Oracle® Solaris 11.2 Handbuch zur Sicherheitscompliance

Teilenr.: E53935
Juli 2014

ORACLE

Inhalt

Verwendung dieser Dokumentation

- **Überblick** – Hier wird beschrieben, wie Sie die Compliance eines Oracle Solaris-Systems mit bestimmten Sicherheitsbenchmarks bewerten und melden können.
- **Zielgruppe** – Sicherheitsadministratoren und Prüfer, die die Sicherheit auf Oracle Solaris 11-Systemen bewerten.
- **Benötigte Vorkenntnisse** – Standortsicherheitsanforderungen.

Produktdokumentationsbibliothek

Aktuelle Informationen und bekannte Probleme mit diesem Produkt finden Sie in der Dokumentationsbibliothek unter http://www.oracle.com/pls/topic/lookup?ctx=E56340.

Zugriff auf Oracle Support

Oracle-Kunden haben Zugriff auf elektronischen Support unter My Oracle Support. Besuchen Sie dazu die Website http://www.oracle.com/pls/topic/lookup?ctx=acc{ENT:#x0026}id=info bzw. die Website http://www.oracle.com/pls/topic/lookup?ctx=acc{ENT:#x0026}id=trs für Hörgeschädigte.

Feedback

Unter http://www.oracle.com/goto/docfeedback können Sie uns Feedback zu dieser Dokumentation geben.

♦ ♦ ♦ KAPITEL 1

Melden der Compliance mit Sicherheitsstandards

In diesem Kapitel wird beschrieben, wie Sie die Compliance eines Oracle Solaris-Systems mit bestimmten Sicherheitsstandards, die auch als *Sicherheitsbenchmarks* und *Sicherheitsrichtlinien* bezeichnet werden, bewerten und melden. In diesem Kapitel werden die folgenden Themen behandelt:

Compliance

Systeme, die geltenden Sicherheitsstandards entsprechen, bieten eine sicherere Arbeitsumgebung und sind darüber hinaus leichter zu testen, zu warten und zu schützen. In diesem Release stellt Oracle Solaris Skripte zur Verfügung, mit denen Sie die Compliance Ihres Oracle Solaris-Systems mit zwei Sicherheitsbenchmarks, der Solaris Security Benchmark und dem Payment Card Industry-Data Security Standard (PCI-DSS), bewerten und melden können.

Eine Überprüfung der Systemkonfiguration auf Compliance mit externen und internen Sicherheitsrichtlinien ist von entscheidender Bedeutung. Die Handhabung der Anforderungen bezüglich Sicherheitscompliance und Prüfung macht einen Großteil der Ausgaben für Sicherheit im IT-Bereich aus, darunter Dokumentation, Berichte und die Überprüfung selbst. Organisationen wie Banken, Krankenhäuser und Behörden besitzen jeweils ihre eigenen Complianceanforderungen. Prüfern, die sich mit einem Betriebssystem nicht auskennen, fällt es zum Teil schwer, bei ihren Kontrollen einen Abgleich mit geltenden Sicherheitsanforderungen vorzunehmen. Tools zur Zuordnung von Sicherheitskontrollen zu Anforderungen können Prüfern daher helfen, Zeit und Geld zu sparen.

Die Complianceskripte basieren auf dem Security Content Automation Protocol (SCAP), das in der Programmiersprache Open Vulnerability and Assessment Language (OVAL) verfasst

ist. Die SCAP-Implementierung in Oracle Solaris unterstützt darüber hinaus Skripte, die der Script Check Engine (SCE) entsprechen. Diese Skripte fügen Sicherheitsprüfungen hinzu, die die aktuellen OVAL-Schemas und Probes nicht bieten. Mithilfe weiterer Skripte können weitere Sicherheitsbestimmungen wie z. B. der Gramm-Leach-Bliley Act (GLBA), der Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX) oder der Federal Information Security Management Act (FISMA) erfüllt werden. Links zu diesen Standards finden Sie unter „Compliancereferenz“ [14].

Oracle Solaris-Sicherheitsbenchmarks

Oracle Solaris 11 stellt Complianceskripte für die beiden Standards Solaris und PCI-DSS bereit.

Solaris-Sicherheitsrichtlinien-Benchmark

Die Solaris-Sicherheitsrichtlinien-Benchmark ist ein Standard, der auf einer standardmäßig sicheren („Secure by Default“, SBD) Standardinstallation von Oracle Solaris beruht. Die Benchmark bietet die beiden Profile "Baseline" (Basis) und "Recommended" (Empfohlen). Die Profile sind unter „Messung der Compliance“ [9] beschrieben.

