Sécurité de Site Recovery Manager

Site Recovery Manager 8.1

vmware®

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

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

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

docfeedback@vmware.com

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

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

Table des matières

À propos de la sécurité de VMware Site Recovery Manager

Sécurité de Site Recovery Manager fournit une référence concise sur les fonctions de sécurité de Site Recovery Manager

Pour vous permettre de protéger votre installation de Site Recovery Manager, cette documentation décrit les fonctions de sécurité intégrées à Site Recovery Manageret les mesures que vous pouvez prendre pour la protéger contre les attaques.

- Interfaces externes, ports et services nécessaires au bon fonctionnement de Site Recovery Manager
- Options de configuration et paramètres ayant des implications en matière de sécurité
- Emplacement des fichiers journaux et leur utilité
- Comptes système requis
- Informations sur l'obtention de correctifs de sécurité

Public cible

Ces informations sont destinées aux décideurs, architectes et administrateurs des services informatiques, ainsi qu'à tous ceux qui doivent se familiariser avec les composants de sécurité de Site Recovery Manager.

Référence de sécurité de Site Recovery Manager

1

Utilisez la Référence de sécurité pour découvrir les fonctions de sécurité de votre installation de Site Recovery Manager, ainsi que les mesures que vous pouvez prendre pour protéger votre environnement contre les attaques.

- Services Site Recovery Manager

  L'opération de Site Recovery Manager dépend de différents services qui s'exécutent sur la machine hôte de Site Recovery Manager Server.

- Ports réseau de Site Recovery Manager

  Site Recovery Manager utilise des ports réseau (que vous pouvez configurer) pour communiquer avec des clients et d'autres serveurs. Vous devez vous assurer que les pare-feu ne bloquent pas les utilisés par Site Recovery Manager.

- Fichiers de configuration Site Recovery Manager

  Certains fichiers de configuration Site Recovery Manager de contiennent des paramètres susceptibles d'affecter la sécurité de votre environnement. Les paramètres inappropriés peuvent également avec des répercussions sur le bon fonctionnement de votre environnement Site Recovery Manager.

- Certificats et clés de Site Recovery Manager

  Site Recovery Manager utilise des certificats TLS et des clés privées pour protéger la communication réseau et établir une authentification sécurisée avec d'autres serveurs.

- Informations d'identification stockées par Site Recovery Manager

  Site Recovery Manager stocke les informations d'identification de l'adaptateur de réplication de stockage (SRA) et de la base de données dans un format chiffré dans le Registre Windows.

- Fichiers de licence et de CLUF de Site Recovery Manager

  Les fichiers de licence et de CLUF de Site Recovery Manager sont situés sur la machine hôte de Site Recovery Manager Server.

- Fichiers journaux de Site Recovery Manager

  Site Recovery Manager enregistre les informations sur les opérations dans les fichiers journaux. Ceux-ci ne contiennent aucune information confidentielle, comme les clés privées et les mots de passe.

- Comptes Site Recovery Manager

  Site Recovery Manager utilise Single Sign-On (SSO) pour accéder à vCenter Server et à Platform Services Controller.

- Correctifs et mises à jour de sécurité de Site Recovery Manager

  Vous pouvez appliquer des mises à jour et des correctifs de sécurité Site Recovery Manager au fur et à mesure qu'ils sont fournis par VMware. Vous pouvez appliquer des mises à jour et des correctifs de sécurité du système d'exploitation invité au fur et à mesure qu'ils sont fournis par les fournisseurs du système d'exploitation invité.

- Recommandations pour la sécurisation de Site Recovery Manager Server

  Les recommandations pour la sécurisation de Site Recovery Manager Server peuvent vous permettre de protéger votre environnement d'éventuels problèmes de sécurité.

Services Site Recovery Manager

L'opération de Site Recovery Manager dépend de différents services qui s'exécutent sur la machine hôte de Site Recovery Manager Server.

Tableau 1-1. Services requis par Site Recovery Manager

Nom du service	Temps de démarrage	Description
VMware vCenter Site Recovery Manager Server	Automatique	Fournit les fonctions principales de Site Recovery Manager.
Base de données intégrée de VMware vCenter Site Recovery Manager	Automatique, si vous utilisez la base de données intégrée.	Le serveur vPostgres pour la base de données intégrée de Site Recovery Manager.
Client de VMware vCenter Site Recovery Manager	Automatique	Fournit la fonctionnalité du client de VMware vCenter Site Recovery Manager (Tomcat, interface utilisateur HTML5).
Server	Automatique	Service de Windows prenant en charge le partage de fichiers sur le réseau.
Workstation	Automatique	Service de Windows créant et mettant à jour des connexions à des serveurs distants.
Stockage protégé	Automatique	Service de Windows stockant des données confidentielles.

