HP Operations Agent

适用于 Windows®、 HP-UX、 Solaris、 Linux 和 AIX 操作系统

软件版本：11.00

部署指南

文档发行日期：2010 年 10 月
软件发行日期：2010 年 10 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。

限制权利图例

机密计算机软件。拥有、使用或复制操作需要 HP 的有效许可证。根据 FAR 12.211 和 12.212，商业计算机软件、计算机软件文档和商业项目的技术数据已按照供应商的标准商业许可条款授权给美国政府。

版权声明

商标声明

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

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

UNIX® 是 The Open Group 的注册商标。

致谢

本产品包含由 Eric Young (eay@cryptsoft.com) 编写的加密软件。

本产品包含由 OpenSSL Project (http://www.openssl.org/) 开发用于 OpenSSL 工具包的软件。

本产品包含由 Tim Hudson (tjh@cryptsoft.com) 编写的软件。

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

本产品包含 “zlib” 通用压缩库， Copyright© 1995-2002 Jean-loup Gailly and Mark Adler。

文档更新

此文档的标题页包含以下标识信息：

- 软件版本号，表示软件版本。
- 文档发行日期，在每次更新文档时更改。
- 软件发行日期，表示此版本软件的发行日期。

要检查是否有最新更新或验证您所使用的文档是否为最新版，请转到：

http://h20230.www2.hp.com/selfsolve/manuals

此站点要求您注册 HP Passport 才能登录。要注册 HP Passport ID，请转到：

http://h20229.www2.hp.com/passport-registration.html

或单击 HP Passport 登录页上的 **New users - please register** 链接。

支持

访问 HP Software 在线支持网站：

www.hp.com/go/hpsoftwaresupport

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

HP Software 在线支持为客户提供了自解决功能。您可以通过它快速有效地访问管理业务所需的交互技术支持工具。作为重要的支持客户，您可以享受使用支持网站所带来的以下好处：

- 搜索感兴趣的知识文档
- 提交并跟踪支持案例和改进请求
- 下载软件补丁
- 管理支持合同
- 查找 HP Support 联系人
- 检查有关可用服务的信息
- 加入与其他软件客户的讨论中
- 研究并注册软件培训

大多数支持区域要求您以 HP Passport 用户身份注册才能登录。许多区域还需要支持合同。要注册 HP Passport 用户 ID，请转到：

http://h20229.www2.hp.com/passport-registration.html

要查找有关访问级别的详细信息，请转到：

http://h20230.www2.hp.com/new_access_levels.jsp

目录

1 概述

结合使用 HP Operations Manager (HPOM) 与 HP Operations Agent，您可以创建分布式监视解决方案以监视环境中的多个系统。每个节点上的代理程序都监视系统的性能，并将警报消息发送到 HPOM 中央控制台。除了提供中央控制台监视代理程序的响应外， HPOM 控制台还协助您对代理程序执行某些配置任务。

由 HPOM 管理的大型系统网络经常提出部署和维护代理程序方面的挑战。此指南包含在 HPOM 管理的环境中部署 HP Operations Agent 产品的信息、准则和最佳实践。

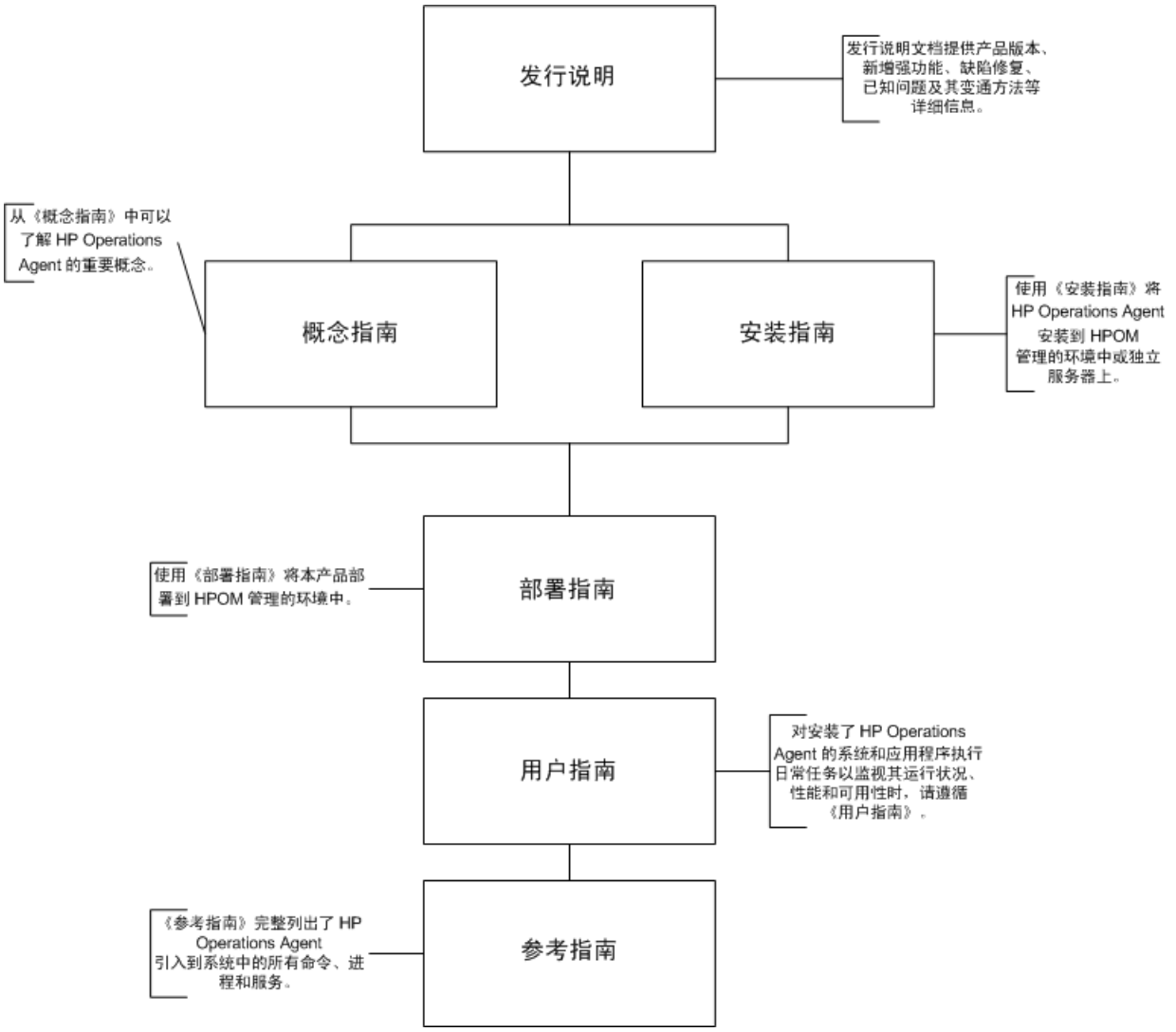
在节点上安装 HP Operations Agent 之后，可使用本指南查看有关以下任务的信息：

- 在节点上部署证书
- 将代理程序配置为在防火墙控制的安全环境中与 HPOM 管理服务器通信
- 配置多个管理服务器的代理程序
- 从 HPOM 控制台远程配置代理程序的数据收集机制
- 在高可用性 (HA) 群集中部署代理程序

文档图

文档图显示了 HP Operations Agent 所有主要文档的列表。需要帮助时，可以通过该图来判断所需文档。

图 1　HP Operations Agent 的文档图



相关文档

可以在产品媒体的 `paperdocs` 目录内找到 HP Operations Agent 的所有用户文档。要检查是否有最新更新或验证您所使用的文档是否为最新版，请转到：

http://h20230.www2.hp.com/selfsolve/manuals

此站点要求您注册 HP Passport 才能登录。要注册 HP Passport ID，请转到：

http://h20229.www2.hp.com/passport-registration.html

或单击 HP Passport 登录页上的 **New users - please register** 链接。

表 1　HP Operations Agent 的用户文档

文档	使用	关键主题
发行说明	有关产品版本、新功能和已知问题的信息，请参考此文档。	• 新功能 • 增强功能 • 修复 • 已知问题和限制
概念指南	《概念指南》帮助您了解不同环境中 HP Operations Agent 的工作机制。	• HP Operations Agent 简介 • HP Operations Agent 的主要组件

表 1　HP Operations Agent 的用户文档

文档	使用	关键主题
安装指南	可以使用 《安装指南》将 HP Operations Agent 安装到以下环境中： • HPOM 管理服务器 （用于 HPOM 管理的分布式管理环境中） • 独立服务器（收集本地服务器的系统性能度量，供 HP Performance Manager 等外部数据分析工具使用）	• 从 HPOM 控制台安装 HP Operations Agent • 手动安装 HP Operations Agent • 许可
用户指南	对 HP Operations Agent 执行日常任务时，如需帮助请参考此指南。	• 管理数据收集 • 生成警报
参考指南	《参考指南》完整地列出了 HP Operations Agent 节点上可用的所有命令、进程和服务。	• 命令行实用程序 • 配置变量

2 配置证书

必须在所有受管节点上安装证书，才方便使用安全套接字层 (SSL) 协议以加密方式进行网络通信。有了证书，节点才能与管理服务器和其他节点安全通信。

管理服务器将证书发到节点，并充当证书颁发机构。每个受管节点都需要来自管理服务器的以下证书：

- **唯一的节点证书。**节点可通过发送其节点证书，向其管理服务器和其他节点标识自身。
- **管理服务器的受信任证书的副本。**节点只有在拥有管理服务器的受信任证书时，才允许来自该管理服务器的通信。

  在有多个管理服务器的环境中，节点上必须存在所有其他管理服务器的受信任证书的副本。

为使节点在 HPOM 管理的环境中能使用证书安全通信，必须在节点上安装代理程序之后安装证书。

安装证书

可以用以下某种方式安装证书：

- 自动申请证书
- 用安装密钥申请证书
- 手动部署证书

自动申请证书

从 HPOM 控制台将代理程序部署到节点时，节点自动从管理服务器申请证书。节点用密钥对证书申请加密。

随即管理服务器批准证书申请。可将此配置为自动执行。批准申请之后，管理服务器将证书发送到节点。如果管理服务器拒绝证书申请，可以通过在受管节点上运行以下命令发送另一申请：

```
ovcert -certreq
```

在要求高度安全的环境中，可通过将证书部署类型设置为手动以禁用自动证书申请。然后必须用安装密钥申请证书，或手动部署证书。

用安装密钥申请证书

要对证书申请加密，可使用安装密钥。可在管理服务器上生成安装密钥，然后将它传输到节点。

用安装密钥申请证书之前，确保 HP Operations Agent 正在节点上运行。代理程序在开始时发送证书申请。如果随后用安装密钥申请证书，则新证书申请将覆盖管理服务器上的原始证书申请。可通过使用代理程序安装默认设置或 ovconfchg 实用程序，将 sec.cm.client 命名空间中的参数 CERTIFICATE_DEPLOYMENT_TYPE 设置为 manual 来抑制第一个证书申请。

要用安装密钥申请证书，请执行以下步骤：

1 用属于 HPOM 管理员组的帐户登录管理服务器。

2 打开命令提示符 (shell)。

3 运行以下命令：

从 HPOM for Windows

ovowcsacm -genInstKey [-file <*文件名*>**] [-pass** <*密码*>**]**

从 HPOM for UNIX 或 HPOM on UNIX/Linux

opccsacm -genInstKey [-file <*文件名*>**] [-pass** <*密码*>**]**

在此实例中：

<*文件名*>：安装密钥文件的名称。

用 <*文件名*> 指定完整路径；否则证书将存储到当前工作目录中。如果不指定 -file 选项，证书将存储到 <*数据目录*>\shared\server\certificates 中。

<*密码*>：稍后从节点申请证书时，需要此密码。可省略此选项。

命令生成安装密钥。

4 将生成的文件安全传输到节点。安装密钥对任何节点都有效。

5 用安装节点所用的帐户登录到节点。

6 打开命令提示符 (shell)。

7 在 UNIX/Linux 节点上，确保 PATH 变量包含 <*安装目录*>/bin 目录的路径。

8 运行以下命令：

ovcert -certreq -instkey <*文件名*>

9 管理服务器必须批准该申请。可将此配置为自动或手动执行。之后，管理服务器将证书发送到节点。

手动部署证书

节点可以将证书申请自动发送到管理服务器。如果要手动在节点上安装证书，可以将节点上的 CERTIFICATE_DEPLOYMENT_TYPE 变量 （在 sec.cm.client 命名空间中）设置为 MANUAL。

