

Guide sur la configuration sécurisée

3 mai 2018

vRealize Automation 7.3



vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

<https://docs.vmware.com/fr/>

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Copyright © 2015–2018 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

Table des matières

| | | |
|----------|--|-----------|
| 1 | Configuration sécurisée | 5 |
| 2 | Informations mises à jour | 6 |
| 3 | vRealize Automation Présentation de la sécurisation de la ligne de base | 7 |
| 4 | Vérification de l'intégrité du support d'installation | 9 |
| 5 | Sécurisation renforcée de l'infrastructure logicielle du système VMware | 10 |
| | Sécurisation renforcée de l'environnement VMware vSphere® | 10 |
| | Sécurisation renforcée sur un hôte IaaS (Infrastructure en tant que service) | 10 |
| | Sécurisation renforcée de Microsoft SQL Server | 11 |
| | Sécurisation renforcée de Microsoft .NET | 11 |
| | Sécurisation renforcée de Microsoft Internet Information Services (IIS) | 12 |
| 6 | Vérification des logiciels installés | 13 |
| 7 | Correctifs et avis de sécurité de VMware | 14 |
| 8 | Configuration sécurisée | 15 |
| | Sécurisation du dispositif vRealize Automation | 15 |
| | Modifier le mot de passe racine | 15 |
| | Vérifier le hachage et la complexité du mot de passe racine | 16 |
| | Vérifier l'historique du mot de passe racine | 17 |
| | Gérer l'expiration des mots de passe | 17 |
| | Gestion de comptes administratifs et Secure Shell (SSH) | 18 |
| | Modifier l'utilisateur de l'interface de gestion de dispositif virtuel | 23 |
| | Définir l'authentification du chargeur de démarrage | 24 |
| | Configurer NTP | 25 |
| | Configuration du protocole TLS pour les données en transit du dispositif vRealize Automation | 25 |
| | Vérification de la sécurité des données au repos | 37 |
| | Configurer les ressources d'application de vRealize Automation | 38 |
| | Personnalisation de la configuration du proxy de la console | 40 |
| | Configuration des en-têtes de réponse de serveur | 42 |
| | Définir le délai d'expiration de session dispositif vRealize Automation | 44 |
| | Gestion des logiciels non essentiels | 44 |
| | Sécurisation du composant IaaS (Infrastructure en tant que service) | 49 |
| | Désactivation du service de temps Windows | 49 |

| | |
|--|----|
| Configuration de TLS pour les données en transit d'IaaS (Infrastructure en tant que service) | 49 |
| Configuration des suites de chiffrement TLS | 51 |
| Vérification de la sécurité du serveur hôte | 52 |
| Protection des ressources d'application | 52 |
| Sécuriser la machine hôte IaaS (Infrastructure en tant que service) | 53 |

9 Configuration de la sécurité réseau des hôtes 55

| | |
|---|----|
| Configuration des paramètres réseau pour les dispositifs VMware | 55 |
| Empêcher le contrôle par l'utilisateur des interfaces réseau | 55 |
| Définir la taille de la file d'attente du backlog TCP | 56 |
| Refuser les demandes d'écho ICMPv4 d'adresse de diffusion | 56 |
| Désactiver le protocole ARP du proxy IPv4 | 57 |
| Refuser les messages de redirection ICMP IPv4 | 57 |
| Refuser les messages de redirection ICMP IPv6 | 58 |
| Journaliser des paquets martiens IPv4 | 59 |
| Utiliser le filtrage de chemin inverse IPv4 | 59 |
| Refuser le transfert IPv4 | 60 |
| Refuser le transfert IPv6 | 61 |
| Utiliser des cookies SYN TCP IPv4 | 61 |
| Refuser les annonces du routeur IPv6 | 62 |
| Refuser les sollicitations du routeur IPv6 | 63 |
| Refuser la préférence du routeur IPv6 dans les sollicitations du routeur | 64 |
| Refuser le préfixe du routeur IPv6 | 64 |
| Refuser les paramètres de limite de sauts d'annonce du routeur IPv6 | 65 |
| Refuser les paramètres d'autoconfiguration d'annonce du routeur IPv6 | 66 |
| Refuser les sollicitations de voisin IPv6 | 67 |
| Limiter le nombre maximal d'adresses IPv6 | 67 |
| Configuration des paramètres réseau pour l'hôte IaaS (Infrastructure en tant que service) | 68 |
| Configuration des ports et des protocoles | 68 |
| Ports utilisateur requis | 69 |
| Ports requis par l'administrateur | 69 |

10 Audit et journalisation 72

Configuration sécurisée

La configuration sécurisée permet aux utilisateurs d'évaluer et d'optimiser la configuration sécurisée des déploiements vRealize Automation.

La configuration sécurisée décrit la vérification et la configuration des déploiements sécurisés pour des environnements vRealize Automation types. Des informations et des procédures permettent aux utilisateurs de prendre des décisions informées sur la configuration de la sécurité.

Public visé

Ces informations s'adressent aux administrateurs système vRealize Automation et autres utilisateurs responsables de la configuration et de la maintenance de la sécurité du système.

Glossaire VMware Technical Publications

VMware Technical Publications fournit un glossaire des termes qui peuvent éventuellement ne pas vous être familiers. Pour consulter la définition des termes utilisés dans la documentation technique VMware, visitez le site Web <http://www.vmware.com/support/pubs>.

Informations mises à jour

Ce *Guide de configuration sécurisée* est mis à jour avec chaque version du produit ou lorsque cela est nécessaire.

Ce tableau fournit l'historique des mises à jour du *Guide de configuration sécurisée*.

| Révision | Description |
|-----------------|---|
| 3 mai 2018 | Modifications mineures. |
| 5 décembre 2017 | Rubrique Activer TLS sur une configuration localhost mise à jour |
| 002535-01 | Mise à jour de la section Définir le délai d'expiration de session dispositif vRealize Automation . |
| 002535-00 | Version initiale. |

vRealize Automation

Présentation de la sécurisation de la ligne de base

3

VMware fournit des recommandations complètes pour vous aider à vérifier et à configurer une ligne de base sécurisée pour votre système vRealize Automation.

Utilisez les outils et les procédures spécifiés par VMware pour vérifier et maintenir une configuration de ligne de base avec sécurisation renforcée sur votre système vRealize Automation. Certains composants vRealize Automation sont installés dans un état sécurisé ou partiellement sécurisé, mais vous devez vérifier la configuration de chaque composant en fonction des recommandations de sécurité de VMware, des stratégies de sécurité de l'entreprise et des menaces connues.

Approche de la sécurité de vRealize Automation

L'approche de la sécurité de vRealize Automation suppose un environnement sécurisé de façon holistique, reposant sur la configuration du système et du réseau, les stratégies de sécurité de l'organisation et les meilleures pratiques de sécurité.

Lors de la vérification et de la configuration de la sécurisation renforcée d'un système vRealize Automation, tenez compte de chacun des éléments suivants, tels que définis par les recommandations de sécurisation renforcée de VMware.

- Déploiement sécurisé
- Configuration sécurisée
- Sécurité du réseau

Afin de garantir la sécurisation renforcée de votre système, suivez les recommandations de VMware et vos stratégies locales de sécurité, car elles se rapportent à chacun de ces concepts.

Composants système

Lors de la préparation de la sécurisation renforcée et de la configuration sécurisée de votre système vRealize Automation, assurez-vous de comprendre l'ensemble des composants et leurs interactions au niveau du système.

Tenez compte des composants suivants lors de la planification et de l'implémentation d'un système sécurisé.

- dispositif vRealize Automation

■ Composant IaaS

Pour vous familiariser avec vRealize Automation et comprendre l'interaction entre les composants, reportez-vous à la section *Fondements et concepts* du centre de documentation de VMware vRealize Automation. Pour plus d'informations sur les déploiements et l'architecture types de vRealize Automation, reportez-vous à la section *Architecture de référence*.

Vérification de l'intégrité du support d'installation

4

Les utilisateurs doivent toujours vérifier l'intégrité du support d'installation avant d'installer un produit VMware.

Vérifiez toujours le hachage SHA1 après avoir téléchargé un fichier ISO, un bundle hors ligne ou un correctif, afin de garantir l'intégrité et l'authenticité des fichiers téléchargés. Si vous obtenez des supports physiques de VMware et si le sceau de sécurité a été rompu, renvoyez le logiciel à VMware en demandant son remplacement.

Après avoir téléchargé le support, utilisez la somme MD5/SHA1 pour vérifier l'intégrité du téléchargement. Comparez la sortie de hachage MD5/SHA1 avec la valeur publiée sur le site Web de VMware. Les hachages SHA1 ou MD5 doivent correspondre.

Pour plus d'informations sur la vérification de l'intégrité du support d'installation, reportez-vous à l'article <http://kb.vmware.com/kb/1537>.

Sécurisation renforcée de l'infrastructure logicielle du système VMware

5

Dans le cadre du processus de sécurisation renforcée, évaluez l'infrastructure logicielle déployée qui prend en charge votre système VMware et vérifiez qu'elle respecte les directives de sécurisation renforcée de VMware.

Avant de renforcer la sécurité de votre système VMware, identifiez et corrigez les défauts de sécurité de l'infrastructure logicielle utilisée, afin de créer un environnement totalement renforcé et sécurisé. Vous devez notamment prendre en compte les composants du système d'exploitation, les logiciels de prise en charge et de base de données. Traitez les problèmes de sécurité à ce niveau, et sur les autres composants impliqués, selon les recommandations du fabricant et autres protocoles de sécurité applicables.

Ce chapitre aborde les rubriques suivantes :

- [Sécurisation renforcée de l'environnement VMware vSphere®](#)
- [Sécurisation renforcée sur un hôte IaaS \(Infrastructure en tant que service\)](#)
- [Sécurisation renforcée de Microsoft SQL Server](#)
- [Sécurisation renforcée de Microsoft .NET](#)
- [Sécurisation renforcée de Microsoft Internet Information Services \(IIS\)](#)

Sécurisation renforcée de l'environnement VMware vSphere®

Évaluez l'environnement de VMware vSphere® et assurez-vous que le niveau approprié de sécurisation renforcée vSphere est appliqué et maintenu.

Pour obtenir plus de conseils sur la sécurisation renforcée, consultez <http://www.vmware.com/security/hardening-guides.html> .

Dans le cadre d'un environnement entièrement renforcé, l'infrastructure VMware vSphere® doit appliquer les directives de sécurité définies par VMware.

Sécurisation renforcée sur un hôte IaaS (Infrastructure en tant que service)

Assurez-vous que votre machine hôte IaaS (Infrastructure en tant que service) Microsoft Windows a été sécurisée de manière renforcée conformément aux directives de VMware.

Consultez les recommandations des directives de sécurisation renforcée et les meilleures pratiques de sécurité de Microsoft Windows, et assurez-vous que votre hôte Windows Server a bien été renforcé. La non-application des recommandations de sécurisation renforcée risque d'entraîner l'exposition à des failles de sécurité connues à partir de composants non sécurisés sur les différentes versions de Windows.

Pour vous assurer que votre version est prise en charge, reportez-vous à la [matrice de prise en charge de vRealize Automation](#).

Contactez votre fournisseur Microsoft pour en savoir plus sur les pratiques en matière de sécurisation renforcée des produits Microsoft.

Sécurisation renforcée de Microsoft SQL Server

Vérifiez que la base de données Microsoft SQL Server est conforme aux directives de sécurité fournies par Microsoft et par VMware.

Consultez les recommandations des directives en matière de sécurisation renforcée ainsi que les meilleures pratiques de sécurité de Microsoft SQL Server. Consultez tous les bulletins de sécurité Microsoft relatifs à la version installée de Microsoft SQL Server. La non-application des recommandations en matière de sécurisation renforcée risque d'entraîner l'exposition à des failles de sécurité connues à partir de composants non sécurisés sur les différentes versions de Microsoft SQL Server.

Pour vous assurer que votre version de Microsoft SQL Server est prise en charge, reportez-vous à la [matrice de prise en charge de vRealize Automation](#).

Contactez votre fournisseur Microsoft pour plus de détails sur les pratiques de sécurisation renforcée pour les produits Microsoft.

Sécurisation renforcée de Microsoft .NET

Dans le cadre d'un environnement entièrement renforcé, Microsoft .NET doit appliquer les directives de sécurité définies par Microsoft et par VMware.

Vérifiez les recommandations définies dans les directives sur la sécurisation renforcée et les meilleures pratiques de sécurité de .NET. En outre, consultez tous les bulletins de sécurité Microsoft concernant la version de Microsoft SQL Server que vous utilisez. La non-application des recommandations en matière de sécurisation renforcée risque d'entraîner l'exposition à des failles de sécurité connues à partir de composants Microsoft.NET non sécurisés.

Pour vous assurer que votre version de Microsoft.NET est prise en charge, reportez-vous à la [matrice de prise en charge de vRealize Automation](#).

Contactez votre fournisseur Microsoft pour plus de détails sur les pratiques de sécurisation renforcée concernant les produits Microsoft.

Sécurisation renforcée de Microsoft Internet Information Services (IIS)

Vérifiez que votre version de Microsoft Internet Information Services (IIS) est conforme à toutes les directives de sécurité de Microsoft et de VMware.

Vérifiez les recommandations figurant dans les directives de sécurisation renforcée et les meilleures pratiques de sécurité de Microsoft IIS. En outre, consultez tous les bulletins de sécurité Microsoft concernant la version d'IIS que vous utilisez. La non-application des recommandations en matière de sécurisation renforcée risque d'entraîner l'exposition à des failles de sécurité connues.

Pour vous assurer que votre version est prise en charge, reportez-vous à la [matrice de prise en charge de vRealize Automation](#).

Contactez votre fournisseur Microsoft pour plus de détails sur les pratiques de sécurisation renforcée concernant les produits Microsoft.

Vérification des logiciels installés

6

Dans la mesure où les vulnérabilités liées aux logiciels tiers et aux logiciels non utilisés augmentent le risque d'accès non autorisé au système et l'interruption de la disponibilité, il est important de vérifier tous les logiciels installés sur les machines hôtes VMware et d'évaluer leur utilisation.

N'installez pas un logiciel qui ne soit pas nécessaire au fonctionnement sécurisé du système sur les machines hôtes VMware. Désinstallez les logiciels non utilisés ou superflus.

Inventaire des logiciels installés non pris en charge

Évaluez votre déploiement VMware et faites l'inventaire des produits installés pour vérifier qu'aucun logiciel non pris en charge n'est installé.

Pour plus d'informations sur les stratégies de prise en charge de produits tiers, reportez-vous à l'article d'assistance de VMware à la page : <https://www.vmware.com/support/policies/thirdparty.html>.

Vérification des logiciels tiers

VMware ne prend pas en charge et ne recommande pas l'installation des logiciels tiers qui n'ont pas été testés et vérifiés. Les logiciels tiers non sécurisés, sans correctifs ou non authentifiés installés sur des machines hôtes VMware, peuvent exposer le système à un accès non autorisé et perturber sa disponibilité. Si vous devez utiliser des logiciels tiers non pris en charge, consultez leurs éditeurs pour connaître les conditions requises pour la configuration sécurisée et l'application de correctifs.

Correctifs et avis de sécurité de VMware



Pour assurer une sécurité optimale de votre système, suivez les avis de sécurité de VMware et appliquez tous les correctifs appropriés.

VMware publie des avis de sécurité pour les produits. Informez-vous et tenez compte de ces avis pour vous assurer que votre produit est protégé contre les menaces connues.

Évaluez l'installation de vRealize Automation, l'application des correctifs et l'historique des mises à niveau, et vérifiez que les avis de sécurité publiés par VMware sont respectés et appliqués.

Pour plus d'informations sur les derniers avis de sécurité de VMware, consultez la page <http://www.vmware.com/security/advisories/>.

Configuration sécurisée

Vérifiez et mettez à jour les paramètres de sécurité des dispositifs virtuels vRealize Automation et du composant IaaS (Infrastructure en tant que service) en fonction de la configuration de votre système. En outre, vérifiez et mettez à jour la configuration des autres composants et applications.

La configuration sécurisée d'une installation vRealize Automation implique de traiter la configuration de chaque composant individuellement, en tenant compte de leurs interactions. Tenez compte de la configuration de tous les composants système pour obtenir une ligne de base raisonnablement sécurisée.

