HP Storage Operations Manager

软件版本:10.10
Windows® 和 Linux® 操作系统

强化指南

文档发布日期:2016 年 1 月
软件发布日期:2016 年 1 月

法律声明

担保

HP产品和服务的唯一担保已在此类产品和服务随附的明示担保声明中提出。此处的任何内容均不构成额外担保。HP不会为此处出现的技术或编辑错误或遗漏承担任何责任。

此处所含信息如有更改，恕不另行通知。

受限权利声明

机密计算机软件。必须拥有HP授予的有效许可证，方可拥有、使用或复制本软件。按照FAR 12.211和12.212，并根据供应商的标准商业许可的规定，商业计算机软件、计算机软件文档与商品技术数据授权给美国政府使用。

版权声明

商标声明

Adobe® 是 Adobe Systems Incorporated 的商标。

AMD 是 Advanced Micro Devices, Inc. 的商标。

 Google™ 是 Google Inc. 的商标。

Intel®、Intel® Itanium® 和 Intel® Xeon® 是 Intel Corporation 在美国和其他国家/地区的商标。

Linux® 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Microsoft®、Windows® 和 Windows Server® 是 Microsoft Corporation 在美国的注册商标。

Oracle 和 Java 是 Oracle 和/或其子公司的注册商标。

Red Hat® 是 Red Hat, Inc. 在美国和其他国家/地区的注册商标。

SAP®、SAP® BusinessObjects™ 和 SAP® BusinessObjects™ Web Intelligence® 是 SAP SE 在德国和其他国家/地区的商标或注册商标。

UNIX® 是 The Open Group 的注册商标。

Oracle 技术 — 受限权利声明

根据 DOD FAR Supplement 提供的程序是“商业计算机软件”，这些程序 (包括文档) 的使用、复制和披露将受限于适用的 Oracle 许可协议中规定的许可限制。否则，根据 Federal Acquisition Regulations 提供的程序是“受限制的计算机软件”，这些程序 (包括文档) 的使用、复制和披露应受限于“FAR 52.227-19, 商业计算机软件 - 限制权利 (1987 年 6 月)”中的限制。Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

有关完整的 Oracle 许可证文本，请参阅 SOM 产品下载文件的 `license-agreements` 目录中的 `open_source_third_party_license_agreements.pdf` 文件。

致谢

产品包括 Apache Software Foundation 开发的软件。
(http://www.apache.org)

产品包括由 Indiana University Extreme!Lab 开发的软件。
(http://www.extreme.indiana.edu)

此产品使用 j-Interop 库与 COM 服务器进行交互操作。
(http://www.j-interop.org)

文档更新

此文档的标题页包含以下标识信息:

- 软件版本号，用于指示软件版本。
- 文档发布日期，该日期将在每次更新文档时更改。
- 软件发布日期，用于指示该版本软件的发布日期。

要检查是否有最新的更新，或者验证是否正在使用最新版本的文档，请访问:

https://softwaresupport.hp.com

需要注册 HP Passport 才能登录此站点。要注册 HP Passport ID，请访问:

https://hpp12.passport.hp.com/hppcf/createuser.do

或单击 HP 软件支持页面顶部的 **Register** 链接。

此外，如果订阅了相应的产品支持服务，则还会收到更新的版本或新版本。有关详细信息，请与您的 HP 销售代表联系。

支持

请访问 HP 软件联机支持网站:**https://softwaresupport.hp.com**

此网站提供了联系信息，以及有关 HP 软件提供的产品、服务和支持的详细信息。

HP 软件联机支持提供客户自助解决功能。通过该联机支持，可快速高效地访问用于管理业务的各种交互式技术支持工具。作为尊贵的支持客户，您可以通过该支持网站获得下列支持:

- 搜索感兴趣的知识文档
- 提交并跟踪支持案例和改进请求
- 下载软件修补程序
- 管理支持合同
- 查找 HP 支持联系人
- 查看有关可用服务的信息
- 参与其他软件客户的讨论
- 研究和注册软件培训

大多数提供支持的区域都要求您注册为 HP Passport 用户再登录，很多区域还要求用户提供支持合同。要注册 HP Passport ID，请访问:

https://hpp12.passport.hp.com/hppcf/createuser.do

要查找有关访问级别的详细信息，请访问:

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now 可访问 HPSW 解决方案和集成门户网站。此网站将帮助您寻找可满足您业务需求的 HP 产品解决方案，包括 HP 产品之间的集成的完整列表以及 ITIL 流程的列表。此网站的 URL 为 **http://h20230.www2.hp.com/sc/solutions/index.jsp**

目录

目录 4
使用本指南 5
通信配置 6
配置 TLS 协议 6
禁用非 SSL 通信 7
加密 8
用户身份验证 9
点击劫持保护 11
加强安全 12
配置 SOM Web 服务器使用的密码 12
限制用户对 SOM Web 服务器的访问 14
禁用 JMX 控制台 14
启动、停止或重新启动所有 SOM 服务 16
我们感谢您提出宝贵的意见! 18

