Oracle® Solaris 11.2 安全遵从性指南

文件号码 E53940
2014 年 7 月

ORACLE

目录

使用此文档

- **概述** – 介绍如何评估和报告 Oracle Solaris 系统是否符合指定的安全基准。
- **目标读者** – 安全管理员以及在 Oracle Solaris 11 系统上评估安全的审计人员。
- **必备知识** – 站点安全要求。

产品文档库

位于 http://www.oracle.com/pls/topic/lookup?ctx=E56344 的文档库中包含此产品的最新信息和已知问题。

获得 Oracle 支持

Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

反馈

可以在 http://www.oracle.com/goto/docfeedback 上提供有关此文档的反馈。

♦ ♦ ♦ 第 1 章

1 报告安全标准遵从性

本章介绍如何评估和报告 Oracle Solaris 系统是否符合安全标准（也称为安全基准和安全策略）。本章包含以下主题：

关于遵从性

符合安全标准的系统不但能够提供更安全的计算环境，而且更易于测试、维护和保护。在此发行版中，Oracle Solaris 提供了用于评估和报告 Oracle Solaris 系统是否符合以下两项安全基准的脚本：Solaris 安全基准和支付卡行业数据安全标准 (PCI DSS)。

配置验证至关重要，它有助于系统符合内外部安全策略。处理安全遵从性和审计要求会涉及大量工作，包括文档编制、报告和自身验证，因此在 IT 安全开销中占很大一部分。诸如银行、医院和政府部门等组织都有专门的遵从性要求。如果对操作系统不熟悉，审计人员很难将各项安全控制措施与相关要求一一对应起来。因此，如果有工具能将安全控制措施映射到各项要求，它无疑能帮助审计人员，进而缩短时间并降低成本。

遵从性脚本基于安全内容自动化协议 (Security Content Automation Protocol, SCAP) 并用开放漏洞与评估语言 (Open Vulnerability and Assessment Language, OVAL) 编写。Oracle Solaris 中的 SCAP 实现还支持符合脚本检查引擎 (Script Check Engine, SCE) 的脚本。这些脚本增加了当前的 OVAL 架构和探测器无法提供的安全检查。此外，也可以使用其他脚本来满足其他监管环境标准，例如《格雷姆-里奇-比利雷法案》(Gramm-Leach-Bliley Act, GLBA)、《健康保险携带及责任法案》(Health Insurance Portability and Accountability Act, HIPAA)、《萨班斯-奥克斯利法案》(Sarbanes Oxley, SOX) 和《联邦信息安全管理法案》(Federal Information Security Management Act, FISMA)。有关这些标准的链接，请参见“遵从性参考资料” [12]。

Oracle Solaris 安全基准

Oracle Solaris 11 提供了适用于以下两项标准的遵从性脚本：Solaris 和 PCI DSS。

Solaris 安全策略基准

Solaris 安全策略基准是一项标准，基于 Oracle Solaris 的“缺省安全”(Secure by Default, SBD) 缺省安装。该基准提供了两个配置文件，即 "Baseline"（基线）和 "Recommended"（建议）。“遵从性评估” [8]中介绍了这两个配置文件。

《在 Oracle Solaris 11.2 中确保系统和连接设备的安全 》中的“使用缺省安全 (Secure by Default) 配置”和《Oracle Solaris 11 安全准则 》中的“Oracle Solaris 可配置的安全性”介绍了构成 SBD 的各项功能。

此基准无法满足 PCI DSS、Internet 安全中心 (Center for Internet Security, CIS) 或适用于 Oracle Solaris 的《美国国防信息系统局安全技术信息指南》(Defense Information Systems Agency-Security Technical Information Guides, DISA-STIG) 基准的要求。

PCI DSS 安全策略基准

PCI DSS 安全策略基准是一项专有信息安全标准，适用于处理主流借记卡和信用卡的持卡人信息的组织。该标准由支付卡行业安全标准委员会定义，目的在于减少信用卡欺诈。

Oracle Solaris 系统需要进行配置才能符合 PCI DSS 标准。遵从性报告会说明未通过和已通过的测试并提供补救步骤。

遵从性评估

要衡量安全遵从性（下称遵从性），应使用一个安全基准或配置文件来衡量系统是否符合该基准（此过程称为评估），然后生成包含评估结果的报告。此外还能以指南的形式打印出报告，用于培训或归档目的。

