Tanium Cloud Workloads User Guide

2026H2 Semiannual Release

Version 1.0

November 17, 2026



The information in this document is subject to change without notice. Further, the information provided in this document is provided "as is" and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium's customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Please visit https://help.tanium.com for the most current Tanium product documentation.

This documentation may provide access to or information about content, products (including hardware and software), and servicesprovided by third parties ("Third Party Items"). With respect to such Third Party Items, Tanium Inc. and its affiliates (i) are not responsible for such items, and expressly disclaim all warranties and liability of any kind related to such Third Party Items and (ii) will not be responsible for any loss, costs, or damages incurred due to your access to or use of such Third Party Items unless expressly set forth otherwise in an applicable agreement between you and Tanium.

Further, this documentation does not require or contemplate the use of or combination with Tanium products with any particular Third Party Items and neither Tanium nor its affiliates shall have any responsibility for any infringement of intellectual property rights caused by any such combination. You, and not Tanium, are responsible for determining that any combination of Third Party Items with Tanium products is appropriate and will not cause infringement of any third party intellectual property rights.

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S.Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years. We certify against the WCAG 2.2 / VPAT 2.5 standards for all major product modules. Tanium performs ongoing reassessments as appropriate, given the scope and type of changes to the UI and product features from release to release. In the most recent testing, the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.2 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

As new products and features are continuously delivered, Tanium will conduct testing to identify potential gaps in compliance with accessibility guidelines. Tanium is committed to making commercially reasonable efforts to address any gaps as quickly as is feasible, given the severity of the issue and scope of the changes. Tanium factors these objectives into the ongoing delivery schedule of features and releases with our existing resources.

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are

©2026 Tanium Inc. All Rights Reserved

committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, Tanium Support atsupport@tanium.com, or email accessibility@tanium.com to make further inquiries.

Tanium is a trademark of Tanium, Inc. in the U.S. and other countries. Third-party trademarks mentioned are the property of the irrespective owners.

Kubernetes®, K8s®, and the Kubernetes logo are registered trademarks of The Linux Foundation®.

Android, ChromeOS, and Google are trademarks of Google LLC.

iOS, iPad, iPadOS, iPhone, Mac, and macOS are trademarks of Apple Inc., and registered in the U.S. and other countries and regions.

Patents: https://www.tanium.com/patents

Tanium Open Source Disclosure : https://tanium.github.io/opensource/

© 2026 Tanium Inc. All rights reserved.

Table of contents

Overview 6
- Sensors and packages with clusters 7
- Interoperability with other Tanium products 8

Requirements 10
- Core platform dependencies 10
- Computer group dependencies 10
- Solution dependencies 10
  - Tanium recommended installation 11
  - Import specific solutions 11
  - Required dependencies 11
  - Feature-specific dependencies 11
- Resource requirements 11
- Third-party software 12
- User role requirements 12

Installing 16
- Before you begin 16
- Import Cloud Workloads 16

Configuring 18
- Configure satellites 18
  - Supported operating systems for Cloud Workloads satellites 18
  - Hardware requirements for Cloud Workloads satellites 18
- Add registries 19
- (Optional) Update the Registry Refresh frequency 21
- Set up Cloud Workloads users 21

Deploying to clusters 23
- (Optional) Upload images to a private registry 23
- Generate the deployment files 25

©2026 Tanium Inc. All Rights Reserved

Deploy the clients 27
Verify the deployment 28
Check the client status in Tanium Client Management 28
Ask a question in Tanium Interact 29
Upgrade client images 29

Reference: Cloud Workloads sensors 31

Reference: Adding a Google Artifact Registry 35
Add a Google Artifact Registry 35
Service account key fields 37

©2026 Tanium Inc. All Rights Reserved

Cloud Workloads overview

With Cloud Workloads, you can manage Kubernetes clusters alongside other Tanium-managed endpoints.

Architecture

To manage clusters, deploy the following client images to the clusters:

Tanium Cluster Client Container

The Tanium Cluster Client Container (T3C) is a containerized version of the Tanium Client that includes all of the necessary utilities and extensions needed by Cloud Workloads.

