# Configuration sécurisée

vRealize Operations Manager 6.4

vmware®

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

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

Le site Web de VMware propose également les dernières mises à jour des produits.

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

# Table des matières

Configuration sécurisée 5

**1** Position en matière de sécurité de vRealize Operations Manager 7

**2** Déploiement sécurisé de vRealize Operations Manager 9
- Vérifier l'intégrité des supports d'installation 9
- Sécurisation renforcée de l'infrastructure logicielle déployée 9
- Passage en revue des logiciels installés et non pris en charge 10
- Avis de sécurité et correctifs VMware 11

**3** Configuration sécurisée de vRealize Operations Manager 13
- Sécuriser la console vRealize Operations Manager 14
- Modifier le mot de passe racine 14
- Gestion de Secure Shell, des comptes administratifs et de l'accès à la console 15
- Définir l'authentification du chargeur d'amorçage 20
- Authentification en mode utilisateur unique ou en mode de maintenance 20
- Surveiller le minimum de comptes d'utilisateur nécessaires 21
- Surveiller le minimum de groupes nécessaires 21
- Réinitialisation du mot de passe d'administrateur vRealize Operations Manager (Linux) 22
- Configurer NTP sur des dispositifs VMware 22
- Désactiver la réponse d'horodatage TCP sur Linux 23
- Activer le mode FIPS 140-2 23
- TLS pour les données en transit 24
- Ressources d'application qui doivent être protégées 27
- Configurer l'authentification client PostgreSQL 28
- Configuration d'Apache 29
- Désactiver les modes de configuration 30
- Gestion des composants logiciels non essentiels 30
- Déploiement installé sur Windows 34
- Déploiement installé sur Linux 36
- Agent Endpoint Operations Management 37
- Activités de configuration sécurisée supplémentaire 43

**4** Sécurité du réseau et communications sécurisées 45
- Configuration des paramètres réseau pour l'installation de l'application virtuelle 45
- Configuration des ports et des protocoles 54

**5** Audit et journalisation de votre système vRealize Operations Manager 57
- Sécurisation du serveur de journalisation distant 57
- Utiliser un serveur NTP autorisé 57
- Considérations relatives au navigateur client 58

Index 59

# Configuration sécurisée

La documentation relative à la *Configuration sécurisée* est destinée à servir de ligne de base sécurisée pour le déploiement de vRealize Operations Manager. Consultez ce document lorsque vous utilisez des outils de surveillance du système pour vous assurer que la configuration de la ligne de base sécurisée est surveillée et maintenue en continu, en cas de modifications inattendues.

Les activités de sécurisation renforcée qui ne sont pas déjà définies par défaut peuvent être effectuées manuellement.

## Public visé

Ces informations sont destinées aux administrateurs de vRealize Operations Manager.

## 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.

# Position en matière de sécurité de vRealize Operations Manager 1

La position en matière de sécurité de vRealize Operations Manager suppose un environnement entièrement sécurisé basé sur une configuration système et réseau, des stratégies de sécurité à l'échelle de l'entreprise et des meilleures pratiques. Il est important que vous effectuiez les activités de sécurisation renforcée conformément aux stratégies de sécurité et aux meilleures pratiques de votre entreprise.

Le document se divise en plusieurs sections :

- Déploiement sécurisé
- Configuration sécurisée
- Sécurité réseau
- Communication

Le guide décrit l'installation de l'application virtuelle. Toutefois, les types de déploiements suivants sont également abordés :

- « Déploiement installé sur Linux », page 36
- « Déploiement installé sur Windows », page 34

Pour vous assurer que votre système est correctement sécurisé, passez en revue les recommandations et évaluez-les par rapport aux stratégies de sécurité de votre entreprise et l'exposition aux risques.

# Déploiement sécurisé de vRealize Operations Manager 2

Vous devez vérifier l'intégrité du support d'installation avant d'installer le produit afin de vous assurer de l'authenticité des fichiers téléchargés.

Ce chapitre aborde les rubriques suivantes :


- « Vérifier l'intégrité des supports d'installation », page 9
- « Sécurisation renforcée de l'infrastructure logicielle déployée », page 9
- « Passage en revue des logiciels installés et non pris en charge », page 10
- « Avis de sécurité et correctifs VMware », page 11


## Vérifier l'intégrité des supports d'installation

Après avoir téléchargé le support, utilisez la valeur de somme MD5/SHA1 pour vérifier l'intégrité du téléchargement. Vérifiez toujours le hachage SHA1 après avoir téléchargé une image ISO, un bundle hors ligne ou un correctif afin de vous assurer de l'intégrité et de l'authenticité des fichiers téléchargés. Si vous obtenez un support physique de VMware et que le sceau de sécurité est brisé, retournez le logiciel à VMware pour l'échanger.

### Procédure

- Comparez la sortie de hachage MD5/SHA1 avec la valeur affichée sur le site Web de VMware.

  Le hachage SHA1 ou MD5 doit correspondre.

  **Remarque** Les fichiers vRealize Operations Manager`6.x-x.pak` sont signés par le certificat d'édition de logiciels VMware. vRealize Operations Manager valide la signature du fichier PAK avant l'installation.

## Sécurisation renforcée de l'infrastructure logicielle déployée

Dans le cadre du processus de sécurisation renforcée, vous devez renforcer la sécurité de l'infrastructure logicielle déployée prenant en charge votre système VMware.

Avant de renforcer la sécurité de votre système VMware, examinez et corrigez les défaillances de sécurité de l'infrastructure logicielle de support afin de créer un environnement totalement sécurisé. Les composants du système d'exploitation, les logiciels de prise en charge et les logiciels de base de données font partie des éléments de l'infrastructure logicielle à prendre en compte. Réglez les questions de sécurité de ces composants et d'autres composants en suivant les recommandations du fabricant ainsi que les protocoles de sécurité pertinents.

### Sécurisation renforcée de l'environnement VMware vSphere

vRealize Operations Manager s'appuie sur un environnement VMware vSphere sécurisé pour offrir des performances optimales et une infrastructure sécurisée.

Évaluez l'environnement VMware vSphere et vérifiez que le niveau approprié de sécurisation renforcée de vSphere est appliqué et maintenu.

Pour plus de recommandations sur la sécurisation renforcée, consultez l'adresse suivante : http://www.vmware.com/security/hardening-guides.html.

#### Sécurisation renforcée pour l'installation de Linux

Consultez les recommandations qui figurent dans les meilleures pratiques de sécurisation renforcée de Linux et assurez-vous de sécuriser suffisamment vos hôtes Linux. Si vous ne respectez pas les consignes de sécurisation renforcée, il se peut que le système s'expose à des défaillances de sécurité connues, à cause de composants non sécurisés dans les différentes versions de Linux.

vRealize Operations Manager est pris en charge pour une installation sur Red Hat Enterprise Linux (RHEL) 6, à partir de la version 6.5.

#### Sécurisation renforcée pour l'installation de Windows

Consultez les recommandations qui figurent dans les meilleures pratiques de sécurisation renforcée de Windows et assurez-vous de sécuriser suffisamment votre hôte Windows Server. Si vous ne respectez pas les recommandations de sécurisation renforcée, il se peut que le système s'expose à des défaillances de sécurité connues, à cause de composants non sécurisés dans les différentes versions de Windows.

Contactez votre fournisseur Microsoft afin de renforcer la sécurisation de vos produits Microsoft.

## Passage en revue des logiciels installés et non pris en charge

Des défaillances de sécurité dans les logiciels inutilisés peuvent augmenter le risque d'accès non autorisé au système et de perturbation de la disponibilité. Passez en revue les logiciels installés sur les machines hôtes VMware et évaluez leur utilisation.

N'installez pas de logiciels qui ne sont pas nécessaires au fonctionnement sécurisé du système sur aucun des hôtes du nœud vRealize Operations Manager. Désinstallez les logiciels inutilisés ou non essentiels.

L'installation de logiciels non pris en charge, non testés ou non approuvés sur des produits d'infrastructure tels que vRealize Operations Manager constitue une menace pour l'infrastructure.

Afin de minimiser la menace pour l'infrastructure, n'installez pas et n'utilisez pas de logiciels tiers qui ne sont pas pris en charge par VMware sur les hôtes VMware fournis.

Évaluez votre déploiement vRealize Operations Manager et votre 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 des produits tiers, consultez le support VMware à l'adresse https://www.vmware.com/support/policies/thirdparty.html.

### Vérifier les logiciels tiers

N'utilisez pas de logiciels tiers que VMware ne prend pas en charge. Vérifiez que tous les logiciels tiers sont configurés de manière sécurisée et que vous avez appliqué les correctifs nécessaires, conformément aux directives du fournisseur tiers.

Les défaillances de sécurité dues à des logiciels tiers non authentiques, non sécurisés ou non corrigés installés sur les machines hôtes VMware peuvent exposer le système à des risques d'accès non autorisé et de perturbation de la disponibilité. Tous les logiciels que VMware ne fournit pas doivent être sécurisés et corrigés de manière adaptée.

Si vous devez utiliser un logiciel tiers que VMware ne prend pas en charge, contactez le fournisseur tiers pour en savoir plus sur les exigences en matière de configuration sécurisée et d'application de correctifs.

## Avis de sécurité et correctifs VMware

VMware publie parfois des avis de sécurité pour ses produits. En vous tenant informé de ces avis de sécurité, vous vous assurez que vous vous bénéficiez du produit sous-jacent le plus sûr et que le produit n'est pas vulnérable aux menaces connues.

Évaluez l'installation, l'application de correctifs et l'historique des mises à niveau de vRealize Operations Manager et vérifiez que vous respectez et appliquez les avis de sécurité VMware.

Il est recommandé de toujours utiliser la version la plus récente de vRealize Operations Manager, car c'est celle qui comprendra les correctifs de sécurité les plus récents.

Pour plus d'informations sur les avis de sécurité VMware actuels, rendez-vous sur http://www.vmware.com/fr/security/advisories/.

# Configuration sécurisée de vRealize Operations Manager 3

En matière de sécurité, la meilleure pratique consiste à sécuriser la console vRealize Operations Manager et à gérer les protocoles Secure Shell (SSH), les comptes administratifs et l'accès à la console. Assurez-vous que votre système est déployé avec des canaux de transmission sécurisés.

Vous devez également suivre certaines meilleures pratiques de sécurité pour exécuter les agents Endpoint Operations Management.

Ce chapitre aborde les rubriques suivantes :


- « Sécuriser la console vRealize Operations Manager », page 14
- « Modifier le mot de passe racine », page 14
- « Gestion de Secure Shell, des comptes administratifs et de l'accès à la console », page 15
- « Définir l'authentification du chargeur d'amorçage », page 20
- « Authentification en mode utilisateur unique ou en mode de maintenance », page 20
- « Surveiller le minimum de comptes d'utilisateur nécessaires », page 21
- « Surveiller le minimum de groupes nécessaires », page 21
- « Réinitialisation du mot de passe d'administrateur vRealize Operations Manager (Linux) », page 22
- « Configurer NTP sur des dispositifs VMware », page 22
- « Désactiver la réponse d'horodatage TCP sur Linux », page 23
- « Activer le mode FIPS 140-2 », page 23
- « TLS pour les données en transit », page 24
- « Ressources d'application qui doivent être protégées », page 27
- « Configurer l'authentification client PostgreSQL », page 28
- « Configuration d'Apache », page 29
- « Désactiver les modes de configuration », page 30
- « Gestion des composants logiciels non essentiels », page 30
- « Déploiement installé sur Windows », page 34
- « Déploiement installé sur Linux », page 36
- « Agent Endpoint Operations Management », page 37
- « Activités de configuration sécurisée supplémentaire », page 43

# Sécuriser la console vRealize Operations Manager

Après avoir installé vRealize Operations Manager, vous devez vous connecter pour la première fois et sécuriser la console de chaque nœud du cluster.

### Prérequis

Installez vRealize Operations Manager.

### Procédure

1 Localisez la console de nœud dans vCenter ou à l'aide d'un accès direct.

Dans vCenter, appuyez sur Alt+F1 pour accéder à l'invite de connexion. Pour des raisons de sécurité, les sessions de terminaux à distance vRealize Operations Manager sont désactivées par défaut.

2 Connectez-vous en tant qu'utilisateur racine.

vRealize Operations Manager ne vous permet pas d'accéder à l'invite de commande tant que vous n'avez pas créé de mot de passe racine.

3 Lorsque vous êtes invité à saisir un mot de passe, appuyez sur **Entrée**.

4 Lorsque vous êtes invité à saisir votre ancien mot de passe, appuyez sur **Entrée**.

5 Lorsque vous êtes invité à saisir le nouveau mot de passe, entrez le mot de passe racine que vous voulez et notez-le pour référence ultérieure.

6 Réinitialisez le mot de passe racine.

7 Déconnectez-vous de la console.

# Modifier le mot de passe racine

Vous pouvez modifier le mot de passe racine pour tout nœud maître ou de données vRealize Operations Manager à tout moment en utilisant la console.

L'utilisateur racine contourne la vérification de la complexité des mots de passe du module `pam_cracklib`, qui se trouve dans le fichier `etc/pam.d/common-password`. Toutes les appliances sécurisées activent `enforce_for_root` pour le module `pw_history`, qui se trouve 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/security/opasswd`.

### Prérequis

Vérifiez que le mot de passe racine de l'appliance répond aux exigences de complexité des mots de passe de votre entreprise. Si le mot de passe du compte commence par `$6$`, il utilise un hachage sha512. Il s'agit du hachage standard pour toutes les appliances sécurisées.

### Procédure

1 Exécutez la commande `# passwd` sur le shell racine de l'appliance.

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

Les informations de hachage s'affichent.

3 Si le mot de passe racine ne contient pas de hachage sha512, exécutez la commande `passwd` afin de le modifier.

## Gérer l'expiration des mots de passe

Configurez toutes les expirations de mots de passe conformément aux stratégies de sécurité de votre entreprise.

Par défaut, toutes les appliances VMware sécurisées utilisent un délai d'expiration des mots de passe de 60 jours. Sur la plupart des appliances sécurisées, le délai d'expiration des mots de passe du compte racine est défini sur 365 jours. La meilleure pratique consiste à vérifier que le délai d'expiration sur tous les comptes répond aux exigences de sécurité et de fonctionnement.

Si le mot de passe racine expire, vous ne pouvez pas le rétablir. Vous devez mettre en œuvre des stratégies propres au site pour éviter l'expiration des mots de passe administratifs et racine.

**Procédure**

1 Connectez-vous à vos appliances virtuelles en tant qu'utilisateur racine et exécutez la commande `# more /etc/shadow` pour vérifier le délai d'expiration des mots de passe sur tous les comptes.