要手动部署证书，请执行以下步骤：

1 用属于 HPOM 管理员组的帐户登录管理服务器。

2 打开命令提示符 (shell)。

3 确保节点已添加到 HPOM 控制台中受管节点的列表中。

4 运行以下命令：

从 HPOM for Windows

ovowcsacm -issue -name <*节点名称*> **[-file** <*文件名*>**] [-coreid** <*OvCoreId*>**] [-pass** <*密码*>**]**

从 HPOM for UNIX 或 HPOM on UNIX/Linux

opccsacm -issue -file <*文件名*> **[-pass** <*密码*>**] -name** <*节点名称*> [**-coreid** <*OvCoreId*>**]**

用 <*文件名*> 指定完整路径；否则证书将存储到当前工作目录中。如果不指定 -file 选项，证书将存储到 <*数据目录*>\shared\server\certificates 中。

在此实例中，

<*节点名称*>：节点的 FQDN 或 IP 地址。

<*OvCoreId*>：节点的核心 ID。要检索已安装代理程序的节点的核心 ID，请在管理服务器上执行以下步骤：

- *在 HPOM for UNIX 或 HPOM on UNIX/Linux 上*

  运行以下命令：

  opcnode -list_id node_list=<*节点名称*>

- *在 HPOM for Windows 上*

  在控制台树中，右键单击节点，然后单击**属性 (Properties)**。将打开节点属性对话框。在节点属性对话框中，转到 “常规 (General)” 选项卡，单击**高级配置 (Advanced Configuration)**。将打开 “高级配置 (Advanced Configuration)” 对话框，显示节点的核心 ID。

<*文件名*>：命令生成的证书文件的名称。如果不指定此选项，则命令会使用默认名称 <*节点名称*>-<OvCoreId>.p12 将文件创建到以下目录中：

- *在 HPOM for UNIX 或 HPOM on UNIX/Linux 上*

  /var/opt/OV/temp/OpC/certificates

- *在 HPOM for Windows 上*

  %OvShareDir%server\certificates

5 将生成的文件安全传输到节点。安装密钥对任何节点都有效。

6 在节点上安装代理程序（如果尚未安装）。使用基于配置文件的安装，并将 CERTIFICATE_DEPLOYMENT_TYPE 变量设置为 manual。同时，使用在管理服务器上生成的相同 OvCoreID（将 sec.cm.client 命名空间中的 CERTIFICATE_SERVER_ID 设置为管理服务器上生成的 ID）。

7 在节点上打开命令提示符 (shell)。

8 如果代理程序正在节点上运行，则运行以下命令：

```
ovc -stop
```

9 要从生成的文件导入证书，请运行以下命令：

ovcert -importcert -file <*文件名*>

该命令可能提示您指定在第 13 页的步骤 4 中提供的密码。

10 在节点上运行以下命令：

```
ovc -start
```

恢复证书

如果丢失了节点上的证书，必须再次创建它们。如果将现有证书备份到文件中，就可以在证书发生故障的情况下恢复它们。要备份证书，请执行以下步骤：

1 以具有根特权或管理特权的身份登录到节点。

2 打开命令提示符 (shell)。

3 运行以下命令：

ovcm -exportcacert -file <*文件名*> **[-pass** <*密码*>**]**

该命令将管理服务器证书备份到用 -file 选项指定的文件中。

4 运行以下命令：

ovcert -exporttrusted [-ovrg <*服务器*>**] -file** <*文件名*>

在此实例中，如果管理服务器安装在 HA 群集中，则<*服务器*> 是 HA 资源组名称。

该命令将管理服务器的受信任证书备份到用 -file 选项指定的文件中。

5 运行以下命令，确定节点证书的别名：

ovcert -list [-ovrg <*服务器*>**]**

节点证书的别名是一长串字符，这些字符出现在输出的 Certificates 部分下面。例如：

```
+-------------------------------------------------------+
| Keystore Content                                      |
+-------------------------------------------------------+
| Certificates:                                         |
cdc7b5a2-9dd6-751a-1450-eb556a844b55 (*)                |
+-------------------------------------------------------+
```

```
| Trusted Certificates:                                    |
|     CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55              |
+----------------------------------------------------------+
```

6 运行以下命令：

ovcert -exportcert -file <*文件名*> **-alias** <*别名*> **[-pass** <*密码*>**]**

该命令将节点证书备份到用 `-file` 选项指定的文件中。

要恢复节点上的证书，请执行以下步骤：

1 以具有根特权或管理特权的身份登录到节点。

2 打开命令提示符 (shell)。

3 要恢复管理服务器证书，请运行以下命令：

ovcm -importcacert -file <*文件名*> **[-pass** <*密码*>**]**

在此实例中，<*文件名*> 是在第 14 页的步骤 3 中指定的文件名。

4 要恢复受信任证书，请运行以下命令：

ovcert -importtrusted -file <*文件名*>

在此实例中，<*文件名*> 是在第 14 页的步骤 4 中指定的文件名。

5 要恢复节点证书，请运行以下命令：

ovcm -importcert -file <*文件名*> **[-pass** <*密码*>**]**

在此实例中，<*文件名*> 是在第 15 页的步骤 6 中指定的文件名。

排除证书问题

要验证是否在节点上正确安装了所有需要的证书，请在节点上运行以下命令：

ovcert -list

命令按以下格式显示输出：

```
+----------------------------------------------------------+
| Keystore Content                                         |
+----------------------------------------------------------+
| Certificates:                                            |      | |
cdc7b5a2-9dd6-751a-1450-eb556a844b55 (*)                   |
+----------------------------------------------------------+
| Trusted Certificates:                                    |
|     CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55              |
+----------------------------------------------------------+
```

输出的 `Certificates` 部分显示节点证书的名称。输出的 `Trusted Certificates` 部分显示管理服务器的受信任证书的名称。

节点证书名称与节点的 `OvCoreID` 参数相同。

受信任证书名称用 CA_ 前缀和受信任证书颁发机构 （管理服务器）的 OvCoreID 参数创建。

丢失节点证书

要检查节点证书是否丢失，请在节点上运行以下命令：

ovcert -list

如果节点证书丢失，命令将按以下格式显示输出：

```
+------------------------------------------------------------+
| Keystore Content                                 |
+------------------------------------------------------------+
| Certificates:                                              |
+------------------------------------------------------------+
| Trusted Certificates:                                      |
|     CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55                 |
+------------------------------------------------------------+
```

空的 Certificates 部分表示节点证书不存在。

要解决这个问题，请执行以下步骤：

1 运行以下命令，从节点删除管理服务器的受信任证书：

ovcert -remove <*证书名称*>

在此实例中，<*证书名称*>是受信任证书的名称 （示例中为 CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55）。

2 运行以下命令，停止操作监视组件的所有进程：

ovc -kill

3 运行以下命令，启动核心进程：

ovc -start CORE

4 如果管理服务器和节点配置为自动部署证书，节点将申请发送到管理服务器，然后管理服务器批准申请。

要检查证书申请是否到达管理服务器，请运行以下命令 （在管理服务器上）：

ovcm -listpending -l

命令输出应在 CN 字段中显示节点的核心 ID。

如果未在 CN 字段中看到节点的核心 ID，请在节点上运行以下命令手动触发证书申请：

ovcert -certreq

如果管理服务器和节点配置为手动部署证书，则按照第 13 页的手动部署证书中的说明操作。

要检查是否在节点上正确安装了证书，请运行以下命令 （在节点上）：

ovcert -list

输出应在 Certificates 部分中显示有效的证书名称 （与节点的核心 ID 相同）。

丢失受信任证书

要检查受信任证书是否丢失，请在节点上运行以下命令：

ovcert -list

如果受信任证书丢失，命令将按以下格式显示输出：

```
+-------------------------------------------------------+
| Keystore Content                                      |
+-------------------------------------------------------+
| Certificates:                                                                 |
| cdc7b5a2-9dd6-751a-1450-eb556a844b55 (*)
+-------------------------------------------------------+
| Trusted Certificates:                                 |
+-------------------------------------------------------+
```

空的 Trusted Certificates 部分表示受信任证书不存在。

可通过从管理服务器或此同一管理服务器管理的另一个节点导入受信任证书，解决此问题。

要从另一个源导入受信任证书，请执行以下步骤：

1. 以具有根特权或管理特权的身份登录到管理服务器或另一个节点 （由同一管理服务器管理）。
2. 运行以下命令：

   ovcert -exporttrusted [-ovrg <*服务器*>**] -file** <*文件名*>

   在此实例中，如果管理服务器安装在 HA 群集中，则 <*服务器*> 是 HA 资源组名称。

   该命令导出用 -file 选项指定的文件中的管理服务器的受信任证书。
3. 将文件传输到节点 （丢失受信任证书的地方）。
4. 要导入受信任证书，请运行以下命令：

   ovcert -importtrusted -file <*文件名*>
5. 要检查是否在节点上正确安装了证书，请运行以下命令 （在节点上）：

   ovcert -list

   输出应在 Trusted Certificates 部分显示有效的证书名称。

丢失节点私钥

要检查节点证书的私钥是否丢失，请在节点上运行以下命令：

ovcert -list

如果节点私钥丢失，命令将按以下格式显示输出：

```
+-------------------------------------------------------+
| Keystore Content                                      |
+-------------------------------------------------------+
| Certificates:                                                                 |
| cdc7b5a2-9dd6-751a-1450-eb556a844b55
+-------------------------------------------------------+
| Trusted Certificates:                                  |
| CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55                |
+-------------------------------------------------------+
```

节点证书名称旁缺少 * 号表示节点私钥丢失。要解决这个问题，必须删除节点证书，然后在节点上安装新证书。执行以下步骤：

1 运行以下命令，从节点删除节点证书：

ovcert -remove <*证书名称*>

在此实例中，<*证书名称*> 是节点证书的名称 （示例中为 cdc7b5a2-9dd6-751a-1450-eb556a844b55）。

2 执行第 16 页的步骤 2 到第 16 页的步骤 4。

3 要检查是否在节点上正确安装了节点私钥，请运行以下命令 （在节点上）：

ovcert -list

输出应在 Certificates 部分中的节点证书名称旁边显示 * 号。

3 在安全环境中部署 HP Operations Agent

HP Operations Agent 和 HPOM 管理服务器使用 HTTPS 协议在网络上相互通信。管理服务器打开到代理程序节点的连接，以执行部署策略和启动操作等任务。
HP Operations Agent 节点打开到管理服务器的连接，以发送消息和响应。

默认情况下，代理程序节点和管理服务器的操作系统分配本地通信端口。但是，代理程序和管理服务器都使用**通信中介器**组件进行入站通信。通信中介器组件默认情况下使用端口 383 接收数据。因此，实际上节点和管理服务器使用两组端口：

- 操作系统分配的出站通信端口
- 通信中介器使用的入站通信端口

在基于防火墙的高度安全的网络中，管理服务器和代理程序节点之间的通信可能会因防火墙设置的限制而失败。在这些场景中，可以执行其他配置任务以在管理服务器和受管节点之间建立双向通信。

规划配置

如果您的网络允许 HTTPS 连接有限制地双向穿过防火墙，则可以在 HPOM 中使用以下配置选项应对这些限制：

- 如果您的网络仅允许从某些本地端口进行出站连接，则可以将 HPOM 配置为使用特定本地端口。
- 如果您的网络仅允许入站连接到某些目标端口，但不是 383 端口，则可以配置备用通信中介器端口 （第 22 页的配置通信中介器端口）。
- 如果您的网络仅允许某些代理系统穿过防火墙打开连接，则可以通过这些代理重定向 HPOM 通信 （请参见第 26 页的配置通过代理的 HTTPS 通信）。
- 如果您的网络仅允许从管理服务器穿越防火墙进行 HTTPS 出站连接，并阻止从节点进行入站连接，则可以配置反向通道代理 (RCP) （第 26 页的高度安全环境中的通信）。

