

Oracle® Fabric Manager 5.0.2 - Sicherheitshandbuch



Teilenr.: E79496-02
November 2016

Teilenr.: E79496-02

Copyright © 2016, Oracle und/oder verbundene Unternehmen. All rights reserved. Alle Rechte vorbehalten.

Diese Software und zugehörige Dokumentation werden im Rahmen eines Lizenzvertrages zur Verfügung gestellt, der Einschränkungen hinsichtlich Nutzung und Offenlegung enthält und durch Gesetze zum Schutz geistigen Eigentums geschützt ist. Sofern nicht ausdrücklich in Ihrem Lizenzvertrag vereinbart oder gesetzlich geregelt, darf diese Software weder ganz noch teilweise in irgendeiner Form oder durch irgendein Mittel zu irgendeinem Zweck kopiert, reproduziert, übersetzt, gesendet, verändert, lizenziert, übertragen, verteilt, ausgestellt, ausgeführt, veröffentlicht oder angezeigt werden. Reverse Engineering, Disassemblierung oder Dekompilierung der Software ist verboten, es sei denn, dies ist erforderlich, um die gesetzlich vorgesehene Interoperabilität mit anderer Software zu ermöglichen.

Die hier angegebenen Informationen können jederzeit und ohne vorherige Ankündigung geändert werden. Wir übernehmen keine Gewähr für deren Richtigkeit. Sollten Sie Fehler oder Unstimmigkeiten finden, bitten wir Sie, uns diese schriftlich mitzuteilen.

Wird diese Software oder zugehörige Dokumentation an die Regierung der Vereinigten Staaten von Amerika bzw. einen Lizenznehmer im Auftrag der Regierung der Vereinigten Staaten von Amerika geliefert, dann gilt Folgendes:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Diese Software oder Hardware ist für die allgemeine Anwendung in verschiedenen Informationsmanagementanwendungen konzipiert. Sie ist nicht für den Einsatz in potenziell gefährlichen Anwendungen bzw. Anwendungen mit einem potenziellen Risiko von Personenschäden geeignet. Falls die Software oder Hardware für solche Zwecke verwendet wird, verpflichtet sich der Lizenznehmer, sämtliche erforderlichen Maßnahmen wie Fail Safe, Backups und Redundancy zu ergreifen, um den sicheren Einsatz dieser Software oder Hardware zu gewährleisten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keinerlei Haftung für Schäden, die beim Einsatz dieser Software oder Hardware in gefährlichen Anwendungen entstehen.

Oracle und Java sind eingetragene Marken von Oracle und/oder ihren verbundenen Unternehmen. Andere Namen und Bezeichnungen können Marken ihrer jeweiligen Inhaber sein.

Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Alle SPARC-Marken werden in Lizenz verwendet und sind Marken oder eingetragene Marken der SPARC International, Inc. AMD, Opteron, das AMD-Logo und das AMD Opteron-Logo sind Marken oder eingetragene Marken der Advanced Micro Devices. UNIX ist eine eingetragene Marke der The Open Group.

Diese Software oder Hardware und die Dokumentation können Zugriffsmöglichkeiten auf oder Informationen über Inhalte, Produkte und Serviceleistungen von Dritten enthalten. Sofern nicht ausdrücklich in einem Vertrag mit Oracle vereinbart, übernehmen die Oracle Corporation und ihre verbundenen Unternehmen keine Verantwortung für Inhalte, Produkte und Serviceleistungen von Dritten und lehnen ausdrücklich jegliche Art von Gewährleistung diesbezüglich ab. Sofern nicht ausdrücklich in einem Vertrag mit Oracle vereinbart, übernehmen die Oracle Corporation und ihre verbundenen Unternehmen keine Verantwortung für Verluste, Kosten oder Schäden, die aufgrund des Zugriffs oder der Verwendung von Inhalten, Produkten und Serviceleistungen von Dritten entstehen.

Barrierefreie Dokumentation

Informationen zu Oracles Verpflichtung zur Barrierefreiheit erhalten Sie über die Website zum Oracle Accessibility Program <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Zugriff auf Oracle-Support

Oracle-Kunden mit einem gültigen Oracle Supportvertrag haben Zugriff auf elektronischen Support über My Oracle Support. Weitere Informationen erhalten Sie unter <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> oder unter <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>, falls Sie eine Hörbehinderung haben.

