HP Storage Operations Manager

软件版本: 10.00
Windows® 和 Linux® 操作系统

部署指南

文档发布日期:2015 年 3 月
软件发布日期:2015 年 3 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。

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。

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

第 1 章: 关于本指南

本指南包含用于管理 SOM 的信息和最佳实践的集合。本指南适用于拥有部署和管理 SOM 安装经验的专家级系统管理员或 HP 支持工程师。开始安装 SOM 前，请先阅读本指南。

注意: 本文档将在有新信息可用时更新。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/group/softwaresupport

有关详细信息，请参阅文档更新 (第 3 页)。

第 2 章: 计划 SOM 部署

计划部署活动对于确保 SOM 服务器能有效管理存储环境至关重要。请使用以下准则计划在您的环境中成功部署 SOM:

- **调整 SOM 和 SHR 服务器大小**
  要管理的环境的大小决定了应如何对服务器进行大小调整和配置。要确定适合您环境的 SOM 服务器配置，请参阅《SOM Support Matrix》中的“Performance and Sizing for the SOM Management Server”。
- **收集系统先决条件**
  确保满足所有系统先决条件后，再尝试安装 SOM。不满足系统要求可能导致安装失败。有关安装先决条件的信息，请参阅《SOM 交互式安装指南》中的“计划安装”。
- **检查防火墙端口配置**
  SOM 服务器使用不同端口与被管环境、浏览器客户端和 SHR 报告服务器通信。端口配置很大程度上由被管设备的代理配置决定。确保已在防火墙配置中启用所需配置，然后再开始产品安装。这样可以避免在部署产品后延迟发现被管环境。有关端口配置详细信息，请参阅端口和防火墙 (第 30 页)。
- **计划租户**
  如果计划在环境中使用多个租户，则先配置租户，再开始发现环境是一个很好的做法。您可以将租户关联到发现地址。通过此发现地址发现的元素将自动与已配置的租户关联。与发现后将元素移动到租户相比，先配置租户再执行发现更简单。有关计划租户的信息，请参阅关于计划租户的建议 (第 49 页)。
- **计划节点组**
  在 SOM 中，许多管理基元 (如数据采集和监视策略) 并非应用到各个元素，而是应用到分组的元素。这意味着可以提前创建组定义，然后发现过程将按照定义将元素分布到不同的组。有关创建节点组的信息，请参阅关于计划节点组的建议 (第 36 页)。
- **确定数据采集策略**
  数据采集策略可以在发现环境前预定义并应用到节点组。发现元素后，将如“计划节点组”中所述，将它们分类为不同的组，然后对这些组应用相应策略。例如，如果遵循将所有 Windows 主机命名为 'win*' 的约定，则可根据该约定创建组定义，并根据需要应用包含自定义新鲜度的数据采集策略。这是一个一次性定义，数据采集策略已涵盖此后发现的 Windows 主机，无需额外的管理开销。

  另外，您可能需要设置环境中要采集的元素的数据级别。默认情况下，系统配置为不采集环境中所有设备上的所有数据。如果要采集一组设备的更深入的数据，可以使用数据采集控制功能进行配置。通过提前计划，可以避免额外的数据采集周期以获取更多数据。

  有关数据采集策略最佳实践的信息，请参阅关于数据采集策略的建议 (第 41 页)
- **配置性能监视**
  一般来说，需要等待环境中所有 (或大多数) 设备的数据采集完成一次，再配置监视策略。您可以参考采集状态仪表板来监视正在运行的采集数。在大型环境中，配置监视策略可与数据采集过程重叠，这可能导致缺少统计信息。有关创建监视策略最佳实践的信息，请参阅关于监视性能的建议 (第 41 页)。
- **决定主机发现策略 - 基于规则的推断/无代理/代理**
  需要小心计划主机发现，因为它们会依据发现的元素数量添加最大的批量。SOM 使用以下机制发现环境中的主机:
  a. 基于规则的推断 - 使用环境中的配置 (如区域、区域别名和主机安全组) 了解存储在各个主机上的分布。
  b. 主机的无代理发现 - 通过使用 WMI、SSH 或本机 API (例如 VMWare) 等机制发现主机，而无需在主机上部署代理。
  c. 通过在主机上部署代理发现 - 在主机上部署代理来发现主机。

  通常，代理部署会产生管理开销。同时，代理提供最大深度的主机信息。

要减少此管理开销，可以将上面列出的方法组合使用。发现交换机 (构造) 和存储系统后，可立即在环境中配置基于规则的推断。使用显示的存储视图和报告了解环境中的存储分布。了解环境中存储的分布后，您将能识别环境中存储量消耗靠前的主机，然后决定使用无代理机制还是基于代理的机制发现这些主机供将来分析之用。

选择无代理发现还是基于代理的发现取决于您需要的主机信息的深度。

有关主机发现的详细信息，请参阅主机发现 (第 37 页)。

- **配置 SOM 报告服务器**
  Service Health Reporter (SHR) 是 SOM 的报告引擎，需要安装在单独的服务器上。确保用于在 SOM 和 SHR 之间进行通信的端口可用。有关所需端口的信息，请参阅端口和防火墙 (第 30 页)。

  有关调整 SHR 服务器大小以适合您的环境的信息，请参阅《SOM Support Matrix》中的“Performance and Sizing for the SOM Reporting Server”。

  安装 SOM 报告服务器并部署 SOM 内容包后，必须配置证书以启用 SOM 服务器和报告服务器之间的文件传输。有关 SOM 服务器的信息，请参阅《Storage Resource Management Reports Guide》中的“Configuring Connections Between SOM Management Server and SOM Reporting Server”。

第 3 章: 计划许可证

HP Storage Operations Manager 通过许可证限制其管理的元素数量。许可基于被管访问端口 (MAP) 计数。有关详细信息，请参考“MAP 计数计算”表。

下面是 SOM 许可的关键点:

- SOM 根据已安装的许可证识别许可的 MAP 计数 (可用容量) 限制。SOM 根据环境中已发现的元素计算 MAP 计数消耗 (已用容量)。当已用容量超过可用容量时，SOM 将阻止发现更多元素。在这种情况下，如果尝试发现元素，将收到错误“已超出许可证容量”。但有效的临时瞬时启动许可证没有发现限制。
- 同一时间只能有一种许可证类型处于活动状态。不能混合使用高级和终极性能包许可证类型。如果同时安装了 SOM 高级许可证和 SOM 终极性能包许可证，则终极性能包将取代高级许可证。可用容量派生自被取代的许可证。
- 您需要 SOM 终极性能包许可证从支持性能采集的设备采集性能度量。SOM 的当前版本允许通过管理服务器的单个实例同时配置和采集 25 个设备的性能度量。
- 您可以通过采购其他许可证来扩展许可的 MAP 计数 (可用容量)。安装新许可证后，将合计可用容量并刷新。但不会合计性能的许可证容量，该容量固定为管理服务器的单个实例配置和采集 25 个设备。

许可证类型

SOM 的当前版本提供三种许可证类型。

许可证类型	有效性	支持性能
SOM 瞬时启动	60 天	是
SOM 高级	无限制	否
SOM 终极性能包	无限制	是

临时瞬时启动许可证

安装 HP Storage Operations Manager 时，将同时安装临时瞬时启动许可证。临时瞬时启动许可证有效期为 60 天。应当尽早获取并安装永久许可证以继续使用 SOM。

获取并安装新许可证

要请求永久许可证，请收集以下信息:

- 权利证书，包含 HP 产品号和订购号。
- 其中一个 SOM 管理服务器的 IP 地址。
- 公司或组织信息。

安装永久许可证

您可以使用 Autopass 用户界面或命令行界面安装永久许可证。

使用命令行

要使用命令提示符在 SOM 管理服务器上安装许可证，请输入以下命令:

```
somlicensemanager.ovpl SOM -install <许可证文件的路径>
```

其中 <许可证文件的路径> 是存储许可证文件的位置。

使用 Autopass 安装永久许可证

要安装永久许可证，请执行以下步骤:

1. 在命令提示符处，输入以下命令打开 Autopass 用户界面:
   ```
   somlicensemanager.ovpl SOM -gui
   ```
2. 在 Autopass 窗口的左窗格中，单击 **License Management**。
3. 单击 **Install License Key**。
4. 单击 **Install/Restore License Key**。
5. 浏览到存储许可证密钥的位置。
6. 查看文件内容。
7. 选择许可证并单击 **Install**。

查看许可证信息

1. 从 SOM 控制台中，单击“帮助”>“系统信息”>“查看许可信息”。
2. 查找“消耗”字段中显示的值。这是 SOM 当前正在管理的 MAP 数 (已用容量)。

查看每个元素消耗的 MAP 计数

您可以查看 SOM 正在管理的每个元素消耗的 MAP 数。此信息显示在“库存”视图中每个元素的“分析”窗格的“图计数”字段中。

MAP 计数计算

元素	描述	MAP 数量	注释
主机	具有单个端口 HBA 的主机 具有双端口 HBA 的主机	1 个 MAP 2 个 MAP	CIM 扩展不另外计算。
	没有 FC 端口的主机	1 个 MAP	
	具有一个 iSCSI 网络卡端口的主机	1 个 MAP	
	无 FC 端口和 iSCSI 网络卡端口但具有 CIM 扩展的主机	1 个 MAP	
	通过 CIM 扩展未发现 FC HBA 的独立服务器	1 个 MAP	
	通过 Windows Management Instrumentation (WMI) 进行的 Windows 服务器无代理发现	至少 1 个 MAP 或每个 FC HBA 端口 1 个 MAP。	
	通过 SSH 进行的 Linux 服务器无代理发现	至少 1 个 MAP 或每个 FC HBA 端口 1 个 MAP。	
	通过 SSH 进行的 AIX 无代理发现	至少 1 个 MAP 或每个 FC HBA 端口 1 个 MAP。	
	通过 SSH 进行的 Solaris 无代理发现	至少 1 个 MAP 或每个 FC HBA 端口 1 个 MAP。	
虚拟服务器	VMware ESX 服务器	至少 1 个 MAP 或每个 FC HBA 端口 1 个 MAP。	五个具有双端口 HBA 的 ESX 服务器算作 10 个 MAP (5*2=10)
	虚拟服务器上的每个 FC 端口	1 个 MAP	将虚拟服务器视为物理主机。
	无 FC 端口的虚拟服务器	1 个 MAP	软件假定一个 MAP。
虚拟机	正在运行 VMTool 的虚拟机，而不管它是通过其虚拟服务器还是 VirtualCenter 发现的	1 个 MAP	

元素	描述	MAP 数量	注释
	已安装 CIM 扩展而不管 VMTool 是否正在运行的虚拟机	1 个 MAP	
	通过 WMI (Windows)、SSH (Linux) 或 CIM 扩展直接发现的每个 VMware 虚拟机来宾操作系统	1 个 MAP	通过 VMTool 进行发现、后续通过无代理 WMI 或 CIM 扩展发现的 VMware 虚拟机来宾操作系统只算作 1 个 MAP。
交换机	交换机上的每个端口 物理交换机的所有端口均算作 MAP	1 个 MAP	• 已安装 GBIC 的所有交换机端口均算作 MAP。 • ISL 链接不算作 MAP。 • 如果交换机端口未获得许可，则不算作 MAP。 • 如果未安装 GBIC 或端口未获得许可，则 SOM 将不会发现这些端口号。仅将发现的端口算作 MAP。
Isilon		节点数 * 5	
HP XP/P9500 外部存储	每个端口	1 个 MAP	所有后端端口均算作 MAP。
EVA、3PAR、EMC VNX/CLARiiON、DMX/VMAX、VPLEX、HUS/USP	每个端口	1 个 MAP	所有后端端口均算作 MAP。
NetApp 7/Celerra		5 个 MAP	仅支持单个节点。
EMC VNX Filer		5 个 MAP	

第 4 章: CIM 扩展

通用信息模型 (CIM) 标准指定有关被管元素的信息结构。CIM 提供一致的数据结构和访问，而不考虑设备供应商。CIM 由分布式管理任务组 (DMTF) 维护。

存储管理主动规范 (SMI-S) 实现异构存储元素的一致管理。SMI-S 基于通用信息模型 (CIM) 和基于 Web 的企业管理 (WBEM) 标准，以便通过 HTTP 访问管理信息。SMI-S 由存储网络行业协会 (SNIA) 维护。

SOM CIM 扩展是在存储主机上运行的采集代理，用于收集有关该主机的信息。在发现和管理主机时，SOM 管理服务器将与 CIM 扩展通信。

要使 SOM 管理服务器能够从主机获取信息，CIM 扩展必须正在运行。CIM 扩展在安装后以及每次主机引导时自动启动。在 HP-UX 主机上，CIM 扩展使用 `/sbin/rc2.d` 脚本。

SOM 可以使用无代理进程管理一些存储主机。但是，无代理方法限制对 SOM 可用的信息。有关详细信息，请参阅《SOM Device Support Matrix》。

CIM 扩展的默认位置为:

- *Windows*:`<驱动器:>\Program Files (x86)\APPQcime\CimExtensions`
- *UNIX 或 Linux*:`/opt/APPQcime/`

安装 CIM 扩展

CIM 扩展使用全球网络存储工业协会 (SNIA) 创建的光纤通道主机总线适配器应用编程接口 (FC-HBA API) 来与主机总线适配器 (HBA) 进行通信。SOM 管理服务器仅支持与符合 HBA API 的 HBA 进行通信。有关 HBA API 的详细信息，请访问 SNIA 网页: **http://www.snia.org**。

SOM 安装介质中的 `hbatest` 程序将在支持 FC-HBA API 的主机上输出所有 HBA 的名称和编号。在某些情况下，`hbatest` 可能会报告找不到 HBA 驱动程序，即使安装了 HBA 驱动程序也是如此。在这种情况下，请尝试安装其他符合 SNIA 版本的 HBA 驱动程序。

