Tanium™ Sicherheitsempfehlungen Anleitung

Version: Alle

12 Januar 2021

Die Informationen in diesem Dokument können ohne Vorankündigung geändert werden. Darüber hinaus werden die Informationen in diesem Dokument ohne Mängelgewähr bereitgestellt und für korrekt gehalten, jedoch ohne jegliche Garantie, weder ausdrücklich noch stillschweigend, außer wie in den Verkaufsbedingungen für Kunden von Tanium angegeben. Sofern nicht anderweitig vorgesehen, übernimmt Tanium keinerlei Haftung, und in keinem Fall haftet Tanium oder seine Lieferanten für indirekte, spezielle, Folge- oder zufällige Schäden, einschließlich, unter anderem aus entgangenen Gewinnen oder Verlusten oder Beschädigung von Daten, die sich aus der Nutzung oder der Unfähigkeit der Nutzung dieses Dokuments ergeben, selbst wenn Tanium Inc. über die Möglichkeit solcher Schäden informiert wurde.

Alle in diesem Dokument verwendeten IP-Adressen sind nicht als tatsächliche Adressen gedacht. Beispiele, Befehlsanzeigeausgaben, Netzwerktopologie-Diagramme und sonstige in diesem Dokument enthaltene Abbildungen werden nur zu Illustrationszwecken dargestellt. Die Verwendung tatsächlicher IP-Adressen in illustrativen Inhalten ist unabsichtlich und zufällig.

Die aktuellsten Produktinformationen von Tanium finden Sie unter https://docs.tanium.com.

Inhaltsverzeichnis

Tanium-Sicherheitsempfehlungen

Tanium bietet verschiedene Ressourcen, einschließlich gehärteter Appliances und Dokumentationen, um Kunden dabei zu helfen, eine sichere Architektur und Konfiguration der Tanium Core Platform zu implementieren. Dieses Dokument bietet einen Überblick über diese Ressourcen und Empfehlungen.

Infrastrukturoptionen

Es gibt zwei grundlegende Infrastrukturoptionen für den Einsatz der Tanium Core Platform:

1. Gehärtete physische oder virtuelle Tanium-Appliance.
2. Windows-Installation auf die vom Kunden bereitgestellte Hardware.

Tanium empfiehlt, wenn möglich eine physische oder virtuelle Appliance einzusetzen. Aktualisierungen für die Appliances werden von Tanium bereitgestellt. Wenn eine Appliance nicht praktikabel ist, kann die Tanium Core Platform auf der vom Kunden bereitgestellten Hardware oder in einer Cloud-Infrastruktur mit virtuellen Windows-Maschinen installiert werden. Verteilungen auf Cloud-Infrastruktur oder vom Kunden bereitgestellter Hardware erfordern, dass der Kunde die ausgewählte Infrastruktur wartet und aktualisiert.

Allgemeine Sicherheitsempfehlungen

Unabhängig davon, wie Tanium bereitgestellt wird, empfiehlt Tanium die folgenden bewährten Verfahren zur Sicherheit.

Sicherer Zugang zur Tanium Console

Tanium empfiehlt, dass Sie den Netzwerkzugang auf die Tanium Console auf spezifische Verwaltungsnetzwerke und spezifische Geräte beschränken. Darüber hinaus sollte der Benutzerzugriff eine mehrstufige Authentifizierung (multi-factor authentication, MFA) erfordern. Tanium unterstützt die mehrstufige Authentifizierung über RADIUS, TACACS+, X.509-basierte Zertifikatsauthentifizierung mit CAC (Common Access Cards) und SAML.

VERWANDTE LINKS

- Referenzhandbuch zur Bereitstellung der Tanium Core Platform: Smartcard-Authentifizierung
- Benutzerhandbuch für die Tanium Core Platform: Verwenden von SAML

Ein gültiges TLS-Zertifikat installieren

Benutzerverbindungen zur Tanium Console werden mit TLS (Transport Layer Security) verschlüsselt. Ein selbstsigniertes Zertifikat wird während des Installationsprozesses generiert. Tanium empfiehlt jedoch, dass Kunden ein gültiges TLS-Zertifikat erhalten und installieren.

VERWANDTE LINKS

- Referenzhandbuch zur Bereitstellung der Tanium Core Platform: SSL-Zertifikate
- Tanium-Support KB: Tanium SSL/TLS- Zertifikate und Schlüssel (Anmeldung erforderlich)

Erweiterte Sicherheit für private Schlüssel von Tanium konfigurieren

Tanium empfiehlt, dass Sie ein Hardware-Sicherheitsmodul (Hardware Security Module, HSM) verwenden, um ein höheres Maß an Schutz für Schlüsselmaterial zu bieten. Wenn Sie ein HSM verwenden, werden Schlüssel auf dem HSM gespeichert, und nicht auf dem Tanium Server, und können nicht vom HSM abgerufen werden. Der Tanium Server interagiert mit dem HSM, der gültige Tanium-Anforderungen unterzeichnet.

VERWANDTE LINKS

- Benutzerhandbuch für die Tanium Console: Verwalten von Tanium-Schlüsseln
- Tanium-Support KB: Verwendung eines HSM : Zur Speicherung kryptographischer Schlüssel (Anmeldung erforderlich)

Verwenden Sie für Aktionen die Zwei-Personen-Integrität

Tanium empfiehlt, dass Sie gegebenenfalls die Funktion zur Aktionsfreigabe aktivieren und verwenden. Wenn die Aktionsfreigabe aktiviert ist, muss jede von einem Benutzer verteilte Aktion zunächst von einem zweiten Mitarbeiter genehmigt werden. Die Aktionsfreigabe mindert deutlich das Risiko eines Bedieners, irrtümlicherweise eine potenziell schädliche Handlung auszugeben.

