HP Network Node Manager i Software

适用于 Windows[®]、 HP-UX、 Linux 和 Solaris 操作系统 软件版本: 9.10



文档发行日期: 2011 年 3 月 软件发行日期: 2011 年 3 月



法律声明

担保

HP 产品和服务担保声明随产品和服务明确呈示,且是唯一的呈示。此处任何内容都不得解释为其他担保。HP 不对 在此处包含的技术或编辑错误或者遗漏负责。

此处包含的信息将随时更改,恕不另行通知。

有限权限声明

机密计算机软件。必须具有 HP 提供的有效许可证才能拥有、使用或复制。基于 FAR 12.211 和 12.212, 商业计算机 软件、计算机软件文档和商业产品的技术数据均已获得美国政府的供应商标准商业许可证。

版权声明

©版权所有 2008-2011 Hewlett-Packard Development Company, L.P.

商标声明

Acrobat® 是 Adobe Systems Incorporated 的商标。

HP-UX R10.20 及更高版本以及 HP-UX R11.00 及更高版本 (32 和 64 位配置) 在所有 HP 9000 计算机上都是 Open Group UNIX 95 品牌产品。

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

Oracle 和 Java 是 Oracle 和 / 或其子公司的注册商标。

UNIX® 是 The Open Group 的注册商标。

Oracle 技术 — 有限权限声明

根据 DOD FAR Supplement 提供的程序是 "商业计算机软件",这些程序 (包括文档)的使用、复制和披露将受 限于适用的 Oracle 许可协议中规定的许可限制。否则,根据 Federal Acquisition Regulations 提供的程序是 "受 限制的计算机软件",这些程序 (包括文档)的使用、复制和披露应受限于 "FAR 52.227-19,商业计算机软件 - 限制权力 (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。

声明

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

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

2011年3月

可用产品文档

除此指南以外, NNMi 还有以下文档可供参阅:

- *HP Network Node Manager i Software 文档列表*—在 HP 手册网站上提供。使用此文件可跟踪此版本的 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。
- 《HP Network Node Manager i Software 安装指南》— 可在产品介质和 NNMi 管理服务器上找到,针对每个 支持的操作系统提供。
- 《HP Network Node Manager i Software 升级参考》— 在 HP 手册网站上提供。
- HP Network Node Manager i Software 发行说明—在产品介质和 NNMi 管理服务器上提供。
- HP Network Node Manager i Software 系统和设备支持列表 在产品介质和 NNMi 管理服务器上提供。
- 《HP Network Node Manager iSPI Network Engineering Toolset 计划与安装指南》— 在 NNM iSPI NET 诊断服务器 产品介质上提供。

要检查最近是否有更新或要验证使用的文档是否为最新版本,请转到:

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

此网站要求您注册获取 HP Passport, 然后才能登录。要注册以获取 HP passport ID, 请转到:

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

或在 HP Passport 登录页上单击 New users - please register (新用户 - 请注册)链接。

如果您订阅了相应的产品支持服务,还将接收到全新或更新的版本。有关详细信息,请联系 HP 销售代表。

支持

访问 HP Software Support Online 网站,网址是:

www.hp.com/go/hpsoftwaresupport

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

HP Software Online Support 提供客户自解决功能。它为您提供一种快速高效的方法来访问交互式技术支持工具以管理您的业务。作为尊贵的支持客户,您可以通过使用支持网站受益:

- 搜索感兴趣的知识文档
- 提交和跟踪支持案例和增强功能请求
- 下载软件补丁
- 管理支持合同
- 查找 HP 支持联系人
- 查看有关可用服务的信息
- 参加与其他软件客户的讨论
- 研究和注册软件培训

大多数支持区域要求您注册为 HP Passport 用户并登录。很多区域还要求提供支持合同。要注册以获取 HP Passport 用户 ID,请转到:

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

要查找有关访问级别的详细信息,请转到:

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

目录

关于本指南	25
本指南有哪些内容?	25
本文档中使用的路径约定	26
修订历史	27
有关 NNMi 的详细信息	28

准备

31

更件和软件要求	33
支持的硬件和软件	33
检查必需补丁	34
系统配置 (UNIX)	35
安装 NNMi 和 NNM iSPI	35
NNMi 与 HP Performance Insight 的共存性	35
NNMi 与 HP Operations Agent 的共存性	36

配置

配置的常规概念
任务流模型
最佳实践:保存现有配置
最佳实践: 使用作者属性 40
用户界面模型
排序
节点组和接口组
分组重叠
节点组成员资格
层次结构 / 包含
设备过滤器
其他过滤器
其他节点
节点组状态
接口组
节点 / 接口 / 地址层次结构
停下来,重新开始
NNMI 進信
通信的概念
进信配直的级别
网络她迟和超时

SNMP 访问控制	49
SNMP 版本首选项	50
管理地址首选项	51
轮询协议	51
通信配置和 nnmsnmp*.ovpl 命令	
计划通信	
默认通信设置	
通信配置区域	53
特定节点配置	54
重试和超时值	
活动协议	54
多个共用字符串或身份验证配置文件	
SNMPv1 和 SNMPv2 共用字符串	55
SNMPv3 身份验证配置文件	55
配置通信	
准备 NNMi 以使用 SNMPv3 隐私协议	
评估通信	
是否为 SNMP 配置了所有节点?	
SNMP 访问当前是否对设备可用?	
管理 IP 地址是否正确?	
NNMi 使用的通信设置是否正确?	
状态轮询器设置是否符合通信设置?	58
调整通信	
NNMi 搜索	
搜索的概念	59
NNMi 通过设备配置文件得出属性	60
计划搜索	61
选择您的主搜索方式	61
基于列表的搜索	
基于规则的搜索	
自动搜索规则	
自动搜索规则排序	
从搜索中排除设备	
Ping 扫描	
来自 SNMP 陷阱的搜索提示	63
自动搜索规则的搜索种子	63
自动搜索规则的最佳实践	
示例	
节点名称解析	
子网连接规则	
搜索种子	
重新搜索间隔	
不搜索对象	
通过 NNMi 监视虚拟 IP 地址	67
配置搜索	
配置自动搜索规则的提示	
配置种子的提示	68
癿 且们 丁 山灰小 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	

评估搜索	69
跟踪初始搜索的进度	69
所有种子都搜索了吗?	69
所有节点都具有有效的设备配置文件吗?	70
所有节点都正确搜索了吗?	70
自动搜索规则	70
IP 地址范围	71
系统对象 ID 范围	71
所有连接和 VLAN 都正确吗?	71
评估第2层连通性	71
NNMi 搜索与重复的 MAC 地址	72
重新搜索设备	72
调整搜索	72
搜索日志文件	73
未编号接口	73
启用未编号接口功能	73
禁用未编号的接口功能	74
	77
	//
状态轮询的概念	77
计划 次念轮询	78
*花期清里	78
NNMI 可以	19
到不	00
停止	01
N 刈组	01
按口组	04 09
1 品组	04 09
り 划北	03 Q1
你此安木朱的奴馅,	04
印里·尔尔·尔································	04
印旦汉口泊仰卫点组····································	04
п且以口血化	05
<u>品且</u> P/A.血化	86
亚础款的发量····································	86
验证网络监视的配置	
接口或节占所属的组是否正确?	
要应用哪些设置?	
要采集哪些数据?	
评估状态轮询的性能	87
状态轮询器是否一直在运行?	
调整状态轮询	89
NNMi 事件	. 91
事件的概念	91
事件生命周期	92
陷阱和事件转发	93

比较: 將第三方 SNMP 陷阱转发到其他应用程序	
MIB	
自定义事件属性	
添加到已关闭的管理事件的 CIA	
事件减少	
事件抑制、强化和减弱	
生命周期转换操作	
计划事件	
NNMi 应处理哪些设备陷阱?	
NNMi 应显示哪些事件?	
NNMi 应如何响应事件?	
NNMi 应从 NNM 管理工作站接收陷阱吗?	100
NNMi 应将陷阱转发到另一个事件接收器吗?	100
配置事件	100
配置事件抑制、强化和减弱	100
配置生命周期转换操作	101
评估事件	101
调整事件	102
启用和配置未定义陷阱的事件	102
NNMi 控制台	105
使田节占组的立例	105
创建节占组	106
出建 ¹ / / / / / / / / / / / / / / / / / / /	106
步骤 2. 创建 "美国" 节占组	106
步骤 2 . 使用过滤器创建 "科罗拉多"节占组	107
步骤 4: 查看节点组成员以检查节点组讨滤器结果	
步骤 5: 为"我的网络"节点组建立节点组层次结构	
步骤 6: 为 "美国"节点组建立节点组层次结构	
配置节点组图	
步骤 1: 创建节点组图	
步骤 2: 查看节点组图	
步骤 3. 配置节点组状态	
步骤 4: 配置节点组图排序	
步骤 5: 将背景图像添加到节点组图	
减少在网络概述图中显示的最大节点数	
减少节点组图上显示的节点数	

高级配置

F可 NNMi	115
准备安装永久许可证密钥	.115
检查许可证类型和被管节点数目	.115
获取和安装永久许可证密钥	.116
使用 Autopass 和 HP 订购号 (在防火墙后不能实现)	.116
使用命令行	.116
获取其他许可证密钥	.116

2011年3月

使用 NNMi 证书	119
概要	120
生成证书颁发机构证书	121
将应用程序故障切换配置为使用自签名证书	124
将应用程序故障切换配置为使用证书颁发机构	126
将高可用性配置为使用自签名或证书颁发机构证书	128
将高可用性配置为使用自签名证书	128
为高可用性配置新证书	128
将全局网络管理功能配置为使用自签名证书	129
将全局网络管理功能配置为使用证书颁发机构	130
将带有应用程序故障切换的全局网络管理配置为使用自签名证书	131
配置与目录服务的 SSL 连接	132
配置 HP BSM V9.xx 的 SSL 连接	133
	100
<u>刈</u> NNMI	139
NNM1 的 SSO 访问	140
为毕个或后用 SSO	141
万位 丁个回 项 甲的 NNM 1 官理服务器后用 SSO	141
NNMI 和 NNM ISPI 的 SSO 访问	142
配直 NNMi 和 HP BSM 或 HP BAC 之间的毕点登求	143
配直 NNM1 和 HP UCMDB 之间的単点金求	144
配直 NNM1 和 HP NA 之间的毕点 登求	145
奈用 550	148
SSO 女生备注	148
配置 Telnet 和 SSH 协议以供 NNMi 使用	151
禁用 Telnet 或 SSH 菜单项	151
为 Windows 上的浏览器配置 Telnet 或 SSH 客户端	152
Windows 操作系统提供的 Telnet 客户端	153
第三方 Telnet 客户端 (标准 Windows)	155
第三方 Telnet 客户端 (Windows on Windows)	156
第三方 SSH 客户端 (标准 Windows 以及 Windows on Windows)	157
在 Linux 上配置 Firefox 使用 Telnet 或 SSH	158
Linux 上的 Telnet	158
Linux 上的安全 Shell	159
用于更改 Windows 注册表的示例文件	160
示例 nnmtelnet.reg	160
示例 nnmputtytelnet.reg	160
示例 nnmtelnet32on64.reg	161
示例 nnmssh.reg	161
	1/0
	103
NNM1 用尸切问信息和配直选坝	163
远坝 1: NNM1	164
远坝 Z: NNMI	165
近坝 3: 日求服务中的所有 NNM1 用尸信息	166
	16'/

将目录服务访问配置更改为支持 NNMi 安全模型	174
目录服务查询	176
目录服务访问	176
目录服务内容	176
由目录服务管理员拥有的信息	180
用户标识	181
配置目录服务中的 NNMi 用户访问 (详细方法)	182
用户组标识	183
配置目录服务中的用户组检索(详细方法)	184
用于存储 NNMi 用户组的目录服务配置	186
对目录服务集成进行故障诊断	187
ldap.properties 配置文件参考	188
示例	192
	102
NN/MI 女王和多性广	193
限制刈豕切凹的影响	194
NNMI 女王侯空	190
女生组 空	190
女生组结构小例	197
NNMI	200
租户	200
他广知构小例	201
WINN (文王中夕位) 10直 配署丁目	203
印旦二六····································	204
印显仙////////////////////////////////////	205
品且又工组	201
显出出 <u>组</u>	210
NNMi 安全、多租户和全局网络管理	210
初始 GNM 配置	210
GNM 维护	213
在 NPS 报告中包含选择界面	213
全局网络管理	215
全局网络管理的好处	215
"全局网络管理"是管理网络的好工具吗?	216
我需要连续的多站点网络监视吗?	216
我的关键设备是可见的吗?	216
许可注意事项	216
实用的全局网络管理示例	217
查看要求	218
区项官埋器和全局官埋器连接	219

初始准备	220
端口可用性: 配置防火墙	220
配置自签名证书	220
配置全局网络管理以供应用程序故障切换	220
NNMi 管理服务器大小调整的注意事项	221
同步系统时钟	221
在全局网络管理中结合使用应用程序故障切换功能与自签名证书	221
在全局网络管理中使用自签名证书	221
在全局网络管理中使用证书颁发机构	221
列出要监视的关键设备	222
查看全局和区域管理器的管理域	
查看 NNM i 帮助主题	223
SSO 和操作菜单	223
为全局网络管理配置单占登录	223
在区域管理器上配置转发过滤器	225
配置转发过滤器, 限制转发的节占	225
田区城管理器连接全局管理器	232
确定从 global1 到 regional1 和 regional2 的连接状态	236
香着 globall 资产	237
断开 global1 和 regional1 之间的通信连接	239
面外 g105a11 将 10g10ha11 之内的起情之设	241
2.9 而心 · · · · · · · · · · · · · · · · · ·	241
设家和威力的学生。	244
田全局管理哭确定设备状态和 NNMi 事件生成	245
为全局网络管理配置应用程序故障切换	246
在全局管理器上配置应用程序故 谙切 拖	246
全局网络管理的故障诊断提示	248
NNMi 帮助中的故障诊断信息	248
时钟同步	248
全局网络管理系统信息	248
从全局管理器同步区域管理器搜索	249
於至於自己的時間也不可以在一個人的一個人的一個人的一個人的一個人的一個人的一個人的一個人的一個人的一個人的	249
从 NNMi 9 0x 升级到 NNMi 9 10	249
全局网络管理支持的 NNMi 版本	249
全局网络管理升级步骤	249
全局网络管理和 NNM iSPI 或第三方集成	250
	200
配置 NNMi Advanced 的 IPv6 功能	251
功能描述	251
先决条件	253
许可	253
受支持配置	254
管理服务器	254
IPv6 的受支持 SNMP MIB	255
安装 NNMi	255
激活 IPv6 功能	255
取消激活 IPv6 功能	257

《NNMi 部署参考》

取消激活之后的 IPv6 监视 取消激活之后的 IPv6 资产 清理 IPv6 资产时的已知问题	258 258 258 259
在 Solaris 区域环境中运行 NNMi 在 Solaris 区域中安装 NNMi	

恢复能力

为 NNMi 配置应用程序故障切换	
应用程序故障切换概述	
应用程序故障切换基本设置	
为 NNMi 配置应用程序故障切换	
使用应用程序故障切换功能	
使用嵌入式数据库的应用程序故障切换行为	
使用 Oracle 数据库的应用程序故障切换行为	
应用程序故障切换场景	
其他 ovstart 和 ovstop 选项	
应用程序故障切换事件	
故障切换后返回原始配置	
NNM iSPI 和应用程序故障切换	279
NNM iSPI 安装信息	279
集成应用程序	280
禁用应用程序故障切换	
管理任务和应用程序故障切换	
应用程序故障切换和升级到 NNMi 9.10	
应用程序故障切换和 NNMi 补丁	
为应用程序故障切换应用补丁 (关闭活动和备用服务器)	286
为应用程序故障切换应用补丁 (保留一个活动 NNMi 管理服务器)	288
应用程序故障切换和重新启动 NNMi 管理服务器	290
应用程序故障切换和从以前的数据库备份恢复(仅嵌入式数据库)	290
网络延迟 / 带宽注意事项	
应用程序故障切换和 NNMi 嵌入式数据库	
应用程序故障切换环境中的网络通信量	293
应用程序故障切换通信量测试	
在高可用性群集中配置 NNMi	
HA 概念	
HA 术语	
NNMi HA 群集场景	
联机帮助页	
验证配置 NNMi 以 HA 运行的先决条件	
配置 HA	305
为 HA 配置 NNMi 证书	305