SOM 安装介质的 `CIMExtensionsCD1` 目录中包含特定于操作系统的 CIM 扩展。

安装 CIM 扩展

1. 验证支持 FC-HBA API 的主机上是否至少有一个主机总线适配器 (HBA)。执行适用于您的环境的步骤:
   - 验证 Windows 主机上的 FC-HBA API 支持 (第 15 页)
   - 验证 HP-UX 主机上的 FC-HBA API 支持 (第 15 页)
   - 验证 Linux 主机上的 FC-HBA API 支持 (第 16 页)
2. 验证端口 4673 是否在主机上可用，以及是否可由 SOM 管理服务器访问。
   或者，标识 CIM 扩展的其他端口。安装后，将 CIM 扩展配置为使用更改 CIM 扩展端口号 (第 21 页)中所述的端口。
3. 在主机上安装 CIM 扩展软件。执行适用于您的环境的步骤:
   - 在 Windows 主机上安装 CIM 扩展软件 (第 16 页)
   - 在 HP-UX 主机上安装 CIM 扩展软件 (第 17 页)

- 在 Linux 主机上安装 CIM 扩展软件 (第 18 页)

提示: 如果安全环境要求您自定义 CIM 扩展或 CIM 扩展安装过程，则可能需要使用第三方工具来部署 CIM 扩展。第三方工具通常用于需要使用变更请求 (RFC) 进程的大型环境中。

验证 Windows 主机上的 FC-HBA API 支持

验证支持 FC-HBA API 的 Windows 主机上是否至少有一个主机总线适配器

1. 在命令窗口中，切换到 SOM 安装介质的 `CimExtensionsCD1/Windows/tools` 目录。
2. 输入以下命令:

   ```
   hbatest.exe -v
   ```

   命令输出的开头应类似于以下示例:

   ```
   hbaapi.dll, version XXXXXXXXXXXXXX will be used to get HBA information.
   HBA API Library version is 2
   hbatest build date:Jun 26 2014:20:14:26
   Number of HBA's is 2
   ****************************************
   ```

   在标头后面，命令输出将列出主机上的每个 HBA。

返回到安装步骤。

验证 HP-UX 主机上的 FC-HBA API 支持

验证支持 FC-HBA API 的 HP-UX 主机上是否至少有一个主机总线适配器

1. 转到 SOM 安装介质的 `CimExtensionsCD1/HPUX/tools` 目录。
2. 运行以下命令:

   ```
   ./hbatest
   ```

   程序将运行其诊断。

HP SNIA 适配器 AXXXXA 来自文件集 FC-FCD、FC-TACHYON-TL。除非在安装操作系统期间故意隔开，否则将默认提供文件集。要查看库的位置，请在命令提示符处输入以下命令:

```
more /etc/hba.conf
```

`hba.conf` 文件包含下列行:

```
com.hp.fcms32 /usr/lib/libhbaapihp.sl #32 bit lib names end in 32
com.hp.fcms64 /usr/lib/pa20_64/libhbaapihp.sl #64 bit lib names end in 64
com.hp.fcd32 /usr/lib/libhbaapifcd.sl
com.hp.fcd64 /usr/lib/pa20_64/libhbaapifcd.sl
```

返回到安装步骤。

验证 Linux 主机上的 FC-HBA API 支持

验证支持 FC-HBA API 的 Linux 主机上是否至少有一个主机总线适配器

1. 转到 SOM 安装介质的 `CimExtensionsCD1/linux/tools` 目录。
2. 运行以下命令:

   ```
   ./hbatest
   ```

   程序将运行其诊断。

用于验证 Emulex SNIA 适配器的驱动程序信息 (仅限 Red Hat Linux)

Emulex 驱动程序不包含 SOM 管理服务器所需的库。必须安装 Emulex HBAnywhere 软件，以便管理服务器可以发现使用 HBAnywhere 配置的主机，以及 HBATool 可以检测到 Emulex 主机总线适配器。

安装 HBAnywhere 软件之后，可以在 `/etc/hba.conf` 文件中查找库的位置。

要在 Linux 主机上查看 `hba.conf` 文件，请运行以下命令:

```
cat /etc/hba.conf
```

输出将先列出库名称，然后列出路径，如以下示例中所示:

- Linux 64 位主机 Emulex 驱动程序示例输出

  ```
  com.emulex.emulexapilibrary /usr/lib64/libemulexhbaapi.so
  com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
  ```

  注意: HBAnywhere CLI 必须用于 IA64 Linux。

- Linux 32 位主机 Emulex 驱动程序示例输出

  ```
  com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
  ```

返回到安装步骤。

在 Windows 主机上安装 CIM 扩展软件

必须具有管理员特权才能在 Windows 主机上安装 CIM 扩展。

如果 Windows 主机上启用了防火墙，请在安装 CIM 扩展之前先打开 CIM 扩展端口。默认 CIM 扩展端口为 4673。有关配置 Windows 防火墙的信息，请参阅 Microsoft Windows 操作系统的文档。

可以交互方式或以静默模式安装 Windows CIM 扩展。使用静默模式在无用户干预的情况下安装具有默认设置的 Windows CIM 扩展。

交互模式

使用交互模式安装 CIM 扩展

1. 以具有管理员特权的用户身份登录 Windows 主机。
2. 将 SOM 安装介质插入 DVD 驱动器。

3. 在 Windows 资源管理器中，切换到 `CimExtensionsCD1\Windows` 目录，然后双击 `InstallCIMExtensions.exe`。
4. 遵循屏幕上的说明。

静默模式

使用静默模式安装 CIM 扩展

1. 验证是否没有其他程序正在运行。
2. 如从 Windows 主机中删除 CIM 扩展 (第 27 页)中所述删除之前版本的 CIM 扩展。
3. 以具有管理员特权的用户身份登录 Windows 主机。
4. 将 SOM 安装介质插入 DVD 驱动器。
5. 在命令窗口中，切换到以下目录:

   ```
   CimExtensionsCD1\Windows
   ```
6. 输入以下命令:

   ```
   InstallCIMExtensions.exe -i silent
   ```

返回到安装步骤。

在 HP-UX 主机上安装 CIM 扩展软件

以下说明适用于 CIM 扩展的本地安装。

必须将适用于 HP-UX 的 CIM 扩展安装到默认目录。如果存在空间问题，例如大量 CIM 扩展二进制文件，请创建指向具有更多空间的文件夹的符号链接。

安装 CIM 扩展

1. 以 `root` 用户身份登录 HP-UX 主机。
2. 将 SOM 安装介质插入 DVD 驱动器。
3. 通过运行以下命令，创建 `/DVD` 目录:

   ```
   mkdir /DVD
   ```
4. 通过在命令提示符处输入以下命令，安装 SOM 安装介质:

   ```
   mount /dev/dsk/c#t#d#  /DVD
   ```

   在此实例中，c、t 和 d 数字对应于 DVD 设备号。

   要找到 DVD 驱动器的 c#t#d#，请在 HP-UX 主机上运行 `ioscan -fnC disk` 命令。
5. 运行以下命令:

   ```
   swinstall -x mount_all_filesystems=false -s /cdrom/HPUX/APPQcime.depot
   APPQcime
   ```

   显示与下面类似的消息时，表示安装完成:

   ```
   analysis and execution succeeded
   ```
6. 通过运行以下命令，卸载 DVD:

   ```
   umount /DVD
   ```

   在此实例中，`/DVD` 是安装了 DVD 的目录名称。

返回到安装步骤。

在 Linux 主机上安装 CIM 扩展软件

以下说明适用于 CIM 扩展的本地安装。

该安装包括两个步骤: 运行 "requires" rpm 以检查依赖性，然后安装完整 RPM。

必须将适用于 Linux 的 CIM 扩展安装到默认目录。如果存在空间问题，例如大量 CIM 扩展二进制文件，请创建指向具有更多空间的文件夹的符号链接。

安装 CIM 扩展

1. 以 `root` 用户身份登录 Linux 主机。
2. 将 SOM 安装介质插入 DVD 驱动器。
3. 切换到 SOM 安装介质的 `CIMExtensionCD1/linux/requires_rpm` 目录。

   ```
   cd /DVD/linux/requires_rpm
   ```

   在此实例中，`/DVD` 是 DVD 驱动器的名称。
4. 当运行 "requires" rpm 仅返回一个预期依赖性错误时，请运行以下命令:

   ```
   rpm -idvh <rpm 软件包名称>
   ```

   在此实例中，`<rpm 软件包名称>` 是下表中列出的 RPM 软件包的名称。

操作系统	RPM
64 位 Red Hat 版本 6 及更高版本	APPQcime-<版本>-<发布>-x86_64.rpm
• x86 上的 Red Hat 32 位安装 • 早于 Red Hat 版本 6 的 64 位安装 • x86 或 x64 上的 SUSE 安装	APPQcime-<版本>-<发布>-i386.rpm
(Red Hat 和 SUSE Linux) 基于 IA64 的安装	APPQcime-<版本>-<发布>-ia64.rpm

   将显示以下输出:

   ```
   Preparing...########################################### [100%]
   1:APPQcime ########################################### [100%]
   ```

   返回到命令提示符时，表示安装已完成。
5. *可选*。验证是否已安装软件包:

   ```
   rpm -qa | grep APPQcime-Requires
   rpm -qa | grep APPQcime
   ```

返回到安装步骤。

配置 CIM 扩展

`cim.extension.parameters` 文件可确定 CIM 扩展的行为。CIM 扩展将在启动时读取此文件。

`cim.extension.parameters-sample` 文件提供模板配置。

这些文件位于以下目录中:

- *Windows*:[安装目录]\CimExtensions\conf
- *UNIX/Linux*:/opt/APPQcime/conf

CIM 扩展的默认行为如下所示:

- SOM 管理服务器必须使用主机上的管理员或根帐户才能与 CIM 扩展进行通信。
- CIM 扩展通过端口 4673 发送和接收通信。
- CIM 扩展将侦听主机的环回地址。

要更改此行为，请通过复制和自定义提供的模板文件 (cim.extension.parameters-sample) 来创建 cim.extension.parameters 文件。

配置 CIM 扩展

1. 以具有管理员或根特权的用户身份登录主机。
2. 切换到 CIM 扩展配置目录:
   - *Windows*:[安装目录]\CimExtensions\conf
   - *UNIX/Linux*:/opt/APPQcime/conf
3. 在相同目录中将 cim.extension.parameters-sample 文件的副本另存为 cim.extension.parameters。
4. 在文本编辑器中，根据需要编辑文件 cim.extension.parameters。
   有关经常更改的参数的信息，请参阅 CIM 扩展参数表。
   有关配置日志文件的信息，请参阅日志文件属性 (第 24 页)。
5. 保存并关闭文件。
6. 重新启动 CIM 扩展。
   - *Windows*:
     从“服务”窗口重新启动 AppStorWin32Agent 服务或重新启动主机。
   - *UNIX/Linux*:
     ```
     /opt/APPQcime/tools/stop
     /opt/APPQcime/tools/start
     ```

经常配置的 CIM 扩展参数

参数	描述
-users	仅限有效主机用户列表中的用户可以发现主机。使用此参数定义的每个用户必须是主机上的有效现有用户，且用户名必须与发现页面上使用的用户名之一相匹配，才能通过身份验证以发现主机。用户无需具有根权限。使用冒号 (:) 分隔多个用户。 用户名的格式取决于操作系统: • *Windows*:指定域名和用户名，例如: -users domain_name\user_name • *UNIX*:指定用户名，而非域名，例如: -users user_name 有关详细信息，请参阅限制可以发现主机的用户 (第 20 页)。

参数	描述
-credentials <用户名>:<密码>	指定主机的用户名和密码以促进 SOM 管理服务器和被管主机之间的通信。此配置无需使用本地操作系统用户/密码数据库来验证凭据。此用户名/密码对仅对 CIM 扩展已知，不会标识主机上的真实用户。指定帐户名可能不存在于主机上。 -users 参数始终优先于 -credentials 参数。要在将 -users 参数已添加到 cim.extension.parameters 文件中时使用 -credentials 参数，请通过在 -users 行的开头插入井号字符 (#) 来注释掉 -users 参数。
-mgmtServerIP <IP 地址>	将 CIM 扩展限制为仅侦听指定的 SOM 管理服务器。 使用逗号分隔多个地址值。例如: -mgmtServerIP 127.0.0.1,192.168.0.1
-port <新端口>	指定 CIM 扩展将访问的端口。例如: -port 1234 请参阅更改 CIM 扩展端口号 (第 21 页)。
-on <IP 地址 1> -on <IP 地址 2:端口>	对于多主系统，将 CIM 扩展限制为仅侦听指定的 IP 地址。 对多个地址使用多个条目。例如: -on <15.218.125.12> -on <15.218.125.123:5432> 请参阅将 CIM 扩展配置为侦听特定的 IP 地址 (第 22 页)。

仅限 UNIX/Linux。有关 CIM 扩展配置的命令行帮助，请运行以下命令:

```
/opt/APPQcime/tools/start -help
```

限制可以发现主机的用户

通过限制对 CIM 扩展的访问，-users 参数可以提高安全性。使用 SOM 管理服务器发现主机时，提供在 -users 参数中指定的用户名之一。

要在不使用根帐户的情况下使用管理服务器发现主机，请为另一个对主机具有更少特权的有效用户帐户提供密码。

首先，将用户添加到参数文件中。然后，登录管理服务器，访问发现页面，并为 jsmythe 提供用户名和密码。只有 jsmythe 的用户名和密码可用于发现主机。

将用户添加到参数文件中

1. 将 CIM 扩展配置目录备份到 CIM 扩展安装目录外的位置:
   - *Windows*:[*安装目录*]\CimExtensions\conf
   - *UNIX/Linux*:/opt/APPQcime/conf
2. 在文本编辑器中，打开 cim.extension.parameters 文件。
3. 添加以下行:

   ```
   -users myname
   ```

   在此实例中，myname 是主机上的有效用户名。

要输入多个用户，请使用冒号分隔它们，例如 `-users myname:jsymthe`。

4. 保存该文件。
5. 重新启动 CIM 扩展。
   - *Windows*:

     从“服务”窗口重新启动 AppStorWin32Agent 服务或重新启动主机。

   - *UNIX/Linux*:

     ```
     /opt/APPQcime/tools/stop
     /opt/APPQcime/tools/start
     ```

更改 CIM 扩展端口号

默认情况下，CIM 扩展使用端口 4673。如果此端口已使用，请按如下方式更改 CIM 扩展:

1. 将 CIM 扩展配置目录备份到 CIM 扩展安装目录外的位置:
   - *Windows*:`[安装目录]\CimExtensions\conf`
   - *UNIX/Linux*:`/opt/APPQcime/conf`
2. 在文本编辑器中，打开 `cim.extension.parameters` 文件。
3. 添加以下行:

   ```
   -port <端口号>
   ```

   将 *<端口号>* 替换为要使用的端口号。
4. 保存该文件。
5. 重新启动 CIM 扩展。
   - *Windows*:

     从“服务”窗口重新启动 AppStorWin32Agent 服务或重新启动主机。

   - *UNIX/Linux*:

     ```
     /opt/APPQcime/tools/stop
     /opt/APPQcime/tools/start
     ```

6. 使用此主机的新端口号更新 SOM 管理服务器。
   a. 打开此主机的“发现地址”表单 (“配置”>“发现”>“发现地址”)。
   b. 在“IP 地址”框中，输入 IP 地址，冒号后跟新的端口号。例如:

      ```
      192.168.1.2:1234
      ```

      在此实例中，192.168.1.2 是主机的 IP 地址，1234 是新的端口号。

      如果已将主机添加到管理服务器上的发现列表 (“配置”>“发现”>“发现地址”)，则必须删除它，然后重新添加。不能列出多个具有不同端口的主机。

将 CIM 扩展配置为侦听特定的 IP 地址

将 CIM 扩展配置为侦听特定的 IP 地址

1. 将 CIM 扩展配置目录备份到 CIM 扩展安装目录外的位置:
   - *Windows*:`[安装目录]\CimExtensions\conf`
   - *UNIX/Linux*:`/opt/APPQcime/conf`
2. 在文本编辑器中，打开 `cim.extension.parameters` 文件。
3. 针对每个要侦听的 IP 地址，添加以下行:

   `-on <IP 地址>`

   将 *<IP 地址>* 替换为某个 IP 地址。还可以添加一个端口。例如，要侦听 IP 地址为 192.168.2.2 的端口 3456，请使用以下文本:

   `-on 192.168.2.2:3456`
4. 保存该文件。
5. 重新启动 CIM 扩展。
   - *Windows*:

     从“服务”窗口重新启动 AppStorWin32Agent 服务或重新启动主机。
   - *UNIX/Linux*:

     ```
     /opt/APPQcime/tools/stop
     /opt/APPQcime/tools/start
     ```
6. 使用此主机的新端口号更新 SOM 管理服务器。
   a. 打开此主机的“发现地址”表单 (“配置”>“发现”>“发现地址”)。
   b. 在“IP 地址”框中，输入 IP 地址，冒号后跟新的端口号。例如:

      `192.168.1.2:1234`

      在此实例中，192.168.1.2 是主机的 IP 地址，1234 是新的端口号。

      如果已将主机添加到管理服务器上的发现列表 (“配置”>“发现”>“发现地址”)，则必须删除它，然后重新添加。不能列出多个具有不同端口的主机。

将 CIM 扩展配置为在防火墙后运行 (仅限 UNIX)

要发现防火墙后的主机，请使用下表作为准则。假设管理服务器要发现 HostA，该主机在三个独立网络中有三个网络接口卡，三个独立的 IP 地址分别为:10.250.250.10、172.31.250.10 和 192.168.250.10。下表提供了配置选项。

- “CIM 扩展的手动启动参数”列提供在主机上手动启动 CIM 扩展时要输入的值。有关如何手动启动 CIM 扩展的详细信息，请参阅手动启动 CIM 扩展 (第 26 页)。
- “cim.extension.parameters 中是否提及”列提供有关修改 `cim.extension.parameters` 文件的信息 (请参阅更改 CIM 扩展端口号 (第 21 页))。
- “步骤 1 发现和 RMI 注册表端口”列提供有关发现列表所需的 IP 地址的信息。CIM 扩展使用 RMI 注册表端口。当使用 4673 以外的端口进行 CIM 扩展时，该端口必须包含在发现 IP 地址内，例如 192.168.1.1:1234。在此实例中，192.168.1.1 是主机的 IP 地址，1234 是 CIM 扩展使用的端口。

防火墙疑难解答

配置	CIM 扩展的手动启动参数	cim.extension.parameters 中是否提及	步骤 1 发现和 RMI 注册表端口
在主机和管理服务器之间打开了防火墙端口 4673。	start		10.250.250.10 *或* 172.31.250.10 *或* 192.168.250.10 通信端口:4673
在主机和管理服务器之间打开了防火墙端口 1234。	start -port 1234	-port 1234	10.250.250.10:1234 *或* 172.31.250.10:1234 *或* 192.168.250.10:1234 通信端口:1234
在 172.31.250.x 子网上，在主机和管理服务器之间打开了防火墙端口 4673。	start -on 172.31.250.10	-on 172.31.250.10	172.31.250.10 通信端口:4673
在 192.168.250.x 子网上，在主机和管理服务器之间打开了防火墙端口 1234。	start -on 192.168.250.10:1234	-on 172.31.250.10:1234	172.31.250.10:1234 通信端口:1234
分别在不同端口上打开了 3 个防火墙端口 1234、5678、9012。	start -on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012	-on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012	10.250.250.10:1234 *或* 172.31.250.10:5678 *或* 192.168.250.10:9012 通信端口: 1234、5678、9012
在主机和管理服务器之间打开了防火墙端口 4673。NAT 环境，其中 10.250.250.10 子网在到达防火墙另一端时转换为 172.16.10.10。	start		172.16.10.10 通信端口: 17001
在主机和管理服务器之间打开了防火墙端口 1234。NAT 环境，其中 10.250.250.10 子网在到达防火墙另一端时转换为 172.16.10.10。	start -port 1234	-port 1234	172.16.10.10 通信端口: 17001
分别在不同端口上打开了 3 个防火墙端口 1234、	start -on 10.250.250.10:1234	-on 10.250.250.10:1234 -on 172.31.250.10:5678	172.16.10.10:1234 *或*

防火墙疑难解答(续)

配置	CIM 扩展的手动启动参数	cim.extension.parameters 中是否提及	步骤 1 发现和 RMI 注册表端口
5678、9012。NAT 环境，其中所有 3 个 NIC 均转换为不同的 172.16.x.x 子网。	-on 172.31.250.10:5678 -on 192.168.250.10:9012	-on 192.168.250.10:9012	172.16.20.20:5678 *或* 172.16.30.30:9012 通信端口: 1234、5678、9012
DNS 不正确或 IP 解析很慢。		jboss.properties, cimom.Dcxws.agency.firstwait=200000 cimom.Dcxws.agency.timeout=200000	任何可访问的 IP 通信端口:4673
无 DNS，不解析。		jboss.properties cimom.Dcxws.agency.firstwait=200000 cimom.Dcxws.agency.timeout=200000	任何可访问的 IP 通信端口:4673
无防火墙。出于安全原因，使用不存在的用户进行发现。	start -credentials string1:string2 在此实例中，string1 在发现中作为“username”提供，而 string2 作为“password”提供。	-credentials username:password	指定发现列表中的用户名和密码。 通信端口:4673
分别在不同端口上打开了 3 个防火墙端口 1234、5678、9012。出于安全原因，使用不存在的用户进行发现。	start -on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012 -credentials string1:string2 在此实例中，string1 在发现中作为“username”提供，而 string2 作为“password”提供。	-on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012 -credentials username:password	10.250.250.10:1234 *或* 172.31.250.10:5678 或 192.168.250.10:9012 指定发现列表中的用户名和密码。 通信端口: 1234、5678、9012

日志文件属性

`cim.extension.parameters` **文件包含每个日志文件的以下属性:**

- `<日志名称>.log.File` **- 设置日志文件的名称和位置。**
- `<日志名称>.log.MaxFileSize` **- 设置最大文件大小 (MB)。**

- <日志名称>.log.MaxBackupIndex - 设置在覆盖文件之前创建的最大文件数。

CIM 扩展日志文件的默认位置为:

- *Windows*:[*安装目录*]\CimExtensions\tools
- *UNIX/Linux*:/opt/APPQcime/tools

日志文件将在达到已配置的大小时回滚。每个日志包含已配置的文件数。

例如，cxws.log 文件将采集大多数 CIM 扩展日志记录信息。CIM 扩展会将启动时间、停止时间和意外错误情况附加到现有 cxws.log 文件。cim.extension.parameters 文件中的默认 cxws.log 文件配置如下所示:

```
-D cxws.log.File=cxws.log
-D cxws.log.MaxFileSize=30MB
-D cxws.log.MaxBackupIndex=3
```

默认情况下，cxws.log 文件会在每次超过 30 MB 时回滚。cxws.log 文件将重命名为 cxws.log.1，并将新建 cxws.log 文件。当 cxws.log 文件再次回滚时，cxws.log.1 将重命名为 cxws.log.2，cxws.log 文件将重命名为 cxws.log.1，并将新建 cxws.log 文件，以此类推，最多可有三个备份日志文件:

- cxws.log
- cxws.log.1
- cxws.log.2
- cxws.log.3

查找 CIM 扩展的版本

查找 CIM 扩展的版本号

- *Windows*:在“程序和功能”控制面板中，检查 AppStorWin32Agent 服务的“状态”列中的值。
- *UNIX 或 Linux*:运行以下命令:

  /opt/APPQcime/tools/status

要查找 CIM 扩展的版本号，请运行以下命令:

```
/opt/APPQcime/tools/start -version
```

输出中将显示 CIM 扩展的版本号和生成日期。例如:

```
Starting CIM Extension for HP-UX
CXWS for mof/cxws/cxws-HPUX.mof
CXWS version x.x.x.x, built on Fri 12-March-xxxx 12:29:49 by dmaltz
```

检查 CIM 扩展的状态

确定 CIM 扩展的状态

- *Windows*:在“服务”窗口中，检查 AppStorWin32Agent 服务的“状态”列中的值。
- *UNIX 或 Linux*:运行以下命令:

  /opt/APPQcime/tools/status

手动启动 CIM 扩展

当已安装的 CIM 扩展正在运行时，SOM 管理服务器只能收集有关主机的信息。

必须具有管理员或根特权才能启动 CIM 扩展。CIM 扩展仅在启动 CIM 扩展的用户帐户特权范围内提供信息。只有管理员或根用户才具有提供管理服务器所需信息的足够特权。如果使用管理员或根特权无法启动 CIM 扩展，管理服务器将显示类似于以下内容的消息:

```
Data is late or an error occurred.
```

启动 CIM 扩展

- *Windows*:从“服务”窗口启动 AppStorWin32Agent 服务。
- *UNIX 或 Linux*:运行以下命令:

  ```
  /opt/APPQcime/tools/start
  ```

提示: 从命令行启动 CIM 扩展时，可以使用 CIM 扩展参数表中的任何选项。

停止 CIM 扩展

当已安装的 CIM 扩展正在运行时，管理服务器只能收集有关主机的信息。

必须具有管理员或根特权才能停止 CIM 扩展。

停止 CIM 扩展

- *Windows*:从“服务”窗口停止 AppStorWin32Agent 服务。
- *UNIX 或 Linux*:运行以下命令:

  ```
  /opt/APPQcime/tools/stop
  ```

自定义 CIM 扩展的 JVM 设置

要自定义 CIM 扩展的 Java 虚拟机 (JVM) 配置，请通过复制并自定义提供的模板文件 (`wrapper.user-sample`) 来创建 `wrapper.user` 文件。将配置文件放到以下目录中:

- *Windows*:`[安装目录]\CimExtensions\conf`
- *UNIX/Linux*:`/opt/APPQcime/conf`

将来每次升级 CIM 扩展后，CIM 扩展都会保留并使用自定义的 `wrapper.user` 文件。

配置 CIM 扩展 JVM

1. 以具有管理员或根特权的用户身份登录主机。
2. 切换到 CIM 扩展配置目录:
   - *Windows*:`[安装目录]\CimExtensions\conf`
   - *UNIX/Linux*:`/opt/APPQcime/conf`

3. 在相同目录中将 `wrapper.user-sample` 文件的副本另存为 `wrapper.user`。
4. 在文本编辑器中，根据 `wrapper.user` 文件中的注释编辑此文件。
5. 保存并关闭文件。
6. 重新启动 CIM 扩展。
   - *Windows*:
     从“服务”窗口重新启动 AppStorWin32Agent 服务或重新启动主机。
   - *UNIX/Linux*:
     `/opt/APPQcime/tools/stop`
     `/opt/APPQcime/tools/start`

删除 CIM 扩展

要从主机中删除 CIM 扩展，请执行以下适用的步骤:

- 从 Windows 主机中删除 CIM 扩展 (第 27 页)
- 从 HP-UX 主机中删除 CIM 扩展 (第 27 页)
- 从 Linux 主机中删除 CIM 扩展 (第 28 页)

从 Windows 主机中删除 CIM 扩展

如果从其中有一个服务正在使用 WMI (如 Microsoft Exchange) 的 Windows 主机删除 CIM 扩展，您将看到一条消息，指示无法停止 WMI 服务。继续删除 CIM 扩展，然后在删除过程完成后重新启动主机。

