Guia de Segurança e Conformidade do Oracle® Solaris 11.2

Número do Item: E53937
Julho de 2014

ORACLE®

Conteúdo

Como usar esta documentação

- **Visão geral** – Descreve como avaliar e gerar relatórios de conformidade de um sistema Oracle Solaris em relação a benchmarks de segurança específicos.
- **Público-alvo** – Administradores de segurança e auditores que avaliam a segurança em sistemas Oracle Solaris 11.
- **Conhecimento necessário** – Requisitos de segurança da empresa.

Biblioteca de documentação do produto

Informações atualizadas e problemas conhecidos deste produto estão incluídos na biblioteca de documentação em http://www.oracle.com/pls/topic/lookup?ctx=E56346.

Acesso ao Oracle Support

Os clientes Oracle têm acesso ao suporte eletrônico por meio do My Oracle Support. Para obter informações, visite http://www.oracle.com/pls/topic/lookup?ctx=acc{ENT:#x0026}id=info ou visite http://www.oracle.com/pls/topic/lookup?ctx=acc{ENT:#x0026}id=trs se você é portador de deficiência auditiva.

Feedback

Forneça comentários sobre essa documentação em http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CAPÍTULO 1

Relatórios de Conformidade com os Padrões de Segurança

Este capítulo descreve como avaliar e gerar relatórios da conformidade de um sistema Oracle Solaris em relação a padrões de segurança, também conhecidos como *benchmarks de segurança* e *políticas de segurança*. Este capítulo aborda os seguintes tópicos:

Sobre conformidade

Sistemas que atendem aos padrões de segurança fornecem ambientes computacionais mais seguros, além de serem mais fáceis de testar, manter e proteger. Nesta versão, o Oracle Solaris fornece scripts que avaliam e geram relatórios da conformidade do seu sistema Oracle Solaris em relação a dois benchmarks de segurança, o Solaris Security Benchmark e o Payment Card Industry-Data Security Standard (PCI DSS).

A validação da configuração para manter o sistema em conformidade com as políticas de segurança externas e internas é de suma importância. A preocupação em atender aos padrões de segurança e os requisitos de auditoria explica grande parte do gasto de segurança com TI, incluindo documentação, relatórios e a própria validação em si. As organizações, como bancos, hospitais e órgãos governamentais, possuem requisitos de conformidade específicos. Os auditores não familiarizados com um sistema operacional podem ter dificuldades para alinhar os controles de segurança com os requisitos. Portanto, as ferramentas que alinham os controles de segurança com os requisitos podem reduzir tempo e custos ao auxiliarem os auditores.

Os scripts de conformidade são baseados no padrão SCAP (Security Content Automation Protocol) que utiliza a linguagem OVAL (Open Vulnerability and Assessment Language). A implementação do SCAP no Oracle Solaris também suporta scripts compatíveis com o SCE (Script Check Engine). Esses scripts adicionam verificações de segurança que não são fornecidas nos esquemas e investigações OVAL. Os scripts adicionais podem ser usados para

atender a outros padrões regulatórios de ambiente, como o GLBA (Gramm-Leach-Bliley Act), o HIPAA (Health Insurance Portability and Accountability Act), o SOX (Sarbanes Oxley) e o FISMA (Federal Information Security Management Act). Para acessar os links para esses padrões, consulte “Referência de conformidade” [13].

Benchmarks de segurança do Oracle Solaris

O Oracle Solaris 11 fornece scripts de conformidade com dois padrões, Solaris e PCI DSS.

Benchmark da política de segurança do Solaris

O benchmark da política de segurança do Solaris é um padrão baseado na instalação padrão “secure by default” (SBD) do Oracle Solaris. O benchmark apresenta dois perfis, Linha de Base e Recomendado. Os perfis são descritos em “Análise de conformidade” [8].

Os recursos contidos no SBD são descritos na seção “Using the Secure by Default Configuration” no “Securing Systems and Attached Devices in Oracle Solaris 11.2 ” e “Segurança configurável do Oracle Solaris” no “Diretrizes de Segurança do Oracle Solaris 11 ”.

Esse benchmark não satisfaz os requisitos do PCI DSS, do CIS (Center for Internet Security) ou o DISA-STIG (Defense Information Systems Agency-Security Technical Information Guides) para o Oracle Solaris.

Benchmark da Política de Segurança do PCI DSS

O benchmark da política de segurança do PCI DSS é um padrão de segurança de informações proprietárias para organizações que lidam com informações dos titulares de cartões de débito e crédito. O padrão é definido pelo Payment Card Industry Security Standards Council. A intenção é reduzir as fraudes em cartões de crédito.

