Guía de cumplimiento de la seguridad de Oracle® Solaris 11.2

Referencia: E53934
Julio de 2014

ORACLE®

Contenido

Uso de esta documentación

- **Descripción general**: se describe cómo evaluar el cumplimiento de un sistema Oracle Solaris conforme a referencias de seguridad especificadas y cómo generar informes al respecto.
- **Destinatarios**: administradores de la seguridad y auditores responsables de evaluar la seguridad de los sistemas Oracle Solaris 11.
- **Conocimientos necesarios**: los requisitos de seguridad del sitio.

Biblioteca de documentación del producto

En la biblioteca de documentación, que se encuentra en http://www.oracle.com/pls/topic/lookup?ctx=E56339, se incluye información de última hora y problemas conocidos para este producto.

Acceso a My Oracle Support

Los clientes de Oracle disponen de asistencia a través de Internet en el portal My Oracle Support. Para obtener más información, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info o, si tiene alguna discapacidad auditiva, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs.

Comentarios

Envíenos comentarios acerca de esta documentación mediante http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CAPÍTULO 1

Generación de informes sobre el cumplimiento de los estándares de seguridad

En este capítulo, se describe cómo evaluar el cumplimiento de un sistema Oracle Solaris con los estándares de seguridad, también llamados *referencias de seguridad* o *políticas de seguridad*, y cómo generar informes al respecto. En este capítulo, se tratan los siguientes temas:

Acerca del cumplimiento

Los sistemas que cumplen con los estándares de seguridad ofrecen entornos informáticos más seguros y además son más fáciles de evaluar, mantener y proteger. En esta versión, Oracle Solaris proporciona secuencias de comandos que permiten evaluar e informar el cumplimiento de su sistema Oracle Solaris con dos referencias de seguridad: la referencia de seguridad Solaris (Solaris Security Benchmark) y el estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS, Payment Card Industry-Data Security Standard).

Es imprescindible validar la configuración para admitir el cumplimiento del sistema con las políticas de seguridad externas e internas. La gestión del cumplimiento de la seguridad y los requisitos de auditoría abarcan un gran porcentaje del gasto en seguridad informática, incluida la documentación, los informes y la validación en sí misma. Organizaciones como los bancos, los hospitales y los gobiernos tienen requisitos de cumplimiento especializados. Puede que a los auditores que no están familiarizados con un sistema operativo les resulte difícil cumplir con los requisitos y los controles de seguridad. Por lo tanto, las herramientas que asignan controles de seguridad a los requisitos permiten reducir los costos y el tiempo, ya que brindan asistencia a los auditores.

Las secuencias de comandos de cumplimiento se basan en el protocolo de automatización de contenidos de seguridad (SCAP, Security Content Automation Protocol) escrito en OVAL

(Open Vulnerability and Assessment Language, lenguaje abierto de vulnerabilidades y evaluación). La implementación de SCAP en Oracle Solaris también admite secuencias de comandos compatibles con SCE (Script Check Engine, motor de comprobación de secuencias de comandos). Estas secuencias de comandos permiten agregar comprobaciones de seguridad que los esquemas y sondeos actuales de OVAL no proporcionan. Se pueden utilizar secuencias de comandos adicionales para cumplir con otros estándares del entorno normativo, como GLBA (Ley Gramm-Leach-Bliley), HIPAA (Ley de Portabilidad y Contabilidad de los Seguros de Salud), SOX (Ley Sarbanes Oxley), y FISMA (Ley Federal de Gestión de Seguridad de la Información). Para obtener los enlaces con estos estándares, consulte “Referencia de cumplimiento” [14].

Referencias de seguridad de Oracle Solaris

Oracle Solaris 11 proporciona secuencias de comandos para el cumplimiento de dos estándares: Solaris y PCI DSS.

Referencia de política de seguridad Solaris

La referencia de política de seguridad Solaris es un estándar basado en la instalación predeterminada SBD (con "seguridad predeterminada") de Oracle Solaris. Esta referencia proporciona dos perfiles, el básico y el recomendado. Los perfiles se describen en “Medición de cumplimiento” [9].

