Hewlett Packard Enterprise

HPE Network Node Manager i Software

软件版本：10.20
适用于 Windows® 和 Linux® 操作系统

部署参考

文档发布日期：2016 年 6 月
软件发布日期：2016 年 6 月

法律声明

担保

Hewlett Packard Enterprise 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。HPE 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 HPE 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。

Oracle Technology - 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 - 受限权利(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，请访问 NNMi 产品 DVD 上的 license-agreements 目录。

版权声明

© 版权所有 2008-2016 Hewlett Packard Enterprise Development LP

商标声明

Adobe® 是 Adobe Systems Incorporated 的商标。

Apple 是 Apple Computer, Inc. 在美国和其他国家/地区的注册商标。

AMD 是 Advanced Micro Devices, Inc. 的商标。

Google™ 是 Google Inc. 的注册商标。

Intel®、Intel® Itanium®、Intel® Xeon® 和 Itanium® 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。

Internet Explorer、Lync、Microsoft、Windows 和 Windows Server 是 Microsoft Corporation 在美国和/或其他国家/地区的注册商标或商标。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。

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

sFlow 是 InMon Corp 的注册商标。

UNIX® 是 The Open Group 的注册商标。

致谢

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

本产品包含由 Visigoth Software Society (http://www.visigoths.org/) 开发的软件。

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.hpe.com/group/softwaresupport/search-result?keyword= 。

此站点要求使用 HP Passport 帐户。如果还不具有该帐户，请单击 HP Passport“Sign in”页面上的 **Create an account** 按钮。

支持

请访问 HPE 软件支持网站：**https://softwaresupport.hpe.com**

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

HPE 软件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 HPE 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://softwaresupport.hpe.com**，然后单击 **注册**。

要查找有关访问级别的详细信息，请访问：
https://softwaresupport.hpe.com/web/softwaresupport/access-levels

目录

第 1 章:关于本指南 19
本指南包含哪些内容? 19
本文档中使用的路径约定 19
修订历史 20
有关 NNMi 的详细信息 20

第 2 章:准备 22
硬件和软件要求 22
支持的硬件和软件 22
检查必需补丁程序 23
系统配置 (Linux) 23
安装 NNMi 和 NNM iSPI 23
NNMi 共存 23
NNM i Smart Plug-In 版本要求 23

第 3 章:配置 24
配置的常规概念 25
任务流模型 26
最佳实践:保存现有配置 26
最佳实践:使用作者属性 26
用户界面模型 26
排序 27
节点组和接口组 27
分组重叠 28
节点组成员资格 28
层次结构/包含 29
设备筛选 29
其他筛选 29
其他节点 30
节点组状态 30
接口组 30
节点接口和地址层次结构 31
重置 NNMi 配置和数据库 31
NNMi 通信 33
通信的概念 34
通信配置的级别 34
网络延迟和超时 35
SNMP 访问控制 35
高可用性 (HA) 环境中的 SNMP 访问控制 36
SNMP 版本首选项 36
管理地址首选项 37
SNMPv3 陷阱和通知 37
轮询协议 38

通信配置和 nnmsnmp*.ovpl 命令 38
计划通信 38
默认通信设置 39
通信配置区域 39
特定节点配置 40
重试和超时值 40
活动协议 40
多个团体字符串或验证配置文件 40
SNMPv1 和 SNMPv2 团体字符串 41
SNMPv3 验证配置文件 41
配置通信 41
配置 SNMP 代理设置 42
使用网络配置协议 (NETCONF) 的设备支持 43
什么是网络配置协议 (NETCONF)? 43
网络配置协议 (NETCONF) 操作 43
在被管设备上启用并配置网络配置协议 (NETCONF) 44
在 NNMi 中配置网络配置协议 (NETCONF) 设备凭据 44
配置虚拟环境的通信 44
监视管理程序上托管的虚拟机的先决条件 45
替换 VMware 默认证书 46
将 NNMi 配置为使用 HTTPS 与管理程序通信 46
启用 HTTP 与管理程序通信 48
评估通信 49
是否为 SNMP 配置了所有节点? 49
SNMP 访问当前是否对设备可用? 49
SNMP 设备的管理 IP 地址是否正确? 49
NNMi 使用的通信设置是否正确? 49
状况轮询器设置是否符合通信设置? 50
微调通信 50
NNMi 发现 51
发现的概念 52
NNMi 通过设备配置文件得出属性 53
计划发现 53
选择您的主发现方式 53
基于列表的发现 53
基于规则的发现 54
自动发现规则 55
自动发现规则排序 55
从发现中排除设备 55
Ping 扫描 55
自动发现规则的发现种子 56
自动发现规则的最佳实践 56
发现规则重叠 56
限制设备类型发现 57
节点名称解析 57
子网连接规则 57
发现种子 58
重新发现间隔 58

不发现对象 59
发现接口范围 59
通过 NNMi 监视虚拟 IP 地址 59
使用来自 SNMP 陷阱的发现提示 60
配置发现 60
配置自动发现规则的提示 60
配置种子的提示 61
发现链路聚合 61
发现服务器到交换机链路聚合 (S2SLA) 61
评估发现 62
跟踪初始发现的进度 62
所有种子都发现了吗？ 62
所有节点都具有有效的设备配置文件吗？ 63
所有节点都正确发现了吗？ 63
自动发现规则 63
IP 地址范围 64
系统对象 ID 范围 64
所有连接和 VLAN 都正确吗？ 64
评估第 2 层连接 64
NNMi 发现与重复的 MAC 地址 65
重新发现设备 65
调整发现 65
发现日志文件 66
未编号接口 66
控制无响应对象的删除操作 66
NNMi 状况轮询 67
状况轮询的概念 68
计划状况轮询 68
轮询清单 68
NNMi 可以监视什么？ 69
停止监视 70
到未监视节点的接口 70
扩展监视 71
计划组 71
接口组 72
节点组 73
计划轮询间隔 74
决定要采集的数据 74
决定要发送到 NNMi 的 SNMP 陷阱 75
配置状况轮询 76
配置接口组和节点组 76
配置接口监视 77
配置节点监视 77
验证默认设置 77
评估状况轮询 78
验证网络监视的配置 78
接口或节点所属的组是否正确？ 78
要应用哪些设置？ 78

要采集哪些数据？ 78
评估状态轮询的性能 79
状况轮询器是否一直在运行？ 79
调整状况轮询 80
NNMi 事件 81
事件的概念 82
事件生命周期 82
陷阱和事件转发 83
比较：将第三方 SNMP 陷阱转发到其他应用程序 84
MIB 85
自定义事件属性 85
添加到已关闭的管理事件的 CIA 86
事件减少 87
事件抑制、强化和减弱 87
生命周期转换操作 88
计划事件 88
NNMi 应处理哪些设备陷阱？ 88
NNMi 应显示哪些事件？ 88
NNMi 应如何响应事件？ 88
NNMi 应将陷阱转发到另一个事件接收器吗？ 89
配置事件 89
配置事件抑制、强化和减弱 89
配置生命周期转换操作 89
配置陷阱日志 90
配置事件日志记录 90
配置陷阱服务器属性 90
配置分配事件时用户名排序顺序所用的语言环境 91
批处理加载事件配置 92
使用 nnmincidentcfgdump.ovpl 生成事件配置文件 92
使用 nnmincidentcfgload.ovpl 加载事件配置 93
评估事件 94
调整事件 94
启用和配置未定义陷阱的事件 94
NNMi 控制台 96
减少在网络概述图中显示的最大节点数 97
减少节点组图上显示的节点数 97
在分析窗格中配置量表 98
限制显示的量表数 98
设置分析窗格中的量表刷新率 98
排除不显示的量表 98
控制节点量表的显示顺序 99
控制接口量表的显示顺序 99
控制自定义轮询器量表的显示顺序 99
了解如何应用量表属性 99
解决量表问题 100
显示的量表太多 100
配置图标签缩放大小和边框 100
配置 Loom 和 Wheel 图的自动折叠阈值 101

禁用分析窗格 101
自定义设备配置文件图标 102
配置表视图的刷新率 102
NNMi 审核 103
禁用审核 105
指定保留 NNMi 审核日志的天数 105
配置 NNMi 审核日志文件中包含的操作 106
关于 NNMi 审核日志文件 107

第 4 章: 恢复能力 109
为 NNMi 配置应用程序故障转移 111
应用程序故障转移概述 112
应用程序故障转移要求 112
为 NNMi 设置应用程序故障转移 113
使用 NNMi 群集设置向导配置群集(仅限嵌入式数据库用户) 115
设置群集通信(可选) 116
使用应用程序故障转移功能 117
使用嵌入式数据库的应用程序故障转移行为 117
使用 Oracle 数据库的应用程序故障转移行为 119
应用程序故障转移场景 121
其他 ovstart 和 ovstop 选项 121
应用程序故障转移事件 121
故障转移后恢复原始配置 122
NNM iSPI 和应用程序故障转移 122
使用嵌入式数据库时的 NNM iSPI 安装信息 122
将 NNM iSPI 部署在现有应用程序故障转移环境中 - 嵌入式数据库 122
随 NNMi 部署 NNM iSPI，然后配置应用程序故障转移 - 嵌入式数据库 124
使用 Oracle 数据库时的 NNM iSPI 安装信息 124
将 NNM iSPI 部署在现有 NNMi 应用程序故障转移环境中 - Oracle 数据库 124
随 NNMi 部署 NNM iSPI，然后配置应用程序故障转移 - Oracle 数据库 125
集成应用程序 126
禁用应用程序故障转移 126
管理任务和应用程序故障转移 128
恢复 NNMi 故障转移环境 128
应用程序故障转移和 NNMi 补丁程序 129
为应用程序故障转移应用补丁程序(关闭活动和备用服务器) 129
为应用程序故障转移应用补丁程序(保留一个活动 NNMi 管理服务器) 131
应用程序故障转移和重新启动 NNMi 管理服务器 133
通信失败后的应用程序故障转移控制 133
应用程序故障转移和从以前的数据库备份恢复(仅嵌入式数据库) 133
群集文件传输警告配置 134
网络延迟/带宽注意事项 134
应用程序故障转移和 NNMi 嵌入式数据库 135
应用程序故障转移环境中的网络流量 136
应用程序故障转移流量测试 136
在高可用性群集中配置 NNMi 138
高可用性概念 139
高可用性术语 140

NNMi 高可用性群集场景 141
联机帮助页 145
验证配置 NNMi 以高可用性运行的先决条件 145
配置高可用性 146
为高可用性配置 NNMi 证书 147
配置 NNMi 以高可用性运行 147
NNMi 高可用性配置信息 150
在主群集节点上配置 NNMi 151
在辅助群集节点上配置 NNMi 154
配置 NNM iSPI 以高可用性运行 156
NNM iSPI Performance for Metrics、NNM iSPI Performance for QA 和 NNM iSPI Performance for Traffic 156
NNM iSPI Performance for QA、NNM iSPI for MPLS、NNM iSPI for IP Multicast 和 NNM iSPI for IP Telephony 156
以 HA 运行的 NNM iSPI Network Engineering Toolset Software 和 NNMi 157
在 Oracle 环境中配置 NNMi 以高可用性运行 157
高可用性环境中 NNMi 对 Oracle 的依懒性 158
在 Oracle 环境中配置 NNMi 以高可用性运行 158
高可用性环境中的共享 NNMi 数据 158
高可用性环境中 NNMi 共享磁盘上的数据 158
在高可用性环境中复制配置文件 159
禁用数据复制 160
在高可用性环境中手动准备共享磁盘 160
配置 SAN 或已实际连接的磁盘 161
在 ov.conf 文件中设置高可用性变量 161
将共享磁盘移到 NNMi HA 资源组中 162
有关 Windows 服务器上的共享磁盘配置的说明 162
在高可用性群集中许可 NNMi 162
维护高可用性配置 163
维护模式 163
将 HA 资源组置于维护模式 163
将 HA 资源组移出维护模式 164
在 HA 群集中维护 NNMi 164
启动和停止 NNMi 164
在群集环境中更改 NNMi 主机名和 IP 地址 164
停止 NNMi 而不执行故障转移 167
在维护之后重新启动 NNMi 167
在 NNMi HA 群集中维护加载项 NNM iSPI 167
取消配置 HA 群集中的 NNMi 168
不以 HA 运行带现有数据库的 NNMi 170
对以 HA 运行的 NNMi 应用补丁程序 170
HA 配置故障排除 171
常见高可用性配置错误 171
RHCS 6 的配置问题 172
HA 资源测试 172
特定于 NNMi 的高可用性故障排除 173
在所有群集节点取消配置之后，对 NNMi 重新启用高可用性 174
NNMi 未以高可用性正确启动 174

故障转移之后看不到对 NNMi 数据的更改 174
nmsdbmgr 在配置高可用性后未启动 175
NNMi 仅在一个高可用性群集节点上正确运行 (Windows) 176
磁盘故障转移未执行 176
无法访问共享磁盘 (Windows) 176
共享磁盘不包含当前数据 176
故障转移之后辅助节点找不到共享磁盘文件 176
常规 HA 故障排除 177
错误：参数个数不正确 177
资源托管子系统进程意外停止 (Windows Server) 178
产品启动超时 (Windows WSCS 2008) 178
主动群集节点上的日志文件未更新 178
无法在特定群集节点上启动 NNMi HA 资源组 178
特定于 NNM iSPI 的高可用性故障排除 179
高可用性配置参考 179
NNMi 高可用性配置文件 180
NNMi 提供的 HA 配置脚本 180
NNMi 高可用性配置日志文件 181
NNMi Northbound 接口 183
NNMi Northbound 接口 184
价值 184
支持的版本 184
术语 184
文档 185
启用 NNMi Northbound 接口 185
使用 NNMi Northbound 接口 185
事件转发 186
事件生命周期状况更改通知 186
事件关联通知 187
事件删除通知 188
事件转发筛选 188
更改 NNMi Northbound 接口 188
禁用 NNMi Northbound 接口 189
NNMi Northbound 接口故障排除 189
应用程序故障转移和 NNMi Northbound 接口 190
本地 Northbound 应用程序 190
远程 Northbound 应用程序 190
NNMi Northbound 接口目标表单参考 190
Northbound 应用程序连接参数 191
NNMi Northbound 接口集成内容 192
NNMi Northbound 接口目标状态信息 194
由 NNMi Northbound 接口使用的 MIB 信息 194

第 5 章: 维护 NNMi 196
NNMi 备份和恢复工具 196
备份和恢复命令 196
备份 NNMi 数据 197
备份类型 197

备份范围 197
恢复 NNMi 数据 199
相同系统恢复 200
不同系统恢复 201
备份和恢复策略 201
定期备份所有数据 201
更改配置之前备份数据 202
升级 NNMi 或操作系统之前备份数据 202
只恢复文件系统文件 202
只备份和恢复嵌入式数据库 202
在高可用性 (HA) 环境中使用备份和恢复工具 203
在 HA 环境中备份的最佳实践 203
在 HA 环境中恢复的最佳实践 203
维护 NNMi 203
管理 NNMi 文件夹的访问控制列表 204
配置节点组 205
配置节点组图设置 205
配置通信设置 205
管理自定义轮询器采集导出 206
更改自定义轮询器采集导出目录 206
更改用于自定义轮询器采集导出的最大磁盘空间量 206
更改自定义轮询器度量累计间隔 207
管理事件操作 207
设置并发操作数目 207
设置 Jython 操作的线程数 208
设置操作服务器名称参数 208
更改操作服务器队列大小 209
事件操作日志 209
覆盖 server.properties 文件中的设置 210
覆盖浏览器语言环境设置 210
配置分配事件时用户名排序顺序所用的语言环境 211
配置 SNMP Set 对象访问特权 212
将 NNMi 配置为要求加密远程访问 213
管理 SNMP 陷阱 213
使用 hosted-on-trapstorm.conf 文件阻止陷阱风暴 213
配置 NNMi 以便验证使用 SNMPv2 或 SNMPv1 管理或者未被发现的节点的 SNMPv3 陷阱 214
配置原因引擎接受陷阱的时间 215
配置自动删除最旧 SNMP 陷阱事件功能 216
启用自动删除最旧 SNMP 陷阱事件功能(无事件存档) 217
启用自动删除最旧 SNMP 陷阱事件功能(启用事件存档) 217
减少存储的 SNMP 陷阱事件数 218
监视自动裁切最旧 SNMP 陷阱事件功能 219
禁用自动删除最旧 SNMP 陷阱事件功能 219
配置 NNMi 以确定代理 SNMP 网关发送的陷阱的原始陷阱地址 220
陷阱地址排序 221
NNMi NmsTrapReceiver 进程 221
配置 NmsTrapReceiver 221

NmsTrapReceiver 安全性 222
启动和停止 NmsTrapReceiver 进程 222
使用 nnmtrapd.conf 和 trapFilter.conf 文件阻止事件 223
配置 NNMi 保留以前支持的 Varbind 顺序 223
配置 ICMP Echo 请求包中的数据负载大小 224
配置 NNMi 如何确定设备的主机名 226
为 NNMi 配置字符集编码设置 226
配置 NNMi 等待 NNM iSPI 许可请求的时间 227
管理用户界面属性 227
修改 NNMi 量表标题以显示 SNMP MIB 变量名称 228
修改 MIB 浏览器参数 228
允许第 2 级操作员删除节点和事件 229
允许第 2 级操作员编辑节点组图 230
允许第 1 级操作员运行状态和配置轮询 231
修改并发 SNMP 请求数 232
修改嵌入式数据库端口 232
修改 NNMi 标准化属性 233
在初始发现之后更改标准化属性 234
修改并发 SNMP 请求数 234
NNMi 自监视 235
抑制对特定节点使用发现协议 236
抑制使用发现协议采集 236
抑制管理出现故障的接口上的 IP 地址监视 237
抑制对大型交换机使用 VLAN 索引 238
抑制使用 VLAN 索引 238
计划服务中断 239
配置传感器状态 239
配置物理传感器状态 239
将物理传感器状态传播到物理组件 239
将物理传感器状态配置为不传播到物理组件 240
覆盖物理传感器状态值 240
配置节点传感器状态 241
将节点传感器状态传播到节点 241
将节点传感器的状态配置为不传播到节点 241
覆盖节点组件状态值 242
导入接口的输入和输出速度 242
NNMi 日志记录 243
NNMi 日志文件 243
登录和注销日志记录 243
更改管理服务器 244
准备 NNMi 配置供移动的最佳实践 244
移动 NNMi 配置和嵌入式数据库 245
移动 NNMi 配置 245
恢复 NNMi 公钥证书 245
任务 1：确定 KeyManager 服务的状态 246
任务 2：备份当前 nnm.keystore 文件 246
任务 3：尝试找到原始 nnm.keystore 文件 246
任务 4：如果可用，则恢复原始 nnm.keystore 文件 247

更改独立 NNMi 管理服务器的 IP 地址 248
更改 NNMi 管理服务器的主机名或域名 248
更改 Oracle 数据库实例连接信息 249
任务 1：更新 Oracle 数据库实例 249
任务 2：更新 NNMi 配置 250
更改 NNMi 用于连接 Oracle 数据库实例的密码 250

第 6 章：高级配置 252
许可 NNMi 252
准备安装永久许可证密钥 253
检查许可证类型和被管节点数目 253
获取和安装永久许可证密钥 254
使用 Autopass 和 HP 订购号(在防火墙后不能实现) 254
使用命令行 254
获取其他许可证密钥 255
管理证书 255
关于 NNMi 证书 255
将现有证书替换为新的自签名或 CA 签名证书 257
生成自签名证书 257
生成 CA 签名证书 258
CA 签名证书的类型 261
在应用程序故障转移环境中使用证书 263
在高可用性环境中使用证书 264
使用默认证书配置高可用性 265
使用新证书配置高可用性 265
在全局网络管理环境中使用证书 265
在全局网络管理环境中配置证书 266
在具有故障转移功能的全局网络管理环境中配置证书 267
配置与目录服务的 SSL 连接 268
对 NNMi 使用单点登录 (SSO) 269
NNMi 的 SSO 访问 270
为单个域启用 SSO 271
为位于不同域中的 NNMi 管理服务器启用 SSO 271
NNMi 和 NNM iSPI 的 SSO 访问 272
禁用 SSO 273
SSO 安全备注 274
将 NNMi 配置为支持公钥基础设施用户验证 275
用户验证策略 276
为 NNMi 配置 PKI 用户验证(X.509 证书验证) 276
使用客户端证书登录 NNMi 279
吊销拥有客户端证书的用户的访问权限 280
在全局网络管理环境中使用 PKI 用户验证时的特殊注意事项 280
证书验证(CRL 和 OCSP) 280
证书验证协议的常规配置 281
配置协议顺序 281
配置协议请求 281
使用 CRL 验证证书 282
启用和禁用 CRL 检查 282

更改 CRL 强制模式 283
更改刷新 CRL 的频率 283
更改 CRL 的最长空闲时间 284
CRL 过期警告 284
更改 CRL 位置 284
使用在线证书状态协议 (OCSP) 验证证书 285
启用和禁用 OCSP 检查 286
更改 OCSP 强制模式 286
启用 Nonce 287
指定 OCSP 响应程序的 URL 287
将 NNMi 配置为限制用于 NNMi 登录访问的证书 288
示例：将 NNMi 配置为要求智能卡登录 289
为 CLI 验证配置 PKI 用户验证 291
设置 ACL 支持非根用户运行 CLI 命令 292
PKI 用户验证问题故障排除 293
配置 Telnet 和 SSH 协议以供 NNMi 使用 294
禁用 Telnet 或 SSH 菜单项 295
为 Windows 上的浏览器配置 Telnet 或 SSH 客户端 295
Windows 操作系统提供的 Telnet 客户端 297
第三方 Telnet 客户端(标准 Windows) 298
第三方 Telnet 客户端 (Windows on Windows) 299
第三方 SSH 客户端(标准 Windows 以及 Windows on Windows) 300
在 Linux 上配置 Firefox 使用 Telnet 或 SSH 301
Linux 上的 Telnet 301
Linux 上的安全 Shell 302
用于更改 Windows 注册表的示例文件 303
示例 nnmtelnet.reg 303
示例 nnmputtytelnet.reg 303
示例 nnmtelnet32on64.reg 303
示例 nnmssh.reg 304
通过 LDAP 将 NNMi 与目录服务集成 305
NNMi 用户访问信息和配置选项 305
内部模式(最初名为“选项 1”)：NNMi 数据库中的所有 NNMi 用户信息 306
混合模式(最初名为“选项 2”)：NNMi 数据库中的部分 NNMi 用户信息，以及目录服务中的部分 NNMi 用户信息 307
外部模式(最初名为“选项 3”)：目录服务中的所有 NNMi 用户信息 308
配置 NNMi 访问目录服务 309
目录服务查询 316
目录服务访问 316
目录服务内容 316
由目录服务管理员拥有的信息 320
用户标识 322
配置目录服务中的 NNMi 用户访问(详细方法) 322
用户组标识 324
配置目录服务中的用户组检索(详细方法) 325
用于存储 NNMi 用户组的目录服务配置 326
目录服务集成故障排除 326
ldap.properties 配置文件参考 327

示例 331
管理 NAT 环境中的重叠 IP 地址 331
什么是 NAT? 331
NAT 的优势是什么? 332
支持哪些类型的 NAT? 332
如何在 NNMi 中实现 NAT? 332
静态 NAT 注意事项 333
硬件和软件要求以及静态 NAT 334
重叠 IP 地址映射 334
专用 IP 地址范围 334
通信和静态 NAT 335
管理对静态 NAT 环境中的管理地址的 ICMP 轮询 335
启用对 NAT 环境中的管理地址的 ICMP 轮询 335
发现和静态 NAT 336
监视静态 NAT 的配置 336
陷阱和静态 NAT 337
SNMPv2c 陷阱 337
SNMPv1 陷阱 338
子网和静态 NAT 340
全局网络管理：静态 NAT 的可选项 341
动态 NAT 和 PAT 注意事项 341
硬件和软件要求以及动态 NAT 和 PAT 343
发现动态 NAT 和 PAT 的配置 343
监视动态 NAT 的配置 343
子网以及动态 NAT 和 PAT 343
全局网络管理：动态 NAT 和 PAT 的必需项 344
在网络地址转换 (NAT) 环境中部署 NNMi 344
NNMi 状况和状态计算 346
NNMi 安全和多租户 347
限制对象访问的影响 348
NNMi 安全模型 349
安全组 349
安全组结构示例 351
NNMi 租户模型 353
租户 353
租户结构示例 354
NNMi 安全和多租户配置 356
配置工具 357
配置租户 359
配置安全组 360
验证配置 361
导出 NNMi 安全和多租户配置 363
NNMi 安全、多租户和全局网络管理 (GNM) 363
初始 GNM 配置 364
GNM 维护 365
在 NPS 报告中包含选择界面 365
全局网络管理 366
全局网络管理的好处 367

全局网络管理是管理网络的好工具吗？ 367
我需要连续的多站点网络监视吗？ 367
我的关键设备是可见的吗？ 368
许可注意事项 368
实用的全局网络管理示例 368
查看要求 369
区域管理器和全局管理器连接 370
初始准备 370
端口可用性：配置防火墙 370
配置自签名证书 371
配置全局网络管理以供应用程序故障转移 371
NNMi 管理服务器大小调整的注意事项 371
同步系统时钟 372
在全局网络管理中结合使用应用程序故障转移功能与自签名证书 372
在全局网络管理中使用自签名证书 372
在全局网络管理中使用证书颁发机构 372
列出要监视的关键设备 372
查看全局和区域管理器的管理域 372
查看 NNMi 帮助主题 373
SSO 和操作菜单 373
为全局网络管理配置单点登录 373
在区域管理器上配置转发筛选 376
配置转发筛选，限制转发的节点 376
用区域管理器连接全局管理器 377
确定从 global1 到 regional1 和 regional2 的连接状况 378
查看 global1 库存 378
断开 global1 和 regional1 之间的通信连接 378
发现和数据同步 379
将自定义属性从区域管理器复制到全局管理器 380
设备的状态轮询或配置轮询 380
用全局管理器确定设备状态和 NNMi 事件生成 382
为全局网络管理配置应用程序故障转移 382
全局网络管理的故障排除提示 383
时钟同步 383
全局网络管理系统信息 383
从全局管理器同步区域管理器发现 384
补救 global1 上损坏的数据库 385
全局网络管理和 NNM iSPI 或第三方集成 385
HP Network Node Manager iSPI Performance for Metrics Software 385
全局网络管理和地址转换协议 385
配置 NNMi Advanced 的 IPv6 功能 386
功能描述 386
先决条件 387
许可 388
支持的配置 388
管理服务器 388
IPv6 的受支持 SNMP MIB 389
安装 NNMi 389

取消激活 IPv6 功能 389
取消激活之后的 IPv6 监视 390
取消激活之后的 IPv6 库存 391
清理 IPv6 库存时的已知问题 391
重新激活 IPv6 功能 391

第 7 章: NNMi 安全性 394
配置 SSL 通信以进行 Web 访问和 RMI 通信 394
允许非根 Linux 用户启动和停止 NNMi 394
为嵌入式数据库工具提供密码 395
配置 NNMi 以启用或禁用 SSLv3 密码 395
配置 NNMi 密码 397
NNMi 数据加密 397
加密配置文件 397
加密配置文件中的文本块 397
加密和应用程序故障转移 398
加密和用户帐户密码 399

使用 HPE Operations Bridge Reporter 查看报告 401
先决条件 401
配置 NNMi 将数据导出到 OBR 401
配置 OBR 以使用 NNMi 采集的数据 402
使用报告 402

将 HP Performance Insight (OVPI) SNMP 自定义报告包采集迁移到 NNMi 403

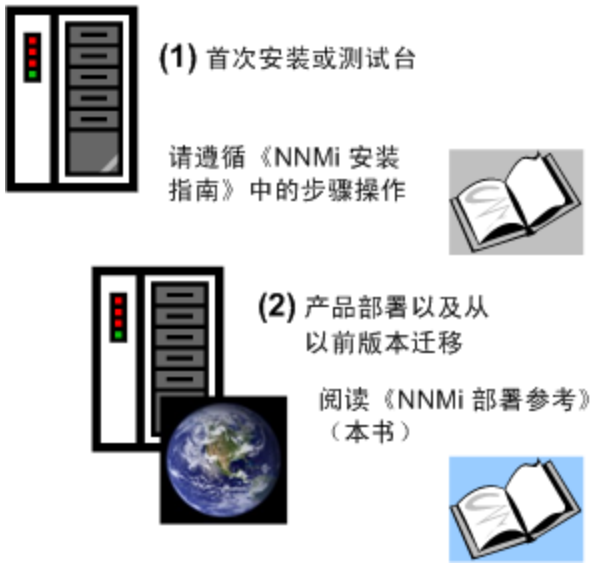
附录 A: 更多信息 406
手动为 NNMi 配置应用程序故障转移 406
NNMi 环境变量 409
本文档中使用的环境变量 409
其他可用的环境变量 410
NNMi 和 NNM iSPI 默认端口 412
HP Network Node Manager i Software 端口 413
NNM iSPI for MPLS 端口 422
NNM iSPI for IP Telephony 端口 426
NNM iSPI for IP Multicast 端口 430
NNM iSPI Performance for Traffic 端口 434
NNM iSPI Performance for QA 端口 445
NNM iSPI Performance for Metrics 和 NPS 端口 449
NNM iSPI NET 端口 451
配置问题疑难解答 452
NNMi 不能始终正确解释和显示 SNMP 数据及 MIB 字符串 452
NNMi 图显示 Linux 服务器而不是 ESXi 服务器和节点 453
NNMi 图显示 ESXi 设备 No SNMP，而不是显示为 ESXi 设备 453
解决方案 453
NNMi 图显示 ESXi 服务器以及在 ESXi 服务器上运行的虚拟机和服务器 454
NNMi 图显示 ESXi 服务器以及在 ESXi 服务器上运行的虚拟机和服务器 454
NNMi 显示有关与主机(NNMi 管理服务器)不匹配的许可证密钥的消息 455

对于某些使用 PAgP(端口聚合协议)的 Cisco 设备，如果故障链路属于端口聚合的一部分，则 NNMi 可能会认为该设备上的端口不再属于端口聚合的一部分 456
我正在使用带 Oracle 数据库的 NNMi。我配置的大型节点组导致生成节点组图时出错 456
我意外地从 NNMi 管理服务器删除了 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 库 457

词汇表 460

发送文档反馈 469

第 1 章: 关于本指南



本章包含以下主题：

- 本指南包含哪些内容？ (第 19 页)
- 本文档中使用的路径约定 (第 19 页)
- 修订历史 (第 20 页)
- 有关 NNMi 的详细信息 (第 20 页)

本指南包含哪些内容？

本指南包含用于部署 HP Network Node Manager i Software(包括 NNMi Premium 和 NNMi Ultimate)的信息集和最佳实践。本指南适用于熟悉在大型安装中部署和管理网络的专家级系统管理员、网络工程师或 HP 支持工程师。

本指南假定您已在有限(测试)环境中安装 NNMi，并熟悉启动配置任务，比如使用快速启动配置向导配置团体字符串、设置网络节点有限范围的发现和创建初始管理员帐户。要详细了解这些任务，请参阅《HP Network Node Manager i Software 交互安装指南》(请参阅可用产品文档)。

HP 会在产品版本之间有新信息可用时更新本指南。有关检索本文档的更新版本的信息，请参阅可用产品文档。

本文档中使用的路径约定

此文档主要使用以下两个 NNMi 环境变量来引用文件和目录位置。此列表显示默认值。实际值取决于在 NNMi 安装期间所做的选择。

- Windows Server:
  - `%NnmInstallDir%:<驱动器>\Program Files (x86)\HP\HP BTO Software`
  - `%NnmDataDir%:<驱动器>\ProgramData\HP\HP BTO Software`

  在 Windows 系统上注意以下事项:
  - NNMi 安装进程将创建这些系统环境变量，因此它们始终对所有用户可用。
  - 路径名称中包含空格时需使用引号(例如，"%NnmInstallDir%\bin\ovstatus" -c)。
- Linux:
  - `$NnmInstallDir:/opt/OV`
  - `$NnmDataDir:/var/opt/OV`

> **备注:** 在 Linux 系统上，如果要使用它们，则必须手动创建这些环境变量。

另外，本文档引用一些 NNMi 环境变量，可以将这些环境变量用作 NNMi 管理服务器上用户登录配置的一部分。这些变量形式为 `NNM_*`。有关该 NNMi 环境变量扩展列表的信息，请参阅其他可用的环境变量 (第 410 页)。

修订历史

下表列出了本文档的每个新版本的主要更改。

文档发布日期	主要更改的说明
2014 年 5 月 (10.00)	初始版本。
2014 年 12 月 (10.01)	向“配置事件”一章添加了**配置语言环境以用于排序顺序**。 向“NNMi 安全”一章添加了**配置 NNMi 以启用或禁用 SSLv3 密码**。 更新了“高级配置”一章中**使用 NNMi 证书**的信息。
2015 年 11 月 (10.10)	向“NNMi 通信”一章添加了**配置虚拟环境的通信**。 从“通过 LDAP 将 NNMi 与目录服务集成”一章中删除了**将目录服务访问配置更改为支持 NNMi 安全模型**。

有关 NNMi 的详细信息

要获取有关 NNMi 产品的完整信息，请将本指南与其他 NNMi 文档结合使用。下表显示迄今为止的所有 NNMi 文档，包括两本指南和白皮书。

> **备注:** 以下所有信息都可以从 **http://h20230.www2.hp.com/selfsolve/manuals** 下载。有关详细信息，请参阅可用产品文档。

您要做什么？	从何处查找详细信息
查看此版本 NNMi 的可用文档列表。	下载 NNMi 文档列表。使用此文件可跟踪此版本 NNMi 的 NNMi 文档集中的增补和修订。单击链接可访问 HP 手册网站上的文档。
安装 NNMi、NNMi Advanced、NNMi Premium 或 NNMi Ultimate(第一次)。	下载《HP Network Node Manager i Software 交互安装指南》。此指南包含安装和卸载产品的基本步骤，以及如何用 NNMi 快速启动配置向导进行初始配置。
计划网络部署，包括系统要求的链接。	请参阅本指南的准备 (第 22 页)。
为生产环境配置 NNMi。	请参阅本指南的配置 (第 24 页)。
查看基于 VMware 管理程序的虚拟网络的 NNMi 配置注意事项。	请参阅管理员帮助中的“发现和监视基于 VMware 管理程序的虚拟网络 (NNMi Advanced)”和“管理基于 VMware 管理程序的虚拟网络 (NNMi Advanced)”。
在后台配置 NNMi。	请参阅本指南的高级配置 (第 252 页)。
维护 NNMi 配置。	请参阅本指南的维护 NNMi (第 196 页)。
从 Network Node Manager i Software 的以前版本升级到 NNMi。	请参阅 HP 手册网站上提供的《HP Network Node Manager i Software 交互安装指南》。
参考 NNMi 环境变量、端口和消息。	请参阅本指南的更多信息 (第 406 页)。
获取有关特定主题的详细信息。	按示例文档和白皮书下载。有关可用白皮书的列表，请参阅《NNMi 文档列表》。
打印 NNMi 帮助。	下载帮助内容的 PDF。有关可用帮助 PDF 的列表，请参阅《NNMi 文档列表》。
安装 HP NNM iSPI NET (NNM iSPI NET) 诊断服务器，并了解 NNM iSPI NET 功能。	从用于 Windows 操作系统的 Network Node Manager SPI for NET 产品类别下载《HP NNM iSPI Network Engineering Toolset Planning and Installation Guide》。 **备注:** NNM iSPI NET 诊断服务器需要 NNM iSPI NET 或 NNMi Ultimate 许可证。有关如何安装和配置此服务器的信息，请参阅《HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide》。
获取有关 NNMi Developer Toolkit (SDK) 的文档。	请参阅许可 NNMi (第 252 页)，查看与 SDK 相关的信息，获取并安装 SDK 许可证，以及查看 SDK 文档和示例。

第 2 章: 准备

本部分包含以下章节：

- 硬件和软件要求 (第 22 页)

硬件和软件要求

本章包含以下主题：

- 支持的硬件和软件 (第 22 页)
- 检查必需补丁程序 (第 23 页)
- 系统配置 (Linux) (第 23 页)
- 安装 NNMi 和 NNM iSPI (第 23 页)
- NNMi 共存 (第 23 页)
- NNM i Smart Plug-In 版本要求 (第 23 页)

支持的硬件和软件

在安装 NNMi 之前，请阅读有关在下表中描述的 NNMi 硬件和软件要求的信息。

备注: 有关此处列出的所有文档的最新版本，请转到：

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

软件和硬件预安装清单

完成(是/否)	要阅读的文档
	《HP Network Node Manager i Software 交互安装指南》 • 文件名 = nnmi_interactive_installation_en.zip • 说明文件名： NNMiReadMeFirst_en.pdf
	《NNMi Release Notes》 • 文件名 = `release_notes_nnmi_zh_CN.pdf` • **NNMi 控制台 = 帮助 > NNMi 文档库 > Release Notes**
	《NNMi Support Matrix》 • 文件名 = `support_matrix_nnmi_zh_CN.pdf` • **NNMi 控制台** = 链接自发行说明

备注: 如果新信息可用，HP 将更新《NNMi Support Matrix》。开始部署 NNMi 之前，请在最新的 NNMi 支持列表中查找您的软件版本，地址如下：

http://www.hp.com/go/hpsoftwaresupport/support_matrices

(必须有 HP Passport ID 才能访问此网站。)

备注: 如果计划安装 NNM Smart Plug-in (NNM iSPI)，请在计划 NNMi 部署时考虑那些产品的系统需求。

检查必需补丁程序

在安装 NNMi 之前，请查看《NNMi Release Notes》了解所需的任何操作系统更新。

系统配置 (Linux)

如果无法在 NNMi 管理服务器上显示 NNMi 联机帮助页，请验证 `MANPATH` 变量是否包含 `/opt/OV/man` 位置。如果未包含该位置，请将 `/opt/OV/man` 位置添加到 `MANPATH` 变量中。

安装 NNMi 和 NNM iSPI

如果计划将任何 HP NNM iSPI 用于 NNMi，则必须在安装任何 HP NNM iSPI 之前先安装 NNMi。

NNMi 共存

将 NNMi 与其他 HP 产品一起使用时，请注意以下几点：

- 如果计划在 NNMi 管理服务器上安装 HP Operations Agent(用于与 HP Operations Manager (HPOM) 通信)，请先安装 NNMi，然后再安装 HP Operations Agent。

备注: 如果还要安装 Network Performance Server (NPS)，则必须在安装 NNMi 之后和安装 Operations Agent 之前安装 NPS。

NNM i Smart Plug-In 版本要求

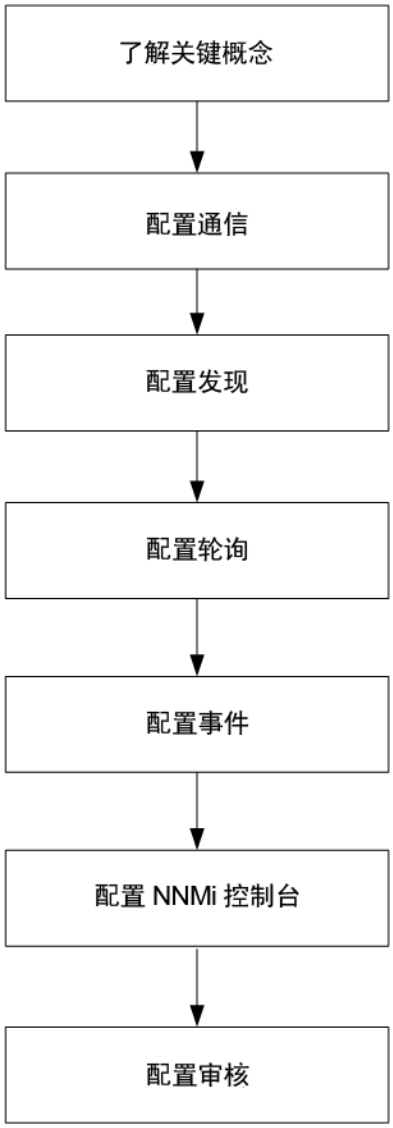
NNMi 和每个 NNM i Smart Plug-In 的版本必须对等。例如，NNM iSPI Performance for Metrics 版本 10.10 仅支持 NNMi 10.10。

有关 NNMi Premium 和 NNMi Ultimate 附带的 iSPI 列表，请参阅位于 http://h20230.www2.hp.com/selfsolve/manuals 的《NNMi Release Notes》。

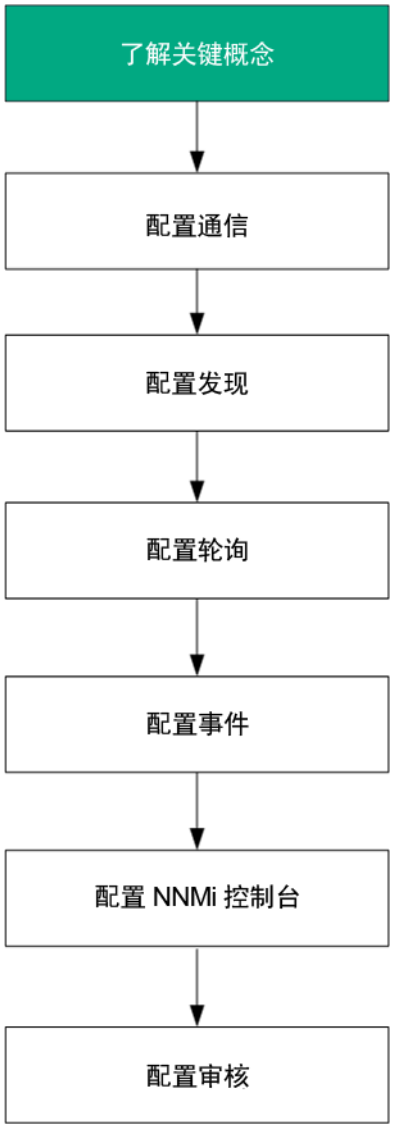
第 3 章: 配置

本部分包含以下各章:

- 配置的常规概念 (第 25 页)
- NNMi 通信 (第 33 页)
- NNMi 发现 (第 51 页)
- NNMi 状况轮询 (第 67 页)
- NNMi 事件 (第 81 页)
- NNMi 控制台 (第 96 页)
- NNMi 审核 (第 103 页)



配置的常规概念



阅读本章以查看概念介绍，本指南中稍后会详细说明。本章还包含应用于所有 HP Network Node Manager i Software (NNMi) 配置区域的一些最佳实践。

本章包含以下主题：

- 任务流模型 (第 26 页)
- 最佳实践：保存现有配置 (第 26 页)
- 最佳实践：使用作者属性 (第 26 页)
- 用户界面模型 (第 26 页)
- 排序 (第 27 页)
- 节点组和接口组 (第 27 页)
- 节点接口和地址层次结构 (第 31 页)
- 重置 NNMi 配置和数据库 (第 31 页)

任务流模型

此指南的配置部分中的各章支持以下任务流：

1. **概念** - 一般性地了解配置区域。本指南中的信息补充了 NNMi 帮助中的信息。
2. **计划** - 决定要如何达到配置。这是创建或更新贵公司的网络管理文档的良好时机。
3. **配置** - 使用 NNMi 控制台、配置文件和命令行界面的组合以将配置输入 NNMi 中。请参阅 NNMi 帮助，以了解特定过程。

   警告: 不支持使用命令行界面(如 PSQL 命令)或外部实用程序在嵌入式数据库中编写、修改或更改配置。尝试这样做可能会对数据库造成不可修复的损坏。

4. **评估** - 在 NNMi 控制台中，检查配置的结果。根据需要调整配置以取得所需结果。
5. **调整** - 可选。调整配置以改进 NNMi 性能。

最佳实践：保存现有配置

在作出任何重大的配置更改之前保存现有配置的副本是一个好的做法。如果不满意配置更改的结果，则很容易恢复为您已保存的配置。

可以用 `nnmconfigexport.ovpl` 命令保存当前配置。要恢复已保存的配置，请使用 nnmconfigimport.ovpl 命令。

有关如何使用这些命令的信息，请参阅相应的参考页或 Linux 联机帮助页。

提示: `nnmconfigexport.ovpl` 命令不保留 SNMPv3 凭据。有关详细信息，请参阅 nnmconfigexport.ovpl 参考页或 Linux 联机帮助页。

另请参阅《HP Network Node Manager i Software Step-by-Step Guide to Using NNMi Import and Export Tools White Paper》。

最佳实践：使用作者属性

很多 NNMi 配置表单包括**作者**属性。

当在这些表单上创建或修改配置时，请将**作者**属性设置为标识您的组织的值。导出 NNMi 配置时，可指定作者值，以仅抽出贵组织已自定义的那些项。

升级 NNMi 时，安装程序不会覆盖其作者值不是 HP 的任何配置。

用户界面模型

某些 NNMi 控制台表单使用事务方法更新数据库。在保存并关闭 NNMi 控制台上的表单后，在 NNMi 控制台表单中进行的更改才会生效。如果关闭包含(该表单或所含表单上的)未保存更改的表单，则 NNMi 会警告您有未保存的更改，并允许您取消关闭操作。

备注: **发现种子**表单是事务方法的一个例外。在**发现配置**表单上提供此表单是为了方便，但

它与其余发现配置无关。出于此原因，必须先保存并关闭**发现配置**表单以实现自动发现规则，才能配置那些规则的发现种子。

排序

某些 NNMi 控制台配置表单包括**排序**属性，此属性设置应用配置的优先级。对于一个配置区域，NNMi 从最小(最低)排序编号到下一个最低排序编号(依此类推)来对照配置评估每一项，直到 NNMi 找到匹配。此时，NNMi 使用来自匹配配置的信息，并停止查找更多匹配。(通信配置是一个例外。NNMi 继续在其他级别搜索信息以完成通信设置。)

排序属性在 NNMi 配置中担当重要角色。如果看到意外的发现或状态结果，则检查该区域的配置排序。

排序应用于本地上下文。由于本地上下文的概念，菜单和菜单项表单包含具有相同排序编号的多个对象。

在以下位置也使用排序编号，但有不同含义：

- **菜单**和**菜单项**表单上的排序将设置在关联菜单的本地上下文中的项顺序。
- **节点组图设置**表单上的拓扑图排序将设置**拓扑图**工作区中的项顺序。

有关**排序**属性如何影响给定配置区域的特定信息，请参阅该区域的 NNMi 帮助。

备注: 对于每个配置区域，将较低的排序编号应用于限制最多的配置，将较高排序编号应用于限制最少的配置。

备注: 对于每个配置区域，所有排序编号必须唯一。在初始配置期间，以标准间隔使用排序编号，以便将来能灵活地修改配置。例如，赋予前三个配置的排序编号为 100、200 和 300。

节点组和接口组

在 NNMi 中，主要筛选技术是对节点或接口分组，然后将设置应用于组或按组筛选可见性。

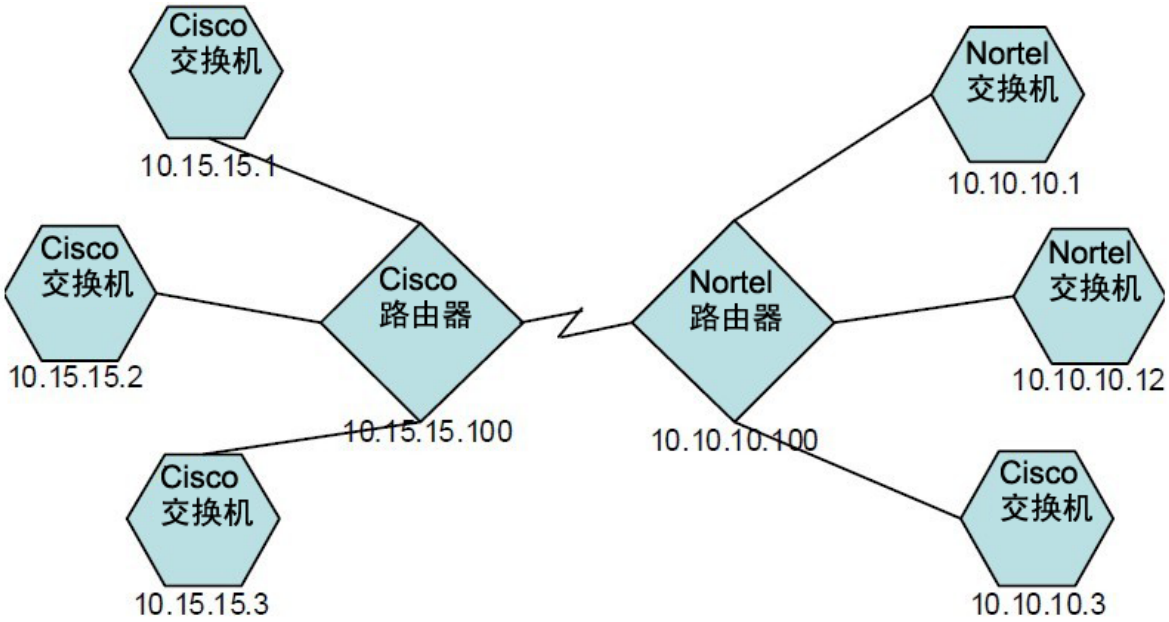
- 节点组可用于以下任何或全部用途：
  - 监视设置
  - 事件负载筛选
  - 表筛选
  - 自定义图视图
  - 对于全局网络管理功能，筛选从区域管理器传递到全局管理器的节点
- 接口组可用于以下任何或全部用途：
  - 从发现中排除接口
  - 监视设置

- 事件负载筛选
- 表筛选

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或接口是组的成员。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：

节点组重叠



- 对于监视用途，您可能希望对所有交换机设置 3 分钟的轮询间隔，而不管供应商或位置如何。可以用设备类别筛选执行此操作。
- 对于维护用途，您可能希望将所有 Cisco 交换机分组在一起，以便可以同时使它们服务中断，以便进行 IOS 升级。可以用供应商筛选执行此操作。
- 对于可见性，您可能希望将 10.10.*.* 站点上的所有设备分到具有传播状态的一个容器中。可以用 IP 地址筛选执行此操作。

具有 IP 地址 10.10.10.3 的 Cisco 交换机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无用的多余条目填充列表之间寻求平衡。

节点组成员资格

NNMi 通过比较每个发现的节点与每个配置的节点组，来确定节点组成员资格。

- 在**其他节点**选项卡上指定的所有节点都是节点组的成员。

  警告: 尽量少用**其他节点**选项卡将节点添加到节点组，因为它会占用 NNMi 管理服务器上的大量资源。

- 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成员。

- 匹配**设备筛选**选项卡上的一个或多个条目(如果有)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。

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时会在发生故障时提供有关对象位置或类型的指示，从而极大增强图视图。NNMi 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，网络可能包含 Cisco 交换机、Cisco 路由器、Nortel 交换机和 Nortel 路由器。可以为 Cisco 设备和所有交换机创建父组。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 Cisco 交换机)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
- 节点的地理位置
- 要同时中断服务的节点类型
- 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，请参考该组的(可配置)传播状态。

> **备注:** 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。

配置界面自动阻止循环的层次结构定义。

设备筛选

在发现期间，NNMi 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。(有关详细信息，请参阅NNMi 通过设备配置文件得出属性 (第 53 页)。)通过收集系统对象 ID，NNMi 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

可以使用其他筛选编辑器来创建自定义逻辑以匹配字段，包括：

- hostname (主机名)
- mgmtIPAddress(管理地址)
- hostedIPAddress(地址)
- sysName(系统名称)

- sysLocation(系统位置)
- sysContact(系统联系人)
- capability(功能唯一键)
- customAttrName(自定义属性名称)
- customAttrValue(自定义属性值)

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 NNMi 帮助中的“指定节点组附加筛选”。

功能主要用于与 NNMi 集成的其他程序。例如，路由器冗余和组件状况将把功能(字段)添加到 NNMi 数据库。可通过检查已发现设备的节点详细信息来查看这些功能。

自定义属性可由 iSPI 添加，您也可创建自己的自定义属性。如果尚未购买 Web 服务 SDK，则必须手动在每个节点的字段中放置值。例如，资产号或序列号可能是非功能属性。

其他节点

最好使用**其他筛选**限定节点组的节点。如果网络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。

警告: 尽量少用**其他节点**选项卡将节点添加到节点组，因为它会占用 NNMi 管理服务器上的大量资源。

节点组状态

使用此配置时，NNMi 用以下算法之一确定节点组的状态：

- 将节点组状态设置为与节点组中任何节点的最严重状态匹配。要使用此方法，请在**状态配置**表单上选中**传播最严重的状态**复选框。
- 使用针对每个目标状态设置的阈值集来设置节点组状态。例如，“轻微”的目标状态的默认阈值是 20%。当节点组中有 20%(或更多)的节点具有“轻微”状态时，NNMi 将节点组的状态设置为“轻微”。要使用此方法，请在**状态配置**表单上取消选中**传播最严重的状态**复选框。可在此表单的**节点组状态设置**选项卡上更改目标阈值的百分比阈值。

由于大型节点组的状态计算可能很占资源，因此默认情况下对新安装的 NNMi 关闭节点组状态计算。对于每个节点组，可以用**节点组**表单上的**计算状态**复选框启用状态计算。

接口组

接口组按 IFType 或其他属性筛选节点内的接口，如 ifAlias、ifDesc、ifName、ifIndex 和 IP 地址等等。接口组没有层次结构或包含，但是您可以根据接口所在节点的节点组进一步限定成员资格。

与节点组类似，可根据自定义功能和属性筛选接口组。

在选项卡内部和选项卡之间，会对接口组资格执行 AND 计算。

备注: 在以下情况下，接口组中的接口并不是在发现期间一开始就被排除：

- 接口组是通过筛选接口组定义中的一个或多个接口功能创建的。
- 接口组是在**排除的接口**发现配置选项中指定的。

接口功能应用到接口组中的某个接口之后，在重新发现期间重新应用排除筛选时将排除该接口。

有关 NNMi 提供的接口功能和**排除的接口**发现配置选项的详细信息，请参阅 NNMi 管理员联机帮助。

节点接口和地址层次结构

NNMi 用以下方式分配监视设置：

1. **接口设置** - NNMi 根据第一个匹配的**接口设置**定义来监视每个节点的接口和 IP 地址。第一个匹配是具有最低排序编号的**接口设置**定义。
2. **节点设置** - NNMi 根据第一个匹配的**节点设置**定义来监视每个节点和每个以前未匹配的接口或 IP 地址。第一个匹配是具有最低排序编号的**节点设置**定义。

   备注: 子节点组包括在排序层次结构中。如果父节点组具有较低排序编号(如 parent=10，child=20)，则为父节点组指定的监视配置也应用于子节点组中的节点。要覆盖父节点组监视配置，请将子节点组的排序编号设置为小于父节点组的数字(例如，parent=20，child=10)。

3. **默认设置** - 如果在步骤 1 或步骤 2 中没有找到节点、接口或 IP 地址的匹配项，则 NNMi 应用默认的监视配置设置。

重置 NNMi 配置和数据库

如果要完全地重新启动发现并重做所有 NNMi 配置，或如果 NNMi 数据库已损坏，则可以重置 NNMi 配置和数据库。此过程将删除 NNMi 的所有配置、拓扑和事件。

有关该过程中标识的命令的信息，请参阅相应的参考页或 Linux 联机帮助页。

请执行以下步骤：

1. 停止 NNMi 服务：

   ovstop -c

2. 可选。因为此过程将删除数据库，所以您在继续之前可能要备份现有数据库：

   nnmbackup.ovpl -type offline -target <备份目录>

3. 可选。如果要保留当前的任何 NNMi 配置，则使用 `nnmconfigexport.ovpl` 命令将 NNMi 配置输出到 XML 文件。

   提示: `nnmconfigexport.ovpl` 命令不保留 SNMPv3 凭据。有关详细信息，请参阅 nnmconfigexport.ovpl 参考页或 Linux 联机帮助页。

4. 可选。使用 `nnmtrimincidents.ovpl` 命令将 NNMi 事件存档。事件以 CSV 格式存档，如 `nnmtrimincidents.ovpl` 参考页或 Linux 联机帮助页中所述。

5. 断开并重新创建 NNMi 数据库。
   - 对于嵌入式数据库，请运行以下命令：

     ```
     nnmresetembdb.ovpl -nostart
     ```

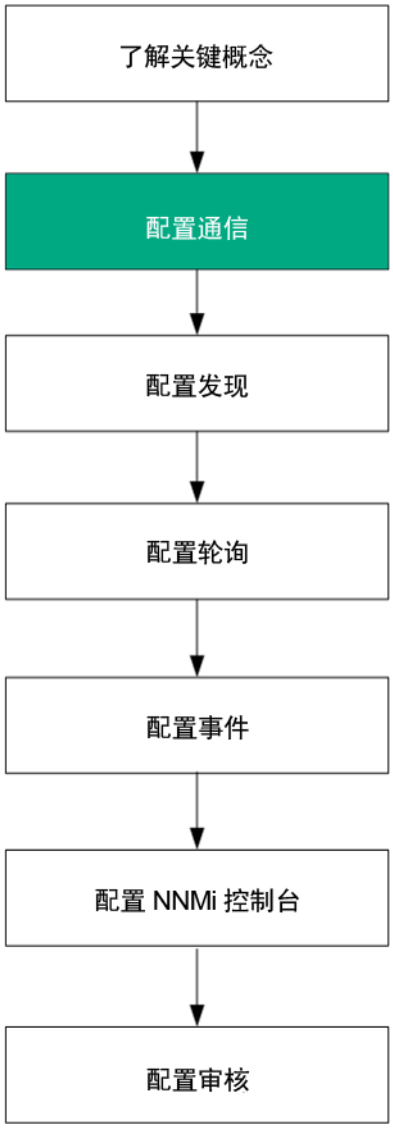
   - 对于 Oracle 数据库，请让 Oracle 数据库管理员断开并重新创建 NNMi 数据库。维护数据库实例名称。
6. 如已安装与 NNMi 集成的 iSPI 或独立产品，则重置这些产品以删除旧的拓扑标识符。有关具体过程，请参阅产品文档。
7. 启动 NNMi 服务：

   ```
   ovstart -c
   ```

   NNMi 现在只有默认配置，就好象您刚在新系统上安装了本产品。
8. 开始配置 NNMi。执行以下某项操作：
   - 使用快速启动配置向导。
   - 将信息输入 NNMi 控制台中的**配置**工作区。
   - 可使用 `nnmconfigimport.ovpl` 命令导入在步骤 3 中保存的部分或全部 NNMi 配置。

提示: 如果您正在使用 `nnmconfigimport.ovpl` 命令导入大量配置(如 9,500 个节点组或 10,000 个事件配置)，请考虑使用 `-timeout` 选项将导入事务超时的默认值 60 分钟(3600 秒)更改为更长的时间值。有关详细信息，请参阅 nnmconfigimport.ovpl 参考页或 Linux 联机帮助页。

NNMi 通信



HP Network Node Manager i Software (NNMi) 使用简单网络管理协议 (SNMP) 和 Internet 控制消息协议 (ICMP ping) 发现设备和监视设备状态及运行状况。

> **备注:** 如果配置了 Web 代理(除 SNMP 代理之外)，NNMi 可以使用其他协议。例如，适用于 **VMware** 环境的 **SOAP** 协议。

要在环境中建立可行通信，请配置 NNMi 的访问凭据和相应的超时，并重试网络的不同设备和区域的值。可以在网络某些区域中禁用某协议以减少流量或不防碍防火墙。

配置的通信值构成 NNMi 发现和状况轮询的基础。为发现或轮询进行查询时，NNMi 对每个设备应用相应的值。因此，如果配置 NNMi 以在网络的某些区域中禁止 SNMP 通信，则 NNMi 发现和 NNMi 状况轮询都不能向该区域发送 SNMP 请求。

警告: 如果设备使用 SNMP v1 或 SNMP v2C，请注意以下几点：

- SNMP v1 和 SNMP v2C 都以明文形式发送信息包。
- 要确保环境安全，请针对 SNMP 陷阱流和设备信息采集使用 SNMP v3 或添加保护(如防火墙控制)。

本章包含以下主题：

- 通信的概念 (第 34 页)
- 计划通信 (第 38 页)
- 配置通信 (第 41 页)
- 评估通信 (第 49 页)
- 微调通信 (第 50 页)

通信的概念

NNMi 主要以请求-响应方式使用 SNMP 和 ICMP。对 ICMP ping 请求的响应验证地址响应。对其他管理协议(如特定 MIB 对象的 SNMP 请求)的响应提供有关节点的更全面信息。

备注: 如果配置了 Web 代理(除 SNMP 代理之外)，NNMi 可以使用其他协议。例如，适用于 **VMware** 环境的 **SOAP** 协议。

以下概念应用于 NNMi 通信配置：

- 通信配置的级别 (第 34 页)
- 网络延迟和超时 (第 35 页)
- SNMP 访问控制 (第 35 页)
- SNMP 版本首选项 (第 36 页)
- SNMPv3 陷阱和通知 (第 37 页)
- 管理地址首选项 (第 37 页)
- 轮询协议 (第 38 页)
- 通信配置和 nnmsnmp*.ovpl 命令 (第 38 页)

通信配置的级别

NNMi 通信配置提供以下级别：

- 特定节点
- 区域
- 全局默认值

在每个级别，可以配置访问凭据、超时值和重试值、管理协议(例如 ICMP 和 SNMP)启用以及管理协议(例如 SNMP)访问设置。如果将某个级别的设置留空，则 NNMi 应用下一个级别的默认值。

与给定节点通信时，NNMi 应用如下配置设置：

1. 如果节点与**特定节点**配置匹配，则 NNMi 使用该配置中的所有通信值。
2. 如果尚未定义任何设置，则 NNMi 确定节点是否属于任何**区域**。因为区域可能重叠，所以 NNMi 使用排序编号最低的匹配区域。NNMi 使用为该区域指定的值来填充适用的特定节点设置(如果有)以外的空白项。不考虑其他区域的设置。
3. 如果仍未定义任何设置，则 NNMi 使用**全局默认值**设置填充剩余的空白项。

用于与特定设备进行通信的值可能会累积生成，直到确定所有必需的设置。

网络延迟和超时

正常网络延迟影响 NNMi 管理服务器为获取对 ICMP 查询的响应而必须等待的时间量。网络的不同区域通常有不同周转时间。例如，NNMi 管理服务器所驻留的本地网络可以提供几乎即时的响应，而通过拨号广域链路访问的远程地理区域的设备发出响应则通常需要长得多的时间。此外，负载重的设备可能太繁忙而无法立即响应 ICMP 查询。决定要配置哪个超时和重试设置时，请考虑这些延迟影响。

可以同时配置网络区域和特定设备的特定超时和重试设置。您选择的设置确定 NNMi 等待响应的时长，以及未收到响应而放弃请求之前 NNMi 请求数据的次数。

对于每个请求重试，NNMi 均会在以前的超时值上加上配置的超时值。因此，两次重试之间的暂停时间变长。例如，当将 NNMi 配置为使用 5 秒超时和三次重试时，NNMi 等待 5 秒获取对第一个请求的响应，等待 10 秒获取对第二个请求的响应，等待 15 秒获取对第三个请求的响应，然后才放弃并进入下一个轮询周期。

SNMP 访问控制

与被管设备上的 SNMP 代理的通信需要访问控制凭据：

- SNMPv1 和 SNMPv2c

  每个 NNMi 请求中的团体字符串必须与响应 SNMP 代理中配置的团体字符串匹配。所有通信都以明文形式(未加密)通过网络。

- SNMPv3

  与 SNMP 代理的通信符合基于用户的安全模型 (USM)。每个 SNMP 代理有配置的用户名及其关联验证要求(验证配置文件)的列表。所有通信格式都通过配置设置控制。NNMi SNMP 请求必须指定有效用户，并遵循为该用户配置的验证和隐私控制。

  - 验证协议根据您对消息摘要算法 5 (MD5) 或安全哈希算法 (SHA) 的选择，使用基于列表的消息验证码 (HMAC)。
  - 隐私协议不使用加密或使用数据加密标准 - 密码块链 (DES-CBC) 对称加密协议。

备注: DES-CBC 被视为弱密码。因此，如果正在使用 DES-CBC，则 HP 建议选择更强的密码。要更改密码选择：

1. 在 NNMi 控制台中，单击**配置**工作区。
2. 展开**事件**文件夹。
3. 展开**陷阱服务器**文件夹。
4. 单击**陷阱转发配置**。
5. 在**隐私协议**列表中，选择一个强密码。

备注: 在 NNMi 管理的节点上配置 SNMPv3 通信时，避免使用 DES-CBC。

NNMi 对网络的某区域(通过 IP 地址筛选或主机名筛选定义)支持指定多个 SNMP 访问控制凭据。NNMi 通过在给定 SNMP 安全级别并行尝试所有配置的值，尝试与该区域中的设备通信。可以指定 NNMi 在该区域中使用的最低 SNMP 安全级别。NNMi 将每个节点返回的第一个值(来自设备的 SNMP 代理的响应)用于发现和监视目的。

另请参阅高可用性 (HA) 环境中的 SNMP 访问控制 (第 36 页)

高可用性 (HA) 环境中的 SNMP 访问控制

在高可用性 (HA) 环境中配置 NNMi 时，将 SNMP 源地址设置为物理群集节点地址。要将 SNMP 源地址设置为 NNM_INTERFACE(已设置为虚拟 IP 地址)，必须编辑 `ov.conf` 文件并将 `IGNORE_NNM_IF_FOR_SNMP` 的值设置为 `OFF`。(默认情况下该值设置为 `ON`。)

要在 HA 环境中将 SNMP 源地址设置为 NNM_INTERFACE:

1. 编辑群集中两个节点上的以下文件：

   Windows：%NnmDataDir%\shared\nnm\conf\ov.conf

   Linux：$NnmDataDir/shared/nnm/conf/ov.conf
2. 将 `IGNORE_NNM_IF_FOR_SNMP` 的值设置为 `OFF`。(默认情况下该值设置为 `ON`。)

   IGNORE_NNM_IF_FOR_SNMP=OFF
3. 停止并重新启动 NNMi 管理服务器：

   备注: 运行 `ovstop` 和 `ovstart` 命令前将节点置于维护模式

   a. 在 NNMi 管理服务器上运行 `ovstop` 命令。
   b. 在 NNMi 管理服务器上运行 `ovstart` 命令。

SNMP 版本首选项

多年以来，SNMP 协议自身已经从 V1 演化到 V2(c)，直至现在的 V3，安全功能(以及其他功能)不断增强。NNMi 可以处理网络环境中的任何这些版本或所有这些版本的任意组合。

NNMi 为特定节点接收到的第一个 SNMP 响应确定 NNMi 用于与该节点通信的通信凭据和 SNMP 版本。

备注: 节点的 SNMP 版本选择会影响 NNMi 接受来自该节点的陷阱：

- 如果传入陷阱的源节点或源对象由 NNMi 使用 SNMPv3 发现，则 NNMi 接受传入的 SNMPv1、SNMPv2c 和 SNMPv3 陷阱。
- 如果传入陷阱的源节点或源对象由 NNMi 使用 SNMPv1 或 SNMPv2c 发现，则 NNMi 丢弃传入的 SNMPv3 陷阱。如果必须接收这些陷阱，请执行相应步骤，将 NNMi 配置为验证不受监视节点的 SNMPv3 陷阱。

指定在网络的每个区域中可接受的 SNMP 版本和安全设置的最小级别。SNMP 最小安全级别字段的选项如下：

- **仅共用(SNMPv1)** - NNMi 尝试使用具有团体字符串、超时和重试次数配置值的 SNMPv1 进行通信。NNMi 不尝试任何 SNMPv2c 或 SNMPv3 设置。
- **仅共用(SNMPv1 或 v2c)** - NNMi 尝试使用具有团体字符串、超时和重试次数配置值的 SNMPv2c 进行通信。如果使用 SNMPv2c 时对任何团体字符串没有响应，则 NNMi 尝试使用具有团体字符串、超时和重试次数配置值的 SNMPv1 进行通信。NNMi 不尝试任何 SNMPv3 设置。
- **团体** - NNMi 尝试使用具有团体字符串、超时和重试次数配置值的 SNMPv2c 进行通信。如果使用 SNMPv2c 时对任何团体字符串没有响应，则 NNMi 尝试使用具有团体字符串、超时和重试次数配置值的 SNMPv1 进行通信。如果都不工作，则 NNMi 尝试 SNMPv3。
- **无验证，无隐私** - 对于没有验证和隐私的用户，NNMi 尝试使用具有超时和重试次数配置值的 SNMPv3 进行通信。如果都不工作，则 NNMi 必要时尝试具有验证但无隐私的用户，然后尝试具有验证和隐私的用户。
- **验证，无隐私** - 对于具有验证而没有隐私的用户，NNMi 尝试使用具有超时和重试次数配置值的 SNMPv3 进行通信。如果都不工作，NNMi 尝试具有验证和隐私的用户。
- **验证，隐私** - 对于具有验证和隐私的用户，NNMi 尝试使用具有超时和重试次数配置值的 SNMPv3 进行通信。

管理地址首选项

节点的**管理地址**是 NNMi 用于与节点的 SNMP 代理通信的地址。可以指定节点的管理地址(在特定节点设置中)，或者可以让 NNMi 从与节点关联的 IP 地址中选择地址。通过从发现中排除某些地址，可以在发现配置设置中微调此行为。有关 NNMi 如何确定管理地址的信息，请参阅 NNMi 帮助中的“节点表单”。

备注: 要发现管理程序，NNMi 需要节点名称，而非管理地址。

NNMi 持续地发现和监视设备。在第一个 NNMi 发现周期之后，当以前发现的 SNMP 代理退出响应(例如，重新配置设备的 SNMP 代理)时，**启用 SNMP 地址重新发现**字段控制 NNMi 的行为。

- 如果选中**启用 SNMP 地址重新发现**复选框，则 NNMi 将重试所有配置值以求搜索到一个有效的值。
- 如果取消选中**启用 SNMP 地址重新发现**复选框，则 NNMi 将此设备报告为“宕机”，并且不尝试查找该设备的另一个通信配置设置。

提示: 启用 SNMP 地址重新发现复选框在通信配置的所有级别都可用。

提示: 发现所有 SNMP 设备和**非 SNMP 设备**自动发现规则配置字段影响 NNMi 使用 SNMP 的方式。有关详细信息，请参阅 NNMi 帮助中的“配置自动发现规则的基本设置”。

SNMPv3 陷阱和通知

NNMi 使用 SNMPv3 与设备通信时，将使用发现过程来标识设备的引擎 ID、引导计数和引擎时间。然后 NNMi 使用此信息以及配置的用户和协议详细信息，开始向设备发送消息。

设备将陷阱发送到 NNMi 时，该设备可能没有 NNMi 信息，因为陷阱是单包事务，无法获取必要信息。因此设备在陷阱中使用自己的引擎 ID、引导计数和引擎时间以及用户名和协议详细信

息。这些设备详细信息必须与为 NNMi 中的设备配置的详细信息相同。无法为 NNMi 中的每个设备配置多个 SNMPv3 用户。

通知是确认的包，因此更像 NNMi 对设备发出的 SNMP 请求，但这次是启动第一个数据包的设备，并且 NNMi 使用确认进行响应。因此该设备执行 NNMi 发现以了解 NNMi 的引擎 ID、引导计数和引擎时间。设备使用的用户名和协议配置必须与 NNMi 陷阱转发配置中的配置(实际上就是 NNMi 的 SNMPv3 代理配置)匹配。

轮询协议

可以阻止 NNMi 在网络某些部分中使用 SNMP 或 ICMP(例如，当基础结构中的防火墙禁止 ICMP 或 SNMP 流量时)。

在网络区域中禁用流向设备的 ICMP 流量会导致在 NNMi 中出现以下结果：

- 可选自动发现规则 ping 扫描功能无法在网络的该区域中找到其他节点。所有节点必须通过响应 MIB 对象请求被播种或可用，比如邻居的 ARP 缓存、Cisco 发现协议 (CDP) 或极限发现协议 (EDP)。除非播种每一个广域网络设备，否则它们可能会丢失。
- 状况轮询器无法监视未配置为响应 SNMP 请求的设备。(但是，如果设备响应 SNMP，则状况轮询器不使用 ICMP。)
- 操作员不能使用**操作 > ping** 在疑难解答期间检查设备可访问性。

在网络区域中禁用流向设备的 SNMP 流量会导致在 NNMi 中出现以下结果：

- 发现只能收集存在的设备的信息。所有设备都接收到 `No SNMP` 设备配置文件。
- 发现无法通过查询来查找其他相邻设备。所有设备必须直接被播种。
- 发现无法收集设备的连接信息，因此设备在 NNMi 图上显示为未连接。
- 对于具有 `No SNMP` 设备配置文件的设备，状况轮询器采用默认设置，即监视仅使用 ICMP (ping) 的设备。
- 状况轮询器无法收集设备的组件运行状况或性能数据。
- 原因引擎无法联系设备以执行邻居分析并找到事件的根源。

通信配置和 nnmsnmp*.ovpl 命令

`nnmsnmp*.ovpl` 命令用于在 NNMi 数据库中查找未指定的设备通信设置的值。此方法要求 ovjboss 进程正在运行。如果 ovjboss 未在运行，则 `nnmsnmp*.ovpl` 命令的行为如下：

- 对于 SNMPv1 和 SNMPv2c 代理，此命令使用任何未指定的通信设置的默认值。
- 对于 SNMPv3 代理，如果指定用户和密码，则此命令使用任何未指定的通信设置的默认值。如果不指定用户和密码，则此命令将失败。

计划通信

作出关于以下方面的决策：

- 默认通信设置 (第 39 页)
- 通信配置区域 (第 39 页)
- 特定节点配置 (第 40 页)
- 重试和超时值 (第 40 页)

- 活动协议 (第 40 页)
- 多个团体字符串或验证配置文件 (第 40 页)

默认通信设置

因为 NNMi 使用默认值完成未为适用区域或特定节点指定的任何配置设置，因此请设置适合网络大部分区域的默认值。

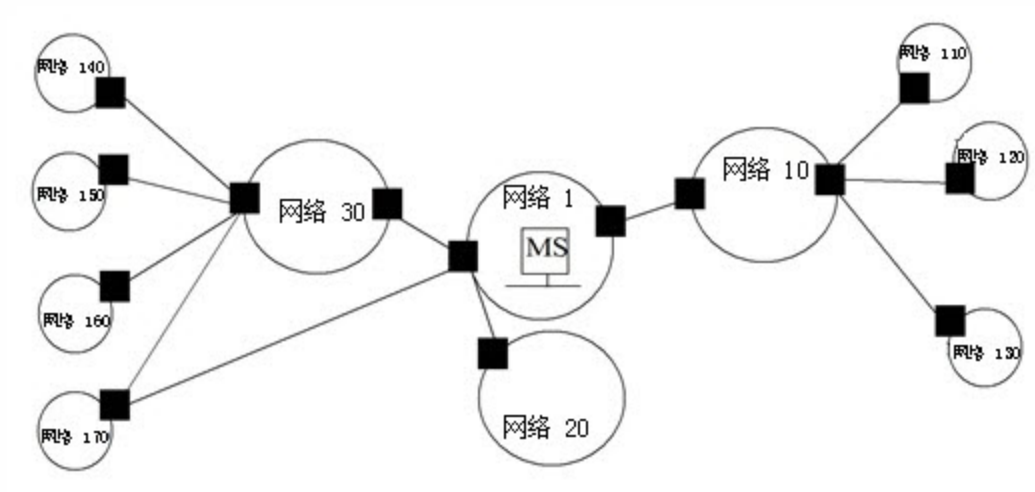
- 是否存在 NNMi 应当尝试的常用团体字符串？
- 网络中合理的默认超时和重试值是多少？

通信配置区域

区域代表相似通信设置有效的网络区域。例如，NNMi 管理服务器周围的本地网络通常非常快速地返回响应。相距多个跃点的网络区域响应时间通常更长。

您无需配置网络的每个子网或区域。可以根据相似延迟时间将区域组合到一个区域中。考虑以下网络映射：

通信区域的网络示例



出于超时和重试目的，可能要配置以下区域：

- 区域 A 代表网络 1
- 区域 B 包括网络 10、网络 20 和网络 30
- 区域 C 代表更偏远的网络

您将决定如何对网络 170 进行最佳分组，具体取决于将流量管理配置设置为首选离 NNMi 管理服务器一个还是两个跃点的路径。

区域还用于对具有相似访问凭据的设备分组。如果网络中的所有路由器都使用相同的团体字符串(或一小组可能的团体字符串)并且可以通过命名约定(例如，`rtrnnn.yourdomain.com`)识别路由器，则可以配置包含所有路由器的区域，以便对它们作相似处理。如果无法使用通配符来对设备分组，则可以将每个设备配置为特定节点。

计划区域配置，以便可以将相同的超时值、重试值以及访问凭据配置应用于区域中的所有节点。

区域定义可以重叠，并且设备可能适合于多个区域。NNMi 应用具有最低排序编号的区域的设置(前提是没有任何其他匹配区域)。

特定节点配置

对于具有唯一通信配置要求的任何设备，使用特定节点设置，以指定该节点的通信设置。特定节点设置的使用示例包括：

- 可能未对 SNMPv2c/SNMPv3 GetBulk 请求作出良好响应的节点
- 名称与其他相似节点的命名模式不匹配的节点

备注: 可以启用或禁用特定设备的 SNMP 通信。请参阅 NNMi 帮助中的特定节点设置表单。

重试和超时值

配置更长超时和更多重试次数可能使繁忙或远程的设备产生更多响应。此较高的响应率消除了错误宕机消息。但是，它也延长了确定实际宕机设备需要引起注意的时间。为网络的每个区域寻求平衡很重要，可能需要一些时间来测试和调整环境中的值。

要了解每个跃点的当前延迟时间，请执行以下操作：

- Windows：对每个网络区域中的设备运行 `tracert`。
- Linux：对每个网络区域中的设备运行 `traceroute`。

活动协议

有两个机会可以控制与网络中的设备通信时 NNMi 生成的流量类型：通信和监视配置设置。基础结构中的防火墙禁止 ICMP 或 SNMP 流量时，使用通信设置。不需要有关设备的特定部分数据时，可使用监视设置微调协议的使用。如果通信或监视设置对设备禁用协议，则 NNMi 不对该设备生成该类型的流量。

备注: 禁用 SNMP 通信将大幅降低网络的 NNMi 状态和运行状况监视。

注明是每个区域还是特定设备应当接收 ICMP 流量。

对于您不提供访问凭据的设备，不需要明确禁用与其的 SNMP 通信。默认情况下，NNMi 将这些设备分配到 `No SNMP` 设备配置文件中，并只使用 ICMP 监视它们。

如果配置了 Web 代理(除 SNMP 代理之外)，NNMi 可以使用其他协议(例如，适用于 VMware 环境的 SOAP 协议)。

另请参阅使用网络配置协议 (NETCONF) 的设备支持 (第 43 页)。

多个团体字符串或验证配置文件

计划对网络的每个区域都尝试的团体字符串和验证配置文件。对于默认和区域设置，可以配置要并行尝试的多个团体字符串和验证配置文件。

备注: 尝试可能的团体字符串时，NNMi 查询可能导致设备的验证失败。NNMi 完成其初始发

现时，您可通知运营部门可以安全地忽略验证失败。另外，通过尽可能紧密地配置区域(和要尝试的关联团体字符串及验证协议)，可以将验证失败次数降至最低。

如果环境使用 SNMPv1 或 v2c 和 SNMPv3，则确定每个区域的最小可接受安全级别。

SNMPv1 和 SNMPv2 团体字符串

对于可接受 SNMPv1 或 v2c 访问的区域，收集区域中使用的团体字符串和特定设备必需的任何唯一团体字符串。

SNMPv3 验证配置文件

如果区域中包含的设备使用 SNMPv3，则确定最低级别的可接受默认验证配置文件、适合每个区域的验证配置文件和特定设备上使用的唯一验证凭据(如果有)。还要确定网络中使用的验证和隐私协议。

对于 SNMPv3 通信，NNMi 支持以下验证协议：

- HMAC-MD5-96
- HMAC-SHA-1

对于 SNMPv3 通信，NNMi 支持以下隐私协议：

- DES-CBC
- TripleDES
- AES-128
- AES-192
- AES-256

可以为每个特定节点或区域设置指定一个(或不指定)验证协议和一个(或不指定)隐私协议。

备注: 如果使用 TripleDES、AES-192 或 AES-256 隐私协议，则需要 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 库，该库在 NNMi 安装过程中自动安装。如果您意外地删除了该库，可以遵循配置问题疑难解答 (第 452 页)中的过程恢复它。

配置通信

阅读本部分中的信息之后，请参阅 NNMi 帮助中的“配置通信协议”，以了解具体步骤。

备注: 在作出任何重大的配置更改之前保存现有配置的副本是一个好的做法。有关详细信息，请参阅最佳实践：保存现有配置 (第 26 页)。

配置通信的以下方面：

- 默认设置
- 区域定义及其设置
- 特定节点设置

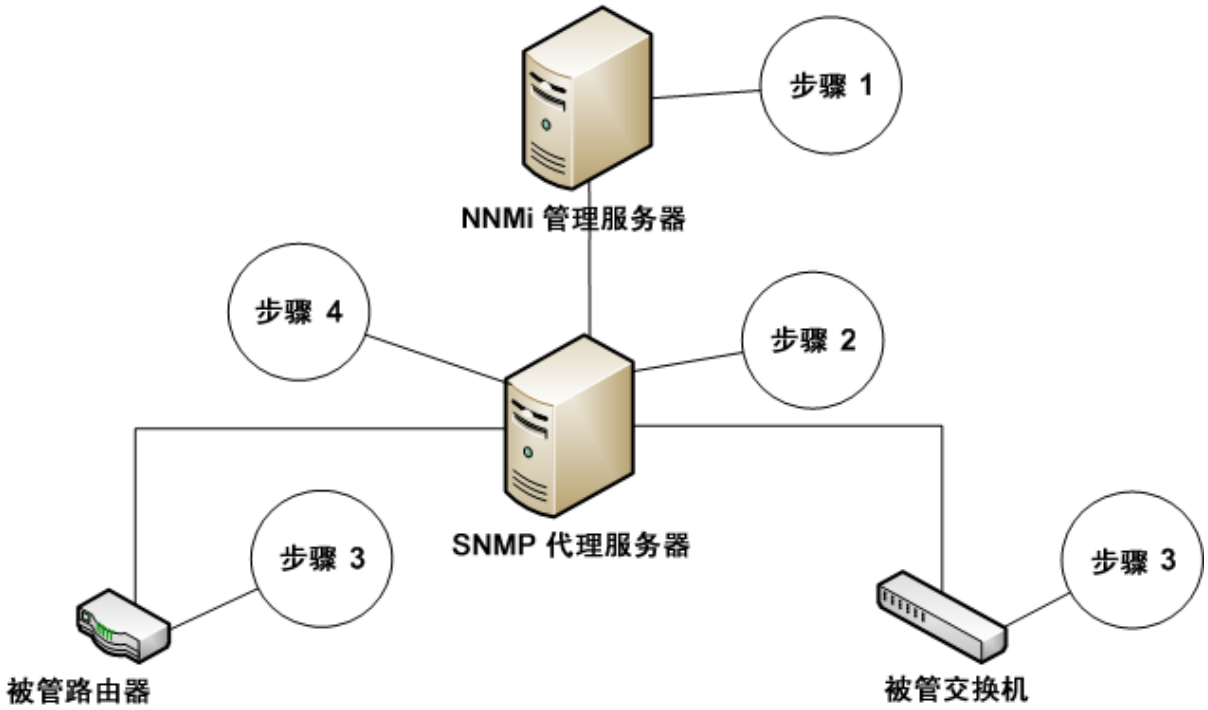
对于特定节点，可以通过 NNMi 控制台或配置文件输入节点设置。

备注: 仔细检查已定义区域的排序编号。如果节点适合于多个区域的成员资格，则 NNMi 将具有最低排序编号的区域中的设置应用于该节点。

配置 SNMP 代理设置

有些网络使用 SNMP 代理与网络设备进行通信。下图显示了 NNMi 所使用的 SNMP 通信步骤(如果您从 NNMi 控制台使用 **配置 > 通信配置**配置 SNMP 代理地址和 SNMP 代理端口)。NNMi 支持允许使用 SecurityPackAgentAddressOid OID (.1.3.6.1.4.1.99.12.45.1.1) 的 SNMP 代理服务器。

使用代理服务器



1. NNMi 管理服务器向 SNMP 代理地址和 SNMP 代理端口发送 SNMP 请求以从托管路由器和托管交换机获取信息。NNMi 管理服务器将托管路由器和交换机的远程地址和端口编码为特殊的代理 varbind SecurityPackAgentAddressOid (.1.3.6.1.4.1.99.12.45.1.1)，并将此 varbind 添加到 SNMP 请求。
2. SNMP 代理服务器读取该特殊的代理 varbind，确定发送 SNMP 请求的位置，然后将 SNMP 请求发送到托管路由器和交换机以获取 NNMi 管理服务器所请求的信息。
3. 托管交换机和路由器使用请求的信息对 SNMP 代理服务器进行响应(使用 SNMP 代理地址和 SNMP 代理端口)。
4. SNMP 代理服务器对 NNMi 管理服务器进行响应(使用配置的 SNMP 端口)。

配置为使用代理服务器时，NNMi 使用以下 OID 来处理 SNMP 响应：

- SecurityPackAgentAddressOid .1.3.6.1.4.1.99.12.45.1.1(来自 SNMP Research NetDiscover SECURITY-PACK-MIB)
- SecurityPackNotificationAddressOid .1.3.6.1.4.1.99.12.45.2.1(来自 SNMP Research NetDiscover SECURITY-PACK-MIB)
- ProxyOid .1.3.6.1.4.1.11.2.17.5.1.0 (HP)

- TrapForwardingAddressTypeOid .1.3.6.1.4.1.11.2.17.2.19.1.1.2.0 (HP)
- TrapForwardingAddressOid .1.3.6.1.4.1.11.2.17.2.19.1.1.3.0 (HP)
- Rfc3584TrapAddressOid .1.3.6.1.6.3.18.1.3.0 (RFC 3584)
- Rfc3584TrapCommunityOid .1.3.6.1.6.3.18.1.4.0 (RFC 3584)

将 NNMi 与 SNMP 代理服务器一起使用时，询问代理供应商是否支持此列表中的 OID。

使用网络配置协议 (NETCONF) 的设备支持

NNMi 主要依靠简单网络管理协议 (SNMP) 作为从支持的设备采集管理信息的方法。但 NNMi 还可能需要对不使用 SNMP 报告必要管理信息的某些特定供应商设备使用网络配置协议 (NETCONF)。

目前 NNMi 使用 NETCONF 仅支持 Juniper Networks QFabric 系统。有关任何更新，请参阅《HP Network Node Manager i Software Device Support Matrix》。

以下部分简单介绍了 NETCONF 以及有关被管设备和 NNMi 所需配置的信息：

什么是网络配置协议 (NETCONF)? (第 43 页)

网络配置协议 (NETCONF) 操作 (第 43 页)

在被管设备上启用并配置网络配置协议 (NETCONF) (第 44 页)

在 NNMi 中配置网络配置协议 (NETCONF) 设备凭据 (第 44 页)

什么是网络配置协议 (NETCONF)?

网络配置协议 (NETCONF)，如 SNMP，是网络管理的 Internet 工程任务组 (IETF) 标准。NETCONF 由 IETF 征求意见 (RFC) 4741 和 4742 (版本 1)定义，稍后由 RFC 6241 和 6242 (版本 1.1)更新。

NETCONF 主要用作设备配置机制，而 SNMP 最常用于监视、轮询和故障通知。这两个协议都报告对 NNMi 有用的管理信息。

发现或重新发现期间，NNMi 使用 NETCONF 采集有关设备的信息(也就是，只读信息)。NNMi 不使用 NETCONF 修改设备配置，也不监视状态或性能度量。

NETCONF 是一个 XML 格式的命令和响应协议，主要在安全 Shell (SSH) 传输上运行。NETCONF 协议在某些方面与传统设备控制台命令行界面 (CLI) 类似，不同之处在于为管理应用程序设计了 XML 格式的命令和结果，而非与设备的人机交互。

NETCONF 是一种比较新的管理协议，因此与 SNMP 相比，在设备供应商间的使用没那么广泛。

如果供应商在 NNMi 管理的设备中实现 NETCONF，请注意以下事项：

- NETCONF 命令通常更特定于供应商，知名度不如 SNMP 中的许多标准 MIB 和特定于供应商的 MIB。因此 NNMi 使用 NETCONF 的功能仍然相当有限。
- 当特定供应商在设备中实现 NETCONF 并报告 NNMi 所需的管理信息时，必须在 NNMi 中添加特定于设备的 NETCONF 支持。有关详细信息，请参阅在被管设备上启用并配置网络配置协议 (NETCONF) (第 44 页)和在 NNMi 中配置网络配置协议 (NETCONF) 设备凭据 (第 44 页)。

网络配置协议 (NETCONF) 操作

NNMi 和被管设备之间的 NETCONF 通信的详细信息对 NNMi 用户是透明的。但以下概述可能有助于进行故障排除：

- NETCONF 客户端(管理应用程序，如 NNMi)建立与被管设备上 NETCONF 服务器(子系统)的 SSH 连接。有效的 SSH 用户名和密码凭据必须由客户端指定，并由设备验证。
- 客户端应用程序和设备以 <hello> 消息的形式交换功能。
- 客户端以远程过程调用 (RPC) 消息形式启动对设备的请求；包括标准 <get> 或 <get-config> 操作，以及为设备定义的任何特定于供应商的操作。
- 设备以 RPC 答复消息形式的操作结果进行响应。
- 客户端应用程序在发送请求并处理响应后，将向设备发送 <close-session> RPC 消息。
- 设备以 <ok> RPC 答复消息确认。
- 最后，两端终止 SSH 连接。

在被管设备上启用并配置网络配置协议 (NETCONF)

您可能需要在被管设备中显式启用并配置 NETCONF，NNMi 才能与该设备通信。有关具体说明，请参阅供应商的设备配置文档。例如，对于 Juniper Networks QFabric 系统，请参阅 Juniper Networks 的《NETCONF XML Management Protocol Guide》中的“Establishing a NETCONF Session”。

被管设备上通常必须满足以下先决条件：

- 在默认 NETCONF TCP 端口 830 或标准 SSH TCP 端口 22 上启用 NETCONF。
- 在设备上为 NETCONF 通信访问配置 SSH 用户名和密码凭据。NNMi 只需要只读权限。

有关支持在 NNMi 中使用 NETCONF 的设备的最新列表，以及任何其他特定于供应商的先决条件和参考资料，请参阅《HP Network Node Manager i Software Device Support Matrix》(“Known Limitations”部分)。

在 NNMi 中配置网络配置协议 (NETCONF) 设备凭据

必须在 NNMi 中配置与被管设备中配置的 NETCONF SSH 凭据匹配的凭据，NNMi 才能使用 NETCONF 与该设备通信。

> **备注:** 如果没有为设备配置正确的 NETCONF 凭据，则 NNMi 发现将继续(仅使用 SNMP)；但 NNMi 中报告的该设备的管理信息可能不完整。

使用 NNMi 控制台在设备相关的特定于节点设置、区域设置或默认设置的**通信配置**、**设备凭据**选项卡中配置 NETCONF 设备凭据设置。

> **备注:** 每个被管设备只能配置一个 SSH 用户和密码。这意味着该设备的常规 SSH 和 NETCONF 会话使用同一组凭据。

配置后，NNMi 将在下一个发现周期中对指定的设备(节点)使用新凭据。

有关如何编辑 NNMi **通信配置**表单的详细说明，请参阅 NNMi 管理员帮助。

配置虚拟环境的通信

本部分描述使 NNMi 能与受支持的虚拟环境通信的配置信息。

监视管理程序上托管的虚拟机的先决条件

NNMi 支持：

- 发现和监视受支持的管理程序。

  在管理程序的节点表单上，每个虚拟机在**托管节点**选项卡上列出。
- 发现和监视每个虚拟机(路由器、交换机、节点等)。

  在虚拟机的节点表单上，**宿主节点**属性显示管理程序的名称。

下表介绍了发现管理程序以及管理程序上托管的虚拟机的先决条件：

监视管理程序及其 VM 的先决条件

要发现的项	先决条件	详细信息
管理程序	管理程序必须支持 SNMP 通信并可使用 SNMP 从 NNMi 进行访问。	不适用
	必须将 NNMi 配置为与关联的 SNMP 代理(IP 地址和团体字符串或 SNMPv3 验证)通信。	要使用 NNMi 用户界面进行配置，请参阅管理员帮助 > 配置通信协议，了解默认、区域或特定节点 SNMP 设置的说明。 要使用 CLI 进行配置，请参阅 `nnmcommunication.ovpl` 参考页或 Linux 联机帮助页了解详细信息。
	必须将 NNMi 配置为使用 HTTPS 与管理程序通信。 **备注:** 仅限 VMware。必须将 VMware 默认证书 (localhost.localdomain) 替换为使用 ESXi 服务器的主机名生成的证书。有关详细信息，请参阅 VMware 文档。有关要在 ESX5.1 和 ESX5.5 服务器上执行的示例步骤，请参阅替换 VMware 默认证书 (第 46 页)	要使用 CLI 进行配置，请参阅将 NNMi 配置为使用 HTTPS 与管理程序通信 (第 46 页)。 要使用 NNMi 用户界面进行配置，请参阅管理员帮助 > 配置通信协议，了解默认、区域或特定节点受信任证书设置的说明。
管理程序上的虚拟机	除了提及的针对管理程序的 SNMP 要求以外，还需要在 NNMi 中配置管理程序设备凭据，以使用管理程序的 Web 服务进行验证。	要使用 NNMi 用户界面进行配置，请参阅管理员帮助 > 配置通信协议，了解默认、区域或特定节点凭据设置的说明。 要使用 CLI 进行配置，请参阅 `nnmcommunication.ovpl` 参考页或 Linux 联机帮助页。

替换 VMware 默认证书

备注: 必须使用完全限定域名作为 ESXi 服务器的主机名才能生成自签名或 CA 签名证书。

默认情况下，VMware 证书使用 localhost.localdomain 作为 ESXi 服务器的主机名。

要用使用 ESXi 服务器的主机名生成的证书替换 VMware 默认证书，请在 ESXi 服务器上执行以下示例步骤：

备注: 此示例描述在 ESX5.1 和 EXS5.5 服务器上执行的步骤。有关最新信息，请参阅描述如何替换 VMware 默认证书的 VMware 文档。

1. 确保 `/etc/hosts` 文件采用以下格式解析主机：

   ```
   #/etc/hosts
   127.0.0.1 localhost.localdomain localhost
   ::1 localhost.localdomain localhost
   10.78.xx.xxx hostname.domain.com hostname
   ```
2. 确保 ESXi 服务器上已启用 SSH。
3. 以具有管理特权的用户身份登录到 ESXi Shell。
4. 导航到以下目录：

   ```
   /etc/vmware/ssl
   ```
5. 使用以下命令通过重命名所有现有证书进行备份：

   ```
   mv rui.crt orig.rui.crt
   mv rui.key orig.rui.key
   ```
6. 要生成新证书，请运行以下命令：

   ```
   /sbin/generate-certificates
   ```
7. 重新启动主机。
8. 确认主机已成功生成新的证书：
   a. 使用以下命令列出证书：

      ```
      ls -la
      ```
   b. 通过 `orig.rui.crt` 和 `orig.rui.key` 比较新证书文件的时间戳(如果原始文件可用)。

将 NNMi 配置为使用 HTTPS 与管理程序通信

备注: 如果需要使用 HTTP 与管理程序通信，请参阅启用 HTTP 与管理程序通信 (第 48 页)。

要启用 NNMi 以使用 HTTPS 协议监视管理程序上托管的 VM(如 VMWare ESXi)，必须使用以下选项之一将管理程序的受信任证书上载到 NNMi：

- 使用 NNMi 用户界面上载受信任的证书。
- 使用命令行界面 (CLI) 上载受信任的证书。

备注: 受信任的证书是 SSL 证书，NNMi 使用该证书通过 HTTPS 协议与管理程序建立受信任的连接。在默认级别和区域级别，NNMi 使用 CA 证书信任使用同一 CA 颁发的证书的管理程序。在节点级别，则使用通过将 FQDN 作为使用者名称生成的管理程序的 SSL 证书(自签名或 CA 签名证书)。

本部分提供通过使用 CLI 上载证书的说明。有关使用 NNMi 用户界面进行上载的说明，请参阅管理员帮助 > 配置通信协议。

要将受信任的证书上载到 NNMi，请执行以下步骤：

1. 获取管理程序的受信任证书，然后将其复制到 NNMi 管理服务器上的临时位置。

   备注: 仅限 VMware。必须将 VMware 默认证书 (localhost.localdomain) 替换为使用 ESXi 服务器的主机名生成的证书。有关详细信息，请参阅 VMware 文档。有关要在 ESX5.1 和 ESX5.5 服务器上执行的示例步骤，请参阅替换 VMware 默认证书 (第 46 页)

2. 验证证书的格式是否受支持。支持的受信任证书的文件扩展名为 `.pem`、`.crt`、`.cer` 和 `.der`。
3. 执行相应命令，在所需级别上载证书。从下表中选择符合您要求的命令：

级别	用途	命令
默认(全局)	在默认级别为组织上载与组织在管理程序上全局使用的证书具有相同签名 CA 的受信任证书。	`nnmcommunication.ovpl addCertificate -default -cert <证书文件的完全限定路径>`
区域	为组织上载与组织在给定区域中的管理程序上使用的证书具有相同签名 CA 的区域受信任证书。	`nnmcommunication.ovpl addCertificate -region <区域名称或 UUID> -cert <证书文件的完全限定路径>`
节点	上载特定管理程序上使用的 SSL 证书(CA 签名或自签名服务器证书)。 **备注:** 必须使用完全限定域名 (FQDN) 作为使用者名称生成自签名或 CA 签名证书。	`nnmcommunication.ovpl addCertificate -nodeSetting <节点名称或 UUID> -cert <证书文件的完全限定路径>`

   示例命令：

   - 默认：`nnmcommunication.ovpl addCertificate -default -cert /tmp/new.pem`
   - 区域：`nnmcommunication.ovpl addCertificate -region region1 -cert /tmp/region1.der`
   - 节点：`nnmcommunication.ovpl addCertificate -nodeSetting node1 -cert /tmp/node1.crt`

4. 成功执行后，命令输出将显示有关已上载证书的信息。验证证书信息。

提示:

- 您可以通过使用 `listCertificates` 和 `removeCertificate` 命令查看或删除已上载的证书。有关详细信息，请参阅 `nnmcommunication.ovpl` 参考页或 Linux 联机帮助页。
- 发现管理程序后，您可以通过使用命令 `updateWebagentSettings` 直接在 Web 代理上，上载、替换或删除证书。有关详细信息，请参阅 `nnmcommunication.ovpl` 参考页或 Linux 联机帮助页。

启用 HTTP 与管理程序通信

默认情况下，NNMi 使用 HTTPS 协议与管理程序通信。

如果需要使用 HTTP，请向 `server.properties` 文件添加所需属性：

1. 导航到 `server.properties` 文件：

   Windows：

   `%NnmDataDir%\nmsas\NNM\server.properties`

   Linux：

   `$NnmDataDir/nmsas/NNM/server.properties`
2. 添加以下行：

   ```
   #Determines whether http should be used to communicate with SOAP agents such as the VMware vSphere API.
   #HP recommends this property only be enabled in demonstration or test environments and that HTTPS be
   #configured for production environments.
   nms.comm.soap.targetconfig.HTTP_ENABLED=true
   ```
3. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 **ovstop** 命令。

   在 NNMi 管理服务器上运行 **ovstart** 命令。

要针对管理程序通信禁用 HTTP：

1. 导航到 `server.properties` 文件：

   Windows：

   `%NnmDataDir%\nmsas\NNM\server.properties`

   Linux：

   `$NnmDataDir/nmsas/NNM/server.properties`
2. 将 HTTP_ENABLED 属性值更改为 false：

   `nms.comm.soap.targetconfig.HTTP_ENABLED=false`
3. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 **ovstop** 命令。

在 NNMi 管理服务器上运行 **ovstart** 命令。

备注: 执行将 NNMi 配置为使用 HTTPS 与管理程序通信 (第 46 页)中所述的步骤。

评估通信

本节列出评估通信设置的进度和成功与否的方法。仅当完成发现之后，才能完成大多数这些任务。

请考虑以下情况：

- 是否为 SNMP 配置了所有节点？ (第 49 页)
- SNMP 访问当前是否对设备可用？ (第 49 页)
- SNMP 设备的管理 IP 地址是否正确？ (第 49 页)
- NNMi 使用的通信设置是否正确？ (第 49 页)
- 状况轮询器设置是否符合通信设置？ (第 50 页)

是否为 SNMP 配置了所有节点？

1. 打开**节点**库存视图。
2. 筛选**设备配置文件**列以包含字符串 `No SNMP`。
   - 对于要管理的每个设备，配置特定节点的通信设置。另外，可以展开区域以包括节点并更新访问凭据。
   - 如果通信设置正确，则验证设备上的 SNMP 代理是否正在运行且配置正确(包括 ACL)。

SNMP 访问当前是否对设备可用？

1. 在库存视图中选择节点。
2. 选择**操作 > 状态轮询**或**操作 > 配置轮询**。

   如果结果显示任何 SNMP 值，则通信正常。

还可以从命令行使用 `nnmsnmpwalk.ovpl` 命令测试通信。有关详细信息，请参阅 nnmsnmpwalk.ovpl 参考页或 Linux 联机帮助页。

SNMP 设备的管理 IP 地址是否正确？

要确定 NNMi 已经为设备选择了哪个管理地址，请执行以下步骤：

1. 在库存视图中选择节点。
2. 选择**操作 > 通信设置**。
3. 在**通信配置**表单上，验证“活动 SNMP 代理设置”列表中列出的 SNMP 代理的管理地址是否正确。

NNMi 使用的通信设置是否正确？

SNMP 团体字符串缺失或不正确可能导致发现无法完成，或可能对发现性能产生负面影响。

要验证为设备配置的通信设置，请使用 `nnmcommunication.ovpl` 命令或执行以下步骤：

1. 在库存视图中选择节点。
2. 选择**操作 > 通信设置**。
3. 在**通信配置**表单上，验证 SNMP 配置设置表中列出的值是否是 NNMi 要用于此节点的设置。

   如果通信设置不正确，则使用 SNMP 配置设置表中的源信息作为解决问题的起点。可能需要更改区域或特定节点的配置或排序编号。

   > **备注:** 对于 VMware 通信，验证 Web 代理表单中的活动设置或使用 nnmcommunication.ovpl listWebAgentSettings 命令。

   有关详细信息，请参阅《NNMi 管理员帮助》。

状况轮询器设置是否符合通信设置？

即使通信设置允许到达网络某区域的协议流量，监视设置中也可能禁用该类型的流量。要确定是否将覆盖设置：

1. 在库存视图中选择节点。
2. 选择**操作 > 监视设置**。

如果监视设置或通信设置对设备禁用某种类型的流量，则 NNMi 不会发送该流量。

微调通信

减少验证失败

如果 NNMi 在发现期间生成太多验证陷阱，则为较小的区域或特定节点配置较小的访问凭据组供 NNMi 尝试。

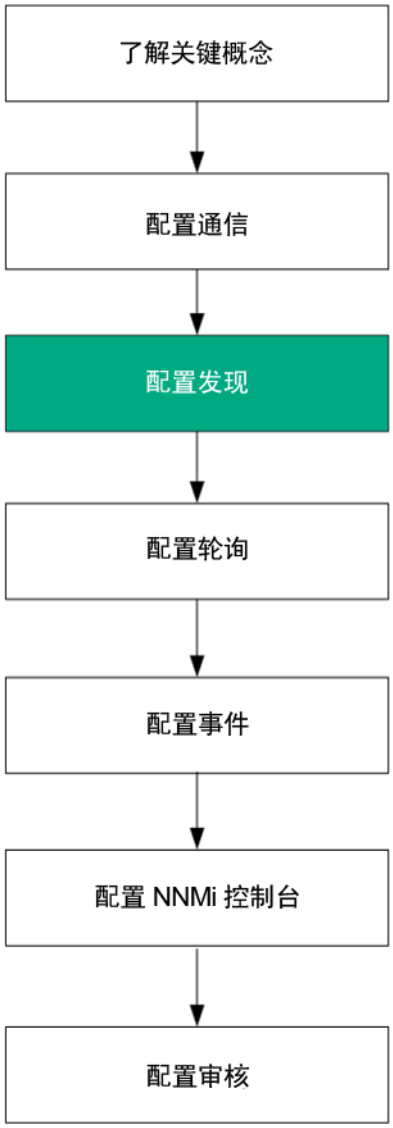
微调超时和重试次数

NNMi 尝试在发现期间使用 SNMP 联系设备时，通信配置确定 NNMi 是否可以采集必要的设备信息。当通信配置不包括正确的 SNMP 团体字符串时，或如果 NNMi 正在发现非 SNMP 设备，则 NNMi 使用配置的 SNMP 超时和重试次数设置。在这种情况下，较大超时值或较多重试次数会对发现的总体性能产生负面影响。如果网络包含已知对 SNMP/ICMP 请求响应较慢的设备，请考虑使用**通信配置**表单上的**区域**或**特定节点设置**选项卡来仅微调这些设备的超时和重试值。

减少默认团体字符串

拥有大量默认团体字符串可能会对发现性能产生负面影响。请不要输入太多默认团体字符串，而是通过在**通信配置**表单上使用**区域**或**特定节点设置**选项卡来微调网络特定区域的团体字符串配置。

NNMi 发现



最重要的网络管理任务之一是保持您的网络拓扑视图最新。HP Network Node Manager i Software (NNMi) 发现将用有关网络中节点的信息填充拓扑库存。NNMi 在螺旋发现进行过程中维护此拓扑信息，确保根源分析和疑难解答工具提供有关事件的准确信息。

本章提供的信息可帮助您配置 NNMi 发现。有关发现工作方式的介绍和有关如何配置发现的详细信息，请参阅 NNMi 帮助中的“发现您的网络”。

本章包含以下主题：

- 发现的概念 (第 52 页)
- 计划发现 (第 53 页)
- 配置发现 (第 60 页)
- 评估发现 (第 62 页)
- 调整发现 (第 65 页)

发现的概念

只发现路由器和交换机的 NNMi 默认行为使您能够专注于关键或最重要设备的网络管理。换句话说，先把目标对准网络的主干。通常，应避免管理终端节点(如个人计算机或打印机)，除非该终端节点被标识为关键资源。例如，数据库和应用程序服务器可能被视为关键资源。

NNMi 提供若干方式来控制发现哪些设备并将它们包括在 NNMi 拓扑中。发现配置可以非常简单，也可以很复杂或介于两者之间，这取决于您如何组织网络以及要用 NNMi 管理的设备。

备注: NNMi 不执行任何默认发现。您必须在 NNMi 拓扑中出现任何设备之前配置发现。

发现的每个节点(物理或虚拟驻留的)都会计入许可证限制数，不管 NNMi 是否在主动管理该节点。NNMi 许可证的容量可能影响发现方式。

跟踪许可证信息时，请注意以下几点：

- **消耗**：NNMi 发现并管理的节点不得超过 NNMi 许可的容量限制(四舍五入)：
  - **VMware** 或 HPE Helion OpenStack 环境：包含 `vnwareVM` 或 `kvmVM` 设备配置文件的每个设备相当于 1/10 个节点。
  - 所有其他设备相当于一个发现的节点。

有关许可证限制的详细信息，请参阅《NNMi 管理员帮助》中的“跟踪 NNMi 许可证”。

- 如果发现的节点数达到或超过许可的容量限制，则除非发生以下情况之一，否则不会发现任何新的节点：
  - 安装许可证扩展。
  - 查看配置设置并将 NNMi 发现限制为仅发现网络环境中的重要节点。然后，删除节点并让 NNMi 重新发现重置节点的被管库存。

备注: 有关配置发现以发现大量节点的信息，请参阅 NNMi 帮助。

状态监视的注意事项也可能影响您的选择。默认情况下，状况轮询器只监视连接到 NNMi 已发现的设备的接口。对于某些网络区域，您可以覆盖此默认值，可以发现超出您负责范围的设备。(有关状况轮询器的信息，请参阅 NNMi 状况轮询 (第 67 页)。)

NNMi 提供两个主要的发现配置模型：

- **基于列表的发现** - 通过种子列表明确告诉 NNMi 应当将哪些设备添加到数据库并加以监视。
- **基于规则的发现** - 告诉 NNMi 应当将哪些网络区域和设备类型添加到数据库，向 NNMi 提供每个区域的起始地址，然后允许 NNMi 发现已定义的设备。

可使用基于列表和基于规则的发现的任意组合来配置 NNMi 应当发现的设备。初始发现将这些设备添加到 NNMi 拓扑，然后螺旋发现会例行地重新发现网络以确保拓扑保持最新。

备注: NNMi 使用租户支持包含重叠地址域的网络，这些域可能存在于网络管理域的静态网络地址转换 (NAT)、动态网络地址转换 (NAT) 或端口地址转换 (PAT) 区域内。如果您具有此类网络，请将重叠地址域放入不同的租户(使用播种发现完成此操作)。有关详细信息，请参阅 NNMi 帮助。

备注: 如果使用 NNMi 管理基于 VMware 管理程序的虚拟网络，请参阅管理员帮助中的“虚拟环境中的租户”帮助主题。

提示: 如果计划配置多租户，请在启动网络发现之前配置租户。

NNMi 通过设备配置文件得出属性

当 NNMi 发现设备时，它使用 SNMP 直接收集某些属性。关键属性之一是 MIB II 系统对象 ID (`sysObjectID`)。NNMi 从系统对象 ID 得出其他属性，如供应商、设备类别和设备系列。

在发现期间，NNMi 采集 MIB II 系统功能，并将它们存储在数据库的拓扑部分中。系统功能在**节点**表单上可见。但是，NNMi 的任何其他部分(特别是监视配置)都不使用这些功能。NNMi 使用设备类别(从系统对象 ID 的设备配置文件)将设备匹配到节点组中。在节点视图表中，**设备类别**列标识每个节点的设备类别。

备注: 如果配置了 Web 代理(除 SNMP 代理之外)，NNMi 可以使用其他协议(例如，适用于 VMware 环境的 SOAP 协议)。

NNMi 附带了版本发行时可用的数千个系统对象 ID 的设备配置文件。可为环境中的唯一设备配置自定义设备配置文件，将这些设备对应到类别、供应商等等。

计划发现

作出关于以下方面的决策：

- 选择您的主发现方式 (第 53 页)
- 自动发现规则 (第 55 页)
- 节点名称解析 (第 57 页)
- 子网连接规则 (第 57 页)
- 发现种子 (第 58 页)
- 重新发现间隔 (第 58 页)
- 不发现对象 (第 59 页)
- 发现接口范围 (第 59 页)
- 通过 NNMi 监视虚拟 IP 地址 (第 59 页)
- 使用来自 SNMP 陷阱的发现提示 (第 60 页)

选择您的主发现方式

决定是执行完全基于列表发现、完全基于规则发现，还是两种方式结合使用。

基于列表的发现

使用基于列表的发现，可明确指定(作为发现种子)NNMi 应发现的每个节点。

备注: NNMi 使用租户支持包含重叠地址域的网络，这些域可能存在于网络管理域的静态网络地址转换 (NAT)、动态网络地址转换 (NAT) 或端口地址转换 (PAT) 区域内。如果您具有此类网络，请将重叠地址域放入不同的租户(使用播种发现完成此操作)。有关详细信息，请参阅 NNMi 帮助。

备注: 如果使用 NNMi 管理基于 VMware 管理程序的虚拟网络，请参阅管理员帮助中的“虚拟环境中的租户”帮助主题。

提示: 如果计划配置多租户，建议采用基于列表的发现方法。

只使用基于列表的发现的好处包括：

- 提供对 NNMi 所管理对象的严密控制。
- 支持在发现时使用非默认租户规范。
- 最简单的配置。
- 适合相对静态的网络。
- 开始使用 NNMi 的一种好方式。可以随后逐渐添加自动发现规则。

只使用基于列表的发现的缺点包括：

- 将新节点添加到网络时，NNMi 不发现它们。
- 必须提供要发现的节点的完整列表。

基于规则的发现

使用基于规则的发现，创建一个或多个自动发现规则，以定义 NNMi 应发现并包括在 NNMi 拓扑中的网络区域。对于每条规则，必须提供一个或多个发现种子(通过明确指定种子或通过启用 Ping 扫描)，然后 NNMi 自动发现网络。

使用基于规则的发现的好处包括：

- 适合大型网络。NNMi 可基于最小配置输入发现大量设备。
- 适合频繁改变的网络。添加到网络的新设备无需管理员干预即可发现(假定每个设备都由自动发现规则涵盖)。
- 确保添加到网络的任何新设备的发现都符合用于以及时方式管理新设备的服务级别协议，或标记未经授权的新设备的安全准则。

使用基于规则的发现的缺点包括：

- 更容易达到许可证限制数。
- 根据网络的结构不同，调整自动发现规则可能很复杂。
- 如果自动发现规则非常广泛，并且 NNMi 发现的设备比您要管理的更多，则您可能希望从 NNMi 拓扑删除不需要的设备。节点删除可能很费时间。
- 所有无种子节点在发现时都将接收默认租户。如果要使用 NNMi 多租户，必须在发现后更新租户分配。

自动发现规则

配置自动发现规则时，必须指定以下内容：

- 自动发现规则排序
- 发现中要排除的设备
- 是否使用 Ping 扫描
- 要使用的发现种子(如有)

自动发现规则排序

自动发现规则的**排序**属性的值通过以下方式影响发现范围：

- IP 地址范围

  如果设备处于两个自动发现规则范围内，则应用具有较低排序编号的自动发现规则的设置。例如，如果自动发现规则排除了一组 IP 地址，则不会有更高排序编号的其他自动发现规则处理那些节点，且该地址范围中的节点不会被发现，除非它们被列为发现种子。
- 系统对象 ID 范围
  - 如果自动发现规则中没有包括 IP 地址范围，则系统对象 ID 设置将应用于具有较高排序编号的所有自动发现规则。
  - 如果自动发现规则中包括 IP 地址范围，则系统对象 ID 范围只应用于自动发现规则内。

从发现中排除设备

- 要阻止发现某些对象类型，请创建具有较低排序编号的自动发现规则，它会忽略您不想发现的系统对象 ID。不要在此规则中包括 IP 地址范围。通过为此自动发现规则指定较低排序编号，该发现过程快速跳过匹配此规则的对象。
- IP 地址范围或系统对象 ID 范围的**被规则忽略**设置只影响该自动发现规则。被忽略范围中的设备可包括在另一个自动发现规则中。

备注: 某些网络使用诸如热备份路由器协议 (HSRP) 和虚拟路由器冗余协议 (VRRP) 的路由协议来提供路由器冗余。在路由器冗余组 (RRG) 中配置路由器时(即使用 HSRP)，在 RRG 中配置的路由器共享受保护的 IP 地址(一个活动和一个备用)。NNMi 不能发现和管理配置了同一受保护 IP 地址的多个 RRG。每个 RRG 都必须有唯一的受保护 IP 地址。

Ping 扫描

可以使用 Ping 扫描在已配置自动发现规则的 IP 地址范围中查找设备。对于初始发现，您可能希望对所有规则启用 Ping 扫描。这样就为不需要配置发现种子的 NNMi 发现提供了足够信息。

备注: Ping 扫描适用于 16 位或更小的子网，例如 `10.10.*.*`。

Ping 扫描尤其适用于发现未控制的 WAN 上的设备，如 ISP 网络。

备注: 防火墙经常将 Ping 扫描视为网络攻击，在这种情况下，防火墙可能会阻止发出 Ping 扫

描的设备的所有流量。

提示： 只对较小的发现范围启用 Ping 扫描。

自动发现规则的发现种子

为每个自动发现规则至少提供一个发现种子。用于提供种子的选项如下：

- 通过在**配置**工作区中的**发现**下单击**种子**，在**发现种子**表单上输入种子。
- 使用 `nnmloadseeds.ovpl` 命令以从种子文件加载信息。
- 至少对于初始发现，要为规则启用 Ping 扫描。
- 将设备配置为将 SNMP 陷阱发送到 NNMi 管理服务器。

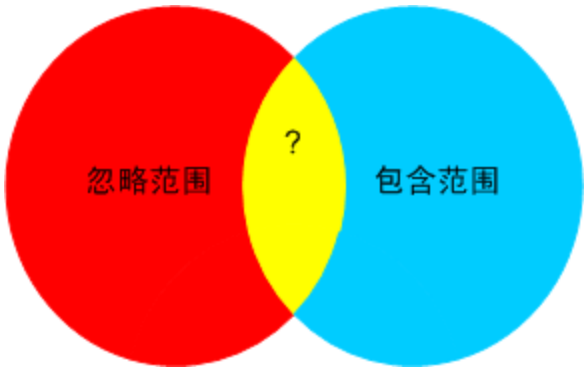
自动发现规则的最佳实践

- 因为 NNMi 自动管理所有发现的设备，所以，请使用精确匹配要管理的网络区域的 IP 地址范围。
  - 可以在自动发现规则中使用多个 IP 地址范围来限制发现。
  - 可以将大型 IP 地址范围添加到自动发现规则，然后从发现中排除该规则内的某些 IP 地址。
- 系统对象 ID 范围规范是前缀，不是绝对值。例如，范围 1.3.6.1.4.1.11 与 1.3.6.1.4.1.11.* 相同。

发现规则重叠

下图显示重叠的两个发现范围。左侧的圆圈表示 NNMi 发现忽略的 IP 地址范围或系统对象 ID 范围。右侧的圆圈表示要发现并包含在 NNMi 拓扑中的 IP 地址范围或系统对象 ID 范围。重叠区域可能会由发现包括或忽略，这取决于这些自动发现规则的排序。

重叠的发现范围



限制设备类型发现

要发现网络中不是打印机的所有 HP 设备，请用一个包括 HP 企业系统对象 ID (1.3.6.1.4.1.11) 的范围创建一条自动发现规则。在此自动发现规则中创建第二个范围，以忽略 HP 打印机的系统对象 ID (1.3.6.1.4.1.11.2.3 9)。不设置 IP 地址范围。

节点名称解析

默认情况下，NNMi 尝试按以下顺序识别节点：

1. DNS 简称
2. sysName 简称
3. IP 地址

> **备注:** 如果您更改了节点的主机名，则在 NNMi 数据反映名称更改之前存在延迟，因为 NNMi 缓存 DNS 名称以增强性能。

以下场景描述了可能要更改节点名称解析的默认顺序的情况：

- 如果组织依赖其他人更新 DNS 配置，则您可能设置一条为添加到网络的每个新设备定义 sysName 的策略。在这种情况下，将选择 sysName 设为节点名称解析的第一选择，这样 NNMi 就可以在新设备被部署到网络中时立即发现它。(在设备的整个生命周期内维护 sysName。)
- 如果组织不设置或维护被管设备的 sysName，则选择 sysName 作为节点名称解析的第三选项。

> **提示：** 如果使用完整或简短 DNS 名称作为主命名约定，请确认具有从 NNMi 管理服务器至所有被管设备的正向和反向 DNS 解析。

> **备注:** 完整 DNS 名称是命名约定时，拓扑图上的标签可能很长。

> **提示：** NNMi 选择最低环回地址作为 Cisco 设备的管理地址，因此，将 DNS 解析放在每个 Cisco 设备的最低环回地址上。

子网连接规则

仅针对基于列表的发现

对于基于列表的发现，NNMi 使用子网连接规则来检测跨 WAN 的连接。NNMi 评估它在可能连接的每个末端发现的设备的子网成员资格(通过检查其 IP 地址和子网前缀)，并查看子网连接规则以找到匹配项。

仅针对基于规则的发现

启用自动发现规则且 NNMi 找到子网前缀配置为 /28 和 /31 之间的设备时：

1. NNMi 检查是否有适用的子网连接规则。
2. 如果发现匹配，则 NNMi 使用子网中的每个有效地址作为提示，并尝试发现该地址。

提示：使用默认连接规则。请只在有问题时修改它们。

发现种子

列出设备以用作发现种子。

提示: 选择首选管理 IP 地址的 NNMi 规则之一将指定使用第一个发现的 IP 地址作为管理地址。可通过将首选 IP 地址配置为种子地址来影响 NNMi。

提示: 对于 Cisco 设备，使用环回地址作为发现种子，因为环回地址比设备上的其他地址的可达性更可靠。确保将 DNS 正确配置为能将设备主机名解析为环回地址。

仅针对基于列表的发现

对基于列表的发现，列出要 NNMi 管理的所有设备。您可以从资产管理软件或某些其他工具导出此列表。

因为 NNMi 不会自动将任何设备添加到此列表，请确保列表包括您负责的或影响监视和状态计算的每个设备。

仅针对基于规则的发现

发现种子对基于规则的发现是可选的：

- 如果为自动发现规则启用 Ping 扫描，则不需要指定该规则的种子。
- 对禁用 Ping 扫描的每个自动发现规则，请为每条规则至少标识一个种子。如果规则包括多个 IP 地址区域，则可能在每个可路由区域都需要种子，因为路由器不能跨 WAN 链路保持 ARP 条目。

提示: 对于最完整的基于规则的发现，请使用路由器而非交换机作为发现种子，因为路由器通常具有比交换机更大的 ARP 缓存。连接到要发现的网络的核心路由器是发现种子的最好选择。

重新发现间隔

NNMi 按照配置的重新发现间隔，重新检查数据库中的每个设备的配置信息。此外，NNMi 从自动发现规则涵盖的每个路由器采集 ARP 缓存，并在网络上查找新节点。

设备的通信相关配置的任何更改(如接口重新编号)都会自动触发 NNMi 更新该设备及其邻近设备的数据。

以下更改不触发自动重新发现；只在配置的重新发现间隔更新设备：

- 节点中的更改(如固件升级或系统联系人)。
- 有新节点添加到网络。

选择重新发现间隔以匹配网络中的更改级别。对于高度动态的网络，可能要使用 24 小时的最小间隔。对于较稳定的网络，可以安全地延长该间隔。

不发现对象

在 NNMi 中，有三种方式可将 NNMi 配置为忽视某些对象：

- 在**通信配置**表单上，可不同程度地关闭 ICMP 通信和/或 SNMP 通信：全局，对于通信区域或特定主机名/IP 地址。有关禁用这两个协议中的一个或全部的影响的信息，请参阅轮询协议 (第 38 页)。
- 在**发现配置**表单上，可设置指示 NNMi 不从某些 IP 地址或 SNMP 系统对象 ID 采集提示的自动发现规则。与条件匹配的节点仍然出现在图和数据库中，但螺旋发现不扩展到超出这些 IP 地址或对象类型的相邻设备。
- 在**发现配置**表单上，可设置指示 NNMi 从数据库排除特定 IP 地址范围和/或 IP 地址的自动发现规则。螺旋发现不在任何节点的地址列表上显示那些地址，也不在建立设备之间的连接时使用那些地址，因此 NNMi 从不监视那些地址的运行状况。
- 在**发现配置**表单的**排除的 IP 地址**选项卡上，您可以通过配置排除的 IP 地址筛选来排除要发现的 IP 地址范围。

  如果在发现节点后将该节点的所有 IP 地址都输入“排除的 IP 地址”列表，则 NNMi 不会删除该节点。此外，除非 NNMi 管理员故意将节点从 NNMi 数据库删除，否则 NNMi 不会删除该节点的完整历史记录。

  > **备注:** 如果排除某个 IP 地址范围，则也将排除网络管理域的静态网络地址转换 (NAT)、动态网络地址转换 (NAT) 或端口地址转换 (PAT) 区域内的任何重复地址。
  >
  > NNMi 使用租户支持包含重叠地址域的网络。如果您具有此类网络，请将重叠地址域放入不同的租户(使用播种发现完成此操作)。有关详细信息，请参阅 NNMi 帮助。

- 在**发现配置**表单的**排除的接口**选项卡上，您可以通过选择接口组从发现过程中排除特定类型的接口。有关详细信息，请参阅 NNMi 帮助。

发现接口范围

NNMi 允许您通过定义筛选来指定要发现的接口范围。当您具有大量节点而又只想发现一部分接口时，此功能特别有用。当您指定要发现的接口范围时，NNMi 不需要该范围之外的接口的相关信息；而是在从设备检索信息后使用“排除的接口”选项筛选接口。因此，基于范围的发现可以提高针对大量设备的发现性能，尤其是在您不需要管理这类设备上的所有接口时。

包含的接口范围筛选(在**发现配置**表单的**包含的接口范围**选项卡上定义)使用系统对象 ID 前缀和 ifIndex 值来定义接口范围。有关详细信息，请参阅 NNMi 帮助。

通过 NNMi 监视虚拟 IP 地址

NNMi 发现和监视诸如共享同一虚拟 IP 地址的群集服务器之类的设备。群集故障转移到新主动节点之后，NNMi 会将此虚拟 IP 地址与新主动节点关联。此关联并非立即发生，因为故障转移和 NNMi 发现更改之间，可能已经过去了一段时间。

您可以执行若干操作来配置 NNMi 以适应您的特定情况：

如果希望 NNMi 监视虚拟 IP 地址，请仅使用以下选项之一：

- 选项 1：对于此选项，NNMi 管理 N+1 个非 SNMP 设备，其中 N 代表以非虚拟 IP 地址发现的群集中的成员数。NNMi 发现额外的 (+1) 非 SNMP 节点，并以虚拟 IP 地址对其进行配置。

不要执行任何操作阻止 NNMi 发现虚拟 IP 地址。NNMi 使用此方法发现与配置为使用此虚拟 IP 地址的设备上的网络接口 (NIC) 卡关联的虚拟 IP 地址和物理 IP 地址。NNMi 将每个设备作为单独的非 SNMP 节点进行发现和监视。