Um sistema Oracle Solaris exige configuração para estar em conformidade com o padrão PCI DSS. O relatório de conformidade indica quais testes falharam e quais foram aprovados, além de fornecer etapas de correção.

Análise de conformidade

Para analisar a conformidade de segurança, denominada *conformidade*, é preciso um benchmark ou perfil de segurança, uma medida de conformidade em relação a esse benchmark, denominada *avaliação* e, em seguida, um relatório dos resultados. O relatório também pode ser impresso em forma de guia para fins de treinamento ou arquivamento.

O Oracle Solaris fornece scripts que analisam dois perfis de segurança no benchmark do Solaris.

- O perfil Baseline do benchmark do Solaris se aproxima muito da instalação padrão SBD do Oracle Solaris.
- O perfil Solaris Recommended oferece às organizações requisitos de segurança mais rígidos do que o perfil Baseline.

  Esses perfis podem ser combinados. Os sistemas compatíveis com o perfil Recommended também são compatíveis com o perfil Baseline.

O benchmark PCI DSS analisa a conformidade do seu sistema com o padrão PCI DSS. Como os requisitos do PCI DSS não têm links de código direto, você deve examinar o relatório quanto à conformidade. Para obter mais informações, consulte Meeting PCI DSS Compliance with Oracle Solaris 11.

Pacote `compliance`

A funcionalidade de conformidade está disponível no pacote `pkg:/security/compliance`, que é instalado com os grupos de pacotes `solaris-small-server` e `solaris-large-server`.

- Para obter informações sobre grupos de pacotes, consulte "Instalação do SO Oracle Solaris" no "Diretrizes de Segurança do Oracle Solaris 11 ".
- Para obter informações sobre pacotes, consulte "Oracle Solaris 11.2 Package Group Lists ".
- Para exibir uma descrição dos pacotes de conformidade, execute o comando `pkg info compliance`.

Avaliação de conformidade do Oracle Solaris

O comando `compliance` é usado para avaliar e gerar relatório da conformidade de um sistema com um benchmark conhecido. O comando de conformidade Oracle Solaris mapeia os requisitos de um benchmark em relação ao código, arquivo ou saída de comando que verifica a conformidade com um requisito específico. Para obter informações sobre esse comando, consulte a página man `compliance`(1M).

Para obter informações sobre o conjunto de ferramentas SCAP que suporta o comando `compliance`, consulte a página `oscap`(8). Para exibir a versão do conjunto de ferramentas SCAP, execute o comando `oscap -V`.

Observação - O conjunto de ferramentas SCAP não pode localizar os relatórios que o comando `oscap` produz, nem pode localizar as descrições de teste. (Localização envolve traduzir o software para o idioma local.)

Avaliação de conformidade de terceiros

A organização de padrões de terceiros CIS fornece ferramentas de verificação de conformidade automatizadas para seu benchmark. Você pode entrar em contato com a CIS para determinar o custo da utilização dessas ferramentas para avaliar a conformidade com o benchmark CIS. As ferramentas CIS podem ser usadas em um sistema Microsoft Windows para verificação da conformidade com o Oracle Solaris.

Avaliação da conformidade com o Oracle Solaris

O comando `compliance` automatiza a avaliação de conformidade, não uma solução. O comando é usado para listar, gerar e excluir avaliações e relatórios. Qualquer usuário pode acessar os relatórios de conformidade. Para gerenciar avaliações e gerar relatórios, é preciso ter direitos. Para obter mais informações, consulte a página man `compliance`(1M).

O comando `compliance` verifica somente os arquivos locais. Se seu sistema monta sistemas de arquivos, você deverá testar separadamente a conformidade dos clientes e dos servidores. Por exemplo, se você montar diretórios home de usuários com base em servidores centrais, execute o comando `compliance` nos sistemas do usuário e em cada servidor que exporta os diretórios home.

Direitos para executar o comando `compliance`

O Oracle Solaris fornece dois perfis de direito para lidar com avaliação de conformidade e geração de relatórios.

- O perfil de direitos Compliance Assessor permite que os usuários executem avaliações, coloquem-nas no armazenamento de avaliações, gerem relatórios e excluam avaliações com base no armazenamento.
- O perfil de direitos Compliance Reporter permite que os usuários gerem novos relatórios de avaliações existentes.

Os subcomandos de conformidade exigem os seguintes direitos:

- Comando `compliance assess` – Exige todos os privilégios e a autorização `solaris.compliance.assess`. O perfil de direitos Compliance Assessor fornece esses perfis.
- Comando `compliance delete` – Exige acesso de gravação para o armazenamento de avaliações e a autorização `solaris.compliance.assess`. O perfil de direitos Compliance Assessor fornece esses perfis.
- Comando `compliance list` – Pode ser executado por qualquer pessoa com direitos básicos. Esse comando fornece total visibilidade para os benchmarks e as avaliações.