Ports réseau de Site Recovery Manager

Site Recovery Manager utilise des ports réseau (que vous pouvez configurer) pour communiquer avec des clients et d'autres serveurs. Vous devez vous assurer que les pare-feu ne bloquent pas les utilisés par Site Recovery Manager.

Site Recovery Manager Server reçoit l'ensemble du trafic entrant sur le port réseau. Le port par défaut est 9086. Si vous configurez Site Recovery Manager pour utiliser une base de données intégrée, la base de données intégrée de Site Recovery Manager reçoit le trafic réseau de l'hôte local sur l'interface en boucle locale. Le port par défaut est 5678.

Vous pouvez sélectionner d'autres ports pour Site Recovery Manager et le trafic de la base de données intégrée pendant le processus d'installation si les ports par défaut sont bloqués ou si d'autres applications les utilisent. Vous devez configurer des stratégies réseau pour activer le trafic sur le port entrant. Pour plus d'informations sur les ports que vous pouvez modifier après l'installation, reportez-vous à la rubrique *Modifier une installation de Site Recovery Manager Server* de la documentation de *Installation et configuration de Site Recovery Manager*.

Site Recovery Manager Server communique avec des hôtes Platform Services Controller, vCenter Serveret ESXi et des baies sur le site local. Vous devez vérifier que les stratégies de pare-feu de réseau activent le trafic vers les ports réseau de tous les composants du site local. Pour obtenir une liste des ports par défaut utilisés par tous les produits VMware, reportez-vous à l'article de la base de connaissances http://kb.vmware.com/kb/1012382.

La connexion entre le site local et le site distant d'une paire d'instances de Site Recovery Manager doit être privée comme un VPN. L'instance locale de Site Recovery Manager Server communique avec Site Recovery Manager Server, Platform Services Controller et vCenter Server sur le site distant et votre fournisseur de réseau doit garantir les stratégies de réseau adéquates pour activer le trafic.

Pour obtenir une liste de tous les ports qui doivent être ouverts pour Site Recovery Manager, consultez la section Ports réseau pour Site Recovery Manager dans la documentation *Installation et configuration de Site Recovery Manager*.

Fichiers de configuration Site Recovery Manager

Certains fichiers de configuration Site Recovery Manager de contiennent des paramètres susceptibles d'affecter la sécurité de votre environnement. Les paramètres inappropriés peuvent également avec des répercussions sur le bon fonctionnement de votre environnement Site Recovery Manager.

Tableau 1-2. Fichiers de configuration Site Recovery Manager

Emplacement de fichier ou de répertoire	Description
installation_folder\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml	Définit la configuration système de Site Recovery Manager Server. **Remarque** Vous ne devez pas déplacer ni supprimer le fichier de configuration. Vous pouvez modifier en toute sécurité les paramètres système d'une instance de Site Recovery Manager en utilisant les **Paramètres avancés** sous l'onglet Paire de sites de l'interface utilisateur de Site Recovery Manager.
installation_folder\VMware\VMware vCenter Site Recovery Manager Embedded Database\bin\vmw_vpg_config\	Contient des fichiers de configuration de base de données intégrée. **Remarque** Vous ne devez pas modifier, déplacer ou supprimer le fichier de configuration.

Tableau 1-2. Fichiers de configuration Site Recovery Manager (suite)

Emplacement de fichier ou de répertoire	Description
installation_folder\VMware\VMware vCenter Site Recovery Manager\config\extension.xml	Définit la configuration de l'extension Site Recovery Manager Server. Le fichier extension.xml contient des définitions des rôles d'utilisateur par défaut et de leurs privilèges. **Remarque** Vous ne devez pas modifier, déplacer ou supprimer le fichier de configuration.
C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\lib\h5dr.properties	Définit la configuration de l'interface utilisateur HTML 5 de Site Recovery Manager. **Remarque** Vous ne devez pas déplacer ni supprimer le fichier de configuration. Vous pouvez modifier en toute sécurité les paramètres de télémétrie de l'interface utilisateur HTML 5 de Site Recovery Manager en modifiant la valeur de *phonehomeEnabled* de True à False et inversement.

Certificats et clés de Site Recovery Manager

Site Recovery Manager utilise des certificats TLS et des clés privées pour protéger la communication réseau et établir une authentification sécurisée avec d'autres serveurs.

