Tanium™ Security Recommendations Guide

Version: All

December 17, 2018

Table of contents

Tanium Security Recommendations

Tanium provides various resources, including hardened appliances and documentation, to help customers implement a secure architecture and configuration of the Tanium Core Platform. This document provides an overview of these resources and recommendations.

Infrastructure options

There are three primary infrastructure options for deploying the Tanium Core Platform:

1. Hardened physical or virtual Tanium appliance.
2. Cloud deployment.
3. Windows installation on customer-provided hardware.

Tanium recommends that you deploy a physical or virtual appliance when possible. Updates for the appliances are provided by Tanium. If an appliance is not practical, Tanium Core Platform software can be installed to customer-provided hardware. Tanium supports automated deployment on supported cloud infrastructure or manual installation on a Windows Server host computer. Deployments on cloud infrastructure or customer-provided hardware require that the customer maintain and update the selected infrastructure.

General security recommendations

Regardless of how Tanium is deployed, we recommend customers follow the security best practices defined below.

Secure access to the Tanium Console

Tanium recommends that network access to the Tanium console be limited to specific management networks and specific devices. In addition, user access should require multi-factor authentication (MFA). Tanium supports multi-factor authentication via RADIUS, TACACS+, X.509 based certificate authentication with Common Access Cards (CAC), and SAML.

RELATED LINKS

- Tanium Core Platform Installation Guide: Smart card authentication
- Tanium Core Platform User Guide: Using SAML

Install a valid TLS Certificate

User connections to the Tanium Console is encrypted via Transport Layer Security (TLS). A self-signed certificate is generated during the installation process. However, Tanium recommends that customers obtain and install a valid TLS certificate.

RELATED LINKS

- Tanium Core Platform Installation Guide: SSL Certificates
- Tanium Support KB: Tanium SSL/TLS Certificates and Keys (login required)

Configure enhanced security for Tanium private keys

Tanium recommends using a Hardware Security Modules (HSM) to provide a higher level of protection for key material. When an HSM is used, key material is stored on the HSM, rather than on the Tanium Server, and cannot be retrieved from the HSM. The Tanium Server interacts with the HSM which signs valid Tanium requests.

RELATED LINKS

- Tanium Support KB: Using an HSM to store cryptographic keys (login required)

Use two-person integrity for actions

Tanium recommends you enable and use the action approval feature be when possible. Action approval is sometimes referred to as “four eyes” control. When action approval is enabled, any action deployed by a user must first be approved by a second knowledgeable employee. Action approval significantly mitigates the risk of an operator mistakenly issuing a potentially harmful action.

RELATED LINKS

- Tanium Core Platform User Guide: Using action approval

Enable and forward Tanium logs

Tanium recommends that audit logs be enabled and forwarded to a centralized log management solution. Tanium supports logging of all actions performed by Tanium users, including user changes related to global settings, computer groups, packages, scheduled actions, saved questions, sensors, users, user groups, and whitelisted URLs.

RELATED LINKS

- Tanium Support KB: Tanium User Audit Logs (login required)

Role-based access control (RBAC)

Tanium supports fine-grained role-based access controls to allow your organization to implement the principle of least privilege. Tanium provides a number of granular roles with each product and supports creation of additional roles with custom privileges. In addition to role-based access controls, permissions may be scoped to a limited set of endpoints using computer groups. Tanium recommends leveraging these features to ensure that the appropriate roles are granted to existing users and new users in order to limit functionality according to the specific job requirements for a given user.

RELATED LINKS

- Tanium Core Platform User Guide: RBAC overview

Infrastructure-specific security recommendations

In addition to the general recommendations, Tanium recommends the following security considerations that are specific to each type of infrastructure.

Securing a Tanium Virtual Appliance

Tanium recommends that the virtual host be appropriately secured in a way that limits access to the guest Tanium virtual appliance. This includes applying appropriate hardening guides and, where possible, requiring MFA to access the host.

Securing a deployment in cloud infrastructure

Tanium recommends that cloud environments hosting Tanium Core Platform servers be subject to strict access controls to ensure that only a well-known and limited group of users may access and alter the cloud resources used by the Tanium deployment. Tanium recommends that you leverage the cloud provider's access controls functionality to isolate the Tanium Core Platform servers from other internal or production systems:

- In Amazon Web Services (AWS) infrastructure, use Organizations and deploy in a Tanium-specific AWS account.
- In a Google Cloud Platform (GCP) infrastructure, deploy Tanium in a Tanium-specific Project.
- In Microsoft Azure infrastructure, deploy Tanium in a Tanium-specific Resource Group.

In addition, follow the security best practices available from your cloud provider and industry standards including, but not limited to, limiting network communications to and

from their virtual network, ensuring MFA is enabled for cloud users, and monitoring cloud API activity.

Securing a deployment in customer-provided Windows infrastructure

When installing Tanium on a Windows Server, Tanium recommends that customers follow the Tanium hardening guide. The guide was developed in cooperation with the Defense Information Systems Agency (DISA) and provides recommendations on how to secure the Tanium Server in a Windows environment.

In addition to following the hardening guide, Tanium also recommends that customers implement strict access controls, in order to mitigate the risk of a domain credential compromise impacting the security of a Tanium Windows installation. At a minimum this should include:

- Restricting inbound access to Windows management protocols via a hardware or software-based firewall, especially those not protected by MFA. Access can also be limited by removing the Windows Server from the domain.
- Limiting the number of services accounts and permissions for service accounts to only the accounts and permissions that are required.

RELATED LINKS

- Tanium Application and Directory Hardening Guide (login required)