2 Pour modifier la date d'expiration du compte racine, exécutez la commande `# 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 spécifique par `root` et en remplaçant le nombre de jours pour répondre aux normes d'expiration de l'entreprise.

Par défaut, le mot de passe racine est défini sur 365 jours.

# Gestion de Secure Shell, des comptes administratifs et de l'accès à la console

Pour les connexions à distance, toutes les appliances sécurisées comprennent le protocole Secure Shell (SSH). SSH est désactivé par défaut sur l'appliance sécurisée.

SSH est un environnement de ligne de commande interactif qui prend en charge les connexions à distance vers un nœud vRealize Operations Manager. SSH nécessite des informations d'identification de compte d'utilisateur hautement privilégié. Les activités SSH contournent généralement le contrôle d'accès basé sur les rôles et les contrôles d'audit du nœud vRealize Operations Manager.

La meilleure pratique consiste à désactiver SSH dans l'environnement de production et de l'activer uniquement pour diagnostiquer ou résoudre les problèmes que vous ne pouvez pas résoudre par d'autres moyens. Laissez cette option activée uniquement lorsque vous en avez besoin dans un but précis et conformément aux stratégies de sécurité de votre entreprise. Si vous activez SSH, assurez-vous qu'il est protégé contre les attaques et que vous ne l'activez qu'aussi longtemps que nécessaire. Selon votre configuration vSphere, vous pouvez activer ou désactiver SSH lorsque vous déployez votre modèle Open Virtualization Format (OVF).

Pour déterminer si SSH est activé sur une machine, il suffit d'essayer d'ouvrir une connexion à l'aide de SSH. Si la connexion s'ouvre et demande les informations d'identification, SSH est activé et est disponible pour établir des connexions.

## Utilisateur racine Secure Shell

Étant donné que les appliances VMware n'incluent pas de comptes d'utilisateur préconfigurés par défaut, le compte racine peut utiliser SSH pour se connecter directement par défaut. Désactivez SSH en tant que racine dès que possible.

Pour répondre aux normes de conformité en matière de non-répudiation, le serveur SSH sur toutes les appliances sécurisées est préconfiguré avec l'entrée wheel AllowGroups pour restreindre l'accès SSH au groupe wheel secondaire. Pour séparer les tâches, vous pouvez modifier l'entrée wheel AllowGroups 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 super-utilisateur, de sorte que les membres du groupe wheel peuvent utiliser la commande su-root, qui nécessite le mot de passe racine. La séparation du groupe permet aux utilisateurs d'utiliser SSH sur l'appliance, mais pas d'utiliser la commande su pour se connecter en tant qu'utilisateur racine. Évitez de supprimer ou de modifier d'autres entrées dans le champ AllowGroups, de manière à garantir le bon fonctionnement de l'appliance. Après avoir effectué une modification, redémarrez le démon SSH en exécutant la commande `# service sshd restart`.

## Activer ou désactiver Secure Shell sur un nœud vRealize Operations Manager

Vous pouvez activer Secure Shell (SSH) sur un nœud vRealize Operations Manager à des fins de dépannage. Par exemple, pour dépanner un serveur, vous pouvez avoir besoin d'y accéder en mode console. Cela est possible via SSH. Désactivez SSH sur un nœud vRealize Operations Manager en mode de fonctionnement normal.

### Procédure

1 Accédez à la console du nœud vRealize Operations Manager à partir de vCenter.

2 Appuyez sur Alt+F1 pour accéder à l'invite de connexion, puis connectez-vous.

3 Exécutez la commande `#chkconfig`.

4 Si le service SSHD est désactivé, exécutez la commande `#chkconfig sshd on`.

5 Exécutez la commande `#service sshd start` pour démarrer le service SSHD.

6 Exécutez la commande `#service sshd stop` pour arrêter le service SSHD.

## Créer un compte administratif local pour Secure Shell

Vous devez créer des comptes administratifs locaux pouvant être utilisés en tant que Secure Shell (SSH) et faisant partie du groupe wheel secondaire, avant de supprimer l'accès SSH racine.

Avant de désactiver l'accès racine direct, vérifiez que les administrateurs autorisés ont accès à SSH à l'aide d'`AllowGroups` et qu'ils peuvent utiliser le groupe wheel et la commande `su` pour se connecter en tant qu'utilisateur racine.

### Procédure

1 Connectez-vous en tant qu'utilisateur racine et exécutez les commandes suivantes.

```
# useradd –d /home/vropsuser –g users –G wheel –m
# passwd username
```

Le groupe wheel est spécifié dans `AllowGroups` pour l'accès SSH. Pour ajouter plusieurs groupes secondaires, utilisez `–G wheel,sshd`.

2 Passez en mode utilisateur et fournissez un nouveau mot de passe qui réponde aux critères de complexité des mots de passe.

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

Si tel est le cas, le mot de passe est mis à jour. Dans le cas contraire, le mot de passe initial est rétabli et vous devez exécuter à nouveau la commande password.

Après avoir créé les comptes de connexion pour autoriser l'accès SSH à distance et utilisé la commande `su` pour vous connecter en tant qu'utilisateur racine à l'aide de l'accès wheel, vous pouvez supprimer le compte racine de la connexion directe SSH.

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

### Suivant

Désactivez les connexions directes en tant qu'utilisateur racine. Par défaut, les dispositifs sécurisés de manière renforcée permettent une connexion directe à la racine via la console. Après avoir créé des comptes administratifs pour la non-répudiation et testé l'accès wheel (`su–root`), désactivez les connexions directes en tant qu'utilisateur racine en modifiant le fichier `/etc/security` en tant qu'utilisateur racine et en remplaçant l'entrée `tty1` par `console`.

## Restreindre l'accès à Secure Shell

Dans le cadre de votre processus de sécurisation renforcée du système, limitez l'accès à Secure Shell (SSH) en configurant le module tcp_wrappers correctement sur toutes les machines hôtes de vos appliances virtuelles VMware. Maintenez également les autorisations de fichier clé SSH requises sur ces appliances.

Toutes les appliances virtuelles VMware comprennent le package tcp_wrappers qui permet aux démons pris en charge par TCP de contrôler les sous-réseaux qui peuvent accéder aux démons compilés avec libwrap. Par défaut, le fichier `/etc/hosts.allow` contient une entrée générique, `sshd: ALL : ALLOW`, qui permet à tous d'accéder à Secure Shell. Restreignez cet accès conformément aux besoins de votre entreprise.

### Procédure

1 Ouvrez le fichier `/etc/hosts.allow` sur une machine hôte d'appliance virtuelle 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 le sous-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 avec l'hôte local et les connexions que les clients établissent sur le sous-réseau 10.0.0.0 sont autorisées.

3 Ajoutez toutes les informations d'identification de la machine appropriées, par exemple, le nom d'hôte, l'adresse IP, le nom de domaine complet (FQDN) et l'adresse de bouclage.

4 Enregistrez le fichier et fermez-le.

## Maintenir les autorisations de fichier clé Secure Shell

Afin de maintenir un niveau adéquat de sécurité, configurez les autorisations de fichier clé Secure Shell (SSH).

### Procédure

1 Afficher les fichiers clés de l'hôte public, qui se trouvent dans `/etc/ssh/*key.pub`.

2 Vérifiez que ces fichiers et le groupe appartiennent à la racine et que les autorisations des fichiers sont définies sur 0644.

Les autorisations sont (-rw-r--r--).

3 Fermez tous les fichiers.

4 Affichez les fichiers clés de l'hôte privé, qui se trouvent dans `/etc/ssh/*key`.

5 Vérifiez que ces fichiers et le groupe appartiennent à la racine et que les autorisations des fichiers sont définies sur 0600.

Les autorisations sont (-rw-------).

6 Fermez tous les fichiers.

## Renforcer la sécurité de la configuration du serveur Secure Shell

Lorsque cela est possible, l'installation de l'application virtuelle (format OVF) présente une configuration sécurisée par défaut. Les utilisateurs peuvent vérifier que leur configuration est suffisamment sécurisée en examinant les services serveur et client dans la section d'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` et vérifiez que les paramètres sont corrects.

| Configuration | Statut |
|---|---|
| Protocole démon du serveur | 2 |
| Chiffrements | Ciphers aes256-ctr,aes128-ctr |
| Transfert TCP | AllowTCPForwarding no |
| Ports de passerelle serveur | Gateway Ports no |
| Transfert X11 | X11Forwarding no |
| Service SSH | Utilisez le champ AllowGroups et spécifiez un groupe bénéficiant d'un accès autorisé. Ajoutez au groupe secondaire les utilisateurs autorisés à utiliser le service. |
| Authentification GSSAPI | GSSAPIAuthentication no, si elle n'est pas utilisée |
| Authentification Kerberos | KerberosAuthentication no, si elle n'est pas utilisée |
| Variables locales (option globale AcceptEnv) | `Désactiver par la mise en commentaire` ou `activer les varialbles LC_* ou LANG seulement` |
| Configuration de tunnel | PermitTunnel no |
| Sessions réseau | MaxSessions 1 |
| Vérification du mode Strict | Strict Modes yes |
| Séparation des privilèges | UsePrivilegeSeparation yes |
| Authentification RSA rhosts | RhostsRSAAuthentication no |
| Compression | Compression delayed ou Compression no |
| Code d'authentification de message | MACs hmac-sha1 |
| Restriction d'accès utilisateur | PermitUserEnvironment no |

2 Enregistrez les modifications et fermez le fichier.

## Renforcer la sécurité de la configuration du client Secure Shell

Dans le cadre du processus de surveillance de la sécurisation renforcée du système, vérifiez la sécurisation du client SSH en examinant le fichier de configuration de ce dernier sur les machines hôtes de vos dispositifs virtuels pour vous assurer que les instructions VMware sont respectées.

### Procédure

1 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.

| Paramètre | Statut |
|---|---|
| **Protocole client** | 2 |
| **Ports passerelle client** | Gateway Ports no |
| **Authentification GSSAPI** | GSSAPIAuthentication no |
| **Variables locales (option globale SendEnv)** | LC_* ou LANG |
| **Chiffrements CBC** | Ciphers aes256-ctr,aes128-ctr |
| **Codes d'authentification de message** | Utilisés uniquement dans l'entrée `MACs hmac-sha1` |

2 Enregistrez les modifications et fermez le fichier.

## Désactiver les connexions directes en tant qu'utilisateur racine

Par défaut, les dispositifs sécurisés de manière renforcée vous permettent d'utiliser la console pour vous connecter directement en tant qu'utilisateur racine. En matière de sécurité, la meilleure pratique consiste à désactiver les connexions directes après avoir créé un compte administratif pour la non-répudiation et testé l'accès wheel en utilisant la commande `su-root`.

### Prérequis

- Suivez les étapes décrites dans la section « Créer un compte administratif local pour Secure Shell », page 16.
- Vérifiez que le système est accessible par un administrateur avant de désactiver les connexions directes en tant qu'utilisateur racine.

### Procédure

1 Connectez-vous en tant qu'utilisateur racine et accédez au fichier `/etc/security`.

Vous pouvez accéder à ce fichier depuis l'invite de commande.

2 Remplacez l'entrée `tty1` par `console`.

### Désactiver l'accès SSH pour le compte d'utilisateur Admin

Il est recommandé de désactiver l'accès SSH pour le compte d'utilisateur Admin. Le compte d'administrateur vRealize Operations Manager et le compte d'administrateur Linux partagent le même mot de passe. En désactivant l'accès SSH de l'utilisateur Admin, vous garantissez une protection élevée en obligeant tous les utilisateurs du SSH à se connecter d'abord avec un compte qui dispose de privilèges limités, avec un mot de passe différent de celui du compte d'administrateur vRealize Operations Manager, puis à passer à un compte qui dispose de plus de privilèges, comme le compte d'administrateur ou le compte racine.

#### Procédure

1 Modifiez le fichier `/etc/ssh/sshd_config`.

Vous pouvez accéder à ce fichier depuis l'invite de commande.

2 Ajoutez l'entrée `DenyUsers admin` n'importe où dans le fichier et sauvegardez-le.

3 Pour redémarrer le serveur sshd, exécutez la commande `service sshd restart`.

## Définir l'authentification du chargeur d'amorçage

Afin d'assurer un niveau approprié de sécurité, configurez l'authentification du chargeur d'amorçage sur vos appliances virtuelles VMware. Si le chargeur d'amorçage du système ne nécessite pas d'authentification, les utilisateurs disposant d'un accès console au système pourraient être capables de modifier la configuration d'amorçage du système ou de démarrer le système en mode utilisateur unique ou en mode de maintenance, ce qui pourrait entraîner un déni de service ou un accès non autorisé au système.

Étant donné que l'authentification du chargeur d'amorçage n'est pas définie par défaut sur les appliances virtuelles VMware, vous devez créer un mot de passe GRUB pour la configurer.

#### Procédure

1 Vérifiez si un mot de passe d'amorçage existe en localisant la ligne `password --md5 <password-hash>` dans le fichier `/boot/grub/menu.lst` sur vos appliances virtuelles.

2 Si aucun mot de passe n'existe, exécutez la commande `# /usr/sbin/grub-md5-crypt` sur votre appliance virtuelle.

Un mot de passe MD5 est généré et la commande alimente 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>`.

## Authentification en mode utilisateur unique ou en mode de maintenance

Si le système n'exige pas d'authentification racine valide avant de démarrer en mode utilisateur unique ou en mode de maintenance, n'importe quel utilisateur qui utilise le mode utilisateur unique ou le mode de maintenance bénéficiera d'un accès privilégié à tous les fichiers du système.

#### Procédure

- Passez en revue le fichier `/etc/inittab` et assurez-vous que les deux lignes suivantes s'affichent : `ls:S:wait:/etc/init.d/rc S` et `~~:S:respawn:/sbin/sulogin`.

# Surveiller le minimum de comptes d'utilisateur nécessaires

Vous devez surveiller les comptes d'utilisateur existants afin de vous assurer que tous les comptes d'utilisateur inutiles sont supprimés.

### Procédure

- Exécutez la commande *hôte*`:~ # cat /etc/passwd` pour vérifier le minimum de comptes d'utilisateur nécessaires.

```
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
haldaemon:x:101:102:User for haldaemon:/var/run/hald:/bin/false
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:100:101:User for D-Bus:/var/run/dbus:/bin/false
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
ntp:x:74:106:NTP daemon:/var/lib/ntp:/bin/false
polkituser:x:103:104:PolicyKit:/var/run/PolicyKit:/bin/false
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
root:x:0:0:root:/root:/bin/bash
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
suse-ncc:x:104:107:Novell Customer Center User:/var/lib/YaST2/suse-ncc-fakehome:/bin/bash
uuidd:x:102:103:User for uuidd:/var/run/uuidd:/bin/false
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
nginx:x:105:108:user for nginx:/var/lib/nginx:/bin/false
admin:x:1000:1003::/home/admin:/bin/bash
tcserver:x:1001:1004:tc Server User:/home/tcserver:/bin/bash
postgres:x:1002:100::/var/vmware/vpostgres/9.3:/bin/bash
```

# Surveiller le minimum de groupes nécessaires

Vous devez surveiller les groupes existants et leurs membres afin de vous assurer que tous les groupes ou accès aux groupes inutiles sont supprimés.