从 Windows 主机中删除 CIM 扩展

1. 以具有管理员特权的用户身份登录 Windows 主机。
2. 打开“程序和功能”或“添加或删除程序”控制面板。
3. 在已安装的程序列表中，右键单击“Windows CIM 扩展”，然后单击“卸载”。
4. 遵循屏幕上的说明。
5. 卸载程序完成后，删除 CIM 扩展安装目录。
   默认位置为:
   `<驱动器>:\Program Files (x86)\APPQcime\CimExtensions`
6. 建议重新启动主机。

从 HP-UX 主机中删除 CIM 扩展

从 HP-UX 主机中删除 CIM 扩展

1. 以 `root` 用户身份登录 HP-UX 主机。
2. 通过运行以下命令，停止 CIM 扩展:
   `/opt/APPQcime/tools/stop`

3. 为确保不在 `/opt/APPQcime` 目录中，请切换到根目录。
4. 运行以下命令:

   ```
   swremove APPQcime
   ```

   预期输出类似于以下示例:

   ```
   * Beginning Execution
   * The execution phase succeeded for hpuxqaX.dnsxxx.com:/".
   * Execution succeeded.
   ```

5. 要删除 `APPQcime` 目录，请运行以下命令:

   ```
   rm -r APPQcime
   ```

从 Linux 主机中删除 CIM 扩展

从 Linux 主机中删除 CIM 扩展

1. 以 `root` 用户身份登录 Linux 主机。
2. 通过运行以下命令，停止 CIM 扩展:

   ```
   /opt/APPQcime/tools/stop
   ```

3. 卸载 "requires" rpm。例如:

   ```
   rpm -e APPQcime-Requires-XX-224
   ```

4. 卸载 CIM 扩展:

   ```
   rpm -e APPQcime
   ```

5. 要删除 `APPQcime` 目录，请运行以下命令:

   ```
   rm -r APPQcime
   ```

CIM 扩展疑难解答

以下主题介绍了对 CIM 扩展进行疑难解答的一些常用方法:

- 代理服务不启动 (仅限 Windows) (第 28 页)
- CIM 扩展因低熵暂停 (仅限 Linux) (第 29 页)

代理服务不启动 (仅限 Windows)

在 Windows Server 2003/2008 R2 IA64 平台上安装代理后，CIM 代理服务 `AppStorWin32Agent` 可能不启动。

在基于 Intel® Itanium® 的计算机上启动代理时，如果 JVM 由于内存分配问题而退出，则会出现此问题。

要解决此问题，请执行以下操作:

1. 在文本编辑器中打开以下文件:

   `[安装目录]\CimExtensions\conf\win32agent.conf`

2. 减小属性 `wrapper.java.maxmemory` 的值。例如，如果当前值为 1024，则将值减小到 512。
3. 从“服务”窗口重新启动 AppStorWin32Agent 服务或重新启动主机。

CIM 扩展因低熵暂停 (仅限 Linux)

有时候，Linux CIM 扩展会因为低熵而在启动时暂停。

Linux 内核使用键盘计时、鼠标移动和 IDE 计时来生成 `/dev/random` 的熵。从这些来源收集的熵存储在熵池中，`/dev/random` 返回的随机值使用此池作为源。这意味着如果熵计数器值太低，`/dev/random` 不会返回任何值，同时将阻止程序读取 `/dev/random`，直到采集到足够的熵。此行为可能在没有键盘、鼠标和 IDE 磁盘的服务器上发生。

1. 要确定 Linux 代理是否由于此问题暂停，请运行以下命令:

   ```
   kill -3 java_process_id
   ```

   在此实例中，java_process_id 是 Linux 代理的 Java 进程的进程 ID，不是 `status` 命令返回的进程 ID。

   上述命令将生成类似于以下示例的堆栈跟踪:

   ```
   INFO | jvm 1 | 2006/11/22 10:56:58 | at java.security.SecureRandom.next
   (Unknown Source)
   INFO | jvm 1 | 2006/11/22 10:56:58 | at java.util.Random.nextInt(Unknown
   Source)
   INFO | jvm 1 | 2006/11/22 10:56:58 | at
   com.sun.net.ssl.internal.ssl.SSLContextImpl.engineInit(Unknown Source)
   INFO | jvm 1 | 2006/11/22 10:56:58 | at javax.net.ssl.SSLContext.init(Unknown
   Source)
   INFO | jvm 1 | 2006/11/22 10:56:58 | at
   com.appiq.cxws.agency.agent.AgentMessageDispatcher.
   createServerSocket(AgentMessageDispatcher.java:1
   INFO | jvm 1 | 2006/11/22 10:56:58 | at
   com.appiq.cxws.agency.agent.AgentMessageDispatcher.
   startAccepting(AgentMessageDispatcher.java:74)
   ```

2. 要修复此问题，在 `/opt/APPQcime/conf/wrapper.conf` 文件的 Java 其他属性部分，搜索属性 `wrapper.java.additional.N=-Djava.security.egd=file:/dev/random`，然后将 `random` 更改为 `urandom`。

   更改完成后，该属性应类似于:

   ```
   wrapper.java.additional.N=-Djava.security.egd=file:/dev/urandom
   ```

3. 重新启动 CIM 扩展:

   ```
   /opt/APPQcime/tools/stop
   /opt/APPQcime/tools/start
   ```

第 5 章: 配置

本章介绍了概念、所需的初始配置、SOM 提供的默认值、一些最佳实践和计划信息，这些内容将帮助您在环境中实施 SOM。

端口和防火墙

下表显示了 SOM 在管理服务器上使用的端口。

图例	
I/O	必须同时在 SOM 服务器和目标设备上打开该端口。
O	必须在目标设备上打开该端口。
I	必须在源服务器上打开该端口，例如 SOM 管理服务器。

SOM 管理服务器上使用的端口

端口	类型	名称	用途	更改配置	输入/输出
80	TCP	nmsas.server.port.web.http	用于 Web UI 和 Web 服务的默认 HTTP 端口；打开此端口后，端口即变为双向。		I/O
443	TCP	nmsas.server.port.web.https	默认安全 HTTPS 端口 (SSL)；用于 Web UI 和 Web 服务。	修改 nms-local.properties 文件	
1098	TCP	nmsas.server.port.naming.rmi	• 由 SOM 命令行工具用于与 SOM 使用的多种服务通信 • HP 建议配置系统防火墙以仅允许 localhost 访问这些端口	修改 nms-local.properties 文件	
1099	TCP	nmsas.server.port.naming.port	• 由 SOM 命令行工具用于与 SOM 使用的多种服务通信。 • HP 建议配置系统防火墙以仅允许 localhost 访问这些端口	修改 nms-local.properties 文件	
3873	TCP	nmsas.server.port.remoting.ejb3	• 由 SOM 命令行工具用于与 SOM 使用的多种服务通信。 • HP 建议配置系统防火墙以仅允许 localhost 访问这些	修改 nms-local.properties 文件	

SOM 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置	输入/输出
			端口		
4444	TCP	nmsas.server.port.jmx.jrmp	• 由 SOM 命令行工具用于与 SOM 使用的多种服务通信。 • HP 建议配置系统防火墙以仅允许 localhost 访问这些端口。	修改 nms-local.properties 文件	
4445	TCP	nmsas.server.port.jmx.rmi	• 由 SOM 命令行工具用于与 SOM 使用的多种服务通信。 • HP 建议配置系统防火墙以仅允许 localhost 访问这些端口	修改 nms-local.properties 文件	
4446	TCP	nmsas.server.port.invoker.unified	• 由 SOM 命令行工具用于与 SOM 使用的多种服务通信。 • HP 建议配置系统防火墙以仅允许 localhost 访问这些端口。	修改 nms-local.properties 文件	
4712	TCP	nmsas.server.port.ts.recovery	内部事务服务端口。	修改 nms-local.properties 文件	
4713	TCP	nmsas.server.port.ts.status	内部事务服务端口。	修改 nms-local.properties 文件	
4714	TCP	nmsas.server. port.ts.id	内部事务服务端口。	修改 nms-local.properties 文件	
5432	TCP	com.hp.ov.nms.postgres.port	此 PostgreSQL 端口是嵌入式数据库用于侦听此 SOM 管理服务器的端口。	修改 nms-local.properties 文件	
8886	TCP	OVsPMD_MGMT	SOM ovspmd (进程管理器) 管理端口。	修改 /etc/services 文件	
8887	TCP	OVsPMD_REQ	SOM ovspmd (进程管理器) 请求端口。	修改 /etc/services 文件	
8989	TCP	com.hp.ov.nms.events.action.server.port	使操作服务器端口可配置。	修改 nnmaction.properties 文件	

用于 SOM 管理服务器与其他系统之间通信的端口

端口	类型	用途	客户端/服务器	输入/输出
80	TCP	SOM 的默认 HTTP 端口；用于 Web UI 和 Web 服务。	服务器	
80	TCP	SOM 用于连接到其他应用程序的默认 HTTP 端口。实际端口取决于 SOM 配置。	客户端	
389	TCP	默认 LDAP 端口。	客户端	
443	TCP	SOM 用于连接到其他应用程序的默认安全 HTTPS 端口；实际端口取决于 SOM 配置。Windows 上 HP OM 的默认 HTTPS 端口。	客户端	
443	TCP	默认安全 HTTPS 端口；用于 Web UI 和 Web 服务。	服务器	
636	TCP	默认安全 LDAP 端口 (SSL)。	客户端	
135	TCP	psexec 端口，管理服务器上的 Windows 无代理。	服务器	
445	TCP	psexec 端口，管理服务器上的 Windows 无代理。	服务器	
139	TCP	winexe 端口，管理服务器上的 Windows 无代理。	服务器	
383	TCP	CMS 上的 LCore 通信端口，用于与 SOM 报告服务器通信。	服务器	

关于 SOM 管理服务器的安全建议

此部分提供用于增强 SOM 管理服务器安全性的信息。

建议将 SOM Web 服务器的流量限制为仅应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。
- 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。

SOM 在启用 JMX 控制台的情况下安装。建议通过将 JMX 控制台定义文件移动到其他位置 (例如上移一个目录级别) 来禁用 JMX 控制台。JMX 控制台定义文件的默认位置为:

- *Windows*:`<SOM 安装目录>\nmsas\common\deploy\jmx-console.sar`
- *Linux*:`$SomInstallDir/nmsas/common/deploy/jmx-console.sar`

节点组

节点组是具有相同设备筛选条件的节点 (元素) 或子节点组的集合。基于预定义的属性将发现元素自动分配给节点组后。

节点组可用于以下任何或全部用途:

- 用于分类，支持您标识系统中的基本类别，如主机、存储系统、交换机和构造。
- 分类使您能更加轻松地进行监视和管理。它可以帮助您将设置应用于组，避免逐个处理元素。例如，您可以在节点组而非各个元素上实现数据采集策略。
- 作为用于自定义不同视图的主要筛选技术。
- 用户访问控制，限制通过安全映射对一组节点的访问。

默认节点组

SOM 提供以下默认节点组。这些节点组将使用与管理域相关的特定信息进行配置。您可根据需要进行更改。

- 所有元素
- FC 构造
- FC 交换机
- 主机
- 存储系统

这些节点组基于在发现过程中派生自系统对象 ID 的设备类别。

节点组成员资格

可以基于环境和要求创建其他节点组。可以定义用于确定节点组成员资格的属性。

使用以下一个或多个选项定义每个节点组:

- 设备筛选 (第 33 页)
- 其他筛选 (第 34 页)
- 其他节点 (第 34 页)
- 子节点组 (第 34 页)

设备筛选

设备筛选提供设备类别、供应商、系列或设备配置文件等类别。节点必须与至少一个规范匹配才能属于此节点组。

在发现期间，SOM 通过 SNMP 查询采集直接信息，并通过设备配置文件从中得到其他信息。通过收集系统对象 ID，SOM 可以通过对正确设备配置文件编制索引，得出以下信息:

- 供应商
- 设备类别

- 该类别中的设备系列

这些除设备配置文件自身外得出的值可用作筛选。例如，可以从特定供应商对所有对象分组，而不管设备类型和系列如何。也可以跨供应商对所有某类设备 (如路由器) 分组。

其他筛选

借助此选项，可以使用基于对象属性列表的布尔表达式指定其他筛选。

使用其他筛选编辑器来创建自定义逻辑以匹配字段，包括:

- tenantName (名称)
- securityGroupName (安全组)
- sysName (系统名称)
- sysLocation (系统位置)
- sysContact (系统联系人)
- hostname (主机名，区分大小写)
- hostedIPAddress (地址)
- mgmtIPAddress (管理地址)
- nodeName

筛选可包括 AND、OR、NOT、EXISTS、NOT EXISTS 和分组 (圆括号) 运算。有关详细信息，请参阅 SOM 联机帮助中的“指定节点组其他筛选”。

其他节点

无论使用了何种筛选，此选项均支持将其他节点添加到节点组。

最好使用“其他筛选”限定节点组的节点。如果环境包含很难用筛选限定的关键设备，则按各个主机名将它们添加到某个组。仅在必要时按各个主机名将节点添加到节点组。

子节点组

支持将节点组添加到节点组，以建立层次结构容器。子节点组将被同样视为其他节点。

节点组评估

SOM 将使用以下条件评估每个发现的节点，以确定其节点组成员资格:

- 匹配“设备筛选”选项卡上的一个或多个条目和“其他筛选”选项卡上所指定筛选的任何节点都是节点组成员。
- 在“其他节点”选项卡上指定的所有节点都是节点组的成员。
- 作为“子节点组”选项卡上指定的至少一个节点组成员的所有节点都是节点组的成员。

分组重叠

无论组定义的预定用途是什么，第一步都是定义哪些节点是组的成员。因为您可以创建不同用途的组，所以每个对象都可以包括在多个组中。请考虑以下示例:

- 您可能希望使用“设备配置文件”筛选将所有 HP 3PAR 阵列分组为单个组。
- 顶级元素将自动分配给存储系统的默认节点组。
- 您可能希望从所有存储阵列采集数据，而不管设备供应商或设备系列如何。