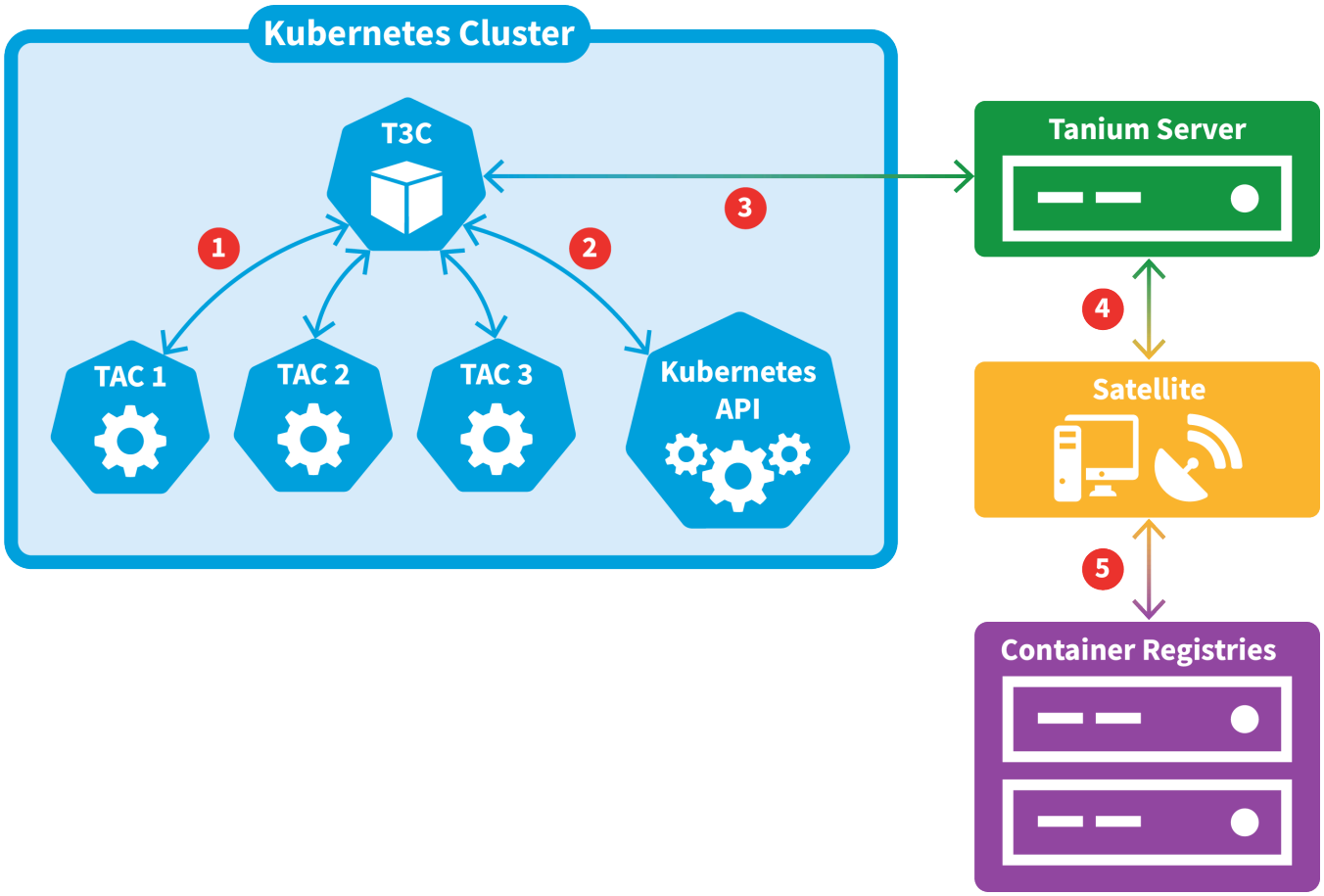
Tanium Admission Controller

The Tanium Admission Controller (TAC) is a high-availability deployment with multiple replicas that monitors cluster lifecycle events and evaluates what actions might be necessary based on enforced policies, such as denying the creation of a resource.

For more information about how to deploy the images, see Deploying to clusters on page 23.

Figure 1. Cloud Workloads architecture

©2026 Tanium Inc. All Rights Reserved



1	The Tanium Cluster Client Container (T3C) sends configuration details to the Tanium Admission Controller (TAC), and the TAC sends details about admission events to the T3C.
2	The T3C communicates with the Kubernetes (K8s) API for pod visibility.
3	The T3C communicates with the Tanium Server to receive configuration details, answer sensors, and report admission events.
4	If Cloud Workloads is configured to scan registries and create Software Bill of Materials (SBOMs), the satellite receives configuration information from the Tanium Server .
5	If Cloud Workloads is configured to scan registries and create SBOMs, the satellite scans the registries configured in Cloud Workloads to create SBOMs, and then sends those SBOMs to the Tanium Server .

Sensors and packages with clusters

Adhere to the following guidelines for sensors and packages that are related to clusters.

©2026 Tanium Inc. All Rights Reserved

Sensors

Use sensors in the Cloud Workloads content set when asking questions to retrieve data from clusters.

> **Note:** Some Tanium-provided sensors are not optimized for use with clusters. Therefore, the results returned might be partially complete or, if required tools are not installed on managed clusters, a sensor might not return results for a cluster.

Packages

Exclude clusters from targeting when you deploy actions that use binary files or scripts that cannot run on clusters. One way to identify clusters to exclude from targeting is by using the **Kubernetes - Is Kubernetes Cluster** sensor. For example, you can ask the following question to get all endpoints that are not part of a cluster:

```
Get Computer Name from all machines with Kubernetes - Is Kubernetes Cluster contains false
```

Interoperability with other Tanium products

Cloud Workloads works with other Tanium products to provide additional features and reporting of related data.

Asset

Use Cloud Workloads with Asset to view managed and unmanaged Kubernetes clusters in your environment. For more information, see Asset User Guide: Viewing containers.

> **Important:** If you add Asset attributes or create views with sensors that apply to Kubernetes clusters, the results include data from Tanium-managed clusters only.

Comply

Use Cloud Workloads with Comply to scan image Software Bill of Materials (SBOMs) in configured

©2026 Tanium Inc. All Rights Reserved

registries for vulnerabilities.

For more information, see Comply User Guide: Create a container registry scan assessment.