在有多台管理服务器的环境中，还可以将管理服务器配置为通过防火墙相互通信。其配置方式与管理服务器和节点之间的通信配置相同。

开始之前

如果只要在 Windows 节点上使用 HP Operations Agent，请跳过此部分。

大多数配置任务都通过 ovconfchg 实用程序执行，该实用程序位于以下目录中：

- 在 HP-UX、 Linux 和 Solaris 上

  /opt/OV/bin

- 在 AIX 上

  /usr/lpp/OV/bin

要从系统上的任何位置运行 ovconfchg 命令（以及其他任何特定于代理程序的命令），必须将 bin 目录添加到系统的 PATH 变量中。在 Windows 系统上，bin 目录会自动添加到 PATH 变量中。要在 UNIX/Linux 系统上将 bin 目录添加到 PATH 变量中，请执行以下步骤：

1 在节点上，打开命令提示符 (shell)。

2 执行以下某项操作：

- 在 HP-UX、 Solaris 或 Linux 节点上，运行命令：

  export PATH=/opt/OV/bin:$PATH

- 在 AIX 节点上，运行命令：

  export PATH=/usr/lpp/OV/bin:$PATH

  系统的 PATH 变量现已设置为指定位置。现在，您可以从系统的任何位置运行特定于代理程序的命令。

配置代理

可以通过代理重定向来自不同网络上的管理服务器和节点的连接。

- 管理服务器打开到代理服务器的连接，比如，以部署策略和检测、进行检测信号轮询或启动操作。代理服务器代表管理服务器打开到节点的连接，并转发管理服务器与节点之间的通信。
- 节点打开到代理服务器的连接，比如，以发送消息和操作响应。代理服务器代表节点打开到管理服务器的连接。

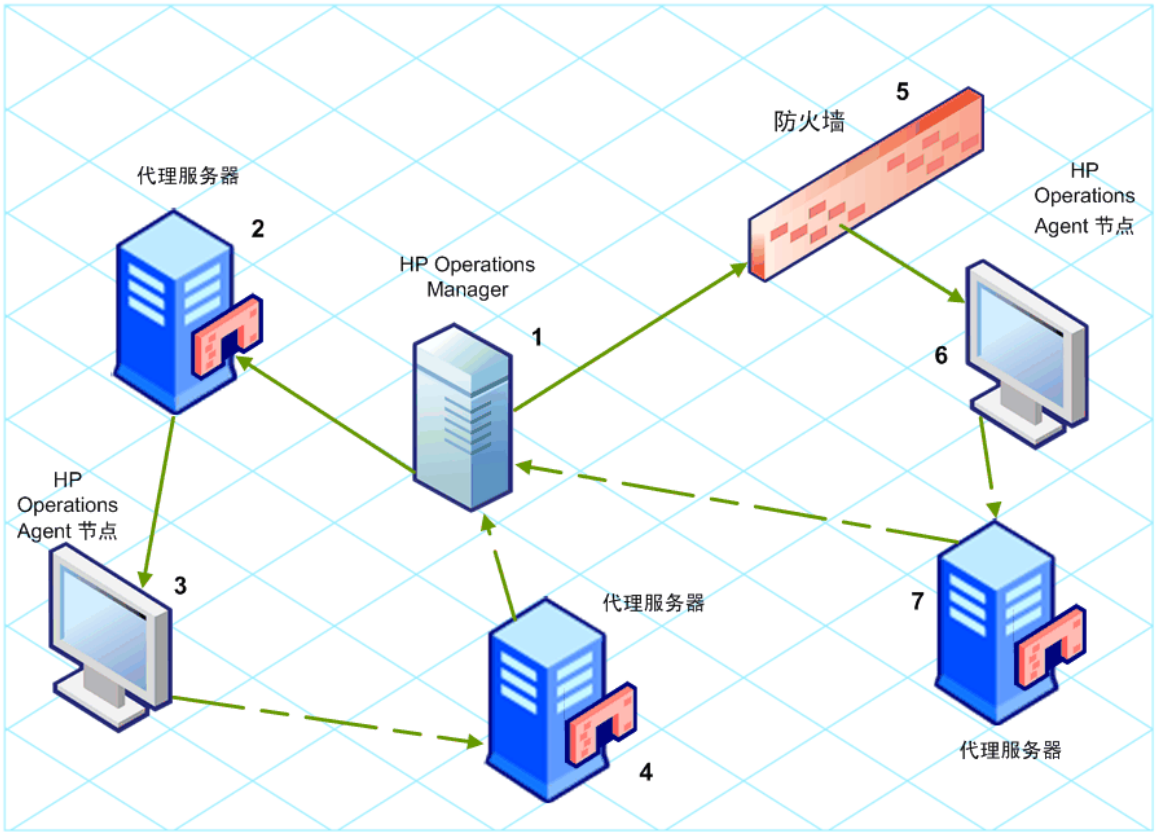
还可以在更复杂的环境中通过代理重定向通信，如下所示：

- 每个管理服务器和节点都可以使用不同的代理服务器相互通信。
- 可将管理服务器和节点配置为按照它们所连接的主机选择正确的代理。

下图显示了管理服务器与节点通过多个代理的连接：

- 管理服务器 (1) 打开到代理 (2) 的连接。该代理代表管理服务器打开到节点 (3) 的连接。
- 节点 (3) 打开到其他代理 (4) 的连接。该代理代表节点打开到管理服务器 (1) 的连接。
- 该网络允许管理服务器 (1) 直接通过防火墙 (5) 与另一个节点 (6) 进行 HTTP 出站连接。（节点 3 和 6 在不同网络上。）
- 防火墙 (5) 不允许 HTTP 入站连接。因此，节点 (6) 通过代理 (7) 打开到管理服务器的连接。

图 2　使用代理通信



PROXY 参数语法

可以在管理服务器和节点上的 bbc.http 命名空间中设置 PROXY 参数，以通过代理重定向 HTTPS 出站通信。可使用以下方式配置此参数：

- 在 HP Operations Agent 安装默认设置中配置这些值。如果需要配置代理的节点很多，建议使用此方式。在创建或迁移节点之前，必须计划并配置安装默认设置。
- 在命令提示符处使用 `ovconfchg`。

PROXY 参数的值可以包含一个或多个代理定义。按以下格式指定每个代理：

<代理主机名>:*<代理端口>*+（*<包含的主机>*）-（*<排除的主机>*）

将 <*包含的主机*> 替换为代理可以通信的主机名或 IP 地址的逗号分隔列表。将 <*排除的主机*> 替换为代理不能连接的主机名或 IP 地址的逗号分隔列表。星号 (*) 是主机名和 IP 地址中的通配符。<*包含的主机*> 和 <*排除的主机*> 都是可选的。

要指定多个代理，请用分号 (;) 分隔每个代理。列表中第一个合适的代理优先。

PROXY 参数值示例

要将节点配置为使用 proxy1.example.com 端口 8080 进行所有出站连接，可以使用以下值：

```
proxy1.example.com:8080
```

要将管理服务器配置为使用 proxy2.example.com:8080 连接主机名与 *.example.com 或 *example.org 匹配但 IP 地址范围在 192.168.0.0 到 192.168.255.255 以外的所有主机，可以使用以下值：

```
proxy2.example.com:8080+(*.example.com,*.example.org)-(192.168.*.*)
```

要扩展上面的示例以使用 proxy3.example.com 仅连接到 backup.example.com，可以使用以下值：

```
proxy3.example.com:8080+(backup.example.com);
proxy2.example.com:8080+(*.example.com,*.example.org)-(192.168.*.*)
```

在上面的示例中， proxy3.example.com:8080+(backup.example.com) 必须在前，因为 proxy2.example.com 的包含列表包括 *.example.com。

要通过代理重定向 HTTPS 通信，请执行以下步骤：

1 以具有管理权限或根权限的用户身份登录到管理服务器或节点，打开命令提示符或 shell。

2 指定节点应使用的代理。可指定不同代理，以根据代理程序要连接的主机使用适当的代理。运行以下命令：

ovconfchg -ns bbc.http -set PROXY <*代理*>

在群集中运行的管理服务器上使用命令 ovconfchg 时，请添加参数 -ovrg <*服务器*>。

配置通信中介器端口

默认情况下，HP Operations Agent 节点使用端口 383 进行入站通信。通信中介器组件通过端口 383 方便了每个 HP Operations Agent 服务器或节点上的入站通信。

可以将任何通信中介器配置为在 383 以外的端口上侦听。如果这样做，还必须在环境中配置其他管理服务器和节点，使它们的出站连接指定到正确的端口。例如，如果将节点的通信中介器配置为在端口 5000 上侦听，则还必须配置管理服务器使其与该节点通信时连接到端口 5000。

PORTS 参数语法

可以在所有相互通信的管理服务器和节点的 bbc.cb.ports 命名空间中设置 PORTS 参数，以配置通信中介器端口。

可使用以下方式配置此参数：

- 安装期间在 HP Operations Agent 安装默认设置的配置文件中配置这些值。如果需要配置通信中介器端口的节点很多，建议使用此方式。在创建或迁移节点之前，必须计划并配置安装默认设置。
- 在命令提示符处使用 **ovconfchg**。

这些值必须包含一个或多个主机名或 IP 地址，并采用以下格式：

<*主机*>:<*端口*>[,<*主机*>:<*端口*>] ...

<*主机*>可以是域名或 IP 地址。例如，要在主机名为 manager1.emea.example.com 的管理服务器上将通信中介器端口配置为 5000，则在该管理服务器上以及其他任何打开到该管理服务器的连接的管理服务器和节点上使用以下命令：

```
ovconfchg -ns bbc.cb.ports -set PORTS manager1.domain.example.com:5000
```

如果需要在多个系统上配置通信中介器端口，则可以使用通配符和范围，如下所示：

- 可以在域名开头添加一个星号 (*) 作为通配符。例如：
  - *.test.example.com:5000
  - *.test.com:5001
  - *:5002
- 可以在 IP 地址末尾添加一到三个星号 (*) 作为通配符。例如：
  - 192.168.1.*:5003
  - 192.168.*.*:5004
  - 10.*.*.*:5005
- 可以用范围替换 IP 地址中的一个八位组。范围必须在任何通配符之前。例如：
  - 192.168.1.0-127:5006
  - 172.16-31.*.*:5007

如果为 PORTS 参数指定多个值，则用逗号 (,) 分隔每个值。例如：

```
ovconfchg -ns bbc.cb.ports -set PORTS
*.test.example.com:5000,10.*.*.*:5005
```

当使用通配符和范围指定的多个值重叠时，管理服务器或节点则按以下顺序选择要使用的端口：

- 完全限定域名。
- 带通配符的域名。
- 完整 IP 地址。
- 使用范围的 IP 地址。
- 带通配符的 IP 地址。

示例

必须针对以下规范配置 HPOM 管理环境：

- 将域 `*.test2.example.com` 中的所有系统配置为对通信中介器使用端口 6000。
- 将 IP 地址第一个八位组为 10 (`10.*.*.*`) 的所有系统配置为对通信中介器使用端口 6001，但以下例外：

  将 IP 地址第二个八位组在 0 到 127 之间 (`10.0-127.*.*`) 的所有系统配置为对通信中介器使用端口 6003。
- 将系统 `manager1.test2.example.com` 配置为对通信中介器使用端口 6002。

要按以上规范配置 HPOM 监视环境，请运行以下命令：

```
ovconfchg -ns bbc.cb.ports -set PORTS
*.test2.example.com:6000,10.*.*.*:6001,manager1.test2.example.com:6002,
10.0-127.*.*:6003
```

只有在监视环境中的*所有*代理程序节点和*所有* HPOM 管理服务器上运行此命令后，更改才会生效。

要查明当前配置了哪个端口，请运行以下命令：

```
bbcutil -getcbport <主机>
```

要将通信中介器配置为使用非默认端口，请执行以下步骤：

确保将环境中所有 HPOM 服务器和 HP Operations Agent 节点上的通信中介器配置为使用相同端口。

1. 登录到 HP Operations Agent 节点。
2. 打开命令提示符或 shell。
3. 运行以下命令以将通信中介器端口设置为非默认值：

   ```
   ovconfchg -ns bbc.cb.ports -set PORTS <主机>:<端口>[,<主机>:<端口>] ...
   ```

   在群集中运行的 HP Operations Agent 节点上使用命令 **ovconfchg** 时，请添加参数 **-ovrg** <*服务器*>，其中 <*服务器*> 为资源组。
4. 在所有代理程序节点和所有管理服务器上运行以上命令。

配置本地通信端口

默认情况下，管理服务器和节点使用本地端口 0 进行出站连接，这意味着由操作系统为每个连接分配本地端口。通常，操作系统将按顺序分配本地端口。例如，如果操作系统向 Internet 浏览器分配了本地端口 5055，然后 HTTPS 代理程序打开连接，那么 HTTPS 代理程序会收到本地端口 5056。