具有 IP 地址 10.10.10.3 的 3PAR 阵列能适用于全部三个组。您希望在具有可配置和查看的大量适用组集合与大量从不使用的多余条目使列表过载之间寻求平衡。

层次结构/包含

您可以创建简单且可重用的原子组，并按层次结构将它们结合起来，以供监视或查看。对节点使用层次结构容器会在发生故障时提供有关对象位置或类型的指示，从而极大地增强图视图。SOM 使您能完全控制组定义及其向下钻取顺序。

可以先创建简单可重用的原子组，然后在您构建层次结构时将它们指定为子组。或者，也可以先指定最大的父组，并接着创建子组。

例如，您的环境可能包含 EMC ClARiiON 存储系统和 VNX Filer。可以为 EMC 设备和所有文件存储创建父组。因为层次结构是在创建父组并指派其子组时指定的，所以每个子组 (如 EMC 设备) 都可以有多个父组。

层次结构能很好地适用于以下情况:

- 具有相似监视需要的节点类型
- 要一起隔离的节点类型
- 按操作员工作责任划分的节点组
- 在图视图和表视图中使用组时

注意:请记住，使用组定义指定监视配置时，层次结构不能指示设置的排序。具有最低排序编号的设置将应用于节点。通过小心地递增排序编号，可模拟设置的继承概念。

计划节点组

SOM 提供默认的节点组集合以简化配置任务。可以使用和修改现有组，或创建自己的组。HP 以后可能会添加更多默认组以简化配置任务。

与设备配置文件的交互

发现每个设备时，SOM 使用设备的系统对象 ID 在可用

设备配置文件列表中建立索引。设备配置文件用于派生设备的其他属性，比如供应商、产品系列和设备类别。

当配置节点组时，可以使用这些派生的属性对设备进行分类以应用数据采集设置。例如，可能要在某个间隔采集整个环境中的所有设备的数据而不考虑供应商。可以使用派生的设备类别 (存储系统) 作为节点组的定义特征。系统对象 ID 映射到类别“存储系统”的所有已发现设备都将接收到节点组的已配置设置。

计划注意事项

确定要对节点进行分组的条件。以下是计划节点组时要考虑的一些因素:

- 哪些是要采集数据的关键设备?
- 是否要按设备类型区分数据采集间隔或收集的数据?
- 是否可以使用 SOM 提供的默认节点组?

关于计划节点组的建议

为环境计划节点组时需要考虑以下关键点:

- 记住，节点组会增加系统开销。因此，请确保在创建节点组时拥有基于需求的有效用例。
- 创建适合明确用途的节点组。在开始计划节点组之前，标识最常使用的用例。例如，您可以创建节点组，用于管理 Windows 主机、Linux 主机或基于供应商、型号或设备配置文件管理存储设备。然后将数据采集或监视策略附加到这些节点组。
- 将不同的节点组用于不同的用途。并非所有为数据采集而创建的节点组都可用于筛选视图或限制节点访问。因此，您将需要根据用途单独配置它们。
- 在创建大量组集合用于监视和查看用途以及不在系统中包含大量从不使用的节点组以避免过载之间找到平衡。
- 不要经常使用“其他节点”选项卡将节点添加到节点组，因为它会占用管理服务器上的大量资源。一般来说，节点组定义应受筛选驱动，并且此功能应作为例外使用。

发现

组成存储区域网络 (SAN) 的设备必须能够被发现，以便 SOM 进行监视和管理。要发现网络中的设备，必须配置要发现的地址，并根据需要提供凭据。

开始计划之前需了解以下发现相关说明:

- SOM 不执行任何默认发现。您必须在库存视图中出现任何元素之前配置发现。
- 发现是按单个地址处理的。配置的每个发现地址的状态指示发现是否成功。
- 初始发现过程需要一些时间，具体取决于已配置的发现地址数。
- 可以创建凭据，然后将凭据关联到多个地址。
- 可以使用“发现提示”选项选择一个值，根据此值，SOM 只调用选定提供程序以发现设备而不是调用所有提供程序，从而缩短发现时间。

发现方法

SOM 提供以下发现方法。

方法	备注
自动发现 (*仅限初始发现*)	初始发现的默认方法。 一次可以发现多个元素。
手动发现	只能发现一个元素。
从文件导入地址	以前安装中的发现设置。

自动发现

对于初始发现，这是建议的默认方法。要发现大量地址时，此方法最适合。预配置时间过后，添加或导入的发现地址将进入发现队列中。

自动发现的相关说明

- 仅在初始发现期间运行一次
- 允许一次发现多个设备，以及扫描一系列 IP 地址。

手动发现

当需要添加单个元素或者要发现的元素比较少时，此方法最适合。在开始发现之前，必须关联特定于设备的凭据。尽管通过此方法可以更严格地控制发现，但是在有大量的地址要发现时，此方法非常耗时。

从文件导入发现设置

如果您具有以前安装中的发现设置，则可以将其导入到管理服务器而不是重新输入信息。导入发现设置功能支持您导入以下信息:

- 要发现的 IP 地址
- 默认用户名和密码 (已加密)
- 无代理主机推断规则

导入的相关说明:

- 要防止为每个管理服务器实例重新输入信息，可以为多个管理服务器实例导入同一个文件。
- 导入文件时，将覆盖以前的设置。
- 如果您在尝试导入发现设置时收到错误消息，请验证您使用的密码是否正确。如果使用的密码正确，则可能是文件已损坏。

当导入发现设置文件时，将触发地址的自动发现。如果不想使用自动发现，可以禁用此选项。

主机发现

SOM 提供以下方法发现和管理主机及其与存储设备的关联。

发现方法	描述
使用 CIM 扩展发现	通过在主机上安装 CIM 扩展来管理主机。
无代理发现	未安装 CIM 扩展的情况下管理主机。
推断的无代理发现	未安装 CIM 扩展的情况下，根据主机安全组、区域和区域别名从主机收集信息。

使用 CIM 扩展发现

SOM CIM 扩展是在存储主机上运行的采集代理，用于收集有关该主机的信息。在发现和管理主机时，SOM 管理服务器将与 CIM 扩展通信。在要管理的每个主机上安装 CIM 扩展。CIM 扩展必须正在运行，管理服务器才能从主机获取信息。

如果在发现主机后更改主机密码，则必须在发现列表中更改此主机的密码，然后必须停止并重新启动该主机上运行的 CIM 扩展再运行发现。

无代理发现

使用无代理发现，管理服务器可以在主机上未安装 CIM 扩展的情况下发现主机。管理服务器支持对 Microsoft Windows、Linux 操作系统和 Solaris 系统上运行的主机进行无代理发现。

管理服务器使用以下服务发现主机:

- Windows Management instrumentation (WMI)，用于发现 Windows 主机。
- 安全 Shell (SSH)，用于发现 Linux 主机。

仅当要发现的主机上未运行 CIM 扩展时，无代理发现才工作。如果管理服务器发现在主机上运行的 CIM 扩展，则默认情况下，它首选使用 CIM 扩展发现而不是无代理发现。

您也可以使用无代理发现来重新发现已使用 CIM 扩展在管理服务器中发现的主机。但是，与主机以及主机上的应用程序关联的所有历史记录信息将从管理服务器中删除。

从主机采集的数据取决于用于从主机收集信息的发现方法。下表汇总了根据发现方法采集的主机数据。使用此表作为指南，计划您的主机发现方法。

推断的无代理发现

SOM 可以在未安装 CIM 扩展的情况下显示和收集主机信息。通过根据在 SAN 中的存储系统和构造上配置的主机安全组、区域或区域别名创建规则，您可以推断无代理主机。推断主机之后，您可以通过提供凭据发现主机。如果发现成功，则会协调所有主机，且推断的主机将成为被管主机。

从主机采集的数据因发现方法不同而异。可以根据要从主机采集的数据类型来计划主机发现。

无代理发现的功能

管理服务器从使用无代理发现功能发现的主机收集以下信息:

- 主机与应用程序、存储和网络设备的关联。
- IP/DNS 相关的信息。
- 收集每个主机的详细配置信息。
- 逻辑存储卷信息，包括安装点、物理设备、驱动器类型和文件系统详细信息。
- 磁盘分区信息，包括磁盘分区名称、映射的逻辑卷、映射的物理驱动器和总容量。
- 磁盘驱动器信息，包括驱动器名称、SCSI 总线信息和映射的磁盘分区。
- 多路径和卷管理器配置详细信息。
- HBA 的相关信息。

无代理发现的限制

尽管无代理发现使管理服务器能够发现和找到大量与主机相关的信息，但是它具有一些限制。

注意: 提到的所有限制都可以通过在主机上安装 CIM 扩展克服。

如果发现过程中提供无代理发现提示，则 SOM 将使用运行 CIM 扩展的主机上的无代理配置发现 Windows 主机。

下面基于无代理主机运行的操作系统列出了其限制:

Windows 主机的限制

- 没有管理员特权的用户帐户无法发现 Windows 主机。
- 不提供公用文件夹和邮箱信息。
- 使用本机卷管理器卷获取数据时，仅提供与磁盘分区和磁盘驱动器相关的有限信息。这是因为管理服务器不支持本机卷管理器软件 Microsoft Virtual Disk Service Dynamic Provider。

Linux 主机的限制

- 对于非根用户帐户，不提供以下信息:
  - 不提供与 Veritas DMP 设备相关的信息。
  - 不提供与系统的序列号和制造商相关的信息。
  - 不提供与磁盘驱动器和磁盘分区相关的信息。
- 对于 Linux 主机，不提供以下性能度量:
  - 磁盘读取
  - 磁盘总数
  - 磁盘利用率
  - 磁盘写入
  - 处理器利用率
- 无代理发现所获得的目标映射的数量可能少于 CIM 扩展返回的目标映射数量。之所以存在这种差异，其原因在于某些 SCSI LUN 值为零的目标映射条目未显示。
- 据观察，包含在管理服务器中发现的 HBA 的 Linux 主机存在以下问题:
  - 对于 HBA，不提供以下信息:
    - 供应商名称
    - 序列号
    - 硬件版本
    - HBA 端口属性页面上的端口类型信息。
  - 当您尝试使用 CIM 扩展重新发现无代理主机时，管理服务器不会根据使用 CIM 扩展获取的信息调整在无代理发现过程中获取的 HBA 信息。将删除使用无代理发现获取的旧 HBA 数据，并使用 CIM 扩展发现采集 HBA 的新信息。因此，使用 CIM 扩展重新发现主机时，与 HBA 相关的所有自定义信息均会删除。
  - 对于包含具有双端口适配器的 HBA 的 Linux 主机，每个端口在 HBA 适配器页面上均显示为单独的适配器，而每个适配器在 HBA 端口页面上均映射到其端口。
  - 执行以下操作时，绑定页面不会更新:
    - 禁用 LUN 的路径。
    - 禁用 HBA 端口。
    - 运行后续数据采集。

此限制可以通过重新启动主机消除。重新启动主机时，绑定页面会自动更新。

租户和初始发现安全组分配

SOM 在存储网络环境中发现元素时，按以下方式建立租户和安全组设置:

提供要发现的地址时，为每个发现地址指定租户。系统为成功发现的 IP 地址自动创建节点。定义租户时，必须指定初始发现安全组。与所定义租户关联的新建节点将映射到与选定租户关联的安全组 (初始发现安全组)。管理员可以随时更改节点的租户和/或安全组分配。

分配到默认安全组的节点在所有视图中可见。要控制对某设备的访问，请将该设备分配到默认安全组以外的安全组。

可以将一个租户中的节点分配到不同的安全组，也可以将一个安全组中的节点分配到不同的租户。

考虑设置安全配置，以便所有新发现节点属于映射到用户组 = SOM 管理员的安全组。这些节点将仅对 SOM 管理员可见，直到管理员将节点特意移动到还对相应 SOM 操作员或来宾可见的安全组中。

租户分配可用于识别网络环境中的节点组。安全组分配允许管理员在 SOM 控制台中将节点限制为只对特定用户组可见。

主机群集

管理服务器完全支持群集管理。群集支持包括下列功能:

- 群集被识别为被管元素。
- 准确报告群集容量利用率。
- 管理服务器支持自动发现若干常用的群集服务器。

关于计划发现的建议

为存储环境计划发现时需要考虑以下关键点:

在用户界面中一次可启动发现地址的最大数目为 1000。要配置超过此数目的地址数，请使用 `somdiscoveryconfigexportimport.ovpl` 命令。

- 要配置批量发现，请在 `ovjboss.jvmargs` 文件中设置以下两个属性。
  - da.bulkDiscoveryQueueSize 默认值:100
  - da.bulkDiscoveryIntervalInSeconds 默认值:20

  该文件位于 `<安装目录>\HP\HP BTO Software\shared\nnm\conf\props\ovjboss.jvmargs`
- 计划发现顺序，确保依次发现交换机、存储系统和主机。这有助于缩短实现连接信息价值的时间。
- 使用“队列发现”选项可自动执行发现过程，而无需手动发现每个地址。
- SOM 需要运行良好的数据库和足够的磁盘空间才能正常工作。如果包括要发现的管理服务器地址并发现管理服务器，则 SOM 将监视其自己的运行状况。您可以使用“系统信息”页面上的“运行状况”选项卡查看产品运行状况。
- 发现的每个节点 (物理或虚拟) 都会计入许可证限制数。许可证的容量可能影响发现方式。

关于数据采集策略的建议

进行数据采集配置时需要考虑以下关键点:

- 为了在尽量减小系统过载的情况下有效采集数据，请将中断期间设置为小于等于新鲜度间隔的一半。例如，如果新鲜度间隔为 24 个小时，则中断期间不应超过 12 个小时。
- 最好确保数据采集不会因为一些非常基础的原因 (如提供程序问题、凭据无效、网络问题和其他类似问题) 而失败。这些失败会增加不必要的系统过载，因为隔离元素之前至少会再重试一次数据采集。隔离此类元素后，请访问采集仪表板中的“失败”饼图，查找报告这些错误的元素。采取适当的操作确保后续的数据采集成功完成，然后手动取消隔离元素。
- 向策略分配优先级时，不要使用连续顺序的数字，例如 0、1、2、3、4、5 等等。最好使用正整数的倍数来设置优先级。例如，使用 5 的倍数作为优先级，如 5、10、15、20，以此类推。假定您要修改优先级为 10 的策略。可以将优先级更改为任何数值，如 12。这种做法在无需更改具有最邻近优先级的所有策略的优先级时很有用。

