Guide de conformité à la sécurité d'Oracle® Solaris 11.2

Référence: E53933
Juillet 2014

ORACLE®

Table des matières

Utilisation de la présente documentation

- **Présentation** : description de l'évaluation et de la présentation sous forme d'état de la conformité d'un système Oracle Solaris aux tests d'évaluation de la sécurité spécifiés.
- **Public visé** : administrateurs et vérificateurs de la sécurité qui évaluent la sécurité sur les systèmes Oracle Solaris 11.
- **Connaissances requises** : exigences du site en matière de sécurité.

Bibliothèque de documentation produit

Les informations de dernière minute et les problèmes connus pour ce produit sont inclus dans la bibliothèque de documentation accessible à l'adresse : http://www.oracle.com/pls/topic/lookup?ctx=E56338.

Accès aux services de support Oracle

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs si vous êtes malentendant.

Commentaires

Faites part de vos commentaires sur cette documentation à la page suivante : http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPITRE 1

Communication de la conformité à des normes de sécurité

Ce chapitre décrit comment évaluer et générer des états sur la conformité d'un système Oracle Solaris à des normes de sécurité, également appelées *tests d'évaluation de la sécurité* et *stratégies de sécurité*. Ce chapitre comprend les sections suivantes :

A propos de la conformité

Les systèmes conformes à des normes de sécurité assurent des environnements informatiques plus sécurisés et sont plus faciles à tester, à entretenir et à protéger. Dans cette version, Oracle Solaris fournit des scripts qui évaluent et génèrent des états sur la conformité de votre système à deux tests d'évaluation de la sécurité : Solaris Security Benchmark et PCI DSS (Payment Card Industry-Data Security Standard).

La validation de la configuration pour assurer la conformité du système à des stratégies de sécurité externes et internes est essentielle. La gestion des exigences relatives à l'audit et à la conformité aux normes de sécurité constitue un poste de dépenses important dans le budget de sécurité informatique, et comprend notamment la documentation, les états et la validation elle-même. Des organisations telles que les banques, les hôpitaux et les administrations publiques ont des exigences de conformité spécifiques. Des auditeurs qui ne sont pas familiarisés avec un système d'exploitation peuvent peiner à mettre en relation les contrôles de sécurité et les exigences. C'est pourquoi des outils qui mettent en relation les contrôles de sécurité et les exigences peuvent être d'un secours précieux et permettre d'économiser temps et argent.

Les scripts de conformité sont basés sur le protocole SCAP (Security Content Automation Protocol) écrit en langage OVAL (Open Vulnerability and Assessment Language). La mise en oeuvre de SCAP dans Oracle Solaris prend également en charge des scripts conformes à SCE

(Script Check Engine). Ces scripts ajoutent des contrôles de sécurité que les schémas OVAL et les sondes ne fournissent pas. Il est possible d'utiliser des scripts supplémentaires pour satisfaire d'autres réglementations environnementales, telles que les lois Gramm-Leach-Bliley (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX), ainsi que Federal Information Security Management Act (FISMA). Pour des liens vers ces normes, reportez-vous à la section “Conformité (informations de référence)” à la page 14.

Tests d'évaluation de la sécurité d'Oracle Solaris

Oracle Solaris 11 fournit des scripts de conformité pour deux normes, Solaris et PCI DSS.

Test d'évaluation de la stratégie de sécurité d'Solaris

Le test d'évaluation de la stratégie de sécurité d'Solaris est une norme basée sur l'installation par défaut "secure by default" (SBD) d'Oracle Solaris. Le test d'évaluation prévoit deux profils, Baseline (de base) et Recommended (recommandé). Les profils sont décrits dans la section “Mesure de la conformité” à la page 9.

Les fonctions qui comprennent SBD sont décrites dans les sections “ Utilisation de la configuration Secure by Default ” du manuel “ Sécurisation des systèmes et des périphériques connectés dans Oracle Solaris 11.2 ” et “ Sécurité configurable d’Oracle Solaris ” du manuel “ Directives de sécurité d’Oracle Solaris 11 ”.