VERWANDTE LINKS

- Benutzerhandbuch für die Tanium Core Platform: Verwenden der Aktionsfreigabe

Tanium-Protokolle aktivieren und weiterleiten

Tanium empfiehlt, dass Sie Prüfprotokolle aktivieren und die Protokolle an eine zentralisierte Protokollverwaltungslösung weiterleiten. Tanium unterstützt die Protokollierung aller von Tanium-Benutzern ausgeführten Aktionen, einschließlich

Benutzeränderungen, die sich auf API-Tokens, Computergruppen, Inhaltssets, Übersichtsseiten, Schlüssel, globale Einstellungen, Pakete, Plugin-Zeitpläne, Privilegien, gespeicherte Fragen, geplante Aktionen, Rollen, Sensoren, Benutzer, Benutzergruppen und auf der Whitelist verzeichnete URLs beziehen.

VERWANDTE LINKS

- Tanium-Support KB: Tanium-Benutzerprüfprotokolle (Anmeldung erforderlich)

Rollenbasierte Zugangskontrolle (RBAC)

Tanium unterstützt feinkörnige, rollenbasierte Zugangskontrollen, die es Ihrem Unternehmen ermöglichen, das Prinzip des geringsten Privilegs zu implementieren. Tanium stellt eine Reihe granularer Rollen bei jedem Produkt bereit und unterstützt die Erstellung zusätzlicher Rollen mit benutzerdefinierten Privilegien. Neben der RBAC können Sie Computergruppen verwenden, um Berechtigungen auf eine begrenzte Anzahl von Endpunkten zu beschränken. Tanium empfiehlt die Nutzung dieser Funktionen, um sicherzustellen, dass die entsprechenden Rollen bestehenden Benutzern und neuen Benutzern gewährt werden, um die Funktionalität gemäß den spezifischen Auftragsanforderungen für einen bestimmten Benutzer zu begrenzen.

VERWANDTE LINKS

- Benutzerhandbuch für die Tanium Core Platform: RBAC-Übersicht

Infrastrukturspezifische Sicherheitsempfehlungen

Zusätzlich zu den allgemeinen Empfehlungen empfiehlt Tanium die folgenden Sicherheitsaspekte, die für jede Art von Infrastruktur spezifisch sind.

Sichern einer virtuellen Tanium-Appliance

Tanium empfiehlt, dass Sie den virtuellen Host sichern, um den Zugriff auf die virtuelle Tanium-Gast-Appliance zu beschränken. Dies beinhaltet die Anwendung geeigneter Härtungsleitfäden und, wenn möglich, die Anforderung, dass MFA auf den Host zugreifen muss.

Sichern einer Bereitstellung in der Cloud-Infrastruktur

Tanium empfiehlt, dass Sie Cloud-Umgebungen, die Tanium Core Platform-Server hosten, strengen Zugangskontrollen unterwerfen, um sicherzustellen, dass nur eine gut bekannte und begrenzte Gruppe von Benutzern Zugang zu den von der Tanium-Verteilung verwendeten Cloud-Ressourcen haben und diese auch verändern können. Tanium empfiehlt, die Zugangskontrollfunktionalität des Cloud-Anbieters zu nutzen, um die

Tanium Core Platform-Server von anderen internen oder Produktionssystemen zu isolieren:

- In der Amazon Web Services (AWS)-Infrastruktur verwenden Sie Organisationen und stellen diese in einem Tanium-spezifischen AWS-Konto bereit.
- In einer Google Cloud Platform (GCP)-Infrastruktur stellen Sie Tanium in einem Tanium-spezifisches Projekt bereit.
- In der Microsoft Azure-Infrastruktur stellen Sie Tanium in einer Tanium-spezifische Ressourcengruppe bereit.

Befolgen Sie außerdem die bewährten Sicherheitspraktiken und Branchenstandards, die von Ihren Cloud-Anbietern zur Verfügung stehen, einschließlich, unter anderem die Beschränkung der Netzwerkkommunikation auf und von ihrem virtuellen Netzwerk, indem Sie sicherstellen, dass die mehrstufige Authentifizierung für Cloud-Benutzer aktiviert ist und die Cloud-API-Aktivität überwacht wird.

Sichern einer Verteilung in einer vom Kunden bereitgestellten Windows-Infrastruktur

Bei der Installation von Tanium auf einem Windows-Server empfiehlt Tanium, dass Kunden den Tanium-Härtungsleitfaden befolgen. Der Leitfaden wurde in Zusammenarbeit mit der Defense Information Systems Agency (DISA) entwickelt und bietet Empfehlungen zur Sicherung von Tanium Server in einer Windows-Umgebung.

Tanium empfiehlt auch, dass Kunden strenge Zugangskontrollen implementieren, um das Risiko zu senken, dass die Sicherheit einer Tanium-Installation unter Windows durch eine Kompromittierung der Domänen-Zugangsdaten beeinträchtigt wird. Dies sollte mindestens Folgendes umfassen:

- Beschränkung des eingehenden Zugriffs auf Windows-Managementprotokolle mit einer hardware- oder softwarebasierten Firewall, insbesondere solche, die nicht durch die mehrstufige Authentifizierung geschützt sind. Der Zugriff kann auch durch Entfernen des Windows-Servers aus der Domäne eingeschränkt werden.
- Begrenzung der Anzahl von Dienstkonten und Berechtigungen für Dienstkonten auf ausschließlich solchen Konten und Berechtigungen, die erforderlich sind.

VERWANDTE LINKS

- Härtungsleitfaden für Tanium-Anwendung und Verzeichnis (Anmeldung erforderlich)