Las funciones que comprenden SBD se describen en “Uso de la configuración de seguridad predeterminada” de “Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ” y “Seguridad configurable de Oracle Solaris” de “Directrices de seguridad de Oracle Solaris 11 ”.

Esta referencia no cumple los requisitos de las referencias de PCI DSS, CIS (Center for Internet Security, centro para la seguridad informática) o DISA-STIG (Defense Information Systems Agency-Security Technical Information Guides, guías de información técnica sobre seguridad del Departamento de Defensa de Sistemas Informáticos) para Oracle Solaris.

Referencia de política de seguridad PCI DSS

La referencia de política de seguridad PCI DSS es un estándar de seguridad de la información de propiedad exclusiva para organizaciones que gestionan información de los titulares de las principales tarjetas de crédito y de débito. El estándar es definido por el consejo de estándares de seguridad del sector de tarjetas de pago (Payment Card Industry Security Standards Council). Tiene por objetivo reducir el fraude mediante tarjetas de crédito.

El sistema Oracle Solaris requiere una configuración que cumpla con el estándar PCI DSS. El informe de cumplimiento indica cuáles pruebas se han superado y cuáles no, y proporciona los pasos para corregir los errores.

Medición de cumplimiento

Para medir el cumplimiento de la seguridad, en adelante denominado *cumplimiento*, se requiere un perfil o referencia de seguridad, una medición del cumplimiento de dicha referencia, denominada *evaluación* y un informe con los resultados. El informe también puede imprimirse en forma de guía, con fines de capacitación o archivado.

Oracle Solaris proporciona secuencias de comandos que miden dos perfiles de seguridad en la referencia Solaris.

- El perfil básico de la referencia Solaris se corresponde estrechamente con la instalación predeterminada SBD de Oracle Solaris.
- A diferencia del perfil básico, el perfil recomendado de Solaris atiende las necesidades de las organizaciones que tengan requisitos de seguridad más estrictos.

  El perfil recomendado incluye al otro. Es decir que los sistemas que cumplan con el perfil recomendado también cumplen con el perfil básico.

La referencia PCI DSS mide el cumplimiento del sistema con el estándar PCI DSS. Dado que los requisitos de PCI DSS no tienen enlaces de código directo, debe examinar el informe para garantizar el cumplimiento. Para obtener más información, consulte Meeting PCI DSS Compliance with Oracle Solaris 11.

Paquete `compliance`

La funcionalidad de cumplimiento está disponible en el paquete `pkg:/security/compliance`, que se instala con los grupos de paquetes `solaris-small-server` y `solaris-large-server`.

- Para obtener información sobre los grupos de paquetes, consulte “Instalación del SO Oracle Solaris” de “Directrices de seguridad de Oracle Solaris 11 ”.
- Para obtener información sobre los paquetes, consulte “Oracle Solaris 11.2 Package Group Lists ”.
- Para que se muestre una descripción de los paquetes de cumplimiento, ejecute el comando `pkg info compliance`.

Evaluación de cumplimiento de Oracle Solaris

El comando `compliance` se utiliza para evaluar e informar el cumplimiento de un sistema con una referencia conocida. El comando de cumplimiento de Oracle Solaris asigna los requisitos de

una referencia al código, el archivo o la salida del comando que verifica la compatibilidad con una requisito específico. Para obtener más información sobre este comando, consulte la página del comando man `compliance`(1M).

Para obtener información sobre el conjunto de herramientas de SCAP que admiten el comando `compliance`, consulte la página del comando man `oscap`(8). Para que se muestre la versión del conjunto de herramientas de SCAP, ejecute el comando `oscap -V`.

Nota - El conjunto de herramientas de SCAP no puede localizar los informes que produce el comando `oscap`, ni tampoco puede localizar las descripciones de las pruebas. (La localización implica traducir el software al idioma local).