Inhalt

Oracle Fabric Manager - Sicherheit	7
Oracle Fabric Manager - Übersicht	7
Allgemeine Sicherheitsgrundsätze	7
Software auf dem neuesten Stand halten	8
Netzwerkzugriff auf kritische Services beschränken	8
Prinzip der geringsten Berechtigungen beachten	8
Systemaktivität überwachen	9
Sicherheitsinformationen müssen immer auf dem neuesten Stand sein	9
Zugriff	9
▼ Dateiberechtigungen überprüfen	10
▼ Zugriff auf Standardkonten kontrollieren	10
SSL-Zertifikat	11
▼ Zugriff durch nicht aufgeführte Benutzer sperren	11
Sicherheit für Oracle Fabric Manager-Plug-ins	12
Sicherheit für Oracle Fabric Monitor	12
Allgemein	12
MySQL	12
PostGres	12

Oracle Fabric Manager - Sicherheit

Dieses Dokument enthält allgemeine Sicherheitsrichtlinien für Oracle Fabric Manager ab Version 5.0.0. Diese Informationen sollen Sie beim Sichern der Oracle Fabric Manager-Software unterstützen.

- [„Oracle Fabric Manager - Übersicht“ \[7\]](#)
- [„Allgemeine Sicherheitsgrundsätze“ \[7\]](#)
- [„Zugriff“ \[9\]](#)
- [Dateiberechtigungen überprüfen \[10\]](#)
- [Zugriff auf Standardkonten kontrollieren \[10\]](#)
- [„SSL-Zertifikat“ \[11\]](#)
- [Zugriff durch nicht aufgeführte Benutzer sperren \[11\]](#)
- [„Sicherheit für Oracle Fabric Manager-Plug-ins“ \[12\]](#)
- [„Sicherheit für Oracle Fabric Monitor“ \[12\]](#)

Oracle Fabric Manager - Übersicht

Oracle Fabric Manager wurde von Oracle als Verwaltungssystem für mehrere Geräte entwickelt, mit dem Oracle Fabric-Geräte (Oracle InfiniBand Switch IS2-46, Oracle Fabric Interconnects und/oder Oracle SDN-Controller) sowie virtuelle Oracle I/O-Geräte inventarisiert und verwaltet werden können. Oracle Fabric Manager ist ein Server-Client-Modell und unterstützt die Konfiguration und Verwaltung virtueller Ressourcen auf der Ebene von Fabric-Gerät, Modul sowie Server oder virtueller Maschine.

Oracle Fabric Manager ist ein browserbasiertes Verwaltungssystem und wird auf einem Remote-Server ausgeführt. Der Remote-Server von Oracle Fabric Manager übersetzt Konfigurations- und Verwaltungsaufgaben von der Oracle Fabric Manager-Benutzeroberfläche und gibt diese Informationen an von Oracle Fabric Manager verwaltete Fabric-Geräte weiter.

Allgemeine Sicherheitsgrundsätze

In diesen Themen werden die Grundsätze beschrieben, die für eine sichere Verwendung von Anwendungen unerlässlich sind.

Software auf dem neuesten Stand halten

Halten Sie die verwendete Version von Oracle Fabric Manager immer aktuell. Sie können die aktuellen Versionen der Software unter <http://support.oracle.com> herunterladen.

Netzwerkzugriff auf kritische Services beschränken

Oracle Fabric Manager verwendet die folgenden Ports:

Port	Beschreibung
8880 oder 8443 (HTTPS)	Wird von Endbenutzern für die Anmeldung bei Oracle Fabric Manager verwendet. Alternativ können Sie aus Sicherheitsgründen diese Ports geschlossen lassen und stattdessen eine RDP-Sitzung öffnen und den lokalen Browser verwenden.
443	Wird von Oracle Fabric Manager für externe Verbindungen zur Konfiguration von Fabric Interconnects und OSDN-Controllern verwendet.
6522	Wird von Oracle Fabric Manager für externe Verbindungen zur Ermittlung von Fabric Interconnects und OSDN-Controllern verwendet.
7443	Wird von Oracle Fabric Manager für externe Verbindungen zur Konfiguration von Oracle InfiniBand-Switches verwendet.
7777	Wird von Oracle Fabric Manager für externe Verbindungen zur Ermittlung von Oracle InfiniBand-Switches verwendet.
22	Wird von Oracle Fabric Manager zum Herunterladen von Protokollen sowie zum Exportieren und Importieren von Backupdateien auf allen Gerätetypen verwendet

Verbinden Sie Oracle Fabric Manager und alle davon gesteuerten Geräte ausschließlich mit einem sicheren Verwaltungsnetzwerk. Verbinden Sie sie nicht mit dem Internet.