但是，如果防火墙限制您可以使用的端口，则可以将管理服务器和节点配置为使用特定的本地端口范围。

CLIENT_PORT 参数语法

可以在管理服务器或节点上的 bbc.http 命名空间中设置 CLIENT_PORT 参数，以配置本地通信端口。可使用以下方式配置此参数：

- 在 HP Operations Agent 安装默认设置中配置这些值。如果需要配置本地通信端口的节点很多，建议使用此方式。在创建或迁移节点之前，必须计划并配置安装默认设置。
- 在命令提示符处使用 ovconfchg。

值必须是采用以下格式的端口范围：

< *低端口号* >-< *高端口号* >

例如，如果防火墙仅允许来自端口 5000 到 6000 的出站连接，则可以使用以下值：

5000-6000

要配置本地通信端口，请执行以下步骤：

1. 登录到 HP Operations Agent 节点。
2. 打开命令提示符或 shell。
3. 通过输入以下命令，指定管理服务器或节点可用于出站连接的本地端口范围：

   ovconfchg -ns bbc.http -set CLIENT_PORT <*低端口号*>-<*高端口号*>

在群集中运行的管理服务器上使用命令 ovconfchg 时，请添加参数 -ovrg <*服务器*>。

配置有多个 IP 地址的节点

如果节点有多个 IP 地址，则代理程序使用以下地址进行通信：

- 通信中介器接受所有 IP 地址上的传入连接。
- 代理程序使用它找到的第一个网络接口打开到管理服务器的连接。
- 为了与 HP Reporter 或 HP Performance Manager 通信，通信守护进程 (CODA) 接受所有 IP 地址上的传入连接。

要将 HP Operations Agent 配置为使用特定 IP 地址，请执行以下步骤：

1. 登录到 HP Operations Agent 节点。
2. 打开命令提示符或 shell。
3. 运行以下命令以设置通信中介器的 IP 地址：

   ovconfchg -ns bbc.cb SERVER_BIND_ADDR <*IP 地址*>

4 运行以下命令以设置代理程序在打开到管理服务器的出站连接时使用的 IP 地址：

ovconfchg -ns bbc.http CLIENT_BIND_ADDR <*IP 地址*>

5 运行以下命令以设置用于 HP Performance Manager 或 HP Reporter 传入连接的 IP 地址：

ovconfchg -ns coda.comm SERVER_BIND_ADDR <*IP 地址*>

配置通过代理的 HTTPS 通信

如果您的网络仅允许某些代理系统穿过防火墙打开连接，则可以通过这些代理重定向 HPOM 通信。以下列表展示了拥有此配置的管理服务器和代理程序的通信工作流程：

1 管理服务器打开到代理的连接。

2 代理代表管理服务器打开到节点的连接，并转发管理服务器与节点之间的通信。

3 节点打开到代理的连接。

4 代理代表节点打开到管理服务器的连接。

要通过代理重定向通信，请执行以下步骤：

1 以具有根特权 / 管理特权的身份登录到管理服务器或节点。

2 在命令提示符处运行以下命令：

ovconfchg -ns bbc.http -set PROXY <*代理*>: <*端口*>

在此实例中，<*代理*> 是代理服务器的 IP 地址或 FQDN；<*端口*> 是代理服务器的通信端口。

在群集中运行的管理服务器上使用命令 ovconfchg 时，请添加参数 -ovrg <*服务器*>。

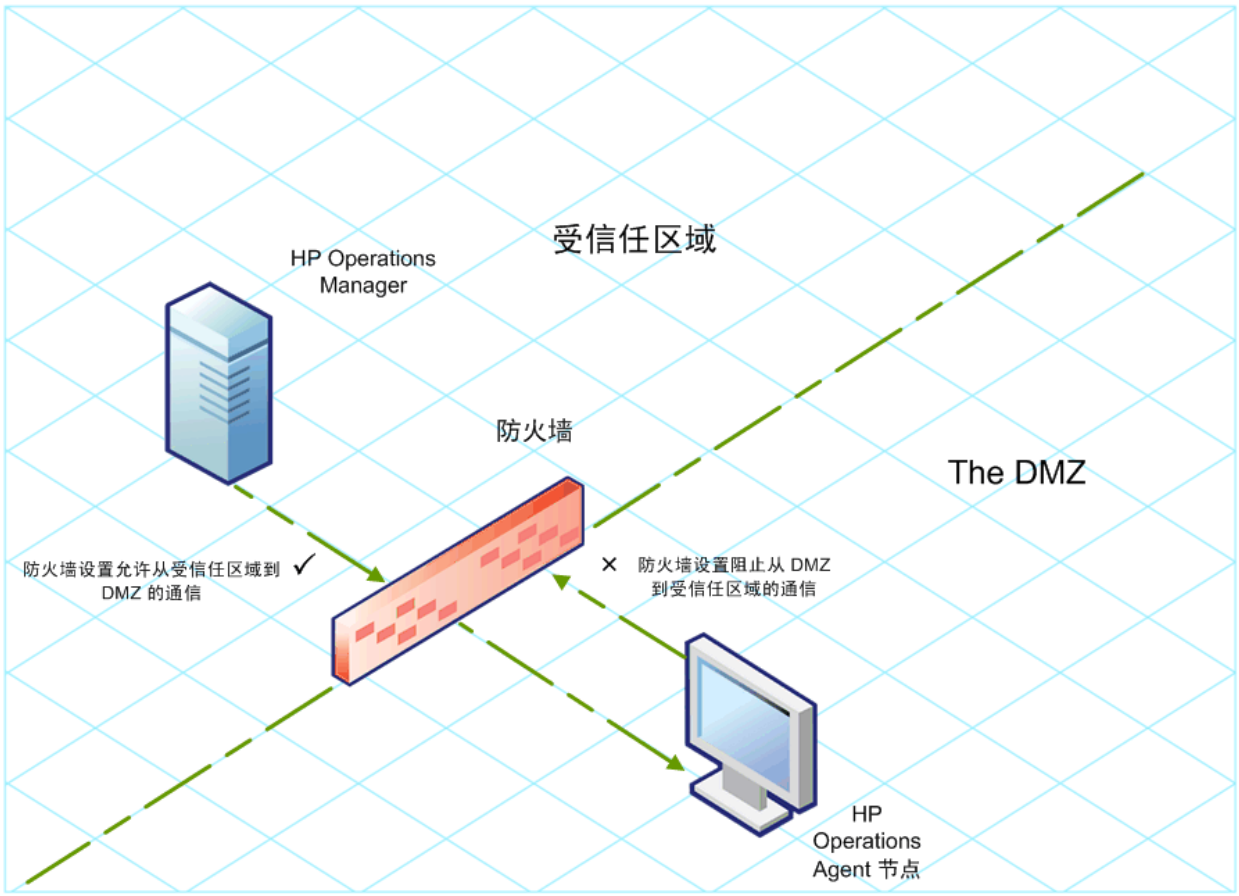
高度安全环境中的通信

在防火墙控制的安全环境中，受信任区域内的系统相互之间可以自由通信和交换信息。但是，特定防火墙设置可以限制与受信任区域以外的系统的通信。不受信任网络（也称为外围区域，**DMZ**）可能由于防火墙设置的限制不能将数据发送到受信任区域。

在很多部署场景中，HPOM 管理服务器可能位于受信任区域，受管节点可能位于 DMZ。如果将防火墙配置为阻止 DMZ 中的系统与受信任区域中的系统通信，则服务器与代理程序之间将无法通信。

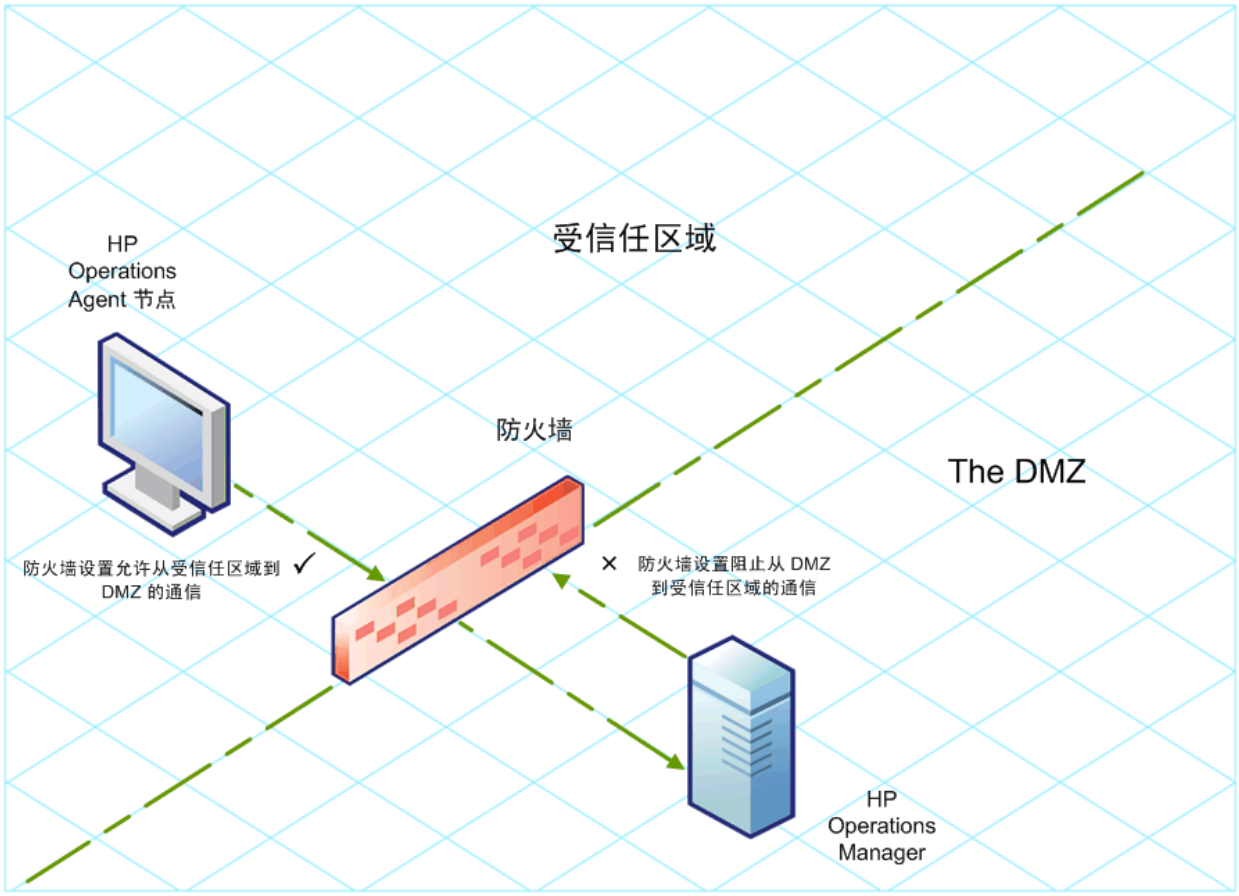
在以下场景中，受管节点位于 DMZ 中，而管理服务器属于受信任区域。此示例中的防火墙设置允许仅出站通信。因此，防火墙会阻止到管理服务器的入站通信。

图 3　DMZ 中的受管节点



在以下场景中，受管节点位于受信任区域，而管理服务器属于 DMZ。此示例中的防火墙设置允许从节点到 HPOM 管理服务器的仅出站通信，阻止到节点的入站通信。

图 4　DMZ 中的 HPOM 管理服务器



反向通道代理简介

启用双向通信的一个简单解决方案是将防火墙设置配置为允许到端口 383（通信中介器端口）的入站通信。但是，这样系统容易受到外部攻击。要启用不允许到通信中介器端口入站通信的安全通信，必须配置反向通道代理 (**RCP**)。