Enforce

Use Cloud Workloads with Enforce to apply policies on Tanium-managed clusters. You can configure and enforce these policy types:

- Allow External Services by IP: Define IP addresses that are allowed in external service resources.
- Allow Images by Registry: Define image registries that are allowed.
- Allow Ingress Actions by Hostname: Define hostnames that are allowed in ingress resources.
- Block Images by Registry: Define image registries that are not allowed.
- Block Images by Tag: Define image tags that are not allowed.
- Block Resources by Version: Define Kubernetes resource API versions that are not allowed.
- Block Rogue Containers: Block all images that are not from a trusted registry.
- Custom OPA: Define a custom OPA policy using the Rego query language.

For more information, see Enforce User Guide: Creating policies for Kubernetes clusters.

Reporting

The **Cloud Workloads Overview** page uses charts to visualize data that are provided by Tanium™ Reporting. For more information, see Reporting User Guide: Working with a single endpoint.

©2026 Tanium Inc. All Rights Reserved

Cloud Workloads requirements

Review the requirements before you install and use Cloud Workloads.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Cloud Workloads. For more information about how to get Cloud Workloads, see Tanium Solutions & Bundles.

  > **Note:** Each node counts toward your licensed seat total.

- Tanium Core Platform server

Computer group dependencies

When you first sign in to Tanium Console, the server automatically imports the `All Kubernetes Clusters` computer group, which Cloud Workloads requires.

Solution dependencies

Other Tanium solutions are required for Cloud Workloads to function (required dependencies) or for specific Cloud Workloads features to work (feature-specific dependencies). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.

> **Note:** Some Cloud Workloads dependencies have their own dependencies, which you can see in the lists of required and feature-specific dependencies below. Where a dependency links to its own user guide, that link opens the guide for the latest version of the solution, not necessarily the minimum version that Cloud Workloads requires.

©2026 Tanium Inc. All Rights Reserved

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Cloud Workloads, the Tanium Server automatically imports all your licensed solutions at the same time. For more information, see Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Cloud Workloads to import, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are earlier than the minimum required for Cloud Workloads, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Cloud Workloads has the following required dependencies:

- Tanium™ Direct Connect
- Tanium™ RDB Service
- Tanium™ Reporting
- Tanium™ Secrets Service

Feature-specific dependencies

If you select only Cloud Workloads to import, you must manually import or update its feature-specific dependencies regardless of Tanium Console or Tanium Core Platform versions. Cloud Workloads has the following feature-specific dependencies:

- Tanium Enforce is required to create and enforce cluster policies.
- Tanium Asset is required to view managed and unmanaged clusters.
- Tanium Comply is required to scan image SBOMs in configured registries for vulnerabilities.

Resource requirements

©2026 Tanium Inc. All Rights Reserved

The resource requirements for the Tanium Admission Controller (TAC) and Tanium Cluster Client Container (T3C) are the same as the Tanium Client. For more information, see Tanium Client Management User Guide: Hardware requirements.

The Kubernetes administrator must specify a default `StorageClass` to dynamically provision persistent volumes (PVs) for Tanium-managed clusters. For more information, see Kubernetes documentation: Dynamic Volume Provisioning - Defaulting Behavior.

Third-party software

Cloud Workloads supports container orchestrator versions in on-premises and cloud environments that are built on the Kubernetes platform version 1.26 and later, such as:

- Red Hat OpenShift 4.13 and later
- Kubernetes 1.26 and later

Cloud Workloads supports the following registry providers:

- Artifactory Container Registry
- AWS Elastic Container Registry (ECR)
- Azure Container Registry
- Docker Hub
- Google Artifact Registry

User role requirements

Predefined roles grant the following permissions, which are required to use Cloud Workloads functionality:

- Table 1. Cloud Workloads solution permissions on page 13
- Cloud Workloads administration, platform content, and global permissions on page 14: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Cloud Workloads users on page 21.

©2026 Tanium Inc. All Rights Reserved

Some Cloud Workloads solution permissions provide permissions that are associated with other solutions. Furthermore, all the platform content permissions and some solution permissions apply to content sets that might contain content for other solutions in addition to Cloud Workloads. If you create custom roles for Cloud Workloads users, be sure to assign all the solution permissions and content set permissions that are required for Cloud Workloads functionality. If you are not sure which permissions are required for a custom role, view the permissions of the predefined roles. For more information, see the following sections of the Tanium Console User Guide:

- RBAC overview (provides an overview of roles, permissions, and content sets)
- Provided role permissions
- View effective role permissions
- Configure a custom role



Note: Do not assign the **Cloud Workloads Service Account** and **Cloud Workloads Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

Cloud Workloads solution permissions

Permission	Cloud Workloads Operator	Cloud Workloads Read Only
Cloud Workloads View the Cloud Workloads workbench	✓ SHOW	✓ SHOW
Cloud Workloads Clusters READ: View managed clusters WRITE: Add clusters to Cloud Workloads	✓ READ WRITE	✓ READ
Cloud Workloads Deployment WRITE: Generate YAML files and Helm charts	✓ WRITE	✗
Cloud Workloads Image History READ: View image run histories	✓ READ	✗
Cloud Workloads Registries READ: View configured registries in Cloud Workloads	✓ READ	✓ READ

©2026 Tanium Inc. All Rights Reserved

Permission	Cloud Workloads Operator	Cloud Workloads Read Only
WRITE: Add, edit, and delete registries in Cloud Workloads	WRITE	
Cloud Workloads Reports READ: View Cloud Workloads reports	✓ READ	✓ READ
Cloud Workloads Sbom READ: View cluster SBOMs	✓ READ	✓ READ
Cloud Workloads Settings READ: View Cloud Workloads settings WRITE: Update Cloud Workloads settings	✓ READ WRITE	✓ READ

The permissions for these roles provide solution permissions for other solutions. To view the provided permissions, see Tanium Console User Guide: View effective role permissions .