- 选项 2：将 NNMi 配置为使用设备的物理 IP 地址作为群集服务器的首选管理地址。有关如何执行此操作的说明，请参阅 NNMi 帮助中的“特定节点设置表单(通信设置)”主题。

> **备注:** NNMi 可能无法立即识别出虚拟 IP 地址从一个主动节点到新主动节点的传输。NNMi 可能使用群集中当前主动节点以外的节点显示虚拟 IP 地址的状态。

如果不希望 NNMi 监视虚拟 IP 地址，请使用 NNMi 控制台执行以下操作：

1. 单击**配置**工作区中的**发现配置**。
2. 单击**排除的 IP 地址**选项卡。
3. 将虚拟 IP 地址或地址范围添加到要从发现中排除的地址列表。
4. 保存更改。

使用来自 SNMP 陷阱的发现提示

NNMi 将所有传入 SNMP 陷阱的源 IP 地址处理为 NNMi 自动发现规则的提示。

有关 SNMP 陷阱事件的详细信息，请参阅 NNMi 管理员帮助。

配置发现

本部分列出配置提示，并提供一些配置示例。阅读本部分中的信息之后，请参阅 NNMi 帮助中的“配置发现”，以了解具体步骤。

> **备注:** 因为一旦**保存并关闭发现种子**表单，NNMi 即会启动来自种子的发现，所以请确保在配置种子之前执行以下操作：
>
> - 完成所有通信配置。
> - 完成所有自动发现规则(如果有)。
> - 配置子网连接规则。
> - 配置名称解析首选项。
> - **保存并关闭**所有配置表单，返回到 NNMi 控制台。

> **提示：** 在作出任何重大的配置更改之前保存现有配置的副本是一个好的做法。有关详细信息，请参阅最佳实践：保存现有配置 (第 26 页)。

配置自动发现规则的提示

定义新自动发现规则时，仔细检查每个设置。对于新规则，默认启用自动发现，默认包括 IP 地址范围，并默认忽略系统对象 ID 范围。

配置种子的提示

配置种子时，请注意以下最佳实践：

- 如果已有文件列出要发现的节点，请将此信息的格式转为种子文件，并用 nnmloadseeds.ovpl 命令将节点列表导入到 NNMi 中。
- 在种子文件中，影响 NNMi 选为管理地址的 IP 地址的一种方式是指定 IP 地址。(如果使用主机名，则 DNS 为每个节点提供 IP 地址。)
- 种子文件中条目的有效格式如下所示：

  ```
  IP_address1 # node name

  IP_address2, <租户 UUID 或租户名称> # node name
  ```

  这些格式对 NNMi 和用户都易读。
- 出于维护目的，最好只用一个种子文件。根据需要添加节点，然后重新运行 nnmloadseeds.ovpl 命令。NNMi 发现新节点，但不重新计算现有节点。

备注: 如果无法加载种子文件，请尝试通过 nmsproc 使该文件可读(644 个权限)。

- 从种子文件删除节点时，不会从 NNMi 拓扑删除它。请直接在 NNMi 控制台中删除节点。
- 从图或库存视图删除节点时不删除种子。
- 如果希望 NNMi 重新发现节点，请从图或库存视图以及**种子**表单(在 NNMi 控制台的**配置**工作区的**发现**区域中)删除该节点，并重新在 NNMi 控制台中输入节点，或运行 nnmloadseeds.ovpl 命令。

仅针对基于规则的发现

- 为发现规则指定种子之前要完全配置好它。即在**发现配置**表单上单击**保存并关闭**。(**发现种子**表单是单独的表单，不是数据库模型中**发现配置**表单的一部分。因此，保存有关**发现种子**表单的信息时，NNMi 立即更新种子配置。)

发现链路聚合

备注: 链路聚合需要 NNMi Advanced 或 NNMi Premium 许可证。

链路聚合 (LAG) 协议支持网络管理员在交换机上配置一组接口作为一个聚合器接口。此配置会并行使用多个接口创建与其他设备的聚合器第 2 层连接，以增加带宽、数据传输速率和冗余。

有关详细信息，请在 NNMi 帮助中搜索“**链路聚合**”。

发现服务器到交换机链路聚合 (S2SLA)

备注: 链路聚合需要 NNMi Advanced 或 NNMi Premium 许可证。

网络管理员经常需要服务器和交换机之间额外的可靠性和更高的资源利用率。许多网络管理员选择使用链路聚合配置协议 (LACP)，因为它被网络设备供应商广泛使用。IT 工程师将服务器到交换机配置两端的端口绑定后将自动协商 LACP。

网络管理员经常选择使用两种交换机到服务器的连接类型之一，以在服务器和交换机之间实现所需的可靠性和资源利用率：

- 选项 1：绑定服务器上的两个或多个端口，并将其连接到交换机上相同的端口数。如果服务器或交换机上的某个端口出现故障，则将激活备用端口。
- 选项 2：绑定服务器和交换机以提供聚合中所有端口的聚合总带宽。

NNMi 提供服务器到交换机链路聚合 (S2SLA) 发现功能，帮助您管理交换机到服务器的连接。要确保 NNMi 可以正确发现节点的 S2SLA 信息，请完成以下任务：

- 默认情况下，Linux 不安装 SNMP 代理包 Net-SNMP。如果您的 NNMi 管理服务器上缺少 Net-SNMP，则必须安装它。
- Linux 上的绑定接口可以使用某个聚合接口的 MAC 地址，但并非必须这么做。绑定的接口可以有一个不属于服务器任何接口的 MAC 地址。

  提示: 聚合中的所有接口均使用相同的 MAC 地址。各种 SNMP 接口表为聚合器和聚合接口返回相同的 MAC 。共享 MAC 在出站包中使用。在交换机的聚合接口上听到此 MAC 时，访问交换机的 FDB 表会显示此 MAC。

  要查看原始 MAC 地址，请使用以下命令：

  ```
  cat /proc/net/bonding/bond0
  ```

评估发现

此部分列出了评估发现进度和是否成功的方式。

跟踪初始发现的进度

NNMi 发现是动态的并持续进行；它不会完成，因此您不会看到“发现已完成”的消息。初始发现和连接过程要花一些时间。以下各项建议估计初始发现进度的方式：

- 在**系统信息**窗口的**数据库**选项卡上，监视节点计数达到所需水平并稳定下来。此窗口不会自动刷新。在初始发现期间，打开**系统信息**窗口若干次。
- 在**配置**工作区的**发现**下，查看**种子**页。刷新此页，直到所有种子都显示节点已创建结果，这表示设备已添加到拓扑数据库。此结果不表示该 NNMi 已从设备采集所有信息并已处理好其连接。
- 为代表性节点打开**节点**表单。**发现状况**字段(位于**常规**选项卡上)变为发现已完成时，NNMi 已收集节点的基本特征以及节点的 ARP 缓存和发现协议邻居(如果适用)。此状况不表示该 NNMi 已完成该设备的连接分析。
- 在**节点**库存视图中，从您网络的不同区域扫描查看关键设备是否存在。
- 打开代表性节点的**第 2 层邻居视图**，确定是否已完成该区域的连接分析。
- 查看**第 2 层连接**和 **VLAN** 库存视图，以估计第 2 层处理的进度。

所有种子都发现了吗？

1. 从**配置**工作区的**发现**下，单击**种子**。
2. 在**种子**页上，按**发现种子结果**列对节点列表排序。对处于错误状况的任何节点，请考虑以下事项：

- **由于无法访问的节点或无法解析的 DNS 名称或 IP 地址而失败的发现** - 对于这些失败类型，请验证网络与节点的连接并检查 DNS 名称解析是否准确。要解决 DNS 问题，请使用 IP 地址为节点播种，或在 `hostnolookup.conf` 文件中包括主机名。对于因 IP 地址不应解析到主机名而产生的问题，请在 `ipnolookup.conf` 文件中包括这些 IP 地址。有关详细信息，请参阅 `hostnolookup.conf` 和 `ipnolookup.conf` 参考页或 Linux 联机帮助页。

- **超过许可证节点计数** - 当发现的设备数达到许可证限制时会出现这种情况。可删除某些发现的节点或购买更多的节点包许可证。

  跟踪许可证信息时，请注意以下几点：

  - **消耗**：NNMi 发现并管理的节点不得超过 NNMi 许可的容量限制(四舍五入)：
    - **VMware** 或 HPE Helion OpenStack 环境：包含 `vnwareVM` 或 `kvmVM` 设备配置文件的每个设备相当于 1/10 个节点。
    - 所有其他设备相当于一个发现的节点。

  有关许可证限制的详细信息，请参阅《NNMi 管理员帮助》中的“跟踪 NNMi 许可证”。

- **已发现节点但没有 SNMP 响应** - 对于已播种设备和通过自动发现而发现的设备，SNMP 通信都可能发生问题。有关详细信息，请参阅评估通信 (第 49 页)。

所有节点都具有有效的设备配置文件吗？

1. 打开**节点**库存视图。
2. 筛选**设备配置文件**列，以包含字符串无设备配置文件。
3. 如果已发现节点但没有设备配置文件，请添加新的设备配置文件(从**配置 > 设备配置文件**)，然后在节点上执行配置轮询以更新其数据。

所有节点都正确发现了吗？

要避免发现时出现问题，NNMi 应仅使用不在管理域中的任何其他节点上出现的唯一 IP 地址来管理节点。例如，如果节点突然消失或与数据库中的另一个节点合并，并且它是路由器冗余组 (RRG) 的一部分，就有特殊要求。要管理参与 RRG 的路由器，必须使用唯一 IP 地址(非保护地址)作为路由器的管理地址，并且必须在该地址上启用 SNMP。

> **备注:** 如果 NNMi 试图使用受保护 IP 地址作为管理地址，则它将无法正确管理路由器。

在**节点**库存视图中检查数据。如果任何节点没有管理地址，则检查通信设置中是否有是否为 SNMP 配置了所有节点？ (第 49 页)中所述的那些节点。

如果预期的节点不在**节点**库存视图中，则检查以下事项：

- 验证每个缺少的节点上是否正确配置了发现协议(例如 CDP)。
- 如果缺少的节点在 WAN 上，则为包括该节点的自动发现规则启用 Ping 扫描。

自动发现规则

仅针对基于列表的发现。

如果看到意外的发现结果，则重新计算自动发现规则。

当 NNMi 发现找到地址提示时，会通过第一个匹配规则来确定是否应创建节点。如果无规则匹配，则 NNMi 发现丢弃提示。自动发现规则的排序编号确定应用自动发现规则配置设置的顺序。

对于每个自动发现规则，请检查以下设置：

- 必须启用**发现包含的节点**，该规则才会自动发现。
- 对于您要为该规则发现的节点类型，验证以下设置是否正确：
  - **发现所有 SNMP 设备**
  - **发现非 SNMP 设备**

  请记住，默认情况下只发现路由器和交换机，而不发现非 SNMP 节点。启用这些设置时若未考虑您的环境，则可能导致 NNMi 发现比预期更多的节点。

IP 地址范围

发现提示的 IP 地址必须匹配 IP 地址范围列表中的**包含在规则中**条目。如果自动发现规则中没有包括 IP 地址范围，则将所有地址提示都视为匹配。(有关此情况，请参阅配置自动发现规则的提示 (第 60 页)。)另外，提示不能匹配任何标记为**被规则忽略**的条目。如果所有检查都成功匹配，则此规则的配置用于处理提示。

- 如果没有发现某些预期存在的设备，请检查配置的 IP 范围，确保那些设备的 IP 地址已包含在范围中，没有被较低排序编号的规则忽略。
- 如果您发现了比所需更多的设备，则修改包括范围，或对不想发现的设备的 IP 地址添加忽略范围。同时，确定启用了**发现所有 SNMP 设备**。

系统对象 ID 范围

来自发现提示的系统对象 ID (OID) 必须匹配系统对象 ID 范围列表中的**包含在规则中**条目。如果自动发现规则中没有包括系统对象 ID 范围，则将所有对象 ID 都视为匹配。另外，OID 不能匹配任何标记为**被规则忽略**的条目。如果所有检查都成功匹配，则此规则的配置用于处理提示。

- 用系统对象 ID 范围可展开自动发现，以包括超过默认量的路由器和交换机，也可以排除特定的路由器和交换机。
- 每个节点都必须同时匹配在被发现并添加到拓扑数据库之前指定的 IP 地址范围和系统对象 ID 范围。

所有连接和 VLAN 都正确吗？

将设备添加到拓扑之后，NNMi 用单独步骤创建第 2 层连接和 VLAN。评估连接和 VLAN 之前，给 NNMi 充分时间进行初始发现。

评估第 2 层连接

要评估第 2 层连接，请为所需的每个网络区域创建节点组，然后显示该节点组的拓扑图。(在**节点组**库存中，选择节点组，然后单击**操作 > 节点组图**。)查找未连接到该图中其他节点的任何节点。

要评估 VLAN，请从 **VLAN** 库存视图打开每个 **VLAN** 表单，然后检查该 VLAN 的端口列表。

NNMi 发现与重复的 MAC 地址

在发现时考虑 MAC 地址有以下好处：

- 增强对 DHCP 或其他更改 IP 地址的节点的支持。
- 对于使用重复 IP 地址配置的节点，增强节点标识。
- 增强对不报告托管 IP 地址的设备的支持。

在发现期间，NNMi 从网络内以太网交换机读取转发数据库 (FDB) 表，以帮助 NNMi 确定网络设备之间的通信路径。NNMi 搜索这些 FDB 表，以查找有关发现的节点的信息。当 NNMi 管理服务器找到对重复介质访问控制 (MAC) 地址的 FDB 引用时，会执行以下操作：

- 如果两个或更多已发现节点包含与同一租户中的相同媒体访问控制 (MAC) 地址关联或与默认租户中的某一节点以及其他任何租户中的一个节点关联的接口，则 NNMi 会忽视 FDB 中针对这些重复 MAC 地址报告的通信路径。这可能导致在包括这些重复 MAC 地址的网络区域中，NNMi 图上缺少连接。

  NNMi Advanced 或 NNMi Premium - 全局网络管理功能：如果两个 NNMi 管理服务器发现的节点包含与同一个媒体访问控制 (MAC) 地址关联的接口，那么全局 NNMi 管理服务器的图可能缺少区域 NNMi 管理服务器的图上可见的连接。
- 如果单个节点包含具有相同 MAC 地址的多个接口，则 NNMi 将收集那些接口的所有通信路径信息，并在 NNMi 图上显示该信息。

在以下情况下，转发数据库 (FDB) 信息可能会导致 NNMi 建立错误的 L2 连接：

- 将 FDB 配置为缓存且包含过时数据时。
- 在使用来自各种供应商的硬件的网络环境中，每个环境生成不同、有时冲突的 FDB 数据。

可选：NNMi 管理员可以将发现配置为对于一个节点组忽略此 FDB 数据。

重新发现设备

1. 执行设备的配置轮询，确认要删除该设备。
2. 删除设备。

如果设备是种子，则删除种子，然后重新添加种子。

调整发现

对于常规发现性能，请微调发现配置以只发现关键和重要设备。

- 按 IP 地址范围和/或系统对象 ID 筛选。
- 限制非 SNMP 设备和任何 SNMP 设备(非交换机或路由器)的发现。

要在命令行上从 NNMi 数据库删除一个或多个节点，请使用 `nnmnodedelete.ovpl` 命令。该命令从 NNMi 数据库删除节点，但不删除种子定义。

要在命令行上从 NNMi 数据库删除一个或多个种子定义，请使用 `nnmseeddelete.ovpl` 命令。

有些特殊发现环境可以通过抑制发现协议采集或 VLAN 索引来补救。有关详细信息，请参阅抑制对特定节点使用发现协议 (第 236 页)或抑制对大型交换机使用 VLAN 索引 (第 238 页)。

发现日志文件

要查看失败的发现类，请在 nnm.log 文件中查看以字符串 com.hp.ov.nms.disco 开头的类的包含关键字 **Exception** 的消息。

有关日志文件的信息，请参阅 NNMi 日志记录 (第 243 页)。

未编号接口

NNMi 支持发现并监视未编号的接口和关联的第 2 层连接，包括全局网络管理 (GNM) 环境中的连接。

如果要在 GNM 环境中启用未编号接口的第 2 层连接，则必须在区域管理器和全局管理器上均执行此操作。

可以使用 NNMi 的**配置 > 发现**工作区配置(启用和禁用)未编号接口的第 2 层连接。有关详细信息，请参阅 NNMi 管理员帮助。

或者，使用 nnmunnumberedcfg.ovpl 命令配置未编号接口的连接。有关详细信息，请参阅 nnmunnumberedcfg.ovpl 参考页或 Linux 联机帮助页。

> **备注:** 节点组不在区域管理器和全局管理器之间复制。

可以使用 nnmunnumberedcfg.ovpl 命令在全局管理器和区域管理器之间复制配置设置。此功能允许您在区域管理器和全局管理器上以不同的方式定义节点组。例如，您可以在全局级别定义所有路由器，但在每个区域管理器只定义一个路由器子集。

建议在全局管理器和区域管理器上进行不同的配置。例如，除非直接从全局管理器管理节点，否则无需在全局管理器上配置可选子集，因为只在区域管理器上收集该数据。

控制无响应对象的删除操作

通过指定对象变得无响应后等待的天数，可以控制以下无响应对象的删除操作：

- 无响应的节点
- 已关闭的连接

要控制无响应对象的删除操作，请执行以下步骤：

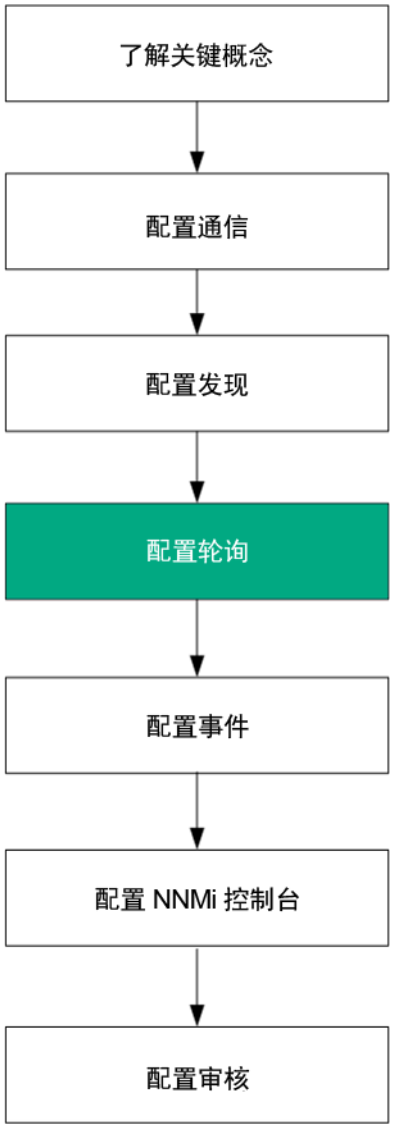
1. 在**配置**工作区，单击**发现配置**。
2. 在**删除无响应对象控件**区域，输入删除适用的对象前系统等待的天数。请注意，值为零 (0) 表示不应删除对象。

指定的等待时段过后，将从数据库中删除无响应的对象。

> **备注:** 在以下任一情况下，NNMi 不会在启用**删除未响应节点**后删除虚拟机节点：
>
> - VM 不支持 SNMP 代理
> - VM 没有任何 IP 地址，因为未安装 VMware Tools
> - 没有为 VM 配置 IP 地址故障监视

有关详细信息，请参阅管理员帮助中的“配置是否删除不响应的节点”帮助主题。

NNMi 状况轮询



本章提供的信息可帮助您通过配置 HP Network Node Manager i Software (NNMi) 状况轮询器服务来扩展和微调网络监视。本章是 NNMi 帮助信息的补充。有关监视功能如何工作的说明以及如何配置监视的详细信息，请参阅 NNMi 帮助中的“监视网络运行状况”。

本章包含以下主题：

- 状况轮询的概念 (第 68 页)
- 计划状况轮询 (第 68 页)
- 配置状况轮询 (第 76 页)
- 评估状况轮询 (第 78 页)
- 调整状况轮询 (第 80 页)

状况轮询的概念

本节简要概述了网络监视，包括状况轮询器用于评估轮询组的顺序。阅读本部分中的信息之后，请继续到计划状况轮询 (第 68 页)，以了解更多特定信息。

与网络发现一样，应当重点对网络中的关键或最重要设备进行网络监视。NNMi 可以只轮询拓扑数据库中的设备。您可控制 NNMi 监视哪些网络设备、要使用的轮询类型和轮询间隔。

可以使用**监视配置**表单中的接口和节点设置来优化设备的轮询状态，并为不同的类、接口类型和节点类型设置不同的轮询类型和间隔。

您可以将状况轮询器数据采集配置为基于 ICMP (ping) 响应，或基于 SNMP 数据。NNMi 自动处理从您启用的数据采集类型到内部实际 MIB 对象的映射，这极大地简化了配置。

> **备注:** 如果配置了 Web 代理(除 SNMP 代理之外)，NNMi 可以使用其他协议(例如，适用于 VMware 环境的 SOAP 协议)。

当计划轮询配置时，应当仔细考虑如何为状况轮询器服务设置接口组和节点组。如果是第一次接触组的概念，请参阅节点组和接口组 (第 27 页)和节点接口和地址层次结构 (第 31 页)，以了解概述信息。

评估的顺序

由于一个接口或节点可能适合于多个组，因此状况轮询器以明确定义的评估顺序应用配置的轮询间隔和轮询类型。对于发现的拓扑中的每个对象：

1. 如果对象是接口，则状况轮询器查找合适的接口组。按从最低到最高的排序编号来评估组。将使用第一个匹配组，并且评估停止。
2. 如果没有接口组捕获到该对象，则按从最低到最高的排序编号来评估节点组。将使用第一个匹配组，并且评估停止。尚未根据其自身特征适合于某个接口组的任何包含的接口从其托管节点继承轮询设置。
3. 对于发现但未包含在任何节点或接口设置定义中的设备，全局监视设置(在**监视配置**表单的**默认设置**选项卡上)建立监视行为。

计划状况轮询

本节提供有关状况轮询器配置(包括轮询配置清单)计划的信息；以及可帮助您计划监视、决定如何创建轮询组和确定轮询处理期间应当捕获的数据类型的更多详细信息。

轮询清单

可以使用以下清单来计划状况轮询器配置。

- 您希望 NNMi 监视什么？
- 被监视项基于对象类型、位置、相对重要性或其他标准时如何逻辑分组？
- NNMi 应当多久监视一次每个分组？
- 应当采集哪些数据来捕获有关受监视项的信息？可能包括：
  - ICMP (ping) 响应
  - SNMP 故障数据

- SNMP 性能数据(如果有一个或多个 NNM Performance iSPI 的许可证)
- 其他 SNMP 组件运行状况数据

> **备注:** 如果配置了 Web 代理(除 SNMP 代理之外)，NNMi 可以使用其他协议(例如，适用于 VMware 环境的 SOAP 协议)。

- 应该将网络设备的哪些 SNMP 陷阱发送到 NNMi?

轮询配置示例

为帮助您了解轮询配置过程，请考虑此示例。假定网络包含来自 ProximiT 的最新代理服务器。必须确保可以访问这些设备，但不必对代理服务器进行 SNMP 监视。

1. NNMi 可以监视什么？

   由于只能监视发现的设备，因此可配置自动发现规则以确保 NNMi 数据库包含 ProximiT 代理服务器。有关配置发现的详细信息，请参阅 NNMi 发现 (第 51 页)。
2. 什么是被监视项的逻辑组？

   将 ProximiT 代理服务器归为一组并对它们应用同一监视设置，这很有意义。因为不对设备执行接口 (SNMP) 监视，所以不需要任何接口组。

   还可以使用此节点组筛选视图、将代理服务器作为组来检查其状态，以及将组置于服务中断状态以更新固件。
3. NNMi 应当多久监视一次每个组？

   对于您的服务级别协议，5 分钟的代理服务器轮询间隔已足够。
4. 应当采集哪些数据？

   在监视配置上这里与其他组有一些区别。对于 ProximiT 代理服务器示例，您启用 ICMP 故障监视，并禁用 SNMP 故障和轮询监视。如果不对组进行 SNMP 故障监视，则不会应用组件运行状况监视。
5. 应该将哪些 SNMP 陷阱从网络设备发送到 NNMi?

   某些 SNMP 陷阱被接收而非等待下一轮询间隔时，NNMi 使用这些陷阱轮询设备。

有关这些配置选择的更多详细计划信息，请参阅以下主题：

- NNMi 可以监视什么？ (第 69 页)
- 计划组 (第 71 页)
- 计划轮询间隔 (第 74 页)
- 决定要采集的数据 (第 74 页)
- 决定要发送到 NNMi 的 SNMP 陷阱 (第 75 页)

NNMi 可以监视什么？

状况轮询器服务监视管理域中要进行主动监视的每个已发现的接口、地址和 SNMP 代理。还可对状况轮询器进行配置，以提供卡、机箱、节点传感器、物理传感器和路由器冗余组监视。

> **备注:** 在大多数情况下，仅轮询连接的接口足以提供准确的根源分析。扩展被监视接口组会影响轮询性能。

如果 NNMi 正在监视管理程序网络环境，则还监视其他对象，包括：

- 管理程序
- 管理程序上托管的虚拟机
- 虚拟交换机
- 上行(表示为接口对象)

提示: 确保虚拟机上已安装 VMware Tools，然后使用 NNMi 提供的虚拟机节点组针对与您的 VM 关联的 IP 地址启用故障轮询。建议采用此实践以确保 NNMi 能够标识底层虚拟机已被删除或移动到不由 NNMi 管理的管理程序中的所有 VM 节点。有关启用故障轮询的详细信息，请参阅《NNMi 管理员帮助》中的“监视的默认设置”。

提示: 使用 NNMi 提供的**虚拟机**节点组针对与您的虚拟机 (VM) 关联的 IP 地址启用故障轮询。建议采用此实践以确保 NNMi 能够标识底层虚拟机已被删除或移动到不由 NNMi 管理的管理程序中的所有 VM 节点。有关详细信息，请参阅《NNMi 管理员帮助》中的“监视的默认设置”和“配置是否删除不响应的节点”。

有关监视的详细信息，请参阅 NNMi 帮助。

另请参阅扩展监视 (第 71 页)

停止监视

NNMi 管理模式用于将设备或接口设置为“非被管”或“服务中断”。“非被管”被视为永久状态；您将不再需要了解该对象的状态。“服务中断”属于临时状态，其中一个或多个对象将脱机并会产生过多宕机事件。

将管理模式视为在所有组设置上的一个设置。只要对象状态设置为“非被管”或“服务中断”，无论其组、轮询间隔或类型是什么，状况轮询器都不与该对象通信。

提示： 无需对您选择发现并放置在数据库中的某些设备和/或接口进行轮询。请记下您将永久设置为“非被管”的对象。可能要创建一个或多个节点组以便您更方便地设置管理模式。

到未监视节点的接口

有时，您想要知道连接到未直接管理的设备的某接口的状态。例如，您希望知道与应用程序或 Internet 服务器的连接是否正常，但您可能并不负责维护该服务器。如果未将该服务器包含在发现规则中，则 NNMi 将面向该服务器的接口视为未连接。

有两个方法可以监视连接到未监视节点的重要接口的状态。

- 发现未监视节点

  将未监视节点添加到 NNMi 拓扑中时，NNMi 把将节点连接到拓扑其余部分的接口视为已连接。然后 NNMi 可以按照监视配置轮询这些接口。NNMi 发现节点处于被管状态。对于您不希望 NNMi 监视的节点，可以取消管理它们。

> **备注:** 不管 NNMi 是否主动管理每个发现的节点，这些节点都计入许可证限制数。

- 轮询未连接的接口

  可以创建一个包含网络设备的节点组，这些网络设备提供与未发现节点的连接。然后启用对该节点组的未连接接口的轮询。

  NNMi 轮询节点组中设备上的所有接口，对于具有多个接口的设备，这可能会增加很多流量。

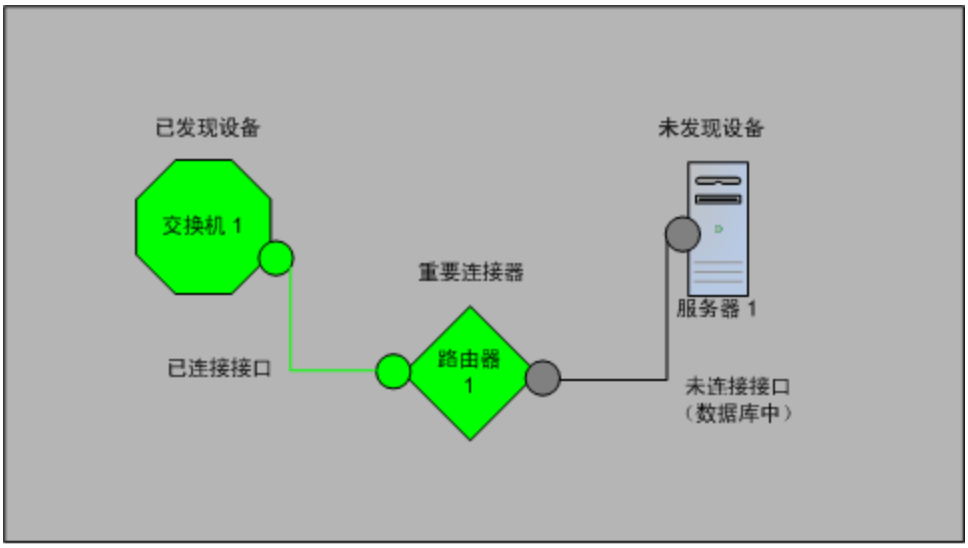
扩展监视

可以扩展监视以包括以下各项：

- 未连接的接口。默认情况下，NNMi 监视的唯一未连接的接口是那些具有 IP 地址且包含在**路由器**节点组中的未连接接口。

  > **备注:** NNMi 将未连接接口定义为未连接到由 NNMi 所发现另一个设备的接口，如下图中所示。

  未连接的接口示例



- 具有 IP 地址的接口(比如路由器接口)。
- 对不支持 SNMP 的设备的 ICMP 轮询。默认情况下，为**非 SNMP 设备**节点组启用 ICMP 轮询。

计划组

在配置监视设置之前，必须设置节点组和接口组。因此，配置节点组和接口组时，必须考虑轮询要求。理想情况下，配置节点组和接口组以便可以频繁监视重要设备，并以较低频率检查非关键设备(如果有的话)。

提示：为网络监视配置一组节点和接口组。配置一套不同的节点组，用于通过图实现网络可视化。

通过**配置 > 节点组**或**配置 > 接口组**工作区定义这些组，并且在默认情况下，它们也是用于筛选事件、节点、接口和地址视图的组。要另外创建一组节点或接口筛选以用于配置监视设置，请打开节点或接口组，并在**节点组**或**接口组**表单上选中**添加到视图筛选列表**复选框。单击**保存并关闭**。

可以在**监视配置**表单的**节点设置**和**接口设置**选项卡上设置节点组或接口组级别的轮询类型和轮询间隔。

确定要依据类似轮询需要对接口和/或设备进行分组的标准。以下是计划时要考虑的一些因素：

- 哪个网络区域包含这些设备？是否有时间约束？
- 是否要按设备类型区分轮询间隔或采集的数据？是否按接口类型？
- NNMi 是否提供了您可以使用的预配置组？

提示：可以按位置或某些其他标准同时为可能处于服务中断模式的对象创建组定义。例如，应用 IOS 升级时，可以将所有 Cisco 路由器置于“服务中断”模式。

接口组

根据标准确定要创建的接口组。请记住，将首先评估接口组(请参阅状况轮询的概念 (第 68 页))。接口组可能引用节点组成员资格，因此您可以先配置节点组再配置接口组来实现计划。

预配置的接口组

NNMi 已配置了几个有用的接口组供您使用。这些接口组包括：

- IFType 与 ISDN 连接相关的所有接口
- 用于语音连接的接口
- 用于点对点通信的接口
- 软件环回接口
- VLAN 接口
- 参与链路聚合协议的接口

HP 以后可能会添加更多默认组以简化配置任务。可以使用和修改现有组，或创建自己的组。

接口组有两种类型的限定条件：托管节点的节点组成员资格以及接口的 IFType 或其他属性。可以选择如下所示组合这些接口：

- 将节点组中节点上的所有接口都分组在一起而不考虑 IFType；请不要选择任何 IFType 或属性(比如名称、别名、描述、速度、索引、地址或其他 IFType 属性)。
- 对具有某些 IFType 或属性集的所有接口分组在一起而不考虑其所驻留的节点。
- 仅对驻留在特定节点组上的具有某 IFType 或属性的接口分组在一起。

节点组

在计划接口组之后，计划节点组。并非所有为监视创建的节点组都可用于筛选视图，因此可以单独配置它们。

预配置节点组

HP 提供默认的节点组集合以简化配置任务。这些节点组集合基于在发现过程中派生自系统对象 ID 的设备类别。默认提供的节点组包括：

- 路由器
- 网络基础结构设备(比如交换机或路由器。)
- Microsoft Windows 系统
- 没有 SNMP 团体字符串的设备
- 重要节点。这由原因引擎在内部使用，在连接器失败时为设备提供特殊处理。有关详细信息，请参阅 NNMi 帮助中的“作为预定义视图筛选的节点组”。
- 虚拟机

HP 以后可能会添加更多默认组以简化配置任务。可以使用和修改现有组，或创建自己的组。

可以使用以下节点属性来限定相关节点的定义：

- 节点上的 IP 地址
- 主机名通配符约定
- 诸如类别、供应商和系列的设备配置文件派生项
- MIB II sysName、sysContact 和 sysLocation

提示: 可以创建简单可重用的原子组并将它们组合为分层群集以供监视或查看。组定义可以重叠，比如“所有路由器”和“IP 地址以 .100 结尾的所有系统”。节点同样也可能适合于多个组。

在创建大量组集合进行配置和轻松查看(不在列表中包含许多可能从来不会使用的条目以避免过载)之间找到平衡。

与设备配置文件的交互

发现每个设备时，NNMi 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归类以应用监视设置。例如，可能要在某个轮询间隔轮询整个网络中的所有交换机而不考虑供应商。可以使用派生的设备类别(交换机)作为节点组的定义特征。系统对象 ID 映射到类别“交换机”的所有已发现设备都将接收到节点组的已配置设置。

提示: 如果 NNMi 正在对管理程序网络环境进行管理，则可能需要创建仅包含虚拟机 (VM) 的节点组。这些节点通过 `vmwareVM` 设备配置文件进行标识。偶尔还可以使用此节点组检查管理程序上不再托管的 VM。选择此节点组后，通过`Hosted On = null`进行筛选，标识这些 VM。还可以使用此节点组对与 VM 关联的 IP 地址启用故障轮询，这也是确保在已删除关联的管理程序的情况下，还继续监视 VM 的最佳实践。

计划轮询间隔

对于每个对象组，选择 NNMi 用于采集数据的轮询间隔。间隔可短至 1 分钟或长达几天以最好地匹配服务级别协议。

提示：较短的间隔有助于尽早了解网络问题；但是，在过短间隔中轮询太多对象可能导致状态轮询器中出现积压。要在环境的资源利用率和轮询间隔之间寻找最佳平衡。

备注: 原因引擎每 24 小时对每个节点执行一次状态轮询，并根据需要更新状态、结论和事件信息。这种状态轮询不会影响为设备配置的轮询间隔定时。

决定要采集的数据

状况轮询器服务使用轮询来收集网络中有关被监视设备的状况信息。可以使用 ICMP 和/或 SNMP 执行轮询。

ICMP (ping)

ICMP 地址监视使用 ping 请求来验证每个被管 IP 地址的可用性。

SNMP 轮询

SNMP 监视验证每个被监视 SNMP 代理是否正在响应 SNMP 查询。

- 高度优化的状况轮询器在每个间隔通过一个查询从每个被监视对象采集配置的 SNMP 信息。保存配置更改时，状况轮询器重新评估每个对象的组成员资格，并重新应用配置的间隔和要采集的数据集。
- SNMP 监视针对所有被监视接口和组件发出 SNMP 查询，从 MIB II 接口表、HostResources MIB 和特定于供应商的 MIB 请求当前值。某些值用于故障监视。如果已安装 NNM iSPI Performance for Metrics，则某些值用于性能测量。

Web 轮询

如果配置了 Web 代理(除 SNMP 代理之外)，NNMi 可以使用其他协议。例如，适用于 **VMware** 环境的 **SOAP** 协议。

SNMP 组件运行状况数据

可以启用或禁用全局级别的组件运行状况监视。组件运行状况故障监视遵循设备的故障轮询间隔设置。

在每次轮询中收集其他数据不影响执行轮询的时间。但是，为每个对象存储的其他数据可能增加状况轮询器的内存要求。

备注: 仅对 NNM iSPI Performance for Metrics 使用性能监视设置。组件运行状况性能监视遵循设备的性能轮询间隔设置。

提示: 监视配置的批量更改对状况轮询器正在进行的操作产生的干扰更小。

决定要发送到 NNMi 的 SNMP 陷阱

以下 SNMP 陷阱被接收而非等待下一轮询间隔时，NNMi 使用这些 SNMP 陷阱轮询设备。

- CempMemBufferNotify
- CiscoColdStart
- CiscoEnvMonFanNotification
- CiscoEnvMonFanStatusChangeNotif
- CiscoEnvMonRedundantSupplyNotification
- CiscoEnvMonSuppStatusChangeNotif
- CiscoEnvMonTemperatureNotification
- CiscoEnvMonTempStatusChangeNotif
- CiscoEnvMonVoltageNotification
- CiscoEnvMonVoltStatusChangeNotif
- CiscoFRUInserted
- CiscoFRURemoved
- CiscoLinkDown
- CiscoLinkUp
- CiscoModuleDown
- CiscoModuleUp
- CiscoModuleStatusChange
- CiscoRFProgressionNotif
- CiscoRFSwactNotif
- CiscoWarmStart
- HSRPStateChange
- IetfVrrpStateChange
- Rc2kTemperature
- RcAggLinkDown
- RcAggLinkUp
- RcChasFanDown
- RcChasFanUp
- RcChasPowerSupplyDown
- RcChasPowerSupplyUp
- Rcn2kTemperature
- RcnAggLinkDown
- RcnAggLinkUp
- RcnChasFanDown
- RcnChasFanUp
- RcnChasPowerSupplyDown
- RcnChasPowerSupplyUp
- RcnSmltIstLinkDown

- RcnSmltIstLinkUp
- RcSmltIstLinkUp
- RcVrrpStateChange
- SNMPColdStart
- SNMPLinkDown
- SNMPLinkUp
- SNMPWarmStart

要强制 NNMi 在接收这些陷阱时轮询某个设备，请将网络设备配置为将这些陷阱发送到 NNMi。

提示: 有关这些 SNMP 陷阱事件配置的详细信息，请从 NNMi 控制台导航到“配置”工作区并选择**事件 > SNMP 陷阱配置**。

另请参阅使用来自 SNMP 陷阱的发现提示 (第 60 页)。

配置状况轮询

本节提供配置提示，并提供一些配置示例。阅读本部分中的信息之后，请参阅 NNMi 帮助中的“配置监视行为”，以了解具体步骤。

备注: 在作出任何重大的配置更改之前保存现有配置的副本是一个好的做法。有关详细信息，请参阅最佳实践：保存现有配置 (第 26 页)。

配置接口组和节点组

在**配置**工作区中创建接口组和节点组。有关详细信息，请参阅 NNMi 帮助中的“创建节点组或接口组”。

示例

例如，要为 ProximiT 代理服务器配置节点组：

1. 打开**配置 > 节点组**，然后单击 ✱ **新建**。
2. 将该组命名为**代理服务器**，并选中**添加到视图筛选列表**。
3. 在**其他筛选**选项卡上，选择 **hostname** 属性，并选择等于 (=) 运算符。
4. 对于值，输入通配符，如 **`prox*.example.com`**。

   如果已经配置 ProximiT 设备的设备配置文件和设备类别，则可以使用**设备筛选**选项卡访问**设备类别**选择器，并且使组基于创建的代理服务器类别。
5. 在组定义上单击 **保存并关闭**。

备注: 您必须先配置节点组然后才能在接口组配置中引用它们。

配置接口监视

状况轮询器先分析接口组成员资格，再分析节点组成员资格。对于创建的每个接口组，以及要使用的任何预先存在的接口组，打开**监视配置**对话框和**接口设置**选项卡，以创建有关状况轮询器应当如何处理该组的一组自定义说明。说明将包括：

- 启用或禁用故障监视
- 设置故障轮询间隔
- 启用或禁用性能轮询(如果有 NNM iSPI Performance for Metrics)
- 设置性能轮询间隔(如果有 NNM iSPI Performance for Metrics)
- 设置性能管理阈值(如果有 NNM iSPI Performance for Metrics)
- 选择 NNMi 是否应当监视组中的未连接接口(或占用 IP 地址的未连接接口)

可以为每个接口组配置不同设置。请记住，状况轮询器按从最低到最高的排序编号来评估列表。

提示: 再次检查排序编号，记住适合于多个组的对象具有应用自排序编号最低的组的设置。

配置节点监视

如果对象不适合于任何配置的接口组，则状况轮询器评估该对象是否符合节点组中的成员资格。编号从最低到最高排序，设置应用于第一个匹配的节点组。

对于每个节点组，依次打开**监视配置**表单和**节点设置**选项卡。创建说明状况轮询器应当如何处理该组的一组自定义说明。说明可以包括：

- 启用或禁用故障监视
- 设置故障轮询间隔
- 启用或禁用性能轮询(如果有 NNM iSPI Performance for Metrics)
- 设置性能轮询间隔(如果有 NNM iSPI Performance for Metrics)
- 设置性能管理阈值(如果有 NNM iSPI Performance for Metrics)
- 选择 NNMi 是否应当监视组中的未连接接口(或占用 IP 地址的未连接接口)

可以为每个节点组配置不同设置。

提示: 再次检查排序编号，记住适合于多个组的对象具有应用自排序编号最低的组的设置。

验证默认设置

状况轮询器对于与定义的接口设置或节点设置不匹配的任何对象应用**默认设置**选项卡中的设置。查看此选项卡上的设置以确保它们在默认级别匹配环境。例如，您将很少轮询所有未连接的接口作为默认设置。

备注: 确保**保存并关闭**控制台的所有**监视配置**对话框，以实现更改。

评估状况轮询

本节列出评估监视设置的进度和成功与否的方法。

验证网络监视的配置

可以确定 NNMi 用于监视给定节点或接口的设置，并且可以随时启动节点的状态轮询。

要验证网络监视的配置，请使用以下检查：

- 接口或节点所属的组是否正确？ (第 78 页)
- 要应用哪些设置？ (第 78 页)
- 要采集哪些数据？ (第 78 页)

接口或节点所属的组是否正确？

通过在**配置**工作区中选择以下任何一项，可以验证哪些接口或节点属于组：

- 节点组
- 接口组

按照帮助中的说明显示组的成员。请记住，对象可以是多个组的成员，并且另一个组可能有更低的排序编号。

另外，通过打开对象(接口或节点)并单击**节点组**或**接口组**选项卡，可以查看对象所属的组的完整列表。此列表按组名称的字母顺序排列，不反映确定所应用设置的排序编号。

如果对象不是组的成员：

1. 在库存视图中检索节点的设备配置文件。
2. 在**配置 > 设备配置文件**下面查看设备配置文件的属性映射。
3. 查看节点组定义的属性要求。

如果不匹配，则可以调整在设备配置文件中派生的类别以强制使该类型的设备适合于节点组。可能需要执行**操作 > 配置轮询**以更新节点的属性，使其适合节点组。

要应用哪些设置？

要检查特定节点、接口或地址当前的监视配置，请在相应的库存视图中选择该对象，并选择**操作 > 监视设置**。NNMi 将显示当前监视设置。

检查**已启用故障轮询**和**故障轮询间隔**的值。如果这些值并不是所需值，请查看**节点组**或**接口组**的值，以查看应用了哪个排序的匹配组。

可能需要为对象选中**操作 > 通信设置**，以确保未禁用流量。

要采集哪些数据？

可以启动特定设备的状态轮询，以验证是否正在对该设备执行预期类型的轮询(SNMP、ICMP)。

> **备注:** 如果配置了 Web 代理(除 SNMP 代理之外)，NNMi 可以使用其他协议。例如，适用于 **VMware** 环境的 **SOAP** 协议。

选择节点，然后单击**操作 > 轮询 > 状态轮询**。

NNMi 执行设备的实时状态检查。输出显示正在执行的轮询的类型和结果。

如果轮询的类型不是预期类型，则检查该节点的监视设置和监视配置的逐个全局、接口或节点设置。

评估状态轮询的性能

通过使用状况轮询器运行状况检查中的信息来量化并评定状况轮询器服务的运行，从而评估环境中的状态轮询性能。

状况轮询器运行状况信息告诉您状态轮询器是否可以满足轮询请求。

状况轮询器是否一直在运行？

随时都可以在**系统信息**窗口的**状况轮询器**选项卡上检查有关状况轮询器服务的当前运行状况统计数据，如下表中所述。

状况轮询器运行状况信息

信息	描述
状态	状况轮询器服务的总体状态
轮询计数器	• 请求的采集 • 完成的采集 • 正在进行中的采集 • 采集请求延迟

在最后 1 分钟内执行跳过的时间	在配置的轮询间隔内未完成的计划的定期轮询数。非零值表示轮询引擎未持续运行或目标被轮询的速度快于它们的响应速度。
	• 监视对象：如果此值继续增加，则表示与目标之间的通信存在问题或 NNMi 已过载。
	• 要执行的操作：在 `nnm.?.0.log` 文件中查找以字符串 `com.hp.ov.nms.statepoller` 开头的类的消息，为跳过的轮询确定目标。
	  • 如果跳过的轮询针对同一目标，请更改配置以按较低频率轮询这些目标或增加这些目标的超时。
	  • 如果跳过的轮询针对不同目标，请检查 NNMi 系统性能，尤其是 ovjboss 的可用内存。

最后 1 分钟内的过时采集	过时采集是至少 10 分钟内未从轮询引擎接收到响应的采集。运行良好的系统应当不存在任何过时采集。
	• 监视对象：如果此值一直增加，则轮询引擎存在问题。
	• 要执行的操作：在 `nnm.?.0.log` 文件中查找以字符串 `com.hp.ov.nms.statepoller` 开头的类的消息，为过时采集确定目标。
	  • 如果过时采集针对单个目标，请在解决问题后再管理该目标。
	  • 如果过时采集针对不同目标，请检查 NNMi 系统和 NNMi 数据库的性

状况轮询器运行状况信息(续)

信息	描述
	能。停止并重新启动 NNMi。
轮询器结果队列长度	• 监视对象：大部分时间此值应接近 0。 • 要执行的操作：如果此队列非常大，则 ovjboss 可能将耗尽内存。
状况映射器队列持续时间	• 监视对象：大部分时间此值应接近 0。 • 要执行的操作：如果队列持续时间非常长，请检查 NNMi 系统和 NNMi 数据库的性能。
状况更新器队列持续时间	• 监视对象：大部分时间此值应接近 0。 • 要执行的操作：如果此队列非常大，请检查 NNMi 系统和 NNMi 数据库的性能。
状况更新器异常	监视对象：此值应为 0。

调整状况轮询

状况轮询的性能受以下关键变量影响：

- 要轮询的设备数/接口数
- 配置的轮询类型
- 轮询每个设备的频率

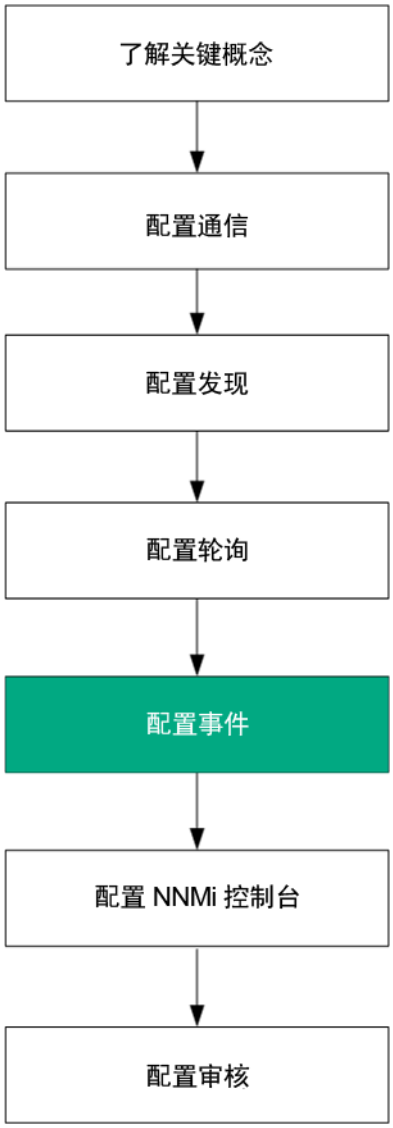
这些变量由网络管理需要驱动。如果状态轮询存在性能问题，请考虑以下配置：

- 由于各个节点的轮询设置是通过其在节点组和接口组中的成员资格控制的，因此请确保组包含具有类似轮询要求的节点或接口。
- 如果正在轮询未连接接口或占用 IP 地址的接口，请检查配置以确保只轮询必需的接口。在**节点设置**或**接口设置**表单上启用这些轮询(不作为**监视配置**表单上的全局设置)，以维护最明确的控制并选择要轮询的最小接口子集。
- 请记住，轮询未连接接口将监视所有未连接的接口。要仅监视具有 IP 地址的未连接接口，请启用对占用 IP 地址的接口的轮询。

与监视配置无关，状态轮询依赖于网络响应，并且可能受总体系统性能影响。尽管使用默认轮询间隔的状态轮询不引入很多网络负载，但如果服务器和被轮询设备之间的网络链路的性能较差，则状态轮询性能也较差。可以配置更长的超时和更少的重试次数以减少网络负载，但这些配置更改只在一定程度有效。及时轮询需要充分的网络性能和足够的系统资源(CPU、内存)。

启用或禁用组件运行状况监视对轮询的及时性没有影响。它只在计划时间内收集其他 MIB 对象。但是，禁用组件运行状况监视可能会减少可由状况轮询器使用的内存量。

NNMi 事件



HP Network Node Manager i Software (NNMi) 提供大量默认事件和关联，这些关联筛选传入 SNMP 陷阱以在 NNMi 控制台中提供可用的多个事件。本章提供的信息可帮助您通过配置 NNMi 事件来微调网络管理。本章是 NNMi 帮助信息的补充。有关 NNMi 事件的说明和如何配置事件的详细信息，请参阅 NNMi 帮助中的“配置事件”。

本章包含以下主题：

- 事件的概念 (第 82 页)
- 计划事件 (第 88 页)
- 配置事件 (第 89 页)
- 批处理加载事件配置 (第 92 页)
- 评估事件 (第 94 页)
- 调整事件 (第 94 页)

事件的概念

NNMi 从以下来源采集网络状态信息：

- NNMi 原因引擎分析网络的状况，并提供每个设备运行状况的持续读数。原因引擎会尽量广泛地评估并确定网络问题的根源。
- 来自网络设备的 SNMP 陷阱。NNMi 原因引擎在其分析期间使用此信息作为症状。
- 来自 HP ArcSight Logger 集成的 Syslog 消息。

NNMi 将此网络状态信息转换成提供对管理网络有用的信息的事件。NNMi 提供很多默认事件关联，从而减少了网络操作员要考虑的事件数。您可以自定义默认事件关联，创建新事件关联以满足您环境中的网络管理需要。

NNMi 控制台中的事件配置定义 NNMi 可以创建的事件类型。如果没有事件配置匹配接收的 SNMP 陷阱 syslog 消息，则丢弃该信息。如果源对象的管理模式在 NNMi 数据库中设置为“未管理”或“服务中断”，或者未对设备进行故障轮询监视，则 NNMi 始终丢弃该传入陷阱。

> **提示:** `nnmtrapconfig.ovpl -dumpBlockList` 输出有关当前事件配置的信息，包括由于不存在或禁用的事件配置而未传递到事件管道中的 SNMP 陷阱。

另外，NNMi 丢弃来自不在 NNMi 拓扑中的网络设备的 SNMP 陷阱。有关更改此默认行为的信息，请参阅 NNMi 帮助中的“处理未解析的传入陷阱”。

有关详细信息，请参阅：

- NNMi 帮助中的“关于事件管道”
- NNMi 帮助中的“NNMi 原因引擎和事件”
- 《HP Network Node Manager i-series Software Causal Analysis White Paper》，可从 **http://h20230.www2.hp.com/selfsolve/manuals**

事件生命周期

下表描述了事件的生命周期阶段。

NNMi 事件生命周期

生命周期状况	描述	状况设置者	事件使用者
无	NNMi 事件管道从所有源接收输入，并根据需要创建事件。	不适用	• NNMi
已减弱	事件在保留位置等待与另一个事件关联。此等待时段的目的是减少事件查看器中的事件。 减弱间隔可随事件类型而异。有关详细信息，请参阅事件抑制、强化和减弱 (第 87 页)。	NNMi	• NNMi
已注册	事件在事件视图中可见。	NNMi	• 用户 • 生命周期转换操

NNMi 事件生命周期(续)

生命周期状况	描述	状况设置者	事件使用者
	事件被转发到任何配置的目标(northbound 或全局管理器)。	用户还可以在事件视图中设置此状况。	作 • 转发事件的集成
进行中	已将事件分配给将调查问题的某用户。 网络管理员定义此状况的特定含义。	用户	• 用户 • 生命周期转换操作 • 转发事件的集成
已完成	事件指示的问题调查已完成，解决方案就绪。 事件识别的问题 网络管理员定义此状况的特定含义。	用户	• 用户 • 生命周期转换操作 • 转发事件的集成
已关闭	表示该 NNMi 确定此事件报告的问题已解决。例如，从设备删除接口时，自动关闭与该接口相关的所有事件。	用户或 NNMi	• 用户 • 生命周期转换操作 • 转发事件的集成

陷阱和事件转发

下表汇总了将陷阱和事件从 NNMi 管理服务器转发到另一个目标的途径。表后的文字比较了 NNMi SNMP 陷阱转发机制与 NNMi Northbound 接口 SNMP 陷阱转发机制。

转发陷阱和 NNMi 事件的支持方式

	NNMi 陷阱转发	NNMi Northbound 接口陷阱转发	全局网络管理陷阱转发
转发的内容	• 来自网络设备的 SNMP 陷阱 • 来自 HP ArcSight Logger 的 Syslog 消息	• 来自网络设备的 SNMP 陷阱 • NNMi 管理事件 • 来自 HP ArcSight Logger 的 Syslog 消息	• 来自网络设备的 SNMP 陷阱 • 来自 HP ArcSight Logger 的 Syslog 消息
转发格式	SNMPv1、v2c 或 v3 陷阱(按原样) (SNMPv3 陷阱可以转换成 SNMPv2c 陷阱)	从 NNMi 事件创建的 SNMPv2c 陷阱	NNMi 事件
添加的信	多数情况下，NNMi 添加	NNMi 添加 varbind 来识别	转发事件中保留由区域

转发陷阱和 NNMi 事件的支持方式(续)

	NNMi 陷阱转发	**NNMi Northbound 接口陷阱转发**	**全局网络管理陷阱转发**
息	varbind 来识别原始源对象。 NNMi 不会修改 SNMPv1 陷阱。	原始源对象。	管理器进程添加到事件的任何信息。
配置位置	**配置**工作区中的**陷阱转发配置**	**集成模块配置**工作区中的 **HPOM**、**Northbound 接口**或 **Netcool**	**SNMP 陷阱配置**表单或 syslog 配置上的**转发到全局管理器**选项卡。
备注		NNMi 提供 NNMi Northbound 接口上生成的几个集成。 另请参阅《HP Network Node Manager i Software—IBM Tivoli Netcool/OMNIbus Integration Guide》和《HP Network Node Manager i Software—HP Operations Manager Integration Guide》。 。	转发应在全局管理器事件视图中可见的远程事件。转发的事件参与全局管理器上的关联。
详细信息	NNMi 帮助中的“配置陷阱转发”	请参阅《NNMi 部署参考》中的“NNMi Northbound 接口”一章。	• NNMi 帮助中的“对 SNMP 陷阱事件配置‘转发到全局管理器’设置”

比较：将第三方 SNMP 陷阱转发到其他应用程序

如果要将 NNMi 从被管设备接收的 SNMP 陷阱转发到另一个应用程序，可使用以下任一方式：

- 使用 NNMi SNMP 陷阱转发机制。有关如何配置 NNMi SNMP 陷阱转发的信息，请参阅 NNMi 帮助中的“配置陷阱转发”。
- 使用 NNMi Northbound 接口 SNMP 陷阱转发机制。有关配置 NNMi Northbound Interface 以转发接收的 SNMP 陷阱的信息，请参阅《NNMi Integration Reference》中的“NNMi Northbound Interface”一章。

接收应用程序识别陷阱的方式随 SNMP 陷阱转发机制而不同：

- Windows(所有)和无原始陷阱转发的 Linux

  此描述应用于默认和 SNMPv3 到 SNMPv2c 转换的转发选项。

Windows NNMi 管理服务器上的 NNMi SNMP 陷阱转发机制在将每个 SNMP 陷阱转发到陷阱目标之前先扩展它。陷阱看似起源于 NNMi 管理服务器。(此信息还应用于**陷阱转发目标**表单上未选择原始陷阱转发选项的 Linux NNMi 管理服务器。)

要确保在陷阱发送设备和接收应用程序中的事件之间存在正确关联，必须对这些陷阱的规则进行自定义以添加 varbind。解释来自 originIPAddress (.1.3.6.1.4.1.11.2.17.2.19.1.1.3) varbind 的值。originIPAddress 值由 originIPAddressType (.1.3.6.1.4.1.11.2.17.2.19.1.1.2) varbind 的值确定，属于通用类型为 InetAddress(InetAddressIPv4 或 InetAddressIPv6)的字节字符串。规则必须读取 originIPAddressType varbind，才能确定 originIPAddress varbind 中 Internet 地址(ipv4(1) 或 ipv6(2))值的类型。规则还可能需要将 originIPAddress 值转换成显示字符串。

有关 NNMi 添加到所转发陷阱的 varbind 的详细信息，请参阅 NNMi 帮助中的“NNMi 提供的陷阱 Varbind”、RFC 2851 和以下文件：

- Windows：`%NNM_SNMP_MIBS\Vendor\Hewlett-Packard\hp-nnmi.mib`
- Linux：`$NNM_SNMP_MIBS/Vendor/Hewlett-Packard/hp-nnmi.mib`

- 带原始陷阱转发的 Linux

  Linux NNMi 管理服务器可以使用与 NNMi 接收陷阱相同的格式转发陷阱。每个陷阱看上去像是由被管设备直接发送到陷阱目标的，因此接收应用程序中配置的现有陷阱处理应有效而无需修改。

  有关详细信息，请参阅 NNMi 帮助中的“陷阱转发目标表单”中的原始陷阱转发选项。

- NNMi Northbound 接口(所有操作系统)

  NNMi Northbound 接口在将每个 SNMP 陷阱转发到陷阱目标之前先扩展它。陷阱看似起源于 NNMi 管理服务器。要确保在陷阱发送设备和接收应用程序中的事件之间存在正确关联，必须对这些陷阱的规则进行自定义以添加 varbind。IncidentNodeHostname (1.3.6.1.4.1.11.2.17.19.2.2.21) 和 IncidentNodeMgmtAddr (1.3.6.1.4.1.11.2.17.19.2.2.24) varbind 识别原始源对象。

MIB

NNMi 要求将以下管理信息库 (MIB) 文件加载到 NNMi 数据库中：

- 在 MIB 表达式中用于自定义轮询器功能和/或折线图的所有 MIB 变量
- NNMi 监视运行状况(例如风扇或电源)的传感器
- (NNM iSPI Performance for Metrics) 阈值监视中使用的所有 MIB 变量

NNMi 要求将以下管理信息库 (MIB) 文件或这些 MIB 文件中定义的陷阱加载到 NNMi 数据库中：

- 所有要转发到 northbound 目标的 SNMP 陷阱
- (NNM iSPI NET) 从陷阱分析报告访问的所有 MIB 变量

提示: NNMi 提供一个列出当前不受支持的 MIB 的 `README.txt` 文件。`README.txt` 文件位于以下目录中：

- Windows：`%NnmInstallDir%\misc\nnm\snmp-mibs`
- Linux：`$NnmInstallDir/misc/nnm/snmp-mibs`

自定义事件属性

NNMi 使用自定义事件属性 (CIA) 将其他信息附加到事件。

- 对于 SNMP 陷阱事件，NNMi 将原始陷阱 varbind 存储为事件的 CIA。
- 对于管理事件，NNMi 将有关信息(例如 com.hp.ov.nms.apa.symptom)添加为事件的 CIA。

可以用事件 CIA 缩小配置范围，如事件生命周期转换操作、抑制、取消重复和强化。还可以用 CIA 缩减事件视图或表单的“操作”菜单上可用的菜单项。

要确定 NNMi 为任何给定事件添加哪些 CIA，请从事件视图打开示例事件，在“自定义属性”选项卡上查看信息。

添加到已关闭的管理事件的 CIA

NNMi 原因引擎确定导致管理事件不再适用的条件时，NNMi 会将该事件的生命周期状况设置为“已关闭”并将下表中列出的 CIA 添加到该事件。NNMi 控制台用户可以在**事件**表单的**关联备注**字段中查看此信息。生命周期转换操作可直接使用 CIA 的值。

自定义已关闭事件的事件属性

名称	描述
cia.reasonClosed	NNMi 取消或关闭事件的原因。该原因也是结论名称，例如 NodeUp 或 InterfaceUp。 如果未设置此字段，则 NNMi 控制台用户已关闭事件。 要确定 cia.reasonClosed CIA 的 NNMi 预期值，请参阅 NNMi 帮助中的“NNMi 如何关闭事件”。
cia.incidentDurationMs	由 NNMi 测得，从状态关闭到恢复的中断持续时间，以毫秒为单位。该值是 cia.timeIncidentDetectedMs 和 cia.timeIncidentResolvedMs CIA 的差。和比较关闭与恢复事件的时间戳相比，这是更准确的测量方式。
cia.timeIncidentDetectedMs	NNMi 原因引擎首先检测到问题的时间戳，以毫秒为单位。
cia.timeIncidentResolvedMs	NNMi 原因引擎检测到问题已解决的时间戳，以毫秒为单位。

NNMi 会将上表中列出的 CIA 添加到最主要和次要的根源事件。例如，NodeDown 事件可以有 InterfaceDown 和 AddressDown 事件作为次要的根源。NNMi 关闭 NodeDown 事件时，NNMi 也会关闭次要事件，并将 CIA 和每个事件上下文的值添加到次要事件。

NNMi 不会将上表中列出的 CIA 添加到以下默认管理事件类型：

- NNMi 控制台用户手动关闭的事件
- NNMi 为响应从 NNMi 数据库删除的对象而关闭的事件
- IslandGroupDown 事件
- NnmClusterFailover、NnmClusterLostStandby、NnmClusterStartup 和 NnmClusterTransfer 事件
- 以下系列中的事件：
  - 关联
  - 许可证
  - NNMi 运行状况
  - 陷阱分析

事件减少

NNMi 提供以下可自定义的关联，用于减少网络操作员在 NNMi 控制台中看到的事件数：

- 成对关联 - 一个事件取消另一个事件。
- 取消重复关联 - 指定时间段中收到事件的多个副本时，将这些副本关联在取消重复事件下。为每个新接收的重复事件重新启动该时间段。这样，NNMi 将关联重复事件，直到关联时间段的整个持续时间内未收到任何重复。
- 速率关联 - 指定时间段内接收到某事件的指定数量的副本时，将这些副本关联在速率事件下。接收到指定数量的事件时，NNMi 就生成速率事件，而不管时间段内还剩余多少时间。

事件抑制、强化和减弱

NNMi 提供了用于最大程度地从事件获益的丰富功能集。对每个事件类型，可以用以下事件配置选项专门定义何时需要某事件：

- 抑制 - 事件与抑制配置匹配时，该事件不会显示在 NNMi 控制台事件视图中。对于那些对某些节点(如路由器和交换机)重要但对其他节点不重要的事件(例如 SNMPLinkDown 陷阱)，事件抑制很有用。
- 强化 - 事件与强化配置匹配时，NNMi 按照事件内容更改一个或多个事件值(如严重度或消息)。事件强化对于处理承载陷阱 varbind(负载)中独特信息的陷阱(如 RMONFallingAlarm)很有用。
- 减弱 - 事件与减弱配置匹配时，NNMi 在减弱间隔的持续时间内延迟该事件的活动。事件减弱为 NNMi 原因引擎对事件执行根源分析提供了时间，这对于在 NNMi 控制台中提供较少、较有意义的事件很有用。

对于每个事件类型，NNMi 都为抑制、强化和减弱提供以下配置级别：

- 接口组设置 - 指定源对象是 NNMi 接口组的成员时的事件行为。可为每个接口组指定不同的行为。
- 节点组设置 - 指定源对象是 NNMi 节点组成员时的事件行为。可为每个节点组指定不同的行为。
- 默认设置 - 指定默认的事件行为。

对于每个事件配置区域(抑制、强化和减弱)，NNMi 都使用以下过程确定特定事件的行为：

1. 检查接口组设置：
   - 如果源对象与任何接口组设置匹配，则执行排序编号最低的匹配中定义的行为，并停止查找匹配。
   - 如果源对象不与任何接口组设置匹配，则继续执行步骤 2。
2. 检查节点组设置：
   - 如果源对象与任何节点组设置匹配，则执行排序编号最低的匹配中定义的行为，并停止查找匹配。
   - 如果源对象不与任何节点组设置匹配，则继续执行步骤 3。
3. 执行默认设置中定义的行为(如果有)。

生命周期转换操作

生命周期转换操作是一个管理员提供的命令，在事件生命周期状况更改为与操作配置匹配时会运行此命令。对于一种事件类型，事件操作配置是特定于一个生命周期状况的。该操作配置确定当此事件类型转换为指定生命周期状况时要运行的命令。该命令可包括将事件信息传递到操作代码的参数。

操作代码可以是在 NNMi 管理服务器上正确运行的任何 Jython 文件、脚本或可执行文件。操作代码可特定于一个事件类型，也可以处理多个事件类型。例如，您可创建一个操作代码，用于在 NNMi 创建 ConnectionDown、NodeDown 或 NodeOrConnectionDown 事件时呼叫网络操作员。您将会配置三个事件操作，这三个事件类型的已注册生命周期状况各用一个。

同样，操作代码可特定于一个生命周期状况更改，也可以响应几个生命周期状况更改。例如，您可创建一个操作代码，用于在 NNMi 创建 InterfaceDown 事件时生成故障单，并在取消 InterfaceDown 事件时关闭故障单。您将为 InterfaceDown 事件配置两个事件操作，一个用于“已注册”状况，一个用于“已关闭”状况。

每个操作配置都可以包括一个基于 CIA 的负载筛选，用于限制操作何时运行。对于其他筛选，可使用事件扩展将 CIA 添加到事件。NNMi 从事件源确定该属性的值。例如，如果已将自定义属性添加到某些节点，则可将此信息添加到事件以作为 CIA，然后将此属性值用作事件操作的负载筛选依据。

计划事件

作出关于以下方面的决策：

- NNMi 应处理哪些设备陷阱？ (第 88 页)
- NNMi 应显示哪些事件？ (第 88 页)
- NNMi 应如何响应事件？ (第 88 页)
- NNMi 应将陷阱转发到另一个事件接收器吗？ (第 89 页)

NNMi 应处理哪些设备陷阱？

确定网络中所需的设备陷阱，并计划每个陷阱的事件配置。NNMi 处理陷阱时无需将 MIB 加载到 NNMi 中。如果 MIB 包含 TRAP-TYPE 或 NOTIFICATION-TYPE 宏，则可为 MIB 中定义的陷阱创建主干事件配置。

决定是否要查看来自不在 NNMi 拓扑中的设备的陷阱。

NNMi 应显示哪些事件？

将默认事件集作为起点是个好选择。您可以逐渐扩展和减少事件集。

通过取消重复、速率配置和成对关联来计划可减少的事件。

有关详细信息，请参阅 NNMi 管理员帮助。

NNMi 应如何响应事件？

发生特定事件时，NNMi 应采取哪些操作(例如，将电子邮件消息发送给网络操作员)？每个操作应在哪个生命周期状况下运行？

有关详细信息，请参阅 NNMi 管理员帮助。

NNMi 应将陷阱转发到另一个事件接收器吗？

如果您的环境包括第三方陷阱整合器，请决定是否将 NNMi SNMP 陷阱转发机制与 NNMi Northbound 接口 SNMP 陷阱转发机制结合使用。

如果选择 NNMi Northbound 接口 SNMP 陷阱转发机制，则对于 NNMi 要转发到事件接收器的所有陷阱都要加载 MIB。

配置事件

本部分列出配置提示，并提供一些配置示例。阅读本部分中的信息之后，请参阅 NNMi 帮助中的“配置事件”，以了解具体步骤。

> **备注:** 在作出任何重大的配置更改之前保存现有配置的副本是一个好的做法。有关详细信息，请参阅最佳实践：保存现有配置 (第 26 页)。

- 配置您计划的事件类型。如果可能，从来自 MIB 中定义的陷阱的主干事件配置开始。
- 加载陷阱转发必需的任何 MIB。
- 验证是否已将设备配置为将陷阱发送到 NNMi 管理服务器。

配置事件抑制、强化和减弱

配置事件抑制、强化和减弱时，注意以下事项：

- 对于每个接口组、节点组或默认设置，都可以指定进一步优化配置何时适用的负载筛选。
- 在事件配置表单的**接口设置**选项卡上配置接口组设置。
- 在事件配置表单的**节点设置**选项卡上配置节点组设置。
- 在事件配置表单的**抑制**、**强化**和**减弱**选项卡上配置默认设置。

配置生命周期转换操作

配置生命周期转换操作时，请注意以下事项：

- 默认情况下，NNMi 在以下位置运行操作：
  - Windows：`%NnmDataDir%\shared\nnm\actions`
  - Linux：`$NnmDataDir/shared/nnm/actions`

  如果操作不在这个位置，则在**生命周期转换操作**表单的**命令**字段中指定操作的绝对路径。

  > **备注:** Jython 文件必须放置在 `actions` 目录中。

- 每次对操作配置进行更改时，NNMi 都重读 actions 目录中的 Jython 文件，并将它们加载到 NNMi 中。

- 属于一种事件类型的操作可作为一个组。
- 有关可传递到操作的 NNMi 信息的信息，请参阅 NNMi 帮助中的“配置事件操作的有效参数”。

配置陷阱日志

NNMi 提供将所有传入的 SNMP 陷阱记录到日志文件(文本文件或 CSV 文件)的功能。陷阱记录到以下位置：

- Windows：`%NnmDataDir%\nnm\log`
- Linux：`$NnmDataDir/nnm/log`

可以使用 `nnmtrapconfig.ovpl` 脚本配置陷阱日志文件。可用的格式选项如下：

- `CSV`(默认)- 以 CSV 格式记录陷阱 (`trap.csv`)。
- `TXT` - 以 TXT 格式记录陷阱 (`trap.log`)。
- `BOTH` - 以 CSV 和 TXT 格式记录陷阱(2 个日志文件)。
- `OFF` - 不记录任何陷阱。

例如，要指定以 BOTH 模式记录陷阱，可以使用以下命令：

`nnmtrapconfig.ovpl -setProp trapLoggingMode BOTH -persist`

请注意，**`-persist`** 参数会导致所有陷阱服务器属性保持生效，即使是在重新启动陷阱服务之后。如果不使用 **`-persist`** 参数，则只有在停止服务后，所有陷阱服务器属性才会生效。

陷阱写入轮询文件中。日志文件大小达到定义的最大限制(使用 `nnmtrapconfig.ovpl` 脚本定义)后，该文件就将重命名为 `trap.<格式>.old`。替换任何现有的文件。

有关详细信息，请参阅 `nnmtrapconfig.ovpl` 参考页或 Linux 联机帮助页。另请参阅 NNMi 帮助中的“配置陷阱日志记录”。

配置事件日志记录

您可以配置事件日志记录，以便将传入的事件信息写入到 `incident.log` 文件。当您想要跟踪和存档事件历史记录时，此功能非常有用。

通过导航到**配置**工作区的**事件配置**区域中的**事件日志记录配置**选项卡并配置相应设置，从而配置并启用事件日志记录。有关详细信息，请参阅 NNMi 帮助。

配置陷阱服务器属性

您可以通过使用 `nnmtrapconfig.ovpl` 脚本来设置陷阱服务器属性 (`nnmtrapserver.properties`)。

> **备注:** 尽管 `nnmtrapserver.properties` 文件已存在，但不要直接编辑此文件；请使用 `nnmtrapconfig.ovpl` 脚本修改此文件。

下表显示陷阱服务器属性的默认值。

陷阱服务器属性和默认值

陷阱服务器属性	默认值
com.hp.ov.nms.trapd.udpPort	162
com.hp.ov.nms.trapd.rmiPort	1097
com.hp.ov.nms.trapd.trapInterface	所有接口
com.hp.ov.nms.trapd.recvSocketBufSize	2048 KB
com.hp.ov.nms.trapd.pipeline.qSize	50000 个陷阱
com.hp.ov.nms.trapd.connectToWinSNMP	false
com.hp.ov.nms.trapd.blocking	true
com.hp.ov.nms.trapd.blockTrapRate	50 个陷阱/秒
com.hp.nms.trapd.unblockTrapRate	50 个陷阱/秒
com.hp.ov.nms.trapd.overallBlockTrapRate	150 个陷阱/秒
com.hp.nms.trapd.overallUnblockTrapRate	150 个陷阱/秒
com.hp.ov.nms.trapd.analysis.minTrapCount	100 个陷阱
com.hp.ov.nms.trapd.analysis.numSources	10 个源
com.hp.ov.nms.trapd.analysis.windowSize	300 秒 (5 分钟)
com.hp.nms.trapd.updateSourcesPeriod	30 秒
com.hp.nms.trapd.notifySourcesPeriod	300 秒
com.hp.ov.nms.trapd.hosted.object.trapstorm.enabled	false
com.hp.ov.nms.trapd.hosted.object.trapstorm.threshold	10 个陷阱/秒
com.hp.ov.nms.trapd.database.fileSize	100 MB
com.hp.ov.nms.trapd.database.fileCount	5 个文件
com.hp.ov.nms.trapd.database.qSize	300000 个陷阱
com.hp.ov.nms.trapd.discohint.cacheSize	5000 个条目
com.hp.ov.nms.trapd.discohint.cacheEntryTimeout	3600 毫秒

有关详细信息，请参阅 `nnmtrapconfig.ovpl` 参考页或 Linux 联机帮助页。

配置分配事件时用户名排序顺序所用的语言环境

NNMi 管理员可以指定 NNMi 管理服务器在分配事件时确定用户名排序顺序所用的语言环境。

备注: 配置的排序顺序语言环境仅应用于**分配事件**对话框。

确定字母顺序时，NNMi 将使用用户的显示名称而非实际登录名，并且不会分别对大小写字母排序。

备注: NNMi 仅使用 sortLocale 中配置的语言环境确定排序顺序。forceClientLocale 属性中指定的浏览器语言环境不影响排序顺序。有关详细信息，请参阅覆盖浏览器语言环境设置 (第 210 页)

备注: 在高可用性 (HA) 下进行更改时，需要更新的 server.properties 文件位于以下位置：<共享磁盘>/NNM/dataDir/nmsas/NNM/server.properties。

要配置分配事件时用于对列出的用户名进行排序的语言环境，请按如下所示编辑 server.properties 文件：

1. 打开以下文件：
   - Windows：%NnmDataDir%\nmsas\NNM\server.properties
   - Linux：$NnmDataDir/nmsas/NNM/server.properties
2. 取消注释 server.properties 文件中的以下行：

   #nmsas.server.sortLocale = en_US
3. 将默认值更改为 NNMi 管理服务器的正确语言环境。例如，要将语言环境更改为俄语，请使用以下条目：

   nmsas.server.sortLocale = ru_RU
4. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 ovstop 命令。
   b. 在 NNMi 管理服务器上运行 ovstart 命令。

批处理加载事件配置

将以下两个脚本与事件配置的批处理加载结合使用：nnmincidentcfgdump.ovpl 和 nnmincidentcfgload.ovpl。

使用 nnmincidentcfgdump.ovpl 生成事件配置文件

NNMi nnmincidentcfgdump.ovpl 脚本向您提供一种创建或更新事件配置以便随后使用 nnmincidentcfgload.ovpl 脚本加载到 NNMi 数据库的方法。以非 xml 格式生成文件。

您可以使用以下目录中提供的格式描述编辑文件：

Windows：%NnmInstallDir%/examples/nnm/incidentcfg

Linux：/opt/OV/examples/nnm/incidentcfg

要为事件配置生成文件，请使用以下示例语法：

```
nnmincidentcfgdump.ovpl -dump <文件名> -u <NNMi 管理员用户名>
-p <NNMi 管理员密码>
```

有关详细信息，请参阅 nnmincidentcfgdump.ovpl 参考页或 Linux 联机帮助页。

备注: 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。

使用 nnmincidentcfgload.ovpl 加载事件配置

NNMi nnmincidentcfgload.ovpl 脚本向您提供一种将事件配置从格式化的配置文件加载到 NNMi 数据库的方法。

提示: 使用 nnmincidentcfgdump.ovpl 脚本以非 xml 格式创建现有事件配置的配置文件。然后，您可以在将此文件加载到 NNMi 数据库之前，根据需要对其进行编辑。

请参阅以下目录了解所需的格式：

Windows：%NnmInstallDir%\examples\nnm\incidentcfg

Linux：/opt/OV/examples/nnm/incidentcfg

要在将事件配置文件加载到 NNMi 数据库之前对其进行验证，请使用以下示例语法：

```
nnmincidentcfgload.ovpl -validate <字段名> -u <NNMi 管理员用户名>
-p <NNMi 管理员密码>
```

要加载事件配置，请使用以下示例语法：

```
nnmincidentcfgload.ovpl -load <字段名> -u <NNMi 管理员用户名>
-p <NNMi 管理员密码>
```

注意以下事项：

- NNMi 更新具有匹配的名称或其他匹配的键标识符的所有配置。

警告: NNMi 还覆盖与这些配置(例如，事件系列)关联的任何代码的值。

- NNMi 添加键标识符不存在于 NNMi 数据库中的所有事件配置。
- NNMi 不更改键标识符与所导出文件中的任何标识符都不匹配的现有事件配置。
- NNMi 解析配置文件中未提供的全局唯一对象标识符 (UUID)。
- 如果 NNMi 无法解析 UUID，则会创建 UUID。

备注: 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。

有关详细信息，请参阅 nnmincidentcfgload.ovpl 参考页或 Linux 联机帮助页。

评估事件

本部分列出了评估事件配置的途径。

- 验证 NNMi 是否已接收来自网络中所有被管设备的陷阱。

  如果 NNMi 未接收陷阱，则验证 NNMi 管理服务器上防火墙的配置。

  > **备注:** 某个防病毒软件包括独立于系统防火墙配置的防火墙。

- 验证最重要的陷阱是否已转换为事件。
- 验证事件操作是否基于正确的生命周期状况转换而运行。
- 验证 NNMi 是否按预期处理事件。

  操作 > 事件配置报告菜单包含用于根据该事件类型的当前配置来测试现有事件的若干选项。使用这些菜单项之一不会改变当前 NNMi 控制台中的事件。

调整事件

减少 NNMi 控制台事件视图中的事件数。使用以下任一方法：

- 对 NNMi 控制台中不需要的任何事件类型禁用事件配置。
- 将您不需要监视的网络对象的管理模式设置为“未管理”或“服务中断”。NNMi 丢弃来自这些节点及其接口的多数传入陷阱。
- 将 NNMi 设置为不监视某些网络对象。NNMi 丢弃来自不受监视的源对象的多数传入陷阱。
- 识别传入事件的其他标准或它们之间的关系。当这些标准或关系出现时，NNMi 识别传入管理事件或 SNMP 陷阱的标准或模式并将相关事件嵌套为关联子级事件，以此来修改事件流。

启用和配置未定义陷阱的事件

NNMi 默认情况下静默丢弃未定义的陷阱。从 NNMi 9.01 开始，NNMi 可标识可能被丢弃的任何未定义的 SNMP 陷阱。

> **备注:** 如果您有权在 NNMi 管理服务器上使用 NNM iSPI NET 或 NNMi Premium，则用接收的陷阱总数 (按 OID) 报告研究丢弃的 SNMP 陷阱。有关详细信息，请参阅 NNMi 帮助中的“分析陷阱信息 (NNM iSPI NET)”。

如果您无权在 NNMi 管理服务器上使用 NNM iSPI NET 或 NNMi Premium，且想将缺失的陷阱作为事件查看，请如下配置未定义的 SNMP 陷阱事件：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS%\nms-jboss.properties`
   - Linux：`$NNM_PROPS/nms-jboss.properties`
2. 在文件中查找类似以下行的部分：

   ```
   #!com.hp.nnm.events.allowUndefinedTraps=false
   ```

   对该行进行如下更改：

```
com.hp.nnm.events.allowUndefinedTraps=true
```

3. 可选。用 nms-jboss.properties 文件中说明的值指定事件严重度。在文件中查找类似以下行的部分：

   ```
   #!com.hp.nnm.events.undefinedTrapsSeverity=NORMAL
   ```

   如下更改此行，用定义的严重度值代替您指定的严重度。

   ```
   com.hp.nnm.events.undefinedTrapsSeverity=YourSpecifiedSeverity
   ```

4. 可选。用 nms-jboss.properties 文件中说明的值指定事件的性质。在文件中查找类似以下的部分：

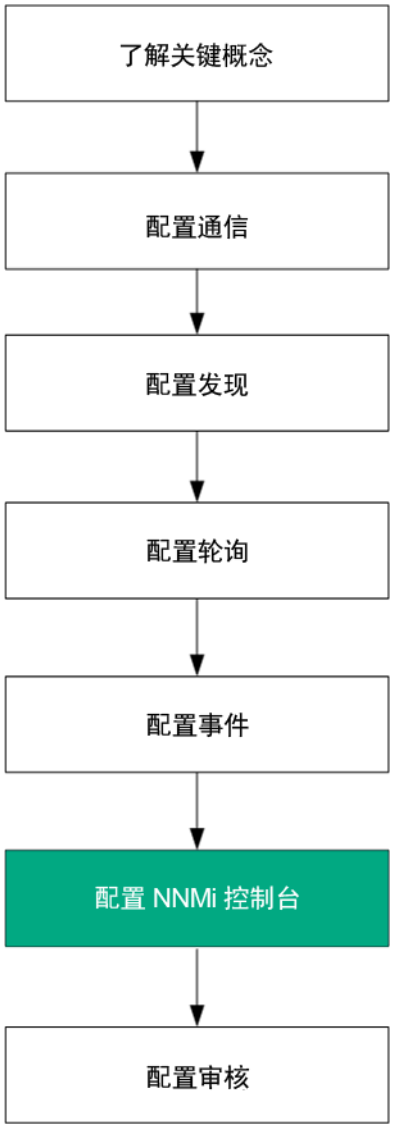
   ```
   #!com.hp.nnm.events.undefinedTrapsNature=INFO
   ```

   如下更改此行，用定义的性质值代替您指定的性质。

   ```
   com.hp.nnm.events.undefinedTrapsNature=YourSpecifiedNature
   ```

5. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 ovstop 命令。
   b. 在 NNMi 管理服务器上运行 ovstart 命令。
6. 查看未定义陷阱的列表，为您要控制的那些陷阱创建新事件配置。如果希望 NNMi 显示新事件，则启用它；如果希望 NNMi 忽略新事件，则禁用它。有关详细信息，请参阅 NNMi 帮助中的“配置 SNMP 陷阱事件”。

NNMi 控制台



通过本章中的信息了解如何使用 NNMi 控制台将 NNMi 配置为以特定方式工作。

本章包含以下主题：

- 减少在网络概述图中显示的最大节点数 (第 97 页)
- 减少节点组图上显示的节点数 (第 97 页)
- 在分析窗格中配置量表 (第 98 页)
- 配置图标签缩放大小和边框 (第 100 页)
- 配置 Loom 和 Wheel 图的自动折叠阈值 (第 101 页)
- 自定义设备配置文件图标 (第 102 页)
- 配置表视图的刷新率 (第 102 页)

减少在网络概述图中显示的最大节点数

网络概述图所显示的图包含在第 3 层网络中频繁连接的最多 250 个节点。如果此图包含过多节点，在移动节点时此图可能响应缓慢，或者变得太复杂而失去查看价值。

可以通过编辑“用户界面配置”表单上的**默认图设置**选项卡上的“最大节点显示数”属性，增加或减少**网络概述**图中显示的最大节点数。

也可以执行以下示例中的步骤，增加或减少**网络概述**图中显示的最大节点数。

例如，要将**网络概述**图中显示的最大节点数从 250 更改为 100，请执行以下步骤：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS%\nms-ui.properties`
   - Linux：`$NNM_PROPS/nms-ui.properties`
2. 查找类似以下行的文本：

   `#!com.hp.nnm.ui.networkOverviewMaxNodes = 250`

   对此行进行如下更改：

   `com.hp.nnm.ui.networkOverviewMaxNodes = 100`

   > **备注:** 确保删除位于行开头的 **#!** 字符。

3. 保存更改。

减少节点组图上显示的节点数

如果将节点组图配置为包含几百个节点，则显示此节点组的图可能显示很多小节点图标，而不是显示希望看到的详细节点图标。要查看此图的更多细节，必须使用缩放功能。

> **备注:** 显示图时使用缩放功能可能使 NNMi 控制台性能下降。

要限制显示的节点数和/或显示的端点数，请执行以下步骤：

1. 在 NNMi 控制台中，单击**配置**。
2. 单击**用户界面配置**。
3. 选择**默认图设置**选项卡。
4. 修改**最大节点显示数**字段中显示的值。
5. 修改**最大端点显示数**字段中显示的值。
6. 单击**保存并关闭**。

有关详细信息，请参阅 NNMi 帮助中的“定义默认图设置”。

在分析窗格中配置量表

分析窗格中的“量表”选项卡显示实时 SNMP 量表，这些量表显示状况轮询器和自定义轮询器的 SNMP 数据。这些量表显示节点、接口、自定义节点采集的数据以及 CPU、Memory、Buffers 或 Backplane 类型的节点组件的数据。

您可以通过编辑以下属性文件来配置量表：

- Windows：`%NNM_PROPS%\nms-ui.properties`
- Linux：`$NNM_PROPS/nms-ui.properties`

对于要设置的每个属性(如果存在)，确保删除位于行开头的注释字符 (`#!`)。

> **备注:** 以下各部分讨论的属性应用于所有节点(也就是说，无法将这些属性应用于单独的节点组)。

> **提示:** 进行任何更改之前，先生成 `nms-ui.properties` 文件的备份副本。确保不要将该备份副本放置在您正在编辑的属性文件所在的目录中。

有关详细信息，另请参阅 `nms-ui.properties` 文件中的注释。

限制显示的量表数

通过编辑以下行并提供所需值，设置要显示的最大量表数：

```
com.hp.nnm.ui.maxGaugePerAnalysisPanel =
```

> **提示:** 显示分析窗格时，较多的量表数会影响性能。较少的量表数会导致量表变大。

设置分析窗格中的量表刷新率

通过编辑以下属性值，设置分析窗格中显示的量表的刷新间隔(以秒为单位)：

```
com.hp.nnm.ui.analysisGaugeRefreshSecs =
```

> **提示:** 将值设置为“0”会导致量表从不刷新。快于 10 秒的刷新率会导致某些 SNMP 代理将其值缓存较短的时间段，从而导致重复的结果。

排除不显示的量表

通过编辑以下行并提供要排除显示的量表列表，定义您不希望显示的量表(针对所有量表视图)：

```
com.hp.nnm.ui.analysisGaugeNoDisplayKeyPatterns =
```

注意以下事项：

- 从所有相关行删除注释字符
- 量表列表中不能包含注释

- 确保量表列表中不存在空行
  空行会在其位置处终止条目
- 此属性的默认设置是注释中的设置
  如果要扩展或修改此配置，则必须包括这些设置；否则，将显示意外数量的量表。

控制节点量表的显示顺序

要控制节点量表的显示顺序，请编辑以下行：

```
com.hp.nnm.ui.analysisGaugeNodeComponentKeys =
```

注意以下事项：

- 此属性设置不支持通配符
- 确保列表中不包含注释或空行
- 此属性的默认设置显示为注释。如果要扩展或修改此配置，则必须包括这些设置；否则，顺序将与配置的顺序不匹配。

控制接口量表的显示顺序

要控制接口量表的显示顺序，请编辑以下行：

```
com.hp.nnm.ui.analysisGaugeInterfaceKeys =
```

此属性设置不支持通配符。确保列表中不包含注释或空行。

此属性的默认设置是注释中的设置。如果要扩展或修改此配置，则必须包括这些设置；否则，顺序将与预期顺序不匹配。

控制自定义轮询器量表的显示顺序

要控制自定义轮询器量表的显示顺序，请编辑以下行：

```
com.hp.ov.nnm.ui.analysisGaugeCustomPolledInstanceKeys =
```

备注: 此属性没有默认设置。

了解如何应用量表属性

按以下顺序应用量表属性：

1. 从状况轮询器检索所有可能量表的列表。
2. 首先应用 analysisGaugeNoDisplayKeyPatterns 以从列表中删除指定的量表。
3. 相应地应用 analysisGaugeNodeComponentKeys、analysisGaugeInterfaceKeys 或 analysisGaugeCustomPolledInstanceKeys 以对所显示量表的列表进行排序。
4. 最后，应用 maxGaugePerAnalysisPanel 以截断所显示的列表。

解决量表问题

本部分包括以下量表问题的故障排除信息：

- 显示的量表太多 (第 100 页)

显示的量表太多

如果量表太多，请执行以下操作：

- 使用 maxGaugePerAnalysisPanel 属性限制显示的量表数量
  有关详细信息，请参阅限制显示的量表数 (第 98 页)。
- 使用 analysisGaugeNoDisplayKeyPatterns 属性删除不需要的量表
  有关详细信息，请参阅排除不显示的量表 (第 98 页)。

配置图标签缩放大小和边框

NNMi 管理员可以使用 nms-ui.properties 文件对图视图进行以下调整：

- 使用缩放功能将节点和端口标签作为图来调整其缩放值。
- 可用于确定图上节点或端口及其标签之间大小差异的最大相对缩放系数。
- 节点和端口标签是否被黑色矩形包围。

> **备注:** 默认情况下，节点和端口的标签被黑色矩形包围，目的是提高标签重叠时的可读性。

下表描述了可更改的属性。

> **提示:** 每个缩放调整属性值均与 NNMi 使用的实际缩放系数相乘。例如，如果将 labelScaleAdjust 的值更改为 .50，则在图上看到的标签将是其正常大小的一半大小。

可在 nms-ui.properties 文件中更改的属性

属性	默认值	描述
!com.hp.nnm.ui.labelScaleAdjust	1.0	调整节点和端口的图标签的缩放大小
!com.hp.nnm.ui.maxLabelScaleAdjust	1.0	调整可用于确定节点或端口及其标签之间大小差异的最大相对缩放系数。
!com.hp.nnm.ui.omitLabelRectangle	true	决定是否使用黑色矩形包围节点和端口标签。 **备注:** 要关闭矩形，请将值设置为 false。

> **备注:** 要实施更改，请重新打开或更改图视图。

配置 Loom 和 Wheel 图的自动折叠阈值

作为 NNMi 管理员，您可以在 Loom 和 Wheel 图极其复杂时，配置图开始自动折叠节点(隐藏接口)和交换机(隐藏端口)的点，从而提高可读性。您可以通过在 nms-ui.properties 文件中调整以下属性来实现这一目的。

Wheel 和 Loom 的自动折叠阈值

属性	描述
com.hp.nnm.ui.wheelAutoCollapseThreshold	使用此属性指定 Wheel 图自动折叠前周围所需的标签数。
com.hp.nnm.ui.loomAutoCollapseThreshold	使用此属性指定 Loom 图自动折叠前整个图中所需的标签数。

要配置自动折叠阈值，请执行以下步骤：

1. 编辑以下文件：
   - Windows：%NNM_PROPS\nms-ui.properties
   - Linux：$NNM_PROPS/nms-ui.properties
2. 根据需要取消对所需属性的注释。有关详细信息，请参阅 nms-ui.properties 文件中的注释。
3. 根据需要更新阈值，然后保存更改。
4. 在 NNMi 控制台中重新打开图以实施更改。

禁用分析窗格

使用 NNMi 时，可通过执行以下步骤，禁用 NNMi 控制台中的分析窗格：

1. 编辑以下文件：
   - Windows：%NNM_PROPS%\nms-ui.properties
   - UNIX：$NNM_PROPS/nms-ui.properties
2. 在文件的末尾添加以下文字：

   # Disables the analysis pane from being shown by default.

   # The analysis pane can still be shown by toggling it open

   # or using the "Show Analysis Pane" menu item.

   # com.hp.nnm.ui.analysisPaneDisabled = true
3. 取消注释属性(最后一行)即可禁用分析窗格。
4. 保存更改。

自定义设备配置文件图标

NNMi 使您能够自定义与设备配置文件或特定节点关联的图标。这些图标显示在表视图、菜单项中，并且在 NNMi 拓扑图上显示为前景图像。

您可以使用 `nnmicons.ovpl` 命令来自定义一个或多个图标。有关详细信息，请参阅 nnmicons.ovpl 参考页或 Linux 联机帮助页。

另请参阅 NNMi 管理员帮助。

配置表视图的刷新率

NNMi 支持 NNMi 管理员覆盖 NNMi 控制台中表视图的默认刷新率。

> **备注:** 最小的建议刷新率为 30 秒。将刷新率设置为少于 30 秒会降低性能。

要覆盖 NNMi 表视图的默认刷新率，请完成以下步骤：

1. 编辑以下文件：

   Windows：`%NMS-PROPS%\nms-ui.properties`

   Linux：`$NNM_PROPS/nms-ui.properties`
2. 确定要更改其刷新率的视图的 `viewInfoId` URL 参数：
   a. 打开要更改其刷新率的视图。
   b. 单击**在新窗口中显示视图**。
   c. 记下 `viewInfoId URL` 参数。例如，**viewInfoId=allIncidentsTableView**。
3. 使用以下格式向 `nms-ui.properties` 添加一行，指定视图及其刷新率(以秒为单位)：

   com.hp.ov.nms.ui.refreshViewSecs.VIEWKEYWORD = SECS

   注意以下事项：

   - **VIEWKEYWORD** 是视图的 viewInfoId URL 参数。
   - **SECS** 是以秒为单位的刷新率。
   - 确保命令行末尾没有额外空格。

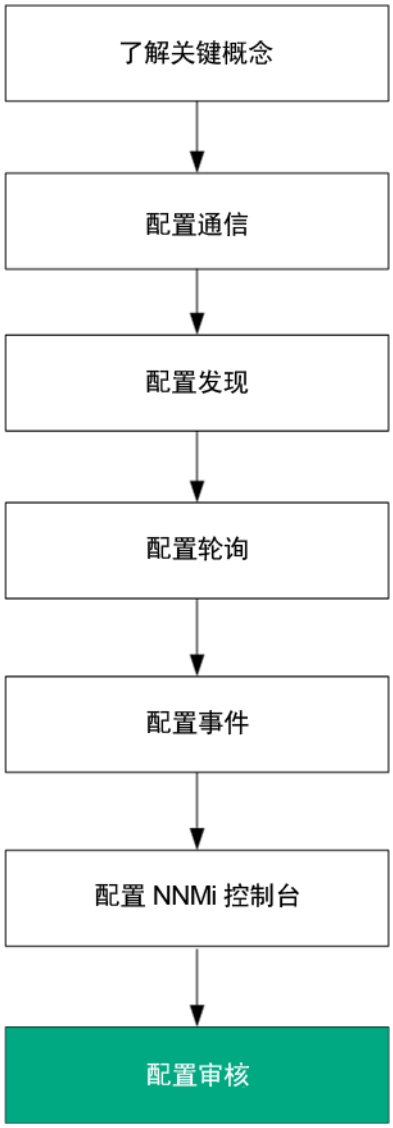
   例如，要将**所有事件**视图的刷新率更改为 120 秒，请将以下行添加到 nms-ui.properties：

   ```
   com.hp.ov.nms.ui.refreshViewSecs.allIncidentsTableView = 120
   ```
4. 保存更改。

要查看新的刷新率，请打开其他视图然后返回到刚配置了刷新率的视图。

> **备注:** 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改时需要停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

NNMi 审核



默认情况下，NNMi 将审核导致对 NNMi 数据库进行更改的用户操作。这些用户操作包括但不限于以下类型：

- 对 NNMi 拓扑对象(例如，节点、节点组、接口和接口组)进行更改。示例包括创建或删除节点组或接口组，以及更改节点组或接口组中的筛选或成员资格。
- 对事件生命周期信息进行更改。示例包括更改事件的所有者或状况。
- 对用户和访问信息进行更改。示例包括更改密码，添加或删除用户帐户或用户组，以及创建租户。
- 使用 NNMi 控制台**配置**工作区或命令行工具进行的配置更改。示例包括修改 SNMP 设置、发现设置和监视配置。
- NNMi 控制台的**操作**菜单中的用户操作。示例包括“配置轮询”和“状态轮询”。

有关写入审核日志的信息类型示例，请参阅关于 NNMi 审核日志文件 (第 107 页)

备注: 默认情况下，审核日志中不包含以下操作或更改：

- 由**系统**用户执行的操作
- 由 NNMi 自动执行的操作或更改不包含在审核日志中。要更改此默认行为，请参阅配置 NNMi 审核日志文件中包含的操作 (第 106 页)

注意以下事项：

- 默认情况下，NNMi 审核处于启用状态。
- 审核信息将每天写入一个日志文件中。
- 审核日志文件位于以下目录：

  提示: 作为 NNMi 管理员，您还可以从 NNMi 控制台**工具 > NNMi 审核日志**菜单选项查看最新的审核日志。

  Windows：%NnmDataDir%\nmsas\NNM\log\audit-<日期>.log

  Linux：$NnmDataDir/nmsas/NNM/log/audit-<日期>.log

- **日志条目示例：**

  2014-04-30T01:20:25.301 joe.operator 10.12.203.55 MODEL abb44ddb-ae52-40d9-855f-f6ab0ab899e1 **UPDATE Node** 151434 172.20.12.7 **managementMode** MANAGED NOTMANAGED

  审核日志中的每个记录包含以下类型的信息：

  - 时间戳
  - 用户名
  - 远程主机的远程地址(如果适用)
  - 记录类型(描述更改类型的类别)
  - 事务 ID(如果适用)
  - 操作(如果适用，执行的操作)
  - 目标对象类型(如果适用，已更改的对象)
  - 可用于对象或操作的其他元数据(如果适用)：
    目标对象 ID
    目标对象名称
    字段名称
    字段旧值
    字段新值

  备注: 密码值将显示为星号，例如：password **********

有关日志文件条目的示例，请参阅关于 NNMi 审核日志文件 (第 107 页)。

- NNMi 会将每个审核日志文件保留 14 天

作为 NNMi 管理员，您可以进行以下配置：

- 禁用审核 (第 105 页)
- 指定保留 NNMi 审核日志的天数 (第 105 页)
- 配置 NNMi 审核日志文件中包含的操作 (第 106 页)

禁用审核

默认情况下，NNMi 审核处于启用状态。

要禁用 NNMi 审核：

1. 打开以下配置文件：

   Windows

   `%NnmDataDir%\nmsas\NNM\conf\nms-audit-config.xml`

   Linux

   `$NnmDataDir/nmsas/NNM/conf/nms-audit-config.xml`
2. 找到包含以下行的文本块：

   `<enabled>true</enabled>`
3. 将 `true` 更改为 `false`：

   `<enabled>false</enabled>`
4. 保存更改。
5. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 `ovstop` 命令。

   在 NNMi 管理服务器上运行 `ovstart` 命令。

指定保留 NNMi 审核日志的天数

默认情况下，NNMi 将每个存档的审核日志文件(每天存档一次)保留 14 天。

要更改 NNMi 保留存档的审核日志文件的天数：

> **备注:** 此数字不影响当天的审核日志文件。

1. 打开以下配置文件：

   Windows

   `%NnmDataDir%\nmsas\NNM\conf\nms-audit-config.xml`

   Linux

   `$NnmDataDir/nmsas/NNM/conf/nms-audit-config.xml`

2. 找到包含以下行的文本块：

   ```
   <retain>14</retain>
   ```

3. 修改包含 NNMi 应将每个审核日志文件保留的天数的行。例如，要将天数更改为一周，请输入：

   ```
   <retain>7</retain>
   ```

   作为响应，NNMi 将保留以下内容：

   - 当前审核日志
   - 每天一个审核日志，额外保留 7 天

4. 保存更改。
5. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 `ovstop` 命令。

   在 NNMi 管理服务器上运行 `ovstart` 命令。

配置 NNMi 审核日志文件中包含的操作

默认情况下，NNMi 将审核导致对 NNMi 数据库进行更改的用户操作。这些用户操作包括但不限于以下类型：

- 对 NNMi 拓扑对象(例如，节点、节点组、接口和接口组)进行更改。示例包括创建或删除节点组或接口组，以及更改节点组或接口组中的筛选或成员资格。
- 对事件生命周期信息进行更改。示例包括更改事件的所有者或状况。
- 对用户和访问信息进行更改。示例包括更改密码，添加或删除用户帐户或用户组，以及创建租户。
- 使用 NNMi 控制台**配置**工作区或命令行工具进行的配置更改。示例包括修改 SNMP 设置、发现设置和监视配置。
- NNMi 控制台的**操作**菜单中的用户操作。示例包括“配置轮询”和“状态轮询”。

有关写入审核日志的信息类型示例，请参阅关于 NNMi 审核日志文件 (第 107 页)

检查 NNMi 审核日志文件之后，您可能发现要包括或排除特定操作、实体或字段的审核。请参阅步骤 3查看示例。

> **提示:** 在每个审核日志消息中，<操作名称> 正好位于 <实体名称> 前面。字段名称显示在 <实体名称> 后面。以下是示例消息，其中操作 (UPDATE)、实体 (Node) 和字段名称 (managementMode) 为粗体：
>
> 2014-04-30T01:20:25.301 joe.operator 10.12.203.55 MODEL abb44ddb-ae52-40d9-855f-f6ab0ab899e1 **UPDATENode** 151434 172.20.12.7 **managementMode** MANAGED NOTMANAGED

要更改 NNMi 审核日志中包含的信息：

1. 打开以下配置文件：

   Windows

   ```
   %NnmDataDir%\nmsas\NNM\conf\nms-audit-config.xml
   ```

Linux

```
$NnmDataDir/nmsas/NNM/conf/nms-audit-config.xml
```

2. 找到包含以下行的文本块：

```
<rules>
<!-- define custom audit rules here.Any rules here will override system defaults -->
</rules>
```

3. 按如下所示修改规则：
   - 要排除审核日志中的单条消息，请使用以下语法：

     ```
     <exclude entity="<实体名称>" field="<字段名称>" action="<操作名称>"/>
     ```

     以下示例不包括此审核日志消息示例：

     2014-04-30T01:20:25.301 joe.operator 10.12.203.55 MODEL abb44ddb-ae52-40d9-855f-f6ab0ab899e1 **UPDATENode** 151434 172.20.12.7 **managementMode** MANAGED NOTMANAGED

     ```
     <exclude entity="Node" field="managementMode" action="UPDATE" />
     ```

   - 要从审核日志中排除实体的所有操作，请使用以下语法：

     ```
     <exclude entity="<实体名称>" />
     ```

     以下示例将从审核日志中排除节点的所有更新操作。

     ```
     <exclude entity="Node" />
     ```

     - 要排除实体的指定操作，请使用以下语法：

     ```
     <exclude entity="<实体名称>" action="<操作名称>" />
     ```

     以下示例将从审核日志中排除节点的所有更新操作。

     ```
     <exclude entity="Node" action="UPDATE" />
     ```

     以下示例将从审核日志中排除节点的所有删除操作：

     ```
     <exclude entity="Node" action="DELETE" />
     ```

   - 要从审核日志中排除任何对象上指定字段的所有操作，请使用以下语法：

     ```
     <exclude field="<字段名称>" />
     ```

     以下示例将从审核日志中排除任何对象上 managementMode 字段的所有更新：

     ```
     <exclude field="managementMode" action="UPDATE" />
     ```

4. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 `ovstop` 命令。

   在 NNMi 管理服务器上运行 `ovstart` 命令。

关于 NNMi 审核日志文件

本部分提供可在审核日志文件中找到的信息类型示例。

- 更改节点的安全组后生成的审核日志条目示例

  以下是在将名为 **mimcisco3** 的节点的安全组从 **Default Security Group** 更改为 **testgrp** 时生成的日志条目示例。

  2014-04-15T01:56:54.979 admin "" MODEL 5fd8ed33-e671-494e-ab25-06d293347c4f **UPDATE Node 50281 mimcisco3** securityGroup "138/**Default Security Group**" 56651/**testgrp**

- 创建用户帐户时生成的审核日志条目示例：

  以下是在为用户 op1 创建帐户时生成的日志条目示例：

  2014-04-15T01:55:48.574 admin "" MODEL 4654e06c-5c1f-4955-bf82-e317dcbf38f3 CREATE Account 56647 **op1** alg "" SHA-256

  2014-04-15T01:55:48.574 admin "" MODEL 4654e06c-5c1f-4955-bf82-e317dcbf38f3 CREATE Account 56647 **op1** external "" false

  2014-04-15T01:55:48.574 admin "" MODEL 4654e06c-5c1f-4955-bf82-e317dcbf38f3 CREATE Account 56647 **op1** name "" op1

  2014-04-15T01:55:48.574 admin "" MODEL 4654e06c-5c1f-4955-bf82-e317dcbf38f3 CREATE Account 56647 **op1** password "" ********

- 为用户组分配用户帐户时生成的审核日志条目示例

  以下是为 **NNMi 第 1 级操作员**用户组分配用户 **op1** 时生成的日志条目示例。

  2014-04-15T01:55:48.597 admin "" MODEL 4654e06c-5c1f-4955-bf82-e317dcbf38f3 CREATE UserGroupMember 56650 5486f4cf-a3e0-4f24-abd6-28f5169f9f92 account "" 56647/**op1**

  2014-04-15T01:55:48.597 admin "" MODEL 4654e06c-5c1f-4955-bf82-e317dcbf38f3 CREATE UserGroupMember 56650 5486f4cf-a3e0-4f24-abd6-28f5169f9f92 **userGroup** "" 141/**level1**

- 更改用户帐户密码时生成的审核日志条目示例：

  以下是在更改 **op2** 用户帐户密码时生成的日志条目示例：

  > **备注:** 第一个用户名是进行更改的用户的名称。第二个用户名是为其更改密码的帐户名称。

  2014-04-15T02:04:39.121 **admin** "" MODEL 0ae97c60-3035-46e0-a20c-20b6da04615f UPDATE Account 56645 **op2 password** ******** ********

第 4 章: 恢复能力

HP Network Node Manager i Software (NNMi) 支持在发生硬件故障时保护 NNMi 数据的两种不同方法：

- 通过在配置相同的系统上维护嵌入式 NNMi 数据库事务日志的副本，NNMi 应用程序故障转移提供灾难恢复。(如果 NNMi 使用 Oracle 数据库，则两个系统在不同时间连接到相同数据库。)
- 通过在共享磁盘上维护嵌入式 NNMi 数据库和配置文件，在高可用性 (HA) 群集中运行 NNMi 时，NNMi 管理服务器的可用性几乎为百分之百。(如果 NNMi 使用 Oracle 数据库，共享磁盘包含 NNMi 配置文件，两个系统在不同时间连接到相同数据库。)

在这两种方法中，如果当前 NNMi 管理服务器失败，则第二个系统自动变成 NNMi 管理服务器。

下表对这两种方法的 NNMi 数据恢复能力进行了多方面的比较。

备注: 如果已购买 NNMi(单独)、NNMi Advanced 以及 NNMi 附带的 NNM iSPI NET 功能，则有两种类型的许可证适用于应用程序故障转移和高可用性环境：

- 应用程序故障转移
  - 生产 - 不管您是否具有应用程序故障转移或高可用性环境，这是为 NNMi、NNMi Advanced 或 NNM iSPI NET 购买的主许可证。将此许可证与主服务器的 IP 地址关联。
  - 非生产 - 此许可证是为用于应用程序故障转移环境而单独购买的。将此许可证与辅助 (备用)服务器的 IP 地址关联。

  高可用性 (HA)
  - 生产 - 不管您是否具有应用程序故障转移或高可用性环境，这是为 NNMi、NNMi Advanced 或 NNM iSPI NET 购买的主许可证。将此许可证与某个物理群集节点的 IP 地址关联。
  - 非生产 - 此许可证是为用于高可用性环境而单独购买的。将此许可证与 NNMi HA 资源组的虚拟 IP 地址关联。
- 如果您已购买 NNMi Premium 或 NNMi Ultimate，则需要使用从 HP 密码交付中心请求的适用于应用程序故障转移或高可用性的一个或多个许可证密钥，而不要按照指示使用非生产许可证。务必请求以下功能：
  - 高可用性：获取 NNMi HA 资源组的虚拟 IP 地址的许可证密钥。此许可证密钥最初在主服务器上使用，然后根据需要在辅助服务器上使用。
  - 应用程序故障转移：获取两个许可证密钥；一个用于主服务器的物理 IP 地址，一个用于备用服务器的物理 IP 地址。

  警告：不要在同一服务器上使用生产和非生产许可证。
- 还可以查看每个 NNM iSPI 的文档，该文档位于以下位置：http://h20230.www2.hp.com/selfsolve/manuals。

NNMi 数据恢复能力比较

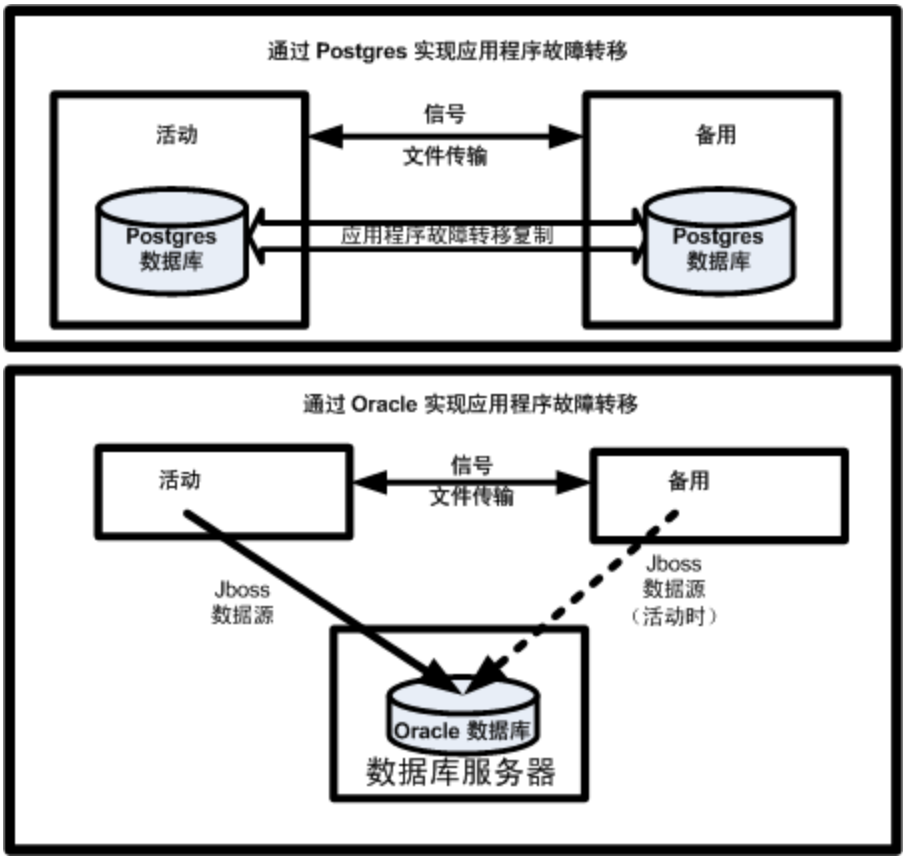
比较项	NNMi 应用程序故障转移	在 HA 群集中运行 NNMi
必需的软件产品	NNMi 或 NNMi Advanced	• NNMi 或 NNMi Advanced • 单独购买的 HA 产品
故障转移所需时间	正常情况下，为 5 到 30 分钟，具体取决于安装的 NNM iSPI 的数量。	正常情况下，为 5 到 30 分钟，具体取决于安装的 NNM iSPI 的数量。
故障转移的透明性	部分。NNMi 管理服务器的 IP 地址更改为备用服务器的物理地址。用户必须使用新 IP 地址连接到 NNMi 控制台。某些应用程序随 NNMi 管理服务器移动，但大多数应用程序(包括 NNM iSPI)不会如此。	完全。所有连接使用 HA 群集的虚拟 IP 地址，该地址在故障转移时不会更改。
活动和备用服务器的相对邻近程度	LAN 或 WAN	LAN 或 WAN(仅针对某些 HA 产品)
安装的许可证	• 初始活动服务器上使用许可证密钥。 • 初始备用服务器上使用许可证密钥。	初始活动服务器上使用许可证密钥并在共享磁盘上管理。
对 NNM iSPI 的支持	支持各不相同。请参阅每个 NNM iSPI 文档。	
与全局网络管理的交互	• 可以为应用程序故障转移或 HA 配置单独的全局管理器。 • 可以为应用程序故障转移或 HA 配置单独的区域管理器。 • 这两个配置分别需要两个物理或虚拟系统。[a] • 如果全局管理器或区域管理器发生故障转移，则 NNMi 将在全局管理器和区域管理器之间重新建立连接。	
NNMi 维护	NNMi 必须从应用程序故障转移群集中排除后才能应用补丁或升级。	NNMi 可以在不取消配置 HA 的情况下应用补丁和升级。

本部分包含以下各章：

- 为 NNMi 配置应用程序故障转移 (第 111 页)
- 在高可用性群集中配置 NNMi (第 138 页)

[a]HA 的虚拟机支持依赖于 HA 软件供应商对虚拟系统的支持。

为 NNMi 配置应用程序故障转移



很多信息技术专业人员依赖于 HP Network Node Manager i Software (NNMi) 在关键网络设备出现故障时通知他们并提供故障的根源。甚至在 NNMi 管理服务器发生故障时，他们还需要 NNMi 继续通知网络设备故障。**NNMi 应用程序故障转移**能够满足此要求，可将 NNMi 进程的应用程序控制从活动 NNMi 管理服务器转移到备用 NNMi 管理服务器，从而保证 NNMi 功能的连续性。

本章包含以下主题：

- 应用程序故障转移概述 (第 112 页)
- 应用程序故障转移要求 (第 112 页)
- 为 NNMi 设置应用程序故障转移 (第 113 页)
- 使用应用程序故障转移功能 (第 117 页)
- 故障转移后恢复原始配置 (第 122 页)
- NNM iSPI 和应用程序故障转移 (第 122 页)
- 集成应用程序 (第 126 页)
- 禁用应用程序故障转移 (第 126 页)
- 管理任务和应用程序故障转移 (第 128 页)
- 网络延迟/带宽注意事项 (第 134 页)

应用程序故障转移概述

应用程序故障转移功能可用于使用嵌入式或 Oracle 数据库的 NNMi 安装。在将系统配置为使用应用程序故障转移功能之后，NNMi 检测 NNMi 管理服务器故障并触发辅助服务器以恢复 NNMi 功能。

以下术语和定义应用于 NNMi 的应用程序故障转移配置：

- **活动**：正在运行 NNMi 进程的服务器。
- **备用**：NNMi 群集中正在等待故障转移事件的系统；此系统未在运行 NNMi 进程。
- **群集成员**：正在使用 JGroups 技术连接到群集的系统上运行的 Java 进程；单个系统上可以有多个成员。
- **Postgres**:NNMi 用于存储拓扑、事件和配置信息之类的信息的嵌入式数据库。
- **群集管理器**：用于监视和管理服务器的应用程序故障转移功能的 `nnmcluster` 进程和工具。

应用程序故障转移要求

要部署应用程序故障转移功能，请在两个服务器上安装 NNMi。本章将这两个 NNMi 管理服务器称为**活动**和**备用**服务器。在正常操作期间，只有活动服务器运行 NNMi 服务。

活动和备用 NNMi 管理服务器是监视来自两个 NNMi 管理服务器的检测信号的群集的一部分。如果活动服务器出现故障，导致其检测信号丢失，则备用服务器将成为活动服务器。

为使应用程序故障转移成功，NNMi 管理服务器必须符合以下要求：

- 两个 NNMi 管理服务器必须运行相同类型的操作系统。例如，如果活动服务器运行 Linux 操作系统，则备用服务器也必须运行 Linux 操作系统。
- 两个 NNMi 管理服务器必须运行相同版本的 NNMi。例如，如果 NNMi 10.01 在活动服务器上运行，则备用服务器上必须运行相同 NNMi 版本 NNMi 10.01。两个服务器上的 NNMi 补丁程序级别也必须相同。
- 两个 NNMi 管理服务器上的系统密码必须相同。
- 对于 Windows 操作系统上的 NNMi 安装，`%NnmDataDir%` 和 `%NnmInstallDir%` 系统变量在两个服务器上必须设置为相同值。
- NNMi 管理服务器必须运行同一数据库。例如，两个 NNMi 管理服务器必须都运行 Oracle 或都运行嵌入式数据库。如果计划使用应用程序故障转移功能，则不能混用两个数据库类型。
- 两个 NNMi 管理服务器必须具有相同的许可属性。例如，节点计数和许可功能必须相同。
- 除非 NNMi 处于初始发现的高级阶段，否则不要启用应用程序故障转移。有关详细信息，请参阅评估发现 (第 62 页)。

为了让应用程序故障转移功能正常运行，活动和备用服务器必须能不受限制地通过网络互相访问。满足此条件后，完成为 NNMi 设置应用程序故障转移 (第 113 页)中所示的步骤。有关详细信息，请参阅NNMi 和 NNM iSPI 默认端口 (第 412 页)。

备注: 如果已购买 NNMi(单独)、NNMi Advanced 以及 NNMi 附带的 NNM iSPI NET 功能，则有两种类型的许可证适用于应用程序故障转移环境：

- 生产 - 不管您是否具有应用程序故障转移或高可用性环境，这是为 NNMi、NNMi Advanced

或 NNM iSPI NET 购买的主许可证。将此许可证与主服务器的 IP 地址关联。

- 非生产 - 此许可证是为用于应用程序故障转移环境而单独购买的。将此许可证与辅助(备用)服务器的 IP 地址关联。

警告：不要在同一服务器上使用生产和非生产许可证。

如果您已购买 NNMi Premium 或 NNMi Ultimate，则需要使用从 HP 密码交付中心请求的适用于应用程序故障转移的一个或多个许可证密钥，而不要按照指示使用非生产许可证。获取两个许可证密钥；一个用于主服务器的物理 IP 地址，一个用于备用服务器的物理 IP 地址。

还可以查看每个 NNM iSPI 的文档，该文档位于以下位置：http://h20230.www2.hp.com/selfsolve/manuals。

备注: 锁定文件或限制网络访问的任何软件都可能导致 NNMi 通信出现问题。将这些应用程序配置为忽略 NNMi 使用的文件和端口。

备注: 在 NNMi 安装或升级过程中，NNMi 安装会选择一个网络接口用于 NNMi 群集通信。选择的网络接口通常是系统上的第一个非环回接口。配置 NNMi 群集时，配置将使用所选的接口。如果必须调整该接口，请执行以下操作：

1. 编辑以下文件：
   - Windows：`%NnmDataDir%\conf\nnm\props\nms-cluster-local.properties`
   - Linux：`$NnmDataDir/conf/nnm/props/nms-cluster-local.properties`
2. 将 `com.hp.ov.nms.cluster.interface` 参数调整为指向所需的接口。

为 NNMi 设置应用程序故障转移

备注: 如果已购买 NNMi(单独)、NNMi Advanced 以及 NNMi 附带的 NNM iSPI NET 功能，则有两种类型的许可证适用于应用程序故障转移环境：

- 生产 - 不管您是否具有应用程序故障转移或高可用性环境，这是为 NNMi、NNMi Advanced 或 NNM iSPI NET 购买的主许可证。将此许可证与主服务器的 IP 地址关联。
- 非生产 - 此许可证是为用于应用程序故障转移环境而单独购买的。将此许可证与辅助(备用)服务器的 IP 地址关联。

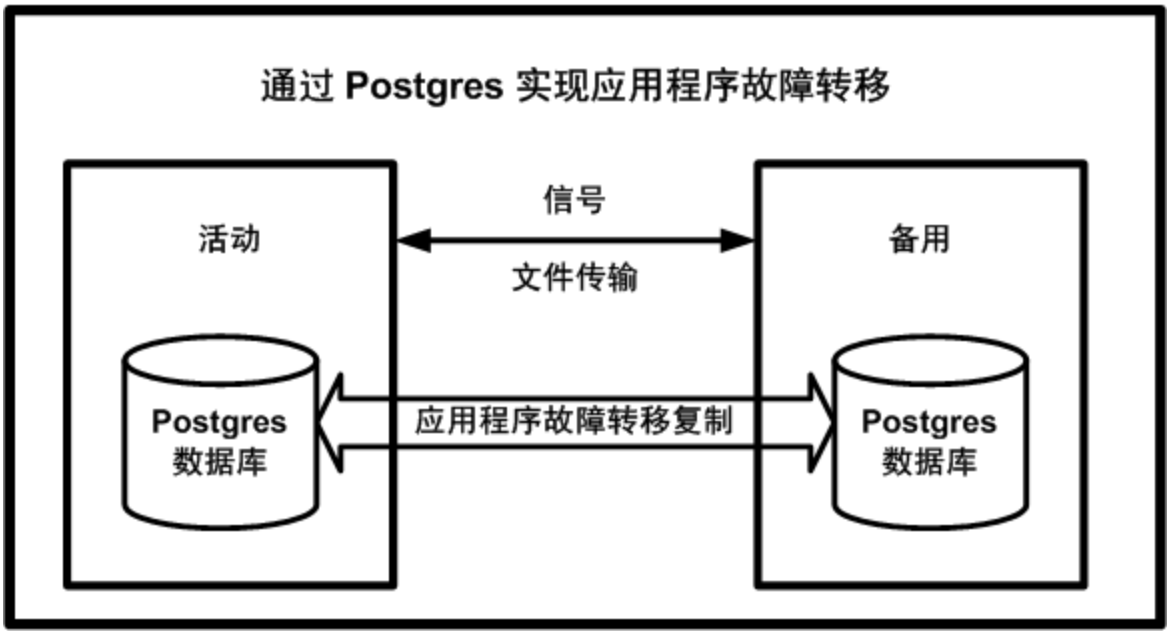
如果您已购买 NNMi Premium 或 NNMi Ultimate，则需要使用从 HP 密码交付中心请求的适用于应用程序故障转移的一个或多个许可证密钥，而不要按照指示使用非生产许可证。务必获取两个许可证密钥；一个用于主服务器的物理 IP 地址，一个用于备用服务器的物理 IP 地址。

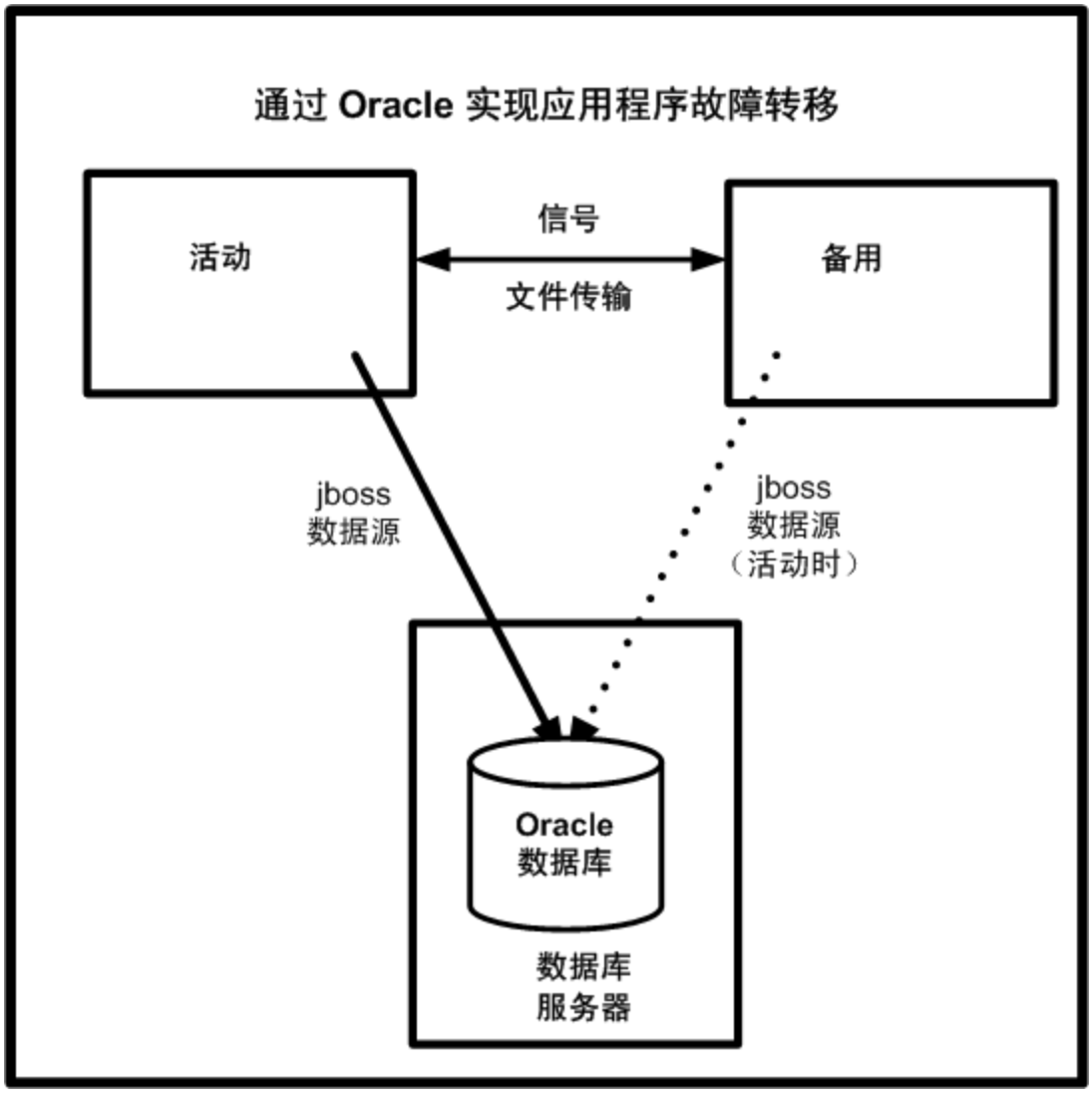
警告：不要在同一服务器上使用生产和非生产许可证。

还可以查看每个 NNM iSPI 的文档，该文档位于以下位置：http://h20230.www2.hp.com/selfsolve/manuals。

1. 如下图中显示的《HP Network Node Manager i Software 交互安装指南》中所述，在活动服务器(服务器 X)和备用服务器(服务器 Y)上安装 NNMi：