为 HA 配置 NNMi		305
NNMi HA 配置信息		306
在主群集节点上配置 NNMi		308
在辅助群集节点上配置 NNMi		310
为 HA 配置 NNM iSPI		.311
NNM iSPI Performance for Metrics、 NNM iSPI Performance for QA 和		
NNM iSPI Performance for Traffic	••••	.311
NNM iSPI for MPLS、 NNM iSPI for IP Multicast 相 NNM iSPI for IP Telephony	•••••	312
以HA 运行的 NNM iSPI Network Engineering Toolset Software 和 NNMi	••••	312
在 Oracle	••••	312
Oracle 上的 NNM1 依赖性	••••	313
在 Oracle 环境中配置 NNMi 以 HA 运行	•••••	313
共享 NNMi 数据	· • • • • •	314
NNMi 共享磁盘上的数据	· • • • • •	314
配置文件的复制	· • • • • •	315
手动准备共享磁盘	· • • • • •	315
配置 SAN 或已实际连接的磁盘	· • • • • •	315
在 ov.conf 文件中设置 HA 变量	· • • • • •	316
将共享磁盘移到 NNMi HA 资源组中	· • • • • •	316
有关 Windows 服务器上的共享磁盘配置的说明	· • • • • •	317
在 HA 群集中许可 NNMi	· • • • • •	317
维护 HA 配置	· • • • • •	318
维护模式	•••••	318
将 HA 资源组置于维护模式	•••••	318
将 HA 资源组从维护模式中除去	· • • • • •	318
在 HA 群集中维护 NNMi	· • • • • •	319
启动和停止 NNMi	· • • • • •	319
在群集环境中更改 NNMi 主机名和 IP 地址	· • • • • •	319
停止 NNMi 而不执行故障切换	· • • • • •	321
在维护之后重新启动 NNMi	· • • • • •	322
在 NNMi HA 群集中维护加载项 NNM iSPI	· • • • • •	322
从 HA 群集取消配置 NNMi	· • • • • •	322
从 HA 群集取消配置 NNMi	· • • • • •	322
不以 HA 运行帯现有数据库的 NNMi	· • • • • •	325
对以 HA 运行的 NNMi 应用补 」	· • • • • •	326
将以 HA 运行的 NNMi 从 NNMi 9.0x 升级到 NNMi 9.10	· • • • • •	327
在 Windows、 Linux 或 Solaris 操作系统上升级带有嵌入式数据库的 NNMi	· • • • • •	327
在 HP-UX 操作系统上升级带有嵌入式数据库的 NNMi	· • • • • •	329
在所有受支持的操作系统上升级带 Oracle 的 NNMi	· • • • • •	330
对 HA 配置进行故障诊断	· • • • • •	331
常见配置错误	· • • • • •	331
HA 资源测试		332

345

常规 HA 故障诊断	333
错误:参数个数不正确	333
资源托管子系统进程意外停止 (Windows Server 2008 R2)	333
产品启动超时 (Solaris)	334
主动群集节点上的日志文件未更新	334
无法在特定群集节点上启动 NNMi HA 资源组	334
特定于 NNMi 的 HA 故障诊断	335
在取消配置所有群集节点之后,对 NNMi 重新启用 HA	336
NNMi 未以 HA 正确启动	336
故障切换之后看不到对 NNMi 数据的更改	337
nmsdbmgr 在配置 HA 后未启动	337
pmd 在配置 HA 后未启动	338
NNMi 仅在一个 HA 群集节点上正确运行 (Windows)	338
磁盘故障切换未执行	338
无法访问共享磁盘 (Windows)	339
共享磁盘不包含当前数据	339
故障切换之后辅助节点找不到共享磁盘文件	339
特定于 NNM iSPI 的 HA 故障诊断	340
HA 配置参考	341
NNMi HA 配置文件	341
NNMi 提供的 HA 配置脚本	341
NNMi HA 配置日志文件	343

维护 NNMi

NNMi 备份和恢复工具	
备份和恢复命令	
备份 NNMi 数据	
备份类型	
备份范围	
恢复 NNMi 数据	
相同系统恢复	
不同系统恢复	
备份和恢复策略	
定期备份所有数据	
更改配置之前备份数据	
升级 NNMi 或操作系统之前备份数据	
只恢复文件系统文件	
只备份和恢复嵌入式数据库	
维护 NNMi	357
管理自定义轮询器采集导出	
更改自定义轮询器采集导出目录	
更改用于自定义轮询器采集导出的最大磁盘空间量	
更改自定义轮询器度量累计间隔	
管理事件操作	
设置并发操作数目	
设置 Jython 操作的线程数	
• • • • • • • • • • • • • • • • • • • •	

设置操作服务器名称参数	
更改操作服务器队列大小	
使用 trapFilter.conf 文件阻止事件	
配置与 NNMi 控制台的仅 HTTPS 通信	
修改 NNMi 标准化属性	
在初始搜索之后更改标准化属性	
修改并发 SNMP 请求数	
NNMi 自监视	
抑制对特定节点使用搜索协议	
抑制使用搜索协议采集	
管理对 NAT 环境中的管理地址的 ICMP 轮询	
启用对 NAT 环境中的管理地址的 ICMP 轮询	
对 NNMi 的更改方式	
抑制对大型交换机使用 VLAN 索引	
抑制使用 VLAN 索引	
了解对 NAT 环境中的管理地址的 ICMP 轮询	
对 NAT 环境中的管理地址的 ICMP 轮询	
NNMi 日志记录	
NNMi 日志文件	
日志文件属性	
更改日志记录文件属性	
文件管理	
	277
史以 NNMI 官埋服务器	
准备 NNM1 配置供移动的最佳头践	
移动 NNMi 配置和嵌入式数据库	
移动 NNMi 配置	
恢复 NNMi 公钥证书	
更改独立 NNMi 管理服务器的 IP 地址	
许可汪意事项	
更改 NNMi 管理服务器的主机名或域名	
更改 Oracle 数据库实例连接信息	
更改 NNMi 用于连接 Oracle 数据库实例的密码	
在 Xap 皮划化环境中运行 NNMi	380
在正在运行的 NNMi 管理服备器上安装 Xen 之后的问题	389
升级自 NNMi 9.0x	391
从现有版本升级 NNMi 管理服务器	
将现有 NNMi 管理服务器升级到 NNMi 9.10	
	205
井 级到个问 NNM1 官埋服务器	
将 NNMi 从 Windows 2003 移到 Windows 2008	397
将 NNMi 从 Windows 2003 更改为 Windows 2008	

迁移 NNMi Oracle 数据		401
迁移 NNMi Oracle 数据	• • • •	401
其他升级信息		
配置差异	• • • •	403
应用程序故障切换	• • • •	404
MIB	••••	405
功能差异	• • • •	405

集成 NNMi

CiscoWorks LAN 管理解决方案	09
HP NNMi–CiscoWorks LMS 集成 4	109
价值	409
集成产品	410
文档	410
启用 HP NNMi–CiscoWorks LMS 集成 4	410
使用 HP NNMi–CiscoWorks LMS 集成	411
更改 HP NNMi–CiscoWorks LMS 集成配置 4	112
禁用 HP NNMi–CiscoWorks LMS 集成 4	112
对 HP NNMi–CiscoWorks LMS 集成进行故障诊断 4	112
CiscoWorks LMS 操作不运行 4	412
陷阱中的"MIB缓存中找不到 OID"消息4	112
HP NNMi–CiscoWorks LMS 集成配置表单参考 4	413
NNMi 管理服务器连接	413
CiscoWorks LMS 服务器连接 4	414
Clarus Systems ClarusIPC Plus ⁺	15
HP NNMi–Clarus Systems ClarusIPC Plus ⁺ 集成 4	115
关于 HP NNMi–Clarus Systems ClarusIPC Plus ⁺ 集成	416
价值	416
集成产品	416
文档	116
启用 HP NNMi–Clarus Systems ClarusIPC Plus ⁺ 集成	416
使用 HP NNMi–Clarus Systems ClarusIPC Plus ⁺ 集成	117
禁用 HP NNMi–Clarus Systems ClarusIPC Plus ⁺ 集成	117
对 HP NNMi–Clarus Systems ClarusIPC Plus ⁺ 集成进行故障诊断	41 7
HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus ⁺ 集成	117
关于 HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus ⁺ 集成	118
价值	118
集成产品	118
文档	118
启用 HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus ⁺ 集成	419
使用 HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus ⁺ 集成	119
禁用 HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus ⁺ 集成	419

对 HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus ⁺ 集成进行故障诊断	420
HP Asset Manager	
HP NNMi–HP Asset Manager 集成	421
价值	421
集成产品	422
文档	422
使用 HP NNMi–HP Asset Manager 集成	422
HP Business Service Management 拓扑	103
HP NNMi_HP BSM 拓扑集成	A94
价值	424
此 <u>出</u>	424
米/风/ 開	424
合用 HP NNMi_HP BSM 拓扑集成	425
使用 HP NNMi-HP BSM 拓扑集成	426
更改 HP NNMi-HP BSM 拓扑集成配置	427
禁用 HP NNMi-HP BSM 拓扑集成	
对 HP NNMi-HP BSM 拓扑集成进行故障诊断	
接口标签在 BSM 用户界面中显示为 MAC 地址	
RTSM 中被管节点的 CI 有重复	
应用程序故障切换和 HP NNMi-HP BSM 拓扑集成	428
HP NNMi–HP BSM 拓扑集成配置表单参考	429
NNMi 管理服务器连接	429
BSM 网关服务器连接	430
BSM 拓扑过滤器	430
HP Universal CMDB	433
HP NNMi-HP UCMDB 集成	433
价值	434
集成产品	434
文档	
使用 HP NNMi–HP UCMDB 集成	
HP Business Availability Center My BSM.	
HP NNMi-HP BAC My BSM 集成	435
价值	436
集成产品	
My BSM 的默认 NNM1 楔块	
配置演示 Portlet	438
创建目定义 NNMi Portlet	
開正 Portlet UKL	439
Portlet 正义 HTML 参考	440
フ HP NNMI-HP BAU My BSM 集成配直半点登求	442
N HP INIMI-HP BAU My BSM 集成进行故障诊断	
ININUI FORTIET 作为豆求贝亟不	442
ININIMI FOFLIEb 不比咖加致	443

	4.40
NNM 18P1 for Performance Portlet 木止佣加敏	443
NNM iSPI for Performance Portlet 显示 AsynchWait_Requests 错误	443
单点登录未正常运行	443
保存 Portlet 定义时, My BSM 报告 HTML 验证错误	443
HP NNMi-HP BAC My BSM 配置表单参考	444
HP Network Automation	447
HP NNMi–HP NA 集成	447
价值	448
前盘······ 隹	1/0
未成) 田・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
	449
后用 HP NNM1-HP NA 集成	449
从 NNMi 9.0x 升级的集成配置	450
新集成配置	451
使用 HP NNMi–HP NA 集成	453
NNMi 和 NA 之间的拓扑同步	453
完期同步注音重项	454
定规同少江志事次	, 404 /E/
又行 HP blade System virtual Connect 反奋	404
田集成提供的 NNM1 切能	455
从 NNMi 控制台启动 NA 视图	455
将 NA 诊断和命令脚本配置为事件操作	456
查看用于访问 NA 的事件操作的结果	457
识别具有不匹配状态的第 2 层连接	457
由集成提供的 NA 功能	458
发送设备配置更改通知	458
从之伏留出皇之伏远和 ····································	/58
	400
任	459
传播设备共用字符串更改	460
NA 事件规则	460
更改 HP NNMi–HP NA 集成	461
禁用 HP NNMi–HP NA 集成	461
对 HP NNMi–HP NA 集成进行故障诊断	462
测试集成	462
NNMi 拓扑中缺少 NA 设备	464
应田程序 按 陪 打 拖 和 HP NNM $_{\rm HP}$ N $_{\rm He}$ 体	161
四川祖川 W库 切贝尔 III IIIIIII III 来风 ····················	, 101 ///
IF NIMI-IF NA 朱成癿直衣牛穸写	404
NNMI 官理版务	465
NA 服务器连接	465
集成行为	466
NA 参考中的 NNMi 集成配置	467
集成通信	467
其他集成行为	468
HP ProCurve Manager Plus	469
HP NNMi–HP ProCurve Manager Plus 集成	469
价值	470
集成产品	470
文档	470

使用 HP NNMi–HP ProCurve Manager Plus 集成	471
HP RAMS MPLS WAN	
HP NNMi–HP RAMS MPLS WAN 集成	
价值	473
集成产品	474
文档	474
使用 HP NNMi–HP RAMS MPLS WAN 集成	474
HP SiteScope	
HP NNMi-HP SiteScope 事件集成	475
关于 HP NNMi–HP SiteScope 事件集成	476
价值	476
集成产品	476
支持的 SiteScope 监视器	476
文档	476
启用 HP NNMi–HP SiteScope 事件集成	477
使用 HP NNMi-HP SiteScope 事件集成	
史改 HP NNMi-HP SiteScope 事件集成	
第用 HP NNMI-HP SiteScope 事件集成	
M Hr NNMI-Hr SiteScope 事件集成近1 00 降らめ	
THAMIN 事件祝園中小亚小 SiteScopeAler LEVent 事件 于注从 SiteScope 事件中的 URL 正確打开 SiteScope	
HP NNMi_HP SiteScope 系统度量集成	479
关于 HP NNMi-HP SiteScope 系统度量集成	
价值	
集成产品	480
支持的 SiteScope 监视器	481
文档	481
启用 HP NNMi–HP SiteScope 系统度量集成	481
使用 HP NNMi–HP SiteScope 系统度量集成	484
更改 HP NNMi-HP SiteScope 系统度量集成	487
将连接从 NNMi 更改为 NPS	487
将连接从 SiteScope 更改到 NNMi	487
禁用 HP NNMi–HP SiteScope 系统度量集成	
祭用从 NNM1 到 NPS 的连接	
第用从 SiteScope 到 NNMI 的建按	
为 HP INIMI-HP SiteScope 杀统侵重朱成进行 故障诊断	
亚ய朱风奴讷加 讼证隹戓配署的 NNM; 遄	
远起来风配量的 NAT 环境中的节占于报告数据	491
HP NNMi-HP SiteScope 系统度量集成配置表单引用	492
HP Systems Insight Manager	
HP NNMI-HP SIM 集成	
1771 <u>组</u> 使	
禾/戏/ 阳・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	

使用 HP NNMi–HP SIM 集成	. 496
更改 HP NNMi–HP SIM 集成配置	. 496
禁用 HP NNMi–HP SIM 集成	. 496
对 HP NNMi–HP SIM 集成进行故障诊断	. 497
SIM 操作不运行	. 497
陷阱中的 "MIB 缓存中找不到 OID"消息	. 497
HP NNMi–HP SIM 集成配置表单参考	. 498
NNMi 管理服务器连接	. 498
SIM 服务器连接	. 499
nGenius Performance Manager	.501
HP NNMi–nGenius Performance Manager 集成	. 502
价值	. 502
集成产品	. 503
文档	. 503
启用 HP NNMi–nGenius Performance Manager 集成	. 503
使用 HP NNMi–nGenius Performance Manager 集成	. 504
禁用 HP NNMi–nGenius Performance Manager 集成	. 504
对 HP NNMi–nGenius Performance Manager 集成进行故障诊断	. 504
NNMi Northbound Interface	505
NNMi Northbound Interface	506
价值	506
иш	506
义义为顺平···································	506
小山	507
义怕	. 507
向用 INIMI Northbound Interface	. 507
使用 INIMI Northbound Interface 車件起空	. 500
事件投及 車件生合国期特式重地通知	. 500
事件生單戶規模心里以通知	. 509
事件大联週知	. 509
事件删陈进知	. 510
事件转反过滤器	. 510
更改 NNMi Northbound Interface	511
禁用 NNMi Northbound Interface	511
对 NNMi Northbound Interface 进行故障诊断	. 512
应用程序故障切换和 NNMi Northbound Interface	. 513
本地 Northbound 应用程序	. 513
远程 Northbound 应用程序	. 514
NNMi Northbound Interface 目标表单参考	. 515
Northbound 应用程序连接参数	. 515
NNMi Northbound Interface 集成内容	. 516
NNMi Northbound Interface 目标状态信息	. 518
HP BSM Operations Management	521
HP NNMi_HP BSM Operations Management 佳成	591
m management 朱成	. 041 500
И ഥ 住	. 044 500
木(株) 阳 テ地	. 044 E00
义怕	. 523

启用 HP NNMi—HP BSM Operations Management 集成	
使用 HP NNMi–HP BSM Operations Management 集成	526
配置项标识符	526
运行状况指示器	
默认策略条件	
自定义策略条件	528
更多信息	528
更改 HP NNMi—HP BSM Operations Management 集成	528
更新新 NNMi 陷阱的 SNMP 陷阱策略条件	529
更改配置参数	529
禁用 HP NNMi—HP BSM Operations Management 集成	530
对 HP NNMi—HP BSM Operations Management 集成进行故障	
BSM Operations Management 事件浏览器个包含转发的事件	
BSM Operations Management 事件浏览器仪包含某些转发的事件	
HP NNM1—HPOM 代理目标表甲参考 (BSM Operations Management 集成)	
BSM Integration Adapter 连接	
BSM Operations Management 集成内容	
BSM Integration Adapter 日标状态信息	
HP Operations Manager	
HP NNMi—HPOM 集成 (代理实施)	
关于 HP NNMi—HPOM 集成 (代理实施)	
价值	540
集成产品	
文档	
启用 HP NNMi—HPOM 集成 (代理实施)	
使用 HP NNMi–HPOM 集成 (代理实施)	546
配置项标识符	
运行状况指示器	546
默认策略条件	
自定义策略条件	548
更多信息	548
更改 HP NNMi—HPOM 集成配置 (代理实施)	548
更新新 NNMi 陷阱的 SNMP 陷阱策略条件	548
更改配置参数	549
禁用 HP NNMi–HPOM 集成(代理实施)	
对 HP NNMi-HPOM 集成 (代理实施)进行故障诊断	550
HPOM 活动消息浏览器不接收任何转发事件	550
HPOM 活动消息浏览器不接收某些转发事件	552
HP NNMi-HPOM 代理目标表单参考(代理实施)	553
HP Operations Agent 连接	553
HPOM 集成内容	
HP Operations Agent 日标状态信息	556
HP NNM1—HPOM 集成 (Web 服务实施)	