Cloud Workloads administration and platform content permissions

Permission	Permission Type	Cloud Workloads Operator	Cloud Workloads Read Only
Action Group	Administration	✓ READ	✓ READ
Action	Platform Content	✓ READ WRITE	✗
Filter Group	Platform Content	✓ READ	✓ READ
Own Action	Platform Content	✓ READ	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Permission Type	Cloud Workloads Operator	Cloud Workloads Read Only
Package	Platform Content	✓ READ	✗
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	Platform Content	✓ READ	✗
Sensor	Platform Content	✓ READ	✓ READ

To view the content sets to which the platform content permissions apply, see View effective role permissions .

©2026 Tanium Inc. All Rights Reserved

Installing Cloud Workloads

About this task

Use the Tanium Console **Solutions** page to install Cloud Workloads.

Before you begin

- Read the release notes.
- Review the Cloud Workloads requirements on page 10.
- Assign the correct roles to users for Cloud Workloads. Review the User role requirements on page 12.
    - To import the Cloud Workloads solution, you must be assigned the Administrator reserved role.

Import Cloud Workloads

About this task

Perform the following steps to install the Cloud Workloads solution on the Tanium Server.

> **Note:** If you have multiple Tanium Servers in an active-active configuration, you only need to perform these steps on one Tanium Server.

1. Sign in to Tanium Console with an account that has the **Administrator** reserved role.
2. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.
3. In the **Content** section, select the checkbox for Cloud Workloads and click **Import**.

©2026 Tanium Inc. All Rights Reserved

Tip: If you need to install any prerequisite Tanium solutions or content, select the corresponding checkboxes for those solutions as well.

4. Review the content to import and click **Begin Import**.

Result

Other Tanium solutions are required for Cloud Workloads to function (required dependencies) or for specific Cloud Workloads features to work (feature-specific dependencies).

©2026 Tanium Inc. All Rights Reserved

Configuring Cloud Workloads

If you did not install Cloud Workloads with the **Apply All Tanium recommended configurations** option, you must enable and configure certain features.

If you specify an action group other than `All Computers`, ensure that the action group includes any satellites you plan to use, and if monitoring non-cluster containers, any of their host addresses.

Configure satellites

Cloud Workloads uses satellites to scan image registries and create Software Bill of Materials (SBOMs). Satellites are specific Tanium Clients that you designate to run certain targeted, secure workloads on behalf of the Tanium Module Server.

If you want to scan image registries and create SBOMs, you must configure at least one satellite in Direct Connect before you add a registry. For more information, see Tanium Direct Connect User Guide: Create satellites.

Supported operating systems for Cloud Workloads satellites

- AlmaLinux 8.x or later
- CentOS 7.x, 8.x
- Debian 10.x or later
- Oracle Linux 7.x or later
- Red Hat Enterprise Linux 7.x or later
- Rocky Linux 8.x or later
- Ubuntu 20.04 or later

Hardware requirements for Cloud Workloads satellites

©2026 Tanium Inc. All Rights Reserved

For best results, ensure that satellites meet the following minimum hardware requirements:

- CPU cores: 4
- RAM: 8 GB
- Free disk space: 500 MB (in addition to disk space required for the Tanium Client and any modules in use)
- Network bandwidth: 10 Mbps between the Module ServerTanium Cloud and the satellite, and between the satellite and targeted endpoints

Both the x64 and x86 architectures are supported.

Note: The satellites that you use for Cloud Workloads must have visibility, or "line of sight", to internal network resources. Do not use a legacy Tanium Client Container (TCC), Tanium Cluster Client Container (T3C), or Tanium Admission Controller (TAC) instance for this purpose.

Add registries

About this task

Add registries to a trusted registries list and configure whether to scan for images and create SBOMs.

1. From the Main menu, go to **Shared Services** > **Cloud Workloads**.
2. Click Settings and then click **Add Registry**.

   Tip: You can also click **Add Registry** in the **Quick Links** section on the Cloud Workloads **Overview** page.
3. Configure the following settings:
   - **Name**: The registry name to display in the user interface.
   - **Provider**: The registry provider.

©2026 Tanium Inc. All Rights Reserved

> **Note:** Use **Other** to add unsupported providers to the list of trusted registries and to prevent images from these registries being marked as rogue. These registries are not used in inventory scanning and SBOM creation.

- **Address**: The registry address.
- (Optional) **Description**: The registry description.
- (Optional) **Enable image registry scanning and SBOM generation**: Select this option if you want to scan the registry for images and create SBOMs. Do not select this option if you only want to add this registry to the list of trusted registries for rogue image detection. If selected, you must provide the following details:

    a. In the **Connection Details** section, provide the registry connection details, such as Key ID and Key Secret.

    Refer to the documentation for your registry provider for more information about the connection details. For more information, see Third-party software on page 12. If you are using Google Artifact Registry, see Reference: Adding a Google Artifact Registry on page 35.

    b. In the **Satellites** section, select the satellites to use when scanning this registry.