Prinzip der geringsten Berechtigungen beachten

Gewähren Sie dem Benutzer oder Administrator die geringsten Berechtigungen, die für das Durchführen der Aufgabe erforderlich sind. Oracle Fabric Manager enthält verschiedene Rollen, die Benutzern erteilt werden können. Diese Rollen gewähren Berechtigungen, die in Art und Umfang unterschiedlich sind.

Verwenden Sie die Funktionen des Sicherheitsmanagers im Navigationsbereich der Benutzeroberfläche, um die Benutzerrollen für Oracle Fabric Manager zu konfigurieren. Mit den Funktionen des Sicherheitsmanagers können Sie auch Fabric-Geräte in bestimmten Netzwerkdomeänen konfigurieren. Einzelheiten zur Verwendung des Sicherheitsmanagers finden Sie in der Dokumentation [Oracle Fabric Manager 5.0.2 Administration Guide](#).

Systemaktivität überwachen

Überwachen Sie die Systemaktivität, um festzustellen, wie gut Oracle Fabric Manager arbeitet und ob ungewöhnliche Aktivitäten protokolliert werden. Prüfen Sie die folgenden Protokolldateien, die Informationen zu Oracle Fabric Manager enthalten:

Windows Server	Linux Server	Oracle Solaris Server
director-<name>.log	director-<name>.log	director-<name>.log
xmsaudit.log.1	xmsaudit.log.1	xmsaudit.log.1
xms-ha.log.1	xms-ha.log.1	xms-ha.log.1
xmsjobs.log.1	xmsjobs.log.1	xmsjobs.log.1
xms.log.1	xms.log.1	xms.log.1
xms-schedule.log.1	xms-schedule.log.1	xms-schedule.log.1
xms-stderr.log	tomcat.log	tomcat.log
xms-stdout.log	catalina.out	catalina.out
commons-daemon.log		catalina.pid

Sicherheitsinformationen müssen immer auf dem neuesten Stand sein

Sie können Sicherheitsinformationen aus mehreren Quellen erhalten.

- Sicherheitsinformationen und Warnungen für zahlreiche Produkte finden Sie unter <http://www.us-cert.gov>.
- Führen Sie die neueste Version der Oracle Virtual Networking-Software aus, und lesen Sie die zugehörige Dokumentation.

Zugriff

Lassen Sie Webzugriff auf Oracle Fabric Manager nur über ein privates Netzwerk hinter der DMZ zu.

Verhindern Sie den lokalen Zugriff auf Oracle Fabric Manager. Dazu können Sie beispielsweise die Oracle Fabric Manager-Ports mit einer Firewall blockieren. Führen Sie das RDP (Remote Desktop Protocol) für den Zugriff auf den Host aus, und stellen Sie über `localhost` die Verbindung mit Oracle Fabric Manager her.

Stellen Sie sicher, dass Oracle Fabric Manager nur über ein sicheres privates Netzwerk mit Fabric-Geräten wie Fabric Interconnects oder Oracle SDN-Controllern kommunizieren kann.

▼ Dateiberechtigungen überprüfen

Prüfen Sie die Dateiberechtigungen, nachdem Sie die Oracle Fabric Manager-Software installiert haben. Mit der folgenden Prozedur können Sie die Berechtigungen für Linux oder Oracle Solaris überprüfen.

1. **Bevor Sie Oracle Fabric Manager installieren, erstellen Sie einen Benutzer namens `xsigo`.**

Erstellen Sie eine Datei namens `~xsigo/.profile`, und fügen Sie die folgende Zeile ein:

```
umask 077
```

Vergewissern Sie sich, dass dieses Profil angewendet wurde. Geben Sie dazu die folgenden Befehle ein, und überprüfen Sie, ob die Ausgabe `077` lautet.

```
# su xsigo
# umask
0077
```

2. **Installieren Sie Oracle Fabric Manager.**

Weitere Informationen finden Sie unter [„Installing the Software“ in Oracle Fabric Manager 5.0.2 Installation Guide](#).