### Procédure

- Exécutez la commande `<host>:~ # cat /etc/group` pour vérifier le minimum de groupes nécessaires et l'appartenance aux groupes.

```
audio:x:17:
bin:x:1:daemon
cdrom:x:20:
console:x:21:
daemon:x:2:
dialout:x:16:u1,tcserver,postgres
disk:x:6:
floppy:x:19:
haldaemon:!:102:
kmem:x:9:
mail:x:12:
man:x:62:
messagebus:!:101:
modem:x:43:
nobody:x:65533:
nogroup:x:65534:nobody
ntp:!:106:
```

```
polkituser:!:105:
public:x:32:
root:x:0:admin
shadow:x:15:
sshd:!:65:
suse-ncc:!:107:
sys:x:3:
tape:!:103:
trusted:x:42:
tty:x:5:
utmp:x:22:
uuidd:!:104:
video:x:33:u1,tcserver,postgres
wheel:x:10:root,admin
www:x:8:
xok:x:41:
maildrop:!:1001:
postfix:!:51:
users:x:100:
vami:!:1002:root
nginx:!:108:
admin:!:1003:
vfabric:!:1004:admin,wwwrun
```

# Réinitialisation du mot de passe d'administrateur vRealize Operations Manager (Linux)

En matière de sécurité, la meilleure pratique consiste à réinitialiser le mot de passe vRealize Operations Manager sur les clusters Linux pour les installations vApp ou Linux.

### Procédure

1 Connectez-vous à la console distante du nœud maître en tant que racine.

2 Entrez la commande `$VMWARE_PYTHON_BIN $VCOPS_BASE/../vmware-vcopssuite/utilities/sliceConfiguration/bin/vcopsSetAdminPassword.py --reset`, puis suivez les invites.

# Configurer NTP sur des dispositifs VMware

Si la source horaire est capitale, désactivez la synchronisation temporelle de l'hôte et utilisez NTP (Network Time Protocol) sur les dispositifs VMware. Vous devez configurer un serveur NTP distant approuvé pour la synchronisation de l'heure. Le serveur NTP doit être un serveur de temps de référence ou être au moins synchronisé avec un serveur de ce type.

Le démon NTP sur les dispositifs virtuels VMware fournit des services de temps synchronisés. 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 de potentielles attaques et intrusions malveillantes via un audit et une journalisation détaillés. Pour plus d'informations sur les consignes de sécurité NTP, visitez le site Web NTP.

Le fichier de configuration NTP est situé sur chaque dispositif dans `/etc/ntp.conf`.

### Procédure

1 Accédez au fichier de configuration `/etc/ntp.conf` sur la machine hôte de votre dispositif virtuel.

2 Définissez les droits de propriété du fichier sur **`root:root`**.

3 Définissez les autorisations sur **0640**.

4 Pour limiter le risque d'une attaque par déni de service par amplification sur le service NTP, ouvrez le fichier `/etc/ntp.conf` et assurez-vous que les lignes de restriction y figurent.

```
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.

Pour plus d'informations sur les consignes de sécurité NTP, rendez-vous sur http://support.ntp.org/bin/view/Main/SecurityNotice.

# Désactiver la réponse d'horodatage TCP sur Linux

Utilisez la réponse d'horodatage TCP pour estimer le temps d'activité de l'hôte distant et empêcher de nouvelles attaques. Il est par ailleurs possible de relever l'empreinte digitale de certains systèmes d'exploitation en fonction du comportement de leurs horodatages TCP.

### Procédure

- Désactivez la réponse d'horodatage TCP sur Linux.
  a Pour définir la valeur de `net.ipv4.tcp_timestamps` sur `0`, exécutez la commande `sysctl –w net.ipv4.tcp_timestamps=0`.
  b Ajoutez la valeur `ipv4.tcp_timestamps=0` dans le fichier par défaut `sysctl.conf`.

# Activer le mode FIPS 140-2

La version d'OpenSSL livrée avec vRealize Operations Manager 6.3 et ses versions ultérieures est certifiée FIPS 140-2. Cependant, le mode FIPS n'est pas activé par défaut.

Vous pouvez activer le mode FIPS si des algorithmes de cryptographie certifiés FIPS doivent être utilisés avec le mode FIPS activé pour des raisons de conformité de sécurité.

### Procédure

1 Pour remplacer le fichier `mod_ssl.so`, exécutez la commande suivante :

```
cd /usr/lib64/apache2–prefork/
cp mod_ssl.so mod_ssl.so.old
cp mod_ssl.so.FIPSON.openssl1.0.2 mod_ssl.so
```

2 Adaptez votre configuration Apache2 en modifiant le fichier `/etc/apache2/ssl–global.conf`.

3 Recherchez la ligne `<IfModule mod_ssl.c>` et ajoutez la directive `SSLFIPS on` en dessous.

4 Pour réinitialiser la configuration Apache, exécutez la commande `service apache2 restart`.

# TLS pour les données en transit

En matière de sécurité, la meilleure pratique consiste à s'assurer que le système est déployé avec des canaux de transmission sécurisés.

## Configurer des protocoles fiables pour vRealize Operations Manager

Les protocoles tels que SSLv2 et SSLv3 ne sont plus considérés comme sûrs. En outre, il est recommandé de désactiver TLS 1.0. Activez uniquement TLS 1.1 et TLS 1.2.

### Vérifier le bon usage des protocoles dans le gestionnaire Apache HTTPD

vRealize Operations Manager désactive SSLv2 et SSLv3 par défaut. Vous devez désactiver les protocoles faibles sur tous les équilibreurs de charge avant de mettre le système en production.

#### Procédure

1 Exécutez la commande `grep SSLProtocol /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf | grep -v '#'` à partir de l'invite de commande afin de vérifier que les protocoles SSLv2 et SSLv3 sont désactivés.

   Si les protocoles sont désactivés, la commande renvoie la sortie suivante : `SLProtocol All -SSLv2 -SSLv3`

2 Pour désactiver également le protocole TLS 1.0, exécutez la commande `sed -i "/^[^#]*SSLProtocol/ c\SSLProtocol All -SSLv2 -SSLv3 -TLSv1" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` à partir de l'invite de commande.

3 Pour redémarrer le serveur Apache2, exécutez la commande `/etc/init.d/apache2 restart` à partir de l'invite de commande.

### Vérifier le bon usage des protocoles dans le gestionnaire GemFire TLS

vRealize Operations Manager désactive le protocole SSLv3 par défaut. Vous devez désactiver les protocoles faibles sur tous les équilibreurs de charge avant de mettre le système en production.

#### Procédure

1 Vérifiez que les protocoles sont activés. Pour vérifier que les protocoles sont activés, exécutez les commandes suivantes sur chaque nœud :

   ```
   grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.properties | grep -v '#'
   ```

   Le résultat suivant doit apparaître :

   ```
   cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
   grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.native.properties | grep -v '#'
   ```

   Le résultat suivant doit apparaître :

   ```
   cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
   grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties | grep -v '#'
   ```

   Le résultat suivant doit apparaître :

   ```
   cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
   ```

2 Désactivez le protocole TLS 1.0.

a Accédez à l'interface utilisateur d'administration : `url/admin`.

b Cliquez sur **Mettre hors ligne**.

c Pour désactiver les protocoles SSLv3 et TLS 1.0, exécutez les commandes suivantes :

```
sed –i "/^[^#]*cluster–ssl–protocol/ c\cluster–ssl–protocols=TLSv1.2
TLSv1.1" /usr/lib/vmware–vcops/user/conf/gemfire.properties
sed –i "/^[^#]*cluster–ssl–protocol/ c\cluster–ssl–protocols=TLSv1.2
TLSv1.1" /usr/lib/vmware–vcops/user/conf/gemfire.native.properties
sed –i "/^[^#]*cluster–ssl–protocol/ c\cluster–ssl–protocols=TLSv1.2
TLSv1.1" /usr/lib/vmware–vcops/user/conf/gemfire.locator.properties
```

Répétez cette étape pour chaque nœud.

d Accédez à l'interface utilisateur d'administration.

e Cliquez sur **Mettre en ligne**.

3 Réactivez le protocole TLS 1.0.

a Accédez à l'interface utilisateur d'administration pour mettre le cluster hors ligne : `url/admin`.

b Cliquez sur **Mettre hors ligne**.

c Pour vous assurer que les protocoles SSLv3 et TLS 1.0 sont désactivés, exécutez les commandes suivantes :

```
sed –i "/^[^#]*cluster–ssl–protocol/ c\cluster–ssl–protocols=TLSv1.2 TLSv1.1
TLSv1" /usr/lib/vmware–vcops/user/conf/gemfire.properties
sed –i "/^[^#]*cluster–ssl–protocol/ c\cluster–ssl–protocols=TLSv1.2 TLSv1.1
TLSv1" /usr/lib/vmware–vcops/user/conf/gemfire.native.properties
sed –i "/^[^#]*cluster–ssl–protocol/ c\cluster–ssl–protocols=TLSv1.2 TLSv1.1
TLSv1" /usr/lib/vmware–vcops/user/conf/gemfire.locator.properties
```

Répétez cette étape pour chaque nœud.

d Accédez à l'interface utilisateur d'administration pour mettre le cluster en ligne.

e Cliquez sur **Mettre en ligne**.

## Configurer vRealize Operations Manager pour l'utilisation de chiffrements forts

Pour une sécurité maximale, vous devez configurer les composants de vRealize Operations Manager pour l'utilisation de chiffrements forts. Pour vous assurer que seuls des chiffrements forts sont sélectionnés, désactivez l'utilisation des chiffrements faibles. Configurez le serveur pour qu'il prenne en charge uniquement les chiffrements forts et pour qu'il utilise des clés suffisamment grandes. Par ailleurs, configurez les chiffrements dans l'ordre approprié.

vRealize Operations Manager désactive l'utilisation des suites de chiffrement à l'aide de l'échange de clés DHE par défaut. Assurez-vous de désactiver les mêmes suites de chiffrement faibles sur tous les équilibreurs de charge avant la mise en production du système.

### Utilisation de chiffrements forts

Le chiffrement négocié entre le serveur et le navigateur détermine la méthode d'échange de clés et la force du chiffrement utilisée dans une session TLS.

## Vérifier le bon usage des suites de chiffrement dans le gestionnaire Apache HTTPD

Pour une sécurité maximale, vérifiez le bon usage des suites de chiffrement dans le gestionnaire Apache httpd.

### Procédure

1 Pour vérifier l'utilisation appropriée des suites de chiffrement dans Apache httpd, exécutez la commande `grep SSLCipherSuite /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf | grep -v '#'` à partir de l'invite de commande.

Si le gestionnaire Apache httpd utilise les suites de chiffrement appropriées, la commande renvoie la sortie suivante : `SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA +AES:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH`

2 Pour configurer l'utilisation appropriée des suites de chiffrement, exécutez la commande `sed -i "/^[^#]*SSLCipherSuite/ c\SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH +AES:RSA+AES:\!aNULL\!ADH:\!EXP:\!MD5:\!3DES:\!CAMELLIA:\!PSK:\!SRP:\!DH" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` à partir de l'invite de commande.

Exécutez cette commande si la sortie obtenue à l'étape 1 diffère de la sortie attendue.

Cette commande désactive toutes les suites de chiffrement qui utilisent les méthodes d'échange de clés DH et DHE.

3 Exécutez la commande `/etc/init.d/apache2 restart` à partir de l'invite de commande pour redémarrer le serveur Apache2.

4 Pour réactiver DH, supprimez `!DH` des suites de chiffrement en exécutant la commande `sed -i "/^[^#]*SSLCipherSuite/ c\SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH +AES:RSA+AES:\!aNULL\!ADH:\!EXP:\!MD5:\!3DES:\!CAMELLIA:\!PSK:\!SRP" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` à partir de l'invite de commande.

5 Exécutez la commande `/etc/init.d/apache2 restart` à partir de l'invite de commande pour redémarrer le serveur Apache2.

## Vérifier le bon usage des suites de chiffrement dans le gestionnaire GemFire TLS

Pour une sécurité maximale, vérifiez le bon usage des suites de chiffrement dans le gestionnaire GemFire TLS.

### Procédure

1 Pour vérifier que les suites de chiffrement et les protocoles sont activés, exécutez les commandes suivantes sur chaque nœud :

```
grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.properties | grep -v '#'

grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.native.properties | grep -v '#'

grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties | grep -v '#'
```

2 Configurez les suites de chiffrement appropriées.

a Accédez à l'interface utilisateur d'administration : *URL*`/admin`.

b Pour mettre le cluster hors ligne, cliquez sur **Mettre hors ligne**.

c Pour configurer les suites de chiffrement appropriées, exécutez les commandes suivantes :

```
sed –i "/^[^#]*cluster–ssl–ciphers/ c\cluster–ssl–
ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware–
vcops/user/conf/gemfire.properties

sed –i "/^[^#]*cluster–ssl–ciphers/ c\cluster–ssl–
ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware–
vcops/user/conf/gemfire.native.properties

sed –i "/^[^#]*cluster–ssl–ciphers/ c\cluster–ssl–
ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware–
vcops/user/conf/gemfire.locator.properties
```

Répétez cette étape pour chaque nœud.

d Accédez à l'interface utilisateur d'administration : *URL*/admin.

e Cliquez sur **Mettre en ligne**.

# Ressources d'application qui doivent être protégées

En matière de sécurité, la meilleure pratique consiste à s'assurer que les ressources d'application sont protégées.

Suivez les étapes ci-dessous pour vous assurer que les ressources d'application sont protégées.

### Procédure

1 Exécutez la commande `Find / –path /proc –prune –o –type f –perm +6000 –ls` pour vérifier que les fichiers ont un ensemble de bits SUID et GUID bien défini.

La liste suivante s'affiche :