   在 NNMi 中设置应用程序故障转移





2. 对于服务器 X 上的每个许可证，如许可 NNMi (第 252 页)中所述获取服务器 Y 所需的许可证，并将它安装到服务器 Y 上。
3. 在每个服务器上运行 **ovstop** 命令以关闭 NNMi。

> **备注:** 如果在将 Oracle 作为数据库时使用应用程序故障转移，则备用服务器上的 NNMi 进程应当已经停止。

4. 如果在将 Oracle 作为数据库时使用应用程序故障转移，则遵循手动为 NNMi 配置应用程序故障转移 (第 406 页)中的配置步骤。

使用 NNMi 群集设置向导配置群集(仅限嵌入式数据库用户)

NNMi 群集设置向导将自动执行在 NNMi 中配置群集以使用应用程序故障转移的过程。通过该向导可以：

- 指定并验证群集节点
- 定义群集属性和端口
- 将两个节点的 nnm.keystore 和 nnm.truststore 文件内容合并到单个 nnm.keystore 和 nnm.truststore 文件中

1. 在支持的 Web 浏览器中输入以下内容来启动群集设置向导：

   http://<NNMi 服务器>:<端口>/cluster

   - <NNMi 服务器> 是 NNMi 主机的值。
   - <端口> 是 NNMi 端口的值。

2. 输入您的系统**用户名**和**密码**，然后单击**登录**按钮以登录到 NNMi。
3. 输入**本地主机名**和**远程群集节点**值以定义群集节点，然后单击**下一步**。
4. 在“通信结果”页上，查看通信验证结果。如果出现错误，则单击**上一步**解决问题；否则单击**下一步**。

   绿色状态消息指示已成功连接到远程群集节点。
5. 在“定义群集属性”页上，输入**群集名称**，定义**备份间隔**(以小时为单位)，并指定是否启用自动故障转移。单击**下一步**。
6. 在“定义群集端口”页上，输入**起始群集端口**和**文件传输端口**值。

   备注: NNMi 群集使用 4 个以**起始群集端口**开头的连续端口。

7. 单击**下一步**。
8. 查看提供的摘要信息。单击**上一步**返回更改配置信息；否则单击**提交**保存群集配置。

   最后的摘要指示信息是否成功写入配置文件。
9. 通过在两个节点上运行 **ovstop** 命令，立即在这两个节点上停止 NNMi。
10. 通过在两个节点上运行 **nnmcluster** 命令，验证这两个节点是否可以群集。如果节点无法群集，则参阅手动为 NNMi 配置应用程序故障转移 (第 406 页)。
11. 使用 **nnmcluster** 命令在所需的活动节点上启动 NNMi。等待 NNMi 报告 ACTIVE(参阅手动为 NNMi 配置应用程序故障转移 (第 406 页))。
12. 使用 **ovstart** 命令启动备用节点。

设置群集通信(可选)

在安装期间，NNMi 查询系统上的所有网络接口卡 (NIC) 以查找一个用于群集通信(选择第一个可用 NIC)。如果系统有多个 NIC，则可以通过执行以下操作，选择用于 nnmcluster 操作的 NIC：

1. 运行 nnmcluster -interfaces 以列出所有可用接口。有关详细信息，请参阅 nnmcluster 参考页或 UNIX 联机帮助页。
2. 编辑以下文件：
   - Windows：

     %NnmDataDir%\conf\nnm\props\nms-cluster-local.properties

- Linux：

  `$NnmDataDir/conf/nnm/props/nms-cluster-local.properties`

3. 查找包含与下面类似的文本的行：

   `com.hp.ov.nms.cluster.interface =<值>`

4. 根据需要更改值。

   备注: 接口值必须是有效的接口；否则，群集可能无法启动。

5. 保存 `nms-cluster-local.properties` 文件。

   备注: `com.hp.ov.nms.cluster.interface` 参数允许 NNMi 管理员选择用于 nnmcluster 通信的通信接口。此接口不是用于嵌入式数据库或安全套接字层通信的接口。

   备注: 要配置通信以便特定接口采用应用程序故障转移，请使用 `com.hp.ov.nms.cluster.member.hostnames` 参数中的 IP 地址，而不是使用主机名。设置以下文件中的 `com.hp.ov.nms.cluster.member.hostnames` 参数：

   Windows：

   `%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`

   Linux：

   `$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`

使用应用程序故障转移功能

在两个 NNMi 管理服务器都在运行群集管理器之后，且有一个活动节点和一个备用节点，则可以使用群集管理器查看群集状态。群集管理器有三个模式：

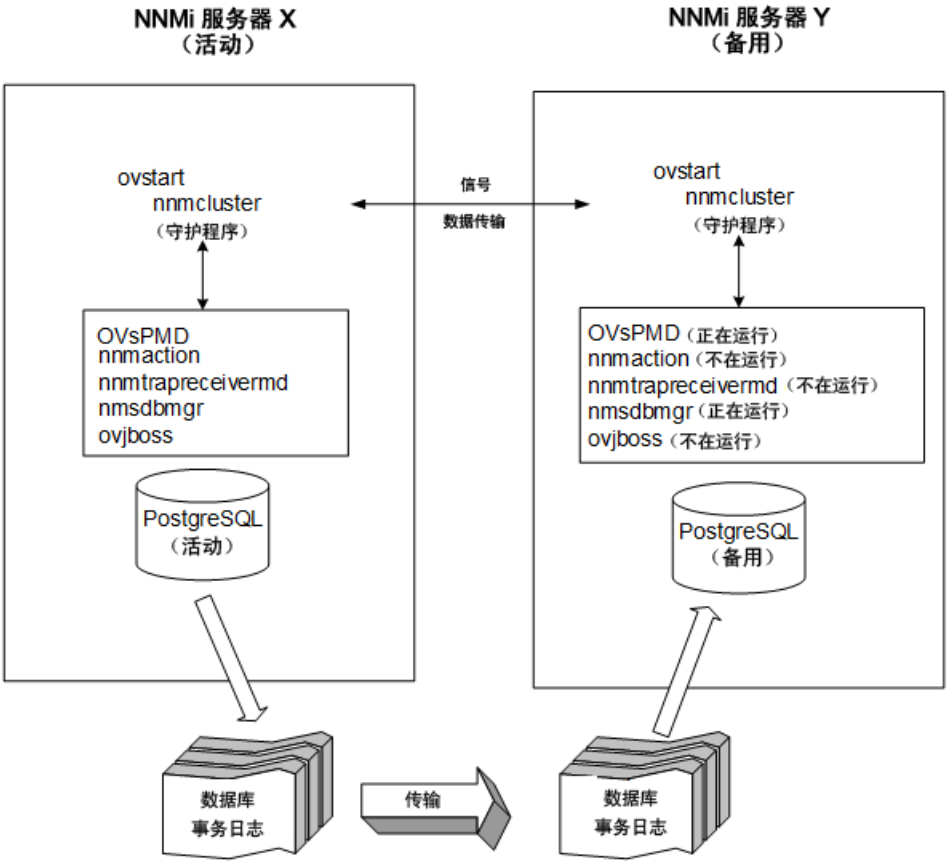
- **守护程序模式**：群集管理器进程在后台运行，并使用 **ovstop** 和 **ovstart** 命令启动和停止 NNMi 服务。
- **交互模式**：群集管理器运行 NNMi 管理员可在其中查看和更改群集属性的交互会话。例如，NNMi 管理员可使用此会话来启用或禁用应用程序故障转移功能，或者关闭守护程序进程。
- **命令行模式**：NNMi 管理员在命令提示符处查看和更改群集属性。

有关详细信息，请参阅 nnmcluster 参考页或 Linux 联机帮助页。

使用嵌入式数据库的应用程序故障转移行为

下图显示使用嵌入式数据库的两个 NNMi 管理服务器的应用程序故障转移配置。阅读本章的其余内容时，请参考此图。

应用程序故障转移配置(嵌入式数据库)



备注: 如果从群集中删除备用服务器，并将该服务器作为独立服务器运行，然后将其重新添加到该群集中，则可能会收到数据库错误。如果出现此错误，请从命令行运行以下命令：`nnmcluster dbsync`。

NNMi 在应用程序故障转移中包括流复制功能，用于将数据库事务从活动服务器发送到备用服务器，从而使备用服务器与活动服务器保持同步。这样就无需在故障转移时在备用服务器上导入数据库事务日志(在早期 NNMi 版本中这样做)，因此大大减少了备用服务器替代活动服务器所需的时间。此功能的另一个优势是：只在需要时将数据库备份文件从一个节点发送到另一个节点，并且在定期传输数据库事务文件的情况下，需要发送大量数据库备份文件的时候应该很少。

备注: 对于活动节点和备用节点，如果启用了防火墙，请确保用于嵌入式数据库的端口(默认情况下端口为 5432)是打开的。在以下文件中设置此端口：

Windows：`%NNM_CONF%\nnm\props\nms-local.properties`

Linux：`$NNM_CONF/nnm/props/nms-local.properties`

在启动活动和备用节点之后，备用节点检测活动节点，请求来自活动节点的数据库备份，但不启动 NNMi 服务。将此数据库备份存储为单个 Java-ZIP 文件。如果备用节点已有来自之前群集连接的 ZIP 文件，且 NNMi 发现文件已与活动服务器同步，将不重新传输文件。

活动和备用节点都在运行时，活动节点将数据库事务日志定期发送到备用节点。您可以通过在 nms-cluster.properties 文件中更改 com.hp.ov.nms.cluster.timeout.archive 参数的值，修改此数据传输的频率。这些事务日志累积在备用节点上，任何时候需要激活它时都在备用节点上可用。

备用节点从活动节点接收完整数据库备份时，它将信息放置到它的嵌入式数据库中。它还创建 recovery.conf 文件以通知嵌入式数据库，在它可用于其他服务之前应拥有所有接收的事务日志。

如果活动节点出于某种原因变为不可用，则通过运行 **ovstart** 命令启动 NNMi 服务，使备用节点成为活动节点。在启动剩余的 NNMi 服务之前，备用 NNMi 管理服务器将导入事务日志。

如果活动 NNMi 系统失败，则备用系统开始发现和轮询活动。此转换使 NNMi 能够保持对网络的监视和轮询，与此同时您可以对失败的系统进行诊断和修复。

备注:

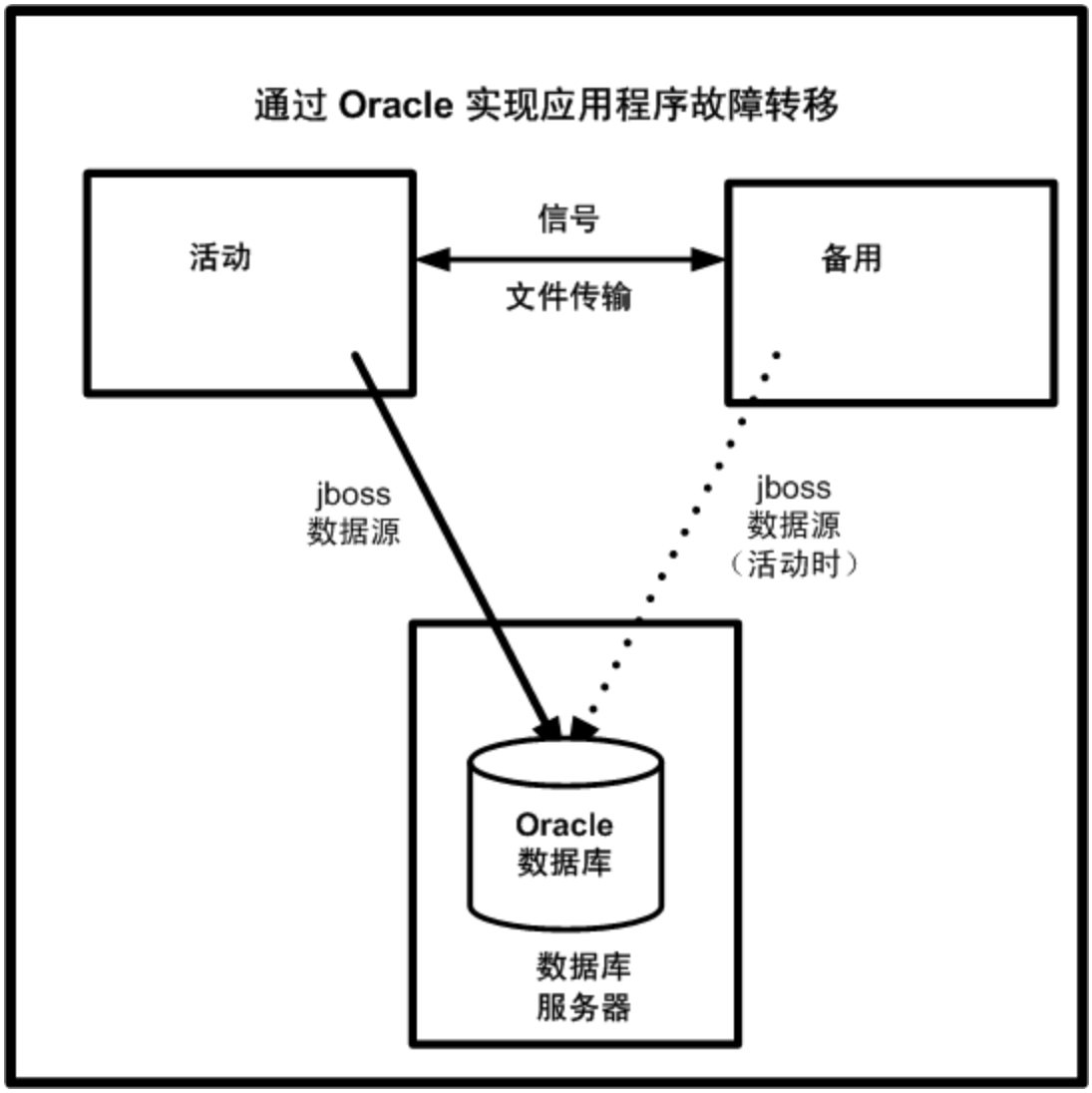
- NNMi 在应用程序故障转移后将自动重新同步拓扑、状况和状态。
- 在重新同步期间不要停止 NNMi。

  为帮助确保重新同步已完成，请在应用程序故障转移后让 NNMi 运行几小时。实际所需时间取决于节点数、状况更改量和执行重新同步时接收到的陷阱数据。
- 如果 NNMi 必须在重新同步完成之前停止，则应重新运行一次重新同步并允许完成。
- 要执行整个管理服务器的手动重新同步，请运行：nnmnoderediscover.ovpl –all –fullsync

使用 Oracle 数据库的应用程序故障转移行为

下图显示使用 Oracle 数据库的两个 NNMi 管理服务器的应用程序故障转移配置。阅读本章的其余内容时，请参考此图。

应用程序故障转移配置(Oracle 数据库)



如果活动节点出于某种原因变为不可用，则通过运行 **ovstart** 命令启动 NNMi 服务，使备用节点成为活动节点。

如果活动 NNMi 系统失败，则备用系统开始发现和轮询活动。此转换使 NNMi 能够保持对网络的监视和轮询，与此同时您可以对失败的系统进行诊断和修复。

备注:

- 因为 NNMi 在应用程序故障转移后进行重新同步，所以状态和事件的更新会延迟。
- 如果您在此重新同步期间看到以下消息，并不表示出现问题：

  原因引擎的队列过大导致状态和事件的更新延迟。这可能是因为在执行升级、应用程序故障转移和从备份恢复后需要重新同步，或需要手动重新同步。
- 在此重新同步期间不要停止 NNMi。要确保重新同步已完成，请在应用程序故障转移后保持 NNMi 运行几小时。

应用程序故障转移场景

有几个可能问题可导致活动 NNMi 管理服务器停止发送检测信号并启动故障转移：

- 场景 1：活动 NNMi 管理服务器出现故障。
- 场景 2：系统管理员关闭或重新启动活动 NNMi 管理服务器。
- 场景 3：NNMi 管理员关闭群集。
- 场景 4：活动和备用 NNMi 管理服务器之间的网络连接出现故障。

  在场景 4 中，两个 NNMi 管理服务器都在活动状况下运行。网络设备恢复联机时，两个 NNMi 管理服务器自动协商哪个节点应成为新的主动节点。

其他 ovstart 和 ovstop 选项

在配置了应用程序故障转移的 NNMi 管理服务器上使用 **ovstop** 和 **ovstart** 命令时，NNMi 运行以下命令：

- ovstart:**nnmcluster -daemon**
- ovstop:**nnmcluster -disable -shutdown**

> **备注:** 如果运行 **ovstop** 命令，则 NNMi 不会故障转移到备用节点。HP 设计了 **ovstop** 命令来支持临时维护停止。要手动启动故障转移，请用 **ovstop** 命令加 **-failover** 选项。有关详细信息，请参阅 ovstop 参考页或 Linux 联机帮助页。

ovstop 命令的以下选项应用于在应用程序故障转移群集中配置的 NNMi 管理服务器：

- **ovstop -failover**：此命令停止本地的守护程序模式的群集进程，并强制故障转移到备用 NNMi 管理服务器。如果之前禁用了故障转移模式，则重新启用它。此命令等价于：**nnmcluster -enable -shutdown**
- **ovstop -nofailover**：此命令禁用故障转移模式，然后停止本地的守护程序模式的群集进程。不发生故障转移。此命令等价于：**nnmcluster -disable -shutdown**
- **ovstop -cluster**：此命令停止活动节点和备用节点，并从群集中删除它们。此命令等价于：**nnmcluster -halt**

> **备注:** 如果在运行 Linux 操作系统的 NNMi 管理服务器上运行 **shutdown** 命令，则 **ovstop** 命令会自动运行，并禁用应用程序故障转移。这可能不是您所希望的结果。要控制维护时段内的应用程序故障转移，请使用 **nnmcluster -acquire** 和 **nnmcluster -relinquish** 命令按您所希望的方式设置活动节点和备用节点，然后再运行 shutdown 命令。有关详细信息，请参阅 nnmcluster 参考页或 Linux 联机帮助页。

应用程序故障转移事件

只要 nnmcluster 进程或使用 **nnmcluster** 命令的用户将节点作为活动节点启动，NNMi 就生成以下事件之一：

- NnmClusterStartup:已启动 NNMi 群集，但不存在活动节点。因此，节点是在活动状况下启动的。此事件的严重度为正常。
- NnmClusterFailover:NNMi 群集检测到活动节点故障。备用节点随即启用，并在新的活动节点上启动 NNMi 服务。此事件的严重度为重大。

故障转移后恢复原始配置

如果活动节点出现故障且备用节点用作活动节点，则在修复以前的活动节点之后，可以返回到原始配置。

执行以下步骤：

1. 解决以前活动节点的问题。
2. 在所需活动节点上运行以下命令以返回到原始配置：

   nnmcluster -acquire

有关详细信息，请参阅 nnmcluster 参考页或 Linux 联机帮助页。

NNM iSPI 和应用程序故障转移

如果部署符合以下要求，则可以为与 NNMi 一起部署的 Smart Plug-in (iSPI) 使用应用程序故障转移功能：

- NNM iSPI 在 NNMi 管理服务器上运行。
- 仅限嵌入式数据库。NNM iSPI 与 NNMi 使用相同的嵌入式数据库实例。
- 仅限 Oracle 数据库。NNM iSPI 使用的 Oracle 数据库实例必须与 NNMi 使用的 Oracle 数据库实例不同。

NNM iSPI Performance for Metrics 和 NNM iSPI Performance for Traffic 是此描述的例外。如果计划配置 NNMi 应用程序故障转移功能，则必须在专用服务器上安装这些 iSPI。在这种情况下，故障转移发生之后，iSPI 自动连接到新的 NNMi 管理服务器。有关在已安装 NNMi 的应用程序故障转移环境中安装这些 iSPI 的详细信息，请参阅 NNM iSPI Performance for Metrics 和 NNM iSPI Performance for Traffic 文档。

有关详细信息，请参阅 NNM iSPI Performance for Metrics 中的“应用程序故障转移支持”、NNM iSPI Performance for QA 或 NNM iSPI Performance for Traffic 帮助。

使用嵌入式数据库时的 NNM iSPI 安装信息

将 NNM iSPI 部署在现有应用程序故障转移环境中 - 嵌入式数据库

要在已经是应用程序故障转移群集一部分的 NNMi 管理服务器上安装 NNM iSPI(IP Telephony、MPLS 或 Multicast)，请执行以下步骤：

1. (仅适用于 NNM iSPI 升级)作为预防措施，请备份所有必要的配置详细信息和 NNMi 数据：
   - 继续前，请在活动和备用 NNMi 管理服务器上运行 `nnmconfigexport.ovpl` 脚本。有关信息，请参阅最佳实践：保存现有配置 (第 26 页)。
   - 继续前，请在活动和备份 NNMi 管理服务器上备份 NNMi 数据。有关信息，请参阅备份范围 (第 197 页)。
2. 请在活动 NNMi 管理服务器上运行 `nnmcluster -dbsync` 命令，并等待命令完成。
3. 执行以下步骤来禁用应用程序故障转移：
   a. 在备用 NNMi 管理服务器上，运行以下命令：

      ```
      nnmcluster -shutdown
      ```

b. 在备用 NNMi 管理服务器上编辑以下文件：
   - Windows：%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties
   - Linux：$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties
c. 注释掉 com.hp.ov.nms.cluster.name 选项并保存此文件。
d. 在两个 NNMi 管理服务器上编辑以下文件：
   - Windows：%NnmDataDir%\shared\nnm\databases\Postgres\postgresql.conf
   - Linux：$NnmDataDir/shared/nnm/databases/Postgres/postgresql.conf
e. 删除以下行，这些行由应用程序故障转移自动添加。下面是这些行的可能外观的示例。这些行在您的服务器上的外观可能略有不同。

```
# The following lines were added by the NNM cluster.
archive_command = ...
archive_timeout = 900
max_wal_senders = 4
archive_mode = 'on'
wal_level = 'hot_standby'
hot_standby = 'on'
wal_keep_segments = 500
listen_addresses = 'localhost,16.78.61.68'
```

   请务必保存更改。
f. 删除以下位置的 recovery.conf 和 recovery.done 文件(如果它们存在)：
   - Windows：%NnmDataDir%\shared\nnm\databases\Postgres\
   - Linux：$NnmDataDir/shared/nnm/databases/Postgres/
g. 创建以下触发器文件，以告知 Postgres 停止以备用模式运行并开始完全运行：
   - Windows：%NnmDataDir%\tmp\postgresTriggerFile
   - Linux：%NnmDataDir%/tmp/postgresTriggerFile\

4. 通过执行以下步骤，在活动和备用服务器上安装或升级 NNM iSPI 并启用应用程序故障转移：
   a. 在备用 NNMi 管理服务器上运行 ovstart 命令。这将使 NNMi 服务处于独立(非群集)状态。
   b. 如 iSPI 安装或升级文档中所述，在备用 NNMi 管理服务器上安装或升级 NNM iSPI。
   c. 在活动 NNMi 管理服务器上运行 nnmcluster -halt 命令。
   d. 在活动 NNMi 管理服务器上编辑以下文件：
      - Windows：%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties
      - Linux：$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties
   e. 注释掉 com.hp.ov.nms.cluster.name 选项并保存此文件。
   f. 在活动 NNMi 管理服务器上运行 ovstart 命令。这将使 NNMi 服务处于独立(非群集)状态。
   g. 如 iSPI 安装或升级文档中所述，在活动 NNMi 管理服务器上安装或升级 NNM iSPI。

h. 在活动和备用两个 NNMi 管理服务器上编辑以下文件：
   - Windows：%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties
   - Linux：$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties

i. 取消对 com.hp.ov.nms.cluster.name 选项的注释并保存每个文件。

j. 在活动 NNMi 管理服务器上运行 nmcluster -daemon 命令。

k. 等待几分钟，让活动 NNMi 管理服务器成为群集中的第一个主动节点。在活动 NNMi 管理服务器上运行 nnmcluster -display 命令，并在显示结果中搜索术语 ACTIVE，就像在 ACTIVE_NNM_STARTING 或 ACTIVE_SomeOtherState 中一样。不要继续执行，除非您知道活动 NNMi 管理服务器是主动节点。

5. 在备用 NNMi 管理服务器上运行 nmcluster -daemon 命令。
6. 在主动节点上，运行以下命令：

   nnmcluster -dbsync

随 NNMi 部署 NNM iSPI，然后配置应用程序故障转移 - 嵌入式数据库

要随 NNMi 安装 NNM iSPI(IP Telephony、MPLS 或 Multicast)，然后再配置应用程序故障转移，请执行以下步骤：

1. 在主服务器和辅助服务器上安装 NNMi 和 NNM iSPI。
2. 在主服务器和辅助服务器上为 NNM iSPI 安装非生产许可证。
3. 按为 NNMi 设置应用程序故障转移 (第 113 页)中所述配置应用程序故障转移。NNM iSPI 会自动针对应用程序故障转移进行配置。

使用 Oracle 数据库时的 NNM iSPI 安装信息

将 NNM iSPI 部署在现有 NNMi 应用程序故障转移环境中 - Oracle 数据库

要在已经是使用 Oracle 数据库的应用程序故障转移群集一部分的 NNMi 管理服务器上安装或升级 NNM iSPI(IP Telephony、MPLS 或 Multicast)，请执行以下步骤：

1. (仅适用于 NNM iSPI 升级)作为预防措施，请备份所有必要的配置详细信息和 NNMi 数据：
   - 继续前，请在活动和备用 NNMi 管理服务器上运行 nnmconfigexport.ovpl 脚本。有关信息，请参阅最佳实践：保存现有配置 (第 26 页)。
   - 继续前，请在活动和备份 NNMi 管理服务器上备份 NNMi 数据。有关信息，请参阅备份范围 (第 197 页)。
   - 使用相应的数据库命令备份 Oracle 数据库上的所有 NNMi 数据。
2. 执行以下步骤来禁用应用程序故障转移：
   a. 在活动 NNMi 管理服务器上运行 nnmcluster -shutdown 命令。
   b. 等待几分钟，使旧的备用 NNMi 管理服务器成为新的活动 NNMi 管理服务器。
   c. 在新的活动(旧的备用)NNMi 管理服务器上运行 nnmcluster -display 命令。

d. 在显示结果中搜索 ACTIVE_NNM_RUNNING 状态。重复前面的步骤，直至看到 ACTIVE_NNM_RUNNING 状态。
e. 在新的活动(旧的备用)NNMi 管理服务器上运行 nnmcluster -halt 命令。
f. 在新的活动(旧的备用)NNMi 管理服务器上重复运行 nnmcluster -display 命令，直至看不到 DAEMON 进程。
g. 在两个服务器上运行 ovstatus -a 命令，并确保 NNMi 进程都已停止。
h. 在活动和备用 NNMi 管理服务器上，编辑以下文件并注释掉 com.hp.ov.nms.cluster.name 选项。
   - Windows：%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties
   - Linux：$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties

3. 按照以下步骤先后在活动和备用 NNMi 管理服务器上安装或升级 NNM iSPI：
   a. 在活动 NNMi 管理服务器上，运行 ovstart 命令。这将使 NNMi 服务处于独立(非群集)状态。
   b. 如 iSPI 安装或升级文档中所述，在 NNMi 管理服务器上安装或升级 NNM iSPI。
   c. 在活动 NNMi 管理服务器上运行 ovstop 命令。
   d. 在备用 NNMi 管理服务器上，运行 ovstart 命令。这将使 NNMi 服务处于独立(非群集)状态。
   e. 如 iSPI 安装或升级文档中所述，在 NNMi 管理服务器上安装或升级 NNM iSPI。
   f. 在备用 NNMi 管理服务器上运行 ovstop 命令。
4. 执行以下步骤来启用应用程序故障转移：
   a. 在活动和备用 NNMi 管理服务器上，编辑以下文件并取消注释 com.hp.ov.nms.cluster.name 选项。
      - Windows：%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties
      - Linux：$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties
   b. 在活动 NNMi 管理服务器上运行 nmcluster -daemon 命令。
   c. 等待几分钟，让活动 NNMi 管理服务器成为群集中的第一个主动节点。在活动 NNMi 管理服务器上运行 nnmcluster -display 命令，并在显示结果中搜索术语 ACTIVE，就像在 ACTIVE_NNM_STARTING 或 ACTIVE_SomeOtherState 中一样。除非您知道活动 NNMi 管理服务器是主动节点，否则不要继续执行后续步骤。
   d. 在备用 NNMi 管理服务器上运行 nmcluster -daemon 命令。

随 NNMi 部署 NNM iSPI，然后配置应用程序故障转移 - Oracle 数据库

要随 NNMi 安装 NNM iSPI(IP Telephony、MPLS 或 Multicast)，然后再配置应用程序故障转移，请执行以下步骤：

1. 在用作主服务器的含 Oracle 的服务器 1(主 NNMi 管理服务器)上，安装 NNMi 和必需的 NNM iSPI(IP Telephony、Multicast 或 MPLS)。
2. 在主 NNMi 管理服务器上运行 ovstop 命令。
3. 在用作辅助服务器的含 Oracle 的服务器 2(辅助 NNMi 管理服务器)上，安装 NNMi。
4. 合并一台服务器上的密钥库，并将密钥库同时复制到主服务器和辅助服务器。有关详细信息，请参阅在应用程序故障转移环境中使用证书 (第 263 页)。

5. 在辅助 NNMi 管理服务器上启动 NNMi 服务。
6. 在用作辅助服务器的含 Oracle 的辅助 NNMi 管理服务器上安装所需的 NNM iSPI。

   备注: 确保输入与在主 NNMi 管理服务器上安装 NNM iSPI 时使用的 Web 服务客户端详细信息相同的内容。

7. 按为 NNMi 设置应用程序故障转移 (第 113 页)中所述配置应用程序故障转移。

   备注: 需要记住的是，您已经在执行此步骤期间合并了密钥库。配置应用程序故障转移期间，请跳过这些步骤。

集成应用程序

当其他 HP 软件或第三方产品与 NNMi 集成时，NNMi 应用程序故障转移对集成的影响取决于产品如何与 NNMi 通信。有关详细信息，请参阅相应的集成文档。

如果集成产品必须用有关 NNMi 管理服务器的信息配置，则应用以下信息：

- 如果是长期的，可更新集成产品配置中的 NNMi 管理服务器信息。有关详细信息，请参阅相应的集成文档。
- 如果停止看来是暂时的，则服务器 X 恢复工作后，可继续使用集成产品。要使服务器 X 恢复工作，请执行以下步骤：

1. 在服务器 X 上，运行以下命令：

   nnmcluster -daemon

   服务器 X 加入群集，并假定处于备用状态。
2. 在服务器 X 上，运行以下命令：

   nnmcluster -acquire

   服务器 X 变为活动状态。

如果预计原始服务器 X 将中断服务较长一段时间，则可以更新集成产品中的 NNMi 管理服务器 IP 地址。有关如何修改 IP 地址字段的说明，请参阅集成产品文档。

禁用应用程序故障转移

以下信息说明如何完全禁用应用程序故障转移。按以下指示完成操作，包括应用程序故障转移群集中配置的活动和备用 NNMi 管理服务器上的操作。

备注: 如果已购买 NNMi(单独)、NNMi Advanced 以及 NNMi 附带的 NNM iSPI NET 功能，则有两种类型的许可证适用于应用程序故障转移：

- 生产 - 不管您是否具有应用程序故障转移或高可用性环境，这是为 NNMi、NNMi Advanced 或 NNM iSPI NET 购买的主许可证。将此许可证与主服务器的 IP 地址关联。
- 非生产 - 此许可证是为用于应用程序故障转移环境而单独购买的。将此许可证与辅助(备用)服务器的 IP 地址关联。

如果您已购买 NNMi Premium 或 NNMi Ultimate，则需要使用从 HP 密码交付中心请求的适用于应用程序故障转移的一个或多个许可证密钥，而不要按照指示使用非生产许可证。获取两个许可证密钥；一个用于主服务器的物理 IP 地址，一个用于备用服务器的物理 IP 地址。

警告：不要在同一服务器上使用生产和非生产许可证。

还可以查看每个 NNM iSPI 的文档，该文档位于以下位置：http://h20230.www2.hp.com/selfsolve/manuals。

1. 在活动 NNMi 管理服务器上运行 **nnmcluster -enable** 命令。
2. 在活动 NNMi 管理服务器上运行 **nnmcluster -shutdown** 命令。
3. 等待几分钟，使旧的备用 NNMi 管理服务器成为新的活动 NNMi 管理服务器。
4. 在新的活动(旧的备用)NNMi 管理服务器上运行 **nnmcluster -display** 命令。
5. 在显示结果中搜索 ACTIVE_NNM_RUNNING 状态。重复步骤 4，直至看到 ACTIVE_NNM_RUNNING 状态。
6. 在新的活动(旧的备用)NNMi 管理服务器上运行 **nnmcluster -shutdown** 命令。
7. 在新的活动(旧的备用)NNMi 管理服务器上重复运行 **nnmcluster -display** 命令，直至看不到 DAEMON 进程。
8. 编辑在群集中配置的两个 NNMi 管理服务器的以下文件：
   - Windows：%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties
   - Linux：$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties
9. 在两个 NNMi 管理服务器上注释掉 com.hp.ov.nms.cluster.name 选项，并保存每个文件。
10. 在两个 NNMi 管理服务器上编辑以下文件：
    - Windows：%NnmDataDir%\shared\nnm\databases\Postgres\postgresql.conf
    - Linux：$NnmDataDir/shared/nnm/databases/Postgres/postgresql.conf
11. 删除以下行，这些行由应用程序故障转移自动添加。下面是这些行的可能外观的示例。这些行在您的服务器上的外观可能略有不同。

    ```
    # The following lines were added by the NNM cluster.
    archive_command = ...
    archive_timeout = 900
    max_wal_senders = 4
    archive_mode = 'on'
    wal_level = 'hot_standby'
    hot_standby = 'on'
    wal_keep_segments = 500
    listen_addresses = 'localhost,16.78.61.68'
    ```

    请务必保存更改。
12. 如果这些是 Windows NNMi 管理服务器，则导航到服务(本地)控制台，并在每个服务器上执

行以下操作：

a. 将 HP NNM Cluster Manager 的启动类型设置为禁用。

b. 将 HP OpenView Process Manager 的启动类型设置为自动。

13. 创建以下触发器文件，以告知 Postgres 停止以备用模式运行并开始完全运行：

    Windows：%NnmDataDir%\tmp\postgresTriggerFile

    Linux：$NnmDataDir/tmp/postgresTriggerFile

14. 只在以前的活动 NNMi 管理服务器上运行 **ovstart** 命令。在应用程序故障转移配置中，这是有永久 NNMi 许可证的 NNMi 管理服务器。

15. 如果在以前的备用服务器上使用非生产许可证。则不要在以前的备用 NNMi 管理服务器上运行 **ovstart** 命令。在应用程序故障转移配置中，这是有非生产许可证的 NNMi 管理服务器。要将此 NNMi 管理服务器作为独立服务器运行，必须购买并安装永久许可证。有关详细信息，请参阅许可 NNMi (第 252 页)。

16. 如果两个 NNMi 管理服务器都成功启动，则从备用和活动 NNMi 管理服务器删除以下目录：

    - Windows：%NnmDataDir%\shared\nnm\databases\Postgres_standby
    - Linux：$NnmDataDir/shared/nnm/databases/Postgres_standby

    > **备注:** 此目录是默认目录，并且是位于 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.archivedir 参数的值。这些说明假定您未更改此值。如果更改了 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.archivedir 参数的值，则删除等于新值的目录。

17. 从备用和活动 NNMi 管理服务器删除以下目录：

    - Windows：%NnmDataDir%\shared\nnm\databases\Postgres.OLD
    - Linux：$NnmDataDir/shared/nnm/databases/Postgres.OLD

管理任务和应用程序故障转移

以下信息说明执行管理任务(如打补丁和重新启动 NNMi 管理服务器)时，如何有效管理应用程序故障转移。

恢复 NNMi 故障转移环境

在一组不同的服务器上恢复 NNMi 故障转移环境需要获取 NNMi 活动系统和备用系统的备份，在所需服务器上恢复它们，还需要更改某些属性文件中的主机名。

要恢复 NNMi 故障转移环境，请执行以下步骤：

1. 在源故障转移环境中获取活动系统和备用系统上的所有 NNMi 数据的完整脱机备份。有关详细信息，请参阅备份 NNMi 数据 (第 197 页)。
2. 将备份文件分别复制到目标活动系统和备用系统。
3. 将 NNMi 安装到和备份所处相同的版本和补丁程序级别。
4. 在活动系统和备用系统上恢复 NNMi 数据。

- **嵌入式数据库**：使用 nnmrestore.ovpl 命令执行完整恢复。有关详细信息，请参阅备份和恢复策略 (第 201 页)。
- **Oracle 数据库**：使用类似于以下内容的恢复命令仅恢复系统文件。有关详细信息，请参阅只恢复文件系统文件 (第 202 页)。

  ```
  nnmrestore.ovpl -partial -source nnmi_backups\offline\<最新备份>
  ```

5. 在活动和备用 NNMi 管理服务器上，执行以下操作：
   a. 识别活动和备用 NNMi 管理服务器的主机名。
   b. 打开以下文件。
      - Windows：%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties
      - Linux：$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties
   c. 将活动和备用节点的主机名添加到 com.hp.ov.nms.cluster.member.hostnames 参数。

      ```
      com.hp.ov.nms.cluster.member.hostnames = fqdn_for_active, fqdn_for_standby
      ```
6. 配置 NNMi 故障转移环境以使用 SSL 证书进行安全通信。有关详细信息，请参阅管理证书 (第 255 页)。

应用程序故障转移和 NNMi 补丁程序

两个 NNMi 管理服务器必须运行相同的 NNMi 版本和补丁程序级别。要向活动和备用 NNMi 管理服务器添加补丁程序，请使用以下某个过程：

- 为应用程序故障转移应用补丁程序(关闭活动和备用服务器) (第 129 页)

  当您不在乎网络监视中断时，请使用此过程。
- 为应用程序故障转移应用补丁程序(保留一个活动 NNMi 管理服务器) (第 131 页)

  当您必须避免任何网络监视中断时，请使用此过程。

为应用程序故障转移应用补丁程序(关闭活动和备用服务器)

此过程会使两个 NNMi 管理服务器在打补丁过程中有一段时间处于非活动状态。要将补丁程序应用于配置了应用程序故障转移的 NNMi 管理服务器，请执行以下步骤：

1. 作为预防措施，继续前，请在活动和备用 NNMi 管理服务器上运行 **nnmconfigexport.ovpl** 脚本。有关信息，请参阅最佳实践：保存现有配置 (第 26 页)。
2. 作为预防措施，继续前，请在活动和备用 NNMi 管理服务器上备份 NNMi 数据。有关信息，请参阅备份范围 (第 197 页)。
3. 记录 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.name 属性值。安装补丁程序之后，您将需要此值。此文件位于以下位置：
   - Windows：%nnmDataDir%\shared\nnm\conf\props\nms-cluster.properties
   - Linux：$nnmDataDir/shared/nnm/conf/props/nms-cluster.properties
4. 作为预防措施，请在活动 NNMi 管理服务器上完成以下步骤：
   a. 运行 **nnmcluster** 命令。
   b. 仅嵌入式数据库：在 NNMi 提示之后，输入 **dbsync**，然后按 Enter。查看显示的信息，确保包含以下消息：

      ACTIVE_DB_BACKUP：这意味着活动 NNMi 管理服务器正在执行新备份。

      ACTIVE_NNM_RUNNING：这意味着活动 NNMi 管理服务器完成了上一条消息所指的备份。

STANDBY_READY：显示备用 NNMi 管理服务器的前一状态。

STANDBY_RECV_DBZIP：这意味着备用 NNMi 管理服务器正在从活动 NNMi 管理服务器接收新备份。

STANDBY_READY：这意味着备用 NNMi 管理服务器已准备好在活动 NNMi 管理服务器出现故障时执行工作。

5. 在活动 NNMi 管理服务器上运行 **nnmcluster -halt** 命令。该操作关闭活动和备用 NNMi 管理服务器上的所有 nnmcluster 进程。
6. 要验证两个服务器上都未运行 nnmcluster 节点，请在活动和备用 NNMi 管理服务器上完成以下步骤。
   a. 运行 **nnmcluster** 命令。
   b. 验证是否除了标记的节点 (SELF) 之外，不存在其他 nnmcluster 节点。
   c. 运行 **exit** 或 **quit** 以停止在步骤 a 中启动的交互 nnmcluster 进程。
7. 在活动 NNMi 管理服务器上，注释掉 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.name 参数。
   a. 编辑以下文件：
      - Windows：%NNM_SHARED_CONF%\props\nms-cluster.properties
      - Linux：$NNM_SHARED_CONF/props/nms-cluster.properties
   b. 注释掉 com.hp.ov.nms.cluster.name 参数。
   c. 保存更改。
8. 遵循 NNMi 补丁程序附带的说明将该补丁程序应用于活动 NNMi 管理服务器。
9. 在活动 NNMi 管理服务器上，取消 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.name 参数的注释。

   备注: 在补丁程序安装期间，com.hp.ov.nms.cluster.name 属性值将替换为 NNMi 默认值。取消包含 com.hp.ov.nms.cluster.name 参数的行的注释后，还需要将 com.hp.ov.nms.cluster.name 属性值替换为安装补丁程序前所配置的值。

   a. 编辑以下文件：
      - Windows：%NNM_SHARED_CONF%\props\nms-cluster.properties
      - Linux：$NNM_SHARED_CONF/props/nms-cluster.properties
   b. 在活动 NNMi 管理服务器上，取消 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.name 参数的注释。
   c. 将 com.hp.ov.nms.cluster.name 属性的默认值替换为安装补丁程序前在 nms-cluster.properties 中配置的名称。
   d. 保存更改。
10. 在活动 NNMi 管理服务器上运行 **ovstart** 命令。
11. 通过查看 NNMi 控制台中**帮助 > 系统信息**窗口的**产品**选项卡上的信息，验证在活动 NNMi 管理服务器上是否正确安装了补丁程序。
12. 运行 **nnmcluster -dbsync** 命令以创建新备份。
13. 在备用 NNMi 管理服务器上，如步骤 a 到步骤 c 中所示，注释掉 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.name 参数。
14. 向备用 NNMi 管理服务器应用 NNMi 补丁程序。

15. 在备用 NNMi 管理服务器上，如步骤 a 到步骤 c 中所示，取消 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.name 参数的注释并进行更新。
16. 在备用 NNMi 管理服务器上运行 **ovstart** 命令。
17. 如果安装了 NNM iSPI Performance for QA、NNM iSPI Performance for Metrics 或 NNM iSPI Performance for Traffic；正在使用应用程序故障转移功能；并完成了上述打补丁过程，则在活动和备用 NNMi 管理服务器上运行每个 NNM iSPI 的 NNM iSPI 支持脚本。

为应用程序故障转移应用补丁程序(保留一个活动 NNMi 管理服务器)

此过程会在打补丁过程中始终保留一个活动 NNMi 管理服务器。

> **备注:** 此进程会持续监视网络，但 NNMi 会丢失在此打补丁过程中发生的事务日志。

要将 NNMi 补丁程序应用于配置了应用程序故障转移的 NNMi 管理服务器，请执行以下步骤：

1. 作为预防措施，继续前，请在活动和备用 NNMi 管理服务器上运行 **nnmconfigexport.ovpl** 脚本。有关信息，请参阅最佳实践：保存现有配置 (第 26 页)。
2. 作为预防措施，继续前，请在活动和备用 NNMi 管理服务器上备份 NNMi 数据。有关信息，请参阅备份范围 (第 197 页)。
3. 记录 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.name 属性值。安装补丁程序之后，您将需要此值。此文件位于以下位置：

   Windows：%nnmDataDir%\shared\nnm\conf\props\nms-cluster.properties

   Linux：$nnmDataDir/shared/nnm/conf/props/nms-cluster.properties
4. 在其中一个节点上运行 **nnmcluster**。
5. 在上一个步骤中使用的 NNMi 管理服务器上输入 **dbsync** 以同步这两个数据库。

   > **备注:** **dbsync** 选项适用于使用嵌入式数据库的 NNMi 管理服务器。不要在配置为使用 Oracle 数据库的 NNMi 管理服务器上使用 **dbsync** 选项。
6. 等待活动 NNMi 管理服务器恢复到 ACTIVE_NNM_RUNNING，备用 NNMi 管理服务器恢复到 STANDBY_READY，然后再继续操作。
7. 从 **nnmcluster** 命令退出。
8. 通过在备用 NNMi 管理服务器上运行以下命令，在备用 NNMi 管理服务器上停止群集：**nnmcluster -shutdown**
9. 继续之前，确保以下进程和服务终止：
   - postgres
   - ovjboss
10. 继续之前，确保 nnmcluster 进程终止。如果 nnmcluster 进程未终止，请在必要的情况下手动终止 nnmcluster 进程。
11. 在备用 NNMi 管理服务器上编辑以下文件：

    Windows：%nnmDataDir%\shared\nnm\conf\props\nms-cluster.properties

    Linux：$nnmDataDir/shared/nnm/conf/props/nms-cluster.properties

12. 通过在行的最前面放置 #注释掉群集名称，然后保存更改：

    #com.hp.ov.nms.cluster.name = NNMicluster
13. 在备用 NNMi 管理服务器上安装 NNMi 补丁程序。
14. 此时，备用 NNMi 管理服务器已打补丁但停止，而活动 NNMi 管理服务器未打补丁但在运行。停止活动 NNMi 管理服务器，并立即使备用 NNMi 管理服务器联机以监视网络。
15. 通过在活动 NNMi 管理服务器上运行以下命令，在活动 NNMi 管理服务器上关闭群集：
    nnmcluster -halt
16. 确保 nnmcluster 进程终止。如果该进程在几分钟内都不会终止，请手动终止 nnmcluster 进程。
17. 在备用 NNMi 管理服务器上，取消 nms-cluster.properties 文件中的群集名称的注释。

    备注: 在补丁程序安装期间，com.hp.ov.nms.cluster.name 属性值将替换为 NNMi 默认值。取消包含 com.hp.ov.nms.cluster.name 参数的行的注释后，还需要将 com.hp.ov.nms.cluster.name 属性值替换为安装补丁程序前所配置的值。

    a. 编辑以下文件：
       - Windows：%NNM_SHARED_CONF%\props\nms-cluster.properties
       - Linux：$NNM_SHARED_CONF/props/nms-cluster.properties
    b. 在活动 NNMi 管理服务器上，取消 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.name 参数的注释。
    c. 将 com.hp.ov.nms.cluster.name 属性的默认值替换为安装补丁程序前在 nms-cluster.properties 中配置的名称。
    d. 保存更改。
18. 通过在备用 NNMi 管理服务器上运行以下命令，在备用 NNMi 管理服务器上启动群集：
    nnmcluster -daemon
19. 在活动 NNMi 管理服务器上安装 NNMi 补丁程序。
20. 此时，上一个活动 NNMi 管理服务器已打补丁但脱机。通过执行以下步骤，使其回到群集 (备用 NNMi 管理服务器)中：
    a. 在活动 NNMi 管理服务器上，取消 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.name 参数的注释。
    b. 将 com.hp.ov.nms.cluster.name 属性的默认值替换为安装补丁程序前在 nms-cluster.properties 中配置的名称。
    c. 使用以下命令启动活动 NNMi 管理服务器：
       nnmcluster -daemon
21. 要监视进度，请在活动和备用 NNMi 管理服务器上运行以下命令：

    nnmcluster

    等待上一个活动 NNMi 管理服务器完成从上一个备用 NNMi 管理服务器检索数据库的操作。
22. 在上一个活动 NNMi 管理服务器显示 STANDBY_READY 之后，在上一个活动 NNMi 管理服务器上运行以下命令：
    nnmcluster -acquire
23. 如果安装了 NNM iSPI Performance for QA、NNM iSPI Performance for Metrics 或 NNM iSPI Performance for Traffic；正在使用应用程序故障转移功能；并完成了上述打补丁过程，则在活动和备用 NNMi 管理服务器上运行每个 NNM iSPI 的 NNM iSPI 支持脚本。

应用程序故障转移和重新启动 NNMi 管理服务器

可以随时重新启动备用 NNMi 管理服务器，无需特殊说明。如果重新启动备用和活动 NNMi 管理服务器，请先重新启动活动 NNMi 管理服务器。

要重新启动活动或备用 NNMi 管理服务器，请执行以下操作。

1. 在 NNMi 管理服务器上运行 **nnmcluster -disable** 命令以禁用应用程序故障转移功能。
2. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。
3. 在 NNMi 管理服务器上运行 **nnmcluster -enable** 命令以启用应用程序故障转移功能。

> **备注:** 有关 NNMi 的 TrapReceiver 进程及其与故障转移的关系的重要信息，请参阅 NNMi NmsTrapReceiver 进程 (第 221 页)。

通信失败后的应用程序故障转移控制

在两个群集节点之间的通信故障得到解决之后，在发生通信故障之前运行时间最长的 NNMi 管理服务器(换句话说，上一个活动服务器)将指定为活动服务器。

应用程序故障转移和从以前的数据库备份恢复(仅嵌入式数据库)

活动和备用 NNMi 管理服务器配置了应用程序故障转移时，要从原始备份恢复 NNMi 数据库，请执行以下步骤：

1. 在活动 NNMi 管理服务器上运行 **nnmcluster -halt** 命令。
2. 在活动和备用 NNMi 管理服务器上删除或移动以下目录：
   - Windows：`%NnmDataDir%\shared\nnm\databases\Postgres_standby`
   - Linux：`$NnmDataDir/shared/nnm/databases/Postgres_standby`
3. 在活动 NNMi 管理服务器上恢复数据库：
   a. 修改以下文件以注释掉群集名称：
      - Windows：`%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
      - Linux：`$NnmDataDir/shared/nnm/conf/props\nms-cluster.properties`
   b. 将数据库恢复正常。请参阅恢复 NNMi 数据 (第 199 页)。
   c. 在活动 NNMi 管理服务器上运行 **ovstop** 命令。
   d. 修改以下文件以取消群集名称的注释：
      - Windows：`%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
      - Linux：`$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`
4. 在活动 NNMi 管理服务器上运行 **ovstart** 命令。
5. 等待活动 NNMi 管理服务器生成新备份。要验证此步骤是否已完成，请运行 **nnmcluster -display** 命令，并查找 `ACTIVE_NNM_RUNNING` 消息。

6. 在备用 NNMi 管理服务器上运行 **ovstart** 命令。备用 NNMi 管理服务器复制和解压缩新备份。要验证此步骤是否已完成，请运行 **nnmcluster -display** 命令，并查找 STANDBY_READY 消息。

群集文件传输警告配置

NNMi 应用程序故障转移功能会持续同步数据库文件和配置文件，即定期将这些文件从主服务器传输到备用服务器。网络传输问题可能会导致文件传输失败，以致于数据库变得不同步。

NNMi 会在内部跟踪自上次文件传输失败以来经过的时间，并在文件传输持续失败时在 NNMi 运行状况报告中生成运行状况警告。如下表所示，系统会为不同的超时持续时间生成不同的运行状况警告。您也可以根据自身要求重新配置这些持续时间。

生成运行状况警告的持续时间

运行状况警告级别	超时持续时间
轻微	15 分钟
重大	30 分钟
严重	45 分钟

要重新配置运行状况警告超时持续时间，请在 nms-cluster.properties 文件中取消对以下属性的注释并做出相应修改。

- #com.hp.ov.nms.cluster.timeout.filetransfer.MINOR = 15
- #com.hp.ov.nms.cluster.timeout.filetransfer.MAJOR = 30
- #com.hp.ov.nms.cluster.timeout.filetransfer.CRITICAL = 45

nms-cluster.properties 文件位于：

Windows：%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties

Linux：$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties

备注: 轻微、重大或严重对应的文件传输超时持续时间应：

- 大于目录扫描间隔
- 是目录扫描间隔的整数倍

例如，如果目录扫描间隔为 15 分钟，轻微、重大或严重警告对应的传输超时持续时间可以分别为 30 (15*2)、45 (15*3) 和 60 (15*4) 分钟。您可以在 nms-cluster.properties 文件中找到 com.hp.ov.nms.cluster.timeout.scandir 属性来确认目录扫描间隔。

有关访问和使用 NNMi 运行状况报告的信息，请参阅 NNMi 联机帮助。

网络延迟/带宽注意事项

NNMi 应用程序故障转移是通过在群集中的节点之间交换连续检测信号来实现的。它使用同一网络通道交换其他数据文件，如 NNMi 嵌入式数据库、数据库事务日志以及其他 NNMi 配置文件。通过 WAN(广域网)实现 NNMi 应用程序故障转移时， HP 建议使用高性能、低延迟的连接。

即使始终压缩此文件，NNMi 嵌入式数据库也可以变得很大，可增至 1GB 或更大。而且，在内置备份间隔(默认为 6 小时的配置参数)期间，NNMi 会生成成百上千条事务日志。每条事务日志可能有数 MB，最大可为 16 MB。(这些文件也经过压缩)。从 HP 测试环境采集的示例数据显示如下：

```
Number of nodes managed:15,000

Number of interfaces:100,000

Time to complete spiral discovery of all expected nodes:12 hours

Size of database:850MB (compressed)

During initial discovery:~10 transaction logs per minute (peak of ~15/min)

-----------------------------

10 TxLogs/minute X 12 hours = 7200 TxLogs @ ~10MB = ~72GB
```

对于通过网络发送，这是很大的数据量。如果两个节点之间的网络无法满足 NNMi 应用程序故障转移的带宽需要，则备用节点接收这些数据库文件时就可能延后。如果活动服务器出现故障，这可能增加潜在数据丢失的可能性。

同样，如果两个节点之间的网络有很高延迟或可靠性差，则可能在节点之间导致虚假检测信号丢失。例如，当检测信号不能及时响应且备用节点假定活动节点已发生故障时，就可能发生上述情况。检测到检测信号丢失涉及若干因素。只要网络能满足应用程序故障转移的数据传输需要，NNMi 即可避免虚假的故障转移通知。

HP 验证多子网 NNMi 应用程序故障转移时，活动和备用服务器在美国，一个在科罗拉多，另一个在休斯顿。这就提供了可接受的带宽和延迟，不会有虚假故障转移。

应用程序故障转移和 NNMi 嵌入式数据库

应用程序故障转移适用于 NNMi 10.01 的嵌入式和 Oracle 数据库。但是，对于 Oracle，数据库驻留在与任何 NNMi 管理服务器分开的服务器上，当配置 NNMi 以使用 Oracle 数据库时，不发生数据库复制。这会减少使用 Oracle 数据库进行应用程序故障转移的网络需要。相比于使用嵌入式数据库进行应用程序故障转移，使用 Oracle 进行应用程序故障转移只占用不到 1% 的网络需求量。此部分中包含的信息说明与使用嵌入式数据库进行应用程序故障转移相关的 NNMi 流量信息。

将 NNMi 配置为使用嵌入式数据库进行应用程序故障转移后，NNMi 执行以下操作：

1. 活动节点执行数据库备份，在单个 ZIP 文件中存储数据。
2. NNMi 将此 ZIP 文件跨网络发送到备用节点。
3. 备用节点展开 ZIP 文件，并将嵌入式数据库配置为首次启动时导入事务日志。
4. 主动节点上的嵌入式数据库根据数据库活动来生成事务日志。
5. 应用程序故障转移将事务日志跨网络发送到备用节点，它们会累积在磁盘上。
6. 当备用节点变为活动节点时，NNMi 会启动，且数据库跨网络导入所有事务日志。该操作需要的时间取决于文件数和这些文件中所存储信息的复杂性(某些文件与大小相近的其他文件相比导入时间更长)。
7. 备用节点导入所有事务日志之后，数据库变为可用，且备用节点启动剩余的 NNMi 进程。
8. 原始备用节点现在变为活动节点，并重新从步骤 1 开始。

应用程序故障转移环境中的网络流量

在应用程序故障转移环境中，NNMi 从活动节点将多个项跨网络传输到备用节点：

- 数据库活动：数据库备份，作为一个 ZIP 文件。
- 事务日志。
- 定期的检测信号，这样每个应用程序故障转移节点都能验证另一个节点是否仍在运行。
- 文件比较列表，这样备用节点可验证其文件与活动节点上的那些文件同步。
- 其他事件，如参数更改(启用/禁用故障转移等)，节点加入或退出群集。

前两项产生应用程序故障转移使用的网络流量的 99%。此部分更详细地介绍这两项。

数据库活动：NNMi 生成所有数据库活动的事务日志。数据库活动包含 NNMi 中的所有活动。该活动包括但不限于以下数据库活动：

- 发现新节点。
- 发现有关节点、接口、VLAN 及其他被管对象的属性。
- 状况轮询和状态更改。
- 事件和根源分析。
- NNMi 控制台中的操作员操作。

不在您控制范围内的数据库活动。例如，网络中断导致 NNMi 生成多个事件。这些事件触发网络上设备的状况轮询，导致 NNMi 中的设备状态更新。恢复中断时，其他节点启动事件导致进一步的状态更改。整个此活动都更新数据库中的条目。

尽管嵌入式数据库本身随数据库活动增长，但它会达到与您所在环境对应的稳定大小，以后只会随时间适度增长。

数据库事务日志：嵌入式数据库的工作方式为创建一个空的 16 MB 文件，然后将数据库事务信息写入该文件。NNMi 关闭该文件，在 15 分钟之后(或将 16 MB 数据写入该文件之后，以先发生的为准)使之可用于应用程序故障转移。这意味着，完全空闲的数据库将每 15 分钟生成一个事务日志文件，此文件实质是空的。应用程序故障转移会压缩所有事务日志，因此空的 16 MB 文件压缩到不足 1MB。满的 16MB 文件压缩到大约 8 MB。请记住，在数据库活动频繁时期，应用程序故障转移会在更短时间内生成更多的事务日志，因为每个文件会更快变满。

应用程序故障转移流量测试

以下测试平均每分钟约生成 2 个事务日志文件，每个文件的平均大小为 7 MB。这归因于每次故障转移事件增加的额外 5000 个节点的与发现相关的数据库活动。此测试用例中的数据库最后稳定在大约 1.1GB(按备份 ZIP 文件的大小测量)，有 31000 个节点和 960000 个接口。

测试方法：前 4 个小时内，测试人员用 5000 个节点作为 NNMi 的种子，并等待发现稳定下来。4 小时后，测试人员引发故障转移(备用节点变为活动节点，以前的活动节点变为备用节点)。故障转移后，测试人员立即添加大约 5000 多个节点，再等待 4 小时以使 NNMi 发现进程稳定，随后引发下一次故障转移(故障回复到以前的活动节点)。测试人员重复此周期若干次，使故障转移之间的时间有所变化(4 小时，然后 6 小时，然后再 2 小时)。每次故障转移事件后，测试人员都测量以下数据：

- 数据库备份 ZIP 文件(节点第一次变为活动时创建)的大小。
- 事务日志：文件总数和磁盘空间利用率。
- 在引发故障转移前一刻，NNMi 数据库中的节点数和接口数。
- 完成故障转移的时间。它包括从活动节点上运行初始 `ovstop` 命令到备用节点完全活动且 NNMi 开始运行的时间。

下表汇总了结果：

应用程序故障转移测试结果

小时	DB.zip 大小 (MB)	日志 Tx 日志	Tx 日志 (GB)	节点	接口	故障转移时间(分钟)
4	6.5	50	0.3	5,000	15,000	5
8	34	500	2.5	12,000	222,000	10
12	243	500	2.5	17,000	370,000	25
16	400	500	3.5	21,500	477,000	23
20	498	500	3.5	25,500	588,000	32
26	618	1100	7.5	30,600	776,000	30
28	840	400	2.2	30,600	791,000	31
30	887	500	2.5	30,700	800,000	16

观测结果：NNMi 将文件从活动节点传输到备用节点时，平均传输速率约为 5 GB/4 小时，连续吞吐量约为 350 KB/秒 (千字节每秒)或 2.8 MB/秒 (兆位每秒)。

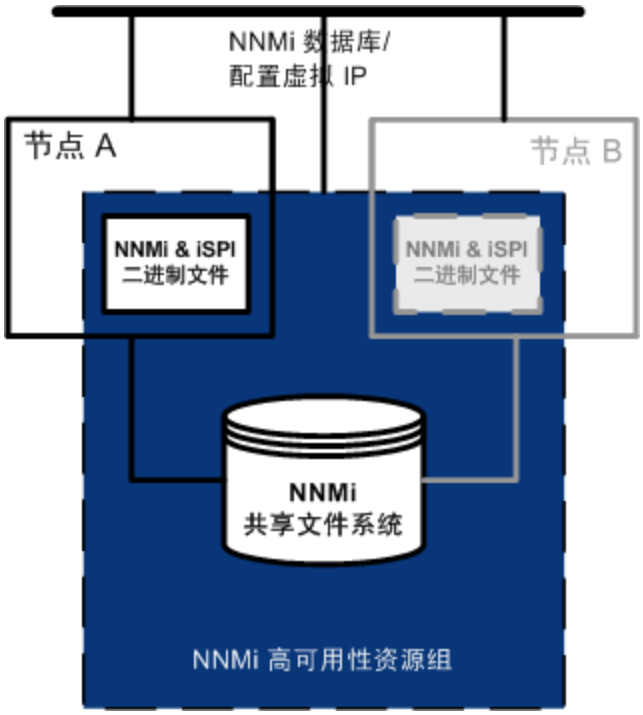
备注: 此数据不包括任何其他应用程序故障转移流量，比如检测信号、文件一致性检查或其他应用程序故障转移通信。此数据还排除了网络 I/O 的开销，比如包报头。此数据只包括每个文件的内容跨网络移动的实际网络负载。

备注: 由 NNMi 应用程序故障转移环境生成的流量有很大突发性。应用程序故障转移每五分钟识别一次活动节点上的新事务日志，并将这些日志发送到备用节点。根据网络速度的不同，备用节点应在短时间中接收所有新文件，因此在该 5 分钟间隔的剩余时间内网络相对空闲。

每次活动和备用节点交换角色(备用节点变为活动节点，活动节点变为备用节点)时，新的活动节点都将生成完整的数据库备份，并跨网络发送到新的备用节点。此数据库备份还会定期发生，默认情况下每 24 小时备份一次。每次 NNMi 生成新备份时，都将此备份发送到备用节点。拥有在备用节点上可用的这一新备份可减少故障转移时间，因为在该 24 小时间隔中 NNMi 生成的所有事务日志已在数据库中，不需要在故障转移时导入。

以上部分提供的信息将帮助您理解在将 NNMi 与使用嵌入式数据库的应用程序故障转移结合使用时，在故障转移之后网络可能如何运作。

在高可用性群集中配置 NNMi



高可用性 (HA) 是指在正在运行的配置的某个方面发生故障时实现不中断服务的硬件和软件配置。HA 群集定义了结合使用以确保发生故障转移时功能和数据的连续性的一组硬件和软件。

NNMi 支持将 NNMi 配置为在 HA 群集中若干单独购买的 HA 产品之一下运行。大多数 NNM Smart Plug-in (iSPI)(但不包括 NNM iSPI NET 诊断服务器)也可以 HA 运行。

备注: NNM iSPI NET 诊断服务器可以与 NNM iSPI NET 和 NNMi Ultimate 一起安装。

备注: 在高可用性群集中配置 NNMi 时，执行本章中包含的标准配置过程非常重要。不支持非标准配置。

本章提供用于配置 NNMi 在 HA 环境中运行的模板。本章不提供关于配置 HA 产品的端到端说明。NNMi 提供的 HA 配置命令是用于受支持 HA 产品的命令的相关包装程序。

备注: 使用 NNMi HA 命令确保为 NNMi 正确配置 HA。

提示: 如果计划在 NNMi 管理服务器上安装任何 NNM iSPI，另请参阅这些 NNM iSPI 的文档。

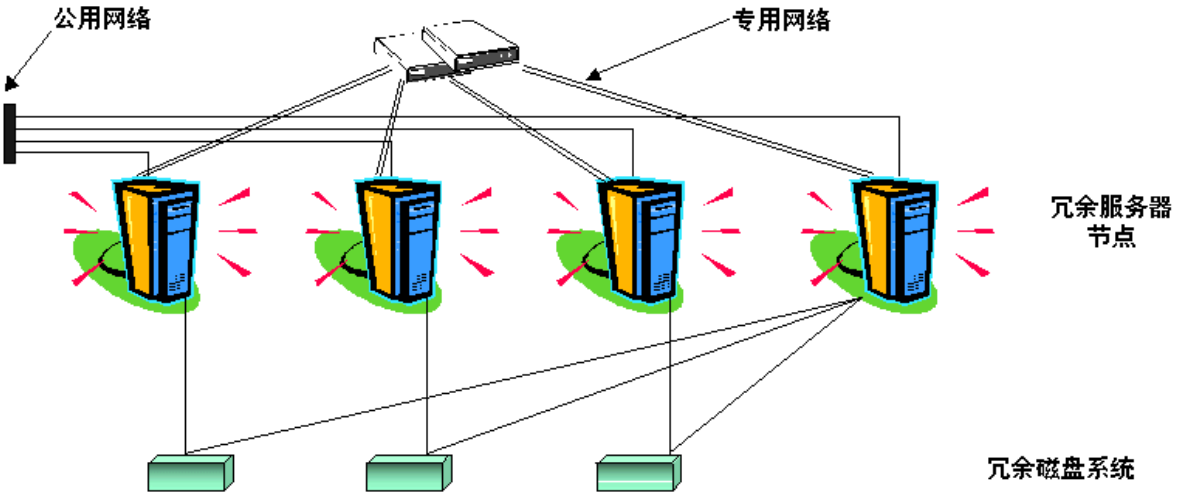
本章包含以下主题：

- 高可用性概念 (第 139 页)
- 验证配置 NNMi 以高可用性运行的先决条件 (第 145 页)
- 配置高可用性 (第 146 页)
- 高可用性环境中的共享 NNMi 数据 (第 158 页)
- 在高可用性群集中许可 NNMi (第 162 页)
- 维护高可用性配置 (第 163 页)
- 取消配置 HA 群集中的 NNMi (第 168 页)
- 对以 HA 运行的 NNMi 应用补丁程序 (第 170 页)
- HA 配置故障排除 (第 171 页)
- 高可用性配置参考 (第 179 页)

高可用性概念

群集体系结构为群集中的多个节点提供了单个全局一致的流程和资源管理视图。下图显示群集体系结构示例。

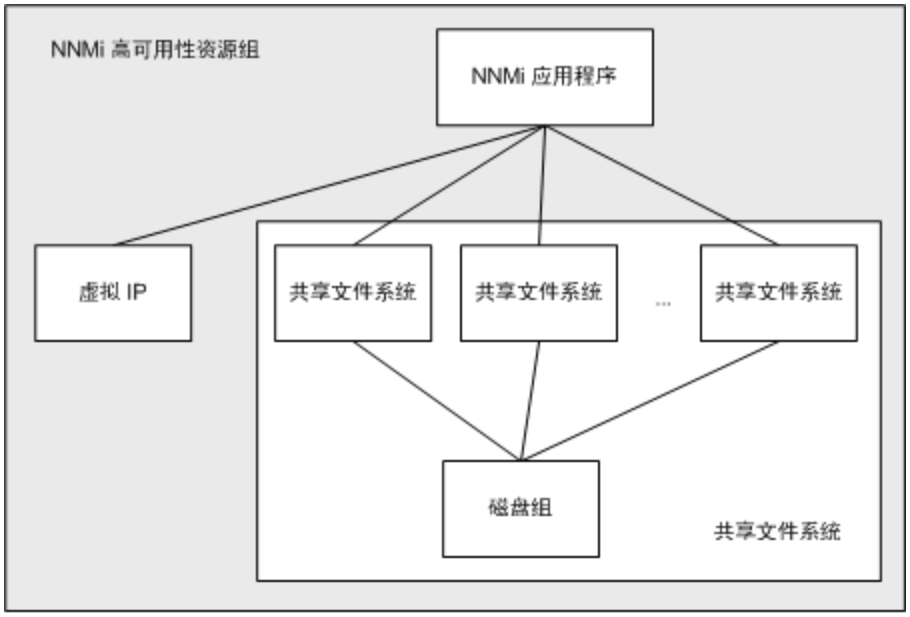
高可用性群集的体系结构



群集中的每个节点连接到一个或多个公共网络，并还连接到一个专用的互连网络，代表用于在群集节点之间传输数据的通信通道。

在当今的群集环境中，如 Veritas Cluster Server、Microsoft Failover Clustering 或 Microsoft 群集服务，应用程序表示为复合型资源，这些资源是使应用程序能够在群集环境中运行的简单操作。资源由 **HA 资源组**组成，它表示在群集环境中运行的应用程序。下图显示高可用性 (HA) 资源组示例。

典型高可用性资源组布局



此文档使用术语 HA 资源组指定任何群集环境中的一组资源。每个 HA 产品对 HA 资源组使用不同的名称。下表列出了每个受支持 HA 产品所用的等同于此文档中的 HA 资源组的术语。(有关每个 HA 产品的特定受支持版本，请参阅《NNMi Support Matrix》。)

受支持 HA 产品中用于 HA 资源组的术语

HA 产品	缩写	HA 资源组的等同术语
Windows Server Failover Clustering	WSFC	资源组
Veritas Cluster Server	VCS	服务组
Red Hat Cluster Suite	RHCS	服务

高可用性术语

下表列出并定义了一些常用高可用性 (HA) 术语。

常用 HA 术语

术语	描述
HA 资源组	在群集环境(在 HA 产品下)中运行的应用程序。HA 资源组可以同时是表示群集中应用程序的群集对象。
卷组	配置为形成单个大型存储区域的一个或多个磁盘驱动器。
逻辑卷	卷组中可以用作单独文件系统或设备交换空间的任意大小的空间。
主群集节点	安装软件产品的第一个系统，并且是配置 HA 的第一个系统。 将共享磁盘安装在主群集节点上以进行初始设置。

常用 HA 术语(续)

术语	描述
	主群集节点通常是第一个主动群集节点，但是您无需在 HA 配置完成之后保持这一主群集节点指定。当您下次更新 HA 配置时，另一个节点可能成为主群集节点。
辅助群集节点	在主群集节点针对 HA 进行了完全配置之后添加到 HA 配置的任何系统。
主动群集节点	当前正在运行 HA 资源组的系统。
被动群集节点	已针对 HA 作了配置但是当前未在运行 HA 资源组的任何系统。如果主动群集节点出现故障，则 HA 资源组故障转移到一个可用被动群集节点，该节点即成为该 HA 资源组的主动群集节点。

NNMi 高可用性群集场景

备注: NNMi 支持群集，应用程序可以在两个以上的群集节点上运行。有关详细信息，请参阅 nms-ha 联机帮助页和 nnmdatareplicator.ovpl 参考页或 Linux 联机帮助页。

对于 NNMi 高可用性 (HA) 配置，将成为 HA 资源组一部分的每个系统上都安装了 NNMi。NNMi 数据库安装在单独磁盘上，可由在每个系统上运行的 NNMi 程序访问。(在任何给定时间，只有一个系统即主动群集节点可访问共享磁盘。)

此方式对于嵌入式和第三方数据库解决方案有效。

备注: 仅在主动群集节点上运行 NNMi 数据库备份和恢复脚本。

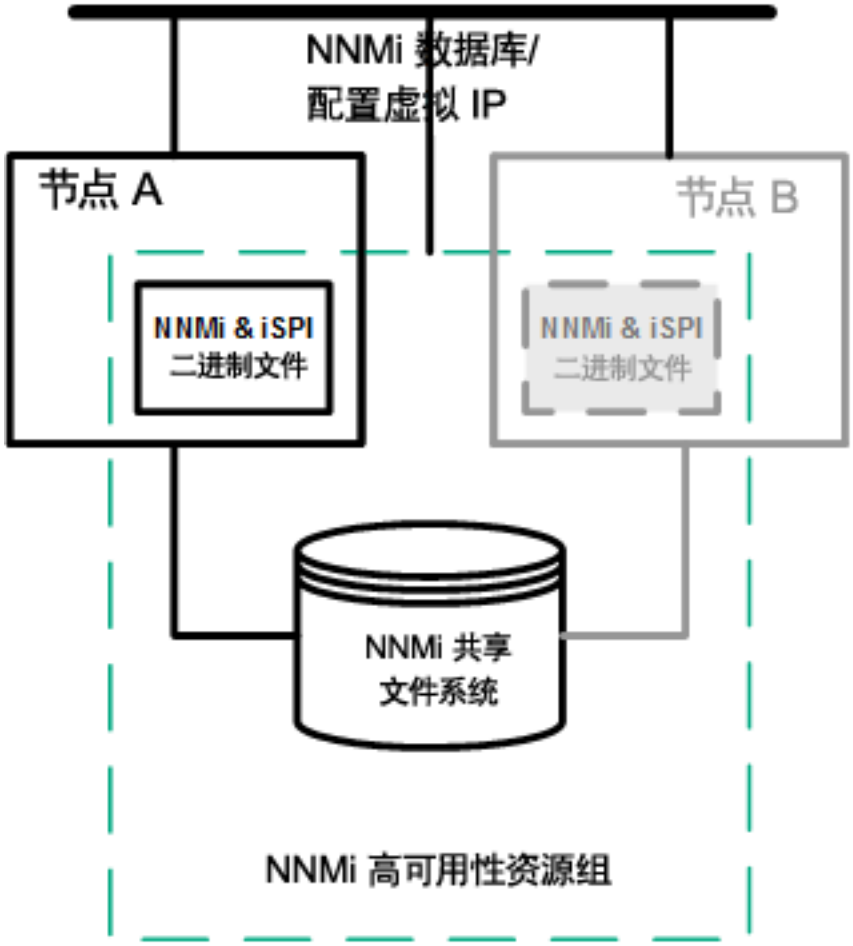
仅针对 NNMi 的场景

下图显示 NNMi HA 群集场景的图形表示。在此图中，NNMi HA 资源组与 NNMi HA 群集同义。

节点 A 和节点 B 都是完全安装的 NNMi 管理服务器，包含该系统上运行的 NNMi 程序以及任何 NNM iSPI。主动群集节点将访问共享磁盘以获取运行时数据。其他产品通过 HA 资源组的虚拟 IP 地址连接到 NNMi。

如果群集包含两个以上的 NNMi 节点，则按类似于下图中的节点 B 的方式配置其他节点。

NNMi HA 群集的基本场景

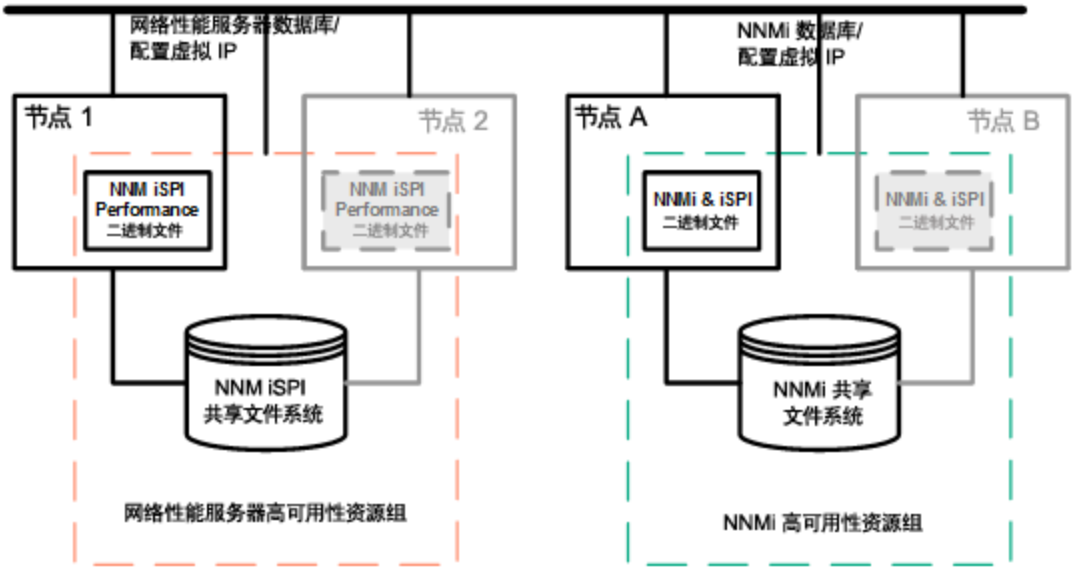


有关如何实施此场景的信息，请参阅配置 NNMi 以高可用性运行和配置 NNM iSPI 以高可用性运行。

NNMi 以及独立服务器场景上的 NNM Performance iSPI

如果正在独立服务器上运行任何 NNM Performance iSPI，则可以配置这些 NNM iSPI 作为 NNMi HA 群集中的单独 HA 资源组运行，如下图中所示。NNMi HA 资源组与仅针对 NNMi 的场景所述的情况相同。

独立服务器上 NNMi 和 NNM Performance iSPI 的 HA



有关如何实施此场景的信息，请参阅配置 NNMi 以高可用性运行和配置 NNM iSPI 以高可用性运行。

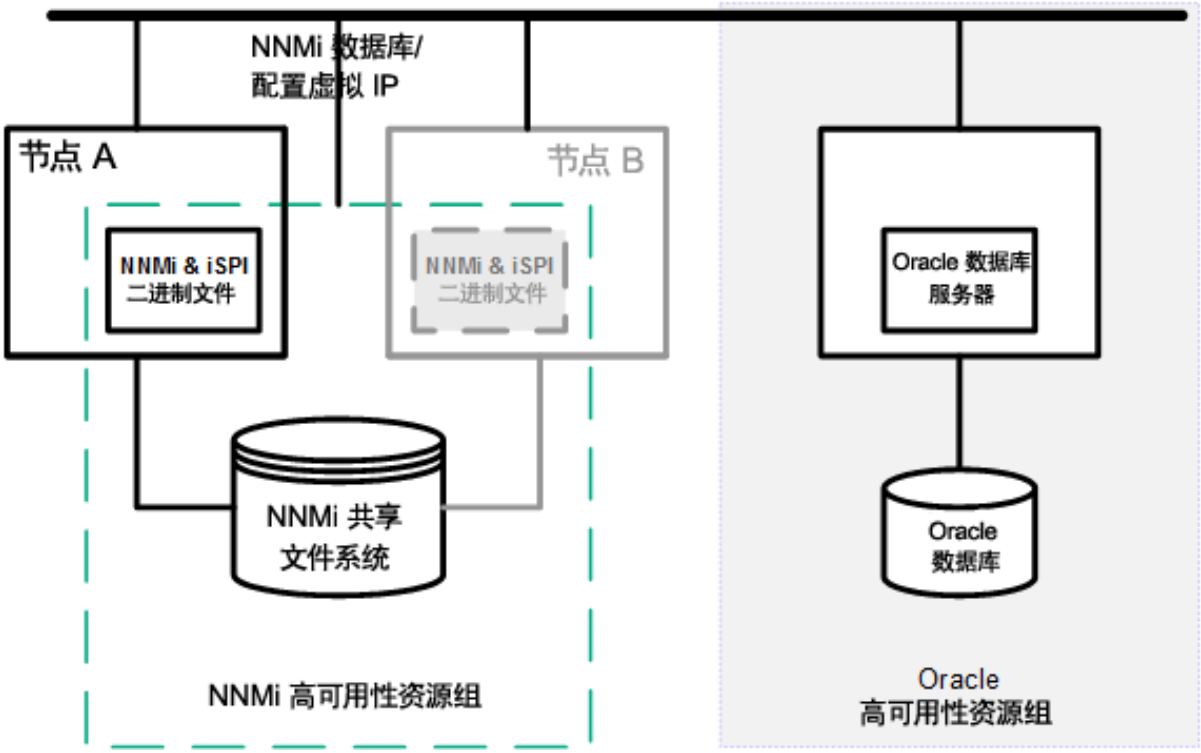
- 独立服务器上的 NNM Performance iSPI 的其他选项如下：
- 在没有 HA 的单个系统上运行 NNM Performance iSPI。评估 NNM iSPI 以及在不需要性能数据始终可用的环境中工作时，请使用此方式。
- 将 NNM Performance iSPI 配置为在不同于 NNMi 所用的 HA 群集下运行。在这种情况下，必须手动管理 NNMi 上 NNM Performance iSPI 的依赖性。

带 Oracle 数据库的 NNMi 场景

如果 NNMi 实现将 Oracle 用作主 NNMi 数据库，则出于性能原因，Oracle 数据库应当在独立服务器上，如下图中所示。因此，必须在 NNMi HA 群集中配置两个 HA 资源组：

- NNMi HA 资源组包含 NNMi 节点和共享磁盘，用于存放不存储于 Oracle 数据库中的 NNMi 数据。
- Oracle HA 资源组包含 Oracle 数据库服务器和数据库磁盘。

带 Oracle 数据库的 NNMi 的 HA

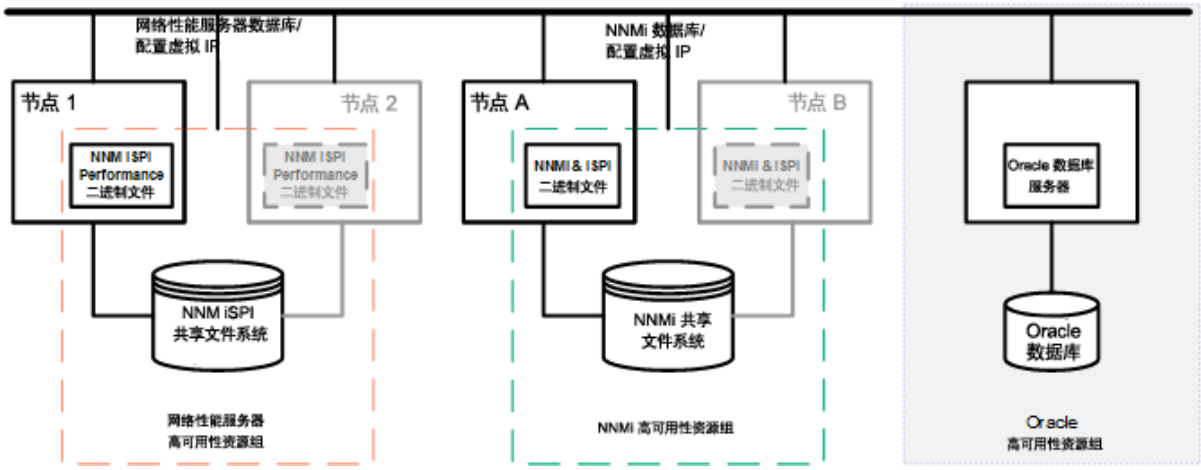


有关如何实施此场景的信息，请参阅在 Oracle 环境中配置 NNMi 以高可用性运行 (第 157 页)和配置 NNM iSPI 以高可用性运行 (第 156 页)。

带 Oracle 数据库的 NNMi 以及独立服务器场景上的 NNM Performance iSPI

如果 NNMi 实现将 Oracle 用作主 NNMi 数据库，并且正在独立服务器上运行任何 NNM Performance iSPI，则可以在 NNMi HA 群集中配置三个 HA 资源组，如下图中所示。

独立服务器上带 Oracle 数据库的 NNMi 和 NNM Performance iSPI 的 HA



有关如何实施此场景的信息，请参阅在 Oracle 环境中配置 NNMi 以高可用性运行 (第 157 页)和配置 NNM iSPI 以高可用性运行 (第 156 页)。

联机帮助页

NNMi 将提供以下联机帮助页，帮助您进行 NNMi 高可用性配置：

- nnm-ha
- nnmhaconfigure.ovpl
- nnmhaunconfigure.ovpl
- nnmhadisk.ovpl
- nnmhaclusterinfo.ovpl
- nnmhastartrg.ovpl
- nnmhastoprg.ovpl

在 Windows 操作系统上，这些联机帮助页是作为文本文件提供的。

验证配置 NNMi 以高可用性运行的先决条件

成功配置 NNMi 以高可用性 (HA) 运行取决于很多因素：

- 适当的硬件
- 对 HA 产品的了解
- 有条不紊的配置方法

开始配置 NNMi 以 HA 运行之前，需完成以下准备：

1. 通过检查《NNMi Support Matrix》中的信息，验证 NNMi 是否支持 HA 产品。
2. 阅读 HA 产品文档，熟悉该产品的功能，以进行设计决策。

   提示: HA 产品文档更改很频繁。确保有最近的版本可用。

3. 验证要作为节点包含在 NNMi HA 群集中的每个系统是否符合以下要求：
   - 符合 HA 产品文档中描述的所有要求。
   - 至少包括两个网络接口卡 (NIC 卡)。

     备注: 查看 HA 产品、操作系统和 NIC 卡文档以确定这些产品是否都兼容。

   - 支持使用 HA 资源组的虚拟 IP 地址。此 IP 地址是用于 NNMi 许可证的 IP 地址。

     备注: MSFC 需要多个虚拟 IP 地址，一个用于 HA 群集，每个 HA 资源组各对应一个虚拟 IP 地址。在这种情况下，NNMi HA 资源组的虚拟 IP 地址是用于 NNMi 许可证的 IP 地址。

   - 支持使用共享磁盘或磁盘阵列

     备注: 查看 HA 产品、操作系统和磁盘制造商文档以确定这些产品 (包括相关 SCSI 卡) 是否都兼容。

- 符合《NNMi Support Matrix》中所述的 NNMi 的所有要求。

4. 如果计划在 NNMi HA 群集中运行任何 NNM iSPI，请参阅有关其他 HA 配置先决条件的相应 NNM iSPI 文档。
5. 分配以下虚拟 IP 地址和主机名：
   - 对于 HA 群集，分配一个虚拟 IP 地址(仅 WSFC)
   - 对于每个要配置的 HA 资源组，分配一个虚拟 IP 地址
6. 从任何系统使用 `nslookup` 命令验证在步骤 5中分配的所有 IP 地址和主机名是否都有正确的 DNS 响应。
7. 验证每个系统的操作系统都有 HA 产品和 NNMi 的正确版本和补丁程序级别。
8. 如有必要，请安装 HA 产品。
9. 如在高可用性环境中手动准备共享磁盘 (第 160 页)中所述准备共享磁盘。
10. 对 HA 产品使用命令来配置(如有必要)和测试 HA 群集。

    HA 群集提供诸如检查应用程序检测信号和启动故障转移之类的功能。HA 群集配置必须至少包含以下各项：
    - (仅 Linux)ssh 和/或 remsh
    - (仅 Windows)可进行 DNS 解析的 HA 群集虚拟 IP 地址
    - HA 群集的可 DNS 解析的虚拟主机名
    - 唯一且特定于 NNMi 的资源组。

      备注: NNMi 期望 NNMi HA 资源组包括所有必需资源。否则，请使用 HA 产品功能来管理 NNMi HA 资源组与其他 HA 资源组之间的依赖性。例如，如果 Oracle 正在单独的 HA 资源组中运行，则配置 HA 产品以确保在 HA 产品启动 NNMi HA 资源组之前已完全启动 Oracle HA 资源组。
    - WSFC：使用 Failover Cluster Management for Windows Server 的群集创建向导。
    - VCS：不必要。产品安装已创建 HA 群集。
    - RHCS：添加 RHCS 文档中所述的服务(cman、rgmanager)。

    有关测试将放置到 NNMi HA 资源组中的资源的信息，请参阅HA 资源测试 (第 172 页)。

配置高可用性

本部分描述用于为 NNMi 执行新的高可用性 (HA) 配置的过程。它包含以下主题：

- 为高可用性配置 NNMi 证书 (第 147 页)
- 配置 NNMi 以高可用性运行 (第 147 页)
- 配置 NNM iSPI 以高可用性运行 (第 156 页)
- 在 Oracle 环境中配置 NNMi 以高可用性运行 (第 157 页)

备注: 配置 HA 时，请注意以下常规准则：

- RHCS 配置要求在 HA 群集中的每个节点上完全重新启动 HA 群集守护程序，包括所有应用程序。请相应地规划配置。
- 请勿使用 RHCS luci Web 界面更改 NNMi 资源组。如果对 NNMi 资源组进行了更改，luci Web 界面将从 /etc/cluster/cluster.conf 删除 NNMi 资源组全局变量。为使 NNMi HA 功能正常运行，需要 NNMi 资源组全局变量。
- 默认情况下，SNMP 源地址将在 HA 环境中设置为物理群集节点地址。要将 SNMP 源地址设置为 NNM_INTERFACE(已设置为虚拟 IP 地址)，必须编辑 ov.conf 文件并将 IGNORE_NNM_IF_FOR_SNMP 的值设置为 OFF。(默认情况下该值设置为 ON。)
- 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改时需要停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

为高可用性配置 NNMi 证书

NNMi 安装过程为 NNMi 控制台和 NNMi 数据库之间的安全通信配置自签名证书。配置 NNMi 以高可用性 (HA) 运行的过程在主群集节点和辅助群集节点之间正确共享了自签名证书。不需要执行任何额外步骤即可对以 HA 运行的 NNMi 使用默认证书。

如果要为 NNMi 通信使用其他自签名证书或证书颁发机构 (CA) 签署的证书，则必须执行某些额外操作。获取新证书之后，完成在高可用性环境中使用证书 (第 264 页)中所示的步骤。可以在配置 NNMi 以 HA 运行之前或之后完成此过程。

配置 NNMi 以高可用性运行

配置 NNMi 以高可用性 (HA) 运行的两个独立阶段如下：

1. 将 NNMi 数据文件复制到共享磁盘。
   - 在主节点上执行此任务，如在主群集节点上配置 NNMi (第 151 页)的步骤 1到步骤 9所述。
2. 配置 NNMi 以 HA 运行。
   - 在主节点上执行此任务，如在主群集节点上配置 NNMi (第 151 页)的步骤 10到步骤 15所述。
   - 在辅助节点上同样执行此任务，如在辅助群集节点上配置 NNMi (第 154 页)中所述。

将一个 HA 群集节点指定为主 NNMi 管理服务器。这是需要在大多数时间处于主动状态的节点。配置主节点，然后将 HA 群集中的所有其他节点配置为辅助节点。

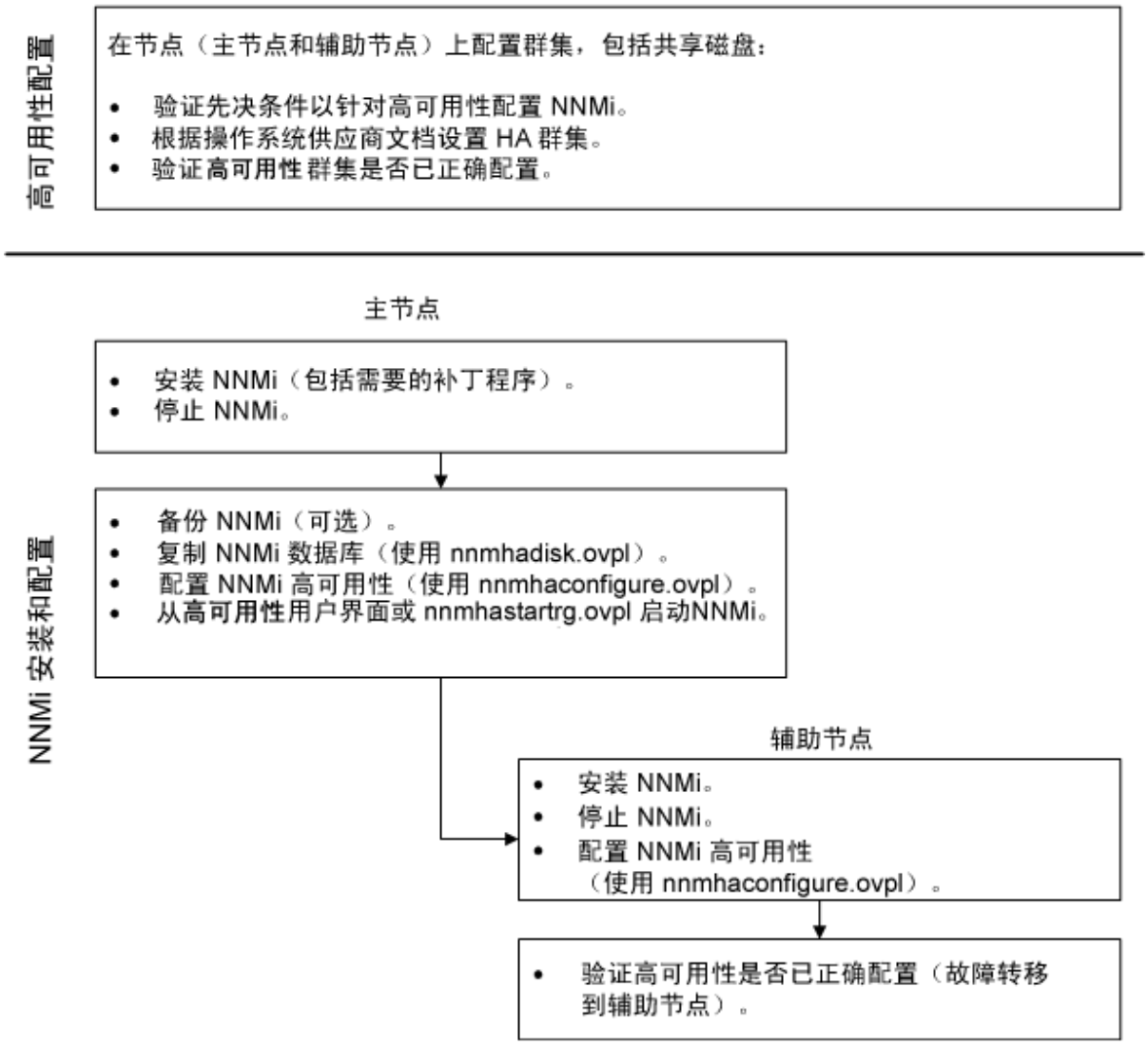
警告: 不能同时在多个群集节点上配置 NNMi 以 HA 运行。在一个群集节点上完成 HA 配置过程之后，在下一个节点上继续 HA 配置，以此类推，直到在群集环境中的所有节点上配置了以 HA 运行的 NNMi。

备注:

- 故障转移期间 NNMi 控制台无响应。故障转移完成之后，NNMi 用户必须登录才能继续其 NNMi 控制台会话。
- 有关 NNMi 的 TrapReceiver 进程及其与故障转移的关系的重要信息，请参阅 NNMi NmsTrapReceiver 进程 (第 221 页)。

下图提供了 NNMi HA 配置过程的图解。

NNMi HA 配置工作流程



备注: 如果在 HA 配置期间遇到错误，则执行以下操作：

1. 通过运行 `nnmhaunconfigure.ovpl` 命令，从 HA 环境取消配置 NNMi。
2. 更正由错误消息指示的状况。
3. 通过运行 `nnmhaconfigure.ovpl` 命令，将 NNMi 重新配置到 HA 环境中。

(仅 RHCS)为使 nnmhaconfigure.ovpl 和 nnmhaunconfigure.ovpl 命令正常运行，<failoverdomains/> 标记必须存在于 /etc/cluster/cluster.conf 文件中。

<failoverdomains/> 标记将嵌入到资源管理器部分，例如：

```
...
...
<rm>
 <failoverdomains/>
</rm>
```

nnmhaconfigure.ovpl 命令要求 <failoverdomains/> 标记使用以下示例结构创建 NNMi 资源组：

```
...
<rm>
  <failoverdomains>
    <failoverdomain name="<rg-name>-dom" nofailback="0"
ordered="0" restricted="1">
        <failoverdomainnode name="<node1>" priority="1"/>
        <failoverdomainnode name="<node2>" priority="1"/>
    </failoverdomain>
   </failoverdomains>
   <service autostart="1" domain="<rg-name>-dom"
exclusive="0" name="nnmha" recovery="relocate">
      <ip address="<addr>" monitor_link="1">
          <fs device="<nnmhalvol>" force_fsck="1"
force_unmount="1" fsid="" fstype="ext3"
mountpoint="<nnm-hamount>" name="nnmha-mount"
options="" self_fence="0">
          <NNMscript GLOBAL_VARIABLES="NNM_INTERFACE=
<virtual hostname>;HA_LOCALE=en_US.UTF-8;
HA_MOUNT_POINT=/<nnm-hamount>"
file="/var/opt/OV/hacluster/<rg-name>/nnmharhcs"
name="nnmha-APP"/>
          </fs>
     </ip>
```

```
  </service>
</rm>
```

nnmhaunconfigure.ovpl 命令还要求使用上述结构删除节点的 failoverdomain 条目。

有关详细信息，请参阅 nnmhaunconfigure.ovpl 和 nnmhaconfigure.ovpl 参考页或 Linux 联机帮助页。

NNMi 高可用性配置信息

高可用性 (HA) 配置脚本将采集有关 NNMi HA 资源组的信息。请先准备下表中列出的信息，然后再配置 NNMi HA。以交互方式执行 HA 脚本 (nnmhaconfigure.ovpl) 时需要此信息，具体取决于您的操作系统或 HA 软件。

NNMi HA 主节点配置信息

HA 配置项	描述
HA 资源组	包含 NNMi 的 HA 群集的资源组名称。此名称必须唯一、特定于 NNMi，且当前未使用。有关有效名称的信息，请参阅 HA 系统提供商的参考材料。 在输入 HA 资源组名称时，NNMi 会针对 Linux 和 Windows 系统生成以下资源： <资源组名称>-IP <资源组名称>-Mount <资源组名称>-App 此外，对于 Windows 系统，在输入虚拟主机名时还会生成以下资源： <虚拟主机名>
虚拟主机短名称	虚拟主机的短名称。此主机名必须映射到 HA 资源组的虚拟 IP 地址。nslookup 命令必须能够解析虚拟主机短名称和虚拟 IP 地址。 **备注:** 如果 NNMi 无法解析虚拟主机短名称或虚拟主机 IP 地址，则 HA 配置脚本可能会导致系统不稳定。因此，HP 建议您实施辅助命名策略(例如：在 Windows 操作系统的 %SystemRoot%\system32\drivers\etc\hosts 文件中或者在 UNIX 操作系统的 /etc/hosts 文件中输入信息)，以防在 NNMi HA 配置期间无法使用 DNS。
虚拟主机网络掩码	用于虚拟主机 IP 地址的子网掩码(必须是 IPv4 地址)。
虚拟主机网络接口	正在运行虚拟主机 IP 地址的网络接口。例如： • Windows：局域连接 • Linux：eth0

NNMi HA 主节点配置信息(续)

HA 配置项	描述
共享文件系统类型	用于 HA 资源组的共享磁盘配置的类型。可能值如下： • 磁盘 - 共享磁盘是使用标准文件系统类型的实际挂接的磁盘。HA 配置脚本可以配置共享磁盘。有关详细信息，请参阅此表中的文件系统类型条目。 • 无 - 共享磁盘使用磁盘选项所述以外的其他配置，例如 NFS。运行 HA 配置脚本之后，按在高可用性环境中手动准备共享磁盘 (第 160 页)中所述配置共享磁盘。
文件系统类型	(仅 Linux)共享磁盘(如果共享文件系统类型是磁盘)的文件系统类型。HA 配置脚本将此值传递到 HA 产品，以便它可以确定如何验证磁盘。 HP 已经测试以下共享磁盘格式： • Windows：基本(请参阅有关 Windows 服务器上的共享磁盘配置的说明 (第 162 页))；SAN • Linux：ext2、ext3 和 vxfs(用于 VCS 和 RHCS) **备注:** HA 产品支持其他文件系统类型。如果使用 HP 尚未测试的共享磁盘格式，则在运行 NNMi HA 配置脚本时，请先准备好磁盘，再将 NNMi 配置为以 HA 运行，然后将共享文件系统类型指定为无。
磁盘信息(磁盘组、卷组和/或逻辑卷名称，具体取决于所用的操作系统)	与 NNMi 共享文件系统的磁盘信息关联的名称。 **备注:** 当您在 UNIX 平台上创建/附加磁盘(例如，使用 vxfs 或 lvm)时，将创建不同的项，如磁盘组、卷组、逻辑卷。这些项的名称由系统管理员在创建时分配。NNMi 不强制实施任何命名约定。有关贵公司的命名信息，请与系统管理员联系。
安装点	用于安装 NNMi 共享磁盘的目录位置。此安装点必须在各个系统间保持一致。(即每个节点必须使用相同的安装点名称。)例如： • Windows：`S:\` **备注:** 请指定驱动器完整路径。`S` 和 `S:` 是不可接受的格式，不能用于访问共享磁盘。 • Linux：`/nnmmount`

在主群集节点上配置 NNMi

在主群集节点上完成以下过程。

备注: 如果要将 Oracle 用作主 NNMi 数据库，请先参阅在 Oracle 环境中配置 NNMi 以高可用性

运行 (第 157 页)。

1. 如果尚未执行此操作，请完成验证配置 NNMi 以高可用性运行的先决条件 (第 145 页)的过程。
2. 如果尚未满足要求，请安装 NNMi(包括可能已提供的最新合并补丁程序)，然后验证 NNMi 是否正常工作。
3. 如果希望在此 NNMi 管理服务器上运行任何 NNM iSPI，请先参阅配置 NNM iSPI 以高可用性运行 (第 156 页)，然后继续执行此过程。
4. 使用 `nnmbackup.ovpl` 命令或另一个数据库命令，备份所有 NNMi 数据。例如：

   ```
   nnmbackup.ovpl -type offline -scope all -target nnmi_backups
   ```

   有关此命令的详细信息，请参阅 NNMi 备份和恢复工具 (第 196 页)。
5. 定义磁盘设备组(和逻辑卷)，至少包括 NNMi HA 资源组的一个共享磁盘。例如：
   - WSFC：使用磁盘管理配置磁盘安装点并格式化磁盘。
   - VCS：

     使用 `vxdiskadm`、`vxassist` 和 `mkfs` 等 VSF 命令添加并初始化磁盘、按空间分配磁盘以及创建逻辑卷。
   - RHCS：

     使用 `pvcreate`、`vgcreate` 和 `lvcreate` 等 LVM 命令初始化磁盘，创建卷组和逻辑卷。

     备注: NNMi 需要将 RHCS 群集配置为满足以下条件：`/etc/cluster/cluster.conf` 文件中指定的群集节点名称必须完全能使 NNMi 正确启动和停止。

   对于 Linux 操作系统，参考网站如下：
   http://www.unixguide.net/unixguide.shtml
6. 创建目录安装点(例如，`S:\` 或 `/nnmmount`)，然后安装共享磁盘：
   - Windows：使用 Windows 资源管理器和磁盘管理工具来分配驱动器号。

     警告: 使用磁盘管理工具以确保共享磁盘显示为**联机**。如果显示为**已保留**，则表示 WSFC 已控制共享磁盘。从 WSFC 用户界面使用**删除**操作删除 WSFC 对共享磁盘的控制。还可以使用磁盘管理工具确认**保留**标志已更改为**联机**。
   - Linux：
     - 使用 `mkdir` 和 `mount` 命令。
     - 验证共享磁盘目录安装点是否已使用以下各项创建：用户为 `root`，组为 `sys`，并且权限设为 `755`。例如：

       ```
       ls -l /nnmmount
       ```

       警告: 配置之后，HA 产品就会管理磁盘安装。不要用此安装点更新文件系统表。
7. 停止 NNMi：

ovstop -c

> **备注:** 如果要包含在此 HA 资源组中的节点上已经安装 NNMi，则此时您还要在该节点上运行 ovstop -c。

8. 将 NNMi 数据库复制到共享磁盘：
   - Windows：

     %NnmInstallDir%\misc\nnm\ha\nnmhadisk.ovpl NNM -to <HA 安装点>

   - Linux：

     $NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM -to <HA 安装点>

> **备注:** 为防止数据库损坏，请仅运行此命令(带 -to 选项)一次。有关备选项的信息，请参阅在所有群集节点取消配置之后，对 NNMi 重新启用高可用性 (第 174 页)。

9. (仅 Linux)卸载共享磁盘，并取消激活磁盘组：

   umount <HA 安装点>

   vgchange -a n <磁盘组>

10. 验证 NNMi 是否未在运行：

    ovstop -c

11. (仅 RHCS)执行以下操作将必需的 NNM 脚本资源添加到 /usr/share/cluster/cluster.rng 文件中：
    a. 保存 cluster.rng 文件的副本。
    b. 编辑 /usr/share/cluster/cluster.rng 文件，如下所示：
       i. 找到 <define name="CHILDREN">。
       ii. 将文件 /opt/OV/misc/nnm/ha/NNMscript.rng 的内容嵌入到上一步中找到的语句前面。

           例如，转到 <define name="CHILDREN"> 的上一行并输入：

           ```
           :r /opt/OV/misc/nnm/ha/NNMscript.rng
           ```

       iii. 在 CHILDREN XML 块中，添加以下粗体文本：

           ```
           <define name="CHILDREN">
            <zeroOrMore>
             <choice>
                 …
                 <ref name="SCRIPT"/>
                 <ref name="NNMSCRIPT"/>
                 <ref name="NETFS"/>
           ```

       iv. 保存 cluster.rng 文件。

c. 将 /opt/OV/misc/nnm/ha/NNMscript.sh 文件复制到 /usr/share/cluster，并确保其具有 755 权限以及 root:root 所有权。

d. 重新启动 ccsd 服务或重新引导。

e. 如果在上一步中重新引导了系统，则在继续群集配置之前，请先停止 NNMi：

```
ovstop -c
```

f. 验证 NNMi 是否未在运行：

```
ovstatus -c
```

12. 配置 NNMi HA 资源组：

- Windows：

```
%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM
```

- Linux：

```
$NnmInstallDir/misc/nnm/ha/nnmhaconfigure.ovpl NNM
```

13. (仅 Linux)默认情况下，NNMi 在已运行 nnmhaconfigure.ovpl 命令的用户所在的语言环境中启动。要更改 NNMi 语言环境，请运行以下命令：

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -set HA_LOCALE <语言环境>
```

14. 在步骤 12 中，确定为共享文件系统类型指定的值：

- 对于类型磁盘，nnmhaconfigure.ovpl 命令已配置共享磁盘。继续执行步骤 15。
- 对于类型无，按在高可用性环境中手动准备共享磁盘 (第 160 页)中所述准备共享磁盘，然后继续执行步骤 15。

15. 启动 NNMi HA 资源组：

- Windows：

```
%NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM <资源组>
```

- Linux：

```
$NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM <资源组>
```

如果 NNMi 未正确启动，请参阅HA 配置故障排除 (第 171 页)。

警告: 现在 NNMi 正在以 HA 运行，对于正常操作，请不要使用 ovstart 和 ovstop 命令。仅当出于 HA 维护目的指示您这样做时，才使用这些命令。

在辅助群集节点上配置 NNMi

每次在一个辅助群集节点上完成以下过程。

1. 如果尚未执行此操作，请完成在主群集节点上配置 NNMi (第 151 页)的过程。
2. 如果尚未执行此操作，请完成验证配置 NNMi 以高可用性运行的先决条件 (第 145 页)的过程。

3. 如果尚未满足要求，请安装 NNMi(包括可能已提供的最新合并补丁程序)，然后验证 NNMi 是否正常工作。
4. 安装在主群集节点上配置 NNMi (第 151 页)的步骤 3 中所安装的 NNM iSPI。
5. 停止 NNMi：

   ovstop -c
6. 为共享磁盘创建安装点(例如，`S:\`或 `/nnmmount`)。

   > **备注:** 该安装点必须使用您在在主群集节点上配置 NNMi (第 151 页)过程的步骤 6 中创建的相同安装点名称。

7. (仅 RHCS)执行以下操作将必需的 NNM 脚本资源添加到 `/usr/share/cluster/cluster.rng` 文件中：
   a. 保存 `cluster.rng` 文件的副本。
   b. 编辑 `/usr/share/cluster/cluster.rng` 文件，如下所示：
      i. 找到 `<define name="CHILDREN">`
      ii. 将文件 `/opt/OV/misc/nnm/ha/NNMscript.rng` 的内容嵌入到上一步中找到的语句前面。

      例如，转到 `<define name="CHILDREN">` 的上一行并输入：

      ```
      :r /opt/OV/misc/nnm/ha/NNMscript.rng
      ```

      iii. 在 CHILDREN XML 块中，添加以下粗体文本：

      ```
      <define name="CHILDREN">
       <zeroOrMore>
        <choice>
              …
              <ref name="SCRIPT"/>
              <ref name="NNMSCRIPT"/>
              <ref name="NETFS"/>
      ```

      iv. 保存 `cluster.rng` 文件。
8. (仅 RHCS)将 NNMi 自定义脚本复制到位，然后重新启动 HA 群集守护程序。
   a. 将 `/opt/OV/misc/nnm/ha/NNMscript.sh` 文件复制到以下位置：

      `/usr/share/cluster/NNMscript.sh`
   b. 停止 `/sbin/ccsd` 进程，然后重新启动该进程。
9. 配置 NNMi HA 资源组：
   - Windows：**%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM**
   - Linux：**$NnmInstallDir/misc/nnm/ha/nnmhaconfigure.ovpl NNM**

   命令请求此信息时，提供 HA 资源组名称。
10. 验证配置是否已成功：

- Windows：

  ```
  %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl
  -group <资源组> -nodes
  ```

- Linux：

  ```
  $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl
  -group <资源组> -nodes
  ```

该命令输出列出所指定 HA 资源组的所有已配置节点。

11. (可选)测试配置，方法是使主节点上的 NNMi HA 资源组脱机，然后使辅助节点上的 NNMi HA 资源组联机。

配置 NNM iSPI 以高可用性运行

如果您希望在 NNMi 管理服务器上运行任何 NNM iSPI，请先阅读这一部分，然后配置 NNMi 以 HA 运行。

NNM iSPI Performance for Metrics、 NNM iSPI Performance for QA 和 NNM iSPI Performance for Traffic

NNM iSPI Performance for Metrics 可以安装在 NNMi 管理服务器或独立服务器上。

NNM iSPI Performance for Traffic 具有两个不同的组件(流量主组件和流量叶组件)，它们可以安装在 NNMi 管理服务器或独立服务器上，也可以混合安装在两者上(一个组件在 NNMi 管理服务器上，另一个组件在远程服务器上)。

备注:

- 如果 NNM iSPI(或组件)将安装在 NNMi 管理服务器上，请先安装该产品，然后配置 NNMi 以 HA 运行。
- 如果 NNM iSPI(或组件)将安装在独立服务器上，请先配置 NNMi 以 HA 运行，然后再安装该产品。在 NNM iSPI 安装期间，请提供 NNMi HA 资源组虚拟主机名作为 NNMi 管理服务器名称。

有关安装 NNM iSPI 的详细信息，请参阅相应的 NNM iSPI 安装指南。

NNM iSPI Performance for QA、 NNM iSPI for MPLS、 NNM iSPI for IP Multicast 和 NNM iSPI for IP Telephony

NNM iSPI Performance for QA、NNM iSPI for MPLS、NNM iSPI for IP Multicast 和 NNM iSPI for IP Telephony 只能安装在 NNMi 管理服务器上。

有关配置 NNM iSPI 以 HA 运行的信息，请参阅相应 NNM iSPI 的文档。

以 HA 运行的 NNM iSPI Network Engineering Toolset Software 和 NNMi

NNM iSPI Network Engineering Toolset Software SNMP 陷阱分析和 Microsoft Visio 导出功能随 NNMi Premium 或 NNMi Ultimate 产品自动安装。要使这些工具以 HA 运行，不需要执行额外的步骤。

NNM iSPI NET 诊断服务器不能包含在 NNMi HA 资源组中。不要在 NNMi 管理服务器上安装此组件。要在 NNMi HA 资源组以外的系统上运行 NNM iSPI NET 诊断服务器，请执行以下步骤：

备注: NNM iSPI NET 诊断服务器需要 NNM iSPI NET 或 NNMi Ultimate 许可证。有关如何安装和配置此服务器的信息，请参阅《HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide》。

1. 完整配置 NNMi HA 资源组。
2. 在 NNMi HA 资源组以外的系统上安装 NNM iSPI NET 诊断服务器。在 NNM iSPI NET 诊断服务器安装期间，提供 NNMi HA 资源组虚拟主机名作为 NNM 服务器主机名。

   有关详细信息，请参阅《NNM iSPI Network Engineering Toolset Software Planning and Installation Guide》。

如果在以 HA 运行的 NNMi 管理服务器上已经安装 NNM iSPI NET 诊断服务器，请先卸载 NNM iSPI NET 诊断服务器，然后配置 NNMi 以 HA 运行。

警告: 卸载 NNM iSPI NET 诊断服务器将删除所有现有报告。

备注: 保存现有报告也许可行(如此处所述)，但以下过程未经测试：

1. 使用 MySQL Workbench 执行现有 `nnminet` 数据库的备份。

   在 dev.mysql.com 的“downloads”(下载)区域中提供了 MySQL Workbench。
2. 卸载 NNM iSPI NET 诊断服务器。
3. 配置 NNMi 以 HA 运行。
4. 在单独的系统上安装 NNM iSPI NET 诊断服务器。
5. 运行任何流程之前，使用 MySQL Workbench 将 `nnminet` 数据库恢复到新安装的系统上。

在 Oracle 环境中配置 NNMi 以高可用性运行

本部分详细概述了配置带 Oracle 数据库的 NNMi 以高可用性 (HA) 运行的过程。

备注: 可用的 Oracle 配置很多，并且配置过程会根据 Oracle 版本而变化。有关配置 Oracle 以 HA 运行以及创建 NNMi 对于 Oracle HA 资源组的依赖性的最准确信息，请参阅 HA 产品文档。还可以转到 Oracle 网站 (www.oracle.com)，以了解有关 HA 产品的相应 Oracle 配置的信息。

高可用性环境中 NNMi 对 Oracle 的依懒性

Oracle 和 NNMi 都以高可用性 (HA) 运行时，NNMi HA 资源组必须包含未存储在 Oracle 数据库中的 NNMi 数据的共享磁盘。

此外，请考虑以下信息：

- 如果 HA 产品支持依赖性，则建议的方法是将每个产品配置为在单独的 HA 资源组中运行。Oracle HA 资源组必须在 NNMi HA 资源组启动之前完全启动。如果两个 HA 资源组在同一 HA 群集中，可以修改群集配置以设置资源组顺序。如果 HA 资源组在不同的 HA 群集中，确保符合 NNMi HA 资源组对于 Oracle HA 资源组的依赖性。
- 如果 HA 产品不支持依赖性，则在 NNMi HA 资源组中包括 Oracle 系统和 NNMi 系统。

在 Oracle 环境中配置 NNMi 以高可用性运行

1. 如果计划以高可用性 (HA) 运行 Oracle，则首先完成该配置。
2. 为 NNMi 创建空的 Oracle 数据库实例。
3. 在主 NNMi 节点上，安装 NNMi(包括可能已提供的最新合并补丁程序)。在安装期间，执行以下操作：
   a. 选择 **Oracle** 数据库类型，然后选择**主服务器安装**。
   b. 指定 Oracle HA 资源组(如果适用)的虚拟 IP 地址或主机名。
4. 在主 NNMi 节点上，配置 NNMi 以 HA 运行(如在主群集节点上配置 NNMi (第 151 页)中所述)。
5. 设置 NNMi 对于 Oracle HA 资源组的依赖性。

   有关具体说明，请参阅 HA 产品文档。
6. 在辅助 NNMi 节点上，安装 NNMi(包括可能已提供的最新合并补丁程序)。在安装期间，执行以下操作：
   - 选择 **Oracle** 数据库类型，然后选择**辅助服务器安装**。
   - 指定 Oracle HA 资源组(如果适用)的虚拟 IP 地址或主机名。
7. 在辅助 NNMi 节点上，配置 NNMi 以 HA 运行(如在辅助群集节点上配置 NNMi (第 154 页)中所述)。
8. 对于每个其他的辅助 NNMi 节点，重复步骤 6 和步骤 7。

高可用性环境中的共享 NNMi 数据

以高可用性 (HA) 运行的 NNMi 实现需要使用单独的磁盘以在 HA 群集中的所有 NNMi 节点之间共享文件。

> **备注:** 使用 Oracle 作为主数据库的 NNMi 实施还需要使用单独的磁盘以存放共享数据。

高可用性环境中 NNMi 共享磁盘上的数据

本部分列出当 NNMi 以高可用性 (HA) 运行时共享磁盘上维护的 NNMi 数据文件。

这些位置按以下方式映射到共享磁盘位置：

- Windows：
  - %NnmInstallDir% 映射到 %HA_MOUNT_POINT%\NNM\installDir
  - %NnmDataDir% 映射到 %HA_MOUNT_POINT%\NNM\dataDir
- Linux：
  - $NnmInstallDir 映射到 $HA_MOUNT_POINT/NNM/installDir
  - $NnmDataDir 映射到 $HA_MOUNT_POINT/NNM/dataDir

移动到共享磁盘的目录如下：

- Windows：
  - %NnmDataDir%\shared\nnm\databases\Postgres
    嵌入式数据库；使用 Oracle 数据库时不存在。
  - %NnmDataDir%\log\nnm
    NNMi 日志目录。
  - %NnmDataDir%\nmsas\NNM\log
    NNMi 审核日志目录。
  - %NnmDataDir%\nmsas\NNM\conf
    用于配置审核日志文件的 NNMi 目录。
  - %NnmDataDir%\nmsas\NNM\data
    由 ovjboss 使用的事务存储。
- Linux：
  - $NnmDataDir/shared/nnm/databases/Postgres
    嵌入式数据库；使用 Oracle 数据库时不存在。
  - $NnmDataDir/log/nnm
    NNMi 日志目录。
  - %NnmDataDir/nmsas/NNM/log
    NNMi 审核日志目录。
  - %NnmDataDir/nmsas/NNM/conf
    用于配置审核日志文件的 NNMi 目录。
  - $NnmDataDir/nmsas/NNM/data
    由 ovjboss 使用的事务存储。

nnmhadisk.ovpl 命令将向/从共享磁盘复制这些文件。按照本章指示运行此命令。有关此命令语法的摘要，请参阅 nnm-ha 联机帮助页。

在高可用性环境中复制配置文件

NNMi 高可用性 (HA) 实现使用文件复制在 HA 群集中的所有 NNMi 节点上维护 NNMi 配置文件的副本。

默认情况下，NNMi 管理文件复制，在故障转移过程中将 NNMi 配置文件从主动节点复制到被动节点。nnmdatareplicator.conf 文件指定包括在数据复制中的 NNMi 文件夹和文件。

禁用数据复制

可以按如下所示禁用数据复制：

1. 编辑以下文件：
   - Windows：%NnmDataDir%\shared\nnm\conf\ov.conf
   - Linux：$NnmDataDir/shared/nnm/conf/ov.conf
2. 包括以下行：

   DISABLE_REPLICATION=DoNotReplicate
3. 保存更改。

   备注: 当您更改活动节点上的文件(例如，配置文件)时，这些文件在进行故障转移时自动复制到备用节点。
4. 重新启动 NNMi 管理服务器：

   备注: 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改需要停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

   a. 在 NNMi 管理服务器上运行 ovstop 命令。
   b. 在 NNMi 管理服务器上运行 ovstart 命令。

在高可用性环境中手动准备共享磁盘

如果共享磁盘的格式受 HP 支持，则高可用性 (HA) 配置脚本将准备共享磁盘，您可以忽略本部分的内容。有关支持的磁盘格式的详细信息，请参阅NNMi 高可用性配置信息 (第 150 页)。

如果共享磁盘使用未经测试的配置(如 HA 产品支持的磁盘格式)，您必须手动准备磁盘。在 HA 配置期间对文件系统类型输入值无，然后配置共享磁盘和共享磁盘的 NNMi HA 资源组使用。

提示: 您可以在配置 NNMi HA 资源组之前或之后配置磁盘。

要手动准备共享磁盘，请执行以下步骤：

1. 如配置 SAN 或已实际连接的磁盘 (第 161 页)中所述配置共享磁盘。
2. 通过完成以下两个步骤，将 NNMi HA 资源组配置为能识别磁盘：
   - 在 ov.conf 文件中设置高可用性变量 (第 161 页)
   - 将共享磁盘移到 NNMi HA 资源组中 (第 162 页)

配置 SAN 或已实际连接的磁盘

连接磁盘并将磁盘格式化为 vxfs 或 ext3 文件系统。要配置 SAN 或已实际连接的磁盘，请执行以下步骤：

1. 验证共享磁盘是否未配置为在系统引导时安装。
   资源组负责监视共享磁盘。
2. 连接设备：
   - 对于 SAN 磁盘，将 SAN 设备添加到网络。
     SAN 磁盘上的逻辑卷应处于独占模式(如果该模式可用)。
   - 对于已实际连接的磁盘，使用 Y 电缆挂接磁盘。
3. 将操作系统条目添加到所有群集节点(磁盘组、逻辑卷、卷组和磁盘)：
   - 对于 SAN 磁盘，这些条目引用 SAN。
   - 对于已实际连接的磁盘，这些条目引用磁盘硬件。
4. 使用支持的磁盘格式对磁盘进行格式化。有关详细信息，请参阅NNMi 高可用性配置信息 (第 150 页)。
5. 确保 SAN 已安装。

   提示: 对于 Linux 系统，参考网站如下：**http://www.unixguide.net/unixguide.shtml**
6. 卸载并取出磁盘。
7. 要测试配置，请将磁盘添加到资源组并启动故障转移。

在 ov.conf 文件中设置高可用性变量

NNMi 高可用性 (HA) 资源组使用以下变量访问共享磁盘：

- `HA_POSTGRES_DIR=<HA 安装点>/NNM/dataDir/shared/nnm/databases/Postgres`
- `HA_EVENTDB_DIR=<HA 安装点>/NNM/dataDir/shared/nnm/eventdb`
- `HA_NNM_LOG_DIR=<HA 安装点>/NNM/dataDir/log`
- `HA_JBOSS_DATA_DIR=<HA 安装点>/NNM/dataDir/nmsas/NNM/data`
- `HA_MOUNT_POINT=<HA 安装点>`
- `HA_CUSTOMPOLLER_DIR=<HA 安装点>/NNM/dataDir/shared/nnm/databases/custompoller`

提示: 如果计划在 NNMi HA 资源组中运行任何 NNM iSPI，还要为那些 NNM iSPI 中的每一个设置 ov.conf 变量。有关详细信息，请参阅相应 NNM iSPI 的文档。

要在 `ov.conf` 文件中设置产品变量，以便访问共享磁盘，请为上面的每个变量运行以下命令：

- Windows：

  ```
  %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -set <变量> <值>
  ```
- Linux：