    > **Note:**
    > - This **Enable image registry scanning** option is not available if Asset and Comply are not installed, or when you select **Other** as the provider type.
    > - Select more than one satellite to distribute the work and improve scanning performance.
    > - For more information about satellites, see Tanium Direct Connect User Guide: Managing satellites.

4. Click **Save**.

©2026 Tanium Inc. All Rights Reserved

(Optional) Update the Registry Refresh frequency

About this task

The registry refresh frequency determines how often inventory scans are initiated on connected registries. The default refresh frequency is 1 hour, which means that registries are scanned every hour to check for new images. If a scan is not complete before the next scan starts, the next scan begins when the running scan ends. When new images are identified, they are queued for SBOM creation, and the satellite endpoint processes the queue and generates SBOMs.

1. From the Main menu, go to **Shared Services** > **Cloud Workloads**.
2. Click Settings.
3. In the **Registry Refresh** section, click Edit and update the refresh frequency. Click **Save**.

Set up Cloud Workloads users

You can use the following set of predefined user roles to set up Cloud Workloads users.

Cloud Workloads Operator

Assign the **Cloud Workloads Operator** role to users who manage the configuration and deployment of Cloud Workloads functionality to endpoints. This role can perform the following tasks:

- Configure Cloud Workloads service settings.
- View and modify Cloud Workloads configurations.
- Dismiss or reject approvals for Cloud Workloads tasks in Tanium Endpoint Configuration.
- Add, edit, and delete registries in Cloud Workloads.
- Add clusters to Cloud Workloads.
- Generate YAML files and Helm charts.
- View image run histories.
- View reports.

©2026 Tanium Inc. All Rights Reserved

- View cluster SBOMs.

Cloud Workloads Read Only

Assign the **Cloud Workloads Read Only** role to users who need visibility into Cloud Workloads data. This role can perform the following tasks:

- View Cloud Workloads service settings.
- View clusters in Cloud Workloads.
- View image run histories.
- View reports.
- View cluster SBOMs.

For more information about specific permissions for each role, see User role requirements on page 12.

For more information about assigning user roles, see Tanium Console User Guide: Manage role assignments for a user.

©2026 Tanium Inc. All Rights Reserved

Deploying to clusters

Before you begin

For clusters managed using the legacy Tanium Client Container, uninstall the legacy Tanium Client Container from the cluster.

About this task

To deploy the Tanium Admission Controller (TAC) and the Tanium Cluster Client Container (T3C) images to your cluster, you need to generate and use a deployment YAML file or Helm chart. The deployment configures the following setup in your cluster:

- A pod that runs the Tanium Admission Controller with attached, persistent storage
- A pod that runs the Tanium Cluster Client Container with attached, persistent storage



Note:

- The Tanium Admission Controller and Tanium Cluster Client Container do not require privileged containers or `root` access.
- You can use a Helm chart instead of a YAML file to deploy these clients if you need to pre-populate fields within the configuration file.
- The Tanium deployment requests a `PersistentVolumeClaim` using the default `StorageClass`. If the cluster does not have a default `StorageClass`, the deployment fails. For more information, see Kubernetes documentation: Dynamic Volume Provisioning - Defaulting Behavior and Kubernetes documentation: Change the default StorageClass.

(Optional) Upload images to a private registry

The Tanium public registry hosts images for the TAC and T3C. If you do not want to use the Tanium

©2026 Tanium Inc. All Rights Reserved

public registry as the source location for deployment, upload the TAC and T3C images to a private registry. The following examples provide guidance on how to add the images to a private registry by creating images or pushing Helm charts.

Create images

Before you upload the images, generate the deployment files so that you know which image versions to upload. The deployment YAML file and Helm chart reference specific image versions, and those versions must exist in your private registry. For more information, see Generate the deployment files on page 25.

Record the Tanium Cluster Client Container (T3C) and Tanium Admission Controller (TAC) image versions from the generated file. In a YAML file, the versions appear in the `image` fields. In a Helm command, they appear as the `t3cImageTag` and `tacImageTag` values.

One way to upload images to your private registry is to use the docker buildx imagetools command with the following sources:

- taniumcontainers.azurecr.io/t3c
- taniumcontainers.azurecr.io/tac

For example, in the Docker CLI, run the following commands. Replace `<t3c_version>` and `<tac_version>` with the versions that you recorded.

```
$ docker buildx imagetools create --tag <your_private_registry>/t3c:<t3c_version>
taniumcontainers.azurecr.io/t3c:<t3c_version>
$ docker buildx imagetools create --tag <your_private_registry>/tac:<tac_version>
taniumcontainers.azurecr.io/tac:<tac_version>
```

Important:

Include the version tag on both the source and the destination. If you omit the tag, Docker uses the `latest` tag, and the images in your private registry do not match the versions that the deployment files reference. The deployment then fails with an `ImagePullBackOff` error.

You can use a more recent version of the images than the generated deployment files reference. To see the available versions, list the tags in the Tanium public registry with a registry client such as

©2026 Tanium Inc. All Rights Reserved

skopeo list-tags or crane ls. If you upload a different version, update the `t3cImageTag` and `tacImageTag` values in your Helm command, or the `image` fields in your YAML file, to match the version that you uploaded.

For more information about these Docker commands, see Docker Documentation: docker buildx imagetools create.

