Recommandations de sécurité Tanium™ Guide

Version : Tout

23 décembre 2020

Les informations contenues dans ce document peuvent être modifiées sans préavis. En outre, les informations fournies dans ce document sont fournies « telles quelles » et considérées comme exactes, mais présentées sans garantie de quelque nature que ce soit, expresse ou implicite, excepté dans les conditions générales de vente de Tanium. Sauf disposition contraire, Tanium décline toute responsabilité de quelque sorte que ce soit, et en aucun cas Tanium ou ses fournisseurs ne seront tenus responsables de dommages indirects, spéciaux, consécutifs ou accessoires, y compris, sans s'y limiter, de pertes de profits, de pertes ou d'endommagement de données découlant de l'utilisation ou de l'incapacité d'utiliser ce document, même si Tanium Inc. a été informé de la possibilité de tels dommages.

Les adresses IP utilisées dans ce document ne sont pas censées être des adresses réelles. Les exemples, la sortie d'affichage de commande, les diagrammes de topologie réseau et les autres figures incluses dans ce document sont montrés à titre d'illustration uniquement. Toute utilisation d'adresses IP réelles dans un contenu illustratif est involontaire et accidentelle.

Rendez-vous sur https://docs.tanium.com pour obtenir la documentation produit Tanium la plus récente.

Table des matières

Recommandations de sécurité Tanium

Tanium fournit diverses ressources, notamment des appliances renforcées et de la documentation, afin d'aider les clients à implémenter une architecture et une configuration sécurisées de la Tanium Core Platform. Ce document fournit un aperçu de ces ressources et recommandations.

Options d'infrastructure

Il existe deux options d'infrastructure principales pour déployer le logiciel Tanium Core Platform :

1. Appliance Tanium physique ou virtuelle renforcée.
2. Installation de Windows sur matériel fourni par client.

Tanium recommande de déployer une appliance physique ou virtuelle lorsque cela est possible. Les mises à jour des appliances sont fournies par Tanium. Si une appliance n'est pas pratique, le logiciel Tanium Core Platform peut être installé sur le matériel fourni par le client ou sur une infrastructure Cloud avec des ordinateurs virtuels Windows. Les déploiements sur l'infrastructure cloud ou le matériel fourni par le client nécessitent que le client maintienne et mette à jour l'infrastructure sélectionnée.

Recommandations générales de sécurité

Quel que soit le mode de déploiement de Tanium, nous recommandons aux clients de suivre les meilleures pratiques de sécurité définies ci-dessous.

Accès sécurisé à la console Tanium

Tanium recommande que l'accès réseau à la console Tanium soit limité à des réseaux de gestion et des appareils spécifiques. En outre, l'accès utilisateur nécessite une authentification à plusieurs facteurs (MFA). Tanium prend en charge l'authentification à plusieurs facteurs via RADIUS, TACACS+, l'authentification de certificat basée sur X.509 avec des cartes d'accès commun (CAC) et SAML.

LIENS CONNEXES

- Guide de référence du déploiement de Tanium Core Platform : Authentification par smart card
- Guide d'utilisation de Tanium Core Platform : Utilisation de SAML

Installation d'un certificat TLS valide

Les connexions utilisateur à la console Tanium sont cryptées via TLS. Un certificat auto-signé est généré pendant le processus d'installation. Toutefois, Tanium recommande que les clients obtiennent et installent un certificat TLS valide.

LIENS CONNEXES

- Guide de référence du déploiement de Tanium Core Platform : Certificats SSL
- Assistance Tanium KB : Certificats et clés SSL/TLS Tanium (connexion requise)

Configuration de la sécurité renforcée des clés privées Tanium

Tanium recommande d'utiliser un module matériel de sécurité (Hardware Security Modules, HSM) afin de fournir un niveau de protection plus élevé pour le matériel clé. Lorsque vous utilisez un HSM, les clés sont stockées sur le HSM, plutôt que sur le serveur Tanium et vous ne pouvez pas les récupérer depuis le HSM. Le serveur Tanium interagit avec le HSM qui signe les requêtes Tanium valides.

LIENS CONNEXES

- Guide d'utilisation de la console Tanium : Gestion des clés Tanium
- Assistance Tanium KB : Utilisation d'un HSM pour stocker les clés cryptographiques (connexion requise)

Utilisation de l'intégrité à deux personnes pour les actions

Tanium vous recommande d'activer et d'utiliser la fonction d'approbation d'action lorsque cela est possible. Lorsque l'approbation d'action est activée, toute action déployée par un utilisateur doit d'abord être approuvée par un deuxième employé. L'approbation d'action atténue considérablement le risque que l'opérateur émette par erreur une action potentiellement préjudiciable.