```
354131   24 –rwsr–xr–x   1 polkituser root 23176 /usr/lib/PolicyKit/polkit–set–default–helper
354126   20 –rwxr–sr–x   1 root     polkituser    19208 /usr/lib/PolicyKit/polkit–grant–
helper
354125   20 –rwxr–sr–x   1 root     polkituser    19008 /usr/lib/PolicyKit/polkit–explicit–
grant–helper
354130   24 –rwxr–sr–x   1 root     polkituser    23160 /usr/lib/PolicyKit/polkit–revoke–
helper
354127   12 –rwsr–x–––   1 root     polkituser    10744 /usr/lib/PolicyKit/polkit–grant–
helper–pam
354128   16 –rwxr–sr–x   1 root     polkituser    14856 /usr/lib/PolicyKit/polkit–read–auth–
helper
 73886   84 –rwsr–xr–x   1 root     shadow      77848 /usr/bin/chsh
 73888   88 –rwsr–xr–x   1 root     shadow      85952 /usr/bin/gpasswd
 73887   20 –rwsr–xr–x   1 root     shadow      19320 /usr/bin/expiry
 73890   84 –rwsr–xr–x   1 root     root        81856 /usr/bin/passwd
 73799  240 –rwsr–xr–x   1 root     root       238488 /usr/bin/sudo
 73889   20 –rwsr–xr–x   1 root     root        19416 /usr/bin/newgrp
 73884   92 –rwsr–xr–x   1 root     shadow      86200 /usr/bin/chage
 73885   88 –rwsr–xr–x   1 root     shadow      82472 /usr/bin/chfn
 73916   40 –rwsr–x–––   1 root     trusted     40432 /usr/bin/crontab
296275   28 –rwsr–xr–x   1 root     root        26945 /usr/lib64/pt_chown
353804  816 –r–xr–sr–x   1 root     mail       829672 /usr/sbin/sendmail
278545   36 –rwsr–xr–x   1 root     root        35792 /bin/ping6
278585   40 –rwsr–xr–x   1 root     root        40016 /bin/su
278544   40 –rwsr–xr–x   1 root     root        40048 /bin/ping
278638   72 –rwsr–xr–x   1 root     root        69240 /bin/umount
```

```
278637  100 -rwsr-xr-x   1 root     root        94808 /bin/mount
475333   48 -rwsr-x---   1 root     messagebus    47912 /lib64/dbus-1/dbus-daemon-launch-
helper
 41001   36 -rwsr-xr-x   1 root     shadow      35688 /sbin/unix_chkpwd
 41118   12 -rwsr-xr-x   1 root     shadow      10736 /sbin/unix2_chkpwd
```

2 Exécutez la commande `find / -path */proc -prune -o -nouser -o -nogroup` pour vérifier que tous les fichiers de la vApp ont un propriétaire.

   S'il n'y a aucun résultat, tous les fichiers ont un propriétaire.

3 Exécutez la commande `find / -name "*.*" -type f -perm -a+w | xargs ls -ldb` pour vérifier qu'aucun des fichiers n'est un fichier inscriptible par tout le monde en examinant les autorisations de tous les fichiers sur la vApp.

   Aucun des fichiers ne doit inclure l'autorisation `xx2`.

4 Exécutez la commande `find / -path */proc -prune -o ! -user root -o -user admin -print` pour vérifier que les fichiers appartiennent au bon utilisateur.

   S'il n'y a aucun résultat, tous les fichiers appartiennent soit à `root` soit à `admin`.

5 Exécutez la commande `find /usr/lib/vmware-casa/ -type f -perm -o=w` pour vous assurer que les fichiers du répertoire `/usr/lib/vmware-casa/` ne sont pas inscriptibles par tout le monde.

   Il ne doit pas y avoir de résultats.

6 Exécutez la commande `find /usr/lib/vmware-vcops/ -type f -perm -o=w` pour vous assurer que les fichiers du répertoire `/usr/lib/vmware-vcops/` ne sont pas inscriptibles par tout le monde.

   Il ne doit pas y avoir de résultats.

7 Exécutez la commande `find /usr/lib/vmware-vcopssuite/ -type f -perm -o=w` pour vous assurer que les fichiers du répertoire `/usr/lib/vmware-vcopssuite/` ne sont pas inscriptibles par tout le monde.

   Il ne doit pas y avoir de résultats.

# Configurer l'authentification client PostgreSQL

Vous pouvez configurer le système pour l'authentification du client. Vous pouvez configurer le système pour l'authentification trust locale. Cela permet à tout utilisateur local, y compris le super-utilisateur de la base de données, de se connecter en tant qu'utilisateur PostgreSQL sans mot de passe. Si vous souhaitez fournir une défense solide et si vous ne faites pas confiance à tous les comptes d'utilisateur locaux, utilisez une autre méthode d'authentification. La méthode md5 est définie par défaut. Vérifiez que la méthode md5 est définie pour toutes les connexions locales et hôtes.

Vous trouverez les paramètres de configuration de l'authentification client pour l'instance de service Postgres dans `/storage/db/vcops/vpostgres/data/pg_hba.conf`. Vérifiez que la méthode md5 est définie pour toutes les connexions locales et hôtes.

Vous trouverez les paramètres de configuration de l'authentification client pour l'instance de service postgres-repl dans `/storage/db/vcops/vpostgres/repl/pg_hba.conf`. Vérifiez que la méthode md5 est définie pour toutes les connexions locales et hôtes.

**Remarque** Ne modifiez pas les paramètres de configuration client pour le compte d'utilisateur PostgreSQL.

# Configuration d'Apache

## Désactiver la navigation dans les répertoires Web

En matière de sécurité, la meilleure pratique consiste à s'assurer que l'utilisateur ne peut pas parcourir un répertoire car cela pourrait accroître le risque d'exposition aux attaques par traversée de répertoires.

### Procédure

- Vérifiez que la navigation dans les répertoires Web est désactivée pour tous les répertoires.
  a. Ouvrez les fichiers `/etc/apache2/default-server.conf` et `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` dans un éditeur de texte.
  b. Vérifier que pour chaque liste `<Directory>`, l'option `Indexes` de la balise concernée est omise de la ligne `Options`.

## Supprimer l'exemple de code pour le serveur Apache2

Apache inclut deux exemples de script CGI (Common Gateway Interface), `printenv` et `test-cgi`. Un serveur Web de production doit contenir uniquement les composants nécessaires sur le plan opérationnel. Ces composants sont susceptibles de divulguer à un pirate des informations critiques sur le système.

En matière de sécurité, la meilleure pratique consiste à supprimer les scripts CGI du répertoire `cgi-bin`.

### Procédure

- Pour supprimer les scripts `test-cgi` et `prinenv`, exécutez les commandes `rm /usr/share/doc/packages/apache2/test-cgi` et `rm /usr/share/doc/packages/apache2/printenv`.

## Vérifier les jetons de serveur pour le serveur Apache2

Dans le cadre de votre processus de sécurisation renforcée du système, vérifiez les jetons de serveur pour le serveur Apache2. L'en-tête de réponse de serveur Web figurant dans une réponse HTTP peut contenir plusieurs champs d'information. Les informations incluent la page HTML demandée, le type et la version du serveur Web, le système d'exploitation et sa version, ainsi que les ports associés au serveur Web. Elles fournissent aux utilisateurs malveillants d'importantes données sans qu'ils aient besoin d'utiliser de nombreux outils.

La directive `ServerTokens` doit être définie sur `Prod`. Par exemple, `ServerTokens Prod`. Cette directive détermine si le champ d'en-tête de réponse du serveur qui est renvoyé aux clients inclut une description du système d'exploitation et des informations sur les modules compilés.

### Procédure

1. Pour vérifier les jetons de serveur, exécutez la commande `cat /etc/apache2/sysconfig.d/global.conf | grep ServerTokens`.
2. Pour modifier `ServerTokens OS` par `ServerTokens Prod`, exécutez la commande `sed -i 's/\(ServerTokens\s\+\)OS/\1Prod/g' /etc/apache2/sysconfig.d/global.conf`.

### Désactiver la méthode de suivi pour le serveur Apache2

Dans les opérations de production standard, l'utilisation de diagnostics peut révéler des vulnérabilités inconnues entraînant la corruption des données. Pour empêcher l'utilisation incorrecte des données, désactivez la méthode HTTP `Trace`.

#### Procédure

1 Pour vérifier la méthode `Trace` pour le serveur Apache2, exécutez la commande suivante `grep TraceEnable /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf`.

2 Pour désactiver la méthode `Trace` pour le serveur Apache2, exécutez la commande suivante `sed -i "/^[^#]*TraceEnable/ c\TraceEnable off" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf`.

## Désactiver les modes de configuration

Lorsque vous installez, configurez ou gérez vRealize Operations Manager, la meilleure pratique consiste à modifier la configuration ou les paramètres pour activer le dépannage et le débogage de votre installation.

Listez et vérifiez chacune des modifications effectuées pour vous assurer qu'elles sont correctement sécurisées. N'intégrez pas les modifications à la production si vous n'êtes pas sûr qu'elles soient correctement sécurisées.

## Gestion des composants logiciels non essentiels

Pour minimiser les risques de sécurité, supprimez ou configurez les logiciels non essentiels de vos machines hôtes vRealize Operations Manager.

Configurez tous les logiciels que vous ne supprimez pas conformément aux recommandations du fabricant et aux meilleures pratiques de sécurité afin de minimiser le risque qu'ils entraînent des failles de sécurité.

### Sécuriser le gestionnaire de stockage de masse USB

Sécuriser le gestionnaire de stockage de masse USB pour l'empêcher de se charger par défaut sur les appliances vRealize et pour empêcher son utilisation comme gestionnaire de périphériques USB avec les appliances vRealize. Les pirates potentiels peuvent exploiter ce gestionnaire pour installer des logiciels malveillants.

#### 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 vos appliances vRealize pour empêcher les pirates potentiels de l'exploiter.

Le fait de lier le protocole Bluetooth à la pile réseau est inutile et augmente la surface d'attaque de l'hôte. Empêcher le gestionnaire de protocole Bluetooth module de chargement par défaut sur les appareils vRealize.

#### Procédure

1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.

2 Assurez-vous que la ligne `install bluetooth /bin/true` apparaît dans ce fichier.

3 Enregistrez le fichier et fermez-le.

## Sécuriser le Stream Control Transmission Protocol

Empêchez le module Stream Control Transmission Protocol (SCTP) de se charger par défaut sur les appliances vRealize. Les pirates potentiels pourraient exploiter ce protocole pour compromettre la sécurité de votre système.

Configurez votre système pour empêcher le chargement du module SCTP à moins que cela ne soit absolument nécessaire. SCTP est un protocole de couche de transport normalisé par l'IETF inutilisé. Le fait de lier ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux non privilégiés peuvent pousser le noyau à charger un gestionnaire des protocoles de manière dynamique en utilisant le protocole afin d'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 sctp /bin/true
```

3 Enregistrez le fichier et fermez-le.

## Sécuriser le Datagram Congestion Control Protocol

Dans le cadre de vos activités de sécurisation renforcée, empêchez le module Datagram Congestion Control Protocol (DCCP) de se charger par défaut sur les appliances vRealize. Les pirates potentiels pourraient exploiter ce protocole pour compromettre la sécurité de votre système.

Évitez de charger le module DCCP à moins que cela ne soit absolument nécessaire. DCCP est un protocole de couche de transport proposé, qui n'est pas utilisé. Le fait de lier ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux non privilégiés peuvent pousser le noyau à charger un gestionnaire des protocoles de manière dynamique en utilisant le protocole afin d'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 protocole Reliable Datagram Sockets

Dans le cadre de vos activités de sécurisation renforcée, empêchez le protocole Reliable Datagram Sockets (RDS) de se charger par défaut sur vos appliances vRealize. Les pirates potentiels pourraient exploiter ce protocole pour compromettre la sécurité de votre système.

Le fait de lier le protocole RDS à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux non privilégiés peuvent pousser le noyau à charger un gestionnaire des protocoles de manière dynamique en utilisant le protocole afin d'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 Transparent Inter-Process Communication Protocol

Dans le cadre de vos activités de sécurisation renforcée, empêchez le module Transparent Inter-Process Communication protocol (TIPC) de se charger par défaut sur les machines hôtes de vos appliances virtuelles. Les pirates potentiels pourraient exploiter ce protocole pour compromettre la sécurité de votre système.

Le fait de lier le protocole TIPC à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux non privilégiés peuvent pousser le noyau à charger un gestionnaire des protocoles de manière dynamique en utilisant le protocole afin d'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 Internet Packet Exchange

Empêchez le protocole Internet Packet Exchange (IPX) de se charger par défaut sur les appliances vRealize. Les pirates potentiels pourraient exploiter ce protocole pour compromettre la sécurité de votre système.

Évitez de charger le module du protocole IPX à moins que cela ne soit absolument nécessaire. Le protocole IPX est un protocole de couche réseau obsolète. Le fait de lier ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux non privilégiés peuvent pousser le système à charger un gestionnaire des protocoles de manière dynamique en utilisant le protocole afin d'ouvrir un socket.

### Procédure

1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.

2 Assurez-vous que la ligne `install ipx /bin/true` apparaît dans ce fichier.

3 Enregistrez le fichier et fermez-le.

## Protocole Appletalk sécurisé

Empêchez le protocole Appletalk de se charger par défaut sur les appliances vRealize. Les pirates potentiels pourraient exploiter ce protocole pour compromettre la sécurité de votre système.

Évitez de charger le module du protocole Appletalk à moins que cela ne soit absolument nécessaire. Le fait de lier ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux non privilégiés peuvent pousser le système à charger un gestionnaire des protocoles de manière dynamique en utilisant le protocole afin d'ouvrir un socket.

### Procédure

1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.

2 Assurez-vous que la ligne `install appletalk /bin/true` apparaît dans ce fichier.

3 Enregistrez le fichier et fermez-le.

## Protocole DECnet sécurisé

Empêchez le protocole DECnet de se charger par défaut sur votre système. Les pirates potentiels pourraient exploiter ce protocole pour compromettre la sécurité de votre système.

Évitez de charger le module du protocole DECnet à moins que cela ne soit absolument nécessaire. Le fait de lier ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux non privilégiés peuvent pousser le système à charger un gestionnaire des protocoles de manière dynamique en utilisant le protocole afin d'ouvrir un socket.

### Procédure

1 Ouvrez le fichier `/etc/modprobe.conf.local` du protocole DECnet dans un éditeur de texte.

2 Assurez-vous que la ligne `install decnet /bin/true` apparaît dans ce fichier.

3 Enregistrez le fichier et fermez-le.

## Module Firewire sécurisé

Empêchez le module Firewire de se charger par défaut sur les appliances vRealize. Les pirates potentiels pourraient exploiter ce protocole pour compromettre la sécurité de votre système.

Évitez de charger le module Firewire à moins que cela ne soit absolument nécessaire.

### Procédure

1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.

2 Assurez-vous que la ligne `install ieee1394 /bin/true` apparaît dans ce fichier.

3 Enregistrez le fichier et fermez-le.

## Consignation des messages du noyau

`kernel.printk` dans le fichier `/etc/sysctl.conf` indique les spécifications de consignation d'impression du noyau.