Push Helm charts

One way to create Helm charts for your private registry is to use the Helm pull and push commands. You can pull from the following repository:

- oci://taniumcontainers.azurecr.io/helm

For example, in the Helm CLI, run the following commands:

```
helm pull oci://taniumcontainers.azurecr.io/helm/tanium-cluster-manager
helm push tanium-cluster-manager.tgz oci://<your_private_registry>/helm
```

For more information about these Helm commands, see Helm Documentation: Helm Pull and Helm Documentation: Helm Push.

> **Note:**
>
> The Helm command that **Cloud Workloads** generates always references the Tanium public registry as the chart source. If you push the chart to your private registry, edit the generated command to replace oci://taniumcontainers.azurecr.io/helm/tanium-cluster-manager with your own repository. If your cluster cannot reach the Tanium public registry, the generated command fails until you make this change.

Next steps

Add the private registry to Cloud Workloads. For more information, see Add registries on page 19.

Generate the deployment files

About this task

©2026 Tanium Inc. All Rights Reserved

From Cloud Workloads, generate a YAML file or Helm chart that you can use to deploy the Tanium Admission Controller and Tanium Cluster Client Container to your clusters.

1. From the Main menu, go to **Shared Services** > **Cloud Workloads**.
2. From the **Quick Links** section of the **Cloud Workloads Overview** page, click **Add Cluster**.
3. In the **Provider** list, select the target cluster provider.
4. In the **T3C Source** list, select the registry from which you want to pull the image for the Tanium Cluster Client Container.

   Tip: To pull the image from Tanium's registry, select **Tanium Public Registry**. For more information about pulling the image from a private registry that is not on the list, see Add registries on page 19.
5. In the **TAC Source** list, select the registry from which you want to pull the image for the Tanium Admission Controller.

   Tip: To pull the image from Tanium's registry, select **Tanium Public Registry**. For more information about pulling the image from a private registry that is not on the list, see Add registries on page 19.
6. (Optional) In the **Proxy Server List** field, specify one or more URLs for the clients to use to connect to the Tanium Server. These URLs must be accessible from the cluster on which you deploy these images.

   Important:
   If the cluster connects to the Tanium Server through a Zone Server, use the Zone Server URLs.
7. In the **Cluster Name** field, enter a name that adheres to the following requirements:
   - This name must be a valid computer name that is 63 characters or less and contain only lowercase letters, numbers, and hyphens. The name cannot start or end with a hyphen.
   - This name must also conform to the naming requirements for your orchestrator. Consult the documentation for your orchestrator for details. For more information about Kubernetes requirements, see Kubernetes Documentation: Object Names and

©2026 Tanium Inc. All Rights Reserved

IDs.

8. Record the cluster name for future reference. When upgrading images, you need to use the same name when you create a new YAML file or Helm chart.
9. (Optional) In the **Cluster Labels** field, add labels to identify this cluster. You can use these labels for targeting and for sorting on results pages. Ensure that the labels adhere to the following requirements:
    - These labels must be 63 characters or less and contain only letters, numbers, hyphens, underscores, and periods. Labels must begin and end with a letter or number.
    - These labels must also conform to the naming requirements for your orchestrator. Consult the documentation for your orchestrator for details. For more information about Kubernetes requirements, see Kubernetes Documentation: Labels and Selectors - Syntax and character set.
10. Record the cluster labels for future reference. When upgrading, you need to use the same labels when you create a new YAML file or Helm chart.
11. Click **Generate**.
12. Download the YAML file or copy the Helm chart:
    a. To install or upgrade the clients by using a YAML file, click **Download YAML File**.
    b. To install the clients by using a Helm chart, click **Copy** in the **Install Command Line** section.
    c. To upgrade the clients by using a Helm chart, click **Copy** in the **Upgrade Command Line** section.

Deploy the clients

About this task

Use the YAML file or the Helm chart that you generated in the previous task to deploy the clients to a cluster. The steps vary based on the orchestration platform that you are using in your environment. Consult the documentation for your platform for the specific steps. The following steps provide an example of using a YAML file for a Kubernetes environment. Adjust your commands to match your environment and configuration file.

©2026 Tanium Inc. All Rights Reserved

Important: The Tanium deployment requests a `PersistentVolumeClaim` using the default `StorageClass`. If the cluster does not have a default `StorageClass`, the deployment fails. For more information, see Kubernetes documentation: Dynamic Volume Provisioning - Defaulting Behavior and Kubernetes documentation: Change the default StorageClass.

1. Copy the YAML file to your Kubernetes environment.
2. In your Kubernetes environment, open a command prompt and run the following command:
   `kubectl apply -f <relative_path_to_YAML_file>`
   Install the Kubernetes command line tool (`kubectl`) if it is not installed. For more information, see Kubernetes: Install Tools. For more information about the `apply` command, see Kubernetes: kubectl reference.

   Note: If you created your own YAML files or Helm charts and are presented with the End-User License Agreement (EULA) prompt when you install the clients, ensure that you accept the EULA. If you do not accept, the clients cannot start. YAML files and Helm charts generated from the Tanium Console implicitly accept the EULA by default.

Verify the deployment

To confirm that the clients were installed successfully, you can either check the client status or ask a question.

Check the client status in Tanium Client Management

1. From the Main menu of your Tanium Server, go to **Administration** > **Configuration** > **Client Status**.
2. Confirm that the cluster appears in the list. The cluster might take up to 5 minutes to appear in the list.

