Site Recovery Manager-Sicherheit

Site Recovery Manager 6.5

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-002309-00

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

http://www.vmware.com/de/support/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Infos über VMware Site Recovery Manager - Sicherheit

Site Recovery Manager-Sicherheit stellt eine umfassende Referenz für die Sicherheitsfunktionen von Site Recovery Manager bereit.

In diesem Handbuch werden die in Site Recovery Manager integrierten Sicherheitsfunktionen sowie die Maßnahmen, die Sie zum Schutz Ihrer Site Recovery Manager-Installation ergreifen können, beschrieben.

- Externe Schnittstellen, Ports und Dienste, die für einen ordnungsgemäßen Betrieb von Site Recovery Manager erforderlich sind
- Konfigurationsoptionen und -einstellungen, die Auswirkungen auf die Sicherheit haben.
- Speicherort und Zweck der Protokolldateien
- Erforderliche Systemkonten
- Informationen zum Bezug der neuesten Sicherheits-Patches

Zielgruppe

Diese Informationen sind für IT-Entscheidungsträger, -Architekten, -Administratoren und andere Personen bestimmt, die sich mit den Sicherheitskomponenten von Site Recovery Manager vertraut machen müssen.

Site Recovery Manager-Sicherheitsreferenz 1

Verwenden Sie die Sicherheitsreferenz, um sich mit den Sicherheitsfunktionen Ihrer Site Recovery Manager-Installation und den Maßnahmen zum Schutz Ihrer Umgebung vor Angriffen vertraut zu machen.

- Best Practices für den Schutz von Site Recovery Manager Server auf Seite 13

  Best Practices für den Schutz von Site Recovery Manager Server können Ihre Umgebung vor möglichen Sicherheitsproblemen schützen.

Site Recovery Manager -Dienste

Der Betrieb von Site Recovery Manager ist von verschiedenen Diensten abhängig, die auf der virtuellen Site Recovery Manager Server-Hostmaschine ausgeführt werden.

Tabelle 1-1. Von Site Recovery Manager benötigte Dienste

Dienstname	Startzeit	Beschreibung
VMware vCenter Site Recovery Manager Server	Automatisch	Bietet die Kernfunktionen von Site Recovery Manager.
Eingebettete Datenbank von VMware vCenter Site Recovery Manager	Automatisch, sofern Sie die eingebettete Datenbank verwenden	Der vPostgres-Server für die eingebettete Site Recovery Manager-Datenbank.
Server	Automatisch	Windows-Dienst, der die Dateifreigabe über das Netzwerk unterstützt.
Workstation	Automatisch	Windows-Dienst, der Verbindungen zu Remote-Servern erstellt und erhält.
Protected Storage	Automatisch	Windows-Dienste, die vertrauliche Daten speichern.

Site Recovery Manager -Netzwerkports

Site Recovery Manager verwendet Netzwerkports, die Sie konfigurieren können, um mit Clients und anderen Servern zu kommunizieren. Sie müssen sicherstellen, dass Firewalls nicht die von Site Recovery Manager verwendeten Ports blockieren.

Site Recovery Manager Server empfängt den gesamten eingehenden Datenverkehr auf einem Netzwerkport. Der Standardport lautet 9086. Wenn Sie Site Recovery Manager für die Verwendung einer eingebetteten Datenbank konfigurieren, empfängt die eingebettete Site Recovery Manager-Datenbank den localhost-Netzwerkdatenverkehr auf der lokalen Loopback-Schnittstelle. Der Standardport lautet 5678.

Sie können für den Datenverkehr von Site Recovery Manager und von eingebetteten Datenbanken während des Installationsvorgangs andere Ports auswählen, wenn die Standardports blockiert sind bzw. von anderen Anwendungen verwendet werden. Sie müssen Netzwerkrichtlinien konfigurieren, um den Datenverkehr auf dem eingehenden Port zu aktivieren. Informationen zu den Ports, die nach der Installation geändert werden können, finden Sie unter dem Thema *Ändern einer Site Recovery Manager Server-Installation* in der Dokumentation zu *Installation und Konfiguration von Site Recovery Manager*.