LIENS CONNEXES

- Guide d'utilisation de la Tanium Core Platform : Utilisation de l'approbation d'action

Activation et transfert des journaux Tanium

Tanium recommande que les journaux d'audit soient activés et transmis à une solution centralisée de gestion des journaux. Tanium prend en charge la journalisation de toutes les actions effectuées par les utilisateurs Tanium, y compris les modifications d'utilisateur liées aux jetons API, groupes d'ordinateurs, jeux de contenus, tableaux de bord, clés, paramètres globaux, packages, calendriers de plug-in, privilèges, questions enregistrées,

actions planifiées, rôles, capteurs, utilisateurs, groupes d'utilisateurs et listes blanches d'URL.

LIENS CONNEXES

- Assistance Tanium KB : Journaux d'audit des utilisateurs Tanium (connexion requise)

Contrôle d'accès basé sur les rôles (Role-based access control, RBAC)

Tanium prend en charge des contrôles d'accès basés sur les rôles (RBAC) fins, afin de permettre à votre organisation de mettre en œuvre le principe du moindre privilège. Tanium offre un certain nombre de rôles granulaires avec chaque produit et prend en charge la création de rôles supplémentaires avec des privilèges personnalisés. En plus des contrôles d'accès basés sur les rôles (RBAC), vous pouvez utiliser des groupes d'ordinateurs pour limiter les permissions à un ensemble restreint de points de terminaison. Tanium recommande de tirer parti de ces fonctionnalités pour s'assurer que les rôles appropriés sont accordés aux utilisateurs existants et aux nouveaux utilisateurs, afin de limiter les fonctionnalités en fonction des exigences spécifiques de job pour un utilisateur donné.

LIENS CONNEXES

- Guide d'utilisation de la Tanium Core Platform : Vue d'ensemble du RBAC

Recommandations de sécurité spécifiques de l'infrastructure

En plus des recommandations générales, Tanium recommande les considérations de sécurité suivantes spécifiques à chaque type d'infrastructure.

Sécurisation d'une appliance virtuelle Tanium

Tanium vous recommande de sécuriser l'hôte virtuel afin de limiter l'accès à l'appliance virtuelle Tanium invitée. Cela inclut l'application des guides de renforcement appropriés et, dans la mesure du possible, l'exigence d'une authentification à plusieurs facteurs pour l'accès à l'hôte.

Sécurisation d'un déploiement dans une infrastructure Cloud

Tanium recommande que les environnements Cloud hébergeant les serveurs Tanium Core Platform soient soumis à des contrôles d'accès stricts, afin de garantir que seul un groupe d'utilisateurs bien connu et limité puisse accéder aux ressources Cloud utilisées par le déploiement Tanium et les modifier. Tanium recommande d'exploiter la fonctionnalité des contrôles d'accès du fournisseur cloud pour isoler les serveurs de la Tanium Core Platform des autres systèmes internes ou de production :

- Dans une infrastructure Amazon Web Services (AWS), utilisez Organizations (Organisations) et déployez dans un compte AWS spécifique à Tanium.
- Dans une infrastructure Google Cloud Platform (GCP), déployez Tanium dans un projet spécifique à Tanium.
- Dans une infrastructure Microsoft Azure, déployez Tanium dans un groupe de ressources spécifique à Tanium.

En outre, suivez les meilleures pratiques de sécurité disponibles auprès de votre fournisseur cloud, ainsi que les normes du secteur, ceci incluant, notamment, de limiter les communications réseau vers et depuis leur réseau virtuel, en vous assurant que l'authentification à plusieurs facteurs est activée pour les utilisateurs cloud et en surveillant l'activité API cloud.

Sécurisation d'un déploiement dans l'infrastructure Windows fournie par le client

Lors de l'installation de Tanium sur un Windows Server, Tanium recommande aux clients de suivre le guide de renforcement de Tanium. Le guide a été développé en coopération avec l'Agence des systèmes d'information de défense (Defense Information Systems Agency, DISA) et fournit des recommandations sur la manière de sécuriser le serveur Tanium dans un environnement Windows.

Tanium recommande également que les clients mettent en œuvre des contrôles d'accès stricts, afin d'atténuer le risque d'un compromis d'identification de domaine affectant la sécurité d'une installation Windows Tanium. Cela doit au minimum inclure :

- Restreindre l'accès entrant aux protocoles de gestion Windows via un pare-feu matériel ou logiciel, en particulier ceux qui ne sont pas protégés par une authentification à plusieurs facteurs. L'accès peut également être limité en supprimant le Windows Server du domaine.
- Limiter le nombre de comptes de services et les permissions pour les comptes de service uniquement aux comptes et permissions requis.

LIENS CONNEXES

- Guide de renforcement des répertoires et applications Tanium (connexion requise)