关于 HP NNMi–HPOM 集成 (Web 服务实施)	557
价值	558
集成产品	559
文档	559
启用 HP NNMi–HPOM 集成 (Web 服务实施)	559
HPOM for Windows	559
HPOM for UNIX 和 HPOM for Linux	561
使用 HP NNMi–HPOM 集成 (Web 服务实施)	563
用法示例	563
正常情况: MSI 条件未知	564
更多信息	564
更改 HP NNMi–HPOM 集成配置 (Web 服务实施)	564
禁用 HP NNMi–HPOM 集成 (Web 服务实施)	565
对于所有 HPOM 管理服务器	565
对于一个 HPOM 管理服务器	565
对 HP NNMi–HPOM 集成 (Web 服务实施)进行故障诊断	565
HPOM 不接收任何转发事件	565
HPOM 不接收某些转发事件	568
NNMi HPOM 消息浏览器中不提供事件信息	568
NNMi 和 HPOM 不同步	568
集成不能通过防火墙运行	569
HP NNMi-HPOM Web 服务集成配置表单参考	570
NNM i 管理服务器连接	570
HPOM 管理服务器连接	571
集成行为	572
事件过滤器	573
事件过滤器示例	574
事件过滤器限制	575
LID NINIAR Internetten Adentiale fen Nieten el Cefermen	577
HP INIMI Integration Module for Netcool Software	
价估	578
り ഥ · · · · · · · · · · · · · · · · · ·	
★/风/ Ⅲ	579
文句 ····································	
庙田 HP NNMi Integration Module for Notcool Software	581
更为 HP NNMi Integration Module for Netcool Software	589
並用 HP NNMi Integration Module for Netcool Software 林田 HP NNMi Integration Module for Netcool Software	582
对 HP NNMi Integration Module for Netcool Software 进行故障诊断	583
Notcool/OMNIbus 不接收任何转发的 NNM; 管理事件	583
Netwool/OMNIbus 不按收其此转发的 NNM; 管理事件:	
自动第9 目在接的 NNM; 表的时出错	505
旧约和4匹达取的ININII 农牛时田田	504 595
III INTANI Integration module for Network of 中心水牛多方	505 525
在成内容	505 586
來/writg ····································	500
日 マルアハ心 旧心 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	

Matters (以前称作 AlarmPoint))]
HP NNMi–xMatters 集成	92
关于 HP NNMi–xMatters 集成 55	92
价值	92
集成产品	93
文档55	93
启用 HP NNMi–xMatters 集成 55	93
使用 HP NNMi-xMatters 集成 55	94
禁用 HP NNMi-xMatters 集成 59	95
对 HP NNMi-xMatters 集成进行故障诊断 59	95
HP NNMi-xMatters 移动访问集成 55	95
关于 HP NNMi-xMatters 移动访问集成 55	95
价值	95
集成产品	95
文档	96
启用 HP NNMi–xMatters 移动访问集成59	96
使用 HP NNMi-xMatters 移动访问集成 59	96
禁用 HP NNMi-xMatters 移动访问集成 59	97
对 HP NNMi-xMatters 移动访问集成进行故障诊断5	97

更多信息

NNMi 环境变量	
本文档中使用的环境变量	601
其他可用环境变量	601
NNMi 9.10 和已知端口	605
建议的配置更改	
消息和解决方案	609
问题和解决方案	
Glossary	615
感谢您的反馈!	

关于本指南



(1) 首次安装或测试台

请遵循《NNMi 安装 指南》中的步骤操作





以前版本迁移

阅读《NNMi 部署参考》 (本书)



本章包含以下主题:

- 本指南有哪些内容?
- 本文档中使用的路径约定 •
- 修订历史 •
- 有关 NNMi 的详细信息 •

本指南有哪些内容?

本指南包含用于部署 HP Network Node Manager i Software (包括 NNMi 和 NNMi Advanced) 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 启动配置向导配置共用字符串、设置网络节点有限范围的搜索和创建初始管理员帐户。要更 详细地了解这些任务,请参阅《NNMi 安装指南》(参阅第3页的可用产品文档)。

HP 在有新信息可用时,会在产品版本之间更新此指南。有关检索本文档的更新版本的信 息,请参阅第3页的可用产品文档。

本文档中使用的路径约定

对位于 NNMi bin 目录中的命令,本文档不包括命令路径。 NNMi bin 目录的位置如下:

- Windows Server 2008: < 驱动器>\Program Files\HP\HP BTO Software\bin
- UNIX[®]: /opt/OV/bin

本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 2008:
 - %NnmInstallDir%: <驱动器>\Program Files\HP\HP BTO Software
 - %NnmDataDir%: < 驱动器>\ProgramData\HP\HP BTO Software

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。

- UNIX:
 - \$NnmInstallDir: /opt/OV
 - \$NnmDataDir: /var/opt/OV
- 在 UNIX 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,您可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根据。这些变量形式为 NNM_*。有关该 NNMi 环境变量扩展列表的信 息,请参阅第 601 页的其他可用环境变量。

修订历史

下表列出了本文档的每个新版本的主要更改。

文档发行日期	主要更改的描述
2011年3月(9.10)	完全更新。 • 英语第四版。 • 日语第三版。

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。



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,请参阅第3页的可用产品文档。

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的 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 或 NNMi Advanced (第一次)。	下载《NNMi 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。
	 HP Network Node Manager i Software 安装指南(用于 Windows 操作系统)
	 HP Network Node Manager i Software 安装指南(用于 HP-UX 操作系统)
	• HP Network Node Manager i Software 安装指南(用于 Linux 操作系统)
	• HP Network Node Manager i Software 安装指南(用于 Solaris 操作系统)
计划网络部署,包括系统要求的链接。	请参阅本指南的第31页的准备。
为生产环境配置 NNMi。	请参阅本指南的第37页的配置。
在后台配置 NNMi。	请参阅本指南的第113页的高级配置。
维护 NNMi 配置。	请参阅本指南的第 345 页的维护 NNMi。
从 Network Node Manager i Software (NNMi 9.0x) 的以前版本升级到 NNMi。	请参阅本指南的第 391 页的升级自 NNMi 9.0x。
从 Network Node Manager (NNM 6.x/7.x) 的以前版本升级到 NNMi。	下载《NNMi升级参考》。
更详细地了解与 NNMi 集成的产品。	请参阅本指南的第407页的集成 NNMi。
参考 NNMi 环境变量、端口和消息。	请参阅本指南的第599页的更多信息。
获取有关特定主题的详细信息。	按示例文档和白皮书下载。

2011年3月

您要做什么?	从何处查找详细信息
打印 NNMi 帮助。	下载帮助内容的 PDF。
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 计 划和安装指南》。
获取有关 NNM 开发人员工具包 (SDK) 的 文档。	下载《HP Network Node Manager i Software 开发人员工具包指南》。



本部分包含以下章:

• 硬件和软件要求

硬件和软件要求

本章包含以下主题:

- 支持的硬件和软件
- 检查必需补丁
- 系统配置 (UNIX)
- 安装 NNMi 和 NNM iSPI
- NNMi 与 HP Performance Insight 的共存性
- NNMi 与 HP Operations Agent 的共存性

支持的硬件和软件

在安装 NNMi 之前,请阅读有关在表 1 中描述的 NNMi 硬件和软件要求的信息。



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

表1	软件和硬件预安装清单
· · · ·	

完成 (是 / 否)	要阅读的文档
	《NNMi 安装指南》
	• 文件名 = install-guide_zh_CN.pdf
	• Windows 介质 = DVD 主驱动器 (根)
	• UNIX 介质 = 根目录
	• NNMi 控制台 = 帮助 > NNMi 文档库 > 安装指南
	NNMi 发行说明
	• 文件名 = releasenotes_zh_CN.html
	• Windows 介质 = DVD 主驱动器 (根)
	• UNIX 介质 = 根目录
	• NNMi 控制台 = 帮助 > NNMi 文档库 > 发行说明
	NNMi 系统和设备支持列表
	• 文件名 = supportmatrix_zh_CN.html
	• Windows 介质 = DVD 主驱动器 (根)
	• UNIX 介质 = 根目录
	• NNMi 控制台 = 链接自发行说明



如果新信息可用, HP 将更新 NNMi 系统和设备支持列表。在部署 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。)



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

NNMi 提供嵌入式 Java 虚拟机和 JDK V1.6。Java 需要特定操作系统补丁才能正确工作。 如果计划在运行 HP-UX 操作系统的服务器上安装 NNMi,可以运行 HPjconfig 命令以 查看服务器是否已安装所需补丁。运行 HPJconfig 时,请针对 JDK V1.6 做出正确选择。 有关在 HP-UX 上安装和运行 HPjconfig 的详细信息,请访问以下 URL:

https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPJCONFIG

如果计划在运行受支持操作系统(HP-UX 除外)的服务器上安装 NNMi,请参考这些操 作系统的发行说明。

系统配置 (UNIX)

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,需要在安装任何 HP NNM iSPI 之前先安装 NNMi。

NNMi 与 HP Performance Insight 的共存性

如果计划将 NNMi 与 HP Performance Insight 安装在同一台服务器上,请遵循此过程以 避免发生安装顺序和端口冲突问题:

1 首先安装 HP Performance Insight。

请在完成步骤1和步骤2之后再安装NNMi。

- 2 停止所有 HP Performance Insight 进程。
- 3 安装 NNMi。请参阅《NNMi 安装指南》,以了解具体说明。
- 4 停止所有 NNMi 进程:

ovstop -c

- 5 修改 nms-local.properties 文件以解决任何端口冲突。可在以下目录中找到此文件:
 - Windows: %NNM CONF%\nnm\props
 - UNIX: \$NNM CONF/nnm/props
- 6 启动 HP Performance Insight 进程。
- 7 启动所有 NNMi 进程:

ovstart -c

当 NNMi 与 HP Performance Insight 安装在同一台服务器上,卸载 NNMi 会导致运行 HP PI MIB 浏览器时发生异常。要阻止此异常,请完成以下步骤:

- 1 卸载 NNMi。
- 2 重新创建 snmpmib MIB 数据库:
 - a mkdir -p /var/opt/OV/shared/nnm/conf/
 - b /opt/OV/lbin/nnmloadmib -load /usr/OVPI/mibs/GENMIB2IF.mib
- 3 使用 nnmloadmib.ovpl 命令加载其他 MIB。

NNMi 与 HP Operations Agent 的共存性

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。
配置

本部分包含以下各章:

- 配置的常规概念
- NNMi 通信
- NNMi 搜索
- NNMi 状态轮询
- NNMi 事件
- NNMi 控制台





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
- 最佳实践:保存现有配置
- 最佳实践:使用作者属性
- 用户界面模型
- 排序
- 节点组和接口组
- 节点/接口/地址层次结构
- 停下来,重新开始

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。
- 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 UNIX 联机帮助页。

nnmconfigexport.ovpl 命令不保留 SNMPv3 凭证。有关详细信息,请参阅 nnmconfigexport.ovpl 参考页或 UNIX 联机帮助页。

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。



搜索种子表单是事务方法的一个例外。在**搜索配置**表单上提供此表单是为了方便,但它与其 余搜索配置无关。出于此原因,必须先保存并关闭**搜索配置**表单以实现自动搜索*规则*,才能 配置那些规则的搜索种子。

排序

某些 NNMi 控制台配置表单包括**排序**属性,此属性设置配置应用的优先级。对于一个配置 区域, NNMi 从最小(最低)排序编号到下个最低排序编号(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。如果看到意外的搜索或状态结果,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。

- **最佳实践** 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。
- **最佳实践** 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,主要过滤技术是对节点或接口分组,然后将设置应用于组或按组过滤可见性。 节点组可用于以下任何或全部用途:

- 监视设置
- 事件负载过滤
- 表过滤
- 自定义图视图
- 对于全局网络管理功能,过滤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一或全部两个用途:

- 从搜索中排除接口
- 监视设置
- 事件负载过滤
- 表过滤

您可以根据任何可过滤的属性来创建节点组的层次结构,从而控制图视图向下钻取和/或监视设置的继承。

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:



- 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。可以用设备类别过滤器执行此操作。
- 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,供进行 IOS 升级。可以用供应商过滤器执行此操作。
- 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 地址过滤器执行此操作。

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 通过比较每个搜索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。



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。
- 匹配设备过滤器选项卡上的一个或多个条目(如果有)和其他过滤器选项卡上所指定过滤器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。

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。

设备过滤器

在搜索期间,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,请参阅第 60 页的 NNMi 通过设备配置文件得出属性。)通过采集系统对象 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过滤器。

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。

其他过滤器

可以使用其他过滤器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)

过滤器可包括 AND、OR、NOT、EXISTS、NOT EXISTS 和分组(圆括号)操作。有关详细信息,请参阅 NNMi 帮助中的*指定节点组其他过滤器*。

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。可通过检查已搜索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

Λ

最好使用**其他过滤器**限定节点组的节点。如果网络包含很难用过滤器限定的关键设备,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。

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清空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。(从 NNMi 8.x 升级将保留以前的状态计算设置。)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 或其他属性过滤节点内的接口,如 ifAlias、 ifDescr、 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过滤接口组。

在选项卡内部和选项卡之间,会对接口组资格执行 AND 计算。

节点 / 接口 / 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。

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。

停下来,重新开始

如果要完全地重新启动搜索并重做所有 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 UNIX 联机帮助页。

遵循以下步骤:

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。

nnmconfigexport.ovpl 命令不保留 SNMPv3 凭证。有关详细信息,请参阅 nnmconfigexport.ovpl 参考页或 UNIX 联机帮助页。

- 4 可选。使用 nnmtrimincidents.ovpl 命令可将 NNMi 事件存档。
- 5 丢弃并重新创建 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 数据库管理员丢弃并重新创建 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。执行以下某个操作:
 - 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。



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) 搜索设备和监视设备状态及运行状况。要在环境中建立可行通信,请配置 NNMi 的访问凭证和相应的超时,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通信量或不防碍防火墙。

配置的通信值构成 NNMi 搜索和状态轮询的基础。为搜索或轮询进行查询时,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 搜索和 NNMi 状态轮询都不能向该区域 发送 SNMP 请求。

本章包含以下主题:

- 通信的概念
- 计划通信
- 配置通信
- 评估通信
- 调整通信

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。对特定 MIB 对象的 SNMP 请求的响应提供有关节点的更全面信息。

以下概念应用于 NNMi 通信配置:

- 通信配置的级别
- 网络延迟和超时
- SNMP 访问控制
- SNMP 版本首选项
- 管理地址首选项
- 轮询协议
- 通信配置和 nnmsnmp*.ovpl 命令

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,可以配置访问凭证,超时和重试值、ICMP和 SNMP协议支持以及 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 ICMP 和 SNMP 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 和 SNMP 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 或 SNMP 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后才放弃, 然后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证:

• SNMPv1 和 SNMPv2c

每个 NNMi 请求中的共用字符串必须与响应 SNMP 代理中配置的共用字符串匹配。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 户名及其关联身份验证要求(身份验证配置文件)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身份验证和隐 私控制。

- 身份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。

NNMi 对网络的某区域(通过 IP 地址过滤器或主机名过滤器定义)支持指定多个 SNMP 访问控制凭证。通过在给定 SNMP 安全级别并行尝试所有配置的值, NNMi 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)用于搜索和监视目的。

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证 和 SNMP 版本。

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 搜索,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 搜索,则 NNMi 丢弃传入的 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(仅 SNMPv1)— NNMi 尝试使用具有共用字符串、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 尝试使用具有共用字符串、超时和重试次数配置值的 SNMPv2c 进行通信。如果使用 SNMPv2c 时对任何共用字符串没有响应,则 NNMi 尝试使用具有共用字符串、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。
- 共用—NNMi 尝试使用具有共用字符串、超时和重试次数配置值的 SNMPv2c 进行通信。 如果使用 SNMPv2c 时对任何共用字符串没有响应,则 NNMi 尝试使用具有共用字符 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 对于没有身份验证和隐私的用户,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 必要时尝试具有身份验证但无隐私的用户,然后尝试具有身份验证和隐私的用户。
- 验证,无隐私 对于具有身份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 尝试具有身份验证和隐私的 用户。
- 验证, 隐私 对于具有身份验证和隐私的用户, 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。通过从搜 索中排除某些地址,可以在搜索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*。

NNMi 持续地搜索和监视设备。*在第一个NNMi 搜索周期*之后,当以前搜索的 SNMP 代理 退出响应(例如,重新配置设备的 SNMP 代理)时,**启用 SNMP 地址重新搜索**字段控制 NNMi 的行为。

- 如果选中启用 SNMP 地址重新搜索复选框,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 地址重新搜索复选框,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。

启用 SNMP 地址重新搜索复选框在通信配置的所有级别都可用。



搜索所有 SNMP 设备和非 SNMP 设备自动搜索规则配置字段影响 NNMi 使用 SNMP 的方式。 有关详细信息,请参阅 NNMi 帮助中的*配置自动搜索规则的基本设置*。

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 通信量时)。

在网络某区域中禁用对设备的 ICMP 通信量导致在 NNMi 中发生以下结果:

- 可选自动搜索规则 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 搜索协议 (CDP)或极限搜索协议 (EDP)。除非播种每一个广域网络设备,否则它们可能会丢失。
- 状态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,则状态轮询器不使用 ICMP。)
- 操作员不能使用操作 > ping 在故障诊断期间检查设备可达性。

在网络某区域中禁用对设备的 ICMP 通信量导致在 NNMi 中发生以下结果:

- 搜索只能采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。
- 搜索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。

- 搜索无法采集设备的连接性信息,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,状态轮询器遵从监视默认值即仅使用 ICMP (ping) 的设备。
- 状态轮询器无法采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
- 通信配置区域
- 特定节点配置
- 重试和超时值
- 活动协议
- 多个共用字符串或身份验证配置文件