Ce chapitre aborde les rubriques suivantes :

- [Sécurisation du dispositif vRealize Automation](#)
- [Sécurisation du composant IaaS \(Infrastructure en tant que service\)](#)

Sécurisation du dispositif vRealize Automation

Vérifiez et mettez à jour les paramètres de sécurité pour le dispositif vRealize Automation en fonction de la configuration de votre système.

Configurez les paramètres de sécurité pour vos dispositifs virtuels et leurs systèmes d'exploitation hôtes. En outre, définissez ou vérifiez la configuration d'autres applications et composants associés. Dans certains cas, vous devez vérifier les paramètres existants, alors que dans d'autres vous devez modifier ou ajouter des paramètres afin d'obtenir une configuration appropriée.

Modifier le mot de passe racine

Vous pouvez modifier le mot de passe racine pour le dispositif vRealize Automation afin de répondre aux exigences de sécurité applicables.

Modifiez le mot de passe racine sur le dispositif vRealize Automation à l'aide de l'interface VAMI (Virtual Appliance Management Interface). Vérifiez que le mot de passe racine répond aux exigences de complexité des mots de passe d'entreprise de votre organisation.

Procédure

- 1 Ouvrez l'interface VAMI de votre dispositif vRealize Automation.

`https://vRealizeAppliance-url:5480`

- 2 Sélectionnez l'onglet **Admin** de l'interface VAMI.
- 3 Sélectionnez le sous-menu **Admin**.
- 4 Entrez le mot de passe existant dans la zone de texte **Mot de passe d'administrateur actuel**.
- 5 Entrez le nouveau mot de passe dans la zone de texte **Nouveau mot de passe d'administrateur**.
- 6 Entrez le nouveau mot de passe dans la zone de texte **Confirmez le nouveau mot de passe d'administrateur**.
- 7 Cliquez sur **Enregistrer les paramètres** pour enregistrer les modifications.

Vérifier le hachage et la complexité du mot de passe racine

Vérifiez que le mot de passe racine répond aux exigences de complexité des mots de passe d'entreprise de votre organisation.

La validation de la complexité du mot de passe racine est requise, car l'utilisateur racine contourne la vérification de la complexité du mot de passe du module `pam_cracklib` qui est appliquée aux comptes d'utilisateurs.

Le mot de passe de compte doit commencer par `6`, ce qui indique un hachage sha512. Il s'agit du hachage standard pour tous les dispositifs sécurisés.

Procédure

- 1 Pour vérifier le hachage du mot de passe racine, connectez-vous en tant qu'utilisateur racine et exécutez la commande `# more /etc/shadow`.

Les informations de hachage s'affichent.

Figure 8-1. Résultats du hachage de mot de passe

```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KzK4SS44UEHPfAtgs
P/:16346:0:365:7:::
```

- 2 Si le mot de passe racine ne contient pas de hachage sha512, exécutez la commande `passwd` pour le modifier.

Tous les dispositifs sécurisés activent `enforce_for_root` pour le module `pw_history`, disponible dans le fichier `/etc/pam.d/common-password`. Par défaut, le système mémorise les cinq derniers mots de passe. Les anciens mots de passe sont stockés pour chaque utilisateur dans le fichier `/etc/securetty/passwd`.

Vérifier l'historique du mot de passe racine

Vérifiez que l'historique du mot de passe est appliqué pour le compte racine.

Tous les dispositifs sécurisés activent `enforce_for_root` pour le module `pw_history`, disponible dans le fichier `/etc/pam.d/common-password`. Par défaut, le système mémorise les cinq derniers mots de passe. Les anciens mots de passe sont stockés pour chaque utilisateur dans le fichier `/etc/securetty/passwd`.

Procédure

- 1 Exécutez la commande suivante :

```
cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so
```

- 2 Assurez-vous que `enforce_for_root` apparaît dans les résultats renvoyés.

```
password required pam_pwhistory.so enforce_for_root remember=5 retry=3
```

Gérer l'expiration des mots de passe

Configurez toutes les expirations de mot de passe des comptes conformément aux stratégies de sécurité de votre organisation.

Par défaut, tous les comptes du dispositif virtuel VMware renforcé appliquent un délai d'expiration de mot de passe de 60 jours. Sur la plupart des dispositifs renforcés, l'expiration de mot de passe du compte racine est fixée à 365 jours. Il est recommandé de vérifier que la date d'expiration de l'ensemble des comptes répond aux normes de sécurité et d'opération.

Si le mot de passe racine expire, vous ne pouvez pas le rétablir. Vous devez implémenter des stratégies propres au site pour éviter l'expiration des mots de passe d'administration et racines.

Procédure

- 1 Connectez-vous aux machines du dispositif virtuel en tant qu'utilisateur racine et exécutez la commande suivante pour vérifier la date d'expiration des mots de passe sur tous les comptes.

```
# cat /etc/shadow
```

Les informations d'expiration du mot de passe figurent dans le cinquième champ (les champs sont séparés par le signe deux-points) du fichier caché. L'expiration du mot de passe racine est définie en jours.

Figure 8-2. Champ de date d'expiration de mot de passe

```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870:0:60:7:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870:0:60:7:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KzK4SS44UEHPfAtgsB6iy1nJYbBk
zRbYR1mvJiX.pJpub0AEpP/:16346:0:365:7:::
sshd:!:16332:0:60:7:::
```

- 2 Pour modifier le délai d'expiration du compte racine, exécutez une commande au format suivant :

```
# passwd -x 365 root
```

Dans cette commande, 365 indique le nombre de jours jusqu'à l'expiration du mot de passe. Utilisez la même commande pour modifier n'importe quel utilisateur, en remplaçant le compte concerné par « racine » et en remplaçant le nombre de jours conformément aux normes d'expiration de l'organisation.

Gestion de comptes administratifs et Secure Shell (SSH)

Pour les connexions à distance, tous les dispositifs renforcés incluent le protocole SSH (Secure Shell). Utilisez uniquement le protocole SSH lorsque cela est nécessaire et gérez-le de façon à préserver la sécurité du système.

SSH est un environnement interactif de ligne de commande qui prend en charge les connexions à distance aux dispositifs virtuels VMware. Par défaut, l'accès SSH nécessite des informations d'identification de compte d'utilisateur avec des privilèges élevés. Les activités SSH de l'utilisateur racine contournent généralement le contrôle d'accès basé sur les rôles (RBAC) et les audits des dispositifs virtuels.

Il est recommandé de désactiver le mode SSH dans un environnement de production et de l'activer uniquement pour résoudre les problèmes que vous ne pouvez pas résoudre par d'autres moyens. Cette option doit rester activée uniquement pour des objectifs spécifiques et conformément aux stratégies de sécurité de votre organisation. Le mode SSH est désactivé par défaut sur le dispositif vRealize Automation. Selon votre configuration vSphere, vous pouvez activer ou désactiver le mode SSH lors du déploiement du modèle OVF (Open Virtualization Format).

Pour opérer un test simple et déterminer si le mode SSH est activé sur une machine, essayez d'ouvrir une connexion via SSH. Si la connexion s'ouvre et que des informations d'identification sont demandées, le mode SSH est activé et disponible pour les connexions.

Compte d'utilisateur racine SSH (Secure Shell)

Les dispositifs VMware n'incluant pas de comptes d'utilisateur préconfigurés, le compte racine peut utiliser le mode SSH pour se connecter directement par défaut. Désactivez le mode SSH en tant qu'utilisateur racine dès que possible.

À des fins de conformité avec les normes de non-répudiation, le serveur SSH de tous les dispositifs renforcés est préconfiguré avec l'entrée du groupe wheel AllowGroups pour limiter l'accès SSH au groupe secondaire (wheel). Pour séparer les tâches, vous pouvez modifier le champ AllowGroups du groupe wheel dans le fichier `/etc/ssh/sshd_config` pour utiliser un autre groupe tel que `sshd`.

Le groupe wheel est activé avec le module `pam_wheel` pour l'accès superutilisateur, ce qui permet aux membres du groupe wheel d'utiliser `su-root`, où le mot de passe racine est requis. La séparation des groupes permet aux utilisateurs d'utiliser le mode SSH pour le dispositif, mais pas d'utiliser le script `su-to-root`. Ne supprimez ni ne modifiez aucune autre entrée dans le champ AllowGroups, afin d'assurer le bon fonctionnement du dispositif. Une fois la modification effectuée, redémarrez le démon SSH en exécutant la commande suivante : `# service sshd restart`.

Activer ou désactiver le protocole SSH (Secure Shell) sur les dispositifs vRealize Automation

Activez le protocole SSH (Secure Shell) sur le dispositif vRealize Automation uniquement à des fins de dépannage. Désactivez le mode SSH sur ces composants au cours des opérations normales de production.

Vous pouvez activer ou désactiver le protocole SSH sur le dispositif vRealize Automation au moyen de la console VAMI (Virtual Appliance Management Interface).

Procédure

- 1 Accédez à la console VAMI (Virtual Appliance Management Interface) de votre dispositif vRealize Automation.
: `https://vRealizeAppliance url:5480`
- 2 Cliquez sur l'onglet **Admin**.
- 3 Cliquez sur le sous-menu **Admin**.
- 4 Activez la case **Activer le service SSH** pour activer le mode SSH ou désactivez-la pour le désactiver.
- 5 Cliquez sur **Enregistrer les paramètres** pour enregistrer les modifications.

Créer un compte d'administrateur local pour Secure Shell

Pour garantir la sécurité, il est recommandé de créer et de configurer des comptes administratifs locaux pour Secure Shell (SSH) sur vos machines hôtes de dispositif virtuel. En outre, supprimez l'accès SSH racine après la création des comptes appropriés.

Créez des comptes administratifs locaux pour SSH ou pour les membres du groupe wheel secondaire, ou pour les deux. Avant de désactiver un accès racine direct, vérifiez que les administrateurs autorisés peuvent accéder à SSH à l'aide d'AllowGroups, et qu'ils peuvent utiliser l'accès su-to-root avec le groupe wheel.

Procédure

- 1 Connectez-vous au dispositif virtuel en tant qu'utilisateur racine et exécutez les commandes suivantes avec le nom d'utilisateur approprié.

```
# useradd -g users <username> -G wheel -m -d /home/username
# passwd username
```

Wheel est le groupe spécifié dans AllowGroups pour les accès SSH. Pour ajouter plusieurs groupes secondaires, utilisez `-G wheel,sshd`.

- 2 Fournissez ensuite un nouveau mot de passe pour l'utilisateur afin d'appliquer la vérification de la complexité du mot de passe.

```
# su -username
# username@hostname:~>passwd
```

Si la complexité du mot de passe est conforme, le mot de passe est mis à jour. Si la complexité du mot de passe n'est pas conforme, le mot de passe d'origine est rétabli et vous devez relancer la commande de mot de passe.

- 3 Pour supprimer une connexion directe à SSH, modifiez le fichier `/etc/ssh/sshd_config` en remplaçant `(#)PermitRootLogin yes` par `PermitRootLogin no`.

Vous pouvez également activer ou désactiver SSH dans l'interface VAMI (Virtual Appliance Management Interface) en activant ou en désactivant la case **Connexion SSH de l'administrateur activée** dans l'onglet **Admin**.

Suivant

Désactivez les connexions directes en tant qu'utilisateur racine. Par défaut, les dispositifs renforcés autorisent une connexion directe à la racine via la console. Une fois que vous avez créé des comptes administratifs pour la non-répudiation et que vous les avez testés pour un accès wheel su-root, désactivez les connexions racines directes en modifiant le fichier `/etc/security` en tant qu'utilisateur racine et en remplaçant l'entrée `tty1` par `console`.

- 1 Ouvrez le fichier `/etc/securetty` dans un éditeur de texte.
- 2 Localisez `tty1` et remplacez-le par `console`.
- 3 Enregistrez le fichier et fermez-le.

Limiter l'accès Secure Shell (SSH)

Dans le cadre de la sécurisation renforcée du système, limitez l'accès Secure Shell (SSH) en configurant le module `tcp_wrappers` de façon appropriée sur toutes les machines hôtes du dispositif virtuel VMware. Gérez également les autorisations de fichiers clés SSH requises sur ces dispositifs.

Tous les dispositifs virtuels VMware incluent le module `tcp_wrappers` pour autoriser les démons pris en charge par `tcp` à contrôler les sous-réseaux de réseau pouvant accéder aux démons compilés avec `LibWrap`. Par défaut, le fichier `/etc/hosts.allow` contient une entrée générique (`Sshd: ALL : ALLOW`) qui donne accès à Secure Shell. Limitez cet accès conformément aux directives de votre organisation.

Procédure

- 1 Ouvrez le fichier `/etc/hosts.allow` sur la machine hôte du dispositif virtuel dans un éditeur de texte.
- 2 Modifiez l'entrée générique dans votre environnement de production, afin d'inclure uniquement les entrées de l'hôte local et du sous-réseau du réseau de gestion pour les opérations sécurisées.

```
sshd:127.0.0.1 : ALLOW
sshd: [::1] : ALLOW
sshd: 10.0.0.0 :ALLOW
```

Dans cet exemple, toutes les connexions d'hôte local ainsi que les connexions réalisées par les clients sur le sous-réseau `10.0.0.0` sont autorisées.

- 3 Ajoutez tous les éléments d'identification des machines nécessaires : nom d'hôte, adresse IP, nom de domaine complet (FQDN) et bouclage, par exemple.
- 4 Enregistrez le fichier et fermez-le.

Renforcer la configuration du serveur Secure Shell

Dans la mesure du possible, tous les dispositifs VMware doivent disposer d'une configuration sécurisée de manière renforcée par défaut. Les utilisateurs peuvent vérifier que leur configuration est suffisamment renforcée en examinant les paramètres des services serveur et client dans la section des options globales du fichier de configuration.

Si possible, limitez l'utilisation du serveur SSH à un sous-réseau de gestion dans le fichier `/etc/hosts.allow`.

Procédure

- 1 Ouvrez le fichier de configuration de serveur `/etc/ssh/sshd_config` sur le dispositif VMware et vérifiez que les paramètres sont corrects.

| Configuration | État |
|----------------------------|--------------------------|
| Protocole démon du serveur | Protocole 2 |
| Chiffrements CBC | aes256-ctr et aes128-ctr |
| Transfert TCP | AllowTCPForwarding no |

| Configuration | État |
|--|---|
| Ports de passerelle serveur | GatewayPorts no |
| Transfert X11 | X11Forwarding no |
| Service SSH | Utilisez le champ AllowGroups pour spécifier une autorisation d'accès pour le groupe. Ajoutez des membres appropriés à ce groupe. |
| Authentification GSSAPI | GSSAPIAuthentication no (si non utilisé) |
| Authentification Keberos | KeberosAuthentication no (si non utilisé) |
| Variables locales (option globale AcceptEnv) | Définissez ces variables sur disabled by commenting out ou sur enabled for LC_* or LANG variables. |
| Configuration de tunnel | PermitTunnel no |
| Sessions réseau | MaxSessions 1 |
| Connexions simultanées de l'utilisateur | Définissez cette valeur sur 1 pour l'utilisateur racine et tout autre utilisateur. Le fichier /etc/security/limits.conf doit également être configuré avec le même paramètre. |
| Vérification en mode strict | StrictModes yes |
| Séparation des privilèges | UsePrivilegeSeparation yes |
| Authentification RSA rhosts | RhostsESAAuthentication no |
| Compression | Compression delayed ou Compression no |
| Code d'authentification de message | MACs hmac-sha1 |
| Limitation d'accès utilisateur | PermitUserEnvironment no |

2 Enregistrez les modifications et fermez le fichier.

Renforcer la configuration du client SSH (Secure Shell)

Dans le cadre de la sécurisation renforcée du système, vérifiez la sécurisation renforcée du client SSH en examinant le fichier de configuration du client SSH sur les machines hôtes du dispositif virtuel, afin de vous assurer que la configuration est conforme aux directives de VMware.