Site Recovery Manager Server kommuniziert auf der lokalen Site mit Platform Services Controller, vCenter Server, ESXi-Hosts und Arrays. Sie müssen sicherstellen, dass die Netzwerk-Firewall-Richtlinien den Datenverkehr zu den Netzwerkports aller Komponenten auf der lokalen Site aktivieren. Eine Liste der Standardports, die von allen VMware-Produkten verwendet werden, finden Sie unter http://kb.vmware.com/kb/1012382.

Die Verbindung zwischen der lokalen Site und der Remote-Site eines Site Recovery Manager-Paars muss privat sein, wie z. B. VPN. Der lokale Site Recovery Manager Server kommuniziert auf der Remote-Site mit Site Recovery Manager Server, Platform Services Controller und vCenter Server, und Ihr Netzwerkanbieter muss sicherstellen, dass die entsprechenden Netzwerkrichtlinien zur Aktivierung des Datenverkehrs vorhanden sind.

Eine Liste der Ports, die für Site Recovery Manager geöffnet sein müssen, finden Sie unter http://kb.vmware.com/kb/2147112.

Site Recovery Manager -Konfigurationsdateien

Einige Site Recovery Manager-Konfigurationsdateien enthalten Einstellungen, die möglicherweise die Sicherheit Ihrer Umgebung beeinträchtigen. Unpassende Einstellungen können sich auch auf das ordnungsgemäße Funktionieren Ihrer Site Recovery Manager-Umgebung auswirken.

Tabelle 1-2. Site Recovery Manager -Konfigurationsdateien

Speicherorte von Dateien oder Verzeichnissen	Beschreibung
installation_folder\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml	Definiert die Systemkonfiguration von Site Recovery Manager Server. **Hinweis** Verschieben oder löschen Sie die Konfigurationsdatei nicht. Sie können die Systemeinstellungen einer Site Recovery Manager-Instanz ändern. Verwenden Sie dazu die Registerkarte **Erweiterte Einstellungen** auf der Seite „Verwalten“ der vSphere Web Client-Benutzeroberfläche.
installation_folder\VMware\VMware vCenter Site Recovery Manager Embedded Database\bin\vmw_vpg_config\	Enthält Konfigurationsdateien der eingebetteten Datenbank. **Hinweis** Ändern, verschieben oder löschen Sie die Konfigurationsdatei nicht.
installation_folder\VMware\VMware vCenter Site Recovery Manager\config\extension.xml	Definiert die Konfiguration der Site Recovery Manager Server-Erweiterung. Die Datei extension.xml enthält Definitionen von Standard-Benutzerrollen und deren Privilegien. **Hinweis** Ändern, verschieben oder löschen Sie die Konfigurationsdatei nicht.

Site Recovery Manager -Zertifikate und -Schlüssel

Site Recovery Manager verwendet TLS-Zertifikate und private Schlüssel, um die Netzwerkkommunikation zu schützen und um die Authentifizierung mit anderen Servern sicher einzurichten.

CA-Zertifikat oder privater Schlüssel oder beides	Speicherort und Beschreibung
TLS-Zertifikat und Schlüssel für Site Recovery Manager Server-Endpunkt	Im Ordner Certificates\vmware-dr\Personal\Certificates im Windows-Zertifikatspeicher. Site Recovery Manager generiert das Zertifikat, sofern Sie während der Installation kein benutzerdefiniertes Zertifikat zur Verfügung stellen.
TLS-Zertifikat und Schlüssel für solution-Benutzer, die während der Installation von Site Recovery Manager erstellt wurden	Im Ordner Certificates\vmware-dr\su-*Site Recovery Manager-UUID*\Certificates im Windows-Zertifikatspeicher.