Certificat d'autorité de certification ou clé privée ou les deux	Emplacement et description
Certificat TLS et clé pour le point de terminaison de Site Recovery Manager Server	Dans le dossier Certificates\vmware-dr\Personal\Certificates du magasin de certificats Windows. Site Recovery Manager génère le certificat si vous ne fournissez pas de certificat personnalisé au cours de l'installation.
Certificat TLS et clé pour l'utilisateur de la solution créé pendant l'installation de Site Recovery Manager	Dans le dossier Certificates\vmware-dr\su-*Site Recovery Manager UUID*\Certificates du magasin de certificats Windows.
Certificat TLS et clé pour l'utilisateur de solution sur le site distant	Dans le dossier Certificates\vmware-dr\remote-su-*Site Recovery Manager UUID*\Certificates du magasin de certificats Windows. Site Recovery Manager crée les fichiers pendant le processus de couplage.
Certificat TLS et clé pour l'utilisateur de solution de l'interface utilisateur HTML5 créés pendant l'installation de Site Recovery Manager	Dans le fichier C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\lib\h5dr.keystore.

Certificat d'autorité de certification ou clé privée ou les deux	Emplacement et description
Certificat TLS et clé pour le point de terminaison du serveur Tomcat	Dans le fichier `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\conf\h5dr-server.keystore`. Il s'agit du même certificat TLS et de la même clé que ceux du point de terminaison de Site Recovery Manager Server.
Certificat d'autorité de certification pour Site Recovery Manager Server et certificat TLS	Fichier *`installation_folder`*`\VMware\VMware vCenter Site Recovery Manager\bin\`*`SRM_Server_IP_addressca`*`.p7b`. Site Recovery Manager génère le certificat si vous ne fournissez pas de certificat personnalisé au cours de l'installation. Vous pouvez importer le certificat dans un keystore approuvé de client pour autoriser les utilisateurs à approuver implicitement le certificat Site Recovery Manager Server.

Remarque N'extrayez pas et ne partagez pas les informations relatives aux clés privées pour protéger votre instance de Site Recovery Manager.

Pour plus d'informations sur les mécanismes d'authentification de Site Recovery Manager, reportez-vous à la rubrique *Authentification de Site Recovery Manager* dans le *Guide d'installation et de configuration de Site Recovery Manager*.

Informations d'identification stockées par Site Recovery Manager

Site Recovery Manager stocke les informations d'identification de l'adaptateur de réplication de stockage (SRA) et de la base de données dans un format chiffré dans le Registre Windows.

Vous avez accès aux informations d'identification lorsque vous êtes membre du groupe Administrateurs.

Chemin d'accès au Registre	Description
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Vmware DR\Creds\db:`*`nom de la banque de données`*	Informations d'identification pour accéder à la base de données Site Recovery Manager à l'aide de la banque de données système *nom de la banque de données*.
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Vmware DR\Creds\storage-arraymanager `*`ID du gestionnaire`*`-nom d'utilisateur`	Nom d'utilisateur que le SRA doit utiliser lors de la connexion au gestionnaire de baies identifié par l'*ID du gestionnaire*.
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ Vmware DR\Creds\storage-arraymanager-`*`ID du gestionnaire`*`-mot de passe`	Mot de passe que le SRA doit utiliser lors de la connexion au gestionnaire de baies identifié par l'*ID du gestionnaire*.

Les informations d'identification pour le keystore Java `h5dr.keystore` sont stockées dans le fichier `h5dr.properties` situé dans le dossier `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\lib\`. Les informations d'identification pour le keystore Java `h5dr-server.keystore` sont stockées dans le fichier `server.xml` situé dans le dossier `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\conf\`.

Fichiers de licence et de CLUF de Site Recovery Manager

Les fichiers de licence et de CLUF de Site Recovery Manager sont situés sur la machine hôte de Site Recovery Manager Server.

Tableau 1-3. Fichiers de licence et de CLUF de Site Recovery Manager

Fichier ou répertoire	Description
installation_folder\VMware\VMware vCenter Site Recovery Manager\en\	Répertoire contenant les fichiers du contrat de licence utilisateur final Site Recovery Manager.
installation_folder\VMware\VMware vCenter Site Recovery Manager\en\open_source_license.txt	Fichier de licence Open Source Site Recovery Manager.
installation_folder\VMware\VMware vCenter Site Recovery Manager Embedded Database\share\EULA-en.rtf	Fichier du contrat de licence utilisateur final de la base de données intégrée Site Recovery Manager.
installation_folder\VMware\VMware vCenter Site Recovery Manager Embedded Database\share\open_source_license.txt	Fichier de licence Open Source de la base de données intégrée Site Recovery Manager.