Die zur standardmäßigen Sicherheit gehörigen Funktionen werden unter „Using the Secure by Default Configuration“ in „Securing Systems and Attached Devices in Oracle Solaris 11.2 “ und unter „Konfigurierbare Sicherheit in Oracle Solaris“ in „Oracle Solaris 11 – Sicherheitsbestimmungen “ beschrieben.

Diese Benchmark erfüllt nicht die Anforderungen des PCI-DSS oder den CIS- (Center for Internet Security) und DISA-STIG-Benchmarks (Defense Information Systems Agency-Security Technical Information Guides) für Oracle Solaris.

PCI-DSS-Sicherheitsrichtlinien-Benchmark

Die PCI-DSS-Sicherheitsrichtlinien-Benchmark ist ein proprietärer Standard zur Datensicherheit in Organisationen, die Kreditkarteninformationen führender Kreditkartenanbieter verwenden. Der Standard wird von dem Gremium "Payment Card Industry Security Standards Council" definiert. Ziel ist es, Kreditkartenbetrug zu unterbinden.

Ein Oracle Solaris-System muss für eine Konformität mit dem PCI DSS-Standard entsprechend konfiguriert werden. Der Compliancebericht zeigt an, welche Tests erfolgreich bzw. nicht erfolgreich waren, und bietet Schritte zur Korrektur an.

Messung der Compliance

Eine Messung der Sicherheitscompliance, im Folgenden einfach *Compliance* genannt, setzt eine Sicherheitsbenchmark oder ein Profil voraus, eine Messung der Compliance im Vergleich zu dieser Benchmark (*Bewertung* genannt) und einen abschließenden Bericht der Ergebnisse. Der Bericht kann zu Schulungs- oder Archivierungszwecken auch in Form einer Anleitung ausgedruckt werden.

Oracle Solaris stellt Skripte bereit, die zwei Sicherheitsprofile in der Solaris-Benchmark messen.

- Das Profil "Baseline" (Basis) der Solaris-Benchmark entspricht eng der standardmäßigen SBD-Installation von Oracle Solaris.
- Das Solaris-Profil "Recommended" (Empfohlen) erfüllt den Bedarf von Organisationen, die strengere Sicherheitsanforderungen als im "Baseline"-Profil vorgegeben benötigen.

  Diese Profile sind ineinander verschachtelt. Systeme, die mit dem Profil "Recommended" konform sind, sind auch automatisch mit dem Profil "Baseline" konform.

Die PCI-DSS-Benchmark misst die Compliance Ihres Systems mit dem Standard PCI-DSS. Da die PCI-DSS-Anforderungen keine direkt codierten Links besitzen, müssen Sie den Bericht auf Compliance überprüfen. Weitere Informationen finden Sie unter Meeting PCI DSS Compliance with Oracle Solaris 11.

`compliance`-Package

Die Compliancefunktion ist über das Package `pkg:/security/compliance` verfügbar, das innerhalb der Packagegruppen `solaris-small-server` und `solaris-large-server` installiert wird.

- Informationen zu Packagegruppen finden Sie im Abschnitt „Installieren von Oracle Solaris-BS“ in „Oracle Solaris 11 – Sicherheitsbestimmungen “.
- Informationen zu Packages finden Sie in „Oracle Solaris 11.2 Package Group Lists “.
- Um eine Beschreibung der Compliancepackages anzuzeigen, geben Sie den Befehl `pkg info compliance` aus.

Oracle Solaris-Compliancebewertung

Mit dem Befehl `compliance` können Sie die Compliance eines Systems mit einer bestimmten Benchmark bewerten und melden. Über den Oracle Solaris-Compliancebefehl werden die Anforderungen einer Benchmark dem Code, der Datei oder der Befehlsausgabe zugeordnet, mit dem bzw. der die Compliance mit einer bestimmten Anforderung überprüft wird. Weitere Informationen zu diesem Befehl finden Sie auf der Manpage `compliance`(1M).

Informationen zu den SCAP-Tools, die den `compliance`-Befehl unterstützen, finden Sie auf der Manpage `oscap`(8). Um die Version der SCAP-Tools anzuzeigen, geben Sie den Befehl `oscap -V` aus.

Anmerkung - Mit den SCAP-Tools können die vom `oscap`-Befehl erzeugten Berichte sowie die Testbeschreibungen nicht lokalisiert werden. (Lokalisierung umfasst die Übersetzung der Software in die jeweilige Landessprache.)

Bewertung der Compliance mit Produkten von Drittanbietern

Die Drittanbieter-Standardorganisation CIS bietet Tools zur automatischen Compliancеprüfung ihrer Benchmark. Wenden Sie sich an CIS, um den Preis für die Verwendung dieser Tools zur Messung der Compliance in Bezug auf die CIS-Benchmark zu erfahren. CIS-Tools zur Prüfung der Oracle Solaris-Compliance können auf Microsoft Windows-Systemen verwendet werden.