Il y a 4 valeurs spécifiées :

- `console loglevel`. La plus basse priorité de messages imprimés sur la console.
- `default loglevel`. Le niveau le plus bas pour les messages sans niveau de journal spécifique.
- Le niveau le plus bas possible pour le niveau de journal de la console.
- La valeur par défaut pour le niveau de journal de la console.

Il y a huit entrées possibles pour chaque valeur.

- `define KERN_EMERG "<0>" /* system is unusable */`
- `define KERN_ALERT "<1>" /* action must be taken immediately */`
- `define KERN_CRIT "<2>" /* critical conditions */`
- `define KERN_ERR "<3>" /* error conditions */`
- `define KERN_WARNING "<4>" /* warning conditions */`
- `define KERN_NOTICE "<5>" /* normal but significant condition */`
- `define KERN_INFO "<6>" /* informational */`
- `define KERN_DEBUG "<7>" /* debug-level messages */`

Définissez les valeurs `kernel.printk` sur **`3 4 1 7`** et assurez-vous que la ligne `kernel.printk=3 4 1 7` est présente dans le fichier `/etc/sysctl.conf`.

# Déploiement installé sur Windows

## Utilisation du service de temps Windows

Si la source horaire est capitale, vous devez désactiver la synchronisation temporelle de l'hôte et utiliser des serveurs temporels autorisés.

Vous pouvez utiliser des serveurs temporels autorisés dans un environnement de production comme moyen d'effectuer le suivi précis des actions des utilisateurs et de détecter de potentielles attaques et intrusions malveillantes via un audit et une journalisation détaillés.

## TLS pour les données en transit

En matière de sécurité, la meilleure pratique consiste à s'assurer que le système est déployé avec des canaux de transmission sécurisés.

### Configurer vRealize Operations Manager pour l'utilisation de chiffrements forts

La force du chiffrement utilisé dans une session TLS est déterminée par le chiffrement négocié entre le serveur et le navigateur. Pour que seuls des chiffrements forts soient sélectionnés, vous devez modifier le serveur afin de désactiver l'utilisation des chiffrements faibles. De plus, vous devez configurer les chiffrements dans l'ordre approprié. Configurez le serveur pour qu'il prenne en charge uniquement les chiffrements forts et pour qu'il utilise des clés suffisamment grandes.

### Configurer des protocoles fiables pour vRealize Operations Manager

Les protocoles tels que SSLv2 et SSLv3 ne sont plus considérés comme sûrs. En matière de protection de la couche de transport, la meilleure pratique consiste à prendre en charge uniquement les protocoles TLS.

Avant la production, vous devez vérifier que SSLv2 et SSLv3 sont désactivés.

### Désactiver les chiffrements faibles

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, NULL ou eNULL. L'absence d'authentification les expose à des attaques de type « intercepteur ».

Vous devez également désactiver l'échange de clés anonyme Diffie-Hellman (ADH, Anonymous Diffie-Hellman), les chiffrements d'exportation (EXP, chiffrements comportant DES), les clés de taille inférieure à 128 bits pour crypter le trafic de charge utile, l'utilisation de l'algorithme Message Digest 5 (MD5) en tant que mécanisme de hachage pour le trafic de charge utile, ainsi que les suites de chiffrement International Data Encryption Algorithm (IDEA) et Rivest Cipher 4 (RC4) car elles sont vulnérables aux attaques.

#### Désactiver les chiffrements faibles dans le gestionnaire Apache HTTPD

Désactivez les chiffrements faibles et activez les chiffrements forts utilisés dans le gestionnaire Apache HTTPD.

#### Prérequis

Pour une sécurité maximale, comparez les chiffrements du gestionnaire Apache HTTPD sur vRealize Operations Manager à ceux de la liste des chiffrements acceptables et désactivez tous les chiffrements considérés comme faibles. Cela vous aidera à éviter des attaques de type « intercepteur ».

#### Procédure

1 Ouvrez le fichier `C:\vmware\vrealize-operations\vmware-vcopssuite\utilities\conf` dans un éditeur de texte.

2 Vérifiez que le fichier contient la ligne `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH`.

3 Enregistrez les modifications et fermez le fichier.

#### Activer l'échange de clés Diffie-Hellman

L'échange de clés Diffie-Hellman comporte des failles. Désactivez toutes les suites de chiffrement contenant DH, DHE et EDH.

Ces suites de chiffrement sont désormais désactivées par défaut. Vous pouvez les activer si vous devez les utiliser.

#### Procédure

1 Ouvrez le fichier `C:\vmware\vrealize-operations\vmware-vcopssuite\utilities\conf`.

2 Trouvez la ligne `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH`.

3 Supprimez `!DH:` pour que la ligne se présente comme suit : `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:@STRENGTH`.

4 Enregistrez et fermez le fichier.

## Désactiver les modes de configuration

Lorsque vous installez, configurez ou gérez vRealize Operations Manager, la meilleure pratique consiste à modifier la configuration ou les paramètres pour activer le dépannage et le débogage de votre installation.

Listez et vérifiez chacune des modifications effectuées pour vous assurer qu'elles sont correctement sécurisées. N'intégrez pas les modifications à la production si vous n'êtes pas sûr qu'elles soient correctement sécurisées.

## Vérification de la ligne de base sécurisée du serveur hôte

Vous pouvez utiliser l'outil Microsoft Baseline Security Analyzer (MBSA) pour vérifier si votre serveur dispose des mises à jour ou des correctifs à chaud les plus récents. Vous pouvez utiliser MBSA pour installer tous les correctifs de sécurité manquants de Microsoft afin de maintenir votre serveur à jour vis-à-vis des recommandations de sécurité de Microsoft. Vous pouvez télécharger cet outil à partir du site de Microsoft.

Vous trouverez le dernier outil disponible au moment de la publication du présent document ici :http://www.microsoft.com/fr-fr/download/details.aspx?id=7558.

**Remarque** Contactez votre fournisseur Microsoft pour obtenir des conseils sur le meilleur moyen d'utiliser cet outil.

## Vérifier que le serveur hôte est configuré de manière sécurisée

Vous pouvez utiliser l'Assistant Configuration de la sécurité de Windows (SCW, Security Configuration Wizard) et le Gestionnaire de conformité de sécurité Microsoft pour vérifier que le serveur hôte est configuré de manière sécurisée.

1 Démarrez l'Assistant Configuration de la sécurité à partir des outils administratifs 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.

2 Comparez le rapport avec les derniers conseils en matière de sécurisation renforcée du Gestionnaire de conformité de sécurité Microsoft approprié pour votre serveur Windows.

3 En fonction des résultats, vous pouvez configurer les paramètres de sécurité pour chaque fonctionnalité, comme les services de 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, rendez-vous sur http://technet.microsoft.com/fr-fr/library/cc754997.aspx.

**Remarque** Contactez votre fournisseur Microsoft pour obtenir des conseils sur le meilleur moyen d'utiliser ces outils.

# Déploiement installé sur Linux

## Activation de service NTP

Si la source horaire est capitale, vous pouvez désactiver la synchronisation temporelle de l'hôte et utiliser le protocole NTP (Network Time Protocol). L'utilisation de NTP dans un environnement de production permet d'effectuer le suivi précis des actions des utilisateurs et de détecter de potentielles attaques et intrusions malveillantes via un audit et une journalisation détaillés.

Le démon ntp est inclus sur l'appliance et est utilisé pour fournir des services de temps synchronisés. Vous trouverez le fichier de configuration de NTP dans `/etc/ntp.conf`.

## TLS pour les données en transit

En matière de sécurité, la meilleure pratique consiste à s'assurer que le système est déployé avec des canaux de transmission sécurisés.

### Configurer des protocoles fiables pour vRealize Operations Manager

Les protocoles tels que SSLv2 et SSLv3 ne sont plus considérés comme sûrs. En matière de protection de la couche de transport, la meilleure pratique consiste à prendre en charge uniquement les protocoles TLS.

Avant la production, vous devez vérifier que SSLv2 et SSLv3 sont désactivés.

### Configurer vRealize Operations Manager pour l'utilisation de chiffrements forts

La force du chiffrement utilisé dans une session TLS est déterminée par le chiffrement négocié entre le serveur et le navigateur. Pour que seuls des chiffrements forts soient sélectionnés, vous devez modifier le serveur afin de désactiver l'utilisation des chiffrements faibles. De plus, vous devez configurer les chiffrements dans l'ordre approprié. Configurez le serveur pour qu'il prenne en charge uniquement les chiffrements forts et pour qu'il utilise des clés suffisamment grandes.

### Désactiver les chiffrements faibles

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, NULL ou eNULL. L'absence d'authentification les expose à des attaques de type « intercepteur ».

Vous devez également désactiver l'échange de clés anonyme Diffie-Hellman (ADH, Anonymous Diffie-Hellman), les chiffrements d'exportation (EXP, chiffrements comportant DES), les clés de taille inférieure à 128 bits pour crypter le trafic de charge utile, l'utilisation de l'algorithme Message Digest 5 (MD5) en tant que mécanisme de hachage pour le trafic de charge utile, ainsi que les suites de chiffrement International Data Encryption Algorithm (IDEA) et Rivest Cipher 4 (RC4) car elles sont vulnérables aux attaques.

#### Désactiver les chiffrements faibles dans le gestionnaire Apache HTTPD

Désactivez les chiffrements faibles et activez les chiffrements forts utilisés dans le gestionnaire Apache HTTPD. Pour éviter les attaques de type « intercepteur », comparez les chiffrements du serveur Apache HTTPD sur vRealize Operations Manager à ceux de la liste des chiffrements acceptables et désactivez tous les chiffrements considérés comme faibles.

#### Procédure

1 Ouvrez le fichier `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` dans un éditeur de texte.

2 Vérifiez que le fichier contient la ligne `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH`.

3 Enregistrez et fermez le fichier.

#### Activer l'échange de clés Diffie-Hellman

L'échange de clés Diffie-Hellman comporte des failles. Vous devez désactiver toutes les suites de chiffrement contenant DH, DHE et EDH. Ces suites de chiffrement sont désactivées par défaut. Vous pouvez les activer si vous devez les utiliser.

#### Procédure

1 Ouvrez le fichier `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf`.

2 Trouvez la ligne `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH`.

3 Supprimez `!DH:` pour que la ligne se présente comme suit : `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:@STRENGTH`.

4 Enregistrez et fermez le fichier.

### Désactiver les modes de configuration

Lorsque vous installez, configurez ou gérez vRealize Operations Manager, la meilleure pratique consiste à modifier la configuration ou les paramètres pour activer le dépannage et le débogage de votre installation.

Listez et vérifiez chacune des modifications effectuées pour vous assurer qu'elles sont correctement sécurisées. N'intégrez pas les modifications à la production si vous n'êtes pas sûr qu'elles soient correctement sécurisées.

### Vérification de la configuration sécurisée du serveur hôte

Pour assurer le fonctionnement sécurisé de vRealize Operations Manager, vous devez sécuriser et vérifier les activités de sécurisation renforcée.

Pour plus d'informations, consultez les conseils relatifs à la sécurisation renforcée de Red Hat Enterprise Linux 6 conformément aux stratégies de sécurité de votre entreprise.

## Agent Endpoint Operations Management

L'agent Endpoint Operations Management ajoute une détection basée sur des agents et des capacités de suivi à vRealize Operations Manager.

L'agent Endpoint Operations Management est installé directement sur les hôtes et peut avoir ou non le même niveau de confiance que le serveur Endpoint Operations Management. Vous devez donc vérifier que les agents sont installés de manière sécurisée.

## Meilleures pratiques de sécurité pour l'exécution d'agents Endpoint Operations Management

Vous devez suivre certaines meilleures pratiques de sécurité lors de l'utilisation de comptes d'utilisateur.

- Pour une installation en mode silencieux, retirez l'ensemble des informations d'identification et des empreintes du certificat du serveur stockées dans le fichier `AGENT_HOME/conf/agent.properties`.
- Utilisez un compte d'utilisateur vRealize Operations Manager réservé spécifiquement à l'enregistrement d''agents Endpoint Operations Management. Pour plus d'informations, consultez la section « Rôles et Privilèges » dans vRealize Operations Manager, dans l'aide de vRealize Operations Manager.
- Une fois l'installation terminée, désactivez le compte d'utilisateur vRealize Operations Manager que vous utilisez pour l'enregistrement d'agents. Vous devez activer l'accès utilisateur pour les activités d'administration d'agents. Pour plus d'informations, consultez la section Configuration des utilisateurs et des groupes dans vRealize Operations Manager dans l'aide de vRealize Operations Manager.
- Si un système qui exécute un agent est compromis, vous pouvez révoquer le certificat d'agent à l'aide de l'interface utilisateur de vRealize Operations Manager en supprimant la ressource d'agent. Pour plus d'informations, reportez-vous à la section Révocation d'un agent.

## Autorisations minimales requises pour la fonctionnalité d'agent

Vous avez besoin d'autorisations pour installer et modifier un service. Si vous souhaitez découvrir un processus en cours d'exécution, le compte d'utilisateur que vous utilisez pour exécuter l'agent doit également posséder les privilèges d'accès aux processus et aux programmes. Pour les installations sur le système d'exploitation Windows, vous avez besoin d'autorisations pour installer et modifier un service. Pour les installations Linux, vous avez besoin d'une autorisation pour installer l'agent en tant que service si vous installez l'agent à l'aide d'un programme d'installation RPM.

Les informations d'identification minimales requises pour que l'agent s'enregistre sur le serveur vRealize Operations Manager sont celles d'un utilisateur bénéficiant du rôle d'agent de gestion, sans aucune attribution à des objets au sein du système.

### Fichiers et autorisations de plate-forme basée sur Linux

Une fois que vous avez installé l'agent Endpoint Operations Management, le propriétaire est l'utilisateur qui installe l'agent.

Le répertoire d'installation et les autorisations de fichier, telles que 600 et 700, sont attribués au propriétaire lorsque l'utilisateur qui installe l'agent Endpoint Operations Management décompresse le fichier TAR ou installe le RPM.

**Remarque** Lorsque vous décompressez le fichier ZIP, il est possible que les autorisations ne soient pas appliquées correctement. Assurez-vous que les autorisations sont correctes.

Tous les fichiers qui sont créés et écrits par l'agent reçoivent des autorisations 700 avec comme propriétaire l'utilisateur qui exécute l'agent.