Procédure

- Ouvrez le fichier de configuration du client SSH (/etc/ssh/ssh_config) et vérifiez que les paramètres de la section des options globales sont corrects.

| Configuration | État |
|--|--|
| Protocole du client | Protocole 2 |
| Ports de la passerelle du client | GatewayPorts no |
| Authentification GSSAPI | GSSAPIAuthentication no |
| Variables locales (option globale SendEnv) | Variables LC_* ou LANG uniquement |
| Chiffrements CBC | aes256-ctr et aes128-ctr uniquement |
| Codes d'authentification de message | Utilisés pour l'entrée MACs hmac-sha1 uniquement |

- 2 Enregistrez les modifications et fermez le fichier.

Vérification des autorisations de fichier de clé Secure Shell

Afin de minimiser les risques d'attaques malveillantes, gérez les autorisations de fichier de clé SSH critiques sur les machines hôtes du dispositif virtuel.

Après la configuration ou la mise à jour de votre configuration SSH, vérifiez toujours que les autorisations de fichier de clé SSH suivantes restent inchangées.

- Les fichiers de clé hôte publique situés dans `/etc/ssh/*key.pub` appartiennent à l'utilisateur racine et disposent d'autorisations définies sur 0644 (`-rw-r--r--`).
- Les fichiers de clé hôte privée situés dans `/etc/ssh/*key` appartiennent à l'utilisateur racine et disposent d'autorisations définies sur 0600 (`-rw-----`).

Vérifier les autorisations de fichier de clés SSH

Assurez-vous que les autorisations SSH sont appliquées aux fichiers de clés publiques et de clés privées.

Procédure

- 1 Vérifiez les fichiers de clés publiques SSH en exécutant la commande suivante : `ls -l /etc/ssh/*key.pub`
- 2 Assurez-vous que le propriétaire est de type racine, que le propriétaire du groupe est de type racine et que les autorisations des fichiers sont définies sur 0644 (`-rw-r--r--`).
- 3 Corrigez les problèmes en exécutant les commandes suivantes.
`chown root /etc/ssh/*key.pub`
`chgrp root /etc/ssh/*key.pub`
`chmod 644 /etc/ssh/*key.pub`
- 4 Vérifiez les fichiers de clés privées SSH en exécutant la commande suivante : `ls -l /etc/ssh/*key`
- 5 Corrigez les problèmes en exécutant les commandes suivantes.
`chown root /etc/ssh/*key`
`chgrp root /etc/ssh/*key`
`chmod 600 /etc/ssh/*key`

Modifier l'utilisateur de l'interface de gestion de dispositif virtuel

Vous pouvez ajouter et supprimer des utilisateurs sur l'interface de gestion de dispositif virtuel pour créer le niveau approprié de sécurité.

Le compte d'utilisateur racine pour l'interface de gestion de dispositif virtuel utilise PAM pour l'authentification, donc les niveaux de coupure définis par PAM s'appliquent également. Si vous n'avez pas correctement isolé l'interface de gestion de dispositif virtuel, un verrouillage du compte racine système peut se produire si un pirate tente de forcer la connexion. En outre, lorsque le compte racine est considéré comme insuffisant pour fournir la non-répudiation par plusieurs personnes de votre organisation, vous pouvez décider de modifier l'utilisateur Admin de l'interface de gestion.

Prérequis

Procédure

- 1 Exécutez la commande suivante pour créer un nouvel utilisateur et l'ajouter au groupe d'interface de gestion de dispositif virtuel.

```
useradd -G vami,root user
```

- 2 Créez un mot de passe pour l'utilisateur.

```
passwd user
```

- 3 (Facultatif) Exécutez la commande suivante pour désactiver l'accès racine à l'interface de gestion de dispositif virtuel.

```
usermod -R vami root
```

Remarque La désactivation d'un accès racine à l'interface de gestion de dispositif virtuel désactive également la possibilité de mettre à jour le mot de passe de l'administrateur, ou le mot de passe racine, dans l'onglet Admin.

Définir l'authentification du chargeur de démarrage

Pour fournir un niveau de sécurité adapté, configurez l'authentification du chargeur de démarrage sur vos dispositifs virtuels VMware.

Si le chargeur de démarrage du système ne requiert aucune authentification, les utilisateurs ayant accès à la console système peuvent modifier la configuration de démarrage du système ou démarrer le système en mode mono-utilisateur unique ou en mode de maintenance, ce qui peut entraîner un déni de service ou un accès système non autorisé. Étant donné que l'authentification du chargeur de démarrage n'est pas définie par défaut sur les dispositifs virtuels VMware, vous devez créer un mot de passe GRUB pour la configurer.

Procédure

- 1 Vérifiez si un mot de passe de démarrage existe en localisant la ligne `password --md5 <password-hash>` dans le fichier `/boot/grub/menu.lst` sur les dispositifs virtuels.
- 2 S'il n'existe aucun mot de passe, exécutez la commande `# /usr/sbin/grub-md5-crypt` sur votre dispositif virtuel.

Un mot de passe MD5 est généré et la commande fournit la sortie de hachage md5.

- 3 Ajoutez le mot de passe au fichier `menu.lst` en exécutant la commande `# password --md5 <hash from grub-md5-crypt>`.

Configurer NTP

Pour les sources d'heure critiques, désactivez la synchronisation date/heure de l'hôte et utilisez le protocole NTP (Network Time Protocol) sur le dispositif vRealize Automation.

Le démon NTP sur le dispositif vRealize Automation fournit des services de synchronisation d'heure. Le protocole NTP est désactivé par défaut. Vous devez donc le configurer manuellement. Si possible, utilisez NTP dans des environnements de production pour effectuer le suivi des actions des utilisateurs et pour détecter d'éventuelles attaques malveillantes et intrusions au moyen d'un audit et d'une journalisation détaillés. Pour plus d'informations sur les avis de sécurité NTP, consultez le site Web NTP.

Le fichier de configuration NTP est situé dans le dossier `/etc/` sur chaque dispositif. Vous pouvez activer le service NTP pour le dispositif vRealize Automation et ajouter des serveurs de temps dans l'onglet **Admin** de l'interface VAMI.

Procédure

- 1 Ouvrez le fichier de configuration `/etc/ntp.conf` sur la machine hôte de votre dispositif virtuel dans un éditeur de texte.
- 2 Définissez la propriété de fichier sur **root:root**.
- 3 Définissez les autorisations sur **0640**.
- 4 Pour réduire les risques d'une attaque par déni de service avec technique d'amplification sur le service NTP, ouvrez le fichier `/etc/ntp.conf` et assurez-vous que les lignes `restrict` figurent dans le fichier.

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

- 5 Enregistrez les modifications et fermez les fichiers.

Configuration du protocole TLS pour les données en transit du dispositif vRealize Automation

Assurez-vous que votre déploiement vRealize Automation utilise des protocoles TLS forts afin de sécuriser les canaux de transmission pour les composants du dispositif vRealize Automation.

Pour ne pas compromettre les performances, le protocole TLS n'est pas activé pour les connexions localhost entre certains services d'application. Lorsqu'une défense poussée est requise, activez TLS sur toutes les communications localhost.

Important Si vous arrêtez TLS sur l'équilibrage de charge, désactivez les protocoles non sécurisés tels que SSLv2, SSLv3 et TLS 1.0 sur tous les équilibres de charge.

Activer TLS sur une configuration localhost

Par défaut, certaines communications localhost n'utilisent pas TLS. Vous pouvez activer TLS sur l'ensemble des connexions localhost pour assurer une sécurité renforcée.

Procédure

- 1 Connectez-vous au dispositif vRealize Automation au moyen du mode SSH.
- 2 Définissez des autorisations pour le keystore vCAC en exécutant les commandes suivantes.

```
usermod -A vco,coredump,pivotal vco
chown vcac.pivotal /etc/vcac/vcac.keystore
chmod 640 /etc/vcac/vcac.keystore
```

- 3 Mettez à jour la configuration de HAProxy.

- a Recherchez les lignes contenant la chaîne suivante :

```
server local 127.0.0.1... et ajoutez la ligne suivante à la fin de ces lignes : ssl verify
none
```

Cette section contient également d'autres lignes :

| | |
|--------------------|---------------------|
| backend-horizon | backend-vro |
| backend-vra | backend-artifactory |
| backend-vra-health | |

- b Pour backend-horizon, remplacez le port 8080 par 8443.

- 4 Obtenez le mot de passe de keystorePass.

- a Recherchez la propriété `certificate.store.password` dans le fichier `/etc/vcac/security.properties`.

Par exemple, `certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`.

- b Déchiffrez la valeur au moyen de la commande suivante :

```
vcac-config prop-util -d --p VALUE
```

Par exemple, `vcac-config prop-util -d --p s2enc~iom0GXATG+RB8ff7Wdm4Bg==`.

5 Configurez le service vRealize Automation.

- a Ouvrez le fichier `/etc/vcac/server.xml`.
- b Ajoutez l'attribut suivant à la balise de connecteur, en remplaçant `certificate.store.password` par la valeur du mot de passe de magasin de certificats figurant dans `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache"
keystorePass="certificate.store.password"
```

6 Configurez le service vRealize Orchestrator.

- a Ouvrez le fichier `/etc/vco/app/server.xml`.
- b Ajoutez l'attribut suivant à la balise de connecteur, en remplaçant `certificate.store.password` par la valeur du mot de passe de magasin de certificats figurant dans `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache"
keystorePass="certificate.store.password"
```

7 Redémarrez les services vRealize Orchestrator, vRealize Automation et HAProxy.

```
service vcac-server restart
service vco-server restart
service haproxy restart
```

Remarque Si le serveur vCO ne redémarre pas, redémarrez l'ordinateur hôte.

8 Configurez l'interface VAMI (Virtual Appliance Management Interface).

- a Ouvrez le fichier `/opt/vmware/share/htdocs/service/café-services/services.py`.
- b Remplacez la ligne `conn = httpLib.HTTP()` par `conn = httpLib.HTTPS()` pour renforcer la sécurité.

Activer la conformité FIPS (Federal Information Processing Standard) 140-2

Le dispositif vRealize Automation utilise désormais la version certifiée Federal Information Processing Standard (FIPS) 140-2 d'OpenSSL pour les données en transit via TLS sur tout le trafic réseau, entrant et sortant.

Vous pouvez activer ou désactiver le mode FIPS dans l'interface de gestion du dispositif vRealize Automation. Vous pouvez également configurer le mode FIPS à partir de la ligne de commande lorsque vous êtes connecté en tant qu'utilisateur racine, au moyen des commandes suivantes :

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Lorsque le mode FIPS est activé, le trafic réseau entrant et sortant du dispositif vRealize Automation sur le port 443 applique le chiffrement conforme à la norme FIPS 140-2. Quel que soit le paramètre FIPS, vRealize Automation applique la norme AES-256 pour protéger les données sécurisées stockées sur le dispositif vRealize Automation.

Remarque Actuellement, vRealize Automation assure une conformité FIPS partielle, car certains composants internes n'utilisent pas encore de modules de chiffrement certifiés. Si des modules certifiés n'ont pas encore été implémentés, le chiffrement AES-256 est utilisé par tous les algorithmes de chiffrement.

Remarque La procédure suivante fait redémarrer la machine physique lorsque vous modifiez la configuration.

Procédure

- 1 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https:// vrealize-automation-appliance-FQDN:5480`
- 2 Sélectionnez **Paramètres vRA > Paramètres de l'hôte**.
- 3 Cliquez sur le bouton situé sous l'en-tête Actions dans la partie supérieure droite pour activer ou désactiver le mode FIPS.
- 4 Cliquez sur **Oui** pour redémarrer le dispositif vRealize Automation

Vérifier que les protocoles SSLv3, TLS 1.0 et TLS 1.1 sont désactivés

Dans le cadre du processus de sécurisation renforcée, assurez-vous que le dispositif vRealize Automation déployé utilise des canaux de transmission sécurisés.

Prérequis

Effectuez [Activer TLS sur une configuration localhost](#).

Procédure

- 1 Vérifiez que les protocoles TLS 1.1, TLS 1.0 et SSLv3 sont désactivés dans les gestionnaires https HAProxy sur dispositif vRealize Automation.

| Fichier à examiner | Vérifier la présence de ces éléments | Sur la ligne appropriée, comme indiqué |
|---------------------------------------|--|---|
| /etc/haproxy/conf.d/20-vcac.cfg | no-sslv3 no-tls10 no-tls11 force-tls12 | bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tls10 no-tls11 |
| /etc/haproxy/conf.d/30-vro-config.cfg | no-sslv3 no-tls10 no-tls11 force-tls12 | bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tls10 no-tls11 |

- 2 Redémarrez le service.

```
service haproxy restart
```

- 3 Ouvrez le fichier /opt/vmware/etc/lighttpd/lighttpd.conf et vérifiez que les entrées désactivées correctes s'affichent.

Remarque Aucune directive n'impose la désactivation de TLS 1.0 ou TLS 1.1 dans Lighttpd. Vous pouvez atténuer partiellement la restriction d'utilisation de TLS 1.0 et TLS 1.1 en appliquant OpenSSL afin de ne pas utiliser les suites de chiffrement de TLS 1.0 et TLS 1.1.

```
ssl.use-ssl2 = "disable"
ssl.use-ssl3 = "disable"
```

- 4 Vérifiez que les protocoles SSLv3, TLS 1.0 et TLS 1.1 sont désactivés pour le proxy de la console sur dispositif vRealize Automation.

- a Modifiez le fichier /etc/vcac/security.properties en ajoutant ou en modifiant la ligne suivante :

```
consoleproxy.ssl.server.protocols = TLSv1.2
```

- b Redémarrez le serveur en exécutant la commande suivante :

```
service vcac-server restart
```

- 5 Vérifiez que les protocoles SSLv3, TLS 1.0 et TLS 1.1 sont désactivés pour le service vCO.
 - a Localisez la balise <Connector> dans le fichier /etc/vco/app-server/server.xml et ajoutez l'attribut suivant :

```
sslEnabledProtocols = "TLSv1.2"
```

- b Redémarrez le service vCO en exécutant la commande suivante.

```
service vco-server restart
```

- 6 Vérifiez que les protocoles SSLv3, TLS 1.0 et TLS 1.1 sont désactivés pour le service vRealize Automation.
 - a Ajoutez les attributs suivants à la balise <Connector> dans le fichier /etc/vcac/server.xml.

```
sslEnabledProtocols = "TLSv1.2"
```

- b Redémarrez le service vRealize Automation en exécutant la commande suivante :

```
service vcac-server restart
```

- 7 Vérifiez que les protocoles SSLv3, TLS 1.0 et TLS 1.1 sont désactivés pour RabbitMQ.

Ouvrez le fichier /etc/rabbitmq/rabbitmq.config et vérifiez que {versions, ['tlsv1.2', 'tlsv1.1']} apparaissent dans les sections ssl et ssl_options.

```
[
  {ssl, [
    {versions, ['tlsv1.2', 'tlsv1.1']},
    {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
  {rabbit, [
    {tcp_listeners, [{"127.0.0.1", 5672}]},
    {frame_max, 262144},
    {ssl_listeners, [5671]},
    {ssl_options, [
      {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
      {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
      {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
      {versions, ['tlsv1.2', 'tlsv1.1']},
      {ciphers, ["AES256-SHA", "AES128-SHA"]},
      {verify, verify_peer},
      {fail_if_no_peer_cert, false}
    ]},
    {mnesia_table_loading_timeout, 600000},
    {cluster_partition_handling, autoheal},
    {heartbeat, 600}
  ]},
  {kernel, [{net_ticktime, 120}]}
].
```

- 8 Redémarrez le serveur RabbitMQ.

```
# service rabbitmq-server restart
```

- 9 Vérifiez que les protocoles SSLv3, TLS 1.0 et TLS 1.1 sont désactivés pour le service vIDM.

Ouvrez le fichier `opt/vmware/horizon/workspace/conf/server.xml` pour chaque instance du connecteur contenant `SSLEnabled="true"` et assurez-vous que la ligne suivante est présente.

```
sslEnabledProtocols="TLSv1.2"
```

Désactiver TLS 1.0

Désactivez TLS 1.0 sur les composants vRealize Automation concernés.

Aucune directive n'impose la désactivation de TLS 1.0 dans Lighttpd. La limitation portant sur TLS 1.0 peut être partiellement atténuée en s'assurant qu'OpenSSL n'utilise pas de suites de chiffrement TLS 1.0, comme décrit dans l'étape 2 ci-dessous.