Evaluación de cumplimiento de terceros

La organización de estándares de terceros CIS proporciona herramientas de comprobación automatizada de cumplimiento para su referencia. Puede ponerse en contacto con CIS para determinar el costo de utilizar estas herramientas para evaluar el cumplimiento de la referencia de CIS. Las herramientas de CIS se pueden utilizar en un sistema Microsoft Windows para comprobar el cumplimiento de Oracle Solaris.

Evaluación del cumplimiento de Oracle Solaris

El comando `compliance`automatiza la evaluación de cumplimiento, no la corrección de errores. El comando se utiliza para listar, generar y suprimir evaluaciones e informes. Cualquier usuario puede acceder a los informes de cumplimiento. Para gestionar las evaluaciones y generar informes se requieren derechos. Para obtener más información, consulte la página del comando man `compliance`(1M).

El comando `compliance` comprueba solamente los archivos locales. Si el sistema monta sistemas de archivos, debe probar por separado el cumplimiento de los clientes y los servidores. Por ejemplo, si monta los directorios principales de usuario desde los servidores centrales, ejecute el comando `compliance` en los sistemas de usuario y en cada servidor que exporte los directorios principales.

Derechos para ejecutar el comando `compliance`

Oracle Solaris proporciona dos perfiles de derechos para gestionar la evaluación de cumplimiento y la generación de informes.

- El perfil de derechos de asesor de cumplimiento permite a los usuarios realizar evaluaciones, colocarlas en el almacén de evaluaciones, generar informes y suprimir evaluaciones del almacén.
- El perfil de derechos de generador de informes de cumplimiento permite a los usuarios generar nuevos informes a partir de evaluaciones existentes.

Los subcomandos de cumplimiento requieren los siguientes derechos:

- Comando `compliance assess`: requiere todos los privilegios y la autorización `solaris.compliance.assess`. El perfil de derechos de asesor de cumplimiento proporciona estos derechos.
- Comando `compliance delete`: requiere el acceso de escritura en el almacén de evaluaciones y la autorización `solaris.compliance.assess`. El perfil de derechos de asesor de cumplimiento proporciona estos derechos.
- Comando `compliance list`: cualquiera que disponga de derechos básicos puede ejecutarlo. Este comando proporciona visibilidad completa tanto de las referencias como de las evaluaciones.
- Comando `compliance report`: puede ser ejecutado por cualquier usuario, pero la cantidad de funcionalidades varía de acuerdo a los derechos del usuario. Los usuarios que tienen asignado el perfil de asesor de cumplimiento o de generador de informes de cumplimiento pueden generar nuevos informes en el almacén de evaluaciones. Todos los usuarios pueden consultar los informes existentes, pero sólo los usuarios con derechos básicos no pueden generar informes.

Creación de informes y evaluaciones de cumplimiento

Las evaluaciones de cumplimiento son completas. Los informes pueden incluir todos los elementos de la evaluación o pueden incluir un subconjunto de la información de la evaluación. Ejecute las evaluaciones con regularidad (por ejemplo, mediante la tarea `cron`) para supervisar el cumplimiento de su sistema.

▼ Ejecución de informes de cumplimiento

De manera predeterminada, los paquetes `solaris-small-server` y `solaris-large-server` incluyen el paquete `compliance`. Los paquetes `solaris-desktop` y `solaris-minimal` no incluyen el paquete `compliance`.

Antes de empezar Debe tener asignado el perfil de derechos de instalación de software para agregar paquetes al sistema. Se debe tener asignados los derechos de administrador para ejecutar la mayoría de los comandos de cumplimiento, como se describe en “Derechos para ejecutar el comando `compliance`” [10]. Para obtener más información, consulte “Uso de sus derechos

administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Instale el paquete `compliance`.**

```
# pkg install compliance
```

El siguiente mensaje indica que el paquete está instalado:

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

Para obtener más información, consulte la página del comando man `pkg`(1).

Nota - Instale el paquete en cada zona en la que pretenda ejecutar pruebas de cumplimiento.

2. **Cree una evaluación.**

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

`-p` Indica el nombre del perfil. El nombre del perfil distingue entre mayúsculas y minúsculas.