Ce test d'évaluation ne remplit pas les conditions des tests d'évaluation de PCI DSS, du CIS (Centre pour la Sécurité sur Internet) ni des guides DISA-STIG (Defense Information Systems Agency-Security Technical Information Guides) pour Oracle Solaris.

Test d'évaluation de la stratégie de sécurité de PCI DSS

Le test d'évaluation de la stratégie de sécurité PCI DSS est une norme de sécurité des informations destinée aux entreprises qui manipulent des informations relatives aux titulaires des principales cartes de débit et de crédit. La norme est définie par le Conseil des normes de sécurité PCI. L'objectif est de réduire les risques de fraude sur les cartes de crédit.

Un système Oracle Solaris nécessite d'être configuré pour être conforme à la norme PCI DSS. L'état sur la conformité donne le résultat des tests (échec / réussite) et indique comment remédier aux carences.

Mesure de la conformité

Pour mesurer la conformité à la sécurité, appelée *conformité* dans la suite de ce manuel, les éléments suivants sont nécessaires : un test d'évaluation de la sécurité ou profil, une mesure de la conformité à ce test d'évaluation, appelée *évaluation* et un état contenant le résultat de l'évaluation. Vous pouvez également imprimer l'état sous la forme d'un guide destiné à l'archivage ou à la formation.

Oracle Solaris fournit des scripts qui mesurent deux profils de sécurité dans le test d'évaluation d'Solaris.

- Le profil Baseline (de base) du test d'évaluation d'Solaris est très semblable à l'installation SBD par défaut d'Oracle Solaris.
- Le profil Recommended (recommandé) d'Solaris satisfait des exigences de sécurité plus élevées que le profil Baseline.

  Ces profils s'imbriquent. Les systèmes conformes au profil Recommended sont également conformes au profil Baseline.

Le test d'évaluation PCI DSS mesure la conformité de votre système à la norme PCI DSS. Les exigences PCI DSS ne disposant pas de liens directs au code, vous devez consulter l'état pour des informations sur la conformité. Pour plus d'informations, reportez-vous à la section Meeting PCI DSS Compliance with Oracle Solaris 11.

Package `compliance`

La fonctionnalité de conformité est disponible dans le package `pkg:/security/compliance`, qui est installé conjointement avec les groupes de packages `solaris-small-server` et `solaris-large-server`.

- Pour plus d'informations sur les groupes de packages, reportez-vous à la section “ Installation du SE OracleÂ Solaris ” du manuel “ Directives de sécurité d’Oracle Solaris 11 ”.
- Pour plus d'informations sur les packages, reportez-vous à “ Oracle Solaris 11.2 Package Group Lists ”.
- Pour afficher une description des packages de conformité, exécutez la commande `pkg info compliance`.

Evaluation de la conformité d'Oracle Solaris

La commande `compliance` sert à évaluer et à présenter sous forme d'états la conformité d'un système à un test d'évaluation connu. La commande de conformité d'Oracle Solaris mappe les

exigences d'un test d'évaluation sur le code, le fichier ou la sortie de commande qui vérifie la conformité à une exigence particulière. Pour plus d'informations sur cette commande, reportez-vous à la page de manuel `compliance`(1M).

Pour plus d'informations sur la prise en charge de l'ensemble d'outils SCAP qui prend en charge la commande `compliance`, reportez-vous à la page de manuel `oscap`(8). Pour afficher la version de l'ensemble d'outils SCAP, exécutez la commande `oscap -V`.

Remarque - L'ensemble d'outils SCAP n'est pas en mesure de localiser les états générés par la commande `oscap` ni les descriptions des tests (la localisation comprend la traduction du logiciel dans la langue locale).