Fichiers journaux de Site Recovery Manager

Site Recovery Manager enregistre les informations sur les opérations dans les fichiers journaux. Ceux-ci ne contiennent aucune information confidentielle, comme les clés privées et les mots de passe.

Journaux Site Recovery Manager Server

Site Recovery Manager stocke les fichiers journaux système dans le répertoire `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs`. Les messages les plus récents de Site Recovery Manager Server sont placés dans le fichier `vmware-dr-`*`number`*`.log`.

Si vous redémarrez Site Recovery Manager Server ou si le fichier actuel doit dépasser la limite de taille définie pour le fichier,Site Recovery Manager archive le fichier journal actuel et crée un nouveau fichier journal.

Pour modifier le répertoire du fichier journal, entrez un nom de répertoire personnalisé dans l'élément XML du répertoire dans le fichier de configuration *`installation_directory`*`\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml`. Vous pouvez également modifier le niveau de journal de chaque composant en mettant à jour l'élément XML logLevel dans le fichier `vmware-dr.xml`. Le niveau par défaut de tous les composants est détaillé.

Important Configurez des listes de contrôle d'accès pour restreindre l'accès aux fichiers journaux.

Tableau 1-4. Niveaux de journal

Niveau	Description
error	Affiche uniquement les erreurs enregistrées dans le journal.
info	Affiche les informations, erreurs et avertissements enregistrés dans le journal.
trivia	Affiche les informations, erreurs, avertissements, détails et trivia enregistrés dans le journal.
détaillé	Affiche les informations, erreurs, avertissements et détails enregistrés dans le journal.
avertissement	Affiche les erreurs et les avertissements enregistrés dans le journal.

Site Recovery Manager prend notamment en charge les composants suivants :

- Par défaut
- Réplication
- Récupération
- Stockage
- StorageProvider
- Vdb
- Persistance

Le fichier `vmware-dr-number.log` ne contient aucun message de sécurité concernant le processus d'authentification et les connexions avec le site distant.

Journaux de l'interface utilisateur de Site Recovery .

Site Recovery Manager stocke les fichiers journaux de l'interface utilisateur de Site Recovery dans le répertoire `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-clients\logs`. Les derniers messages sont placés dans le fichier `dr.log`.

Vous pouvez modifier le niveau de journalisation de chaque composant en mettant à jour l'élément de valeur du niveau dans le fichier `log4j.xml` dans le répertoire `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\webapps\dr\WEB-INF\classes`. Le niveau par défaut de tous les composants est info.

Tableau 1-5. Niveaux de journal

Niveau	Description
error	Affiche uniquement les erreurs enregistrées dans le journal.
warn	Affiche les erreurs et les avertissements enregistrés dans le journal.
info	Affiche les informations, erreurs et avertissements enregistrés dans le journal.

Tableau 1-5. Niveaux de journal (suite)

Niveau	Description
debug	Affiche les débogages, informations, erreurs et avertissements enregistrés dans le journal.
trace	Affiche les informations les plus détaillées.

Le serveur Tomcat utilisé par l'interface utilisateur de Site Recovery prend en charge des composants tels que :

- E/S HTTP asynchrones
- Par heure d'appel du gestionnaire
- Catalogues VC L10N
- SRM
- VR
- Commun

Comptes Site Recovery Manager

Site Recovery Manager utilise Single Sign-On (SSO) pour accéder à vCenter Server et à Platform Services Controller.

Comptes d'utilisateurs

Dans la configuration par défaut, les administrateurs vCenter Server disposent des droits d'accès d'administration à Site Recovery Manager. Vous devez utiliser les informations d'identification de l'administrateur lorsque vous essayez de vous connecter à Site Recovery Manager pour la première fois après l'installation.

Si vous disposez d'informations d'identification d'administrateur, vous pouvez accorder l'accès à Site Recovery Manager à d'autres utilisateurs à l'aide de vSphere Web Client.

Pour plus d'informations sur les rôles, les privilèges et les autorisations de Site Recovery Manager, reportez-vous à la section *Privilèges, rôles et autorisations de Site Recovery Manager* dans la documentation *Administration de Site Recovery Manager*.