Bewerten der Oracle Solaris-Compliance

Mit dem Befehl `compliance` wird die Compliancebewertung automatisiert, nicht die Korrektur. Der Befehl wird zum Auflisten, Generieren und Löschen von Bewertungen und Berichten verwendet. Auf Complianceberichte können alle Benutzer zugreifen. Zur Verwaltung der Bewertungen und zum Generieren von Berichten sind entsprechende Rechte erforderlich. Weitere Informationen finden Sie auf der Manpage `compliance`(1M).

Über den Befehl `compliance` werden nur lokale Dateien geprüft. Wenn in Ihrem System Dateisysteme gemountet sind, müssen Sie die Compliance der Clients und der Server getrennt testen. Beispiel: Wenn Sie die Standardverzeichnisse der Benutzer über zentrale Server mounten, führen Sie den `compliance`-Befehl auf den Benutzersystemen und auf jedem Server aus, der die Standardverzeichnisse exportiert.

Rechte zur Ausführung des `compliance`-Befehls

Oracle Solaris stellt zwei Rechteprofile für die Compliancebewertung und Berichtgenerierung bereit.

- Das Rechteprofil "Compliance Assessor" (Compliancebewerter) berechtigt Benutzer, Bewertungen auszuführen, sie im Bewertungsspeicher abzulegen, Berichte zu generieren und Bewertungen aus dem Speicher zu löschen.
- Das Rechteprofil "Compliance Reporter" (Complianceberichte) berechtigt Benutzer zur Generierung neuer Berichte aus vorhandenen Bewertungen.

Für die Complianceunterbefehle sind folgende Rechte erforderlich:

- `compliance assess`-Befehl – Erfordert sämtliche Berechtigungen sowie die Autorisierung `solaris.compliance.assess`. Das Rechteprofil "Compliance Assessor" stellt diese Rechte bereit.
- `compliance delete`-Befehl – Erfordert Schreibzugriff auf den Bewertungsspeicher sowie die Autorisierung `solaris.compliance.assess`. Das Rechteprofil "Compliance Assessor" stellt diese Rechte bereit.
- `compliance list`-Befehl – Kann von allen Benutzern mit Basisrechten ausgeführt werden. Dieser Befehl bietet eine vollständige Sichtbarkeit der Benchmarks und Bewertungen.
- `compliance report`-Befehl – Kann von allen Benutzern ausgeführt werden. Die Reichweite der Funktionen hängt jedoch von den Rechten des jeweiligen Benutzers ab. Benutzer, denen entweder das Profil "Compliance Assessor" oder "Compliance Reporter" zugewiesen ist, können neue Berichte im Bewertungsspeicher generieren. Alle Benutzer können vorhandene Berichte anzeigen. Benutzer, die lediglich über Basisrechte verfügen, können jedoch keine Berichte generieren.

Erstellen von Compliancebewertungen und -berichten

Compliancebewertungen decken jeweils das gesamte System ab. Berichte können sämtliche Objekte in der Bewertung umfassen oder nur eine Teilmenge der Informationen in der Bewertung. Führen Sie Bewertungen regelmäßig aus, beispielsweise als `cron`-Job, um die Compliance Ihres Systems zu überwachen.

▼ So führen Sie Complianceberichte aus

Die Packages `solaris-small-server` und `solaris-large-server` umfassen standardmäßig das Package `compliance`. Die Packages `solaris-desktop` und `solaris-minimal` beinhalten das Package `compliance` hingegen nicht.

Bevor Sie beginnen Sie benötigen das Rechteprofil "Software Installation" (Softwareinstallation), um dem System Packages hinzuzufügen. Für die meisten Compliancebefehle benötigen Sie Admin-Rechte, wie unter „Rechte zur Ausführung des `compliance`-Befehls“ [10] beschrieben. Weitere Informationen finden Sie im Abschnitt „Using Your Assigned Administrative Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

1. **Installieren Sie das Package `compliance`.**

   ```
   # pkg install compliance
   ```

   Über folgende Nachricht wird angezeigt, dass das Package installiert wurde:

   ```
   No updates necessary for this image.
   ```

Weitere Informationen finden Sie auf der Manpage pkg(1).

Anmerkung - Installieren Sie das Package in jeder Zone, in der Sie Compliancetests ausführen wollen.

2. Erstellen Sie eine Bewertung.

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
 No assessments available
# compliance -p profile -a assessment-directory
```

`-p` Gibt den Namen des Profils an. Der Profilname ist abhängig von der Groß-/Kleinschreibung.

`-a` Gibt den Verzeichnisnamen der Bewertung an. Der Standardname beinhaltet einen Zeitstempel.

Beispiel: Mit dem folgenden Befehl wird eine Bewertung über das Profil "Recommended" erstellt.