关于监视性能的建议

以下是在配置监视策略时需要考虑的一些建议:

- 创建过多监视策略会增加系统开销。应仅为设备和这些设备上要监视的度量创建监视策略。
- 创建策略期间设置的默认间隔为 15 分钟。建议间隔不要小于 15 分钟，否则会使系统过载。如果使用的间隔必须小于 15 分钟，则强烈建议将此间隔应用于一组非常有限的设备，并尽早将其更改为默认间隔。
- 向策略分配优先级时，不要使用连续顺序的数字，例如 0、1、2、3、4、5 等等。最好使用正整数的倍数来设置优先级。例如，使用 5 的倍数作为优先级，如 5、10、15、20，以此类推。假定您要修改优先级为 10 的策略。可以将优先级更改为任何数值，如 12。这种做法在无需更改具有最邻近优先级的所有策略的优先级时很有用。
- 由于度量采集是策略驱动的，因此请使用精心计划的方法来优化度量采集:
  - 通过标识环境中的高优先级设备，有效地计划节点组。例如，逻辑上与节点组相关的组收集器不会将主机收集器关联到存储系统节点组。
  - 如上所述，合理地设置计划间隔。
  - 在环境中配置监视策略前，确保已针对大部分环境完成一轮数据采集。可从采集状态仪表板中对此进行验证。一般来说，不要在有大量数据采集处于 ‘正在运行’ 状况时配置监视策略。

基于 LDAP 的身份验证

本章包含将 SOM 与目录服务集成以合并存储用户名、密码和 (可选) SOM 用户组分配的相关信息。它包含以下主题:

SOM 用户访问信息和配置选项

以下各项将结合在一起定义 SOM 用户:

- **用户名**唯一标识 SOM 用户。用户名用于访问 SOM 并接收事件分配。
- **密码**与用户名关联，以控制对 SOM 控制台或 SOM 命令的访问。
- **SOM 用户组**成员资格控制所提供的信息以及用户可以在 SOM 控制台中执行的操作类型。用户组成员资格还控制 SOM 命令对于用户是否可用。

如果已将 LDAP 配置为 SOM 的目录服务，则必须选择外部模式进行用户身份验证。

用户帐户	密码	用户组	用户组成员资格
目录服务	目录服务	SOM	目录服务

外部模式:目录服务中的所有 SOM 用户信息

使用此选项，SOM 将访问目录服务以获取全部用户访问信息，此信息是在 SOM 外部定义的并且对其他应用程序可用。一个或多个目录服务组中的成员资格确定用户所在的 SOM 用户组。

SOM 用户访问信息的配置和维护是共同执行的，如此处所述:

- 目录服务管理员在目录服务中维护用户名、密码和组成员资格。
- SOM 管理员在 SOM 控制台中将目录服务组映射到 SOM 用户组。
- SOM 管理员将配置 SOM `ldap.properties` 文件，以针对用户名和组向 SOM 描述目录服务数据库架构。

HP 建议使用以下配置过程:

1. 配置并验证目录服务中的 SOM 用户名和密码检索。
2. 配置目录服务中的 SOM 用户组检索。

有关与目录服务集成以获取全部用户信息的信息，请参阅本章的其余部分以及 *SOM* 帮助。

配置 SOM 访问目录服务

目录服务访问在 `ldap.properties` 文件中配置。要配置目录服务中的用户访问，请执行适合您的目录服务的步骤。

- 用于 Microsoft Active Directory 的步骤
- 用于其他目录服务的步骤
- 将目录服务组映射到 SOM 用户组 (第 44 页)

用于 Microsoft Active Directory 的步骤

1. 备份 SOM 附带的 `ldap.properties` 文件，然后在任何文本编辑器中打开此文件。
2. 用以下文本覆盖文件内容:

   ```
   java.naming.provider.url=ldap://<我的 LDAP 服务器>:389/
   bindDN=<我的域>\\<我的用户名>
   bindCredential=<我的密码>
   baseCtxDN=CN=Users,DC=<我的主机名>,DC=<我的公司名>,DC=<我的后缀>
   baseFilter=CN={0}
   defaultRole=guest
   #rolesCtxDN=CN=Users,DC=<我的主机名>,DC=<我的公司名>,DC=<我的后缀>
   roleFilter=member={1}
   uidAttributeID=member
   userRoleFilterList=admin;level2;level1
   ```

3. 指定用于访问目录服务的 URL。在以下行中:

   ```
   java.naming.provider.url=ldap://<我的 LDAP 服务器>:389/
   ```

   将 *<我的 LDAP 服务器>* 替换为 Active Directory 服务器的完全限定主机名 (例如:`myserver.example.com`)。

   提示: 要指定多个目录服务 URL，请用一个空格字符 ( ) 分隔每个 URL。

4. 指定有效目录服务用户的凭据。在以下行中:

   ```
   bindDN=<我的域>\\<我的用户名>
   bindCredential=<我的密码>
   ```

   执行以下替换:

   - 将 *<我的域>* 替换为 Active Directory 域的名称。
   - 将 *<我的用户名>* 和 *<我的密码>* 替换为用于访问 Active Directory 服务器的用户名和密码。

5. 指定用于存储用户记录的那部分目录服务域。在以下行中:

   ```
   baseCtxDN=CN=Users,DC=<我的主机名>,DC=<我的公司名>,
     DC=<我的后缀>
   ```

   将 *<我的主机名>*、*<我的公司名>* 和 *<我的后缀>* 替换为 Active Directory 服务器的完全限定主机名的各个部分 (例如，对于主机名 `myserver.example.com`，指定:`DC=myserver,DC=example,DC=com`)。

用于其他目录服务的步骤

1. 备份 SOM 附带的 `ldap.properties` 文件，然后在任何文本编辑器中打开此文件。
2. 指定用于访问目录服务的 URL。在以下行中:

   ```
   #java.naming.provider.url=ldap://<我的 LDAP 服务器>:389/
   ```

   执行以下操作:

   - 取消代码行的注释 (方法是删除 # 字符)。
   - 将 *<我的 LDAP 服务器>* 替换为目录服务器的完全限定主机名 (例如:`myserver.example.com`)。

提示: 要指定多个目录服务 URL，请用一个空格字符 ( ) 分隔每个 URL。

3. 指定用于存储用户记录的那部分目录服务域。在以下行中:

   `baseCtxDN=ou=People,o=myco.com`

   将 `ou=People,o=myco.com` 替换为存储用户记录的那部分目录服务域。
4. 指定用于登录到 SOM 的用户名的格式。在以下行中:

   `baseFilter=uid={0}`

   将 `uid` 替换为目录服务域中的用户名属性。

将目录服务组映射到 SOM 用户组

复制 SOM 中 LDAP 组的 DN。通过目录服务名称将 SOM 中的 admin、level1 或 level2 角色映射到 LDAP 组。

1. 在 SOM 控制台中，将预定义 SOM 用户组映射到其在目录服务中的对应方:
   a. 从工作区导航面板，选择“配置”>“安全性”>“用户组”。将显示“用户组”视图。
   b. 双击 admin 行。
   c. 在“目录服务名称”字段中，输入 SOM 管理员的目录服务组的完整可分辨名称 (DN)。
   d. 单击“保存并关闭”。
   e. 对于每个 guest、level1 和 level2 行，重复步骤 b 到步骤 d。

   提示:这些映射提供 SOM 控制台访问。访问 SOM 控制台的每个用户所在的目录服务组必须映射到此步骤中指定的某一预定义 SOM 用户组。
2. 对于目录服务中包含一个或多个 SOM 用户的其他组，请在 SOM 控制台中新建用户组:
   a. 从工作区导航面板，选择“配置”>“安全性”>“用户组”。将显示“用户组”视图。
   b. 单击“新建”，然后输入组的信息:
      - 将 Unique Name 设置为任何唯一值。建议使用短名称。
      - 将“显示名称”设置为应该向用户显示的值。
      - 将“目录服务名称”设置为目录服务组的完整可分辨名称。
      - 将“描述”设置为描述此 SOM 用户组用途的文本。
   c. 单击“保存并关闭”。
   d. 对于 SOM 用户的每个额外目录服务组，重复步骤 b 和步骤 c。

安全性

在 SOM 中提供了安全和多租户模型，用于限制用户对 SOM 数据库中对象信息的访问。对于自定义操作员的责任区域视图，此限制很有用。它还通过 SOM 的按组织配置支持服务提供程序。

默认情况下，所有控制台用户都可以查看 SOM 数据库中所有对象的信息。如果环境可接受此默认配置，则无需阅读此部分。

此部分着重介绍 SOM 安全和租户模型，并提供配置建议和示例。涵盖以下主题:

- SOM 安全模型 (第 45 页)
- SOM 租户模型 (第 49 页)
- 一些安全配置示例 (第 52 页)

SOM 安全模型

SOM 安全模型提供对 SOM 数据库中的对象的用户访问控制。此模型适用于需要限制 SOM 用户对特定对象进行访问的任何网络管理组织。SOM 安全模型具有以下好处:

- 提供用于限制 SOM 控制台操作员网络视图的方式。操作员可以侧重于特定设备类型或网络区域。
- 用于自定义操作员对 SOM 拓扑的访问。可以按节点配置操作员访问级别。
- 简化了符合安全配置的节点组的配置和维护。
- 可以独立于 SOM 租户模型单独使用。

安全组

在 Storage Operations Manager 安全模型中，通过用户组和安全组间接控制用户对节点的访问。拓扑中的每个节点只与一个安全组相关联。一个安全组可以与多个用户组相关联。

每个用户帐户都映射到以下用户组:

- 一个或多个以下默认用户组:
  - 管理员
  - 全局操作员
  - 第 1 级操作员
  - 第 2 级操作员
  - 来宾用户

  此映射是 SOM 控制台访问必需的，并可确定哪些操作在 SOM 控制台内可用。如果用户帐户映射到以上多个 SOM 用户组，则用户将接收所允许操作的超集。

  注意: 全局操作员用户组仅授予对拓扑对象的访问。一个用户必须分配到其他某个用户组 (第 1 级、第 2 级或来宾) 后，才能访问控制台。

  管理员不应将全局操作员用户组映射到任何安全组，因为默认情况下，此用户组映射到所有安全组。
- (*可选*) 映射到安全组的自定义用户组。
  这些映射提供对 Storage Operations Manager 数据库中的对象的访问。每个映射包括适用于安全组节点的对象访问特权级别。

默认安全组

在新安装中，默认安全组是所有节点的初始安全组分配。默认情况下，所有用户都可以查看默认安全组中的所有对象。您可以控制节点到默认安全组的配置，以及用户对默认安全组中的对象的访问。

关于计划安全组的建议

- 将每个用户帐户只映射到一个默认用户组。
- 不要将默认用户组映射到安全组。

- 由于映射到管理员用户组的任何用户帐户都可以对 SOM 数据库中的所有对象进行管理员级别的访问，因此不要将此用户帐户映射到任何其他用户组。
- 通常，应将相关元素配置为属于同一安全组。相关元素的一些示例包括:
  - 如果某个虚拟机属于某个安全组，则该虚拟机的虚拟服务器也应在该安全组中。
  - 属于远程复制对的存储卷所在的阵列应包含在同一个组中。
  - 提供后端存储的阵列应与存储仿真器处于同一个安全组中。
  - 群集成员和群集应包含在同一个组中。
  - 从阵列为主机提供存储时，主机、阵列和路径中的构造元素需包含在同一个组中。
  - 物理交换机中包含的虚拟交换机也应映射到同一个安全组。

用于计划安全组的示例方法

下面概述了用于计划安全组配置的高级步骤:

1. 分析被管网络拓扑以确定用户需要访问的节点组。
2. 删除默认用户组与默认安全组和“未解析事件”安全组之间的默认关联。
   完成此步骤确保用户不会无意中获取他们不应当管理的节点的访问权。此时，仅管理员可以访问拓扑中的对象。
3. 为节点的每个子集配置安全组。请记住: 给定节点只能属于一个安全组。
   a. 创建安全组。
   b. 将相应的节点分配到每个安全组。
4. 配置自定义用户组。
   a. 对于每个安全组，针对用户访问权的每个级别配置用户组。
      - 如果在 Storage Operations Manager 数据库中存储用户组成员资格，则还没有向这些用户组映射任何用户。
      - 如果在目录服务中存储用户组成员资格，则将每个用户组的“目录服务名称”字段设置为目录服务中该组的可分辨名称。