Compte d'utilisateur de la `Solution`

Site Recovery Manager crée un utilisateur `solution` au cours de l'installation et l'utilise pendant l'authentification auprès de vCenter Server. L'utilisateur `solution` est unique pour chaque instance de Site Recovery Manager et est réservé à un usage interne par Site Recovery Manager, vCenter Server et Platform Services Controller.

Site Recovery Manager crée un utilisateur `solution` supplémentaire sur chaque site distant pendant le processus de couplage des sites qui n'utilisent pas le mode Enhanced Linked Mode.
Site Recovery Manager utilise l'utilisateur `solution` pour effectuer les opérations nécessaires sur le site distant.

Site Recovery Manager crée un utilisateur `solution` pour l'interface utilisateur HTML5 pendant l'installation et l'utilise dans l'interface utilisateur HTML5 pendant l'authentification avec vCenter Server. L'utilisateur de la solution est unique pour chaque instance de Site Recovery Manager et est réservé à un usage interne par le client de l'interface utilisateur HTML5 de Site Recovery Manager, vCenter Server et Platform Services Controller.

Remarque Vous ne devez pas supprimer ni modifier les rôles et les privilèges associés aux comptes d'utilisateurs `solution`.

Pour plus d'informations sur les utilisateurs et `solution` et l'authentification entre le site local et le site distant, reportez-vous à la rubrique *Authentification de Site Recovery Manager* dans la documentation *Installation et configuration de Site Recovery Manager*.

Correctifs et mises à jour de sécurité de Site Recovery Manager

Vous pouvez appliquer des mises à jour et des correctifs de sécurité Site Recovery Manager au fur et à mesure qu'ils sont fournis par VMware. Vous pouvez appliquer des mises à jour et des correctifs de sécurité du système d'exploitation invité au fur et à mesure qu'ils sont fournis par les fournisseurs du système d'exploitation invité.

Versions des systèmes d'exploitation hôte de Site Recovery Manager

Pour plus d'informations sur les systèmes d'exploitation hôte pris en charge pour Site Recovery Manager Server, consultez la section *Matrices de compatibilité de Site Recovery Manager 8.1* sur https://docs.vmware.com/fr/Site-Recovery-Manager/8.1/rn/srm-compat-matrix-8-1.html.

Application des correctifs et mises à jour de sécurité de Site Recovery Manager

Vous appliquez les correctifs et mises à jour de sécurité de Site Recovery Manager en effectuant une mise à niveau sur place de votre installation de Site Recovery Manager existante. Pour plus d'informations sur la mise à niveau de Site Recovery Manager, consultez la section *Mise à niveau sur place de Site Recovery Manager Server* dans *Installation et configuration de Site Recovery Manager*.

Recommandations pour la sécurisation de Site Recovery Manager Server

Les recommandations pour la sécurisation de Site Recovery Manager Server peuvent vous permettre de protéger votre environnement d'éventuels problèmes de sécurité.

L'opération sécurisée de Site Recovery Manager dépend de la configuration et de la maintenance adéquates du système d'exploitation de Site Recovery Manager Server.

- Exécutez Site Recovery Manager uniquement sur un système d'exploitation hôte, une base de données et du matériel pris en charge. Si Site Recovery Manager ne s'exécute pas sur un système d'exploitation hôte pris en charge, Site Recovery Manager peut ne pas fonctionner correctement.
- Appliquez les mises à jour du système d'exploitation les plus récentes pour protéger le système d'exploitation hôte des attaques malveillantes. Appliquez les mises à jour et les correctifs de Site Recovery Manager les plus récents pour traiter tous les problèmes connus rencontrés avec Site Recovery Manager.
- Vérifiez l'intégrité de votre déploiement de Site Recovery Manager lorsque vous exécutez Site Recovery Manager en tant que machine virtuelle. Reportez-vous à la rubrique *Recommandations en matière de sécurité des machines virtuelles* dans la documentation de *vSphere Security*.
- Limitez l'installation de logiciels et désactivez les services que Site Recovery Manager n'utilise pas pour libérer des ressources et limiter le risque d'attaques sur le serveur. Les logiciels et services inutiles consomment les ressources du CPU, du stockage, de la mémoire et de la bande passante et augmentent les risques d'attaques sur le serveur.
- Autorisez uniquement les administrateurs à accéder au serveur. Pour limiter le nombre de comptes qu'un pirate peut utiliser, limitez le nombre de comptes pouvant accéder au serveur.
- Vérifiez les ports réseau qu'utilise Site Recovery Manager et configurez un pare-feu pour protéger votre serveur.