Procédure

- 1 Désactivez TLS 1.0 dans le gestionnaire https HAProxy sur le dispositif vRealize Automation.
 - a Ajoutez `no-tls10` à la fin de l'entrée suivante dans le fichier `/etc/haproxy/conf.d/20-vcac.cfg`.


```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers TLSv1+HIGH:!aNULL:!eNULL:!3DES:!RC4:!CAMELLIA:!DH:!kECDHE:@STRENGTH no-ssl3 no-tls10
```
 - b Ajoutez `no-tls10` à la fin de l'entrée suivante dans le fichier `/etc/haproxy/conf.d/30-vro-config.cfg`.


```
bind :8283 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers TLSv1+HIGH:!aNULL:!eNULL:!3DES:!RC4:!CAMELLIA:!DH:!kECDHE:@STRENGTH no-ssl3 no-tls10
```

Remarque Pour réactiver TLS 1.0, supprimez `no-tls10` de la directive de liaison.

- 2 Dans Lighttpd, vérifiez qu'OpenSSL n'utilise pas de suites de chiffrement TLS 1.0.
 - a Modifiez la ligne `ssl.cipher-list` dans le fichier `/opt/vmware/etc/lighttpd/lighttpd.conf` comme suit.

```
ssl.cipher-list = "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256"
```

- b Redémarrez lighttpd à l'aide de la commande suivante :


```
service vami-lighttpd restart
```

- 3 Désactivez TLS 1.0 pour le proxy de la console sur le dispositif vRealize Automation.
 - a Ajoutez ou modifiez la ligne suivante dans le fichier `/etc/vcac/security.properties`.
`consoleproxy.ssl.server.protocols = TLSv1.2, TLSv1.1`
 - b Redémarrez le serveur en exécutant la commande suivante :
`service vcac-server restart`

Remarque Pour réactiver TLS 1.0, ajoutez TLSv1 comme suit, puis redémarrez le service vcac-server :

```
consoleproxy.ssl.server.protocols = TLSv1.2,TLSv1.1, TLSv1
```

- 4 Désactivez TLS 1.0 pour le service vCO.
 - a Recherchez la balise `<Connector>` dans le fichier `/etc/vco/app-server/server.xml` et ajoutez-y l'attribut suivant :
`sslEnabledProtocols = "TLSv1.1,TLSv1.2"`
 - b Redémarrez le service vCO en exécutant la commande suivante :
`service vco-server restart`
- 5 Désactivez TLS 1.0 pour le service vRealize Automation.
 - a Localisez la balise `<Connector>` dans le fichier `/etc/vcac/server.xml` et ajoutez-y l'attribut suivant :
`sslEnabledProtocols = "TLSv1.1,TLSv1.2"`
 - b Redémarrez le service vRealize Automation en exécutant les commandes suivantes.
`service vcac-server restart`

Remarque Pour réactiver TLS 1.0, ajoutez TLSv1 à `sslEnabledProtocols`. Par exemple, `sslEnabledProtocols = "TLSv1.1,TLSv1.2,TLSv1"`.

6 Désactivez TLS 1.0 pour RabbitMQ.

- a Ouvrez le fichier `/etc/rabbitmq/rabbitmq.config` et vérifiez que `tlsv1.2` et `tlsv1.1` sont ajoutés aux sections `ssl` et `ssl_options` comme indiqué dans l'exemple suivant.

```
[
  {ssl, [
    {versions, ['tlsv1.2', 'tlsv1.1']},
    {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
  {rabbit, [
    {tcp_listeners, [{"127.0.0.1", 5672}]},
    {frame_max, 262144},
    {ssl_listeners, [5671]},
    {ssl_options, [
      {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
      {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
      {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
      {versions, ['tlsv1.2', 'tlsv1.1']},
      {ciphers, ["AES256-SHA", "AES128-SHA"]},
      {verify, verify_peer},
      {fail_if_no_peer_cert, false}
    ]},
    {mnesia_table_loading_timeout, 600000},
    {cluster_partition_handling, autoheal},
    {heartbeat, 600}
  ]},
  {kernel, [{net_ticktime, 120}]}
].
```

- b Redémarrez le serveur RabbitMQ en exécutant la commande suivante :

```
# service rabbitmq-server restart
```

Configuration des suites de chiffrement TLS pour les composants vRealize Automation

Pour obtenir une sécurité maximale, vous devez configurer les composants vRealize Automation pour utiliser des chiffrements forts.

Le chiffrement négocié entre le serveur et le navigateur détermine la force du chiffrement utilisé dans une session TLS.

Pour vous assurer que seuls des chiffrements forts sont sélectionnés, désactivez les chiffrements faibles dans les composants vRealize Automation . Configurez le serveur pour prendre en charge uniquement les chiffrements forts et pour utiliser des clés suffisamment grandes. En outre, configurez tous les chiffrements dans l'ordre approprié.

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, aNULL ou eNULL. Désactivez également l'échange de clés anonyme Diffie-Hellman (ADH), les chiffrements de niveau exportation (EXP, chiffrements contenant des algorithmes DES), les tailles de clé inférieures à 128 bits pour le chiffrement du trafic de la charge utile, l'utilisation de la fonction MD5 comme mécanisme de hachage pour le trafic de charge utile, les suites de chiffrement IDEA et les suites de chiffrement RC4. Assurez-vous également que les suites de chiffrement utilisant l'échange de clés Diffie-Hellman (DHE) sont désactivées.

Désactiver les chiffrements faibles dans HAProxy

Vérifiez les chiffrements du service HA proxy du dispositif vRealize Automation par rapport à la liste de chiffrements acceptables et désactivez tous ceux qui sont considérés comme faibles.

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, aNULL ou eNULL. Désactivez également l'échange de clés anonyme Diffie-Hellman (ADH), les chiffrements de niveau exportation (EXP, chiffrements contenant des algorithmes DES), les tailles de clé inférieures à 128 bits pour le chiffrement du trafic de la charge utile, l'utilisation de la fonction MD5 comme mécanisme de hachage pour le trafic de charge utile, les suites de chiffrement IDEA et les suites de chiffrement RC4.

Procédure

- 1 Vérifiez les entrées de chiffrement du fichier `/etc/haproxy/conf.d/20-vcac.cfg` de la directive de liaison et désactivez ceux qui sont considérés comme faibles.

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers TLSv1+HIGH:!aNULL:!eNULL:!3DES:!RC4:!CAMELLIA:!DH:!kECDHE:@STRENGTH no-ssl3 no-tls10
```

- 2 Vérifiez les entrées de chiffrement du fichier `/etc/haproxy/conf.d/30-vro-config.cfg` de la directive de liaison et désactivez ceux qui sont considérés comme faibles.

```
bind :8283 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers TLSv1+HIGH:!aNULL:!eNULL:!3DES:!RC4:!CAMELLIA:!DH:!kECDHE:@STRENGTH no-ssl3 no-tls10
```

Désactiver les chiffrements faibles dans le service de proxy de console du dispositif vRealize Automation

Vérifiez les chiffrements du service de proxy de console du dispositif vRealize Automation par rapport à la liste de chiffrements acceptables et désactivez tous ceux qui sont considérés comme faibles.

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, aNULL ou eNULL. Désactivez également l'échange de clés anonyme Diffie-Hellman (ADH), les chiffrements de niveau exportation (EXP, chiffrements contenant des algorithmes DES), les tailles de clé inférieures à 128 bits pour le chiffrement du trafic de la charge utile, l'utilisation de la fonction MD5 comme mécanisme de hachage pour le trafic de charge utile, les suites de chiffrement IDEA et les suites de chiffrement RC4.

Procédure

- 1 Ouvrez le fichier `/etc/vcac/security.properties` dans un éditeur de texte.

- 2 Ajoutez une ligne dans le fichier pour désactiver les suites de chiffrement indésirables.

Utilisez une variante de la ligne suivante :

```
consoleproxy.ssl.ciphers.disallowed=cipher_suite_1, cipher_suite_2,etc
```

Par exemple, pour désactiver les suites de chiffrement AES 128 et AES 256, ajoutez la ligne suivante :

```
consoleproxy.ssl.ciphers.disallowed=TLS_DH_DSS_WITH_AES_128_CBC_SHA,
TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

- 3 Redémarrez le serveur à l'aide de la commande suivante.

```
service vcac-server restart
```

Désactiver les chiffrements faibles dans le service vCO de dispositif vRealize Automation

Vérifiez les chiffrements du service vCO de dispositif vRealize Automation par rapport à la liste de chiffrements acceptables et désactivez tous ceux qui sont considérés comme faibles.

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, aNULL ou eNULL. Désactivez également l'échange de clés anonyme Diffie-Hellman (ADH), les chiffrements de niveau exportation (EXP, chiffrements contenant des algorithmes DES), les tailles de clé inférieures à 128 bits pour le chiffrement du trafic de la charge utile, l'utilisation de la fonction MD5 comme mécanisme de hachage pour le trafic de charge utile, les suites de chiffrement IDEA et les suites de chiffrement RC4.

Procédure

- 1 Recherchez la balise <Connector> dans le fichier /etc/vco/app-server/server.xml.
- 2 Modifiez ou ajoutez l'attribut de chiffrement pour utiliser les suites de chiffrement souhaitées.

Reportez-vous à l'exemple suivant :

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```

Désactiver les chiffrements faibles dans le service RabbitMQ de dispositif vRealize Automation

Vérifiez le chiffrement du service RabbitMQ de dispositif vRealize Automation par rapport à la liste de chiffrements acceptables et désactivez tous ceux qui sont considérés comme faibles.

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, aNULL ou eNULL. Désactivez également l'échange de clés anonyme Diffie-Hellman (ADH), les chiffrements de niveau exportation (EXP, chiffrements contenant des algorithmes DES), les tailles de clé inférieures à 128 bits pour le chiffrement du trafic de la charge utile, l'utilisation de la fonction MD5 comme mécanisme de hachage pour le trafic de charge utile, les suites de chiffrement IDEA et les suites de chiffrement RC4.

Procédure

- 1 Évaluez les suites de chiffrement prises en charge en exécutant la commande

```
# /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites()'.
```

Les chiffrements renvoyés dans l'exemple suivant représentent uniquement les chiffrements pris en charge. Le serveur RabbitMQ n'utilise, ni n'annonce ces chiffrements, sauf si la configuration spécifiée dans le fichier `rabbitmq.config` l'autorise.

```
[ "ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-SHA384",
  "ECDHE-ECDSA-AES256-SHA384", "ECDHE-RSA-AES256-SHA384",
  "ECDH-ECDSA-AES256-GCM-SHA384", "ECDH-RSA-AES256-GCM-SHA384",
  "ECDH-ECDSA-AES256-SHA384", "ECDH-RSA-AES256-SHA384",
  "DHE-RSA-AES256-GCM-SHA384", "DHE-DSS-AES256-GCM-SHA384",
  "DHE-RSA-AES256-SHA256", "DHE-DSS-AES256-SHA256", "AES256-GCM-SHA384",
  "AES256-SHA256", "ECDHE-ECDSA-AES128-GCM-SHA256",
  "ECDHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES128-SHA256",
  "ECDHE-RSA-AES128-SHA256", "ECDH-ECDSA-AES128-GCM-SHA256",
  "ECDH-RSA-AES128-GCM-SHA256", "ECDH-ECDSA-AES128-SHA256",
  "ECDH-RSA-AES128-SHA256", "DHE-RSA-AES128-GCM-SHA256",
  "DHE-DSS-AES128-GCM-SHA256", "DHE-RSA-AES128-SHA256", "DHE-DSS-AES128-SHA256",
  "AES128-GCM-SHA256", "AES128-SHA256", "ECDHE-ECDSA-AES256-SHA",
  "ECDHE-RSA-AES256-SHA", "DHE-RSA-AES256-SHA", "DHE-DSS-AES256-SHA",
  "ECDH-ECDSA-AES256-SHA", "ECDH-RSA-AES256-SHA", "AES256-SHA",
  "ECDHE-ECDSA-DES-CBC3-SHA", "ECDHE-RSA-DES-CBC3-SHA", "EDH-RSA-DES-CBC3-SHA",
  "EDH-DSS-DES-CBC3-SHA", "ECDH-ECDSA-DES-CBC3-SHA", "ECDH-RSA-DES-CBC3-SHA",
  "DES-CBC3-SHA", "ECDHE-ECDSA-AES128-SHA", "ECDHE-RSA-AES128-SHA",
  "DHE-RSA-AES128-SHA", "DHE-DSS-AES128-SHA", "ECDH-ECDSA-AES128-SHA",
  "ECDH-RSA-AES128-SHA", "AES128-SHA"]
```

- 2 Sélectionnez les chiffrements pris en charge et conformes aux exigences de sécurité de votre organisation.

Par exemple, pour autoriser uniquement ECDHE-ECDSA-AES128-GCM-SHA256 & ECDHE-ECDSA-AES256-GCM-SHA384, examinez le fichier `/etc/rabbitmq/rabbitmq.config` et ajoutez la ligne suivante à `ssl` et `ssl_options`.

```
{ciphers, ["ECDHE-ECDSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-GCM-SHA384"]}
```

- 3 Redémarrez le serveur RabbitMQ à l'aide de la commande suivante.

```
service rabbitmq-server restart
```

Vérification de la sécurité des données au repos

Vérifiez la sécurité des utilisateurs et des comptes de base de données utilisés avec vRealize Automation.

Utilisateur Postgres

Le compte d'utilisateur Postgres Linux est lié au rôle de compte de superutilisateur de la base de données Postgres. Ce compte est verrouillé par défaut. Il s'agit de la configuration la plus sécurisée pour cet utilisateur, car il est accessible uniquement à partir du compte d'utilisateur racine. Ne déverrouillez pas ce compte d'utilisateur.

Rôles de compte d'utilisateur de base de données

Les rôles par défaut des comptes d'utilisateur Postgres ne doivent pas être utilisés en dehors de les fonctionnalités de l'application. Pour prendre en charge l'examen d'une base de données qui n'est pas celle par défaut ou les activités de rapport, vous devez créer un compte supplémentaire et le protéger correctement par un mot de passe.

Dans la ligne de commande, exécutez le script suivant :

```
vcac-vami add-db-user newUsername newPassword
```

Cela ajoutera un nouvel utilisateur et un mot de passe fourni par l'utilisateur.

Remarque Ce script doit être exécuté sur la base de données Postgres principale si une configuration Postgres HA maître/esclave a été définie.

Configurer l'authentification du client PostgreSQL

Assurez-vous que l'authentification d'approbation locale n'est pas configurée dans la base de données PostgreSQL du dispositif vRealize Automation. En effet, cette configuration permet à tout utilisateur local, y compris le superutilisateur de la base de données, de se connecter en tant qu'utilisateur PostgreSQL sans mot de passe.

Remarque Le compte de superutilisateur Postgres doit rester un compte d'approbation locale.

La méthode d'authentification md5 est recommandée, car elle envoie des mots de passe chiffrés.

Les paramètres de configuration de l'authentification du client résident dans le fichier `/storage/db/pgdata/pg_hba.conf`.

| # | TYPE | DATABASE | USER | ADDRESS | METHOD |
|--|------|----------|----------|--------------|--------|
| # "local" is for Unix domain socket connections only | | | | | |
| local | all | | postgres | | trust |
| # IPv4 local connections: | | | | | |
| #host | all | | all | 127.0.0.1/32 | md5 |
| hostssl | all | | all | 127.0.0.1/32 | md5 |

```
# IPv6 local connections:
#host      all             all             ::1/128         md5
hostssl    all             all             ::1/128         md5

# Allow remote connections for VCAC user.
#host      vcac             vcac            0.0.0.0/0       md5
hostssl    vcac             vcac            0.0.0.0/0       md5
hostssl    vcac             vcac            ::0/0           md5
# Allow remote connections for VCAC replication user.
#host      vcac             vcac_replication 0.0.0.0/0       md5
hostssl    vcac             vcac_replication 0.0.0.0/0       md5
hostssl    vcac             vcac_replication ::0/0           md5
# Allow replication connections by a user with the replication privilege.
#host      replication      vcac_replication 0.0.0.0/0       md5
hostssl    replication      vcac_replication 0.0.0.0/0       md5
hostssl    replication      vcac_replication ::0/0           md5
```

Si vous modifiez le fichier `pg_hba.conf`, vous devez redémarrer le serveur Postgres en exécutant les commandes suivantes afin que les modifications soient appliquées.

```
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

Configurer les ressources d'application de vRealize Automation

Vérifiez les ressources d'application de vRealize Automation et limitez les autorisations de fichier.

Procédure

- 1 Exécutez la commande suivante pour vérifier que les fichiers incluant des bits SUID et GUID sont bien définis.