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 应当尝试的常用共用字符串?
- 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。相距多个跳数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:



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,具体取决于将通信量管理配置设置为首选离 NNMi 管理服务器一个还是两个跳数的路径。

区域还用于对具有相似访问凭证的设备分组。如果网络中的所有路由器都使用相同共用字符串(或一小组可能的共用字符串)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、重试值以及访问凭证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

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。

要获取每个跳数的当前延迟时间的信息,请执行以下操作:

- Windows: 对每个网络区域中的设备运行 tracert。
- UNIX: 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 生成的通信量类型:通信和监视配置设置。基础结构中的防火墙禁止 ICMP 或 SNMP 通信量时,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通信量。

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应当接收 ICMP 通信量。

对于您不提供访问凭证的设备,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。

多个共用字符串或身份验证配置文件

计划对网络的每个区域都尝试的共用字符串和身份验证配置文件。对于默认和区域设置,可以配置要并行尝试的多个共用字符串和身份验证配置文件。

尝试可能的共用字符串时,NNMi查询可能导致设备的身份验证失败。NNMi完成其初始 搜索时,您可通知运营部门可以安全地忽略身份验证失败。另外,通过尽可能紧密地配置 区域(和要尝试的关联共用字符串及身份验证协议),可以将身份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 共用字符串

对于可接受 SNMPv1 或 v2c 访问的区域,采集区域中使用的共用字符串和特定设备必需的 任何唯一共用字符串。

SNMPv3 身份验证配置文件

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身份验证配置文件、 适合每个区域的身份验证配置文件和特定设备上使用的唯一身份验证凭证(如果有)。还要 确定网络中使用的身份验证和隐私协议。

对于 SNMPv3 通信, NNMi 支持以下身份验证协议:

- 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)身份验证协议和一个 (或不指定) 隐私协议。



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。有关详细信息,请参阅第 56 页 的准备 NNMi 以使用 SNMPv3 隐私协议。

配置通信

阅读本节中的信息之后,请参阅 NNMi 帮助中的 配置通信协议,以了解具体过程。

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,请参阅第40页的最佳实践:保存现有配置。

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。

保存并关闭 NNMi 控制台的所有通信配置表单,以实现更改。

最佳实践 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。

准备 NNMi 以使用 SNMPv3 隐私协议

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。

要使 NNMi 能够使用 AES-192、 AES-256 和 TripleDES 隐私协议进行 SNMPv3 通信, 请遵循以下步骤:

1 从适用于 Java 开发人员的 "Oracle 技术网" 网站

(http://www.oracle.com/technetwork/java/index.html) 下载 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 库。 直接链接是: https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/ CDS-CDS_Developer-Site/en_US/-/USD/ViewProductDetail-Start? ProductRef=jce_policy-6-oth-JPR@CDS-CDS_Developer

- 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
 - UNIX: \$NnmInstallDir/nonOV/jdk/nnm/jre/lib/security
- 3 通过运行以下命令,重新启动 ovjboss:
 - a ovstop ovjboss
 - b ovstart ovjboss

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。仅当完成搜索之后,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?
- SNMP访问当前是否对设备可用?
- 管理 IP 地址是否正确?
- NNMi 使用的通信设置是否正确?
- 状态轮询器设置是否符合通信设置?

是否为 SNMP 配置了所有节点?

- 1 打开**节点**资产视图。
- 2 过滤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 点并更新访问凭证。
 - 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 在资产视图中选择节点。
- 2 选择操作 > 轮询 > 状态轮询或操作 > 轮询 > 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 UNIX 联机帮助页。

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,请遵循以下步骤:

- 1 在资产视图中选择节点。
- 2 选择操作 > 配置详细信息 > 通信设置。
- 3 在通信配置窗口中,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 共用字符串缺失或不正确可能导致搜索无法完成,或可能对搜索性能产生负面影响。要验证为设备配置的通信设置,请使用 nnmcommconf.ovpl 命令或遵循以下步骤:

- 1 在资产视图中选择节点。
- 2 选择操作 > 配置详细信息 > 通信设置。
- 3 在通信配置窗口中,验证 SNMP 配置设置表中列出的值是否是要 NNMi 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。

状态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通信量,监视设置中也可能禁用该类型的通信量。 要确定是否将覆盖设置:

- 1 在资产视图中选择节点。
- 2 选择操作 > 配置详细信息 > 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通信量,则 NNMi 不会发送该通信量。

调整通信

- **减少身份验证失败** 如果 NNMi 在搜索期间生成太多身份验证陷阱,则为较小的区域或特定节点配置较小的访问凭证组供 NNMi 尝试。
- **调整超时和重试次数** NNMi 尝试在搜索期间使用 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 共用字符串时,或如果 NNMi 正在搜索非 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搜索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。
- **减少默认共用字符串** 拥有大量默认共用字符串可能会对搜索性能产生负面影响。请不要输入太多默认共用字符 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共用字 符串配置。

NNMi 搜索



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) 搜索 将用网络中有关节点的信息填充拓扑资产。 NNMi 在螺旋搜索进行过程中维护此拓扑信息,确保根源分析和故障诊 断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 搜索。有关搜索工作方式的介绍和有关如何配置搜索的详细信息,请参阅 NNMi 帮助中的 搜索您的网络。

如果您有使用 NNM 6.x/7.x 的经验,并希望了解 NNMi 9.10 中的搜索有哪些变化,请参阅《NNMi 升级参考》中的"网络搜索",以了解这些差异的高级概述。

本章包含以下主题:

- 搜索的概念
- 计划搜索
- 配置搜索
- 评估搜索
- 调整搜索

搜索的概念

只搜索路由器和交换机的 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搜索哪些设备并将它们包括在 NNMi 拓扑中。搜索配置可以非常简单,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。

NNMi 不执行任何默认搜索。您必须在 NNMi 拓扑中出现任何设备之前配置搜索。

搜索的每个节点(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搜索方式。

状态监视的注意事项也可能影响您的选择。默认情况下,状态轮询器只监视连接到 NNMi 已搜索的设备的接口。对于某些网络区域,您可以覆盖此默认值,可以搜索超出您负责范围 的设备。(有关状态轮询器的信息,请参阅第 77 页的 NNMi 状态轮询。)

NNMi 提供两个主要的搜索配置模型:

- **基于列表的搜索** 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。
- 基于规则的搜索 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 搜索已定义的设备。

可使用基于列表和基于规则的搜索的任意组合来配置 NNMi 应当搜索的设备。初始搜索将 这些设备添加到 NNMi 拓扑,然后螺旋搜索会例行地重新搜索网络以确保拓扑保持最新。

如果计划配置多租户,请在启动网络搜索之前配置租户。

NNMi 通过设备配置文件得出属性

当 NNMi 搜索设备时,它使用 SNMP 直接采集某些属性。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。

在搜索期间,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。

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。

计划搜索

作出关于以下方面的决策:

- 选择您的主搜索方式
- 自动搜索规则
- 节点名称解析
- 子网连接规则
- 搜索种子
- 重新搜索间隔
- 不搜索对象

选择您的主搜索方式

决定是执行完全基于列表搜索、完全基于规则搜索,还是两种方式结合使用。

基于列表的搜索

使用基于列表的搜索,可明确指定(作为搜索种子)NNMi应搜索的每个节点。

如果计划配置多租户,建议采用基于列表的搜索方法。

只使用基于列表的搜索的好处包括:

- 提供对 NNMi 所管理对象的严密控制。
- 支持在搜索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搜索规则。

只使用基于列表的搜索的缺点包括:

- 将新节点添加到网络时, NNMi 不搜索它们。
- 必须提供要搜索的节点的完整列表。

基于规则的搜索

使用基于规则的搜索,创建一个或多个自动搜索规则,以定义 NNMi 应搜索并包括在 NNMi 拓扑中的网络区域。对于每条规则,必须提供一个或多个搜索种子(通过明确指定 种子或通过启用 Ping 扫描),然后 NNMi 自动搜索网络。

使用基于规则的搜索的好处包括:

• 适合大型网络。 NNMi 可基于最小配置输入搜索大量设备。

- 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搜索(假定每个设备都由自动搜索规则涵盖)。
- 确保添加到网络的任何新设备的搜索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。

使用基于规则的搜索的缺点包括:

- 更容易达到许可证限制数。
- 根据网络的结构不同,调整自动搜索规则可能很复杂。
- 如果自动搜索规则非常广泛,并且 NNMi 搜索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。
- 所有无种子节点在搜索时都将接收默认租户。如果要使用 NNMi 多租户,必须在搜索后 更新租户分配。

仅针对基于规则的 自动搜索规则 搜索

自动搜索规则排序

自动搜索规则的排序属性的值通过以下方式影响搜索范围:

IP 地址范围

如果设备处于两个自动搜索规则范围内,则应用具有较低排序编号的自动搜索规则的设置。例如,如果自动搜索规则排除了一组 IP 地址,则不会有更高排序编号的其他自动 搜索规则处理那些节点,且该地址范围中的节点不会被搜索,除非它们被列为搜索种子。

- 系统对象 ID 范围
 - 如果自动搜索规则中没有包括 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搜索规则。
 - 如果自动搜索规则中包括 IP 地址范围,则系统对象 ID 范围只应用于自动搜索规则内。

从搜索中排除设备

- 要阻止搜索某些对象类型,请创建具有较低排序编号的自动搜索规则,它会忽略您不想 搜索的系统对象 ID。不要在此规则中包括 IP 地址范围。通过为此自动搜索规则指定较 低排序编号,该搜索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搜索规则。被忽略范围 中的设备可包括在另一个自动搜索规则中。

搜索配置表单的排除的 IP 地址选项卡上列出的地址应用于所有自动搜索规则。除非将这些地址配置为搜索种子,否则不会将它们添加到 NNMi 拓扑。(搜索种子始终会被搜索。)

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 搜索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 扫描在已配置自动搜索规则的 IP 地址范围中查找设备。对于初始搜索,您可能希望对所有规则启用 Ping 扫描。这样就为不需要配置搜索种子的 NNMi 搜索提供了足够信息。



Ping 扫描适用于 16 位或更小的子网,例如 10.10.*.*。

Ping 扫描尤其适用于搜索未控制的 WAN 上的设备,如 ISP 网络。

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 扫描的设备的所有通信量。

最佳实践

只对较小的搜索范围启用 Ping 扫描。

来自 SNMP 陷阱的搜索提示

从 NNMi 9.01 起, NNMi 将接收的 SNMP 陷阱的源 IP 地址处理为自动搜索规则的提示。 此功能对于搜索 WAN 上的设备特别有用。

自动搜索规则的搜索种子

为每个自动搜索规则至少提供一个搜索种子。用于提供种子的选项如下:

- 在搜索配置表单的搜索种子选项卡上输入种子。
- 使用 nnmloadseeds.ovpl 命令以从种子文件加载信息。
- 至少对于初始搜索,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。

自动搜索规则的最佳实践

- 因为 NNMi 自动管理所有搜索的设备,所以,请使用精确匹配要管理的网络区域的 IP 地 址范围。
 - 可以在自动搜索规则中使用多个 IP 地址范围来限制搜索。
 - 可以将大型 IP 地址范围添加到自动搜索规则, 然后从搜索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。

示例

搜索规则重叠

图 1 显示重叠的两个搜索范围。左侧的圆圈表示 NNMi 搜索忽略的 IP 地址范围或系统对 象 ID 范围。右侧的圆圈表示要搜索并包含在 NNMi 拓扑中的 IP 地址范围或系统对象 ID 范围。重叠区域可能会由搜索包括或忽略,这取决于这些自动搜索规则的排序。

图1 重叠的搜索范围



限制设备类型搜索

要搜索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搜索规则。在此自动搜索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

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搜索它。(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。

最佳实践 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。



搜索

完整 DNS 名称是命名约定时,拓扑图上的标签可能很长。

最佳实践 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。(NNMi 8.0x 选择最高环回地址作为管理地址。)

子网连接规则

- **仅针对基于列表的** 对于基于列表的搜索, NNMi 使用子网连接规则来检测跨 WAN 的连接。NNMi 评估它在 搜索 可能连接的每个末端搜索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。
- **仅针对基于规则的** 启用自动搜索规则且 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 如果搜索匹配,则 NNMi 使用子网中的每个有效地址作为提示,并尝试搜索该地址。

最佳实践 使用默认连接规则。请只在有问题时修改它们。

搜索种子

列出设备以用作搜索种子。

- 最佳实践 选择首选管理 IP 地址的 NNMi 规则之一将指定使用第一个搜索的 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。
- **最佳实践** 对于 Cisco 设备,使用环回地址作为搜索种子,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** 对基于列表的搜索,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 搜索 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 搜索

搜索种子对基于规则的搜索是可选的:

- 如果为自动搜索规则启用 Ping 扫描,则不需要指定该规则的种子。
- 对禁用 Ping 扫描的每个自动搜索规则,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。
- **最佳实践** 对于最完整的基于规则的搜索,请使用路由器而非交换机作为搜索种子,因为路由器通常具 有比交换机更大的 ARP 缓存。连接到要搜索的网络的核心路由器是搜索种子的最好选择。

重新搜索间隔

NNMi 按照配置的重新搜索间隔,重新检查数据库中的每个设备的配置信息。此外,NNMi 从自动搜索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搜索;只在配置的重新搜索间隔更新设备:

- 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。

选择重新搜索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。

不搜索对象

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,请参阅第 51 页的轮询协议。
- 在搜索配置表单上,可设置指示 NNMi 不从某些 IP 地址或 SNMP 系统对象 ID 采集提示的自动搜索规则。与条件匹配的节点仍然出现在图和数据库中,但螺旋搜索不扩展到超出这些 IP 地址或对象类型的相邻设备。
- 在搜索配置表单上,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 自动搜索规则。螺旋搜索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。

通过 NNMi 监视虚拟 IP 地址

NNMi 搜索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。群集故障切换到新主动节点之后, 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, 因为故障切换和 NNMi 搜索更改之间,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 搜索的群集中的成员数。NNMi搜索额外的(+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 搜索虚拟 IP 地址。 NNMi 使用此方法搜索与配置为使 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 节点进行搜索和监视。

• 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。

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搜索配置。
- 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搜索中排除的地址列表。
- 4 保存工作。

配置搜索

本部分列出配置提示,并提供一些配置示例。读完这部分信息之后,请参阅 NNMi 帮助中的 配置搜索,以了解具体步骤。



因为一旦**保存并关闭搜索种子**表单, NNMi 即会启动来自种子的搜索, 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。
- 完成所有自动搜索规则(如果有)。
- 配置子网连接规则。
- 配置名称解析首选项。
- 始终选择保存并关闭直到返回控制台。

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,请参阅第 40 页的最佳实践:保存现有配置。

配置自动搜索规则的提示

• 定义新自动搜索规则时,仔细检查每个设置。对于新规则,默认启用自动搜索,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

- 如果已有文件列出要搜索的节点,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 地址 1 # 节点名称
 - IP 地址 2, <租户 UUID 或租户名称> # 节点名称

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 搜索新节点,但不重新计算现有节点。
- 从种子文件删除节点时,不会从 NNMi 拓扑删除它。直接在 NNMi 控制台中删除节点。
- 从图或资产视图删除节点时不删除种子。
- 如果希望 NNMi 重新搜索节点,请从图或资产视图 以及 NNMi 控制台中的搜索配置表 单上的搜索种子选项卡删除该节点,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 搜索

 为搜索规则指定种子之前要完全配置好它。即在搜索配置表单上单击保存并关闭。(尽管 它似乎已连接,但搜索种子选项卡是单独的表单,不是数据库模型中搜索配置表单的一部 分。因此,保存有关搜索种子选项卡的信息时,NNMi立即更新种子配置。)

评估搜索

此部分列出了评估搜索进度和是否成功的方式。

跟踪初始搜索的进度

NNMi 搜索是动态的并持续进行;它不会完成,因此您不会看到"搜索已完成"的消息。 初始搜索和连接过程要花一些时间。以下各项建议估计初始搜索进度的方式:

- 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。在初始搜索期间,打开系统信息窗口若干次。
- 在搜索配置表单上查看搜索种子选项卡。刷新此选项卡,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通性。
- 为代表性节点打开节点表单。搜索状态字段变为搜索已完成时,NNMi 已采集节点的基本 特征以及节点的 ARP 缓存和搜索协议邻居(如果适用)。此状态不表示该 NNMi 已完 成该设备的连通性分析。
- 在节点资产视图中,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通性分析。
- 查看第2层连接和 VLAN 资产视图,以估计第2层处理的进度。

所有种子都搜索了吗?

- 1 打开搜索配置表单。
- 2 在**搜索种子**选项卡上,按**搜索种子结果**列对节点列表排序。对处于错误状态的任何节点, 请考虑以下事项:
 - 由于无法访问的节点或无法解析的 DNS 名称而失败的搜索——对于这些失败类型,请 验证网络与节点的连通性并检查准确的 DNS 名称解析。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。

- 超过许可证节点计数 这场景发生在搜索的设备数达到许可证限制时。可删除某些搜索的节点或购买更多的节点包许可证。
- 已搜索节点但没有 SNMP 响应 对于已播种设备和通过自动搜索而搜索的设备, SNMP 通信都可能发生问题。有关详细信息,请参阅第 56 页的评估通信。

所有节点都具有有效的设备配置文件吗?

- 1 打开**节点**资产视图。
- 2 过滤设备配置文件列,以包含字符串无设备配置文件。
- 3 如果已搜索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。

所有节点都正确搜索了吗?