使用本指南

本文档提供用于增强 SOM 安装安全性的信息。本文档中的信息适用于 SOM 10.10。有关该产品其他版本的安全配置，请参阅该版本的相应文档。

除非在过程中另有指定，否则本文档中内容的预期使用模式如下:

1. 停止所有 SOM 服务 (请参阅启动、停止或重新启动所有 SOM 服务 (第 16 页))。
2. 按本文档中所述应用所需的配置。

   备注: 请记住，进行任何更改之前，请将每个配置文件备份到 SOM 目录结构以外的位置。

3. 启动所有 SOM 服务 (请参阅启动、停止或重新启动所有 SOM 服务 (第 16 页))。

通信配置

此主题描述了 SOM 中用于通信的默认安全配置。

- 默认情况下，SOM 可以使用 HTTP 和 HTTPS 与 Web 浏览器通信。

  备注: 建议按禁用非 SSL 通信 (第 7 页)中所述禁用 HTTP 通信。

- 与 SOM Web 服务器进行 HTTPS 通信所用的默认 SSL 协议是 SSLv2Hello、TLSv1.0、TSLv1.1 和 TLSv1.2。

  备注: 建议禁用 TLSv1.0 和 TLSv1.1，除非与不支持 TLSv1.2 的应用程序通信时需要这些协议。有关说明，请参阅配置 TLS 协议 (第 6 页)。

配置 TLS 协议

默认情况下，SOM 支持以下协议:

- SSLv2Hello
- TLSv1.0
- TLSv1.1
- TLSv1.2

建议禁用 TLSv1.0 和 TLSv1.1，除非与不支持 TLSv1.2 的应用程序通信时需要这些协议。

将这些协议配置为使用以下文件中的 `com.hp.ov.nms.ssl.PROTOCOLS` 参数:

- *Windows*:

  ```
  %OvDataDir%\nmsas\nnm\server.properties
  ```

- *Linux*:

  ```
  /var/opt/OV/nmsas/nnm/server.properties
  ```

禁用非 SSL 通信

默认情况下，SOM 支持同时使用 HTTP 和 HTTPS 与 Web 浏览器通信。

要禁用 HTTP 通信，请在以下文件中将 `com.hp.ov.nms.ui.https.only` 参数设置为 true:

- *Windows*:

  ```
  %OvDataDir%\shared\nnm\conf\props\nms-ui.properties
  ```

- *Linux*:

  ```
  /var/opt/OV/shared/nnm/conf/props/nms-ui.properties
  ```

例如：

```
com.hp.ov.nms.ui.https.only = true
```

加密

此主题描述了 SOM 中用于加密和哈希的默认安全配置。

- 在安装期间，SOM 使用 2048 位加密密钥、SHA1 和 RSA 生成自签名证书。

  备注: HP 建议使用 CA 签名证书，而不是由 SOM 提供的自签名证书。

- 对于 SOM 中的本地身份验证，SOM 使用加盐 SHA-256 密码哈希来存储 SOM 用户密码。
- 对于 SOM 数据库中所存储设备密码的加密，SOM 使用 AES 128 算法。

用户身份验证

用户可以使用本地用户帐户或多个外部身份验证组件之一在 SOM 控制台中进行身份验证。每种方法都要求进行管理设置。

本地用户帐户

本地用户帐户仅特定于 SOM 安装。SOM 不支持对本地用户帐户进行密码策略配置。

备注: 如果您环境的安全标准需要特定的密码策略 (例如，最小密码长度或密码到期)，则建议使用外部机制进行用户身份验证。请参阅外部身份验证 (第 9 页)。

有关创建本地 SOM 用户帐户的信息，请参阅 SOM 帮助中的“配置用户帐户”。

外部身份验证

外部身份验证组件的管理员确定使用该组件的所有用户和所有应用程序的安全行为。

SOM 支持以下外部身份验证方法:

- 与目录服务集成。有关信息，请参阅《SOM 部署指南》中的“基于 LDAP 的身份验证”。
- PKI 用户身份验证，其中包括对智能卡 (如通用访问卡 (CAC)) 的支持。有关信息，请参阅《SOM 部署指南》中的“将 SOM 配置为支持公钥基础结构用户身份验证”。

SOM 控制台会话超时

默认情况下，SOM 控制台会话超时为 18 小时。SOM 管理员可以在“用户界面配置”表单 (“配置”>“用户界面”>“用户界面配置”) 上的“控制台超时”字段中为所有 SOM 控制台 用户更改此值。

备注: 建议根据您环境的策略配置会话超时。

点击劫持保护

SOM 进行了如下配置: 当链接与 SOM 管理服务器来自 SAMEORIGIN 时，在新框架中打开链接的页面。此配置无法更改。

加强安全

您可以通过应用以下任意或全部更改来加强 SOM 的安全:

- 配置 SOM Web 服务器使用的密码 (第 12 页)
- 限制用户对 SOM Web 服务器的访问 (第 14 页)
- 禁用 JMX 控制台 (第 14 页)

配置 SOM Web 服务器使用的密码

SOM 支持使用以下密码与 SOM Web 服务器进行安全通信:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

要更改 SOM 可以使用的协议列表，请取消以下文件中的 com.hp.ov.nms.ssl.CIPHERS 参数的注释并配置该参数:

- *Windows*:

  %OvDataDir%\shared\nnm\conf\props\nms-jboss.properties

- *Linux*:

  /var/opt/OV/shared/nnm/conf/props/nms-jboss.properties

此参数包含一个或多个密码的有序列表。如果 SOM 无法使用列表中的第一个密码建立 SOM Web 服务器与用户的 Web 浏览器之间的连接，SOM 会尝试使用下一个密码，以此类推。(上述列表显示默认密码排序。)

您可以编辑 com.hp.ov.nms.ssl.CIPHERS 参数的值，删除 SOM 不应使用的密码并更改 SOM 尝试使用可用密码的顺序。

如果更改支持的密码列表，HP 建议按强度顺序对密码列表进行排序。即，将 256 位加密置于 128 位加密之上。

HP 建议更改密码列表的顺序，将 256 位加密置于 128 位加密之上并按如下方式删除最弱的加密算法:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256

例如:

```
com.hp.ov.nms.ssl.CIPHERS=TLS_ECDHE_RSA_WITH_AES_128_CBC_
SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_
CBC_SHA256
```

备注:

- com.hp.ov.nms.ssl.CIPHERS 参数的值必须是不包含空格且为一个连续行的逗号分隔列表。
- 在更改之前保存密码列表。从 com.hp.ov.nms.ssl.CIPHERS 列表中删除密码可能会阻止 SOM 启动。
- Web 浏览器必须至少支持一个配置的密码。

限制用户对 SOM Web 服务器的访问

建议将 SOM Web 服务器的流量限制为仅具有访问权限的用户。限制此流量的可能方式包括:

- 在 SOM 管理服务器前面配置防火墙。

  有关 SOM 使用的端口的信息，请参阅《SOM 部署指南》中的"端口和防火墙"。

- 仅隔离用户通过特定网络接口对 SOM 管理服务器进行的访问。

禁用 JMX 控制台

在进行疑难解答之前，建议禁用 JMX 控制台。

要禁止访问 JMX 控制台，请添加以下内容：

```
<!-- disable the jmx-console -->
<realm name="jmx-console">
    <mode>NO_ACCESS</mode>
</realm>
```

在以下文件的 realms 块内：

- *Windows*:

  ```
  %OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml
  ```

- *Linux*:

  ```
  /var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml
  ```

例如：

```
<!-- realms describes the configuration of specific
services or applications -->
<realms>
    <!-- valid modes are X509 or FORM -->
    <realm name="console">
        <mode>FORM</mode>
    </realm>
    <!-- disable the jmx-console -->
    <realm name="jmx-console">
        <mode>NO_ACCESS</mode>
    </realm>
</realms>
```

然后，运行以下命令重新读取 nms-auth-config.xml 文件：

```
somsecurity.ovpl -reloadAuthConfig
```

要重新启用 JMX 控制台进行疑难解答，请注释掉前面的配置，然后重新运行 reload 命令。

启动、停止或重新启动所有 SOM 服务

先停止 SOM 服务，再更改 SOM 配置，可以避免在 SOM 数据库中存储冲突的数据。某些步骤需要重新启动 SOM 服务才能读取更新的配置。

启动所有 SOM 服务

- *Windows*:执行以下某个操作:
  - 从 Windows“开始”菜单，运行“所有程序”>“HP”>“Storage Operations Manager”>“ovstart”。
  - 运行以下命令:

    ```
    %OvInstallDir%\bin\ovstart
    ```
- *Linux*:运行以下命令:

  ```
  /opt/OV/bin/ovstart
  ```

停止所有 SOM 服务

- *Windows*:执行以下某个操作:
  - 从 Windows“开始”菜单，运行“所有程序”>“HP”>“Storage Operations Manager”>“ovstop”。
  - 运行以下命令:

    ```
    %OvInstallDir%\bin\ovstop
    ```
- *Linux*:运行以下命令:

  ```
  /opt/OV/bin/ovstop
  ```

重新启动所有 SOM 服务

- *Windows*:执行以下某个操作:
  - 从 Windows“开始”菜单，运行“所有程序”>“HP”>“Storage Operations Manager”>“ovstop”，然后运行“所有程序”>“HP”>“Storage Operations Manager”>“ovstart”。
  - 运行以下命令:

    ```
    %%OvInstallDir%\bin\ovstop

    %OvInstallDir%\bin\ovstart
    ```

- *Linux*:运行以下命令:

  ```
  /opt/OV/bin/ovstop

  /opt/OV/bin/ovstart
  ```

我们感谢您提出宝贵的意见!

如果您对本文档有任何意见，可以通过电子邮件与文档团队联系。如果在此系统上配置了电子邮件客户端，请单击以上链接，此时将打开一个电子邮件窗口，主题行中为以下信息:

强化指南反馈，2016 年 1 月 (Storage Operations Manager 10.10)

只需在电子邮件中添加反馈并单击“发送”即可。

如果没有可用的电子邮件客户端，请将以上信息复制到 Web 邮件客户端的新邮件中，然后将您的反馈发送至 storage-management-doc-feedback@hpe.com 。