3. **Überprüfen Sie nach der Installation die Berechtigungsstufe der Produktdateien, um zu ermitteln, ob global schreibgeschützte oder nicht schreibgeschützte Dateien vorhanden sind.**

Mit diesen Linux-Befehlen sollten keine Dateien abgerufen werden:

```
find /opt/xsigo/xms/ -perm -o=r
find /opt/xsigo/xms/ -perm -o=w
```

4. **Korrigieren Sie die Berechtigungen aller ermittelten Dateien.**

▼ Zugriff auf Standardkonten kontrollieren

Oracle Fabric Manager enthält standardmäßig zwei automatisch autorisierte Benutzer:

- root (Windows: administrator)
- ofmadmin

Stellen Sie sicher, dass Angreifer keine Benutzer im System erstellen können, die Zugriff auf diese Konten haben.

1. **Stellen Sie eine sichere, zentralisierte Authentifizierung für das System bereit.**
2. **Erstellen Sie unmittelbar nach der Installation von Oracle Fabric Manager einen Benutzer namens `ofmadmin`, und legen Sie für dieses Konto ein zufälliges Kennwort fest.**

Weitere Informationen finden Sie unter „Assign a Role to a User“ in *Oracle Fabric Manager 5.0.2 Administration Guide*.

SSL-Zertifikat

Installieren Sie ein ordnungsgemäß signiertes SSL-Zertifikat für Oracle Fabric Manager. Weitere Details finden Sie unter „Configuring a Certificate for Oracle Fabric Manager“ in *Oracle Fabric Manager 5.0.2 Installation Guide*.

▼ Zugriff durch nicht aufgeführte Benutzer sperren

Standardmäßig erhalten nicht aufgeführte Benutzer keinen Zugriff auf Oracle Fabric Manager. Für aufgeführte Benutzer sind neben dem zugrunde liegenden Benutzerkonto des Hostbetriebssystems auch in Oracle Fabric Manager Benutzerrollen definiert. Wenn eine Einstellung geändert wird, sodass nicht aufgeführte Benutzer Zugriff erhalten, können sich Benutzer mit einem auf dem Host authentifizierbaren Konto bei Oracle Fabric Manager anmelden und die Operatorrolle (d.h. Lesezugriff) erhalten. Wenn nicht aufgeführte Benutzer gesperrt werden, können sie zwar möglicherweise auf dem Host authentifiziert werden, erhalten jedoch keinen Zugriff auf Oracle Fabric Manager, d.h. die Authentifizierung erscheint nicht erfolgreich.

Um diese Sicherheitsebene zu prüfen, stellen Sie sicher, dass der Zugriff durch nicht aufgeführte Benutzer deaktiviert ist.

1. **Klicken Sie auf das Symbol für Fabric Manager Maintenance.**
2. **Suchen Sie die Option "Nicht aufgeführte Benutzer zulassen".**

Wenn neben dieser Option ein Häkchen angezeigt wird, entfernen Sie es, um den Zugriff zu deaktivieren.

Sicherheit für Oracle Fabric Manager-Plug-ins

Oracle Fabric Manager können verschiedene Plug-in-Module hinzugefügt werden. Treffen Sie dieselben allgemeinen Sicherheitsvorkehrungen, wenn Sie ein Plug-in-Modul installieren und verwenden möchten.

Befolgen Sie außerdem die spezifischen Sicherheitsrichtlinien für jedes Plug-in. Sicherheitsinformationen für einige Plug-in-Module finden Sie in „[Sicherheit für Oracle Fabric Monitor](#)“ [12].

Sicherheit für Oracle Fabric Monitor

Wenn Sie das Plug-in-Modul "Oracle Fabric Monitor" mit Oracle Fabric Manager verwenden, befolgen Sie neben den allgemeinen Sicherheitspraktiken für Oracle Fabric Manager außerdem diese Richtlinien.

Allgemein

- Die Datenbank muss sich in einem Verwaltungsnetzwerk hinter der DMZ befinden.
- Erstellen Sie Backups der Datenbank.

MySQL

Sichern Sie die MySQL-Funktionen dieses Plug-in-Moduls. Weitere Informationen finden Sie unter <http://dev.mysql.com/doc/refman/5.7/en/security-guidelines.html>.

PostGres

Sichern Sie die postgres-Funktionen dieses Plug-in-Moduls. Weitere Informationen finden Sie in den Sicherheitsrichtlinien für die enthaltene Version von postgres unter <http://www.postgresql.org/docs/>.