```
find / -path /proc -prune -o -type f -perm +6000 -ls
```

La liste suivante doit s'afficher.

```
2197357  24 -rwsr-xr-x  1 polkituser root      23176 Mar 31  2015 /usr/lib/PolicyKit/polkit-
set-default-helper
2197354  16 -rwxr-sr-x  1 root    polkituser  14856 Mar 31  2015 /usr/lib/PolicyKit/polkit-
read-auth-helper
2197353  12 -rwsr-x---  1 root    polkituser  10744 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper-pam
2197352  20 -rwxr-sr-x  1 root    polkituser  19208 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper
2197351  20 -rwxr-sr-x  1 root    polkituser  19008 Mar 31  2015 /usr/lib/PolicyKit/polkit-
explicit-grant-helper
2197356  24 -rwxr-sr-x  1 root    polkituser  23160 Mar 31  2015 /usr/lib/PolicyKit/polkit-
revoke-helper
2188203  460 -rws--x--x  1 root    root      465364 Apr 21 22:38 /usr/lib64/ssh/ssh-keysign
2138858  12 -rwxr-sr-x  1 root    tty       10680 May 10  2010 /usr/sbin/utempter
2142482  144 -rwsr-xr-x  1 root    root     142890 Sep 15  2015 /usr/bin/passwd
2142477  164 -rwsr-xr-x  1 root    shadow   161782 Sep 15  2015 /usr/bin/chage
```

| | | | | | | | | | |
|---------|-----|------------|---|------|------------|--------|--------|------|---|
| 2142467 | 156 | -rwsr-xr-x | 1 | root | shadow | 152850 | Sep 15 | 2015 | /usr/bin/chfn |
| 1458298 | 364 | -rwsr-xr-x | 1 | root | root | 365787 | Jul 22 | 2015 | /usr/bin/sudo |
| 2142481 | 64 | -rwsr-xr-x | 1 | root | root | 57776 | Sep 15 | 2015 | /usr/bin/newgrp |
| 1458249 | 40 | -rwsr-x--- | 1 | root | trusted | 40432 | Mar 18 | 2015 | /usr/bin/crontab |
| 2142478 | 148 | -rwsr-xr-x | 1 | root | shadow | 146459 | Sep 15 | 2015 | /usr/bin/chsh |
| 2142480 | 156 | -rwsr-xr-x | 1 | root | shadow | 152387 | Sep 15 | 2015 | /usr/bin/gpasswd |
| 2142479 | 48 | -rwsr-xr-x | 1 | root | shadow | 46967 | Sep 15 | 2015 | /usr/bin/expiry |
| 311484 | 48 | -rwsr-x--- | 1 | root | messagebus | 47912 | Sep 16 | 2014 | /lib64/dbus-1/dbus-daemon-launch-helper |
| 876574 | 36 | -rwsr-xr-x | 1 | root | shadow | 35688 | Apr 10 | 2014 | /sbin/unix_chkpwd |
| 876648 | 12 | -rwsr-xr-x | 1 | root | shadow | 10736 | Dec 16 | 2011 | /sbin/unix2_chkpwd |
| 49308 | 68 | -rwsr-xr-x | 1 | root | root | 63376 | May 27 | 2015 | /opt/likewise/bin/ksu |
| 1130552 | 40 | -rwsr-xr-x | 1 | root | root | 40016 | Apr 16 | 2015 | /bin/su |
| 1130511 | 40 | -rwsr-xr-x | 1 | root | root | 40048 | Apr 15 | 2011 | /bin/ping |
| 1130600 | 100 | -rwsr-xr-x | 1 | root | root | 94808 | Mar 11 | 2015 | /bin/mount |
| 1130601 | 72 | -rwsr-xr-x | 1 | root | root | 69240 | Mar 11 | 2015 | /bin/umount |
| 1130512 | 36 | -rwsr-xr-x | 1 | root | root | 35792 | Apr 15 | 2011 | /bin/ping6 |
| 2012 | | | | | | | | | /lib64/dbus-1/dbus-daemon-launch-helper |

- Exécutez la commande suivante pour vérifier que tous les fichiers du dispositif virtuel ont un propriétaire.

```
find / -path /proc -prune -o -nouser -o -nogroup
```

- Vérifiez les autorisations de tous les fichiers du dispositif virtuel pour vous assurer qu'aucun d'entre eux ne peut faire l'objet d'une écriture par tout le monde en exécutant la commande suivante.

```
find / -name ".*" -type f -perm -a+w | xargs ls -ldb
```

- Exécutez la commande suivante pour vérifier que seul l'utilisateur vcac possède les fichiers appropriés.

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" | egrep -v -e "*/vmware-vcac/*"
```

Si aucun résultat n'apparaît, tous les fichiers corrects appartiennent uniquement à l'utilisateur vcac.

- Vérifiez que les fichiers suivants sont accessibles en écriture uniquement par l'utilisateur vcac.

```
/etc/vcac/vcac/security.properties
```

```
/etc/vcac/vcac/solution-users.properties
```

```
/etc/vcac/vcac/sso-admin.properties
```

```
/etc/vcac/vcac/vcac.keystore
```

```
/etc/vcac/vcac/vcac.properties
```

Vérifiez également les fichiers suivants et leurs sous-répertoires.

```
/var/log/vcac/*
```

```
/var/lib/vcac/*
```

```
/var/cache/vcac/*
```

- 6 Vérifiez que seul l'utilisateur vcac ou racine peut lire les fichiers corrects dans les répertoires et sous-répertoires suivants.

```
/etc/vcac/*
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

- 7 Vérifiez que les fichiers corrects appartiennent uniquement à l'utilisateur racine ou vco, comme illustré dans les répertoires et sous-répertoires suivants.

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
/var/cache/vco/*
```

- 8 Vérifiez que les fichiers corrects sont accessibles en écriture uniquement par l'utilisateur racine ou vco, comme illustré dans les répertoires suivants et leurs sous-répertoires.

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
/var/cache/vco/*
```

- 9 Vérifiez que les fichiers corrects sont accessibles en lecture seule par l'utilisateur racine ou vco, comme illustré dans les répertoires et sous-répertoires suivants.

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
/var/cache/vco/*
```

Personnalisation de la configuration du proxy de la console

Vous pouvez personnaliser la configuration de la console distante de vRealize Automation afin de simplifier le dépannage et les méthodes d'organisation.

Lorsque vous installez, configurez ou maintenez vRealize Automation, vous pouvez modifier certains paramètres pour activer le dépannage et le débogage de votre installation. Répertoriez et vérifiez chacune des modifications effectuées pour vous assurer que les composants applicables sont correctement sécurisés en fonction de l'utilisation requise. Ne les appliquez pas dans un environnement de production si vous n'êtes pas certain que les modifications de configuration sont correctement sécurisées.

Personnaliser le délai d'expiration des tickets de VMware Remote Console

Vous pouvez personnaliser la période de validité des tickets de la console distante permettant d'établir des connexions VMware Remote Console.

Lorsqu'un utilisateur établit des connexions VMware Remote Console, le système crée et renvoie des informations d'identification à usage unique pour une connexion spécifique à une machine virtuelle. Vous pouvez définir le délai d'expiration du ticket sur un intervalle de temps spécifié en minutes.

Procédure

- 1 Ouvrez le fichier `/etc/vcac/security.properties` dans un éditeur de texte.
- 2 Ajoutez au fichier une ligne au format `consoleproxy.ticket.validitySec=30`.
Sur cette ligne, la valeur numérique indique le nombre de minutes au terme desquelles le ticket expirera.
- 3 Enregistrez le fichier et fermez-le.
- 4 Redémarrez le serveur vCAC à l'aide de la commande `/etc/init.d/vcac-server restart`.

La valeur du délai d'expiration du ticket est réinitialisée sur la période spécifiée en minutes.

Personnaliser le port de serveur proxy de la console

Vous pouvez personnaliser le port sur lequel le proxy de console VMware Remote Console écoute les messages.

Procédure

- 1 Ouvrez le fichier `/etc/vcac/security.properties` dans un éditeur de texte.
- 2 Ajoutez au fichier une ligne au format `consoleproxy.service.port=8445`.
La valeur numérique indique le numéro de port du service proxy de la console, dans ce cas 8445.
- 3 Enregistrez le fichier et fermez-le.
- 4 Redémarrez le serveur vCAC à l'aide de la commande `/etc/init.d/vcac-server restart`.

Le port du service proxy est remplacé par le numéro de port spécifié.

Configurer l'en-tête de réponse X-XSS-Protection

Ajoutez l'en-tête de réponse X XSS-Protection au fichier de configuration haproxy.

Procédure

- 1 Ouvrez le fichier `/etc/haproxy/conf.d/20-vcac.cfg` pour le modifier.

- 2 Ajoutez les lignes suivantes dans la section frontale :

```
rspdel X-XSS-Protection:\ 1;\ mode=block
rspadd X-XSS-Protection:\ 1;\ mode=block
```

- 3 Rechargez la configuration HAProxy à l'aide de la commande suivante.

```
/etc/init.d/haproxy reload
```

Configurer l'en-tête de réponse HTTP Strict Transport Security

Ajoutez l'en-tête de réponse HTTP Strict Transport Security (HSTS) à la configuration HAProxy.

Procédure

- 1 Ouvrez le fichier `/etc/haproxy/conf.d/20-vcac.cfg` pour le modifier.
- 2 Ajoutez les lignes suivantes dans la section frontale :

```
rspdel Strict-Transport-Security:\ max-age=31536000
rspadd Strict-Transport-Security:\ max-age=31536000
```

- 3 Rechargez la configuration HAProxy à l'aide de la commande suivante.

```
/etc/init.d/haproxy reload
```

Configurer l'en-tête de réponse X-Frame-Options

L'en-tête de réponse X-Frame-Options est dupliquée dans certains cas.

Il se peut que l'en-tête de réponse X-Frame-Options apparaisse deux fois, car le service vIDM ajoute cet en-tête au serveur principal ainsi qu'au service HAProxy. Pour empêcher cette duplication, vous pouvez appliquer une configuration appropriée.

Procédure

- 1 Ouvrez le fichier `/etc/haproxy/conf.d/20-vcac.cfg` pour le modifier.
- 2 Recherchez la ligne suivante dans la section frontale :

```
rspadd X-Frame-Options:\ SAMEORIGIN
```

- 3 Ajoutez les lignes suivantes avant la ligne localisée à l'étape précédente :

```
rspdel X-Frame-Options:\ SAMEORIGIN
```

- 4 Rechargez la configuration HAProxy à l'aide de la commande suivante.

```
/etc/init.d/haproxy reload
```

Configuration des en-têtes de réponse de serveur

Pour garantir la sécurité, il est recommandé de configurer le système vRealize Automation pour limiter l'accès aux informations par des pirates.

Dans la mesure du possible, réduisez au strict minimum les informations partagées par votre système concernant les identités et la version. Les pirates et autres entités malveillantes pourraient utiliser ces informations pour cibler votre serveur Web ou une version spécifique.

Configurer l'en-tête de réponse du serveur Lighttpd

Il est recommandé de créer un en-tête de serveur vide pour le serveur lighttpd du dispositif vRealize Automation.

Procédure

- 1 Ouvrez le fichier `/opt/vmware/etc/lighttpd/lighttpd.conf` dans un éditeur de texte.
- 2 Ajoutez `server.tag = " "` au fichier.
- 3 Enregistrez les modifications et fermez le fichier.
- 4 Redémarrez le serveur lighttpd en exécutant la commande `# /opt/vmware/etc/init.d/vami-lighttpd restart`.

Configurer l'en-tête de réponse TCServer pour le dispositif vRealize Automation

Il est recommandé de créer un en-tête de serveur vide personnalisé pour l'en-tête de réponse TCServer utilisé avec le dispositif vRealize Automation afin de limiter la possibilité qu'un pirate obtienne des informations importantes.

Procédure

- 1 Ouvrez le fichier `/etc/vco/app-server/server.xml` dans un éditeur de texte.
- 2 Dans chaque élément `<Connector>`, ajoutez `server=" "`.
Par exemple : `<Connector protocol="HTTP/1.1" server="" />`
- 3 Enregistrez les modifications et fermez le fichier.
- 4 Redémarrez le serveur à l'aide de la commande suivante.
`service vco-server restart`

Configurer l'en-tête de réponse de serveur IIS (Internet Information Services)

Il est recommandé de créer un en-tête de serveur vide personnalisé pour le serveur IIS (Internet Information Services) utilisé avec le dispositif Identity Appliance pour limiter le risque que des pirates obtiennent des informations importantes.

Procédure

- 1 Ouvrez le fichier `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` dans un éditeur de texte.
- 2 Recherchez `RemoveServerHeader=0` et remplacez-le par `RemoveServerHeader=1`.
- 3 Enregistrez les modifications et fermez le fichier.

- 4 Redémarrez le serveur en exécutant la commande `iisreset`.

Suivant

Désactivez l'en-tête X-Powered By d'IIS en supprimant les en-têtes de réponse HTTP dans la liste de la console du Gestionnaire des services Internet.

- 1 Ouvrez la console du Gestionnaire des services Internet.
- 2 Ouvrez l'en-tête de réponse HTTP et supprimez-le de la liste.
- 3 Redémarrez le serveur en exécutant la commande `iisreset`.

Définir le délai d'expiration de session dispositif vRealize Automation

Configurez le paramètre de délai d'expiration de session sur dispositif vRealize Automation conformément à la stratégie de sécurité de votre entreprise.

Le délai d'expiration de session par défaut de dispositif vRealize Automation pour l'inactivité de l'utilisateur est de 30 minutes. Pour modifier cette valeur de délai d'expiration conformément à la stratégie de sécurité de votre organisation, modifiez le fichier `web.xml` sur la machine hôte dispositif vRealize Automation.

Procédure

- 1 Ouvrez le fichier `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` dans un éditeur de texte.
- 2 Recherchez `session-config` et définissez la valeur de délai d'expiration de la session. Reportez-vous à l'exemple de code suivant.

```
<!-- 30 minutes session expiration time -->
<session-config>
    <session-timeout>30</session-timeout>
    <tracking-mode>COOKIE</tracking-mode>
    <cookie-config>
        <path>/</path>
    </cookie-config>
</session-config>
```

- 3 Redémarrez le serveur en exécutant la commande suivante :
`service vcac-server restart`

Gestion des logiciels non essentiels

Pour réduire les risques de sécurité, supprimez ou configurez les logiciels non essentiels de vos machines hôtes vRealize Automation.

Configurez tous les logiciels que vous ne supprimez pas conformément aux recommandations du fabricant et aux meilleures pratiques de sécurité, afin de minimiser les risques de failles de sécurité.

Sécuriser le gestionnaire de stockage de masse USB

Sécurisez le gestionnaire de stockage de masse USB pour empêcher son utilisation en tant que gestionnaire de périphériques USB sur les machines hôtes du dispositif virtuel VMware, car il pourrait être utilisé pour compromettre la sécurité de votre système.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne `install usb-storage /bin/true` apparaît dans le fichier.
- 3 Enregistrez le fichier et fermez-le.

Sécuriser le gestionnaire de protocole Bluetooth

Sécurisez le gestionnaire de protocole Bluetooth sur les machines hôtes du dispositif virtuel pour empêcher les pirates potentiels de l'exploiter.

La liaison du protocole Bluetooth à la pile réseau n'est pas nécessaire et risque d'augmenter la surface d'attaque de l'hôte.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne suivante apparaît dans ce fichier.
`install bluetooth /bin/true`
- 3 Enregistrez le fichier et fermez-le.

Sécuriser le protocole Stream Control Transmission (SCTP)

Empêchez le protocole Stream Control Transmission (SCTP) de se charger sur votre système par défaut, car il pourrait être utilisé par des pirates pour compromettre la sécurité de votre système.