Evaluation de la conformité à des tests tiers

L'organisation de normes tierces CIS fournit des outils de vérification de la conformité automatisés pour son test d'évaluation. Vous pouvez contacter CIS pour connaître le coût de l'utilisation de ces outils pour évaluer la conformité au test d'évaluation de CIS. Les outils CIS peuvent être utilisés sur un système Microsoft Windows pour vérifier la conformité d'Oracle Solaris.

Vérification de la conformité d'Oracle Solaris

La commande `compliance` automatise l'évaluation de la conformité, mais pas les mesures de correction. Cette commande permet de répertorier, de générer et de supprimer les évaluations et les états. Tous les utilisateurs peuvent accéder aux états sur la conformité. Des droits sont nécessaires pour assurer la gestion des évaluations et générer des états. Pour plus d'informations, reportez-vous à la page de manuel `compliance`(1M).

La commande `compliance`contrôle les fichiers locaux uniquement. Si votre système monte des systèmes de fichiers, vous devez tester séparément la conformité des clients et celle des serveurs. Par exemple, si vous montez les répertoires personnels des utilisateurs à partir de serveurs centrtaux, exécutez la commande `compliance` sur les systèmes des utilisateurs et sur chaque serveur qui exporte les répertoires personnels.

Droits d'exécution de la commande `compliance`

Oracle Solaris fournit deux profils de droits pour gérer l'évaluation de la conformité et la génération des états.

- Le profil de droits Compliance Assessor (évaluateur de la conformité) permet aux utilisateurs d'effectuer des évaluations, de les placer dans un magasin d'évaluations, de générer des états et de supprimer des évaluations du magasin.
- Le profil de droits Compliance Reporter (rapporteur de conformité) permet aux utilisateurs de générer de nouveaux états à partir d'évaluations existantes.

Les sous-commandes de conformité nécessitent les droits suivants :

- Commande `compliance assess` : requiert tous les privilèges et l'autorisation `solaris.compliance.assess`. Le profil de droits Compliance Assessor (évaluateur de la conformité) offre ces droits.
- Commande `compliance delete` : nécessite l'accès en écriture au magasin d'évaluations et l'autorisation `solaris.compliance.assess`. Le profil de droits Compliance Assessor (évaluateur de la conformité) offre ces droits.
- Commande `compliance list` : peut être exécutée par tout utilisateur disposant de droits élémentaires. Cette commande offre une visibilité totale sur les tests d'évaluation et les évaluations.
- Commande `compliance report` : peut être exécutée par n'importe quel utilisateur, mais l'étendue des fonctionnalités varie selon des droits de l'utilisateur. Les utilisateurs auxquels les profils Compliance Assessor ou Compliance Reporter sont affectés peuvent générer de nouveaux états dans le magasin d'évaluations. Tous les utilisateurs peuvent voir les états existants, mais les utilisateurs disposant uniquement de droits élémentaires ne peuvent pas générer d'états.

Création d'évaluations de la conformité et d'états sur la conformité

Les évaluations de la conformité sont complètes. Les états peuvent inclure tous les éléments de l'évaluation ou uniquement un sous-ensemble des informations qu'elle contient. Exécutez régulièrement des évaluations, par exemple en tant que travail `cron`, pour surveiller la conformité de votre système.

▼ Exécution d'états sur la conformité

Par défaut, les packages `solaris-small-server` et `solaris-large-server` incluent le package `compliance`. Les packages `solaris-desktop` et `solaris-minimal` n'incluent pas le package `compliance`.

Avant de commencer

Vous devez disposer du profil Software Installation (installation de logiciels) pour ajouter des packages au système. Vous devez disposer de droits d'administration pour la plupart des commandes de conformité, comme décrit à la section “Droits d'exécution de la commande `compliance`” à la page 10. Pour plus d'informations, reportez-vous à la section “ A l’aide de

vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

1. **Installez le package `compliance`.**

```
# pkg install compliance
```

Le message suivant indique que le package est installé :

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

Pour plus d'informations, reportez-vous à la page de manuel pkg(1).

Remarque - Installez le package dans chaque zone dans laquelle vous prévoyez d'exécuter des tests de compatibilité.