  ```
  $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -set <变量> <值>
  ```

备注: 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改需要停止并重新启动 NNMi 管理服务器，则在运行 `ovstop` 和 `ovstart` 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

将共享磁盘移到 NNMi HA 资源组中

按照产品文档修改磁盘配置文件，以将共享磁盘移动到 NNMi HA 资源组中。例如：

提示: 还可以使用此进程将其他资源(如 NIC 卡或备份磁盘)添加到 NNMi HA 资源组。

- WSFC：使用故障转移管理将资源添加到资源组。
- VCS：将磁盘条目和链接添加到 HA 配置文件中，方法是使用 `/opt/VRTSvcs/bin/hares` 命令。例如：
- RHCS：

  `/etc/cluster/cluster.conf`

有关 Windows 服务器上的共享磁盘配置的说明

备注: 根据 Microsoft 知识库文章 237853，具有 Windows Server 的群集不支持动态磁盘。

为确保正确配置磁盘，请查看位于以下网站上的信息：

- http://support.microsoft.com/kb/237853
- http://www.petri.co.il/difference_between_basic_and_dynamic_disks_in_windows_xp_2000_2003.htm

在高可用性群集中许可 NNMi

NNMi 需要以下两个许可证才能在高可用性 (HA) 群集中运行 NNMi：

- 一个与某个物理群集节点的 IP 地址锁定的生产许可证
- 一个与 NNMi HA 资源组的虚拟 IP 地址锁定的非生产许可证

NNMi 许可证密钥在共享磁盘上管理。因此，每个 NNMi HA 资源组对于每个单独许可的产品，只需要非生产许可证密钥。

在 HA 群集中许可 NNMi 时，必须使用主动节点上许可证文件的新信息更新共享磁盘上的 `licenses.txt` 文件。完成以下过程，以在 HA 群集中正确许可 NNMi。

- 如果您已购买 NNMi Premium 或 NNMi Ultimate，则需要使用从 HP 密码交付中心请求的适用于高可用性的一个或多个许可证密钥，而不要按照指示使用非生产许可证。获取 NNMi HA 资源组的虚拟 IP 地址的许可证密钥。此许可证密钥最初在主服务器上使用，然后根据需要在辅助服务器上使用。

警告: 不要在同一服务器上使用生产和非生产许可证。

要在 HA 群集中正确许可 NNMi，请在主动 NNMi 群集节点上执行以下步骤：

1. 如许可 NNMi (第 252 页)中所述为每个订购产品获取并安装永久许可证密钥。提示输入 NNMi 管理服务器的 IP 地址时，请提供 NNMi HA 资源组的虚拟 IP 地址。
2. 使用主动节点上 `LicFile.txt` 文件中的新信息更新共享磁盘上的 `licenses.txt` 文件。执行以下某项操作：
   - 如果 `licenses.txt` 文件存在于共享磁盘上的 `NNM` 目录中，则将主动节点上 `LicFile.txt` 中的新许可证密钥追加到共享磁盘上的 `licenses.txt`。
   - 如果共享磁盘上不存在 `licenses.txt` 文件，则将 `LicFile.txt` 从主动节点复制到共享磁盘上 `NNM` 目录中的 `licenses.txt`。

   在主动节点上，`LicFile.txt` 文件位于以下位置：
   - Windows：`%NnmDataDir%\shared\nnm\conf\licensing\LicFile.txt`
   - Linux：`$NnmiDataDir/shared/nnm/conf/licensing/LicFile.txt`

   在共享磁盘上，`licenses.txt` 文件的示例位置如下：
   - Windows：`S:\NNM\licenses.txt`
   - Linux：`/nnmount/NNM/licenses.txt`

维护高可用性配置

本部分描述如何执行以下高可用性配置维护任务：

维护模式 (第 163 页)

在 HA 群集中维护 NNMi (第 164 页)

在 NNMi HA 群集中维护加载项 NNM iSPI (第 167 页)

维护模式

需要将 NNMi 补丁程序或更新应用到 NNMi 的较新版本时，请将 NNMi HA 资源组置于维护模式，以防止在此过程中发生故障转移。NNMi HA 资源组处于维护模式时，您(或安装脚本)可以根据需要在主(主动)群集节点上运行 `ovstop` 和 `ovstart` 命令。

> **警告:** 不要在辅助(备份)群集节点上运行 `ovstart` 或 `ovstop` 命令。

将 HA 资源组置于维护模式

将 HA 资源组置于维护模式会禁用 HA 资源组监视。HA 资源组处于维护模式时，停止和启动该 HA 资源组中的产品不会导致故障转移。

要将 HA 资源组置于维护模式，请在主动群集节点上创建以下文件：

- Windows：`%NnmDataDir%\hacluster\<资源组>\maintenance`
- Linux：`$NnmDataDir/hacluster/<资源组>/maintenance`

备注: maintenance 文件的内容如下:

- 要禁用 HA 资源组的监视，请创建 maintenance 文件。该文件可以为空，也可以包含关键字 NORESTART。
- 为防止 NNMi 在配置过程中启动，maintenance 文件的第一行只能包含一个词: NORESTART

将 HA 资源组移出维护模式

将 HA 资源组移出维护模式会重新启用 HA 资源组监视。停止该 HA 资源组中的产品会导致该 HA 资源组故障转移到被动群集节点。

要将 HA 资源组移出维护模式，请执行以下步骤:

1. 验证 NNMi 是否在正确运行:

   ovstatus -c

   所有 NNMi 服务应当显示状况“RUNNING”。
2. 启动维护之前，从作为主动群集节点的节点删除 maintenance 文件。将 HA 资源组置于维护模式 (第 163 页)中描述了此文件。

在 HA 群集中维护 NNMi

本部分描述如何执行在高可用性 (HA) 群集中维护 NNMi 所需的以下任务。

启动和停止 NNMi (第 164 页)

在群集环境中更改 NNMi 主机名和 IP 地址 (第 164 页)

停止 NNMi 而不执行故障转移 (第 167 页)

在维护之后重新启动 NNMi (第 167 页)

启动和停止 NNMi

备注: NNMi 正以高可用性 (HA) 运行时，不要使用 ovstart 和 ovstop 命令，除非出于 HA 维护目的而指示您这样做。

为正常运行，请使用 NNMi 提供的 HA 命令或相应的 HA 产品命令来启动和停止 HA 资源组。

在群集环境中更改 NNMi 主机名和 IP 地址

群集环境中的节点可以有多个 IP 地址和主机名。如果节点成为另一个子网的成员，则可能需要更改其 IP 地址。因此，IP 地址或完全限定域名可能会更改。

例如，在 Linux 系统上，IP 地址和相关主机名通常是在以下某个文件中配置的:

- /etc/hosts
- 域名服务 (DNS)
- 网络信息服务 (NIS)

NNMi 还为 NNMi 数据库中的被管节点配置管理服务器的主机名和 IP 地址。

如果将要从非名称服务器环境移至名称服务器环境(即，DNS 或 BIND)，请确保名称服务器可以解析新 IP 地址。

在 IP 网络中可使用主机名标识被管节点。虽然节点可能有多个 IP 地址，但是可以使用主机名确定特定节点。系统主机名是使用 `hostname` 命令时返回的字符串。

更改 NNMi HA 资源组的虚拟主机名或 IP 地址时，必须使用主动节点上许可证文件的新信息更新共享磁盘上的 `licenses.txt` 文件。完成以下过程以正确更新 HA 配置。

要更改 NNMi HA 资源组的虚拟主机名或 IP 地址，请在主动 NNMi 群集节点上执行以下步骤：

备注: 如果已购买 NNMi(单独)、NNMi Advanced 以及 NNMi 附带的 NNM iSPI NET 功能，则有两种类型的许可证适用于应用程序故障转移和高可用性环境：

- 应用程序故障转移
  - 生产 - 不管您是否具有应用程序故障转移或高可用性环境，这是为 NNMi、NNMi Advanced 或 NNM iSPI NET 购买的主许可证。将此许可证与主服务器的 IP 地址关联。
  - 非生产 - 此许可证是为用于应用程序故障转移环境而单独购买的。将此许可证与辅助(备用)服务器的 IP 地址关联。

  高可用性 (HA)
  - 生产 - 不管您是否具有应用程序故障转移或高可用性环境，这是为 NNMi、NNMi Advanced 或 NNM iSPI NET 购买的主许可证。将此许可证与某个物理群集节点的 IP 地址关联。
  - 非生产 - 此许可证是为用于高可用性环境而单独购买的。将此许可证与 NNMi HA 资源组的虚拟 IP 地址关联。
- 如果您已购买 NNMi Premium 或 NNMi Ultimate，则需要使用从 HP 密码交付中心请求的适用于应用程序故障转移或高可用性的一个或多个许可证密钥，而不要按照指示使用非生产许可证。务必请求以下功能：
  - 高可用性：获取 NNMi HA 资源组的虚拟 IP 地址的许可证密钥。此许可证密钥最初在主服务器上使用，然后根据需要在辅助服务器上使用。
  - 应用程序故障转移：获取两个许可证密钥；一个用于主服务器的物理 IP 地址，一个用于备用服务器的物理 IP 地址。

  警告：不要在同一服务器上使用生产和非生产许可证。
- 还可以查看每个 NNM iSPI 的文档，该文档位于以下位置：http://h20230.www2.hp.com/selfsolve/manuals。

1. 将 NNMi HA 资源组的先前虚拟 IP 地址转换为 NNMi HA 资源组的新虚拟 IP 地址，并安装对应于此虚拟 IP 地址的许可证密钥。

   警告: 此时不要安装新的许可证密钥。

2. 将 NNMi HA 资源组置于维护模式(如将 HA 资源组置于维护模式 (第 163 页)中所述)。
3. 停止 NNMi HA 资源组：

- Windows：

  %NnmInstallDir%\misc\nnm\ha\nnmhastoprg.ovpl NNM <资源组>

- Linux：

  $NnmInstallDir/misc/nnm/ha/nnmhastoprg.ovpl NNM <资源组>

4. 更改 NNMi HA 资源组的 IP 地址或节点名称：
   a. 在 ov.conf 文件中，编辑要作为新主机名或 IP 地址的 NNM_INTERFACE 条目。
   b. 在 ovspmd.auth 文件中，编辑所有包含旧主机名的行以包含新主机名。

   在以下位置提供 ov.conf 和 ovspmd.auth 文件：

   - Windows：%NnmDataDir%\shared\nnm\conf
   - Linux：$NnmDataDir/shared/nnm/conf

5. 如果更改了 NNMi HA 资源组的节点名称，请使用 nnmsetofficialfqdn.ovpl 命令设置 NNMi 以使用 NNMi HA 资源组的新完全限定域名。例如：

   ```
   nnmsetofficialfqdn.ovpl newnnmi.servers.example.com
   ```

   有关详细信息，请参阅 nnmsetofficialfqdn.ovpl 参考页或 Linux 联机帮助页。

6. 更改群集配置以使用新 IP 地址：
   - WSFC：

     在 Failover Cluster Management 中，打开 **<资源组>**。

     双击 **<资源组>-ip**，选择**参数**，然后输入新 IP 地址。

   - VCS：

     $NnmInstallDir/misc/nnm/ha/nnmhargconfigure.ovpl NNM <资源组> -set_value <资源组>-ip
     Address <新 IP 地址>

   - RHCS：

     在主动 HA 群集节点上，编辑 /etc/cluster/cluster.conf 文件，以将 ip address="<旧 IP 地址>" 替换为 ip address="<新 IP 地址>"。然后运行 ccs_tool update /etc/cluster/cluster.conf 更新所有其他系统。

7. 如许可 NNMi (第 252 页)中所述安装 NNMi HA 资源组的新虚拟 IP 地址的许可证密钥。
8. 使用主动节点上 LicFile.txt 文件中的新信息更新共享磁盘上的 licenses.txt 文件。执行以下某项操作：
   - 如果 licenses.txt 文件存在于共享磁盘上的 NNM 目录中，则将主动节点上 LicFile.txt 中的新许可证密钥追加到共享磁盘上的 licenses.txt。
   - 如果共享磁盘上不存在 licenses.txt 文件，则将 LicFile.txt 从主动节点复制到共享磁盘上 NNM 目录中的 licenses.txt。

   在主动节点上，LicFile.txt 文件位于以下位置：

- Windows：`%NnmDataDir%\shared\nnm\conf\licensing\LicFile.txt`
- Linux：`$NnmDataDir/shared/nnm/conf/licensing/LicFile.txt`

在共享磁盘上，`licenses.txt` 文件的示例位置如下：

- Windows：`S:\NNM\licenses.txt`
- Linux：`/nnmount/NNM/licenses.txt`

9. 启动 NNMi HA 资源组：
   - Windows：

     %NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM <资源组>

   - Linux：

     $NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM <资源组>

10. 验证 NNMi 是否正确启动：

    ovstatus -c

    所有 NNMi 服务应当显示状况“RUNNING”。
11. 使 NNMi HA 资源组脱离维护模式(如将 HA 资源组移出维护模式 (第 164 页)中所述)。

停止 NNMi 而不执行故障转移

需要执行 NNMi 维护时，可以在主动群集节点上停止 NNMi，而不故障转移到当前被动节点。

在主动群集节点上执行以下步骤：

1. 将 NNMi HA 资源组置于维护模式(如将 HA 资源组置于维护模式 (第 163 页)中所述)。
2. 停止 NNMi：

   ovstop -c

在维护之后重新启动 NNMi

如果已采用阻止故障转移的方式停止 NNMi，则执行以下步骤以重新启动 NNMi 和 HA 监视：

1. 启动 NNMi：

   ovstart -c
2. 验证 NNMi 是否正确启动：

   ovstatus -c

   所有 NNMi 服务应当显示状况“RUNNING”。
3. 使 NNMi HA 资源组脱离维护模式(如将 HA 资源组移出维护模式 (第 164 页)中所述)。

在 NNMi HA 群集中维护加载项 NNM iSPI

NNM iSPI 紧密链接到 NNMi。在 NNMi HA 群集中的节点上安装加载项 NNM iSPI 时，请使用 NNMi HA 群集维护过程的书面指示。

取消配置 HA 群集中的 NNMi

从高可用性 (HA) 群集删除 NNMi 节点的过程包括撤消该 NNMi 实例的 HA 配置。然后可以将该 NNMi 实例作为独立管理服务器运行，也可以从该节点卸载 NNMi。

> **备注:** 卸载 NNMi 之前，以相反顺序删除所有 NNMi 补丁程序，从最新的补丁程序开始。补丁程序删除过程会因 NNMi 管理服务器上运行的操作系统而异。有关安装和删除说明，请参阅补丁程序文档。

如果要保留 NNMi 的高可用性配置，HA 群集必须包含一个主动运行 NNMi 的节点以及至少一个被动 NNMi 节点。如果要从 HA 群集完全删除 NNMi，请在该群集中的所有节点上取消配置 HA 功能。

要完全取消配置 HA 群集中的 NNMi，请执行以下步骤：

1. 确定该 HA 群集中哪个节点是主动节点。在任何节点上，运行以下命令：
   - Windows：

     ```
     %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -group <资源组> -activeNode
     ```

   - Linux：

     ```
     $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -group <资源组> -activeNode
     ```

2. 在每个被动节点上，从 HA 群集中取消配置任何加载项 NNM iSPI。

   有关信息，请参阅每个 NNM iSPI 的文档。
3. 在 HA 群集中的任何节点上，验证所有被动节点上的加载项 NNM iSPI 是否已在 HA 群集中取消配置：
   - Windows：

     ```
     %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_
     PRODUCTS
     ```

   - Linux：

     ```
     $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_
     PRODUCTS
     ```

   命令输出以 `<iSPI PM 名称>[主机名列表]` 格式列出加载项 iSPI 配置。例如：

   ```
   PerfSPIHA[hostname1, hostname2]
   ```

   这时，输出中应该只有主动节点主机名。如果被动节点主机名出现在输出中，则重复步骤 2，直到此命令输出仅包含主动节点主机名。
4. 在主动节点上，从 HA 群集中取消配置任何加载项 NNM iSPI。

   有关信息，请参阅每个 NNM iSPI 的文档。在 HA 群集中的任何节点上，验证所有节点上的加载项 NNM iSPI 是否已在 HA 群集中取消配置：
   - Windows：

     ```
     %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_
     PRODUCTS
     ```

- Linux：

  $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS

如果任何主机名出现在输出中，则重复步骤 6，直到此命令输出指示未配置任何 iSPI。

5. 在每个被动节点上，从 HA 群集中取消配置 NNMi：
   - Windows：

     %NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM <资源组>

   - Linux：

     $NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM <资源组>

     此命令删除对共享磁盘的访问，但不取消配置磁盘组或卷组。

6. 在每个被动节点上，将特定于 NNMi HA 资源组的文件移到单独的位置以便安全地保存：%NnmDataDir%\hacluster\<资源组>\ 文件夹。

   提示: 如果未计划重新配置 NNMi HA 资源组，则无需保存这些文件的副本。

7. 在主动节点上，停止 NNMi HA 资源组：
   - Windows：

     %NnmInstallDir%\misc\nnm\ha\nnmhastoprg.ovpl NNM <资源组>

   - Linux：

     $NnmInstallDir/misc/nnm/ha/nnmhastoprg.ovpl NNM <资源组>

   此命令不会除去对共享磁盘的访问。它也不会取消配置磁盘组或卷组。

8. 在主动节点上，取消配置 HA 群集中的 NNMi：
   - Windows：

     %NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM <资源组>

   - Linux：

     $NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM <资源组>

   此命令删除对共享磁盘的访问，但不取消配置磁盘组或卷组。

9. 在每个主动节点上，将特定于 NNMi HA 资源组的文件移到单独的位置以便安全地保存：%NnmDataDir%\hacluster\<资源组>\ 文件夹

   提示: 如果未计划重新配置 NNMi HA 资源组，则无需保存这些文件的副本。

10. 卸载共享磁盘。
    - 如果需要在某个时候重新配置 NNMi HA 群集，可以使磁盘保持当前状况。
    - 如果要将共享磁盘用于其他用途，请复制要保留的所有数据(如不以 HA 运行带现有数据库的 NNMi (第 170 页)中所述)，然后使用 HA 产品命令取消配置磁盘组和卷组。

不以 HA 运行带现有数据库的 NNMi

如果要在带有现有数据库的任何节点上不以 HA 运行 NNMi，请执行以下步骤：

1. 在主动节点(如果仍有一个存在)上，确保 NNMi 未在运行：

   ovstop

   或者，通过使用任务管理器 (Windows) 或 ps 命令 (Linux)，检查 ovspmd 进程的状态。
2. 在当前节点(不以 HA 运行 NNMi 的节点)上，验证 NNMi 是否未在运行：

   ovstop

   > **警告:** 要防止数据损坏，请确保没有任何 NNMi 实例正在运行和访问共享磁盘。

3. (仅 Linux)激活磁盘组，例如：

   vgchange -a e <磁盘组>
4. 使用相应的操作系统命令安装共享磁盘。例如：
   - Windows：使用“服务器管理器 -> 磁盘管理”。
   - Linux：`mount /dev/vgnnm/lvnnm /nnmmount`
5. 将 NNMi 文件从共享磁盘复制到本地磁盘：
   - Windows：

     %NnmInstallDir%\misc\nnm\ha\nnmhadisk.ovpl NNM -from <HA 安装点>
   - Linux：

     $NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM -from <HA 安装点>
6. 使用相应的操作系统命令卸载共享磁盘。例如：
   - Windows：使用 Windows 资源管理器。
   - Linux：`umount /nnmmount`
7. (仅 Linux)取消激活磁盘组，例如：

   vgchange -a n <磁盘组>
8. 如许可 NNMi (第 252 页)中所述，获取并安装此 NNMi 管理服务器的物理 IP 地址的永久生产许可证密钥。
9. 启动 NNMi：

   ovstart -c

   NNMi 现正运行先前由 NNMi HA 资源组使用的数据库的副本。手动从 NNMi 配置中除去不想通过此 NNMi 管理服务器管理的任何节点。

对以 HA 运行的 NNMi 应用补丁程序

要对 NNMi 应用补丁程序，请在高可用性 (HA) 维护模式中工作。请执行以下步骤：

1. 确定 HA 群集中的哪个节点是主动节点：
   - Windows：

     %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -group <资源组> -activeNode

   - Linux：

     $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -group <资源组> -activeNode

2. 在每个被动节点上，将 NNMi HA 资源组置于维护模式(如将 HA 资源组置于维护模式 (第 163 页)中所述)。

   包括 NORESTART 关键字。
3. 在每个被动节点上，应用相应的补丁程序。

   警告: 不要在辅助(备份)群集节点上运行 ovstart 或 ovstop 命令。

4. 在所有被动节点上，将 NNMi HA 资源组移出维护模式(如将 HA 资源组移出维护模式 (第 164 页)中所述)。
5. 故障转移到被动节点。
6. 转到之前处于活动状态(步骤 1 中)的节点，然后执行以下步骤：
   a. 将节点的 NNMi HA 资源组置于维护模式(如将 HA 资源组置于维护模式 (第 163 页)中所述)。

      包括 NORESTART 关键字。
   b. 在节点上应用相应的补丁程序。

      警告: 不要在辅助(备份)群集节点上运行 ovstart 或 ovstop 命令。

   c. 在节点上，将 NNMi HA 资源组移出维护模式(如将 HA 资源组移出维护模式 (第 164 页)中所述)。

HA 配置故障排除

本部分包括以下主题：

- 常见高可用性配置错误 (第 171 页)
- RHCS 6 的配置问题 (第 172 页)
- HA 资源测试 (第 172 页)
- 常规 HA 故障排除 (第 177 页)
- 特定于 NNMi 的高可用性故障排除 (第 173 页)
- 特定于 NNM iSPI 的高可用性故障排除 (第 179 页)

常见高可用性配置错误

以下列出了某些常见的高可用性 (HA) 配置错误：

- 磁盘配置不正确
  - VCS：如果探测不到资源，则配置一定存在某种错误。如果探测不到磁盘，则操作系统可能无法再访问此磁盘。
  - 手动测试磁盘配置，并根据 HA 文档确认此配置是否适当。
- 磁盘正在使用中，无法为 HA 资源组启动。

  启动 HA 资源组之前，始终要检查确认磁盘未激活。
- WSFC：网络配置错误

  如果网络流量流经多个 NIC 卡，则激活占用大量网络带宽的程序(如 NNMi ovjboss 进程)时，RDP 会话将失败。
- 某些 HA 产品在引导时不会自动重新启动。

  有关如何配置引导时的自动重新启动的信息，请参阅 HA 产品文档。
- 直接添加对操作系统的 NFS 或其他访问(资源组配置应管理此问题)。
- 故障转移或 HA 资源组脱机期间在共享磁盘安装点中。

  HA 会终止阻止共享磁盘卸载的任何进程。
- 将 HA 群集虚拟 IP 地址重用为 HA 资源虚拟 IP 地址(适用于一个系统上的资源而非另一个系统上的资源)
- 超时太短。如果产品出现故障， HA 产品可能使 HA 资源超时并导致故障转移。

  WSFC：在 Failover Cluster Management 中，检查**等待资源启动的时间**设置的值。NNMi 将此值设置为 15 分钟。可以增大该值。
- 不使用维护模式

  创建维护模式是为了调试 HA 故障。如果您尝试使某个资源组在系统上处于联机状态，但该资源组不久便发生故障转移，请使用维护模式保持该资源组为联机状态，以查明故障点。
- 不查看群集日志(群集日志可显示很多常见错误)。

RHCS 6 的配置问题

如果 ricci 服务关闭或被故意禁用，则 HA 环境中的两个系统之间的 `/etc/cluster/cluster.conf` 文件版本可能不同。因此，请定期监视 `cluster.conf` 文件，以确保文件版本同步。

如果 `cluster.conf` 文件版本不同步，则在尝试执行以下任何操作时可能遇到问题：

- 应用对 `cluster.conf` 的更改
- 取消配置资源组
- 启动群集
- 使用 `clustat` 命令

HA 资源测试

本部分描述了测试将放置到 NNMi HA 资源组中的资源的常规方法。此测试可识别硬件配置问题。建议在将 NNMi 配置为以高可用性 (HA) 运行之前执行此测试。记下产生正确结果的配置值，并在执行 NNMi HA 资源组的完整配置时使用这些值。

有关此处列出的任何命令的特定详细信息，请参阅 HA 产品的最新文档。

要测试 HA 资源，请执行以下步骤：

1. 如有必要，启动 HA 群集。
2. (仅 Windows)验证是否为 HA 群集定义了以下虚拟 IP 地址：
   - HA 群集的虚拟 IP 地址
   - 每个 HA 资源组一个虚拟 IP 地址

   这些 IP 地址中的每一个都不应该用在其他地方。
3. 将 HA 资源组添加到 HA 群集。

   为该 HA 资源组使用非生产名称，如 `test`。
4. 测试与 HA 资源组的连接：
   a. 将资源组的虚拟 IP 地址和相应的虚拟主机名作为资源添加到 HA 资源组。

      使用将随后与 NNMi HA 资源组关联的值。
   b. 从主动群集节点故障转移到被动群集节点，以验证 HA 群集是否能够正确进行故障转移。
   c. 从新的主动群集节点故障转移到新的被动群集节点，以验证能够故障恢复。
   d. 如果资源组未正确地故障转移，则登录到主动节点，然后验证是否正确配置了 IP 地址并可访问该地址。同时验证防火墙未阻止该 IP 地址。
5. 如配置 SAN 或已实际连接的磁盘 (第 161 页)中所述配置共享磁盘。
6. 测试与共享磁盘的连接：
   a. 如将共享磁盘移到 NNMi HA 资源组中 (第 162 页)中所述，将共享磁盘作为资源添加到 HA 资源组。
   b. 从主动群集节点故障转移到被动群集节点，以验证 HA 群集是否能够正确进行故障转移。
   c. 从新的主动群集节点故障转移到新的被动群集节点，以验证能够故障恢复。
   d. 如果资源组未正确地故障转移，则登录到主动节点，然后验证磁盘是否已安装并可用。
7. 记录用于配置共享磁盘的命令和输入。配置 NNMi HA 资源组时，可能需要此信息。
8. 从每个节点删除资源组：
   a. 删除 IP 地址条目。
   b. 使资源组脱机，然后从节点删除资源组。

   目前，可以使用 NNMi 提供的工具将 NNMi 配置为以 HA 运行。

特定于 NNMi 的高可用性故障排除

本部分中的主题仅适用于 NNMi 的高可用性 (HA) 配置。它们包括：

- 在所有群集节点取消配置之后，对 NNMi 重新启用高可用性 (第 174 页)
- NNMi 未以高可用性正确启动 (第 174 页)
- 故障转移之后看不到对 NNMi 数据的更改 (第 174 页)
- nmsdbmgr 在配置高可用性后未启动 (第 175 页)
- NNMi 仅在一个高可用性群集节点上正确运行 (Windows) (第 176 页)
- 磁盘故障转移未执行 (第 176 页)
- 无法访问共享磁盘 (Windows) (第 176 页)

- 共享磁盘不包含当前数据 (第 176 页)
- 故障转移之后辅助节点找不到共享磁盘文件 (第 176 页)

在所有群集节点取消配置之后，对 NNMi 重新启用高可用性

所有 NNMi 高可用性 (HA) 群集节点已取消配置后，ov.conf 文件不再包含对 NNMi 共享磁盘的任何安装点引用。

要重新创建安装点引用，而不覆盖共享磁盘上的数据，请在主节点上执行以下步骤：

1. 如果 NNMi 正在运行，则停止它：

   ovstop -c
2. 重新设置对共享磁盘的引用：
   - Windows：

     %NnmInstallDir%\misc\nnm\ha\nnmhadisk.ovpl NNM -setmount <HA 安装点>
   - Linux：

     $NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM -setmount <HA 安装点>
3. 在 ov.conf 文件中，验证与 HA 安装点相关的条目。

   有关 ov.conf 文件的位置，请参阅NNMi 高可用性配置文件 (第 180 页)。

NNMi 未以高可用性正确启动

NNMi 未正确启动时，需要调试判断该问题是虚拟 IP 地址或硬盘的硬件问题，还是某种形式的应用程序故障。在此调试过程中，将系统置于无 NORESTART 关键字的维护模式。

1. 在 HA 群集中的主动节点上，通过创建以下维护文件，禁用 HA 资源组监视：
   - Windows：%NnmDataDir%\hacluster\<资源组>\maintenance
   - Linux：$NnmDataDir/hacluster/<资源组>/maintenance
2. 启动 NNMi：

   ovstart
3. 验证 NNMi 是否正确启动：

   ovstatus -c

   所有 NNMi 服务应当显示状况“RUNNING”。如果不是这种情况，则诊断未正确启动的进程。
4. 完成故障排除之后，删除维护文件：
   - Windows：%NnmDataDir%\hacluster\<资源组>\maintenance
   - Linux：$NnmDataDir/hacluster/<资源组>/maintenance

故障转移之后看不到对 NNMi 数据的更改

NNMi 配置指向未在运行 NNMi 的其他系统。要解决问题，请验证 ov.conf 文件是否有以下项的相应条目：

- NNM_INTERFACE=<虚拟主机名>
- HA_RESOURCE_GROUP=<资源组>
- HA_MOUNT_POINT=<HA 安装点>
- NNM_HA_CONFIGURED=YES
- HA_POSTGRES_DIR=<HA 安装点>/NNM/dataDir/shared/nnm/databases/Postgres
- HA_EVENTDB_DIR=<HA 安装点>/NNM/dataDir/shared/nnm/eventdb
- HA_CUSTOMPOLLER_DIR=<HA 安装点>/NNM/dataDir/shared/nnm/databases/custompoller
- HA_NNM_LOG_DIR=<HA 安装点>/NNM/dataDir/log
- HA_JBOSS_DATA_DIR=<HA 安装点>/NNM/dataDir/nmsas/NNM/data
- HA_LOCALE=C

有关 ov.conf 文件的位置，请参阅NNMi 高可用性配置文件 (第 180 页)。

nmsdbmgr 在配置高可用性后未启动

此情况通常是由于没有先运行带 -to 选项的 nnmhadisk.ovpl 命令，就在运行 nnmhaconfigure.ovpl 命令后启动 NNMi 而造成的。在这种情况下，ov.conf 文件中的 HA_POSTGRES_DIR 条目指定共享磁盘上嵌入式数据库的位置，但此位置对 NNMi 不可用。

要解决此问题，请执行以下步骤：

1. 在高可用性 (HA) 群集中的主动节点上，通过创建以下维护文件，禁用 HA 资源组监视：
   - Windows：%NnmDataDir%\hacluster\<资源组>\maintenance
   - Linux：$NnmDataDir/hacluster/<资源组>/maintenance
2. 将 NNMi 数据库复制到共享磁盘：
   - Windows：

     %NnmInstallDir%\misc\nnm\ha\nnmhadisk.ovpl NNM -to <HA 安装点>

   - Linux：

     $NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM -to <HA 安装点>

   > **警告:** 为防止数据库损坏，请仅运行此命令(带 -to 选项)一次。有关备选项的信息，请参阅在所有群集节点取消配置之后，对 NNMi 重新启用高可用性 (第 174 页)。

   - Windows：

     %NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM <资源组>

   - Linux：

     $NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM <资源组>

3. 启动 NNMi：

   ovstart

4. 验证 NNMi 是否正确启动：

   ovstatus -c

   所有 NNMi 服务应当显示状况“RUNNING”。
5. 完成故障排除之后，删除维护文件：
   - Windows：%NnmDataDir%\hacluster\<资源组>\maintenance
   - Linux：$NnmDataDir/hacluster/<资源组>/maintenance

NNMi 仅在一个高可用性群集节点上正确运行 (Windows)

Windows 操作系统需要两个不同的虚拟 IP 地址，一个用于高可用性 (HA) 群集，一个用于 HA 资源组。

如果 HA 群集的虚拟 IP 地址与 NNMi HA 资源组的相同，则 NNMi 只能在与 HA 群集 IP 地址关联的节点上正常运行。

要纠正此问题，请将 HA 群集的虚拟 IP 地址更改为此网络的唯一值。

磁盘故障转移未执行

操作系统不支持共享磁盘时，会发生这种情况。查看 HA 产品、操作系统和磁盘制造商文档以确定这些产品是否都兼容。

如果发生磁盘故障，则 NNMi 不启动故障转移。最可能出现的情况是 nmsdbmgr 由于 HA_POSTGRES_DIR 目录不存在而失败。验证共享磁盘是否已安装，以及相应的文件是否可访问。

无法访问共享磁盘 (Windows)

命令 nnmhaclusterinfo.ovpl -config NNM -get HA_MOUNT_POINT 未返回任何内容。

必须完全限定共享磁盘在 HA 配置期间的驱动器安装点(例如，S:\)。

要纠正此问题，请在 HA 群集中的每个节点上运行 nnmhaconfigure.ovpl 命令。完全指定共享磁盘安装点的驱动器。

共享磁盘不包含当前数据

以文本“无”来响应 nnmhaconfigure.ovpl 命令有关磁盘类型的问题时，会绕过用于设置 ov.conf 文件中磁盘相关变量的代码。要解决此问题，请遵循在高可用性环境中手动准备共享磁盘 (第 160 页)中的步骤操作。

故障转移之后辅助节点找不到共享磁盘文件

此情况的最常见原因是在未安装共享磁盘的情况下运行了带 -to 选项的 nnmhadisk.ovpl 命令。在这种情况下，将数据文件复制到本地磁盘，因此这些文件在共享磁盘上不可用。

要解决此问题，请执行以下步骤：

1. 在高可用性 (HA) 群集中的主动节点上，通过创建以下维护文件，禁用 HA 资源组监视：
   - Windows：%NnmDataDir%\hacluster\<资源组>\maintenance
   - Linux：$NnmDataDir/hacluster/<资源组>/maintenance

2. 登录到主动节点，然后验证磁盘是否已安装并可用。
3. 停止 NNMi：

   ovstop
4. 将 NNMi 数据库复制到共享磁盘：
   - Windows：

     %NnmInstallDir%\misc\nnm\ha\nnmhadisk.ovpl NNM -to <HA_ 安装点>
   - Linux：

     $NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM -to <HA 安装点>

   警告: 为防止数据库损坏，请仅运行此命令(带 -to 选项)一次。有关备选项的信息，请参阅在所有群集节点取消配置之后，对 NNMi 重新启用高可用性 (第 174 页)。
5. 启动 NNMi HA 资源组：
   - Windows：

     %NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM <资源组>
   - Linux：

     $NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM <资源组>
6. 启动 NNMi：

   ovstart
7. 验证 NNMi 是否正确启动：

   ovstatus -c

   所有 NNMi 服务应当显示状况“RUNNING”。
8. 完成故障排除之后，删除维护文件：
   - Windows：`%NnmDataDir%\hacluster\<资源组>\maintenance`
   - Linux：`$NnmDataDir/hacluster/<资源组>/maintenance`

常规 HA 故障排除

本部分中的主题适用于 NNMi 和 NNM iSPI 的 HA 配置。它们包括：

- 错误：参数个数不正确 (第 177 页)
- 资源托管子系统进程意外停止 (Windows Server) (第 178 页)
- 主动群集节点上的日志文件未更新 (第 178 页)
- 无法在特定群集节点上启动 NNMi HA 资源组 (第 178 页)

错误：参数个数不正确

产品 Perl 模块的名称对于大多数 NNMi 高可用性 (HA) 配置命令是必需参数。

- 对于 NNMi，请使用值 `NNM`。
- 要确定对 NNM iSPI 使用的值，请参阅该 NNM iSPI 的文档。

资源托管子系统进程意外停止 (Windows Server)

在运行 Windows Server 操作系统的计算机上启动高可用性 (HA) 群集资源会意外停止资源托管子系统 (Rhs.exe) 进程。

有关此已知问题的信息，请参阅 Microsoft 支持网站文章《The Resource Hosting Subsystem (Rhs.exe) process stops unexpectedly when you start a cluster resource in Windows Server》，可访问 http://support.microsoft.com/kb/978527 以查看此文章。

提示: 始终在特定于资源组的单独资源监视器 (rhs.exe) 中运行 NNMi 资源。

产品启动超时 (Windows WSCS 2008)

升级到 NNMi 10.01 之后，如果故障转移群集管理器中的 app 资源 (<资源>-app) 从“待定”更改为“失败”，则可能出现超时问题。如果发生此情况，请执行以下操作：

1. 使用 `cluster log /gen` 命令生成 `cluster.log` 文件。
2. 打开位于以下目录的日志：

   ```
   C:\Windows\cluster\reports\cluster.log
   ```

3. 如果在 cluster.log 文件中看到与下面类似的错误，则表示有 `DeadlockTimeout` 问题：

   ```
   ERR [RHS] Resource <资源名称>-APP handling deadlock.Cleaning current operation.
   ```

   `DeadlockTimeout` 是代理被阻止时进行故障转移的总时间。`PendingTimeout` 表示联机或脱机操作。`DeadlockTimeout` 默认值是 45 分钟 (2,700,000 毫秒)，`PendingTimeout` 默认值是 30 分钟 (1,800,000 毫秒)。

   可以更改 `DeadlockTimeout` 和 `PendingTimeout` 值。例如，要将 `DeadlockTimeout` 设置为 75 分钟、将 `PendingTimeout` 设置为 60 分钟，可以运行以下命令：

   ```
   cluster res "<资源组>-APP" /prop DeadlockTimeout=4500000
   ```

   ```
   cluster res "<资源组>-APP" /prop PendingTimeout=3600000
   ```

   有关详细信息，请参阅高可用性供应商文档

主动群集节点上的日志文件未更新

这种属于正常情况。发生这种情况是因为日志文件已被重定向到共享磁盘。

对于 NNMi，查看位于 `ov.conf` 文件中的 `HA_NNM_LOG_DIR` 所指定位置的日志文件。

无法在特定群集节点上启动 NNMi HA 资源组

如果 `nnmhastartrg.ovpl` 或 `nnmhastartrg.ovpl` 命令不能正确启动、停止或切换 NNMi HA 资源组，请查看以下信息：

- MSFC：
  - 在 Failover Cluster Management 中，查看 NNMi HA 资源组和底层资源的状况。
  - 查看事件查看器日志中是否有任何错误。
- VCS：

- 运行 **/opt/VRTSvcs/bin/hares -state** 以查看资源状况。
- 对于失败的资源，查看 /var/VRTSvcs/log/<资源>.log 文件以了解失败的资源。资源由代理类型引用，例如：IP*.log、Mount*.log 和 Volume*.log。

如果找不到问题根源，可以通过使用 HA 产品命令，手动启动 NNMi HA 资源组：

1. 安装共享磁盘。
2. 将虚拟主机分配到网络接口：
   - MSF：
     - 启动 Failover Cluster Management。
     - 展开资源组。
     - 右键单击 **<资源组>-ip**，然后单击**联机**。
   - VCS：**/opt/VRTSvcs/bin/hares -online <资源组>-ip -sys <本地主机名>**
   - RHCS：运行 /usr/sbin/cmmodnet 以添加 IP 地址。
3. 启动 NNMi HA 资源组。例如：
   - Windows：

     ```
     %NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM
     -start <资源组>
     ```

   - Linux：

     ```
     $NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM
     -start <资源组>
     ```

返回码 0 表示 NNMi 已成功启动。

返回码 1 表示 NNMi 未正确启动。

特定于 NNM iSPI 的高可用性故障排除

有关对以高可用性运行的 NNM iSPI 进行故障排除的信息，请参阅该 NNM iSPI 的文档。

高可用性配置参考

本部分包含以下高可用性配置项的参考信息：

NNMi 高可用性配置文件 (第 180 页)

NNMi 提供的 HA 配置脚本 (第 180 页)

NNMi 高可用性配置日志文件 (第 181 页)

NNMi 高可用性配置文件

下表列出了 NNMi 高可用性 (HA) 配置文件。这些文件适用于 NNMi 管理服务器上的 NNMi 和加载项 NNM iSPI。将这些文件安装到以下位置：

- Windows：`%NnmDataDir%\shared\nnm\conf`
- Linux：`$NnmDataDir/shared/nnm/conf`

NNMi HA 配置文件

文件名	描述
ov.conf	由 `nnmhaclusterinfo.ovpl` 命令更新，用于描述 NNMi HA 实现。NNMi 进程读取此文件以确定 HA 配置。
nnmdatareplicator.conf	由 `nnmdatareplicator.ovpl` 命令使用，用于确定从主动节点到被动节点的数据复制中包含哪些 NNMi 文件夹和文件。如果您复制 NNMi 配置时使用其他方法，请参阅此文件以了解要包含的数据的列表。 有关详细信息，请参阅该文件中的注释。

NNMi 提供的 HA 配置脚本

下表列出了 NNMi 附带的 HA 配置脚本。NNMi HA 配置脚本中列出的 NNMi 提供的脚本是可用于为具有客户 Perl 模块的任何产品配置 HA 的方便脚本。如果需要，您可以使用 HA 产品提供的命令配置 NNMi 以 HA 运行。

在 NNMi 管理服务器上，将 NNMi 提供的 HA 配置脚本安装到以下位置：

- Windows：`%NnmInstallDir%\misc\nnm\ha`
- Linux：`$NnmInstallDir/misc/nnm/ha`

NNMi HA 配置脚本

脚本名称	描述
nnmhaconfigure.ovpl	为 HA 群集配置 NNMi 或 NNM iSPI。 在 HA 群集中的所有节点上运行此脚本。
nnmhaunconfigure.ovpl	从 HA 群集中取消配置 NNMi 或 NNM iSPI。 (可选)在 HA 群集中的一个或多个节点上运行此脚本。
nnmhaclusterinfo.ovpl	检索有关 NNMi 的群集信息。 根据需要在 HA 群集中的任何节点上运行此脚本。
nnmhadisk.ovpl	向/从共享磁盘复制 NNMi 和 NNM iSPI 数据文件。 在 HA 配置期间，在主节点上运行此脚本。 在其他时间，按照本章中的说明运行此脚本。
nnmhastartrg.ovpl	在 HA 群集中启动 NNMi HA 资源组。 在 HA 配置期间，在主节点上运行此脚本。

NNMi HA 配置脚本(续)

脚本名称	描述
nnmhastoprg.ovpl	在 HA 群集中停止 NNMi HA 资源组。 在 HA 取消配置期间，在主节点上运行此脚本。

下表中列出的 NNMi 提供的脚本由 NNMi HA 配置脚本中列出的脚本使用。不要直接运行下表中列出的脚本。

NNMi HA 支持脚本

脚本名称	描述
nnmdatareplicator.ovpl	检查 `nnmdatareplicator.conf` 配置文件中是否有更改，并将文件复制到远程系统。
nnmharg.ovpl	在 HA 群集中启动、停止和监视 NNMi。 对于 VCS 配置，由 VCS 用于启动、停止和监视脚本。(`nnmhargconfigure.ovpl` 将配置此用法。) 还由 `nnmhastartrg.ovpl` 用于启用和禁用跟踪。
nnmhargconfigure.ovpl	配置 HA 资源和资源组。由 `nnmhaconfigure.ovpl` 和 `nnmhaunconfigure.ovpl` 使用。
nnmhastart.ovpl	在 HA 群集中启动 NNMi。由 `nnmharg.ovpl` 使用。
nnmhastop.ovpl	在 HA 群集中停止 NNMi。由 `nnmharg.ovpl` 使用。
nnmhamonitor.ovpl	在 HA 群集中监视 NNMi 进程。由 `nnmharg.ovpl` 使用。
nnmhamscs.vbs	是用于创建脚本以在 MSFC HA 群集中启动、停止和监视 NNMi 进程的一种模板。生成的脚本由 MSFC 使用，并存储在以下位置：`%NnmDataDir%\hacluster\<资源组>\hamscs.vbs`

NNMi 高可用性配置日志文件

以下日志文件适用于 NNMi 管理服务器上 NNMi 和加载项 NNM iSPI 的 HA 配置：

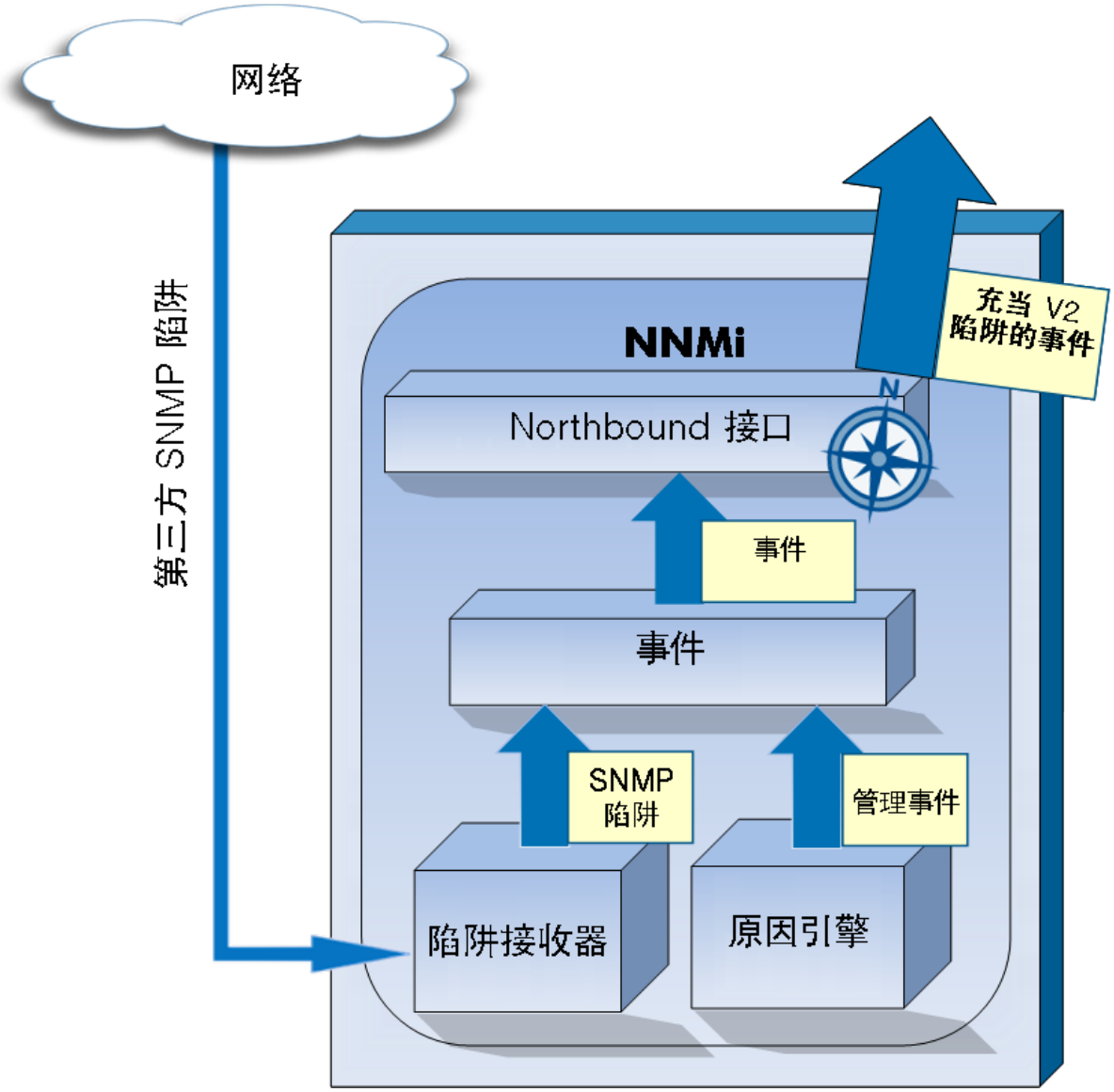
- Windows 配置：
  - `%NnmDataDir%\tmp\HA_nnmhaserver.log`
  - `%NnmDataDir%\log\haconfigure.log`
- Linux 配置：
  - `$NnmDataDir/tmp/HA_nnmhaserver.log`
  - `$NnmDataDir/log/haconfigure.log`
- Windows 运行时：

- 事件查看器日志
- %HA_MOUNT_POINT%\NNM\dataDir\log\nnm\ovspmd.log
- %HA_MOUNT_POINT%\NNM\dataDir\log\nnm\public\postgres.log
- %HA_MOUNT_POINT%\NNM\dataDir\log\nnm\public\nmsdbmgr.log
- %HA_MOUNT_POINT%\NNM\dataDir\log\nnm\nnm.log
- %SystemRoot%\Cluster\cluster.log
  这是关于群集运行时问题的日志文件，内容包括：添加和删除资源及资源组；其他配置问题；启动和停止问题。

- Linux：
  - /var/adm/syslog/syslog.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/ovspmd.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/postgres.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/nmsdbmgr.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/nnm.log

提示: 可能还需要查看 HA 供应商日志。例如，Veritas 将日志文件存储在 /var/VRTSvcs/log 文件夹中。RHCS 将日志消息记录在 syslog 中。

NNMi Northbound 接口



HP Network Node Manager i Software (NNMi) 提供 NNMi Northbound 接口，用于将 NNMi 事件转发到任何可以接收 SNMPv2c 陷阱的应用程序。对于每个 NNMi 管理服务器，可以实现连接到多个 northbound 应用程序的 NNMi Northbound 接口，对每个应用程序都单独进行配置。

NNMi 支持使用 NNMi Northbound 接口与以下产品集成：

- HP Business Service Management (BSM) 平台的 Operations Management 功能。
- HP Operations Manager (HPOM) 活动消息浏览器。
- IBM Tivoli Netcool/OMNIbus。
- HP ArcSight Logger

要与其他 northbound 应用程序集成，请遵循本章中的说明。

本章包含以下主题：

- NNMi Northbound 接口 (第 184 页)
- 启用 NNMi Northbound 接口 (第 185 页)
- 使用 NNMi Northbound 接口 (第 185 页)
- 更改 NNMi Northbound 接口 (第 188 页)
- 禁用 NNMi Northbound 接口 (第 189 页)
- NNMi Northbound 接口故障排除 (第 189 页)
- 应用程序故障转移和 NNMi Northbound 接口 (第 190 页)
- NNMi Northbound 接口目标表单参考 (第 190 页)

NNMi Northbound 接口

NNMi Northbound 接口将 NNMi 管理事件作为 SNMPv2c 陷阱转发到 northbound 应用程序。northbound 应用程序可筛选、处理和显示 NNMi 陷阱。northbound 应用程序还可提供工具，用于在 NNMi 陷阱的上下文中访问 NNMi 控制台。

NNMi Northbound 接口可以将事件生命周期状况更改通知、事件关联通知和事件删除通知发送到 northbound 应用程序。这样，northbound 应用程序可以复制 NNMi 原因分析的结果。

NNMi Northbound 接口还可以将 NNMi 接收的 SNMP 陷阱转发到 northbound 应用程序。

价值

NNMi Northbound 接口通过第三方或自定义的事件合并器实现事件合并。NNMi Northbound 接口利用可用于将 NNMi 与其他应用程序集成的信息扩展事件。

支持的版本

本章中的信息适用于 NNMi 版本 9.00 或更高版本。

有关受支持的硬件平台和操作系统的最新信息，请参阅《NNMi Support Matrix》。

术语

本章使用以下术语：

- Northbound 应用程序 - 可以接收和处理 SNMPv2c 陷阱的任何应用程序。
- 陷阱接收组件 - 接收 SNMP 陷阱的那部分 northbound 应用程序。
  - 某些应用程序包含一个可单独安装的组件，用于接收 SNMP 陷阱并转发到另一个组件进行处理。
  - 对于不包含此类组件的任何 northbound 应用程序，“陷阱接收组件”与“northbound 应用程序”同义。
- NNMi Northbound 接口 - 将 NNMi 事件作为 SNMPv2c 陷阱转发到 northbound 应用程序的 NNMi 功能。
- Northbound 目标 - NNMi Northbound 接口的一个配置，定义与 northbound 应用程序的陷阱接收组件的连接，并指定 NNMi 将发送到该 northbound 应用程序的陷阱类型。

文档

本章描述如何配置 NNMi 以将 NNMi 事件转发到任何 northbound 应用程序。有关特定 northbound 应用程序的信息，请参阅该应用程序的文档。

启用 NNMi Northbound 接口

警告: NNMi 不限制通过 UDP 在 SNMP 陷阱中发送的信息量。如果传输路径中的任何网络硬件无法处理某数量的陷阱数据，或者，如果网络流量很大，则陷阱可能丢失。因此，建议在 NNMi 管理服务器上安装 northbound 应用程序的陷阱接收组件。northbound 应用程序负责确保可靠信息传输。

要启用 NNMi Northbound 接口，请执行以下步骤：

1. 如有必要，配置 northbound 应用程序以了解 NNMi 陷阱定义。
2. 在 NNMi 管理服务器上，配置 NNMi 事件转发：
   a. 在 NNMi 控制台中，打开 **HP NNMi–Northbound 接口目标**表单(**集成模块配置 > Northbound 接口**)，然后单击**新建**。

      (如果已选择可用目标，则单击**重置**以使**新建**按钮可用。)
   b. 选中**启用**复选框以激活表单上的其余字段。
   c. 输入用于连接到 northbound 应用程序的信息。

      有关这些字段的信息，请参阅 Northbound 应用程序连接参数 (第 191 页)。
   d. 指定用于将内容发送到 northbound 应用程序的发送选项和事件筛选。

      有关这些字段的信息，请参阅 NNMi Northbound 接口集成内容 (第 192 页)。
   e. 单击表单底部的**提交**。

      将打开新窗口，其中显示状态消息。如果消息指出设置有问题，则单击**返回**，然后按照错误消息文本的建议调整值。
3. 可选。通过创建从 northbound 应用程序访问 NNMi 视图的 URL，创建与 NNMi 的上下文交互。

   有关信息，请在 NNMi 控制台中单击**帮助 > NNMi 文档库 > 通过 URL 在其他位置集成 NNMi**。

使用 NNMi Northbound 接口

启用 NNMi Northbound 接口时，northbound 目标确定 NNMi 发送到 northbound 应用程序的信息。以适用于您的网络环境的方式配置 northbound 应用程序以显示和解释转发陷阱。有关 NNMi 发送到 northbound 应用程序的陷阱内容和格式的完整信息，请参阅 `hp-nnmi-nbi.mib` 和 `hp-nnmi-registration.mib` 文件。

NNMi 仅将每个管理事件、SNMP 陷阱或通知陷阱的一个副本发送到 northbound 目标。NNMi 不会将陷阱排队。NNMi 转发陷阱时，如果 northbound 应用程序的陷阱接收组件不可用，则该陷阱将丢失。

本部分描述集成可以发送的陷阱类型。有关设置内容配置的信息，请参阅 NNMi Northbound 接口集成内容 (第 192 页)。

事件转发

管理事件

如果 northbound 目标包含管理事件，则当每个管理事件更改为“已注册”生命周期状况时，NNMi 将它发送到 northbound 应用程序。

已转发的管理事件的 OID 是 NNMi 控制台中**管理事件配置**表单上的 SNMP 对象 ID。NNMi 将转发 OID 为 1.3.6.1.4.1.11.2.17.19.2.0.9999 的所有自定义管理事件。

第三方 SNMP 陷阱

如果 northbound 目标包含第三方 SNMP 陷阱，则当关联的事件更改为“已注册”生命周期状况时，NNMi 将每个传入 SNMPv1、v2c 或 v3 格式的陷阱转发到 northbound 应用程序。NNMi 按顺序保留原始陷阱 varbind(如 MIB 中所定义)，并将特定于 NNMi 的 varbind 追加到消息负载。如果原始陷阱不包含所有定义的 varbind，则 NNMi 对缺失 varbind 填充 NULL 值。如果 MIB 未加载到 NNMi 中，则只有特定于 NNMi 的 varbind 会追加到稍后要转发的陷阱中。

对于第三方 SNMP 陷阱，注意以下事项：

- 因为 NNMi 从其 SNMP 陷阱事件重新构造陷阱，因此所转发陷阱始终使用 SNMPv2c 格式，而与 NNMi 接收原始陷阱时使用的格式无关。
- 所转发 SNMP 陷阱将 NNMi 管理服务器显示为源对象。要确定原始源对象，请检查第 (n+21) 个 varbind IncidentNodeHostname (1.3.6.1.4.1.11.2.17.19.2.2.21) 和第 (n+24) 个 varbind IncidentNodeMgmtAddr (1.3.6.1.4.1.11.2.17.19.2.2.24) 的值，其中 n 是 MIB 中为陷阱定义的 varbind 数目。

如果 NNMi 管理的任何设备也会将陷阱发送到 northbound 应用程序，则 northbound 应用程序必须管理重复的设备陷阱。

有关陷阱转发机制的比较，请参阅《NNMi 部署参考》中的“陷阱和事件转发”。

事件生命周期状况更改通知

此部分中的信息随在 **HP NNMi–Northbound Interface 目标**页中选择的**发送选项**而异。

增强的已关闭陷阱

如果 northbound 目标包含增强的已关闭通知，则当 NNMi 中事件的生命周期状况更改为“已关闭”时，NNMi 将 EventLifecycleStateClosed (1.3.6.1.4.1.11.2.17.19.2.0.1000) 陷阱发送到 northbound 应用程序。EventLifecycleStateClosed 陷阱包含原始事件中的大部分数据。未包含上一生命周期状况值。EventLifecycleStateClosed 陷阱在第六个 varbind IncidentUuid (1.3.6.1.4.1.11.2.17.19.2.2.6) 中标识原始事件。

状况更改陷阱

如果 northbound 目标包含生命周期状况更改通知，则当 NNMi 中事件的生命周期状况更改为“正在进行”、“已完成”或“已关闭”时，NNMi 将 LifecycleStateChangeEvent (1.3.6.1.4.1.11.2.17.19.2.0.1001) 陷阱发送到 northbound 应用程序。northbound 应用程序会将 LifecycleStateChangeEvent 与原始事件关联。

LifecycleStateChangeEvent 陷阱在以下 varbind 中标识原始事件和生命周期状况更改：

- IncidentUuid，第六个 varbind (1.3.6.1.4.1.11.2.17.19.2.2.6)

  此值与管理事件中的第六个 varbind 或第三方 SNMP 陷阱 varbind 中的第 (n+6) 个 varbind 的值相匹配。

- IncidentLifecycleStatePreviousValue，第七个 varbind (1.3.6.1.4.1.11.2.17.19.2.2.200)
- IncidentLifecycleStateCurrentValue，第八个 varbind (1.3.6.1.4.1.11.2.17.19.2.2.201)

下表列出生命周期状况的可能整数值。

名称	整数值
已注册	1
进行中	2
已完成	3
已关闭	4
已减弱	5

事件关联通知

如果 northbound 目标包含事件关联通知，则 NNMi 将事件关联陷阱作为 NNMi 原因分析关联事件发送到 northbound 应用程序。northbound 应用程序可以使用陷阱中的信息以复制关联更改。

单个关联陷阱

对于单个关联陷阱选项，集成发送以下关联陷阱：

- EventDedupCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1100)
- EventImpactCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1101)
- EventPairwiseCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1102)
- EventRateCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1103)
- EventApaCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1104)
- EventCustomCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1105)

每个陷阱在以下 varbind 中标识一个父子级事件关联关系：

- IncidentCorrelationIndicatorParentUuid，第六个 varbind (1.3.6.1.4.1.11.2.17.19.2.2.6)
- IncidentCorrelationIndicatorChildUuid，第七个 varbind (1.3.6.1.4.1.11.2.17.19.2.2.300)

组关联陷阱

对于组关联选项，集成发送以下关联陷阱：

- EventDedupCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2100)
- EventImpactCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2101)
- EventPairwiseCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2102)
- EventRateCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2103)
- EventApaCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2104)
- EventCustomCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2105)

每个陷阱在以下 varbind 中标识父子级事件关联关系：

- IncidentCorrelationIndicatorParentUuid，第六个 varbind (1.3.6.1.4.1.11.2.17.19.2.2.6)
- IncidentCorrelationIndicatorChildCount，第七个 varbind (1.3.6.1.4.1.11.2.17.19.2.2.301)
- IncidentCorrelationIndicatorChildUuidCsv，第八个 varbind (1.3.6.1.4.1.11.2.17.19.2.2.302)

  此值是子级事件 UUID 的逗号分隔值列表。

事件删除通知

如果 northbound 目标包含事件删除通知，则在 NNMi 中删除事件时，NNMi 将 EventDeleted (1.3.6.1.4.1.11.2.17.19.2.0.3000) 陷阱发送到 northbound 应用程序。EventDeleted 陷阱在第六个 varbind IncidentUuid (1.3.6.1.4.1.11.2.17.19.2.2.6) 中标识原始事件。

事件转发筛选

如果 northbound 目标包含事件筛选，则筛选中的对象标识符 (OID) 将(根据所选配置选项)包含或排除以下事件类型：

- NNMi 管理事件
- 第三方 SNMP 陷阱
- EventLifecycleStateClosed 陷阱
- LifecycleStateChangeEvent 陷阱
- EventDeleted 陷阱
- 关联通知陷阱

  以下备注适用于关联通知陷阱：

  - 如果事件筛选阻止转发某一关联的父级事件，则 NNMi 不将关联通知陷阱发送到 northbound 应用程序。
  - 如果事件筛选阻止转发某一关联的子级事件，则转发关联通知陷阱不包含该子级事件的 UUID。(如果关联通知陷阱不包含任何子级事件 UUID，则 NNMi 不将该陷阱发送到 northbound 应用程序。)
  - 将转发 DuplicateCorrelation 管理事件，而与 EventDedupCorrelation 或 EventDedupCorrelationGroup 关联通知陷阱无关。同样，将转发 RateCorrelation 管理事件，而与 EventRateCorrelation 或 EventRateCorrelationGroup 关联通知陷阱无关。如果事件筛选阻止转发其中某个关联通知陷阱，则 NNMi 可能仍然转发关联的管理事件。

更改 NNMi Northbound 接口

要更改 NNMi Northbound 接口配置参数，请执行以下步骤：

1. 在 NNMi 控制台中，打开 **HP NNMi–Northbound 接口目标**表单(**集成模块配置 > Northbound**)。
2. 选择目标，然后单击**编辑**。
3. 对值进行相应修改。

有关此表单上字段的信息，请参阅 NNMi Northbound 接口目标表单参考 (第 190 页)。

4. 验证表单顶部的**已启用**复选框是否选中，然后单击表单底部的**提交**。
   更改会立即生效。

禁用 NNMi Northbound 接口

禁用 northbound 目标时，不会发生任何 SNMP 陷阱排队。

要停止将 NNMi 事件转发到 northbound 应用程序，请执行以下步骤：

1. 在 NNMi 控制台中，打开 **HP NNMi–Northbound 接口目标**表单(**集成模块配置 > Northbound**)。
2. 选择目标，然后单击**编辑**。
   或者，单击**删除**以完全删除所选目标的配置。
3. 取消选中表单顶部的**已启用**复选框，然后单击表单底部的**提交**。
   更改会立即生效。

NNMi Northbound 接口故障排除

如果 NNMi Northbound 接口没有按预期工作，则执行以下步骤，直到问题得到解决：

1. 验证陷阱目标端口是否未被防火墙阻塞。
   确保 NNMi 管理服务器可以通过主机和端口对 northbound 应用程序进行直接寻址。
2. 验证集成是否正在正确运行：
   a. 在 NNMi 控制台中，打开 **HP NNMi–Northbound 接口目标**表单(**集成模块配置 > Northbound**)。
   b. 选择目标，然后单击**编辑**。
   c. 验证**已启用**复选框是否已选中。
3. 如果 northbound 目标包含管理事件，则验证以下功能：
   a. 在 NNMi 控制台的**已关闭的重大事件**视图中，打开任何事件。
   b. 将事件生命周期状况设置为**已注册**，然后单击 **保存**。
   c. 将事件生命周期状况设置为**已关闭**，然后单击 **保存并关闭**。
   d. 30 秒后，确定 northbound 应用程序是否接收到此事件的 EventLifecycleStateClosed 陷阱(或 LifecyleStateChangeEvent 陷阱)。
      - 如果 northbound 应用程序接收到陷阱，请继续执行步骤 4。
      - 如果 northbound 应用程序未接收陷阱，则配置新 northbound 目标与其他 northbound 应用程序连接，然后从步骤 a 重复此测试。
        如果重复测试成功，则问题来自于第一个 northbound 应用程序。请参考该应用程序的文档以获取故障排除信息。
        如果重复测试失败，则联系 HP 支持以获取帮助。
4. 如果 northbound 目标包含 SNMP 陷阱，则验证以下功能：
   a. 通过在 NNMi 管理服务器上输入以下命令，对 NNMi 拓扑中的节点生成 SNMP 陷阱：

```
nnmsnmpnotify.ovpl -u username -p password -a \
discovered_node NNMi_node linkDown
```

其中 `discovered_node` 是 NNMi 拓扑中节点的主机名或 IP 地址，`NNMi_node` 是 NNMi 管理服务器的主机名或 IP 地址。

b. 30 秒后，确定 northbound 应用程序是否接收到转发陷阱。
   - 如果 northbound 应用程序接收到陷阱，则说明 NNMi Northbound 接口正在正常运行。
   - 如果 northbound 应用程序未接收陷阱，则配置新 northbound 目标与其他 northbound 应用程序连接，然后从步骤 a 重复此测试。

     如果重复测试成功，则问题来自于第一个 northbound 应用程序。请参考该应用程序的文档以获取故障排除信息。

     如果重复测试失败，则联系 HP 支持以获取帮助。

应用程序故障转移和 NNMi Northbound 接口

如果 NNMi 管理服务器将参与 NNMi 应用程序故障转移，则此主题中的信息适用于任何实现 NNMi Northbound 接口以将陷阱发送到 northbound 应用程序的集成。

NNMi 发送到 northbound 应用程序的陷阱在 NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2) 中包含 NNMi URL。在应用程序故障转移之前接收到的陷阱引用的对象现在成为备用 NNMi 管理服务器。如果 URL 指向该备用 NNMi 管理服务器，则使用该 URL 值的任何操作(例如，启动 NNMi 控制台)将失败。

本地 Northbound 应用程序

如果 northbound 应用程序的陷阱接收组件位于 NNMi 管理服务器上，则以下注意事项适用于 NNMi Northbound 接口的配置：

- northbound 应用程序的陷阱接收组件必须以完全相同的方式在活动和备用 NNMi 管理服务器上安装和配置。在这两个 NNMi 管理服务器的同一端口上配置 SNMP 陷阱接收。
- 仅在主 NNMi 管理服务器上配置 NNMi Northbound 接口。

  在 **HP NNMi–Northbound 接口目标**表单上，选择 **NNMi FQDN** 或**使用环回**选项用于**主机**标识。

在启动时，NNMi Northbound 接口确定当前 NNMi 管理服务器的正确名称或 IP 地址。这样，Northbound 接口将陷阱发送到活动 NNMi 管理服务器上的 northbound 应用程序的陷阱接收组件。

远程 Northbound 应用程序

如果 northbound 应用程序的陷阱接收组件不位于 NNMi 管理服务器上，则仅在主 NNMi 管理服务器上配置 NNMi Northbound 接口。在 **HP NNMi–Northbound 接口目标**表单上，选择**其他**选项用于**主机**标识。

NNMi Northbound 接口目标表单参考

HP NNMi–Northbound 接口目标表单包含用于配置 NNMi 和 northbound 应用程序之间通信的参数。此表单是通过**集成模块配置**工作区提供的。(在 **HP NNMi–Northbound 接口目标**表单上，单击**新建**；或选择目标，然后单击**编辑**。)

> **备注:** 只有具有管理员角色的 NNMi 用户才可以访问 **HP NNMi–Northbound 接口目标**表单。

HP NNMi–Northbound 接口目标表单包含以下方面的信息：

- Northbound 应用程序连接参数 (第 191 页)
- NNMi Northbound 接口集成内容 (第 192 页)
- NNMi Northbound 接口目标状态信息 (第 194 页)

要应用集成配置更改，请更新 **HP NNMi–Northbound 接口目标**表单上的值，然后单击**提交**。

Northbound 应用程序连接参数

下表列出了用于配置 northbound 应用程序连接的参数。

Northbound 应用程序连接信息

字段	描述
主机	包含 northbound 应用程序陷阱接收组件的服务器的完全限定域名(首选)或 IP 地址。 集成支持用以下方法标识服务器： • **NNMi FQDN** NNMi 管理与 NNMi 管理服务器上的 northbound 应用程序的连接，并且**主机**字段变为只读。 这是 NNMi 管理服务器上的 northbound 应用程序的建议配置。 • **使用环回** NNMi 管理与 NNMi 管理服务器上的 northbound 应用程序的连接，并且**主机**字段变为只读。 • **其他** 在**主机**字段中输入用于标识 northbound 应用程序服务器的主机名或 IP 地址。 NNMi 将验证**主机**字段中的主机名或 IP 地址是否未配置为环回适配器。 这是默认配置。 **备注:** 如果 NNMi 管理服务器参与 NNMi 应用程序故障转移，请参阅应用程序故障转移和 NNMi Northbound 接口 (第 190 页)，以了解有关应用程序故障转移对集成的影响的信息。
端口	northbound 应用程序接收 SNMP 陷阱的 UDP 端口。 输入特定于 northbound 应用程序的端口号。 **备注:** 如果 northbound 应用程序的陷阱接收组件位于 NNMi 管理服务器上，则此端口号必须不同于 NNMi 用于接收 SNMP 陷阱的端口(如 NNMi 控制台中**通信配置**表单上的 **SNMP 端口**字段中所设置)。
团体字符串	northbound 应用程序用于接收陷阱的只读团体字符串。 如果 northbound 应用程序配置需要在所接收的 SNMP 陷阱中有团体字符

Northbound 应用程序连接信息(续)

字段	描述
	串，则输入该值。 如果 northbound 应用程序配置不需要特定团体字符串，则使用默认值 `public`。

NNMi Northbound 接口集成内容

Northbound 接口内容配置信息列出的参数用于配置 NNMi Northbound 接口发送到 northbound 应用程序的内容。

NNMi Northbound 接口内容配置信息

字段	描述
事件	事件转发规范。 • **管理** NNMi 仅将 NNMi 生成的管理事件转发到 northbound 应用程序。 • **第三方 SNMP 陷阱** NNMi 仅将 NNMi 从被管设备接收到的 SNMP 陷阱转发到 northbound 应用程序。 • **Syslog** NNMi 仅使用 NorthBound 集成模块将 NNMi 从被管设备接收到的 ArcSight Syslog 消息转发到 northbound 应用程序。 一旦启用 northbound 目标，NNMi 就开始转发事件。 有关详细信息，请参阅事件转发 (第 186 页)。
生命周期状况更改	事件更改通知规范。 • **增强已关闭** 对于更改为“已关闭”生命周期状况的每个事件，NNMi 会将“事件已关闭”陷阱发送到 northbound 应用程序。 这是默认配置。 • **状况已更改** 对于生命周期状况更改为“正在进行”、“已完成”或“已关闭”的每个事件，NNMi 将“事件生命周期状况已更改”陷阱发送到 northbound 应用程序。 • **两者** 对于更改为“已关闭”生命周期状况的每个事件，NNMi 会将“事件已关闭”陷阱发送到 northbound 应用程序。另外，对于生命周期状况更改为“正在进行”、“已完成”或“已关闭”的每个事件，集成将“事件生命周期状况已更改”陷阱发送到 northbound 应用程序。 **备注:** 在此例中，每次事件更改为“已关闭”生命周期状态时，集成都会发送两个通知陷阱：“事件已关闭”陷阱和“事件生命周期状态已更

NNMi Northbound 接口内容配置信息(续)

字段	描述
	改”陷阱。 有关详细信息，请参阅事件生命周期状况更改通知 (第 186 页)。
关联	事件关联通知规范。 • **无** NNMi 不会将 NNMi 原因分析生成的事件关联通知给 northbound 应用程序。 这是默认配置。 • **单个** NNMi 为从 NNMi 原因分析产生的每个父子级事件关联关系发送陷阱。 • **组** NNMi 对于列出关联到父级事件的所有子级事件的每个关联发送一个陷阱。 有关详细信息，请参阅事件关联通知 (第 187 页)。
删除	事件删除规范。针对在**事件**字段中进行的选择，此选项会配置是否向 northbound 应用程序发送一个删除陷阱。 • **不发送** 从 NNMi 中删除事件时，NNMi 不会通知 northbound 应用程序。 这是默认配置。 • **发送** 对于 NNMi 中删除的每个事件，NNMi 会向 northbound 应用程序发送一个删除陷阱。 有关详细信息，请参阅事件删除通知 (第 188 页)。
NNMi 控制台访问	URL 中的连接协议规范，用于从 northbound 应用程序浏览到 NNMi 控制台。NNMi 发送到 northbound 应用程序的陷阱在 NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2) 中包含 NNMi URL。 配置页默认使用与 NNMi 配置相匹配的设置。 如果将 NNMi 控制台配置为接受 HTTP 和 HTTPS 连接，则可以在 NNMi URL 中更改 HTTP 连接协议规范。例如，如果 northbound 应用程序的所有用户都在内部网上，则可以将从 northbound 应用程序对 NNMi 控制台的访问设置为通过 HTTP。要更改用于从 northbound 应用程序连接到 NNMi 控制台的协议，请相应选择 **HTTP** 选项或 **HTTPS** 选项。
事件筛选	集成用于筛选发送到 northbound 应用程序的事件的对象标识符 (OID) 列表。每个筛选条目可以是有效数字 OID(例如，.1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9)或 OID 前缀(例如，.1.3.6.1.6.3.1.1.5.*)。 选择以下某个选项： • **无**

NNMi Northbound 接口内容配置信息(续)

字段	描述
	NNMi 将所有事件发送到 northbound 应用程序。 这是默认配置。 • **包含** NNMi 仅发送与筛选中识别出的 OID 相匹配的特定事件。 • **排除** NNMi 发送所有事件，不包括与筛选中识别出的 OID 相匹配的特定事件。 指定事件筛选： • 要添加筛选条目，请在下部的文本框中输入文本，然后单击**添加**。 • 要删除筛选条目，请从上部框中的列表选择该条目，然后单击**删除**。 有关详细信息，请参阅事件转发筛选 (第 188 页)。

NNMi Northbound 接口目标状态信息

下表列出了 northbound 目标的只读状态信息。此信息对于验证集成是否正常运行很有用。

NNMi Northbound 接口目标状态信息

字段	描述
陷阱目标 IP 地址	目标主机名解析而得的 IP 地址。 此值对于此 northbound 目标唯一。
运行时间(秒)	自 northbound 组件上次启动以来经过的时间(秒)。NNMi 发送到 northbound 应用程序的陷阱在 sysUptime 字段 (1.3.6.1.2.1.1.3.0) 中包含此值。 对于使用 NNMi Northbound 接口的所有集成，此值都相同。要查看最新值，请刷新表单，或者关闭并重新打开表单。
NNMi URL	连接到 NNMi 控制台的 URL。NNMi 发送到 northbound 应用程序的陷阱在 NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2) 中包含此值。 此值对于此 northbound 目标唯一。

由 NNMi Northbound 接口使用的 MIB 信息

完成以下步骤以将特定的 MIB 加载到 NNMi，然后查看用于事件通知的管理信息(这些通知由 NNMi northbound 集成发送)。

1. 从命令提示符，运行 **`nnmloadmib.ovpl -load hp-nnmi.mib`** 命令以加载 `hp-nnmi.mib` 文件。
2. 从命令提示符，运行 **`nnmloadmib.ovpl -load p-nnmi-registration.mib`** 命令以加载 `hp-nnmi-registration.mib` 文件。
3. 从命令提示符，运行 **`nnmloadmib.ovpl -load hp-nnmi-nbi.mib`** 命令以加载 `hp-nnmi-nbi.mib` 文件。

4. 可选步骤：从命令提示符，运行 **nnmloadmib.ovpl -load hp-nnmi-ispi-perf-nbi.mib** 命令以加载 hp-nnmi-ispi-perf-nbi.mib 文件。
5. 从 NNMi 控制台，打开**配置**工作区。
6. 单击 **MIB -> 加载的 MIB**。
7. 双击您刚加载的每个 MIB，然后单击 **MIB 变量**查看 MIB 信息。

第 5 章: 维护 NNMi

本部分包含以下各章：

- NNMi 备份和恢复工具 (第 196 页)
- 维护 NNMi (第 203 页)
- NNMi 日志记录 (第 243 页)
- 更改管理服务器 (第 244 页)

NNMi 备份和恢复工具

良好的备份和恢复策略是确保任何业务连续操作的关键。HP Network Node Manager i Software (NNMi) 是网络操作的重要资产，应当定期备份。

与 NNMi 安装相关的两类关键数据如下：

- 文件系统中的文件
- 关系数据库(嵌入式或外部)中的数据

本章说明 NNMi 提供用于备份和恢复重要 NNMi 文件和数据的工具。

本章包含以下主题：

- 备份和恢复命令 (第 196 页)
- 备份 NNMi 数据 (第 197 页)
- 恢复 NNMi 数据 (第 199 页)
- 备份和恢复策略 (第 201 页)
- 只备份和恢复嵌入式数据库 (第 202 页)
- 在高可用性 (HA) 环境中使用备份和恢复工具 (第 203 页)

备份和恢复命令

NNMi 提供以下脚本，用于备份和恢复 NNMi 数据：

- `nnmbackup.ovpl` - 备份所有必要的文件系统数据(包括配置信息)和 NNMi 嵌入式数据库中存储的任何数据。
- `nnmrestore.ovpl` - 恢复使用 `nnmbackup.ovpl` 脚本创建的备份。
- `nnmbackupembdb.ovpl` - NNMi 运行时，创建 NNMi 嵌入式数据库(而非文件系统数据)的完整备份。
- `nnmrestoreembdb.ovpl` - 恢复使用 `nnmbackupembdb.ovpl` 脚本创建的备份。
- `nnmresetembdb.ovpl` - 断开 NNMi 嵌入式数据库表。运行 `ovstart` 命令以重新创建表。

有关命令语法，请参阅相应的参考页或 Linux 联机帮助页。

备份 NNMi 数据

NNMi 备份命令 (nnmbackup.ovpl) 会将关键的 NNMi 文件系统数据和 NNMi Postgres 数据库中的部分或所有表复制到指定的目标目录。

每个备份操作会将文件存储在目标目录内名为 nnm-bak-<时间戳> 的父目录中。可以指定 -noTimestamp 选项以节省磁盘空间。如果使用 -noTimestamp 选项，则父目录只需命名为 nnm-bak。在上一次备份后使用 -noTimestamp 选项执行备份时，上一次备份将重命名为 nnm-bak.previous，从而创建轮询备份。此重命名将在完成第二次备份后进行，以防止备份数据出现任何丢失。

NNMi 备份命令可创建备份数据的 tar 存档，您也可以使用自己的工具压缩备份文件。随后可以使用任何合适的工具保存备份副本。

提示: 如果您的 NNMi 实现使用 Oracle 作为主 NNMi 数据库，则 NNMi 备份和恢复命令只处理 NNMi 文件系统数据。外部数据库维护应作为现有数据库备份和恢复过程的一部分来处理。

备份和恢复数据可能包括，也可能不包括来自您的网络环境中安装的任何 NNM iSPI 的数据。有关详细信息，请查看每个 NNM iSPI 附带的文档。

警告: 任何能锁定文件的软件(如防病毒或系统备份软件)都可中断 NNMi 对 NNMi 数据库的访问。这可能导致问题，如不能读取或写入正由另一个进程(如防病毒应用程序)使用的文件。对于 NNMi Postgres 数据库，配置这些应用程序以排除 NNMi 数据库目录(Windows 上为 %NNM_DB%，Linux 上为 $NNM_DB)。可用 nnmbackup.ovpl 定期备份 NNMi 数据库。

有关详细信息，请参阅 nnmbackup.ovpl 参考页或 Linux 联机帮助页。

备份类型

NNMi 备份命令支持两类备份：

- NNMi 正在运行时，发生联机备份。NNMi 确保在备份的数据中同步数据库表。在联机备份过程中，操作员可以主动使用 NNMi 控制台，而其他进程可以与 NNMi 数据库交互。您可以如备份范围 (第 197 页)中所述，使用联机备份备份所有 NNMi 数据或根据功能只备份部分数据。对于嵌入式 NNMi 数据库，nmsdbmgr 服务必须正在运行。对于外部数据库，备份包括 NNMi 文件系统数据。备份外部数据库时不一定要运行 NNMi 进程。
- NNMi 完全停止时，发生脱机备份。使用脱机备份，备份范围仅应用于文件系统文件。脱机备份始终包括完整 NNMi 数据库，而不管备份范围如何。对于嵌入式 NNMi 数据库，备份将复制 Postgres 数据库文件。对于外部数据库，备份仅包括 NNMi 文件系统数据。

备份范围

NNMi 备份命令提供多个范围来定义备份多少 NNMi。

配置范围

配置范围 (-scope config) 大致对应于 NNMi 控制台的**配置**工作区中的信息。

配置范围包括以下数据：

- 对于联机备份，只是那些存储 NNMi 配置信息的嵌入式数据库表。
- 对于脱机备份，为整个嵌入式数据库。
- 对于所有备份，为配置范围文件和目录中所列的文件系统中的 NNMi 配置信息。

拓扑范围

拓扑范围 (-scope topology) 大致对应于 NNMi 控制台的**库存**工作区中的信息。因为网络拓扑依赖用于发现该拓扑的配置，所以拓扑范围包括配置范围。

拓扑范围包括以下数据：

- 对于联机备份，只是那些存储 NNMi 配置和网络拓扑信息的嵌入式数据库表。
- 对于脱机备份，为整个嵌入式数据库。
- 对于所有备份，为以下第一个表中所列的文件系统中的 NNMi 配置信息。当前，没有与拓扑范围关联的文件系统文件。

事件范围

事件范围 (-scope event) 大致对应于 NNMi 控制台的**事件浏览**工作区中的信息。因为事件依赖于与其相关的网络拓扑，所以事件范围包括配置和拓扑范围。

事件范围包括以下数据：

- 对联机备份，只是那些存储 NNMi 配置、网络拓扑和事件信息的嵌入式数据库表。
- 对于脱机备份，为整个嵌入式数据库。
- 对于所有备份，为以下第一个表中所列的文件系统中的 NNMi 配置信息，以及事件范围文件和目录中所列的 NNMi 事件信息。

所有范围

完整备份 (-scope all) 包括所有重要的 NNMi 文件和完整嵌入式数据库。

配置范围文件和目录

目录或文件名	描述
%NnmInstallDir%/conf(仅 Windows)	配置信息
%NnmInstallDir%\misc\nms\lic $NnmInstallDir/misc/nms/lic	其他许可证信息
%NnmInstallDir%\nmsas\server\nms\conf $NnmInstallDir/nmsas/server/nms/conf	jboss 配置
%NnmDataDir%\conf $NnmDataDir/conf	可能由其他 HP 产品共享的配置
%NnmDataDir%\conf\nnm\props $NnmDataDir/conf/nnm/props	本地 NNMi 配置属性文件
%NnmDataDir%\shared\nnm\conf\licensing\LicFile.txt $NnmDataDir/shared/nnm/conf/licensing/LicFile.txt	许可证信息
%NnmDataDir%\NNMVersionInfo	NNMi 版本信息文件

配置范围文件和目录(续)

目录或文件名	描述
$NnmDataDir/NNMVersionInfo	
%NnmDataDir%\shared\nnm\user-snmp-mibs $NnmDataDir/shared/nnm/user-snmp-mibs	共享用户添加的 SNMP MIB 信息
%NnmDataDir%\shared\nnm\actions $NnmDataDir/shared/nnm/actions	共享生命周期转换操作
%NnmDataDir%\shared\nnm\certificates $NnmDataDir/shared/nnm/certificates	共享 NNMi SSL 证书
%NnmDataDir%\shared\nnm\conf $NnmDataDir/shared/nnm/conf	共享 NNMi 配置信息
%NnmDataDir%\shared\nnm\conf\licensing $NnmDataDir/shared/nnm/conf/licensing	共享 NNMi 许可证配置信息
%NnmDataDir%\shared\nnm\lrf $NnmDataDir/shared/nnm/lrf	共享 NNMi 组件注册文件
%NnmDataDir%\shared\nnm\conf\props $NnmDataDir/shared/nnm/conf/props	共享 NNMi 配置属性文件
%NnmDataDir%\shared\nnm\www\htdocs\images $NnmDataDir/shared/nnm/www/htdocs/images	NNMi 节点组图的共享背景图像

在此上下文中，共享目录中的文件就是在 NNMi 应用程序故障转移或高可用性环境中与另一个 NNMi 管理服务器共享的文件。

事件范围文件和目录

目录或文件名	描述
$NnmDataDir/log/nnm/signin.0.0.log	NNMi 控制台登录日志

恢复 NNMi 数据

NNMi 恢复脚本 (nnmrestore.ovpl) 将备份数据放在 NNMi 管理服务器上。备份的类型和范围决定 NNMi 可以恢复的内容。

备注: 如果用 nnmrestore.ovpl 脚本在第二个 NNMi 管理服务器上放置数据库记录，则两个 NNMi 管理服务器必须有相同类型的操作系统和 NNMi 版本及补丁程序级别。

将备份数据从一个 NNMi 管理服务器放置到另一个 NNMi 管理服务器意味着这两个服务器有相同的数据库 UUID。在第二个 NNMi 管理服务器上恢复 NNMi 之后，请从原始 NNMi 管理服务器卸载 NNMi。

卸载 NNMi 之前，以相反顺序删除所有 NNMi 补丁程序，从最新的补丁程序开始。补丁程序删除过程会因 NNMi 管理服务器上运行的操作系统而异。有关安装和删除说明，请参阅补丁程序文档。

- 为恢复联机备份，NNMi 将文件系统数据复制到正确位置，并覆盖包括在备份中的数据库表的内容。恢复自备份以来删除的对象，并删除自备份以来创建的对象。另外，在备份之后更改的任何对象都恢复为备份时的状况。对于嵌入式 NNMi 数据库，`nmsdbmgr` 服务必须正在运行。对于外部数据库，恢复只包括 NNMi 文件系统数据，且无需运行 NNMi 进程。
- 为恢复脱机备份，NNMi 覆盖文件系统中的 Postgres 文件，用备份的内容完全替换数据库文件。对于外部数据库，备份仅包括 NNMi 文件系统数据。

使用 `-force` 选项，`nnmrestore.ovpl` 命令将停止所有 NNMi 进程，启动 `nmsdbmgr` 服务(如果从 NNMi 嵌入式数据库的联机备份恢复)，恢复数据，然后重新启动所有 NNMi 进程。

如果提供的源是 tar 文件，则 NNMi 恢复命令将 tar 文件解压缩到当前工作目录中的临时文件夹。在这种情况下，要么确保当前工作目录有足够存储空间来支持临时文件夹，要么在运行恢复命令之前解压缩存档。

备注: 因为数据库架构在一个 NNMi 版本与下一个之间可能更改，所以数据备份不能跨 NNMi 版本共享。

备注: NNMi 在备份恢复后将自动重新同步拓扑、状况和状态。

在重新同步期间不要停止 NNMi。为帮助确保重新同步已完成，NNMi 应在备份恢复后保持运行几小时。实际所需时间取决于节点数、状况更改量和执行重新同步时接收到的陷阱数据。

如果 NNMi 必须在重新同步完成之前停止，则应重新运行一次重新同步并允许完成。

要执行整个管理服务器的手动重新同步，请运行：`nnmnoderediscover.ovpl -all -fullsync`

相同系统恢复

可以在单个系统上使用备份和恢复命令进行数据恢复。以下项在备份和恢复过程之间不能更改：

- NNMi 版本(包括任何补丁程序)
- 操作系统类型
- 字符集(语言)
- 主机名
- 域

不同系统恢复

您可以用备份和恢复命令将数据从一个 NNMi 管理服务器传输到另一个。不同系统恢复的用途包括从系统故障中恢复，以及在操作系统升级期间将 NNMi 转换到其他系统。

备注: 因为 NNMi UUID 在数据库恢复期间复制到目标系统，所以源系统和目标系统现在似乎在运行 NNMi 的相同实例。从源系统卸载 NNMi。

卸载 NNMi 之前，以相反顺序删除所有 NNMi 补丁程序，从最新的补丁程序开始。补丁程序删除过程会因 NNMi 管理服务器上运行的操作系统而异。有关安装和删除说明，请参阅补丁程序文档。

提示: 要以相似配置创建多个可用的 NNMi 管理服务器(如部署全局网络管理时)，请使用 `nnmconfigexport.ovpl` 和 `nnmconfigimport.ovpl` 命令。

对不同系统恢复，两个系统上的以下项必须相同：

- NNMi 版本(包括任何补丁程序)
- 操作系统类型和版本
- 字符集(语言)

两个系统之间的以下项可以不同：

- 主机名
- 域

对不同系统恢复，`nnmrestore.ovpl` 命令不将许可证信息复制到新系统。为新 NNMi 管理服务器获取并应用新许可证。有关详细信息，请参阅许可 NNMi (第 252 页)。

备份和恢复策略

本部分讨论以下备份和恢复策略：

- 定期备份所有数据 (第 201 页)
- 更改配置之前备份数据 (第 202 页)
- 升级 NNMi 或操作系统之前备份数据 (第 202 页)
- 只恢复文件系统文件 (第 202 页)

定期备份所有数据

灾难恢复计划应包括所有 NNMi 数据的定期计划的完整备份。无需关闭 NNMi 也能创建此备份。如果将备份合并到脚本中，则使用 `-force` 选项确保备份开始之前 NNMi 的状况正确。例如：

```
nnmbackup.ovpl -force -type online -scope all -archive
  -target nnmi_backups\periodic
```

如果必须在硬件故障之后恢复 NNMi 数据，则执行以下步骤：

1. 重建或获得新硬件。
2. 将 NNMi 安装到和备份所处相同的版本和补丁程序级别。

3. 恢复 NNMi 数据：
   - 如果恢复 NNMi 管理服务器满足相同系统恢复 (第 200 页)中列出的要求，则运行与以下示例类似的命令：

     ```
     nnmrestore.ovpl -force -lic
     -source nnmi_backups\periodic\newest_backup
     ```

   - 如果恢复 NNMi 管理服务器不符合相同系统恢复的要求，但满足不同系统恢复 (第 201 页)中列出的要求，则运行与以下示例类似的命令：

     ```
     nnmrestore.ovpl -force
       -source nnmi_backups\periodic\newest_backup
     ```

     根据需要更新许可证。

更改配置之前备份数据

开始更改配置之前，根据需要执行有范围的备份(如备份范围 (第 197 页)中所述)。这样，如果配置更改没有达到希望的效果，还能回到已知可用的配置。例如：

```
nnmbackup.ovpl -type online -scope config
-target nnmi_backups\config
```

要将此备份恢复到同一 NNMi 管理服务器，请停止所有 NNMi 进程，然后运行与以下示例类似的命令：

```
nnmrestore.ovpl -force -source nnmi_backups\config\newest_backup
```

升级 NNMi 或操作系统之前备份数据

进行重大系统更改(包括升级 NNMi 或操作系统)之前，执行所有 NNMi 数据的完整备份。要确保在备份之后没有对 NNMi 数据库作出更改，请停止所有 NNMi 进程，并创建脱机备份。例如：

```
nnmbackup.ovpl -type offline -scope all
-target nnmi_backups\offline
```

如果 NNMi 在系统更改之后不能正确运行，则回滚更改或设置其他 NNMi 管理服务器，并确保符合在不同系统恢复 (第 201 页)中列出的要求。然后运行与以下示例类似的命令：

```
nnmrestore.ovpl -lic -source nnmi_backups\offline\newest_backup
```

只恢复文件系统文件

要覆盖 NNMi 文件而不影响数据库表，则运行与以下示例类似的命令：

```
nnmrestore.ovpl -partial
-source nnmi_backups\offline\newest_backup
```

NNMi 实现使用 Oracle 作为主 NNMi 数据库时，该命令很有用。

只备份和恢复嵌入式数据库

NNMi 提供的 `nnmbackupembdb.ovpl` 和 `nnmrestoreembdb.ovpl` 命令只用于备份和恢复 NNMi 嵌入式数据库。此功能在您试验 NNMi 配置设置时，可用于创建数据的快照。`nnmbackupembdb.ovpl` 和

nnmrestoreembdb.ovpl 命令仅执行联机备份。至少 nmsdbmgr 服务必须正在运行。

有关详细信息，请参阅 nnmbackup.ovpl 参考页或 Linux 联机帮助页。

每个备份操作会将文件存储在目标目录内名为 nnm-bak-<时间戳> 的父目录中。可以指定 -noTimestamp 选项以节省磁盘空间。如果使用 -noTimestamp 选项，则父目录只需命名为 nnm-bak。在上一次备份后使用 -noTimestamp 选项执行备份时，上一次备份将重命名为 nnm-bak.previous，从而创建轮询备份。此重命名将在完成第二次备份后进行，以防止备份数据出现任何丢失。

备注: 将数据恢复到嵌入式数据库之前，运行 nnmresetembdb.ovpl 命令。此命令确保数据库不包含任何错误，从而消除违反数据库约束的可能性。有关运行嵌入式数据库重置命令的信息，请参阅 nnmresetembdb.ovpl 参考页或 Linux 联机帮助页。

在高可用性 (HA) 环境中使用备份和恢复工具

本部分包括在高可用性环境中使用备份和恢复工具时要考虑的有用提示。

在 HA 环境中备份的最佳实践

在 HA 环境中使用 NNMi 备份工具时，请注意以下最佳实践：

- 使用活动(主)系统执行备份。(不建议对备份(辅助)节点进行备份，因为配置文件可能过时，并且由于备份节点无权访问共享磁盘，不会包括共享磁盘信息。)
- 共享磁盘必须连接到活动节点。如果使用 cron 作业，请验证共享磁盘是否已安装。
- 使系统进入维护模式(以免触发故障转移)。
- 仅使用 nnmbackup.ovpl 脚本在活动节点上执行联机备份。
- 定期运行脱机备份。

有关详细信息，请参阅 nnmbackup.ovpl 参考页或 Linux 联机帮助页。

在 HA 环境中恢复的最佳实践

在 HA 环境中使用 NNMi 恢复工具时，请注意以下最佳实践

- 验证共享磁盘是否已安装。
- 验证系统是否处于维护模式。
- 使用 nnmrestore.ovpl 脚本执行恢复。

有关详细信息，请参阅 nnmrestore.ovpl 参考页或 Linux 联机帮助页。

有关在 HA 环境中使用 NNMi 的详细信息，请参阅在高可用性群集中配置 NNMi (第 138 页)。

维护 NNMi

NNMi 管理服务器正常运行之后，可以执行维护任务以优化几个 NNMi 功能。

本章包含以下主题：

- 管理 NNMi 文件夹的访问控制列表 (第 204 页)
- 配置节点组 (第 205 页)
- 配置节点组图设置 (第 205 页)
- 配置通信设置 (第 205 页)
- 管理自定义轮询器采集导出 (第 206 页)
- 管理事件操作 (第 207 页)
- 覆盖 server.properties 文件中的设置 (第 210 页)
- 管理 SNMP 陷阱 (第 213 页)
- 使用 nnmtrapd.conf 和 trapFilter.conf 文件阻止事件 (第 223 页)
- 配置 NNMi 保留以前支持的 Varbind 顺序 (第 223 页)
- 配置 ICMP Echo 请求包中的数据负载大小 (第 224 页)
- 配置 NNMi 如何确定设备的主机名 (第 226 页)
- 为 NNMi 配置字符集编码设置 (第 226 页)
- 配置 NNMi 等待 NNM iSPI 许可请求的时间 (第 227 页)
- 管理用户界面属性 (第 227 页)
- 修改并发 SNMP 请求数 (第 232 页)
- 修改嵌入式数据库端口 (第 232 页)
- 修改 NNMi 标准化属性 (第 233 页)
- 修改并发 SNMP 请求数 (第 232 页)
- NNMi 自监视 (第 235 页)
- 抑制对特定节点使用发现协议 (第 236 页)
- 抑制管理出现故障的接口上的 IP 地址监视 (第 237 页)
- 抑制对大型交换机使用 VLAN 索引 (第 238 页)
- 计划服务中断 (第 239 页)
- 配置传感器状态 (第 239 页)
- 导入接口的输入和输出速度 (第 242 页)

管理 NNMi 文件夹的访问控制列表

您在运行时可能会遇到要求您修改运行 `HP NNM Action Server` 的用户名的情况，如设置操作服务器名称参数 (第 208 页)中所示。如果您更改了运行操作服务器的用户名而没有修改用户名权限，则 `HP NNM Action Server` 可能不会启动，并且 NNMi 可能不会在运行事件操作时记录消息。此部分包括防止这种情况发生需执行的操作。

NNMi (Everest) 包含对以下目录的权限更改：

- `/var/opt/OV/log/nnm/public`
- `/var/opt/OV/shared/perfSpi`

尽管 NNMi Everest 的现有权限数(针对 `/var/opt/OV/log/nnm/public` 文件夹)是 755，但 NNMi 使用 ACL 调整数据库用户 (`nmsdbmgr`) 和 nnmaction 用户 (`bin`) 的访问权限。在 NNMi Everest 后续安装过程中(安装或升级脚本的一部分)，安装脚本会更改 `/var/opt/OV/log/nnm/public` 文件夹权限并添加 ACL。

如果安装脚本由于某种意外错误而无法在 /var/opt/OV/log/nnm/public 文件夹上设置 ACL，则该脚本将保留 /var/opt/OV/log/nnm/public 文件夹全局可写，而 NNMi 安装应该会成功完成。在成功安装 NNMi 之后，如果您想要限制对 /var/opt/OV/log/nnm/public 文件夹的全局写权限，请参阅系统管理文档，了解如何为 NNMi 管理服务器的操作系统设置 ACL。

对于 /var/opt/OV/log/nnm/public 文件夹，使用 Linux ACL(访问控制列表)调整用户访问。配置 ACL 是扩展 owner/group/other 权限的有用方法。以下所有 Linux 平台都支持 ACL：RedHat 和 SuSE。

例如，在运行以下命令之后，USER 变量所表示的用户将获得对 **/var/opt/OV/log/nnm/public** 文件夹的写权限。在没有运行以下命令的情况下，**/var/opt/OV/log/nnm/public** 文件夹的权限数是 755，并且根用户之外的任何人都不能写入该目录中的文件。

```
setfacl -m user:<用户>:rwx /var/opt/OV/log/nnm/public
```

有关如何使用 setfacl 命令的信息，请参阅 Linux 联机帮助页。

配置节点组

NNMi 提供命令行工具帮助您实现节点组配置的自动化。nnmnodegroup.ovpl 命令支持您创建、列出、修改和删除节点组。

有关详细信息，请参阅 nnmnodegroup.ovpl 参考页或 Linux 联机帮助页。

配置节点组图设置

除了使用 NNMi 控制台配置节点组图设置以外，您还可以使用 nnmnodegroupmapsettings.ovpl 命令行工具配置节点组图设置。nnmnodegroupmapsettings.ovpl 工具支持您创建、修改和删除节点组图设置。该工具还允许您以 TXT、XML 或 CSV 格式列出当前节点组图设置。

提示: 刷新当前运行 NNMi 的 Web 浏览器，立即查看对节点组图设置所作更改的效果。

有关详细信息，请参阅 nnmnodegroupmapsettings.ovpl 参考页或 Linux 联机帮助页。

配置通信设置

您可以使用 nnmcommunication.ovpl 命令行工具配置 NNMi 通信设置。nnmcommunication.ovpl 工具支持您创建、列出、修改和删除通信设置。该工具可生成文本表格、文本列表或 XML 格式的列表。

管理员还可以使用 nnmcommunication.ovpl 工具绕过正常配置，锁定并直接管理字段的 SNMP 代理设置，如管理地址和团体字符串。

nnmcommunication.ovpl 工具不支持加载、添加或删除 SNMP 代理端口或 SNMP 代理地址。已弃用代理设置，并将在将来的版本中删除。

有关详细信息，请参阅 nnmcommunication.ovpl 参考页或 Linux 联机帮助页。

管理自定义轮询器采集导出

通过使用 SNMP MIB 表达式指定 NNMi 应轮询的其他信息，NNMi 自定义轮询器功能使您能够对网络管理采取主动操作。

自定义轮询器采集定义要收集(轮询)的信息以及 NNMi 如何对收集的数据作出反应。有关更多详细信息，请参阅 NNMi 帮助中的“创建自定义轮询器采集”和“配置自定义轮询”。另请参阅《HP Network Node Manager i Software Step-by-Step Guide to Custom Poller White Paper》。

自定义轮询器功能需要您在处理文件时将文件从导出目录中删除。

> **备注:** 不要长期存储导出文件；如果它们占用的空间超过了所配置的最大磁盘空间，NNMi 将删除较旧的文件，并创建新文件。除非您处理这些文件并将它们存储于其他位置，否则您将丢失这些文件。

更改自定义轮询器采集导出目录

NNMi 将您导出的所采集数据写入以下目录中：

- Windows：`%NNmDataDir%\shared\nnm\databases\custompoller\export`
- Linux：`$NnmDataDir/shared/nnm/databases/custompoller/export`

要更改 NNMi 写入自定义轮询器文件的目录，请执行以下步骤：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS%\nms-custompoller.properties`
   - Linux：`$NNM_PROPS/nms-custompoller.properties`
2. 查找 `exportdir` 条目，此条目与以下行类似：

   `#!com.hp.nnm.custompoller.exportdir=<用于导出自定义轮询器度量的基本目录>`

   要配置 NNMi 以将自定义轮询器采集信息写入 `C:\CustomPoller` 目录中，请将该行作如下更改：

   `com.hp.nnm.custompoller.exportdir=C:\CustomPoller`
3. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

更改用于自定义轮询器采集导出的最大磁盘空间量

要更改 NNMi 将数据导出到 采集名称`.csv` 文件时使用的最大磁盘空间量，请执行以下步骤：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS%\nms-custompoller.properties`
   - Linux：`$NNM_PROPS/nms-custompoller.properties`
2. 查找 `maxdiskspace` 条目，此条目与以下行类似：

#!com.hp.nnm.custompoller.maxdiskspace=1000

要配置 NNMi 为每个采集名称 .csv 文件保留最多 2000 MB (2 GB) 的存储空间，请将该行作如下更改：

com.hp.nnm.custompoller.maxdiskspace=2000

3. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

更改自定义轮询器度量累计间隔

NNMi 设置将数据写入文件之前自定义轮询器采集度量的累计时间长度(分钟)。

要更改自定义轮询器度量累计间隔，请执行以下步骤：

1. 编辑以下文件：
   - Windows：%NNM_PROPS%\nms-custompoller.properties
   - Linux：$NNM_PROPS/nms-custompoller.properties
2. 查找类似以下内容的行：

   #!com.hp.nnm.custompoller.accumulationinterval=5

   要配置 NNMi 以十分钟(而不是默认的五分钟)的时间长度采集度量，请将该行作如下更改：

   com.hp.nnm.custompoller.accumulationinterval=10
3. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

管理事件操作

可以将操作配置为在事件生命周期中的任何时间自动运行。例如，可能要配置在生成所配置类型的事件时发生的操作。有关详细信息，请参阅 NNMi 帮助中的“为事件配置操作”。

要调整操作参数，请遵循以下部分中所示的步骤。

> **备注:** 为避免出现意外结果(比如非预期的内存增长、事件操作处理时间增加)，HP 建议不要更改事件操作处理的默认属性值。

设置并发操作数目

要修改 NNMi 可以运行的并发操作数目，请执行以下步骤：

1. 编辑以下文件：
   - Windows：%NNM_PROPS%\shared\nnmaction.properties
   - Linux：$NNM_PROPS/shared/nnmaction.properties

2. 查找类似以下内容的行：

   #!com.hp.ov.nms.events.action.numProcess=10

   要配置 NNMi 以启用 20 个并发操作(而不是默认值)，请将该行作如下更改：

   com.hp.ov.nms.events.action.numProcess=20

   > **备注:** 确保删除位于行开头的 **#!** 字符。

3. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

设置 Jython 操作的线程数

要修改操作服务器用于运行 jython 脚本的线程数，请执行以下步骤：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS%\shared\nnmaction.properties`
   - Linux：`$NNM_PROPS/shared/nnmaction.properties`
2. 查找类似以下内容的行：

   #!com.hp.ov.nms.events.action.numJythonThreads=10

   要配置 NNMi 以启用 20 个线程供运行 jython 脚本(而不是默认值)，请将该行作如下更改：

   com.hp.ov.nms.events.action.numJythonThreads=20

   > **备注:** 确保删除位于行开头的 **#!** 字符。

3. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

设置操作服务器名称参数

如果您在 Windows 操作系统上运行 NNMi 管理服务器，则使用本地系统帐户将 `HP NNM Action Server` 作为 Windows 服务运行。这意味着您必须使用本地系统帐户运行操作服务器操作。

要修改在 Windows NNMi 管理服务器上运行 `HP NNM Action Server` Windows 服务的用户名，请更改 `HP NNM Action Server` 服务的 `LogOn` 属性。

如果您在 Linux 操作系统上运行 NNMi 管理服务器，则使用 `bin` 用户名运行操作服务器。要修改在这些操作系统上运行操作服务器的用户名，请完成以下步骤：

1. 编辑以下文件：

   `$NNM_PROPS/nnmaction.properties`

2. 查找类似以下内容的行：

#!com.hp.ov.nms.events.action.userName=bin

要配置 NNMi 用根用户而不是默认用户运行操作服务器，请将该行作如下更改：

com.hp.ov.nms.events.action.userName=root

> **备注:** 确保删除位于行开头的 **#!** 字符。

3. 保存更改。
4. 重新启动操作服务器：
   a. 在 NNMi 管理服务器上运行 **ovstop nnmaction** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart nnmaction** 命令。

更改操作服务器队列大小

对于以高执行速率使用长操作命令字符串的操作(比如对陷阱风暴的响应)，操作服务器可能占用大量内存。为了提供更好的操作服务器性能，HP 对操作服务器可以占用的内存大小设置了限制。

要修改这些限制，请执行以下步骤：

1. 编辑以下文件：
   - %NNM_PROPS%\shared\nnmaction.properties
   - $NNM_PROPS/shared/nnmaction.properties
2. 查找类似以下内容的两行：
   - com.hp.ov.nms.events.action.jvmargs.minMemsize=-Xms6m
   - com.hp.ov.nms.events.action.jvmargs.maxMemsize=-Xmx30m
3. 上面的参数显示最小内存大小设置为 6MB，最大内存大小设置为 30MB。调整这些参数以符合需要。
4. 保存更改。
5. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

事件操作日志

当操作运行时，将输出记录到关联的事件操作日志文件中。要查看所选事件的日志内容，请使用**工具 > 事件操作日志**菜单选项。下表描述日志中包含的各项：

事件操作日志项

项	描述
命令	事件发生时运行的脚本
事件名称	在事件配置中定义的事件名称

事件操作日志项(续)

项	描述
事件 UUID	事件的 UUID(**注册**选项卡中)
命令类型	命令(**Jython** 或 **ScriptOrExecutable**)的类型
生命周期状况	事件的生命周期状况(**已注册**、**正在处理**、**已完成**或**已关闭**)
退出代码	返回命令代码(类似于错误代码)
标准输出	操作的标准输出
标准错误	标准错误输出
执行状态	每个操作已确定的状态

覆盖 server.properties 文件中的设置

备注: 请注意，一个系统可能有两个 server.properties 文件。

以下文件由产品安装程序创建并包含为应用程序实例自定义应用程序服务器的属性。客户不能修改此文件，将在代码维护(升级或打补丁)期间替换此文件。

Windows: `%NnmDataDir%\NNM\server\server.properties`

Linux: `$NnmDataDir/NNM/server/server.properties`

客户使用以下文件配置应用程序以适应其环境，升级或打补丁期间产品不会修改此文件。此文件会覆盖其他文件中配置的值。因此所有自定义均在此文件中完成。

Windows: `%NnmDataDir%\nmsas\NNM\server.properties`

Linux: `$NnmDataDir/nmsas/NNM/server.properties`

本部分描述如何在 `nmsas/NNM/server.properties` 文件中覆盖以下设置:

覆盖浏览器语言环境设置 (第 210 页)

配置 SNMP Set 对象访问特权 (第 212 页)

将 NNMi 配置为要求加密远程访问 (第 213 页)

覆盖浏览器语言环境设置

可以使用以下 server.properties 文件强制所有 NNMi 客户端使用给定语言环境值，而不管浏览器语言环境值为何:

Windows: `%NnmDataDir%\nmsas\NNM\server.properties`

Linux: `$NnmDataDir/nmsas/NNM/server.properties`

使用 server.properties 文件设置此值后，将忽略浏览器语言环境值。

要覆盖浏览器语言环境设置，请执行以下操作:

1. 打开 server.properties 文件：

   Windows：`%NnmDataDir%\nmsas\NNM\server.properties`

   Linux：`$NnmDataDir/nmsas/NNM/server.properties`
2. 导航到 `nmsas.server.forceClientLocale`。
3. 将 nmsas.server.forceClientLocale 设置为以下任一个：

   `nmsas.server.forceClientLocale=` <两个字母的 ISO 语言代码>

   例如，要仅使用 ISO 语言代码将语言环境设置为英语，请输入以下内容：

   `nmsas.server.forceClientLocale = en`

   `nmsas.server.forceClientLocale=` <两个字母的 ISO 语言代码>_<两个字母的 ISO 国家/地区代码>

   例如，要使用 ISO 语言代码和国家/地区代码将语言环境设置为英语，请输入以下内容：

   `nmsas.server.forceClientLocale = en_US`
4. 重新启动 NNMi ovjboss 服务：

   在 NNMi 管理服务器上运行 `ovstop ovjboss` 命令。

   在 NNMi 管理服务器上运行 `ovstart` 命令。

备注: 对 `server.properties` 文件所作的更改只在 ovjboss 启动时读取。

有关详细信息，请参阅 `server.properties` 文件中的注释。

配置分配事件时用户名排序顺序所用的语言环境

NNMi 管理员可以指定 NNMi 管理服务器在分配事件时确定用户名排序顺序所用的语言环境。

备注: 配置的排序顺序语言环境仅应用于**分配事件**对话框。

确定字母顺序时，NNMi 将使用用户的显示名称而非实际登录名，并且不会分别对大小写字母排序。

备注: NNMi 仅使用 `sortLocale` 中配置的语言环境确定排序顺序。`forceClientLocale` 属性中指定的浏览器语言环境不影响排序顺序。有关详细信息，请参阅覆盖浏览器语言环境设置 (第 210 页)

备注: 在高可用性 (HA) 下进行更改时，需要更新的 server.properties 文件位于以下位置：<共享磁盘>`/NNM/dataDir/nmsas/NNM/server.properties`。

要配置分配事件时用于对列出的用户名进行排序的语言环境，请按如下所示编辑 `server.properties` 文件：

1. 打开以下文件：
   - Windows：`%NnmDataDir%\nmsas\NNM\server.properties`
   - Linux：`$NnmDataDir/nmsas/NNM/server.properties`

2. 取消注释 server.properties 文件中的以下行：

   #nmsas.server.sortLocale = en_US

3. 将默认值更改为 NNMi 管理服务器的正确语言环境。例如，要将语言环境更改为俄语，请使用以下条目：

   nmsas.server.sortLocale = ru_RU

4. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 ovstop 命令。
   b. 在 NNMi 管理服务器上运行 ovstart 命令。

配置 SNMP Set 对象访问特权

您可以使用以下文件配置在用户具有访问权限的节点上使用 SNMP Set 功能所需的对象访问特权。

Windows：%NnmDataDir%\nmsas\NNM\server.properties

Linux：$NnmDataDir/nmsas/NNM/server.properties

有关 SNMP Set 功能的详细信息，请参阅 NNMi 操作员帮助。有关对象访问特权的详细信息，请参阅 NNMi 管理员帮助。

要为 SNMP Set 功能配置对象访问特权，请执行以下操作：

1. 打开 server.properties 文件：

   Windows：%NnmDataDir%\nmsas\NNM\server.properties

   Linux：$NnmDataDir/nmsas/NNM/server.properties

2. 添加以下行：

   permission.override.com.hp.nnm.SNMP_SET=<对象访问角色>

   <对象访问角色> 的有效值包括：

   com.hp.nnm.ADMIN

   com.hp.nnm.LEVEL2

   com.hp.nnm.LEVEL1

   com.hp.nnm.GUEST

   例如，要启用**管理员对象**和**第 2 级操作员对象**对象访问特权以使用 SNMP Set 功能，请输入以下内容：

   permission.override.com.hp.nnm.SNMP_SET=com.hp.nnm.ADMIN,com.hp.nnm.LEVEL2

3. 包括您要启用访问的每个对象访问特权。
4. 重新启动 NNMi ovjboss 服务：

   在 NNMi 管理服务器上运行 ovstop ovjboss 命令。

   在 NNMi 管理服务器上运行 ovstart 命令。

备注: 对 server.properties 文件所作的更改只在 ovjboss 启动时读取。

将 NNMi 配置为要求加密远程访问

管理员可以禁用从网络到 NNMi 的 HTTP 以及其他未加密的的访问。

> **备注:** 在将 NNMi 配置为仅允许加密的远程访问之前，请确保全局网络管理、NNM iSPI 及其他集成支持 SSL。先将它们配置为支持 SSL，再将 NNMi 配置为仅允许加密的远程访问。

要禁用从网络到 NNMi 的 HTTP 以及其他未加密的访问，请如下所示编辑 server.properties 文件：

1. 编辑以下文件(如果该文件不存在，您可能需要创建它)：
   - Windows：`%NnmDataDir%\nmsas\NNM\server.properties`
   - Linux：`$NnmDataDir/nmsas/NNM/server.properties`
2. 将下面四行添加到 `server.properties` 文件中：

   ```
   nmsas.server.net.bind.address = 127.0.0.1
   nmsas.server.net.bind.address.ssl = 0.0.0.0
   nmsas.server.net.hostname = localhost
   nmsas.server.net.hostname.ssl = ${com.hp.ov.nms.fqdn}
   ```
3. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 `ovstop` 命令。
   b. 在 NNMi 管理服务器上运行 `ovstart` 命令。

经过上述修改后，NNMi 将不“侦听”来自远程系统的 HTTP 请求；但 localhost 访问仍将支持 HTTP 请求。

管理 SNMP 陷阱

本部分描述如何执行以下任务：

- 使用 hosted-on-trapstorm.conf 文件阻止陷阱风暴 (第 213 页)
- 配置 NNMi 以便验证使用 SNMPv2 或 SNMPv1 管理或者未被发现的节点的 SNMPv3 陷阱 (第 214 页)
- 配置原因引擎接受陷阱的时间 (第 215 页)
- 配置自动删除最旧 SNMP 陷阱事件功能 (第 216 页)
- 配置 NNMi 以确定代理 SNMP 网关发送的陷阱的原始陷阱地址 (第 220 页)

使用 hosted-on-trapstorm.conf 文件阻止陷阱风暴

NNMi 提供一种方法来阻止来自托管设备(包括接口)的陷阱风暴。

1. 运行 `nnmtrapconfig.ovpl` 脚本。包括适当的 `-hostedOnTrapstorm` 和 `-hostedOnThreshold` 值(如 nnmtrapconfig.ovpl 参考页或 Linux 联机帮助页中所述)来配置陷阱服务。使用 `-setProp` 参数重新配置陷阱服务器以反映属性更改。
2. (可选)要更改任何现有配置，请编辑以下文件：

- Windows： `%NnmDataDir%\shared\nnm\conf\hosted-object-trapstorm.conf`
- Linux： `$NnmDataDir/shared/nnm/conf/hosted-object-trapstorm.conf`

依照 hosted-object-trapstorm.conf 参考页或 Linux 联机帮助页中所述的格式进行更改。

3. 如果更改了 `hosted-object-trapstorm.conf` 文件，则必须依次运行 `nnmtrapconfig.ovpl -stop` 和 `nnmtrapconfig.ovpl -start to` 来重新启动陷阱服务。有关详细信息，请参阅 nnmtrapconfig.ovpl 参考页或 Linux 联机帮助页。

> **备注:** 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

配置 NNMi 以便验证使用 SNMPv2 或 SNMPv1 管理或者未被发现的节点的 SNMPv3 陷阱

如果 NNMi 正在从满足以下任一条件的节点接收 SNMPv3 陷阱，请按照此部分中的步骤执行操作：

- 设备是使用 SNMPv2 或 SNMPv1 管理的
- 设备未由 NNMi 发现

您可以配置 NNMi，以便将这些设备的 SNMPv3 引擎 ID 添加到 SNMPv3 缓存中。通过用这种方式配置 NNMi，NNMi 可以验证并存储这些 SNMPv3 陷阱。

要配置 NNMi 以便接收和存储使用 SNMPv2 或 SNMPv1 管理或者未被发现的节点的 SNMPv3 陷阱：

1. 在 NNMi 控制台中，导航到**配置 > 通信设置**。在默认、区域或特定节点设置级别配置条目，使每个入站陷阱均有相应配置可用于验证陷阱。有关详细信息，请参阅 NNMi 帮助中的“配置默认 SNMPv3 设置”。

   > **提示:** 好的做法是使用包括 SNMPv3 节点地址范围在内的区域或为每一个配置特定节点设置。

2. 在 NNMi 控制台中，导航到**配置 > 事件 > 事件配置**。
3. 取消选中**丢弃未解析的 SNMP 陷阱和 Syslog 消息**。

   取消选中**丢弃未解析的 SNMP 陷阱和 Syslog 消息**后，NNMi 会保留从其尚未发现的节点发送的陷阱。
4. 在 NNMi 管理服务器上运行 `ovstop` 命令。
5. 编辑以下文件：

   Windows： `%NNM_PROPS%\nms-communication.properties`

   Linux： `$NNM_PROPS/nms-communication.properties`
6. 在文件的末尾添加以下行：

   `com.hp.nnm.snmp.engineid.file=<文件路径>file.txt`

<文件路径>file.txt 条目是包含设备的文件的完整路径和文件名。

进行这些配置更改后，每次重新启动 NNMi 进程时，NNMi 会将这些条目从此文件读取到 SNMPv3 缓存中。

备注: 在 Linux NNMi 管理服务器上，文件路径为常见格式，如 /var/opt/OV/etc。

在 Windows NNMi 管理服务器上，忽略驱动器并使用正斜杠作为分隔符。例如，指定一个文件如 `C:/temp/file.txt` 作为 `/temp/file.txt`。

7. 保存更改。
8. 编辑 <文件路径>file.txt 文件：
   a. 添加设备的 IP 地址、端口和引擎 ID，每一项用逗号分隔。
   b. 在每一单独的行中为每个设备添加一个条目。

      引擎 ID 是一系列十六进制字节。NNMi 忽略字符大小写，可识别空格。

      使用以下示例创建您的条目：

      16.1.2.3,161,80 00 00 09 30 00 00 1f e9 a3 33 01

      16.1.2.4,161,80 00 00 11 03 00 00 2d 51 99 30 00

      1050:0000:0000:0000:0005:0600:300c:326b, 161, 800000090300001f9ea33000

      ff06::c3,161,80 00 00 09 03 00 00 1f 9A A3 30 00

   a. 在 NNMi 管理服务器上运行 `ovstart` 命令以启动 NNMi 并读取 <文件路径>file.txt 文件。
   b. 查看 Boot.log 文件以验证 NNMi 是否已读取文件。

      该文件应包含指示已读取文件的日志消息，消息类似以下文本：

      ```
      2012-10-17 14:44:44.876 INFO  [NnmTrapService] Start:Populate engineIDs from file
      2012-10-17 14:45:08.017 INFO  [SnmpV3EngineIdCachePopulator] Successfully loaded 3 V3
       Engine IDs from file /temp/patch2/v3hosts.txt
      ```

      如果未能将节点映射到有效配置，则您应看到类似以下内容的消息：

      ```
      2012-10-17 14:45:03.485 WARNING [SnmpV3EngineIdCachePopulator] V3
      Engine IDs:Could not resolve SNMPv3 configuration for 16.1.2.6
      ```

      如果您看到类似于以上的消息，请调整该节点的**配置 > 通信配置**设置。

备注: 如果需要从缓存或 <文件路径>file.txt 文件中删除某个条目，则最好从 <文件路径>file.txt 删除该条目，然后重新启动 NNMi：

1. 在 NNMi 管理服务器上运行 `ovstop` 命令。
2. 在 NNMi 管理服务器上运行 `ovstart` 命令。

配置原因引擎接受陷阱的时间

当常规时间或可预测时间内大范围区域的网络不可用时，NNMi 支持通过禁止将陷阱发送到原因引擎来减轻原因引擎分析负载。要禁止发送陷阱，作为 NNMi 管理员，您可以配置 NNMi 原因引擎停止从事件系统接受陷阱的时间。

备注: 此功能不会妨碍发送到 NNMi 控制台的陷阱。

发送到原因引擎的陷阱用于触发状况轮询器先于状况轮询器轮询策略决定的计划来轮询节点。禁止发送陷阱时，在从状况轮询器获取更新的信息前，NNMi 必须等待直到达到计划的轮询间隔。在任何情况下，NNMi 原因引擎通过使用 NNMi 状况轮询器的状况流得出包含或不包含陷阱的相同结论。

要配置原因引擎停止接受陷阱的时间，请执行以下步骤：

1. 创建以下文件：

   Windows：`%NNM_PROPS%\shared\nms-apa.properties`

   Linux：`$NNM_PROPS/shared/nms-apa.properties`
2. 将以下内容添加到文件：

   ```
   PROPERTY NAME: com.hp.ov.nms.apa.trapGateSchedule
   ```

   使用以下示例作为准则：

   在以下示例中，陷阱在午夜流动，上午 8:30 被禁止，然后在上午 10:00 再次流动，在下午 4:30 再次被禁止：

   ```
   com.hp.ov.nms.apa.trapGateSchedule = ENABLE_APA_TRAPS  08:30  10:00 16:30
   ```

   在以下示例中，陷阱在午夜被禁止，上午 8:30 再次流动，然后在上午 10:00 被禁止，在下午 4:30 再次流动：

   ```
   com.hp.ov.nms.apa.trapGateSchedule = DISABLE_APA_TRAPS  08:30  10:00 16:30
   ```
3. 保存更改。
4. 重新启动 NNMi 管理服务器
   a. 在 NNMi 管理服务器上运行 `ovstop` 命令。
   b. 在 `NNMi` 管理服务器上运行 `ovstart` 命令。

配置自动删除最旧 SNMP 陷阱事件功能

为保持 NNMi 以高级别执行，NNMi 在其数据库中存储一定数量的 SNMP 陷阱之后，丢弃传入的 SNMP 陷阱(包括 syslog 消息)。您可以使用自动删除最旧 SNMP 陷阱事件功能来控制存储在 NNMi 数据库中的 SNMP 陷阱数量并保留传入的重要 SNMP 陷阱。

备注: NNMi 仅删除非根源 SNMP 陷阱事件。

默认情况下禁用自动删除最旧 SNMP 陷阱事件功能。启用自动删除最旧 SNMP 陷阱事件功能之后，NNMi 会从 NNMi 数据库中删除最旧的 SNMP 陷阱事件。

提示: 要手动从 NNMi 数据库中删除 SNMP 陷阱事件，请使用 `nnmtrimincidents.ovpl` 脚本。有关详细信息，请参阅 nnmtrimincidents.ovpl 参考页或 Linux 联机帮助页。

启用自动删除最旧 SNMP 陷阱事件功能(无事件存档)

假定您要启用自动删除最旧 SNMP 陷阱事件功能，以便在 NNMi 数据库中的 SNMP 陷阱事件数超过 60,000 后删除 30,000 个 SNMP 陷阱事件(包括 syslog 消息)。对于此示例，您不希望 NNMi 在删除 SNMP 陷阱事件前对它们进行存档。完成以下步骤：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS\nms-jboss.properties`
   - Linux：`$NNM_PROPS/nms-jboss.properties`
2. 找到包含以下行的文本块：

   `#!com.hp.nnm.events.snmpTrapAutoTrimStartPercentage=50`
3. 取消代码行的注释并进行编辑，以呈现以下内容：

   `com.hp.nnm.events.snmpTrapAutoTrimStartPercentage=60`
4. 找到包含以下行的文本块：

   `#!com.hp.nnm.events.snmpTrapAutoTrimPercentageToDelete=25`
5. 取消代码行的注释并进行编辑，以呈现以下内容：

   `com.hp.nnm.events.snmpTrapAutoTrimPercentageToDelete=50`
6. 找到包含以下行的文本块：

   `#!com.hp.nnm.events.snmpTrapAutoTrimSetting=Disabled`
7. 取消代码行的注释并进行编辑，以呈现以下内容：

   `com.hp.nnm.events.snmpTrapsAutoTrimSetting=TrimOnly`
8. 重新启动 NNMi 管理服务器：
   a. 在 NNMi 管理服务器上运行 **`ovstop`** 命令。
   b. 在 NNMi 管理服务器上运行 **`ovstart`** 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

`com.hp.nnm.events.snmpTrapMaxStoreLimit` 的默认值是 100,000。在这种配置下，NNMi 在从 NNMi 数据库存储 60,000 个 SNMP 陷阱事件(包括 syslog 消息)之后，将使用以下公式从 NNMi 数据库中删除 30,000 个 SNMP 陷阱事件：

(**`com.hp.nnm.events.snmpTrapAutoTrimStartPercentage X`**

`com.hp.nnm.events.snmpTrapMaxStoreLimit X`

`com.hp.nnm.events.snmpTrapAutoTrimPercentageToDelete`

启用自动删除最旧 SNMP 陷阱事件功能(启用事件存档)

假定您要启用自动删除最旧 SNMP 陷阱事件功能，以便在 NNMi 数据库中的 SNMP 陷阱事件数超过 80,000 后删除 60,000 个 SNMP 陷阱事件(包括 syslog 消息)。对于此示例，您希望 NNMi 在删

除 SNMP 陷阱事件前对它们进行存档。完成以下步骤：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS\nms-jboss.properties`
   - Linux：`$NNM_PROPS/nms-jboss.properties`
2. 找到包含以下行的文本块：

   `#!com.hp.nnm.events.snmpTrapAutoTrimStartPercentage=50`
3. 取消代码行的注释并进行编辑，以呈现以下内容：

   `com.hp.nnm.events.snmpTrapAutoTrimStartPercentage=80`
4. 找到包含以下行的文本块：

   `#!com.hp.nnm.events.snmpTrapAutoTrimPercentageToDelete=25`
5. 取消代码行的注释并进行编辑，以呈现以下内容：

   `com.hp.nnm.events.snmpTrapAutoTrimPercentageToDelete=75`
6. 找到包含以下行的文本块：

   `#!com.hp.nnm.events.snmpTrapAutoTrimSetting=Disabled`
7. 将此行编辑为如下所示：

   `com.hp.nnm.events.snmpTrapsAutoTrimSetting=TrimAndArchive`
8. 重新启动 NNMi：
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

`com.hp.nnm.events.snmpTrapMaxStoreLimit` 的默认值是 100,000。在这种配置下，NNMi 在从 NNMi 数据库存储 80,000 个 SNMP 陷阱事件(包括 syslog 消息)之后，将使用以下公式从 NNMi 数据库中先存档再删除 60,000 个 SNMP 陷阱事件：

`com.hp.nnm.events.snmpTrapAutoTrimStartPercentage X`

`com.hp.nnm.events.snmpTrapMaxStoreLimit X`

`com.hp.nnm.events.snmpTrapAutoTrimPercentageToDelete`

> **提示:** 有关陷阱事件存档文件(包括如何自定义默认存档文件路径)的信息，请参阅 `nnmtrimincidents.ovpl` 参考页或 Linux 联机帮助页。

减少存储的 SNMP 陷阱事件数

如果不需要 NNMi 长时间保留 SNMP 陷阱事件，则可以考虑减少 NNMi 数据库中存储的 SNMP 陷阱事件的数量。

> **备注:** NNMi 在其数据库中的 SNMP 陷阱事件数达到 100,000 后，开始丢弃 SNMP 陷阱(包括

syslog 消息)。不支持将此限制设置为更高的数字，因为这样做会导致 NNMi 性能下降。

假定您要将存储的 SNMP 陷阱事件(包括 syslog 消息)的最大数量减少为 50,000 个 SNMP 陷阱事件。为此，请完成以下步骤：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS\nms-jboss.properties`
   - Linux：`$NNM_PROPS/nms-jboss.properties`
2. 找到包含以下行的文本块：

   `#!com.hp.nnm.events.snmpTrapMaxStoreLimit=100000`
3. 取消代码行的注释并进行编辑，以呈现以下内容：

   `com.hp.nnm.events.snmpTrapMaxStoreLimit=50000`
4. 重新启动 NNMi 管理服务器：
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

监视自动裁切最旧 SNMP 陷阱事件功能

从 **NNMi 控制台**中，单击**帮助 > 系统信息 > 运行状况**以检查自动删除最旧 SNMP 陷阱事件功能的运行状况。NNMi 还将生成以下有关自动删除最旧 SNMP 陷阱事件功能的报警。

- 在存储的 SNMP 陷阱事件(包括 syslog 消息)的数量达到 **`com.hp.nnm.events.snmpTrapMaxStoreLimit`** 值的 100% 之后，NNMi 会生成一个严重报警。
- 在存储的 SNMP 陷阱事件(包括 syslog 消息)的数量达到 **`com.hp.nnm.events.snmpTrapMaxStoreLimit`** 值的 95% 之后，NNMi 会生成一个 `snmpTrapLimitMajorAlarm` 报警。
- 在存储的 SNMP 陷阱事件(包括 syslog 消息)的数量达到 **`com.hp.nnm.events.snmpTrapMaxStoreLimit`** 值的 90% 之后，NNMi 会生成一个 `snmpTrapLimitWarningAlarm` 报警。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

禁用自动删除最旧 SNMP 陷阱事件功能

要禁用自动删除最旧事件功能，请完成以下步骤：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS\nms-jboss.properties`
   - Linux：`$NNM_PROPS/nms-jboss.properties`
2. 找到包含以下行的文本块：

   `com.hp.nnm.events.snmpTrapAutoTrimSetting`
3. 取消代码行的注释并进行编辑，以呈现以下内容：

   `com.hp.nnm.events.snmpTrapAutoTrimSetting=Disabled`
4. 重新启动 NNMi 管理服务器：
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

配置 NNMi 以确定代理 SNMP 网关发送的陷阱的原始陷阱地址

使用 NNMi 中的默认配置时，代理 SNMP 网关发送的陷阱可能不会显示原始陷阱地址。管理员可以配置 NNMi 以确定原始陷阱地址。

注意以下事项：

- NNMi 包含以下自定义事件属性：`cia.originaladdress`。NNMi 与 `com.hp.nnm.trapd.useUdpHeaderIpAddress` 属性一起确定 `cia.originaladdress` 属性的含义。
- `com.hp.nnm.trapd.useUdpHeaderIpAddress` 参数的值默认为 false，因此 NNMi 通常忽略 `cia.originaladdress` 属性。
- 将 `com.hp.nnm.trapd.useUdpHeaderIpAddress` 值设置为 true 后，`cia.originaladdress` 属性将提供 SNMP 代理地址的值。

当您想要在 NNMi 中使用 UDP 头地址作为源，并且仍然需要被管设备实际 SNMP 地址的访问权限时，将 `com.hp.nnm.trapd.useUdpHeaderIpAddress` 的值设置为 true 很有用。

备注: `com.hp.nnm.trapd.useUdpHeaderIpAddress` 属性为 false(默认设置)时，`cia.originaladdress` 和 `cia.address` 属性包含相同的值。

要配置 NNMi 以使用 `cia.originaladdress` 的值确定原始陷阱地址，请执行以下操作：

1. 编辑以下文件：

   Windows：`%NNM_PROPS%\nms-jboss.properties`

   Linux：`$NNM_PROPS/nms-jboss.properties`
2. 搜索包含以下行的文本块：

   `#!com.hp.nnm.trapd.useUdpHeaderIpAddress=false`

3. 取消以下代码行的注释并进行编辑，以呈现以下内容：

   `com.hp.nnm.trapd.useUdpHeaderIpAddress=true`

4. 保存更改。
5. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 `ovstop` 命令。

   在 NNMi 管理服务器上运行 `ovstart` 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

NNMi 使用 `cia.originaladdress` 的值确定原始陷阱地址。

陷阱地址排序

NNMi 对源地址进行如下分析：

- `com.hp.nnm.trapd.useUdpHeaderIpAddress` 属性设置为 true 的 SNMPv1 和 SNMPv2c 陷阱使用以下地址顺序：

  rfc3584TrapAddress (.1.3.6.1.6.3.18.1.3.0)

  nnmTrapForwardingAddress (.1.3.6.1.4.1.11.2.17.2.19.1.1.3.0)

  securityPackNotificationAddress (.1.3.6.1.4.1.99.12.45.2.1.0)

  proxyOid (.1.3.6.1.4.1.11.2.17.5.1.0)

  IP 报头中的源地址

- `com.hp.nnm.trapd.useUdpHeaderIpAddress` 属性设置为 false 的 SNMPv1 陷阱使用以下地址顺序：

  rfc3584TrapAddress (.1.3.6.1.6.3.18.1.3.0)

  nnmTrapForwardingAddress (.1.3.6.1.4.1.11.2.17.2.19.1.1.3.0)

  securityPackNotificationAddress (.1.3.6.1.4.1.99.12.45.2.1.0)

  proxyOid (.1.3.6.1.4.1.11.2.17.5.1.0)

  v1 陷阱中的代理地址字段

  IP 报头中的源地址

NNMi NmsTrapReceiver 进程

NNMi 提供的独立 NmsTrapReceiver 进程可帮助尽可能减少在故障转移期间丢失的 SNMP 陷阱。NmsTrapReceiver 同时在活动节点和备用节点上运行。

配置 NmsTrapReceiver

NNMi 提供以下用户可配置的设置：

- trapReceiverReplay

  当备用节点切换为活动节点时，trapReceiverReplay 设置是在故障转移后用于在启动期间回放陷阱的时间增量。(默认值是 10 秒。)

  备注: trapReceiverReplay 设置仅适用于应用程序故障转移和高可用性 (HA) 环境。

- trapReceiverJmsTTL

  trapReceiverJmsTTL 选项可设置 TrapReceiver 缓存陷阱的最大时间。默认设置是 5 分钟。如果 jboss 发生故障的时间比此时间长，数据将丢失。

  提示: 在配置此设置之前，请对故障转移计时以确定基准，然后将 trapReceiverJmsTTL 设置为该时间的两倍。

有关如何修改此类设置的详细信息，请参阅 `nnmtrapconfig.ovpl` 参考页或 Linux 联机帮助页。

备注: 为正常运行，同步活动节点和备用节点之间的时钟至关重要。否则，可能会出现大量重复数据或陷阱丢失。

有关详细信息，请参阅 `nnmtrapconfig.ovpl` 参考页或 Linux 联机帮助页。

备注: 在高可用性下进行 TrapReceiver 更改时，必须在群集中的两个节点上都进行更改。然后，需要停止并重新启动 TrapReceiver 进程(请参阅启动和停止 NmsTrapReceiver 进程 (第 222 页))。

NmsTrapReceiver 安全性

NNMi 提供的 nnmchangetrappw.ovpl 命令允许您更改 NmsTrapReceiver 密码。

备注: 在高可用性环境中，如果在活动 NNMi 管理服务器上更改密码，建议停止并重新启动备用 NNMi 管理服务器上的 NmsTrapReceiver。

有关详细信息，请参阅 `nnmchangetrappw.ovpl` 参考页或 Linux 联机帮助页。

启动和停止 NmsTrapReceiver 进程

NmsTrapReceiver 进程由操作系统自动启动(Linux：init.d nettrap；Windows：HP NNM NmsTrapReceiver 服务)。NmsTrapReceiver 进程还可以由 ovstart 启动(如果 ovstart 检测到 NmsTrapReceiver 进程未在运行)。

如果需要手动启动或停止 NmsTrapReceiver，请使用操作系统服务。

备注: ovstart 和 ovstop 命令仅启动和停止 jboss 管道以处理陷阱，而非远程陷阱服务器。

使用 nnmtrapd.conf 和 trapFilter.conf 文件阻止事件

如果流经 NNMi 管理服务器的事件数达到会导致 NNMi 阻止新到达事件的比率，请注意以下事项：

- NNMi 会生成 TrapStorm 事件，指示此事件被阻止。
- NNMi 还可能生成重大运行状况消息，指示事件比率较高并将阻止事件。

要减少事件数，请使用以下任一方法：

- 使用 nnmtrapd.conf 文件阻止事件进入 NNMi 中以减少事件流量。

  备注: 如果使用 nnmtrapd.conf 文件方法，则 NNMi 仍然使用这些事件计算陷阱比率并将其写入陷阱二进制库。通过使用 nnmtrapd.conf 文件方法，只能停止在数据库中创建或存储事件。

  有关详细信息，请参阅 nnmtrapd.conf 参考页或 Linux 联机帮助页。
- 使用 trapFilter.conf 阻止 NNMi 事件管道中较早的事件，从而防止将这些事件计入陷阱比率计算分析，或防止将这些事件存储在 NNMi 陷阱二进制库中。

  提示: 通过将设备 IP 地址或 OID 添加到 trapFilter.conf 文件，可以阻止这些高流量事件，并避免事件流量问题。

  有关详细信息，请参阅 trapFilter.conf 参考页或 Linux 联机帮助页。

配置 NNMi 保留以前支持的 Varbind 顺序

所有 SNMPv2 陷阱均包含 sysUptime.0 和 snmpTrapOID.0 OID 作为第一个和第二个 varbind。

备注: 如果 SNMPv2 陷阱包含 sysUptime.0 或 snmpOID.0 作为陷阱参数，则它们可能在 NNMi 中以 varbind 列表中非第一和第二的位置显示为其他 varbind。

NNMi 9.21 (patch 1) 之前， NNMi 会从 varbind 列表删除 sysUpTime.0 和 snmpTrapOID.0 OID 的所有实例。

自 NNMi 9.21 (patch 1) 起，当 OID 为陷阱定义的一部分并且在所接收陷阱的 varbind 列表的非第一和第二位置出现时，NNMi 将保留它们。此更改将更改使用 sysUpTime.0 或 snmpTrapOID.0 OID 作为陷阱参数的陷阱的 varbind 顺序。

在以下示例中，第一个粗体 varbind 包含 snmpTrapOID.0 的值，第二个粗体 varbind 包含 sysUpTime.0 的值。如此示例中所示，这些 varbind 在 varbind 列表中的非第一和第二位置显示为其他 varbind。

//0:SNMP MESSAGE (0x30):115 bytes

//2: INTEGER VERSION (0x2) 1 bytes:1 (SNMPv2C)

//5: OCTET-STR COMMUNITY (0x4) 6 bytes:"public"

//13: V2-TRAP-PDU (0xa7):102 bytes

//15: INTEGER REQUEST-ID (0x2) 2 bytes:18079

//19: INTEGER ERROR-STATUS (0x2) 1 bytes: noError(0)

//22: INTEGER ERROR-INDEX (0x2) 1 bytes:0

//25: SEQUENCE VARBIND-LIST (0x30):90 bytes

//27: SEQUENCE VARBIND (0x30):13 bytes

//29: **OBJ-ID (0x6) 8 bytes:.1.3.6.1.2.1.1.3.0**

//39: TIMETICKS (0x43) 1 bytes:9

//42: SEQUENCE VARBIND (0x30):32 bytes

//**44**: **OBJ-ID (0x6) 10 bytes:.1.3.6.1.6.3.1.1.4.1.0**

//56: OBJ-ID (0x6) 18 bytes:.1.3.6.1.6.3.1.1.5.3.1.3.6.1.4.1.9.1.14

//76: SEQUENCE VARBIND (0x30):14 bytes

//78: OBJ-ID (0x6) 9 bytes:.1.3.6.1.2.1.2.2.1.1

//89: INTEGER (0x2) 1 bytes:92

//92: SEQUENCE VARBIND (0x30):23 bytes

//94: OBJ-ID (0x6) 10 bytes:.1.3.6.1.6.3.1.1.4.3.0

//106: OBJ-ID (0x6) 9 bytes:.1.3.6.1.4.1.11.2.3.14

提示: 仅当希望 NNMi 从 varbind 列表删除 `sysUpTime.0` 和 `snmpTrapOID.0` 的所有实例时，才将 `com.hp.nnm.events.preserveOldVarbindListOrder` 属性设置为 true。

要保留原始的 NNMi 行为，请执行以下操作：

1. 编辑以下文件：

   Windows： `%NNM_PROPS%\nms-jboss.properties`

   Linux： `$NNM_PROPS/nms-jboss.properties`
2. 搜索包含以下行的文本块：

   ```
   #!com.hp.nnm.events.preserveOldvarbindListOrder=false
   ```
3. 取消以下代码行的注释并进行编辑，以呈现以下内容：

   ```
   com.hp.nnm.events.preserveOldvarbindListOrder=true
   ```
4. 保存更改。
5. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 `ovstop` 命令。

   在 NNMi 管理服务器上运行 `ovstart` 命令。

配置 ICMP Echo 请求包中的数据负载大小

网络延迟的一个定义就是 ICMP 包完成到目标设备并返回这一往返的时间。低延迟指示网络效率更高。

测试网络延迟的一个常见方法是调整 ICMP 轮询频率和 NNMi 所管理的管理地址的 ICMP Echo 请求包数据负载大小。考虑到较大的包的网络延迟比较小的包更长，因此 NNMi 允许使用不同大小的包进行试验来测试网络延迟。

您可以配置 NNMi 在 ICMP Echo 请求包中发送的属于节点组中节点或接口组中接口的 IP 地址的数据负载大小。例如，您可以修改发送到节点组或接口组的 ICMP Echo 请求包的大小，同时调整管理地址轮询时间，比较网络延迟。

要配置属于节点组中节点或接口组中接口的地址的不同负载大小，请完成以下步骤：

1. 编辑以下文件：

   Windows：`%NNM_PROPS%\nms-mon-config.properties`

   Linux：`$NNM_PROPS/nms-mon-config.properties`
2. 找到包含以下行的文本块：

   ```
   #!com.hp.nnm.icmp.payload.sizeInBytes=4096
   ```
3. 取消代码行的注释并进行编辑，将 4096 值更改为您需要的负载值，以呈现以下内容：

   ```
   com.hp.nnm.icmp.payload.sizeInBytes=4096
   ```

   `sizeInBytes` 参数使用的最小值为 12 字节，最大值为 65492 字节。

备注: 要配置数据负载大小，必须至少定义其中一个组属性。如果未如以下步骤中所述定义任一组属性，则 NNMi 将忽略 `com.hp.nnm.icmp.payload.sizeInBytes` 属性。

1. 找到包含以下行的文本块：

   ```
   #!com.hp.nnm.icmp.nodegroup.name=My Node Group
   ```
2. 取消代码行的注释并进行编辑，将“我的节点组”设置更改为您计划由 NNMi 监视设置引用的节点组，以呈现以下内容：

   ```
   com.hp.nnm.icmp.nodegroup.name=My Node Group
   ```

   备注: 您指定的节点组名称需是由 NNMi 监视设置引用的节点组。
3. 找到包含以下行的文本块：

   ```
   #!com.hp.nnm.icmp.ifacegroup.name=My Interface Group
   ```
4. 取消代码行的注释并进行编辑，将“我的接口组”设置更改为您计划由 NNMi 监视设置引用的接口组，以呈现以下内容：

   ```
   com.hp.nnm.icmp.ifacegroup.name=My Interface Group
   ```

   备注: 您指定的接口组名称需是由 NNMi 监视设置引用的接口组。
5. 重新启动 NNMi 管理服务器

   在 NNMi 管理服务器上运行 `ovstop` 命令：

   在 NNMi 管理服务器上运行 `ovstart` 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

配置 NNMi 如何确定设备的主机名

对于 NNMi 9.0 和较早版本，NNMi 在环回接口上查找所有可用的 IP 地址，为发现的设备找到有效的主机名。对于 NNMi 9.0 或更高版本，NNMi 开始使用管理 IP 地址(作为默认配置)确定发现的设备的主机名。

您可以将 HostNameMatchManagementIP 属性更改为 false，即可将 NNMi 配置为使用 NNMi 9.0 之前的方法为发现的设备找到有效主机名。

提示: 在大多数情况下，请保留此属性的默认值，即 true。有关 HostNameMatchManagementIP 属性的详细信息，请参阅 nms-disco.properties 文件。

要将 HostNameMatchManagementIP 属性更改为 false，请执行以下操作：

1. 编辑以下文件：

   Windows：%NNM_PROPS%\nms-disco.properties

   Linux：$NNM_PROPS/nms-disco.properties
2. 搜索包含以下属性的文本块：

   ```
   HostNameMatchManagementIP=true
   ```
3. 对属性值进行如下更改：

   ```
   HostNameMatchManagementIP=false
   ```
4. 保存操作。
5. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 ovstop 命令。

   在 NNMi 管理服务器上运行 ovstart 命令。

NNMi 在环回接口上查找所有可用的 IP 地址，为发现的设备找到有效的主机名。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

为 NNMi 配置字符集编码设置

根据为 NNMi 管理服务器配置的语言环境，您可能需要配置 NNMi 用于解释 SNMP OCTETSTRING 数据的源编码。为此，请按如下所示编辑 nms-jboss.properties 文件：

1. 编辑以下文件：
   - Windows：%NNM_PROPS%\nms-jboss.properties
   - Linux：$NNM_PROPS/nms-jboss.properties
2. 搜索包含以下行的文本块：

   ```
   #!com.hp.nnm.sourceEncoding=UTF-8
   ```
3. 取消以下代码行的注释并进行编辑，以呈现以下内容：