Configurez votre système pour empêcher le module SCTP de se charger, sauf si cela est absolument nécessaire. Le protocole SCTP est un protocole de couche de transport normalisé par l'IETF qui est devenu obsolète. La liaison de ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le noyau, en ouvrant un socket à l'aide de ce protocole.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne suivante apparaît dans ce fichier.
`install sctp /bin/true`
- 3 Enregistrez le fichier et fermez-le.

Sécuriser le protocole Datagram Congestion (DCCP)

Dans le cadre de la sécurisation renforcée du système, empêchez le protocole Datagram Congestion (DCCP) de se charger sur les machines hôtes du dispositif virtuel par défaut, car il pourrait être utilisé pour compromettre la sécurité de votre système.

Évitez de charger le module du protocole DCCP, sauf si cela est absolument nécessaire. Le protocole DCCP résulte d'une proposition de protocole de couche de transport qui n'est pas utilisée. La liaison de ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le noyau en utilisant le protocole pour ouvrir un socket.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que les lignes DCCP apparaissent dans le fichier.

```
install dccp/bin/true
install dccp_ipv4/bin/true
install dccp_ipv6/bin/true
```

- 3 Enregistrez le fichier et fermez-le.

Sécuriser le pontage réseau

Empêchez le module de pontage réseau de se charger sur votre système par défaut, car ce module pourrait être utilisé pour compromettre la sécurité de votre système.

Configurez votre système pour empêcher le réseau de se charger, sauf si cela est absolument nécessaire. En effet, des pirates pourraient l'exploiter pour contourner le partitionnement du réseau et ses mesures de sécurité.

Procédure

- 1 Exécutez la commande suivante sur toutes les machines hôtes du dispositif virtuel VMware.

```
# rmmod bridge
```

- 2 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 3 Assurez-vous que la ligne suivante apparaît dans ce fichier.

```
install bridge /bin/false
```

- 4 Enregistrez le fichier et fermez-le.

Sécuriser le protocole Reliable Datagram Sockets (RDS)

Dans le cadre de la sécurisation renforcée du système, empêchez le protocole Reliable Datagram Sockets (RDS) de se charger sur les machines hôtes du dispositif virtuel par défaut, car il pourrait être utilisé pour compromettre la sécurité de votre système.

La liaison du protocole RDS à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le système en utilisant le protocole pour ouvrir un socket.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne `install rds /bin/true` apparaît dans ce fichier.
- 3 Enregistrez le fichier et fermez-le.

Sécuriser le protocole Transparent Inter-Process Communication (TIPC)

Dans le cadre de la sécurisation renforcée du système, empêchez le protocole Transparent Inter-Process Communication (TIPC) de se charger sur les machines hôtes du dispositif virtuel par défaut. car il pourrait être utilisé pour compromettre la sécurité de votre système.

La liaison du protocole TIPC à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le noyau en utilisant le protocole pour ouvrir un socket.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne `install tipc /bin/true` apparaît dans ce fichier.
- 3 Enregistrez le fichier et fermez-le.

Sécuriser le protocole Internetwork Packet Exchange (IPX)

Empêchez le protocole IPX (Internetwork Packet Exchange) de se charger sur votre système par défaut. car il pourrait être utilisé par des pirates pour compromettre la sécurité de votre système.

Évitez de charger le module du protocole IPX, sauf si cela est absolument nécessaire. Le protocole IPX est un protocole de couche réseau obsolète. La liaison de ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le système en utilisant le protocole pour ouvrir un socket.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne suivante apparaît dans ce fichier.
`install ipx /bin/true`
- 3 Enregistrez le fichier et fermez-le.

Sécuriser le protocole Appletalk

Empêchez le protocole Appletalk de se charger sur votre système par défaut, car il pourrait être utilisé par des pirates pour compromettre la sécurité de votre système.

Évitez de charger le module du protocole Appletalk, sauf si cela est absolument nécessaire. La liaison de ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le système en utilisant le protocole pour ouvrir un socket.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne suivante apparaît dans ce fichier.

```
install appletalk /bin/true
```
- 3 Enregistrez le fichier et fermez-le.

Sécuriser le protocole DECnet

Empêchez le protocole DECnet de se charger sur votre système par défaut, car il pourrait être utilisé par des pirates pour compromettre la sécurité de votre système.

Évitez de charger le module du protocole DECnet, sauf si cela est absolument nécessaire. La liaison de ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le système en utilisant le protocole pour ouvrir un socket.

Procédure

- 1 Ouvrez le fichier de protocole DECnet `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne suivante apparaît dans ce fichier.

```
install decnet /bin/true
```
- 3 Enregistrez le fichier et fermez-le.

Sécuriser le module Firewire

Empêchez le module Firewire de se charger sur votre système par défaut, car il pourrait être utilisé par des pirates pour compromettre la sécurité de votre système.

Évitez de charger le module Firewire, sauf si cela est absolument nécessaire.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne suivante apparaît dans ce fichier.

```
install ieee1394 /bin/true
```
- 3 Enregistrez le fichier et fermez-le.

Sécurisation du composant IaaS (Infrastructure en tant que service)

Lorsque vous renforcez la sécurité de votre système, sécurisez le composant IaaS (Infrastructure en tant que service) vRealize Automation et sa machine hôte pour les protéger contre les pirates.

Vous devez configurer le paramètre de sécurité du composant IaaS (Infrastructure en tant que service) vRealize Automation et de l'hôte sur lequel il réside. Vous devez définir ou vérifier la configuration des autres applications et composants connexes. Dans certains cas, vous pouvez vérifier les paramètres existants, dans d'autres vous devez modifier ou ajouter des paramètres pour une configuration appropriée.

Désactivation du service de temps Windows

Pour garantir la sécurité, il est recommandé d'utiliser des serveurs de temps autorisés plutôt que la synchronisation date/heure des hôtes dans un environnement de production vRealize Automation.

Dans un environnement de production, désactivez la synchronisation date/heure des hôtes et utilisez des serveurs de temps autorisés pour assurer le suivi précis des actions des utilisateurs et identifier d'éventuelles attaques malveillantes et intrusions au moyen d'un audit et d'une journalisation détaillés.

Configuration de TLS pour les données en transit d'IaaS (Infrastructure en tant que service)

Assurez-vous que votre déploiement vRealize Automation utilise des protocoles TLS forts afin de sécuriser les canaux de transmission pour les composants IaaS (Infrastructure en tant que service).

Les protocoles de chiffrement SSL (Secure Sockets Layer) et TLS (Transport Layer Security), ce dernier ayant été plus récemment développé, garantissent la sécurité du système lors des communications réseau entre différents composants système. La norme du protocole SSL étant plus ancienne, un grand nombre de ses implémentations ne fournissent plus une sécurité adéquate contre les attaques potentielles. De graves faiblesses ont été identifiées avec des protocoles SSL antérieurs, notamment SSLv2 et SSLv3. Ces protocoles ne sont plus considérés comme sécurisés.

Selon les stratégies de sécurité de votre organisation, vous pouvez également désactiver TLS 1.0.

Remarque Lors de l'arrêt de TLS sur l'équilibrage de charge, désactivez également les protocoles faibles tels que SSLv2, SSLv3 et TLS 1.0 si nécessaire.

Désactiver SSLv3 dans IIS (Internet Information Services)

Pour garantir la sécurité, il est recommandé de désactiver SSLv3 dans Internet Information Services (IIS) sur la machine de serveur hôte IaaS (Infrastructure en tant que service).

Procédure

- 1 Exécutez l'éditeur de Registre Windows en tant qu'administrateur.

- 2 Accédez à
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\ dans la fenêtre du Registre.
- 3 Cliquez avec le bouton droit sur **Protocoles** et sélectionnez **Nouvelle > Clé**.
- 4 Entrez **SSL 3.0**.
- 5 Dans l'arborescence de navigation, cliquez avec le bouton droit sur la nouvelle clé **SSL 3.0**. Dans le menu contextuel, sélectionnez **Nouvelle > Clé** et entrez **Client**.
- 6 Dans l'arborescence de navigation, cliquez avec le bouton droit sur la nouvelle clé **SSL 3.0**. Dans le menu contextuel, sélectionnez **Nouvelle > Clé** et entrez **Server**.
- 7 Dans l'arborescence de navigation, dans la section SSL 3.0, cliquez avec le bouton droit sur **Client** et sélectionnez **Nouvelle > Valeur DWORD (32 bits)** et entrez **DisabledByDefault**.
- 8 Dans l'arborescence de navigation, dans la section SSL 3.0, sélectionnez **Client** et, dans le volet de droite, double-cliquez sur **DisabledByDefault** et saisissez **1**.
- 9 Dans l'arborescence de navigation, dans la section SSL 3.0, cliquez avec le bouton droit sur **Serveur** et sélectionnez **Nouvelle > Valeur DWORD (32 bits)** et entrez **Enabled**.
- 10 Dans l'arborescence de navigation, dans la section SSL 3.0, sélectionnez **Serveur** et, dans le volet de droite, double-cliquez sur **DWORD** et entrez **0**.
- 11 Redémarrez le serveur Windows.

Désactiver TLS 1.0 pour IaaS

Afin de garantir une sécurité maximale, configurez le service IaaS pour utiliser le pooling et désactivez TLS 1.0.

Pour plus d'informations, reportez-vous à l'article <https://support.microsoft.com/en-us/kb/245030> dans la Base de connaissances de Microsoft.

Procédure

- 1 Configurez le service IaaS pour utiliser le pooling au lieu de sockets Web.
 - a Mettez à jour le fichier de configuration de Manager Service C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config en ajoutant les valeurs suivantes dans la section <appSettings>.

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```
 - b Redémarrez Manager Service (service VMware vCloud Automation Center).

2 Assurez-vous que TLS 1.0 est désactivé sur le serveur IaaS.

- a Exécutez l'éditeur de Registre en tant qu'administrateur.
- b Dans la fenêtre du Registre, accédez à
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\
- c Cliquez avec le bouton droit sur Protocoles et sélectionnez **Nouvelle > Clé**, puis entrez **TLS 1.0**.
- d Dans l'arborescence de navigation, cliquez avec le bouton droit sur la clé TLS 1.0 que vous venez de créer. Dans le menu contextuel, sélectionnez **Nouvelle > Clé** et entrez **Client**.
- e Dans l'arborescence de navigation, cliquez avec le bouton droit sur la clé TLS 1.0 que vous venez de créer. Dans le menu contextuel, sélectionnez **Nouvelle > Clé** et entrez **Server**.
- f Dans l'arborescence de navigation, dans la section TLS 1.0, cliquez avec le bouton droit sur **Client**, puis cliquez sur **Nouvelle > Valeur DWORD 32 bits** et entrez **DisabledByDefault**.
- g Dans l'arborescence de navigation, dans la section TLS 1.0, sélectionnez **Client**. Dans le volet de droite, double-cliquez sur **DisabledByDefault** (valeur DWORD) et entrez **1**.
- h Dans l'arborescence de navigation, dans la section TLS 1.0, cliquez avec le bouton droit sur **Serveur** et sélectionnez **Nouvelle > Valeur DWORD 32 bits** et entrez **Enabled**.
- i Dans l'arborescence de navigation, dans la section TLS 1.0, sélectionnez **Serveur**. Dans le volet de droite, double-cliquez sur **Activé** (valeur DWORD) et saisissez **0**.
- j Redémarrez le serveur Windows.

Configuration des suites de chiffrement TLS

Pour obtenir une sécurité maximale, vous devez configurer les composants vRealize Automation pour utiliser des chiffrements forts. Le chiffrement négocié entre le serveur et le navigateur détermine la force du chiffrement utilisé dans une session TLS. Pour vous assurer que seuls des chiffrements forts sont sélectionnés, désactivez les chiffrements faibles dans les composants vRealize Automation. Configurez le serveur pour prendre en charge uniquement les chiffrements forts et pour utiliser des clés suffisamment grandes. En outre, configurez tous les chiffrements dans l'ordre approprié.

Suites de chiffrement non acceptables

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, aNULL ou eNULL. Désactivez également l'échange de clés anonyme Diffie-Hellman (ADH), les chiffrements de niveau exportation (EXP, chiffrements contenant des algorithmes DES), les tailles de clé inférieures à 128 bits pour le chiffrement du trafic de la charge utile, l'utilisation de la fonction MD5 comme mécanisme de hachage pour le trafic de charge utile, les suites de chiffrement IDEA et les suites de chiffrement RC4. Assurez-vous également que les suites de chiffrement utilisant l'échange de clés Diffie-Hellman (DHE) sont désactivées.

Vérification de la sécurité du serveur hôte

Une bonne pratique de sécurité consiste à vérifier la configuration de la sécurité des machines de votre serveur hôte IaaS (Infrastructure en tant que service).

Microsoft fournit plusieurs outils de vérification de la sécurité sur les machines du serveur hôte. Contactez votre fournisseur Microsoft pour obtenir des conseils sur l'utilisation la plus appropriée de ces outils.

Vérifier la sécurité de la ligne de base du serveur hôte

Exécutez Microsoft Baseline Security Analyzer (MBSA) pour vérifier rapidement que votre serveur dispose des dernières mises à jour ou des correctifs les plus récents. Vous pouvez utiliser MBSA pour installer des correctifs de sécurité manquants de Microsoft, afin de maintenir votre serveur à jour conformément aux recommandations de sécurité de Microsoft.

Téléchargez la dernière version de l'outil MBSA sur le site Web de Microsoft.

Vérifier la configuration de sécurité du serveur hôte

Utilisez l'Assistant Configuration de la sécurité de Windows et le kit de ressources Gestionnaire de conformité de sécurité Microsoft pour vérifier que le serveur hôte est configuré de manière sécurisée.

Exécutez l'Assistant Configuration de la sécurité de Windows à partir des outils d'administration de votre serveur Windows. Cet outil peut identifier les rôles de votre serveur et les fonctionnalités installées, notamment la mise en réseau, les pare-feu Windows et les paramètres de Registre. Comparez le rapport avec les derniers conseils en matière de sécurisation renforcée du Gestionnaire de conformité de sécurité Microsoft correspondant à votre serveur Windows. Selon les résultats, vous pouvez ajuster précisément les paramètres de sécurité pour chaque fonctionnalité, tels que les services réseau, les paramètres de compte et les pare-feu Windows, et appliquer les paramètres à votre serveur.

Pour plus d'informations sur l'Assistant Configuration de la sécurité de Windows, consultez le site Web Microsoft Technet.

Protection des ressources d'application

Pour garantir la sécurité, il est recommandé de vérifier que tous les fichiers IaaS (Infrastructure en tant que service) pertinents disposent d'autorisations appropriées.

Vérifiez les fichiers IaaS (Infrastructure en tant que service) par rapport à votre installation IaaS. Dans la plupart des cas, les sous-dossiers et fichiers de chaque dossier doivent avoir les mêmes paramètres que le dossier.

| Répertoire ou fichier | Groupe ou utilisateurs | Contrôle total | Modifier | Lire et exécuter | Lecture | Écriture |
|---|------------------------|----------------|----------|------------------|---------|----------|
| VMware\vmCAC\Agents \<agent_name> \logs | SYSTÈME | X | X | X | X | X |
| | administrateur | X | X | X | X | X |
| | Administrateurs | X | X | X | X | X |

| Répertoire ou fichier | Groupe ou utilisateurs | Contrôle total | Modifier | Lire et exécuter | Lecture | Écriture |
|--|------------------------|----------------|----------|------------------|---------|----------|
| VMware\vmCAC\Agents\ <agent_name> \temp | SYSTÈME | X | X | X | X | X |
| | administrateur | X | X | X | X | X |
| | Administrateurs | X | X | X | X | X |
| VMware\vmCAC\Agents\ | SYSTÈME | X | X | X | X | X |
| | Administrateurs | X | X | X | X | X |
| | Utilisateurs | | | X | X | |
| VMware\vmCAC\Distributed Execution Manager\ | SYSTÈME | X | X | X | X | X |
| | Administrateurs | X | X | X | X | X |
| | Utilisateurs | | | X | X | |
| VMware\vmCAC\Distributed Execution Manager\DEM\Logs | SYSTÈME | X | X | X | X | X |
| | administrateur | X | X | X | X | X |
| | Administrateurs | X | X | X | X | X |
| VMware\vmCAC\Distributed Execution Manager\DEO\Logs | SYSTÈME | X | X | X | X | X |
| | administrateur | X | X | X | X | X |
| | Administrateurs | X | X | X | X | X |
| VMware\vmCAC\Management Agent\ | SYSTÈME | X | X | X | X | X |
| | Administrateurs | X | X | X | X | X |
| | Utilisateurs | | | X | X | |
| VMware\vmCAC\Server\ | SYSTÈME | X | X | X | X | X |
| | Administrateurs | X | X | X | X | X |
| | Utilisateurs | | | X | X | |
| VMware\vmCAC\Web API | SYSTÈME | X | X | X | X | X |
| | Administrateurs | X | X | X | X | X |
| | Utilisateurs | | | X | X | |

Sécuriser la machine hôte IaaS (Infrastructure en tant que service)

Pour garantir la sécurité, il est recommandé de vérifier les paramètres de base sur votre machine hôte IaaS (Infrastructure en tant que service) pour vous assurer qu'elle est conforme aux directives de sécurité.