**Tableau 3-1.** Fichiers et autorisations Linux

| Répertoire ou fichier | Autorisations | Groupes d'utilisateurs | Lecture | Écrire | Exécuter |
|---|---|---|---|---|---|
| *agent directory*/bin | 700 | Propriétaire | Oui | Oui | Oui |
| | | Groupe | Non | Non | Non |
| | | Tout | Non | Non | Non |
| *agent directory*/conf | 700 | Propriétaire | Oui | Oui | Oui |

**Tableau 3-1.** Fichiers et autorisations Linux (suite)

| Répertoire ou fichier | Autorisations | Groupes d'utilisateurs | Lecture | Écrire | Exécuter |
|---|---|---|---|---|---|
| | | Groupe | Non | Non | Non |
| | | Tout | Non | Non | Non |
| *agent directory*/log | 700 | Propriétaire | Oui | Oui | Non |
| | | Groupe | Non | Non | Non |
| | | Tout | Non | Non | Non |
| *agent directory*/data | 700 | Propriétaire | Oui | Oui | Oui |
| | | Groupe | Non | Non | Non |
| | | Tout | Non | Non | Non |
| *agent directory*/bin/ep-agent.bat | 600 | Propriétaire | Oui | Oui | Non |
| | | Groupe | Non | Non | Non |
| | | Tout | Non | Non | Non |
| *agent directory*/bin/ep-agent.sh | 700 | Propriétaire | Oui | Oui | Oui |
| | | Groupe | Non | Non | Non |
| | | Tout | Non | Non | Non |
| *agent directory*/conf/* (tous les fichiers du répertoire `conf`) | 600 | Propriétaire | Oui | Oui | Oui |
| | | Groupe | Non | Non | Non |
| | | Tout | Non | Non | Non |
| *agent directory*/log/* (tous les fichiers du répertoire `log`) | 600 | Propriétaire | Oui | Oui | Non |
| | | Groupe | Non | Non | Non |
| | | Tout | Non | Non | Non |
| *agent directory*/data/* (tous les fichiers du répertoire `data`) | 600 | Propriétaire | Oui | Oui | Non |
| | | Groupe | Non | Non | Non |
| | | Tout | Non | Non | Non |

## Fichiers et autorisations de plate-forme basée sur Windows

Pour une installation basée sur Windows de l'agent Endpoint Operations Management, l'utilisateur qui installe l'agent doit disposer des autorisations nécessaires pour installer et modifier le service.

Une fois que vous avez installé l'agent Endpoint Operations Management, le dossier d'installation et tous ses sous-répertoires et fichiers devraient être uniquement accessibles au SYSTÈME, au groupe d'administrateurs et à l'utilisateur de l'installation. Lorsque vous installez l'agent Endpoint Operations Management à l'aide du fichier `ep-agent.bat`, assurez-vous que le processus de sécurisation renforcée a bien fonctionné. Il est conseillé à l'utilisateur installant l'agent de prendre note de tous les messages d'erreur éventuels. Si le processus de sécurisation renforcée échoue, l'utilisateur peut appliquer ces autorisations manuellement.

**Tableau 3-2.** Fichiers et autorisations Windows

| Répertoire ou fichier | Groupes d'utilisateurs | Contrôle total | Modifier | Lecture et exécution | Lecture | Écrire |
|---|---|---|---|---|---|---|
| <agent directory>/bin | SYSTÈME | Oui | - | - | - | - |
| | l'administrateur | Oui | - | - | - | - |

**Tableau 3-2.** Fichiers et autorisations Windows (suite)

| Répertoire ou fichier | Groupes d'utilisateurs | Contrôle total | Modifier | Lecture et exécution | Lecture | Écrire |
|---|---|---|---|---|---|---|
| | Utilisateur de l'installation | Oui | - | - | - | - |
| | Utilisateurs | | - | - | - | - |
| <agent directory>/conf | SYSTÈME | Oui | - | - | - | - |
| | l'administrateur | Oui | - | - | - | - |
| | Utilisateur de l'installation | Oui | - | - | - | - |
| | Utilisateurs | | - | - | - | - |
| <agent directory>/log | SYSTÈME | Oui | - | - | - | - |
| | l'administrateur | Oui | - | - | - | - |
| | Utilisateur de l'installation | Oui | - | - | - | - |
| | Utilisateurs | | - | - | - | - |
| <agent directory>/data | SYSTÈME | Oui | - | - | - | - |
| | l'administrateur | Oui | - | - | - | - |
| | Utilisateur de l'installation | Oui | - | - | - | - |
| | Utilisateurs | | - | - | - | - |
| <agent directory>/bin/hq-agent.bat | SYSTÈME | Oui | - | - | - | - |
| | l'administrateur | Oui | - | - | - | - |
| | Utilisateur de l'installation | Oui | - | - | - | - |
| | Utilisateurs | | - | - | - | - |
| <agent directory>/bin/hq-agent.sh | SYSTÈME | Oui | - | - | - | - |
| | l'administrateur | Oui | - | - | - | - |
| | Utilisateur de l'installation | Oui | - | - | - | - |
| | Utilisateurs | | - | - | - | - |
| <agent directory>/conf/* (tous les fichiers du répertoire `conf`) | SYSTÈME | Oui | - | - | - | - |
| | l'administrateur | Oui | - | - | - | - |
| | Utilisateur de l'installation | Oui | - | - | - | - |
| | Utilisateurs | | - | - | - | - |
| <agent directory>/log/* (tous les fichiers du répertoire `log`) | SYSTÈME | Oui | - | - | - | - |
| | l'administrateur | Oui | - | - | - | - |

**Tableau 3-2.** Fichiers et autorisations Windows (suite)

| Répertoire ou fichier | Groupes d'utilisateurs | Contrôle total | Modifier | Lecture et exécution | Lecture | Écrire |
|---|---|---|---|---|---|---|
| | Utilisateur de l'installation | Oui | - | - | - | - |
| | Utilisateurs | | - | - | - | - |
| <agent directory>/data/* (tous les fichiers du répertoire `data`) | SYSTÈME | Oui | - | - | - | - |
| | l'administrateur | Oui | - | - | - | - |
| | Utilisateur de l'installation | Oui | - | - | - | - |
| | Utilisateurs | | - | - | - | - |

## Ports ouverts sur un hôte d'agent

Le processus d'agent écoute les commandes sur deux ports, 127.0.0.1:2144 et 127.0.0.1:32000, qui sont configurables. Ces ports peuvent être attribués de façon arbitraire. C'est pourquoi le numéro de port exact peut varier. L'agent n'ouvre pas de ports sur les interfaces externes.

**Tableau 3-3.** Minimum de ports requis

| Port | Protocole | Direction | Commentaires |
|---|---|---|---|
| 443 | TCP | Sortant | Utilisé par l'agent pour les connexions sortantes sur HTTP, TCP ou ICMP. |
| 2144 | TCP | Écoute | Interne uniquement. Configurable. Utilisé pour la communication inter-processus entre l'agent et la ligne de commande qui le charge et le configure. Le processus d'agent écoute sur ce port.<br>**Remarque** Le numéro de port est attribué de façon arbitraire et peut varier. |
| 32000 | TCP | Écoute | Interne uniquement. Configurable. Utilisé pour la communication inter-processus entre l'agent et la ligne de commande qui le charge et le configure. Le processus d'agent écoute sur ce port.<br>**Remarque** Le numéro de port est attribué de façon arbitraire et peut varier. |

## Révocation d'un agent

Si, pour une raison quelconque, vous devez révoquer un agent (par exemple lorsqu'un système avec un agent en cours d'exécution est compromis) vous pouvez supprimer la ressource d'agent à partir du système. Toute requête ultérieure échouera à la vérification.

Utilisez l'interface utilisateur vRealize Operations Manager pour révoquer le certificat d'agent en retirant la ressource d'agent. Pour plus d'informations, consultez « Suppression de la ressource d'agent », page 41.

Une fois que le système est à nouveau sécurisé, vous pouvez rétablir l'agent. Pour plus d'informations, consultez « Rétablir une ressource d'agent », page 42.

### Suppression de la ressource d'agent

Vous pouvez utiliser le vRealize Operations Manager pour révoquer le certificat d'agent en retirant la ressource d'agent.

#### Prérequis

Pour préserver la continuité de la ressource avec les données de mesure enregistrées précédemment, créez un enregistrement du jeton d'agent Endpoint Operations Management qui s'affiche dans les détails de la ressource.

### Procédure

1 Naviguez jusqu'à l'Explorateur d'inventaire dans l'interface utilisateur vRealize Operations Manager.

2 Ouvrez l'arborescence Types d'adaptateurs.

3 Ouvrez la liste des adaptateurs EP Ops.

4 Sélectionnez **Agent EP Ops - *NOM_HÔTE_DNS_***.

5 Cliquez sur **Modifier l'objet**.

6 Enregistrez l'ID d'agent, qui correspond à la chaîne de jeton de l'agent.

7 Fermez la boîte de dialogue Modifier l'objet.

8 Sélectionnez **Agent EP Ops - *NOM_HÔTE_DNS_*** et cliquez sur **Supprimer l'objet**.

## Rétablir une ressource d'agent

Lorsque l'état sécurisé d'un système est récupéré, vous pouvez rétablir un agent révoqué. De cette manière, l'agent peut continuer à générer des rapports sur les mêmes ressources sans perdre de données historiques. Pour ce faire, vous devez créer un nouveau fichier de jeton Endpoint Operations Management en utilisant le même jeton enregistré avant la suppression de la ressource d'agent. Reportez-vous à la section Suppression de la ressource d'agent.

### Prérequis

- Assurez-vous que vous avez la chaîne de jeton Endpoint Operations Management enregistré.
- Utilisez le jeton de ressource enregistré avant la suppression de la ressource d'agent à partir du serveur vRealize Operations Manager.
- Assurez-vous que vous disposez du privilège Gérer un agent.

### Procédure

1 Créez le fichier de jeton d'agent avec l'utilisateur qui exécute l'agent.

Par exemple, exécutez la commande suivante pour créer un fichier de jeton contenant le jeton 123-456-789.

- Sur Linux :

```
echo 123-456-789 > /etc/epops/epops-token
```

- Sur Windows :

```
echo 123-456-789 > %PROGRAMDATA%\VMware\Ep Ops Agent\epops-token
```

Dans cet exemple, le fichier de jeton est enregistré à l'emplacement réservé aux jetons par défaut pour cette plate-forme.

2 Installez un nouvel agent et enregistrez-le auprès du serveur vRealize Operations Manager. Assurez-vous que l'agent charge le jeton que vous avez inséré dans le fichier de jeton.

Vous devez disposer du privilège Gérer un agent pour effectuer cette action.

### Révocation de certificat d'agent et mise à jour des certificats

Le processus de redélivrance est lancé à partir de l'agent à l'aide de l'argument de ligne de commande `setup`. Lorsqu'un agent qui est déjà inscrit utilise l'argument de ligne de commande `setup` `ep-agent.sh setup` et indique les informations d'identification requise, une nouvelle commande `registerAgent` est envoyée au serveur.

Le serveur détecte que l'agent est déjà inscrit et lui envoie un nouveau certificat client sans créer de nouvelle ressource d'agent. Du côté de l'agent, le nouveau certificat client remplace l'ancien. Si le certificat du serveur est modifié et que vous exécutez la commande `ep-agent.sh setup`, vous verrez un message qui vous demande de faire confiance au nouveau certificat. Vous avez également la possibilité d'indiquer le nouveau certificat de serveur dans le fichier `agent.properties` avant d'exécuter la commande `ep-agent.sh setup`, afin de rendre le processus silencieux.

#### Prérequis

Gérez les privilèges des agents pour révoquer et mettre à jour les certificats.

#### Procédure

- Sur les systèmes d'exploitation basés sur Linux, exécutez la commande `ep-agent.sh setup` sur l'hôte de l'agent. Sur les systèmes d'exploitation basés sur Windows, exécutez la commande `ep-agent.bat setup`.

  Si l'agent détecte que le certificat du serveur a été modifié, un message s'affiche. Acceptez le nouveau certificat si vous lui faites confiance et qu'il est valide.

### Exécution du correctif et mise à jour de l'agent Endpoint Operations Management

Si besoin, de nouveaux bundles d'agent Endpoint Operations Management sont disponibles indépendamment des versions de vRealize Operations Manager.

Les correctifs ou les mises à jour ne sont pas fournis pour l'agent Endpoint Operations Management. Vous devez installer la dernière version disponible de l'agent comprenant les derniers correctifs de sécurité. Les correctifs de sécurité critiques seront communiqués conformément aux instructions de sécurité VMware. Consultez la section relative aux consignes de sécurité.

## Activités de configuration sécurisée supplémentaire

### Vérifier les paramètres de compte d'utilisateur du serveur

Il est recommandé de vérifier qu'aucun compte d'utilisateur inutile n'existe pour les comptes d'utilisateur et les paramètres locaux et de domaine.

Restreignez tout compte d'utilisateur non lié au fonctionnement de l'application aux comptes requis pour l'administration, la maintenance et le dépannage. Restreignez l'accès distant à partir de comptes d'utilisateur de domaine au minimum requis pour assurer la maintenance du serveur. Contrôlez et vérifiez strictement ces comptes.

### Supprimer et désactiver les applications inutiles

Supprimez les applications inutiles des serveurs hôtes. Chaque application supplémentaire et inutile augmente le risque d'exposition en raison de ses vulnérabilités inconnues ou non corrigées.

## Désactiver les ports et services inutiles

Vérifiez le pare-feu du serveur de l'hôte pour obtenir la liste des ports ouverts permettant le trafic.

Bloquez tous les ports qui ne sont pas répertoriés comme indispensables pour vRealize Operations Manager dans la section « Configuration des ports et des protocoles », page 54 de ce document, ou qui ne sont pas requis. Vérifiez également les services exécutés sur votre serveur hôte et désactivez ceux qui ne sont pas requis.

# Sécurité du réseau et communications sécurisées 4

En matière de sécurité, la meilleure pratique consiste à passer en revue et modifier les paramètres de communication réseau de vos appliances virtuelles VMware et des machines hôtes. Vous devez également configurer les ports entrants et sortants minimum pour vRealize Operations Manager.

Ce chapitre aborde les rubriques suivantes :


- « Configuration des paramètres réseau pour l'installation de l'application virtuelle », page 45
- « Configuration des ports et des protocoles », page 54


## Configuration des paramètres réseau pour l'installation de l'application virtuelle

Pour garantir que votre dispositif virtuel VMware et vos machines hôtes autorisent uniquement les communications sécurisées et essentielles, vérifiez et modifiez leurs paramètres de communication réseau.

### Empêcher les utilisateurs de contrôler les interfaces réseau

En matière de sécurité, la meilleure pratique consiste à limiter la capacité de modifier le réglage des interfaces réseau aux utilisateurs privilégiés. Si des utilisateurs manipulent les interfaces réseau, cela risquerait d'entraîner le contournement des mécanismes de sécurité du réseau ou un déni de service. Assurez-vous que les interfaces réseau ne sont pas configurées pour le contrôle par les utilisateurs.