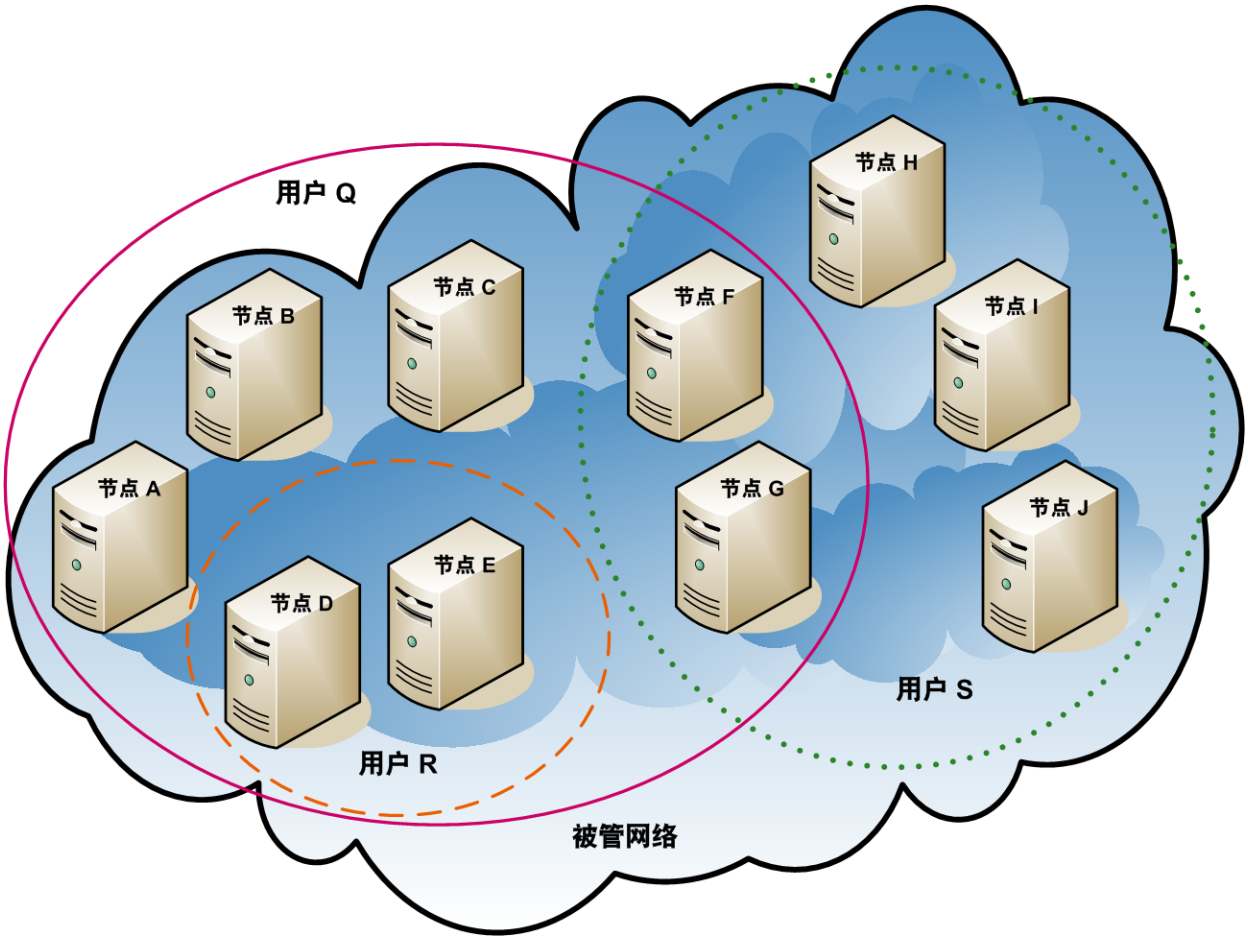
   b. 将每个自定义用户组映射到正确的安全组。为每个映射设置相应的对象访问特权。
5. 配置用户帐户。
   - 如果在 Storage Operations Manager 数据库中存储用户组成员资格，则执行以下操作:
     - 为可以访问控制台的每个用户创建用户帐户对象。(配置用户帐户的过程取决于是否使用目录服务登录 Storage Operations Manager 控制台。)
     - 将每个用户帐户映射到一个默认用户组 (用于访问控制台)。
     - 将每个用户帐户映射到一个或多个自定义用户组 (用于访问拓扑对象)。
   - 如果在目录服务中存储用户组成员资格，请验证每个用户是否属于一个默认用户组和一个或多个自定义用户组。
6. 验证配置。
7. 维护配置。
   - 监视添加到默认安全组的节点，并将这些节点移到正确的安全组。
   - 将新的控制台用户添加到正确的用户组。

安全组结构示例

下图中的三个椭圆表示用户需要查看此 Storage Operations Manager 拓扑示例中的节点的主分组。要获取完全用户访问控制，四个唯一子组的每一个都需要对应于唯一的安全组。每个唯一安全组可以映射到一个或多个用户组，以表示对该安全组中对象的可用用户访问级别。

安全组映射示例列出了此拓扑的安全组和可能的自定义用户组之间的映射。(此安全模型的实际实现可能不需要所有这些自定义用户组。)用户帐户映射示例列出了此拓扑的几个用户帐户和用户组之间的映射。

用户访问要求的拓扑示例



安全组映射示例

安全组	安全组的节点	用户组	对象访问特权
SG1	A、B、C	UG1 管理员	管理员对象
		UG1 第 2 级操作员	第 2 级操作员对象
		UG1 第 1 级操作员	第 1 级操作员对象
		UG1 来宾	来宾对象

安全组映射示例(续)

安全组	安全组的节点	用户组	对象访问特权
SG2	D、E	UG2 管理员	管理员对象
		UG2 第 2 级操作员	第 2 级操作员对象
		UG2 第 1 级操作员	第 1 级操作员对象
		UG2 来宾	来宾对象
SG3	F、G	UG3 管理员	管理员对象
		UG3 第 2 级操作员	第 2 级操作员对象
		UG3 第 1 级操作员	第 1 级操作员对象
		UG3 来宾	来宾对象
SG4	H、I、J	UG4 管理员	管理员对象
		UG4 第 2 级操作员	第 2 级操作员对象
		UG4 第 1 级操作员	第 1 级操作员对象
		UG4 来宾	来宾对象

用户帐户映射示例

用户帐户	用户组	节点访问	备注
用户 Q	SOM 第 2 级操作员	无	此用户对粉红色椭圆 (实线) 中的节点具有第 2 级操作员访问权。
	UG1 第 2 级操作员	A、B、C	
	UG2 第 2 级操作员	D、E	
	UG3 第 2 级操作员	F、G	
用户 R	SOM 第 1 级操作员	无	此用户对橙色椭圆 (虚线) 中的节点具有第 1 级操作员访问权。
	UG2 第 1 级操作员	D、E	
用户 S	SOM 第 2 级操作员	无	此用户对绿色椭圆 (点线) 中的节点具有第 2 级操作员访问权。
	UG3 第 2 级操作员	F、G	
	UG4 第 2 级操作员	H、I、J	

用户帐户映射示例(续)

用户帐户	用户组	节点访问	备注
用户 T	SOM 第 2 级操作员	无	此用户对拓扑示例中的所有节点具有访问权 (特权级别可以变化)。 此用户具有对节点 D 和 E 的管理访问权，但看不到需要管理访问权的工具的菜单项。如果此用户有权访问管理服务器，则此用户可以仅对节点 D 和 E 运行需要管理访问权的命令行工具。
	UG1 来宾	A、B、C	
	UG2 管理员	D、E	
	UG3 第 2 级操作员	F、G	
	UG4 第 1 级操作员	H、I、J	

SOM 租户模型

Storage Operations Manager 租户模型可将拓扑发现和数据严格分离到租户 (也称为组织或客户) 中。此模型适合供服务提供程序 (尤其是被管服务提供程序和大型企业) 使用。

Storage Operations Manager 租户模型具有以下好处:

- 标记每个节点属于的组织。
- 满足限制操作员对客户数据的访问权限的调整要求。
- 简化了符合租户配置的节点组的配置和维护。
- 简化了安全配置。

租户

SOM 租户模型在安全配置中引入了组织的理念。拓扑中的每个节点仅属于一个租户。租户提供 Storage Operations Manager 数据库中的逻辑分离。通过安全组管理对象访问。

对于每个节点，首次发现节点并将其添加到 Storage Operations Manager 数据库时，进行初始发现租户分配。Storage Operations Manager 将发现的所有节点分配到默认租户。因此，如果使用安全模型而未配置任何租户，则所有节点都会分配到默认租户。默认情况下，所有用户都有权访问 (通过默认安全组) 与此租户关联的所有对象。管理员可以在发现后随时更改节点的租户。

每个租户定义包括一个初始发现安全组，即默认安全组。Storage Operations Manager 将节点与默认租户一起分配到默认安全组。管理员可以在发现后随时更改节点的安全组。

注意:更改节点的租户时，不会自动更改节点的安全组。

关于计划租户的建议

请在计划租户配置时考虑以下建议:

- 在发现期间配置租户可以降低手动将发现的元素分配到各个租户的管理开销。
- 对于小型组织，每个租户一个安全组可能已足够。

- 可能希望将大组织细分为多个安全组。
- 要防止用户跨组织访问节点，请确保每个安全组仅包含一个租户的节点。

用于计划租户的示例方法

下列步骤概述了用于计划和配置多租户的高级方法:

1. 分析客户需求以确定在 Storage Operations Manager 环境中需要多少租户。
   建议仅在通过单个管理服务器管理多个单独网络时使用租户。
2. 分析被管拓扑以确定哪些节点属于每个租户。
3. 分析每个租户的拓扑以确定 Storage Operations Manager 用户需要访问的节点组。
4. 删除默认用户组与默认安全组和“未解析事件”安全组之间的默认关联。

   完成此步骤确保用户不会无意中获取他们不应当管理的节点的访问权。此时，仅管理员可以访问拓扑中的对象。
5. 创建识别的安全组和租户。
   对于每个租户，将初始发现安全组设置为默认安全组或具有受限访问权的租户特定安全组。此方法确保租户的新节点在一般情况下不可见，除非管理员配置了访问权。
6. 将租户分配到种子，准备发现。

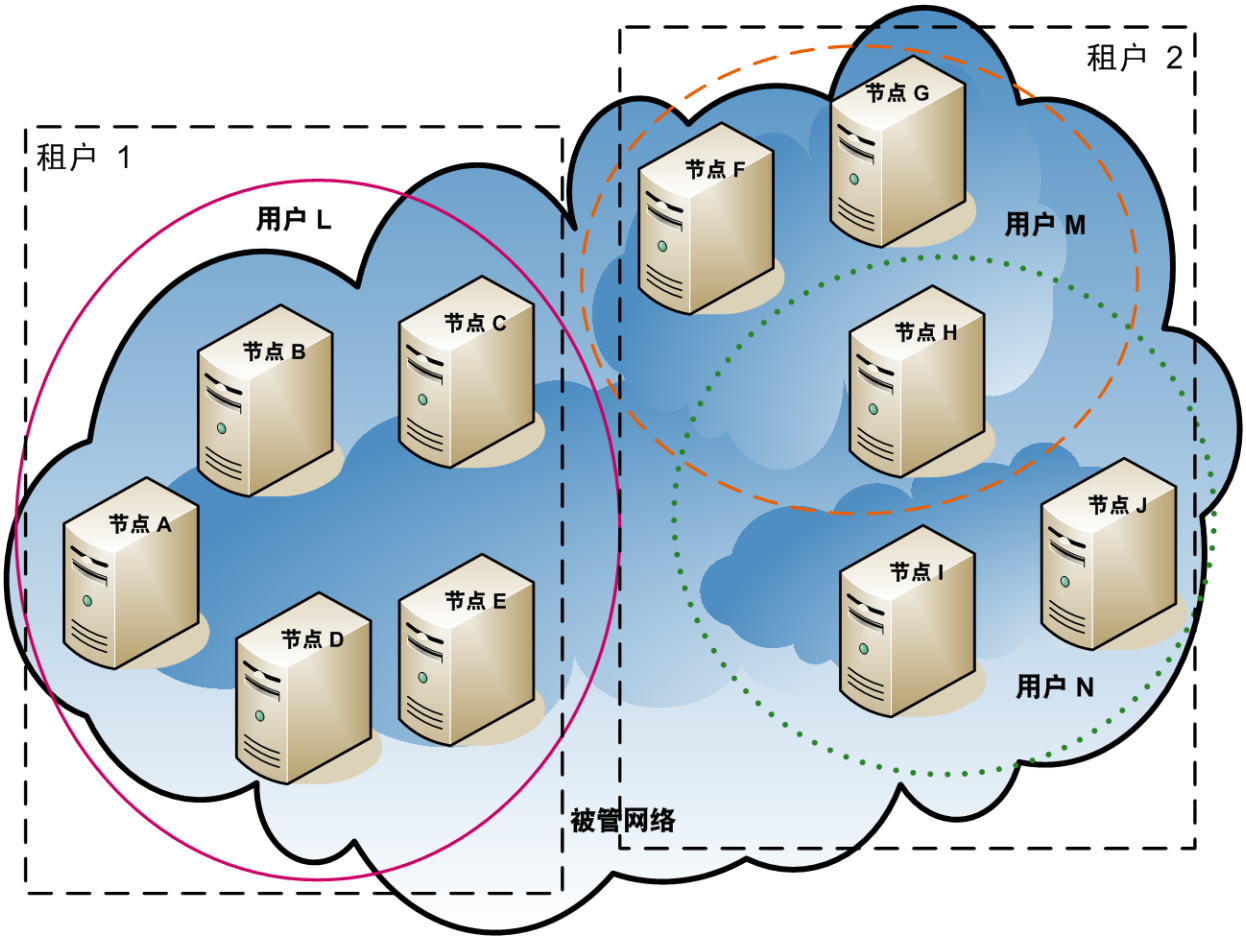
   提示:发现一组节点之后，可以更改初始发现安全组的值。使用此方法限制将节点手动重新分配到安全组。
7. 发现完成后，执行以下操作:
   a. 验证每个节点的租户，并根据需要进行更改。
   b. 验证每个节点的安全组，并根据需要进行更改。

租户结构示例

下图显示了包含两个租户 (用矩形表示) 的 Storage Operations Manager 拓扑示例。三个椭圆表示用户需要查看其节点的主分组。租户 1 的拓扑作为一个组进行管理，因此它仅需要一个安全组。租户 2 的拓扑在重叠集合中管理，因此它被分隔为三个安全组。

多租户安全组映射示例列出了此拓扑的安全组和可能的自定义用户组之间的映射。(此安全模型的实际实现可能不需要所有这些自定义用户组。)多租户用户帐户映射示例列出了此拓扑的几个用户帐户和用户组之间的映射。