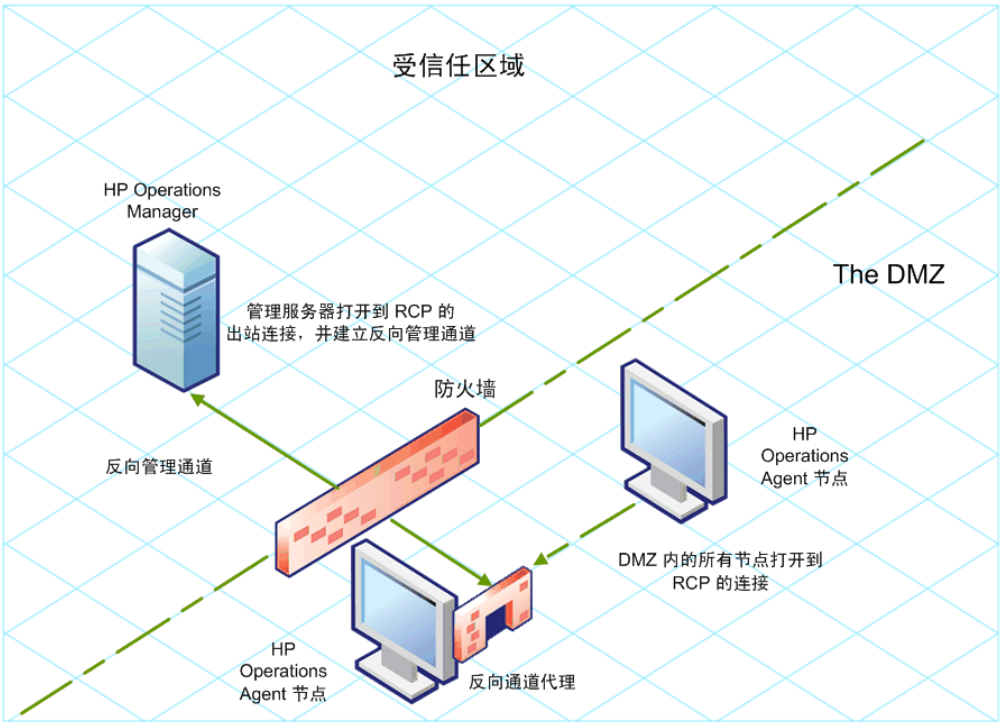
属于 DMZ 的系统而不是受信任区域内的系统打开到 RCP 的连接。您可以将受信任区域内的系统配置为打开到 RCP 的出站通信通道（反向管理通道）。受信任区域内的系统维持出站通道；DMZ 内的系统通过 RCP 使用反向管理通道向受信任区域发送详细信息。

当节点位于 DMZ 而管理服务器位于受信任区域时， HPOM 设置使用以下工作流程：

- 在 DMZ 内的节点上配置 RCP。
- DMZ 内的所有节点打开到 RCP 的连接。

- 管理服务器打开到 RCP 的出站连接，并建立反向管理通道。反向管理通道允许管理服务器接受来自于 RCP 的入站数据，但不涉及任何额外端口。
- DMZ 内的所有节点通过反向管理通道与 HPOM 管理服务器通信。

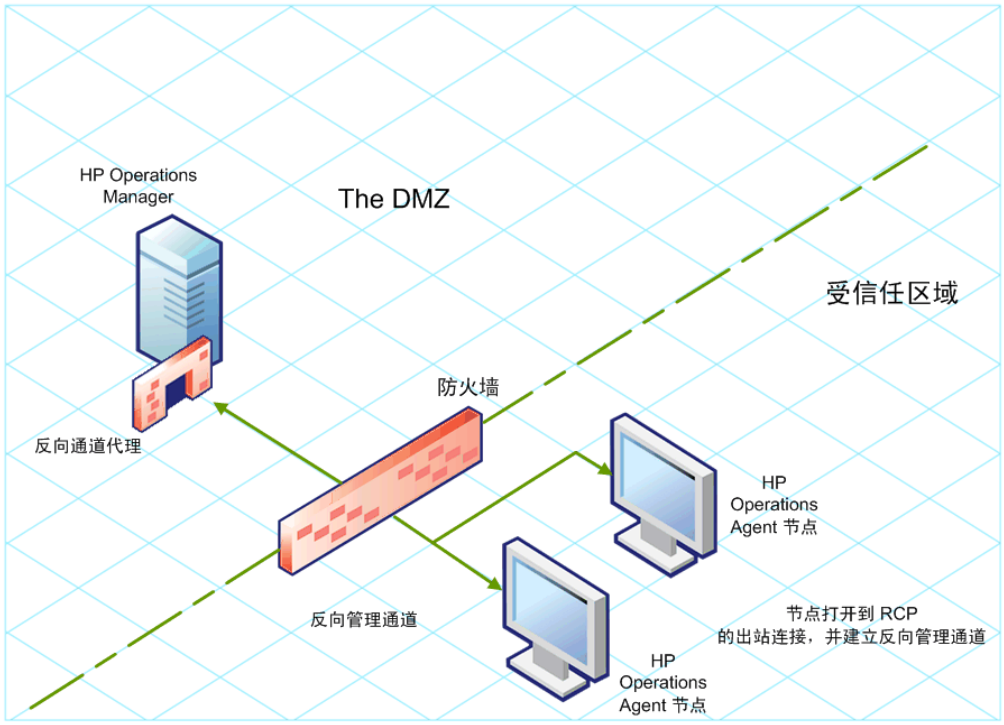
图 5　通过 RCP 与 DMZ 中节点的安全通信



当节点位于受信任区域而管理服务器位于 DMZ 时， HPOM 设置使用以下工作流程：

- 在 DMZ 内的管理服务器上配置 RCP。
- 节点打开到 RCP 的出站连接，并建立反向管理通道。反向管理通道允许节点接受来自于 RCP 的入站数据，但不涉及任何额外端口。
- DMZ 内的管理服务器通过反向管理通道与节点通信。

图 6　通过 RCP 与 DMZ 中管理服务器的安全通信



在仅出站环境中配置安全通信

要在仅出站环境中配置通过 RCP 和反向管理通道的安全通信，请执行以下任务：

任务 1：　配置 RCP

在配置 RCP 之前，必须配置节点证书。

要配置 RCP，请执行以下步骤：

1　以具有管理特权或根特权的用户身份登录到节点或管理服务器 （具体取决于其网络位置）。

2　打开命令提示符或 shell。

3　运行以下命令：

ovconfchg -ns bbc.rcp -set SERVER_PORT <*端口号*>。

> 在群集中运行的 HPOM 管理服务器上使用命令 **ovconfchg** 时，请添加参数 **-ovrg** <*服务器*>，其中 <*服务器*> 为资源组。

在此实例中，<*端口号*> 是 RCP 将使用的端口号。确保指定的端口未被其他应用程序使用。

4　注册 RCP 组件以便 ovc 启动、停止和监视它。输入以下命令：

a　**ovcreg -add** <*安装目录*>**/newconfig/DataDir/conf/bbc/ovbbcrcp.xml**

b **ovc -kill**

c **ovc -start**

任务 2: 配置反向管理通道

为了利用创建的 RCP 方便仅出站防火墙环境中的入站通信，必须配置反向管理通道。要配置反向管理通道，请执行以下步骤：

1 以具有管理特权或根特权的用户身份登录到节点或管理服务器 （具体取决于其网络位置）。

2 打开命令提示符或 shell。

3 运行以下命令以创建反向管理通道：

ovconfchg [-ovrg <*服务器*>**] -ns bbc.cb -set ENABLE_REVERSE_ADMIN_CHANNELS true**

> 在群集中运行的 HPOM 管理服务器上使用命令 **ovconfchg** 时，请添加参数 **-ovrg** <*服务器*>，其中 <*服务器*> 为资源组。

4 运行以下命令以指定 RCP 详细信息：

a **ovconfchg [-ovrg** <*服务器*>**] -ns bbc.cb -set RC_CHANNELS <rcp>:<端口>[,<OvCoreId>][;<rcp2>...]**

b **ovconfchg [-ovrg** <*服务器*>**] -ns bbc.cb -set PROXY <rcp>:<端口>[,<OvCoreId>][;<rcp2>...]**

在此实例中，

<*rcp*>：配置了 RCP 的系统的 FQDN 或 IP 地址。

<*端口*>：为 RCP 配置的端口号 （在第 30 页的步骤 3 中为 SERVER_PORT 变量指定的端口）

<*OvCoreID*>：配置了 RCP 的系统的核心 ID。

另外，还可以使用配置文件提供 RCP 详细信息。有关详细信息，请参见第 32 页的用配置文件指定 RCP 详细信息。

5 *可选*。将服务器配置为自动恢复失败的反向管理通道连接。默认情况下，服务器不恢复失败的连接。要更改默认设置，请运行以下命令：

ovconfchg [-ovrg <*服务器*>**] -ns bbc.cb -set RETRY_RC_FAILED_CONNECTION TRUE**

6 *可选*。设置服务器连接 RCP 的最大尝试次数。默认情况下，此值设置为 -1（无限）。要更改默认设置，请运行以下命令：

ovconfchg [-ovrg <*服务器*>**] -ns bbc.cb -set MAX_RECONNECT_TRIES** <*尝试次数*>

7 *可选*。将管理服务器配置为在反向管理通道连接失败时生成警告消息。默认情况下，管理服务器不生成失败消息。要更改默认设置，请运行以下命令：

ovconfchg [-ovrg <*服务器*>**] -ns bbc.cb -set RC_ENABLE_FAILED_OVEVENT TRUE**

如果将 RETRY_RC_FAILED_CONNECTION 设置为 TRUE，则管理服务器不生成消息。

8 *可选*。要检查反向管理通道是否打开，请运行以下命令：

ovbbccb -status

输出中将列出所有打开的反向管理通道。

9 *可选*。要恢复失败的反向管理通道，请运行以下命令：

ovbbccb -retryfailedrcp [-ovrg <*服务器*>**]**

反向管理通道的性能注意事项

反向管理通道的性能可能取决于与通道连接的节点数。RC_MAX_WORKER_THREADS 变量可帮助您调整反向管理通道的性能。

要使用 RC_MAX_WORKER_THREADS 变量，请执行以下步骤：

1 登录到建立反向管理通道的节点。

2 记下代理程序建立通道所用的时间。可以通过运行 **ovbbccb -status** 命令确定这个时间。**ovbbccb -status** 命令输出显示来自于系统的反向管理通道的状态。重复运行 **ovbbccb -status** 命令，即可确定代理程序建立通道所用的大致时间。

3 计算建立通道的预期时间与代理程序建立通道大致所用的实际时间的比率。

4 将 RC_MAX_WORKER_THREADS 变量设置为该比率的更高位整数。使用以下命令设置此变量：

ovconfchg -ns bbc.cb -set RC_MAX_WORKER_THREADS <*最大线程数*>

用配置文件指定 RCP 详细信息

可以使用配置文件指定 RCP 的详细信息。要使用配置文件，请执行以下步骤：

1 创建文本文件。

2 按以下格式在新行中指定每个 RCP 的详细信息：

<rcp>:<端口>[,<OvCoreId>]

在此实例中，

<*rcp*>：配置了 RCP 的系统的 FQDN 或 IP 地址。

<*端口*>：为 RCP 配置的端口号 （在第 30 页的步骤 3 中为 SERVER_PORT 变量指定的端口）

<*OvCoreID*>：配置了 RCP 的系统的核心 ID。

3 将文件保存在以下位置：

<*数据目录*>\conf\bbc

4 运行以下命令：

ovconfchg [-ovrg <*服务器*>**] -ns bbc.cb -set RC_CHANNELS_CFG_FILES** <*文件名*>

在此实例中，

<*文件名*>：在第 32 页的步骤 1 中创建的文件的名称。

为多个系统配置一个 RCP

可以在 DMZ 中只配置一个 RCP，然后将 DMZ 中的其他系统配置为使用该 RCP。要达到这一目的，必须将 DMZ 中所有系统的 PROXY 变量设置为托管 RCP 的系统的 IP 地址 （或 FQDN）和端口。要将多个系统配置为使用一个 RCP，请执行以下步骤：

1 以具有根特权或管理特权的身份登录到节点。

2 打开命令提示符 (shell)。

3 运行以下命令：

ovconfchg -ns bbc.http -set PROXY
“<*rcp*>**:**<*端口*>**+**<*包含的主机*>**-**<*排除的主机*>”

在此实例中，

<*rcp*>：配置了 RCP 的系统的 FQDN 或 IP 地址。

<*端口*>：为 RCP 配置的端口号 （在第 30 页的步骤 3 中为 SERVER_PORT 变量指定的端口）

<*包含的主机* >：指定打开到 RCP 的反向管理通道的系统的 FQDN 或 IP 地址。在此场景中，必须指定属于受信任区域的管理服务器的 FQDN 或 IP 地址。如果要使用多台管理服务器，则可以指定多个 FQDN，中间用逗号隔开。