#### Procédure

1 Pour vérifier les paramètres de contrôle des utilisateurs, exécutez la commande `#grep –i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*`.

2 Assurez-vous que chaque interface est définie sur `NON`.

### Définir la taille de la file d'attente pour le backlog TCP

En matière de sécurité, la meilleure pratique consiste à configurer une taille de file d'attente par défaut pour le backlog TCP sur les machines hôtes des appliances VMware. Pour limiter le risque d'attaques par déni de service TCP, sélectionnez une taille de file d'attente par défaut adaptée pour le backlog TCP. Le paramètre par défaut recommandé est 1280.

#### Procédure

1 Exécutez la commande `# cat /proc/sys/net/ipv4/tcp_max_syn_backlog` sur chaque machine hôte des appliances VMware.

2 Définissez la taille de la file d'attente pour le backlog TCP.

   a Ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.

   b Définissez la taille par défaut de la file d'attente pour le backlog TCP en ajoutant l'entrée suivante au fichier.

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

   c Enregistrez les modifications et fermez le fichier.

## Refuser une requête par écho ICMPv4 vers une adresse de diffusion

Les réponses aux requêtes par écho ICMP (Internet Control Message Protocol) fournissent un vecteur aux attaques par amplification et peuvent permettre à des agents malveillants de cartographier le réseau plus facilement. Configurer votre système pour ignorer les requêtes par écho ICMPv4 offre une protection contre de telles attaques.

### Procédure

1 Exécutez la commande `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` pour vérifier que le système n'envoie pas de réponses aux requêtes par écho ICMP vers les adresses de diffusion.

2 Configurez les systèmes hôtes pour refuser les requêtes par écho ICMPv4 vers les adresses de diffusion.

   a Ouvrez le fichier `/etc/sysctl.conf` sur une machine hôte Windows dans un éditeur de texte.

   b Si la valeur de cette entrée n'est pas définie sur `1`, ajoutez l'entrée `net.ipv4.icmp_echo_ignore_broadcasts=1`.

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour désactiver le proxy ARP IPv4

Le proxy ARP IPv4 permet à un système d'envoyer des réponses aux demandes ARP sur une interface au nom des hôtes connectés à une autre interface. Vous devez désactiver le proxy ARP IPv4 pour éviter tout partage d'informations non autorisé. Désactivez le paramètre afin d'éviter la fuite d'informations d'adressage entre les segments réseau reliés.

### Procédure

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp|egrep "default|all"` pour vérifier si le proxy ARP est désactivé.

2 Configurez le système hôte pour désactiver le proxy ARP IPv4.

   a Ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.

   b Si les valeurs ne sont pas définies sur `0`, ajoutez les entrées ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `0`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour ignorer les messages de redirection ICMP IPv4

En matière de sécurité, la meilleure pratique consiste à vérifier que le système hôte ignore les messages de redirection ICMP (Internet Control Message Protocol) IPv4. Un message de redirection ICMP malveillant peut provoquer une attaque de type « intercepteur ». Les routeurs utilisent des messages de redirection ICMP pour informer les hôtes qu'un itinéraire plus direct existe pour une destination. Ces messages modifient le tableau de routage de l'hôte et ne sont pas authentifiés.

### Procédure

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep "default|all"` sur le système hôte pour vérifier que le système hôte ignore les messages de redirection IPv4.

2 Configurez le système hôte pour ignorer les messages de redirection ICMP IPv4.

   a Ouvrez le fichier `/etc/sysctl.conf`.

   b Si les valeurs ne sont pas définies sur `0`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `0`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour ignorer les messages de redirection ICMP IPv6

En matière de sécurité, la meilleure pratique consiste à vérifier que le système hôte ignore les messages de redirection ICMP (Internet Control Message Protocol) IPv6. Un message de redirection ICMP malveillant peut provoquer une attaque de type « intercepteur ». Les routeurs utilisent des messages de redirection ICMP pour informer les hôtes qu'un itinéraire plus direct existe pour une destination. Ces messages modifient le tableau de routage de l'hôte et ne sont pas authentifiés.

### Procédure

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects|egrep "default|all"` sur le système hôte et vérifiez si ce dernier ignore les messages de redirection IPv6.

2 Configurez le système hôte pour ignorer les messages de redirection ICMP IPv6.

   a Ouvrez le fichier `/etc/sysctl.conf` pour configurer le système hôte de manière à ignorer les messages de redirection IPv6.

   b Si les valeurs ne sont pas définies sur `0`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `0`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour refuser les redirections ICMP IPv4

En matière de sécurité, la meilleure pratique consiste à vérifier que le système hôte refuse les redirections ICMP (Internet Control Message Protocol) IPv4. Les routeurs utilisent des messages de redirection ICMP pour informer les serveurs qu'un itinéraire direct existe pour une destination donnée. Ces messages contiennent des informations issues du tableau de routage du système pouvant révéler des parties de la topologie du réseau.

### Procédure

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/send_redirects|egrep "default|all"` sur le système hôte pour vérifier qu'il refuse les redirections ICMP IPv4.

2 Configurez le système hôte pour refuser les redirections ICMP IPv4.

   a Ouvrez le fichier `/etc/sysctl.conf` pour configurer le système hôte.

   b Si les valeurs ne sont pas définies sur `0`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `0`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour consigner les paquets martiens IPv4

En matière de sécurité, la meilleure pratique consiste à vérifier que le système hôte consigne les paquets martiens IPv4. Les paquets martiens contiennent des adresses que le système reconnaît comme non valides. Configurez le système hôte afin qu'il consigne les messages de manière à pouvoir 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"` pour vérifier que l'hôte consigne les paquets martiens IPv4.

2 Configurez le système hôte pour consigner les paquets martiens IPv4.

   a Ouvrez le fichier `/etc/sysctl.conf` pour configurer le système hôte.

   b Si les valeurs ne sont pas définies sur `1`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `1`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour utiliser le filtrage du chemin inverse IPv4

En matière de sécurité, la meilleure pratique consiste à configurer vos machines hôtes pour l'utilisation du filtrage du chemin inverse IPv4. Le filtrage du chemin inverse protège contre les adresses source falsifiées en amenant le système à ignorer les paquets ayant des adresses source sans itinéraire ou dont l'itinéraire ne désigne pas l'interface d'origine.

Configurez votre système de manière à utiliser le filtrage du chemin inverse, si possible Selon le rôle du système, le filtrage du chemin inverse peut amener le système à ignorer un trafic légitime. Dans ce cas, vous devrez peut-être utiliser un mode moins sécurisé ou bien désactiver complètement le filtrage du chemin inverse.

**Procédure**

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"` sur le système hôte afin de vérifier si ce dernier utilise le filtrage du chemin inverse IPv4.

2 Configurez le système hôte de manière à utiliser le filtrage du chemin inverse d'IPv4.

   a Ouvrez le fichier `/etc/sysctl.conf` pour configurer le système hôte.

   b Si les valeurs ne sont pas définies sur `1`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `1`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour refuser les transferts IPv4

En matière de sécurité, la meilleure pratique consiste à vérifier que le système hôte refuse les transferts IPv4. Si le système est configuré pour les transferts IP et qu'il n'est pas désigné comme routeur, il peut être utilisé pour contourner la sécurité du réseau en fournissant une voie de communication non filtrée par les périphériques réseau.

**Procédure**

1 Exécutez la commande `# cat /proc/sys/net/ipv4/ip_forward` pour vérifier si l'hôte refuse les transferts IPv4.

2 Configurez le système hôte pour refuser les transferts IPv4.

   a Ouvrez le fichier `/etc/sysctl.conf` pour configurer le système hôte.

   b Si la valeur n'est pas définie sur `0`, ajoutez l'entrée suivante au fichier ou mettez à jour l'entrée existante en conséquence. Définissez la valeur sur `0`.

   ```
   net.ipv4.ip_forward=0
   ```

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour refuser le transfert des paquets IPv4 routés par la source

Les paquets routés par la source permettent à la source du paquet de suggérer que les routeurs transfèrent le paquet via un chemin différent de celui configuré sur le routeur. Celui-ci peut être utilisé pour contourner les mesures de sécurité du réseau.

Cette disposition ne s'applique qu'au transfert de trafic routé par la source, comme lorsque le transfert IPv4 est activé et que le système fonctionne comme un routeur.

**Procédure**

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/accept_source_route|egrep "default|all"` pour vérifier que le système n'utilise pas de paquets IPv4 routés par la source

2 Configurez le système hôte pour refuser le transfert des paquets IPv4 routés par la source.

   a Ouvrez le fichier `/etc/sysctl.conf` avec un éditeur de texte.

   b Si les valeurs ne sont pas définies sur `0`, assurez-vous que `net.ipv4.conf.all.accept_source_route=0` et `et.ipv4.conf.default.accept_source_route=0` sont définis sur `0`.

   c Enregistrez et fermez le fichier.

## Configurer le système hôte pour refuser les transferts IPv6

En matière de sécurité, la meilleure pratique consiste à vérifier que le système hôte refuse les transferts IPv6. Si le système est configuré pour les transferts IP et qu'il n'est pas désigné comme routeur, il peut être utilisé pour contourner la sécurité du réseau en fournissant une voie de communication non filtrée par les périphériques réseau.

### Procédure

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding|egrep "default|all"` pour vérifier que l'hôte refuse les transferts IPv6.

2 Configurez le système hôte pour refuser les transferts IPv6.

   a Ouvrez le fichier `/etc/sysctl.conf` pour configurer le système hôte.

   b Si les valeurs ne sont pas définies sur `0`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `0`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour utiliser des Syncookies TCP IPv4

En matière de sécurité, la meilleure pratique consiste à vérifier que le système hôte utilise des Syncookies TCP (Transmission Control Protocol) IPv4. Une attaque SYN flood TCP peut provoquer un déni de service en remplissant le tableau des connexions TCP d'un système avec des connexions à l'état SYN_RCVD. Les Syncookies sont utilisés de manière à ne pas rechercher de connexion jusqu'à la réception d'un ACK, de manière à vérifier que l'initiateur tente d'établir une connexion valide et n'est pas une source d'attaque flood.

Cette technique ne fonctionne pas d'une manière totalement conforme aux normes, mais est uniquement activée lorsqu'une condition de flood est détectée et permet de défendre le système tout en continuant à prendre en charge les requêtes valides.

### Procédure

1 Exécutez la commande `# cat /proc/sys/net/ipv4/tcp_syncookies` pour vérifier que le système hôte utilise des Syncookies TCP IPv4.

2 Configurez le système hôte pour utiliser des Syncookies TCP IPv4.

   a Ouvrez le fichier `/etc/sysctl.conf` pour configurer le système hôte.

   b Si la valeur n'est pas définie sur `1`, ajoutez l'entrée suivante au fichier ou mettez à jour l'entrée existante en conséquence. Définissez la valeur sur `1`.

   ```
   net.ipv4.tcp_syncookies=1
   ```

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour refuser les annonces du routeur IPv6

En matière de sécurité, la meilleure pratique consiste à vérifier que le système hôte refuse l'acceptation des annonces de routeur ainsi que les redirections ICMP (Internet Control Message Protocol), à moins que cela ne soit nécessaire. Avec IPv6, les systèmes peuvent configurer les périphériques réseau en utilisant automatiquement les informations du réseau. Du point de vue de la sécurité, il est préférable de configurer les informations importantes manuellement plutôt que d'accepter celles provenant du réseau de manière non authentifiée.

### Procédure

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra|egrep "default|all"` sur le système hôte afin de vérifier si le système refuse l'acceptation des annonces de routeur et les redirections ICMP, à moins que cela ne soit nécessaire.

2 Configurez le système hôte pour refuser les annonces du routeur IPv6.

   a Ouvrez le fichier `/etc/sysctl.conf`.

   b Si les valeurs ne sont pas définies sur `0`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `0`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour refuser les sollicitations du routeur IPv6

En matière de sécurité, la meilleure pratique consiste à vérifier que le système hôte refuse les sollicitations du routeur IPv6, à moins que cela ne soit nécessaire. 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 statiquement, il est inutile d'envoyer une sollicitation.

### Procédure

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations|egrep "default|all"` pour vérifier que le système hôte refuse les sollicitations du routeur IPv6, à moins que cela ne soit nécessaire.

2 Configurez le système hôte pour refuser les sollicitations du routeur IPv6.

   a Ouvrez le fichier `/etc/sysctl.conf`.

   b Si les valeurs ne sont pas définies sur `0`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `0`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour refuser la préférence du routeur IPv6 dans les sollicitations de routeur

En matière de sécurité, la meilleure pratique consiste à vérifier que votre système hôte refuse les sollicitations du routeur IPv6, à moins que cela ne soit nécessaire. La préférence de routeur dans le paramètre de sollicitations détermine les préférences de routeur. Si les adresses sont attribuées statiquement, il est inutile de recevoir une 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 le système hôte pour vérifier si le système hôte refuse les sollicitations du routeur IPv6.

2 Configurez le système hôte pour refuser la préférence du routeur IPv6 dans les sollicitations de routeur.

   a Ouvrez le fichier `/etc/sysctl.conf`.

   b Si les valeurs ne sont pas définies sur `0`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `0`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour refuser le préfixe du routeur IPv6

En matière de sécurité, la meilleure pratique consiste à vérifier que le système hôte refuse les informations de préfixe du routeur IPv6, à moins que cela ne soit nécessaire. Le paramètre `accept ra pinfo` contrôle si le système accepte les informations de préfixe issues du routeur. Si les adresses sont attribuées statiquement, le système ne reçoit aucune information de préfixe de routeur.

### Procédure

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo|egrep "default|all"` pour vérifier que le système refuse les informations de préfixe de routeur.

2 Configurez le système hôte pour refuser le préfixe du routeur IPv6.

   a Ouvrez le fichier `/etc/sysctl.conf`.

   b Si les valeurs ne sont pas définies sur `0`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `0`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour refuser les paramètres de limite de sauts d'annonce du routeur IPv6

En matière de sécurité, la meilleure pratique consiste à vérifier que le système refuse les paramètres de limite de sauts d'annonce du routeur IPv6 provenant d'une annonce du routeur, à moins que cela ne soit nécessaire. Le paramètre `accept_ra_defrtr` permet de contrôler si le système accepte les paramètres de limite de sauts provenant d'une annonce de routeur. Définissez-le sur `0` pour empêcher qu'un routeur ne modifie votre 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"` pour vérifier que le système hôte refuse les paramètres de limite de sauts d'annonce du routeur IPv6.

