succeeded, 8 warnings, and 2 failures. A specific failed test is highlighted: '1.1.12 Ensure that the etcd data directory ownership is set to etcd:etcd (Automated)'.

Cluster	rovmug		
Kubernetes version	v1.23.8+vmware.3		
Nodes	3		
Started	Thursday, March 02, 2023, 08:43am		
85 Tests	75 Succeeded	8 Warning	2 Failed
<b>Failed tests</b>			
1.1.12 Ensure that the etcd data directory ownership is set to etcd:etcd (Automated)			



**Ukázka prostředí Tanzu  
Mission Control**