要避免搜索时出现问题,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。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**资产视图中检查数据。如果任何节点没有管理地址,则检查通信设置中是否有第57页的是否为 SNMP 配置了所有节点?中所述的那些节点。

如果预期的节点不在节点资产视图中,则检查以下事项:

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

仅基于列表的搜索 自动搜索规则

如果看到意外的搜索结果,则重新计算自动搜索规则。

当 NNMi 搜索找到地址提示时,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 搜索丢弃提示。自动搜索规则的排序编号确定应用自动搜索规则配置设置的顺序。

对于每个自动搜索规则,请检查以下设置:

- 必须启用搜索包含的节点,该规则才会自动搜索。
- 对于您要为该规则搜索的节点类型,验证以下设置是否正确:
 - 一 搜索所有 SNMP 设备
 - 一 搜索非 SNMP 设备

请记住,默认情况下只搜索路由器和交换机,而不搜索非 SNMP 节点。启用这些设置时若未考虑您的环境,则可能导致 NNMi 搜索比预期更多的节点。

IP 地址范围

搜索提示的 IP 地址必须匹配 IP 地址范围列表中的包含在规则中条目。如果自动搜索规则中没有包括 IP 地址范围,则将所有地址提示都视为匹配。(有关此情况,请参阅第 68 页的配置自动搜索规则的提示。)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。

- 如果没有搜索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。
- 如果您搜索了比所需更多的设备,则修改包括范围,或对不想搜索的设备的 IP 地址添加忽略范围。同时,确定启用了搜索所有 SNMP 设备。

系统对象 ID 范围

来自搜索提示的系统对象 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。 如果自动搜索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 范围可展开自动搜索,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搜索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充分时间进行初始搜索。

评估第 2 层连通性

要评估第2层连通性,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**资产中,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 资产视图打开每个 VLAN 表单,然后检查该 VLAN 的端口列表。

NNMi 搜索与重复的 MAC 地址

在搜索期间,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,以查找有关搜索的节点的信息。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:

如果两个或更多被搜索节点包含与相同 MAC 地址关联的接口, NNMi 会忽视 FDB 中这些重复的 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—*全局网络管理功能*:如果两个NNMi 管理服务器都搜索了包含与相同 MAC 地址关联的接口的节点,全局 NNMi 管理服务器图可能缺少区域 NNMi 管理服 务器图上可见的连接。

 如果单个节点包含具有相同 MAC 地址的多个接口, 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。

重新搜索设备

- 1 执行设备的配置轮询。
- 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。

调整搜索

对于常规搜索性能,请微调搜索配置以只搜索关键和重要设备。

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

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。

有些特殊搜索环境可以通过抑制搜索协议采集或 VLAN 索引来补救。有关详细信息,请参阅第 366 页的抑制对特定节点使用搜索协议或第 369 页的抑制对大型交换机使用 VLAN 索引。
搜索日志文件

在 nnm.?.0.log 文件中, 查找对于以字符串 com.hp.ov.nms.disco 开头的类包含关键字 Exception 的消息。有关日志文件的信息,请参阅第 373 页的 NNMi 日志记录。

未编号接口

在 NNMi 9.10 补丁 2 之前,除非启用 xDP,否则 NNMi 不搜索未编号接口的第 2 层连接。 NNMi 9.10 补丁 2 提供了未编号接口搜索和监视解决方案,它支持使用默认 MIB-II ipRoutingTable 和 ipCidrRoutingTable 的设备。

此部分中描述的解决方案为 NNMi 9.10 提供了搜索和监视 IPv4 未编号接口和及关联的第 2 层连接的方式。

此部分中说明的解决方案在全局网络管理配置中功能如下:

- 它在远程 NNMi 管理服务器上能正常运行。
- 它仅适用于在 NNMi 管理服务器上处理该服务器上管理的节点。
- 它不适用于在全局 NNMi 管理服务器上处理由远程 NNMi 管理服务器管理的节点。

启用未编号接口功能

- 1 创建包括含有未编号接口的设备的节点组。创建包含设备标识符的单个节点组,或创 建表示包含设备标识符的多个子节点组的父节点组。
- 2 创建以下文件:

Windows: %NNM DATA%\shared\nnm\conf\disco\UnnumberedNodeGroup.conf

UNIX: \$NNM_DATA/shared/nnm/conf/disco/UnnumberedNodeGroup.conf

3 将单个节点组名称添加到此文件。同样,此文件必须包含含有设备标识符的单个节点组的名称,或者也可以是表示包含设备标识符的多个子节点组的父节点组的名称。

这是包含具有未编号接口的设备的节点组的名称。 未编号节点组

在上面显示的示例中,名为"未编号节点组"的节点组存在于 NNMi中。将注释信息 添加为由 # 字符开头的单独行。

4 可选步骤:创建以下文件:

Windows: %NNM DATA%\shared\nnm\conf\disco\UnnumberedSubnets.conf

UNIX: \$NNM DATA/shared/nnm/conf/disco/UnnumberedSubnets.conf

5 *可选步骤*:将信息添加到此文件以显示需要 NNMi 搜索的特定路由地址范围。可按随 机顺序将多行 IPv4 CIDR 子网条目添加到此文件。

如果不创建和配置此文件,则 NNMi 将针对己配置节点组中的那些节点执行完整 MIB-II 路由表走查;通过使用 UnnumberedSubnets.conf 文件, NNMi 只从指定子网目标中的那些路由请求 MIB 数据。这是使用此文件的好习惯,可减少设备上的搜索通信量和对性能的影响。

下面是 UnnumberedSubnets.conf 文件的一些示例条目。

10.1.5.0/18 #This entry filters the following routes: 10.1.0-63.

15.2.126.0/16 #This entry filters the following routes: 15.2.*.*

192.168.1.0/24 #This entry filters the following routes: 192.168.1.0-255

- 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。
- 7 等待 NNMi 以完成下一个搜索周期。
- 8 要查找所有未编号接口,请配置新的接口组,以包括拥有名为 UnnumberedNextHop 的 自定义属性的那些接口。

🐵 🥪 💾 🎦 保存并关闭 🥩 🗙 빼除接口组 🔛			
▼基本	ifType 过滤器 其他过滤器		
名称 Unnumbered Interfaces	•		
添加甲枫图过速器列表 ☑ 节点组	使用 like 或 not like 运算符时,请使用"(星号)与字符串中的零个或多个字符匹 配,使用?(问号)与字符串中的一个字符精确匹配。 要创建包括起始地址和结束地址的 P 地址范围,请使用 between 运算符。有效示 例ipAddress between 10.10.11 AND 10.10.1255 有关详细信息,请量串北处。		
您可以使用 Impe 过滤器和其他过滤器来过滤接口 组。如果同时使用 Impe 过滤器和其他过滤器,那么 接口必须与至少一个 Impe 过滤器及其他过滤器规范 匹配才能属于该节点组。如果选择节点组,则接口必 须属于该节点组的成员节点。请参阅"帮助 → 使用接 口组表单"。	过速器编辑器 属性 运算符 值 customAttrValue ▼ = ▼ Unnumbered Node Group		

9 要查看由此解决方案创建的第2层连接,请导航到第2层连接视图;然后从路由查找源。

用2层邻居视图 》用2层邻居视图 >	
□ 状态 名称	▲ 拓扑源
🔲 🔝 🙆 🚫 Hist-1[mgmt0],L	SOB-1[mgmt0] CDP
🔲 🛅 🖾 🛇 ROADM[pdcc0],	Site3[pdcc1] ROUTES
🔲 🗐 🖾 🛇 Small Subnets-B	BTPNJ02ML0_A6[ethernetCsmacd [14]],B SUBMETCONNECTION
🔲 🛅 🔼 Small Subnets-B	BTPNJ02ML0_A6[ethernetCsmacd [25]],B SUBNETCONNECTION
🔲 🛅 🖾 📀 Small Subnets-B	BTPNJ02ML0_A6[ethernetCsmacd [37]],B SUBNETCONNECTION
/	

禁用未编号的接口功能

如果决定禁用未编号接口功能,则完成以下步骤:

1 删除以下文件:

Windows: %NNM DATA%\shared\nnm\conf\disco\UnnumberedNodeGroup.conf

UNIX: \$NNM DATA/shared/nnm/conf/disco/UnnumberedNodeGroup.conf

2011年3月

2 删除以下文件 (如果存在):

Windows: %NNM_DATA%\shared\nnm\conf\disco\UnnumberedSubnets.conf *UNIX*: \$NNM_DATA/shared/nnm/conf/disco/UnnumberedSubnets.conf

- 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。
- 4 等待 NNMi 以完成下一个搜索周期。

有关详细信息,请参阅 UnnumberedNodeGroup.conf 和 UnnumberedNodeGroup.conf 参 考页或 UNIX 联机帮助页。

NNMi 状态轮询



本章提供的信息可帮助您通过配置 HP Network Node Manager i Software (NNMi) 状态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。

如果您有使用 NNM 6.x/7.x 的经验,并且要了解 NNMi 9.10 中监视功能有哪些更改,请参阅《NNMi 升级参考》中的"状态监视"以了解对差异的高级概述。

本章包含以下主题:

- 状态轮询的概念
- 计划状态轮询
- 配置状态轮询
- 评估状态轮询
- 调整状态轮询

状态轮询的概念

本节简要概述了网络监视,包括状态轮询器用于评估轮询组的顺序。阅读本节中的信息之后,请继续到第78页的计划状态轮询,以了解更多特定信息。

与网络搜索一样,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。

可以将状态轮询器数据采集配置为基于 ICMP (ping) 响应或 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。

当计划轮询配置时,应当仔细考虑如何为状态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,请参阅第41页的节点组和接口组和第45页的节点/接口/地址层次结构,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,因此状态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。对于搜索的拓扑中的每个对象:
 - 如果对象是接口,则状态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 对于搜索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。

计划状态轮询

本节提供有关状态轮询器配置(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态轮询器配置。

- □ NNMi 可以监视什么?
- □ 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被监视项的信息?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

2011年3月

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。您需要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?

由于只能监视搜索的设备,因此可配置自动搜索规则以确保 NNMi 数据库包含 ProximiT 代理服务器。有关配置搜索的详细信息,请参阅第 59 页的 NNMi 搜索。

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过滤视图、将代理服务器作为组来检查其状态,以及将组设置为服 务中断以更新固件。

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。

有关这些配置选择的更多详细计划信息,请参阅以下主题:

- 第 79 页的 NNMi 可以监视什么?
- 一 第81页的计划组
- 一 第83页的计划轮询间隔
- 第84页的决定要采集的数据

NNMi 可以监视什么?

默认情况下, NNMi 状态轮询器使用 SNMP 轮询来监视以下各项:

- 连接到 NNMi 搜索的设备上的另一个已知接口的接口。
- 主机 IP 寻址的路由器接口。
- 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。

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。

NNMi 将未连接接口定义为未连接到由 NNMi 搜索的另一个设备的接口,如下所示。



- 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。

到未监视节点的接口

有时,需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 含在搜索规则中,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。

• 搜索未监视节点

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 将该节点,因为它处于被管状态。对于您不希望 NNMi 监视的节点,可以取消管理它们。



• 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搜索节点的连接。然后启用对该节点组的未连接接口的轮询。

NNMi 轮询节点组的设备上的*所有*接口,对于具有多个接口的设备,这可能会添加大量通信量。

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。服务中断用于临时状态,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,状态轮询器都不与其通信。

最佳实践 无需对您选择搜索并放置在数据库中的某些设备和/或接口进行轮询。请注意您将永久设置 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。

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)。

最佳实践 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,它们也是用于过滤 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过滤器以用于配置监视设 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过滤器列表复选框。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?是否有定时约束?
- 是否要按设备类型区分轮询间隔或采集的数据?或是按接口类型区分?
- NNMi 是否提供了您可以使用的预配置组?
- 最佳实践 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(请参阅第77页的状态轮询的概念)。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 己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
- 用于点到点通信的接口
- 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过滤视图,因此可 以单独配置它们。 2011年3月

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搜索过程中派生自系统 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 共用字符串的设备
- 重要节点。这由原因引擎在内部用于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 作为预定义视图过滤器的节点组。

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
- 最佳实践 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 (不在列表中过载许多可能从来不会使用的条目) 之间找到平衡。

与设备配置文件的 搜索每个设备时, 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 **交互** 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"的所有已搜索设备都将 接收到节点组的已配置设置。

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。

最佳实践 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。

决定要采集的数据

状态轮询器服务使用轮询来采集网络中有关被监视设备的状态信息。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 SNMP 监视验证每个被监视 SNMP 代理是否正在响应 SNMP 查询。

- 高度优化的状态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,状态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。

SNMP 组件运行状况 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数据 询间隔设置。

在每次轮询中采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 增加状态轮询器的内存要求。

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。

<mark>最佳实践</mark> 批量监视配置更改较少破坏状态轮询器正在进行的操作。

配置状态轮询

本节提供配置提示,并提供一些配置示例。阅读本节中的信息之后,请参阅 NNMi 帮助的 *配置监视行为*,以了解特定过程。



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,请参阅第 40 页的最佳实践:保存现有配置。

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。

2011年3月

- 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**,并单击**新建**。
 - 2 将该组命名为代理服务器,并选中添加到视图过滤器列表。
 - 3 在其他过滤器选项卡上,选择 hostname 属性,并将运算符保留设置为 =。
 - 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,则可以使用设备过滤器选项 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。

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

状态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,以创建有关状态 轮询器应当如何处理该组的一组自定义说明。说明将包括:

- 启用或禁用故障轮询
- 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,状态轮询器按从最低到最高的排序编号来评估列表。

最佳实践 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,则状态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。创建说明状态轮询器应当如何 处理该组的一组自定义说明。说明可以包括:

- 启用或禁用故障轮询
- 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。

最佳实践 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

状态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。



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。

评估状态轮询

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。

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 在资产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>轮询>配置轮询以更新节点的属性,从而使其适合于节点组。

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,请在相应的资产视图中选择该对象,并选择 操作 > 配置详细信息 > 监视设置。 NNMi 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。如果这些值并不是预期值,请查看**节点组**或接口组的值,以查看按编号排序应用了哪个匹配的组。

可能需要为对象选中操作 > 配置详细信息 > 通信设置,以确保没有对其禁用通信量。

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)。选择某节点,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

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

状态轮询器是否一直在运行?

随时都可以在系统信息窗口的状态轮询器选项卡上检查有关状态轮询器服务的当前运行状况统计数据,如表2中所述。

表 2 状态轮询器运行状况信息

信息	描述
状态	状态轮询器服务的总体状态
轮询计数器	 在最后1分钟内请求的采集 在最后1分钟内完成的采集 正在进行中的采集
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 文件中查找有关以字符串 com.hp.ov.nms.statepoller 开头的类的 消息,以确定已跳过轮询的目标。 — 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 文件中查找有关以字符串 com.hp.ov.nms.statepoller 开头的类的消息,以确定过时采集的目标。 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 数据库的性能。停止并重新启动 NNMi。
轮询器结果队列 长度	 监视对象:此值大多数时间都应接近于 0。 要执行的操作:如果此队列非常大,则 ovjboss 可能将耗尽内存。
状态映射器输入 队列长度	 监视对象:此值大多数时间都应接近于 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。
状态更新程序排 队时间长度	 监视对象:此值大多数时间都应接近于 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。

调整状态轮询

状态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。它只在计划时间内采集其他 MIB 对象。但是,禁用组件运行状况监视可能会减少可由状态轮询器使用的内存量。





HP Network Node Manager i Software (NNMi) 提供大量默认事件和关联,这些关联过滤传入 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*。

如果您有使用 NNM 6.x/7.x 的经验,并且要了解 NNMi 9.10 中事件监视有哪些变化,请参阅《NNMi 升级参考》中的"自定义事件监视"以了解这些差异的高级概述。

本章包含以下主题:

- 事件的概念
- 计划事件
- 配置事件
- 评估事件
- 调整事件

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。原因引擎会在 任何可能的时候广泛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。
- 从一个或多个 NNM 6.x/7.x 管理工作站转发的 NNM 6.x/7.x 事件。

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 陷阱或 NNM 6.x/7.x 事件,则丢弃该信息。如果陷阱源的管理模式在 NNMi 数据库中设置为未管理或服务中断,则 NNMi 始终丢弃该传入陷阱。

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*处理未解决的传入陷阱*。

有关详细信息,请参阅以下内容:

- NNMi 帮助中的*关于事件管道*
- NNMi 帮助中的 NNMi 原因引擎和事件
- NNMi 原因分析白皮书,可从 http://h20230.www2.hp.com/selfsolve/manuals 获得

事件生命周期

表3描述了事件的生命周期阶段。

表 3 NNMi 事件生命周期

生命周期状态	描述	状态设置者	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 第97页的事件抑制、强化和减弱。	NNMi	• NNMi
已注册	事件在事件视图中可见。 事件被转发到任何配置的目标(northbound 或全局管 理器)。	NNMi 用户还可以在 事件视图中设 置此状态。	 用户 生命周期转换操作 转发事件的集成

2011年3月

表 3 NNMi 事件生命周期(续)

生命周期状态	描述	状态设置者	事件使用者
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态的特定含义。	用户	 用户 生命周期转换操作 转发事件的集成
己完成	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态的特定含义。	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 已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

表 4 总结了将陷阱和事件从 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 Interface SNMP 陷阱转发机制。