多租户拓扑示例



多租户安全组映射示例

安全组	安全组的节点	用户组	对象访问特权
T1 SG	A、B、C、D、E	T1 管理员	管理员对象
		T1 第 2 级操作员	第 2 级操作员对象
		T1 第 1 级操作员	第 1 级操作员对象
		T1 来宾	来宾对象
T2 SGa	F、G	T2_a 管理员	管理员对象
		T2_a 第 2 级操作员	第 2 级操作员对象
		T2_a 第 1 级操作员	第 1 级操作员对象
		T2_a 来宾	来宾对象

多租户安全组映射示例(续)

安全组	安全组的节点	用户组	对象访问特权
T2 SGb	H	T2_b 管理员	管理员对象
		T2_b 第 2 级操作员	第 2 级操作员对象
		T2_b 第 1 级操作员	第 1 级操作员对象
		T2_b 来宾	来宾对象
T2 SGc	I、J	T2_c 管理员	管理员对象
		T2_c 第 2 级操作员	第 2 级操作员对象
		T2_c 第 1 级操作员	第 1 级操作员对象
		T2_c 来宾	来宾对象

多租户用户帐户映射示例

用户帐户	用户组	节点访问	备注
用户 L	SOM 第 2 级操作员	无	此用户对粉红色椭圆 (实线) 中的节点具有第 2 级操作员访问权，此椭圆将所有节点分组为租户 1。
	T1 第 2 级操作员	A、B、C、D、E	
用户 M	SOM 第 1 级操作员	无	此用户对橙色椭圆 (虚线) 中的节点具有第 1 级操作员访问权，此椭圆将一部分节点分组为租户 2。
	T2_a 第 1 级操作员	F、G	
	T2_b 第 1 级操作员	H	
用户 N	SOM 第 2 级操作员	无	此用户对绿色椭圆 (点线) 中的节点具有第 2 级操作员访问权，此椭圆将一部分节点分组为租户 2。
	T2_b 第 2 级操作员	H	
	T2_c 第 2 级操作员	I、J	

一些安全配置示例

以下示例显示了可能的安全策略。将这些示例用作配置安全性的准则。请选择最符合您的安全配置要求的示例:

- 示例:将节点访问划分为两个或更多个用户组 (第 52 页)
- 示例:允许一部分用户访问一部分节点 (第 54 页)

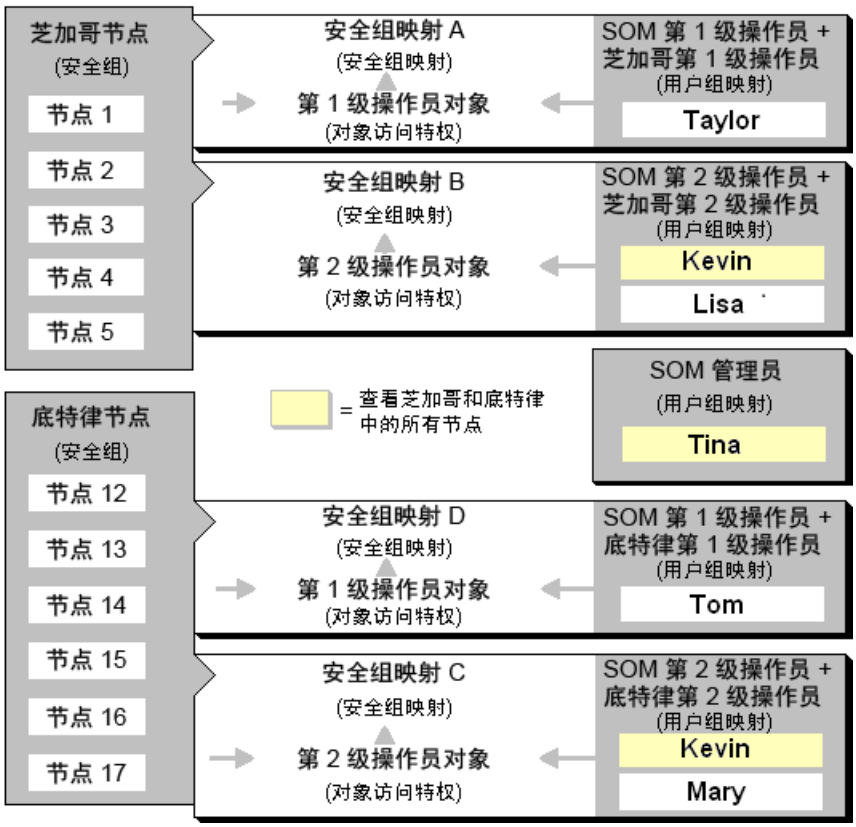
示例:将节点访问划分为两个或更多个用户组

此示例配置安全性，基于以下位置划分网络监视职责:

- 芝加哥
- 底特律

每个位置包括第 1 级操作员 (访问特权限制多于第 2 级操作员) 和第 2 级操作员。Tina 是管理员，负责处理上述两个位置的网络监视。Kevin 是芝加哥和底特律的后备人员，必须访问位于芝加哥和底特律的节点。

下图演示了安全要求:



下表列出了每个位置的 SOM 控制台 (SOM 用户组) 和节点访问要求 (用户组、对象访问特权和安全组)。

注意: 如果希望所有操作员都看到所有菜单选项，但只能基于自身的对象访问特权运行这些选项，则可以将所有操作员都设为 SOM 第 2 级操作员。

安全配置示例

用户帐户	SOM 用户组	用户组	对象访问特权	安全组
Tina	SOM 管理员	不适用。SOM 管理员可以访问所有节点。	不适用。SOM 管理员有所有节点的管理员特权。	不适用。SOM 管理员可以访问所有节点。
Kevin	SOM 第 2 级操作员	芝加哥第 2 级操作员 底特律第 2 级操作员	第 2 级操作员对象	芝加哥节点，底特律节点
Lisa	SOM 第 2 级操作员	芝加哥第 2 级操作员	第 2 级操作员对象	芝加哥节点

安全配置示例(续)

用户帐户	SOM 用户组	用户组	对象访问特权	安全组
Taylor	SOM 第 1 级操作员	芝加哥第 1 级操作员	第 1 级操作员对象	芝加哥节点
Mary	SOM 第 2 级操作员	底特律第 2 级操作员	第 2 级操作员对象	底特律节点
Tom	SOM 第 1 级操作员	底特律第 1 级操作员	第 1 级操作员对象	底特律节点

要设置芝加哥和底特律的安全，请执行以下步骤:

- 删除到默认用户组的默认安全组映射: 第 1 级操作员、第 2 级操作员和来宾用户。

  注意: 将默认用户组提供给不涉及安全配置的管理员。删除这些安全组映射后，用户组将只提供到 SOM 控制台的访问，而不是提供到 SOM 控制台以及所有节点的访问。

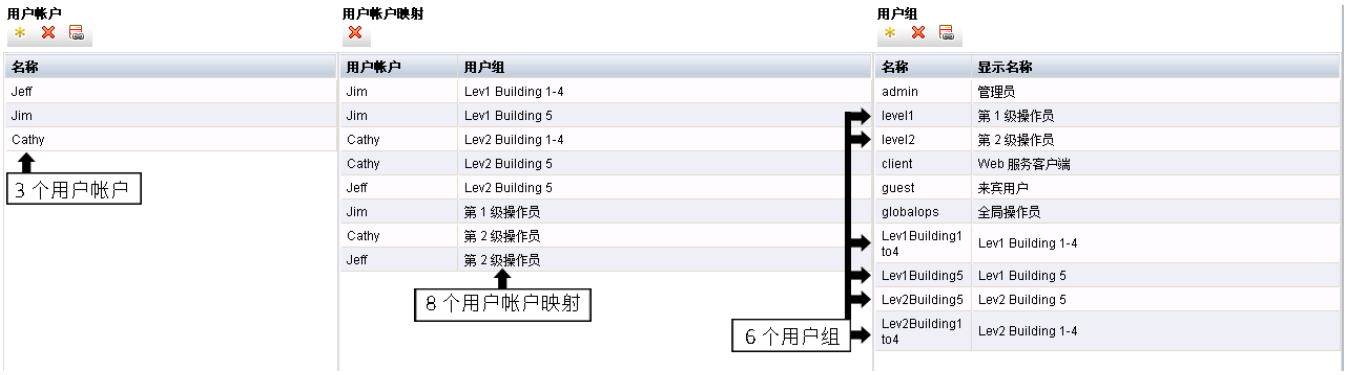
- 创建用户帐户。请参阅安全配置示例表。
- 创建芝加哥和底特律安全组所需的其他用户组 (芝加哥第 2 级操作员、芝加哥第 1 级操作员、底特律第 2 级操作员、底特律第 1 级操作员)。(请参阅安全配置示例表。)
- 将用户帐户映射到 SOM 用户组。(请参阅安全配置示例表。)
- 创建底特律和芝加哥的安全组。
- 将每个安全组映射到新的用户组。(请参阅安全配置示例表。)
  - “ChicagoLevel1” 用户组到 “芝加哥节点”
  - “DetroitLevel1” 用户组到 “底特律节点”
  - “DetroitLevel2” 用户组到 “底特律节点”
- 将节点分配到相应的安全组。
- 查看配置更改的摘要。
- 保存配置更改。

示例:允许一部分用户访问一部分节点

此示例配置安全性，允许一部分用户仅访问 5 栋中的节点。其余用户可以访问 SOM 发现的所有节点。

此位置包括第 1 级操作员 (访问特权限制多于第 2 级操作员) 和第 2 级操作员。Jeff 是只能访问 5 栋中的节点的第 2 级操作员。

注意: 确保创建映射到 SOM 管理员用户组的用户帐户，以便此人能访问 “配置” 工作区和网络中的所有节点。有关详细信息，请参阅联机帮助中的主题 “恢复管理员角色”。



下表列出了每个用户帐户的 SOM 控制台访问要求 (SOM 用户组) 和节点访问要求 (用户组、对象访问特权和安全组)。

注意: 如果希望所有操作员都看到所有菜单选项，但只能基于自身的对象访问特权运行这些选项，则可以将所有操作员都设为 SOM 第 2 级操作员。

安全配置示例

用户帐户	SOM 用户组	用户组	对象访问特权	安全组
Jim	SOM 第 1 级操作员	Lev1Buildings1-4 Lev1Building5	第 1 级操作员对象	默认安全组
Cathy	SOM 第 2 级操作员	Lev2Buildings1-4 Lev2Building5	第 2 级操作员对象	默认安全组
Jeff	SOM 第 2 级操作员	Lev2Building5	第 2 级操作员对象	5 栋节点

要设置此位置的安全，请执行以下步骤:

- 删除到用户组的默认安全组映射: 第 1 级操作员、第 2 级操作员和来宾

  注意: 将 SOM 用户组提供给不涉及安全配置的管理员。删除这些安全组映射后，SOM 用户组将只提供到 SOM 控制台的访问，而不是提供到 SOM 控制台以及所有节点的访问。

- 创建用户帐户。(请参阅安全配置示例表。)
- 创建其他用户组。(请参阅安全配置示例表。)
- 将用户帐户映射到 SOM 用户组。(请参阅安全配置示例表。)
  - 将“Jim”分配到“Lev1Building1-4”和“Lev1Building5”用户组
  - 将“Cathy”分配到 **SOM 第 2 级操作员**、“Lev2Building1-4”和“Lev2Building5”用户组
  - 将“Jeff”分配到 **SOM 第 2 级操作员**和“Lev2Building 5”用户组。
- 创建 5 栋安全组。
- 将每个安全组映射到新的用户组。(请参阅安全配置示例表。)
  - “Lev1Building5”用户组到“5 栋节点”。
  - “Lev2Building1-4”用户组到“默认安全组”
  - “Lev2Building5”用户组到“5 栋节点”。

- **将节点分配到相应的安全组。**
- **查看配置更改的摘要。**

第 6 章: 备份和恢复 SOM 嵌入式数据库

SOM 提供了以下命令用于备份和恢复 SOM 嵌入式数据库。此功能在创建和恢复数据快照时很有用。

开始备份和恢复操作前，请先确保 `somdbmgr` 服务正在运行。

命令和描述

命令

`sombackupembdb.ovpl [-?|-h|-help] [-force] [-noTimeStamp] - target <目录>`

在 SOM 运行时创建 SOM 嵌入式数据库的完整备份 (排除文件系统数据)。

参数	描述

`-?`
`-h`
`-help`
	显示 `sombackupembdb.ovpl` 命令的语法和用法。

`-force`	如果 SOM 尚未运行，则启动 SOM。
`-noTimeStamp`	从备份名称中删除时间戳。
`-target <目录>`	(*必需*) 指定需要备份的数据的目标目录。

`somrestoreembdb.ovpl [-?|-h|-help] [-force] -source <文件>`

恢复通过使用 `sombackupembdb.ovpl` 脚本创建的备份。

参数	描述

`-?`
`-h`
`-help`
	显示 `serestoreembdb.ovpl` 命令的语法和用法。

`-force`	根据需要停止或启动 SOM。
`-source <文件>`	(*必需*) 指定保存需要恢复的数据的源文件名称。

`somresetembdb.ovpl`

删除 SOM 嵌入式数据库表。运行 ovstart 命令以重新创建表。

重置数据库时，如果计划下次使用不同的用户进行发现，则建议手动删除 `repository` 文件夹的内容。该文件夹位于以下位置:

- **Windows**:<*安装目录*>\HP\HP BTO Software\se\repository
- **Linux**:<*安装目录*>/var/opt/OV/se/repository/root/cimv2

参数	描述
-? -h -help	显示 somrestoreembdb.ovpl 命令的语法和用法。
-force	根据需要停止或启动 SOM。
-source <文件>	(*必需*) 指定保存需要恢复的数据的源文件名称。

我们感谢您提出宝贵的意见!

如果您对本文档有任何意见，请通过电子邮件联系文档团队。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:

部署指南反馈，2015 年 3 月 (Storage Operations Manager 10.00)

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@hp.com 。