`-a` Indica el nombre de directorio de la evaluación. El nombre predeterminado incluye un registro de hora.

Por ejemplo, el comando siguiente crea una evaluación con el perfil recomendado.

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

El comando crea un directorio en `/var/share/compliance/assessments` denominado `recommended` que contiene la evaluación en tres archivos: un archivo log, un archivo XML y un archivo HTML.

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

Si ejecuta este comando de nuevo, los archivos no se reemplazan. Debe eliminar los archivos antes de reutilizar un directorio de evaluación.

3. **(Opcional) Cree un informe personalizado.**

```
# compliance report -s -pass,fail,notselected
```

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

Este comando crea un informe que contiene los elementos en formato HTML que hayan fallado o que no se hayan seleccionado. El informe se ejecuta en relación con la evaluación más reciente.

Puede ejecutar informes personalizados de manera repetida. Sin embargo, puede ejecutar los informes completos, es decir, la evaluación, sólo una vez en el directorio original.

4. **Vea el informe completo.**

   Puede ver el archivo log en un editor de texto, ver el archivo HTML en un explorador o ver el archivo XML en un visor de XML.

   Por ejemplo, para ver el informe personalizado en HTML del paso anterior, escriba la siguiente entrada en el explorador:

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

5. **Corrija los fallos que la política de seguridad requiera para pasar la prueba.**

   a. **Complete la corrección de errores de la entrada que haya fallado.**

   b. **Si la corrección incluye reiniciar el sistema, reinicie el sistema antes de ejecutar la evaluación de nuevo.**

6. **(Opcional) Ejecute el comando `compliance` como una tarea `cron`.**

   ```
   # cron -e
   ```

   Para las evaluaciones de cumplimiento diarias que se ejecutan a las 2:30 a. m., `root` agrega la siguiente entrada:

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

   Para las evaluaciones de cumplimiento semanales que se ejecutan a la 1:15 a. m., `root` agrega la siguiente entrada:

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

   Para las evaluaciones mensuales que se ejecutan el primer día de cada mes a las 4:00 a. m., `root` agrega la siguiente entrada:

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

   Para las evaluaciones que se ejecutan el primer lunes de cada mes a las 3:45 a. m., `root` agrega la siguiente entrada:

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

7. **(Opcional) Cree una guía para algunas o todas las referencias que se instalan en el sistema.**

```
# compliance guide -a
```

Una guía contiene la lógica de cada comprobación de seguridad y los pasos que se deben seguir para corregir los errores de una comprobación. Las guías pueden ser útiles para llevar a cabo capacitaciones y como directrices para pruebas futuras. De manera predeterminada, en el momento de la instalación, se crean guías para cada perfil de seguridad. Si agrega o cambia una referencia, puede crear una nueva guía.

Referencia de cumplimiento

El área de cumplimiento de la seguridad informática supone que usted está familiarizado con muchos estándares, acrónimos y procesos. Las siguientes listas de términos y referencias se proporcionan para su comodidad.

Los siguientes programas implementan las evaluaciones de cumplimiento y la generación de informes:

- El protocolo de automatización de contenidos de seguridad (SCAP, Security Content Automation Protocol)
- Las herramientas de SCAP (OpenSCAP)
- El lenguaje abierto de vulnerabilidades y evaluación (OVAL, Open Vulnerability and Assessment Language)
- El formato de descripción de listas de comprobación de configuración ampliable (XCCDF, eXtensible Configuration Checklist Description Format)

Los siguientes organismos proporcionan leyes o estándares de cumplimiento:

- El centro de la seguridad informática (CIS, Center for Internet Security)
- La Ley Federal de Gestión de Seguridad de la Información (FISMA)
- La Ley Gramm-Leach-Bliley (GLBA)
- La Ley de Portabilidad y Contabilidad de los Seguros de Salud (HIPAA)
- El estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS, Payment Card Industry-Data Security Standard)
- Ley Sarbanes Oxley (SOX)