Sécurisez les comptes, applications, ports et services sur la machine hôte IaaS.

Vérifier les paramètres de compte d'utilisateur de serveur

Vérifiez qu'il n'existe pas de paramètres et de comptes d'utilisateur local et de domaine inutiles. Tout compte d'utilisateur non associé aux fonctions d'application doit être réservé à l'administration, à la maintenance et au dépannage. Limitez l'accès distant à partir de comptes d'utilisateurs de domaine au minimum requis pour maintenir le serveur. Réalisez des contrôles et audits stricts de ces comptes.

Supprimez les applications inutiles

Supprimez toutes les applications inutiles des serveurs hôtes. Les applications inutiles augmentent le risque d'exposition en raison de leurs vulnérabilités inconnues ou non corrigées.

Désactiver les ports et services inutiles

Passez en revue la liste des ports ouverts du pare-feu du serveur hôte. Bloquez tous les ports qui ne sont pas requis pour le composant IaaS ou le fonctionnement critique du système. Consultez [Configuration des ports et des protocoles](#). Vérifiez les services en cours d'exécution sur votre serveur hôte et désactivez ceux qui ne sont pas requis.

Configuration de la sécurité réseau des hôtes

9

Pour assurer une protection maximale contre les menaces de sécurité connues, configurez les paramètres d'interface et de communication réseau sur toutes les machines hôtes VMware.

Dans le cadre d'un plan de sécurité complet, configurez les paramètres de sécurité d'interface réseau pour les dispositifs virtuels VMware et les composant IaaS (Infrastructure en tant que service) conformément aux directives de sécurité établies.

Ce chapitre aborde les rubriques suivantes :

- [Configuration des paramètres réseau pour les dispositifs VMware](#)
- [Configuration des paramètres réseau pour l'hôte IaaS \(Infrastructure en tant que service\)](#)
- [Configuration des ports et des protocoles](#)

Configuration des paramètres réseau pour les dispositifs VMware

Pour vous assurer que les machines hôtes du dispositif virtuel VMware prennent uniquement en charge des communications sécurisées et importantes, vérifiez et modifiez leurs paramètres de communication réseau.

Examinez la configuration du protocole IP du réseau de vos machines hôtes VMware et configurez les paramètres réseau conformément aux directives de sécurité. Désactivez tous les protocoles de communication non essentiels.

Empêcher le contrôle par l'utilisateur des interfaces réseau

Pour garantir la sécurité, il est recommandé d'accorder aux utilisateurs uniquement les privilèges système indispensables pour effectuer leurs tâches sur les machines hôtes du dispositif VMware.

Le fait d'autoriser des comptes d'utilisateur disposant de privilèges à manipuler des interfaces réseau risque de créer des mécanismes de contournement de la sécurité réseau ou un déni de service. Limitez les possibilités de modification des paramètres d'interface réseau aux utilisateurs disposant de privilèges.

Procédure

- 1 Exécutez la commande suivante sur chaque machine hôte du dispositif VMware.

```
# grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*
```

- 2 Assurez-vous que chaque interface est définie sur NO.

Définir la taille de la file d'attente du backlog TCP

Pour fournir un niveau de défense contre les attaques malveillantes, configurez une taille de file d'attente de backlog TCP par défaut sur les machines hôtes du dispositif VMware.

Définissez les tailles des files d'attente de backlog TCP sur une taille par défaut appropriée pour une meilleure prévention contre les attaques de service ou de refus du TCP. La valeur par défaut recommandée du paramètre est de 1 280.

Procédure

- 1 Exécutez la commande suivante sur chaque machine hôte du dispositif VMware.

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```

- 2 Ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Définissez la taille de la file d'attente du backlog TCP par défaut en ajoutant l'entrée suivante au fichier.

```
net.ipv4.tcp_max_syn_backlog=1280
```

- 4 Enregistrez les modifications et fermez le fichier.

Refuser les demandes d'écho ICMPv4 d'adresse de diffusion

Pour garantir la sécurité, il est recommandé de vérifier que les machines hôtes du dispositif VMware ignorent les demandes d'écho d'adresse de diffusion ICMP.

Les réponses pour diffuser les demandes d'écho ICMP (Internet Control Message Protocol) fournissent un vecteur d'attaque d'amplification et peuvent faciliter le mappage réseau par des agents malveillants. La configuration des machines hôtes de dispositif pour ignorer les demandes d'écho ICMPv4 fournit une protection contre de telles attaques.

Procédure

- 1 Exécutez la commande `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` sur les machines hôtes du dispositif virtuel VMware pour confirmer qu'elles refusent des demandes d'écho d'adresse de diffusion IPv4.

Si les machines hôtes sont configurées pour refuser les redirections IPv4, cette commande renvoie la valeur 0 pour `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`.

- 2 Pour configurer une machine hôte de dispositif virtuel pour refuser les demandes d'écho d'adresse de diffusion ICMPv4, ouvrez le fichier `/etc/sysctl.conf` sur les machines hôtes Windows dans un éditeur de texte.
- 3 Localisez l'entrée contenant `net.ipv4.icmp_echo_ignore_broadcasts=0`. Si la valeur de cette entrée n'est pas définie sur zéro ou si l'entrée n'existe pas, ajoutez-la ou mettez à jour l'entrée existante.

- 4 Enregistrez les modifications et fermez le fichier.

Désactiver le protocole ARP du proxy IPv4

Assurez-vous que le protocole ARP du proxy IPv4 est désactivé, s'il n'est pas requis sur les machines hôtes du dispositif VMware, afin d'empêcher le partage non autorisé d'informations.

Le protocole ARP du proxy IPv4 permet à un système d'envoyer des réponses aux demandes ARP sur une interface pour le compte d'hôtes connectés à une autre interface. Désactivez cette fonctionnalité si elle ne sert pas à empêcher la fuite d'informations d'adressage entre les segments réseau attachés.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | egrep "default|all"` sur les machines hôtes du dispositif virtuel VMware pour vérifier que le protocole ARP du proxy IPv4 est désactivé.

Si le protocole ARP du proxy IPv6 est désactivé sur les machines hôtes, cette commande renvoie des valeurs 0.

```
/proc/sys/net/ipv4/conf/all/proxy_arp:0
/proc/sys/net/ipv4/conf/default/proxy_arp:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer le protocole ARP du proxy IPv6 sur les machines hôtes, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv4.conf.default.proxy_arp=0
net.ipv4.conf.all.proxy_arp=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser les messages de redirection ICMP IPv4

Pour garantir la sécurité, il est recommandé de vérifier que les machines hôtes du dispositif virtuel VMware refusent les messages de redirection ICMP IPv4.

Les routeurs utilisent des messages de redirection ICMP pour informer les hôtes qu'une route plus directe existe pour une destination. Un message de redirection ICMP malveillant peut faciliter une attaque de l'intercepteur. Ces messages modifient la table de routage de l'hôte et ne sont pas authentifiés. Assurez-vous que votre système est configuré pour les ignorer s'ils ne sont pas nécessaires.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` sur les machines hôtes de dispositif VMware afin de confirmer le refus des messages de redirection IPv4.

Si les machines hôtes sont configurées pour refuser les redirections IPv4, cette commande renvoie ce qui suit :

```
/proc/sys/net/ipv4/conf/all/accept_reidrects:0
```

```
/proc/sys/net/ipv4/conf/default/accept_redirects:0
```

- 2 Si vous devez configurer une machine hôte de dispositif virtuel pour refuser les messages de redirection IPv4, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Vérifiez les valeurs des lignes qui commencent par `net.ipv4.conf`.

Si les valeurs des entrées suivantes ne sont pas définies sur zéro ou si les entrées n'existent pas, ajoutez-les au fichier ou mettez à jour les entrées existantes.

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

- 4 Enregistrez les modifications et fermez le fichier.

Refuser les messages de redirection ICMP IPv6

Pour garantir la sécurité, il est recommandé de vérifier que les machines hôtes du dispositif virtuel VMware refusent les messages de redirection ICMP IPv6.

Les routeurs utilisent des messages de redirection ICMP pour informer les hôtes qu'une route plus directe existe pour une destination. Un message de redirection ICMP malveillant peut faciliter une attaque de l'intercepteur. Ces messages modifient la table de routage de l'hôte et ne sont pas authentifiés. Assurez-vous que votre système est configuré pour les ignorer s'ils ne sont pas nécessaires.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` sur les machines hôtes du dispositif virtuel VMware pour confirmer le refus des messages de redirection IPv6.

Si les machines hôtes sont configurées pour refuser les redirections IPv6, cette commande renvoie ce qui suit :

```
/proc/sys/net/ipv6/conf/all/accept_redirects:0
```

```
/proc/sys/net/ipv6/conf/default/accept_redirects:0
```

- 2 Pour configurer une machine hôte de dispositif virtuel pour refuser les messages de redirection IPv4, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.

- 3 Vérifiez les valeurs des lignes qui commencent par `net.ipv6.conf`.

Si les valeurs des entrées suivantes ne sont pas définies sur zéro ou si elles n'existent pas, ajoutez-les au fichier ou mettez à jour les entrées existantes.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Enregistrez les modifications et fermez le fichier.

Journaliser des paquets martiens IPv4

Pour garantir la sécurité, il est recommandé de vérifier que les machines hôtes du dispositif virtuel VMware journalisent les paquets martiens IPv4.

Les paquets martiens contiennent des adresses identifiées comme non valides par le système. Configurez les machines hôtes pour journaliser ces messages, de façon à identifier les configurations incorrectes ou les attaques en cours.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians | egrep "default|all"` sur les machines hôtes du dispositif VMware pour vérifier la journalisation des paquets martiens IPv4.

Si les machines virtuelles sont configurées pour journaliser les paquets martiens, elles renvoient ce qui suit :

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/conf/default/log_martians:1
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer des machines virtuelles pour journaliser des paquets martiens IPv4, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Vérifiez les valeurs des lignes qui commencent par `net.ipv4.conf`.

Si la valeur des entrées suivantes n'est pas définie sur 1 ou si ces entrées n'existent pas, ajoutez-les au fichier ou mettez à jour les entrées existantes.

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

- 4 Enregistrez les modifications et fermez le fichier.

Utiliser le filtrage de chemin inverse IPv4

Pour garantir la sécurité, il est recommandé de vérifier que les machines hôtes de VMware utilisent le filtrage de chemin inverse IPv4.

Le filtrage de chemin inverse constitue une protection contre l'usurpation des adresses source en provoquant le rejet des paquets dont les adresses source n'ont aucune route ou dont la route ne pointe pas vers l'interface d'origine. Configurez vos machines hôtes pour utiliser le filtrage de chemin inverse autant que possible. Dans certains cas, selon le rôle système, le filtrage de chemin inverse peut entraîner le rejet d'un trafic légitime. Si vous rencontrez de tels problèmes, vous devrez éventuellement utiliser un mode plus permissif ou désactiver complètement le filtrage de chemin inverse.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter | egrep "default|all"` sur les machines hôtes du dispositif virtuel VMware pour vérifier qu'elles utilisent le filtrage de chemin inverse IPv4.

Si les machines virtuelles utilisent le filtrage de chemin inverse IPv4, cette commande renvoie ce qui suit :

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/rp_filter:1
```

Si vos machines virtuelles sont correctement configurées, aucune autre action n'est requise.

- 2 Si vous devez configurer le filtrage de chemin inverse IPv4 sur des machines hôtes, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Vérifiez les valeurs des lignes qui commencent par `net.ipv4.conf`.

Si les valeurs des entrées suivantes ne sont pas définies sur 1 ou si elles n'existent pas, ajoutez-les au fichier ou mettez à jour les entrées existantes.

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

- 4 Enregistrez les modifications et fermez le fichier.

Refuser le transfert IPv4

Vérifiez que les machines hôtes du dispositif VMware refusent le transfert IPv4.

Si le système est configuré pour le transfert IP et n'est pas un routeur désigné, les pirates peuvent l'utiliser pour contourner la sécurité du réseau en fournissant un chemin de communication non filtré par les périphériques réseau. Configurez les machines hôtes du dispositif virtuel pour refuser le transfert IPv4 afin d'éliminer ce risque.

Procédure

- 1 Exécutez la commande `# cat /proc/sys/net/ipv4/ip_forward` sur les machines hôtes du dispositif VMware afin de confirmer qu'elles refusent les transferts IPv4.

Si les machines hôtes sont configurées pour refuser le transfert IPv4, cette commande renvoie la valeur 0 pour `/proc/sys/net/ipv4/ip_forward`. Si les machines virtuelles sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Pour configurer une machine hôte de dispositif virtuel pour refuser le transfert IPv4, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Localisez l'entrée contenant `net.ipv4.ip_forward=0`. Si la valeur de cette entrée n'est pas définie sur zéro ou si l'entrée n'existe pas, ajoutez-la ou mettez à jour l'entrée existante.
- 4 Enregistrez les modifications et fermez le fichier.

Refuser le transfert IPv6

Pour garantir la sécurité, il est recommandé de vérifier que vos systèmes hôtes de dispositif VMware refusent le transfert IPv6.

Si le système est configuré pour le transfert IP et n'est pas un routeur désigné, les pirates peuvent l'utiliser pour contourner la sécurité du réseau en fournissant un chemin de communication non filtré par les périphériques réseau. Configurez les machines hôtes de dispositif virtuel pour refuser le transfert IPv6 afin d'éliminer ce risque.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding | egrep "default|all"` sur les machines hôtes du dispositif VMware pour vérifier qu'elles refusent le transfert IPv6.

Si les machines hôtes sont configurées pour refuser le transfert IPv6, cette commande renvoie ce qui suit :

```
/proc/sys/net/ipv6/conf/all/forwarding:0
/proc/sys/net/ipv6/conf/default/forwarding:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer une machine hôte pour refuser le transfert IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Vérifiez les valeurs des lignes qui commencent par `net.ipv6.conf`.

Si les valeurs des entrées suivantes ne sont pas définies sur zéro ou si les entrées n'existent pas, ajoutez les entrées ou mettez à jour les entrées existantes en conséquence.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Enregistrez les modifications et fermez le fichier.

Utiliser des cookies SYN TCP IPv4

Vérifiez que les machines hôtes du dispositif VMware utilisent des cookies SYN TCP IPv4.

Une attaque par saturation de type SYN TCP peut provoquer un déni de service en remplissant le tableau des connexions TCP d'un système avec des connexions dans l'état SYN_RCVD. Les cookies SYN empêchent le suivi d'une connexion jusqu'à réception de l'accusé de réception suivant en vérifiant que l'initiateur tente d'établir une connexion valide et qu'il n'est pas une source de saturation. Cette technique n'est pas totalement conforme aux normes. Elle est activée uniquement en cas de saturation et permet de protéger le système tout en continuant à traiter les demandes de service valides.

Procédure

- 1 Exécutez la commande `# cat /proc/sys/net/ipv4/tcp_syncookies` sur les machines hôtes du dispositif VMware pour vérifier qu'elles utilisent des cookies SYN TCP IPv4.

Si les machines hôtes sont configurées pour refuser le transfert IPv4, cette commande renvoie une valeur de 1 pour `/proc/sys/net/ipv4/tcp_syncookies`. Si les machines virtuelles sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer un dispositif virtuel pour utiliser des cookies SYN TCP IPv4, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.

- 3 Localisez l'entrée contenant `net.ipv4.tcp_syncookies=1`.

Si la valeur de cette entrée n'est pas actuellement définie sur un ou si elle n'existe pas, ajoutez l'entrée ou mettez à jour l'entrée existante.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser les annonces du routeur IPv6

Vérifiez que les machines hôtes VMware refusent l'acceptation des annonces du routeur et les redirections ICMP sauf exigence contraire du système.

IPv6 permet aux systèmes de configurer leurs périphériques réseau en utilisant automatiquement des informations provenant du réseau. Pour des raisons de sécurité, la configuration manuelle d'informations de configuration importantes est préférable à une acceptation sans authentification à partir du réseau.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"` sur les machines hôtes de dispositif VMware pour vérifier qu'elles refusent les annonces du routeur.

Si les machines hôtes sont configurées pour refuser les annonces du routeur IPv6, cette commande renvoie des valeurs 0 :

```
/proc/sys/net/ipv6/conf/all/accept_ra:0
/proc/sys/net/ipv6/conf/default/accept_ra:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer une machine hôte pour refuser les annonces du routeur IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.