<*排除的主机*>:指定不需要通过 RCP 联系的系统的 FQDN 或 IP 地址。可以指定多个 FQDN，中间用逗号隔开。但是，必须指定本地系统的 FQDN 和主机名 （中间用逗号隔开） 。例如，
ovconfchg -ns bbc.http -set PROXY
“**<rcp>:<端口>-<本地主机>,<本地主机>.domain.com**”

4 如果系统是 HP Operations Agent 节点，请运行以下命令重新启动消息代理程序：

ovc -restart opcmsga

5 在 DMZ 中的所有系统上重复步骤 3 和步骤 4。

RCP 的性能注意事项

如果只为一个系统配置 RCP，则只要满足代理程序系统的最低要求就已足够。

如果要配置供多个代理程序节点使用的 RCP，则必须确保 RCP 系统将来能够无重大时间延迟地处理所有传入请求。

验证通过 RCP 的通信

在配置 RCP 并建立反向管理通道之后，可以执行以下任务以验证服务器与节点之间是否已成功建立通信：

任务 1： 验证与 RCP 的通信

要验证 DMZ 中的系统是否可以与 RCP 通信，请执行以下步骤：

1 以具有根特权或管理特权的身份登录到 DMZ 中的系统。

2 打开命令提示符 (shell)。

3 运行以下命令：

bbcutil -gettarget <*FQDN*>

在此实例中，<*FQDN*> 是建立到 RCP 的反向管理通道的系统的 FQDN。如果管理服务器位于受信任区域，请指定管理服务器的 FQDN。

如果 RCP 创建成功，输出应显示以下消息：

HTTP Proxy: <*rcp*>:<*端口*>

在此实例中，

<*rcp*>：配置了 RCP 的系统的 FQDN 或 IP 地址。

<*端口*>：为 RCP 配置的端口号 （在第 30 页的步骤 3 中为 SERVER_PORT 变量指定的端口）

任务 2： 检查反向管理通道

要验证是否已正确建立反向管理通道，请执行以下步骤：

1 以具有根特权或管理特权的身份登录到受信任区域中的系统。

2 打开命令提示符 (shell)。

3 运行以下命令：

ovbbccb -status

如果通道已正确建立，输出应显示以下消息：

```
HTTP Communication Reverse Channel Connections

Opened:

system1.mydomain.com:1025 BBC 11.00.000; ovbbcrcp 11.00.000

system2.mydomain.com:1025 BBC 11.00.000; ovbbcrcp 11.00.000

system3.mydomain.com:1025 BBC 11.00.000; ovbbcrcp 11.00.000

system4.mydomain.com:1025 BBC 11.00.000; ovbbcrcp 11.00.000
```

在此示例中，系统已建立到以下 RCP 系统的反向管理通道：system1、system2、system3 和 system4。

如果到 RCP 的反向管理通道失败，则 **ovbbccb -status** 命令将按以下格式显示状态：

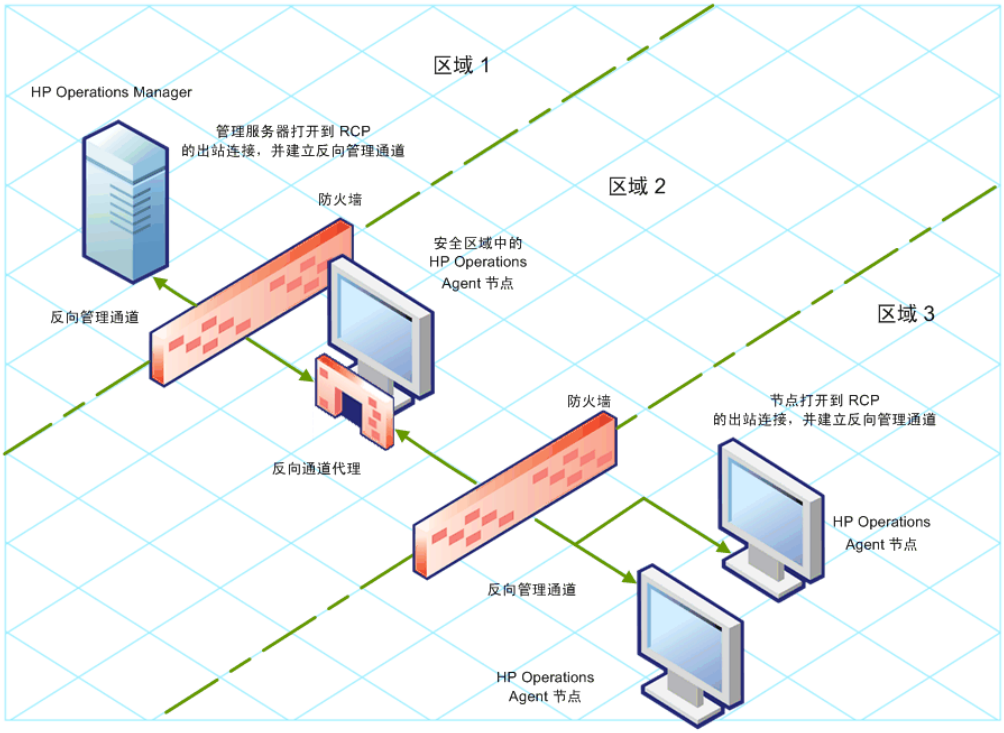
```
Pending:

system5.mydomain.com:1025 Connection To Host Failed
```

通过两个防火墙的通信

在某些情况下，管理环境中包括了两个不同防火墙：管理服务器在一个防火墙后面，节点组在另一个防火墙后面。

图 7　使用两个防火墙的安全通信



在此场景中，必须在中间区域（区域 2）中的系统上安装代理程序，并在该系统上配置 RCP。在区域 3 中配置节点并在区域 1 中配置管理服务器以建立到 RCP 的反向管理通道之后，服务器与节点通过 RCP 进行双向通信。

要在此场景中配置安全双向通信，请执行以下步骤：

1　在区域 2 中的节点上安装代理程序。

2　在区域 2 中的该节点上配置 RCP。

3　配置从管理服务器到 RCP 的反向管理通道。

4　配置从区域 3 中的节点到 RCP 的反向管理通道。

4 高可用性群集中的 HP Operations Agent

可使用 HP Operations Agent 监视高可用性 (HA) 群集中的节点。为了能监视 HA 群集中的群集感知应用程序，必须根据以下准则部署代理程序：

- 群集中的所有节点必须存在于 HPOM 控制台中受管节点的列表中。
- 必须在 HA 群集中的每个节点上安装 HP Operations Agent。
- **虚拟节点。**如果使用安装了 HPOM for UNIX 8.35、 HPOM on UNIX/Linux 9.1x 或 HPOM for Windows 9.00 的节点，可以利用虚拟节点的概念。虚拟节点是由常用资源组链接的一组物理节点。代理程序可以根据资源组中的更改，在物理节点上自动启用或禁用策略。

  对于 HPOM for Windows 8.1x，虚拟节点功能不可用。

  要监视 HA 群集中的节点，请只在虚拟节点上而不是在每个物理节点上部署监视策略。因此，在开始监视群集感知应用程序之前就在 HPOM 控制台中创建 HA 群集的虚拟节点很重要。

  以下是在 HPOM 控制台中创建虚拟节点的准则：

  — 虚拟节点本身不能是物理节点。

  — 虚拟节点不支持 DHCP、自动部署和证书。

  — 不能在虚拟节点上安装代理程序。

监视 HA 群集中的节点

可将 HP Operations Agent 配置为监视在 HA 群集中的节点上运行的群集感知应用程序。

要监视 HA 群集中的节点上的群集感知应用程序，请执行以下步骤：

1 *仅限 Microsoft Cluster Server 群集。*请确保包含被监视资源的资源组包含网络名称和 IP 地址资源。

2 识别您需要用来监视群集感知应用程序的策略。

3 创建描述群集感知应用程序的 XML 文件，并将它命名为 `apminfo.xml`。

  此文件用于定义将监视的资源组，并将这些资源组映射到应用程序实例。

apminfo.xml 文件有以下格式：

apminfo.xml 文件中的包标记之间不允许有换行符。

```
<?xml version="1.0" ?>
   <APMClusterConfiguration>
       <Application>
            <Name> 群集感知应用程序的名称。 </Name>
                 <Instance>
                <Name> 第一个实例的应用程序名称。
实例名称用于启动和停止命令，并对应于消息中指定此实例的名称。
</Name>
                   <Package> 运行应用程序的第一个实例的资源组。 </Package>
                 </Instance>
                 <Instance>
                    <Name> 第二个实例的应用程序名称。 </Name>
                    <Package> 运行应用程序的第二个实例的资源组。 </Package>
                 </Instance>
           </Application>
        </APMClusterConfiguration>
```

apminfo.xml 的 DTD

```
<!ELEMENT APMClusterConfiguration (Application+)>
<!ELEMENT Application (Name, Instance+)>
<!ELEMENT Name (#PCDATA)>
<!ELEMENT Instance (Name, Package)>
<!ELEMENT Package (#PCDATA)>
```

示例

在下面的示例中，资源组的名称是 **SQL-Server**，网络 （或实例）名称是 CLUSTER04：

```
<?xml version="1.0" ?>
<APMClusterConfiguration>
<Application>
<Name>dbspi_mssqlserver</Name>
<Instance>
<Name>CLUSTER04</Name>
<Package>SQL-Server</Package>
</Instance>
```

```
</Application>

</APMClusterConfiguration>
```

4 将群集中每个节点上完成的 apminfo.xml 文件保存在以下目录中：

- 在 Windows 上：*%OvDataDir%*conf\conf\
- 在 UNIX/Linux 上：/var/opt/OV/conf/conf/

5 创建描述要成为群集感知的策略的 XML 文件。文件名的格式必须是 <*应用程序名称*>.apm.xml。<*应用程序名称*> 必须与 apminfo.xml 文件中的 <Application><Name> 标记的内容相同。<*应用程序名称*>.apm.xml 文件包括在步骤 2 中标识的策略名称。

创建 <*应用程序名称*>.apm.xml 文件时，请使用以下格式：

```
<?xml version="1.0" ?>

  <APMApplicationConfiguration>

  <Application>

 <Name> 群集感知应用程序的名称 （必须与 apminfo.xml 文件中的
<Application><Name> 的内容匹配）。 </Name>

  <Template> 应为群集感知的第一个策略。 </Template>

  <Template> 应为群集感知的第二个策略。 </Template>

<startCommand> 可选命令，每当应用程序的实例启动时，代理程序即运行该命令。
</startCommand>

<stopCommand> 可选命令，每当应用程序的实例停止时，代理程序即运行该命令。
</stopCommand>

  </Application>

  </APMApplicationConfiguration>
```

停止和启动命令可以使用以下变量：

变量	描述
$instanceName	要启动或停止的实例的名称（如 <Instance><Name> 中所列）。
$instancePackage	要启动或停止的资源组的名称（如 <Instance><Package> 中所列）。
$remainingInstances	此应用程序的剩余实例数。
$openViewDirectory	代理程序上的命令目录。

示例

以下名为 dbspi_mssqlserver.apm.xml 的示例文件显示数据库的智能插件如何配置 Microsoft SQL Server 的策略。

```
<?xml version="1.0"?>

<APMApplicationConfiguration>

<Application>
```

```
<Name>dbspi_mssqlserver</Name>
<Template>DBSPI-MSS-05min-Reporter</Template>
<Template>DBSPI-MSS-1d-Reporter</Template>
<Template>DBSPI-MSS-05min</Template>
<Template>DBSPI-MSS-15min</Template>
<Template>DBSPI-MSS-1h</Template>
<Template>DBSPI-MSS6-05min</Template>
<Template>DBSPI-MSS6-15min</Template>
<Template>DBSPI-MSS6-1h</Template>
<Template>DBSPI Microsoft SQL Server</Template>
<StartCommand>dbspicol ON $instanceName</StartCommand>
<StopCommand>dbspicol OFF $instanceName</StopCommand>
</Application>
</APMApplicationConfiguration>
```

6 将群集中每个节点上完成的<*应用程序名称*>.apm.xml 文件保存在以下目录中：

- 在 Windows 上：*%OvDataDir%*bin\instrumentation\conf
- 在 UNIX/Linux 上：/var/opt/OV/bin/instrumentation/conf