```
com.hp.nnm.sourceEncoding=UTF-8
```

4. 使用 nms-jboss.properties 文件中显示的说明和示例修改步骤 3 中显示的 UTF-8 属性值。
5. 保存更改。
6. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 ovstop 命令。

   在 NNMi 管理服务器上运行 ovstart 命令。

> **备注:** 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

配置 NNMi 等待 NNM iSPI 许可请求的时间

如果您注意到 NNMi 控制台响应缓慢或无响应，并且已安装一个或多个 NNM iSPI，则可能需要调整 NNMi 等待 NNM iSPI 许可请求响应的时间。

NNMi 等待 NNM iSPI 许可请求响应的默认时间为 20 秒。

要更改此默认值，请完成以下步骤：

1. 打开以下文件：

   Windows：%NNM_PROPS%\nms-jboss.properties

   Linux：$NNM_PROPS/nms-jboss.properties
2. 找到包含以下行的文本块：

   ```
   #!com.hp.ov.nms.licensing.EXTENSION_WAIT_TIMEOUT=20
   ```
3. 取消代码行的注释并进行修改，以呈现以下内容：

   com.hp.ov.nms.licensing.EXTENSION_WAIT_TIMEOUT=<以秒为单位的时间>

   例如，要将响应时间更改为 25 秒，请输入以下内容：

   ```
   com.hp.ov.nms.licensing.EXTENSION_WAIT_TIMEOUT=25
   ```

> **提示:** 可进行一些试验将此参数调整为最佳值。将参数调整为较高的值，减缓响应 NNM iSPI 的速度，如在较慢的服务器上运行的过忙的 NNM iSPI。

4. 重新启动 NNMi 管理服务器

   在 NNMi 管理服务器上运行 ovstop 命令。

   在 NNMi 管理服务器上运行 ovstart 命令。

管理用户界面属性

本部分描述如何在 ui.properties 文件中设置以下用户界面属性：

修改 NNMi 量表标题以显示 SNMP MIB 变量名称 (第 228 页)

修改 MIB 浏览器参数 (第 228 页)

允许第 2 级操作员删除节点和事件 (第 229 页)
允许第 2 级操作员编辑节点组图 (第 230 页)
允许第 1 级操作员运行状态和配置轮询 (第 231 页)

修改 NNMi 量表标题以显示 SNMP MIB 变量名称

NNMi 分析窗格中的**节点传感器量表**和**物理传感器量表**选项卡包含可在轮询 MIB OID 时显示 NNMi 组件名称的量表。这有助于您了解哪个量表与哪个组件相关。如果 NNMi 针对一个节点显示许多量表，则节点传感器名称可帮助区分量表。例如，如果某个节点包含大量的 CPU，则 NNMi 对各个 CPU 显示不同的名称。

此功能禁用时，NNMi 对所有 CPU 显示相同的 SNMP MIB 变量名称。

如果要将此属性更改为将量表标题显示为 SNMP MIB 变量名称而非 NNMi 节点传感器名称，请完成以下步骤：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS\nms-ui.properties`
   - Linux：`$NNM_PROPS/nms-ui.properties`
2. 找到包含以下行的文本块：

   ```
   com.hp.nnm.ui.analysisGaugeTitleIsNodeComponentName = true
   ```
3. 将以下行编辑为如下所示：

   ```
   com.hp.nnm.ui.analysisGaugeTitleIsNodeComponentName = false
   ```
4. 保存更改。
5. 重新启动 NNMi：
   a. 在 NNMi 管理服务器上运行 **ovstart** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstop** 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

修改 MIB 浏览器参数

如果使用 NNMi MIB 浏览器(**操作 > MIB 信息 > 浏览 MIB** 菜单)获取有关节点的信息，并提供该节点的可选 SNMP 团体字符串，则 NNMi MIB 浏览器将对 MIB 浏览器 SNMP 通信使用位于 nms-ui.properties 文件中的 MIB 浏览器参数。

备注: 如果使用 MIB 浏览器时不提供团体字符串，则 NNMi 将使用为节点建立的**通信配置**设置(如有)。这些设置使用**配置**工作区中的**通信设置**视图在 NNMi 控制台中配置。有关详细信息，请参阅 NNMi 帮助中的“配置通信协议”。

要修改 nms-ui.properties 文件中的 MIB 浏览器参数，请执行以下步骤：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS\nms-ui.properties`
   - Linux：`$NNM_PROPS/nms-ui.properties`
2. 找到包含以下行的文本块：

   `# MIB Browser Parameters`
3. 通过搜索包含以下文本的行，找到 `# MIB Browser Parameters` 下面的 MIB 浏览器参数：

   `mibbrowser`
4. 在 nms-ui.properties 文件中按照说明修改 MIB 浏览器参数。
5. 保存更改。
6. 重新启动 NNMi：
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

允许第 2 级操作员删除节点和事件

默认情况下，NNMi 允许 NNMi 管理员在 NNMi 中创建、编辑或删除节点或事件。可以为分配到 NNMi 第 2 级 (L2) 操作员用户组的帐户配置删除节点或事件的功能。可以使用以下某个方法实现这一点：

- (推荐)提升所需 L2 用户的特权以删除所需节点或事件。可使用 NNMi Web 控制台完成此操作。有关详细信息，请参阅 NNMi 管理员帮助。
- 将 NNMi 配置为在全局范围内启用 L2 用户以删除节点或事件。通过修改特定 NNMi 属性文件来覆盖默认特权，可完成此操作。

  警告: 仅使用覆盖方法即可实现全局启用。启用后，您无法在 NNMi Web 控制台中控制 L2 用户访问特权。

要启用 L2 用户以编辑或删除节点、其关联事件或这两者，请执行以下步骤：

1. 打开以下文件：

   Windows：`%NNM_PROPS%\nms-topology.properties`

   Linux：`$NNM_PROPS/nms-topology.properties`
2. 根据需要附加以下行：
   - 要启用 L2 用户以删除节点，请附加以下行：

     `permission.override.com.hp.nnm.DELETE_OBJECT=com.hp.nnm.ADMIN,com.hp.nnm.LEVEL2`
   - 要启用 L2 用户以删除事件，请附加以下行：

     `permission.override.com.hp.nnm.incident.DELETE=com.hp.nnm.ADMIN,com.hp.nnm.LEVEL2`

3. 保存该文件。
4. 重新启动 NNMi：
   - 在 NNMi 管理服务器上运行 ovstop 命令。
   - 在 NNMi 管理服务器上运行 ovstart 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

允许第 2 级操作员编辑节点组图

默认情况下，NNMi 允许 NNMi 管理员通过创建、修改和删除节点组编辑图。您也可以为分配到 NNMi 第 2 级操作员用户组的帐户配置此功能。

如果必须更改 NNMi 以允许分配到 NNMi 第 2 级操作员用户组的用户帐户创建、修改和删除其具有访问权限的节点上的节点组，请执行以下操作：

1. 打开以下文件：

   Windows：`%NNM_PROPS%\nms-ui.properties`

   Linux：`$NNM_PROPS/nms-ui.properties`
2. 搜索以下文本块并取消其注释。

   ```
   #!com.hp.nnm.ui.level2MapEditing = true
   ```
3. 保存更改。
4. 重新启动 NNMi：
   a. 在 NNMi 管理服务器上运行 **ovstart** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstop** 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

完成步骤 1 到步骤 4 后，NNMi 控制台发生如下更改：

- **库存 > 节点组**菜单为 NNMi 第 2 级操作员显示创建和删除工具栏图标。
- **库存 > 节点组**菜单包含 NNMi 第 2 级操作员的**操作 > 删除**菜单项。
- **所有节点组**文件夹显示在**拓扑图**工作区中。有关详细信息，请参阅 NNMi 联机帮助中的“关于工作区”。
- 对于节点组图，NNMi 控制台包含**保存布局**工具栏按钮和**文件 > 保存布局**菜单项。
- **保存布局**操作菜单的行为取决于是否为节点组图配置了节点组图设置。如果节点组图无节点组图设置，则必须创建一个。

您也可以配置 NNMi 以便 NNMi 第 2 级操作员用户有权创建节点组图设置：

1. 从 NNMi 控制台中，打开**拓扑图 > 节点组概述**。
2. 双击所需节点组。

NNMi 将打开与选定节点组关联的节点组图。

3. 打开要修改的节点组图设置：

   选择**文件 > 打开节点组图设置**。

4. 将**保存布局所需的最低 NNMi 角色**设置为“第 2 级操作员”。
5. 保存更改。

现在 NNMi 第 2 级操作员可以从节点组图视图创建、编辑和删除节点组图设置。

允许第 1 级操作员运行状态和配置轮询

NNMi 允许分配到 NNMi 第 2 级操作员用户组的用户帐户在其具有访问权限的节点上运行状态轮询和配置轮询。必须在 NNMi 控制台中更改“菜单项”配置，并在 `nms-topology.properties` 文件中更改每个帐户的对象访问特权级别。

要更改“菜单项”配置，使 NNMi 允许分配到 NNMi 第 1 级操作员用户组的用户帐户查看状态轮询菜单项，请执行以下操作：

1. 打开**配置 -> 用户界面 -> 菜单项 -> 状态轮询**表单。
2. 从**菜单项**选项卡中，滚动到**状态轮询**菜单项标签。
3. 从**菜单项上下文**选项卡中，打开每个必须更改的**所需 NNMi 角色**和**对象类型**项的条目。
4. 将您希望第 1 级操作员可执行状态轮询的每个对象类型的**所需 NNMi 角色**的值更改为“第 1 级操作员”。

   此步骤使分配到 NNMi 第 1 级操作员用户组的用户帐户可以查看指定对象类型的状态轮询操作。

要更改 NNMi 以允许分配到 NNMi 第 1 级操作员用户组的用户帐户查看配置轮询菜单项，请执行以下操作：

1. 打开**配置 -> 用户界面 -> 菜单项 -> 配置轮询**表单。
2. 从**菜单项上下文**选项卡中，打开每个必须更改的**所需 NNMi 角色**和**对象类型**项的条目。
3. 将您希望第 1 级操作员可配置轮询的每个对象类型的**所需 NNMi 角色**的值更改为“第 1 级操作员”。

   此步骤使分配到 NNMi 第 1 级操作员用户组的用户帐户可以查看指定对象类型的配置轮询操作。

备注: 您必须编辑 `nms-topology.properties` 文件才能允许分配到 NNMi 第 1 级操作员用户组的用户帐户从 NNMi 控制台同时运行状态轮询命令和配置轮询命令。如果您未完成这些步骤，NNMi 将在“操作”菜单中显示“状态轮询”和“配置轮询”选项，但用户尝试运行状态轮询或配置轮询命令时将看到错误消息。

要更改状态轮询和配置轮询所需的访问级别(所需的对象访问特权级别)，

1. 打开以下文件：

   Windows：`%NNM_PROPS%\nms-topology.properties`

   Linux：`$NNM_PROPS/nms-topology.properties`

2. 滚动到文件底部，然后添加以下行更改状态轮询：

```
permission.override.com.hp.nnm.STATUS_
POLL=com.hp.nnm.ADMIN,com.hp.nnm.LEVEL2,com.hp.nnm.LEVEL1
```

3. 添加以下行更改配置轮询：

   ```
   permission.override.com.hp.nnm.CONFIG_
   POLL=com.hp.nnm.ADMIN,com.hp.nnm.LEVEL2,com.hp.nnm.LEVEL1
   ```

4. 保存更改。
5. 重新启动 NNMi 管理服务器：
   a. 在 NNMi 管理服务器上运行 ovstop 命令。
   b. 在 NNMi 管理服务器上运行 ovstart 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

修改并发 SNMP 请求数

NNMi 保留了对一个节点发出三个并发 SNMP 请求的限制。这会降低节点的 SNMP 代理丢弃响应的风险。

可以将此值调整为更高，这将导致发现速度加快。但是，如果将值设置得太高，会增加丢弃响应的风险，并使发现的准确度降低。

如果要修改此限制，则执行以下步骤：

1. 编辑以下文件：
   - Windows：%NNM_PROPS%\nms-communication.properties
   - UNIX：$NNM_PROPS/nms-communication.properties
2. 要增大节点的并发 SNMP 请求的当前数目，请执行以下操作：
   a. 查找类似以下内容的行：

      ```
      #!com.hp.ov.nms.comm.snmp.maxConcurrentRequests=3
      ```

   b. 取消属性的注释：

      ```
      com.hp.ov.nms.comm.snmp.maxConcurrentRequests=3
      ```

      备注: 要取消属性的注释，请删除行开头的 #! 字符。

   c. 将现有值更改为所需的节点的并发 SNMP 请求数目。
   d. 保存更改。
3. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

修改嵌入式数据库端口

如果要将 NNMi 配置为对嵌入式数据库使用不同的端口，请执行以下步骤：

1. 编辑以下文件：
   - Windows：`%NNM_CONF%\nnm\props\nms-local.properties`
   - Linux：`$NNM_CONF/nnm/props/nms-local.properties`
2. 查找类似以下内容的行：

   `#!com.hp.ov.nms.postgres.port=5432`
3. 取消属性的注释：

   `com.hp.ov.nms.postgres.port=5432`

   > **提示:** 要取消属性的注释，请删除行开头的 `#!` 字符。
4. 将现有值更改为新端口号。
5. 保存更改。
6. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

修改 NNMi 标准化属性

NNMi 以区分大小写的格式存储主机名和节点名。这意味着 NNMi 控制台提供的所有搜索、排序和筛选操作都将返回区分大小写的结果。如果您使用的 DNS 服务器返回一系列保留大小写的节点名和主机名(包括全大写、全小写以及大小写混合)，则可能产生不是最佳的结果。

可以更改几个 NNMi 标准化属性以符合特定需要。好的做法是在对 NNMi 播种以进行初始发现之前进行这些更改。HP 建议您在部署期间(但在运行初始发现之前)对这一部分中的设置进行调整。

如果运行初始发现后又决定更改标准化属性，则可以运行 **nnmnoderediscover.ovpl -all** 脚本以启动完整发现。有关详细信息，请参阅 nnmnoderediscover.ovpl 参考页或 Linux 联机帮助页。

可以更改以下属性：

- 将发现的节点名规范化为 `UPPERCASE`、`LOWERCASE` 或 `OFF`。
- 将发现的主机名规范化为 `UPPERCASE`、`LOWERCASE` 或 `OFF`。

要更改标准化属性，请执行以下步骤：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS%\nms-topology.properties`
   - Linux：`$NNM_PROPS/nms-topology.properties`
2. 要配置 NNMi 以规范化发现的名称，请查找类似以下内容的行：

   `#!com.hp.ov.nms.topo.NAME_NORMALIZATION=OFF`

   a. 取消属性的注释：

      `com.hp.ov.nms.topo.NAME_NORMALIZATION=OFF`

> **备注:** 要取消属性的注释，请删除行开头的 **#!** 字符。

b. 将 OFF 更改为 LOWERCASE 或 UPPERCASE。
c. 保存更改。

3. 要配置 NNMi 以规范化发现的主机名，请查找类似以下内容的行：

   #!com.hp.ov.nms.topo.NAME_NORMALIZATION=OFF

   a. 取消属性的注释：

      com.hp.ov.nms.topo.HOSTNAME_NORMALIZATION=OFF

   b. 将 OFF 更改为 LOWERCASE 或 UPPERCASE。
   c. 保存更改。

4. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

> **备注:** 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

在初始发现之后更改标准化属性

在初始发现之后更改标准化属性将导致 NNMi 与属性更改不一致，直到进行下一次发现。要对此进行补救，请在更改 NNMi 标准化属性之后运行 **nnmnoderediscover.ovpl -all** 脚本以启动完整发现。

修改并发 SNMP 请求数

NNMi 保留了对一个节点发出三个并发 SNMP 请求的限制。这会降低节点的 SNMP 代理丢弃响应的风险。

可以将此值调整为更高，这将导致发现速度加快。但是，如果将值设置得太高，会增加丢弃响应的风险，并使发现的准确度降低。

如果要修改并发 SNMP 请求数限制，请执行以下步骤：

1. 打开以下文件：

   Windows：%NNM_PROPS%\nms-communication.properties

   Linux：$NNM_PROPS/nms-communication.properties

2. 查找类似以下内容的行：

   #!com.hp.ov.nms.comm.snmp.maxConcurrentRequests=3

3. 取消属性的注释：

   com.hp.ov.nms.comm.snmp.maxConcurrentRequests=3

提示: 要取消属性的注释，请删除行开头的 #! 字符。

4. 将现有值更改为所需的节点的并发 SNMP 请求数目。
5. 保存更改。
6. 重新启动 NNMi 管理服务器。

   在 NNMi 管理服务器上运行 `ovstop` 命令。

   在 NNMi 管理服务器上运行 `ovstart` 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

NNMi 自监视

NNMi 执行自监视检查，包括内存、CPU 和磁盘资源。当 NNMi 管理服务器资源不足或者检测到严重情况后，NNMi 将生成事件。

要查看 NNMi 运行状况信息，请使用以下某个方法：

- 从 NNMi 控制台，单击**帮助 > 系统信息**，然后单击**运行状况**选项卡。
- 要获取详细的自监视报告，请选择**帮助 > NNMi 系统信息 > 运行状况**，然后单击**查看详细的运行状况报告 (支持)**。
- 运行 **`nnmhealth.ovpl`** 脚本。

在 NNMi 检测到自监视运行状况异常之后，NNMi 在 NNMi 控制台的底部和表单的顶部显示状态消息。

要禁用此警告消息，请完成以下步骤：

1. 打开以下文件：
   - Windows：`%NNM_PROPS\nms-ui.properties`
   - Linux：`$NNM_PROPS/nms-ui.properties`
2. 找到包含以下行的文本块：

   ```
   #!com.hp.nms.ui.health.disablewarning=false
   ```
3. 取消以下代码行的注释并进行编辑，以呈现以下内容：

   ```
   com.hp.nms.ui.health.disablewarning==true
   ```
4. 保存更改。
5. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **`ovstop`** 命令。
   b. 在 NNMi 管理服务器上运行 **`ovstart`** 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop`

和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

抑制对特定节点使用发现协议

NNMi 使用几个协议来发现网络设备之间的第 2 层连接。有很多已定义的发现协议。例如，链路层发现协议 (LLDP) 是行业标准协议，此外还有很多特定于供应商的协议，比如针对 Cisco 设备的 Cisco 发现协议 (CDP)。

可以配置 NNMi 以抑制针对指定设备的发现协议采集。有些特殊情况可以通过抑制发现协议采集来补救。

下面是一些示例：

- Enterasys 设备：使用 SNMP 从一些 Enterasys 设备上的 Enterasys 发现协议 (EnDP) 和 LLDP 表采集信息可能会导致 NNMi 内存耗尽问题。通过配置 NNMi 以跳过对这些设备的 EnDP 和 LLDP 处理可以防止出现此问题。为此，请将设备的管理地址添加到 disco.SkipXdpProcessing 文件，如抑制使用发现协议采集 (第 236 页)中所示。

  备注: 一些 Enterasys 设备上的新操作系统版本支持 **set snmp timefilter break** 命令。在这些 Enterasys 设备上，运行 **set snmp timefilter break** 命令。如果使用此命令配置设备，则无需在 disco.SkipXdpProcessing 文件中列出设备。

- Nortel 设备：很多 Nortel 设备使用 SynOptics Network Management Protocol (SONMP) 来发现第 2 层布局和连接。这些设备中的一些设备在多个接口上使用相同 MAC 地址，并且使用此协议并不能很好地工作。如果两个互连的 Nortel 设备显示在错误的接口集之间存在第 2 层连接，并且此连接显示连接源为 SONMP，则您可能会遇到此问题。
  对于此示例，最好将 NNMi 配置为不使用 SONMP 协议来派生显示为参与错误连接的设备的第 2 层连接。为此，请将两个设备的管理地址添加到 disco.SkipXdpProcessing 文件，如抑制使用发现协议采集 (第 236 页)中所示。

抑制使用发现协议采集

如果要抑制此采集，请执行以下步骤：

1. 创建以下文件：
   - Windows：%NnmDataDir%\shared\nnm\conf\disco\disco.SkipXdpProcessing
   - Linux：$NnmDataDir/shared/nnm/conf/disco/disco.SkipXdpProcessing

   disco.SkipXdpProcessing 文件区分大小写。
2. 将设备 IP 地址添加到要抑制协议采集的所有设备的 disco.SkipXdpProcessing 文件。遵循 disco.SkipXdpProcessing 参考页或 Linux 联机帮助页中显示的说明。
3. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

   备注: 抑制一个或多个节点的发现协议处理可能会导致被管网络的第 2 层布局中发生某

些错误。HP 不对这些错误负责。

备注: ovjboss 服务在启动时读取 disco.SkipXdpProcessing 文件。在启动 NNMi 之后，如果进行任何更改，请重新启动 NNMi，如此步骤中所示。

备注: 如果在任何 Enterasys 设备上运行了 **setsnmp timefilter break** 命令，则从 disco.SkipXdpProcessing 文件删除设备地址，然后重新启动 NNMi，如此步骤中所示。当 NNMi 使用发现协议时，它会显示更准确的第 2 层映射。

有关详细信息，请参阅 disco.SkipXdpProcessing 参考页或 Linux 联机帮助页。

抑制管理出现故障的接口上的 IP 地址监视

NNMi 用户通常使用同一 IP 配置多个接口，接口管理启动时，地址会响应 ICMP 请求，而接口管理出现故障时不响应 ICMP 请求。这种情况下，这些出现管理故障的接口及其 IP 地址不应影响节点状态。

默认情况下，NNMi 会抑制管理出现故障的接口上的 IP 地址监视，从而防止节点状态发生改变。

可以通过执行以下操作，配置是否在管理出现故障的接口上执行 IP 地址监视：

1. 打开位于以下位置的 nms-disco.properties 文件：

   Windows：%NnmDataDir%\shared\nnm\conf\props\nms-disco.properties

   Linux：$NnmDataDir/shared/nnm/conf/props/nms-disco.properties
2. 在文件中查找类似以下的部分：

   ```
   #!com.hp.ov.nms.disco.suppressMonitoringOfAddressOnAdminDownInterface=true
   ```
3. 您可以对属性进行如下配置：

   要抑制管理出现故障的接口上的 IP 地址监视，请取消代码行的注释以将属性设置为 true(默认设置)。代码行类似以下内容：

   ```
   com.hp.ov.nms.disco.suppressMonitoringOfAddressOnAdminDownInterface=true
   ```

   要使 NNMi 在管理出现故障的接口上监视 IP 地址，请取消代码行的注释并对属性值进行如下编辑：

   ```
   com.hp.ov.nms.disco.suppressMonitoringOfAddressOnAdminDownInterface=false
   ```
4. 保存对 nms-disco.properties 文件的更改。
5. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 ovstop 命令。

   在 NNMi 管理服务器上运行 ovstart 命令。

抑制对大型交换机使用 VLAN 索引

NNMi 用于了解被管网络中交换机设备之间的第 2 层连接的一个方法是从交换机检索 dot1dTpFdbTable (FDB)。但对于 Cisco 交换机，NNMi 必须使用 VLAN 索引方法才能检索整个 FDB。如果每个设备上配置了很多 VLAN，则通过 VLAN 索引检索 FDB 可能需要数小时才能完成。

Cisco 交换机通常配置为使用 Cisco Discovery Protocol (CDP)。CDP 被视为用于了解第 2 层连接的上佳方法。位于网络核心的大型交换机可能包含很多 VLAN。这些交换机通常不直接连接终端节点。如果要管理的交换机不直接连接终端节点，则可能要在这些大型交换机上抑制 FDB 的采集。NNMi 仍然使用从 CDP 采集的数据完成第 2 层发现。这些大型交换机是抑制 VLAN 索引的主要备选设备。不要在网络边缘连接了很多终端节点的较小交换机(通常称为访问交换机)上抑制 VLAN 索引。

可以配置 NNMi 以抑制 VLAN 索引。为此，NNMi 管理员需要创建大型交换机的管理地址或地址范围并将其添加到 disco.NoVLANIndexing 文件，如抑制使用 VLAN 索引 (第 238 页)中所示。ovjboss 服务在启动时会读取 disco.NoVLANIndexing 文件。如果 NNMi 管理员在 ovjboss 服务启动之后对 disco.NoVLANIndexing 文件进行更改，那么在下次 ovjboss 服务启动之后，这些更改才会生效。默认情况下，disco.NoVLANIndexing 文件不存在。如果 disco.NoVLANIndexing 不存在，则此功能被禁用，并且 NNMi 尝试使用 VLAN-indexing 在所有设备上采集整个 FDB 表。

抑制使用 VLAN 索引

如果要禁用此 vlan-indexing，请执行以下步骤：

> **备注:** 抑制一个或多个节点的 vlan 索引可能会导致被管网络的第 2 层布局中发生某些错误。HP 不对这些错误负责。

1. 创建以下文件：
   - Windows：%NnmDataDir%\shared\nnm\conf\disco\disco.NoVLANIndexing
   - Linux：$NnmDataDir/shared/nnm/conf/disco/disco.NoVLANIndexing

   disco.NoVLANIndexing 文件区分大小写。
2. 将设备 IP 地址或地址范围添加到要禁用 vlan 索引的所有设备的 disco.NoVLANIndexing 文件。遵循 disco.NoVLANIndexing 参考页或 UNIX 联机帮助页中显示的说明。
3. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

   > **备注:** ovjboss 服务在启动时读取 disco.NoVLANIndexing 文件。

> **备注:** 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

有关详细信息，请参阅 disco.Disco.NoVLANIndexing 参考页或 Linux 联机帮助页。

计划服务中断

NNMi 允许使用 nnmscheduledoutage.ovpl 命令计划任意节点集的服务中断。例如，您可能需要计划服务中断以便对一组路由器进行每周维护，或更换节点的电源。

有关详细信息，请参阅 nnmscheduledoutage.ovpl 参考页或 Linux 联机帮助页。

提示: 有关使用 NNMi 控制台计划服务中断的详细信息，请参阅 NNMi 帮助。

配置传感器状态

NNMi 包含以下物理传感器和节点传感器，监视这些传感器可帮助确定状态：

物理传感器和节点传感器

物理传感器	是否默认将状态传播到物理组件？	节点传感器	是否默认将状态传播到节点？
FAN	是	CPU	否
POWER_ SUPPLY	是	MEMORY	是
TEMPERATURE	否	BUFFERS	否
VOLTAGE	否	DISK_ SPACE	否
BACK_PLANE	是		

备注: 默认情况下，FAN、POWER_SUPPLY、BACK_PLANE 和 MEMORY 将其状态传播到物理组件级别。例如，如果风扇的状态指示器为红色，则其对应的物理组件(机箱)接收黄色的状态指示器。在这种情况下，将向查看某机箱状态的用户发出警报，告知该机箱的组件出现某种故障的事实。

配置物理传感器状态

通过执行以下部分中的步骤，可以配置是否将物理传感器的状态传播到物理组件(例如，机箱)级别。

将物理传感器状态传播到物理组件

1. 如果尚不存在，使用名称 nnm-apa.properties 在以下目录中创建一个新属性文件：

   Windows：%NnmDataDir%\shared\nnm\conf\props

   Linux：$NnmDataDir/shared/nnm/conf/props
2. 在该属性文件中，使用文本编辑器包括以下文本：

   com.hp.ov.nms.apa.PhysicalSensorPropagateToPhysicalComponentStatus_<类型>=true

其中 <类型> 是物理传感器。有关详细信息，请参阅配置传感器状态 (第 239 页)。

3. 保存该属性文件。
4. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 ovstop 命令。

   在 NNMi 管理服务器上运行 ovstart 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

将物理传感器状态配置为不传播到物理组件

1. 如果尚不存在，请使用名称 nnm-apa.properties 在以下目录中创建一个新属性文件：

   Windows：%NnmDataDir%\shared\nnm\conf\props

   Linux：$NnmDataDir/shared/nnm/conf/props
2. 在该属性文件中，使用文本编辑器包括以下文本：

   com.hp.ov.nms.apa.PhysicalSensorNoPropagateToPhysicalComponentStatus_<类型>=true

   其中 <类型> 是物理传感器。有关详细信息，请参阅配置传感器状态 (第 239 页)。
3. 保存该属性文件。
4. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 ovstop 命令。

   在 NNMi 管理服务器上运行 ovstart 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

覆盖物理传感器状态值

默认情况下，由原因引擎将三个传感器状况值(None、Warning 和 Unavailable)映射到最多一个 Normal 状态。您可以覆盖这些默认状况映射，使 None、Warning 和 Unavailable 映射到 Critical。

要覆盖物理传感器状态值：

1. 如果尚不存在，请使用名称 nnm-apa.properties 在以下目录中创建一个新属性文件：

   Windows：%NnmDataDir%\shared\nnm\conf\props

   Linux：$NnmDataDir/shared/nnm/conf/props
2. 在该属性文件中，使用文本编辑器包括下面的一行、两行或全部三行(如果适用)：

   com.hp.ov.nms.apa.PhysicalSensorValueReMappedToDown_None=true

   com.hp.ov.nms.apa.PhysicalSensorValueReMappedToDown_Warning=true

   com.hp.ov.nms.apa.PhysicalSensorValueReMappedToDown_Unavailable= true
3. 保存该属性文件。
4. 重新启动 NNMi 管理服务器

在 NNMi 管理服务器上运行 ovstop 命令。

在 NNMi 管理服务器上运行 ovstart 命令。

备注: 可以将 Unavailable 状况映射到 Unpolled 状态(因为 Unavailable 意味着测量设备不可用)。这种情况会经常发生，因为是传感器不起作用，而非组件不起作用。要将 Unavailable 映射到 Unpolled，请使用刚刚所述的相同过程，但在步骤 2 中请使用以下文本：

```
com.hp.ov.nms.apa.PhysicalSensorValueReMappedToUnpolled_Unavailable= true
```

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

配置节点传感器状态

通过执行以下部分中的步骤，可以配置是否将节点传感器的状态传播到节点级别。

将节点传感器状态传播到节点

1. 如果尚不存在，使用名称 nnm-apa.properties 在以下目录中创建一个新属性文件：

   Windows：%NnmDataDir%\shared\nnm\conf\props

   Linux：$NnmDataDir/shared/nnm/conf/props
2. 在该属性文件中，使用文本编辑器包括以下文本：

   com.hp.ov.nms.apa.NodeSensorPropagateToNodeStatus_<类型>=true

   其中 <类型> 是节点传感器。有关详细信息，请参阅配置传感器状态 (第 239 页)。
3. 保存该属性文件。
4. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 ovstop 命令。

   在 NNMi 管理服务器上运行 ovstart 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

将节点传感器的状态配置为不传播到节点

1. 如果尚不存在，使用名称 nnm-apa.properties 在以下目录中创建一个新属性文件：

   Windows：%NnmDataDir%\shared\nnm\conf\props

   Linux：$NnmDataDir/shared/nnm/conf/props
2. 在该属性文件中，使用文本编辑器包括以下文本：

   com.hp.ov.nms.apa.NodeSensorNoPropagateToNodeStatus_<类型>=true

   其中 <类型> 是节点传感器。有关详细信息，请参阅配置传感器状态 (第 239 页)。
3. 保存该属性文件。

4. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 ovstop 命令。

   在 NNMi 管理服务器上运行 ovstart 命令。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

覆盖节点组件状态值

默认情况下，由原因引擎将三个节点组件状况值(None、Warning 和 Unavailable)映射到最多一个 Normal 状态。您可以覆盖这些默认状况映射，使 None、Warning 和 Unavailable 映射到 Critical。

覆盖节点组件状态值：

1. 如果尚不存在，使用名称 nnm-apa.properties 在以下目录中创建一个新属性文件：
   - Windows：%NnmDataDir%\shared\nnm\conf\props
   - Linux：$NnmDataDir/shared/nnm/conf/props
2. 在该属性文件中，使用文本编辑器包括下面的一行、两行或全部三行(如果适用)：

   ```
   com.hp.ov.nms.apa.NodeComponentValueReMappedToDown_None: true
   com.hp.ov.nms.apa.NodeComponentValueReMappedToDown_Warning: true
   com.hp.ov.nms.apa.NodeComponentValueReMappedToDown_Unavailable: true
   ```

   备注: 可以将 Unavailable 状况映射到 Unpolled 状态(因为 Unavailable 意味着测量设备不可用)。这种情况会经常发生，因为是传感器不起作用，而非组件不起作用。要将 Unavailable 映射到 Unpolled，请使用以下文本：

   ```
   com.hp.ov.nms.apa.NodeComponentValueReMappedToUnpolled_Unavailable: true
   ```

3. 保存该属性文件。
4. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 ovstop 命令。

   在 NNMi 管理服务器上运行 ovstart 命令。

   备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

导入接口的输入和输出速度

NNMi 允许您使用 nnmsetiospeed.ovpl 命令导入接口的输入和输出速度。此命令支持您指定一组接口或某个给定节点所有接口的输入和输出速度。您还可以使用逗号分隔值 (CSV) 文件指定导

入标准。导入的值显示在 NNMi 控制台的“接口”表单中。

有关详细信息，请参阅 nnmsetiospeed.ovpl 参考页或 Linux 联机帮助页。

NNMi 日志记录

本部分描述 NNMi 日志文件格式以及如何更改日志文件属性以记录登录和注销活动：

- NNMi 日志文件 (第 243 页)
- 登录和注销日志记录 (第 243 页)

有关更改审核日志文件的信息，另请参阅 NNMi 审核 (第 103 页)。

NNMi 日志文件

要调查 HP Network Node Manager i Software (NNMi) 性能或观察 NNMi 进程和服务的行为方式，可以查看显示进程和服务活动的历史记录的日志文件。这些文件可从以下位置获取：

- Windows：%NnmDataDir%\log\nnm\
- Linux：$NnmDataDir/log/nnm

NNMi 以 name.log 文件名格式存储这些日志文件。任何存档的日志文件都附加一个数字，采用名称 .log.%g 格式。

- name 是日志文件的基本名称。
- %g 与存档的日志文件的存档编号相关。追加的最高存档编号表示最早的文件。

在日志文件的大小超过配置的限制后，该日志文件可以变为存档的日志文件。在日志文件超过配置的限制后，上个活动日志文件将存档。例如，在 NNMi 将 nnm.log 文件存档为 nnm.log.1 文件后，NNMi 开始记录到新的 nnm.log 文件。

NNMi 在以下日志记录级别记录消息：

- SEVERE：与异常 NNMi 行为相关的事件。
- WARNING：指示可能会引起问题的事件，以及 SEVERE 日志记录级别中包含的所有消息。
- INFO：写入到 NNMi 控制台(或其等价设备)中的消息，以及 WARNING 日志记录级别中包含的所有消息。

登录和注销日志记录

NNMi 10.01 没有配置为针对登录或注销 NNMi 控制台的每个用户生成日志条目。如果要将 NNMi 配置为记录登录和注销活动，请执行以下操作：

1. 编辑以下文件：
   - Windows：%NnmDataDir%\shared\nnm\conf\props\nnm-logging.properties
   - Linux：$NnmDataDir/shared/nnm/conf/props/nnm-logging.properties
2. 搜索包含以下行的文本块：

   com.hp.ov.nnm.log.signin.level = OFF
3. 将此行修改为如下所示：

```
com.hp.ov.nnm.log.signin.level = INFO
```

4. 保存更改。
5. 重新启动 NNMi 管理服务器：
   a. 在 NNMi 管理服务器上运行 **ovstop**。
   b. 在 NNMi 管理服务器上运行 **ovstart**。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

更改管理服务器

可以在另一个系统上复制 HP Network Node Manager i Software 配置，例如，要从测试环境移动到生产环境时或更改 NNMi 管理服务器的硬件时。

可以更改 NNMi 管理服务器的 IP 地址，而不影响 NNMi 配置。

本章包含以下主题：

- 准备 NNMi 配置供移动的最佳实践 (第 244 页)
- 移动 NNMi 配置和嵌入式数据库 (第 245 页)
- 移动 NNMi 配置 (第 245 页)
- 恢复 NNMi 公钥证书 (第 245 页)
- 更改独立 NNMi 管理服务器的 IP 地址 (第 248 页)
- 更改 NNMi 管理服务器的主机名或域名 (第 248 页)
- 更改 Oracle 数据库实例连接信息 (第 249 页)
- 更改 NNMi 用于连接 Oracle 数据库实例的密码 (第 250 页)

准备 NNMi 配置供移动的最佳实践

以下最佳实践应用于将 NNMi 配置移动到其他系统：

- 如果节点组配置使用主机名识别被管节点，则生产和测试 NNMi 管理服务器必须使用相同的 DNS 服务器。如果生产和测试系统使用不同的 DNS 服务器，则被管节点的已解析名称中的更改可能导致两个 NNMi 管理服务器之间存在不同的轮询设置。
- 可以只将配置导出给一个作者。创建对组或公司来说唯一的新作者值。创建或修改以下任何项时，指定此作者值：
  - 设备配置文件
  - 事件配置
  - URL 操作
- 如果计划安装 Smart Plug-in (iSPI)，请参阅相应的 NNM iSPI 文档。所有 NNM iSPI 的文档都可从 HP 软件产品手册网站 (http://support.openview.hp.com/selfsolve/manuals) 获取。

移动 NNMi 配置和嵌入式数据库

要移动 NNMi 配置和嵌入式数据库(例如从测试系统到生产系统)，请在源(测试)系统上执行所有 NNMi 数据的完整备份，然后将备份恢复到目标(生产)系统。

要确保在备份之后没有对 NNMi 数据库作出更改，请停止所有 NNMi 进程，并创建脱机备份。例如：

```
nnmbackup.ovpl -type offline -scope all -target nnmi_backups\offline
```

确保新系统符合不同系统恢复 (第 201 页)中列出的要求，然后运行与以下示例类似的命令：

```
nnmrestore.ovpl -source nnmi_backups\offline\newest_backup
```

警告: NNMi 使用相同 SSL 证书来访问数据库(嵌入式或外部)和支持对 NNMi 控制台的 HTTPS 访问。当 NNMi 进程第一次在源系统上启动时，会创建用于访问数据库的证书。此证书包含在备份和恢复数据中。如果没有此证书，NNMi 将无法从目标系统访问数据库。

但是，对于对 NNMi 控制台的 HTTPS 访问，必须在目标系统上生成 SSL 证书。因为当前实现的 jboss 不支持证书合并，并且如果系统是通过恢复来自其他系统的数据而建立的，则 NNMi 不支持对 NNMi 控制台的 HTTPS 访问。如果目标系统必须支持对 NNMi 控制台的 HTTPS 访问，请使用移动 NNMi 配置 (第 245 页)中描述的过程，然后在目标系统上开始全新的数据采集。

移动 NNMi 配置

使用 `nnmconfigexport.ovpl` 命令将 NNMi 配置输出到 XML 文件。然后，使用 `nnmconfigimport.ovpl` 命令，将此配置从 XML 文件移至新系统上的 NNMi 中。

警告: 在使用 nnmconfigimport.ovpl 脚本导入文件之前，不要编辑使用 nnmconfigexport.ovpl 脚本导出的文件。

有关这些命令的信息，请参阅相应的参考页或 Linux 联机帮助页。

提示: `nnmconfigexport.ovpl` 命令不保留 SNMPv3 凭据。有关详细信息，请参阅 `nnmconfigexport.ovpl` 参考页或 Linux 联机帮助页。

备注: 只能移动 NNMi 配置。HP 不支持将拓扑或事件数据从一个 NNMi 管理服务器移动到其他 NNMi 管理服务器。HP 也不支持移动 iSPI 数据，比如为 NNM iSPI Performance for Metrics 采集的性能数据。

恢复 NNMi 公钥证书

警告: 如果 NNMi 管理服务器参与 NNMi 应用程序故障转移或是高可用性 (HA) 群集的成员，请联系支持代表以获取帮助。

nnm.keystore 文件存储 NNMi 用于加密的公钥证书。NNMi 安装进程创建 nnm.keystore 文件，并将此文件中的证书链接到 NNMi 数据库(Postgres 或 Oracle)中的 nms_sec_key 记录。

如果之后卸载 NNMi，但在随后重新安装之前不删除(Oracle 用户的级联删除)NNMi 的 Oracle 用户和数据库表，则 nms_sec_key 条目对新创建的 nnm.keystore 文件无效。

要恢复 NNMi 公钥证书，请完成以下任务：

任务 1：确定 KeyManager 服务的状态 (第 246 页)

任务 2：备份当前 nnm.keystore 文件 (第 246 页)

任务 3：尝试找到原始 nnm.keystore 文件 (第 246 页)

任务 4：如果可用，则恢复原始 nnm.keystore 文件 (第 247 页)

任务 1：确定 KeyManager 服务的状态

1. 运行以下命令：

   ```
   ovstatus -v ovjboss
   ```

2. 在命令输出中，验证 KeyManager 服务是否未在运行，这通常表示 nnm.keystore 文件损坏或丢失。

   > **备注:** 如果 ovstatus 输出显示 KeyManager 服务已启动，请联系支持代表以获取帮助。

任务 2：备份当前 nnm.keystore 文件

1. 切换到包含 NNMi 信任库的目录：

   Windows：%NnmDataDir%\shared\nnm\certificates

   Linux：$NnmDataDir/shared/nnm/certificates

2. 出于备份目的，保存以下文件的副本：

   ```
   nnm.keystore
   ```

   ```
   nnm.truststore
   ```

任务 3：尝试找到原始 nnm.keystore 文件

1. 确定 NNMi 数据库中的安全密钥的指纹：
   - 对于嵌入式 Postgres 数据库，输入以下内容：
     - Windows：

       ```
       %NnmInstallDir%\nonOV\Postgres\bin\psql -U postgres
       -d nnm -c "<数据库命令>"
       ```

     - Linux：

       ```
       $NnmInstallDir/nonOV/Postgres/bin/psql -U postgres
       -d nnm -c "<数据库命令>"
       ```

用以下 SQL 命令字符串替换 <数据库命令>:

```
select fingerprint from nms_sec_key;
```

- 对于 Oracle 数据库，请求 Oracle 数据库管理员在相应的 Oracle 管理工具中运行 <数据库命令>(之前在此步骤中针对嵌入式数据库有述)。

命令结果应当是单个数据库行。正确的 nnm.keystore 文件还包含此指纹。

2. 识别要测试的备份 nnm.keystore 文件。

   此文件可能在原始安装目录中的 NNMi 管理服务器的备份中。

3. 测试备份 nnm.keystore 文件的指纹：

   a. 切换到包含 NNMi 证书的目录：

      Windows：%NnmDataDir%\shared\nnm\certificates

      Linux：$NnmDataDir/shared/nnm/certificates

   b. 检查密钥库的内容：

      - Windows：

        ```
        %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool -list
        -keystore nnm.keystore
        ```

      - Linux：

        ```
        $NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -list
        -keystore nnm.keystore
        ```

      当提示输入密钥库密码时，输入：nnmkeypass

      密钥库输出形式为：

      ```
      Keystore type: jks
      Keystore provider:SUN
      Your keystore contains 1 entry
      selfsigned, Oct 28, 2008, keyEntry,
      Certificate fingerprint (MD5):29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
      ```

   c. 将此 nnm.keystore 文件中的 MD5 指纹的值与 NNMi 数据库中的指纹(来自此任务的步骤 1)进行比较。

      - 如果指纹完全匹配，则已经找到此 NNMi 数据库的合适 nnm.keystore 文件。继续执行任务 4：如果可用，则恢复原始 nnm.keystore 文件 (第 247 页)。
      - 如果指纹不完全匹配，则使用其他 nnm.keystore 文件执行此任务。

备注: 如果无法使用上面的过程找到原始 nnm.keystore 文件，请联系支持代表以获取帮助。不要继续执行任务 4：如果可用，则恢复原始 nnm.keystore 文件 (第 247 页)。

任务 4：如果可用，则恢复原始 nnm.keystore 文件

如果找到正确的 nnm.keystore 文件，请执行以下步骤以恢复该文件：

1. 停止 NNMi 管理服务器。

   在 NNMi 管理服务器上运行 `ovstop` 命令。
2. 将找到的 `nnm.keystore` 文件复制到以下位置中的现有文件上：

   Windows：`%NnmDataDir%\shared\nnm\certificates`

   Linux：`$NnmDataDir/shared/nnm/certificates`
3. 启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 `ovstart` 命令。
4. 运行以下命令：

   ```
   ovstatus -v ovjboss
   ```
5. 在命令输出中，验证 KeyManager 服务是否已启动。

在验证 NNMi 正在正常运行之后，可以删除来自任务 2：备份当前 nnm.keystore 文件 (第 246 页)的 `nnm.keystore` 文件的备份副本。

更改独立 NNMi 管理服务器的 IP 地址

要更改 NNMi 管理服务器的 IP 地址，请执行以下步骤：

1. 导航到 `http://www.webware.hp.com`。
2. 登录；然后按照提示获取新 IP 地址的许可证密钥。
3. 将新许可证密钥复制到名为 `license.txt` 的文本文件。
4. 在命令提示符处，输入以下命令：

   ```
   nnmlicense.ovpl NNM -f license.text -nosync
   ```

   ```
   ovstop
   ```
5. 用新 IP 地址配置 NNMi 管理服务器。
6. 配置 DNS 服务器以识别 NNMi 管理服务器的新 IP 地址。
7. 重新启动 NNMi 管理服务器。
8. 在命令提示符处，输入以下命令：

   ```
   nnmlicense.ovpl NNM -g
   ```
9. 在 **Autopass:许可证管理**对话框中，单击**删除许可证密钥**。
10. 选择附加到要删除的旧 IP 地址的许可证密钥。
11. 选择**永久删除许可证**。
12. 单击**删除**；然后关闭对话框。

更改 NNMi 管理服务器的主机名或域名

备注: 如果 NNMi 管理服务器参与 NNMi 应用程序故障转移或是高可用性 (HA) 群集的成员，请联系支持代表以获取帮助。

要更改 NNMi 管理服务器的主机名和/或域名，请使用 `nnmsetofficialfqdn.ovpl` 命令将 NNMi 设置为使用 NNMi 管理服务器的新完全限定域名 (FQDN)。例如：

```
nnmsetofficialfqdn.ovpl newnnmi.servers.example.com
```

有关详细信息，请参阅 `nnmsetofficialfqdn.ovpl` 参考页或 Linux 联机帮助页。

备注: FQDN 是与域名组合在一起的主机名。如果更改域名或主机名，则将更改 NNMi 管理服务器的 FQDN。SSL 证书始终链接到 FQDN。证书中的通用名称 (CN) 字段必须与服务器 FQDN 匹配。因此，如果更改 FQDN，则必须拥有具有匹配的 CN 的新 SSL 证书。`nnmsetofficialfqdn.ovpl` 将更新 NNMi 管理服务器的 FQDN，并创建与新 FQDN 匹配的新自签名证书。但如果在使用 CA 证书，则必须生成新的 CA 证书。有关详细信息，请参阅生成 CA 签名证书 (第 258 页)。

如果更改 NNMi 管理服务器的 IP 地址(无论 FQDN 是否发生变化)，则必须获取新证书。有关详细信息，请参阅更改独立 NNMi 管理服务器的 IP 地址 (第 248 页)。

更改 Oracle 数据库实例连接信息

NNMi 一次可以连接一个 Oracle 数据库实例。可以配置此连接。

更改 Oracle 数据库实例连接信息的原因包括：

- 必须更改 Oracle 数据库服务器名称。
- 用于连接数据库的端口与另一个进程冲突，或者公司政策要求使用非默认端口。
- 必须重命名数据库实例(例如，为了符合公司政策)。
- 必须更换 Oracle 数据库服务器硬件。

要更改 NNMi 使用的 Oracle 数据库实例，请完成以下任务：

任务 1：更新 Oracle 数据库实例 (第 249 页)

任务 2：更新 NNMi 配置 (第 250 页)

任务 1：更新 Oracle 数据库实例

1. 停止 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 `ovstop` 命令
2. 通过移动数据库、重命名 Oracle 数据库服务器或其他必要的更改来准备 Oracle 数据库。
3. 验证目标 Oracle 数据库实例是否符合以下先决条件：
   - 存在数据库实例。
   - 数据库实例用当前 NNMi 数据填充。
   - 使用 Oracle 工具将 NNMi 数据从工作数据库实例复制到目标数据库实例。
   - 数据库实例正在运行。

任务 2：更新 NNMi 配置

1. 备份数据库连接配置文件：

   切换到以下目录：

   Windows：%NnmInstallDir%\nonOV\jboss\nms\server\nms\

   Linux：$NnmInstallDir/nonOV/jboss/nms/server/nms/

   在 nms 目录中，创建名为 deploy.save 的目录。

   将 nms-ds.xml 文件从 deploy 目录复制到 deploy.save 目录。

   > **警告:** 启动时，ovjboss 进程读取 deploy 目录层次结构中的所有文件。由于此原因，请将所部署文件的备份副本保存到 deploy 目录层次结构以外的某个位置，如在此示例中使用 deploy.save 目录所示。

2. 编辑数据库连接配置文件：

   切换到 deploy 目录。

   在任何文本编辑器中，打开 nms-ds.xml 文件。

   找到 connection-url 条目。

   例如：

   ```
   <connection-url>jdbc:oracle:thin:@ohost:1521:nnmidb1</connection-url>
   ```

   请关注此条目中的最后三个参数。它们的格式是 oracle_hostname:database_port:database_instance_name

   更改 connection-url 条目中的第四、第五和第六个参数中的一个或多个。

   例如：

   要指向其他 Oracle 数据库服务器，请将 ohost 更改为其他主机名。

   要在其他端口上连接到 Oracle 数据库服务器，请将 1521 更改为其他端口号。

   要连接到其他 Oracle 数据库实例，请将 nnmidb1 更改为其他数据库实例名称。

   > **备注:** 此数据库实例必须已存在。

   保存 nms-ds.xml 文件。

3. 启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 ovstart 命令。

更改 NNMi 用于连接 Oracle 数据库实例的密码

如果更改 Oracle 配置以使用其他密码连接到 NNMi 数据库实例，请执行以下步骤更新 NNMi 配置：

1. 停止 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 ovstop 命令。

2. 运行 nnmchangedbpw.ovpl 命令并遵循提示操作。

3. 启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 `ovstart` 命令。

有关详细信息，请参阅 `nnmchangedbpw.ovpl` 参考页或 Linux 联机帮助页。

第 6 章: 高级配置

本部分包含以下各章：

- 许可 NNMi (第 252 页)
- 管理证书 (第 255 页)
- 对 NNMi 使用单点登录 (SSO) (第 269 页)
- 将 NNMi 配置为支持公钥基础设施用户验证 (第 275 页)
- 配置 Telnet 和 SSH 协议以供 NNMi 使用 (第 294 页)
- 通过 LDAP 将 NNMi 与目录服务集成 (第 305 页)
- 管理 NAT 环境中的重叠 IP 地址 (第 331 页)
- NNMi 安全和多租户 (第 347 页)
- 全局网络管理 (第 366 页)
- 配置 NNMi Advanced 的 IPv6 功能 (第 386 页)

许可 NNMi

如果您未安装永久许可证密钥，NNMi 产品包含临时的瞬时启动许可证密钥，有效期为安装 NNMi 之后 60 天。此临时的瞬时启动许可证密钥使您能够使用 NNMi Ultimate 功能。应当尽早获取并安装永久许可证密钥。

备注: 如果已购买 NNMi(单独)、NNMi Advanced 以及 NNMi 附带的 NNM iSPI NET 功能，则有两种类型的许可证适用于应用程序故障转移和高可用性环境：

- 应用程序故障转移
  - 生产 - 不管您是否具有应用程序故障转移或高可用性环境，这是为 NNMi、NNMi Advanced 或 NNM iSPI NET 购买的主许可证。将此许可证与主服务器的 IP 地址关联。
  - 非生产 - 此许可证是为用于应用程序故障转移环境而单独购买的。将此许可证与辅助 (备用)服务器的 IP 地址关联。

  高可用性 (HA)
  - 生产 - 不管您是否具有应用程序故障转移或高可用性环境，这是为 NNMi、NNMi Advanced 或 NNM iSPI NET 购买的主许可证。将此许可证与某个物理群集节点的 IP 地址关联。
  - 非生产 - 此许可证是为用于高可用性环境而单独购买的。将此许可证与 NNMi HA 资源组的虚拟 IP 地址关联。
- 如果您已购买 NNMi Premium 或 NNMi Ultimate，则需要使用从 HP 密码交付中心请求的适用于应用程序故障转移或高可用性的一个或多个许可证密钥，而不要按照指示使用非生产许可证。务必请求以下功能：

- 高可用性：获取 NNMi HA 资源组的虚拟 IP 地址的许可证密钥。此许可证密钥最初在主服务器上使用，然后根据需要在辅助服务器上使用。
- 应用程序故障转移：获取两个许可证密钥；一个用于主服务器的物理 IP 地址，一个用于备用服务器的物理 IP 地址。

警告：不要在同一服务器上使用生产和非生产许可证。

- 还可以查看每个 NNM iSPI 的文档，该文档位于以下位置：http://h20230.www2.hp.com/selfsolve/manuals。

要查看 NNMi Ultimate 许可证所附带功能的列表，请参阅《HP NNMi Software Release Notes》的“licensing”部分。

准备安装永久许可证密钥

临时的瞬时启动许可证有 250 个节点的限制。如果一直在使用瞬时启动许可证密钥运行 NNMi，则您所管理的节点数目可能大于永久许可证支持的数目。

跟踪许可证信息时，请注意以下几点：

- **消耗**：NNMi 发现并管理的节点不得超过 NNMi 许可的容量限制(四舍五入)：
  - **VMware** 或 HPE Helion OpenStack 环境：包含 `vnwareVM` 或 `kvmVM` 设备配置文件的每个设备相当于 1/10 个节点。
  - 所有其他设备相当于一个发现的节点。

有关许可证限制的详细信息，请参阅《NNMi 管理员帮助》中的“跟踪 NNMi 许可证”。

- 如果发现的节点数达到或超过许可的容量限制，则除非发生以下情况之一，否则不会发现任何新的节点：
  - 安装许可证扩展。
  - 查看配置设置并将 NNMi 发现限制为仅发现网络环境中的重要节点。然后，删除节点并让 NNMi 重新发现重置节点的被管库存。

  有关详细信息，请参阅 NNMi 联机帮助。

检查许可证类型和被管节点数目

要确定 NNMi 正在使用的许可证类型，请执行以下步骤：

1. 在 NNMi 控制台中，单击**帮助 > 关于 HP Network Node Manager i Software**。
2. 在**关于 HP Network Node Manager i Software** 窗口中，单击**许可信息**。
3. 查找**消耗**字段中显示的值。这是 NNMi 当前正在管理的节点数。

   跟踪许可证信息时，请注意以下几点：
   - **消耗**：NNMi 发现并管理的节点不得超过 NNMi 许可的容量限制(四舍五入)：
     - **VMware** 或 HPE Helion OpenStack 环境：包含 `vnwareVM` 或 `kvmVM` 设备配置文件的每个设

备相当于 1/10 个节点。
- 所有其他设备相当于一个发现的节点。

有关许可证限制的详细信息，请参阅《NNMi 管理员帮助》中的“跟踪 NNMi 许可证”。

有关许可证限制的详细信息，请参阅《NNMi 管理员帮助》中的“跟踪 NNMi 许可证”。

4. 如果永久许可证支持的节点数目少于 NNMi 当前正在管理的数目，请使用 NNMi 控制台删除不重要的节点。有关详细信息，请参阅 NNMi 帮助中的“删除节点”。

获取和安装永久许可证密钥

要请求永久许可证密钥，请收集以下信息：

- 权利证书，包含 HP 产品号和订购号
- 某台 NNMi 管理服务器的 IP 地址
- NNMi HA 资源组的虚拟 IP 地址(如果许可证适用于以 HA 运行的 NNMi)
- 公司或组织信息

使用 Autopass 和 HP 订购号(在防火墙后不能实现)

要获取并安装永久许可证密钥，请执行以下步骤：

1. 在命令提示符处，输入以下命令，以打开 Autopass 用户界面：

   nnmlicense.ovpl NNM -gui

2. 在 Autopass 窗口的左边，单击**许可证管理**。
3. 单击**安装许可证密钥**。
4. 单击**获取/安装许可证密钥**。
5. 输入 HP 订购号，并遵循 Autopass 提示以完成许可证密钥获取过程。
6. NNMi 自动完成安装。

使用命令行

如果自动过程不能运行至完成(例如，如果 NNMi 管理服务器在防火墙后运行)，则执行以下步骤：

1. 要获取许可证密钥，请通过以下地址访问 HP 密码交付服务：

   https://webware.hp.com/welcome.asp

2. 在 NNMi 管理服务器上，在命令提示符处输入以下命令以更新系统并存储许可证数据文件：

   nnmlicense.ovpl NNM -license_file

   (产品许可证 ID (NNM) 区分大小写。)

   有关详细信息，请参阅 nnmlicense.ovpl 参考页或 Linux 联机帮助页。

3. NNMi 自动完成安装。

获取其他许可证密钥

请联系 HP 销售代表或授权 Hewlett-Packard 零售商，以了解有关 NNMi 许可结构的信息以及如何针对企业安装添加许可级别。

要获取其他许可证密钥，请访问 HP 许可证密钥交付服务：

https://webware.hp.com/welcome.asp

有关详细信息，请参阅 NNMi 帮助中的“扩展许可容量”。

开发人员注意事项： 使用 NNMi Developer Toolkit，通过集成自定义 Web 服务客户端，可以增强 NNMi 的功能。安装 NNMi 开发人员许可证之后，NNMi 将在 `doc` 文件夹中创建 `sdk-dev-kit.jar` 文件。解压缩 `sdk-dev-kit.jar` 文件以查看 NNMi Developer Toolkit 文档和示例。

管理证书

证书使浏览器能识别 Web 服务器。此证书可以自签名或由 CA(证书颁发机构)签名。`nnm.keystore` 文件存储私钥和证书及其相应的公钥。`nnm.truststore` 文件包含来自您希望与其通信的那一方的证书或来自您信任的证书颁发机构的证书，用于识别其他方。NNMi 在 `nnm.keystore` 和 `nnm.truststore` 文件中都包含自签名证书。

要使用某些 NNMi 功能，NNMi 管理服务器需要彼此共享其证书。本章包含的配置说明可用于在 NNMi 管理服务器之间复制这些证书，以及用 `nnmcertmerge.ovpl` 脚本将这些证书合并到 `nnm.keystore` 和 `nnm.truststore` 文件中。本章还包含用新的自签名证书或 CA 签名证书替换已过期证书的说明。

管理员可以禁用从网络对 NNMi 进行 HTTP 以及其他未加密的的访问。请参阅将 NNMi 配置为要求加密远程访问 (第 213 页)。

本章包含以下主题：

- 关于 NNMi 证书 (第 255 页)
- 将现有证书替换为新的自签名或 CA 签名证书 (第 257 页)
- 在应用程序故障转移环境中使用证书 (第 263 页)
- 在高可用性环境中使用证书 (第 264 页)
- 在全局网络管理环境中使用证书 (第 265 页)
- 配置与目录服务的 SSL 连接 (第 268 页)

关于 NNMi 证书

本部分描述可帮助您使用证书的有用术语。请熟悉下表中提及的术语。

证书术语

概念	描述
密钥	**信任库：** NNMi 信任库是 `nnm.truststore` 文件，存储来自希望 NNMi 信任的源的公

证书术语(续)

概念	描述
库和信任库	钥。 **密钥库**：NNMi 密钥库是 `nnm.keystore` 文件，其中导入的是 NNMi 服务器的私钥。 nnm.truststore 和 nnm.keystrore 文件位于： • Linux：`$NNM_DATA/shared/nnm/certificates/` • Windows：`%NNM_DATA%\shared\nnm\certificates\`
默认 NNMi 证书	NNMi 与使用默认属性生成的自签名证书一起安装。您可以使用其他自签名或 CA 签名证书替换默认证书。
工具	证书由 Java 的 Keytool 实用程序生成和管理。此外，NNMi 还提供 `nnmmergecert.ovpl` 实用程序，用于合并证书以在 NNMi 系统内建立信任。此程序在 HA、故障转移和 GNM-RNM 安装中使用。
支持的加密算法	NNMi 接受使用 RSA 算法生成的证书。不支持 DSA 算法。
自签名证书	自签名证书通常用于建立服务器和已知客户端组之间的安全通信。NNMi 与使用默认属性生成的自签名证书一起安装。 **备注:** 用户尝试在 Web 浏览器中访问 NNMi Web 控制台时，配置为使用自签名证书的 NNMi 实例将显示警告消息。
CA 签名证书	作为证书签名请求的响应收到的签名服务器证书中将包含 CA 签名的 NNMi 证书以及一个或多个 CA 证书(如果存在多个 CA 证书，则也称为证书链)。 **备注:** 这些证书可能在单个文件中，也可能在两个单独的文件中。
根 CA 证书	标识信任其为服务器和用户签名证书的机构。
中级 CA 证书	由根 CA 或本身是机构、而非服务器或用户的中级 CA 签名的证书。 **备注:** 从 NNMi 服务器证书到根 CA 证书的证书列表，包括所有中级 CA 证书，称为证书链。

将现有证书替换为新的自签名或 CA 签名证书

NNMi 安装期间将创建并安装自签名证书。通常会在以下任一场景中替换证书：

- 使用新的自签名或 CA 签名证书代替默认证书。
- 续订已过期的证书。

要替换证书，请执行以下操作：

1. 生成自签名证书。有关详细信息，请参阅生成自签名证书 (第 257 页)。
2. 如果您的组织要求由 CA 对证书签名，则生成 CSR(证书签名请求)文件并获取 CA 签名证书。有关详细信息，请参阅生成 CA 签名证书 (第 258 页)
3. 打开以下文件，并将 `com.hp.ov.nms.ssl.KEY_ALIAS` 变量更新为生成证书时所用的 `<alias>` 的值。
   - Windows：`%NNM_CONF%\nnm\props\nms-local.properties`
   - Linux：`$NNM_CONF/nnm/props/nms-local.properties`
4. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 `ovstop` 命令。
   b. 在 NNMi 管理服务器上运行 `ovstart` 命令。

   > **备注:** 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

5. 使用以下语法测试到 NNMi 控制台的 HTTPS 访问：

   https://<完全限定域名>:<端口号>/nnm/。

   如果使用的是 CA 签名证书并且浏览器信任 CA，则它会信任与 NNMi 控制台的 HTTPS 连接。

   如果使用的是自签名证书，则浏览器将显示一条警告消息，告知到 NNMi 控制台的 HTTPS 连接不受信任。

生成自签名证书

要生成自签名证书，请执行以下步骤：

1. 切换到 NNMi 管理服务器上包含 `nnm.keystore` 和 `nnm.truststore` 文件的目录：
   - Windows：`%NnmDataDir%\shared\nnm\certificates`
   - Linux：`$NnmDataDir/shared/nnm/certificates`
2. 保存 `nnm.keystore` 文件的备份副本。

   > **备注:**
   > - 如果要替换现有 NNMi 证书，请在完成这些步骤之后再删除现有证书。NNMi 必须使用安装的旧证书和新证书启动至少一次，以便将加密信息传输到新证书。

- 确保别名如下一步中所述指向新证书，确保 NNMi 将 NNMi 管理服务器上的新证书提供给客户端服务器。

3. 从系统生成私钥。用 keytool 命令生成此私钥：
   a. 准确地按如下所示运行命令：
      - Windows：`%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -genkeypair -validity 3650 -keyalg rsa -keystore nnm.keystore -storepass nnmkeypass - alias <别名名称>`
      - Linux：`$NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -genkeypair -validity 3650 -keyalg rsa -keystore nnm.keystore -storepass nnmkeypass -alias <别名名称>`

      备注: 别名(此示例中称为 <别名名称>)表示新创建的密钥。尽管别名可以是任意字符串，但 HP 建议使用完全限定域名 (FQDN) 后跟一个后缀，帮助您轻松标识正确的版本。例如，您可以使用 `myserver.mydomain-<编号>` 或 `myserver.mydomain-<日期>` 作为别名名称。

   b. 输入请求的信息。

      警告: 提示输入姓名时，请输入系统的 FQDN。

      这样就生成了自签名证书。

      要获取 CA 签名证书，需要另外生成 CSR 文件并将该文件提交给 CA。有关详细信息，请参阅生成 CA 签名证书 (第 258 页)。

生成 CA 签名证书

要获取并安装 CA 签名证书，请执行以下步骤：

1. 生成自签名证书。有关详细信息，请参阅生成自签名证书 (第 257 页)。
2. 运行以下命令创建 CSR(证书签名请求)文件：
   - Windows：**`%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -keystore nnm.keystore -certreq -storepass nnmkeypass -alias <别名名称> -file CERTREQFILE`**
   - Linux：**`$NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -keystore nnm.keystore -certreq -storepass nnmkeypass -alias <别名名称> -file CERTREQFILE`**

   备注:
   - 在以上命令中，<别名名称>对应于生成证书时提供的别名。
   - 有关 keytool 命令的详细信息，请在 **http://www.oracle.com/technetwork/java/index.html** 上搜索“Key and Certificate Management Tool”(密钥和证书管理工具)。

3. 将 CSR 发送到负责签名并返回证书文件的 CA 签名颁发机构。有关各种类型的 CA 证书的信息，请参阅CA 签名证书的类型 (第 261 页)。

4. 将包含这些证书的文件复制到 NNMi 管理服务器上的某位置。对于此示例，请将文件复制到以下位置：
   - Windows：`%NnmDataDir%\shared\nnm\certificates`
   - Linux：`$NnmDataDir/shared/nnm/certificates`
5. 切换到 NNMi 管理服务器上包含 `nnm.keystore` 和 `nnm.truststore` 文件的目录：
   - Windows：`%NnmDataDir%\shared\nnm\certificates`
   - Linux：`$NnmDataDir/shared/nnm/certificates`
6. 运行以下命令将证书导入 `nnm.keystore` 文件：

   Windows：
   - **%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -importcert -trustcacerts -keystore nnm.keystore -storepass nnmkeypass -alias <别名名称> -file** <myserver.crt>

   Linux：
   - **$NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -importcert -trustcacerts -keystore nnm.keystore -storepass nnmkeypass -alias <别名名称> -file** <myserver.crt>

   备注:
   - 在以上命令中，
     - <myserver.crt> 对应于签名服务器证书存储位置的完整路径。
     - <别名名称> 对应于生成证书时提供的别名。
   - 如果使用 **-storepass** 选项并提供密码，则密钥库程序不提示您输入密钥库密码。如果不使用 **-storepass** 选项，则在提示输入密钥库密码时输入 **nnmkeypass**。
7. 系统提示您是否信任证书时，输入：**y**

   将证书导入密钥库的示例输出

   此命令的输出形式为：

   ```
   Owner:CN=NNMi_server.example.com
   Issuer:CN=NNMi_server.example.com
   Serial number:494440748e5
   Valid from:Tue Oct 28 10:16:21 MST 2008 until:Thu Oct 04 11:16:21 MDT 2108
   Certificate fingerprints:
   MD5:29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
   SHA1:C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03
   Trust this certificate?[no]:y
   Certificate was added to keystore
   ```
8. 运行以下命令将证书导入 `nnm.truststore` 文件：

- Windows：

  ```
  %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -import -alias <别名名称> -keystore nnm.truststore -file <myca.crt>
  ```

- Linux：

  ```
  $NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -import -alias <别名名称> -keystore nnm.truststore -file <myca.crt>
  ```

  备注:
  - 在以上命令中，
    - `<myca.crt>` 对应于 CA 证书存储位置的完整路径。
    - `<别名名称>` 对应于生成证书时提供的别名。
  - 如果使用 **-storepass** 选项并提供密码，则密钥库程序不提示您输入密钥库密码。如果不使用 **-storepass** 选项，则在提示输入密钥库密码时输入 **nnmkeypass**。

9. 在系统提示您输入信任库密码时，输入：**ovpass**。
10. 检查信任库的内容：
    - Windows：

      %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool -list -keystore nnm.truststore

    - Linux：

      $NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -list -keystore nnm.truststore

    在系统提示您输入信任库密码时，输入：**ovpass**

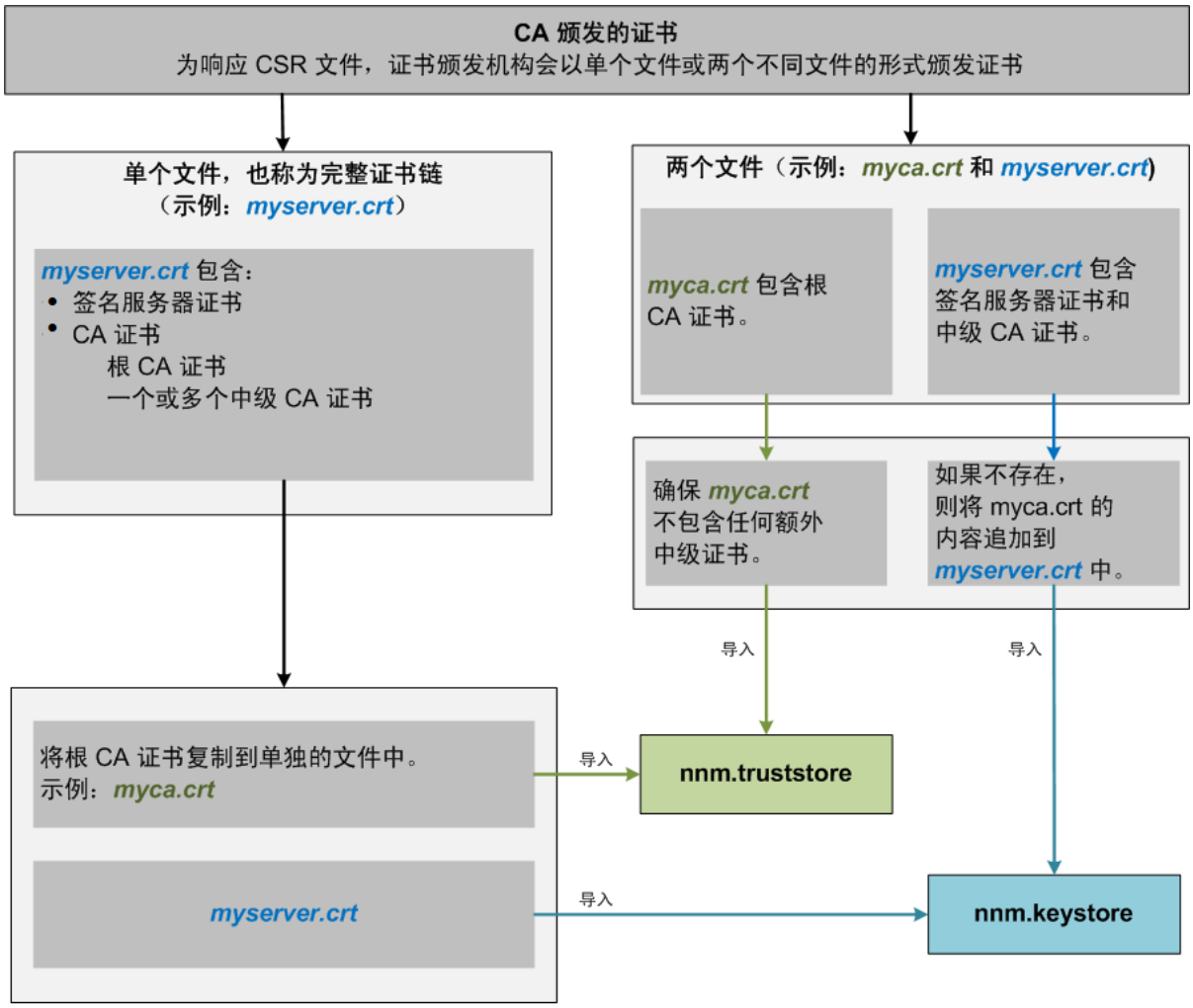
    示例信任库输出

    信任库输出形式为：

    ```
    Keystore type: jks

    Keystore provider:SUN

    Your keystore contains 1 entry

    nnmi_ldap, Nov 14, 2008, trustedCertEntry,

    Certificate fingerprint (MD5):29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
    ```

    提示: 信任库可以包括多个证书。

CA 签名证书的类型



备注: 如果 CA 采用其他形式返回证书，请与 CA 提供商联系，了解有关如何获取证书链和根 CA 证书的说明。

证书颁发机构 (CA) 应为您提供以下项之一：

- 包含**服务器证书**的签名服务器证书文件(CA 签名的 NNMi 证书)以及一个或多个 CA 证书。本部分将签名服务器证书称为 `myserver.crt`。

  CA 证书可以是下列任意一个：

  - 根 CA 证书 - 标识信任其为服务器和用户签名证书的机构。
  - 中级 CA 证书 - 由根 CA 或本身是机构、而非服务器或用户的中级 CA 签名的证书。

    备注: 从 NNMi 服务器证书到根 CA 证书的证书列表，包括所有中级 CA 证书，称为**证书链**。

- 一个签名服务器证书以及一个包含一个或多个 CA 证书的单独文件。本部分将签名的服务器证书称为 myserver.crt，将 CA 证书称为 myca.crt。myserver.crt 文件应包含单个服务器证书或证书链，而不包含应位于 myca.crt 文件中的根 CA 证书。

要使用新证书配置 NNMi，必须将证书链和根 CA 证书分别导入 nnm.keystore 和 nnm.truststore。将服务器证书导入到 nnm.keystore 文件中时使用 myserver.crt 文件，将 CA 证书导入到 nnm.truststore 文件中时使用 myca.crt 文件。

备注: 如果 CA 采用其他形式返回证书，请与 CA 提供商联系，了解有关获取单独的证书链和根 CA 证书的说明。

如果提供了一个包含完整证书链的文件，请将根 CA 证书从该文件复制到 myca.crt 文件。使用 myca.crt 文件导入 nnm.truststore，以便 NNMi 信任颁发证书的 CA。

如果提供了两个文件，请将 myca.crt 文件内容添加到 myserver.crt 末尾(如果后者不包括前者)，并从 myca.crt 中删除任何额外的中级证书(如果有)。这将使 myserver.crt 文件包含完整的证书链，而 myca.crt 文件包含根 CA 证书。

备注: 使用 CA 时，通常只会将根 CA 证书添加到 nnm.truststore。将中级 CA 证书或服务器证书添加到 nnm.truststore 将导致这些证书被显式信任，并且不针对其他信息(例如吊销)进行检查。仅在 CA 需要时将其他证书添加到 nnm.truststore。

以下示例显示了从 CA 签名颁发机构收到的文件的可能内容：

单独的服务器证书文件和 CA 证书文件：


```
-----BEGIN CERTIFICATE-----
Sample/AVQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
.....................................................................
.....................................................................
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
```


服务器证书和 CA 证书合并在一个文件中：


```
-----BEGIN CERTIFICATE-----
Sample1/VQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
.....................................................................
.....................................................................
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
```

-----BEGIN CERTIFICATE-----

Sample2/Gh0dHA6Ly9jb3JwMWRjc2cyLnNnLmludC5wc2FnbG9iYWwuY29tL0Nlc

RaOCApwwggKYMB0GA1UdDgQWBBSqaWZzCRcpvJWOFPZ/Be9b+QSPyDAfBgNVHSMC

.....

.....

Wp5Lz1ZJAOu1VHbPVdQnXnlBkx7V65niLoaT90Eqd6laliVlJHj7GBriJ90uvVGu

BQagggEChoG9bGRhcDovLy9DTj1jb3JwMWRjc2cyL==

-----END CERTIFICATE-----

在应用程序故障转移环境中使用证书

将证书用于应用程序故障转移

配置应用程序故障转移功能时，必须将两个节点的 nnm.keystore 和 nnm.truststore 文件的内容合并到单个 nnm.keystore 和 nnm.truststore 文件中。

完成以下步骤，将应用程序故障转移功能配置为使用自签名或 CA 签名证书。

警告: 如果对带有应用程序故障转移功能的 NNMi 使用自签名证书，并且未完成以下步骤，则 NNMi 进程不会在备用 NNMi 管理服务器(此示例中的服务器 Y)上正确启动。

1. 切换到服务器 Y 上的以下目录：
   - Windows：%NnmDataDir%\shared\nnm\certificates
   - Linux：$NnmDataDir/shared/nnm/certificates
2. 将 nnm.keystore 和 nnm.truststore 文件从服务器 Y 复制到服务器 X 上的某个临时位置。剩余步骤将引用这些文件位置作为 <密钥库> 和 <信任库>。
3. 在服务器 X 上运行以下命令将服务器 Y 的证书合并到服务器 X 的 nnm.keystore 和 nnm.truststore 文件中。

   Windows：

   ```
   nnmcertmerge.ovpl -keystore <密钥库> -truststore <信任库>
   ```

   Linux：

```
nnmcertmerge.ovpl -keystore <密钥库> -truststore <信任库>
```

4. 将合并的 nnm.keystore 和 nnm.truststore 文件从服务器 X 复制到服务器 Y，以使两个节点都有合并的文件。这些文件的位置如下：
   - Windows：%NnmDataDir%\shared\nnm\certificates
   - Linux：$NnmDataDir/shared/nnm/certificates
5. 在服务器 X 和服务器 Y 上运行以下命令。验证两个服务器显示的结果(包括完全限定域名)是否匹配。如果它们不匹配，请不要继续操作，而是重新执行263 到264。

   Windows：

   ```
   %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -list -keystore
   %NnmDataDir%\shared\nnm\certificates\nnm.keystore -storepass nnmkeypass
   ```

   Linux：

   ```
   $NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -list -keystore
   $NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass
   ```
6. 在服务器 X 和服务器 Y 上运行以下命令。验证两个服务器显示的结果(包括完全限定域名)是否匹配。如果它们不匹配，请不要继续操作，而是重新执行263 到264。

   Windows：

   ```
   %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -list -keystore
   %NnmDataDir%\shared\nnm\certificates\nnm.truststore
   -storepass ovpass
   ```

   Linux：

   ```
   $NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -list -keystore
   $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass
   ```
7. 继续按照为 NNMi 配置应用程序故障转移 (第 111 页)配置应用程序故障转移功能。

在高可用性环境中使用证书

本部分描述如何在 HA 环境中将 NNMi 配置为使用自签名证书或证书颁发机构证书。

对高可用性使用证书

使用默认证书配置高可用性

配置 NNMi 以 HA 运行的过程在主群集节点和辅助群集节点之间正确共享了默认自签名证书。不需要执行任何额外步骤即可对以 HA 运行的 NNMi 使用默认证书。

使用新证书配置高可用性

本部分将创建名为 newcert 的新自签名或 CA 证书。完成以下步骤，用此新 CA 或自签名证书配置 HA。

备注: 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改需要停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

提示: 可如高可用性环境中的共享 NNMi 数据 (第 158 页)中所述，在配置 NNMi 以 HA 运行之前或之后完成此过程。

1. 在完成步骤 2 之前，切换到 NNMi_HA1 上的以下目录：
   - Windows：%NnmDataDir%\shared\nnm\certificates
   - Linux：$NnmDataDir/shared/nnm/certificates
2. 在 NNMi_HA1 上，运行以下命令，将 newcert 导入到 nnm.keystore 文件中：
   - Windows：**%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool -import -alias newcert 别名 -keystore nnm.keystore -file newcert**
   - Linux：**$NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -import -alias newcert 别名 -keystore nnm.keystore -file newcert**
3. 在活动 (NNMi_HA1) 和备用 (NNMi_HA2) 节点上编辑以下文件：
   - Windows：%NnmDataDir%\conf\nnm\props\nms-local.properties
   - Linux：$NnmDataDir/conf/nnm/props/nms-local.properties
4. 在 NNMi_HA1 和 NNMi_HA2 上的 nms-local.properties 文件中更改以下行。

   com.hp.ov.nms.ssl.KEY_ALIAS = 新证书别名
5. 保存更改。

在全局网络管理环境中使用证书

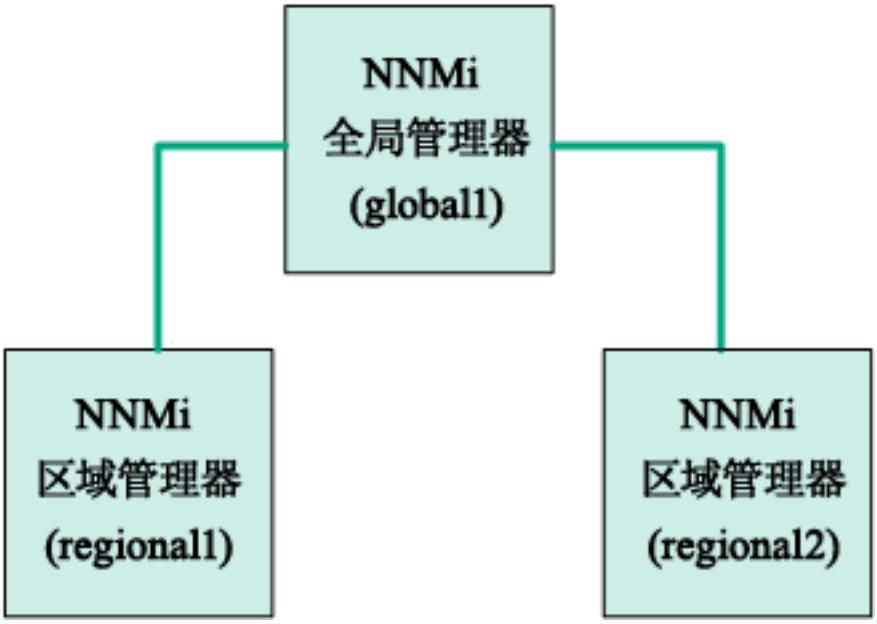
在全局网络管理环境中配置证书

在 NNMi 安装期间，安装脚本创建 NNMi 管理服务器的自签名证书。此证书包含的别名含有节点的完全限定域名。安装脚本将此自签名证书添加到 NNMi 管理服务器的 nnm.keystore 和 nnm.truststore 文件中。

完成以下步骤，将全局网络管理功能配置为根据下图使用自签名/CA 签名证书。

开始之前，确保已在区域管理器系统上创建所需的证书。有关详细信息，请参阅将现有证书替换为新的自签名或 CA 签名证书 (第 257 页)。

全局网络管理



1. 切换到 regional1 和 regional2 上的以下目录：
   - Windows： %NnmDataDir%\shared\nnm\certificates
   - Linux： $NnmDataDir/shared/nnm/certificates
2. 将 nnm.truststore 文件从 regional1 和 regional2 上的上述位置复制到 global1 上的某个临时位置。
3. 在 global1 上运行以下命令，将 regional1 和 regional2 证书合并到 global1 的 nnm.truststore 文件中。

   Windows：

   a. **nnmcertmerge.ovpl -truststore regional1_nnm.truststore_location**
   b. **nnmcertmerge.ovpl -truststore regional2_nnm.truststore_location**

   Linux

   a. **nnmcertmerge.ovpl -truststore regional1_nnm.truststore_location**
   b. **nnmcertmerge.ovpl -truststore regional2_nnm.truststore_location**
4. 在 global1 上运行以下命令序列：
   a. 在 global1 NNMi 管理服务器上运行 **ovstop**。
   b. 在 global1 NNMi 管理服务器上运行 **ovstart**。

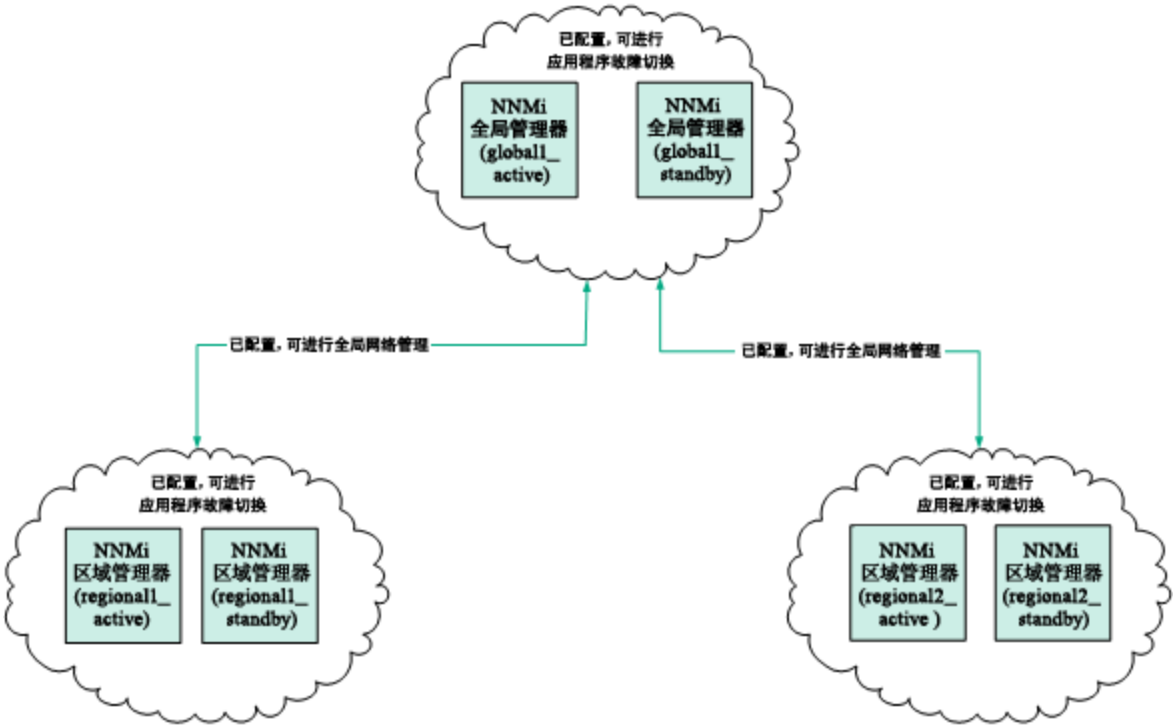
备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

在具有故障转移功能的全局网络管理环境中配置证书

在 NNMi 安装期间，安装脚本将创建 NNMi 管理服务器的自签名证书。此证书包含的别名含有节点的完全限定域名。安装脚本将此自签名证书添加到 NNMi 管理服务器的 nnm.keystore 和 nnm.truststore 文件中。

此示例将全局网络管理配置和应用程序故障转移功能结合使用，如下图中所示：

全局网络管理与应用程序故障转移



完成以下步骤，将全局网络管理功能配置为根据上图使用应用程序故障转移。

1. 对上图中所示的每个应用程序故障转移群集，请遵循在应用程序故障转移环境中使用证书 (第 263 页)中所示的说明操作。
2. 完成应用程序故障转移要求 (第 112 页)中所示的应用程序故障转移配置。

3. 对于 regional1_active and regional2_active，请遵循在全局网络管理环境中配置证书 (第 266 页)中所示的说明。

配置与目录服务的 SSL 连接

默认情况下，启用目录服务通信之后，NNMi 使用 LDAP 协议从目录服务检索数据。如果目录服务需要 SSL 连接，必须使 SSL 协议能够加密在 NNMi 和目录服务之间传送的数据。

SSL 要求在目录服务主机和 NNMi 管理服务器之间存在信任关系。要创建该信任关系，请将证书添加到 NNMi 信任库。证书使 NNMi 管理服务器能确认目录服务主机的身份。

要安装用于 SSL 通信的信任库证书，请执行以下步骤：

1. 从目录服务器获取贵公司的信任库证书。目录服务管理员应能提供此文本文件的副本。
2. 切换到包含 NNMi 信任库的目录：
   - Windows：%NnmDataDir%\shared\nnm\certificates
   - Linux：$NnmDataDir/shared/nnm/certificates

   从 certificates 目录中运行此过程中的所有命令。
3. 将贵公司的信任库证书导入 NNMi 信任库中：
   a. 运行以下命令：
      - Windows：

        %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -import -alias nnmi_ldap -keystore nnm.truststore -file <目录服务器证书.txt>
      - Linux：

        $NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -import -alias nnmi_ldap -keystore nnm.truststore -file <目录服务器证书.txt>

        其中 <目录服务器证书.txt> 是贵公司的信任库证书。
   b. 系统提示您输入密钥库密码时，输入：**ovpass**
   c. 系统提示您是否信任证书时，输入：**y**

      将证书导入信任库中的输出示例

      来自此命令的输出形式为：

      ```
      Owner:CN=NNMi_server.example.com

      Issuer:CN=NNMi_server.example.com

      Serial number:494440748e5

      Valid from:Tue Oct 28 10:16:21 MST 2008 until:Thu Oct 04 11:16:21 MDT 2108

      Certificate fingerprints:

      MD5:29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02

      SHA1:C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03
      ```

```
Trust this certificate?[no]:y

Certificate was added to keystore
```

4. 检查信任库的内容：
   - Windows：

     %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -list -keystore nnm.truststore

   - Linux：

     $NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -list -keystore nnm.truststore

   系统提示您输入密钥库密码时，输入：**ovpass**

   示例信任库输出

   信任库输出形式为：

```
Keystore type: jks

Keystore provider:SUN

Your keystore contains 1 entry

nnmi_ldap, Nov 14, 2008, trustedCertEntry,

Certificate fingerprint (MD5):29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
```

   提示: 信任库可以包括多个证书。

5. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 ovstop 命令。
   b. 在 NNMi 管理服务器上运行 ovstart 命令。

   备注: 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改需要停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

有关 keytool 命令的详细信息，请在 **http://www.oracle.com/technetwork/java/index.html** 上搜索 “Key and Certificate Management Tool”(密钥和证书管理工具)。

对 NNMi 使用单点登录 (SSO)

可以配置 HP Network Node Manager i Software (NNMi) 单点登录 (SSO) 以方便从 NNMi 控制台访问 NNM iSPI。如果使用 SSO，当登录到 NNMi 控制台时，您无需再次登录即可访问 NNM iSPI 和其他 HP 应用程序。SSO 提供对 NNM iSPI 和其他 HP 应用程序更方便的访问，同时维护访问的安全级别。在注销 NNMi 控制台(或 NNMi 控制台会话超时)之后，必须重新输入登录凭据，才能从 NNMi 控制台外部访问 NNM iSPI 和其他 HP 应用程序 URL。

安装期间 SSO 未启用。如果是这样，那么从一个 NNMi 管理服务器浏览至另一个时会将您从第一个管理服务器中注销，这样做的好处甚微。要阻止此情况发生，最初禁用 SSO，使您能够在多个 NNMi 管理服务器之间协调设置 `initString` 和 `protectedDomains` 参数，如本章中所述。

本章包含以下主题：

- NNMi 的 SSO 访问 (第 270 页)
- 为单个域启用 SSO (第 271 页)
- 为位于不同域中的 NNMi 管理服务器启用 SSO (第 271 页)
- NNMi 和 NNM iSPI 的 SSO 访问 (第 272 页)
- 禁用 SSO (第 273 页)
- SSO 安全备注 (第 274 页)

NNMi 的 SSO 访问

要在几个 NNMi 管理服务器之间浏览，必须执行以下某个操作：

> **备注:** 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改需要停止并重新启动 NNMi 管理服务器，则在运行 `ovstop` 和 `ovstart` 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

- 编辑 `nms-ui.properties` 文件，使 `com.hp.nms.ui.sso.initString` 和 `com.hp.nms.ui.sso.protectedDomains` 的参数值在各个 NNMi 管理服务器之间相同。确保将 `com.hp.nms.ui.sso.domain` 参数设置为与 NNMi 管理服务器所在的域匹配。
  - 如果 NNMi 管理服务器仅驻留在一个网络域中，请遵循为单个域启用 SSO (第 271 页)中所示的说明。
  - 如果 NNMi 管理服务器驻留在多个网络域中，请遵循为位于不同域中的 NNMi 管理服务器启用 SSO (第 271 页)中所示的说明获取详细信息。
- 编辑 `nms-ui.properties` 文件，确保已禁用 SSO。有关详细信息，请参阅禁用 SSO (第 273 页)。

如果选择不完成其中某个操作，则每次浏览到不同 NNMi 管理服务器时，将自动退出前一个 NNMi 管理服务器。

将 SSO 用于 NNMi 全局网络管理功能时有几个特殊注意事项。有关详细信息，请参阅SSO 和操作菜单 (第 373 页)和为全局网络管理配置单点登录 (第 373 页)。

如果 NNMi 管理服务器的域名较短，不带点(形如 `mycompany`)，则将立即从 NNMi 控制台中注销。SSO 浏览器 Cookie 限制需要域名至少包含一个点，比如 `mycompany.com`。要对此进行补救，请完成以下步骤：

1. 在文本编辑器中打开以下文件：
   - Windows：`%NNM_PROPS%/nms-ui.properties`
   - Linux：`$NNM_PROPS/nms-ui.properties`
2. 对于此示例，搜索以下字符串：

   ```
   com.hp.nms.ui.sso.domain = mycompany
   ```

并用以下字符串替换它：

```
com.hp.nms.ui.sso.domain = mycompany.com
```

3. 运行以下命令以提交更改：

   nnmsso.ovpl -reload

   有关详细信息，请参阅 nnmsso.ovpl 参考页或 Linux 联机帮助页。

为单个域启用 SSO

要启用 SSO 以在单个域中使用，请完成以下步骤：

> **备注:** 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改需要停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

1. 打开以下文件：
   - Windows：%NNM_PROPS%\nms-ui.properties
   - Linux：$NNM_PROPS/nms-ui.properties
2. 在文件中查找类似以下的部分：

   ```
   com.hp.nms.ui.sso.isEnabled = false
   ```

   对它进行如下更改：

   ```
   com.hp.nms.ui.sso.isEnabled = true
   ```
3. 在文件中查找类似以下的部分：

   ```
   com.hp.nms.ui.sso.domain = mycompany.com
   ```

   将 mycompany.com 更改为 NNMi 管理服务器所在的域。确保在单个域中启用 SSO 时只列出一个域。
4. 在文件中查找类似以下的部分：

   ```
   com.hp.nms.ui.sso.protectedDomains = mycompany.com
   ```

   将 mycompany.com 更改为 NNMi 管理服务器所在的域。确保在单个受保护域中启用 SSO 时只列出一个受保护的域。
5. 运行以下命令以提交更改：

   nnmsso.ovpl -reload

   有关详细信息，请参阅 nnmsso.ovpl 参考页或 Linux 联机帮助页。

为位于不同域中的 NNMi 管理服务器启用 SSO

可以为两个或多个 NNMi 管理服务器配置 SSO。此示例说明如何为位于不同域中的三个 NNMi 管理服务器配置 SSO。如果必须为两个或更多 NNMi 管理服务器配置 SSO，并且这些系统驻留在不同域中，请完成以下步骤：

备注: 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改需要停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

1. 打开以下文件：
   - Windows：`%NNM_PROPS%\nms-ui.properties`
   - Linux：`$NNM_PROPS/nms-ui.properties`
2. 在文件中查找类似以下的部分：

   ```
   com.hp.nms.ui.sso.isEnabled = false
   ```

   对它进行如下更改：

   ```
   com.hp.nms.ui.sso.isEnabled = true
   ```
3. 在文件中查找类似以下的部分：

   ```
   com.hp.nms.ui.sso.domain = group1.mycompany.com
   ```

   确保域名至少包含一个点。
4. 在文件中查找类似以下的部分：

   ```
   com.hp.nms.ui.sso.protectedDomains=group1.mycompany.com
   ```

   对它进行如下更改：

   ```
   com.hp.nms.ui.sso.protectedDomains=group1.mycompany.com, group2.yourcompany.com,
   group3.yourcompany.com
   ```
5. 在文件中查找类似以下的部分：

   ```
   com.hp.nms.ui.sso.initString =初始化字符串
   ```

   NNMi 管理服务器必须共享相同初始化字符串，才能在 SSO 配置中工作。将 SSO 配置中包含的所有 NNMi 管理服务器上的初始化字符串更改为相同值。
6. 运行以下命令以提交更改：

   `nnmsso.ovpl -reload`

   有关详细信息，请参阅 nnmsso.ovpl 参考页或 Linux 联机帮助页。
7. 多次重复步骤 1 到步骤 6，以配置其余两个 NNMi 管理服务器。对于剩余的每个 NNMi 管理服务器，在步骤 3中用 group2 或 group3 代替 group1。

NNMi 和 NNM iSPI 的 SSO 访问

启用 SSO 后，NNMi 和 NNM iSPI 之间的 SSO 不需要 `initString` 配置。

要使用 SSO，请访问 NNMi，如下所示：

- 按以下形式使用正确的 URL：

  <协议>://**<完全限定域名>:<端口号>/nnm/ <协议>** 表示 http 或 https。

  <完全限定域名> 表示 NNMi 管理服务器的正式完全限定域名 (FQDN)。

<端口号> 是连接到 NNMi 控制台的端口，它在 NNMi 安装期间分配并在以下文件中指定：

- Windows：`%NnmDataDir%\conf\nnm\props\nms-local.properties`
- Linux：`$NnmDataDir/conf/nnm/props/nms-local.properties`

- 使用有效帐户登录 NNMi。

为使 SSO 工作，对 NNMi 和 NNM iSPI 的 URL 访问必须共享通用网络域名。另外，URL 不得包括 IP 地址。如果没有 NNMi 管理服务器的 FQDN，则可以改用 NNMi 管理服务器的 IP 地址。但是，这样做会禁用 NNM iSPI 的单点登录，并且必须在下一次访问任何 NNM iSPI 时再次登录。

要确定 NNMi 管理服务器的正式 FQDN，请使用以下某个方法：

- 使用 **`nnmofficialfqdn.ovpl`** 命令显示在安装期间设置的正式 FQDN 的值。有关详细信息，请参阅 nnmofficialfqdn.ovpl 参考页或 Linux 联机帮助页。
- 在 NNMi 控制台中，单击**帮助 > 系统信息**。在**服务器**选项卡上，查找正式 FQDN 语句。

如果必须更改安装期间设置的正式 FQDN，请使用 **`nnmsetofficialfqdn.ovpl`** 命令。有关详细信息，请参阅 nnmsetofficialfqdn.ovpl 参考页或 Linux 联机帮助页。

> **备注:** 在安装之后，系统帐户仍然有效。仅基于命令行安全和恢复目的而使用系统帐户。

到 NNM iSPI 的 SSO 需要用户通过包含正式 FQDN 的 URL 访问 NNMi 控制台。通过非正式域名 (比如 IP 地址或缩写版域名)访问 NNMi 控制台时，可以配置 NNMi 以将 NNMi URL 重定向到正式 FQDN。在配置 NNMi 以重定向 URL 之前，必须配置相应的正式 FQDN。有关信息，请参阅 NNMi 帮助。

在使 NNMi 重定向 URL 之后，注意以下事项：

- 可以使用对要访问的 NNMi 管理服务器有效的任何主机名登录 NNMi 控制台。例如，如果请求 http://localhost/nnm，则 NNMi 重定向到诸如 http://host.mydomain.com/nnm 的 URL。
- 如果无法使用 http://host.mydomain.com/nnm 访问 NNMi 控制台，则使用以下方法直接访问 NNMi 控制台：

  <协议>://<完全限定域名>:<端口号>launch?cmd=showMain.
  <协议> 表示 http 或 https。

  <完全限定域名> 表示 NNMi 管理服务器的正式完全限定域名 (FQDN)。

  <端口号> 是连接到 NNMi 控制台的端口，它在 NNMi 安装期间分配并在以下文件中指定：

  - Windows：`%NnmDataDir%\conf\nnm\props\nms-local.properties`
  - Linux：`$NnmDataDir/conf/nnm/props/nms-local.properties`

禁用 SSO

如果需要禁用 SSO，请完成以下步骤：

> **备注:** 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改需要停止并重新启动 NNMi 管理服务器，则在运行 `ovstop` 和 `ovstart` 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

1. 打开以下文件：
   - Windows：`%NNM_PROPS%\nms-ui.properties`
   - Linux：`$NNM_PROPS/nms-ui.properties`
2. 在文件中查找类似以下的部分：

   `com.hp.nms.ui.sso.isEnabled = true`

   将 `isEnabled` 属性更改为 `false`：

   `com.hp.nms.ui.sso.isEnabled = false`
3. 运行以下命令以提交更改：

   `nnmsso.ovpl -reload`

   有关详细信息，请参阅 nnmsso.ovpl 参考页或 Linux 联机帮助页。

SSO 安全备注

1. 可通过以下方式使用 SSO 安全中的 `initString` 参数：

   SSO 使用对称加密 来验证并创建 SSO 令牌。配置中的 `initString` 参数用于密钥的初始化。应用程序创建令牌，并且使用相同 `initString` 参数的每个应用程序都验证令牌。

   > **备注:** 以下信息非常重要：
   > - 如果未设置 `initString` 参数，则无法使用 SSO。
   > - `initString` 参数是机密信息，在发布、传输和持续性方面应视为机密的。
   > - 相互集成的应用程序可以使用 SSO 共享 `initString`。
   > - `initString` 的最小长度是 12 个字符。
2. 一般禁用 SSO，除非特别情况需要启用。
3. 使用最低验证框架并发布其他集成应用程序信任的 SSO 令牌的应用程序确定所有应用程序的验证安全级别。

   HP 建议只有使用强大和安全的验证框架的应用程序才能发布 SSO 令牌。
4. 对称加密的含意：

   SSO 使用对称加密发布和验证 SSO 令牌。因此，使用 SSO 的任何应用程序都可以发布令牌，由共享相同 `initString` 的所有其他应用程序信任。

   当共享 `initString` 的应用程序位于不受信任的位置或在此位置可访问时，存在此潜在风险。
5. 用户角色：

   SSO 不在集成的应用程序之间共享用户角色。因此，集成的应用程序必须监视用户角色。HP 建议在所有集成的应用程序之间共享相同用户注册表(如 LDAP/AD)。

   管理用户角色失败可能导致安全性被破坏和应用程序负面行为。例如，相同用户名可能在集成应用程序中分配给不同的角色。

情况可能为：用户登录到应用程序 A，然后访问使用容器或应用程序验证的应用程序 B。管理用户角色失败将强制用户手动登录应用程序 B，并输入用户名。如果用户输入的用户名不同于登录到应用程序 A 的用户名，则可能发生以下意外行为：如果用户随后从应用程序 A 或应用程序 B 访问第三个应用程序(应用程序 C)，则用户将使用分别登录到应用程序 A 或应用程序 B 的用户名访问应用程序 C。

6. 身份管理器用于验证：

   身份管理器中所有未受保护的资源必须在 SSO 配置中配置为不安全的 URL 设置。

7. SSO 演示模式：
   - 仅将 SSO 演示模式用于演示目的。
   - 仅在不安全网络中使用演示模式。
   - 不要在生产中使用演示模式。不应将演示模式与生产模式以任何方式组合使用。

将 NNMi 配置为支持公钥基础设施用户验证

NNMi 支持通过公钥基础设施 (PKI) 进行用户验证，这样用户必须使用 X.509 客户端证书登录 NNMi，无需使用密码。本章中的信息说明如何配置 NNMi(使用 PKI 用户验证)将证书映射到 NNMi 用户帐户。

备注: PKI 用户验证包括对智能卡登录(如通用访问卡 (CAC) 和个人身份验证 (PIV) 卡)的支持。

启用 NNMi 使用 PKI 用户验证后，NNMi 用户无需使用特定于 NNMi 的用户名和密码即可登录 NNMi。

使用此方法，NNMi 会通过读取 PKI 证书获取用户名。要获取 NNMi 用户角色，需要在 NNMi 中定义用户的角色或将 NNMi 配置为使用轻量级目录访问协议 (LDAP)。

备注: PKI 用户验证使用 HTTPS 协议。

备注: PKI 用户验证用于在功能上代替轻量级单点登录 (LW-SSO)。因此不能同时使用两者。有关详细信息，请参阅禁用 SSO (第 273 页)。

本章包含以下主题：

用户验证策略 (第 276 页)

为 NNMi 配置 PKI 用户验证(X.509 证书验证) (第 276 页)

证书验证(CRL 和 OCSP) (第 280 页)

使用 CRL 验证证书 (第 282 页)

使用在线证书状态协议 (OCSP) 验证证书 (第 285 页)

将 NNMi 配置为限制用于 NNMi 登录访问的证书 (第 288 页)

示例：将 NNMi 配置为要求智能卡登录 (第 289 页)
为 CLI 验证配置 PKI 用户验证 (第 291 页)
PKI 用户验证问题故障排除 (第 293 页)

用户验证策略

NNMi 为 NNMi 用户访问信息的定义和存储位置提供了若干个选项。

下表指示了 PKI 用户验证可用的选项。

用户验证策略

选项	用户验证方法	NNMi 中的用户帐户定义	NNMi 中的用户组定义	组成员资格方法
混合	X.509 证书	是	是	NNMi 用户帐户映射
外部	X.509 证书	否	是	LDAP

在“混合”选项中，NNMi 定义并存储用户组分配。有关在 NNMi 中设置所有用户信息的信息，请参阅 NNMi 帮助中的**配置用户帐户(用户帐户表单)**。

在“外部”选项中，NNMi 使用轻量级目录访问协议 (LDAP) 用户组分配。有关详细信息，请参阅通过 LDAP 将 NNMi 与目录服务集成 (第 305 页)。

为 NNMi 配置 PKI 用户验证(X.509 证书验证)

为 NNMi 配置 PKI 用户验证前，请注意用户帐户名必须与证书中包含的用户名匹配。使用以下某个方法设置角色：

- 要使用 LDAP，请参阅通过 LDAP 将 NNMi 与目录服务集成 (第 305 页)。
- 要使用 NNMi 控制台添加用户帐户，请选中**用户帐户**表单上的**目录服务帐户**复选框，并将**密码**字段留空。然后使用用户帐户名匹配以前的映射规则。

对于 NNMi，在以下文件中启用并自定义 PKI 用户验证：

- Windows：`%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml`
- Linux：`$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml`

要使 NNMi 要求 PKI 用户验证(或称为 X.509 证书验证)，请执行以下步骤：

1. 编辑以下文件：
   - Windows：`%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml`
   - Linux：`$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml`
2. 搜索以下文本块：

```
<realm name="console">
<mode>FORM</mode>
</realm>
```

3. 将找到的行编辑为：

```
<realm name="console">
<mode>X509</mode>
</realm>
```

4. 搜索以下文本块：

```
<principalMapping>
```

5. 将 NNMi 配置为通过编辑 `<principalMapping>` 部分中的项提取(映射)主体。必须知道证书的格式才能完成此步骤。

> **备注:** NNMi 支持若干个提取主体的选项，并且这些选项可以按任何顺序和编号指定。
>
> - 属性元素从 `SubjectDN` 提取字段；例如 `EMAILADDRESS`。
> - 如果在使用 LDAP， 则提取的名称必须与 LDAP 配置所需的名称匹配。有关详细信息，请参阅“通过 LDAP 将 NNMi 与目录服务集成”。
> - 如果使用的是内部帐户，则名称必须与 NNMi 用户帐户名匹配。如果帐户只用于 PKI 用户验证，则应创建为“目录服务帐户”，并且不设置密码(使用 NNMi **用户帐户**表单。选中**目录服务帐户**复选框并将**密码**字段留空)。如果帐户同时用于 PKI 用户验证和密码登陆，则应创建为设置密码的标准帐户。
>
> - `regexp` 元素根据整个 `SubjectDN` 运行正则表达式。
>
> - `subjectAlternativeName` (SAN) 元素可用于类型 `rfc822Name` (这是一个电子邮件地址)。
>
> - 类型为 `otherName` 并且有附加 `oid` 属性的 `subjectAlternativeName` 元素。此选项通常用于 Microsoft 通用主体名称 (UPN) 字段。

除 `nms-auth-config.xml` 文件的 `<principalMapping>` 部分中提供的示例以外，另请参阅以下示例：

示例 1：将以下行编辑为如下所示以使用 EMAIL 字段：

```
<!-- The attribute element extracts a field from the SubjectDN;
for example, EMAILADDRESS, CN, or UID.-->
<attribute>EMAILADDRESS</attribute>
```

示例 2：提取 EMAILADDRESS 字段的一部分时，编辑以下行作为使用较复杂的正则表达式提取字段某部分的示例。要只提取 EMAILADDRESS 字段的名称部分，请使用以下正则表达式：

```
<!-- Extract the name part of the email field which appears first
in the subjectDN.If the subject is EMAILADDRESS=first.last@example.com,
CN=First Last, OU=MyGroup, O=My Company, the mapped username would be
"first.last"--> <regexp group="1">EMAILADDRESS=([^@]+).*</regexp>
```

示例 3：编辑以下行作为使用较复杂的正则表达式匹配字符串中间的字段的示例：

```
<!--Extract the CN field which appears anywhere in the subjectDN.