Oracle Solaris 提供了用于衡量 Solaris 基准中两个安全配置文件的脚本。

- Solaris 基准中的 "Baseline"（基线）配置文件与 Oracle Solaris 的缺省 SBD 安装十分匹配。
- 与 "Baseline"（基线）配置文件相比，Solaris "Recommended"（建议）配置文件可满足各组织更严格的安全要求。

  这两个配置文件嵌套在一起。符合 "Recommended"（建议）配置文件的系统也符合 "Baseline"（基线）配置文件的要求。

PCI DSS 基准可衡量系统是否符合 PCI DSS 标准。由于 PCI DSS 要求不具有直接代码链接，您必须检查遵从性报告。有关更多信息，请参见 Meeting PCI DSS Compliance with Oracle Solaris 11（借助 Oracle Solaris 11 实现 PCI DSS 遵从性）。

`compliance` 软件包

遵从性功能由 `pkg:/security/compliance` 软件包提供，该软件包随 `solaris-small-server` 和 `solaris-large-server` 软件包组一起安装。

- 有关软件包组的信息，请参见《Oracle Solaris 11 安全准则 》中的“安装 Oracle Solaris OS”。
- 有关软件包的信息，请参见《Oracle Solaris 11.2 Package Group Lists 》。
- 要显示 compliance 软件包的说明，请发出 `pkg info compliance` 命令。

Oracle Solaris 遵从性评估

`compliance` 命令用于评估和报告系统是否符合某项已知基准。Oracle Solaris compliance 命令可将基准的各项要求映射到代码、文件或命令输出，然后由后者验证是否符合特定要求。有关此命令的信息，请参见 `compliance(1M)` 手册页。

有关支持 `compliance` 命令的 SCAP 工具集的信息，请参见 `oscap`(8) 手册页。要显示 SCAP 工具集的版本，请发出 `oscap -V` 命令。

注 - SCAP 工具集既无法将 `oscap` 命令生成的报告本地化，也无法将测试说明本地化。（本地化涉及将软件翻译成本地语言。）

第三方遵从性评估

CIS 第三方标准组织为其基准提供了自动化遵从性检查工具。要确定使用这些工具评估 CIS 基准遵从性的成本，请与 CIS 联系。可以在 Microsoft Windows 系统上使用 CIS 工具检查 Oracle Solaris 遵从性。

评估 Oracle Solaris 遵从性

通过 `compliance` 命令，可自动执行遵从性评估，但无法自动执行补救步骤。该命令用于列出、生成和删除评估与报告。任何用户都可以访问遵从性报告。管理评估并生成报告时需要具备相应权限。有关更多信息，请参见 `compliance(1M)` 手册页。

compliance 命令仅能检查本地文件。如果系统挂载了文件系统，则必须分别测试客户机和服务器的遵从性。例如，如果挂载了中央服务器中的用户起始目录，请在用户系统上以及导出该起始目录的每个服务器上运行 compliance 命令。

运行 compliance 命令所需的权限

Oracle Solaris 提供了两个权限配置文件用于处理遵从性评估和报告生成操作。

- "Compliance Assessor"（遵从性评估者）权限配置文件可让用户执行评估、将评估放在评估存储中、生成报告以及从存储中删除评估。
- "Compliance Reporter"（遵从性报告者）权限配置文件可让用户从现有评估生成新报告。

compliance 命令的子命令需要以下权限：

- compliance assess 命令 – 需要所有特权以及 solaris.compliance.assess 授权。"Compliance Assessor"（遵从性评估者）权限配置文件提供了这些权限。
- compliance delete 命令 – 需要对评估存储的写访问权限以及 solaris.compliance.assess 授权。"Compliance Assessor"（遵从性评估者）权限配置文件提供了这些权限。
- compliance list 命令 – 任何拥有基本权限的用户都可以运行此命令。此命令提供对基准和评估的完全可见性。
- compliance report 命令 – 任何用户都可以运行此命令，但其功能范围因用户权限而异。分配了 "Compliance Assessor"（遵从性评估者）或 "Compliance Reporter"（遵从性报告者）配置文件的用户可以在评估存储中生成新报告。所有用户都可以查看现有报告，但仅拥有基本权限的用户无法生成报告。