3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

Si ces entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez-les ou mettez à jour les entrées existantes.

4 Enregistrez les modifications et fermez le fichier.

Refuser les sollicitations du routeur IPv6

Pour garantir la sécurité, il est recommandé de vérifier que les machines hôtes du dispositif VMware refusent les sollicitations du routeur IPv6, sauf si elles sont requises pour garantir le bon fonctionnement du système.

Le paramètre de sollicitations de routeur détermine le nombre de sollicitations de routeur envoyées lorsque vous mettez en place l'interface. Si les adresses sont attribuées de façon statique, il n'est pas nécessaire d'envoyer de sollicitations.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/router_sollicitations | egrep "default|all"` sur les machines hôtes du dispositif VMware pour vérifier qu'elles refusent les sollicitations du routeur IPv6.

Si les machines hôtes sont configurées pour refuser les annonces du routeur IPv6, cette commande renvoie ce qui suit :

```
/proc/sys/net/ipv6/conf/all/router_sollicitations:0
/proc/sys/net/ipv6/conf/default/router_sollicitations:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer des machines hôtes pour refuser les sollicitations du routeur IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.router_sollicitations=0
net.ipv6.conf.default.router_sollicitations=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser la préférence du routeur IPv6 dans les sollicitations du routeur

Vérifiez que les machines hôtes du dispositif VMware refusent les sollicitations du routeur IPv6, sauf si elles sont requises pour garantir le bon fonctionnement du système.

La préférence du routeur dans le paramètre de sollicitations détermine les préférences de routeur. Si les adresses sont attribuées de façon statique, il n'est pas nécessaire de recevoir de préférence de routeur pour les sollicitations.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"` sur les machines hôtes du dispositif VMware pour vérifier qu'elles refusent les sollicitations du routeur IPv6.

Si les machines hôtes sont configurées pour refuser les annonces du routeur IPv6, cette commande renvoie ce qui suit :

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer des machines hôtes pour refuser les sollicitations de route IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes en conséquence.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser le préfixe du routeur IPv6

Vérifiez que les machines hôtes du dispositif VMware refusent les informations de préfixe du routeur IPv6, sauf si elles sont requises pour garantir le bon fonctionnement du système.

Le paramètre `accept_ra_rtr_pref` détermine si le système accepte les informations de préfixe en provenance du routeur. Si les adresses sont attribuées de façon statique, il n'est pas nécessaire de recevoir des informations de préfixe de routeur.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | egrep "default|all"` sur les machines hôtes du dispositif VMware pour vérifier qu'elles refusent les informations de préfixe du routeur IPv6.

Si les machines hôtes sont configurées pour refuser les annonces du routeur IPv6, cette commande renvoie ce qui suit.

```
/proc/sys/net/ipv6/conf/all/accept_ra_pinfo:0
/proc/sys/net/ipv6/conf/default/accept_ra_pinfo:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer des machines hôtes pour refuser les informations de préfixe du routeur IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser les paramètres de limite de sauts d'annonce du routeur IPv6

Vérifiez que les machines hôtes du dispositif VMware refusent les paramètres de limite de sauts de routeur IPv6, sauf s'ils sont nécessaires.

Le paramètre `accept_ra_defrtr` détermine si le système accepte les paramètres de limite de sauts en provenance d'une annonce du routeur. Si vous définissez ce paramètre sur zéro, le routeur ne pourra pas modifier la limite de sauts IPv6 par défaut pour les paquets sortants.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` sur les machines hôtes de dispositif VMware pour vérifier qu'elles refusent les paramètres de limite de sauts de routeur IPv6.

Si les machines hôtes sont configurées pour refuser les paramètres de limite de sauts de routeur IPv6, cette commande renvoie des valeurs 0.

```
/proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
/proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer une machine hôte pour refuser les paramètres de limite de sauts de routeur IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser les paramètres d'autoconfiguration d'annonce du routeur IPv6

Vérifiez que les machines hôtes du dispositif VMware refusent les paramètres d'autoconfiguration du routeur IPv6, sauf s'ils sont nécessaires.

Le paramètre `autoconf` détermine si les annonces du routeur peuvent entraîner l'attribution d'une adresse de monodiffusion globale à une interface par le système.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all"` sur les machines hôtes de dispositif VMware pour vérifier qu'elles refusent les paramètres d'autoconfiguration du routeur IPv6.

Si les machines hôtes sont configurées pour refuser les paramètres d'autoconfiguration du routeur IPv6, cette commande renvoie des valeurs 0.

```
/proc/sys/net/ipv6/conf/all/autoconf:0
/proc/sys/net/ipv6/conf/default/autoconf:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer une machine hôte pour refuser les paramètres d'autoconfiguration du routeur IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser les sollicitations de voisin IPv6

Vérifiez que vos machines hôtes de dispositif VMware refusent les sollicitations de voisin IPv6, sauf si elles sont nécessaires.

Le paramètre `dad_transmits` détermine le nombre de sollicitations de voisin devant être envoyées par adresse (globale et locale du lien) lorsque vous mettez en place une interface pour garantir que l'adresse souhaitée est unique sur le réseau.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | egrep "default|all"` sur les machines hôtes de dispositif VMware afin de confirmer le refus des sollicitations de voisin IPv6.

Si les machines hôtes sont configurées pour refuser les sollicitations de voisin IPv6, cette commande renvoie des valeurs 0.

```
/proc/sys/net/ipv6/conf/all/dad_transmits:0
/proc/sys/net/ipv6/conf/default/dad_transmits:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer une machine hôte pour refuser les sollicitations de voisin IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes.

- 4 Enregistrez les modifications et fermez le fichier.

Limiter le nombre maximal d'adresses IPv6

Assurez-vous que les machines hôtes du dispositif VMware limitent le nombre maximal d'adresses IPv6 au nombre minimal requis pour le fonctionnement du système.

Le paramètre relatif au nombre maximal d'adresses détermine le nombre d'adresses globales IPv6 de diffusion unicast disponibles sur chaque interface. La valeur par défaut est 16, mais vous devez définir le nombre exact d'adresses globales configurées de manière statique conformément à la configuration de votre système.

Procédure

- 1 Exécutez la commande `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"` sur les machines hôtes du dispositif VMware pour vérifier que le nombre maximal d'adresses IPv6 est correctement limité.

Si les machines hôtes sont configurées de façon à limiter le nombre maximal d'adresses IPv6, cette commande renvoie 1.

```
/proc/sys/net/ipv6/conf/all/max_addresses:1
/proc/sys/net/ipv6/conf/default/max_addresses:1
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer le nombre maximal d'adresses IPv6 sur les machines hôtes, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur 1, ajoutez-les ou mettez à jour les entrées existantes.

- 4 Enregistrez les modifications et fermez le fichier.

Configuration des paramètres réseau pour l'hôte IaaS (Infrastructure en tant que service)

Pour garantir la sécurité, il est recommandé de configurer les paramètres de communication réseau sur votre machine hôte de composant IaaS (Infrastructure en tant que service) VMware, conformément aux exigences et aux directives VMware.

Définissez la configuration réseau de la machine hôte IaaS (Infrastructure en tant que service) pour prendre en charge des fonctions vRealize Automation complètes avec la sécurité appropriée.

Reportez-vous à [Sécurisation du composant IaaS \(Infrastructure en tant que service\)](#).

Configuration des ports et des protocoles

Pour garantir la sécurité, il est recommandé de configurer les ports et les protocoles de tous les dispositifs et composants vRealize Automation conformément aux directives de VMware.

Configurez les ports entrants et sortants des composants vRealize Automation, afin d'assurer le fonctionnement correct des composants système critiques. Désactivez tous les protocoles et ports inutiles. Reportez-vous à la section *Architecture de référence de vRealize Automation*.

Ports utilisateur requis

Pour garantir la sécurité, il est recommandé de configurer les ports utilisateur de vRealize Automation conformément aux directives de VMware.

Exposez les ports requis uniquement sur un réseau sécurisé.

| SERVEUR | PORTS |
|--------------------------------|-----------|
| Dispositif vRealize Automation | 443, 8443 |

Ports requis par l'administrateur

Pour garantir la sécurité, il est recommandé de configurer les ports de l'administrateur de vRealize Automation conformément aux directives de VMware.

Exposez les ports requis uniquement sur un réseau sécurisé.

| SERVEUR | PORTS |
|---------------------------------------|-------|
| Serveur vRealize Application Services | 5480 |

Ports du dispositif vRealize Automation

Pour garantir la sécurité, il est recommandé de configurer les ports entrants et sortants de dispositif vRealize Automation conformément aux recommandations de VMware.

Ports entrants

Configurez le nombre minimum de ports entrants requis pour dispositif vRealize Automation. Si nécessaire, configurez des ports facultatifs pour la configuration de votre système.

Tableau 9-1. Minimum de ports entrants requis

| PORT | PROTOCOLE | COMMENTAIRES |
|------------|-----------|--|
| 443 | TCP | Accès à la console vRealize Automation et aux appels d'API. |
| 8443 | TCP | Proxy de console (VMRC). |
| 5480 | TCP | Accès à la console de gestion Web du dispositif virtuel. |
| 5488, 5489 | TCP | Interne. Utilisé par dispositif vRealize Automation pour les mises à jour. |
| 5672 | TCP | Messagerie RabbitMQ. |
| | | Remarque Lors de la mise en cluster des instances de dispositif vRealize Automation, vous devrez configurer les ports ouverts 4369 et 25672. |
| 40002 | TCP | Requis pour le service vIDM. Protège par un pare-feu tout le trafic externe à l'exception du trafic provenant des autres nœuds de dispositif vRealize Automation en cas d'ajout à la configuration HA. |

Si nécessaire, configurez les ports entrants facultatifs.

Tableau 9-2. Ports entrants facultatifs

| PORT | PROTOCOLE | COMMENTAIRES |
|------|-----------|--|
| 22 | TCP | (Facultatif) SSH. Dans un environnement de production, désactivez le service SSH sur le port d'écoute 22 et fermez le port 22. |
| 80 | TCP | (Facultatif) Redirection vers le port 443. |

Ports sortants

Configurez les ports sortants requis.

Tableau 9-3. Minimum de ports sortants requis

| PORT | PROTOCOLE | COMMENTAIRES |
|------------------|-----------|--|
| 25 587 | TCP, UDP | SMTP pour l'envoi d'e-mails de notification sortants. |
| 53 | TCP, UDP | DNS. |
| 67, 68, 546, 547 | TCP, UDP | DHCP. |
| 110, 995 | TCP, UDP | POP pour recevoir des e-mails de notification entrants. |
| 143, 993 | TCP, UDP | IMAP pour recevoir des e-mails de notification entrants. |
| 443 | TCP | IaaS Manager Service sur HTTPS. |

Si nécessaire, configurez les ports sortants facultatifs.

Tableau 9-4. Ports sortants facultatifs

| PORT | PROTOCOLE | COMMENTAIRES |
|------|-----------|--|
| 80 | TCP | (Facultatif) Pour extraire des mises à jour logicielles. Vous pouvez télécharger et appliquer les mises à jour séparément. |
| 123 | TCP, UDP | (Facultatif) Pour la connexion directe au NTP au lieu d'utiliser l'heure de l'hôte. |

Ports IaaS (Infrastructure en tant que service)

Pour garantir la sécurité, il est recommandé de configurer les ports entrants et sortants des composants IaaS (Infrastructure en tant que service) conformément aux directives de VMware.

Ports entrants

Configurez le nombre minimum requis de ports entrants pour les composants IaaS.

Tableau 9-5. Minimum de ports entrants requis

| COMPOSANT | PORT | PROTOCOLE | COMMENTAIRES |
|-----------------|------|-----------|---|
| Manager Service | 443 | TCP | Communication avec les composants IaaS et le dispositif vRealize Automation sur HTTPS. Tous les hôtes de virtualisation gérés par des agents proxy doivent également avoir le port TCP 443 ouvert pour le trafic entrant. |

Ports sortants

Configurez le nombre minimum requis de ports sortants pour les composants laaS.

Tableau 9-6. Minimum de ports sortants requis

| COMPOSANT | PORT | PROTOCOLE | COMMENTAIRES |
|--|------|-----------|---|
| Tout | 53 | TCP, UDP | DNS. |
| Tout | | TCP, UDP | DHCP. |
| Manager Service | 443 | TCP | Communication avec le dispositif vRealize Automation sur HTTPS. |
| Site Web | 443 | TCP | Communication avec Manager Service sur HTTPS. |
| Instances de Distributed Execution Manager | 443 | TCP | Communication avec Manager Service sur HTTPS. |
| agents proxy | 443 | TCP | Communication avec Manager Service et les hôtes de virtualisation sur HTTPS |
| Agent invité | 443 | TCP | Communication avec Manager Service sur HTTPS. |
| Manager Service, site Web | 1433 | TCP | MSSQL. |

Si nécessaire, configurez les ports sortants facultatifs.

Tableau 9-7. Ports sortants facultatifs

| COMPOSANT | PORT | PROTOCOLE | COMMENTAIRES |
|-----------|------|-----------|---------------------|
| Tout | 123 | TCP, UDP | NTP est facultatif. |

Audit et journalisation

Pour garantir la sécurité, il convient de configurer l'audit et la journalisation sur votre système vRealize Automation conformément aux recommandations de VMware.

La journalisation à distance vers un hôte de journalisation central fournit un stockage sécurisé pour les fichiers journaux. En collectant les fichiers journaux sur un hôte central, vous pouvez surveiller l'environnement avec un seul outil. En outre, vous pouvez effectuer une analyse cumulée et rechercher des signes de menaces telles que des attaques coordonnées sur plusieurs entités dans l'infrastructure. La connexion à un serveur de journalisation sécurisé et centralisé peut permettre d'éviter la falsification des journaux tout en fournissant un enregistrement d'audit à long terme.

Vérifier la sécurisation du serveur de journalisation à distance

Souvent, une fois que les pirates ont réussi à déjouer la sécurité de votre machine hôte, ils tentent de rechercher et de falsifier les fichiers journaux pour couvrir leurs traces et garder le contrôle sans être découverts. La sécurisation du serveur de journalisation à distance permet d'éviter la falsification des journaux.

Utiliser un serveur NTP autorisé

Assurez-vous que toutes les machines hôtes utilisent la même source d'heure relative (y compris le décalage de localisation applicable) et que vous pouvez mettre en corrélation la source d'heure relative avec une norme horaire acceptée telle que l'heure UTC (temps universel coordonné). Une approche stricte des sources d'heure vous permet de suivre et de corréliser les actions des intrus lorsque vous passez en revue les fichiers journaux applicables. Des réglages d'heure incorrects compliquent l'analyse et la corrélation des fichiers journaux pour détecter d'éventuelles attaques et peuvent compromettre la précision des audits.

Utilisez au moins trois serveurs NTP de sources d'heure extérieures ou configurez sur un réseau approuvé quelques serveurs NTP locaux dont l'heure est obtenue à partir d'au moins trois sources d'heure extérieures.