Note the optional group before the CN which matches the

previous fields.If the subject is EMAILADDRESS=first.last@example.com,

CN=First Last, OU=MyGroup, O=My Company
```

除 nms-auth-config.xml 文件的 <principalMapping> 部分中提供的示例以外，另请参阅以下示例：

示例 1：将以下行编辑为如下所示以使用 EMAIL 字段：

```
<!-- The attribute element extracts a field from the SubjectDN; for example,

EMAILADDRESS, CN, or UID.-->

<attribute>EMAILADDRESS</attribute>
```

示例 2：提取 EMAILADDRESS 字段的一部分时，编辑以下行作为使用较复杂的正则表达式提取字段某部分的示例。要只提取 EMAILADDRESS 字段的名称部分，请使用以下正则表达式：

```
<!-- Extract the name part of the email field which appears first in

the subjectDN.If the subject is EMAILADDRESS=first.last@example.com,

CN=First Last, OU=MyGroup, O=My Company, the mapped username would be

"first.last"-->

<regexp group="1">EMAILADDRESS=([^@]+).*</regexp>
```

示例 3：编辑以下行作为使用较复杂的正则表达式匹配字符串中间的字段的示例：

```
<!--Extract the CN field which appears anywhere in the subjectDN.

Note the optional group before the CN which matches the previous fields.

If the subject is EMAILADDRESS=first.last@example.com, CN=First Last,

OU=MyGroup, O=My Company

Then the mapped username would be "First Last" -->

<regexp group="2">(.*, )?CN=([^,]+).*</regexp>
```

示例 4：将以下行编辑为如下所示，从使用者备用名称提取电子邮件地址：

```
<!-- Extract the first match of type rfc822Name from the Subject

Alternative Name field of the certificate.-->

<subjectAlternativeName type="rfc822Name" />
```

示例 5：将以下行编辑为如下所示，从使用者备用名称提取特定 OID：

```
<!-- Extract the first match of type otherName with the supplied

OID from the Subject Alternative Name field of the certificate.-->

<subjectAlternativeName type="otherName" oid="1.3.6.1.4.1.311.20.2.3" />
```

> **备注:** 启用调试记录的记录命令如下：
>
> `nnmsetlogginglevel.ovpl`
>
> `com.hp.ov.nms.as.server.auth.x509.NmsCertMapper FINEST`

6. 保存更改。
7. 如果已将信任的 CA 证书安装到信任库，请运行以下脚本使 `nms-auth-config.xml` 文件的更改立即生效：

   ```
   nnmsecurity.ovpl -reloadAuthConfig
   ```

   否则，如果尚未安装证书，请继续以下步骤。
8. 切换到 NNMi 管理服务器上包含 `nnm.truststore` 文件的目录：

   Windows：`%NnmDataDir%\shared\nnm\certificates`

   Linux：`$NnmDataDir/shared/nnm/certificates`
9. 将受信任的 CA 证书导入 `nnm.truststore` 文件。假定 `example_ca.cer` 文件包含您必须使用的证书。运行以下命令将 CA 证书导入到 NNMi nnm.truststore 文件：

   Windows：

   ```
   %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -import -alias myca -keystore
   nnm.truststore -file example_ca.cer
   ```

   Linux：

   ```
   $NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -import -alias myca -keystore
   nnm.truststore -file example_ca.cer
   ```
10. 重新启动 NNMi 服务。
    a. 在 NNMi 管理服务器上运行 `ovstop` 命令。
    b. 在 NNMi 管理服务器上运行 `ovstart` 命令。

> **备注:** 如果在 HA 下进行文件修改，则必须在群集中的两个节点上进行修改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。

现在 NNMi 已配置为使用 PKI 用户验证。无需再使用密码即可登录 NNMi。检查 LDAP 和 NNMi 用户帐户是否正常运行，以及证书和帐户是否已正确配置用户对 NNMi 的访问权限。

使用客户端证书登录 NNMi

要使用客户端证书登录 NNMi，请执行以下步骤：

1. 确保可在浏览器中访问客户端证书。
2. 将浏览器指向 `https://<主机名>/nnm`。
3. NNMi 允许根据您的 NNMi 或 LDAP 帐户配置访问和分配用户角色。

吊销拥有客户端证书的用户的访问权限

要阻止用户访问 NNMi，请执行以下操作之一：

- 如果将用户配置为使用 LDAP 帐户进行访问，请从与 NNMi 关联的所有 LDAP 组删除该用户。
- 如果将用户配置为使用 NNMi 用户帐户进行访问，请从用户组删除该用户并删除其用户帐户。

在任一情况下，用户都不能再登录 NNMi 控制台。

在全局网络管理环境中使用 PKI 用户验证时的特殊注意事项

如果在全局网络管理配置中使用 NNMi，请为全局网络管理配置中的所有 NNMi 管理服务器配置 PKI 用户验证。

证书验证(CRL 和 OCSP)

NNMi 支持两种检查已吊销证书的方法：

- 证书吊销列表 (CRL) - CRL 是从证书颁发机构 (CA) 下载的已吊销证书的列表。
- 在线证书状态协议 (OCSP) - OCSP 是使用名为 OCSP 响应程序的在线服务以交互方式检查单个证书吊销情况的协议。

CRL 和 OCSP 验证是获得相同结果的两种不同方法：拒绝访问任何证书已吊销的用户。在 Web 浏览器中，通常认为 OCSP 更胜一筹，因为浏览器通常要处理许多不同的证书颁发机构 (CA)，下载完整的 CRL 来检查一个网站的效率较低。

但对于经常处理许多客户端并且所有客户端的证书均由同一 CA 颁发的服务器，CRL 检查能显著提高效率，因为可以每天下载一次 CRL，而无需检查每个连接的 OCSP。

同时启用 OCSP 和 CRL 时，默认情况下 NNMi 将先查询 CRL。先执行 CRL 检查是因为通常 CRL 的生存期更长，因此在发生网络服务中断时，恢复能力更强。OCSP 会频繁地执行请求，因此如果网络或 OCSP 响应程序出现故障，用户将无法登录。NNMi 会先尝试获取有效的 CRL 以供后续操作使用，以防网络或 OCSP 响应程序发生故障。

此外，CRL 比较速度比 OCSP 更快；这意味着将证书与磁盘上的列表匹配比通过网络查询单个服务器以验证每个证书更快。因此如果证书已由受信任的实体签名并且尚未过期，则可以查询 CRL 以了解证书是否已吊销。如果已吊销，则无需再检查 OCSP。但如果检查 CRL 后发现证书仍有效，则还将查询 OCSP，确保最近并未吊销证书(并且列出证书的最新 CRL 还不可用)。

同时启用 OCSP 和 CRL 时，NNMi 支持：

- NNMi 先查询 CRL，再查询 OCSP(此为默认行为)。
- 如果 CRL 不可用，则使用 OCSP 代替。
- 如果 OCSP 不可用，则使用 CRL 代替。

证书验证协议的常规配置

可以配置 NNMi 检查已吊销证书的方式。例如，您可以配置协议的使用顺序，以及是否使用所有协议。

NNMi 使用 nms-auth-config.xml 文件配置此类设置。

配置协议顺序

默认情况下，NNMi 先执行 CRL 检查，再执行 OCSP 检查。

要配置证书验证协议检查吊销证书的顺序，请执行以下操作：

1. 编辑以下文件：

   Windows：%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml

   Linux：$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml
2. 在文件的 <revocation> 部分(查找 <revocation> 标记)中搜索以下列文本开头的行：

   ```
   <ordering>
   ```
3. 执行以下某项操作：
   - 要指定先使用 CRL 检查，再使用 OCSP，请将此行编辑为如下所示：

     ```
     <ordering>CRL OCSP</ordering>
     ```
   - 要指定先使用 OCSP 检查，再使用 CRL，请将此行编辑为如下所示：

     ```
     <ordering>OCSP CRL</ordering>
     ```
4. 保存 nms-auth-config.xml 文件。
5. 运行以下命令使更改生效：

   ```
   nnmsecurity.ovpl -reloadAuthConfig
   ```

配置协议请求

可配置 NNMi 执行以下某个与协议请求有关的操作：

- 检查每个证书的所有证书验证协议
- 以首选顺序检查协议列表并在收到有效响应时停止

要配置协议请求，请执行以下操作：

1. 编辑以下文件：

   Windows：%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml

   Linux：$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml
2. 在文件的 <revocation> 部分(查找 <revocation> 标记)中搜索以下列文本开头的行：

   ```
   <mode>
   ```
3. 执行以下某项操作：
   - 要让 NNMi 检查每个证书的所有协议，请将此行编辑为如下所示：

     ```
     <mode>CHECK_ALL</mode>
     ```

- 要让 NNMi 以首选顺序检查协议列表并在收到有效响应时停止，请将此行编辑为如下所示：

  ```
  <mode>FIRST_SUCCESS</mode>
  ```

4. 保存 nms-auth-config.xml 文件。
5. 运行以下命令使更改生效：

   ```
   nnmsecurity.ovpl -reloadAuthConfig
   ```

使用 CRL 验证证书

NNMi 使用 CRL 正确拒绝使用不再受信任的证书对客户端的访问。

备注: 验证期间如果在 CRL 中发现证书的序列号，则 NNMi 不会接受该证书，验证失败。

使用 X.509 验证模式时，NNMi 将默认检查 CRL；但可以通过编辑 nms-auth-config.xml 文件，如以下部分所述，指定 CRL。

备注: NNMi 将 CRL 配置存储在以下位置：

- Windows：%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml
- Linux：$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml

配置文件也有默认版本，可在查看新的可用选项时作参考之用。默认配置文件存储在以下位置：

- Windows：%NnmInstallDir%\newconfig\HPOvNnmAS\nmsas\conf\nms-auth-config.xml
- Linux：$NnmInstallDir/newconfig/HPOvNnmAS/nmsas/conf/nms-auth-config.xml

启用和禁用 CRL 检查

默认情况下，NNMi 启用 CRL 检查。

要配置 CRL 检查，请执行以下步骤：

1. 编辑以下文件：

   Windows：%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml

   Linux：$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml
2. 在文件的 <crl> 部分(查找 <crl> 标记)中搜索以下列文本开头的行：

   ```
   <enabled>
   ```

3. 执行以下某项操作：
   - 要启用 CRL 检查，请将此行更改为如下所示：

     ```
     <enabled>true</enabled>
     ```

   - 要禁用 CRL 检查，请将此行更改为如下所示：

     ```
     <enabled>false</enabled>
     ```

4. 保存 nms-auth-config.xml 文件。

5. 运行以下命令使更改生效：

   nnmsecurity.ovpl -reloadAuthConfig

更改 CRL 强制模式

默认情况下，NNMi 设置为强制 CRL。

要更改产品的 CRL 强制，请执行以下步骤：

1. 编辑以下文件：

   Windows：%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml

   Linux：$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml
2. 在文件的 <crl> 部分(查找 <crl> 标记)中搜索以下列文本开头的行：

   <mode>
3. 将此行更改为下列某个选项：

   <mode><值></mode>

   其中 <值> 是以下值之一：
   - ENFORCE：强制证书中指定的 CRL
   - ATTEMPT：检查 CRL，但在 CRL 不可用时允许访问
   - REQUIRE：在证书中要求并强制 CRL

   备注: 在 REQUIRE 模式中，如果用户证书未指定 CRL 或无可用 CRL，则验证将失败。
4. 保存 nms-auth-config.xml 文件。
5. 运行以下命令使更改生效：

   nnmsecurity.ovpl -reloadAuthConfig

更改刷新 CRL 的频率

要配置 NNMi 刷新 CRL 的频率，请执行以下步骤：

1. 编辑以下文件：

   Windows：%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml

   Linux：$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml
2. 在文件的 <crl> 部分(查找 <crl> 标记)中搜索以下列文本开头的行：

   <refreshPeriod>
3. 将此行更改为如下所示：

   <refreshPeriod><值></refreshPeriod>

   其中 <值> 是整数的小时数或天数(最小值为 1 小时)。

   例如，输入 24h 表示 24 小时，输入 2d 表示 2 天。
4. 保存 nms-auth-config.xml 文件。

5. 运行以下命令使更改生效：

   ```
   nnmsecurity.ovpl -reloadAuthConfig
   ```

更改 CRL 的最长空闲时间

您可以配置 CRL 空闲(未被使用或访问)后 NNMi 保持该 CRL 的时间。

要更改 CRL 的最长空闲时间，请执行以下步骤：

1. 编辑以下文件：

   Windows：`%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux：`$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml`
2. 在文件的 `<crl>` 部分(查找 `<crl>` 标记)中搜索以下列文本开头的行：

   ```
   <maxIdleTime>
   ```
3. 将此行更改为如下所示：

   ```
   <maxIdleTime><值></maxIdleTime>
   ```

   其中 `<值>` 是整数的小时数或天数(最小值为 1 小时)。

   例如，输入 `24h` 表示 24 小时，输入 `2d` 表示 2 天。
4. 保存 `nms-auth-config.xml` 文件。
5. 运行以下命令使更改生效：

   ```
   nnmsecurity.ovpl -reloadAuthConfig
   ```

CRL 过期警告

启用 CRL 检查后，如果 CRL 过期，可能会锁定 NNMi 控制台使用户无法登录。为帮助避免不需要的锁定，NNMi 提供运行状况警告消息，通知管理员 CRL 已过期或即将过期。

一个或多个 CRL 过期时，会发出 CRL 已过期警告(严重度为“重大”)。

一个或多个 CRL 的剩余时间少于其有效期的 1/6 时，会发出 CRL 即将过期警告(严重度为“轻微”)。例如，如果某个 CRL 的有效期为 24 小时，则 NNMi 将在距 CRL 过期不足四小时的时候显示警告。

配置刷新周期，以便 CRL 始终保持最新。正确配置的刷新周期可确保当 CRL 服务器暂时不可用时，已下载的 CRL 剩余足够的有效期。这样 NNMi 就能够继续正常的操作，直到 CRL 服务器可用。在此示例中，刷新周期为八小时可能比较合适。

更改 CRL 位置

默认情况下，NNMi 从证书中嵌入的 HTTP 位置下载 CRL。如果 NNMi 管理服务器无法访问此位置，则管理员可通过其他方式获取所需的 CRL，并将 NNMi 配置为从本地文件系统加载这些 CRL。

备注: 评估证书时，仅考虑由证书颁发者签名的 CRL。

要将 NNMi 配置为从本地文件系统加载 CRL，请执行以下操作：

1. 编辑以下文件：

   Windows：`%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux：`$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml`
2. 在文件的 <crl> 部分(查找 <crl> 标记)中，搜索以下文本块：

   <!--

   CRL 位置的可选规范。如果已设置，NNMi 将把同一 CA 颁发的所有证书视为此 CRL，因为它们均具有此 CRL 位置。可能会列出多个条目。
   <location>file:///var/opt/OV/shared/nnm/certificates/myco.crl</location>

   -->
3. 在 `-->` 标记后插入一行，然后根据您的操作系统输入以下内容：

   Windows：`<location>file:///C:/CRLS/<crl 名称>.crl</location>`

   Linux：`<location>file:///var/opt/OV/shared/nnm/certificates/<crl 名称>.crl</location>`
4. 保存 `nms-auth-config.xml` 文件。
5. 运行以下命令使更改生效：

   ```
   nnmsecurity.ovpl -reloadAuthConfig
   ```

使用在线证书状态协议 (OCSP) 验证证书

NNMi 支持在线证书状态协议 (OCSP) 以交互方式检查吊销的证书。

PKI 用户验证使用 OCSP 通过查询 OCSP 响应程序验证证书的吊销状态。OCSP 响应程序提供有关特定证书的即时、准确的吊销信息，如下所示：

- OCSP 客户端将证书状态请求提交给 OCSP 响应程序。
- OCSP 客户端将相关证书的验收挂起，直到 OCSP 响应程序提供数字签名的响应。
- OCSP 响应程序通过返回以下某个值来指示证书的状态：
  - `Good`(通过；授予用户访问权限)
  - `Revoked`(失败；拒绝用户访问)
  - `Unknown`(失败；拒绝用户访问)

因为每个证书都要查询 OCSP 响应程序，而 CRL 是定期下载的(例如每天一次)，所以 OCSP 响应可能比相应的 CRL 更新。

备注: NNMi 将 OCSP 配置存储在以下位置：

- Windows：`%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml`
- Linux：`$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml`

配置文件的默认版本可在查看新的可用选项时作参考之用。默认配置文件存储在以下位置：

- Windows：`%NnmInstallDir%\newconfig\HPOvNnmAS\nmsas\conf\nms-auth-config.xml`
- Linux：`$NnmInstallDir/newconfig/HPOvNnmAS/nmsas/conf/nms-auth-config.xml`

启用和禁用 OCSP 检查

要配置 OCSP 检查，请执行以下步骤：

1. 编辑以下文件：
   Windows：%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml
   Linux：$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml
2. 在文件的 <ocsp> 部分(查找 <ocsp> 标记)中搜索以下列文本开头的行：

   ```
   <enabled>
   ```

3. 执行以下某项操作：
   - 要启用 OCSP 检查，请将此行更改为如下所示：

     ```
     <enabled>true</enabled>
     ```

   - 要禁用 OCSP 检查，请将此行更改为如下所示：

     ```
     <enabled>false</enabled>
     ```

4. 保存 nms-auth-config.xml 文件。
5. 运行以下命令使更改生效：

   ```
   nnmsecurity.ovpl -reloadAuthConfig
   ```

更改 OCSP 强制模式

默认情况下，NNMi 设置为强制 OCSP。

要更改产品的 OCSP 强制，请执行以下步骤：

1. 编辑以下文件：
   Windows：%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml
   Linux：$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml
2. 在文件的 <ocsp> 部分(查找 <ocsp> 标记)中搜索以下列文本开头的行：

   ```
   <mode>
   ```

3. 将此行更改为下列某个选项：

   ```
   <mode><值></mode>
   ```

   其中 <值> 是以下值之一：
   - ENFORCE：强制证书中指定的 OCSP
   - ATTEMPT：检查 OCSP，但在 OCSP 不可用时允许访问
   - REQUIRE：在证书中要求并强制 OCSP

4. 保存 nms-auth-config.xml 文件。
5. 运行以下命令使更改生效：

   ```
   nnmsecurity.ovpl -reloadAuthConfig
   ```

启用 Nonce

为增强安全性(避免重放攻击)，OCSP 请求程序可将 nonce 添加到证书验证请求中。Nonce 是一个附加到每个请求的随机数字，用于更改加密。启用 nonce 功能后，OCSP 响应程序将使用 nonce 值计算适当的响应。

备注: 使用 nonce 向 OCSP 响应程序添加更多负载，因为它无法预先计算或缓存响应。某些 OCSP 响应程序可能不接受包含 nonce 的请求。

备注: 默认情况下禁用 nonce 功能。

要启用 OCSP nonce 功能，请执行以下步骤：

1. 编辑以下文件：

   Windows：`%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux：`$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml`
2. 在文件的 `<ocsp>` 部分(查找 `<ocsp>` 标记)中搜索以下列文本开头的行：

   ```
   <nonce>
   ```
3. 执行以下某项操作：
   - 要启用 nonce 功能，请将此行更改为如下所示：

     ```
     <nonce>true</nonce>
     ```
   - 要禁用 nonce 功能，使用常规请求，请将此行更改为如下所示：

     ```
     <nonce>false</nonce>
     ```
4. 保存 `nms-auth-config.xml` 文件。
5. 运行以下命令使更改生效：

   ```
   nnmsecurity.ovpl -reloadAuthConfig
   ```

指定 OCSP 响应程序的 URL

(可选)可以将 OCSP 响应程序的 URL 指定如下：

1. 编辑以下文件：

   Windows：`%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux：`$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml`
2. 在文件的 `<ocsp>` 部分(查找 `<ocsp>` 标记)中搜索以下列文本开头的行：

   ```
   <responder>
   ```
3. 将此行编辑为如下所示：

   ```
   <responder><URL></responder>
   ```

   其中 `<URL>` 是与 OCSP 响应程序关联的 URL。
4. 保存 `nms-auth-config.xml` 文件。

5. 运行以下命令使更改生效：

   nnmsecurity.ovpl -reloadAuthConfig

备注: OCSP URL 必须使用 HTTP 协议。

- 如果 nms-auth-config.xml 文件中未指定 OCSP URL，则 NNMi 将自行尝试从证书获取 OCSP 响应程序。
- 如果证书中未指定 OCSP 响应程序，则 NNMi 将使用 <mode> 设置确定要采取的操作：
  - 如果模式为 ENFORCE 或 ATTEMPT，则 NNMi 通过此证书的 OCSP 验证步骤。
  - 如果模式为 REQUIRE，则 NNMi 拒绝该证书。

将 NNMi 配置为限制用于 NNMi 登录访问的证书

如果正在使用具有 PKI 用户验证的 NNMi，可能要限制进行 NNMi 登录访问时将哪些证书视为有效。

NNMi 支持以下类型的限制：

- 证书扩展密钥的使用限制，这可用于限制对基于硬件的证书或其他特定证书的 NNMi 访问。
- 证书颁发者的限制。这些限制旨在防止受信任的证书(不是为登录而加载的证书)被用于创建登录证书。

要将 NNMi 配置为限制用于登录访问的证书，请执行以下操作：

1. 编辑以下文件：

   Windows：%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml

   Linux：$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml
2. 找到包含以下行的文本块：

   <certificateConstraints>
3. 使用以下示例作为指导，将 NNMi 配置为限制用于登录的证书(可以对值进行适当的更换)：

   示例 1：如果需要客户端验证，请编辑以下部分：

   <!-- 客户端验证 -->

   <extKeyUsage>1.3.6.1.5.5.7.3.2</extKeyUsage>

   示例 2：如果需要用户使用 Microsoft 智能卡登录：

   <!-- Microsoft 智能卡登录 -->

   <extKeyUsage>1.3.6.1.4.1.311.20.2.2</extKeyUsage>

   示例 3：要只接受特定 CA 签名的证书：

   <!-- 配置一个或多个受信任的颁发者。完成此配置后，这些颁发者中某一个颁发的客户端证书才能用于客户端验证 -->

   <trustedIssuer>CN=MyIssuer, OU=MyOrgUnit, O=MyOrg, ST=CO, C=US</trustedIssuer>

   备注: 指定多个 extKeyUsage 条目时，证书必须包含所有条目(布尔值为 AND)。指定多个受信任的颁发者时，只有一个必须为证书信任的颁发者(布尔值为 OR)。

4. 运行以下命令使更改生效：

   nnmsecurity.ovpl -reloadAuthConfig

示例：将 NNMi 配置为要求智能卡登录

以下示例说明了如何将 NNMi 配置为使用 PKI 用户验证以要求智能卡登录。

> **备注:** 此示例使用混合用户验证策略。

此示例假定：

- 组织将使用智能卡登录 NNMi。
- 智能卡包含其“使用者备用名称”字段中有电子邮件地址的证书。
- 组织使用 CRL 检查所有证书的吊销情况。

要完成示例配置，请执行以下步骤：

1. 在 NNMi 控制台中，创建名为 myusername@example.com 的具有来宾权限的用户。
   a. 从“用户帐户”视图中，创建 myusername@example.com 用户。

      > **提示:** 在**用户帐户**表单上，确保选中**目录服务帐户**复选框，并将**密码**字段留空。有关详细信息，请参阅 NNMi 帮助。

   b. 从“用户帐户映射”视图中，创建新的用户帐户映射，将 myusername@example.com 用户分配到 NNMi Guest Users 用户组。
2. 编辑以下文件：

   Windows：%NnmDataDir%\nmsas\NNM\conf\nms-auth-config.xml

   Linux：$NnmDataDir/nmsas/NNM/conf/nms-auth-config.xml
3. 搜索以下文本块：

   ```
   <realm name="console">
   <mode>FORM</mode>
   </realm>
   ```
4. 要启用 X.509 证书验证，请将此文本编辑为如下所示：

   ```
   <realm name="console">
   <mode>X509</mode>
   </realm>
   ```
5. 搜索以下文本块：

   ```
   <principalMapping>
   ```
6. 在 <principalMapping> 块中，要从证书的“使用者备用名称”字段中提取 rfc822Name 类型的第一个匹配项，请包含以下行：

   ```
   <subjectAlternativeName type="rfc822Name" />
   ```

7. 在文件的 <crl> 部分(查找 <crl> 标记)中搜索以下列文本开头的行：

   <enabled>

8. 要启用 CRL 检查，请将此行更改为如下所示：

   <enabled>true</enabled>

9. 在文件的 <crl> 部分中，查找包含以下文本的文本块：

   <mode>

10. 为要求并强制使用 CRL，请将此行更改为如下所示：

    <mode>REQUIRE</mode>

11. 找到包含以下行的文本块：

    <certificateConstraints>

12. 如果需要客户端验证，请编辑以下部分：

    <!-- 客户端验证 -->

    <extKeyUsage>1.3.6.1.5.5.7.3.2</extKeyUsage>

13. 如果要求用户使用 Microsoft 智能卡登录，请添加以下行：

    <!-- Microsoft 智能卡登录 -->

    <extKeyUsage>1.3.6.1.4.1.311.20.2.2</extKeyUsage>

14. 保存对 nms-auth-config.xml 文件的更改。
15. 切换到 NNMi 管理服务器上包含 nnm.truststore 文件的目录：

    Windows：%NnmDataDir%\shared\nnm\certificates

    Linux：$NnmDataDir/shared/nnm/certificates

16. 将受信任的 CA 证书导入 nnm.truststore 文件。假定 example_ca.cer 文件包含您必须使用的证书。运行以下命令将 CA 证书导入到 NNMi nnm.truststore 文件：

    Windows：%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -import -alias myca -keystore nnm.truststore -file example_ca.cer

    Linux：$NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -import -alias myca -keystore nnm.truststore -file example_ca.cer

17. 确保用户帐户的名称与证书中包含的用户名 (myusernamе) 匹配。
18. 重新启动 NNMi 服务：
    - 在 NNMi 管理服务器上运行 ovstop 命令。
    - 在 NNMi 管理服务器上运行 ovstart 命令。

现在 NNMi 已配置为要求智能卡登录。

以下文本与进行此示例中所述的配置更改后 nms-auth-config.xml 文件显示的内容类似：

```
<methods>
   <X509>
      <principalMapping>
           <subjectAlternativeName type="rfc822Name" />
```

```
        </principalMapping>
        <certificateConstraints>
             <extKeyUsage>1.3.6.1.5.5.7.3.2</extKeyUsage>
             <extKeyUsage>1.3.6.1.4.1.311.20.2.2</extKeyUsage>
             <trustedIssuer>CN=MyIssuer, OU=MyOrgUnit, O=MyOrg, ST=CO, C=US</trustedIssuer>
        </certificateConstraints>
        <revocation>
           <ordering>CRL OCSP</ordering>
            <mode>CHECK_ALL</mode>
         </revocation>
         <crl>
            <enabled>true</enabled>
             <mode>REQUIRE</mode>
             <!-- refresh CRLs every 12 hours -->
             <refreshPeriod>12h</refreshPeriod>
              <!-- remove CRLs that have not been used for 36 hours -->
              <maxIdleTime>36h</maxIdleTime>
          </crl>
          <ocsp>
            <enabled>false</enabled>
            <mode>ENFORCE</mode>
            <nonce>false</nonce>
          </ocsp>
    </X509>
  </methods>
  <realms>
    <realm name="console">
    <mode>X509</mode>
     </realm>
  </realms>
```

为 CLI 验证配置 PKI 用户验证

授权用户不必导航到 NNMi 控制台即可使用 NNMi 命令行界面 (CLI) 配置 NNMi 设置。

公钥基础设施 (PKI) 用户验证取决于客户端操作系统和执行用户验证的 Web 浏览器设置。因此 CLI 会话无法使用 PKI 用户验证，因为命令在 Web 浏览器环境之外运行。要以非根用户身份启用 CLI 验证，请提供对以下文件的授权用户读取权限(根用户已具有此文件的读取权限)：

Windows：`%NnmDataDir%\nmsas\NNM\conf\nms-users.properties`

Linux：`$NnmDataDir/nmsas/NNM/conf/nms-users.properties`

此文件包含 NNMi“系统”用户的加密密码。可读取此文件的所有用户均可以“系统”用户身份调用 CLI 命令。

备注: 以管理员组成员身份登录的 Windows 用户已具有 `nms-users.properties` 文件的读取权限，因此对属于管理员组的 Windows 用户无需进一步配置。有关配置安全的详细信息，请参阅 NNMi 帮助。

可使用普通的 Linux `chmod` 命令获得对 `nms-users.properties` 文件的读取权限。但建议配置基于操作系统的访问控制列表 (ACL) 以提供对此文件的细化访问控制。有关详细信息，请参阅设置 ACL 支持非根用户运行 CLI 命令 (第 292 页)。

设置 ACL 支持非根用户运行 CLI 命令

不同操作系统间和同一操作系统上不同文件系统类型间的 ACL 命令有很大不同。此外，您可能需要配置操作系统以启用 ACL；例如，在 Linux 上将 `,acl` 条目添加到 `/etc/fstab`。

本部分提供将 Linux(RHEL 和 SuSE)ACL 命令用于 ext3 和 ext4 文件系统的示例。如果您正在使用其他文件系统类型或操作系统，请参阅操作系统 ACL 文档了解详细信息。

此示例赋予操作系统用户 `user1` 对 `nms-users.properties` 文件的读取权限。

备注: 设置 ACL 权限时，请指定给定文件的完整权限集。提供的权限将覆盖以前的权限。

授予权限

1. 使用以下命令查询当前 ACL：

   ```
   chacl -l nms-users.properties
   ```

   输出将如下所示：

   ```
   nms-users.properties [u::rw-,u:user2:r--,u:user3:r--,g::r--,m::r--,o::---]
   ```

2. 将新权限 (`,u:user1:r--`)追加到列表输出的方括号 ([ ]) 中，然后运行以下命令：

   ```
   chacl <ACL 列表中方括号内的结果>,u:user1:r-- nms-users.properties
   ```

备注: ACL 提供用户级别控制和/或组级别控制。还可以创建 Linux 组；例如 nnmiadm, 然后为该组提供对 `nms-users.properties` 文件的读取权限。然后通过向该组添加 Linux 用户或从该组删除用户，授予或除去对 `nms-users.properties` 文件的访问权限，从而授予或除去 CLI 命令对“系统”用户的验证。

警告: 设置 ACL 时应谨慎，因为阻止 `nmsproc` 用户或 `nmsgrp` 组权限的设置不正确可能导致 NNMi 停止运行。

列出 ACL

运行以下命令：

```
chacl -l nms-users.properties
```

删除权限

1. 使用以下命令查询当前 ACL：

   ```
   chacl –l nms-users.properties
   ```

2. 标识并删除要删除的用户 (user1)： `,u:user1:r--`
3. 将 ACL 列表的其余部分粘贴到 chacl 命令中：

   ```
   chacl <除 user1 以外的列表结果> nms-users.properties
   ```

备注: `nms-users.properties` 文件路径中的每个目录都必须可访问。通常这些文件夹的权限限制非常严格，会阻止访问。此路径包含以下目录：

- `$NnmDataDir/nmsas`
- `$NnmDataDir/nmsas/NNM`
- `$NnmDataDir/nmsas/NNM/conf`
- `$NnmDataDir/nmsas/NNM/conf/props`

还可以在这些文件夹或常规 Linux chmod 上使用 ACL，将“搜索”权限(即，执行位或 0711 模式)授予“其他”。

备注: 运行 `nnmrestore.ovpl` 命令可从 NNMi 恢复以及覆盖现有 ACL。在这种情况下，恢复 NNMi 后，需要使用本部分前面描述的将用户添加到 ACL 的过程手动重新创建并应用 ACL。

备注: 在应用程序故障转移或高可用性 (HA) 环境中，必须手动在两个节点上都设置 ACL，方法是登录主节点，运行相应的 ACL 命令，然后在辅助节点上重复该过程。

备注: 在全局网络管理 (GNM) 环境中，每个单独的节点可能都有自己的包含不同用户的 ACL。例如，在区域管理器上具有 CLI 访问权限的用户可能在全局管理器上不具有 CLI 访问权限。

PKI 用户验证问题故障排除

进行 PKI 用户验证期间，用户可能会遇到错误。有关错误列表和可能的原因，请参阅下表。

PKI 用户验证错误和可能原因

错误消息	可能原因
401 Not	使用了 HTTP 而非 HTTPS。

PKI 用户验证错误和可能原因(续)

错误消息	可能原因
Authenticated	有关详细信息，请参阅将 NNMi 配置为要求加密远程访问 (第 213 页)。
	用户没有证书。 有关详细信息，请参阅管理证书 (第 255 页)。
	用户证书不受 `nnm.truststore` 中 CA 的信任。 有关详细信息，请参阅管理证书 (第 255 页)。
	用户证书已过期或尚未生效。 有关详细信息，请参阅管理证书 (第 255 页)。
	用户证书已吊销或吊销检查失败。 有关详细信息，请参阅管理证书 (第 255 页)。
	用户证书约束检查失败。 有关详细信息，请参阅将 NNMi 配置为限制用于 NNMi 登录访问的证书 (第 288 页)。
403 Not Authorized	NNMi 或 LDAP 目录服务中不存在映射的用户名。 有关详细信息，请参阅为 NNMi 配置 PKI 用户验证(X.509 证书验证)(第 276 页)。
	用户名映射的证书主体不正确。 有关详细信息，请参阅为 NNMi 配置 PKI 用户验证(X.509 证书验证)(第 276 页)。
	用户不在提供 NNMi 控制台访问权限的用户组中。 有关详细信息，请参阅 NNMi 帮助中的**配置安全**。

备注: 要进行故障排除，请禁用 HTTP 访问并打开日志记录以帮助确定问题。

配置 Telnet 和 SSH 协议以供 NNMi 使用

操作 > Telnet...(从客户端) 菜单项(通过当前正在运行 NNMi 控制台的 Web 浏览器)对所选节点调用 Telnet 命令。**操作 > 安全 Shell...(从客户端)** 菜单项(通过当前正在运行 NNMi 控制台的 Web 浏览器)对所选节点调用安全 shell (SSH) 命令。默认情况下，Microsoft Internet Explorer 和 Mozilla Firefox 都未定义 Telnet 命令和 SSH 命令，因此使用这两个菜单项中的任何一个都会产生错误消息。

您可对每个 NNMi 用户(基于每个系统)配置 Telnet 和/或 SSH 协议，并且您可以更改 NNMi 控制台菜单项。

本章包含以下主题：

- 禁用 Telnet 或 SSH 菜单项 (第 295 页)
- 为 Windows 上的浏览器配置 Telnet 或 SSH 客户端 (第 295 页)
- 在 Linux 上配置 Firefox 使用 Telnet 或 SSH (第 301 页)
- 用于更改 Windows 注册表的示例文件 (第 303 页)

禁用 Telnet 或 SSH 菜单项

如果部署环境中的 NNMi 用户不需要从 NNMi 控制台进行 Telnet 或 SSH 连接，则可以禁用相应的菜单项，或者将其从 NNMi 控制台中删除。

禁用 NNMi 控制台中的菜单项将应用于登录到此 NNMi 管理服务器上的 NNMi 控制台的所有用户。要禁用 **Telnet** 或**安全 Shell** 菜单项，请执行以下步骤：

1. 在**配置**工作区中，展开**用户界面**，然后选择**菜单项**。
2. 在**菜单项**视图中，选择 **Telnet...(从客户端)** 行或**安全 Shell...(从客户端)** 行，然后单击 **打开**图标。
3. 在**菜单项**表单中，清除**已启用**复选框，然后将**作者**字段设为相应的值。

   更改作者值可以确保该菜单项在升级 NNMi 时保持禁用状态。
4. 保存并关闭此表单。

有关详细信息，请参阅 NNMi 帮助中的“控制操作菜单”。

为 Windows 上的浏览器配置 Telnet 或 SSH 客户端

为 NNMi 用户的 Web 浏览器配置操作系统提供的 Telnet 命令。必须对 NNMi 用户需要运行**操作 > Telnet...(从客户端)** 菜单项的每台计算机和 Web 浏览器执行该过程。

为 NNMi 用户的 Web 浏览器配置第三方 ssh 命令。必须对 NNMi 用户需要运行**操作 > 安全 Shell...(从客户端)** 菜单项的每台计算机和 Web 浏览器执行该过程。

要完成本部分中的任何过程，您必须在计算机上有管理特权。具体步骤取决于浏览器和操作系统的版本(32 位或 64 位)。

要确定 Internet Explorer 的版本，请单击**帮助 > 关于 Internet Explorer**。如果版本信息不包含文本 **64 位版本**，则该 Internet Explorer 是 32 位。

Firefox 只有 32 位版本。

下表标识了每种浏览器和操作系统的组合要使用的过程。

Windows 上 Telnet 和 SSH 配置过程列表

Web 浏览器	Windows 操作系统体系结构	适用过程
32 位 Internet Explorer	32 位	• Windows 操作系统提供的 Telnet 客户端 (第 297 页) • 第三方 Telnet 客户端(标准 Windows) (第 298 页) • 第三方 SSH 客户端(标准 Windows 以及 Windows on Windows) (第 300 页)

Windows 上 Telnet 和 SSH 配置过程列表(续)

Web 浏览器	Windows 操作系统体系结构	适用过程
	64 位 Windows 7	• 第三方 Telnet 客户端(标准 Windows) (第 298 页) • 第三方 SSH 客户端(标准 Windows 以及 Windows on Windows) (第 300 页)
	64 位，除 Windows 7 以外	• 第三方 Telnet 客户端 (Windows on Windows) (第 299 页) • 第三方 SSH 客户端(标准 Windows 以及 Windows on Windows) (第 300 页)
64 位 Internet Explorer	64 位	• Windows 操作系统提供的 Telnet 客户端 (第 297 页) • 第三方 Telnet 客户端(标准 Windows) (第 298 页) • 第三方 SSH 客户端(标准 Windows 以及 Windows on Windows) (第 300 页)
Firefox	32 位	• Windows 操作系统提供的 Telnet 客户端 (第 297 页) • 第三方 Telnet 客户端(标准 Windows) (第 298 页) • 第三方 SSH 客户端(标准 Windows 以及 Windows on Windows) (第 300 页)
	64 位 Windows 7	• 第三方 Telnet 客户端(标准 Windows) (第 298 页) • 第三方 SSH 客户端(标准 Windows 以及 Windows on Windows) (第 300 页)
	64 位，除 Windows 7 以外	• 第三方 Telnet 客户端 (Windows on Windows) (第 299 页) • 第三方 SSH 客户端(标准 Windows 以及 Windows on Windows) (第 300 页)

提示: 本部分中的许多任务涉及编辑 Windows 注册表。您可以创建一个 .reg 文件以供每个用户在其系统上运行，这样就无需直接编辑注册表。有关 .reg 文件的示例，请参阅用于更改 Windows 注册表的示例文件 (第 303 页)。

有关本部分中所述任务的详细信息，请参阅以下 Microsoft 文章：

- 安装 Microsoft 提供的 Telnet 客户端：
  http://technet.microsoft.com/en-us/library/cc771275%28WS.10%29.aspx
- Windows 注册表简介：
  http://support.microsoft.com/kb/256986

- 备份和恢复 Windows 注册表：
  http://support.microsoft.com/kb/322756

Windows 操作系统提供的 Telnet 客户端

此过程适用于以下情况：

- 32 位操作系统上的 32 位 Internet Explorer
- 32 位操作系统上的 32 位 Firefox
- 64 位操作系统上的 64 位 Internet Explorer

备注: Windows 操作系统附带的 Telnet 客户端不使用在 64 位 Windows 操作系统上运行的 32 位版本的 Internet Explorer。要对此进行补救，请使用 64 位版本的 Internet Explorer。Windows 64 位操作系统包括 32 位和 64 位版本的 Internet Explorer。在以下目录中查找这些 Internet Explorer 版本：

- 64 位版本：`%ProgramFiles%/Internet Explorer`
- 32 位版本：`%ProgramFiles(x86)%/Internet Explorer`

要配置操作系统提供的 Telnet 客户端以供 Web 浏览器使用，请执行以下步骤：

1. (仅适用于 Microsoft Windows 7、Microsoft Vista 或 Microsoft Windows Server)通过遵循适用于操作系统的步骤，在计算机上安装操作系统 Telnet 客户端。

   Windows 7 或 Vista：

   a. 在控制面板中，单击**程序**，然后单击**程序和功能**。
   b. 单击“任务”下的**打开或关闭 Windows 功能**。
   c. 在“Windows 功能”对话框中，选中 **Telnet 客户端**复选框，然后单击**确定**。

   Windows Server：

   a. 在 Server Manager 的“功能摘要”下，单击**添加功能**。
   b. 在“添加功能”向导中，选中 **Telnet 客户端**复选框，单击**下一步**，然后单击**安装**。
2. (仅 Internet Explorer)使 Internet Explorer 能够使用 Telnet 协议。
   a. 备份 Windows 注册表。
   b. 使用 Windows 注册表编辑器添加 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL] 键，其值如下：

名称	类型	数据
iexplore.exe	REG_DWORD	0

3. 为 URL:Telnet 协议文件类型设置文件关联。
   a. 备份 Windows 注册表。
   b. 使用 Windows 注册表编辑器修改 [HKEY_CLASSES_ROOT\telnet\shell\open\command] 键，其值如下：

名称	类型	数据
(默认值)	REG_SZ	rundll32.exe url.dll,TelnetProtocolHandler %l

4. %l(使用小写 L)是传递到 Telnet 的参数，通常是节点的 IP 地址或完全限定域名。

> **提示:** 要实施更严格的控制，可以在注册表键中加入二进制文件的路径(单独占一行)。例如：
>
> `"C:\Windows\system32\rundll32.exe"`
>
> `"C:\Windows\system32\url.dll",TelnetProtocolHandler %l`

5. 重新启动 Web 浏览器，然后在浏览器地址栏中，输入 Telnet 命令：

   telnet://<节点>

   <节点> 是运行 Telnet 服务器的节点的 IP 地址或完全限定域名。

   如果系统向您提示一个安全警告，请允许该操作。

   在 Firefox 中，选中**记住我对 Telnet 类型链接的选择**复选框。

第三方 Telnet 客户端(标准 Windows)

此过程适用于以下情况：

- 32 位操作系统上的 32 位 Internet Explorer
- 64 位 Windows 7 操作系统上的 32 位 Internet Explorer
- 32 位操作系统上的 32 位 Firefox
- 64 位操作系统上的 64 位 Internet Explorer

要配置第三方 Telnet 客户端以供 Web 浏览器使用，请执行以下步骤：

1. 获取并安装第三方 Telnet 客户端。

   此过程为安装到 `C:\Program Files\PuTTY\putty.exe` 的 PuTTY 客户端提供示例。PuTTY 客户端可从
   http://www.putty.org 获取。

2. (仅 Internet Explorer)使 Internet Explorer 能够使用 Telnet 协议。
   a. 备份 Windows 注册表。
   b. 使用 Windows 注册表编辑器添加 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL] 键，其值如下：

名称	类型	数据
iexplore.exe	REG_DWORD	0

3. 为 URL:Telnet 协议文件类型设置文件关联。
   a. 备份 Windows 注册表。
   b. 使用 Windows 注册表编辑器修改 [HKEY_CLASSES_ROOT\telnet\shell\open\command] 键，其值如下：

名称	类型	数据
(默认值)	REG_SZ	"C:\Program Files\PuTTY\putty.exe" %l

`%l`(使用小写 L)是传递到 Telnet 的参数，通常是节点的 IP 地址或完全限定域名。

提示: 在 .reg 文件中，使用反斜杠 (\) 字符对引号 (") 和反斜杠 (\) 字符进行转义。

4. 重新启动 Web 浏览器，然后在浏览器地址栏中，输入 Telnet 命令：

   `telnet://<节点>`

   <节点> 是运行 Telnet 服务器的节点的 IP 地址或完全限定域名。

   如果系统向您提示一个安全警告，请允许该操作。

   在 Firefox 中，选中**记住我对 Telnet 类型链接的选择**复选框。

第三方 Telnet 客户端 (Windows on Windows)

此过程适用于以下情况：

- 64 位操作系统(Windows 7 除外)上的 32 位 Internet Explorer
- 32 位操作系统上的 64 位 Firefox

要配置第三方 Telnet 客户端以供 Web 浏览器使用，请执行以下步骤：

1. 获取并安装第三方 Telnet 客户端。

   此过程为安装到 `C:\Program Files\PuTTY\putty.exe` 的 PuTTY 客户端提供示例。PuTTY 客户端可从
   http://www.putty.org 获取。

2. (仅 Internet Explorer)使 Internet Explorer 能够使用 Telnet 协议。
   a. 备份 Windows 注册表。
   b. 使用 Windows 注册表编辑器添加 [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL] 键，其值如下：

名称	类型	数据
iexplore.exe	REG_DWORD	0

3. 为 URL:Telnet 协议文件类型设置文件关联。
   a. 备份 Windows 注册表。
   b. 使用 Windows 注册表编辑器修改 [HKEY_CLASSES_ROOT\Wow6432Node\telnet\shell\open\command] 键，其值如下：

名称	类型	数据
(默认值)	REG_SZ	"C:\Program Files\PuTTY\putty.exe" %l

%l(使用小写 L)是传递到 Telnet 的参数，通常是节点的 IP 地址或完全限定域名。

> **提示:** 在 .reg 文件中，使用反斜杠 (\) 字符对引号 (") 和反斜杠 (\) 字符进行转义。

4. 重新启动 Web 浏览器，然后在浏览器地址栏中，输入 Telnet 命令：

   telnet://<节点>

   <节点> 是运行 Telnet 服务器的节点的 IP 地址或完全限定域名。
   如果系统向您提示一个安全警告，请允许该操作。
   在 Firefox 中，选中**记住我对 Telnet 类型链接的选择**复选框。

第三方 SSH 客户端(标准 Windows 以及 Windows on Windows)

此过程适用于以下情况：

- 32 位或 64 位操作系统上的 32 位 Internet Explorer
- 32 位或 64 位操作系统上的 32 位 Firefox
- 64 位操作系统上的 64 位 Internet Explorer

要配置第三方 SSH 客户端以供 Web 浏览器使用，请执行以下步骤：

1. 获取并安装第三方 SSH 客户端。

   此过程为安装到 C:\Program Files\PuTTY\putty.exe 的 PuTTY 客户端提供示例。PuTTY 客户端可从
   http://www.putty.org 获取。

2. 由于 PuTTY 不能正确解析“ssh://<节点>”输入，因此该示例包含了一个脚本，用于去掉输入参数中的“ssh://”。脚本 C:\Program Files\PuTTY\ssh.js 包含以下命令：

```
host = WScript.Arguments(0).replace(/ssh:/,"").replace(/\//g,"");

shell = WScript.CreateObject("WScript.Shell");

shell.Run("\"c:\\Program Files\\PuTTY\\putty.exe\" -ssh " + host);
```

   > **提示:** 该脚本是针对此示例创建的，未包含在 PuTTY 中。

3. 定义 ssh 协议。
   a. 备份 Windows 注册表。
   b. 使用 Windows 注册表编辑器添加 [HKEY_CLASSES_ROOT\ssh] 键，其值如下：

名称	类型	数据
(默认值)	REG_SZ	URL:ssh Protocol
EditFlags	REG_DWORD	2
FriendlyTypeName	REG_SZ	Secure Shell
URL Protocol	REG_SZ	无值

4. 为 URL:ssh Protocol 文件类型设置文件关联。
   a. 备份 Windows 注册表。
   b. 使用 Windows 注册表编辑器修改 [HKEY_CLASSES_ROOT\ssh\shell\open\command] 键，其值如下：

名称	类型	数据
(默认值)	REG_SZ	"C:\Windows\System32\WScript.exe" "C:\Program Files\PuTTY\ssh.js" %l

   %1(小写 L)是包括协议规范在内的完整 ssh 参数。ssh.js 脚本将 ssh 目标传递给 PuTTY。

   提示: 在 .reg 文件中，使用反斜杠 (\) 字符对引号 (") 和反斜杠 (\) 字符进行转义。

5. 重新启动 Web 浏览器，然后在浏览器地址栏中，输入 ssh 命令：

   ssh://<节点>

   <节点> 是运行 Telnet 服务器的节点的 IP 地址或完全限定域名。
   如果系统向您提示一个安全警告，请允许该操作。
   在 Firefox 中，选中**记住我对 ssh 类型链接的选择**复选框。

在 Linux 上配置 Firefox 使用 Telnet 或 SSH

在 Linux 操作系统上，定义 Telnet 或 ssh 协议，然后配置 Firefox 使用新协议。

要完成本部分中的任何过程，您必须在计算机上有管理特权。

有关详细信息，请访问 **http://kb.mozillazine.org/Register_protocol**。

Linux 上的 Telnet

要在 Linux 操作系统上配置 Firefox 使用 Telnet 协议，请执行以下步骤：

1. 定义 Telnet 协议。
   a. 使用以下内容创建 /usr/local/bin/nnmtelnet 文件：

```
#!/bin/bash
#
# Linux shell script called by Firefox in response to
# telnet://URLs for the NNMi telnet menu.
#
address=`echo $1 | cut -d :-f 2 | sed 's;/;;g'`
port=`echo $1 | cut -d :-f 3`
exec /usr/bin/xterm -e telnet $address $port
```

b. 设置每个用户可执行的脚本权限：

chmod 755 /usr/local/bin/nnmtelnet

2. 针对 Telnet 配置 Firefox 首选项。
   a. 在 Firefox 地址栏中，输入：**about:config**
   b. 在首选项列表中，右键单击，单击**新建**，然后单击 **Boolean**。
   c. 输入首选项名称：**network.protocol-handler.expose.telnet**
   d. 选择首选项值：**false**
3. 配置 Firefox 以使用新定义的协议。
   a. 浏览到 Telnet 链接。

   > **提示:** 可以创建包含该链接的简单 HTML 文件，或者可以使用**操作 > Telnet...(从客户端)**(在 NNMi 控制台中)。直接将链接输入到地址栏中没有相同效果。

   b. 在“启动应用程序”窗口中，单击**选择**，然后选择 /usr/local/bin/nnmtelnet。
   c. 选中**记住我对 Telnet 类型链接的选择**复选框。

Linux 上的安全 Shell

要在 Linux 操作系统上配置 Firefox 使用 ssh 协议，请执行以下步骤：

1. 定义 ssh 协议。
   a. 使用以下内容创建 /usr/local/bin/nnmssh 文件：

```
#!/bin/bash
#
# Linux shell script called by Firefox in response to
# ssh://URLs for the NNMi SSH menu.
#
address=`echo $1 | cut -d :-f 2 | sed 's;/;;g'`
port=`echo $1 | cut -d :-f 3`
exec /usr/bin/xterm -e ssh $address $port
```

   b. 设置每个用户可执行的脚本权限：

chmod 755 /usr/local/bin/nnmssh

2. 针对 SSH 配置 Firefox 首选项。
   a. 在 Firefox 地址栏中，输入：**about:config**
   b. 在首选项列表中，右键单击，单击**新建**，然后单击 **Boolean**。
   c. 输入首选项名称：**network.protocol-handler.expose.ssh**
   d. 选择首选项值：**false**
3. 配置 Firefox 以使用新定义的协议。

a. 浏览到 SSH 链接。

> **提示:** 可以创建包含该链接的简单 HTML 文件，或者可以使用 NNMi 控制台中定义的新 SSH 菜单项。直接将链接输入到地址栏中没有相同效果。

b. 在“启动应用程序”窗口中，单击**选择**，然后选择 `/usr/local/bin/nnmssh`。

c. 选中**记住我对 ssh 类型链接的选择**复选框。

用于更改 Windows 注册表的示例文件

如果许多 NNMi 用户需要使用 Telnet 或 ssh 协议从 NNMi 控制台访问被管节点，您也许能够通过一个或多个 .reg 文件自动执行 Windows 注册表更新。本部分包含示例 .reg 文件，您可以基于这些文件创建自己的 .reg 文件。请注意，对于在 64 位版本 Windows 上运行 32 位应用程序的情况，注册表键的路径不同于应用程序和操作系统的版本匹配时的路径。

有关详细信息，请参阅以下 Microsoft 文章：**http://support.microsoft.com/kb/310516**。

示例 nnmtelnet.reg

此注册表内容示例适用于Windows 操作系统提供的 Telnet 客户端 (第 297 页)。

```
Windows 注册表编辑器版本 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_
DISABLE_TELNET_PROTOCOL]

"iexplore.exe"=dword:00000000

[HKEY_CLASSES_ROOT\telnet\shell\open\command]

@="\"C:\\Windows\\system32\\rundll32.exe\"
\"C:\\Windows\\system32\\url.dll\",TelnetProtocolHandler %l"
```

示例 nnmputtytelnet.reg

此注册表内容示例适用于第三方 Telnet 客户端(标准 Windows) (第 298 页)。

```
Windows 注册表编辑器版本 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_
DISABLE_TELNET_PROTOCOL]

"iexplore.exe"=dword:0c0000000

[HKEY_CLASSES_ROOT\telnet\shell\open\command]

@="\"C:\\Program Files\\PuTTY\\putty.exe\" %l"
```

示例 nnmtelnet32on64.reg

此注册表内容示例适用于第三方 Telnet 客户端 (Windows on Windows) (第 299 页)。

```
Windows 注册表编辑器版本 5.00
```

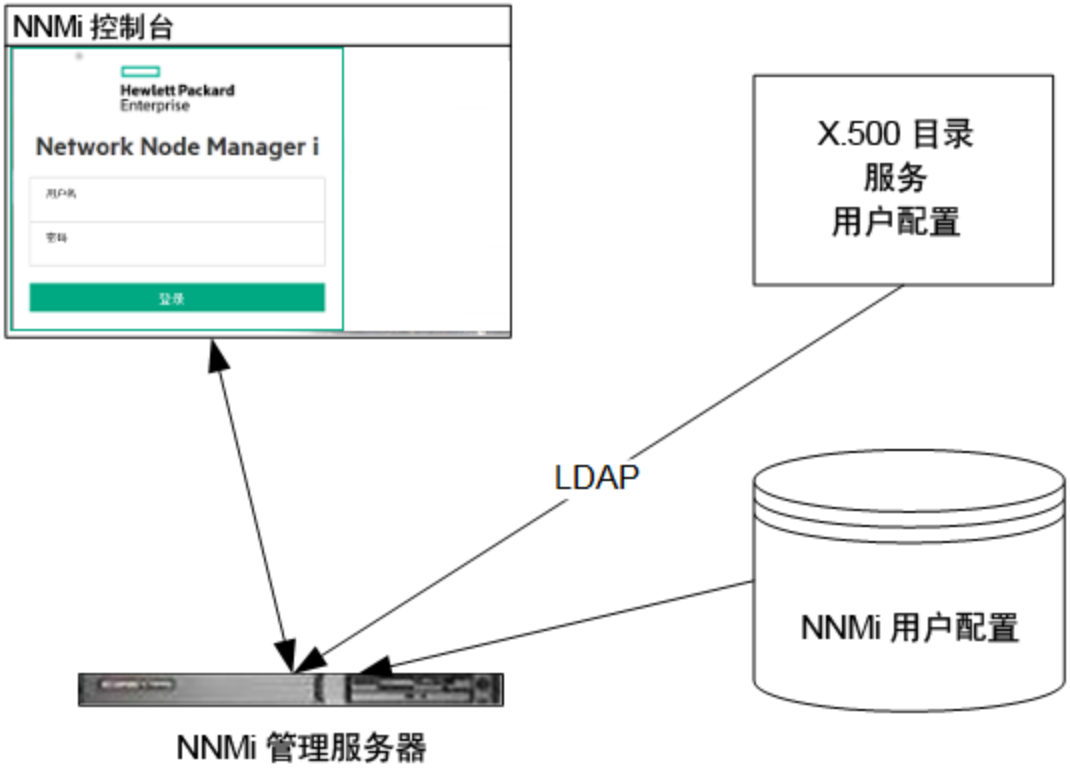
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL]

"iexplore.exe"=dword:00000000

[HKEY_CLASSES_ROOT\Wow6432Node\telnet\shell\open\command]

@="\"C:\\Program Files\\PuTTY\\putty.exe\" %l"
```

示例 nnmssh.reg

此注册表内容示例适用于第三方 SSH 客户端(标准 Windows 以及 Windows on Windows) (第 300 页)。

```
Windows 注册表编辑器版本 5.00

[HKEY_CLASSES_ROOT\ssh]

@="URL:ssh Protocol"

"EditFlags"=dword:00000002

"FriendlyTypeName"="Secure Shell"

"URL Protocol"=""

[HKEY_CLASSES_ROOT\ssh\shell\open\command]

@="\"C:\\Windows\\System32\\WScript.exe\" \"c:\\Program Files\\PuTTY\\ssh.js\" %l"
```

通过 LDAP 将 NNMi 与目录服务集成



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

- NNMi 用户访问信息和配置选项 (第 305 页)
- 配置 NNMi 访问目录服务 (第 309 页)
- 目录服务查询 (第 316 页)
- 用于存储 NNMi 用户组的目录服务配置 (第 326 页)
- 目录服务集成故障排除 (第 326 页)
- ldap.properties 配置文件参考 (第 327 页)

NNMi 用户访问信息和配置选项

以下各项将结合在一起定义 NNMi 用户：

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

NNMi 为 NNMi 用户访问信息的存储位置提供了若干个选项，如以下主题中所述。下表指示用于存储每个配置选项的 NNMi 用户访问信息的数据库。

备注: 如果用户不是使用外部(选项 3)指定的，则 NNMi 没有强制实施密码策略(如密码强度检查和其他帐户保护机制)的机制。建议实施密码策略管理的最佳实践，包括要求用户定期更改密码。

存储用户信息的选项

模式	用户帐户	用户组	用户组成员资格
内部(选项 1)	NNMi	NNMi	NNMi
混合(选项 2)	混合(NNMi 中的帐户名，LDAP 中的帐户密码)	NNMi	NNMi
外部(选项 3)	目录服务	两者	目录服务

NNMi 使用轻量级目录访问协议 (LDAP) 与目录服务通信。如果要将 LDAP 用于 NNMi，请使用上表中所示的以下某个模式：

- 混合模式(最初名为“选项 2”)：NNMi 数据库中的部分 NNMi 用户信息，以及目录服务中的部分 NNMi 用户信息

  使用混合模式包括配置 NNMi，将用户名、用户组和用户组映射存储在 NNMi 数据库中，并依靠目录服务获取用户名和密码(用户帐户)。这意味着账户名信息必须同时存储在 NNMi 和 LDAP 中，但帐户密码应只存储在 LDAP 中。
- 外部模式(最初名为“选项 3”)：目录服务中的所有 NNMi 用户信息

  使用外部模式时，无需向 NNMi 添加用户帐户信息，因为已使用 LDAP 存储所有用户帐户信息。

使用混合模式添加新的用户帐户或修改现有帐户时，必须选中**目录服务帐户**复选框。配置用户帐户时， 对某些用户不要选中**目录服务帐户**复选框，也不要选中它作为其他用户组合内部、混合和外部模式的方法。不支持这样的配置。

当 NNMi 与目录服务集成以获取部分或全部的用户访问信息时，**系统信息**窗口的**服务器**选项卡上的用户帐户和用户组定义语句指示了通过 LDAP 查询获取的信息类型。

NNMi 和其他应用程序之间的单点登录 (SSO) 与 NNMi 用户访问信息的配置或存储位置都无关。

内部模式(最初名为“选项 1”)：NNMi 数据库中的所有 NNMi 用户信息

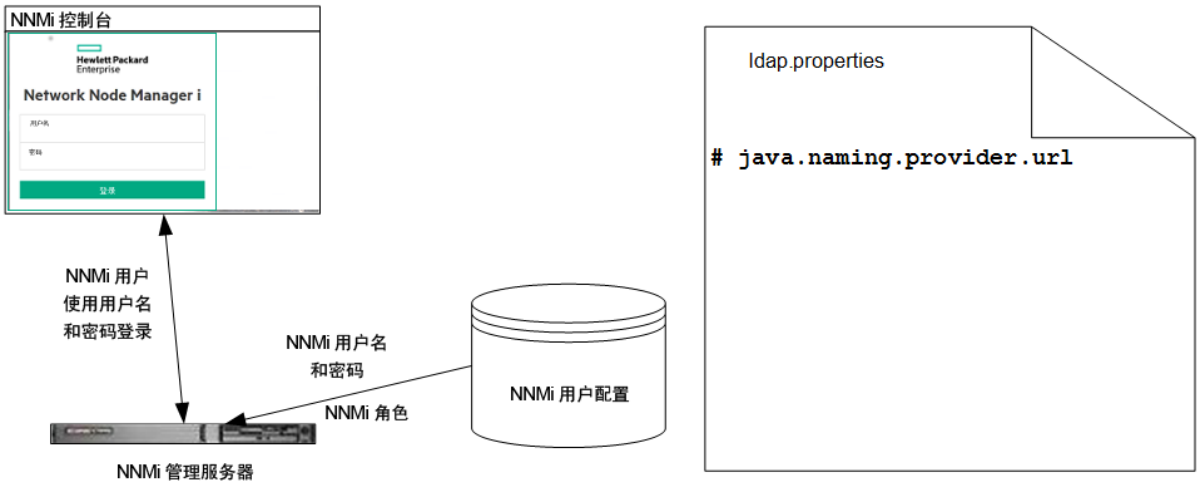
使用内部模式配置，NNMi 将访问 NNMi 数据库以获取全部的用户访问信息，此信息是 NNMi 管理员在 NNMi 控制台中定义并维护的。用户访问信息对于 NNMi 是本地的。NNMi 不访问目录服务，并且 NNMi 将忽略 `ldap.properties` 文件(如下图中的注释行所示)。

下图显示此选项的信息流，适用于以下情况：

- NNMi 用户数目少。
- 没有目录服务可用。

有关在 NNMi 数据库中设置所有用户信息的信息，请参阅 NNMi 帮助中的“使用 NNMi 帐户控制访问”。您无需阅读本章。

内部模式的 NNMi 用户登录信息流



混合模式(最初名为“选项 2”)：NNMi 数据库中的部分 NNMi 用户信息，以及目录服务中的部分 NNMi 用户信息

使用混合模式配置，NNMi 将访问目录服务以获取用户名和密码，此信息是在 NNMi 外部定义的并且还对其他应用程序可用。用户到 NNMi 用户组的映射是在 NNMi 控制台中维护的。NNMi 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和密码。
- NNMi 管理员在 NNMi 控制台中输入用户名(如目录服务中所定义)、用户组定义和用户组映射。
- NNMi 管理员将配置 NNMi `ldap.properties` 文件，以针对用户名向 NNMi 描述目录服务数据库架构。(在下图中，注释行表示 NNMi 不会从目录服务请求用户组信息。)

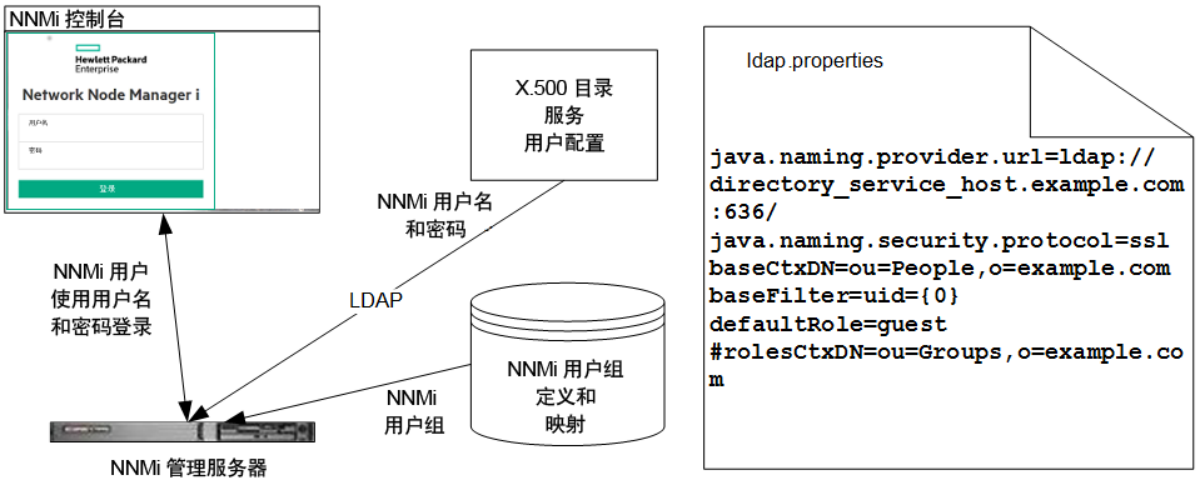
由于用户名必须输入到两个位置中，因此这两个位置都必须执行用户名维护。

下图显示此选项的信息流，适用于以下情况：

- NNMi 用户数目少，并且目录服务可用。
- NNMi 管理员要控制用户组，而不是用户组的每次更改都需要进行目录服务更改。
- 目录服务组定义不易扩展。

有关与目录服务集成以获取用户名和密码的信息，请参阅本章的其余部分以及 NNMi 帮助中的“同时使用目录服务和 NNMi 控制访问”。

使用混合模式的 NNMi 用户登录信息流



外部模式(最初名为“选项 3”)：目录服务中的所有 NNMi 用户信息

使用外部模式配置，NNMi 将访问目录服务以获取全部用户访问信息，此信息是在 NNMi 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 NNMi 用户组。

NNMi 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。
- NNMi 管理员在 NNMi 控制台中将目录服务组映射到 NNMi 用户组。
- NNMi 管理员将配置 NNMi `ldap.properties` 文件，以针对用户名和组向 NNMi 描述目录服务数据库架构。

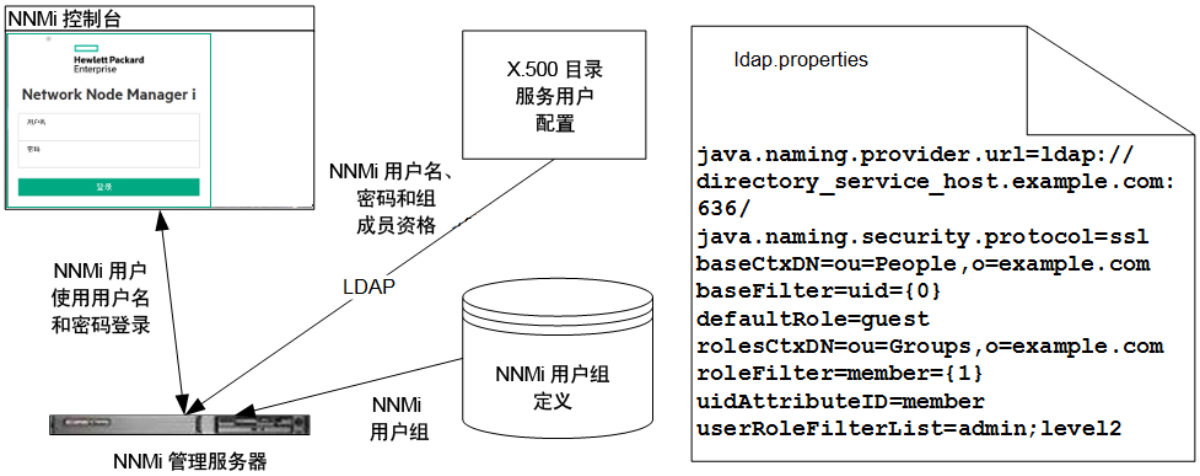
下图显示此选项的信息流，此选项适用于可以修改目录服务以包含需要访问 NNMi 的人员所属的用户组的情况。

因为此选项是混合模式场景的扩展，因此 HP 建议执行以下配置过程：

1. 配置并验证目录服务中的 NNMi 用户名和密码检索。
2. 配置目录服务中的 NNMi 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 NNMi 帮助中的“使用目录服务控制访问”。

使用外部模式的 NNMi 用户登录信息流



配置 NNMi 访问目录服务

目录服务访问在以下文件中配置：

- Windows：`%NNM_SHARED_CONF%\ldap.properties`
- Linux：`$NNM_SHARED_CONF/ldap.properties`

有关此文件的信息，请参阅 ldap.properties 配置文件参考 (第 327 页)。另请参阅示例 (第 331 页)。

有关目录服务的常规结构的信息，请参阅目录服务查询 (第 316 页)。

对于混合模式的配置，完成以下任务：

- 任务 1：备份当前 NNMi 用户信息
- 任务 2：可选。配置与目录服务的安全通信
- 任务 3：配置目录服务中的用户访问
- 任务 4：测试用户名和密码配置
- 任务 9：清除操作以防止意外访问 NNMi
- 任务 10：可选。将用户组映射到安全组 (第 315 页)

对于外部模式的配置，完成以下任务：

- 任务 1 备份当前 NNMi 用户信息
- 任务 2：可选。配置与目录服务的安全通信
- 任务 3：配置目录服务中的用户访问
- 任务 4：测试用户名和密码配置
- 任务 5：(仅配置选项 3)配置目录服务中的组检索

  备注: 如果计划在目录服务中存储 NNMi 用户组，则目录服务必须已配置 NNMi 用户组。有关详细信息，请参阅用于存储 NNMi 用户组的目录服务配置 (第 326 页)。

- 任务 6：(仅配置选项 3)将目录服务组映射到 NNMi 用户组
- 任务 7：(仅配置选项 3)测试 NNMi 用户组配置

- 任务 8：(仅配置选项 3)配置事件分配的 NNMi 用户组
- 任务 9：清除操作以防止意外访问 NNMi
- 任务 10：可选。将用户组映射到安全组

任务 1 备份当前 NNMi 用户信息

在 NNMi 数据库中备份用户信息：

```
nnmconfigexport.ovpl -c account -u <用户>
-p <密码> -f NNMi_database_accounts.xml
```

任务 2 为可选任务。配置与目录服务的安全通信

如果目录服务要求使用安全套接字层 (SSL)，请将贵公司的证书导入到 NNMi 信任库中，如配置与目录服务的 SSL 连接 (第 268 页)中所述。

任务 3 配置目录服务中的用户访问

仅对混合模式和外部模式完成此任务。执行适合您的目录服务的步骤。此任务包括以下部分：

- 用于 Microsoft Active Directory 的简单方法
- 用于其他目录服务的简单方法

(有关详细的配置说明，请参阅用户标识 (第 322 页)。)

用于 Microsoft Active Directory 的简单方法

1. 备份 NNMi 附带的 `ldap.properties` 文件，然后在任意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。如果您计划添加明文密码，请指定对目录服务具有只读访问权限的用户名。如果您计划指定加密密码，请使用以下命令对明文密码进行加密，然后再将其添加到 `ldap.properties` 文件中：

     `nnmldap.ovpl -encrypt <我的密码>`

     > **备注:** 此加密密码仅用于您为其创建此密码的 NNMi 实例。不要尝试将此加密密码用于其他 NNMi 实例。

     有关详细信息，请参阅 nnmldap.ovpl 参考页或 Linux 联机帮助页。

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简单方法

1. 备份 NNMi 附带的 `ldap.properties` 文件，然后在任意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：

   - 取消注释行(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 NNMi 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。

任务 4：测试用户名和密码配置

1. 在 ldap.properties 文件中，设置 defaultRole=guest 用于测试目的。(可以随时更改此值。)
2. 保存 ldap.properties 文件。
3. 通过运行以下命令，强制 NNMi 重新读取 ldap.properties 文件：

   nnmldap.ovpl -reload
4. 使用目录服务中定义的用户名和密码登录到 NNMi 控制台。

   提示: 用 NNMi 数据库中尚未定义的用户名运行此测试。

5. 验证 NNMi 控制台标题栏中的用户名和 NNMi 角色(来宾)。
   - 如果用户可以正常登录，则继续执行此任务的步骤 8。
   - 如果用户不能正常登录，则接下来继续执行步骤 6。

     提示: 在每个测试之后，从 NNMi 控制台注销以清除会话凭据。

6. 通过运行以下命令，测试一个用户的配置：

   nnmldap.ovpl -diagnose <NNMi 用户>

   将 <NNMi 用户> 替换为目录服务中定义的 NNMi 用户的登录名。

   检查命令输出，并作出相应的响应。建议的操作包括：
   - 验证是否正确完成了任务 3。
   - 遵循用户标识 (第 322 页)中的详细配置过程。
7. 重复步骤 1 到步骤 5，直到您在登录到 NNMi 控制台时看到预期结果。
8. 可以登录之后，选择策略：
   - 如果计划在 NNMi 数据库(使用混合模式的配置)中存储 NNMi 用户组成员资格，则继续执行任务 9。
   - 如果计划在目录服务(使用外部模式的配置)中存储 NNMi 用户组成员资格，则接下来继续执行任务 5。

任务 5：(仅外部模式)配置目录服务中的组检索

对配置选项 3 完成此任务。执行适合您的目录服务的步骤。此任务包括以下部分：

- 用于 Microsoft Active Directory 的简单方法
- 用于其他目录服务的简单方法

(有关详细的配置说明，请参阅用户组标识 (第 324 页)。)

用于 Microsoft Active Directory 的简单方法

1. 备份 ldap.properties 文件，然后在任意文本编辑器中打开文件。
2. 指定用于存储组记录的那部分目录服务域。在以下行中：

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

   执行以下操作：

   - 取消注释行(方法是删除 # 字符)。
   - 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简单方法

1. 备份 ldap.properties 文件，然后在任意文本编辑器中打开文件。
2. 指定用于存储组记录的那部分目录服务域。在以下行中：

   ```
   #rolesCtxDN=ou=Groups,o=myco.com
   ```

   执行以下操作：

   - 取消注释行(方法是删除 # 字符)。
   - 将 ou=Groups,o=myco.com 替换为存储组记录的那部分目录服务域。
3. 指定目录服务组定义中组成员名称的格式。在以下行中：

   ```
   roleFilter=member={1}
   ```

   将 member 替换为目录服务域中存储目录服务用户 ID 的组属性的名称。

任务 6：(仅外部模式)将目录服务组映射到 NNMi 用户组

1. 在 NNMi 控制台中，将预定义的 NNMi 用户组映射到其在目录服务中的对应方：
   a. 打开**用户组**视图。
      在**配置**工作区中，展开**安全性**，然后单击**用户组**。
   b. 双击 **admin** 行。
   c. 在**目录服务名称**字段中，输入 NNMi 管理员的目录服务组的完全可分辨名称。
   d. 单击 **保存并关闭**图标。
   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 NNMi 控制台访问。访问 NNMi 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 NNMi 用户组。

2. 对于目录服务中包含一个或多个 NNMi 用户的其他组，请在 NNMi 控制台中创建新用户组：
   a. 打开**用户组**视图。
      在**配置**工作区中，展开**安全性**，然后单击**用户组**。
   b. 单击 ✱ **新建**图标，然后输入组的信息：

- 将**唯一名称**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 NNMi 用户组用途的文本。

c. 单击 **保存并关闭**。

d. 对于 NNMi 用户的每个额外目录服务组，重复步骤 b 和步骤 c。

提示: 这些映射提供 NNMi 控制台中的拓扑对象访问。每个目录服务组可以映射到多个 NNMi 用户组。

任务 7：(仅外部模式)测试 NNMi 用户组配置

1. 保存 `ldap.properties` 文件。
2. 通过运行以下命令，强制 NNMi 重新读取 `ldap.properties` 文件：

   `nnmldap.ovpl -reload`
3. 使用目录服务中定义的用户名和密码登录到 NNMi 控制台。

   备注: 用于运行此测试的用户名在 NNMi 数据库中尚未定义，并且是映射到 admin、level1 或 level2 NNMi 用户组的目录服务组的成员。
4. 验证 NNMi 控制台标题栏中的用户名和 NNMi 角色(如**用户组**视图的**显示名称**字段中所配置)。
   - 如果用户可以正常登录，则继续执行任务 8。
   - 如果用户不能正常登录，则接下来继续执行步骤 5。

   提示: 在每个测试之后，从 NNMi 控制台注销以清除会话凭据。
5. 通过运行以下命令，测试一个用户的配置：

   `nnmldap.ovpl -diagnose <NNMi 用户>`

   将 `<NNMi 用户>` 替换为目录服务中定义的 NNMi 用户的登录名。

   检查命令输出，并作出相应的响应。建议的操作包括：
   - 验证是否正确完成了任务 5。
   - 验证对于每个预定义 NNMi 用户组，是否正确完成了任务 6。
   - 遵循用户组标识 (第 324 页)中的详细配置过程。
6. 重复步骤 1 到步骤 4，直到您在登录到 NNMi 控制台时看到预期结果。

任务 8：(仅外部模式)配置事件分配的 NNMi 用户组

1. 备份 `ldap.properties` 文件，然后在任意文本编辑器中打开文件。
2. 修改 `userRoleFilterList` 参数值以指定 NNMi 操作员可以向其分配事件的 NNMi 角色。

   提示: 格式是一个或多个预定义 NNMi 用户组的唯一名称的分号分隔列表(如用户组标识 (第 324 页)中所定义)。

3. 保存 `ldap.properties` 文件。
4. 通过运行以下命令，强制 NNMi 重新读取 `ldap.properties` 文件：

   `nnmldap.ovpl -reload`
5. 使用目录服务中定义的用户名和密码登录到 NNMi 控制台。
6. 在任何事件视图中，选择事件，然后单击**操作 > 分配 > 分配事件**。验证您是否可以将事件分配给具有 `userRoleFilterList` 参数所指定的各个 NNMi 角色的用户。
7. 重复步骤 1到步骤 6，直到可以将事件分配给每个配置的 NNMi 角色。

任务 9：清除操作以防止意外访问 NNMi

1. 可选。更改 `ldap.properties` 文件中 `defaultRole` 参数的值或注释掉该参数。
2. (仅限混合模式)要在 NNMi 数据库中存储用户组成员资格，请在 NNMi 数据库中如下重置用户访问信息：
   a. 删除任何预先存在的用户访问信息。(删除**用户帐户**视图中的所有行。)

      有关说明，请参阅 NNMi 帮助中的“删除用户帐户”。
   b. 对于每个 NNMi 用户，针对该用户名在**用户帐户**视图中创建新对象。
      - 对于**名称**字段，输入在目录服务中定义的用户名。
      - 选中**目录服务帐户**复选框。
      - 不要指定密码。

      有关详细信息，请参阅 NNMi 帮助中的“用户帐户任务”。
   c. 对于每个 NNMi 用户，将用户帐户映射到一个或多个 NNMi 用户组。

      有关说明，请参阅 NNMi 帮助中的“用户帐户映射任务”。
   d. 更新事件所有权，以使每个分配的事件都与某个有效用户名关联。

      有关说明，请参阅 NNMi 帮助中的“管理事件分配”。
3. (仅限外部模式)要在目录服务中存储用户组成员资格，请在 NNMi 数据库中如下重置用户访问信息：
   a. 删除任何预先存在的用户访问信息。(删除**用户帐户**视图中的所有行。)

      有关说明，请参阅 NNMi 帮助中的“删除用户帐户”。
   b. 更新事件所有权，以使每个分配的事件都与某个有效用户名关联。

      有关说明，请参阅 NNMi 帮助中的“管理事件分配”。

任务 10：可选。将用户组映射到安全组

有关说明，请参阅 NNMi 帮助中的“安全组映射任务”。

目录服务查询

NNMi 使用 LDAP 与目录服务通信。NNMi 发送请求，且目录服务返回存储的信息。NNMi 无法更改在目录服务中存储的信息。

本部分包含以下主题：

- 目录服务访问 (第 316 页)
- 目录服务内容 (第 316 页)
- 由目录服务管理员拥有的信息 (第 320 页)
- 用户标识 (第 322 页)
- 用户组标识 (第 324 页)

目录服务访问

对目录服务的 LDAP 查询使用以下格式：

`ldap://<目录服务主机>:<端口>/<搜索字符串>`

- `ldap` 是协议指示符。目录服务的标准连接和 SSL 连接都使用此指示符。
- <目录服务主机> 是托管目录服务的计算机的完全限定名称。
- <端口> 是目录服务用于 LDAP 通信的端口。非 SSL 连接的默认端口是 389。SSL 连接的默认端口是 636。
- <搜索字符串> 包含信息请求。有关详细信息，请参阅目录服务内容 (第 316 页)以及以下位置提供的 RFC 1959 An LDAP URL Format：
  labs.apache.org/webarch/uri/rfc/rfc1959.txt

可以将 LDAP 查询作为 URL 输入到 Web 浏览器中，以验证您的访问信息是否正确，以及搜索字符串结构是否正确。

> **提示:** 如果目录服务(例如，Active Directory)不允许匿名访问，则目录服务拒绝来自 Web 浏览器的 LDAP 查询。在这种情况下，可以使用第三方 LDAP 浏览器(例如，Apache Directory Studio 中附带的 LDAP 浏览器)验证配置参数。

目录服务内容

目录服务存储诸如用户名、密码和组成员资格之类的信息。要访问目录服务中的信息，必须知道引用信息存储位置的可分辨名称。对于登录应用程序，可分辨名称是可变信息(比如用户名)和固定信息(比如用户名的存储位置)的组合。组成可分辨名称的元素取决于目录服务的结构和内容。

以下示例显示名为 USERS-NNMi-Admin 的一组用户的可能定义。此组列出对 NNMi 具有管理访问权限的目录服务用户 ID。以下是这些示例的相关信息：

- Active Directory 示例用于 Windows 操作系统。
- 其他目录服务示例用于 Linux 操作系统。
- 每个示例中显示的文件是某个轻量级目录交换格式 (LDIF) 文件的一部分。LDIF 文件实现了目录服务信息的共享。
- 每个示例中显示的图是目录服务域的图形表示，用以展开方式查看 LDIF 文件摘录中的信息。

Active Directory 的内容结构示例

在此示例中，以下项是相关项：

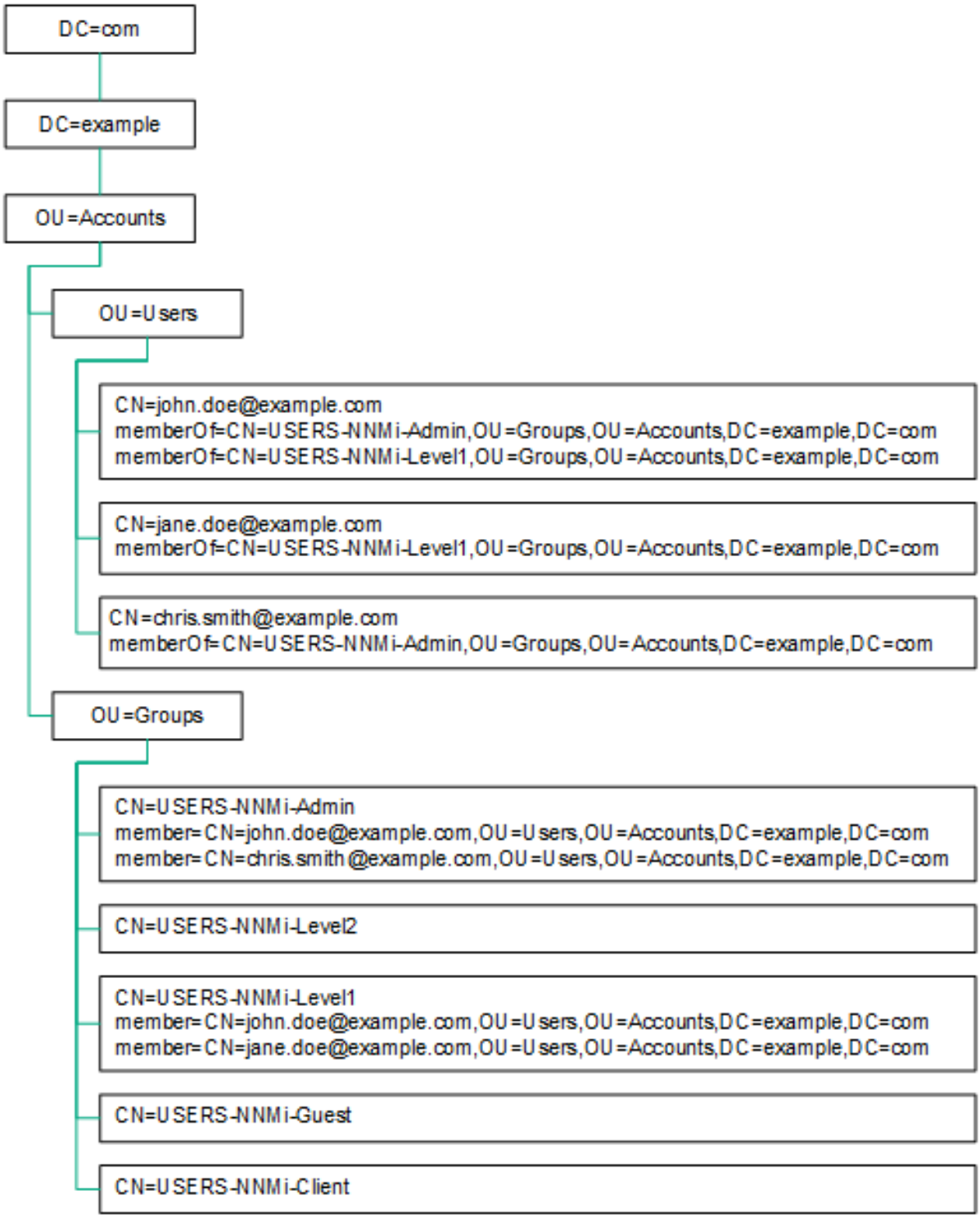
- 用户 John Doe 的可分辨名称是：
  `CN=john.doe@example.com,OU=Users,OU=Accounts,DC=example,DC=com`
- 组 USERS-NNMi-Admin 的可分辨名称是：
  `CN=USERS-NNMi-Admin,OU=Groups,OU=Accounts,DC=example,DC=com`
- 用于存储目录服务用户 ID 的组属性为：
  `member`

示例 LDIF 文件摘录：

```
groups |USERS-NNMi-Admin
dn:CN=USERS-NNMi-Admin,OU=Groups,OU=Accounts,DC=example,DC=com
cn:USERS-NNMi-Admin
description:Group of users for NNMi administration.
member:CN=john.doe@example.com,OU=Users,OU=Accounts,
 DC=example,DC=com
member:CN=chris.smith@example.com,OU=Users,OU=Accounts,
  DC=example,DC=com
```

下图图解了此目录服务域。

Active Directory 域示例



其他目录服务的内容结构示例

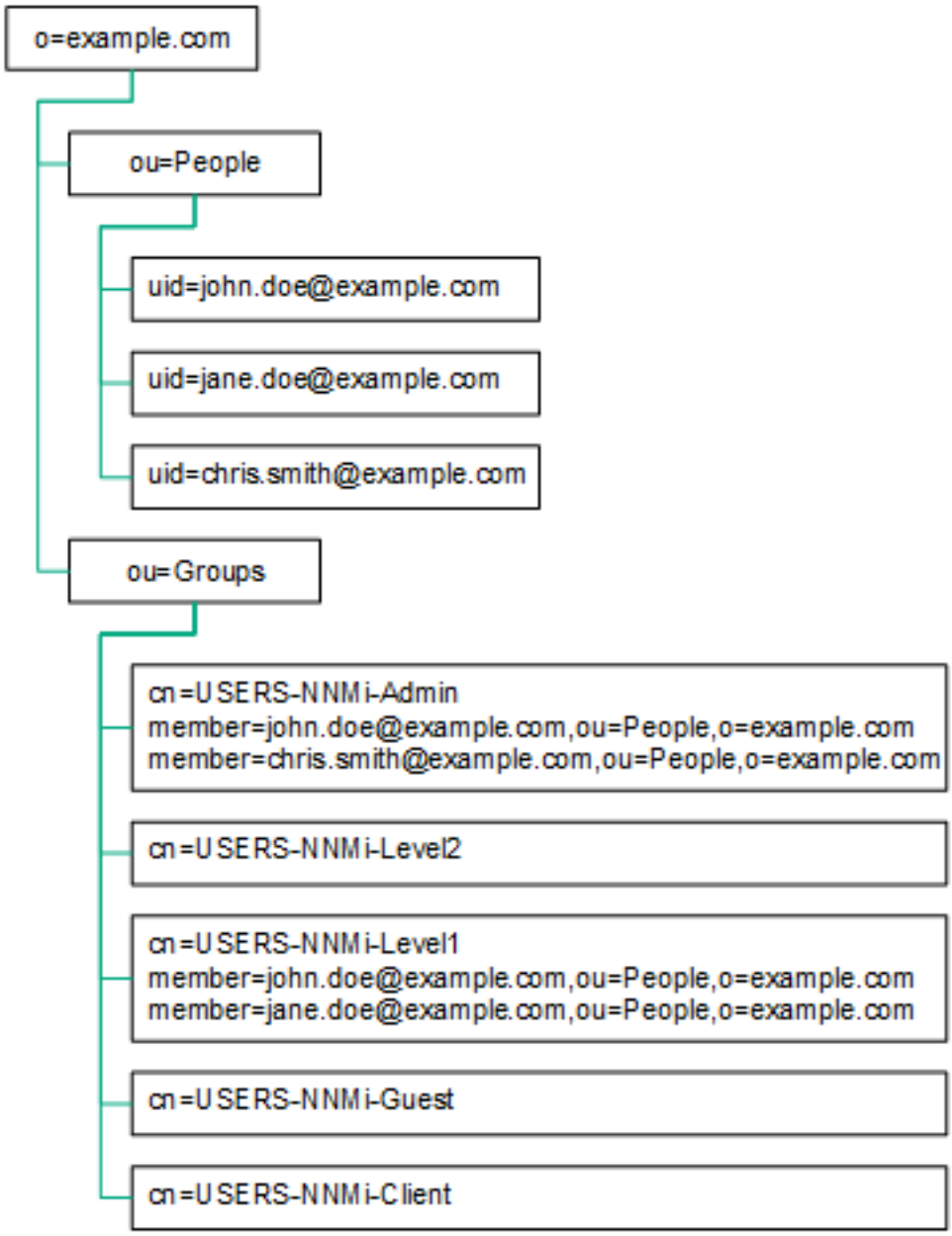
在此示例中，以下项是相关项：

- 用户 John Doe 的可分辨名称是：
  `uid=john.doe@example.com,ou=People,o=example.com`
- 组 USERS-NNMi-Admin 的可分辨名称是：
  `cn=USERS-NNMi-Admin,ou=Groups,o=example.com`
- 用于存储目录服务用户 ID 的组属性为：
  `member`

示例 LDIF 文件摘录：

```
groups |USERS-NNMi-Admin
dn: cn=USERS-NNMi-Admin,ou=Groups,o=example.com
cn:USERS-NNMi-Admin
description:Group of users for NNMi administration.
member: uid=john.doe@example.com,ou=People,o=example.com
member: uid=chris.smith@example.com,ou=People,o=example.com
```

其他目录服务域示例



由目录服务管理员拥有的信息

下表列出了在配置 NNMi 对目录服务进行 LDAP 访问之前，要从目录服务管理员处获取的信息。

- 如果计划将目录服务仅用于获取用户名和密码(仅限混合模式)，则收集有关从目录服务检索用户名和密码的信息。
- 如果计划将目录服务用于获取所有 NNMi 访问信息(仅限外部模式)，则收集以下每个表的信息。

用于从目录服务检索用户名和密码的信息

信息	Active Directory 示例	其他目录服务示例
托管目录服务的计算机的完全限定名称	directory_service_host.example.com	
目录服务用于 LDAP 通信的端口	• 对于非 SSL 连接是 389 • 对于 SSL 连接是 636	
目录服务需要 SSL 连接吗？	如果需要，则获取贵公司信任库证书的副本，并参阅配置与目录服务的 SSL 连接 (第 268 页)。	
存储在目录服务中(以演示目录服务域)的某个用户名的可分辨名称	CN=john.doe@example.com, OU=Users,OU=Accounts, DC=example,DC=com	uid=john.doe@example.com, ou=People,o=example.com

用于从目录服务检索组成员资格的信息

信息	Active Directory 示例	其他目录服务示例
用于标识为用户分配的组的可分辨名称	memberOf 用户属性用于标识这些组。	• ou=Groups,o=example.com • cn=USERS-NNMi-*, ou=Groups,o=example.com
用于标识组中用户的方法	• CN=john.doe@example.com, OU=Users,OU=Accounts, DC=example,DC=com • CN=john.doe@example.com	• cn=john.doe@example.com, ou=People,o=example.com • cn=john.doe@example.com
用于存储目录服务用户 ID 的组属性	member	member
目录服务中应用于 NNMi 访问的组名称	• CN=USERS-NNMi-Admin, OU=Groups,OU=Accounts, DC=example,DC=com • CN=USERS-NNMi-Level2, OU=Groups,OU=Accounts, DC=example,DC=com • CN=USERS-NNMi-Level1, OU=Groups,OU=Accounts, DC=example,DC=com • CN=USERS-NNMi-Client, OU=Groups,OU=Accounts, DC=example,DC=com • CN=USERS-NNMi-Guest, OU=Groups,OU=Accounts, DC=example,DC=com	• cn=USERS-NNMi-Admin, ou=Groups,o=example.com • cn=USERS-NNMi-Level2, ou=Groups,o=example.com • cn=USERS-NNMi-Level1, ou=Groups,o=example.com • cn=USERS-NNMi-Client, ou=Groups,o=example.com • cn=USERS-NNMi-Guest, ou=Groups,o=example.com

用户标识

用户标识适用于混合模式和外部模式。

用户标识的可分辨名称是在目录服务中找到一个用户的完全限定方法。NNMi 将 LDAP 请求中的用户可分辨名称传递到目录服务。

在 ldap.properties 文件中，用户可分辨名称是 baseFilter 值后跟 baseCtxDN 值。如果由目录服务返回的密码与用户输入到 NNMi 控制台中的登录密码相匹配，则用户登录操作将继续进行。

对于混合模式，应用以下信息：

- 对于 NNMi 控制台访问，NNMi 检查以下信息，并授予用户可用的最高特权：
  - ldap.properties 文件中的 defaultRole 参数的值
  - 此用户在 NNMi 控制台中的预定义 NNMi 用户组中的成员资格
- 对于 NNMi 拓扑对象访问，NNMi 将根据此用户在 NNMi 控制台中所属的 NNMi 用户组的安全组映射授予访问权限。

对于外部模式，应用以下信息：

- 对于 NNMi 控制台访问，NNMi 检查以下信息，并授予用户可用的最高特权：
  - ldap.properties 文件中的 defaultRole 参数的值
  - 此用户在目录服务组中的成员资格，这些目录服务组通过**目录服务名称**字段映射到 NNMi 控制台中的预定义 NNMi 用户组
- 对于 NNMi 拓扑对象访问，NNMi 将根据此用户在目录服务中所属组的安全组映射(这些组映射到 NNMi 控制台中的 NNMi 用户组)授予访问权限。

Active Directory 用户标识示例

如果 baseFilter 设置为 CN={0}，baseCtxDN 设置为 OU=Users,OU=Accounts,DC=example,DC=com，并且用户作为 john.doe 登录到 NNMi，则传递到目录服务的字符串如下：

```
CN=john.doe,OU=Users,OU=Accounts,DC=example,DC=com
```

其他目录服务用户标识示例

如果 baseFilter 设置为 uid={0}@example.com，baseCtxDN 设置为 ou=People,o=example.com，并且用户作为 john.doe 登录到 NNMi，则传递到目录服务的字符串如下：

```
uid=john.doe@example.com,ou=People,o=example.com
```

配置目录服务中的 NNMi 用户访问(详细方法)

如果任务 3 中所述的简单方法未能正常运行，则执行以下步骤：

1. 从目录服务管理员处获取所需的用户信息。
2. 通过完成相应的过程，验证目录服务中用户名的格式：
   - 用于 Active Directory 和其他目录服务的 LDAP 浏览器方法：请参阅确定目录服务如何标识用户(LDAP 浏览器方法)。
   - 用于其他目录服务的 Web 浏览器方法：请参阅确定目录服务如何标识用户(Web 浏览器方法)。

3. 在任何文本编辑器中打开 `ldap.properties` 文件。

> **提示:** 有关 `ldap.properties` 文件的信息，请参阅 ldap.properties 配置文件参考 (第 327 页)。

4. 将 `java.naming.provider.url` 参数设置为用于通过 LDAP 访问目录服务的 URL。
   - LDAP 浏览器方法：从 LDAP 浏览器配置中获取此信息。
   - Web 浏览器方法：包含确定目录服务如何标识用户(Web 浏览器方法)中的 <目录服务主机> 和 <端口> 的值。

> **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。

5. 如果已配置了与目录服务的安全通信，则取消以下代码行的注释(或添加以下代码行):

   `java.naming.security.protocol=ssl`
6. (仅 Active Directory)如下设置 `bindDN` 和 `bindCredential` 参数：
   - 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。

     如果您计划添加明文密码，请指定对目录服务具有只读访问权限的用户名。
     如果您计划指定加密密码，请使用以下命令对明文密码进行加密，然后再将其添加到 `ldap.properties` 文件中：

     `nnmldap.ovpl -encrypt <我的密码>`

     > **备注:** 此加密密码仅用于您为其创建此密码的 NNMi 实例。不要尝试将此加密密码用于其他 NNMi 实例。

     有关详细信息，请参阅 nnmldap.ovpl 参考页或 Linux 联机帮助页。
7. 将 `baseCtxDN` 参数设置为对于多个用户都相同的可分辨用户名组成元素。
8. 设置 `baseFilter` 参数将为 NNMi 登录输入的用户名与用户名在目录服务中的存储方式相关联。

   此值是对于每个用户都不同的可分辨用户名组成元素。将实际用户名替换为表达式 `{0}`。
9. 按任务 4 中所述测试配置。

确定目录服务如何标识用户(LDAP 浏览器方法)

在第三方 LDAP 浏览器中，执行以下操作：

1. 导航到用于存储组信息的那部分目录服务域。
2. 标识一组用户，然后检查与该组关联的用户的可分辨名称的格式。

确定目录服务如何标识用户(Web 浏览器方法)

1. 在受支持的 Web 浏览器中，输入以下 URL：

   ldap://<目录服务主机>:<端口>/<用户搜索字符串>

- <目录服务主机> 是托管目录服务的计算机的完全限定名称。
- <端口> 是目录服务用于 LDAP 通信的端口。
- <用户搜索字符串> 是目录服务中存储的一个用户名的可分辨名称。

2. 评估目录服务访问测试的结果。
   - 如果请求超时或者看到目录服务无法访问的消息，则验证 <目录服务主机> 和 <端口> 的值，然后重复执行步骤 1。
   - 如果看到目录服务不包含所请求条目的消息，则验证 <用户搜索字符串> 的值，然后重复执行步骤 1。
   - 如果看到适当的用户记录，则说明访问信息正确。<用户搜索字符串> 的值是可分辨用户名。

用户组标识

用户组标识适用于外部模式。

NNMi 如下确定 NNMi 用户的用户组：

1. NNMi 将 NNMi 控制台中配置的所有用户组的外部名称的值与目录服务组的名称进行比较。
2. 如果存在任何用户组匹配，则 NNMi 将确定 NNMi 用户是否是目录服务中该组的成员。

在 NNMi 控制台中，短文本字符串用于标识授予 NNMi 控制台访问权限的预定义 NNMi 用户组的唯一名称。`ldap.properties` 配置文件中的 `defaultRole` 和 `userRoleFilterList` 参数也需要这些文本字符串。下表将这些组的唯一名称映射到其显示名称。

NNMi 用户组名称映射

中的 NNMi 角色名称 NNMi 控制台	NNMi 配置文件中的用户组唯一名称和文本字符串
管理员	`admin`
全局操作员	`globalops`
第 2 级操作员	`level2`
第 1 级操作员	`level1`
来宾	`guest`
Web 服务客户端	`client`

备注: NNMi 全局操作员用户组 (`globalops`) 仅授予对所有拓扑对象的访问权限。一个用户必须分配到其他某个用户组(`level2`、`level1` 或 `guest`)后，才能访问 NNMi 控制台。

管理员不应将 `globalops` 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。

配置目录服务中的用户组检索(详细方法)

如果任务 5 中所述的简单方法未能正常运行，则执行以下步骤：

1. 从目录服务管理员处获取所需的用户信息。
2. 通过完成相应的过程，验证目录服务中组名和组成员的格式：
   - 用于 Active Directory 的 LDAP 浏览器方法：请参阅确定目录服务如何标识组和组成员资格(用于 Active Directory 的 LDAP 浏览器方法)。
   - 用于其他目录服务的 LDAP 浏览器方法：请参阅确定目录服务如何标识组和组成员资格(用于其他目录服务的 LDAP 浏览器方法)。
   - 用于其他目录服务的 Web 浏览器方法：请参阅确定目录服务如何标识组(Web 浏览器方法)。
3. 在任何文本编辑器中打开 `ldap.properties` 文件。

   提示: 有关 `ldap.properties` 文件的信息，请参阅 ldap.properties 配置文件参考 (第 327 页)。

4. 将 `rolesCtxDN` 参数设置为对于多个组都相同的可分辨组名组成元素。
5. 设置 `roleFilter` 参数以将用户名关联到目录服务的组中用户名的存储方式。将实际用户名替换为以下某个表达式：
   - 使用 `{0}` 表示为登录输入的用户名(例如 `john.doe`)。
   - 使用 `{1}` 表示由目录服务返回的已验证用户的可分辨名称(例如 `uid=john.doe@example.com,ou=People,o=example.com`)。
6. 将 uidAttributeID 参数设置为存储用户 ID 的组属性的名称。
7. 按配置 NNMi 访问目录服务 (第 309 页) 中所述测试配置。

确定目录服务如何标识组和组成员资格(用于 Active Directory 的 LDAP 浏览器方法)

在第三方 LDAP 浏览器中，执行以下操作：

1. 导航到用于存储用户信息的那部分目录服务域。
2. 标识需要访问 NNMi 的用户，然后检查与该用户关联的组的可分辨名称的格式。
3. 导航到用于存储组信息的那部分目录服务域。
4. 标识对应于 NNMi 用户组的组，然后检查与组关联的用户的名称格式。

确定目录服务如何标识组和组成员资格(用于其他目录服务的 LDAP 浏览器方法)

在第三方 LDAP 浏览器中，执行以下操作：

1. 导航到用于存储组信息的那部分目录服务域。
2. 标识对应于 NNMi 用户组的组，然后检查这些组的可分辨名称的格式。
3. 还要检查与组关联的用户的名称格式。

确定目录服务如何标识组(Web 浏览器方法)

1. 在受支持的 Web 浏览器中，输入以下 URL：

   ldap://<目录服务主机>:<端口>/<组搜索字符串>

- <目录服务主机> 是托管目录服务的计算机的完全限定名称。
- <端口> 是目录服务用于 LDAP 通信的端口。
- <组搜索字符串> 是目录服务中存储的组名称的可分辨名称，例如：`cn=USERS-NNMi-Admin,ou=Groups,o=example.com`

2. 评估目录服务访问测试的结果。
   - 如果看到目录服务不包含所请求条目的消息，则验证 <组搜索字符串> 的值，然后重复执行步骤 1。
   - 如果看到适当的组列表，则说明访问信息正确。
3. 检查组属性以确定与该组关联的用户的名称格式。

用于存储 NNMi 用户组的目录服务配置

如果计划在目录服务(外部模式)中存储 NNMi 用户组，则必须使用 NNMi 用户组信息对目录服务进行配置。理想情况下，目录服务已经包含适当的用户组。如果不是这样，则目录服务管理员可以专门为 NNMi 用户组分配创建新用户组。

因为目录服务配置和维护过程取决于特定目录服务软件和贵公司的策略，所以此处不讲述这些过程。

目录服务集成故障排除

1. 通过运行以下命令，验证 NNMi LDAP 配置：

   `nnmldap.ovpl -info`

   如果报告的配置不是预期结果，则验证 `ldap.properties` 文件中的设置。
2. 通过运行以下命令，强制 NNMi 重新读取 `ldap.properties` 文件：

   `nnmldap.ovpl -reload`
3. 通过运行以下命令，测试一个用户的配置：

   `nnmldap.ovpl -diagnose <NNMi 用户>`

   将 `<NNMi 用户>` 替换为目录服务中定义的 NNMi 用户的登录名。

   检查命令输出，并作出相应的响应。
4. 验证目录服务是否包含预期的记录。使用 Web 浏览器或第三方 LDAP 浏览器(例如，Apache Directory Studio 中附带的 LDAP 浏览器)检查目录服务信息。

   有关目录服务查询格式的信息，可参阅以下位置提供的 RFC 1959 An LDAP URL Format：

   http://labs.apache.org/webarch/uri/rfc/rfc1959.txt
5. 查看日志文件以验证登录请求是否正确，并确定是否发生了任何错误：

   Windows：`%NnmDataDir%\log\nnm\nnm.log`

   Linux：`$NnmDataDir/log/nnm/nnm.log`
   - 与以下行类似的消息表示目录服务需要 HTTPS 通信。在这种情况下，如配置与目录服务的 SSL 连接 (第 268 页)中所述启用 SSL。

```
javax.naming.AuthenticationNotSupportedException:[LDAP: error code 13 -
confidentiality required]
```

- 与以下行类似的消息表示与目录服务通信时发生超时。在这种情况下，请增大 ldap.properties 文件中 searchTimeLimit 的值。

```
javax.naming.TimeLimitExceededException:[LDAP: error code 3 - Timelimit Exceeded]
```

ldap.properties 配置文件参考

ldap.properties 文件包含用于与目录服务通信以及构建对目录服务的 LDAP 查询的设置。此文件位置如下：

- Windows：%NNM_SHARED_CONF%\ldap.properties
- Linux：$NNM_SHARED_CONF/ldap.properties

在 ldap.properties 文件中，以下约定适用：

- 要将某行注释掉，请使该行以井号字符 (#) 开头。
- 以下规则适用于特殊字符：
  - 要指定反斜杠字符 (\)、逗号 (,)、分号 (;)、加号 (+)、小于号 (<) 或大于号 (>)，请使用反斜杠字符将字符转义。例如：\\ 或 \+
  - 要包含空格字符 ( ) 作为字符串中的第一个或最后一个字符，请使用反斜杠字符 (\) 将空格字符转义。
  - 要包含井号字符 (#) 作为字符串中的第一个字符，请使用反斜杠字符 (\) 将井号字符转义。

  此处未提到的字符不需要转义或加引号。

备注: 编辑 ldap.properties 文件之后，通过运行以下命令，强制 NNMi 重新读取 LDAP 配置：

```
nnmldap.ovpl -reload
```

下表描述了 ldap.properties 文件中的参数。

备注: 初始 ldap.properties 文件可能未包含下表中列出的所有参数。请添加需要的参数。

ldap.properties 文件中的参数

参数	描述
java.naming.provider.url	指定用于访问目录服务的 URL。 格式是协议 (ldap)，后跟目录服务器的完全限定主机名，(可选)再后跟端口号。例如： java.naming.provider.url=ldap://ldap.example.com:389/ 如果省略端口号，将应用以下默认值： • 对于非 SSL 连接，默认端口是 389。

ldap.properties 文件中的参数(续)

参数	描述
	• 对于 SSL 连接，默认端口是 636。 如果指定多个目录服务 URL，则 NNMi 会在可能的情况下使用第一个目录服务。如果该目录服务不可访问，则 NNMi 查询列表中的下一个目录服务，以此类推。用一个空格字符分隔每个 URL。例如： `java.naming.provider.url=ldap://ldap1.example.com/ ldap://ldap2.example.com/` 配置此参数将启用 NNMi 和目录服务之间的 LDAP 通信。要禁用 LDAP 通信，请注释掉此参数，然后保存文件。NNMi 将忽略 `ldap.properties` 文件中的配置。
java.naming.security.protocol	指定连接协议规范。 • 如果将目录服务配置为使用 LDAP over SSL，则将此参数设置为 `ssl`。例如： `java.naming.security.protocol=ssl` • 如果目录服务不需要 SSL，则使此参数保留被注释掉的状态。 有关详细信息，请参阅配置与目录服务的 SSL 连接 (第 268 页)。

bindDN	对于不允许匿名访问的目录服务(比如 Active Directory)，指定用于访问目录服务的用户名。
	例如：
	`bindDN=region1\\john.doe@example.com`
	• 如果您计划添加明文密码，请指定对目录服务具有只读访问权限的用户名。
	例如：
	`bindCredential=PasswordForJohnDoe`
	• 如果您计划指定加密密码，请使用以下命令对明文密码进行加密，然后再将其添加到 `ldap.properties` 文件中：
	`nnmldap.ovpl -encrypt <我的密码>`
	例如：`bindCredential={ENC}uaF22C+0CF9VozBVYj8OAw==`
	
	此加密密码仅用于您为其创建此密码的 NNMi 实例。不要尝试将此加密密码用于其他 NNMi 实例。
	有关详细信息，请参阅 nnmldap.ovpl 参考页或 UNIX 联机帮助页。

bindCredential	设置 `bindDN` 时，为 `bindDN` 所标识的用户名指定密码。例如： `bindCredential=PasswordForJohnDoe`
baseCtxDN	指定用于存储用户记录的那部分目录服务域。 格式是目录服务属性名称和值的逗号分隔列表。例如： • `baseCtxDN=CN=Users,DC=ldapserver,DC=example,DC=com` • `baseCtxDN=ou=People,o=example.com` 有关详细信息，请参阅用户标识 (第 322 页)。

ldap.properties 文件中的参数(续)

参数	描述

baseFilter	指定用于登录到 NNMi 的用户名的格式。
	格式为目录服务用户名属性的名称以及一个字符串，该字符串用于将输入的用户登录名称关联到目录服务中的名称格式。用户名字符串包含表达式 `{0}`(表示输入的登录用户名)以及匹配目录服务格式的用户名所需的任何其他字符。
	• 如果为 NNMi 登录输入的用户名与目录服务中存储的用户名相同，则该值是替换表达式。例如：
	  • `baseFilter=CN={0}`
	  • `baseFilter=uid={0}`
	• 如果为 NNMi 登录输入的用户名是目录服务中存储的用户名的一部分，请在值中包含其他字符。例如：
	  • `baseFilter=CN={0}@example.com`
	  • `baseFilter=uid={0}@example.com`
	有关详细信息，请参阅用户标识 (第 322 页)。

defaultRole	可选。指定应用于通过 LDAP 登录到 NNMi 的任何目录服务用户的默认角色。将始终应用此参数的值，而与用户组映射的存储位置(在 NNMi 数据库中或在目录服务中)无关。 如果直接为预定义 NNMi 用户组配置用户，则 NNMi 授予该用户默认角色和已分配用户组的特权的超集。 有效值如下：`admin`、`level2`、`level1` 或 `guest`。 请注意，尽管 `admin` 是有效值，但您应谨慎使用，并考虑使 `admin` 成为默认角色的含义。 这些名称是预定义 NNMi 用户组名称的唯一名称。 例如： `defaultRole=guest` 如果被注释掉或被省略，则 NNMi 不使用默认角色。
rolesCtxDN	指定用于存储组记录的那部分目录服务域。 格式是目录服务属性名称和值的逗号分隔列表。例如： • `rolesCtxDN=CN=Users,DC=ldapserver,DC=example,DC=com` • `rolesCtxDN=ou=Groups,o=example.com` 在其他目录服务(非 Active Directory)中，为实现更快的搜索，您可以标识包含 NNMi 用户组的一个或多个目录服务组。如果这些组名称构成某种模式，则可以指定通配符。例如，如果目录服务包含名为 `USERS-NNMi-administrators`、`USERS-NNMi-level1Operators` 之类的组，则可以使用如下所示的搜索上下文：

ldap.properties 文件中的参数(续)

参数	描述
	`rolesCtxDN=cn=USERS-NNMi-*,ou=Groups,o=example.com` 配置此参数将使目录服务通过 LDAP 查询 NNMi 用户组分配。 要禁用目录服务通过 LDAP 查询 NNMi 用户组分配，请注释掉此参数，然后保存文件。NNMi 将忽略 `ldap.properties` 文件中其余与用户组相关的值。 有关详细信息，请参阅用户组标识 (第 324 页)。

roleFilter	指定目录服务组定义中组成员名称的格式。
	格式为用户 ID 的目录服务组属性的名称以及一个字符串，该字符串用于将输入的用户登录名关联到目录服务中的用户 ID 格式。用户名字符串包含以下某个表达式以及匹配目录服务格式的组成员名称所需的任何其他字符。
	• 表达式 `{0}` 表示输入的登录用户名(例如 `john.doe`)。
	与输入的登录(短)用户名匹配的角色筛选的示例如下：
	`roleFilter=member={0}`
	• 表达式 `{1}` 表示由目录服务返回的已验证用户的可分辨名称(例如
	`CN=john.doe@example.com,OU=Users,OU=Accounts,`
	`DC=example,DC=com`
	或
	`uid=john.doe@example.com,ou=People,o=example.com`)。
	关于与(完整)已验证用户名匹配的角色筛选示例：
	`roleFilter=member={1}`
	有关详细信息，请参阅用户组标识 (第 324 页)。

uidAttributeID	指定用于存储目录服务用户 ID 的组属性。 例如： `uidAttributeID=member` 有关详细信息，请参阅用户组标识 (第 324 页)。
userRoleFilterList	可选。限制可以向其所关联用户分配 NNMi 控制台中的事件的 NNMi 用户组。 此列表中的用户组仅应用于通过 LDAP 验证的目录服务用户名。此参数提供了在 NNMi 控制台中分配 NNMi 用户组并将其存储在 NNMi 数据库中时不可用的功能。 格式是一个或多个预定义 NNMi 用户组名称的唯一名称的分号分隔列表。 `userRoleFilterList=admin;globalops;level2;level1`
searchTimeLimit	可选。指定超时值(毫秒)。默认值是 10000(10 秒)。如果在 NNMi 用户登录期间发生超时，请增大此值。 例如： `searchTimeLimit=10000`

示例

用于 Active Directory 的 ldap.properties 文件示例

下面是用于 Active Directory 的 `ldap.properties` 文件示例：

```
java.naming.provider.url=ldap://MYldapserver.example.com:389/
bindDN=MYdomain\\MYusername
bindCredential=MYpassword
baseCtxDN=CN=Users,DC=MYldapserver,DC=EXAMPLE,DC=com
baseFilter=CN={0}
defaultRole=guest
rolesCtxDN=CN=Users,DC=MYldapserver,DC=EXAMPLE,DC=com
rolesCtxDN=CN=Users,DC=MYldapserver,DC=EXAMPLE,DC=com
roleFilter=member={1}
uidAttributeID=member
userRoleFilterList=admin;level2;level1
```

用于其他目录服务的 ldap.properties 文件示例

下面是用于其他目录服务的 `ldap.properties` 文件示例：

```
java.naming.provider.url=ldap://MYldapserver.example.com:389/
baseCtxDN=ou=People,o=EXAMPLE.com
baseFilter=uid={0}
defaultRole=guest
rolesCtxDN=ou=Groups,o=EXAMPLE.com
roleFilter=member={1}
uidAttributeID=member
userRoleFilterList=admin;level2;level1
```

管理 NAT 环境中的重叠 IP 地址

NNMi 可帮助管理网络区域，包括网络地址转换 (NAT) 域实现(可能会产生重复的 IP 地址，并要求对 NNMi 进行配置以处理 NAT 内部/外部 IP 地址对)。NNMi 管理员通过创建租户定义来标识每个 NAT 域。NNMi 使用租户/IP 地址对标识每个节点。除非地址在一个租户的节点组中重复，否则不视为重复。

> **备注:** NAT 域集成上下文以外的重复 IP 地址：如果您的网络包含防火墙或具有重复 IP 地址/MAC 地址的负载平衡器设备(如托管在物理设备上的虚拟实例)。NNMi 管理员使用防火墙和负载平衡器的 sysObjectId 值填充配置文件。然后 NNMi 成功确认具有这些 sysObjectId 值的节点对象的每个实例 (而非视为相同的节点对象全部合并)。

什么是 NAT?

网络地址转换 (NAT) 通常用于互连本地网络与外部(公用)Internet。具体而言，NAT 转换 IP 报头信息，将需要经过公用网络的 IP 包中的专用地址替换为公用地址。通过提供静态或动态外部 IP 地

址，NAT 完成此操作。通过从不使用发送者的 IP 地址进行 Internet 访问将网络地址转换用作 Internet 安全度量。

网络地址转换技术已开发成一种解决方案，以满足对更多 IPv4 地址的不断增长的需求。某些 IP 地址范围(RFC 1918 中所述)已仅指定为内部地址；也就是说，不可通过 Internet 路由。任何人都可以将这些地址用于专用网络， 从而减少必须购买的公用地址数。

NAT 的优势是什么？

NAT 的一些优势包括：

- 重复利用专用 IP 地址
- 通过对外部网络隐瞒内部寻址，增强专用网络的安全性
- 使用较少数量的公用(外部)IP 地址将大量主机连接到全局 Internet，进而节省 IP 地址空间

支持哪些类型的 NAT?

NNMi 支持以下类型的 NAT 协议：

- 静态 NAT - 一种 NAT 类型，将内部 IP 地址映射到外部 IP 地址，其中外部地址始终为同一个 IP 地址(也就是说，每个节点具有一个静态内部/外部地址对)。这允许内部主机(如 Web 服务器)具有一个专用 IP 地址，而同时仍可以通过 Internet 进行访问。
- 动态 NAT - 一种 NAT 类型，其中，外部地址和内部地址之间的映射在会话之间可以发生改变。内部 IP 地址动态映射到可用的公用 IP 地址池中的外部 IP 地址。通常，网络中的 NAT 网关路由器会保留一个已注册公用 IP 地址表，当内部 IP 地址请求访问 Internet 时，该路由器会选择当前未由其他内部 IP 地址使用的 IP 地址。
- 动态端口地址转换(PAT，也称为网络地址和端口转换 (NAPT))- 这种类型的 NAT 不仅动态提供外部 IP 地址，还动态提供端口号。转换地址和端口号允许单个外部地址用于通过 Internet 的多个并发内部地址会话。

如何在 NNMi 中实现 NAT?