2 Si les valeurs ne sont pas définies sur `0`, configurez le système hôte pour refuser les paramètres de limite de sauts d'annonce du routeur IPv6.

   a Ouvrez le fichier `/etc/sysctl.conf`.

   b Si les valeurs ne sont pas définies sur `0`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `0`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour refuser les paramètres autoconf d'annonce du routeur IPv6

En matière de sécurité, la meilleure pratique consiste à vérifier que le système hôte refuse les paramètres `autoconf` d'annonce du routeur IPv6. Le paramètre `autoconf` détermine si les annonces de routeur sont susceptibles d'amener le système à attribuer une adresse de monodiffusion globale à une interface.

### Procédure

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf|egrep "default|all"` pour vérifier si le système hôte refuse les paramètres `autoconf` d'annonce du routeur IPv6.

2 Si les valeurs ne sont pas définies sur `0`, configurez le système hôte pour refuser les paramètres autoconf d'annonce du routeur IPv6.

   a Ouvrez le fichier `/etc/sysctl.conf`.

   b Si les valeurs ne sont pas définies sur `0`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `0`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour refuser les sollicitations de voisin IPv6

En matière de sécurité, la meilleure pratique consiste à vérifier que le système hôte refuse les sollicitations de voisin IPv6, à moins que cela ne soit nécessaire. Le paramètre `dad_transmits` détermine le nombre de sollicitations de voisin qui doivent être envoyées par adresse, y compris les adresses lien-local et globales, lorsque vous mettez en place une interface pour vous assurer que l'adresse voulue est unique sur le réseau.

**Procédure**

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits|egrep "default|all"` pour vérifier que le système hôte refuse les sollicitations de voisin IPv6.

2 Si les valeurs ne sont pas définies sur `0`, configurez le système hôte pour refuser les sollicitations de voisin IPv6.

   a Ouvrez le fichier `/etc/sysctl.conf`.

   b Si les valeurs ne sont pas définies sur `0`, ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `0`.

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

   c Enregistrez les modifications et fermez le fichier.

## Configurer le système hôte pour limiter le nombre maximum d'adresses IPv6

En matière de sécurité, la meilleure pratique consiste à vérifier que l'hôte limite le nombre maximum d'adresses IPv6 qui peuvent être attribuées. Le paramètre relatif au nombre maximum d'adresses détermine combien d'adresses IPv6 de monodiffusion globale peuvent être attribuées à chaque interface. La valeur par défaut est 16, mais vous devez définir ce paramètre sur le nombre d'adresses globales configurées de façon statique requises.

**Procédure**

1 Exécutez la commande `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses|egrep "default|all"` pour vérifier si le système hôte limite le nombre maximum d'adresses IPv6 qui peuvent être attribuées.

2 Si les valeurs ne sont pas définies sur `1`, configurez le système hôte de manière à limiter le nombre maximum d'adresses IPv6 qui peuvent être attribuées.

   a Ouvrez le fichier `/etc/sysctl.conf`.

   b Ajoutez les entrées suivantes au fichier ou mettez à jour les entrées existantes en conséquence. Définissez la valeur sur `1`.

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

   c Enregistrez les modifications et fermez le fichier.

# Configuration des ports et des protocoles

En matière de sécurité, la meilleure pratique consiste à désactiver tous les ports et les protocoles qui ne sont pas essentiels.

Configurez le nombre minimal de ports entrants et sortants pour les composants de vRealize Operations Manager, de sorte que les composants importants du système fonctionnent en production.

## Minimum de ports entrants par défaut

En matière de sécurité, la meilleure pratique consiste à configurer les ports entrants requis pour que vRealize Operations Manager fonctionne en production.

**Tableau 4-1.** Minimum de ports entrants requis

| Port | Protocole | Commentaires |
|---|---|---|
| 443 | TCP | Utilisé pour accéder à l'interface utilisateur de vRealize Operations Manager et à l'interface administrateur de vRealize Operations Manager. |
| 123 | UDP | Utilisé par vRealize Operations Manager pour la synchronisation NTP (Network Time Protocol) sur le nœud maître. |
| 5433 | TCP | Utilisé par les nœuds maîtres et de réplica pour répliquer la base de données globale (vPostgreSQL) lorsque la haute disponibilité est activée. |
| 7001 | TCP | Utilisé par Cassandra pour sécuriser la communication de cluster inter-nœuds.<br>N'exposez pas ce port à Internet. Ajoutez-le à un pare-feu. |
| 9042 | TCP | Utilisé par Cassandra pour sécuriser la communication liée au client entre les nœuds.<br>N'exposez pas ce port à Internet. Ajoutez-le à un pare-feu. |
| 6061 | TCP | Utilisé par les clients pour se connecter à GemFire Locator pour obtenir les informations de connexion aux serveurs dans le système distribué. Surveille également la charge de serveur pour diriger les clients vers les serveurs les moins chargés. |
| 10000-10010 | TCP et UDP | Plage de ports éphémère pour le serveur GemFire utilisée pour la messagerie UDP en monodiffusion et pour la détection de pannes TCP dans un système distribué pair à pair. |
| 20000-20010 | TCP et UDP | Plage de ports éphémère pour le localisateur GemFire utilisée pour la messagerie UDP en monodiffusion et pour la détection de pannes TCP dans un système distribué pair à pair. |

**Tableau 4-2.** Ports entrants facultatifs

| Port | Protocole | Commentaires |
|---|---|---|
| 22 | TCP | Facultatif. Secure Shell (SSH). Le service SSH écoutant sur le port 22 ou tout autre port doit être désactivé dans un environnement de production, et le port 22 doit être fermé. |
| 80 | TCP | Facultatif. Redirection vers 443. |
| 3091-3101 | TCP | Lorsque Horizon View est installé, utilisé pour accéder aux données pour vRealize Operations Manager à partir de Horizon View. |

# Audit et journalisation de votre système vRealize Operations Manager 5

En matière de sécurité, la meilleure pratique consiste à configurer l'audit et la journalisation de votre système vRealize Operations Manager.

L'implémentation détaillée de l'audit et de la journalisation ne constitue pas l'objet de ce document.

La journalisation sur un hôte distant permet de centraliser les journaux et de les stocker en toute sécurité. En collectant les fichiers journaux sur un hôte central, vous pouvez surveiller facilement votre environnement à l'aide d'un outil unique. Vous pouvez également effectuer une analyse cumulée et rechercher les attaques coordonnées réalisées sur plusieurs entités de votre infrastructure. La journalisation sur un serveur dédié centralisé et sécurisé peut contribuer à éviter la falsification des journaux. Elle fournit également des enregistrements d'audit à long terme.

Ce chapitre aborde les rubriques suivantes :


- « Sécurisation du serveur de journalisation distant », page 57
- « Utiliser un serveur NTP autorisé », page 57
- « Considérations relatives au navigateur client », page 58


## Sécurisation du serveur de journalisation distant

En matière de sécurité, la meilleure pratique consiste à vérifier que le serveur de journalisation distant ne peut être configuré que par un utilisateur autorisé et qu'il est sécurisé.

Les pirates ayant violé la sécurité de votre machine hôte peuvent chercher à falsifier les fichiers journaux pour couvrir leurs traces et garder le contrôle sans être découverts.

## Utiliser un serveur NTP autorisé

Assurez-vous que tous les systèmes hôtes utilisent la même source de temps relative, y compris le décalage de localisation pertinente. Vous pouvez mettre en corrélation la source de temps relative avec une norme de temps telle que le temps universel coordonné (UTC).

Vous pouvez aisément suivre et corréler les actions d'un intrus lorsque vous passez en revue les fichiers journaux pertinents. Des paramètres d'heure incorrects peuvent compliquer la tâche consistant à inspecter et mettre en corrélation les fichiers journaux afin de détecter les attaques, et peuvent entraîner des inexactitudes dans les audits. Vous pouvez utiliser au moins trois serveurs NTP à partir de sources de temps externes ou configurer quelques serveurs NTP locaux sur un réseau de confiance obtenant leur temps à partir d'au moins trois sources externes.

# Considérations relatives au navigateur client

En matière de sécurité, la meilleure pratique consiste à ne pas utiliser vRealize Operations Manager à partir de clients non approuvés ou non corrigés, ou à partir de clients utilisant des extensions de navigateur.

# Index


## A

accès à la console **15**
activer le mode FIPS 140-2 **23**
Agent de gestion des opérations de point de terminaison **37**
Apache httpd **24**
applications inutiles, supprimer **43**
audit **57**
authentification du chargeur d'amorçage **20**
authentification en mode de maintenance **20**
authentification en mode utilisateur unique **20**
autorisations de fichier, Secure Shell **17**
autorisations de fichier secure shell **17**
autorisations minimales, fonctionnalité d'agent **38**
avis de sécurité, correctifs **11**

## B

boîtiers virtuels
- activer ou désactiver Secure Shell **16**
- authentification du chargeur d'amorçage **20**
- configurer NTP **22**
- gestionnaire de protocole Bluetooth **30**
- gestionnaire de stockage de masse USB **30**

## C

chiffrements faibles, configurer **34, 36**
chiffrements forts **34, 36**
chiffrements forts, configurer **25**
compte administratif local, création **16**
comptes administratifs **15**
configuration, authentification client PostgreSQL **28**
configuration client, Secure Shell **19**
configuration d'Apache **29**
configuration du client Secure Shell **19**
configuration du serveur, Secure Shell **18**
configuration du serveur Secure Shell **18**
configuration sécurisée **13**
configuration sécurisée du serveur hôte **37**
configurer **31**
configurer des protocoles fiables **34, 36**
configurer les paramètres réseau pour OVF **45**
configurer NTP **22**
considérations relatives au navigateur **58**
consignation des messages du noyau **33**

## D

Datagram Congestion Control Protocol **31**
déploiement sécurisé de vRealize Operations Manager **9**
désactivation, applications inutiles **43**
désactiver l'accès SSH pour le compte d'utilisateur Admin **20**
désactiver la méthode de suivi :serveur Apache2 **30**
désactiver la navigation **29**
désactiver la navigation dans les répertoires **29**
désactiver la réponse d'horodatage TCP **23**
désactiver les chiffrements faibles **34, 37**
désactiver les connexions directes **19**
désactiver les ports inutiles **44**
désactiver les services inutiles **44**
Diffie-Hellman **37**
données en transit **24, 34, 36**

## E

empêcher le contrôle par les utilisateurs **45**
exécution du correctif **43**
expiration des mots de passe **15**

## F

fichiers et autorisation de plate-forme, Linux **38**
fichiers et autorisation de plate-forme, Windows **39**

## G

gestion des logiciels non essentiels **30**
gestionnaire de protocole Bluetooth **30**
gestionnaire de stockage de masse USB **30**
glossaire **5**

## I

infrastructure, sécurisation renforcée **9**
inventaire des logiciels non pris en charge **10**
IPv4, consignation des paquets martiens IPv4 **48**
IPV4, désactiver le proxy ARP **46**
IPv4, ignorer le filtrage du chemin inverse IPv4 **48**

IPv4, ignorer les messages de redirection ICMP **47**
IPv4, refuser les redirections ICMP IPv4 **48**
IPv4, refuser les transferts IPv4 **49**
IPv4, utiliser des syncookies TCP IPv4 **50**
IPv6, ignorer les messages de redirection ICMP **47**
IPv6, limiter le nombre maximum d'adresses IPv6 **54**
IPv6, refuser la préférence dans les sollicitations de routeur **52**
IPv6, refuser le préfixe du routeur ICMP IPv6 **52**
IPv6, refuser les annonces du routeur IPv6 **51**
IPv6, refuser les sollicitations de voisin IPv6 **54**
IPv6, refuser les sollicitations du routeur IPv6 **51**
IPv6, refuser les transferts IPv6 **50**

## J

journalisation **57**

## L

ligne de base sécurisée du serveur hôte **35**
logiciel tiers **11**

## M

machines virtuelles, désactiver le proxy ARP IPv4 **46**
machines virtuelles, refuser une requête par écho ICMPv4 vers une adresse de diffusion **46**
meilleures pratiques, agents de gestion des opérations du point de terminaison **38**
minimum de comptes d'utilisateur **21**
minimum de groupes nécessaires **21**
minimum de ports entrants **55**
mise à jour des certificats **43**
mises à jour **43**
modes de configuration, désactiver **30, 35, 37**
mot de passe d'administrateur vRealize Operations Manager **22**
mot de passe racine, modifier **14**

## N

network time protocol **36**

## O

OVF, paramètres réseau **45**

## P

paquets IPv4 routés par la source **49**
paramètres autoconf IPv6 **53**
paramètres réseau **45**
passer en revue les logiciels installés **10**
ports
  entrant **45**
  sortant **45**
ports et protocoles, configuration **54**
ports ouverts sur un hôte d'agent **41**
position en matière de sécurité **7**
protocole DECnet, sécurisé **33**
protocoles du gestionnaire GemFire TLS **24**
protocoles fiables **34, 36**
protocoles fiables, configurer **24**
Public ciblé **5**

## R

refuser le transfert **49**
refuser les paramètres autoconf du routeur IPv6 **53**
refuser les paramètres de limite de sauts d'annonce du routeur IPv6 **53**
refuser une requête par écho ICMPv4 vers une adresse de diffusion **46**
réinitialisation du mot de passe sur les clusters Linux **22**
ressources d'application, protéger **27**
rétablir une ressource d'agent **42**
révocation d'un agent **41**
révocation de certificat d'agent **43**

## S

Secure Shell, restriction d'accès **17**
Secure Shell, gestion **15**
sécurisation renforcée de l'environnement vSphere **10**
sécurisation renforcée de l'infrastructure **9**
sécurisation renforcée pour l'installation de Linux **10**
sécurisation renforcée pour l'installation de Windows **10**
sécurisé
  module Firewire **33**
  protocole Appletalk **32**
  protocole Internet Packet Exchange **32**
  protocole Reliable Datagram Sockets **31**
  Transparent Inter-Process Communication Protocol **32**
sécuriser la console **14**
sécuriser le serveur de journalisation distant **57**
serveur de journalisation distant > sécurisation **57**
serveur hôte configuré de manière sécurisée **35**
serveur NTP autorisé **57**
service de temps Windows **34**
Stream Control Transmission Protocol **31**
suites de chiffrement dans Apache httpd **26**

suites de chiffrement dans GemFire **26**
suppression de l'exemple de code :serveur Apache2 **29**
supprimer la ressource d'agent **41**
surveiller le minimum de comptes d'utilisateur nécessaires **21**
surveiller le minimum de groupes nécessaires **21**

## T

taille de la file d'attente pour le backlog TCP **45**
TLS pour les données en transit **24, 34, 36**

## U

utilisateur racine, Secure Shell **15**

## V

Vérification du support d'installation **9**
vérifier, paramètres de compte d'utilisateur du serveur **43**
vérifier la ligne de base sécurisée **35**
vérifier les jetons de serveur :serveur Apache2 **29**