Tanium™ Security Recommendations Guide

Version: All

July 14, 2020

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://docs.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 services provided 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 to make interaction with Tanium software more intuitive and to accelerate the time to success. To ensure high accessibility standards, Tanium complies with the U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. We have conducted third-party accessibility assessments over the course of product development for many years, and most recently a comprehensive audit against the WCAG 2.1 / VPAT 2.3 standards for all major product modules was completed in September 2019. 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 best efforts to address any gaps quickly, as is feasible, given the severity of the issue and scope of the changes. These objectives are factored 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 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 TAM, sales representative, or email accessibility@tanium.com to make further inquiries.

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 two primary infrastructure options for deploying the Tanium Core Platform:

1. Hardened physical or virtual Tanium appliance.
2. 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, or to a cloud infrastructure with Windows virtual machines. 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, Tanium recommends the following security best practices.

Secure access to the Tanium Console

Tanium recommends that you limit network access to the Tanium console 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 Deployment Reference Guide: Smart card authentication
- Tanium Core Platform User Guide: Using SAML

Install a valid TLS Certificate

User connections to the Tanium Console are encrypted using 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 Deployment Reference Guide: SSL certificates
- Tanium Support KB: Tanium SSL/TLS Certificates and Keys (login required)

Configure enhanced security for Tanium private keys

Tanium recommends that you use a Hardware Security Module (HSM) to provide a higher level of protection for key material. When you use an HSM, keys are 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 Console User Guide: Managing Tanium keys
- Tanium Support KB: Using an HSM to store cryptographic keys (login required)

Use two-person integrity for actions

Tanium recommends that you enable and use the action approval feature when possible. When action approval is enabled, any action deployed by a user must first be approved by a second 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 you enable audit logs and forward the logs to a centralized log management solution. Tanium supports logging of all actions performed by Tanium users, including user changes related to API tokens, computer groups, content sets, dashboards, keys, global settings, packages, plugin schedules, privileges, saved questions, scheduled actions, roles, sensors, users, and user groups.

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, you can use computer groups to scope permissions to a limited set of endpoints. Tanium recommends leveraging these features to ensure that the appropriate roles are granted to existing users and new users 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 you secure the virtual host to limit 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 you subject cloud environments that host Tanium Core Platform servers 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.

Tanium also recommends that customers implement strict access controls 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 using 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.