NNMi 通过使用租户/IP 地址对标识每个节点来管理 NAT 环境。NNMi 管理员为每个 NAT 地址域创建一个租户定义。租户可标识节点的逻辑分组。例如，Internet 提供商的网络可能有多个实现专用 IP 地址的客户。在 NNMi 中，Internet 提供商可以将每个客户的节点分配到可标识每个客户的特定租户名称。在该逻辑租户分组中：

- NNMi 管理员使用发现种子来标识使用租户/IP 地址对的租户成员节点。
- 子网连接规则在租户的每一组节点中单独应用。
- 路由器冗余组在每个租户中都独立于任何其他租户的节点组接受监视。
- NNMi 只在每个租户的节点组中发现第 2 层连接，之间定义了租户的节点和分配到名为默认租户的租户的节点。
- 将互连多个 NAT 域(比如 NAT 网关路由器)的任何基础设备分配给默认租户。这可确保 NNMi 显示您的工作组(和客户)需要看到的第 2 层连接。
- 安全组可确定 NNMi 用户可以看到的租户数量。分配的安全组可以包含多个租户的节点。有关详细信息，请参阅NNMi 安全和多租户配置 (第 356 页)。

提示: 最佳实践是在网络管理环境中的所有 NAT 域间没有重复的域名系统 (DNS) 名称。

根据您所用的 NAT 协议，NNMi 的实现方法和要求会有所不同。例如，使用动态 NAT 或 PAT 将需要其他硬件和许可证。请根据您的 NAT 协议类型，参阅相应部分：

- 静态 NAT 注意事项 (第 333 页)
- 动态 NAT 和 PAT 注意事项 (第 341 页)

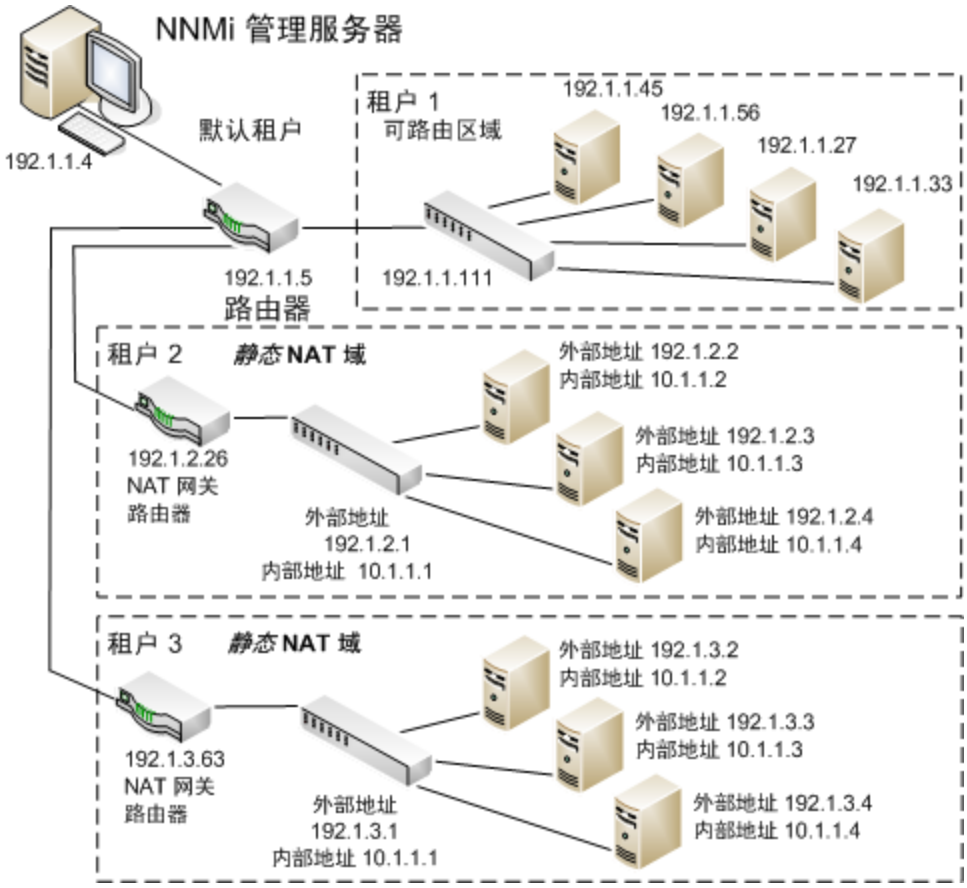
然后参阅在网络地址转换 (NAT) 环境中部署 NNMi (第 344 页)，了解详细信息。

静态 NAT 注意事项

一台 NNMi 管理服务器可以监视任意数量的静态 NAT 实例，只要每个实例均配置有一个唯一的租户即可。有关租户的详细信息，请参阅 NNMi 安全和多租户 (第 347 页)和 NNMi 帮助中的“配置租户”。

有关静态 NAT 配置的示例，请参阅下图。

静态 NAT 配置示例



备注: 属于默认租户的节点可以与任何租户中的任何节点进行第 2 层连接。默认租户以外的任何租户中的节点只能与同一租户或默认租户中的设备进行第 2 层连接。

子网是特定于租户的(也就是说，子网不跨租户)。其优势在于您可以对不同租户使用相同子网。

路由器冗余组 (RRG) 无法跨租户。

提示: 将互连多个 NAT 域(比如 NAT 网关)的任何基础设备分配至默认租户。这可确保 NNMi 显示您的工作组(和客户)需要看到的第 2 层连接。

备注: 默认安全组中的设备可从所有视图中查看。要控制对设备的访问，请将该设备分配至默认安全组以外的安全组。

硬件和软件要求以及静态 NAT

管理静态 NAT 域没有特殊的硬件或软件要求。一个 NNMi 管理服务器可以管理任意数量的包含 NNMi、NNMi Advanced、NNMi Premium 或 NNMi Ultimate 的静态 NAT 域。

重叠 IP 地址映射

NNMi 管理服务器在静态 NAT 域之外时，最好使用重叠地址映射标识每个静态 NAT 内部/外部 IP 地址对。NNMi 针对静态 NAT 域用以下方式使用映射的外部地址/内部地址对：

- 节点表单显示映射地址属性值
- 增强了通信和监视进程。这样可以确保 NNMi 成功计算每个静态 NAT 节点的 SNMP 代理以及被管 IP 地址的状况和状态(另请参阅 NNMi 状况和状态计算 (第 346 页))：
  - NNMi 可以准确地使用 ICMP 故障监视的 IP 地址故障轮询的监视配置设置。
  - NNMi 可以通过使用 ICMP ping 请求(除 SNMP 查询外)准确地确定非 SNMP 节点的第 2 层和第 3 层连接。
- NNMi 可在从 NAT 域生成陷阱时准确确定 SNMP 陷阱源节点。如果在网络中使用了 SNMPv1，则另请参阅第 240 页上的“静态 NAT 环境中的 SNMP 陷阱”。
- 准确计算自定义事件属性：
  - `cia.agentAddress` = 外部 IP 地址(公用地址)。
  - `cia.internalAddress` = 事件源节点的内部 IP 地址。

备注: 如果正在为使用动态 NAT 或 PAT 的网络管理域的区域配置 NNMi，则不要使用重叠 IP 地址映射表单。请参阅动态 NAT 和 PAT 注意事项 (第 341 页)。

专用 IP 地址范围

Internet 工程任务组 (IETF) 和 Internet 地址分配机构 (IANA) 保留以下 IP 地址范围用于专用网络，例如企业局域网 (LAN)、公司办公室或住宅网络。

IPv4 专用地址范围 (RFC 1918)：

- 10.0.0.0 – 10.255.255.255(24 位块)
- 172.16.0.0 – 172.31.255.255(20 位块)
- 192.168.0.0 – 192.168.255.255(16 位块)

IPv6 专用地址范围：

- fc00::/7 地址块 = RFC 4193 唯一本地地址 (ULA)
- fec0::/10 地址块 = 已弃用 (RFC 3879)

通信和静态 NAT

通过自动使用任何可用的重叠地址映射来确定静态 NAT 通信的租户/外部 IP 地址对，NNMi 成功通过静态 NAT 防火墙通信。有关各种好处的信息，请参阅重叠 IP 地址映射 (第 334 页)。

管理对静态 NAT 环境中的管理地址的 ICMP 轮询

在 NAT 环境中，防火墙阻止 NNMi 使用 NAT 节点上的 IP 地址(专用 IP 地址)与这些 NAT 节点进行通信。要对此进行补救，请使用 NAT 地址(公用 IP 地址)与 NNMi 通信。

在 NAT 环境中，节点的管理地址可能不同于该节点上托管的 IP 地址。为使 NNMi 能够发现 NAT 环境中的节点，必须将 NAT 地址作为发现种子添加到 NNMi 中。NNMi 使用此 NAT 地址进行通信，虽然它并不在节点的 `ipAddressTable` 中。

NNMi 提供此功能以避免生成虚假的节点故障事件，并能更好地执行根源分析。

启用对 NAT 环境中的管理地址的 ICMP 轮询

默认情况下，NNMi 自动启用对所有节点的 ICMP 管理地址轮询，包括 NAT 环境中的那些节点。如果您具有 NAT 环境，则强烈建议您不要禁用此设置。

要启用 ICMP 管理地址轮询(如果已禁用)，请执行以下操作：

1. 从工作区导航面板，选择**配置**工作区，展开**监视**文件夹，选择**监视配置**并找到**默认设置**选项卡。
2. 启用 `ICMP` 管理地址轮询。请参阅 NNMi 帮助中的“设置默认监视”。

对 SNMP 代理执行**操作 -> 监视设置**之后，查看 NNMi 显示的信息。显示的信息表示 NNMi 是否启用了管理地址轮询。

启用 ICMP 管理地址轮询时，NNMi 发生如下更改：

- “代理 ICMP 状况”字段出现在以下表单中：
  - 节点表单
  - SNMP 代理表单
  - SNMP 代理表视图
- NNMi 更改管理地址 ICMP 状况的显示位置。NNMi 还更改它确定 SNMP 代理状态的方式。

下表显示 NNMi 为 ICMP 管理地址轮询和 ICMP 故障轮询设置执行的代理 ICMP 和 IP 地址状况轮询操作。

ICMP 配置和生成的状况轮询

ICMP 管理地址轮询	ICMP 故障轮询	代理 ICMP 状况	IP 地址状况
已启用	已禁用	已轮询	未轮询
已启用	已启用	已轮询	已轮询
已禁用	已禁用	未轮询	未轮询
已禁用	已启用	未轮询	已轮询

下表显示由 APA 针对 SNMP 代理和 ICMP 响应而确定的 SNMP 代理状态的更改。

确定 SNMP 代理状态

SNMP 代理响应	管理地址 ICMP 响应	SNMP 代理状态
响应	响应	正常
响应	未响应	轻微
未响应	响应	严重
未响应	未响应	严重

启用管理地址 ICMP 轮询的情况下，APA 现在会在生成结论和事件时考虑管理地址 ICMP 响应和 SNMP 代理响应。

发现和静态 NAT

NNMi 管理员必须创建租户定义来标识网络管理环境中的每个静态 NAT 域。

螺旋发现需要发现种子(租户/IP 地址对)来标识 NAT 域中的每个节点。NNMi 管理员必须为静态 NAT 域中的每个节点创建发现种子。发现种子必须为每个节点提供以下信息：

- 外部 IP 地址(来自外部/内部 IP 地址对的公用地址)
- 租户名称

有关详细信息，请参阅 NNMi 帮助。

备注: 在静态 NAT 环境中添加发现种子(使用 `nnmloadseeds.ovpl` 命令或 NNMi 控制台)时，请确保使用节点的外部(公用)IP 地址。有关详细信息，请参阅 nnmloadseeds.ovpl 参考页或 Linux 联机帮助页。

提示: 最佳实践是不使用重复的域名系统 (DNS) 名称。

监视静态 NAT 的配置

根据网络环境，NNMi 管理员可以选择使用 ICMP 故障监视设置(另请参阅 NNMi 状况和状态计算 (第 346 页))：

- **监视配置 > 节点设置**选项卡，用于配置节点组监视。在“ICMP 故障监视”部分中，进行选择(有关详细信息，请参阅 NNMi 联机帮助)：
  - 管理地址轮询(默认启用并强烈推荐)
  - IP 地址故障轮询(可选)
- **监视配置 > 默认设置**选项卡。在“ICMP 故障监视”部分中，进行选择(有关详细信息，请参阅 NNMi 联机帮助)：

> **备注:** 如果网络环境中还包含任何动态 NAT 域，则默认设置可能不适用，因为您可能希望静态 NAT 域的设置与动态 NAT 域的设置不同。

陷阱和静态 NAT

必须更改 NNMi 管理服务器的被管节点才能从 NAT 网关后的节点接收 SNMP 陷阱。本部分介绍两种类型的 SNMP 陷阱：SNMPv2c 和 SNMPv1。

请注意，NNMi 必须明确解析其接收的每个陷阱的源地址。

SNMPv2c 陷阱

下表显示 SNMPv2c 陷阱的格式，其中 IP 报头形成表的上半部分，SNMP 陷阱协议数据单元 (PDU) 形成表的下半部分。

SNMPv2c 陷阱格式

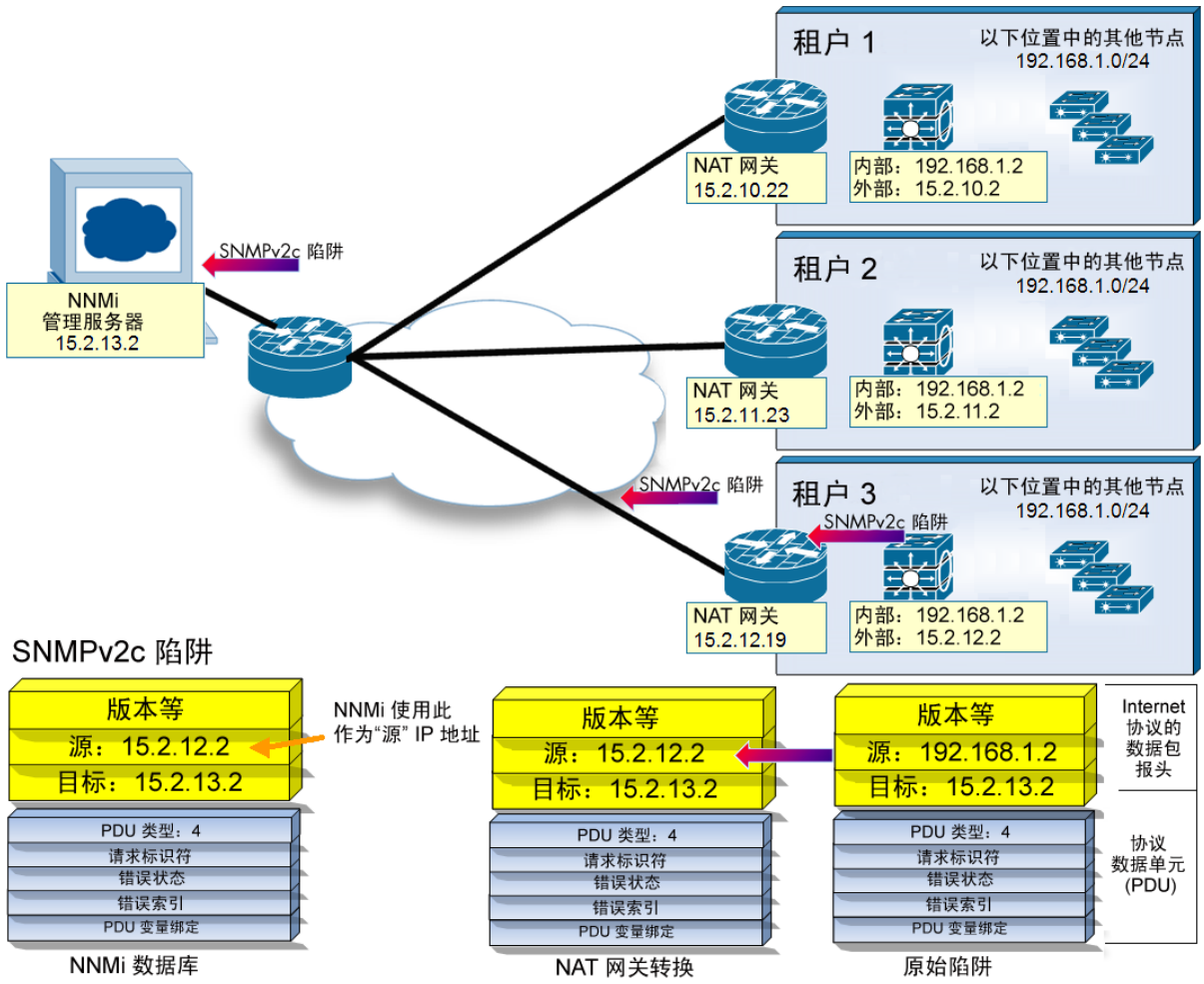
版本及其他信息
源地址
目标地址
PDU 类型：4
请求标识符
错误状态
错误索引
PDU 变量绑定

SNMPv2c 陷阱在 PDU 中没有“代理地址”字段；因此，该陷阱的唯一源字段位于 IP 包报头中。NAT 路由器会正确转换源字段。

在源节点上，确保与内部专用 IP 地址关联的接口作为 NAT 路由器后的设备的所有陷阱源。然后，NAT 网关可以将陷阱转换为正确的公用地址。

下图显示 NAT 网关的正确转换示例。NAT 网关将以源地址 192.168.1.2 开头的陷阱正确转换为地址 15.2.13.2。然后，NNMi 管理服务器正确解析此地址。

SNMPv2c 示例



SNMPv1 陷阱

SNMPv1 陷阱将代理地址嵌入 SNMP 陷阱 PDU。下表显示 SNMPv1 陷阱的格式，其中 IP 报头形成上半部分，SNMP 陷阱 PDU 形成下半部分。

SNMPv1 陷阱格式

版本及其他信息
源地址
目标地址
PDU 类型：4
企业
代理地址
通用陷阱代码

版本及其他信息
源地址
目标地址
特定陷阱代码
时间戳
PDU 变量绑定

由于代理地址是嵌入 PDU 中而非报头中，因此，NAT 路由器通常不会转换此值。您可以允许 NNMi 记录报头中的地址并忽略负载中的代理地址，方法是执行以下操作：

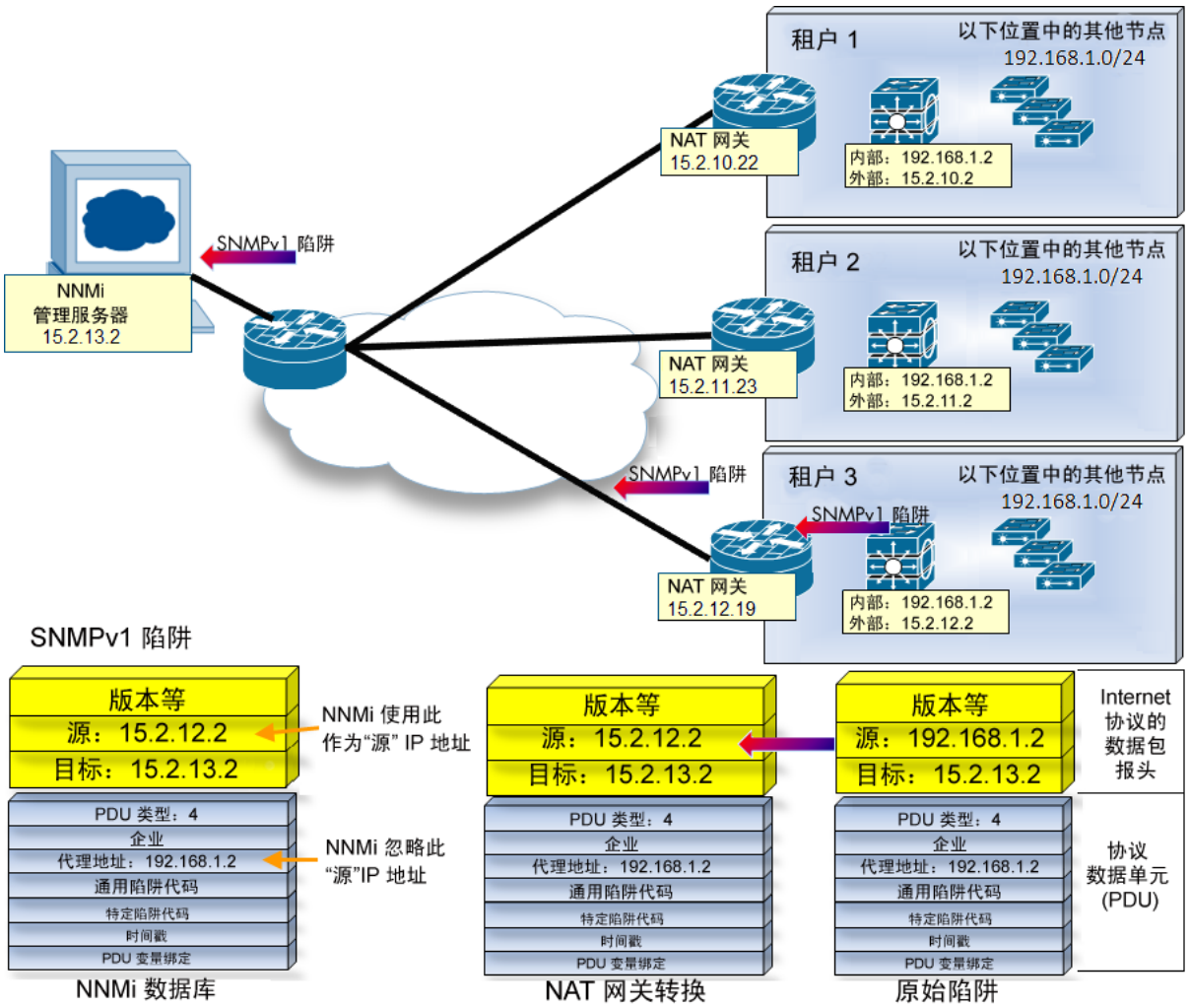
1. 编辑以下文件：
   - Windows：`%NNM_PROPS%\nms-jboss.properties`
   - UNIX：`$NNM_PROPS/nms-jboss.properties`
2. 找到以下行

   ```
   #!com.hp.nnm.trapd.useUdpHeaderIpAddress=false
   ```
3. 将该值更改为 **true** 并删除 **#!** 字符，如下所示：

   ```
   com.hp.nnm.trapd.useUdpHeaderIpAddress=true
   ```
4. 保存文件；然后重新启动 NNMi。

下图显示 NNMi 忽略冲突 IP 地址字段的 SNMPv1 陷阱示例。

SNMPv1 示例



备注: NNMi 提供以下相关的自定义事件属性 (CIA):

- cia.agentAddress - 生成陷阱的 SNMP 代理的 SNMPv1 陷阱数据中存储的 IP 地址。
- cia.internalAddress - 如果静态 NAT 是网络管理域的一部分，则 NNMi 管理员可以将此属性配置为显示映射到所选事件源节点的外部管理地址的内部 IP 地址。

  必须使用重叠 IP 地址映射表单将外部管理 IP 地址(公用地址)映射到此内部地址(专用地址)。有关详细信息，请参阅 NNMi 帮助。

子网和静态 NAT

请注意以下有关子网和 NAT 的事项：

- 子网是特定于租户的(也就是说，子网不跨租户)。其优势在于您可以对不同租户使用相同子网。
- 子网筛选使用租户和地址对。

- 如果您配置了一个子网连接规则，则该规则应用于所有租户。子网的成员在所有租户中必须唯一(每个节点仅分配到一个租户)。子网连接规则可以在默认租户和另一个租户之间建立链接。不过其中一个租户必须是默认租户，否则两个租户之间的链接是不被允许的。

全局网络管理：静态 NAT 的可选项

管理静态 NAT 域时，NNMi 全局网络管理功能是可选的。管理任意数量的静态 NAT 域只需要一台 NNMi 管理服务器。

如果使用全局管理器和区域管理器，则每个区域管理器必须存在至少一个静态或可路由(非转换)地址。这使 NNMi 管理服务器能够彼此通信，保持通信的专用性和安全。有关全局网络管理的详细信息，请参阅全局网络管理 (第 366 页)。

动态 NAT 和 PAT 注意事项

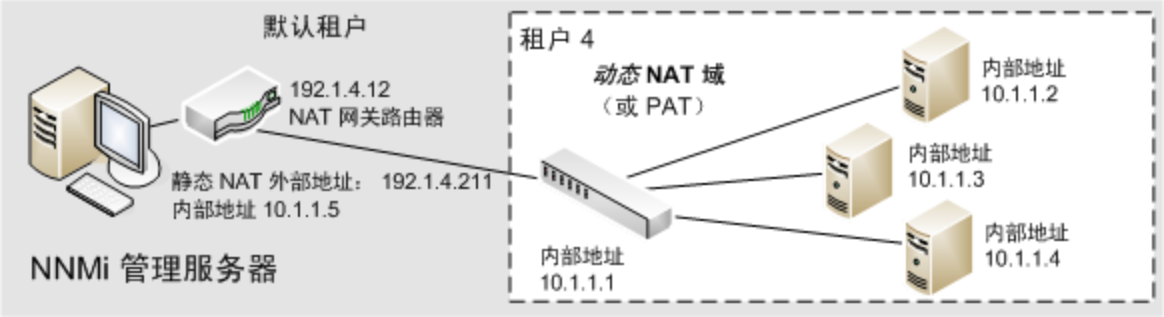
每个动态 NAT 或 PAT 域都需要自己的 NNMi 管理服务器。NNMi 管理服务器必须作为区域管理器参与全局网络管理环境。

NNMi 管理员创建租户定义来标识每个 NAT 域。租户在整个 NNMi 全局网络管理配置中必须唯一。

请参阅动态 NAT 配置的以下两个示例。

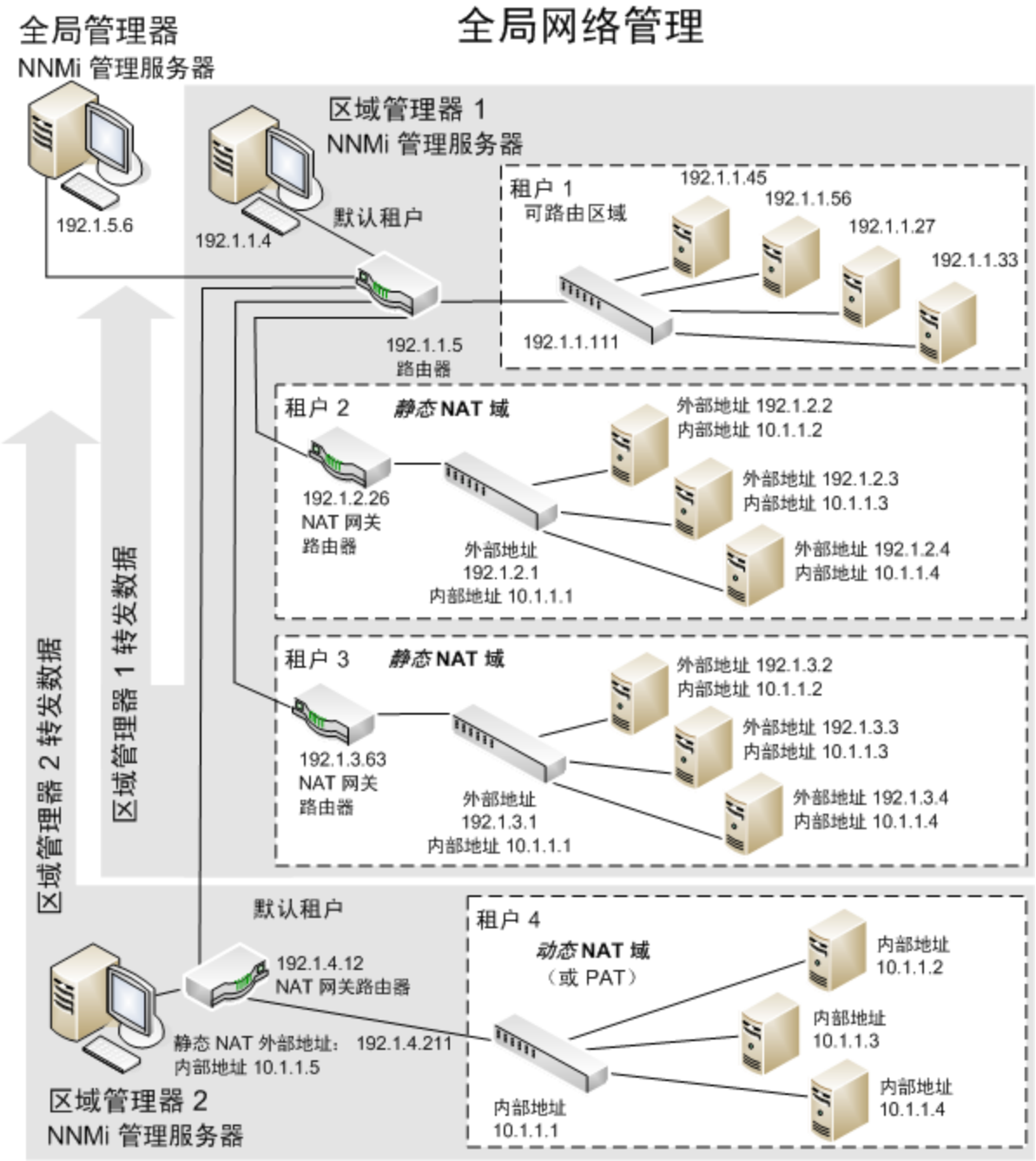
备注: 如果区域管理器位于 NAT 防火墙后面，则它的外部(公用)地址必须是静态的。

动态 NAT 配置示例



有关 NAT 环境中的全局网络管理配置示例，请参阅下图。

NAT 环境中的全局网络管理配置示例



属于默认租户的设备可以与任意租户中的任意设备具有第 2 层连接。默认租户以外的任何租户中的设备只能与同一租户或默认租户中的设备具有第 2 层连接。

提示: 将互连多个 NAT 域(比如 NAT 网关)的任何基础设备分配至默认租户。这可确保 NNMi 显示您的工作组(和客户)需要看到的第 2 层连接。

备注: 默认安全组中的设备可从所有视图中查看。要控制对设备的访问，请将该设备分配至

默认安全组以外的安全组。

有关全局网络管理的详细信息，请参阅全局网络管理 (第 366 页)。有关配置租户的信息，请参阅 NNMi 帮助中的“配置租户”。

硬件和软件要求以及动态 NAT 和 PAT

NNMi Advanced、NNMi Premium 或 NNMi Ultimate 软件是动态 NAT 和 PAT 环境所必需的。

NNMi 区域管理器是配置了动态 NAT 或 PAT 的每个地址域所必需的。

发现动态 NAT 和 PAT 的配置

NNMi 管理员必须创建租户定义以标识网络管理环境中的每个动态 NAT 域。这些租户名称在整个 NNMi 全局网络管理配置中必须唯一。

螺旋发现需要发现种子(租户/ IP 地址对)来标识 NAT 域中的每个节点。NNMi 管理员必须为动态 NAT 域中的每个节点创建发现种子。发现种子必须为每个节点提供以下信息：

- 内部 IP 地址(来自外部地址/内部地址对的公用地址)
- 租户名称

备注: 在动态 NAT 或 PAT 环境添加发现种子(使用 `nnmloadseeds.ovpl` 命令或图形用户界面)时，请确保使用节点的内部 IP 地址。

有关详细信息，请参阅 nnmloadseeds.ovpl 参考页、Linux 联机帮助页或 NNMi 帮助。

监视动态 NAT 的配置

根据网络环境，NNMi 管理员可以选择使用 ICMP 故障监视设置(另请参阅NNMi 状况和状态计算 (第 346 页))：

- **监视配置 > 节点设置**选项卡，用于配置节点组监视。在“ICMP 故障监视”部分中，进行选择(有关详细信息，请参阅 NNMi 联机帮助)：
  - 管理地址轮询(默认启用并强烈推荐)
  - IP 地址故障轮询(可选)
- **监视配置 > 默认设置**选项卡。在“ICMP 故障监视”部分中，进行选择(有关详细信息，请参阅 NNMi 联机帮助)：

备注: 如果网络环境中还包含任何静态 NAT 域，则默认设置可能不适用，因为您可能希望静态 NAT 域的设置与动态 NAT 域的设置不同。

子网以及动态 NAT 和 PAT

使用动态 NAT 或 PAT 环境中的子网时，请注意以下事项：

- 子网是特定于租户的(也就是说，子网不跨租户)。

  提示: 您可以对不同租户使用相同子网。

- 子网筛选使用租户/地址对。
- 如果您配置了一个子网连接规则，则该规则应用于所有租户。子网的成员在所有租户中必须唯一(每个节点仅分配到一个租户)。子网连接规则可以在默认租户和另一个租户之间建立链接。不过其中一个租户必须是默认租户，否则两个租户之间的链接是不被允许的。

全局网络管理：动态 NAT 和 PAT 的必需项

管理动态 NAT 域时，NNMi 全局网络管理功能是必需的。每个动态 NAT 或 PAT 域都需要自己的 NNMi 区域管理器。

每个 NNMi 区域管理器必须存在至少一个静态或可路由(非转换)地址。这使 NNMi 管理服务器能够彼此通信，保持通信的专用性和安全。

备注: 如果区域管理器位于 NAT 防火墙后面，则它的外部地址必须是静态的。

有关全局网络管理的详细信息，请参阅全局网络管理 (第 366 页)。另请参阅 NNMi 帮助中的“全局网络管理的租户最佳实践”。

在网络地址转换 (NAT) 环境中部署 NNMi

执行以下步骤在 NAT 环境中部署 NNMi：

1. 标识并创建网络管理环境中每个 NAT 域的列表。
2. 确定每个 NAT 域中使用的受支持 NAT 类型。
3. 按要求部署与每个 NAT 域有关(在 NAT 域的内部 IP 地址空间之内或之外)的每个 NNMi 管理服务器。请参阅特殊注意事项：

   静态 NAT 注意事项 (第 333 页)

   动态 NAT 和 PAT 注意事项 (第 341 页)
4. 使用 NNMi **配置** > **发现** > **租户**工作区可定义每个 NAT 域中唯一的租户名称。

   备注: 如果在您的部署中使用全局网络管理，则此名称在所有 NNMi 管理服务器(区域管理器和全局管理器)间必须唯一。

5. 确定每个 NAT 域中 NNMi 需要监视的节点。
6. 仅适用于静态 NAT 域：创建任意重叠地址映射以标识分配给每个节点的 NAT 外部/内部 IP 地址对。有关创建重叠地址映射的好处，请参阅重叠 IP 地址映射 (第 334 页)。

   提供以下信息：

   - 租户名称
   - 外部 IP 地址
   - 内部 IP 地址

使用 NNMi **配置 > 发现 > 重叠地址映射**工作区或 `nnmloadipmappings.ovpl` 命令行工具。

有关详细信息，请参阅 NNMi 联机帮助。

7. NNMi 使用节点的内部地址时，防火墙可能会阻止 NNMi 与 NAT 域中的节点通信，具体取决于 NNMi 管理服务器在网络环境中的部署位置。因此，对于**配置 > 通信配置**设置，使用相应的首选管理地址设置(NAT 的外部或内部 IP 地址)。
8. 验证网络环境中 NAT 的监视配置设置：
   - 监视静态 NAT 的配置 (第 336 页)
   - 监视动态 NAT 的配置 (第 343 页)

     如果需要有关监视配置的详细信息，请参阅 NNMi 联机帮助。
9. 为每个节点配置发现种子。

   备注: 将互连多个 NAT 域(比如 NAT 网关路由器)的任何基础设备分配给默认租户。

   使用 NNMi **配置 > 发现 > 种子**工作区或 `loadseeds.ovpl` 命令行工具：
   - 如果 NNMi 管理服务器在内部 IP 地址空间内，则使用内部 IP 地址配置发现种子：
     - Hostname/IP(使用内部 IP 地址)
     - 租户名称
   - 如果 NNMi 管理服务器在内部 IP 地址空间外，则使用外部 IP 地址配置发现种子：
     - Hostname/IP(使用外部 IP 地址)
     - 租户名称

   有关详细信息，请参阅 NNMi 联机帮助。
10. 验证 NNMi 发现是否找到所需的节点。如果未发现，请再次检查您的配置(如上)。
11. 验证 NNMi 设置是否满足您团队的需求：
    - 微调每个节点的安全组分配，控制可在 NNMi 控制台中查看每个节点的团队成员/客户。使用 NNMi 的“配置 > 安全 > 安全组”工作区。
    - 检查应用到这些节点上的监视配置设置并根据需要进行微调。使用 NNMi **配置 > 监视 > 监视配置**工作区。
12. 验证节点间的连接在 NNMi 图上是否按预期显示。如果不是：
    - 验证连接中涉及的两个节点是否分配了正确的租户(默认租户或其他租户)。
    - 验证**配置 > 发现配置的子网连接规则**选项卡设置是否正确。
    - 要强制 NNMi 添加非自动发现的连接，请使用 `nnmconnedit.ovpl` 命令行工具。有关详细信息，请参阅 NNMi 联机**帮助 > NNMi 文档库 > 参考页**。
13. 检查每个节点的 SNMP 代理中配置的 SNMP 陷阱转发规则，以包含相应 NNMi 管理服务器的 IP 地址。
14. 仅适用于静态 NAT 域：在每个静态 NAT 节点上配置 SNMP 代理，确保与 NNMi 重叠地址映射内部地址关联的接口作为发送到 NNMi 管理服务器的所有陷阱的源。
15. 如果网络环境包含 SNMPv1，则对 NNMi 配置进行必要的更改。请参阅陷阱和静态 NAT (第 337 页)。

NNMi 状况和状态计算

默认情况下，NNMi 自动启用对每个节点管理地址的 ICMP 轮询，包括 NAT 环境(**配置 > 监视 > 监视配置**、**默认设置**选项卡、**ICMP 故障监视**部分的**启用管理地址轮询**设置)中的那些节点。如果您具有 NAT 环境，则强烈建议您不要禁用此设置。

> **备注:** 在**库存 > SNMP 代理**视图中，选择一个 SNMP 代理并使用**操作 > 监视设置**命令。显示的信息表示 NNMi 是否启用了此管理地址轮询。

启用管理地址轮询后，“代理 ICMP 状况”字段会出现在以下位置：

- 节点表单
- SNMP 代理表单
- SNMP 代理表视图

下表显示了 NNMi 行为如何随 ICMP 故障监视设置发生变化。表中的第一行显示了 NNMi 默认设置。

监视配置设置和产生的状况轮询器行为

ICMP 故障监视设置		**产生的 NNMi 行为**	
启用管理地址轮询	启用 IP 地址故障轮询	代理 ICMP 状况	IP 地址状况
已启用	已禁用	已轮询	未轮询
已启用	已启用	已轮询	已轮询
已禁用	已禁用	未轮询	未轮询
已禁用	已启用	未轮询	已轮询

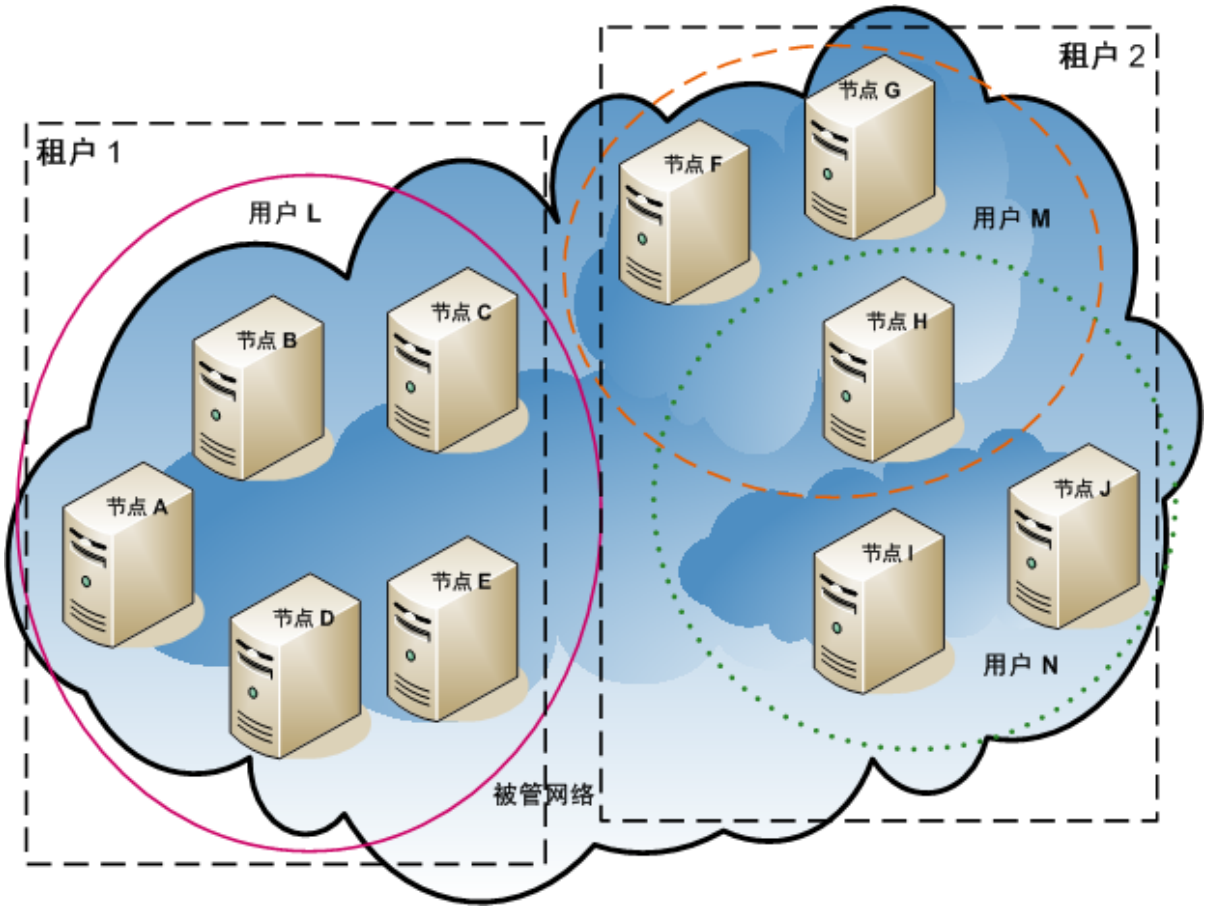
启用**管理地址轮询**后，NNMi 在计算结论和生成事件时会考虑管理地址的 ICMP 响应和 SNMP 代理的响应。

下表显示了由 ICMP 和 SNMP 响应组合确定的 SNMP 代理状态计算。

确定 SNMP 代理状态

SNMP 代理的响应	**管理地址的 ICMP 响应**	**产生的 SNMP 代理状态**
响应	响应	正常
响应	未响应	轻微
未响应	响应	严重
未响应	未响应	严重

NNMi 安全和多租户



备注: NNMi 使用租户支持包含重叠地址域的网络，这些域可能存在于网络管理域的静态网络地址转换 (NAT)、动态 NAT 或动态端口地址转换 (PAT) 区域内。如果您具有此类网络，请将重叠地址域放入不同的租户(使用播种发现完成此操作)。有关详细信息，请参阅管理 NAT 环境中的重叠 IP 地址 (第 331 页)和 NNMi 帮助。

默认情况下，所有 NNMi 控制台用户可以在 NNMi 数据库中查看所有对象的信息。如果环境可接受此默认配置，则无需阅读本章。

在 NNMi 中提供了安全和多租户，用于限制用户对 NNMi 数据库中对象信息的访问。对于自定义网络操作员能够查看的责任区域时，此限制很有用。它还通过 NNMi 的按组织配置支持服务提供程序。

本章描述 NNMi 安全和租户模型并提供配置建议。它包含以下主题：

- 限制对象访问的影响 (第 348 页)
- NNMi 安全模型 (第 349 页)
- NNMi 租户模型 (第 353 页)
- NNMi 安全和多租户配置 (第 356 页)
- NNMi 安全、多租户和全局网络管理 (GNM) (第 363 页)
- 在 NPS 报告中包含选择界面 (第 365 页)

另请参阅《HP Network Node Manager i Software Step-by-Step Guide to Using Security Groups White Paper》。

限制对象访问的影响

配置 NNMi 安全有以下影响：

- 拓扑库存对象：
  - 每个 NNMi 控制台用户只能查看与其 NNMi 用户帐户的配置匹配的节点。
  - 子节点对象(比如接口)从节点继承访问控制。
  - 节点间对象(比如连接)仅在 NNMi 控制台用户有权查看所涉及的至少一个节点时才可见。
  - NNMi 控制台用户只能查看其可以访问组中至少一个节点的节点组。
  - 对于 Network Performance Server (NPS) 报告，NNMi 管理员可以选择性地覆盖对接口的访问控制继承。有关详细信息，请参阅在 NPS 报告中包含选择界面 (第 365 页)。
- 图和路径视图：
  - 图显示 NNMi 控制台用户有权查看两个参与节点的连接。
  - 路径视图省略或显示为 NNMi 控制台用户无权访问其任意中间节点的云。
  - 对于 NNM iSPI for MPLS 和 NNM iSPI for IP Multicast，如果图和路径视图包含 NNMi 控制台用户无权访问的节点，则 NNM iSPI 仅显示节点的连接接口和名称。不可访问的节点的图标是白色的，表示这些节点的状态和详细信息不可用。
  - 对于 NNM iSPI for IP Telephony，如果图和路径视图包含 NNMi 控制台用户无权访问的节点，则 NNM iSPI 仅显示节点的连接接口和名称。不可访问的节点的图标显示 NNMi 状态，但所有尝试操作失败。
- 事件：
  - 对于其源节点在 NNMi 拓扑中的事件，NNMi 控制台用户只能查看该用户有权访问其源节点的事件。
  - 没有源节点的事件(如 NNMi 运行状况和许可管理事件)按组处理。NNMi 管理员确定哪些 NNMi 控制台用户可查看这些事件(通过将用户与“未解析事件”安全组关联)。
  - 由源节点不在 NNMi 拓扑中的陷阱产生的事件的处理方式与无源节点的事件的处理方式相同。如果 NNMi 配置为生成这些事件，则 NNMi 管理员将确定哪些 NNMi 控制台用户可查看这些事件(通过将用户与“未解析事件”安全组关联)。

  备注: 事件分配操作不检查用户访问。NNMi 管理员可能将事件分配给无权查看该事件的 NNMi 控制台用户。
- NNMi 控制台操作：

  - 对于无选择运行的操作，NNMi 控制台用户只能查看他们有权运行的操作。
  - 对于针对一个或多个选定对象运行的操作，NNMi 控制台用户必须具有选定对象的正确访问级别。根据安全配置，NNMi 控制台可能显示对 NNMi 控制台视图中的某些可见对象无效的操作。调用其中某个操作会产生关于此限制的错误消息。
  - 对于图视图和 NNM iSPI 表视图及表单，NNMi 无法区分未知节点和存在于 NNMi 拓扑中但当前用户无法访问的节点。
- MIB 浏览器和折线绘图器：
  - NNMi 控制台用户可查看其有权访问的节点的 MIB 数据和图。
  - NNMi 控制台用户可查看其了解的 SNMP 团体字符串的节点的 MIB 数据。
- NNMi 控制台 URL：

  用户必须先登录到 NNMi 才能从直接 URL 访问 NNMi 控制台视图。NNMi 根据 NNMi 安全配置强制限定该用户的访问权限，并相应地限制可用拓扑。

NNMi 安全模型

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

- 提供用于限制网络的 NNMi 控制台操作员视图的方式。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 NNMi 拓扑的访问。可以按节点配置操作员访问级别。
- 用于按安全组筛选节点(所有属性)视图和 Network Performance Server 报告。
- 简化了符合安全配置的节点组的配置和维护。
- 可以独立于 NNMi 租户模型单独使用。

NNMi 安全的可能用例如下：

- 使 NNMi 操作员能够侧重于站点内的设备类型(自定义图)。
- 使不同站点的 NNMi 操作员能够查看仅显示给定站点上的节点的视图(自定义图)。
- 部署期间的阶段节点。NNMi 管理员可以查看所有节点，而 NNMi 操作员只能查看部署的节点。
- 提供所有 NOC 操作员的完全访问，但限制 NOC 客户的访问。
- 提供中央 NOC 操作员对网络视图的完全访问，但限制区域 NOC 操作员对视图的访问。

安全组

在 NNMi 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。NNMi 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：

- 一个或多个以下预配置的 NNMi 用户组：
  - NNMi 管理员
  - NNMi 全局操作员

- NNMi 第 2 级操作员
- NNMi 第 1 级操作员
- NNMi 来宾用户

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

备注: NNMi Web 服务客户端用户组不授予访问 NNMi 控制台的权限；但是，它可以授予对所有 NNMi 对象的管理员级别访问权限。

备注: NNMi 全局操作员用户组 (globalops) 仅授予对拓扑对象的访问权限。一个用户必须分配到其他某个用户组(level2、level1 或 guest)后，才能访问 NNMi 控制台。

管理员不应将 globalops 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。

- 映射到安全组的零个或多个自定义用户组。

  这些映射提供对 NNMi 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。对象访问特权级别还适用于相关数据库对象，比如接口和事件。例如，对包含接口 X 和 Y 的节点 A 具有第 1 级操作员对象访问特权的用户对以下所有数据库对象都具有第 1 级操作员对象访问特权：

  - 节点 A
  - 接口 X 和 Y
  - 其源对象是节点 A、接口 X 或接口 Y 的事件

NNMi 提供以下安全组：

- 默认安全组

  在新 NNMi 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。NNMi 管理员可以配置哪些节点与默认安全组关联，以及哪些用户可以访问默认安全组中的对象。

- 未解析事件

  “未解析事件”安全组提供对 NNMi 从源节点不在 NNMi 拓扑中的已接收陷阱创建的事件的访问权限。默认情况下，所有用户都可以查看与“未解析事件”安全组关联的所有事件。NNMi 管理员可以配置哪些用户可以访问与“未解析事件”安全组关联的事件。

所有传感器都继承该节点的安全组分配。

备注: 以下最佳实践适用于 NNMi 安全配置：

- 将每个用户帐户只映射到一个预配置的 NNMi 用户组。
- 不要将预配置的 NNMi 用户组映射到安全组。
- 由于映射到 NNMi 管理员用户组的任何用户帐户可以对 NNMi 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。

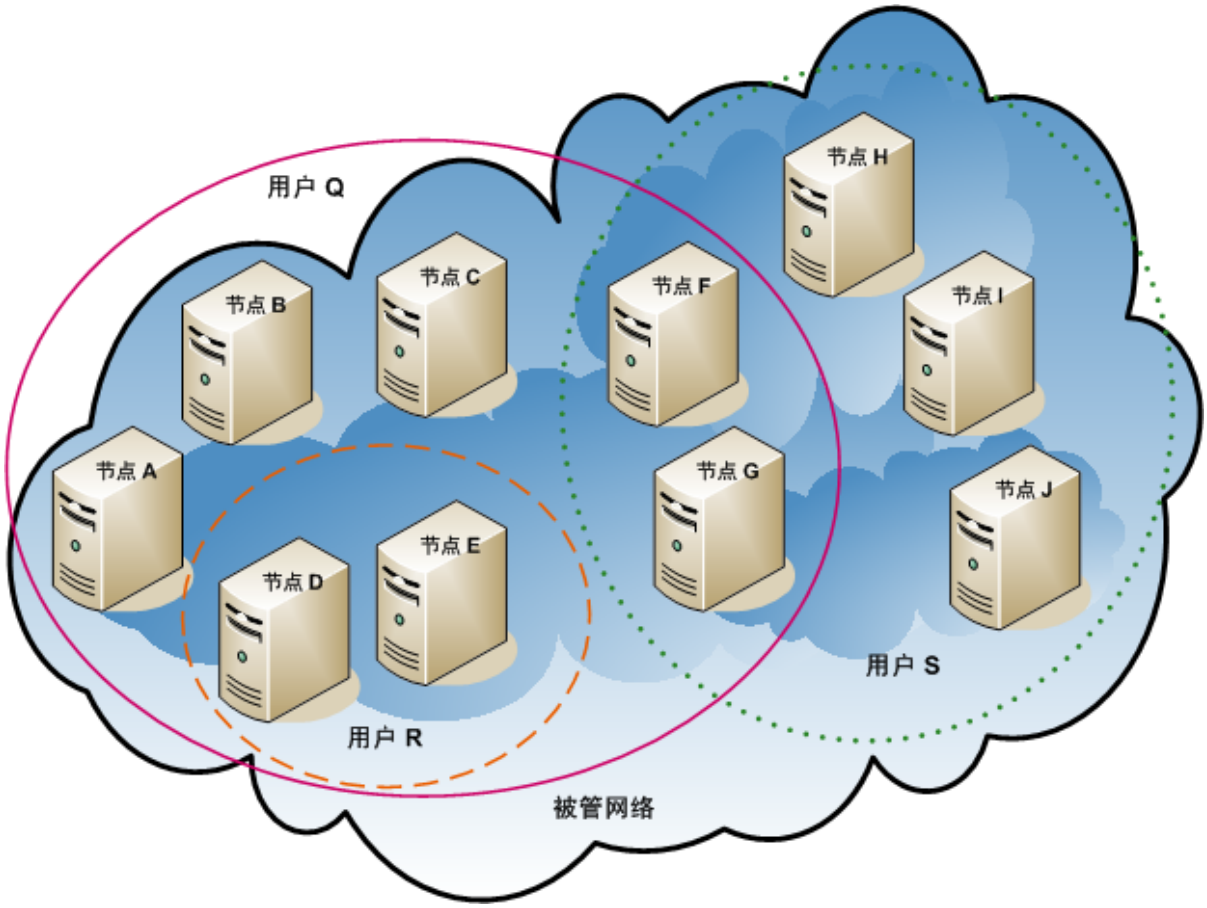
- 为 Web 服务客户端角色创建单独的用户帐户。由于此用户帐户有权访问整个 NNMi 拓扑，因此请将此用户帐户仅映射到 NNMi Web 服务客户端用户组。

安全组结构示例

下图中的三个椭圆表示用户需要查看此 NNMi 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安全组之间的映射，以及此拓扑可能的自定义用户组。(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	对象管理员
		UG1 级别 2	第 2 级操作员对象
		UG1 级别 1	第 1 级操作员对象
		UG1 来宾	对象来宾
SG2	D、E	UG2 管理员	对象管理员
		UG2 级别 2	第 2 级操作员对象
		UG2 级别 1	第 1 级操作员对象
		UG2 来宾	对象来宾
SG3	F、G	UG3 管理员	对象管理员
		UG3 级别 2	第 2 级操作员对象
		UG3 级别 1	第 1 级操作员对象
		UG3 来宾	对象来宾
SG4	H、I、J	UG4 管理员	对象管理员
		UG4 级别 2	第 2 级操作员对象
		UG4 级别 1	第 1 级操作员对象
		UG4 来宾	对象来宾

用户帐户映射示例

用户帐户	用户组	节点访问	备注
用户 Q	NNMi 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 级操作员访问权限。
	UG1 级别 2	A、B、C	
	UG2 级别 2	D、E	
	UG3 级别 2	F、G	
用户 R	NNMi 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 级操作员访问权限。
	UG2 级别 1	D、E	
用户 S	NNMi 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 级操作员访问权限。
	UG3 级别 2	F、G	
	UG4 级别 2	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	NNMi 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限(特权级别可以变化)。 此用户具有对节点 D 和 E 的管理访问权限，但看不到需要管理访问权限的工具的菜单项。如果此用户有权访问 NNMi 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限的命令行工具。
	UG1 来宾	A、B、C	
	UG2 管理员	D、E	
	UG3 级别 2	F、G	
	UG4 级别 1	H、I、J	

NNMi 租户模型

NNMi 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。NNMi 租户模型具有以下好处：

- 标记每个节点属于的组织。
- 用于按租户和安全组筛选节点(所有属性)库存视图和 Network Performance Server 报告。
- 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 NNMi 安全配置。
- 用于在使用地址转换协议时管理重叠地址域。

使用 NNMi 多租户为具有多个从相同 NNMi 管理服务器管理的客户(租户)的服务提供程序提供不同的客户视图。

备注: 一台 NNMi 管理服务器可以监视任意数量的静态网络地址转换 (NAT) 实例，只要每个实例均配置有唯一租户即可。有关详细信息，请参阅管理 NAT 环境中的重叠 IP 地址 (第 331 页)和 NNMi 帮助。

租户

NNMi 租户模型在安全配置中引入了组织的理念。NNMi 拓扑中的每个节点仅属于一个租户。租户提供 NNMi 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 NNMi 数据库时，进行初始发现租户分配。对于种子节点，可以指定分配到每个节点的租户。NNMi 将所有其他发现的节点(包含在自动发现规则中但不直接播种的节点)分配给默认租户。NNMi 管理员可以在发现后随时更改节点的租户。

每个租户定义都包括初始发现安全组。NNMi 将此初始发现安全组和初始发现租户一起分配给节点。NNMi 管理员可以在发现后随时更改节点的安全组。

提示: 更改节点的租户分配不会自动更改安全组分配。

NNMi 提供默认租户。默认情况下，所有 NNMi 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。

所有传感器都继承节点的租户和安全组分配。

备注: 以下最佳实践适用于 NNMi 租户配置：

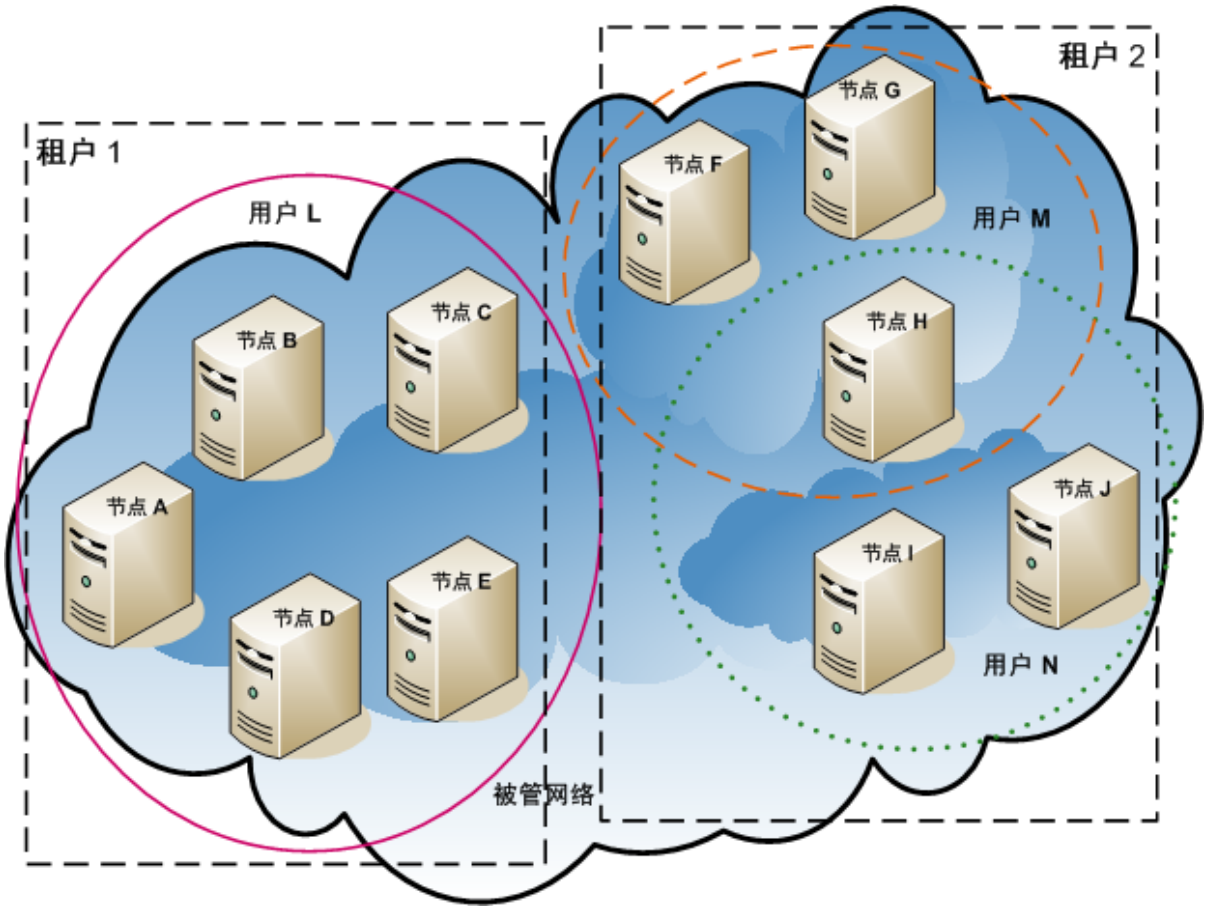
- 对于小型组织，每个租户一个安全组可能已足够。
- 可能希望将大组织细分为多个安全组。
- 要防止用户跨组织访问节点，请确保每个安全组仅包含一个租户的节点。

租户结构示例

下图显示了包含两个租户(以矩形表示)的 NNMi 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安全组之间的映射，以及此拓扑可能的自定义用户组。(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	对象管理员
		T1 级别 2	第 2 级操作员对象
		T1 级别 1	第 1 级操作员对象
		T1 来宾	对象来宾
T2 SGa	F、G	T2_a 管理员	对象管理员
		T2_a 级别 2	第 2 级操作员对象
		T2_a 级别 1	第 1 级操作员对象
		T2_a 来宾	对象来宾

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	对象管理员
		T2_b 级别 2	第 2 级操作员对象
		T2_b 级别 1	第 1 级操作员对象
		T2_b 来宾	对象来宾
T2 SGc	I、J	T2_c 管理员	对象管理员
		T2_c 级别 2	第 2 级操作员对象
		T2_c 级别 1	第 1 级操作员对象
		T2_c 来宾	对象来宾

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	NNMi 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 级操作员访问权限，此椭圆将所有节点分组为租户 1。
	T1 级别 2	A、B、C、D、E	
用户 M	NNMi 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 级操作员访问权限，此椭圆将一部分节点分组为租户 2。
	T2_a 级别 1	F、G	
	T2_b 级别 1	H	
用户 N	NNMi 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 级操作员访问权限，此椭圆将一部分节点分组为租户 2。
	T2_b 级别 2	H	
	T2_c 级别 2	I、J	

NNMi 安全和多租户配置

备注: 一台 NNMi 管理服务器可以监视任意数量的静态网络地址转换 (NAT) 实例，只要每个实例均配置有唯一租户即可。有关详细信息，请参阅管理 NAT 环境中的重叠 IP 地址 (第 331 页)和 NNMi 帮助。

NNMi 安全和多租户配置应用于整个 NNMi 数据库。任何 NNMi 管理员都可以查看和配置对所有租户的所有对象的操作员访问权限。

在 NNMi 管理员定义了至少一个自定义安全组之后，**安全组**字段将显示在所有**节点**表单上，并在**节点**和**节点 (所有属性)** 库存视图中显示为一列。

在 NNMi 管理员定义了至少一个自定义租户之后，**租户**字段将显示在所有**节点**表单上，并在**节点**和**节点 (所有属性)**库存视图中显示为一列。

节点组

要创建符合部分安全或多租户配置的节点组，请根据安全组 UUID、安全组名称、租户 UUID 或租户名称指定节点组其他筛选。使用这些节点组可为监视和事件生命周期转换操作配置按安全组或按租户轮询周期。

> **提示:** 由于安全组和租户名称可以更改，请在其他筛选中指定安全组或租户 UUID。此信息可在配置表单上和 `nnmsecurity.ovpl` 命令输出中获取。

用户组：NNMi 控制台访问

映射到一个预定义 NNMi 用户组的用户帐户可设置 NNMi 角色及 NNMi 控制台中菜单项的可见性。建议授予每个用户帐户与该用户的拓扑对象的最高对象访问特权匹配的 NNMi 角色。

> **备注:** 此建议的例外情况是管理级别，因为 NNMi 管理员可以访问所有拓扑对象。要将某个 NNMi 控制台用户仅配置为 NNMi 拓扑中某些节点的管理员，请将该用户分配到 NNMi 第 2 级操作员或 NNMi 第 1 级操作员用户组。(第 1 级操作员的访问特权低于第 2 级操作员。)另将该用户分配到自定义用户组，该用户组将对象管理员对象访问特权映射到包含拓扑中一部分节点的安全组。

用户组：目录服务

如果在 NNMi 数据库中存储用户组成员资格，则 NNMi 配置区域中的所有对象访问配置通过用户组、用户帐户映射、安全组和安全组映射发生。

如果在目录服务中存储用户组成员资格，请在 NNMi 配置(安全组和安全组映射)与目录服务内容(用户组成员资格)之间共享对象访问配置。不要在 NNMi 数据库中创建用户帐户或用户帐户映射。对于目录服务中的每个适用组，在 NNMi 数据库中创建一个或多个用户组。在 NNMi 中，将每个用户组定义的**目录服务名称**字段设置为目录服务中该组的可分辨名称。

有关详细信息，请参阅通过 LDAP 将 NNMi 与目录服务集成 (第 305 页)。

配置工具

NNMi 提供几个工具来配置多租户和安全。

安全向导

NNMi 控制台中的**安全向导**可用于可视化安全配置。最简单的方法是将节点分配到 NNMi 控制台中的安全组。**查看更改摘要**页将显示当前向导会话中未保存更改的列表。它还表示安全配置的潜在问题。

> **备注:** **安全向导**仅适用于 NNMi 安全配置。它不包括租户信息。

有关使用**安全向导**的信息，请单击向导中的 NNMi 帮助链接。

NNMi 控制台表单

NNMi 控制台中的各个安全和多租户对象的表单可用于一次集中配置的一个方面。有关使用这些表单的信息，请参阅每个表单的 NNMi 帮助。

租户视图包含 NNMi 多租户配置信息。此视图位于**配置**工作区中的**发现**下。每个**租户**表单描述一个 NNMi 租户，并显示当前分配给该租户的节点。节点分配信息是只读的。

要更改节点的租户或安全组分配，请使用**节点**表单或 `nnmsecurity.ovpl` 命令。

在**配置**工作区的**安全**下面可访问以下 NNMi 控制台视图。这些视图包含 NNMi 安全配置信息：

- **用户帐户**
  - 每个**用户帐户**表单描述一个 NNMi 用户，并显示该用户所属的用户组。成员资格信息是只读的。
  - 如果在目录服务中存储用户组成员资格，则用户帐户在 NNMi 控制台中不可见。
- **用户组**

  每个**用户组**表单描述一个 NNMi 用户组，并显示映射到该用户组的用户帐户和安全组。映射信息是只读的。
- **用户帐户映射**
  - 每个**用户帐户映射**表单显示一个用户帐户到用户组的关联。
  - 用户帐户映射的更改不影响当前 NNMi 控制台用户。这些用户将在其下次登录到 NNMi 控制台时接收所有更改。
  - 如果在目录服务中存储用户组成员资格，则用户帐户映射在 NNMi 控制台中不可见。
- **安全组**

  每个**安全组**表单描述一个 NNMi 安全组，并显示当前分配给该安全组的节点。节点分配信息是只读的。
- **安全组映射**
  - 每个**安全组映射**表单显示一个用户组到安全组的关联。
  - 初始配置后，与安全组映射关联的对象访问特权为只读。要更改安全组映射的对象访问特权，请删除该映射并重新创建它。

命令行

`nnmsecurity.ovpl` 命令行界面可用于自动化和批量操作。该工具还提供安全配置的潜在问题报告。

很多 `nnmsecurity.ovpl` 选项支持从逗号分隔值 (CSV) 文件加载输入数据。可在可生成 CSV 输出的文件或系统中维护配置数据，供 `nnmsecurity.ovpl` 命令使用。该命令还可以接受在 NNMi 以外生成的 UUID。

> **提示:** 由于安全组和租户名称不需要唯一，可将安全组或租户 UUID 指定为 `nnmsecurity.ovpl` 命令的输入。

以下示例脚本使用 `nnmsecurity.ovpl` 命令创建两个用户帐户和五个节点的安全配置。

```
#!/bin/sh

# create two users

nnmsecurity.ovpl -createUserAccount -u user1 -p password -role level1

nnmsecurity.ovpl -createUserAccount -u user2 -p password -role level2
```

```
# create two user groups
nnmsecurity.ovpl -createUserGroup local1
nnmsecurity.ovpl -createUserGroup local2
# assign the user accounts to the new user groups
nnmsecurity.ovpl -assignUserToGroup -user user1 -userGroup local1
nnmsecurity.ovpl -assignUserToGroup -user user2 -userGroup local2
# create two security groups
nnmsecurity.ovpl -createSecurityGroup secgroup1
nnmsecurity.ovpl -createSecurityGroup secgroup2
# assign the new user groups to the new security groups
nnmsecurity.ovpl -assignUserGroupToSecurityGroup -userGroup local1
  -securityGroup secgroup1 -role level1
nnmsecurity.ovpl -assignUserGroupToSecurityGroup -userGroup local2
  -securityGroup secgroup2 -role level2
# assign nodes to security groups
nnmsecurity.ovpl -assignNodeToSecurityGroup -node mplspe01 -securityGroup secgroup1
nnmsecurity.ovpl -assignNodeToSecurityGroup -node vwan_router-1 -securityGroup secgroup1
nnmsecurity.ovpl -assignNodeToSecurityGroup -node vwan_router-2 -securityGroup secgroup1
nnmsecurity.ovpl -assignNodeToSecurityGroup -node data_center_1 -securityGroup secgroup2
nnmsecurity.ovpl -assignNodeToSecurityGroup -node mplspe03 -securityGroup secgroup2
```

配置租户

备注: 一台 NNMi 管理服务器可以监视任意数量的静态网络地址转换 (NAT) 实例，只要每个实例均配置有唯一租户即可。有关详细信息，请参阅管理 NAT 环境中的重叠 IP 地址 (第 331 页)和 NNMi 帮助。

NNMi 提供以下方式配置多租户：

- NNMi 控制台中的**租户**表单可用于处理各个租户。
- `nnmsecurity.ovpl` 命令行界面可用于自动化和批量操作。该工具还提供租户配置的潜在问题报告。

定义和配置 NNMi 多租户以将每个 NNMi 拓扑对象分配给租户(组织)是一个周期性过程。此高级别过程描述了一个配置 NNMi 多租户的方法。

请注意以下有关配置 NNMi 多租户的事项：

- NNMi 分配到发现的节点的安全组由与该节点关联的租户的初始发现安全组的值设置 。
- 使用 NNMi 安全模型而不配置 NNMi 租户时，所有节点分配给默认租户。
- 当您播种节点进行 NNMi 发现时，可以指定该节点所属的租户。NNMi 通过自动发现规则发现节点时，NNMi 将该节点分配到默认租户。发现之后，可以更改该节点的租户分配。

计划和配置 NNMi 多租户的一个高级别方法如下：

1. 分析客户需求以确定在 NNMi 环境中需要多少租户。

   建议仅当使用单个 NNMi 管理服务器管理多个单独网络时使用租户。
2. 分析被管网络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 NNMi 用户需要访问的节点组。
4. 删除预定义 NNMi 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限。此时，仅 NNMi 管理员可以访问 NNMi 拓扑中的对象。
5. 配置识别的租户。
   a. 创建识别的安全组。
   b. 创建识别的租户。

      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限的租户特定安全组。此方法确保租户的新节点在一般情况下不可见，除非 NNMi 管理员配置了访问权限。
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：
   - 验证每个节点的租户，并根据需要进行更改。
   - 验证每个节点的安全组，并根据需要进行更改。

   请参阅验证配置 (第 361 页)。

配置安全组

提示: 如果计划将 NNMi 与目录服务集成用于合并用户名、密码和 NNMi 用户组分配(可选)的存储，请在配置 NNMi 安全之前完成该配置。

NNMi 提供以下方式配置安全：

- NNMi 控制台中的**安全向导**可用于可视化安全配置。**查看更改摘要**页将显示当前向导会话中未保存更改的列表。它还表示安全配置的潜在问题。
- NNMi 控制台中的各个安全对象的表单可用于一次集中安全配置的一个方面。
- `nnmsecurity.ovpl` 命令行界面可用于自动化和批量操作。该工具还提供安全配置的潜在问题报告。

定义和配置 NNMi 安全以限制用户对 NNMi 拓扑中对象的访问权限是一个周期性过程。此高级别过程描述了一个配置 NNMi 安全的方法。

提示: 此示例从安全组移到用户帐户。对于配置从用户帐户到安全组的 NNMi 安全的示例，请在 NNMi 帮助中搜索“配置安全示例”。

请注意以下有关配置 NNMi 安全的事项：

- NNMi 分配到发现的节点的安全组由与该节点关联的租户的初始发现安全组的值设置。
- 使用 NNMi 安全模型而不配置 NNMi 租户时，所有节点分配给默认租户。

计划和配置 NNMi 安全的一个高级别方法如下：

1. 分析被管网络拓扑以确定 NNMi 用户需要访问的节点组。
2. 删除预定义 NNMi 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限。此时，仅 NNMi 管理员可以访问 NNMi 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 NNMi 用户访问权限的每个级别配置用户组。
      - 如果在 NNMi 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 NNMi 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 NNMi 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 NNMi 控制台。)
     - 将每个用户帐户映射到一个预定义 NNMi 用户组(用于访问 NNMi 控制台)。
     - 将每个用户帐户映射到一个或多个自定义 NNMi 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预定义 NNMi 用户组和一个或多个自定义用户组。
6. 按验证配置 (第 361 页)中所述验证配置。
7. 维护安全配置。
   - 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 NNMi 控制台用户添加到正确的用户组。

验证配置

要验证安全配置是否正确，请单独验证配置的每个方面。本部分描述验证配置的某些方法。也可以使用其他方法。

> **备注:** NNMi 提供可能的安全配置错误报告。使用 NNMi 控制台中的**工具 > 安全报告**和带 `-displayConfigReport` 选项的 `nnmsecurity.ovpl` 命令访问这些报告。

验证安全组到节点的分配

验证每个节点是否被分配到正确安全组的一个方法是按安全组对**节点**或**节点 (所有属性)**库存视图排序，然后检查分组。

另一个方法是使用带 `-listNodesInSecurityGroup` 选项的 `nnmsecurity.ovpl` 命令。

验证用户组到安全组的分配

验证哪些用户组映射到每个安全组的一个方法是按用户组或安全组排序**安全组映射**视图，然后检查分组。还要验证每个映射的对象访问特权。

另外，在**安全向导**的**映射用户组和安全组**页上，每次选择一个用户组或安全组，以查看该对象的当前映射。

另一个方法是使用带 `-listUserGroupsForSecurityGroup` 选项的 `nnmsecurity.ovpl` 命令。

验证每个用户是否都有 NNMi 控制台访问权限

对于 NNMi 控制台访问，确保将每个用户分配到一个预定义 NNMi 用户组(从最高到最低列出)：

- NNMi 管理员
- NNMi 第 2 级操作员
- NNMi 第 1 级操作员
- NNMi 来宾用户

所有其他用户组分配提供对 NNMi 数据库中对象的访问。

> **备注:** NNMi 全局操作员用户组仅提供对拓扑对象的访问。除非 `globalops` 用户也与具有 NNMi 控制台访问权限的用户组(如 `level2`、`level1` 或 `guest`)关联，否则该用户无法访问 NNMi 控制台。

安全向导的**查看更改摘要**页上列出了没有 NNMi 控制台访问权限的用户。**工具 > 安全报告**菜单项和带 `-displayConfigReport usersWithoutRoles` 选项的 `nnmsecurity.ovpl` 命令也提供此信息。

> **备注:** NNMi 控制台中提供的每个**工具**和**操作**菜单项都与一个默认 NNMi 角色相关联。(要确定分配给每个“操作”菜单项的默认 NNMi 角色，请参阅 NNMi 帮助中的“NNMi 提供的操作”。) 如果将 NNMi 提供的某个菜单项的设置更改为角色级别低于分配给该菜单项的默认 NNMi 角色的角色，则 NNMi 忽略该更改。角色级别低于默认 NNMi 角色的任何用户组都不能访问该菜单项。

验证用户到用户组的分配

验证用户组成员资格的一个方法是按用户帐户或用户组排序**用户帐户映射**视图，然后检查分组。

另外，在**安全向导**的**映射用户帐户和用户组**页上，每次选择一个用户帐户或用户组，以查看该对象的当前映射。

另一个方法是使用带 `-listUserGroups` 和 `-listUserGroupMembers` 选项的 `nnmsecurity.ovpl` 命令。

验证租户到节点的分配

验证每个节点是否分配到正确租户的一个方法是按租户对**节点**或**节点 (所有属性)** 库存视图排序，然后检查分组。

验证当前用户设置

要验证当前登录用户的 NNMi 控制台访问权限，请单击**帮助 > 系统信息**。**产品**选项卡上的**用户信息**部分列出了当前 NNMi 会话的以下信息：

- 在 NNMi 数据库或访问的目录服务中为用户帐户定义的用户名。
- NNMi 角色，此角色对应于用户映射到的预定义 NNMi 用户组的大多数特权(NNMi 管理员、NNMi 第 2 级操作员、NNMi 第 1 级操作员和 NNMi 来宾用户)。此映射确定在 NNMi 控制台中哪些操作可用。
- 映射到此用户名的用户组。此列表包括设置 NNMi 角色的预定义 NNMi 用户组，以及用于访问 NNMi 数据库中对象的任何其他用户组。

导出 NNMi 安全和多租户配置

下表描述了用于导出 NNMi 安全和多租户配置的配置区域(可用于 `nnmconfigexport.ovpl -c`)。这些导出区域对于维护跨多个 NNMi 管理服务器的配置有益，尤其是在全局网络管理环境中。

NNMi 安全和多租户配置导出区域

配置区域	描述
account	导出用户帐户、用户组和用户帐户到用户组的映射。 可用于跨多个 NNMi 数据库共享用户定义。
security	导出租户和安全组。 可用于跨多个 NNMi 数据库共享安全定义。 导入此信息将创建新对象，并更新现有对象，但不删除当前导出中不包括的对象。因此，此选项可安全用于包含本地定义对象的 NNMi 数据库。
securitymappings	导出用户组到安全组的映射。 要完整导出安全和多租户配置，请执行 `account`、`security` 和 `securitymappings` 配置区域的并发导出。

NNMi 安全、多租户和全局网络管理 (GNM)

在全局网络管理 (GNM) 环境中，节点的租户在管理该节点的 NNMi 管理服务器上设置。给定节点的租户 UUID 在 GNM 环境中的每个全局和区域管理器上都相同。

节点的安全组在拓扑中包含该节点的每个 NNMi 管理服务器上设置。因此，对拓扑中对象的用户访问在 GNM 环境中的每个 NNMi 管理服务器上单独配置。全局和区域管理器可能使用相同或不同的安全组定义。

如果希望全局管理器和区域管理器上的用户访问相似，可以采用一些配置技巧，但可能无法完全避免每个 NNMi 管理服务器上的自定义配置。

备注: 每组动态网络地址转换 (NAT) 或动态端口地址转换 (PAT) 除了需要在整个 NNMi 全局网络管理配置中唯一的租户，还需要 NNMi 区域管理器。请参阅管理 NAT 环境中的重叠 IP 地址 (第 331 页)。另请参阅 NNMi 帮助。

提示: 定义全局管理器上的所有租户和安全组。使用 `nnmconfigexport.ovpl -c security` 可以导出租户和安全组定义。在每个区域管理器上，使用 `nnmconfigimport.ovpl` 可以导入租户

和安全组定义。另外，还可以使用 `nnmsecurity.ovpl` 命令使用与另一个 NNMi 管理服务器上相同的 UUID 创建租户和安全组。遵循此建议可确保 GNM 环境中的每个租户和安全组有相同的 UUID。

备注: 如果用户要从全局管理器启动 NPS 报告，则此最佳实践将成为配置的必需部分。

备注: 租户 UUID 必须唯一，但租户名称可以重用。NNMi 将两个同名但 UUID 不同的租户视为两个不同的租户，且无共享配置。

提示: 如果要为每个组织设置一个区域管理器，则区域管理器上的所有节点可以在单个租户中。但是，要在每个区域管理器上配置唯一租户以确保全局管理器上的拓扑数据分离。

从区域管理器转发到全局管理器的事件可能包括某些附加自定义事件属性(CIA)，以传送安全和租户信息。

如果事件的源对象属于默认租户以外的租户，则转发的事件包含以下 CIA：

- cia.tenant.name
- cia.tenant.uuid

如果事件的源对象属于默认安全组以外的安全组，则转发的事件包含以下 CIA：

- cia.securityGroup.name
- cia.securityGroup.uuid

初始 GNM 配置

在首先配置全局网络管理 (GNM) 后，区域管理器使用区域拓扑中节点的相关信息更新全局管理器(根据 GNM 配置)。

仅与默认租户的拓扑同步

对于有自定义安全组和默认租户的 GNM 环境，在全局管理器上，将远程管理的所有节点添加到具有以下配置的全局管理器拓扑中：

- 默认租户
- 设置为默认租户的初始发现安全组的安全组。

与自定义租户的拓扑同步

对于有自定义安全组和自定义租户的 GNM 环境，在全局管理器上，将远程管理的所有节点添加到租户的 UUID 分配到节点的全局管理器拓扑中：如果全局管理器上不存在该租户 UUID，则 GNM 进程将在全局管理器的 NNMi 配置中如下创建该租户：

- 租户 UUID 与区域管理器上的值相同。
- 租户名称与区域管理器上的值相同。
- 初始发现安全组的值设置为与租户同名的安全组。(如果全局管理器上没有此安全组，NNMi 将创建它。)

当节点添加到全局管理器上的拓扑时，它将按全局管理器上的配置分配到租户 UUID 的初始发现安全组。即全局管理器上的安全组关联与区域管理器上的安全组关联无关。

提示: 简化全局管理器上的安全配置的建议包括：

- 维护由每个区域管理器管理的节点的电子表格或其他记录。对于每个节点，注明区域管理器和全局管理器上的预期安全组。在 GNM 配置完成之后，使用 `nnmsecurity.ovpl` 命令验证并更新安全组分配。
- 如果 GNM 环境将包括更新单个全局管理器的多个区域管理器，则每次从一个区域管理器到全局管理器启用 GNM 配置。

  如果合适，可以先更改默认租户(或自定义租户)的初始发现安全组的值，然后再将每个区域管理器添加到 GNM 配置。注意，如果新节点要添加到之前配置的区域管理器上的拓扑，则此方法可能由多个结果。
- 在启用 GNM 之前，在全局管理器上，将区域管理器上使用的每个租户的初始发现安全组设置为操作员无法访问的专用安全组。然后，全局管理器上的管理员需要将节点显式移到其他 NNMi 控制台操作员的相应安全组中。

GNM 维护

下表描述了区域管理器上节点租户或安全组分配的更改是如何影响全局管理器的。

区域管理器上的配置更改对全局管理器的影响

操作	影响
在区域管理器上，将节点分配到不同租户。	全局管理器上的节点更改为分配到不同租户。如果全局管理器上不存在此租户 UUID，将创建它。
在区域管理器上，将节点分配到不同安全组。	全局管理器上无更改。NNMi 管理员可以选择手动复制更改。
在区域管理器上，更改租户的配置(名称、描述或初始发现安全组)。	全局管理器上无更改。NNMi 管理员可以选择手动复制更改。
在区域管理器上，更改安全组的配置(名称或描述)。	全局管理器上无更改。NNMi 管理员可以选择手动复制更改。

在 NPS 报告中包含选择界面

Network Performance Server (NPS) 是随 NNM iSPI Performance for Metrics 软件一起安装的数据库服务器。

默认情况下，节点的所有组件与节点在同一安全组中。对于各个接口，可以覆盖此默认行为，并将接口分配到不同安全组。此覆盖的目的是生成租户特定报告，以包含该租户(客户)在共享设备上相应的接口。这样，每个客户可以看到其接口的接口信息，但看不到设备上的其他接口。

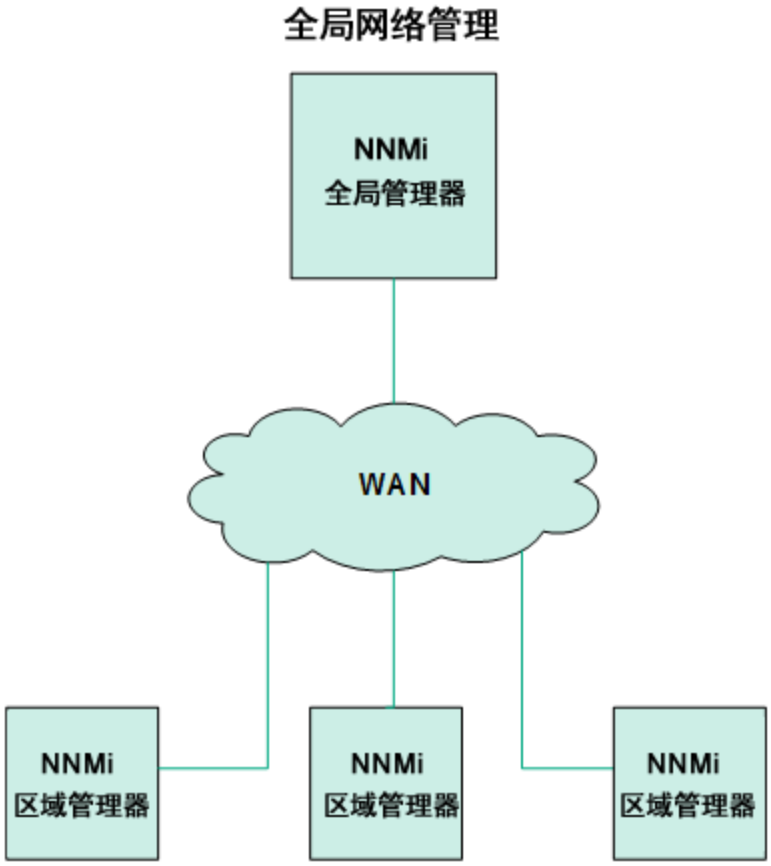
备注: 安全组覆盖仅影响 NPS 报告。不影响用户可见的内容以及在 NNMi 控制台中执行的操作。

要更改接口的安全组分配，请在**接口**表单的**自定义属性**选项卡上或使用 nnmloadattributes.ovpl 命令，将 InterfaceSecurityGroupOverride 自定义属性添加到该接口。将此自定义属性的值设置为安全组的 UUID。例如：

```
InterfaceSecurityGroupOverride=0826c95c-5ec8-4b8c-8998-301e0cf3c1c2
```

备注: 一个接口每次只能属于一个安全组。在接口上设置 InterfaceSecurityGroupOverride 自定义属性将断开该接口与其节点所属安全组之间的关联。

全局网络管理



本章包含以下主题：

- 全局网络管理的好处 (第 367 页)
- 全局网络管理是管理网络的好工具吗？ (第 367 页)
- 实用的全局网络管理示例 (第 368 页)
- 为全局网络管理配置单点登录 (第 373 页)
- 在区域管理器上配置转发筛选 (第 376 页)
- 用区域管理器连接全局管理器 (第 377 页)
- 确定从 global1 到 regional1 和 regional2 的连接状况 (第 378 页)

- 查看 global1 库存 (第 378 页)
- 断开 global1 和 regional1 之间的通信连接 (第 378 页)
- 发现和数据同步 (第 379 页)
- 将自定义属性从区域管理器复制到全局管理器 (第 380 页)
- 设备的状态轮询或配置轮询 (第 380 页)
- 用全局管理器确定设备状态和 NNMi 事件生成 (第 382 页)
- 为全局网络管理配置应用程序故障转移 (第 382 页)
- 全局网络管理的故障排除提示 (第 383 页)
- 全局网络管理和 NNM iSPI 或第三方集成 (第 385 页)
- 全局网络管理和地址转换协议 (第 385 页)

全局网络管理的好处

假定您在位于几个地理位置的多个 NNMi 管理服务器上部署了 HP Network Node Manager i Software (NNMi)。您让每个 NNMi 管理服务器发现和监视网络，以满足发现和监视需要。您可以使用这些现有的 NNMi 管理服务器和配置将特定 NNMi 管理服务器指派为全局管理器，显示组合节点对象数据，而无需其他发现或监视配置更改。

管理网络的不同地理区域时，NNMi 全局网络管理功能使多个 NNMi 管理服务器能一起工作。您将特定 NNMi 管理服务器指派为全局管理器，以显示来自两个或更多区域管理器的组合节点对象数据。

NNMi 全局网络管理功能提供以下好处：

- 全局管理器提供公司范围网络的中心总览视图。
- 易于设置：
  - 每个区域管理器管理员指定在全局管理器级别参与的所有节点对象数据或特定节点组。
  - 每个全局管理器管理员指定允许哪些区域管理器提供信息。
- 在每个服务器上独立生成和管理事件(在每个服务器上可用的拓扑上下文中生成)。

有关其他详细信息，请参阅 NNMi 帮助中的“NNMi 全局网络管理功能”。

备注: 每组动态网络地址转换 (NAT)、动态端口地址转换 (PAT) 或动态网络地址和端口转换 (NAPT) 除了需要在整个 NNMi 全局网络管理配置中唯一的租户，还需要 NNMi 区域管理器。请参阅管理 NAT 环境中的重叠 IP 地址 (第 331 页)。另请参阅 NNMi 帮助。

全局网络管理是管理网络的好工具吗？

本部分包含的问题可帮助您确定 NNMi 全局网络管理功能是否有助于更好地管理网络。

我需要连续的多站点网络监视吗？

您的信息技术组全天候管理位于多个站点的网络设备吗？如果是，您的信息技术组可以使用 NNMi 的全局网络管理功能观测组合的拓扑和事件视图。

我的关键设备是可见的吗？

我能从一个 NNMi 管理服务器查看位于多个位置的关键设备的设备状态和事件吗？

能。您在区域管理器上配置转发筛选。这样，您就能选择要区域管理器发送到全局管理器的节点对象数据。例如，可以在区域管理器上设置转发筛选，使其只将关键设备相关的信息转发到全局管理器。

许可注意事项

有关获取和安装 NNMi 许可证密钥的信息，请参阅许可 NNMi (第 252 页)。

全局管理器和区域管理器上是否都需要 NNMi Advanced、NNMi Premium 或 NNMi Ultimate 许可证？

必须为您计划用作全局管理器的 NNMi 管理服务器购买并安装 NNMi Advanced、NNMi Premium 或 NNMi Ultimate 许可证。

NNMi 区域管理器可使用 NNMi、NNMi Advanced、NNMi Premium 或 NNMi Ultimate 许可证授予许可。

目前对单个地理位置，我有足够的 NNMi 许可证。我可以使用全局网络管理功能并限制全局管理器上需要的新许可证吗？

不可以。您必须为全局管理器购买并安装足够的 NNMi Advanced、NNMi Premium 或 NNMi Ultimate 许可证，使其许可证数达到或超过全局管理器上本地监视的节点数。NNMi 不会根据全局管理器上的许可证容量对不同区域管理器的节点计数。

我增加了区域管理器的 NNMi 许可证数，使得许可节点的总数大于全局管理器上的 NNMi Advanced、NNMi Premium 或 NNMi Ultimate 许可证容量。现在全局管理器未拥有所有区域中的所有节点。为全局管理器购买并安装足够的许可证之后，如何使全局管理器与所有区域管理器同步，以查找并创建之前由于许可证不足而跳过的节点？

要重新同步全局管理器上的拓扑，请执行以下某项操作：

- 等待所有区域管理器上的所有配置的重新发现间隔过去，以便重新发现所有区域中的所有节点。区域管理器重新发现所有区域中的所有节点之后，它将这些重新发现的节点信息发送到全局管理器。全局管理器接收这些节点信息，并在每个区域中为每个节点创建全局节点。
- 在每个区域管理器上运行 **`nnmnoderediscover.ovpl -all`** 脚本。

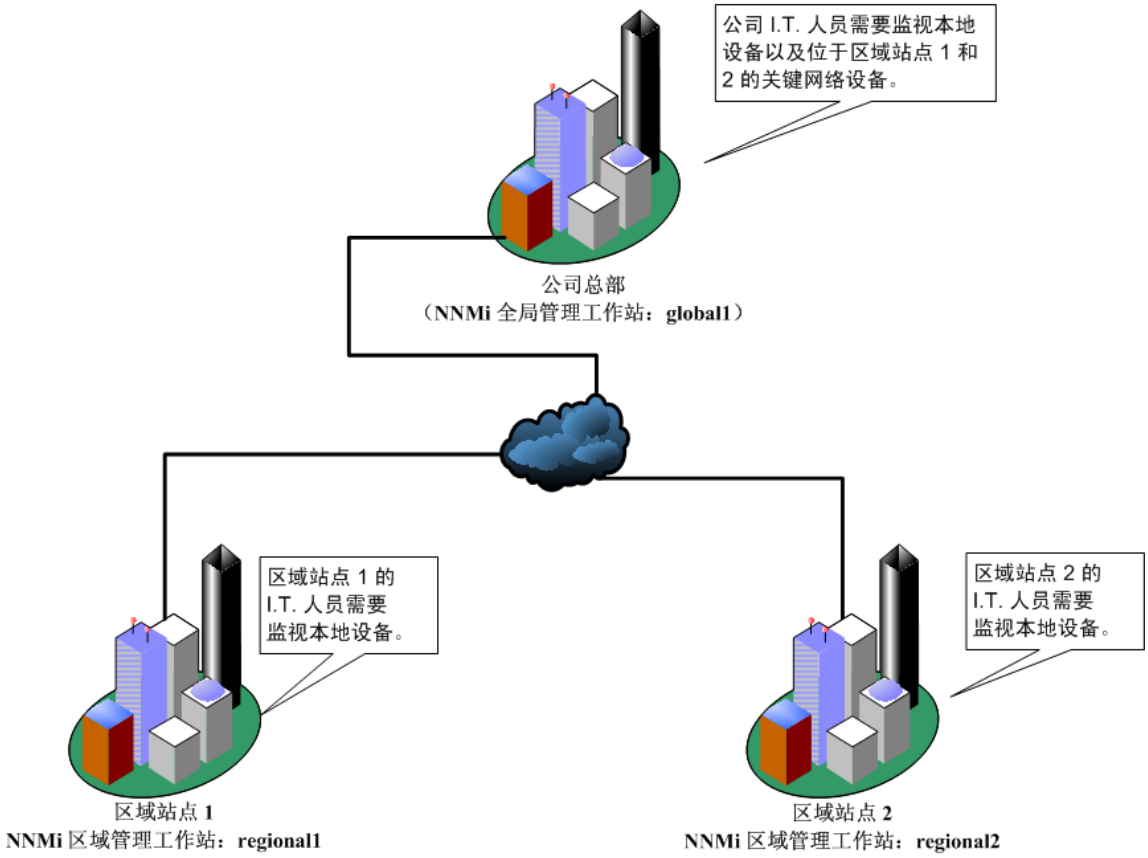
> **备注:** 第二个选项会在网络上造成很大流量，并占用整组 NNMi 管理器的大量 NNMi 资源。此选择不像初始 NNMi 发现那样占用资源，但占用量与执行第一次发现类似。最佳方式是运行每个区域的脚本时隔开一段时间，或等待当前区域管理器的工作负载降至正常再启动下个区域管理器的重新发现。

实用的全局网络管理示例

请参阅下图。在此场景中，贵公司有两个位于不同地理位置的工作场所。公司总部则位于第三个地理区域。三个位置都在运行 NNMi 管理服务器。

从网络角度，公司总部的信息技术专家需要监视本地网络设备以及位于区域位置 1 和 2 的关键网络设备。区域位置 1 和 2 的信息技术专家需要监视其本地的关键网络设备。

示例网络



查看要求

在此示例场景中，公司总部、区域位置 1 和区域位置 2 的 NNMi 管理服务器管理位于各自位置的几个路由器和交换机。

对于此示例，将 NNMi 管理服务器分别视为 `global1`、`regional1` 和 `regional2`。

这些 NNMi 管理服务器配置为发现和监视位于各自位置的关键交换机和路由器。

提示: 无需在其中任何站点重新配置 NNMi 管理服务器发现，即可使用全局网络管理功能。

备注: 在全局网络管理配置期间，您可能试图使用 **`nnmbackup.ovpl`** 脚本备份一个 NNMi 管理服务器，用 **`nnmrestore.ovpl`** 脚本将此备份恢复到第二个 NNMi 管理服务器，然后将这两个 NNMi 管理服务器连接到区域 NNMi 管理服务器。请不要这样做。将备份数据从一个 NNMi 管理服务器放置到另一个 NNMi 管理服务器意味着这两个服务器有相同的数据库 UUID。在第二个 NNMi 管理服务器上恢复 NNMi 之后，将需要从原始 NNMi 管理服务器卸载 NNMi。

卸载 NNMi 之前，以相反顺序删除所有 NNMi 补丁程序，从最新的补丁程序开始。补丁程序删除过程会因 NNMi 管理服务器上运行的操作系统而异。有关安装和删除说明，请参阅补丁程序文档。

公司位置的信息技术组要监视位于区域位置 1 和 2 的关键设备，但他们并不想管理每个设备。

下表结论了监视要求：

全局网络管理的网络要求

位置	NNMi 管理服务器	关键交换机	要管理的区域设备
公司总部	global1	15 个型号为 3500yl HP Procurve 的交换机	来自每个区域位置的所有型号为 3500yl HP Procurve 的交换机
区域位置 1	regional1	15 个型号为 3500yl HP Procurve 的交换机	不适用
区域位置 2	regional2	15 个型号为 3500yl HP Procurve 的交换机	不适用

总之：

- NNMi 管理服务器和 global1 监视公司总部。
- NNMi 管理服务器、regional1 和 regional2 监视每个区域位置。
- 您必须从公司总部查看位于区域位置 1 和 2 的型号为 3500yl Procurve 的交换机的事件和设备信息。
- regional1 和 regional2 都管理位于区域位置 1 的几个常用交换机。

区域管理器和全局管理器连接

配置全局网络管理连接时，要考虑以下信息：

- 在全局管理器和所有区域管理器上使用相同的 NNMi 版本和补丁程序级别。不支持使用不同的 NNMi 版本配置全局网络管理。
- NNMi 允许您配置多个全局管理器与一个区域管理器通信。例如，如果需要第二个全局管理器 global2 与 regional1 通信，则 NNMi 支持配置 global1 和 global2 与 regional1 通信。有关详细信息，请参阅《HP Network Node Manager i Software System and Device Support Matrix》。
- 全局网络管理使用一个连接层。例如，本章中的示例讨论了一个连接层：global1 与 regional1 通信，global1 与 regional2 通信。不要配置 NNMi 用于多个连接级别。例如，不要配置 global1 与 regional1 通信，然后配置 regional1 与 regional2 通信。全局网络管理功能不是为这三层配置设计的。
- 不要将两个 NNMi 管理服务器配置为彼此双向通信。例如，不要配置 global1 与 regional1 通信，然后配置 regional1 与 global1 通信。

初始准备

本部分描述设置示例场景的全局网络管理所需的初始准备。

端口可用性：配置防火墙

为了让全局网络管理功能正常运行，必须验证某些已知端口是否可用于从 global1 到 regional1 和 regional2 的 TCP 访问。NNMi 安装脚本将端口 80 和 443 设置为默认端口；但是，您可以在安装期间更改这些值。

备注: 在本部分讨论的示例中，global1 建立对 regional1 和 regional2 的 TCP 访问。防火墙通常是根据启动连接的服务器配置的。global1 建立与 regional1 和 regional2 的连接之后，通信变成双向的。

编辑以下文件，查看当前值或进行端口配置更改：

- Windows：%NNM_CONF%\nnm\props\nms-local.properties
- Linux：$NNM_CONF/nnm/props/nms-local.properties

下表显示必须可访问的已知端口：

必须可访问的套接字

安全	参数	TCP 端口
非 SSL	nmsas.server.port.web.http	80
	nmsas.server.port.hq	4457
SSL	nmsas.server.port.web.https	443
	nmsas.server.port.hq.ssl	4459

有关详细信息，请参阅NNMi 和 NNM iSPI 默认端口 (第 412 页)。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 ovstop 和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

配置自签名证书

如果计划在 global1 和两个区域 NNMi 管理服务器(regional1 和 regional2)之间结合使用全局网络管理功能和 SSL(安全套接字层)，则必须配置自签名证书。

在 NNMi 安装期间，NNMi 安装脚本在 NNMi 管理服务器上创建自签名证书，以便向其他实体标识自己。必须配置计划用于具有正确证书的全局网络管理功能的 NNMi 管理服务器。完成在全局网络管理环境中使用证书 (第 265 页)中显示的步骤。

配置全局网络管理以供应用程序故障转移

在 NNMi 安装期间，NNMi 安装脚本在 NNMi 管理服务器上创建自签名证书，以便向其他实体标识自己。

要将应用程序故障转移和全局网络管理功能一起使用，必须完成为全局网络管理配置应用程序故障转移 (第 382 页)中所示的步骤。

NNMi 管理服务器大小调整的注意事项

此示例假定您计划在全局网络管理配置中使用现有 NNMi 管理服务器。

请参阅《HP Network Node Manager i Software 交互安装指南》、《NNMi Release Notes》和《NNMi Support Matrix》，以了解有关 NNMi 所需的服务器大小的特定信息。

同步系统时钟

在全局网络管理配置中连接 global1、regional1 和 regional1 之前，同步这些服务器的 NNMi 管理服务器时钟对您很重要。

备注: 您的网络环境中参与全局网络管理(全局管理器和区域管理器)或单点登录 (SSO) 的所有 NNMi 管理服务器都必须使其内部时间的时钟与全局时间同步。

请使用时间同步程序，例如 Linux 工具 Network Time Protocol Daemon (NTPD) 或任一可用的 Windows 操作系统工具。有关详细信息，请参阅 NNMi 帮助中的“时钟同步问题”或“全局网络管理问题故障排除”和 时钟同步 (第 383 页)。

备注: 如果与区域管理器的连接有问题(如服务器时钟同步问题)，则 NNMi 在 NNMi 控制台底部显示警告消息。

在全局网络管理中结合使用应用程序故障转移功能与自签名证书

要在应用程序故障转移配置中使用带自签名证书的全局网络管理功能，请完成在具有故障转移功能的全局网络管理环境中配置证书 (第 267 页)中所述的步骤。

在全局网络管理中使用自签名证书

要使用带自签名证书的全局网络管理功能，必须完成在全局网络管理环境中使用证书 (第 265 页)中所述的步骤。

在全局网络管理中使用证书颁发机构

要使用带证书颁发机构的全局网络管理功能，必须完成在全局网络管理环境中使用证书 (第 265 页)中所述的步骤。

列出要监视的关键设备

创建每个区域管理器所管理设备的列表，并从全局管理器进行监视。例如，创建要从 global1 监视的 regional1 和 regional2 所管理设备的列表。可在转发筛选中使用此信息。有关详细信息，请参阅在区域管理器上配置转发筛选 (第 376 页)。

提示: 仔细考虑限制将信息从 regional1 和 regional2 转发到 global1 的可能后果。以下是计划时要考虑的一些事项：

- 请小心不要排除太多设备，因为 global1 需要来自 regional1 和 regional2 的完整拓扑才能执行完整分析，从而生成准确事件。
- 排除非关键设备有助于您减少 global1 上的系统性能成本。
- 排除非关键设备有助于您改进解决方案的总体可扩展性，并减少 NNMi 需要的网络流量。

查看全局和区域管理器的管理域

查看全局和区域管理器的管理域，帮助确定要从区域管理器转发到全局管理器的信息。

在我们的示例中，NNMi 管理服务器的 global1、regional1 和 regional2 管理各自的节点集。在此示例中，稍后您将配置 regional1 和 regional2 以将有关所管理设备的信息转发到 global1。

用以下过程可以了解 global1、regional1 和 regional2 当前监视的设备。这将帮助您选择要让 regional1 和 regional2 转发到 global1 的关键设备。

对于此示例，完成以下步骤查看此信息：

1. 将浏览器指向 global1 的 NNMi 控制台。
2. 登录。
3. 单击**库存**工作区。
4. 您可以在此查看 global1 当前监视的已发现库存。
5. 将浏览器指向 regional1 的 NNMi 控制台。
6. 登录。
7. 单击**库存**工作区。
8. 查看 regional1 监视的节点，创建要从 global1 监视的设备列表。
9. 将浏览器指向 regional2 的 NNMi 控制台。
10. 登录。
11. 单击**库存**工作区。
12. 查看 regional2 监视的节点，创建要从 global1 监视的设备列表。

查看 NNMi 帮助主题

要查看与全局网络管理相关的所有帮助主题，请完成以下步骤：

1. 从 NNMi 帮助单击**搜索**。
2. 在搜索字段中输入**“全局网络管理”**。
3. 单击**搜索**。

此搜索会找到与全局网络管理相关的 50 多个主题。

SSO 和操作菜单

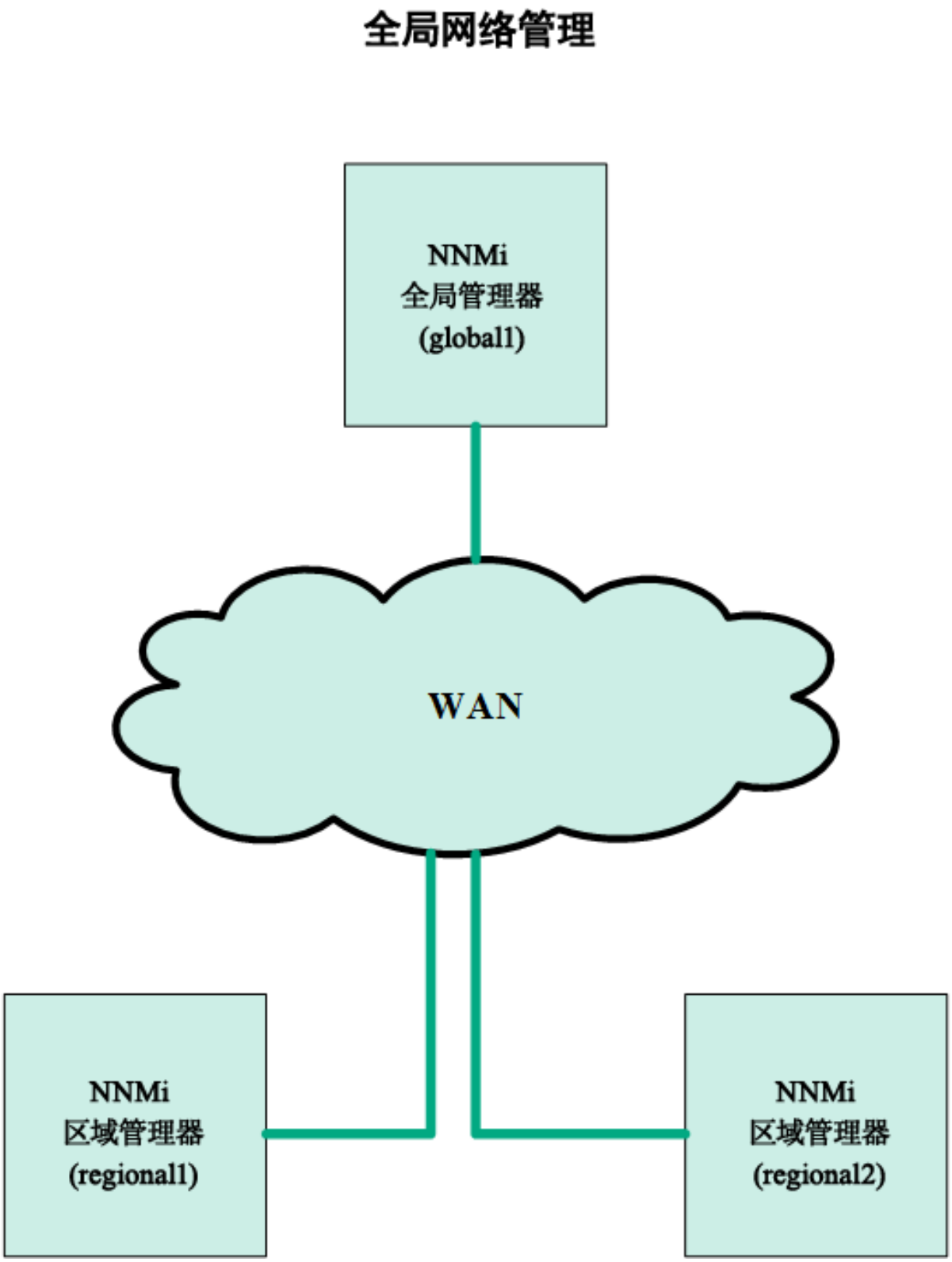
从全局管理器上的 NNMi 控制台，可以选择区域管理器管理的节点，然后用**操作**菜单在所选节点上启动操作。

如果 NNMi 管理服务器之间没有相同的 initString 和 domain 参数，则来自全局管理器的会话信息不会传递到新会话，操作也不会启动。要避免此问题，请遵循为全局网络管理配置单点登录 (第 373 页)中显示的配置步骤操作。

为全局网络管理配置单点登录

您可以配置 NNMi 单点登录 (SSO)，以方便从 NNMi 全局管理器访问 NNMi 区域管理器。

备注: 必须在从全局管理器连接区域管理器之前配置单点登录。有关详细信息，请参阅对 NNMi 使用单点登录 (SSO) (第 269 页)。



SSO 功能在 NNMi 管理服务器之间实现用户名通信，但不包括密码或角色。例如，NNMi 将一个 NNMi 管理服务器 (global1) 上的同一用户名与其他 NNMi 管理服务器(regional1 或 regional2)上

的不同角色关联。这三个 NNMi 管理服务器中的任何一个都可以将不同密码与相同用户名关联。

如果全局和区域管理器驻留在同一管理域中，而您没有如步骤 4 中所示将初始化字符串值从全局 NNMi 管理服务器复制到区域 NNMi 管理服务器，则可能会遇到 NNMi 控制台访问问题。为避免此情况，请使用以下步骤正确配置 SSO，或如禁用 SSO (第 273 页)中所述禁用 SSO。

要配置 SSO 使用全局网络管理功能，请完成以下步骤：

1. 在 global1、regional1 和 regional2 上打开以下文件：
   - Windows：%NNM_PROPS%\nms-ui.properties
   - Linux：$NNM_PROPS/nms-ui.properties
2. 在 global1、regional1 和 regional2 上，在文件中查找类似以下的部分：

   com.hp.nms.ui.sso.isEnabled = false

   对它进行如下更改：

   com.hp.nms.ui.sso.isEnabled = true
3. 找到 global1 的 SSO NNMi 初始化字符串。在 nms-ui.properties 文件中查找类似如下的部分：

   com.hp.nms.ui.sso.initString =初始化字符串
4. 将初始化字符串值从 global1 上的 nms-ui.properties 文件复制到 regional1 和 regional2 上的 nms-ui.properties 文件中。所有服务器都必须对初始化字符串使用相同的值。保存更改。

   备注: NNMi 支持将初始化字符串值从全局 NNMi 管理服务器复制到区域 NNMi 管理服务器。在此步骤中，您已将初始化字符串值从全局管理器复制到两个区域管理器。如果要将 SSO 用于全局网络管理功能，则始终将初始化字符串值从全局管理器复制到区域管理器。

   备注: 如果全局和区域管理器驻留在同一管理域中，而您没有将初始化字符串值从全局 NNMi 管理服务器复制到区域 NNMi 管理服务器，请禁用 SSO 以避免 NNMi 控制台访问问题。有关详细信息，请参阅禁用 SSO (第 273 页)。
5. 如果 global1、regional1 和 regional2 在不同域中，请修改 protectedDomains 内容。为此，请在 nms-ui.properties 文件中查找类似如下的部分：

   com.hp.nms.ui.sso.protectedDomains=group1.mycompany.com

   假定 global1 在 global1.company1.com 中， regional1 在 regional1.company2.com 中，regional2 在 regional2.company3.com 中。对 global1、regional1 和 regional2 上 nms-ui.properties 文件的 protectedDomains 部分进行如下修改：

   com.hp.nms.ui.sso.protectedDomains=regional1.company1.com,
   regional2.company2.com,regional3.company3.com
6. 保存更改。
7. 在 global1、regional1 和 regional2 上运行以下命令序列：

a. ovstop
b. ovstart

备注: 在应用程序故障转移配置中启用单点登录，无需执行手动配置步骤。例如，如果计划在应用程序故障转移配置中配置单点登录，则 NNMi 将以上更改从活动 NNMi 管理服务器复制到备用 NNMi 管理服务器。

在区域管理器上配置转发筛选

在此示例中，global1 与 regional1 和 regional2 通信。要控制您希望全局管理器 global1 从区域管理器 regional1 和 regional2 接收的节点对象数据，必须在 regional1 和 regional2 上配置转发筛选。

配置转发筛选，限制转发的节点

该示例创建了一个节点组，使 regional1 能够只将型号为 Procurve 3500yl 的交换机的节点信息转发到 global1。要创建新节点组并设置这些限制，请完成以下步骤：

1. 从 NNMi 控制台中 regional1 的**配置**工作区，单击**节点组**。
2. 单击**新建**。

   备注: 尽管此示例说明如何创建新的节点筛选，然后用它创建来自 regional1 和 regional2 的转发筛选，但您也可以使用现有筛选中的任何一个来设置从区域 NNMi 管理服务器到全局 NNMi 管理服务器的转发筛选。

   提示: 可创建不包含自己的设备或筛选的容器节点组；然后使用此节点组指定子节点组。您可以使用此方式，用一个容器节点组将节点对象数据转发到全局 NNMi 管理服务器。

3. 单击**设备筛选**选项卡。输入 global1 作为筛选名称，在备注字段中添加有关要创建的筛选的所需注释。
4. 单击**新建**图标以打开节点设备筛选表单。
5. 在下拉菜单中选择交换机路由器设备类别、Hewlett-Packard 设备供应商和 HP Procurve 3500 Fixed-port 交换机设备系列。
6. 在下拉菜单中单击**快速查找**以打开设备配置文件表单。
7. 查找并选择 HP Procurve 3500yl 交换机的配置文件，然后单击**确定**。
8. 单击每个配置表单的**保存并关闭**。
9. 要测试此筛选，请选择 **global1**。
10. 在下拉菜单中单击**显示成员**。
11. 注意，NNMi 已发现 1 个 HP 3500yl 交换机。这表明您创建的筛选正在查找您配置为要查找的特定交换机型号。下个步骤是用您刚创建的这个节点筛选来配置转发筛选。
12. 从 NNMi 控制台中 regional1 的**配置**工作区单击**全局网络管理**。
13. 单击**转发筛选**选项卡。

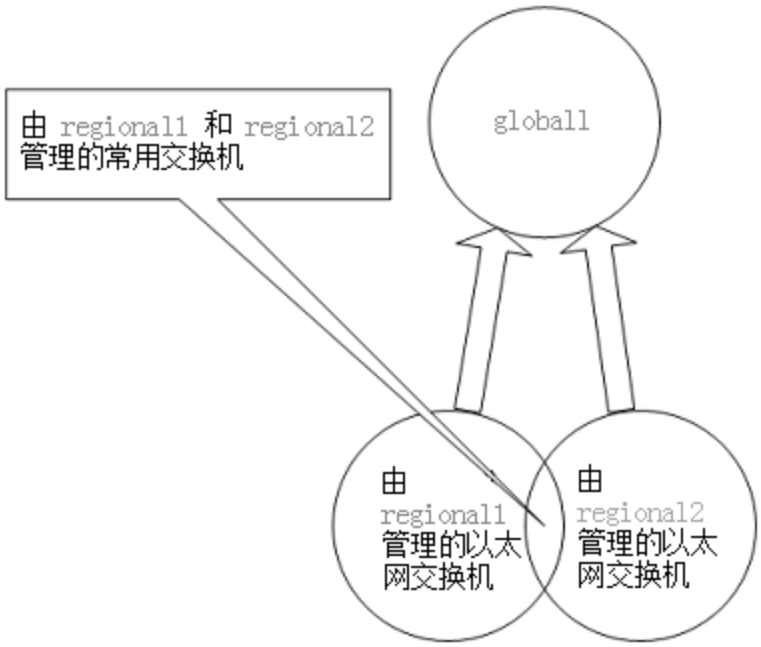
14. 单击**快速查找**。
15. 选择 **global1** 筛选，然后单击**确定**。
16. 单击**保存并关闭**。

这样就完成了在 regional1 上设置转发筛选的任务。对 regional2 完成步骤 1 到步骤 16 之后，您已准备好将 global1 连接到 regional1 和 regional2，如用区域管理器连接全局管理器 (第 377 页) 中所述。

用区域管理器连接全局管理器

在此示例中，regional1 和 regional2 管理几个常用交换机。

要将此常用交换机信息从 regional1 转发到 global1，需要设置所需连接。



为此，您必须将 global1 连接到 regional1，再将它连接到 regional2。通过使用这样的连接顺序，global1 会认为 regional1 是监视这些常用交换机的 NNMi 管理服务器。Global1 还会忽略它从 regional2 接收的有关这些常用交换机的信息。

> **备注:** HP 建议您先小规模地使用此功能，以便更好地了解它如何工作，然后扩展其使用范围来满足网络管理需要。

要首先将 global1 连接到 regional1，然后连接到 regional2，请完成以下步骤：

1. 首先，在全局网络管理配置中连接 global1、regional1 和 regional2 之前，请同步这些服务器的 NNMi 管理服务器时钟。有关详细信息，请参阅 NNMi 帮助中的“时钟同步问题”。

   > **备注:** 如果区域管理器有连接问题(如服务器时钟同步问题)，NNMi 会显示警告消息。

2. 设置从 global1 到 regional1 的连接。
   a. 从 global1NNMi 控制台，单击**配置**工作区中的**全局网络管理**。
   b. 单击**区域管理器连接**。
   c. 单击**新建**图标创建新的区域管理器。
   d. 添加 regional1 的名称和描述信息。
   e. 单击**连接**选项卡。
   f. 单击**新建**图标。
   g. 添加 regional1 的连接信息

      备注: 有关填写此表单的具体信息，请参阅 NNMi 帮助中的**帮助 -> 使用区域管理器连接表单**。

   h. 在每个配置表单中单击**保存并关闭**保存您的更改。
3. 完成步骤 a 到步骤 g，建立 global1 到 regional2 的连接。

确定从 global1 到 regional1 和 regional2 的连接状况

要检查从 global1 到 regional1 和 regional2 的连接状况，请完成以下步骤：

1. 从 global1NNMi 控制台，单击**配置**工作区中的**全局网络管理**。
2. 单击**区域管理器连接**选项卡。
3. 通过检查 regional1 和 regional2 的连接状况，检查它们的状态。注意，连接状况显示为已连接，这意味着它们工作正常。

   有关详细信息，请参阅 NNMi 帮助中的“确定与区域管理器的连接状况”。

等到 NNMi 完成发现之后再继续下一部分。有关详细信息，请参阅《HP Network Node Manager i Software 交互安装指南》中的“检查发现进度”。

查看 global1 库存

在 NNMi 完成发现之后再完成这一部分。有关详细信息，请参阅《HP Network Node Manager i Software 交互安装指南》中的“检查发现进度”。

要查看转发到 global1 的节点信息 regional1，请完成以下步骤：

1. 从 global1 NNMi 控制台，导航到位于**库存**工作区的**按管理服务器显示节点**表单。
2. 假定 regional1 将有关交换机 procurve1.x.y.z 的信息传递到 global1。选择 **regional1** 之后，库存可能如下所示：

完成步骤 1 到步骤 2，查看从连接的其他区域管理器传递到 global1 的设备库存。

断开 global1 和 regional1 之间的通信连接

要关闭(临时或永久)全局管理器(例如 global1)，必须断开全局管理器与区域管理器之间的通信连接。

此示例假定 global1 仍然有 regional1 的活动订购。

要断开 global1 和 regional1 之间的通信连接，请执行以下步骤：

1. 从 global1NNMi 控制台，单击**配置**工作区中的**全局网络管理**。
2. 单击**区域管理器连接**。
3. 检查以确保状态是已连接。如果状态不是已连接，则使用 NNMi 帮助中的全局网络管理问题故障排除主题的信息来诊断问题，然后再继续。
4. 选择 regional1，然后单击**打开**图标。
5. 单击**连接**，选择 **regional1.x.y.z**，然后单击**删除**图标。
6. 单击**保存并关闭**。
7. 在**区域管理器连接**选项卡中，记下 **regional1** 的名称属性值(区分大小写)。在随后的步骤中，RemoteNNMiServerName 变量需要此文本字符串。
8. 单击**保存并关闭**。
9. 在 global1 上的命令行中输入以下命令：

   nnmnodedelete.ovpl -rm regional1 -u NNMiadminUserName **-p** NNMiadminPassword

10. 这些命令从 global1 删除 regional1 转发来的节点记录。这些命令还关闭与从 regional1 转发到 global1 的节点关联的事件。有关详细信息，请参阅 NNMi 帮助中的“断开与区域管理器的通信连接”。
11. 要删除 regional1 的配置记录，请执行以下操作。
    a. 单击**配置**工作区。
    b. 选择**全局网络管理**表单。
    c. 选择**区域管理器连接**选项卡。
    d. 选择 regional1，然后单击删除图标。
    e. 单击**保存并关闭**以保存删除。
12. 对其他连接到 global1 的区域 NNMi 管理服务器(如 regional2)，完成步骤 1 到步骤 11。

发现和数据同步

当网络管理员添加、删除或修改网络、区域服务器(如 regional1 和 regional2)上的设备时，以及发现那些更改并更新全局服务器(如本章示例中的 global1)时，regional1 和 regional2 也将管理员对 global1 所管理节点的管理模式的更改告知 global1。

> **备注:** 为维护一致性，当 regional1 和 regional2 发现设备状况更改时，它们会持续更新 global1，从而使全局和区域服务器上的节点状况保持相同。

任何时候，当 global1 请求 regional1 或 regional2 所管理节点的信息时，regional1 或 regional2 都用请求的信息响应 global1。global1 从不与节点直接通信。global1 执行发现操作时，不会有对设备的重复 SNMP 查询。

global1 在每次 regional1 或 regional2 完成发现时与 regional1 和 regional2 同步。NNMi 使用 FDB(转发数据库)数据计算第 2 层连接。FDB 数据极富动态性，在发现之间变化会很大，尤其是有多个区域服务器连接到全局服务器时。

备注: 同步期间，不在全局服务器上更新对用户或应用程序修改的属性的更改。

每个区域服务器上的重新发现间隔都可调整，并可能导致 global1 和区域管理器之间存在发现准确性差异。重新发现间隔越短，发现就越准确，而 NNMi 产生的网络流量也越大。重新发现间隔越长，发现就越不准确，而 NNMi 产生的网络流量也越少。这意味着您的网络规模增长越大，可能所需的重新发现频率就越低。要设置重新发现间隔，请执行以下步骤：

1. 从 regional1 或 regional2 NNMi 控制台的**配置**工作区中单击**发现配置**。
2. 根据所需的区域服务器启动发现的频率，调整重新发现间隔。全局服务器将在区域服务器完成发现之后立即启动发现。
3. 单击**保存并关闭**。

将自定义属性从区域管理器复制到全局管理器

NNMi 支持在区域管理器上设置自定义属性并将这些自定义属性复制到全局管理器。例如，您可以向区域管理器上的节点添加自定义属性数据，将数据复制到全局管理器后，使用该数据扩展那些节点的事件。

备注: NNMi 支持将节点和接口的自定义属性从区域管理器复制到全局管理器。

可以使用全局管理器的**自定义属性复制**选项卡(在**全局网络管理**配置中)在 NNMi 控制台中配置自定义属性复制。

备注: NNMi 可复制不包含任何用户配置或输入的未编号接口的自定义属性。有关详细信息，请参阅 NNMi 帮助。

此外，还可以使用 nnmgnmattrcfg.ovpl 命令行界面工具执行以下操作：

- 添加要复制的属性
- 禁止复制属性
- 使用批量操作文件添加要复制的属性
- 使用批量操作文件禁止复制属性

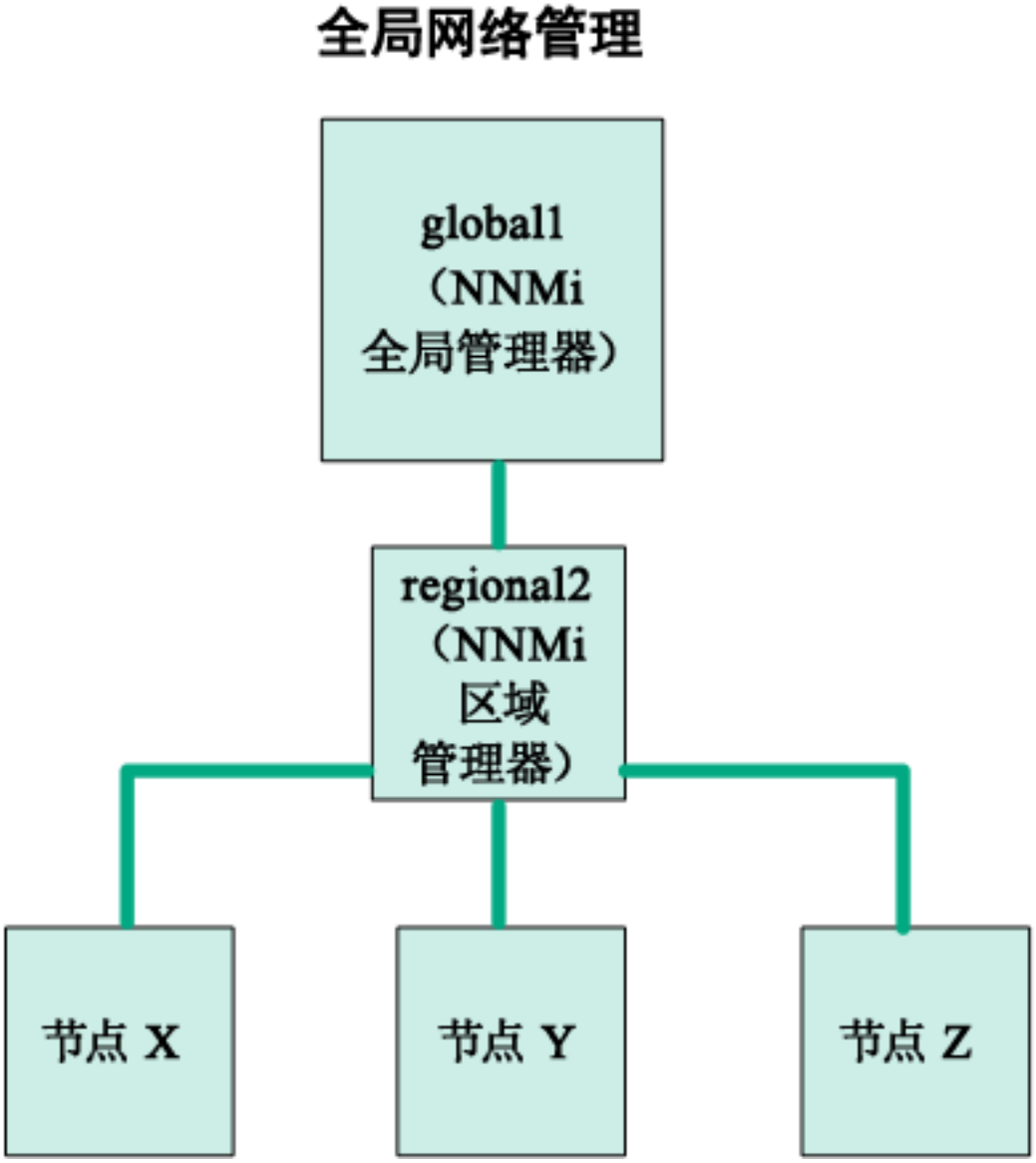
有关详细信息，请参阅 nnmgnmattrcfg.ovpl 参考页或 Linux 联机帮助页。

设备的状态轮询或配置轮询

此示例假定(参阅下图)：

- 区域 NNMi 管理服务器 regional2 发现并管理节点 X
- 全局 NNMi 管理服务器 global1 与区域 NNMi 管理服务器 regional2 连接。

节点的状态轮询或配置轮询



要从 global1 轮询节点 X 的状态，请执行以下操作：

1. 从 global1 的**库存**工作区中单击**节点**。
2. 从节点库存中选择节点 X。
3. 使用**操作 > 状态轮询**菜单项请求节点 X 的状态轮询。
4. NNMi 管理服务器 global1 从区域 NNMi 管理服务器 regional2 请求状态轮询，并在屏幕上显示结果。您从 global1 还是 regional2 启动状态轮询请求都没关系。您会看到相同的状态轮询结果。

如果希望 global1 具有节点 X 的最新发现信息，请执行以下操作从 global1 对节点 X 进行配置轮询。

1. 从 global1 的**库存**工作区中单击**节点**。
2. 从节点库存中选择节点 X。

3. 使用**操作 > 配置轮询**菜单项请求节点 X 的配置轮询。
4. NNMi 管理服务器 global1 从区域 NNMi 管理服务器 regional2 请求配置轮询，并在屏幕上显示结果。您从 global1 还是 regional2 启动配置轮询请求都没关系。您会看到相同的配置轮询结果。

用全局管理器确定设备状态和 NNMi 事件生成

NNMi 管理服务器 global1 侦听来自区域管理器 regional1 和 regional2 的状况更改，并在其本地数据库中更新状况。

NNMi 管理服务器 regional1 和 regional2 上的 NNMi StatePoller 服务计算所监视设备的状况值。global1 接收来自 regional1 和 regional2 的状况值更新。global1 轮询它发现的节点，但不轮询 regional1 和 regional2 管理的节点。

更改 regional1 所管理节点的管理模式之后，也会在 global1 上看到所作的管理模式更改。网络管理员添加、删除或修改由 regional1 或 regional2 管理的网络设备时，regional1 或 regional2 用这些网络设备更改来更新 global1。

global1 使用自己的原因引擎和拓扑生成事件，包括由 regional1 和 regional2 转发给它的节点对象数据。如果拓扑中有差异，这意味着它生成的事件可能与 regional1 和 regional2 事件略有不同。

最好避免在 regional1 或 regional2 上使用转发筛选，因为筛选可能会影响 global1 上的连接。结果可能导致 global1 和两个区域服务器(regional1 和 regional2)之间在根源分析上有差异。多数情况下，如果选择不使用转发筛选，则全局 NNMi 管理服务器将有更大的拓扑。这有助于它得出更准确的根源分析结论。

如果没有其他配置，regional1 不会将陷阱转发到 global1。为此，必须配置 regional1，让它把特定陷阱转发到 global1。HP 建议您将区域管理器配置为只转发较小的重要陷阱，避免全局管理器上负担过重。如果转发的陷阱导致 TrapStorm 事件，则 NNMi 将丢弃转发的陷阱。请参阅 NNMi 控制台中的 TrapStorm 管理事件详细信息。

为全局网络管理配置应用程序故障转移

您可以将全局和区域管理器配置为使用应用程序故障转移。全局或区域管理器自动检测并连接到活动系统。

要配置 global1，让它识别应用程序故障转移，请执行以下操作：

1. 从 global1 NNMi 控制台，单击**配置**工作区中的**全局网络管理**。

   此示例假定：

   - regional1 配置了应用程序故障转移
   - regional1_backup 配置为备用服务器
2. 单击**区域管理器连接**。
3. 选择 regional1，然后单击**打开**图标。
4. 单击**新建**图标。
5. 添加**主机名**、**HTTP 或 HTTPS 端口**、**用户名**和**排序**值。将排序值设置为大于 regional1 值的某个值。
6. 在每个配置表单中单击**保存并关闭**保存您的更改。

如果区域管理器出现故障，则全局管理器执行以下操作：

a. 它连接主服务器。

b. 如果主服务器不响应，它连接辅助服务器。

如果全局系统检测到活动系统没有响应，则它从最低排序号开始，尝试重新连接。

全局网络管理的故障排除提示

本部分包含以下故障排除主题：

提示: 有关全局网络管理故障排除的信息，另请参阅 NNMi 帮助中的**全局网络管理故障排除**主题。

- 时钟同步 (第 383 页)
- 全局网络管理系统信息 (第 383 页)
- 从全局管理器同步区域管理器发现 (第 384 页)
- 补救 global1 上损坏的数据库 (第 385 页)

时钟同步

您的网络环境中参与全局网络管理(全局管理器和区域管理器)或单点登录 (SSO) 的所有 NNMi 管理服务器都必须使其内部时间的时钟与全局时间同步。请使用时间同步程序，例如 Linux 工具 Network Time Protocol Daemon (NTPD) 或任一可用的 Windows 操作系统工具。

如果在 NNMi 控制台底部看到以下消息：

```
NNMi is not connected to 1 Regional Manager(s).See Help ?System Information, Global
Network Management.
```

检查全局管理器上的 `nnm.0.0.log` 文件中的以下消息：

```
警告:由于时钟差异 <秒数>，未连接到系统 <服务器名称>。远程时间为 <日期/时间>。
```

可能时钟已经有偏离，需要重新同步。检查全局管理器上的 `nnm.0.0.log` 文件中的以下消息：

```
警告:由于时钟差异 <秒数>，未连接到系统 <服务器名称>。远程时间为 <日期/时间>。
```