- Comando `compliance report` – Pode ser executado por qualquer pessoa, mas a gama de funcionalidades varia de acordo com os direitos do usuário. Os usuários que recebem o perfil Compliance Assessor ou Compliance Reporter podem gerar novos relatórios no armazenamento de avaliações. Todos os usuários podem visualizar relatórios existentes, mas usuários com apenas direitos básicos não podem gerar relatórios.

Criação de avaliações e relatórios de conformidade

As avaliações de conformidade estão concluídas. Os relatórios podem incluir cada item na avaliação ou podem incluir um subconjunto das informações na avaliação. Execute avaliações com frequência, por exemplo, como um job `cron`, para monitorar a conformidade do seu sistema.

▼ Como executar relatórios de conformidade

Por padrão, os pacotes `solaris-small-server` e `solaris-large-server` incluem o pacote `compliance`. Os pacotes `solaris-desktop` e `solaris-minimal` não incluem o pacote `compliance`.

Antes de começar Você deve receber o perfil de direitos Software Installation para adicionar pacotes ao sistema. Você deve receber direitos administrativos para a maioria dos comandos de conformidade, conforme descrito em “Direitos para executar o comando `compliance`” [10]. Para obter mais informações, consulte “Using Your Assigned Administrative Rights” no “Securing Users and Processes in Oracle Solaris 11.2 ”.

1. **Instale o pacote `compliance`.**

```
# pkg install compliance
```

A seguinte mensagem indica que o pacote foi instalado:

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

Para obter mais informações, consulte a página man `pkg`(1).

Observação - Instale o pacote em todas as zonas onde você pretende executar testes de conformidade.

---

2. **Crie uma avaliação.**

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
```

```
solaris: Baseline, Recommended
Assessments:
 No assessments available
# compliance -p profile -a assessment-directory
```

`-p` Indica o nome do perfil. O nome do perfil diferencia maiúsculas de minúsculas.

`-a` Indica o nome do diretório da avaliação. O nome padrão inclui um carimbo de data/hora.

Por exemplo, o comando a seguir cria uma avaliação usando o perfil Recommended.

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

O comando cria um diretório em `/var/share/compliance/assessments` denominado `recommended` que contém a avaliação em três arquivos: um arquivo de log, um arquivo XML e um arquivo HTML.

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

Se você executar esse comando novamente, os arquivos não serão substituídos. Você deve remover os arquivos antes de reutilizar um diretório de avaliações.

3. (Opcional) Crie um relatório personalizado.

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

Esse comando cria um relatório que contém itens não selecionados ou com falha no formato HTML. O relatório é executado na avaliação mais recente.

É possível executar relatórios personalizados repetidamente. No entanto, você pode executar os relatórios completos, ou seja, a avaliação, apenas uma vez no diretório original.

4. Visualize o relatório completo.

É possível visualizar o arquivo de log em um editor de texto, visualizar o arquivo HTML em um navegador ou o arquivo XML em um visualizador XML.

Por exemplo, para visualizar o relatório HTML personalizado na etapa anterior, digite a seguinte entrada no navegador:

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

5. Corrija as falhas para que sua política de segurança possa avançar.

a. Conclua a correção para a entrada que apresentou a falha.

b. **Se a correção incluir a reinicialização do sistema, reinicialize o sistema antes de executar a avaliação novamente.**

6. **(Opcional) Execute o comando `compliance` como um job `cron`.**

```
# cron -e
```

Para avaliações diárias de conformidade às 2h30m, `root` adiciona a seguinte entrada:

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

Para avaliações semanais de conformidade aos domingos à 1h15m, `root` adiciona a seguinte entrada:

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

Para avaliações mensais no primeiro dia do mês às 4h, `root` adiciona a seguinte entrada:

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

Para avaliações na primeira segunda-feira do mês às 3h45m, `root` adiciona a seguinte entrada:

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

7. **(Opcional) Crie um guia para alguns ou todos os benchmarks instalados no seu sistema.**

```
# compliance guide -a
```

Um guia contém a lógica para cada verificação de segurança e as etapas para corrigir uma verificação com falha. Os guias podem ser úteis para treinamento e como diretrizes para testes futuros. Por padrão, os guias para cada perfil de segurança são criados na instalação. Se você adicionar ou alterar um benchmark, deverá criar um novo guia.

Referência de conformidade

A área de conformidade relativa à segurança do computador pressupõe familiaridade com muitos padrões, acrônimos e processos. As listas a seguir de termos e referências são fornecidas para sua conveniência.

Os seguintes programas implementam avaliações e geração de relatórios de conformidade:

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

Os seguintes órgãos fornecem padrões e leis de conformidade:

- 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)