CA-Zertifikat oder privater Schlüssel oder beides	Speicherort und Beschreibung
TLS-Zertifikat und Schlüssel für `solution`-Benutzer auf der Remote-Site	Im Ordner `Certificates\vmware-dr\remote-su-`*`Site Recovery Manager-UUID`*`\Certificates` im Windows-Zertifikatspeicher. Site Recovery Manager erstellt die Dateien während des Koppelungsvorgangs.
CA-Zertifikat für Site Recovery Manager Server und TLS-Zertifikat	Datei *`installation_folder`*`\VMware\VMware vCenter Site Recovery Manager\bin\`*`SRM_Server_IP_addressca`*`.p7b` Site Recovery Manager generiert das Zertifikat, sofern Sie während der Installation kein benutzerdefiniertes Zertifikat zur Verfügung stellen. Sie können das Zertifikat in einen Client-Speicher der vertrauenswürdigen Schlüssel importieren, sodass Benutzer dem Site Recovery Manager Server-Zertifikat implizit vertrauen können.

Hinweis Extrahieren oder teilen Sie zum Schutz Ihrer Site Recovery Manager-Instanz keine Informationen über private Schlüssel.

Weitere Informationen zu Site Recovery Manager-Authentifizierungsmechanismen finden Sie unter dem Thema *Site Recovery Manager-Authentifizierung* im *Installations- und Konfigurationshandbuch für Site Recovery Manager*.

Von Site Recovery Manager gespeicherte Anmeldedaten

Site Recovery Manager speichert die Anmeldedaten des Speicherreplizierungsadapters (SRA) und der Datenbank in der Windows-Registrierung im verschlüsselten Format.

Sie haben Zugriff auf die Anmeldedaten, wenn Sie Mitglied der Administratorgruppe sind.

Registrierungspfad	Beschreibung
`HKEY_LOCAL_MACHINE\System\CurrentControl-Set\services\Vmware DR\Creds\db:`*`Datenspeicher-name`*	Anmeldedaten für den Zugriff auf die Site Recovery Manager-Datenbank unter Verwendung des *Dateispeichername*-Systemdatenspeichers.
`HKEY_LOCAL_MACHINE\System\ CurrentControl-Set\services\Vmware DR\Creds\storage-arraymana-ger `*`Manager-ID`*`-username`	Benutzername, der vom SRA beim Herstellen der Verbindung zum durch *Manager-ID* identifizierten Array-Manager verwendet werden muss.
`HKEY_LOCAL_MACHINE\System\ CurrentControl-Set\services\ Vmware DR\Creds\storage-arrayma-nager-`*`Manager-ID`*`-password`	Kennwort, das vom SRA beim Herstellen der Verbindung zum durch *Manager-ID* identifizierten Array-Manager verwendet werden muss.

Lizenz- und EULA-Dateien von Site Recovery Manager

Die Lizenz- und EULA-Dateien von Site Recovery Manager befinden sich auf der Site Recovery Manager Server-Hostmaschine.

Tabelle 1-3. Lizenz- und EULA-Dateien von Site Recovery Manager

Datei oder Verzeichnis	Beschreibung
`installation_folder``\VMware\VMware vCenter Site Recovery Manager\en\`	Verzeichnis mit den Dateien zur Endbenutzerlizenzvereinbarung für Site Recovery Manager.
`installation_folder``\VMware\VMware vCenter Site Recovery Manager\en\open_source_license.txt`	Site Recovery Manager-Open-Source-Lizenzdatei.
`installation_folder` `\VMware\VMware vCenter Site Recovery Manager\en\ open_source_licen-se_vix.txt`	Virtual Infrastructure Extension-API-Open-Source-Lizenzdatei.

Tabelle 1-3. Lizenz- und EULA-Dateien von Site Recovery Manager (Fortsetzung)

Datei oder Verzeichnis	Beschreibung
installation_folder\VMware\VMware vCenter Site Recovery Manager Embedded Database\share\EULA-en.doc	Dateien zur Endbenutzerlizenzvereinbarung für die eingebettete Datenbank von Site Recovery Manager.
installation_folder\VMware\VMware vCenter Site Recovery Manager Embedded Database\share\open_source_license.txt	Open-Source-Lizenzdatei für die eingebettete Datenbank von Site Recovery Manager.