在发出此警告几分钟后，NNMi 断开区域管理器连接。在 NNMi 控制台底部出现以下消息：

```
NNMi is not connected to 1 Regional Manager(s).See Help ?System Information,
Global Network Management.
```

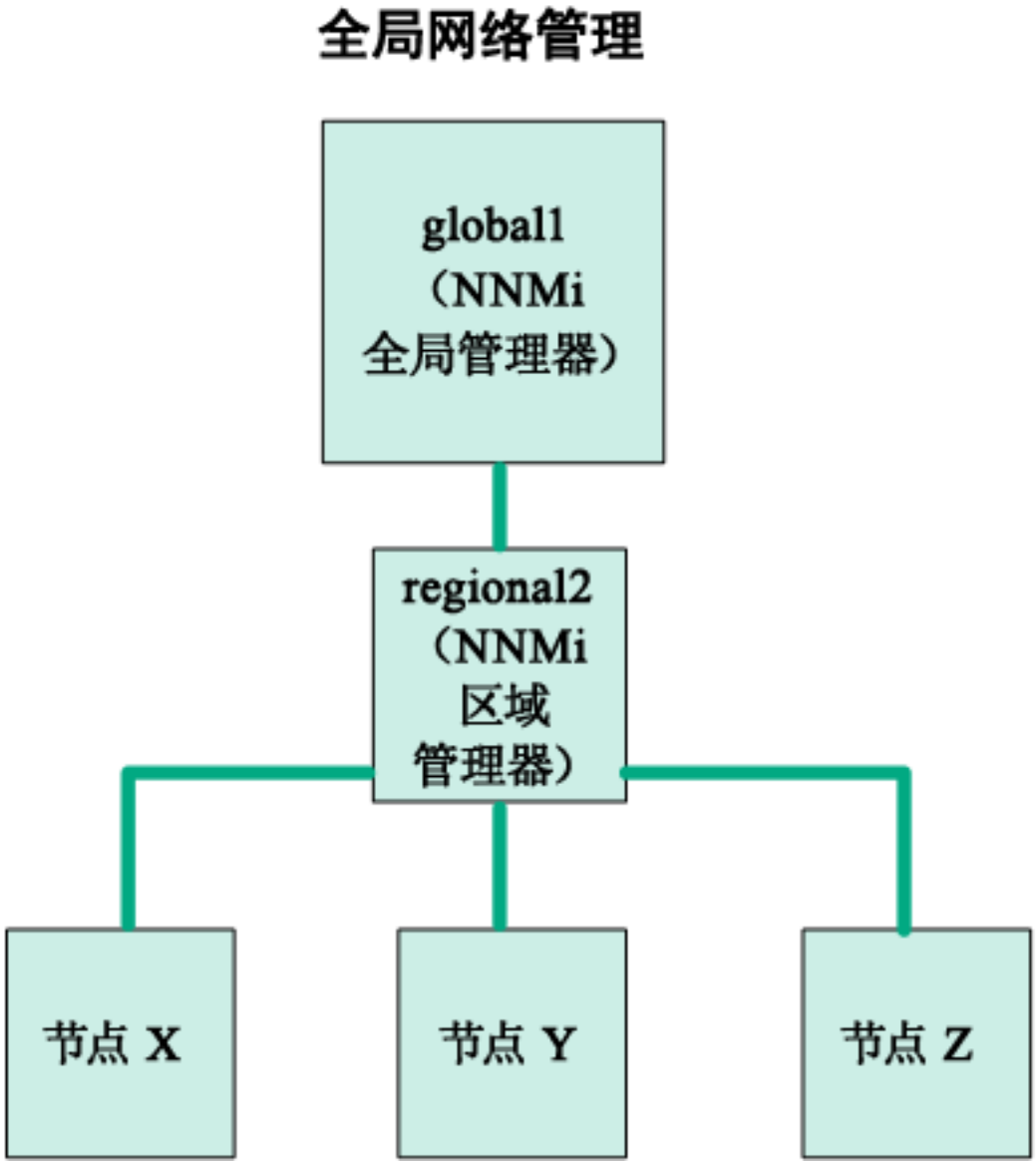
全局网络管理系统信息

选择**帮助 > 系统信息**，然后单击**全局网络管理**选项卡，查看有关全局网络管理连接的信息。

从全局管理器同步区域管理器发现

如果您注意到 global1 和 regional2 之间的信息不一致，请从 global1 运行 **nnmnoderediscover.ovpl** 脚本，从而使得 global1 与 regional2 同步。该操作还会使 regional2 用任何新发现的结果更新 global1。

此示例使用下图中显示的网络。



运行以下命令将节点 X、Y 和 Z 与 global1 同步：

nnmnoderediscover.ovpl -u username -p password -rm regional2。

提示: 可以将 **-fullsync** 标志与 **nnmnoderediscover.ovpl** 命令一起使用以同步轮询的所有对象状况和状态(尽管这会花费更多时间并且会增加系统上的负载)。有关详细信息，请参阅 nnmnoderediscover.ovpl 参考页或 Linux 联机帮助页。

- NNMi 在手动重新同步后将自动重新同步拓扑、状况和状态。
- 在重新同步期间不要停止 NNMi。为帮助确保重新同步已完成，请在手动重新同步后让 NNMi 运行几小时。实际所需时间取决于节点数、状况更改量和执行重新同步时接收到的陷阱数据。
- 如果 NNMi 必须在重新同步完成之前停止，则应重新运行一次重新同步并允许完成。
- 要执行整个管理服务器的手动重新同步，请运行：`nnmnoderediscover.ovpl -all -fullsync`

补救 global1 上损坏的数据库

如果 `global1` 服务中断，需要恢复其数据库，则您将面临以下几种情形：

1. 如果成功地恢复了 `global1` 的数据库，则 `regional1` 和 `regional2` 与 `global1` 同步其缓存信息。`global1` 重新联机之后，没有手动步骤需要执行。
2. 如果 `global1` 服务中断较长一段时间，则步骤 1 可能不会奏效。作为补救，请在 `global1` 上运行 **`nnmnoderediscover.ovpl`** 脚本，从而在 `global1`、`regional1` 和 `regional2` 上启动新发现。在这种情况下，可以在关键设备上运行状态轮询，以便更快获取更新后的状态信息。
3. 如果无法恢复 `global1` 的数据库，则应提交支持呼叫，使用 **`nnmsubscription.ovpl`** 脚本从 `regional1` 和 `regional2` 数据库清除旧的 `global1` 数据。

全局网络管理和 NNM iSPI 或第三方集成

每个 NNM iSPI 或第三方集成都有自己独特的部署准则。对本章中的示例，可以将某些 NNM iSPI 只部署在 `regional1` 上，只部署在 `global1` 上，也可以同时部署在 `regiona1` 和 `global1` 上。对其他 NNM iSPI 或第三方集成，在 `regional1` 和 `global1` 上都必须安装它们。有关详细信息，请参阅 NNM iSPI 或第三方集成的文档。

HP Network Node Manager iSPI Performance for Metrics Software

如果将 NNMi 部署在全局网络管理环境中，则必须执行以下操作：

1. 为每台 NNMi 管理服务器部署一个 Network Performance Server (NPS) 实例。每台区域管理器和全局管理器必须安装并部署了单独的 NPS 实例。
2. 在每台区域管理器和全局管理器上运行一次支持脚本。

全局网络管理和地址转换协议

每组动态网络地址转换 (NAT)、动态端口地址转换 (PAT) 或动态网络地址和端口转换 (NAPT) 除了需要在整个 NNMi 全局网络管理配置中唯一的租户，还需要 NNMi 区域管理器。请参阅管理 NAT 环境中的重叠 IP 地址 (第 331 页)。另请参阅 NNMi 帮助。

配置 NNMi Advanced 的 IPv6 功能

必须购买并安装 NNMi Advanced、NNMi Premium 或 NNMi Ultimate 许可证，才能使用 IPv6 管理功能。

NNMi 中的 IPv6 管理启用对 IPv6 地址(包括其接口、节点和子网)的发现和监视。要提供无缝集成，NNMi 将扩展其 IP 地址模型以包括 IPv4 和 IPv6 地址。NNMi 将尽量以同等方式处理所有 IP 地址；与 IPv4 地址关联的大多数功能同样可用于 IPv6 地址。但仍存在某些例外情况。有关 NNMi 控制台中所显示的 IPv6 信息的详细信息，请参阅 NNMi 帮助。

本章包含以下主题：

- 功能描述 (第 386 页)
- 先决条件 (第 387 页)
- 许可 (第 388 页)
- 支持的配置 (第 388 页)
- 安装 NNMi (第 389 页)
- 取消激活 IPv6 功能 (第 389 页)
- 重新激活 IPv6 功能 (第 391 页)

功能描述

NNMi IPv6 管理功能提供以下功能：

- 对“仅 IPv6”设备和双堆栈设备进行 IPv6 库存发现
  - IPv6 地址
  - IPv6 子网
  - IPv6 地址、子网、接口和节点之间的关联
- 以下操作的本机 IPv6 SNMP 通信：
  - 节点发现
  - 接口监视
  - 陷阱和通知接收及转发
- 双堆栈的设备的 IPv4 或 IPv6 通信(管理地址)的自动选择。通过 NNMi 控制台使用位于**配置**工作区中的**通信配置**将 SNMP 管理地址首选项设置为 IPv4 或 IPv6。
- IPv6 地址故障监视的本机 ICMPv6 通信。
- 使用 IPv6 地址或主机名对设备发现播种
- 使用 IPv6 第 3 层邻居发现提示进行自动 IPv6 设备发现
- 使用第 2 层邻居发现提示(LLDP(链路层发现协议)IPv6 邻居信息)进行自动 IPv6 设备发现
- IPv4 和 IPv6 信息的合并显示
  - 节点、接口、地址、子网和关联的库存视图
  - IPv4 和 IPv6 设备的第 2 层邻居视图及拓扑图

  - IPv4 和 IPv6 设备的第 3 层邻居视图及拓扑图
  - 事件、结论和根源分析
- NNMi 控制台操作：对 IPv6 地址和节点执行 Ping 和 traceroute 操作
- 使用 IPv6 地址和地址范围的 NNMi 配置
  - 通信配置
  - 发现配置
  - 监视配置
  - 节点组和接口组
  - 事件配置
- 对 IPv6 库存和事件的 SDK Web 服务支持
- 对 IPv6 接口的 NNM iSPI Performance for Metrics 支持

NNMi IPv6 管理功能不包含以下操作：

- IPv6 子网连接的发现
- 将 IPv6 Ping 扫描用于发现
- IPv6 网络路径视图(智能路径)
- IPv6 链路本地地址故障监视
- 使用 IPv6 链路本地地址作为发现种子

先决条件

请查看《NNMi 部署参考》、《NNMi Release Notes》和《NNMi Support Matrix》中关于管理服务器规范和 NNMi 安装的详细信息。

要使用本机 IPv6 通信，NNMi 管理服务器必须是双堆栈系统，即它同时使用 IPv4 和 IPv6 进行通信。

> **备注:** 如果您已在 HP NNMi 上配置 IPv6 发现并且正在使用 HP Universal CMDB (UCMDB) 集成，则 UCMDB HP Discovery and Dependency Mapping (DDM) 导入任务将失败。需要禁用 IPv6 发现才能结合使用 HP UCMDB 集成与 HP NNMi。

IPv6 的其他要求包括：

- 必须在至少一个网络接口上启用并配置 IPv4。
- 必须启用 IPv6，并且在连接到要管理的 IPv6 网络的至少一个网络接口上配置全局单播地址或唯一本地单播地址。
- 必须在 NNMi 管理服务器上配置 IPv6 路由以使 NNMi 能够与您希望 NNMi 使用 IPv6 进行发现和监视的任何设备进行通信。

> **备注:** 可以使用“仅 IPv4”NNMi 管理服务器，但这样做将使 NNMi 不能全面管理 IPv4/IPv6 双堆栈设备。例如，如果使用“仅 IPv4”管理服务器，则 NNMi 无法发现“仅 IPv6”设备，无法使用

IPv6 种子和提示进行发现，并且无法监视拥有 IPv6 地址的设备上是否发生故障。

由 NNMi 管理服务器使用的 DNS 服务器必须能够在主机名和 IPv6 地址之间进行双向解析。例如，它必须能够解析为 AAAA DNS 记录，以及从 AAAA DNS 记录进行解析。这表示 DNS 服务器必须将主机名映射到 128 位 IPv6 地址。如果能够处理 IPv6 的 DNS 服务器不可用，NNMi 将仍然正常运行；但是 NNMi 既不确定也不显示使用 IPv6 地址的节点的 DNS 主机名。

许可

必须购买并安装 NNMi Advanced、NNMi Premium 或 NNMi Ultimate 许可证，才能使用 IPv6 管理功能。有关获取和安装 NNMi 许可证的信息，请参阅许可 NNMi (第 252 页)。

NNMi 产品包括临时的瞬时启动许可证密码。这是临时而有效的 NNMi Advanced 许可证。应当尽可能早获取并安装永久许可证密码。

支持的配置

有关 NNMi 的受支持操作系统配置的更多信息，请参阅《NNMi Support Matrix》。

管理服务器

下表显示“仅 IPv4”和双堆栈 NNMi 管理服务器的功能。

管理服务器功能

功能	仅 IPv4	双堆栈
IPv4 通信(SNMP，ICMP)	受支持	受支持
IPv6 通信(SNMP，ICMPv6)	不受支持	受支持
双堆栈被管节点	受支持	受支持
使用 IPv4 种子的发现	受支持	受支持
使用 IPv6 种子的发现	不受支持	受支持
IPv4 地址和子网库存	受支持	受支持
IPv6 地址和子网库存	受支持	受支持
使用 SNMP 的接口状态和性能	受支持	受支持
使用 ICMP 的 IPv4 地址状态	受支持	受支持
使用 ICMPv6 的 IPv6 地址状态	不受支持	受支持

管理服务器功能(续)

功能	仅 IPv4	双堆栈
仅 IPv6 被管节点	不受支持	受支持
使用 IPv6 种子的发现	不受支持	受支持
IPv6 地址和子网库存	不受支持	受支持
使用 SNMP 的接口状态和性能	不受支持	受支持
使用 ICMPv6 的 IPv6 地址状态	不受支持	受支持
仅 IPv4 被管节点	受支持	受支持
使用 IPv4 种子的节点发现	受支持	受支持
使用 IPv4 种子的节点发现	受支持	受支持
使用 SNMP 的接口状态和性能	受支持	受支持
使用 SNMP 的接口状态和性能	受支持	受支持
IPv4 地址和子网库存	受支持	受支持

IPv6 的受支持 SNMP MIB

NNMi 对于 IPv6 支持以下 SNMP MIB：

- RFC 4293(当前 IETF 标准)
- RFC 2465(原始 IETF 提案)
- Cisco IP-MIB

安装 NNMi

在 NNMi 安装期间，安装脚本会激活 IPv6 功能；但如果需要，您可以通过编辑 `nms-jboss.properties` 文件手动取消激活这些 IPv6 功能。

取消激活 IPv6 功能后还可以重新激活。有关详细信息，请参阅取消激活 IPv6 功能 (第 389 页)和重新激活 IPv6 功能 (第 391 页)。

取消激活 IPv6 功能

可通过执行以下操作以管理方式禁用 IPv6 功能：

1. 打开 nms-jboss.properties 文件。查看以下位置：

   Windows：%NNM_PROPS%\nms-jboss.properties

   Linux：$NNM_PROPS/nms-jboss.properties

   > **备注:** NNMi 提供每个属性的完整描述，在 nms-jboss.properties 文件中将它们显示为注释。

2. 要在 NNMi 中取消激活 IPv6 通信：
   a. 找到以 # Enable Java IPv6 Communication 开头的文本。
   b. 找到以下行：
   c. java.net.preferIPv4Stack=false
   d. 将此行编辑为如下所示：

      java.net.preferIPv4Stack=true

      确保此行未被注释。
3. 要在 NNMi 中取消激活总体 IPv6 管理：
   a. 找到以 # Enable NNMi IPv6 Management 开头的文本。
   b. 找到以下行：

      com.hp.nnm.enableIPv6Mgmt=true

   c. 将此行编辑为如下所示：

      com.hp.nnm.enableIPv6Mgmt=false

      确保此行未被注释。
   d. 保存并关闭 nms-jboss.properties 文件。
4. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 ovstop 命令。
   b. 在 NNMi 管理服务器上运行 ovstart 命令。

   > **备注:** 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改需要停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

5. 使用以下命令检查 NNMi 进程：

   ovstatus -v ovjboss

有关更改 NNMi 许可证的信息，请参阅许可 (第 388 页)。

。

取消激活之后的 IPv6 监视

如果 IPv6 管理或 IPv6 通信已完全被禁用，则 StatePoller 服务立即停止使用 ICMPv6 监视 IPv6 地址。NNMi 将这些地址的 IP 地址状况设置为未轮询。如果选择地址，然后使用此地址的**操作** >

监视设置，NNMi 将显示 `Fault ICMP Polling enabled: false`，即使关联的监视配置规则已启用 IP 地址故障轮询。

取消激活之后的 IPv6 库存

在 NNMi 完整发现了 IPv6 库存后，在以下场景中即可让 NNMi 自动清理它：

- 打开主 IPv6 交换机，然后关闭它，并重新启动 NNMi。

  NNMi 不立即删除 IPv6 库存。NNMi 在下一个发现周期中删除 SNMP 节点的 IPv6 库存。NNMi 不删除非 SNMP IPv6 节点。必须从 NNMi 库存中手动删除 IPv6 节点。
- 仅限 NNMi Advanced。您的 NNMi Advanced 许可证已过期或某位用户删除了许可证。NNMi 开始使用 NNMi 基本许可证，并且基本许可证有足够容量以继续管理所有发现的节点。

  NNMi 立即从其库存删除所有非 SNMP IPv6 节点。NNMi 重新发现所有 SNMP 节点，并删除所有 IPv6 数据。
- 仅限 NNMi Advanced。您的 NNMi Advanced 许可证已过期或某位用户删除了许可证。NNMi 开始使用 NNMi 基本许可证，并且基本许可证没有足够容量以继续管理所有发现的节点。NNMi 立即删除所有非 SNMP IPv6 节点。

清理 IPv6 库存时的已知问题

在下列情况下，您可能会遇到剩余的 IPv6 库存：

NNMi 成功使用 SNMP 来管理 IPv6 节点，然后节点在下一次发现之前变得无法访问。

由于现有发现系统的设计，发现过程无法更新不能使用 SNMP 通信的节点。要删除这些剩余节点，必须解决通信问题，然后使用位于 NNMi 控制台中的**操作 > 配置轮询**命令从这些节点获取配置信息。对于本机 IPv6 节点，直接从 NNMi 控制台删除节点。

重新激活 IPv6 功能

> **备注:** 需要 IPv6 通信的功能(例如“仅 IPv6”设备的发现以及 IPv6 地址状态的监视)需要 NNMi 管理服务器配置 IPv6 全局单播地址并使它可运行。

以下过程说明了如何在取消激活 IPv6 功能后将其重新激活。

1. 编辑 `nms-jboss.properties` 文件。查看以下位置：

   Windows：%NNM_PROPS%\nms-jboss.properties

   Linux：`$NNM_PROPS/nms-jboss.properties`

   > **备注:** NNMi 提供每个属性的完整描述，在 `nms-jboss.properties` 文件中将它们显示为注释。

2. 找到以 `# Enable NNMi IPv6 Management` 开头的文本。
3. 要在 NNMi 中启用 IPv6 通信，请取消以下属性的注释：

   ```
   java.net.preferIPv4Stack=false
   ```

> **注意**：要取消属性的注释，请删除行开头的 #! 字符。

4. 找到以 # Enable NNMi IPv6 Management 开头的文本。
5. 要在 NNMi 中启用总体 IPv6 管理，请取消以下属性的注释：

   com.hp.nnm.enableIPv6Mgmt=true

6. 保存并关闭 nms-jboss.properties 文件。
7. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

   > **备注:** 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改需要停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

8. 使用以下命令检查 NNMi 进程：

   ovstatus -v ovjboss

   成功启动的输出应该类似以下内容：

```
object manager name: ovjboss
state:               RUNNING
PID:                 <进程 ID 号>
last message:        Initialization complete.
exit status:         -
additional info:
SERVICE                                  STATUS
CommunicationModelService                        Service is started
CommunicationParametersStatsService              Service is started
CustomPoller                                     Service is started
IslandSpotterService                             Service is started
ManagedNodeLicenseManager                        Service is started
MonitoringSettingsService                        Service is started
NamedPoll                                        Service is started
msApa                                            Service is started
NmsCustomCorrelation                             Service is started
NmsDisco                                         Service is started
NmsEvents                                        Service is started
```

```
NmsEventsConfiguration                          Service is started
NmsExtensionNotificationService                 Service is started
NnmTrapService                                  Service is started
PerformanceSpiAdapterTopologyChangeService      Service is started
PerformanceSpiConsumptionManager                Service is started
RbaManager                                      Service is started
RediscoverQueue                                 Service is started
SpmdjbossStart                                  Service is started
StagedIcmp                                      Service is started
StagedSnmp                                      Service is started
StatePoller                                     Service is started
TrapConfigurationService                        Service is started
TrustManager                                    Service is started
```

9. 重新激活 IPv6 之后，NNMi 视图将立即包含新发现节点的 IPv6 库存。在下一个发现周期中，NNMi 视图显示与以前所发现节点关联的 IPv6 库存。
10. (可选)为双堆栈被管节点设置 SNMP 管理地址首选项。双堆栈被管节点是可以使用 IPv4 或 IPv6 通信的节点。为此，请完成以下步骤：
    a. 从 NNMi 控制台，单击位于**配置**工作区中的**通信配置**。
    b. 找到**管理地址选择**部分。在 IP 版本首选项字段中选择 IPv4、IPv6 或任何。
    c. 保存更改。
    d. 重新启动 NNMi 管理服务器：

       在 NNMi 管理服务器上运行 **ovstop** 命令。

       在 NNMi 管理服务器上运行 **ovstart** 命令。

> **备注:** 在高可用性 (HA) 下进行文件更改时，必须在群集中的两个节点上都进行更改。如果更改需要停止并重新启动 NNMi 管理服务器，则在运行 ovstop 和 ovstart 命令前必须将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

为了加快执行速度，请选择已知为双堆栈节点的节点，然后使用 NNMi 控制台中的**操作 > 配置轮询**命令。还可以使用 nnmnoderediscover.ovpl 脚本将节点添加到 NNMi 发现队列。有关详细信息，请参阅 nnmnoderediscover.ovpl 参考页或 Linux 联机帮助页。

在 NNMi 管理服务器上启用 IPv6 通信之后，NNMi 开始使用 ICMPv6 来监视节点是否发生 IPv6 地址故障。

第 7 章: NNMi 安全性

本章包含以下主题：

- 配置 SSL 通信以进行 Web 访问和 RMI 通信 (第 394 页)
- 允许非根 Linux 用户启动和停止 NNMi (第 394 页)
- 为嵌入式数据库工具提供密码 (第 395 页)
- 配置 NNMi 以启用或禁用 SSLv3 密码 (第 395 页)
- 配置 NNMi 密码 (第 397 页)
- NNMi 数据加密 (第 397 页)

配置 SSL 通信以进行 Web 访问和 RMI 通信

NNMi 包括一组默认密码，在 Web 访问和 Java Remote Method Invocation (RMI) 通信中配置安全套接字层 (SSL) 时使用这组密码。这些密码列在 nms-jboss.properties 文件中。

警告: 在未得到 HP 批准的情况下不得在密码列表中添加或删除密码，这样做可能会导致产品损坏或使产品变得无法正常运行。

允许非根 Linux 用户启动和停止 NNMi

备注: 如果 `/opt/OV` 目录位于配置了 `nosuid` 选项集的分区上，则非根用户功能不可用。请查看 `/etc/fstab`，确定该分区是否配置了 `nosuid` 选项集。

NNMi 提供一种允许非根 Linux 用户启动和停止 NNMi 的方法。执行以下操作：

1. 作为根用户，编辑以下文件：

   `$NnmDataDir/shared/nnm/conf/ovstart.allow`

2. 包括希望其能够启动和停止 NNMi 的非根用户 (一行一个用户)。
3. 保存更改。

备注: 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

为嵌入式数据库工具提供密码

要运行嵌入式数据库工具(例如 psql)，NNMi 需要密码。NNMi 提供了默认密码，用户应使用 nnmchangeembdbpw.ovpl 脚本更改此密码。

> **备注:** 您必须在 Windows 系统上以管理员身份或在 Linux 系统上以根用户身份登录，才能运行 nnmchangeembdbpw.ovpl 脚本。有关详细信息，请参阅 nnmchangeembdbpw.ovpl 参考页或 Linux 联机帮助页。

如果已在高可用性 (HA) 环境中配置 NNMi，则只在主群集节点上运行 nnmchangeembdbpw.ovpl 脚本。

只在主群集节点上：

1. 将主群集节点置于维护模式。

   有关将节点置于维护模式的详细信息，请参阅维护模式 (第 163 页)。
2. 停止所有 NNMi 进程：

   Windows：%NNM_BIN%\ovstop -c

   Linux：$NNM_BIN/ovstop -c
3. 重新启动 nnmsdbmgr：

   Windows：%NNM_BIN%\ovstart nnmsdbmgr

   Linux：$NNM_BIN/ovstart nnmsdbmgr
4. 要更改嵌入式数据库密码，请运行 nnmchangeembdbpw.ovpl 脚本。

   Windows：%NNM_BIN%\nnmchangeembdbpw.ovpl

   Linux：$NNM_BIN/nnmchangeembdbpw.ovpl
5. 为确保已将更改复制到复制目录，以便能复制到辅助群集节点，请运行 nnmdatareplication.ovpl 脚本：

   Windows：%NNM_DATA%\misc\nnm\ha\nnmdatareplication.ovpl NNM

   Linux：$NNM_DATA/misc/nnm/ha/nnmdatareplication.ovpl NNM
6. 重新启动所有 NNMi 进程：

   Windows：%NNM_BIN%\ovstart

   Linux：$NNM_BIN/ovstart
7. 使主群集节点脱离维护模式。
8. 故障转移到辅助群集节点。

   > **备注:** 为了复制 Postgres 密码，辅助群集节点不得处于维护模式。

在此节点上启动 NNMi 资源组时，应用程序会自动将密码复制到辅助群集节点。

配置 NNMi 以启用或禁用 SSLv3 密码

您可以修改 NNMi 密码列表。但请确保通过将本部分中讨论的属性文件复制到其他目录来保留原始信息。默认情况下，NNMi 禁用 SSLv3 密码。您可能需要启用 SSLv3 密码才能解决 Web 浏

览器通信问题。例如，您可能会收到类似于以下内容之一的连接错误：

- 安全连接失败
- 无法显示此页面

如果您还要使用驻留在 NNMi 管理服务器上的 NNM iSPI 软件并为 NNMi 启用 SSLv3 密码，则还必须为每个 iSPI 启用 SSLv3。有关启用和禁用 SSLv3 的信息，请参阅每个对应 NNM iSPI 的《部署参考》。

在高可用性 (HA) 下进行更改时，需要更新的 server.properties 文件位于以下位置：<共享磁盘>/NNM/dataDir/nmsas/NNM/server.properties。

要配置 NNMi 以启用 SSLv3 密码，请执行以下操作：

1. 打开以下文件：

   Windows：%NnmDataDir%\nmsas\NNM\server.properties

   Linux：$NnmDataDir/nmsas/NNM/server.properties
2. 编辑以下行：

   ```
   com.hp.ov.nms.ssl.PROTOCOLS = SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2
   ```

   以包含 SSLv3。例如：

   ```
   com.hp.ov.nms.ssl.PROTOCOLS = SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2,SSLv3
   ```

   备注: 您可以删除此行中包含的任何协议。

3. 保存该文件。

   备注: 如果还要为一个或多个 iSPI 启用 SSLv3，请在停止并启动 NNMi 管理服务器之前按照接下来的步骤所述进行这些更改。

4. 停止 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 ovstop 命令。
5. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 ovstart 命令。

要在启用 SSLv3 密码后禁用它们，请执行以下操作：

1. 打开以下文件：

   Windows：%NnmDataDir%\nmsas\NNM\server.properties

   Linux：$NnmDataDir/nmsas/NNM/server.properties
2. 编辑以下行：

   ```
   com.hp.ov.nms.ssl.PROTOCOLS = SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2,SSLv3
   ```

   以删除 SSLv3。例如：

   ```
   com.hp.ov.nms.ssl.PROTOCOLS = SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2
   ```

3. 保存该文件。

> **备注:** 如果还要为一个或多个 iSPI 在启用 SSLv3 后将其禁用，请在停止并启动 NNMi 管理服务器之前按照接下来的步骤所述进行这些更改。

4. 停止 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 `ovstop` 命令。
5. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 `ovstart` 命令。

配置 NNMi 密码

有关 NNMi 使用的密码的信息，请参阅《NNMi 强化指南》中的“配置 NNMi Web 服务器使用的密码”。

NNMi 数据加密

NNMi 可合并产品许多区域中的数据加密。例如：

- 在群集节点之间发送的应用程序故障转移加密消息。
- NNMi 将用户帐户密码以加密形式存储在 NNMi 数据库中。
- 在区域管理器和全局管理器之间发送的全局网络管理 (GNM) 加密消息。

NNMi 使用一种跨若干 NNMi 组件的数据加密方法。NNMi 数据加密支持以下加密类型：

- 对称加密 — 双方共享相同的密钥
- 非对称 — 公钥和私钥加密，每一方均拥有另一方的公钥，但保留自己的私钥
- 消息摘要(哈希) — 单向加密(无法解密)，任意长度的字符串缩短为固定长度的字符串。

加密配置文件

NNMi 加密框架包括可进行编辑以配置您的组织的加密设置的一组文件。这些文件位于以下文件夹中：

- Windows：`%NnmDataDir%\shared\nnm\conf\crypto`
- Linux：`$NnmDataDir/shared/nnm/conf/crypto`

> **警告:** 加密配置文件主要供高级用户使用。编辑加密配置文件时要极其小心。对这些文件进行不正确的编辑会导致严重问题。例如，对应用程序故障转移的加密参数进行任何更改都将导致应用程序故障转移不再起作用。同样，更改系统和数据库密码加密设置将导致 NNMi 不再启动。更改不同 NNMi 子系统的加密配置时，请参阅以下部分了解要遵循的步骤。

加密配置文件中的文本块

加密配置文件包括以下文本块：

`<allowed>`

`<allowed>` 块定义允许在加密配置文件的其他位置使用的提供程序类型、算法和密钥最小长度。

> **备注:** 如果尝试使用不被允许的算法或密钥长度，NNMi 将生成加密错误。

> **提示:** 提供程序是提供加密算法实现的供应程序(或实体)。

加密配置文件中列出的算法与这些文件中列出的提供程序关联。

`<default>`

`<default>` 块列出用于所有受支持组件的默认设置。例如，`<default>` 块列出一个对称算法，一个非对称算法和一个摘要。如果为给定组件定义了组件块，则该组件使用其组件块中指定的算法(换句话说，组件块定义会覆盖 `<default>` 块)。否则，组件会针对该组件使用的特定加密类型(从 `<default>` 块)请求默认算法。

每个组件仅使用一种加密类型(对称、非对称或摘要)。例如，应用程序故障转移仅使用对称加密，因此在应用程序故障转移组件块中指定非对称或摘要算法是无效且不必要的。

> **备注:** 默认块或组件块中列出的密钥大小必须至少为 `<allowed>` 块中列出的大小(如需要，可更大)。例如，如果 `<allowed>` 块包括 AES-128，则 AES-192 也有效。但如果 `<allowed>` 块中指定 AES-192，则 AES-128 无效。

加密和应用程序故障转移

要更改加密配置以实现应用程序故障转移(例如更改加密算法或密钥长度)，请执行以下操作：

1. 通过在两个节点上运行 ovstop 命令停止 NNMi 和 nnmcluster 进程。请注意，在配置了应用程序故障转移的 NNMi 管理服务器上使用 ovstop 命令时，NNMi 将自动运行以下命令：

   ```
   nnmcluster -disable -shutdown
   ```

2. 根据需要编辑 nnmcluster-crypto-config.xml 文件。

   > **备注:** 应用程序故障转移仅使用对称加密，因此添加非对称或摘要无任何作用，删除对称将导致故障。

3. 保存对 `nnmcluster-crypto-config.xml` 文件的更改。
4. 删除旧密钥文件。

   > **提示:** 文件位置在 `nnmcluster-crypto-config.xml` 文件中定义。

5. 通过运行以下命令生成新密钥文件：

   ```
   nnmcluster -genkey
   ```

6. 将编辑过的 `nnmcluster-crypto-config.xml` 文件和新密钥文件复制到群集中的另一节点(位于同一文件夹中)。

现在，两个节点上定义加密算法和密钥的 nnmcluster-crypto-config.xml 文件是相同的。同时，两个节点上的密钥本身也相同。

7. 通过在活动节点和备用节点上运行 nnmcluster 重新启动群集。

   在活动节点上运行 nnmcluster -daemon。

   > **备注:** 等待节点成为活动节点。

   在备用节点上运行 nnmcluster -daemon。

> **备注:** 如果未删除旧密钥文件，则您将收到类似以下的错误：
>
> 警告:生成新的加密密钥将需要关闭 NNMi 群集。
>
> 是否要继续 (y/n)?
>
> y
>
> 错误:尝试生成新的加密密钥失败。
>
> 最可能的原因是密钥大小增加，
> 当前密钥无效。
>
> 请删除现有密钥并重试。

加密和用户帐户密码

> **备注:** 此信息不适用于轻量级目录访问协议 (LDAP) 或通用访问卡 (CAC) 帐户。

使用 NNMi 控制台创建的 NNMi 用户帐户存储在 NNMi 数据库中。这些用户的密码经哈希处理，存储在数据库中。

当用户登录 NNMi 控制台或使用命令行界面 (CLI) 工具时，会对用户提供的密码进行哈希处理并与存储在数据库中的哈希值进行比较。如果用户提供的密码正确，则这两个哈希字符串匹配，用户通过验证。

NNMi 的较早版本 (9.x) 针对哈希用户密码使用加密算法，现在看来已过时。NNMi 针对用户帐户密码使用更强大的算法。但是由于哈希是单向加密，因此从 NNMi 9.x 升级到 10.x 期间不能解密用户密码然后重新加密。

升级时，所有现有用户的密码仍使用旧加密算法存储在数据库中。但是，使用旧算法对密码进行哈希处理的用户成功登录后，将自动使用加密配置文件中指定的新哈希算法对用户提供的密码进行重新加密。

这意味着所有密码都将随着升级后每个用户第一次登录缓慢地更新。将来更改加密配置文件时也同样如此。在下一次成功登录时，用户密码升级到使用新哈希算法。

> - 是否升级用户密码取决于是否存在 <allowed> 块中列出的较早的旧算法(例如 MD5)。因此在所有密码完成迁移前，请保留 <allowed> 块中列出的较早的旧算法。
> - 如果 <allowed> 块中不存在较早的旧算法，则无法重新对数据库中经哈希处理的现有密码进行哈希处理。因此，关联用户无法登录，并且 NNMi 无法使用新算法重新加密密码。

- 如果已从 `<allowed>` 块中删除较早的旧算法，则管理员必须删除并重新创建受影响的用户，或重置使用较早旧算法加密密码的用户的相应密码。

使用以下命令确定用户的密码是使用加密配置文件中列出的算法还是加密配置文件中不再指定的较早旧算法加密的：

```
nnmsecurity.ovpl -listUserAccounts legacy
```

有关详细信息，请参阅 `nnmsecurity.ovpl` 参考页或 Linux 联机帮助页。

使用 HPE Operations Bridge Reporter 查看报告

要使用 NNMi 采集的数据执行有效的网络性能分析，可以使用 HPE Operations Bridge Reporter (OBR)。

先决条件

- 已安装和配置 NPS。
- 不得将 NPS 和 OBR 安装在同一系统上。
- 不得将 NNMi 和 OBR 安装在同一系统上。
- 如果 NNMi 和 NPS 安装在同一系统上，则必须完成以下其他任务：
  a. 转到 NNMi 管理服务器上的以下目录：
     - Windows：`%nnmdatadir%\shared`
     - Linux：`/var/opt/OV/shared`
  b. 手动与用户 `NpsUsr` 共享 `perfSpi` 目录。

  > **备注：**在安装 NPS 期间创建 `NpsUsr`。

配置 NNMi 将数据导出到 OBR

要使 OBR 使用 NNMi 采集的数据，请执行以下操作：

1. 以根用户或管理员身份登录到 NNMi 管理服务器。
2. 用文本编辑器打开以下文件：
   - 在 Windows 上：`%nnmdatadir%\shared\perfSpi\conf\nmsAdapter.conf`
   - 在 Linux 上：`/var/opt/OV/shared/perfSpi/conf/nmsAdapter.conf`
3. 在文件的末尾添加以下行：
   `exportToSHR:true`
4. 保存该文件。
5. 转到以下目录：
   - 在 Windows 上：`%nnminstalldir%\bin`
   - 在 Linux 上：`/opt/OV/bin`
6. 通过运行以下命令，重新启动 NNMi：

- 在 Windows 上
  i. **ovstop -c**
  ii. **ovstart -c**
- 在 Linux 上
  i. **./ovstop -c**
  ii. **./ovstart -c**

配置 OBR 以使用 NNMi 采集的数据

要配置 OBR 以使用 NNMi 采集的数据，请按照《HP Service Health Reporter 10.00 管理指南》的配置 SHR 以使用 NNMi 数据部分中的说明操作。

使用报告

要使用 OBR 报告监视网络性能，请执行以下操作：

1. 在 Web 浏览器中启动 SHR BI Launchpad 门户。
2. 以管理员身份登录到 SHR BI Launchpad 门户。
3. 转到“文档”选项卡。
4. 要查看有关网络接口的报告，请展开“网络接口运行状况”，然后双击报告。
5. 要查看有关网络设备的报告，请展开“网络组件运行状况”，然后双击报告。

将 HP Performance Insight (OVPI) SNMP 自定义报告包采集迁移到 NNMi

如果您正在使用 NNMi 自定义轮询器功能和 HP Performance Insight (OVPI)，则可将 OVPI 中的自定义报告包采集迁移到 NNMi。OVPI 采集迁移后，可用于 NNMi 自定义轮询器功能。

通过使用 SNMP MIB 表达式指定 NNMi 应轮询的其他信息，NNMi 自定义轮询器功能使您能够对网络管理采取主动操作。

自定义轮询器采集定义要收集(轮询)的信息以及 NNMi 如何对收集的数据作出反应。有关更多详细信息，请参阅 NNMi 帮助中的“创建自定义轮询器采集”和“配置自定义轮询”。另请参阅《HP Network Node Manager i Software Step-by-Step Guide to Custom Poller White Paper》。

备注: 使用这些步骤只能迁移 OVPI 中基于 SNMP 的自定义报告包采集。

要将与 OVPI 自定义报告包关联的 SNMP 采集迁移到 NNMi，请执行以下步骤：

1. 识别需要从 OVPI 迁移到 NNMi 的采集策略。
2. 使用 OVPI `collection_manager` 工具将采集策略从 OVPI 服务器导出到这些自定义报告包中。例如：

   备注: OVPI 服务器可以是远程轮询器或运行采集的卫星服务器。

   ```
   collection_manager -export <文件名>
   ```

   有关详细信息，请参阅 `collection_manager` 参考页。
3. 采集 NNMi 自定义轮询器采集所需的其他信息。可使用以下任一方法向 `nnmmigrateovpli.ovpl` 命令提供此信息：

   将单个 TEEL 文件的信息指定为 `nnmmigrateovpi.ovpl` 命令行参数。例如：

   ```
   nnmmigrateovpi.ovpl –policyName myPolicy –teelFile /tmp/OVPI/myTeel.TEEL
   –pollInterval 300 –nodeGroup myNodeGroup
   ```

   使用 -policyFile 参数将一个策略文件中的多个 TEEL 文件指定到 `nnmmigrateovpi.ovpl` 命令。例如：

   ```
   nnmmigrateovpi.ovpl -policyFile  CP_policy_config.txt   -teelDir /tmp/OVPI
   -batchFile generated_CP_commands.txt
   ```

   导出的 OVPI 采集策略文件包含以下列：`policy_name`、`table_name`、`poll_interval`、`datapipe_name`、`poll_from`、`user_name`、`server_name`、`group`、`group_server`、`desc`

   下表显示了此导出信息是如何与 `nnmmigrateovpi.ovpl` 命令中的必需信息相关的：

OVPI 采集策略文件列	nnmmigrate.ovpl 中的必填字段
policy_name	策略名称

(续)

OVPI 采集策略文件列	nnmmigrate.ovpl 中的必填字段
table_name	TEEL 文件名
poll_interval	轮询间隔
group	节点组

要提取 OVPI 采集策略文件的信息，请使用以下 Linux 命令：

```
cut -f1,2,3,8 -d','  ovpi_collection_policy.txt > CP_policy_config.txt
```

其中 ovi_collection_policy.txt 是示例导出 OVPI 采集策略文件的名称，CP_policy_config.txt 是用作 nnmcustompollerconfig.ovpl 命令输入的示例策略文件 (<策略文件>) 的名称。

4. 检查导出 OVPI 采集策略文件的内容。检查内容时，请注意以下事项：
   - 假定 OVPI 导出采集策略中的 table_name 字段与不带 teel 扩展名的 TEEL 文件名相同。如果 TEEL 文件名与 table_name 不同，则需要手动编辑文件，使 table_name 与 TEEL 文件名匹配。
   - 组名称可能不与 NNMi 中的节点组对应。如果这些名称不匹配，请执行以下任一操作：
     - 将信息指定到迁移命令时，更改此组名称，使之与 NNMi 节点组名称匹配。
     - 创建与导出的组名称匹配的节点组。
5. 找到 OVPI 采集策略中使用的 TEEL 文件。
6. 将 TEEL 文件复制到 NNMi 系统上的临时位置。
7. 使用 nnmmigrateovpi.ovpl 生成支持使用 TEEL 文件中包含的数据配置自定义轮询器采集的必要命令。

   提示: 可以使用 nnmmigrateovpi.ovpl 迁移单个或多个 TEEL 文件。

   有关详细信息，请参阅 nnmmigrateovpi.ovpl 参考页。

   警告: 生成的自定义轮询器配置命令中的某些字段使用默认值。如果需要，可修改这些字段以符合您的要求。有关详细信息，请参阅 nnmmigrateovpi.ovpl 参考页。

以下步骤描述了使用 nnmmigrateovpi.ovpl 命令迁移多个采集的示例。此示例假定您已按照之前步骤所述创建并检查了导出 OVPI 采集策略文件的内容。

1. 运行 nnmmigrateovpi.ovpl 命令：

   ```
   nnmmigrateovpi.ovpl -policyFile  <文件名>   -teelDir <TEEL 文件
   所在目录> [ -batchFile <生成的命令写入的文件名>]
   ```

   例如：

   ```
   nnmmigrateovpi.ovpl -policyFile  CP_policy_config.txt   -teelDir /tmp/OVPI
   -batchFile generated_CP_commands.txt
   ```

2. 通过如下 NNMi 自定义轮询器配置命令 nnmcustompollerconfig.ovpl 使用新批文件：

```
nnmcustompollerconfig.ovpl  -batch <批处理命令文件>
```

例如：

```
nnmcustompollerconfig.ovpl  -batch generated_CP_commands.txt
```

NNMi 使用批处理命令文件中包含的配置信息创建自定义轮询器采集。

3. 要从 NNMi 控制台查看这些自定义轮询器采集，请执行以下操作：
   a. 导航到**配置**工作区。
   b. 单击展开**监视**。
   c. 选择**自定义轮询器配置**。
   d. 导航到**自定义轮询器采集**选项卡。
      您将看到已创建的自定义轮询器采集的列表。

附录 A: 更多信息

本部分包含以下附录：

- 手动为 NNMi 配置应用程序故障转移 (第 406 页)
- NNMi 环境变量 (第 409 页)
- NNMi 和 NNM iSPI 默认端口 (第 412 页)
- 配置问题疑难解答 (第 452 页)

手动为 NNMi 配置应用程序故障转移

此附录中包含的步骤提供使用 NNMi 群集设置向导配置应用程序故障转移的备选方法。

备注: 如果在将 Oracle 作为数据库时使用应用程序故障转移，则必须遵循此附录中的配置步骤，包括以下先决条件操作：

必须使用“辅助服务器安装”选项来安装备用服务器。如果将备用服务器作为主服务器安装，请卸载该服务器并使用“辅助服务器安装”选项重新安装。

卸载 NNMi 之前，以相反顺序删除所有 NNMi 补丁程序，从最新的补丁程序开始。补丁程序删除过程会因 NNMi 管理服务器上运行的操作系统而异。有关安装和删除说明，请参阅补丁程序文档。

要手动配置应用程序故障转移，请执行以下步骤：

1. 在两个节点上运行 **ovstop**。
2. 用 `nms-cluster.properties` 文件中包含的详细说明，配置服务器 X(活动)和服务器 Y(备用)的应用程序故障转移功能。使用以下过程：

   备注: 编辑在以下步骤中表示取消文件中文本块内代码行的注释并修改文本。

   a. 编辑以下文件：
      - Windows：`%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
      - Linux：`$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`

   b. 声明 NNMi 群集的唯一名称。配置活动和备用服务器时，使用相同名称。

      ```
      com.hp.ov.nms.cluster.name=MyCluster
      ```

   c. 将群集中所有节点的主机名添加到 nms-cluster.properties 文件中的 `com.hp.ov.nms.cluster.member.hostnames` 参数：

      ```
      com.hp.ov.nms.cluster.member.hostnames = fqdn_for_active, fqdn_for_standby
      ```

> **备注:** 在 NNMi 9.0x 中，应用程序故障转移功能支持可自动发现网络上的群集主机的 UDP 解决方案。从 NNMi 9.2x 开始，HP 取消了 UDP 解决方案，仅支持 TCP 解决方案。如果从 NNMi 9.0x 迁移，必须完成步骤 c 来定义群集主机名，应用程序故障转移才能起作用。

d. 可选。在 `nms-cluster.properties` 文件中定义其他 com.hp.ov.nms.cluster* 参数。遵循 `nms-cluster.properties` 文件中包含的说明来修改每个参数

> **备注:** 如果在将 Oracle 作为数据库时使用应用程序故障转移，则 NNMi 忽略 `nms-cluster.properties` 文件中包含的数据库参数。

3. 根据所采取的方法，完成在应用程序故障转移环境中使用证书 (第 263 页)中指示的操作。

> **警告:** 配置应用程序故障转移功能时，必须将两个节点的 `nnm.keystore` 和 `nnm.truststore` 文件内容合并到单个 `nnm.keystore` 和 `nnm.truststore` 文件中。必须选择方法并完成步骤 3 指示的一组操作

4. 将以下文件从服务器 X 复制到服务器 Y：
   - Windows：

     `%NnmDataDir%\shared\nnm\conf\nnmcluster\cluster.keystore`

   - Linux：

     `$NnmDataDir/shared/nnm/conf/nnmcluster/cluster.keystore`

5. 在服务器 X 和服务器 Y 上运行以下命令：**nnmcluster**
   两个服务器都应当显示如下所示的信息：

```
============================== Current cluster state ==============================

State ID:000000001000000005

Date/Time:15 Mar 2011 - 09:37:58 (GMT-0600)

Cluster name:ThisCluster (key CRC:626,187,650)

Automatic failover:已启用

NNM database type:嵌入式

NNM configured ACTIVE node is:NO_ACTIVE

NNM current ACTIVE node is:NO_ACTIVE

Cluster members are:

  Local?    NodeType  State                    OvStatus     Hostname/Address

  ------    --------  -----                    --------     ----------------------------

* REMOTE    ADMIN     n/a                      n/a
serverX.xxx.yyy.yourcompany.com/16.78.61.68:7800
```

```
  (SELF)    ADMIN     n/a                        n/a
serverY.xxx.yyy.yourcompany.com/16.78.61.71:7800
```

显示信息中应当同时列出服务器 X 和服务器 Y。如果不显示有关这两个节点的信息，则表明它们没有相互通信。以下是继续前需要检查和更正的事项：

- 服务器 X 和服务器 Y 上的群集名称可能不同。
- 服务器 X 和服务器 Y 上的密钥 CRC 可能不同。在服务器 X 和服务器 Y 上检查以下文件的内容：

  Windows：`%NnmDataDir%\shared\nnm\conf\nnmcluster\cluster.keystore`

  Linux：`$NnmDataDir/shared/nnm/conf/nnmcluster/cluster.keystore`
- 服务器 X 或服务器 Y 上的防火墙可能阻止节点通信。
- 确保已合并 `nnm.keystore` 和 `nnm.truststore` 文件。在运行 **nnmcluster** 命令之后应该能看到显示此错误。
- 服务器 X 和服务器 Y 运行不同的操作系统。例如，假定服务器 X 运行 Linux 操作系统，服务器 Y 运行 Windows 操作系统。在运行 **nnmcluster** 命令之后应该能看到显示此错误。
- 服务器 X 和服务器 Y 运行不同 NNMi 版本。例如，假定服务器 X 运行 NNMi 10.01，服务器 Y 运行 NNMi 10.01 Patch 1(可用后)。在运行 **nnmcluster** 命令之后应该能看到显示此错误。

6. 在服务器 X 上启动 NNMi 群集管理器：

   `nnmcluster -daemon`

   > **备注:** 在 NNMi 管理服务器 X 上运行 **nnmcluster -daemon** 命令之后，NNMi 群集管理器完成以下启动例程：
   >
   > - 将 NNMi 管理服务器 X 连接到群集。
   > - 检测以确认没有其他 NNMi 管理服务器存在。
   > - NNMi 管理服务器 X 假定为活动状况。
   > - 在 NNMi 管理服务器 X(活动服务器)上启动 NNMi 服务。
   > - 创建数据库备份。
   >
   > 有关详细信息，请参阅 nnmcluster 参考页或 Linux 联机帮助页。

7. 等待几分钟，让服务器 X 成为群集中的第一个主动节点。在服务器 X 上运行 **nnmcluster -display** 命令，并在显示结果中搜索术语 `ACTIVE`，就像在 `ACTIVE_NNM_STARTING` 或 `ACTIVE_SomeOtherState` 中一样。不要继续执行步骤 8，除非您知道服务器 X 是活动节点。
8. 在服务器 Y 上，启动 NNMi 群集管理器：

   `nnmcluster -daemon`

   > **备注:** 在 NNMi 管理服务器 Y 上运行 **nnmcluster -daemon** 命令之后，NNMi 群集管理器完

成以下启动例程：

- 将 NNMi 管理服务器 Y 连接到群集。
- 检测以确认 NNMi 管理服务器 X 存在，并处于活动状况。屏幕会显示 STANDBY_INITIALIZING。
- 比较 NNMi 管理服务器 Y 上与 NNMi 管理服务器 X 上的数据库备份。如果两者不匹配，则将新数据库备份从 NNMi 管理服务器 X(活动)发送至 NNMi 管理服务器 Y(备用)。屏幕会显示 STANDBY_RECV_DBZIP。
- NNMi 管理服务器 Y 接收最小的一组事务日志，它们能满足使备份适用于其备用状况的最低需要。屏幕会显示 STANDBY_RECV_TXLOGS。
- NNMi 管理服务器 Y 进入等待状况，从 NNMi 管理服务器 X 连续接收新的事务日志和检测信号。屏幕会显示 STANDBY_READY。

有关详细信息，请参阅 nnmcluster 参考页或 Linux 联机帮助页。

9. 如果发生故障转移，则服务器 X 的 NNMi 控制台不再起作用。关闭服务器 X 的 NNMi 控制台会话，并登录到服务器 Y(新的活动服务器)。指示 NNMi 用户在其浏览器中存储两个书签，一个到服务器 X(活动 NNMi 管理服务器)，一个到服务器 Y(备用 NNMi 管理服务器)。如果发生故障转移，则用户可以连接到服务器 Y(备用 NNMi 管理服务器)。
10. 指示网络运营中心 (NOC) 人员将其设备配置将陷阱发送到服务器 X 和服务器 Y。服务器 X (活动)运行时，它处理转发的陷阱，且服务器 Y(备用)忽略转发的陷阱。

NNMi 环境变量

HP Network Node Manager i Software (NNMi) 提供很多可用的环境变量，可供在文件系统中导航和编写脚本时使用。

本附录包含以下主题：

- 本文档中使用的环境变量 (第 409 页)
- 其他可用的环境变量 (第 410 页)

本文档中使用的环境变量

此文档主要使用以下两个 NNMi 环境变量来引用文件和目录位置。此列表显示默认值。实际值取决于在 NNMi 安装期间所做的选择。

- Windows Server：
  - %NnmInstallDir%:<驱动器>\Program Files (x86)\HP\HP BTO Software
  - %NnmDataDir%:<驱动器>\ProgramData\HP\HP BTO Software

> **备注：** 在 Windows 系统上，NNMi 安装进程创建这些系统环境变量，因此它们始终对所有用户可用。

- Linux：
  - `$NnmInstallDir:/opt/OV`
  - `$NnmDataDir:/var/opt/OV`

> **备注：** 在 Linux 系统上，如果要使用它们，则必须手动创建这些环境变量。

另外，本文档引用一些 NNMi 环境变量，可以将这些环境变量用作 NNMi 管理服务器上用户登录配置的一部分。这些变量形式为 `NNM_*`。有关该 NNMi 环境变量扩展列表的信息，请参阅其他可用的环境变量 (第 410 页)。

其他可用的环境变量

NNMi 管理员定期访问某些 NNMi 文件位置。NNMi 提供的脚本可设置许多用于导航到经常访问位置的环境变量。

要设置 NNMi 环境变量的扩展列表，请使用类似以下示例的命令：

- Windows：`"C:\Program Files (x86)\HP\HP BTO Software\bin\nnm.envvars.bat"`
- Linux：`. /opt/OV/bin/nnm.envvars.sh`

运行操作系统命令之后，可以使用 Windows 操作系统的环境变量默认位置或 Linux 操作系统的环境变量默认位置中显示的 NNMi 环境变量，以到达常用的 NNMi 文件位置。

Windows 操作系统的环境变量默认位置

变量	Windows(示例)
%NNM_BIN%	C:\Program Files (x86)\HP\HP BTO Software\bin
%NNM_CONF%	C:\ProgramData\HP\HP BTO Software\conf
%NNM_DATA%	C:\ProgramData\HP\HP BTO Software\
%NNM_DB%	C:\ProgramData\HP\HP BTO Software\shared\nnm\databases
%NNM_JAVA%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jdk\hpsw\bin\java.exe
%NNM_JAVA_PATH_SEP%	;
%NNM_JRE%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jdk\hpsw
%NNM_LOG%	C:\ProgramData\HP\HP BTO Software\log
%NNM_LRF%	C:\ProgramData\HP\HP BTO Software\shared\nnm\lrf
%NNM_PRIV_LOG%	C:\ProgramData\HP\HP BTO Software\log

Windows 操作系统的环境变量默认位置(续)

变量	Windows(示例)
%NNM_PROPS%	C:\ProgramData\HP\HP BTO Software\shared\nnm\conf\props
%NNM_SHARED_CONF%	C:\ProgramData\HP\HP BTO Software\shared\nnm\conf
%NNM_SHARE_LOG%	C:\ProgramData\HP\HP BTO Software\log
%NNM_SNMP_MIBS%	C:\Program Files (x86)\HP\HP BTO Software\misc\nnm\snmp-mibs
%NNM_TMP%	C:\ProgramData\HP\HP BTO Software\tmp
%NNM_USER_SNMP_MIBS%	C:\ProgramData\HP\HP BTO Software\shared\nnm\user-snmp-mibs
%NNM_WWW%	C:\ProgramData\HP\HP BTO Software\shared\nnm\www

Linux 操作系统的环境变量默认位置

变量	Linux
$NNM_BIN	/opt/OV/bin
$NNM_CONF	/var/opt/OV/conf
$NNM_DATA	/var/opt/OV
$NNM_DB	/var/opt/OV/shared/nnm/databases
$NNM_JAVA	/opt/OV/nonOV/jdk/hpsw/bin/java
$NNM_JAVA_PATH_SEP	:
$NNM_JRE	/opt/OV/nonOV/jdk/nnm
$NNM_LOG	/var/opt/OV/log
$NNM_LRF	/var/opt/OV/shared/nnm/lrf
$NNM_PRIV_LOG	/var/opt/OV/log
$NNM_PROPS	/var/opt/OV/shared/nnm/conf/props
$NNM_SHARED_CONF	/var/opt/OV/shared/nnm/conf
$NNM_SHARE_LOG	/var/opt/OV/log
$NNM_SNMP_MIBS	/opt/OV/misc/nnm/snmp-mibs
$NNM_TMP	/var/opt/OV/tmp
$NNM_USER_SNMP_MIBS	/var/opt/OV/shared/nnm/user-snmp-mibs
$NNM_WWW	/var/opt/OV/shared/nnm/www

NNMi 和 NNM iSPI 默认端口

此附录显示 NNMi 和 NNM iSPI 进行网络通信时所用的默认端口。如果产品之间发生端口冲突，可如更改配置列中所示更改其中的多数端口号。

此外，后续主题记录了各个 HP 网络管理软件产品使用的端口。

- HP Network Node Manager i Software 端口 (第 413 页)
- NNM iSPI for MPLS 端口 (第 422 页)
- NNM iSPI for IP Telephony 端口 (第 426 页)
- NNM iSPI for IP Multicast 端口 (第 430 页)
- NNM iSPI Performance for Traffic 端口 (第 434 页)
- NNM iSPI Performance for QA 端口 (第 445 页)
- NNM iSPI Performance for Metrics 和 NPS 端口 (第 449 页)
- NNM iSPI NET 端口 (第 451 页)

HP Network Node Manager i Software 端口

NNMi 端口分为以下几类：

- 在 NNMi 管理服务器上使用的端口
- 用于 NNMi 管理服务器与其他系统之间通信的端口
- 全局网络管理要求可访问套接字

在 NNMi 管理服务器上使用的端口

下表显示了 NNMi 在管理服务器上使用的端口。NNMi 会侦听这些端口。如果发生端口冲突，可如更改配置列中所示更改其中的多数端口号。有关详细信息，请参阅 nnm.ports 参考页或 Linux 联机帮助页。

备注: 为使应用程序故障转移成功，请打开 TCP 端口 7800-7810。为使应用程序故障转移功能正常运行，活动和备用 NNMi 管理服务器必须能不受限制地通过网络访问彼此。

在 NNMi 管理服务器上使用的端口

端口	类型	名称	用途	更改配置
80	TCP	nmsas.server.port.web.http	默认 HTTP 端口 - 用于 Web UI 和 Web 服务 - 在 GNM 配置中，NNMi 使用此端口建立从全局管理器到区域管理器的通信 - 一旦此端口	修改 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。 还可以在安装期间更改此配置。

在 **NNMi** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
			打开，它就成为双向端口	
162	UDP	trapPort	SNMP 陷阱端口	使用 `nnmtrapconfig.ovpl` Perl 脚本修改。有关详细信息，请参阅 nnmtrapconfig.ovpl 参考页或 Linux 联机帮助页。
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 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。
1098	TCP	nmsas.server.port.naming.rmi	- 由 NNMi 命令行工具用于与 NNMi 使用的多种服务通信 - HP 建议配置系统防火墙以仅允许 localhost 访问这些端口	修改 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。
1099	TCP	nmsas.server.port.naming.port	- 由 NNMi 命令行工具用于与 NNMi 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	修改 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。

在 NNMi 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
			这些端口	
3873	TCP	nmsas.server.port.remoting.ejb3	- 由 NNMi 命令行工具用于与 NNMi 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 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。
4444	TCP	nmsas.server.port.jmx.jrmp	- 由 NNMi 命令行工具用于与 NNMi 使用的多种服务通信 - HP 建议配置系统防火墙以仅允许 localhost 访问这些端口	修改 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。
4445	TCP	nmsas.server.port.jmx.rmi	- 由 NNMi 命令行工具用于与 NNMi 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	修改 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。

在 **NNMi** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
			这些端口	
4446	TCP	nmsas.server.port.invoker.unified	- 由 NNMi 命令行工具用于与 NNMi 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 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。
4457	TCP	nmsas.server.port.hq	- 用于未加密的全局网络管理流量。 - 消息从全局管理器传递到区域管理器 - 一旦此端口打开，它就成为双向端口	修改 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。
4459	TCP	nmsas.server.port.hq.ssl	- 用于加密的全局网络管理流量。 - 消息从全局管理器传递到区域管理器 - 一旦此端口	修改 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。

在 NNMi 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
			打开，它就成为双向端口	
4712	TCP	nmsas.server.port.ts.recovery	内部事务服务端口	修改 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。
4713	TCP	nmsas.server.port.ts.status	内部事务服务端口	修改 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。
4714	TCP	nmsas.server.port.ts.id	内部事务服务端口	修改 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。
5432	TCP	com.hp.ov.nms.postgres.port	此 PostgreSQL 端口是嵌入式数据库用于侦听此 NNMi 管理服务器的端口。	修改 `%NNM_CONF%\nnm\props\nms-local.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-local.properties` 文件 (Linux)。
7800-7810	TCP		- 用于应用程序故障转移的 JGroups 端口 - 如果不使用应用程序故障转移，HP 建议配置系统防	修改 `%NNM_CONF%\nnm\props\nms-cluster.properties` 文件 (Windows) 或 `$NNM_CONF/nnm/props/nms-cluster.properties` 文件 (Linux)。

在 NNMi 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
			火墙以限制对这些端口的访问	
8886	TCP	OVsPMD_MGMT	NNMi ovspmd (进程管理器) 管理端口	修改 /etc/services 文件。
8887	TCP	OVsPMD_REQ	NNMi ovsmpd (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	操作服务器端口	修改 %NnmInstallDir%\misc\nnm\props\shared\nnmaction.properties 文件 (Windows) 或 $NnmInstallDir/misc/nnm/props/shared/nnmaction.properties 文件 (Linux)。

用于 NNMi 管理服务器与其他系统之间通信的端口

下表显示了 NNMi 用于和其他系统通信的部分端口。如果有防火墙将 NNMi 与这些系统分隔开来，则必须在防火墙中打开其中的多个端口。实际的端口组取决于您配置与 NNMi 一起使用的集成组以及如何配置那些集成。如果列 4 表示客户端，则 NNMi 连接或发送到此端口；如果列 4 表示服务器，则 NNMi 在此端口上侦听。

用于 NNMi 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
80	TCP	NNMi 的默认 HTTP 端口；用于 Web UI 和 Web 服务	服务器
80	TCP	NNMi 连接到其他应用程序的默认 HTTP 端口。实际端口取决于 NNMi 配置。	客户端

用于 NNMi 管理服务器与其他系统之间通信的端口(续)

端口	类型	用途	客户端，服务器
161	UDP	SNMP 请求端口	客户端
162	UDP	SNMP 陷阱端口 - NNMi 接收的陷阱	服务器
162	UDP	SNMP 陷阱端口；陷阱转发、Northbound 接口或 NetCool 集成	客户端
389	TCP	默认 LDAP 端口	客户端
395	UDP	nGenius Probe SNMP 陷阱端口	客户端
443	TCP	NNMi 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 NNMi 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	默认的安全 LDAP 端口 (SSL)	客户端
1741	TCP	默认的 CiscoWorks LMS Web 服务端口	客户端
4457	TCP	用于未加密的全局网络管理流量。连接从全局管理器到区域管理器。	客户端，服务器
4459	TCP	用于加密的全局网络管理流量。连接从全局管理器到区域管理器。	客户端，服务器
7800-7810	TCP	用于应用程序故障转移的 JGroups 端口	客户端和服务器
8004	TCP	NNMi 的默认 HTTP 端口(如果另一个 Web 服务器已占用端口 80)。用于 Web UI 和 Web 服务。为 NNMi 管理服务器验证实际 HTTP 端口。	服务器
8080	TCP	如果和 NNMi 安装在相同的系统上，则为连接到 NA 的默	客户端

用于 NNMi 管理服务器与其他系统之间通信的端口(续)

端口	类型	用途	客户端，服务器
		认 HTTP 端口。 HP UCMDB Web 服务的默认 HTTPS 端口	
8443 或 8444	TCP	连接到 HP OM for UNIX 的默认 HTTP 端口	客户端
9300	TCP	连接到 NNM iSPI Performance for Metrics 的默认 HTTP 端口	客户端
50000	TCP	连接到 SIM 的默认 HTTPS 端口	客户端

备注: 如果将 NNMi 配置为使用 ICMP 故障轮询或 Ping 扫描进行发现，则将防火墙配置为使 ICMP 包通过防火墙。

备注: NNMi-HP OM 集成的 Web 服务途径不能通过防火墙工作，但使用 Northbound 接口的 NNMi-HP OM 集成能通过防火墙工作。

全局网络管理要求可访问套接字

下表显示需能从全局 NNMi 管理服务器访问区域 NNMi 管理服务器的已知端口。全局网络管理功能要求为 TCP 打开这些端口，以便能从全局 NNMi 管理服务器访问区域 NNMi 管理服务器。区域 NNMi 管理服务器不会打开返回到全局 NNMi 管理服务器的套接字。

全局网络管理要求可访问套接字

安全	参数	TCP 端口
非 SSL	nmsas.server.port.web.http	80
	nmsas.server.port.hq	4457

全局网络管理要求可访问套接字(续)

安全	参数	TCP 端口
SSL	nmsas.server.port.web.https	443
	nmsas.server.port.hq.ssl	4459

NNM iSPI for MPLS 端口

下表显示了 HP Network Node Manager iSPI for MPLS Software 在管理服务器上使用的端口。如果端口冲突，几乎所有这些端口号都可以使用以下位置中的 server.properties 文件进行更改：`%NnmDataDir%/nmsas/mpls/server.properties`。

在 HP Network Node Manager iSPI for MPLS Software 管理服务器上使用的端口

端口	类型	名称	用途	更改配置
5432	TCP	com.hp.ov.nms.postgres.port	此 PostgreSQL 端口是嵌入式数据库用于侦听此 NNMi 管理服务器的端口。此端口应是在 nms-local.properties 文件中为 NNMi 配置的相同端口。	N/A
24040	TCP	nmsas.server.port.web.http	默认 HTTP 端口 - 用于 Web UI。	修改 `%NnmDataDir%\nmsas\mpls\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/mpls/server.properties` 文件 (Linux)。还可以在安装期间更改此配置。
24041	TCP	nmsas.server.port.remoting.ejb3	默认 EJB3 远程连接器端口	修改 `%NnmDataDir%\nmsas\mpls\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/mpls/server.properties` 文件 (Linux)。

在 **HP Network Node Manager iSPI for MPLS Software** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
24043	TCP	nmsas.server.port.web.https	默认安全 HTTPS 端口 (SSL) - 用于 Web UI。	修改 `%NnmDataDir%\nmsas\mpls\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/mpls/server.properties` 文件 (Linux)。还可以在安装期间更改此配置。
24044	TCP	nmsas.server.port.jmx.jrmp	默认 RMI 对象端口(JRMP 调用程序)	修改 `%NnmDataDir%\nmsas\mpls\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/mpls/server.properties` 文件 (Linux)。
24045	TCP	nmsas.server.port.invoker.unified	默认 RMI 远程服务器连接器端口	修改 `%NnmDataDir%\nmsas\mpls\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/mpls/server.properties` 文件 (Linux)。
24046	TCP	nmsas.server.port.naming.port	默认启动 JNP 服务端口(JNDI 提供程序)	修改 `%NnmDataDir%\nmsas\mpls\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/mpls/server.properties` 文件 (Linux)。还可以在安装期间更改此配置。
24047	TCP	nmsas.server.port.hq	用于未加密的全局网络管理流量。	修改 `%NnmDataDir%\nmsas\mpls\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/mpls/server.properties` 文件 (Linux)。

在 **HP Network Node Manager iSPI for MPLS Software** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
24048	TCP	nmsas.server.port.jmx.rmi	默认 RMI 池调用程序端口	修改 `%NnmDataDir%\nmsas\mpls\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/mpls/server.properties` 文件 (Linux)。
24049	TCP	nmsas.server.port.naming.rmi	RMI 命名服务的默认端口	修改 `%NnmDataDir%\nmsas\mpls\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/mpls/server.properties` 文件 (Linux)。
24092	TCP	nmsas.server.port.hq.ssl	用于加密的全局网络管理流量。	修改 `%NnmDataDir%\nmsas\mpls\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/mpls/server.properties` 文件 (Linux)。
24712	TCP	nmsas.server.port.ts.recovery	事务服务使用的默认恢复端口。	修改 `%NnmDataDir%\nmsas\mpls\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/mpls/server.properties` 文件 (Linux)。
24713	TCP	nmsas.server.port.ts.status	事务服务使用的默认状态端口。	修改 `%NnmDataDir%\nmsas\mpls\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/mpls/server.properties` 文件 (Linux)。
24714	TCP	nmsas.server.port.ts.id	事务服务使用的默认端口。	修改 `%NnmDataDir%\nmsas\mpls\server.p`

在 **HP Network Node Manager iSPI for MPLS Software** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
				roperties 文件 (Windows) 或 $NnmDataDir/nmsas/mpls/server.properties 文件 (Linux)。

NNM iSPI for IP Telephony 端口

下表显示了 NNM iSPI for IP Telephony 在管理服务器上使用的端口。如果端口冲突，几乎所有这些端口号都可以使用以下位置中的 `server.properties` 文件进行更改：`%NnmDataDir%/nmsas/ipt/server.properties`。

在 NNM iSPI for IP Telephony 管理服务器上使用的端口

端口	类型	名称	用途	更改配置
5432	TCP	com.hp.ov.nms.postgres.port	此 PostgreSQL 端口是嵌入式数据库用于侦听此 NNMi 管理服务器的端口。此端口应是在 nms-local.properties 文件中为 NNMi 配置的相同端口。	N/A
10080	TCP	nmsas.server.port.web.http	默认 HTTP 端口 - 用于 Web UI。	修改 `%NnmDataDir%\nmsas\ipt\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/ipt/server.properties` 文件 (Linux)。还可以在安装期间更改此配置。
10083	TCP	nmsas.server.port.naming.rmi	RMI 命名服务的默认端口	修改 `%NnmDataDir%\nmsas\ipt\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/ipt/server.properties` 文件 (Linux)。
10084	TCP	nmsas.server.port.jmx.jrmp	默认 RMI 对象	修改

在 **NNM iSPI for IP Telephony** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
			端口(JRMP 调用程序)	%NnmDataDir%\nmsas\ipt\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/ipt/server.properties 文件 (Linux)。
10085	TCP	nmsas.server.port.jmx.rmi	默认 RMI 池调用程序端口	修改 %NnmDataDir%\nmsas\ipt\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/ipt/server.properties 文件 (Linux)。
10086	TCP	nmsas.server.port.invoker.unified	默认 RMI 远程服务器连接器端口	修改 %NnmDataDir%\nmsas\ipt\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/ipt/server.properties 文件 (Linux)。
10087	TCP	nmsas.server.port.hq	用于未加密的全局网络管理流量。	修改 %NnmDataDir%\nmsas\ipt\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/ipt/server.properties 文件 (Linux)。
10089	TCP	nmsas.server.port.remoting.ejb3	默认 EJB3 远程连接器端口	修改 %NnmDataDir%\nmsas\ipt\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/ipt/server.properties 文件 (Linux)。
10092	TCP	nmsas.server.port.hq.ssl	用于加密的全局网络管理流量。	修改 %NnmDataDir%\nmsas\ipt\server.properties 文件 (Windows) 或

在 **NNM iSPI for IP Telephony** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
				`$NnmDataDir/nmsas/ipt/server.properties` 文件 (Linux)。
10099	TCP	nmsas.server.port.naming.port	默认启动 JNP 服务端口(JNDI 提供程序)	修改 `%NnmDataDir%\nmsas\ipt\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/ipt/server.properties` 文件 (Linux)。还可以在安装期间更改此配置。
10443	TCP	nmsas.server.port.web.https	默认安全 HTTPS 端口 (SSL) - 用于 Web UI。	修改 `%NnmDataDir%\nmsas\ipt\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/ipt/server.properties` 文件 (Linux)。还可以在安装期间更改此配置。
14712	TCP	nmsas.server.port.ts.recovery	事务服务使用的默认恢复端口。	修改 `%NnmDataDir%\nmsas\ipt\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/ipt/server.properties` 文件 (Linux)。
14713	TCP	nmsas.server.port.ts.status	事务服务使用的默认状态端口。	修改 `%NnmDataDir%\nmsas\ipt\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/ipt/server.properties` 文件 (Linux)。
14714	TCP	nmsas.server.port.ts.id	事务服务使用的默认端口。	修改 `%NnmDataDir%\nmsas\ipt\server.properties` 文件 (Windows) 或

在 **NNM iSPI for IP Telephony** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
				`$NnmDataDir/nmsas/ipt/server.properties` 文件 (Linux)。

NNM iSPI for IP Multicast 端口

下表显示了 NNM iSPI for IP Multicast 在管理服务器上使用的端口。如果端口冲突，几乎所有这些端口号都可以使用以下位置中的 `server.properties` 文件进行更改：`%NnmDataDir%/nmsas/multicast/server.properties`。

在 NNM iSPI for IP Multicast 管理服务器上使用的端口

端口	类型	名称	用途	更改配置
5432	TCP	com.hp.ov.nms.postgres.port	此 PostgreSQL 端口是嵌入式数据库用于侦听此 NNMi 管理服务器的端口。此端口应是在 nms-local.properties 文件中为 NNMi 配置的相同端口。	N/A
8084	TCP	nmsas.server.port.web.http	默认 HTTP 端口 - 用于 Web UI。	修改 `%NnmDataDir%\nmsas\multicast\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/multicast/server.properties` 文件 (Linux)。还可以在安装期间更改此配置。
14083	TCP	nmsas.server.port.naming.rmi	RMI 命名服务的默认端口	修改 `%NnmDataDir%\nmsas\multicast\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/multicast/server.properties` 文件 (Linux)。

在 **NNM iSPI for IP Multicast** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
14084	TCP	nmsas.server.port.jmx.jrmp	默认 RMI 对象端口(JRMP 调用程序)	修改 `%NnmDataDir%\nmsas\multicast\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/multicast/server.properties` 文件 (Linux)。
14085	TCP	nmsas.server.port.jmx.rmi	默认 RMI 池调用程序端口	修改 `%NnmDataDir%\nmsas\multicast\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/multicast/server.properties` 文件 (Linux)。
14086	TCP	nmsas.server.port.invoker.unified	默认 RMI 远程服务器连接器端口	修改 `%NnmDataDir%\nmsas\multicast\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/multicast/server.properties` 文件 (Linux)。
14087	TCP	nmsas.server.port.hq	用于未加密的全局网络管理流量。	修改 `%NnmDataDir%\nmsas\multicast\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/multicast/server.properties` 文件 (Linux)。
14089	TCP	nmsas.server.port.remoting.ejb3	默认 EJB3 远程连接器端口	修改 `%NnmDataDir%\nmsas\multicast\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/multicast/server.properties` 文件 (Linux)。
14092	TCP	nmsas.server.port.hq.ssl	用于加密的全局网络管理流	修改 `%NnmDataDir%\nmsas\multicast\server.p`

在 **NNM iSPI for IP Multicast** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
			量。	roperties 文件 (Windows) 或 $NnmDataDir/nmsas/multicast/server.properties 文件 (Linux)。
14099	TCP	nmsas.server.port.naming.port	默认启动 JNP 服务端口(JNDI 提供程序)	修改 %NnmDataDir%\nmsas\multicast\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/multicast/server.properties 文件 (Linux)。还可以在安装期间更改此配置。
14102	TCP	nmsas.server.port.ts.id	事务服务使用的默认端口。	修改 %NnmDataDir%\nmsas\multicast\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/multicast/server.properties 文件 (Linux)。
14103	TCP	nmsas.server.port.ts.recovery	事务服务使用的默认恢复端口。	修改 %NnmDataDir%\nmsas\multicast\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/multicast/server.properties 文件 (Linux)。
14104	TCP	nmsas.server.port.ts.status	事务服务使用的默认状态端口。	修改 %NnmDataDir%\nmsas\multicast\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/multicast/server.properties 文件 (Linux)。
14443	TCP	nmsas.server.port.web.https	默认安全 HTTPS 端口 (SSL) - 用于	修改 %NnmDataDir%\nmsas\multicast\server.properties 文件 (Windows) 或

在 **NNM iSPI for IP Multicast** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
			Web UI。	`$NnmDataDir/nmsas/multicast/server.properties` 文件 (Linux)。还可以在安装期间更改此配置。

NNM iSPI Performance for Traffic 端口

NNM iSPI Performance for Traffic 端口分为以下几类：

- 在 NNM iSPI Performance for Traffic 管理服务器(流量主组件)上使用的端口
- 在 NNM iSPI Performance for Traffic 管理服务器(流量叶组件)上使用的端口
- 用于 NNM iSPI Performance for Traffic 管理服务器与其他系统之间通信的端口

在 NNM iSPI Performance for Traffic 管理服务器(流量主组件)上使用的端口

下表显示了 NNM iSPI Performance for Traffic(流量主组件)在管理服务器上使用的端口。如果端口冲突，几乎所有这些端口号都可以使用以下位置中的 `server.properties` 文件进行更改：`%NnmDataDir%/nmsas/traffic-master/server.properties`。

在 NNM iSPI Performance for Traffic 管理服务器(流量主组件)上使用的端口

端口	类型	名称	用途	更改配置
5432	TCP	com.hp.ov.nms.postgres.port	此 PostgreSQL 端口是嵌入式数据库用于侦听此 NNMi 管理服务器的端口。此端口应是在 nms-local.properties 文件中为 NNMi 配置的相同端口	N/A
12080	TCP	nmsas.server.port.web.http	默认 HTTP 端口 - 用于 Web UI。	修改 `%NnmDataDir%\nmsas\traffic-master\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traff`

在 **NNM iSPI Performance for Traffic** 管理服务器(流量主组件)上使用的端口(续)

端口	类型	名称	用途	更改配置
				ic-master/server.properties 文件 (Linux)。还可以在安装期间更改此配置。
12043	TCP	nmsas.server.port.web.https	默认安全 HTTPS 端口 (SSL) - 用于 Web UI。	修改 %NnmDataDir%\nmsas\traffic-master\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/traffic-master/server.properties 文件 (Linux)。还可以在安装期间更改此配置。
12083	TCP	nmsas.server.port.naming.rmi	RMI 命名服务的默认端口	修改 %NnmDataDir%\nmsas\traffic-master\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/traffic-master/server.properties 文件 (Linux)。
12084	TCP	nmsas.server.port.jmx.jrmp	默认 RMI 对象端口 (JRMP 调用程序)	修改 %NnmDataDir%\nmsas\traffic-master\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/traff

在 **NNM iSPI Performance for Traffic** 管理服务器(流量主组件)上使用的端口(续)

端口	类型	名称	用途	更改配置
				ic-master/server.properties 文件 (Linux)。
12085	TCP	nmsas.server.port.jmx.rmi	默认 RMI 池调用程序端口	修改 %NnmDataDir%\nmsas\traffic-master\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/traffic-master/server.properties 文件 (Linux)。
12086	TCP	nmsas.server.port.invoker.unified	默认 RMI 远程服务器连接器端口	修改 %NnmDataDir%\nmsas\traffic-master\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/traffic-master/server.properties 文件 (Linux)。
12087	TCP	nmsas.server.port.hq	用于未加密的全局网络管理流量。	修改 %NnmDataDir%\nmsas\traffic-master\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/traffic-master/server.propertie

在 **NNM iSPI Performance for Traffic** 管理服务器(流量主组件)上使用的端口(续)

端口	类型	名称	用途	更改配置
				s 文件 (Linux)。
12089	TCP	nmsas.server.port.remoting.ejb3	默认 EJB3	修改 `%NnmDataDir%\nmsas\traffic-master\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traffic-master/server.properties` 文件 (Linux)。
12092	TCP	nmsas.server.port.hq.ssl	用于加密的全局网络管理流量。	修改 `%NnmDataDir%\nmsas\traffic-master\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traffic-master/server.properties` 文件 (Linux)。
12099	TCP	nmsas.server.port.naming.port	默认启动 JNP 服务端口(JNDI 提供程序)	修改 `%NnmDataDir%\nmsas\traffic-master\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traffic-master/server.properties` 文件 (Linux)。还可以在安装期间更改此配置。

在 **NNM iSPI Performance for Traffic** 管理服务器(流量主组件)上使用的端口(续)

端口	类型	名称	用途	更改配置
12712	TCP	nmsas.server.port.ts.recovery	事务服务使用的默认恢复端口。	修改 `%NnmDataDir%\nmsas\traffic-master\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traffic-master/server.properties` 文件 (Linux)。
12713	TCP	nmsas.server.port.ts.status	事务服务使用的默认状态端口。	修改 `%NnmDataDir%\nmsas\traffic-master\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traffic-master/server.properties` 文件 (Linux)。
12714	TCP	nmsas.server.port.ts.id	事务服务使用的默认端口。	修改 `%NnmDataDir%\nmsas\traffic-master\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traffic-master/server.properties` 文件 (Linux)。

在 NNM iSPI Performance for Traffic 管理服务器(流量叶组件)上使用的端口

下表显示了 NNM iSPI Performance for Traffic(流量叶组件)在管理服务器上使用的端口。如果端口冲突，几乎所有这些端口号都可以使用以下位置中的 `server.properties` 文件进行更改：`%NnmDataDir%/nmsas/traffic-leaf/server.properties`。

在 NNM iSPI Performance for Traffic 管理服务器(流量叶组件)上使用的端口

端口	类型	名称	用途	更改配置
5432	TCP	com.hp.ov.nms.postgres.port	此 PostgreSQL 端口是嵌入式数据库用于侦听此 NNMi 管理服务器的端口。此端口应是在 nms-local.properties 文件中为 NNMi 配置的相同端口。	N/A
11080	TCP	nmsas.server.port.web.http	默认 HTTP 端口 - 用于 Web UI。	修改 `%NnmDataDir%\nmsas\traffic-leaf\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traffic-leaf/server.properties` 文件 (Linux)。还可以在安装期间更改此配置。
11043	TCP	nmsas.server.port.web.https	默认安全 HTTPS 端口 (SSL) - 用于 Web UI。	修改 `%NnmDataDir%\nmsas\traffic-leaf\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traff`

在 **NNM iSPI Performance for Traffic** 管理服务器(流量叶组件)上使用的端口(续)

端口	类型	名称	用途	更改配置
				ic-leaf/server.properties 文件 (Linux)。还可以在安装期间更改此配置。
11083	TCP	nmsas.server.port.naming.rmi	RMI 命名服务的默认端口	修改 %NnmDataDir%\nmsas\traffic-leaf\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/traffic-leaf/server.properties 文件 (Linux)。
11084	TCP	nmsas.server.port.jmx.jrmp	默认 RMI 对象端口(JRMP 调用程序)	修改 %NnmDataDir%\nmsas\traffic-leaf\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/traffic-leaf/server.properties 文件 (Linux)。
11085	TCP	nmsas.server.port.jmx.rmi	默认 RMI 池调用程序端口	修改 %NnmDataDir%\nmsas\traffic-leaf\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/traffic-

在 **NNM iSPI Performance for Traffic** 管理服务器(流量叶组件)上使用的端口(续)

端口	类型	名称	用途	更改配置
				leaf/server.properties 文件 (Linux)。
11086	TCP	nmsas.server.port.invoker.unified	默认 RMI 远程服务器连接器端口	修改 %NnmDataDir%\nmsas\traffic-leaf\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/traffic-leaf/server.properties 文件 (Linux)。
11087	TCP	nmsas.server.port.hq	用于未加密的全局网络管理流量。	修改 %NnmDataDir%\nmsas\traffic-leaf\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/traffic-leaf/server.properties 文件 (Linux)。
11089	TCP	nmsas.server.port.remoting.ejb3	默认 EJB3 远程连接器端口	修改 %NnmDataDir%\nmsas\traffic-leaf\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/traffic-leaf/server.properties 文件 (Linux)。

在 **NNM iSPI Performance for Traffic** 管理服务器(流量叶组件)上使用的端口(续)

端口	类型	名称	用途	更改配置
11092	TCP	nmsas.server.port.hq.ssl	用于加密的全局网络管理流量。	修改 `%NnmDataDir%\nmsas\traffic-leaf\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traffic-leaf/server.properties` 文件 (Linux)。
11099	TCP	nmsas.server.port.naming.port	默认启动 JNP 服务端口(JNDI 提供程序)	修改 `%NnmDataDir%\nmsas\traffic-leaf\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traffic-leaf/server.properties` 文件 (Linux)。还可以在安装期间更改此配置。
11712	TCP	nmsas.server.port.ts.recovery	事务服务使用的默认恢复端口。	修改 `%NnmDataDir%\nmsas\traffic-leaf\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traffic-leaf/server.properties` 文件 (Linux)。

在 **NNM iSPI Performance for Traffic** 管理服务器(流量叶组件)上使用的端口(续)

端口	类型	名称	用途	更改配置
11713	TCP	nmsas.server.port.ts.status	事务服务使用的默认状态端口。	修改 `%NnmDataDir%\nmsas\traffic-leaf\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traffic-leaf/server.properties` 文件 (Linux)。
11714	TCP	nmsas.server.port.ts.id	事务服务使用的默认端口。	修改 `%NnmDataDir%\nmsas\traffic-leaf\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/traffic-leaf/server.properties` 文件 (Linux)。

用于 NNM iSPI Performance for Traffic 管理服务器与其他系统之间通信的端口

下表显示了 NNM iSPI Performance for Traffic 用于和其他系统通信的部分端口。如果有防火墙将 NNM iSPI Performance for Traffic 与这些系统分隔开，则必须在防火墙中打开其中的多个端口。实际的端口组取决于您配置与 NNM iSPI Performance for Traffic 一起使用的集成组以及如何配置那些集成。如果列 4 表示客户端，则 NNM iSPI Performance for Traffic 将连接或发送到此端口；如果列 4 表示服务器，则 NNM iSPI Performance for Traffic 将侦听此端口。

管理服务器与其他系统之间进行通信所用的端口

端口	类型	用途	客户端或服务器
任何可用端口	TCP	Avaya 流	服务器
任何可用端口	TCP	RTCP 服务器	服务器
22	TCP	Cisco/Avaya SSH 通信	客户端
22/23	TCP	Cisco FTP/SFTP 通信	服务器
23	TCP	Avaya Survivable 通信	客户端
8000(可配置)	TCP	.NET 代理(IPT 附带)	客户端
8443	TCP	Cisco AXL 通信	客户端

NNM iSPI Performance for QA 端口

下表显示了 NNM iSPI Performance for QA 在管理服务器上使用的端口。如果端口冲突，几乎所有这些端口号都可以使用以下位置中的 `server.properties` 文件进行更改：`%NnmDataDir%/nmsas/qa/server.properties`。

在 NNM iSPI Performance for QA 管理服务器上使用的端口

端口	类型	名称	用途	更改配置
5432	TCP	com.hp.ov.nms.postgres.port	此 PostgreSQL 端口是嵌入式数据库用于侦听此 NNMi 管理服务器的端口。此端口应是在 nms-local.properties 文件中为 NNMi 配置的相同端口。	N/A
54040	TCP	nmsas.server.port.web.http	默认 HTTP 端口 - 用于 Web UI。	修改 `%NnmDataDir%\nmsas\qa\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/qa/server.properties` 文件 (Linux)。还可以在安装期间更改此配置。
54041	TCP	nmsas.server.port.remoting.ejb3	用于调用远程 ejb 调用。	修改 `%NnmDataDir%\nmsas\qa\server.properties` 文件 (Windows) 或 `$NnmDataDir/nmsas/qa/server.properties` 文件 (Linux)。
54043	TCP	nmsas.server.port.web.https	默认安全	修改

在 **NNM iSPI Performance for QA** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
			HTTPS 端口 (SSL) - 用于 Web UI。	%NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。还可以在安装期间更改此配置。
54045	TCP	nmsas.server.port.invoker.unified	由 jboss 远程服务使用。	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。
54046	TCP	nmsas.server.port.naming.port	默认启动 JNP 服务端口(JNDI 提供程序)	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。还可以在安装期间更改此配置。
54047	TCP	nmsas.server.port.hq	用于未加密的全局网络管理流量。	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。
54048	TCP	nmsas.server.port.jmx.rmi	默认 RMI 池调用程序端口	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。
54049	TCP	nmsas.server.port.naming.rmi	RMI 命名服务的	修改

在 **NNM iSPI Performance for QA** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
			默认端口	%NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。
54084	TCP	nmsas.server.port.jmx.jrmp	默认 RMI 对象端口(JRMP 调用程序)	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。
54086	TCP	nmsas.server.port.invoker.unified	默认 RMI 远程服务器连接器端口	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。
54087	TCP	nmsas.server.port.hq	用于未加密的全局网络管理流量。	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。
54088	TCP	nmsas.server.port.hq.ssl	用于加密的全局网络管理流量。	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。
54089	TCP	nmsas.server.port.remoting.ejb3	默认 EJB3 远程连接器端口	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或

在 **NNM iSPI Performance for QA** 管理服务器上使用的端口(续)

端口	类型	名称	用途	更改配置
				$NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。
54092	TCP	nmsas.server.port.hq.ssl	用于加密的全局网络管理流量。	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。
54712	TCP	nmsas.server.port.ts.recovery	事务服务使用的默认恢复端口。	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。
54713	TCP	nmsas.server.port.ts.status	事务服务使用的默认状态端口。	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。
54714	TCP	nmsas.server.port.ts.id	事务服务使用的默认端口。	修改 %NnmDataDir%\nmsas\qa\server.properties 文件 (Windows) 或 $NnmDataDir/nmsas/qa/server.properties 文件 (Linux)。

NNM iSPI Performance for Metrics 和 NPS 端口

下表显示了 NNM iSPI Performance for Metrics 和 Network Performance Server (NPS) 所需的端口。如果端口冲突，几乎可以更改所有这些端口号。

备注: 如果 NNMi 和 NPS 不共存，则也需要用于操作系统网络文件共享的网络端口(在 Linux 上为 NFS 服务，在 Windows 上为 Windows 文件共享)。

NNM iSPI Performance for Metrics 和 NPS 所需的端口

端口	类型	名称	用途	更改配置
9300	TCP	NPS UI	默认 HTTP 端口 - 用于 Web UI 和 BI Web 服务。	使用 configureWebAccess.ovpl 更改。
9301	TCP	Sybase ASE	Sybase ASE(BI 内容管理器数据库)。由在同一服务器上运行的进程使用。	不支持更改。
9302	TCP	Sybase IQ Agent	Sybase IQ Agent 服务。由在同一服务器上运行的进程使用。	不支持更改。
9303	TCP	Sybase IQ - PerfSPI DB	用于存储所有 NPS ExtensionPack 数据的 Sybase IQ 数据库。由在同一服务器上运行的进程使用。	不支持更改。

NNM iSPI Performance for Metrics 和 NPS 所需的端口(续)

端口	类型	名称	用途	更改配置
9305	TCP	NPS UI - SSL	默认安全 HTTPS 端口 (SSL) - 用于 Web UI 和 BI Web 服务。	使用 configureWebAccess.ovpl 更改。
9306	TCP	数据库 SQL 重写代理 - PerfSPI DB	Perfspi 数据库的 SQL 重写代理 - 由 BI 服务器使用。由在同一服务器上运行的进程使用。	不支持更改。
9308	TCP	Sybase ASE 备份服务器	BI 内容管理器数据库的 Sybase ASE 备份服务器。由在同一服务器上运行的进程使用。	不支持更改。

NNM iSPI NET 端口

下表显示了由 NNM iSPI NET 诊断服务器 使用的端口。NNM iSPI NET 诊断服务器安装 HP Operations Orchestration (HP OO)。有关详细信息，请参阅《HP Operations Orchestration Administrator's Guide》。

由 NNM iSPI NET 诊断服务器使用的端口

端口	类型	名称	用途	更改配置
3306	TCP	MySQL 数据库端口	提供对 MySQL 数据库的访问。	不支持更改。
8080	TCP	jetty http 端口	默认 HTTP 端口 - 用于 Web UI 和 Web 服务。	不支持安装后修改。
8443	TCP	jetty SSL/https 端口	默认 HTTPS 端口 - 用于 Web UI 和 Web 服务。	不支持安装后修改。
9004	TCP	HP OO RAS 端口	提供对 HP OO Remote Action Service 的访问。	不支持更改。

配置问题疑难解答

本部分包含一些常见问题及其解决方法。

NNMi 不能始终正确解释和显示 SNMP 数据及 MIB 字符串

症状

这是因为 NNMi 并不始终知道用哪个字符集来解释此数据。结果是 NNMi 显示来自某些 SNMP 陷阱以及其他 octetstring 数据的乱码字符串，如 `sysDescription`、`sysContact` 以及其他数据。

解决方案

解决方案是使用正确字符集解释此数据。

对于因使用不正确的字符集而导致显示乱码文本的 SNMP 陷阱及其他 octetstring 数据，请执行以下操作：

1. 编辑以下文件：
   - Windows：`%NNM_PROPS%\nms-jboss.properties`
   - Linux：`$NNM_PROPS/nms-jboss.properties`
2. 从如下开头的行中删除注释(`#!`字符)：

   `#!com.hp.nnm.sourceEncoding=`
3. 使用 `nms-jboss.properties` 文件中显示的示例，将 `com.hp.nnm.sourceEncoding` JVM 属性设置为环境当前支持的源编码的逗号分隔列表。这些示例显示 Shift_JIS、EUC_JP、UTF-8 和 ISO-8859-1 字符集的组合。
4. 保存更改。
5. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 `ovstop` 命令

   在 NNMi 管理服务器上运行 `ovstart` 命令

   > **备注：**在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。
6. 要测试更改，请将可疑陷阱重新发送到 NNMi，并确保乱码显示问题不再发生。

   如果乱码文本包含二进制数据或出于任何原因无法解释的数据，请执行以下操作来将 NNMi 配置为以十六进制格式显示字符串：

   a. 打开以下文件：

      Windows：`%NNMDATADIR%\shared\nnm\conf\nnmvbnosrcenc.conf`

Linux：`$NNMDATADIR/shared/nnm/conf/nnmvbnosrcenc.conf`

b. 添加 NNMi 以乱码格式显示的陷阱 OID、varbind OID 值组合。同时添加您不希望 NNMi 解码的任何 varbind 值组合，如二进制数据。用 `nnmvbnosrcenc.conf` 文件中显示的示例作为模板来配置组合。该操作告诉 NNMi 在事件表单中使用十六进制值来显示自定义事件属性值。

c. 保存更改。

d. 重新启动 NNMi 管理服务器：

   在 NNMi 管理服务器上运行 `ovstop` 命令。

   在 NNMi 管理服务器上运行 `ovstart` 命令。

> **备注：**在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

e. 测试您的更改，确保这些更改将使得以前的乱码字符串以十六进制显示。

NNMi 图显示 Linux 服务器而不是 ESXi 服务器和节点

症状

已经在已启用 Net-SNMP 代理的 Linux 服务器上部署了 VMWARE。

解决方案

如果希望 NNMi 发现并显示 ESXi 服务器，必须完成 ESXi 服务器和节点的裸机安装。有关详细信息，请访问 http://www.vmware.com。

NNMi 图显示 ESXi 设备 No SNMP，而不是显示为 ESXi 设备

解决方案

必须安装并启用 ESXi SNMP 代理，NNMi 才能发现和映射 ESXi 服务器及节点。也许您卸载或禁用了 ESXi SNMP 代理。

解决方案

为解决此问题，请安装或启用 ESXi SNMP 代理。有关详细信息，请访问 http://www.vmware.com。

NNMi 图显示 ESXi 服务器以及在 ESXi 服务器上运行的虚拟机和服务器

症状

NNMi 显示云状符号连接的所有这些系统。只有当您不想在 NNMi 图上看到 ESXi 服务器(包括虚拟机和服务器)时，它才成为一个问题。

解决方案

如果不希望 NNMi 显示 ESXi 服务器(包括虚拟机和服务器)，请执行以下操作：

1. 打开 NNMi 控制台。
2. 转到显示要删除节点的拓扑图；删除表示 ESXi 服务器以及在其上运行的虚拟机和服务器的节点。
3. 单击**配置**工作区中的**发现配置**。
4. 单击**自动发现规则**选项卡。
5. 创建新的自动发现规则。
6. 在排序字段中输入相对较小的数字将赋予此规则较高的优先级。请勿选中发现包含的节点复选框。
7. 为此规则添加新的 IP 地址范围。
8. 对于表示 ESXi 服务器及其运行的虚拟机和服务器的节点，添加这些节点的单个 IP 地址或 IP 地址范围；然后将范围类型更改为被规则包含而不是被规则忽略。
9. 单击**保存并关闭**三次以保存您的工作。

> **备注:** NNMi 图显示 Linux 服务器而不是 ESXi 服务器和节点。

NNMi 图显示 ESXi 服务器以及在 ESXi 服务器上运行的虚拟机和服务器

症状

NNMi 显示云状符号连接的所有这些系统。只有当您不想在 NNMi 图上看到 ESXi 服务器(包括虚拟机和服务器)时，它才成为一个问题。

解决方案

如果不希望 NNMi 显示 ESXi 服务器(包括虚拟机和服务器)，请执行以下操作：

1. 打开 NNMi 控制台。
2. 转到显示要删除节点的拓扑图；删除表示 ESXi 服务器以及在其上运行的虚拟机和服务器的节点。
3. 单击**配置**工作区中的**发现配置**。
4. 单击**自动发现规则**选项卡。
5. 创建新的自动发现规则。
6. 在排序字段中输入相对较小的数字将赋予此规则较高的优先级。请勿选中发现包含的节点复选框。
7. 为此规则添加新的 IP 地址范围。
8. 对于表示 ESXi 服务器及其运行的虚拟机和服务器的节点，添加这些节点的单个 IP 地址或 IP 地址范围；然后将范围类型更改为被规则包含而不是被规则忽略。
9. 单击**保存并关闭**三次以保存您的工作。

备注: NNMi 图显示 Linux 服务器而不是 ESXi 服务器和节点。

NNMi 显示有关与主机(NNMi 管理服务器)不匹配的许可证密钥的消息

症状

如果有人安装了用与 NNMi 管理服务器的 IP 地址不匹配的 IP 地址创建的 NNMi 许可证密钥，则会发生这种情况。

解决方案

解决方案是删除无效的许可证密钥：

1. 在命令提示符处，输入以下命令，以打开 Autopass 用户界面：

   nnmlicense.ovpl NNM -gui
2. 在 Autopass 窗口的左边，单击**删除许可证密钥**。
3. 选择无效的许可证密钥。
4. 单击**删除**。

通过将 **NNM** 替换为受影响产品，对任何其他受影响的 NNMi 产品集成重复步骤 1 到步骤 4。例如，要使用与 NNM iSPI Network Engineering Toolset Software 相关的许可证，请通过以下命令打开 Autopass 用户界面：

nnmlicense.ovpl iSPI-NET -gui

有关许可的其他信息，请参阅许可 NNMi (第 252 页)。

对于某些使用 PAgP(端口聚合协议)的 Cisco 设备，如果故障链路属于端口聚合的一部分，则 NNMi 可能会认为该设备上的端口不再属于端口聚合的一部分

症状

这会导致 NNMi 不报告端口聚合的降级状况。

解决方案

从 NNMi 9.0x 补丁 4 开始，提供一项可帮助 NNMi 更好管理使用 PAgP 的 Cisco 设备的功能。您可以配置此 NNMi 功能，以尝试确定故障接口是否仍被配置为端口聚合的一部分。要启用此功能，请执行以下操作：

1. 打开以下文件：
   - Windows：`%NNM_PROPS%\nms-disco.properties`
   - Linux：`$NNM_PROPS/nms-disco.properties`
2. 查找 `enablePagpOperDownHeuristic` 条目，此条目与以下行类似：

   `#!com.hp.ov.nms.disco.enablePagpOperDownHeuristic=false`

   要启用 `enablePagpOperDownHeuristic`，对此行进行如下更改：

   `com.hp.ov.nms.disco.enablePagpOperDownHeuristic=true`

   > **备注:** 确保删除位于行开头的 **#!** 字符。
3. 重新启动 NNMi 管理服务器。
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

> **备注:** 在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop` 和 `ovstart` 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

我正在使用带 Oracle 数据库的 NNMi。我配置的大型节点组导致生成节点组图时出错

症状

如果如下配置 NNMi，就可能发生这种情况：

- 使用带 Oracle 数据库的 NNMi。
- 创建包含子节点组的顶层节点组。
- 任何子节点组都包含 1000 个或更多成员。
- 为这些节点组在**节点组图设置 -> 连接 -> 节点组连接**部分中选择以下任一选项或同时选择两者：
  - **节点到节点组**
  - **节点组到节点组**

解决方案

要对此进行补救，请将子节点组限制为少于 1000 个成员，或者对于这些节点组不选择**节点组图设置 -> 连接 -> 节点组连接**部分中的**节点到节点组**和/或**节点组到节点组**。

我意外地从 NNMi 管理服务器删除了 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 库

症状

可以在 NNMi 控制台中的 **SNMPv3 设置**表单中指定要用于与 SNMPv3 设备通信的隐私协议。仅当在 NNMi 管理服务器上安装 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 库后，AES-192、AES-256 和 TripleDES 协议才可供选择。

解决方案

如果您意外地删除了 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 库，并且需要使 NNMi 能够使用 AES-192、AES-256 和 TripleDES 隐私协议进行 SNMPv3 通信，请执行以下步骤：

1. 从适用于 Java 开发人员的“Oracle 技术网”网站下载 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 库。
2. 解压缩下载包，然后将 JAR 文件(`local_policy.jar` 和 `US_export_policy.jar`)复制到以下位置：
   - Windows：`%NnmInstallDir%\nonOV\jdk\nnm\jre\lib\security`
   - Linux：`$NnmInstallDir/nonOV/jdk/nnm/jre/lib/security`
3. 重新启动 NNMi 管理服务器：
   a. 在 NNMi 管理服务器上运行 **ovstop** 命令。
   b. 在 NNMi 管理服务器上运行 **ovstart** 命令。

备注：在高可用性 (HA) 下进行文件更改时，需要在群集中的两个节点上都进行更改。对于使用 HA 配置的 NNMi，如果更改要求停止并重新启动 NNMi 管理服务器，则必须在运行 `ovstop`

和 ovstart 命令之前将节点置于维护模式。有关详细信息，请参阅维护模式 (第 163 页)。

词汇表

A

account
在 NNMi 中，供用户或用户组访问 NNMi 的方式。NNMi 用户帐户在 NNMi 控制台中设置，并实现预定的用户角色。请参阅系统帐户和用户角色。

ARP 缓存
ARP（地址解析协议）缓存是将数据链路层（OSI 第 2 层）地址映射到网络层（OSI 第 3 层）地址的操作系统表。数据链路层地址通常是 MAC 地址，而网络层地址通常是 IP 地址。在基于规则的发现中，NNMi 在发现的节点上使用 ARP 缓存条目（以及其他技术）查找可对照当前发现规则检查的其他节点。

H

HA
在本指南中是指一种硬件和软件配置，在部分配置出现故障时提供不间断的服务。高可用性 (HA) 意味着该配置有冗余组件，即使某个组件出现故障，也能保证应用程序的持续运行。可将 NNMi 配置为支持若干商业上可用的 HA 解决方案之一。与应用程序故障转移相对应。

HA 资源组
在当今的高可用性环境中，如 HP ServiceGuard、Veritas Cluster Server 或 Microsoft 群集服务，应用程序表示为复合型资源，如应用程序自身、其共享文件系统和虚拟 IP 地址。资源由 HA 资源组组成，它表示在群集环境中运行的应用程序。

HP Network Node Manager i Software
一种 HP 软件产品（缩写为 NNMi），设计用于辅助网络管理及整合网络管理活动，包括进行中的网络节点发现、监视事件和网络故障管理。主要从 NNMi 控制台访问。

I

ICMP
Internet 协议组 (TCP/IP) 的核心协议之一。NNMi 使用 ICMP Ping 再辅以 SNMP 查询来进行状况轮询。

Internet 控制消息协议
Internet 协议组 (TCP/IP) 的核心协议之一。NNMi 使用 ICMP Ping 再辅以 SNMP 查询来进行状况轮询。

iSPI
I 系列中的 Smart Plug-in。NNM iSPI 为 NNMi 添加功能，包括特定技术（如 MPLS）或特定域（如网络工程）。

L

L2
参考多层通信模型（开放系统互连，OSI）的数据链路层。数据链路层在网络中跨物理链路移动数据。NNMi 第 2 层视图提供有关设备的物理连接的信息。

L3
参考多层通信模型（开放系统互连，OSI）的网络层。通过网络层可了解网络中相邻节点的地址、选择路由及服务质量。NNMi 第 3 层视图提供有关路由连接的信息。

M

MIB
SNMP 中有关被管网络的数据集合，以层次结构形式组织。管理信息库中的数

据对象是指被管设备的特征。NNMi 通过使用 MIB 数据对象(有时称为“MIB 对象”、“对象”或“MIB”) 对被管节点进行 SNMP 查询和从其接收 SNMP 陷阱，以此采集网络管理信息。

N

NNM 6.x/7.x 事件
一个 NNMi 术语，是指从较早的 NNM 管理工作站转发到 NNMi 的事件。NNMi 提供事件视图，可用于浏览 NNMi 从这些转发的事件生成的事件。

NNM iSPI
I 系列中的 Smart Plug-in。NNM iSPI 为 NNMi 添加功能，包括特定技术(如 MPLS) 或特定域(如网络工程) 。

NNMi
一种 HP 软件产品(缩写为 NNMi) ，设计用于辅助网络管理及整合网络管理活动，包括进行中的网络节点发现、监视事件和网络故障管理。主要从 NNMi 控制台访问。

NNMi 控制台
NNMi 用户界面。操作员和管理员用 NNMi 控制台执行 NNMi 中的网络管理任务。

O

OID
SNMP 中用于标识管理信息库数据对象的数字序列。OID 由用点分隔的数字组成，其中每个数字表示 MIB 层次结构中该层的特定数据对象。OID 是等价于 MIB 对象名称的数字表示，例如 MIB 对象名称 iso.org.dod.internet.mgmt.mib-2.bgp.bgpTraps.bgpEstablished 等价于其 OID 1.3.6.1.2.1.15.0.1。

ovstart 命令
启动 NNMi 所管理进程的命令。在命令提示符处调用。请参阅 ovstart 参考页或 UNIX 联机帮助页。

ovstatus 命令
报告 NNMi 所管理进程的当前状态的命令。可从 NNMi 控制台(工具 > NNMi 状态) 或命令提示符处调用。请参阅 ovstatus 参考页或 UNIX 联机帮助页。

ovstop 命令
停止 NNMi 所管理进程的命令。在命令提示符处调用。请参阅 ovstop 参考页或 UNIX 联机帮助页。

P

Ping 扫描
一种网络探测技术，将 ICMP ECHO 请求发送到多个 IP 地址，以确定将哪些地址分配给响应节点。在基于规则的发现中启用时，NNMi 可以在配置的 IP 地址范围内使用 Ping 扫描来查找其他节点。某些网络管理员会阻止 ICMP ECHO 请求，因为 Ping 扫描可能被用于拒绝服务攻击。

PostgreSQL
NNMi 默认情况下用来存储拓扑、事件和配置之类信息的开源关系数据库。NNMi 还可以配置为对其多数表使用 Oracle 而非 PostgreSQL。

R

RCA
在 NNMi 中，根源分析 (RCA) 是指 NNMi 用于判断网络问题根源的一类问题解决方法。在 NNMi 中，根源是找到相关问题症状即可解决的可处理问题。NNMi 以两种关键方式使用根源识别：通知用户可处理问题是什么，在根源问题解决后再显示次要问题的症状报告。根源的确定可能导致被管对象的状态更改和/

或生成根源事件。NNMi 如何使用 RCA 的示例场景：被管路由器出现故障，来自 NNMi 管理服务器的路由器另一端的被管节点无法再响应状况轮询查询。NNMi 用 RCA 确定状况轮询故障是次要问题症状。它将路由器故障报告为根源事件，并抑制禁止报告下游节点的问题症状，直到根源路由器故障得到解决。

S

SNMP
OSI 模型的应用层（第 7 层）的简单协议操作，通过它，远程用户可以检查或更改网络元素的管理信息。SNMP 是 NNMi 用于在被管节点上与代理进程交换网络管理信息的主导协议。NNMi 支持三个最常见的 SNMP 版本：SNMPv1、SNMPv2c 和 SNMPv3。

SNMP 陷阱
使用轮询（从 SNMP 代理请求响应）的网络管理是有利于简化的 SNMP 设计原则。但是，提供该协议也是用于将未请求消息从 SNMP 代理发送到 SNMP 管理器进程（在此案例中为 NNMi）的通信。未请求的代理消息称为“陷阱”，由 SNMP 代理针对内部状况更改或故障状况而生成。NNMi 从接收的 SNMP 陷阱生成事件，显示在 SNMP 陷阱事件浏览视图中。

SNMP 陷阱风暴
大量未请求的 SNMP 代理消息，可使 SNMP 管理器进程（在此案例中为 NNMi）不堪重负。可以在 NNMi 中使用 nnmtrapconfig.ovpl 命令配置 SNMP 陷阱风暴阈值。传入陷阱速率超过指定的阈值速率时，NNMi 将阻止陷阱，直到陷阱速率低于重置速率。

sysObjectID
在 NNMi 中，用于识别网络元素的模型或类型的 SNMP 对象标识符的专用术语。系统对象 ID 是网络元素的管理信息库对象的一部分，发现期间由 NNMi 从各个节点查询。可按其系统对象 ID 分类的网络元素类型示例包括：HP ProCurve 交换机系列的任何成员、HP J8715A ProCurve Switch 和 HP IPF 系统的 HP SNMP 代理。其他供应商的网络元素可同样按照其系统对象 ID 分类。系统对象 ID 的关键用途是定义 NNMi 设备配置文件，这些配置文件指定网络元素的特征，只要已知网络元素类型即可推导出特征。

播

播种发现
基于种子列表的进程，它发现并返回仅关于指定为种子的节点的详细网络信息。基于列表的发现为特定查询和任务维护有限的网络库存。与基于规则的发现相对应。另请参阅发现进程和螺旋发现。

地

地址提示
NNMi 使用 SNMP ARP 缓存查询发现的 IP 地址；CDP、EDP 或其他发现协议查询；或 Ping 扫描。NNMi 进一步查询作为发现提示的 IP 地址，然后根据基于规则的发现中当前的发现规则检查结果。

第

第 2 层
参考多层通信模型（开放系统互连，OSI）的数据链路层。数据链路层在网络中跨物理链路移动数据。NNMi 第 2 层视图提供有关设备的物理连接的信息。

第 3 层
参考多层通信模型（开放系统互连，OSI）的网络层。通过网络层可了解网络中相邻节点的地址、选择路由及服务

质量。NNMi 第 3 层视图提供有关路由连接的信息。

端

端口
在网络硬件环境中，是指用于将信息传递到网络设备或从其传递出信息的连接器。

断

断开的接口
从 NNMi 的角度来看，断开的接口就是未连接到 NNMi 所发现的另一个设备的接口。默认情况下，NNMi 只监视具有 IP 地址且包含在路由器节点组的节点中的未连接接口。

对

对象标识符
SNMP 中用于标识管理信息库数据对象的数字序列。OID 由用点分隔的数字组成，其中每个数字表示 MIB 层次结构中该层的特定数据对象。OID 是等价于 MIB 对象名称的数字表示，例如 MIB 对象名称 iso.org.dod.internet.mgmt.mib-2.bgp.bgpTraps.bgpEstablished 等价于其 OID 1.3.6.1.2.1.15.0.1。

发

发现规则
用户定义的 IP 地址和/或系统对象 ID（对象标识符）的范围，用于限制基于规则的发现过程。在 NNMi 控制台“发现配置”部分的“自动发现规则”下，配置发现规则。另请参阅基于规则的发现。

发现过程
在此过程中 NNMi 采集有关网络节点的信息以使其能处于被管状态。初始发现作为两阶段的过程运行，返回设备库存信息，然后返回网络连接信息。初始发现之后，发现过程持续进行。在基于列表的发现中，这意味着如果种子列表中的设备发生配置更改，则将会更新设备。在基于规则的发现中，如果新设备与当前发现规则匹配，也会被添加。对设备或设备组的发现也可以根据需要从 NNMi 控制台或命令行启动。另请参阅螺旋发现、基于规则的发现和基于列表的发现。

发现提示
NNMi 使用 SNMP ARP 缓存查询发现的 IP 地址；CDP、EDP 或其他发现协议查询；或 Ping 扫描。NNMi 进一步查询作为发现提示的 IP 地址，然后根据基于规则的发现中当前的发现规则检查结果。

发现种子
通过充当网络发现过程的起点，帮助 NNMi 发现网络的节点。例如，种子可能是管理环境中的核心路由器。每个种子都通过 IP 地址或主机名识别。除非已配置基于规则的发现，否则会将 NNMi 的发现过程限制为指定种子的基于列表的发现。

高

高可用性
在本指南中是指一种硬件和软件配置，在部分配置出现故障时提供不间断的服务。高可用性 (HA) 意味着该配置有冗余组件，即使某个组件出现故障，也能保证应用程序的持续运行。可将 NNMi 配置为支持若干商业上可用的 HA 解决方案之一。与应用程序故障转移相对应。

根

根源分析
在 NNMi 中，根源分析 (RCA) 是指 NNMi 用于判断网络问题根源的一类问题解决

方法。在 NNMi 中，根源是找到相关问题症状即可解决的可处理问题。NNMi 以两种关键方式使用根源识别：通知用户可处理问题是什么，在根源问题解决后再显示次要问题的症状报告。根源的确定可能导致被管对象的状态更改和/或生成根源事件。NNMi 如何使用 RCA 的示例场景：被管路由器出现故障，来自 NNMi 管理服务器的路由器另一端的被管节点无法再响应状况轮询查询。NNMi 用 RCA 确定状况轮询故障是次要问题症状。它将路由器故障报告为根源事件，并抑制禁止报告下游节点的问题症状，直到根源路由器故障得到解决。

根源事件
"关联性"属性设置为"根源"的 NNMi 事件。NNMi 使用根源分析 (RCA) 建立根源事件，作为发现相关问题症状后即可解决的可处理问题。请参阅根源分析。

公

公钥证书
用于网络安全和加密中，包含用来绑定公钥与身份信息的数字签名的文件。用于确认公钥属于个人还是组织的证书。NNMi 使用 SSL 证书，这些证书包含公钥和私钥，用于客户端-服务器通信的验证和加密。

故

故障轮询
关键 NNMi 监视活动，NNMi 发出其被管接口、IP 地址和 SNMP 代理的 ICMP Ping 和/或状态 MIB 的 SNMP 只读查询，以确定每个被管对象的状况。用户可以在 NNMi 控制台的"配置"工作区中的"监视配置"下，自定义为不同接口组、节点组和节点执行的故障轮询的类型。故障轮询是状况轮询的子集。

管

管理服务器
NNMi 管理服务器是安装 NNMi 软件的计算机系统。NNMi 进程和服务在 NNMi 管理服务器上运行。(以前的 NNM 版本对此系统使用的术语是"NNM 管理工作站"。)

管理信息库
SNMP 中有关被管网络的数据集合，以层次结构形式组织。管理信息库中的数据对象是指被管设备的特征。NNMi 通过使用 MIB 数据对象(有时称为"MIB 对象"、"对象"或"MIB") 对被管节点进行 SNMP 查询和从其接收 SNMP 陷阱，以此采集网络管理信息。

规

规则
用户定义的 IP 地址和/或系统对象 ID (对象标识符) 的范围，用于限制基于规则的发现过程。在 NNMi 控制台"发现配置"部分的"自动发现规则"下，配置发现规则。另请参阅基于规则的发现。

基

基于规则的发现
通常称为自动发现，NNMi 可以使用基于规则的发现，根据用户指定的发现规则来查找 NNMi 应添加到其数据库的节点。NNMi 在所发现节点的数据中查找发现提示，然后根据指定的发现规则检查这些候选项。在 NNMi 控制台"发现配置"部分的"自动发现规则"下，配置发现规则。与基于列表的发现相对应。

基于列表的发现
基于种子列表的进程，它发现并返回仅关于指定为种子的节点的详细网络信息。基于列表的发现为特定查询和任务维护有限的网络库存。与基于规则的发

现相对应。另请参阅发现进程和螺旋发现。

简

简单网络管理协议
OSI 模型的应用层(第 7 层) 的简单协议操作，通过它，远程用户可以检查或更改网络元素的管理信息。SNMP 是 NNMi 用于在被管节点上与代理进程交换网络管理信息的主导协议。NNMi 支持三个最常见的 SNMP 版本：SNMPv1、SNMPv2c 和 SNMPv3。

角

角色
作为设置用户访问的一部分，NNMi 管理员将预配置的用户角色分配给每个 NNMi 用户帐户。用户角色决定哪些用户帐户可以访问 NNMi 控制台，以及哪些工作区和操作对于每个用户帐户均可用。NNMi 提供以下分层的用户角色，这些角色由程序预定义且无法修改：管理员、Web 服务客户端、第 2 级操作员、第 1 级操作员和来宾。另请参阅用户帐户。

阶

阶段
NNMi 根源分析中使用的术语，指一段特定的持续时间，它由主故障触发，在此期间次级故障被抑制或关联在主故障下。

接

接口
用于将节点连接到网络的物理端口。

接口组
NNMi 的主要筛选技术之一，将接口分组，以便将设置应用于组或按组筛选可见性。接口组可用于以下任一或全部操作：配置监视、筛选表视图，以及自定义图视图。另请参阅节点组。

节

节点
在网络上下文中，是指网络中的计算机系统或设备(例如打印机、路由器或网桥) 。而且能够响应 SNMP 查询的节点还向 NNMi 提供最全面的管理信息，NNMi 还可以对非 SNMP 节点执行受限管理。

节点组
NNMi 的主要筛选技术之一，将节点分组，以便将设置应用到组或按组筛选可见性。节点组可用于以下任一或全部操作：配置监视、筛选表视图，以及自定义图视图。另请参阅接口组。

结

结论
在 NNMi 中由原因引擎生成和使用的支持详细信息，它明确说明了原因引擎如何确定被管对象的状态和根源事件的更多细节。

卷

卷组
计算机存储虚拟化术语，指配置为组成单个大型存储区域的一个或多个磁盘驱动器。NNMi 支持的若干高可用性产品在其共享文件系统中使用卷组。

控

控制器
在 NNMi 应用程序故障转移中，用于具有主群集状况的群集成员的 JGroups 术语。JGroups 基于最低 IP 地址确定群集的哪个成员是控制器。

控制台
NNMi 用户界面。操作员和管理员用 NNMi 控制台执行 NNMi 中的网络管理任务。

逻

逻辑卷
计算机存储虚拟化术语，指卷组中可以用作单独文件系统或设备交换空间的任意大小的空间。NNMi 支持的若干高可用性产品在其共享文件系统中使用逻辑卷。

螺

螺旋发现
NNMi 持续改进的网络拓扑信息，包括有关 NNMi 管理的网络中库存、包含、关系和连接的信息。另请参阅发现进程、基于规则的发现和基于列表的发现。

嵌

嵌入式数据库
NNMi 包含的数据库。NNMi 还可以配置为对其多数表使用外部 Oracle 数据库而不是嵌入式数据库。另请参阅 PostgreSQL。

区

区域
NNMi 中的设备分组，用于配置超时值和访问凭据之类的通信设置。

区域管理器
全局网络管理部署中的 NNMi 管理服务器，它提供设备发现、轮询和陷阱接收，并将信息转发到全局管理器。

全

全局管理器
全局网络管理部署中的 NNMi 管理服务器，它整合来自分布式 NNMi 区域管理器服务器的数据。全局管理器提供跨整个环境的拓扑和事件的统一视图。全局管理器必须有 NNMi Advanced 许可证。

全局网络管理
NNMi 的分布式部署，用一个或多个全局管理器整合来自一个或多个地理上分散分布的区域管理器的数据。

群

群集
NNMi 环境中的硬件和软件分组，由高可用性技术或使用 jboss 群集功能链接起来，共同确保组件过载或出现故障时功能和数据的连续性。群集中的计算机通常通过高速 LAN 彼此连接。通常，部署群集是为了改进可用性和/或性能。

群集成员或节点
NNMi 环境中的高可用性或 jboss 群集中的一个系统，已配置或将配置为支持 NNMi 高可用性或应用程序故障转移。

事

事件
NNMi 中与网络相关的通知，在 NNMi 控制台事件视图和表单中显示。NNMi 包括允许用户根据事件属性筛选事件的多个“事件管理”和“事件浏览”视图。多数事件视图显示 NNMi 直接生成的事件(有时称为管理事件) 。NNMi 还包括用于浏览从 SNMP 陷阱和 NNM 6.x/7.x 事件生成的事件的视图。

团

团体字符串
SNMPv1 和 SNMPv2c 实现中使用的一种类似于密码的机制，用于 SNMP 代理对 SNMP 查询的验证。SNMP 包中以明文形式传递团体字符串，使得它容易受到包嗅探的攻击。SNMPv3 提供用于验证的更强安全机制。

拓

拓扑(网络)
通信网络中网络布局的架构性描述，包括其节点和连接。

系

系统对象 ID
在 NNMi 中，用于识别网络元素的模型或类型的 SNMP 对象标识符的专用术语。系统对象 ID 是网络元素的管理信息库对象的一部分，发现期间由 NNMi 从各个节点查询。可按其系统对象 ID 分类的网络元素类型示例包括：HP ProCurve 交换机系列的任何成员、HP J8715A ProCurve Switch 和 HP IPF 系统的 HP SNMP 代理。其他供应商的网络元素可同样按照其系统对象 ID 分类。系统对象 ID 的关键用途是定义 NNMi 设备配置文件，这些配置文件指定网络元素的特征，只要已知网络元素类型即可推导出特征。

系统帐户
在 NNMi 中，供 NNMi 安装期间使用的特殊帐户。安装之后，NNMi 系统帐户应仅用于命令行安全和恢复目的。与用户帐户相对应。

陷

陷阱
使用轮询(从 SNMP 代理请求响应) 的网络管理是有利于简化的 SNMP 设计原则。但是，提供该协议也是用于将未请求消息从 SNMP 代理发送到 SNMP 管理器进程(在此案例中为 NNMi) 的通信。未请求的代理消息称为“陷阱”，由 SNMP 代理针对内部状况更改或故障状况而生成。NNMi 从接收的 SNMP 陷阱生成事件，显示在 SNMP 陷阱事件浏览视图中。

虚

虚拟 IP 地址
未绑定到任何特定网络硬件的 IP 地址，在高可用性配置中用于根据当前故障转移或负载平衡需要，将连续的网络流量发送到最适合的服务器。

虚拟主机名
与虚拟 IP 地址关联的主机名。

应

应用程序故障转移
NNMi 中的可选功能(由用户配置并借助于 jboss 群集支持) ，如果当前活动服务器出现故障，则将 NNMi 进程的控制转移给备用服务器。

用

用户角色
作为设置用户访问的一部分，NNMi 管理员将预配置的用户角色分配给每个 NNMi 用户帐户。用户角色决定哪些用户帐户可以访问 NNMi 控制台，以及哪些工作区和操作对于每个用户帐户均可用。NNMi 提供以下分层的用户角色，这些角色由程序预定义且无法修改：管理员、Web 服务客户端、第 2 级操作员、第 1 级操作员和来宾。另请参阅用户帐户。

用户帐户
在 NNMi 中，供用户或用户组访问 NNMi 的方式。NNMi 用户帐户在 NNMi 控制台中设置，并实现预定的用户角色。请参阅系统帐户和用户角色。

原

原因
表示一个事件(原因) 和另一个事件(结果，第一个事件的直接后果) 之间的关系。NNMi 用因果关系分析算法分析事件循环，确定用于解决网络问题的解决方案。

原因引擎
一种 NNMi 技术，使用基于原因的方法将根源分析 (RCA) 应用于网络症状。原因引擎 RCA 由某些情况触发，包括由于状况轮询、SNMP 陷阱和特定事件而检测到的更改。原因引擎使用 RCA 确定被管对象的状态，得出有关它们的结论，并生成根源事件。

种

种子
通过充当网络发现过程的起点，帮助 NNMi 发现网络的节点。例如，种子可能是管理环境中的核心路由器。每个种子都通过 IP 地址或主机名识别。除非已配置基于规则的发现，否则会将 NNMi 的发现过程限制为指定种子的基于列表的发现。

主

主动群集节点
在应用程序故障转移或高可用性配置中当前运行 NNMi 进程的服务器。

状

状况
对于和 MIB II ifAdminStatus、MIB II ifOperStatus、性能或可用性相关的自报告被管对象响应，NNMi 通常使用术语“状况”。与状态相对应。

状况轮询
由 NNMi 的状况轮询器执行的定向监视，它用 ICMP Ping 和 SNMP 查询来检索被管对象的故障、性能、组件运行状况和可用性数据。另请参阅故障轮询。

状态
在 NNMi 中，表示其总体状况的被管对象属性。状态由原因引擎根据被管对象的未决结论来计算。与状况相对应。

自

自动发现
通常称为自动发现，NNMi 可以使用基于规则的发现，根据用户指定的发现规则来查找 NNMi 应添加到其数据库的节点。NNMi 在所发现节点的数据中查找发现提示，然后根据指定的发现规则检查这些候选项。在 NNMi 控制台“发现配置”部分的“自动发现规则”下，配置发现规则。与基于列表的发现相对应。

发送文档反馈

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

关于部署参考 (Network Node Manager i Software 10.20) 的反馈

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 network-management-doc-feedback@hpe.com 。

我们感谢您提出宝贵的意见！