---

2. **Créez une évaluation.**

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

`-p` Indique le nom du profil. Le nom du profil distingue les majuscules et les minuscules.

`-a` Indique le nom du répertoire de l'évaluation. Le nom par défaut inclut un horodatage.

Par exemple, la commande suivante crée une évaluation à l'aide du profil Recommended.

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

La commande crée dans `/var/share/compliance/assessments` un répertoire nommé `recommended` qui contient l'évaluation dans trois fichiers : un fichier journal, un fichier XML et un fichier HTML.

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

Si vous exécutez à nouveau cette commande, les fichiers ne sont pas remplacés. Vous devez supprimer les fichiers avant de réutiliser un répertoire d'évaluation.

3. **(Facultatif) Créez un état personnalisé.**

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

Cette commande crée un état contenant des éléments ayant subi un échec et des éléments non sélectionnés au format HTML. L'état est exécuté par rapport à la dernière évaluation.

Vous pouvez exécuter des états personnalisés de façon répétée. Toutefois, vous ne pouvez exécuter les états complets, c'est-à-dire l'évaluation, qu'une seule fois dans le répertoire d'origine.

4. **Affichez l'état complet.**

   Vous pouvez visualiser le fichier journal dans un éditeur de texte, visualiser le fichier HTML dans un navigateur ou visualiser le fichier XML dans une visionneuse de XML.

   Par exemple, pour afficher l'état HTML personnalisé de l'étape qui précède, saisissez l'entrée suivante dans le navigateur :

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

5. **Corrigez tous les échecs dont la réussite est nécessaire pour votre stratégie de sécurité.**

   a. **Terminez la correction pour l'entrée qui a subi un échec.**

   b. **Si la correction inclut la réinitialisation du système, réinitialisez le système avant d'exécuter à nouveau l'évaluation.**

6. **(Facultatif) Exécutez la commande `compliance`en tant que tâche `cron`.**

   ```
   # cron -e
   ```

   Pour des évaluations de conformité quotidiennes à 2h30, `root` ajoute l'entrée suivante :

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

   Pour des évaluations de conformité hebdomadaires à 1h15 le dimanche, `root` ajoute l'entrée suivante :

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

   Pour des évaluations mensuelles le premier jour du mois à 4h00, `root` ajoute l'entrée suivante :

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

   Pour des évaluations le premier lundi du mois à 3h45, `root` ajoute l'entrée suivante :

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

7. **(Facultatif) Créez un guide pour tout ou partie des évaluations qui sont installées sur votre système.**

```
# compliance guide -a
```

Un guide comprend les raisons de chaque contrôle de sécurité et les étapes à suivre pour corriger une vérification ayant échoué. Les guides peuvent être utiles dans le cadre de formations et en guise d'instructions pour les tests ultérieurs. Par défaut, des guides sont créés pour chaque profil de sécurité lors de l'installation. Si vous ajoutez ou modifiez un test d'évaluation, vous pouvez créer un nouveau guide.

Conformité (informations de référence)

Dans le cadre de la sécurité informatique, le domaine de la conformité suppose la connaissance de nombreuses normes, acronymes et processus. Les listes et termes suivants pourront vous être utiles.

Les programmes suivants mettent en oeuvre l'évaluation de la conformité et la génération d'états :

- Le protocole SCAP (Security Content Automation Protocol)
- Les outils SCAP (OpenSCAP)
- Le langage OVAL (Open Vulnerability and Assessment Language)
- Le format XCCDF (eXtensible Configuration Checklist Description Format)

Les organismes suivants fournissent des normes de conformité ou des lois :

- Le Centre pour la sécurité sur Internet (CIS)
- La loi Federal Information Security Management Act (FISMA)
- La loi Gramm-Leach-Bliley Act (GLBA)
- La loi HIPAA (Health Insurance Portability and Accountability Act)
- La norme PCI DSS (Payment Card Industry-Data Security Standard)
- La loi Sarbanes Oxley (SOX)