7 确保资源组所在的物理节点都是受管节点。

8 运行以下命令，在所有物理节点上检查 XML 文件的语法：

- 在 Windows 上：*%OvInstallDir%***\bin\ovappinstance -vc**
- 在 HP-UX、 Linux 或 Solaris 上：**/opt/OV/bin/ovappinstance -vc**
- 在 AIX 上：**/usr/lpp/OV/bin/ovappinstance -vc**

9 *可选*。某些物理节点 （如多宿主主机）的标准主机名可能与群集配置中节点的名称不同。如果是这样，代理程序将无法正确判断资源组的当前状态。将代理程序配置为使用它在群集配置中的主机名：

a 获取物理节点在群集配置中的名称：

ovclusterinfo -a

b 将代理程序配置为使用它在群集配置中的节点名称：

ovconfchg -ns conf.cluster -set CLUSTER_LOCAL_NODENAME <*名称*>

在此实例中， <*名称*> 是在 **ovclusterinfo -a** 的输出中报告的节点的名称。

10 运行以下命令，在每个物理节点上重新启动代理程序：

a **ovc -stop**

b **ovc -start**

11 如果使用 HPOM for Windows 8.1x，则在 HA 群集中的所有物理节点上部署标识用于监视群集感知应用程序的策略 （步骤 2 中）。

对于所有其他类型的管理服务器，则在为群集创建的虚拟节点上部署标识用于监视群集感知应用程序的策略 （步骤 2 中）。

代理程序用户

默认情况下， HP Operations Agent 定期检查资源组的状态。在 UNIX 和 Linux 节点上，代理程序使用特定于群集应用程序的命令，这些命令通常只能由根用户运行。在 Windows 节点上，代理程序使用 API，而不是运行命令。

如果更改代理程序的用户，则代理程序可能不再具有成功运行群集命令所需的权限。在这种情况下，运行群集命令时，必须将代理程序配置为使用安全程序 （如 sudo 或 .do）。

要将用非根帐户运行的代理程序配置为运行群集命令，请执行以下步骤：

1 以具有根特权的身份登录到节点。

2 转到以下目录：

在 HP-UX、Linux 或 Solaris 上：

`/opt/OV/bin`

在 AIX 上：

`/usr/lpp/OV/bin`

3 运行以下命令停止代理程序：

`ovc -kill`

4 要将代理程序配置为使用安全程序，请输入以下命令：

`ovconfchg -ns ctrl.sudo -set OV_SUDO` <*安全程序*>

在此实例中， <*安全程序*> 是希望代理程序使用的程序的名称，例如 `/usr/local/bin/.do`。

5 运行以下命令启动代理程序：

`ovc -start`

5 远程配置性能收集组件

可以从管理服务器远程对受管节点执行某些配置任务。除了在每个节点上本地执行性能收集组件的配置任务外，还可以从 HPOM 控制台使用一组特殊的策略和工具来配置并使用性能收集组件的多个节点。

只有在 HPOM for Windows 或 HPOM on UNIX/Linux 管理服务器上安装了 HP Operations Agent 部署包时，此功能才可用。在 HPOM for UNIX 8.x 管理服务器上，此功能不可用。

开始之前

开始从 HPOM 控制台远程配置和控制性能收集组件之前，必须在运行代理程序的节点上部署 `HP Operations Agent` 检测组中的检测文件。

要从 HPOM for Windows 控制台部署检测，请执行以下步骤：

如果监视群集节点，请确保在构成群集的所有节点上部署检测，不要在虚拟节点上部署

1. 在控制台树中，右键单击运行代理程序的节点或节点组，然后单击**所有任务 (All Tasks) > 部署检测 (Deploy Instrumentation)**。将打开 “部署检测 (Deploy Instrumentation)” 对话框。
2. 在 “部署检测 (Deploy Instrumentation)” 对话框中，单击 **HP Operations Agent**，然后单击**确定 (OK)**。开始在节点上部署必要的检测文件。

要从 HPOM on UNIX/Linux 控制台部署检测，请执行以下步骤：

如果监视群集节点，请确保在构成群集的所有节点上部署检测，不要在虚拟节点上部署。

1. 登录到管理 UI。
2. 单击**部署 (Deployment) > 部署配置 (Deploy Configuration)**。
3. 在 “分布参数 (Distribution Parameters)” 部分选择 “检测 (Instrumentation)”，然后单击**请选择 (Please Select)**。将打开 “选择器 (Selector)” 弹出框。
4. 在 “选择器 (Selector)” 弹出框中，选择运行代理程序的节点。
5. 选择 “强制更新 (Force Update)” 选项覆盖旧的检测文件。

   在从旧版本的代理程序升级的节点上选择此选项。

6. 单击**分发 (Distribute)**。

部署 OA-PerfCollComp-opcmsg 策略

当性能收集组件生成警报时，OA-PerfCollComp-opcmsg 策略将警报消息发送到 HPOM 消息浏览器。该策略位于 **HP Operations Agent > 性能收集组件 (Performance Collection Component) > 消息拦截器 (Message Interceptor)** 策略组中。在部署性能收集组件的其他策略之前，先在节点上部署此策略。

如果监视群集节点，请确保在构成群集的所有节点上部署策略，不要在虚拟节点上部署。

配置性能收集组件

HP Operations Agent 的性能收集组件的行为取决于以下文件中指定的配置设置：

- 收集参数文件 (`parm`)
- 警报定义文件 (`alarmdef`)

有关收集参数和警报定义文件的详细信息，请参见《HP Operations Agent 概念指南》中的 *“性能收集组件”* 部分。

配置 parm 文件

`parm` 文件定义 scope 收集器的数据收集机制。 HP Operations Agent 在每个节点上放置 `parm` 文件，该文件可在以下路径中找到：

- 在 HP-UX、 Solaris、 AIX 和 Linux 上：`/var/opt/perf/`
- 在 Windows 上：*%ovdatadir%*

您可以修改 `parm` 文件中指定的设置，以自定义数据收集机制。但是，如果用 HP Operations Agent 管理很多节点，在每个节点上修改 `parm` 文件的每个单独副本就变得有些困难。

使用 HPOM 控制台，可以从管理服务器将修改后的 `parm` 文件集中部署到多个节点。

从 HPOM for Windows

HPOM for Windows 控制台为您提供 ConfigFile 策略，这些策略帮助您从中央管理服务器跨多个节点部署对 `parm` 文件的任何更改。不同 ConfigFile 策略可用于不同的节点操作系统。

要通过编辑 `parm` 文件修改收集机制，请执行以下步骤：

1. 标识希望修改后的收集机制生效的节点。
2. 在控制台树中，单击**策略管理 (Policy management) → 策略组 (Policy groups) → HP Operations Agent → 性能收集组件 (Performance Collection Component) → 收集配置 (Collection configuration)**。用于配置 `parm` 文件的 ConfigFile 策略显示在详细信息窗格中。
3. 为希望修改后的收集机制生效的平台双击 ConfigFile 策略 （例如：对于 HP-UX，双击 `parm` 文件）。将打开 “<*平台*> 的 `parm` 文件”对话框。

4 在“数据 (Data)”选项卡中修改设置。有关 parm 文件中配置参数的更多详细信息，请参见《HP Operations Agent 用户指南》中的 *“parm 文件参数”* 部分。

5 单击**保存并关闭 (Save and Close)**。在详细信息窗格中，策略的版本增加了 .1。

6 在您选择的节点上部署更新后的策略。

如果监视群集节点，请确保在构成群集的所有节点上部署策略，不要在虚拟节点上部署。

从 HPOM on UNIX/Linux 9.10

HPOM on UNIX/Linux 9.10 控制台为您提供 ConfigFile 策略，这些策略帮助您从中央管理服务器跨多个节点部署对 parm 文件的任何更改。不同 ConfigFile 策略可用于不同的节点操作系统。

要从 HPOM for UNIX 9.10 控制台通过编辑 parm 文件修改收集机制，请执行以下步骤：

1 标识希望修改后的收集机制生效的节点。

2 在控制台中，单击**浏览 (Browse)** → **所有策略组 (All Policy Groups)**。页面上将显示所有可用策略组的列表。

3 单击 **H**。将显示 HP Operations Agent 策略组。

4 单击 **HP Operations Agent**，单击**性能收集组件 (Performance Collection Component)**，然后单击**收集配置 (Collection Configuration)**。将显示 parm 文件的可用 ConfigFile 策略的列表。

5 为希望修改后的收集机制生效的平台单击 ConfigFile 策略。将显示**策略 “OA_<*平台*> ParmPolicy”** 页面。

6 单击  ，然后单击**编辑 （原始模式）**。将显示 “编辑配置文件策略...(Edit Config File policy...)” 页面。

7 在“内容 (Content)”选项卡中修改设置。有关 parm 文件中配置参数的更多详细信息，请参见《HP Operations Agent 用户指南》中的 *“parm 文件参数”* 部分。

8 单击**保存 (Save)**。

9 在您选择的节点上部署更新后的策略。

如果监视群集节点，请确保在构成群集的所有节点上部署策略，不要在虚拟节点上部署。

配置 alarmdef 文件

警报定义文件 (alarmdef) 为性能子代理程序提供默认警报生成流程规范。HP Operations Agent 在每个节点上放置 alarmdef 文件，该文件可在以下路径中找到：

- 在 HP-UX、 Solaris、 AIX 和 Linux 上：/var/opt/perf/
- 在 Windows 上：*%ovdatadir%*

您可以修改 alarmdef 文件中的默认设置，以自定义警报生成机制。可以使用 HPOM 控制台在多个节点上集中分发修改后的 alarmdef 文件。

从 HPOM for Windows

HPOM for Windows 控制台为您提供 ConfigFile 策略，这些策略帮助您从中央管理服务器跨多个节点部署对 `parm` 文件的任何更改。不同 ConfigFile 策略可用于不同的节点操作系统。

要通过编辑 `alarmdef` 文件修改收集机制，请执行以下步骤：

1 标识希望修改后的收集机制生效的节点。

2 在控制台树中，单击**策略管理 (Policy management)** → **策略组 (Policy groups)** → **HP Operations Agent** → **性能收集组件 (Performance Collection Component)** → **警报定义 (Alarm definition)**。用于配置 `alarmdef` 文件的 ConfigFile 策略显示在详细信息窗格中。

3 为希望修改后的收集机制生效的平台双击 ConfigFile 策略（例如：对于 HP-UX，双击 alarmdef 文件）。将打开 ***"<平台> 的 alarmdef 文件"*** 对话框。

4 在“数据 (Data)”选项卡中修改设置。有关 `alarmdef` 文件中配置参数的更多详细信息，请参见《HP Operations Agent 用户指南》中的 *"alarmdef 文件参数"* 部分。

5 单击**保存并关闭 (Save and Close)**。在详细信息窗格中，策略的版本增加了 `.1`。

6 在您选择的节点上部署更新后的策略。

如果监视群集节点，请确保在构成群集的所有节点上部署策略，不要在虚拟节点上部署。

从 HPOM on UNIX/Linux 9.10

HPOM on UNIX/Linux 9.10 控制台为您提供 ConfigFile 策略，这些策略帮助您从中央管理服务器跨多个节点部署对 `alarmdef` 文件的任何更改。不同 ConfigFile 策略可用于不同的节点操作系统。

要从 HPOM for UNIX 9.10 控制台通过编辑 `alarmdef` 文件修改收集机制，请执行以下步骤：

1 标识希望修改后的警报机制生效的节点。

2 在控制台中，单击**浏览 (Browse)** → **所有策略组 (All Policy Groups)**。页面上将显示所有可用策略组的列表。

3 单击 **H**。将显示 HP Operations Agent 策略组。

4 单击 **HP Operations Agent**，单击**性能收集组件 (Performance Collection Component)**，然后单击**警报定义 (Alarm Definition)**。将显示 `alarmdef` 文件的可用 ConfigFile 策略的列表。

5 为希望修改后的收集机制生效的平台单击 ConfigFile 策略。将显示**策略 "OA_<*平台*> AlarmdefPolicy"** 页面。

6 单击  ，然后单击**编辑 （原始模式）**。将显示 “编辑配置文件策略...(Edit Config File policy...)” 页面。

7 在 “内容 (Content)” 选项卡中修改设置。有关 `alarmdef` 文件中配置参数的更多详细信息，请参见《HP Operations Agent 用户指南》中的 *"alarmdef 文件参数"* 部分。