```
# compliance -p Recommended -a recommended
```

Der Befehl erstellt unter `/var/share/compliance/assessments` ein Verzeichnis mit dem Namen `recommended`, das die Bewertung in drei Dateien enthält: eine Logdatei, eine XML-Datei und eine HTML-Datei.

```
# cd /var/share/compliance/assessments/recommended
# ls
recommended.html
recommended.txt
recommended.xml
```

Wenn Sie diesen Befehl erneut ausführen, werden die Dateien nicht ersetzt. Sie müssen die Dateien entfernen, bevor Sie ein Bewertungsverzeichnis erneut verwenden können.

3. (Optional) Erstellen Sie einen benutzerdefinierten Bericht.

```
# compliance report -s -pass,fail,notselected
/var/share/compliance/assessments/recommended/report.-pass,fail,notselected.html
```

Mit diesem Befehl wird ein Bericht erstellt, der nicht erfolgreiche und nicht gewählte Objekte im HTML-Format enthält. Der Bericht wird anhand der aktuellsten Bewertung ausgeführt.

Sie können benutzerdefinierte Berichte wiederholt ausführen. Die vollständigen Berichte, d. h. die Bewertung, können Sie im Ausgangsverzeichnis jedoch nur einmal ausführen.

4. **Zeigen Sie den vollständigen Bericht an.**

   Sie können die Logdatei in einem Texteditor, die HTML-Datei in einem Browser oder die XML-Datei in einem XML-Viewer anzeigen.

   Beispiel: Um den benutzerdefinierten HTML-Bericht aus dem vorigen Schritt anzuzeigen, geben Sie folgenden Browsereintrag ein:

   ```
   file:///var/share/compliance/assessments/recommended/report.-pass,fail,notselected.html
   ```

5. **Beheben Sie alle Fehler, die Ihre Sicherheitsrichtlinie für eine erfolgreiche Bewertung erfordert.**

   a. **Führen Sie für den nicht erfolgreichen Eintrag die Korrekturmaßnahme durch.**

   b. **Wenn die Korrekturmaßnahme einen Neustart des Systems umfasst, starten Sie das System vor der erneuten Ausführung der Bewertung neu.**

6. **(Optional) Führen Sie den `compliance`-Befehl als `cron`-Job aus.**

   ```
   # cron -e
   ```

   Für eine tägliche Compliancebewertung um 2:30 Uhr fügt `root` folgenden Eintrag hinzu:

   ```
   30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
   ```

   Für eine wöchentliche Compliancebewertung jeden Sonntag um 1:15 Uhr fügt `root` folgenden Eintrag hinzu:

   ```
   15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
   ```

   Für monatliche Bewertungen jeweils am Ersten des Monats um 4:00 Uhr fügt `root` folgenden Eintrag hinzu:

   ```
   0 4 1 * * /usr/bin/compliance assess -b pci-dss
   ```

   Für Bewertungen jeweils am ersten Montag des Monats um 3:45 Uhr fügt `root` folgenden Eintrag hinzu:

   ```
   45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
   ```

7. **(Optional) Erstellen Sie einen Leitfaden für einige oder alle auf Ihrem System installierten Benchmarks.**

   ```
   # compliance guide -a
   ```

   Ein Leitfaden enthält die Begründung für die einzelnen Sicherheitsprüfungen sowie die zur Behebung einer nicht erfolgreichen Prüfung vorzunehmenden Schritte. Leitfäden können auch zu Schulungszwecken und als Richtlinien für zukünftige Tests dienen. Leitfäden für die

einzelnen Sicherheitsprofile werden standardmäßig bei der Installation erstellt. Wenn Sie eine Benchmark hinzufügen oder ändern, erstellen Sie vielleicht einen neuen Leitfaden.

Compliancereferenz

Der Compliancebereich der Rechnersicherheit setzt Vertrautheit im Umgang mit zahlreichen Standards, Akronymen und Prozessen voraus. Der Einfachheit halber wird Ihnen im Folgenden eine Liste mit Begriffen und Referenzen zur Verfügung gestellt.

In folgenden Programmen sind Funktionen zur Compliancebewertung und -berichterstattung implementiert:

- Security Content Automation Protocol (SCAP)
- SCAP-Tools (OpenSCAP)
- Open Vulnerability and Assessment Language (OVAL)
- eXtensible Configuration Checklist Description Format (XCCDF)

Folgende Gremien stellen Compliancestandards oder -gesetze bereit:

- Center for Internet Security (CIS)
- Federal Information Security Management Act (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry-Data Security Standard (PCI DSS)
- Sarbanes Oxley (SOX)