©2026 Tanium Inc. All Rights Reserved

Note:

For Cloud Workloads, Kubernetes nodes are not reflected on the **Client Status** page or in the Total endpoints count on the **Home** page. To find the count of managed Kubernetes nodes, complete the following steps:

a. Ask the following question in Tanium Interact:

```
Get Kubernetes - Cluster Node Info from all machines with
Kubernetes - Cluster Node Info:Node Internal IP matches
"^[1-9].*"
```

b. In the results grid, select the **Cached** view.

Ask a question in Tanium Interact

In Tanium Interact, ask one of the following questions and confirm that the cluster appears in the results:

- `Get Kubernetes - Cluster Name from all machines`

  Note: Endpoints that are not in a cluster return `N/A on <operating_system>`.

- `Get Computer Name from all machines with Kubernetes - Is Kubernetes Cluster contains "True"`

Upgrade client images

About this task

To upgrade the Tanium Admission Controller and Tanium Cluster Client Container images, generate a new deployment YAML file or Helm chart with the same **Cluster Name** and **Cluster Labels** as the original installation and deploy it to the cluster. For more information, see Generate the deployment files on page 25 and Deploy the clients on page 27. If you use a private registry, complete the following steps in order.

1. Generate the new deployment YAML file or Helm chart command line.

©2026 Tanium Inc. All Rights Reserved

2. Record the T3C and TAC image versions from the generated file.
3. Upload those image versions to your private registry. For more information, see (Optional) Upload images to a private registry on page 23.
4. If you use a Helm chart, replace the chart repository in the generated command with your own repository.
5. Deploy the generated file to the cluster.

Result

If you deploy before you upload the new image versions, the cluster cannot pull the images and the pods fail with an `ImagePullBackOff` error.

Next steps

- Use Enforce to enforce policies on your clusters. For more information, see Enforce User Guide: Creating policies for Kubernetes clusters.
- Use Comply to scan registries for vulnerabilities. For more information, see Comply User Guide: Create a container registry scan assessment.
- Use Asset to view managed and unmanaged clusters. For more information, see Asset User Guide: Viewing containers.

©2026 Tanium Inc. All Rights Reserved

Reference: Cloud Workloads sensors

Use the sensors provided by the Cloud Workloads solution to retrieve information from managed clusters.

Cloud Workloads sensors

Sensor	Description
Image Registry Status	Returns the status of the satellites designated for image scanning.
Is Kubernetes Node	Returns whether the endpoint is a Kubernetes node.
Kubernetes - Cluster Labels	Returns Tanium labels that are assigned to the Kubernetes cluster.
Kubernetes - Cluster Name	Returns the name that is assigned to the Kubernetes cluster.
Kubernetes - Cluster Node Info	Returns the following details about the nodes in the cluster: • Node Name • Node Internal IP • Labels • Pod Count • Container Runtime Version • Machine ID • Running Pod Count
Kubernetes - Container Details	Returns the following container details for Kubernetes pods: • Namespace • Pod name • Container ID • Image Hash • Image Name • Is Privileged • Is Rogue

©2026 Tanium Inc. All Rights Reserved

Sensor	Description
	• Image Tag • Image Registry
Kubernetes - Correlation ID	Returns the correlation ID assigned to the Kubernetes cluster.
Kubernetes - Is Kubernetes Cluster	Returns whether the endpoint is a Kubernetes cluster.
Kubernetes - Node Machine IDs	Returns the machine IDs of all nodes in the cluster.
Kubernetes - Number of Nodes [1]	Returns the count of the nodes reported by the Kubernetes cluster.
Kubernetes - Number of Running Pods	Returns the count of running pods in the Kubernetes cluster.
Kubernetes - Number of Running Pods with Rogue Containers	Returns the count of running pods with rogue containers in the Kubernetes cluster.
Kubernetes - Orchestrator Version	Returns the orchestrator version.
Kubernetes - Provider	Returns the cloud service provider name of the Kubernetes cluster.
Kubernetes - Server Version [1]	Returns the server version of the Kubernetes cluster.
Linux Machine ID	Returns the machine ID of a Linux host running systemd.
Pod Availability	Returns the pod availability in two columns, *Number of Available Pods* and *Number of Unavailable Pods*.
Pod Details	Returns the following pod details: • Namespace • Pod Name • Pod Annotations • Pod Labels • UID • Restart Policy • Phase • Is Control Plane Node

©2026 Tanium Inc. All Rights Reserved

Sensor	Description
	• Rogue Container ID For more information about pod details, see the Kubernetes documentation .
Pods Running inside Cluster	Returns the following information about the pods that are running inside a cluster. • Namespace • Pod Name • Containers Running Rogue Images
Running Container Data	Returns the following counts related to containers that are running: • Number of running containers • Number of Running Unprivileged Containers • Number of Running Privileged Containers • Number of Running Rogue Containers • Number of Containers Running Longer than Two Days • Number of Containers Running Longer than Five Days • Number of Containers Running Longer than Seven Days • Number of Containers Running Longer than Thirty Days • Number of Unprivileged Containers Running Longer than Two Days • Number of Unprivileged Containers Running Longer than Five Days • Number of Unprivileged Containers Running Longer than Seven Days • Number of Unprivileged Containers Running Longer than Thirty Days • Number of Privileged Containers Running Longer than Two Days • Number of Privileged Containers Running Longer than Five Days • Number of Privileged Containers Running Longer than Seven Days • Number of Privileged Containers Running Longer than Thirty Days
Running Container Details	Returns the following details from containers that are running: • Computer Name • Container ID • Image Hash • Image Name

©2026 Tanium Inc. All Rights Reserved

Sensor	Description
	• Is Privileged • Is Rogue • Image Tag • Image Registry
Running Instances of Image [1]	Returns the running instances of the image that matches the specified parameters.