创建遵从性评估和报告

遵从性评估现已完成。报告可以包含评估中的每一项，也可以包含评估中的信息子集。请定期运行评估（例如以 cron 作业的形式运行）以监视系统的遵从性。

▼ 如何运行遵从性报告

缺省情况下，solaris-small-server 和 solaris-large-server 软件包含有 compliance 软件包。solaris-desktop 和 solaris-minimal 软件包不含 compliance 软件包。

开始之前 您必须分配有 "Software Installation"（软件安装）权限配置文件才能向系统添加软件包。您必须分配有大多数 compliance 命令的管理权限，如“运行 compliance 命令所需的权限” [10]中所述。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

1. **安装 compliance 软件包。**

```
# pkg install compliance
```

以下消息指示软件包已安装：

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

有关更多信息，请参见 pkg(1) 手册页。

注 - 在计划运行遵从性测试的每个区域中安装该软件包。

---

2. 创建评估。

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

-p 指示配置文件的名称。配置文件名称区分大小写。

-a 指示评估的目录名称。缺省名称包含时间戳。

例如，以下命令将使用 "Recommended"（建议）配置文件创建评估。

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

该命令会在 /var/share/compliance/assessments 中创建名为 recommended 的目录，而且目录中含有三个评估文件，分别是一个日志文件、一个 XML 文件和一个 HTML 文件。

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

再次运行此命令时，这些文件不会被替换。必须先删除文件，然后才能重复使用评估目录。

3. （可选） 创建定制报告。

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

此命令会以 HTML 格式创建包含未通过项和未选定项的报告。该报告针对最近的评估运行。

可以重复运行定制报告。但是，只能在原始目录中运行完整报告（即评估）一次。

4. 查看完整报告。

可以在文本编辑器中查看日志文件，在浏览器中查看 HTML 文件，或者在 XML 查看器中查看 XML 文件。

例如，要查看先前步骤所生成的 HTML 报告，请键入以下浏览器条目：

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

5. 修复安全策略要求必须通过的未通过项。

   a. 完成对未通过项的修复。

   b. 如果修复步骤包括重新引导系统，请先重新引导系统，然后再次运行评估。

6. （可选） 以 **cron** 作业的形式运行 **compliance** 命令。

   ```
   # cron -e
   ```

   对于在凌晨 2:30 运行的每日遵从性评估，root 将添加以下条目：

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

   对于在星期日凌晨 1:15 运行的每周遵从性评估，root 将添加以下条目：

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

   对于在每个月第一天凌晨 4:00 运行的每月评估，root 将添加以下条目：

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

   对于在每个月第一个星期一凌晨 3:45 运行的评估，root 将添加以下条目：

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

7. （可选） 针对系统上安装的部分或全部基准创建指南。

   ```
   # compliance guide -a
   ```

   该指南将包含每个安全检查的基本原理以及未通过的检查的修复步骤。这些指南可用于培训目的，也可用作日后测试的准则。缺省情况下，安装时会为每个安全配置文件创建指南。如果添加或更改了基准，您可以创建新指南。

遵从性参考资料

计算机安全的遵从性领域假定用户熟悉许多标准、首字母缩略词和过程。以下是为方便用户而提供的术语和参考资料列表。

以下程序可实施遵从性评估和报告：

- 安全内容自动化协议 (Security Content Automation Protocol, SCAP)

- SCAP 工具 (OpenSCAP)
- 开放漏洞与评估语言 (Open Vulnerability and Assessment Language, OVAL)
- 可扩展配置核对表描述格式 (eXtensible Configuration Checklist Description Format, XCCDF)

以下机构提供了遵从性标准或法规：

- Internet 安全中心 (Center for Internet Security, CIS)
- 《联邦信息安全管理法案》(Federal Information Security Management Act, FISMA)
- 《格雷姆-里奇-比利雷法案》(Gramm-Leach-Bliley Act, GLBA)
- 《健康保险携带及责任法案》(Health Insurance Portability and Accountability Act, HIPAA)
- 支付卡行业数据安全标准 (Payment Card Industry-Data Security Standard, PCI DSS)
- 《萨班斯-奥克斯利法案》(Sarbanes Oxley, SOX)