8 单击**保存 (Save)**。

9 在您选择的节点上部署更新后的策略。

如果监视群集节点，请确保在构成群集的所有节点上部署策略，不要在虚拟节点上部署。

远程使用 HP Operations Agent

可以用 HPOM 控制台启动、停止、监视和查看 HP Operations Agent 的详细信息。可以从 HPOM 控制台使用不同工具管理 HP Operations Agent 的操作。必须在部署代理程序的节点上启动这些工具。运行工具的结果显示在以下部分中：

- *HPOM for Windows*

  “工具状态 (Tool Status)”窗口中的 “工具输出 (Tool Output)”部分

- *HPOM on UNIX/Linux*

  Java GUI (HPOM for UNIX Operational UI) 中的 “应用程序输出 (Application Output)”窗口

可以从 HPOM 控制台使用以下工具：

启动代理程序	在受管节点上启动 HP Operations Agent。
停止代理程序	在受管节点上停止 HP Operations Agent。
重新启动代理程序	在受管节点上重新启动 HP Operations Agent。
查看状态	查看受管节点上 HP Operations Agent 进程、服务和守护进程的状态。
查看版本信息	查看受管节点上 HP Operations Agent 的版本。
刷新警报服务	刷新性能收集组件的警报服务。
扫描性能组件的日志文件	扫描节点上的 scope 收集器使用的日志文件。
检查性能组件的参数文件语法	帮助您检查受管节点中参数文件的语法。
检查性能组件的 alarmdef 文件语法	帮助您检查受管节点中 alarmdef 文件的语法。

查看策略部署后操作的状态	帮助您检查节点上 parm 或 alarmdef 策略的部署状态。启动此工具时，请确保将 `parm` 或 `alarmdef`（根据适用情况）指定为工具参数。 可以在使用 HPOM for Windows 时，在 “编辑参数 (Edit Parameters)” 窗口中的 “参数 (Parameter)” 框中设置工具参数。 使用 HPOM on UNIX/Linux 时，打开该工具的 “编辑工具状态 (Edit Tool Status)” 页面，转到 “OVO 工具 (OVO Tool)” 选项卡，然后在 “参数 (Parameters)” 框中指定工具参数
设置 Realtime 永久许可证	设置 HP Ops OS Inst to Realtime Inst LTU 的永久许可证。
设置 Glance 永久许可证	设置 Glance Software LTU 的永久许可证。
获取许可证状态	显示节点上 LTU 的状态。

6 监视 HP Operations Agent

HP Operations Agent 部署包为您提供一组监视 HP Operations Agent 运行状况的策略。使用这些策略，您可以确保必要的代理程序进程未停止，且未处于无响应状态。

在 HPOM 管理服务器上安装 HP Operations Agent 部署包时，将创建自监视策略组。自监视策略组包括确保 HP Operations Agent 平稳运行所需的策略。

只有在 HPOM for Windows 或 HPOM on UNIX/Linu 管理服务器上安装了 HP Operations Agent 部署包时，自监视策略组和监视 HP Operations Agent 进程运行状况的策略才可用。在 HPOM for UNIX 8.x 管理服务器上，这些策略不可用。

开始之前

开始用自监视策略监视 HP Operations Agent 之前，必须在运行代理程序的节点上部署 `HP Operations Agent` 检测组中的检测文件。

要从 HPOM for Windows 控制台部署检测，请执行以下步骤：

如果监视群集节点，请确保在构成群集的所有节点上部署检测，不要在虚拟节点上部署。

1. 在控制台树中，右键单击运行代理程序的节点或节点组，然后单击**所有任务 (All Tasks) > 部署检测 (Deploy Instrumentation)**。将打开 “部署检测 (Deploy Instrumentation)” 对话框。
2. 在 “部署检测 (Deploy Instrumentation)” 对话框中，单击 **HP Operations Agent**，然后单击**确定 (OK)**。开始在节点上部署必要的检测文件。

要部署检测，请执行以下步骤：

如果监视群集节点，请确保在构成群集的所有节点上部署检测，不要在虚拟节点上部署。

1. 登录到管理 UI。
2. 单击**部署 (Deployment) > 部署配置 (Deploy Configuration)**。
3. 在 “分布参数 (Distribution Parameters)” 部分选择 “检测 (Instrumentation)”，然后单击**请选择 (Please Select)**。将打开 “选择器 (Selector)” 弹出框。
4. 在 “选择器 (Selector)” 弹出框中，选择运行代理程序的节点。

5 选择 “强制更新 (Force Update)” 选项覆盖旧的检测文件。

在从旧版本的代理程序升级的节点上选择此选项。

6 单击**分发 (Distribute)**。

自监视策略

可使用自监视策略监视 HP Operations Agent 的以下组件的运行状况：

- **opcmona** （监视代理程序）
- **opcmsga** （消息代理程序）
- **opcmsgi** （消息拦截器）
- **opcacta** （操作代理程序）
- **scope** （数据收集器）
- **opcle** （日志文件封装器）
- **opctrapi** （陷阱拦截器）
- **coda** （通信守护进程）
- **perfd**

自监视策略组包括以下策略：

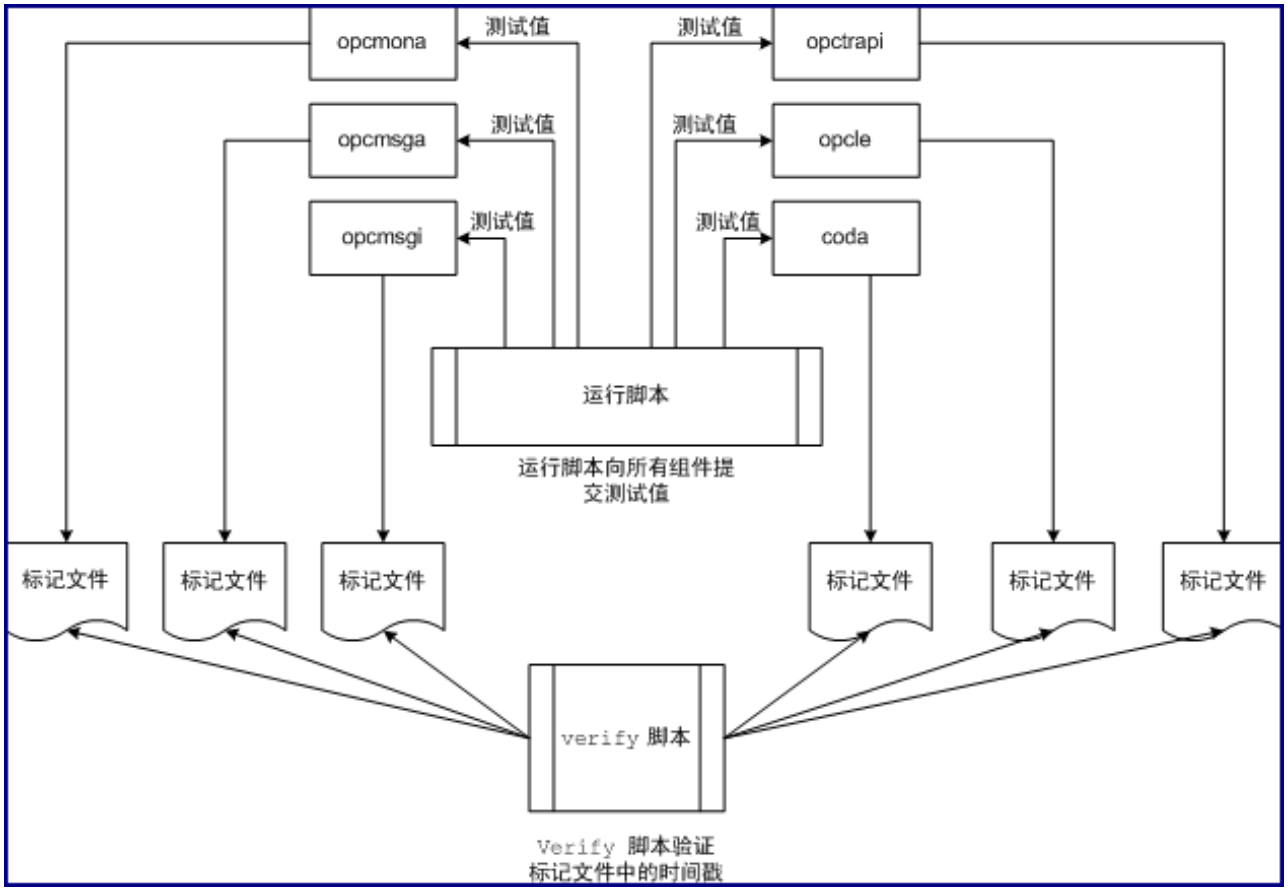
- **OA-SelfMonTstMonaExt**：测试监视代理程序。
- **OA-SelfMonVerifyMon**：由监视代理程序验证标记文件
- **OA-SelfMonTstLe**：测试日志文件封装器
- **OA-SelfMonVerifyLe**：由日志文件封装器验证标记文件
- **OA-SelfMonTstTrapi**：测试 SNMP 陷阱拦截器
- **OA-SelfMonTstMsgi**：测试消息拦截器
- **OA-SelfMonTstActa**：测试操作代理程序
- **OA-SelfMonTstAll**：测试除 `opcle`、 `opcmona`、 `opcmsgi` 和 `opctrapi` 以外的所有进程。

要监视 `opctrapi` 组件的运行状况和可用性，必须正在节点上运行 SNMP 陷阱守护进程 / 服务。

用 `HP Operations Agent` 检测组部署的脚本和程序将测试值（一分钟一次）发送到 HP Operations Agent 的不同组件。同时为每个监视的组件创建**标记文件**。监视的组件成功接收来自于 `HP Operations Agent` 检测脚本的测试值后，相应标记文件将用时间戳更新。

`HP Operations Agent` 检测的 `verify` 脚本持续 （**三分钟**一次）监视标记文件的状态。当脚本发现标记文件中的时间戳早于当前时间时 （意味着监视的组件未能收到测试值），会将警报消息发送到 HPOM 消息浏览器。

图 8　自监视脚本的工作流程



部署自监视策略

不能选择性地部署自监视策略组中可用的策略。这些策略相互依赖，因此，所有策略都必须同时部署在节点上。

要从 HPOM for Windows 控制台部署自监视策略，请执行以下步骤：

1　在 HPOM 控制台的控制台树中，展开**策略管理 (Policy management) > 策略组 (Policy groups) > HP Operations Agent**。

2　右键单击 “自监视 (Self Monitoring)”，然后在单击**所有任务 (All Tasks) > 部署到 (Deploy on)**。将打开 “将策略部署到 (Deploy Policies on)” 对话框。

3　在 “将策略部署到 (Deploy Policies on)” 对话框中选择节点，然后单击**确定 (OK)**。 HPOM 开始在所选节点上部署自监视策略。

如果监视群集节点，请确保在构成群集的所有节点上部署策略，不要在虚拟节点上部署。

要从 HPOM on UNIX/Linux 控制台部署自监视策略，请执行以下步骤：

1 登录到管理 UI。

2 单击 **OMU**，然后单击**浏览 (Browse) > 所有策略组 (All Policy Groups)**。将打开 “所有策略组 (All Policy Groups)” 页面。

3 在 “所有策略组 (All Policy Groups)” 页面上选择 **HP Operations Agent** 策略组，从 “选择操作 (Choose an Action)” 下拉列表中选择**分配到节点 / 节点组 (Assign to Node/Node Group)**，然后单击  。将打开 “选择器 (Selector)” 弹出框。

4 在 “选择器 (Selector)” 弹出框中，选择运行代理程序的节点，然后单击**确定 (OK)**。

如果监视群集节点，请确保在构成群集的所有节点上部署策略，不要在虚拟节点上部署。

查看组件的状态

当自监视策略在一个组件中检测到故障时，它们将触发代理程序将相应的警报消息发送到 HPOM 消息浏览器。来自于自监视策略的消息始终带有前缀 `Self Monitor`。可以打开带 `Self Monitor` 前缀的消息来查看故障的详细信息。

此外，可以检查节点上的标记文件，以检查代理程序组件是否在运行。标记文件可在以下位置找到：

- *在 Windows 上：%ovdatadir%*`tmp\OpC\selfmon`
- *在 UNIX/Linux 上：*`/var/opt/OV/tmp/selfmon`

可以用文本编辑器程序打开标记文件，并检查最后的时间戳。如果最后的时间戳早于三分钟，则可以判定监视的组件未正常运行。

索引