[1] This sensor is not registered with the Tanium Data Service by default. For more information about registering the sensor for data collection, see Register or unregister sensors for collection .

©2026 Tanium Inc. All Rights Reserved

Reference: Adding a Google Artifact Registry

Add a Google Artifact Registry to the trusted registries list and configure connection details for image scanning.

Before you begin

- Ensure that the service account has the `Artifact Registry Reader` role (`roles/artifactregistry.reader`) on the project that hosts the repository. This is the minimum role required to read images. If the service account is in a different project than the registry, you must grant this role explicitly in that project. For more information, see the Google Cloud documentation: Configure access control.
- Obtain a service account key JSON file from Google Cloud IAM. For more information, see the Google Cloud documentation: Create and delete service account keys.

> **Important:** Save the key file immediately after creation. The key file cannot be re-downloaded after it is created.

> **Best Practice:** Store the key file in a secure location and rotate it regularly.

Add a Google Artifact Registry

Add a Google Artifact Registry to the trusted registries list and configure connection details for image scanning.

1. From the Main menu, go to **Shared Services** > **Cloud Workloads**. Click Settings and then click **Add Registry**.

> **Tip:** You can also click **Add Registry** in the **Quick Links** section on the Cloud Workloads **Overview** page.

©2026 Tanium Inc. All Rights Reserved

2. Configure the following settings:
    - **Name**: The registry name to display in the user interface.
    - **Provider**: Select **Google Artifact Registry (GAR)**.
    - **Address**: The registry address in the format `LOCATION-docker.pkg.dev/PROJECT-ID/REPOSITORY`. For example `us-central1-docker.pkg.dev/my-project/my-repo`. For more information, see the Google Cloud documentation: Docker repository and image names.
    - (Optional) **Description**: The registry description.
    - (Optional) **Enable image registry scanning and SBOM generation**: Select this option to scan the registry for images and create SBOMs. If selected, you must provide the following details:

        a. In the **Connection Details** section, identify the Artifact Registry repository to scan:

            - **Project**: The Google Cloud project name that hosts the Artifact Registry repository.
            - **Location**: The region or multi-region where the repository is hosted, for example `us`, `us-central1`, or `europe-west1`. For a list of supported locations, see the Google Cloud documentation: Repository locations.
            - **Repository**: The name of the Artifact Registry repository to scan.

        Then provide the service account key details that Cloud Workloads uses to authenticate to Google Cloud. All service account key fields are required. Copy each value directly from the service account key JSON file that you downloaded from Google Cloud IAM. For field descriptions, see Service account key fields on page 37.

        b. In the **Satellites** section, select the satellites to use when scanning this registry.

©2026 Tanium Inc. All Rights Reserved

Note:

- Select more than one satellite to distribute the work and improve scanning performance.
- For more information about satellites, see Tanium Direct Connect User Guide: Managing satellites.

3. Click **Save**.

Service account key fields

The following fields correspond to properties in the service account key JSON file that you download from Google Cloud IAM.

Service account key fields

Field	Description
Type	The credential type. Corresponds to the `type` property in the key file. The value is typically `service_account`.
Project ID	The Google Cloud project ID. Corresponds to the `project_id` property in the key file.
Private Key ID	The unique identifier for the private key. Corresponds to the `private_key_id` property in the key file.
Private Key	The RSA private key in PEM encoding. Corresponds to the `private_key` property in the key file. Include the full key, including the `-----BEGIN PRIVATE KEY-----` and `-----END PRIVATE KEY-----` lines. **Note:** Remove any `\n` characters before you paste the key into the field.
Client Email	The service account email address. Corresponds to the `client_email` property in the key file. The format is `SERVICE_ACCOUNT_NAME@PROJECT_ID.iam.gserviceaccount.com`.
Client ID	The unique numeric identifier for the service account. Corresponds to the `client_id` property in the key file.
Auth URI	The URI used for authentication. Corresponds to the `auth_uri` property in the key file. The value is typically `https://accounts.google.com/o/oauth2/auth`.

©2026 Tanium Inc. All Rights Reserved

Field	Description
Token URI	The URI used to obtain access tokens. Corresponds to the `token_uri` property in the key file. The value is typically `https://oauth2.googleapis.com/token`.
Auth Provider X509 Cert URL	The URL for the Google public X.509 certificates used to verify tokens. Corresponds to the `auth_provider_x509_cert_url` property in the key file. The value is typically `https://www.googleapis.com/oauth2/v1/certs`.
Client X509 Cert URL	The URL for the public X.509 certificate for the service account. Corresponds to the `client_x509_cert_url` property in the key file.
Universe Domain	The Google Cloud universe domain. Corresponds to the `universe_domain` property in the key file. The value is typically `googleapis.com`.

©2026 Tanium Inc. All Rights Reserved