Site Recovery Manager -Protokolldateien

Site Recovery Manager zeichnet Betriebsinformationen in den Protokolldateien auf. Die Protokolldateien enthalten keine vertraulichen Informationen, wie z. B. private Schlüssel oder Kennwörter.

Site Recovery Manager speichert die Protokolldateien im Verzeichnis `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs`. Die letzten Meldungen von Site Recovery Manager Server befinden sich in der Datei `vmware-dr-`*`number`*`.log`.

Wenn Sie Site Recovery Manager Server neu starten oder die aktuelle Datei die festgelegte maximale Dateigröße überschreiten muss, archiviert Site Recovery Manager die aktuelle Protokolldatei und erstellt eine neue Protokolldatei.

Geben Sie zum Ändern des Verzeichnisses für die Protokolldatei den benutzerdefinierten Namen eines Verzeichnisses in das XML-Element für das Verzeichnis in der Konfigurationsdatei *`installation_directory`*`\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml` ein. Sie können auch die Protokollierungsebene jeder Komponente ändern, indem Sie das logLevel-XML-Element in der Datei `vmware-dr.xml` ändern. Die Standardebene aller Komponenten ist „Ausführlich“.

Wichtig Konfigurieren Sie Zugriffssteuerungslisten, um den Zugriff auf die Protokolldateien einzuschränken.

Tabelle 1-4. Protokollierungsebenen

Ebene	Beschreibung
Fehler	Zeigt nur Protokolleinträge für Fehler an
Info	Zeigt Protokolleinträge für Informationen, Fehler und Warnungen an
Ausführlich (erweitert)	Zeigt erweiterte ausführliche Protokolleinträge für Informationen, Fehler, Warnungen und ausführliche Protokolleinträge an
Ausführlich	Zeigt ausführliche Protokolleinträge für Informationen, Fehler und Warnungen an
Warnung	Zeigt Protokolleinträge für Fehler und Warnungen an

Site Recovery Manager unterstützt Komponenten wie die folgenden:

- Standard
- Replizierungen
- Wiederherstellungen
- Speicher
- StorageProvider
- Vdb

- Persistenz

Die Datei `vmware-dr-Nummer.log` enthält keine Sicherheitsmeldungen zum Authentifizierungsvorgang und zu den Verbindungen mit der Remoteseite.

Site Recovery Manager -Konten

Site Recovery Manager verwendet Single Sign-On (SSO) für den Zugriff auf vCenter Server und Platform Services Controller.

Benutzerkonten

Die vCenter Server-Administratoren haben in der Standardkonfiguration Administratorzugriff auf Site Recovery Manager. Sie müssen die Administratoranmeldedaten verwenden, wenn Sie zum ersten Mal nach der Installation versuchen, sich bei Site Recovery Manager anzumelden.

Wenn Sie über Anmeldedaten des Administrators verfügen, können Sie anderen Benutzern mithilfe des vSphere Web Client Zugriff auf Site Recovery Manager gewähren.

Weitere Informationen zu Site Recovery Manager-Rollen, -Rechten und -Berechtigungen finden Sie unter *Site Recovery Manager-Rechte, -Rollen und -Berechtigungen* in der Dokumentation zu *Verwalten von Site Recovery Manager* .

`Solution` -Benutzerkonto

Site Recovery Manager erstellt während der Installation einen `solution`-Benutzer und verwendet diesen während der Authentifizierung mit vCenter Server. Der `solution`-Benutzer ist für jede Site Recovery Manager-Instanz eindeutig und ist der internen Verwendung durch Site Recovery Manager, vCenter Server und Platform Services Controller vorbehalten.

Site Recovery Manager erstellt während des Koppelungsvorgangs von Sites, die den erweiterten verknüpften Modus nicht verwenden, auf jeder Remote-Site einen zusätzlichen `solution`-Benutzer. Site Recovery Manager verwendet den `solution`-Benutzer, um erforderliche Vorgänge auf der Remote-Site durchzuführen.

Hinweis Sie dürfen die Rollen und Rechte, die mit den `solution`-Benutzerkonten verknüpft sind, nicht löschen oder ändern.

Weitere Informationen zu den `solution`-Benutzern und zur Authentifizierung zwischen der lokalen Site und der Remote-Site finden Sie unter dem Thema *Site Recovery Manager-Authentifizierung* in der Dokumentation zu *Installation und Konfiguration von Site Recovery Manager*.

Sicherheits-Updates und -Patches für Site Recovery Manager

Sie können Sicherheits-Updates und -Patches für Site Recovery Manager anwenden,wie sie von VMware bereitgestellt werden. Sie können Sicherheits-Updates und -Patches des Hostbetriebssystems anwenden, wie sie von den Anbietern des Hostbetriebssystems bereitgestellt werden.

Site Recovery Manager -Hostbetriebssystem-Versionen

Informationen zu den unterstützten Hostbetriebssystemen für Site Recovery Manager Server finden Sie in *Kompatibilitätstabellen für Site Recovery Manager 6.5* unter https://www.vmware.com/support/srm/srm-compat-matrix-6-5.html.

Installieren von Site Recovery Manager -Patches und -Sicherheits-Updates

Sie installieren Site Recovery Manager-Sicherheits-Patches und -Updates durch Ausführen eines direkten Upgrades Ihrer vorhandenen Site Recovery Manager-Installation. Informationen zum Aktualisieren von Site Recovery Manager finden Sie unter dem Thema *Direktes Upgrade von Site Recovery Manager Server* in *Installation und Konfiguration von Site Recovery Manager*.

Best Practices für den Schutz von Site Recovery Manager Server

Best Practices für den Schutz von Site Recovery Manager Server können Ihre Umgebung vor möglichen Sicherheitsproblemen schützen.

Der sichere Betrieb von Site Recovery Manager hängt von der ordnungsgemäßen Konfiguration und Wartung des Site Recovery Manager Server-Betriebssystems ab.

- Führen Sie Site Recovery Manager nur auf unterstützten Hostbetriebssystemen, Datenbanken und Hardwarekonfigurationen aus. Wenn Site Recovery Manager nicht auf einem unterstützten Hostbetriebssystem ausgeführt wird, wird Site Recovery Manager möglicherweise nicht ordnungsgemäß ausgeführt.
- Wenden Sie die neuesten Updates und Patches des Betriebssystems an, um das Hostbetriebssystem vor böswilligen Angriffen zu schützen. Wenden Sie die neuesten Site Recovery Manager-Updates und -Patches an, um bekannte Probleme mit Site Recovery Manager zu lösen.
- Stellen Sie die Integrität Ihrer Site Recovery Manager-Bereitstellung sicher, wenn Sie Site Recovery Manager als VM ausführen. Informationen dazu finden Sie unter dem Thema *Virtuelle Maschine – Empfohlene Vorgehensweisen für die Sicherheit* in der Dokumentation zu *vSphere-Sicherheit*.
- Begrenzen Sie die Installation von Software und deaktivieren Sie Dienste, die Site Recovery Manager nicht verwendet. Auf diese Weise können Sie Ressourcen verfügbar machen und die Wahrscheinlichkeit von Angriffen auf den Server reduzieren. Nicht benötigte Software und Dienste verbrauchen CPU-, Speicher-, Arbeitsspeicher- und Bandbreitenressourcen und erhöhen die Wahrscheinlichkeit von Angriffen auf den Server.
- Gestatten Sie nur Administratoren den Zugriff auf den Server. Reduzieren Sie zur Begrenzung der Anzahl von Konten, die ein Angreifer verwenden könnte, die Anzahl von Konten mit Zugriffsberechtigungen auf den Server.
- Überprüfen Sie die von Site Recovery Manager verwendeten Netzwerkports und konfigurieren Sie eine Firewall für den Schutz Ihres Servers.

Index