表 4 转发陷阱和 NNMi 事件的支持方式

	NNMi 陷阱转发	NNMi Northbound Interface 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 NNM 管理工作站的 NNM 6.x/7.x 事件 	 来自网络设备的 SNMP 陷阱 NNMi 管理事件 	 来自网络设备的 SNMP 陷阱 来自 NNM 管理工作站的 NNM 6.x/7.x 事件
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
添加的信息	多数情况下, NNMi 添加 varbind 来识别原始陷阱源。 NNMi 不会修改 SNMPv1 陷阱。	NNMi 添加 varbind 来识别原 始陷阱源。	转发事件中保留由区域管理器进程添加到事件的任何信息。

表 4 转发陷阱和 NNMi 事件的支持方式 (续)

	NNMi 陷阱转发	NNMi Northbound Interface 陷阱转发	全局网络管理陷阱转发
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 Interface 或 Netcool	SNMP 陷阱配置表单或远程 NNM 6.x/7.x 事件配置表单上的转发到 全局管理器选项卡
说明		 NNMi 提供 NNMi Northbound Interface 上生成的几个集成: 第 505 页的 NNMi Northbound Interface 第 539 页的 HP NNMi— HPOM 集成(代理实施) 第 577 页的 HP NNMi Integration Module for Netcool Software 	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。
有关详细信息	NNMi 帮助中的 <i>配置陷阱转发</i>	第 508 页的使用 NNMi Northbound Interface	 NNMi 帮助中的对SNMP 陷阱事件配置"转发到全 局管理器"设置 NNMi 帮助中的对远程 6.x/7.x 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 Interface 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,请参阅第 516 页的表 56 中的事件。

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UNIX

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强化它。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 UNIX 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
- UNIX: \$NNM_SNMP_MIBS/Vendor/Hewlett-Packard/hp-nnmi.mib
- 带原始陷阱转发的 UNIX

UNIX NNMi 管理服务器上的 NNMi SNMP 陷阱转发机制可以用 NNMi 接收陷阱的 相同格式转发陷阱。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 Interface (所有操作系统)

NNMi Northbound Interface 在将每个 SNMP 陷阱转发到陷阱目标之前先强化它。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 识别原始陷阱源。

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)的节点组件
- (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

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** 将该事件的生命周期状态设置为已关闭并将表 5 中列出的 CIA 添加到事件。 **NNMi** 控制台用户可以在**事件**表单的**关联** 说明字段中看见此信息。生命周期转换操作可直接使用 CIA 的值。

名称	描述
cia.reasonClosed	NNMi 取消或关闭事件的原因。该原因也是总结名称,例如 NodeUp 或 InterfaceUp。
	如果未反直此子校,则 NNMi 控制台用户已大闭事件。 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。

表 5 自定义已关闭事件的事件属性

NNMi 将表 5 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不将表 5 中列出的 CIA 添加到以下的默认管理事件类型:

- 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,在事件生命周期状态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态的。该操作 配置确定当此事件类型转换为指定生命周期状态时要运行的命令。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态各用 一个。 类似地,操作代码可特定于一个生命周期状态更改,也可以响应几个生命周期状态更改。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,一个用于已注册状态,一个用于已关闭状态。

每个操作配置都可以包括一个基于 CIA 的负载过滤器,用于限制操作何时运行。对于其他 过滤,可使用事件强化将 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 用作某事件操作的负载过滤器的依据。

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?
- NNMi 应显示哪些事件?
- NNMi 应如何响应事件?
- NNMi 应从 NNM 管理工作站接收陷阱吗?
- NNMi 应将陷阱转发到另一个事件接收器吗?

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 处理陷阱时无需加载进 MIB。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。您可以随时间的推移来扩展和减少事件集。 通过取消重复、速率配置和成对关联来计划可减少的事件。

NNMi 应如何响应事件?

特定事件发生时, 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态下运行?

NNMi 应从 NNM 管理工作站接收陷阱吗?

如果您的环境包括将继续与 NNMi 一起管理网络区域的一个或多个 NNM 6.x/7.x 管理工作站,则确定将帮助 NNMi 操作员管理网络的 NNM 6.x/7.x 事件。为应在 NNMi 控制台中可用的每个 NNM 6.x/7.x 事件计划事件配置。

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 Interface SNMP 陷阱转发机制结合使用。

如果选择 NNMi Northbound Interface 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。读完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。



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,请参阅第 40 页的最佳实践:保存现有配置。

- 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过滤器。
- 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
 - UNIX: \$NNM DATA/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。

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。

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。

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态转换而运行。
- 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 节点及其接口的任何传入陷阱。
- 将 NNMi 设置为不监视某些网络对象。NNMi 丢弃来自不受监视的陷阱源的任何传入 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。

如果您有权在 NNMi 管理服务器上使用 NNM iSPI NET,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, 且想将丢弃的陷阱作为事件查 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
 - UNIX: \$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= 您指定的严重度

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= 您指定的性质

- 5 通过运行以下命令,重新启动 ovjboss:
 - a ovstop ovjboss
 - b ovstart ovjboss
- 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:

- 使用节点组的实例
- 减少在网络概述图中显示的最大节点数
- 减少节点组图上显示的节点数

使用节点组的实例

配置节点组的实例如下所示。

我的网络:包含其他节点组的顶层*容器*节点组。

- 美国:包含其他节点组的中间*容器*节点组。
 - 科罗拉多: 包含位于科罗拉多州的节点的节点组。

注意以下事项:

- 最佳实践是提前设计节点组图布局。
- 最佳实践是配置一组节点和接口组用于网络监视。配置一套不同的节点组,用于通过图 实现网络可视化。
- 在此示例中,科罗拉多是包含节点的唯一节点组。
- NNMi 提供多种方式来配置节点组和节点组图。熟悉本文档所述步骤之后,您可能会找 到创建后续节点组和节点组图的更加高效的方式。

本文档将指导您完成以下步骤以配置节点组和节点组图:

创建节点组

- 步骤 1: 创建"我的网络"节点组
- 步骤 2: 创建"美国"节点组
- 步骤 3: 使用过滤器创建"科罗拉多"节点组
- 步骤 4: 查看节点组成员以检查节点组过滤器结果
- 步骤 5: 为"我的网络"节点组建立节点组层次结构
- 一 步骤 6: 为"美国"节点组建立节点组层次结构



父节点组可能不包含任何节点,而只包含定义中的子节点组。在此示例中,我的网络和美国 节点组是只包含子节点组的父节点组。

配置节点组图

- 步骤 1: 创建节点组图
- 步骤 2: 查看节点组图
- 步骤 3: 配置节点组状态
- 一 步骤 4: 配置节点组图排序
- 步骤 5: 将背景图像添加到节点组图

创建节点组

我们从创建要包含在节点组图中的节点组开始。

步骤 1: 创建"我的网络"节点组

要创建我的网络节点组:

- 1 导航到配置工作区。
- 2 选择**节点组**。
- 3 单击**新建**图标。
- 4 在名称属性中,输入:我的网络。
- 5 在说明属性中,输入: 这是顶层节点组。
- 6 单击**保存并关闭**以保存此配置。

步骤 2: 创建"美国"节点组

- 1 导航到配置工作区。
- 2 选择**节点组**。
- 3 单击新建图标。
- 4 在名称属性中,输入:美国。
- 5 单击**保存并关闭**以保存此配置。

步骤 3: 使用过滤器创建 "科罗拉多"节点组

要创建科罗拉多节点组,请使用过滤器编辑器建立用于选择节点的过滤器。

- 如果可能,请使用**其他过滤器**选项卡,而不是使用**其他节点**选项卡指定节点列表。使用节点 组过滤器,NNMi就能在有新节点添加到网络中时,将节点自动放置到正确的节点组中。
 - 1 导航到配置工作区。
 - 2 选择**节点组**。
 - 3 单击**新建**图标。
 - 4 在名称属性中,输入:科罗拉多。
 - 5 选择**其他过滤器**选项卡。
 - 6 单击或指定希望 NNMi 在节点与您输入的两个主机名值之一匹配时匹配节点。
 - 7 在过滤器编辑器的属性字段中,选择 hostname。

如果选择 hostname,将指定 NNMi 在确定节点是否属于此节点组时应当匹配主机名值。

8 在运算符字段中,选择 like。

选择 like 将允许您在搜索中使用通配符。

- 9 在值字段中,输入表示要节点组包含的设备的值。例如,**cisco*.ntc.example.com** 表示名为 cisco<*替换为此文本*>.<*网络域*> 的设备。
- 10 单击追加。
- 11 在属性字段中,选择 hostname。
- 12 在运算符字段中,选择 like。
- 13 在值字段中,输入表示要添加到科罗拉多节点组的剩余设备名称的通配符。对于此示例, 请使用 cisco?*。
- 14 单击追加。
- 15 单击保存以保存节点组而不关闭窗口。

步骤 4: 查看节点组成员以检查节点组过滤器结果

要测试节点组过滤器,可以查看您刚刚创建的节点组的成员。 选择操作-> 节点组详细信息-> 显示成员以启动包含节点组中所有节点的视图。

检查节点组过滤器定义结果,直到您确信节点组过滤器是正确的。

步骤 5:为 "我的网络"节点组建立节点组层次结构

建立节点组的层次结构,从顶层节点组我的网络开始。

- 1 返回到**配置**工作区中的**节点组**选项,以查看您创建的节点组的列表。
- 2 导航到我的网络节点组;然后单击打开。
- 3 单击子节点组选项卡。
- 4 单击新建图标。
- 5 在**子节点组**属性中,单击查找图标并选择快速查找。

使用快速查找选择对象 (如节点组,如果它已经存在)。

- 6 选择**美国**作为子节点组。
- 7 单击**保存**。
- 8 单击保存并关闭以保存更改并关闭节点组层次结构表单。
- 9 单击保存并关闭以保存更改并关闭节点组表单。

步骤 6:为"美国"节点组建立节点组层次结构

接下来,建立**科罗拉多**作为**美国**节点组的子节点组。重复步骤 5:为 "我的网络"节点组建 立节点组层次结构中所述的相同步骤,使 "科罗拉多"节点组成为 "美国"节点组的子节 点组。

您已准备好为已创建的每个节点组创建节点组图。

配置节点组图

步骤 1: 创建节点组图

要创建每个节点组的节点组图,请使用操作菜单。

- 1 打开要创建图的节点组:
 - a 返回到配置工作区中的节点组选项,以查看您创建的节点组的列表。
 - b 导航到所需的节点组,并单击**打开**图标。
- 2 选择操作 -> 映射 -> 节点组图以显示节点组图。
- 3 放置节点和节点组图的图标。
- 4 单击保存布局图标以创建节点组图。
- **即**使不更改节点位置,也要始终使用**保存布局**创建节点组图。**保存布局**将创建节点组图。

此时会出现对话框,确认您成功创建了节点组图。

- **5** 单击确定。
- 6 对创建的每个节点组重复步骤1到5。
步骤 2: 查看节点组图

既然已经创建节点组图,就可以查看图以检查其内容。

- 1 导航到**拓扑图**工作区。
- 2 选择节点组概述。
- 3 选择顶层图:我的网络。
- 4 通过双击子节点组图的图标导航到此处。
- 5 使用返回按钮可以返回到上一张图。

步骤 3: 配置节点组状态

NNMi 允许您配置如何计算节点组的状态。配置节点组状态时,请确定 NNMi 应使用以下哪种方法:

- 使用节点组中节点的最严重状态。
- 指定 NNMi 使用的百分比计算。

状态配置是全局配置。默认情况下, NNMi 使用节点组中节点的最严重状态。

- 1 导航到配置工作区。
- 2 选择**状态配置**。
- 3 检查状态配置表单,以熟悉默认百分比。要使用百分比,必须取消选中传播最严重的状态 选项,然后保存更改。

步骤 4: 配置节点组图排序

节点组图排序用于帮助确定按哪种顺序在拓扑图工作区下显示图。

在此示例中,使用节点组图排序指定我的网络节点组图应首先显示在拓扑图工作区的列表中。

- 1 导航到配置工作区。
- 2 选择节点组图设置。

如以下示例中所示,所有用户定义图的默认拓扑图排序值都是 50。

要指示 NNMi 在**拓扑图**工作区下将我的网络作为第一张图列出,请将拓扑图排序值更改为小于列表中任何其他图的拓扑图排序值的数字;例如 5。

- 3 打开我的网络节点组图。
- 4 在**拓扑图排序**属性中,将值更改为 5。
- 5 单击**保存并关闭**以保存更改并关闭表单。

还可以指定是否一开始就在 NNMi 控制台中显示图。为此,请使用**配置**工作区的**用户界面配** 置选项。

1 导航到配置工作区。

- 2 单击用户界面配置。
- 3 在初始视图属性中,使用下拉菜单选择拓扑图工作区中的第一个节点组。 此操作将使我的网络图成为初始视图。 要验证初始视图,请从 NNMi 注销再重新登录。我的网络图应是您在 NNMi 控制台中 看到的视图。

步骤 5: 将背景图像添加到节点组图

要在图上包括背景图形,请对所选节点组图使用节点组图设置表单。

- 1 导航到**配置**工作区。
- 2 单击用户界面。
- 3 单击**节点组图设置**。
- **4** 打开**我的网络**节点组图。
- 5 导航到**背景图像**选项卡。
- 6 单击 http://MACHINE:PORT/nnmdocs/images/。

NNMi 显示 HP 所提供图形的列表。

- 7 右键单击 world.png 链接。
- 8 选择**复制链接位置**。
- 9 关闭目录列表窗口。

将复制的链接粘贴到背景图像属性中。

▶ 记下背景图像缩放值,以备将来需要更改时参考。

- 10 单击保存并关闭以保存更改。
- 11 导航到拓扑图工作区,并选择我的网络,以查看带背景图形的新图。

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。可以按以下示例所示,增加或减少在网络概述图中显示的最大节点数。

假定要将网络概述图中显示的最大节点数从 250 更改为 100。为此,请遵循以下步骤:

- 1 编辑以下文件:
 - Windows: %NNM_PROPS%\nms-ui.properties
 - UNIX: \$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

- 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。显示图时 使用缩放功能可能使 NNMi 控制台性能下降。

补救办法是通过执行以下操作限制显示的节点数和/或显示的端点数:

- 1 在 NNMi 控制台中,单击配置。
- 2 单击位于用户界面下的用户界面配置。
- 3 选择**默认图设置**选项卡。
- 4 修改最多节点显示数目字段中显示的值。
- 5 修改最大的端点显示数目字段中显示的值。
- 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。



本部分包含以下各章:

- 许可 NNMi
- 使用 NNMi 证书
- 对 NNMi 使用单点登录
- 配置 Telnet 和 SSH 协议以供 NNMi 使用
- 通过 LDAP 将 NNMi 与目录服务集成
- NNMi 安全和多租户
- 全局网络管理
- 配置 NNMi Advanced 的 IPv6 功能
- 在 Solaris 区域环境中运行 NNMi

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 Advanced 功能。应当尽早获取并安装永久许可证密钥。

要查看 NNMi Advanced 许可证所附带功能的列表,请参阅 HP NNMi Software 发行说明的"许可"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。永久许可证生效时, NNMi 会自动取消管理其选择的节点,以达成许可证限制。

如果希望控制永久许可证不再管理哪些节点,请在安装新许可证密钥之前,使用 NNMi 控制台删除不重要的节点。

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,请遵循以下步骤:

- 1 在 NNMi 控制台中,单击**帮助 > 关于 Network Node Manager**。
- 2 在关于 HP Network Node Manager i Software 窗口中,单击许可信息。

(NNMi 控制台登录页上也提供了许可信息。)

- 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。
- 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
- NNMi 管理服务器的 IP 地址
- 群集的虚拟 IP 地址 (如果许可证适用于以 HA 运行的 NNMi)

```
对于以 HA 运行的 NNMi, NNMi 生产许可证与群集的虚拟 IP 地址相关联。另外, HA 群集中的一个节点需要 NNMi 非生产许可证。
```

• 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,请遵循以下步骤:

1 在命令提示符下,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),则遵循 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 -f 许可证文件

(产品许可证 ID (MMM) 区分大小写。)

有关详细信息,请参阅 nnmlicense.ovpl 参考页或 UNIX 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 开发人员工具包,您可以通过集成自定义的 Web 服务客户端来增强 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 开发人员工 具包文档和示例。

使用 NNMi 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 文件中都包括自签名证书。

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。

本章包含以下主题:

- 概要
- 生成证书颁发机构证书
- 将应用程序故障切换配置为使用自签名证书
- 将应用程序故障切换配置为使用证书颁发机构
- 将高可用性配置为使用自签名或证书颁发机构证书
- 将全局网络管理功能配置为使用自签名证书
- 将全局网络管理功能配置为使用证书颁发机构
- 将带有应用程序故障切换的全局网络管理配置为使用自签名证书
- 配置与目录服务的 SSL 连接
- 配置 HP BSM V9.xx 的 SSL 连接



针对您的特殊需要配置证书时,请使用以下信息来作为指导:

- 如果在使用 CA 证书,请遵循第 121 页的生成证书颁发机构证书中所示的说明。
- 如果配置了全局和/或区域 NNMi 管理服务器以使用应用程序故障切换功能,则还有些额 外的配置步骤。完成全局网络管理配置之前,如第 124 页的将应用程序故障切换配置为使 用自签名证书中所述合并每个群集的 NNMi 管理服务器的 nnm.keystore 和 nnm.truststore 文件。
- 如果需要使用"证书颁发机构",并配置了全局和/或区域 NNMi 管理服务器以使用应用程序故障切换功能,则还有些额外的配置步骤。首先,按第 121 页的生成证书颁发机构证书中所示的说明操作,然后在完成全局网络管理配置之前,如第 126 页的将应用程序故障切换配置为使用证书颁发机构中所述合并每个群集的 NNMi 管理服务器的nnm.keystore 和 nnm.truststore 文件。
- 如果配置全局和/或区域 NNMi 管理服务器以使用高可用性,则在完成全局网络管理配置之前,如第128页的将高可用性配置为使用自签名或证书颁发机构证书中所述在虚拟主机的 nnm.keystore 和 nnm.truststore 文件中创建自签名证书。
- 正确配置每个 HA 或应用程序故障切换群集后,通过将 nnm.truststore 文件从主动区域节点复制到主动全局节点并合并信任库,从而启用全局网络管理功能。必须对每个主动区域节点执行此操作。查看第 131 页的将带有应用程序故障切换的全局网络管理配置为使用自签名证书中所示的信息。如果 NNMi 管理服务器使用按第 121 页的生成证书颁发机构证书中所示的步骤生成的 CA 证书,则那些 CA 证书就是需要合并到全局信任库中的全部证书。
- 如果在全局网络管理配置中配置 NNMi 管理服务器,随后决定将区域和/或全局改成在应用程序故障切换群集中,请遵循第 124 页的将应用程序故障切换配置为使用自签名证书中所示的说明操作。需要使用在该部分中所示的命令来正确配置 nnm.keystore 和 nnm.truststore 文件;然后将修改后的 nnm.truststore 文件复制到全局 NNMi 管理服务器,并将它合并至其 nnm.truststore 文件中。
- 如果在全局网络管理配置中配置 NNMi 管理服务器,随后决定将区域和/或全局改成使用 HA,请遵循第 128 页的将高可用性配置为使用自签名或证书颁发机构证书中所示的说明操作。
- 启用目录服务通信之后, NNMi 从目录服务使用 LDAP 协议以检索数据。如果目录服务需 要 SSL 连接,请遵循第 132 页的配置与目录服务的 SSL 连接中所示的说明操作。

生成证书颁发机构证书

Λ

如果计划使用 CA (证书颁发机构),则完成以下步骤以生成 CA 证书。

如果计划将 CA 用于 NNMi,则用 RSA 算法对证书签名。不支持 DSA 算法。

- 1 切换到 NNMi 管理服务器上包含 nnm.keystore 和 nnm.truststore 文件的目录:
 - Windows: %NNM_DATA%\shared\nnm\certificates
 - UNIX: \$NNM_DATA/shared/nnm/certificates
- 2 保存 nnm.keystore 文件的备份副本。
- 3 从系统生成私钥。用 keytool 命令可以生成此私钥:
 - a 运行以下命令:
 - Windows: %NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe
 -genkeypair -validity 3650 -keyalg rsa -keystore
 nnm.keystore -storepass nnmkeypass -alias 我的服务器.我的域
 - UNIX: \$NnmInstallDir/nonOV/jdk/nnm/bin/keytool
 -genkeypair -validity 3650 -keyalg rsa -keystore
 nnm.keystore -storepass nnmkeypass -alias 我的服务器.我的域

此示例中称为我的服务器.我的域的别名表示新创建的密钥。尽管别名可以是 任何字符串,但 HP 建议对我的服务器.我的域别名变量使用系统的完全限定 域名。

Linux 操作系统上的 keytool 命令与此步骤中使用的 keytool 命令或命令选项 不兼容。

b 输入请求的信息。

重要信息:提示输入姓和名时,请输入系统的FQDN (完全限定域名)。

- 4 运行以下命令以创建 CSR (证书签名请求) 文件:
 - Windows: %NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe
 -keystore nnm.keystore -certreq -storepass nnmkeypass
 -alias 我的服务器.我的域 -file CERTREQFILE
 - UNIX: \$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -keystore nnm.keystore -certreq -storepass nnmkeypass -alias 我的服 务器.我的域 -file CERTREQFILE

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)。

5 将 CSR 发送到 CA 签名颁发机构。他们应为您提供以下项之一:

- 签名证书,名为 myserver.crt。myserver.crt 文件包含服务器证书(文件中最 前面的证书)和一个或多个 CA(证书颁发机构)证书(文件中后面的证书)。将 CA 证书复制到名为 myca.crt 的新文件中。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。
- 两个文件,在此过程中称为 myserver.crt 和 CA.crt。将 CA.crt 文件内容添加到 myserver.crt 文件的末尾。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。

以下示例显示了您从 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/AVQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwd0ZXR3b3Js eGVSZXZvY2F0aW9uTGlzdD9iYXN1P29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw 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 eGVSZXZvY2F0aW9uTGlzdD9iYXN1P29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt== END CERTIFICATE
BEGIN CERTIFICATE Sample2/Gh0dHA6Ly9jb3JwMWRjc2cyLnNnLmludC5wc2FnbG9iYWwuY29tL0Nlc
RaOCApwwggKYMB0GA1UdDgQWBBSqaWZzCRcpvJWOFPZ/Be9b+QSPyDAfBgNVHSMC
Wp5Lz1ZJAOu1VHbPVdQnXnlBkx7V65niLoaT90Eqd6laliVlJHj7GBriJ90uvVGu
BQagggEChoG9bGRhcDovLy9DTj1jb3JwMWRjc2cyL==

- 6 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: %NNM_DATA%\shared\nnm\certificates
 - UNIX: \$NNM_DATA/shared/nnm/certificates

将证书导入密钥库的

示例输出

使用之前步骤中生成的证书替换自签名证书:

- 1 切换到 NNMi 管理服务器上包含 nnm.keystore 和 nnm.truststore 文件的目录:
 - Windows: %NNM_DATA%\shared\nnm\certificates
 - UNIX: \$NNM_DATA/shared/nnm/certificates
- 2 运行以下命令以将服务器证书和 CA 证书导入到 NNMi nnm.keystore 文件中:

Windows:

%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -importcert -trustcacerts -keystore nnm.keystore -storepass nnmkeypass -alias 我的服务器.我的域 -file myserver.crt

UNIX:

\$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -importcert
 -trustcacerts -keystore nnm.keystore -storepass nnmkeypass
 -alias 我的服务器.我的域 -file myserver.crt

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,则提示输入密钥库密码时输入nnmkeypass。

3 系统提示您是否信任证书时, 输入: y

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
SHA1: 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 运行以下命令以将 CA 证书导入到 NNMi nnm.truststore 文件中:
 - Windows:

%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -import -alias 我的 CA -keystore nnm.truststore -file myca.crt

— UNIX:

\$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -import -alias 我的 CA -keystore nnm.truststore -file myca.crt

5 系统提示您输入信任库密码时,输入: ovpass。

123

- 6 检查信任库的内容:
 - Windows: %NnmInstallDir%\nonOV\jdk\nnm\bin\keytool -list \ -keystore nnm.truststore
 - UNIX: \$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list \ -keystore nnm.truststore

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

- 7 编辑以下文件:
 - Windows: %NNM_CONF%\nnm\props\nms-local.properties
 - UNIX: \$NNM_CONF/nnm/props/nms-local.properties
- 8 将 com.hp.ov.nms.ssl.KEY_ALIAS 变量更新为用于*我的服务器.我的域* 的值。请务 必保存工作。
- 9 通过运行以下命令,重新启动 ovjboss:
 - a ovstop ovjboss
 - b ovstart ovjboss
- 10 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/。如果浏览器信任 CA,则它会信任到 NNMi 控制台的 HTTPS 连接。

将应用程序故障切换配置为使用自签名证书

图 2 将自签名证书用于应用程序故障切换

活动 NNMi 管理服务器 (服务器 X)	备用 NNMi
	管理服务器 (服务器 Y)

Λ

配置应用程序故障切换功能时,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 程序故障切换功能配置为根据上图使用自签名证书。

如果对带有应用程序故障切换功能的 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 在完成步骤 2 之前, 切换到服务器 Y 上的以下目录:
 - Windows: %NNM_DATA%\shared\nnm\certificates
 - UNIX: \$NNM_DATA/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。其余步骤将这些文件位置参考为 < 密钥库 > 和 < 信任库 >。
- 3 在服务器 X上运行以下命令以将服务器 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>

UNIX:

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: %NNM_DATA%\shared\nnm\certificates
 - UNIX: \$NNM_DATA/shared/nnm/certificates
- 5 在服务器 X 和服务器 Y 上运行以下命令。验证来自这两个服务器的显示结果(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,而是重做步骤1到步骤7。

Windows:

```
%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -list
-keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore
-storepass nnmkeypass
```

UNIX:

\$NnmInstallDir/nonOV/jdk/nnm/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。验证来自这两个服务器的显示结果(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,而是重做步骤1到步骤7。

Windows:

```
%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -list
-keystore
%NnmDataDir%\shared\nnm\certificates\nnm.truststore
-storepass ovpass
```

UNIX:

\$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list -keystore
\$NnmDataDir/shared/nnm/certificates/nnm.truststore
-storepass ovpass

7 继续配置第 271 页的步骤 6 的应用程序故障切换功能。



将应用程序故障切换配置为使用证书颁发机构

图 3 将 CA 证书用于应用程序故障切换

活动 NNMi 管理服务器 (服务器 X)	备用 NNMi
	管理服务器 (服务器 Y)

配置应用程序故障切换功能时,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。完成以下步骤,将应用程 序故障切换功能配置为根据上图使用 CA 证书。



如果对带有应用程序故障切换功能的 NNMi 使用 CA 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 遵循第 121 页的生成证书颁发机构证书中所示对 NNMi_standby 的说明。
- 2 在完成步骤 3 之前, 切换到服务器 Y 上的以下目录:
 - Windows: %NNM_DATA%\shared\nnm\certificates
 - UNIX: \$NNM_DATA/shared/nnm/certificates
- 3 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位置作为 <密钥库>和 <信任库>。
- 4 在服务器 X上运行以下命令以将服务器 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>
```

UNIX:

nnmcertmerge.ovpl -keystore <密钥库> -truststore <信任库>

- 5 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: %NNM_DATA%\shared\nnm\certificates
 - UNIX: \$NNM_DATA/shared/nnm/certificates
- 6 在服务器 x 和服务器 y 上运行以下命令。验证来自这两个服务器的显示结果(包括hp.com完全限定域名)是否匹配。如果它们不匹配,请不要继续操作,而是重做步骤 1 到步骤 7。

Windows:

```
%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -list
-keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore
-storepass nnmkeypass
```

UNIX:

\$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list -keystore
\$NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass
nnmkeypass

7 在服务器 X 和服务器 Y 上运行以下命令。验证来自这两个服务器的显示结果(包括 hp.com 完全限定域名)是否匹配。如果它们不匹配,请不要继续操作,而是重做步骤 1 到步骤 7。

Windows:

```
%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -list
-keystore
%NnmDataDir%\shared\nnm\certificates\nnm.truststore
-storepass ovpass
```

UNIX:

\$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list -keystore
\$NnmDataDir/shared/nnm/certificates/nnm.truststore
-storepass ovpass

8 继续配置第 271 页的步骤 6 的应用程序故障切换功能。

虽然在第 127 页的步骤 5 中手动完成了以下自动操作,但是在启动应用程序故障切换 功能之后, NNMi 会自动将合并的密钥库和信任库信息从服务器 X 复制到服务器 Y。

将高可用性配置为使用自签名或证书颁发机构证书

图 4 对高可用性使用证书



将高可用性配置为使用自签名证书

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自签名证书。 对运行于高可用性之下的 NNMi 使用默认证书,无需执行任何额外步骤。

为高可用性配置新证书

假定您创建了名为 newcert 的新自签名或 CA 证书。完成以下步骤,用此新 CA 或自签名 证书配置高可用性。

可如第 305 页的配置 HA 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: %NNM_DATA%\shared\nnm\certificates
 - UNIX: \$NNM_DATA/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\nnm\bin\keytool -import -alias 新证书别名 -keystore nnm.keystore -file newcert
 - UNIX: \$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -import -alias 新证书别名 -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: %NNM DATA%\conf\nnm\props\nms-local.properties
 - UNIX: \$NNM_DATA/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。

将全局网络管理功能配置为使用自签名证书

在 NNMi 安装期间,安装脚本创建 NNMi 管理服务器的自签名证书。此证书包含一个别名,该别名包含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。

假定您希望全局网络管理配置以图 5 为模型。

图 5 全局网络管理



完成以下步骤,将全局网络管理功能配置为根据图5使用自签名证书。

- 1 在完成步骤 2 之前, 切换到 regional1 和 regional2 上的以下目录:
 - Windows: %NNM_DATA%\shared\nnm\certificates
 - UNIX: \$NNM_DATA/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 上运行以下命令以将 regional1 和 regional2 证书合并到 global1 的 nnm.truststore 文件中。

Windows:

a nnmcertmerge.ovpl -truststore regional1 nnm. 信任库位置

b nnmcertmerge.ovpl -truststore *regional2_nnm. 信任库位置* UNIX

- a nnmcertmerge.ovpl -truststore regional1_nnm. 信任库位置
- b nnmcertmerge.ovpl -truststore *regional2 nnm. 信任库位置*
- 4 在 global1 上运行以下命令序列:
 - a ovstop ovjboss
 - b ovstart ovjboss

将全局网络管理功能配置为使用证书颁发机构

在 NNMi 安装期间,安装脚本创建 NNMi 管理服务器的自签名证书。此证书包含一个别名,该别名包含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。

假定您希望全局网络管理配置以图 6 为模型。

图 6 将证书用于全局网络管理



- 1 对于 regional1 和 regional2, 请遵循第 121 页的生成证书颁发机构证书中所示的 说明操作。
- 2 在完成步骤 3 之前, 切换到 regional1 和 regional2 上的以下目录。
 - Windows: %NNM_DATA%\shared\nnm\certificates
 - UNIX: \$NNM_DATA/shared/nnm/certificates
- 3 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。
- 4 在 global1 上运行以下命令以将 regional1 和 regional2 证书合并到 global1 的 nnm.truststore 文件中。

Windows:

```
a nnmcertmerge.ovpl -truststore regional1_nnm. 信任库位置
```

```
b nnmcertmerge.ovpl -truststore regional2_nnm. 信任库位置
UNIX
```

- a nnmcertmerge.ovpl -truststore *regional1 nnm. 信任库位置*
- b nnmcertmerge.ovpl -truststore *regional2_nnm. 信任库位置*
- 5 在 global1 上运行以下命令序列:
 - a ovstop ovjboss
 - b ovstart ovjboss

将带有应用程序故障切换的全局网络管理配置为使用自签名证书

如上所述,在 NNMi 安装期间,安装脚本创建 NNMi 管理服务器的自签名证书。此证书包含一个别名,该别名包含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。

假定您希望如图7中所示,让全局网络管理配置对应用程序故障切换功能建模。

图 7 全局网络管理与应用程序故障切换



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切换:

- 对上图中所示的每个应用程序故障切换群集,请遵循第 124 页的将应用程序故障切换配置为使用自签名证书中所示的说明操作。
- 2 完成第 268 页的应用程序故障切换基本设置中所示的应用程序故障切换配置。
- 3 对于 regional1_active 和 regional2_active,请遵循第 129 页的将全局网络管理 功能配置为使用自签名证书中所示的说明操作。

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,请遵循以下步骤:

- 1 从目录服务器获取贵公司信任库证书。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: %NNM DATA%\shared\nnm\certificates
 - UNIX: \$NNM_DATA/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\b\bin\keytool -import
 -alias nnmi_ldap -keystore nnm.truststore
 -file <目录服务器证书.txt>
 - UNIX: \$NnmInstallDir/nonOV/jdk/b/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 Trust this certificate? [no]: y Certificate was added to keystore

- 4 检查信任库的内容:
 - Windows: %NnmInstallDir%\nonOV\jdk\b\bin\keytool.exe -list -keystore nnm.truststore
 - UNIX: \$NnmInstallDir/nonOV/jdk/b/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:D7:29:02:29:02:29:02:29:02
○ 信任库可以包括多个证书。
5 通过运行以下命令,重新启动 ovjboss:

a ovstop ovjboss
b ovstart ovjboss
b ovstart ovjboss

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)。

配置 HP BSM V9.xx 的 SSL 连接

要配置 HP BSM 的 SSL 连接,请遵循以下步骤:

1 使用以下命令从 nnm.keystore 文件导出 NNMi 证书:

Windows:
 %NnmInstallDir%\nonOV\jdk\b\bin\keytool.exe -export -alias
 主机名.selfsigned -file C:\temp\cert -keystore
 %NnmDataDir%\shared\nnm\certificates\nnm.keystore -storepass
 nnmkeypass

- UNIX: \$NnmInstallDir/nonOV/jdk/b/bin/keytool -export -alias 主机名.selfsigned -file /tmp/cert -keystore \$NnmDataDir/ shared/nnm/certificates/nnm.keystore -storepass nnmkeypass
- 2 确认显示了 Certificate stored in file <目录>:\cert 消息。
- 3 将证书从在步骤1中创建的 cert 文件复制到 BSM 服务器。
- 4 在 BSM 服务器上打开命令窗口。
- 5 用 cd C:\HPBSM\JRE64\bin 命令更改目录。

6 运行以下命令: keytool.exe -import -keystore <目录>:
 \HPBSM\odb\conf\security\server.keystore -storepass hppass
 -trustcacerts -file <目录>\cert。

当系统询问您是否 Trust this certificate? 时,请务必回答 yes。以下程序清单 是运行此命令后所发生情况的示例。

Owner: CN=hpbsm_server.example.com Issuer: CN=hpbsm_server.example.com Serial number: 4d525d0e Valid from: Wed Feb 09 11:23:26 EET 2011 until: Fri Jan 16 11:23:26 EET 2111 Certificate fingerprints: MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2 SHA1: 42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B Signature algorithm name: SHA1withRSA Version: 1 Trust this certificate? [no]: yes Certificate was added to keystore

7 运行步骤 6 中所示命令,用 server.truststore 替换 server.keystore:

keytool.exe -import -keystore <目录>: \HPBSM\odb\conf\security\server.truststore -storepass hppass -trustcacerts -file <目录>:\certo

当系统询问您是否 Trust this certificate? 时,请务必回答 yes。以下程序清单 是运行此命令后所发生情况的示例。

8 要将 NNMi 证书添加到 JRE,请运行以下命令:

```
keytool.exe -import -file<目录>:\cert -keystore<目录>:
\HPBSM\JRE\lib\security\cacerts -trustcacerts -storepass
changeit₀
```

当系统询问您是否 Trust this certificate? 时,请务必回答 yes。以下程序清单 是运行此命令后所发生情况的示例。

Owner: CN=hpbsm_server.example.com Issuer: CN=hpbsm_server.example.com Serial number: 4d525d0e

9 要将 NNMi 证书添加到 JRE64,请运行以下命令:

```
keytool.exe -import -file <目录>:\cert -keystore <目录>:
\HPBSM\JRE64\lib\security\cacerts -trustcacerts -storepass
changeit。
```

当系统询问您是否 Trust this certificate? 时,请务必回答 yes。以下程序清单 是运行此命令后所发生情况的示例。

10 要将 BSM 证书导入到 NNMi 管理服务器中,请完成以下步骤:

a 在BSM服务器上运行以下命令:
 keytool.exe -export -alias clientcert -file
 <目录>:\truststore -keystore <目录>:
 \HPBSM\odb\conf\security\server.truststore -storepass hppass

命令完成之后,在 <目录>:\truststore 文件中存储 BSM 9.01 信任库证书。

b 在 BSM 服务器上运行以下命令: keytool.exe -export -alias hpcert -file <*目录*>:\keystore -keystore <*目录*>: \HPBSM\odb\conf\security\server.keystore -storepass hppass

命令完成之后,在 <目录>:\keystore 文件中存储 BSM 9.01 密钥库证书。

- k truststore 和 keystore 文件复制到 NNMi 管理服务器上的临时目录。这些 文件在剩余命令中显示为驻留在 NNMi 管理服务器上的 <*目录*>: \temp\keystore、 <*目录*>:\temp\truststore、
 /*tmp*/keystore and /*tmp*/truststore 位置。
- d 要合并密钥库证书,请在 NNMi 管理服务器上运行以下命令:

```
    Windows:
    keytool -import -alias hpcert -keystore
    %NnmDataDir%\shared\nnm\certificates\nnm.keystore
    -storepass nnmkeypass -file <目录:\temp\keystore</li>
```

```
    UNIX:
keytool -import -alias hpcert -keystore $NnmDataDir/
shared/nnm/certificates/nnm.keystore -storepass
nnmkeypass -file
/tmp/keystore
```

```
____
```

- e 要合并信任库证书,请在 NNMi 管理服务器上运行以下命令:
 - Windows:

```
keytool -import -alias clientcert -keystore
%NnmDataDir%\shared\nnm\certificates\nnm.truststore
-storepass ovpass -file < 目录>:/temp/truststore
```

— UNIX:

```
keytool -import -alias clientcert -keystore $NnmDataDir/
shared/nnm/certificates/nnm.truststore -storepass ovpass
-file
/tmp/truststore
```

- 11 可选:在 NNMi 管理服务器上运行以下命令序列:
 - a ovstop
 - b ovstart
- 12 *可选*:在 NNMi 管理服务器和 BSM 服务器上运行以下命令。比较输出,以确保密钥库 证书驻留在这两个服务器上:
 - NNMi 管理服务器:
 - Windows: keytool.exe -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore -storepass nnmkeypass
 - UNIX: keytool -list -keystore
 \$NnmDataDir/shared/nnm/certificates/nnm.keystore
 -storepass nnmkeypass
 - BSM 服务器: keytool.exe -list -keystore <目录>:
 \HPBSM\odb\conf\security\server.keystore -storepass hppass

- 13 *可选*:在 NNMi 管理服务器和 BSM 服务器上运行以下命令。比较输出,以确保信任库 证书驻留在这两个服务器上:
 - *NNMi 管理服务器*:
 - Windows: keytool.exe -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm.truststore -storepass ovpass
 - UNIX: keytool -list -keystore
 \$NnmDataDir/shared/nnm/certificates/nnm.truststore
 -storepass ovpass
 - BSM 服务器: keytool.exe -list -keystore <目录>: \HPBSM\odb\conf\security\server.truststore -storepass hppass

对 NNMi 使用 单点登录

可以配置 HP Network Node Manager i Software (NNMi) 单点登录 (SSO) 以简化从 NNMi 控制台到 NNM iSPI 的访问。使用 SSO 时,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。在退出 NNMi 控制台(或 NNMi 控制台会话超时)之后,必须重新输入登录凭证,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:

- 第140页的 NNMi 的 SSO 访问
- 第 141 页的为单个域启用 SSO
- 第 141 页的为位于不同域中的 NNMi 管理服务器启用 SSO
- 第142页的 NNMi 和 NNM iSPI 的 SSO 访问
- 第143页的配置 NNMi 和 HP BSM 或 HP BAC 之间的单点登录
- 第144页的配置 NNMi 和 HP UCMDB 之间的单点登录
- 第 145 页的配置 NNMi 和 HP NA 之间的单点登录
- 第 148 页的禁用 SSO
- 第 148 页的 SSO 安全备注

NNMi 的 SSO 访问

要在几个 NNMi 管理服务器之间浏览, 需要执行以下某个操作:

- 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。
 - 如果使 NNMi 管理服务器仅驻留在一个网络域中,请遵循第 141 页的为单个域启 用 SSO 中所示的说明。
 - 如果使 NNMi 管理服务器驻留在多个网络域中,请遵循第 141 页的为位于不同域 中的 NNMi 管理服务器启用 SSO 中所示的说明获取详细信息。
- 编辑 nms-ui.properties file,确保禁用 SSO。有关详细信息,请参阅第 148 页的 禁用 SSO。

如果选择不完成其中某个操作,则每次浏览不同 NNMi 管理服务器 时,将自动退出前一 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 第 223 页的 SSO 和操作菜单和第 223 页的为全局网络管理配置单点登录。

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
 - UNIX: \$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
```

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:

- 1 编辑以下文件:
 - Windows: %NNM PROPS%\nms-ui.properties
 - UNIX: \$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

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。如果需要为两个或更多 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:

- 1 编辑以下文件:
 - Windows: %NNM_PROPS%\nms-ui.properties
 - UNIX: \$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

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

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。
 - <完全限定的域名>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
- UNIX: \$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 UNIX 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。

如果需要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 UNIX 联机帮助页。

▶ 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。
- <完全限定的域名>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
- UNIX: \$NnmDataDir/conf/nnm/props/nms-local.properties

配置 NNMi 和 HP BSM 或 HP BAC 之间的单点登录

使用相同初始化字符串值并且还共享通用网络域名的所有 HP 企业应用程序都可以使用单 点登录。

如果 NNMi 和 HP Business Service Management (BSM) 或 HP Business Availability Center (BAC) 用户名对于特定个人完全相同,则该用户可以登录"My BSM"门户,并且 无需再次登录 NNMi 即可查看 NNMi Portlet。此单点登录功能在两个产品之间映射用户 名,但不映射密码。用于登录"My BSM"和 NNMi 的密码可以不同。单点登录不映射用 户角色,因此用户在每个应用程序中可以有不同特权。例如,用户可以在 BSM 或 BAC 中 拥有普通特权,而在 NNMi 中拥有管理员特权。

要将单点登录访问从 BSM 或 BAC 配置到 NNMi,请确保这两个应用程序使用相同的初始 化字符串。可以将该字符串从任一应用程序复制到另一个应用程序。选择使用哪个初始化字 符串值时,请考虑交互的所有应用程序。如有必要,还请更新其他应用程序的初始化字符串 配置。 BSM 或 BAC 初始化 如下查找 BSM 或 BAC 初始化字符串:

字符串

1 访问 BSM 或 BAC 的 JMX 控制台,地址是:

http://<BSM 或BAC 主机名>:<BSM 或BAC 的JMX 端口>/jmx-console/

- 选择**服务 =LW-SSO 配置**(在 Topaz 下面)。
 初始化字符串是 InitString 参数的值。
- 3 如果更改 InitString 参数的值,请单击应用更改。
- NNMi 初始化字符串 如下查找 NNMi 初始化字符串:
 - 1 在文本编辑器中打开以下文件:
 - Windows: %NNM_PROPS%\nms-ui.properties
 - UNIX: \$NNM_PROPS/nms-ui.properties
 - 2 搜索字符串 initString。

初始化字符串是不带引号的 initString 参数的值。

例如,如果 nms-ui.properties 文件包含以下文本:

initString=E091F3BA8AE47032B3B35F1D40F704B4

则初始化字符串是:

E091F3BA8AE47032B3B35F1D40F704B4

3 如果更改步骤 2 中显示的 initString 参数的值,则运行以下命令以提交更改:

nnmsso.ovpl -reload

配置 NNMi 和 HP UCMDB 之间的单点登录

使用相同初始化字符串值并且还共享通用网络域名的所有 HP 企业应用程序都可以使用单 点登录。

如果 NNMi 和 HP Universal CMDB (UCMDB) 用户名对特定个人完全相同,则该用户可 以登录 NNMi 控制台,并且无需登录 UCMDB 即可启动 UCMDB 视图。此单点登录功能 在两个产品之间映射用户名,但不映射密码。用于登录 NNMi 和 UCMDB 的密码可以不 同。单点登录不映射用户角色,因此用户在每个应用程序中可以有不同特权。例如,用户可 以在 NNMi 中拥有普通特权,而在 UCMDB 中拥有管理员特权。

要从 NNMi UCMDB 配置单点登录访问,请确保这两个应用程序使用相同的初始化字符 串。可以将该字符串从任一应用程序复制到另一个应用程序。选择使用哪个初始化字符串值 时,请考虑交互的所有应用程序。如有必要,还请更新其他应用程序的初始化字符串配置。

UCMDB 初始化 如下查找 UCMDB 初始化字符串:

字符串

1 从以下网址访问 UCMDB 的 JMX 控制台:

http://<UCMDB 主机名>:<UCMDB JMX 端口>/jmx-console/
2011年3月

- 选择**服务 =LW-SSO 配置**(在 Topaz 下面)。
 初始化字符串是 InitString 参数的值。
- 3 如果更改 InitString 参数的值,请单击**应用更改**。

NNMi 初始化字符串 如下查找 NNMi 初始化字符串:

- 1 在文本编辑器中打开以下文件:
 - Windows: %NNM PROPS%\nms-ui.properties
 - UNIX: \$NNM_PROPS/nms-ui.properties
- 2 搜索字符串 initString。

初始化字符串是不带引号的 initString 参数的值。

例如,如果 nms-ui.properties 文件包含以下文本:

initString=E091F3BA8AE47032B3B35F1D40F704B4

则初始化字符串是:

E091F3BA8AE47032B3B35F1D40F704B4

3 如果更改 initString 参数的值,则运行以下命令以提交更改:

nnmsso.ovpl -reload

配置 NNMi 和 HP NA 之间的单点登录

使用相同初始化字符串值并且还共享通用网络域名的所有 HP 企业应用程序都可以使用单 点登录。

如果 NNMi 和 HP Network Automation (NA) 用户名对特定个人完全相同,则该用户可以 登录 NNMi,并且无需登录 NA 即可查看 NA 页。此单点登录功能在两个产品之间映射用 户名,但不映射密码。用于登录 NNMi 和 NA 的密码可以不同。单点登录不映射用户角色, 因此用户在每个应用程序中可以有不同特权。例如,用户可以在 NNMi 中拥有第1级操作 员特权,而在 NA 中拥有管理员特权。

要将单点登录访问从 NNMi 配置到 NA,请确保这两个应用程序使用相同初始化字符串。可以将该字符串从任一应用程序复制到另一个应用程序。选择使用哪个初始化字符串值时,请考虑交互的所有应用程序。如有必要,还请更新其他应用程序的初始化字符串配置。

NNMi 初始化字符串 在 NNMi 管理服务器上,如下查找 NNMi 初始化字符串:

- 1 在文本编辑器中打开以下文件:
 - Windows: %NNM PROPS%\nms-ui.properties
 - UNIX: \$NNM PROPS/nms-ui.properties
- 2 搜索字符串 initString。

初始化字符串是不带引号的 initString 参数的值。

例如,如果 nms-ui.properties 文件包含以下文本:

initString=E091F3BA8AE47032B3B35F1D40F704B4

则初始化字符串是:

E091F3BA8AE47032B3B35F1D40F704B4

3 如果更改 initString 参数的值,则运行以下命令以提交更改:

nnmsso.ovpl -reload

NA 初始化字符串 在 NA 服务器上,如下查找 NA 初始化字符串:

- 1 在文本编辑器中打开以下文件:
 - Windows: %NA HOME%\server\ext\jboss\server\default\conf\lwssofmconf.xml
 - UNIX: \$NA_HOME/server/ext/jboss/server/default/conf/lwssofmconf.xml

NA_HOME 环境变量的默认值如下所示:

- Windows: C:/na
- UNIX: /opt/NA
- 2 在 enableLWSSO 标记中,将 enableLWSSOFramework 属性设置为 true:

enableLWSSOFramework="true"

- 3 在 lwssoValidation 块中,执行以下操作:
 - 将 domain 标记的值设置为 NA 服务器的完整域名。例如,如果 NA 服务器的主机 名是 na.location.example.com,则设置 <域>location.example.com</domain>。



此步骤假定 NNMi 管理服务器与 NA 服务器在同一域中。如果不是,则必须将 NNMi 管理服务器的域的 DNSDomain 元素添加到 trustedHosts 块。

• 在 crypto 标记中,将 initString 属性设置为 NNMi nms-ui.properties 文件 中 initString 属性的值。



参与 SSO 的所有应用程序的 crypto 块中的设置必须相同。

4 在 trustedHosts 块中,将 DNSDomain 标记设置为 lwssoValidation 块中 domain 标记的值,例如:

<DNS 域>location.example.com</DNS 域>



此步骤假定 NNMi 管理服务器与 NA 服务器在同一域中。如果 NA 服务器与 NNMi 管理服务器不在同一域中,请为这两个域都添加 DNSDomain 条目。

5 确保参与 SSO 的所有应用程序的 GMT (格林威治标准时间)时差都小于 15 分钟。尽 管它们可以在不同时区中,但转换为 GMT 后的时差应当相同。

- 6 重新启动 NA jboss 服务器:
 - Windows: 在 NA 用户界面中的管理 > 启动/停止服务页上,重新启动管理引擎。
 - *UNIX*: 运行以下命令:

/etc/init.d/truecontrol restart

禁用 SSO

如果需要禁用 SSO,请完成以下步骤:

- 1 编辑以下文件:
 - Windows: %NNM PROPS%\nms-ui.properties
 - UNIX: \$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

对它进行如下更改:

com.hp.nms.ui.sso.isEnabled = false

3 运行以下命令以提交更改:

nnmsso.ovpl -reload

SSO 安全备注

1 SSO 安全中的机密 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。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 使用最低身份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 用程序的身份验证安全级别。

HP 建议只有使用强大和安全的身份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 的应用程序在不受信任位置中驻留或可访问时,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,相同用户名可能在各种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身份验证的应用程序 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),则用户将分别使用登录到应用程序 A 或应用程序 B 的用户名访问应用程序 C。

6 身份管理器用于身份验证:

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。

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:

- 第 151 页的禁用 Telnet 或 SSH 菜单项
- 第 152 页的为 Windows 上的浏览器配置 Telnet 或 SSH 客户端
- 第158页的在 Linux 上配置 Firefox 使用 Telnet 或 SSH
- 第 160 页的用于更改 Windows 注册表的示例文件

禁用 Telnet 或 SSH 菜单项

如果您的部署环境中的 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,请遵循以下步骤:

- 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 _____。

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 > Secure 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。

表6标识了每种浏览器和操作系统的组合要使用的过程。

表 6 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	 第 153 页的 Windows 操作系统提供的 Telnet 客 户端 第 155 页的第三方 Telnet 客户端 (标准 Windows) 第 157 页的第三方 SSH 客户端 (标准 Windows 以及 Windows on Windows)
	64 位 Windows 7	 第 155 页的第三方 Telnet 客户端 (标准 Windows) 第 157 页的第三方 SSH 客户端 (标准 Windows 以及 Windows on Windows)
	64 位,除 Windows 7 以外	 第 156 页的第三方 Telnet 客户端 (Windows on Windows) 第 157 页的第三方 SSH 客户端 (标准 Windows 以及 Windows on Windows)

2011年3月

Web 浏览器	Windows 操作系统体系 结构	适用过程
64 位 Internet Explorer	64 位	 第 153 页的 Windows 操作系统提供的 Telnet 客 户端 第 155 页的第三方 Telnet 客户端 (标准 Windows) 第 157 页的第三方 SSH 客户端 (标准 Windows 以及 Windows on Windows)
Firefox	32 位	 第 153 页的 Windows 操作系统提供的 Telnet 客 户端 第 155 页的第三方 Telnet 客户端 (标准 Windows) 第 157 页的第三方 SSH 客户端 (标准 Windows 以及 Windows on Windows)
	64 位 Windows 7	 第 155 页的第三方 Telnet 客户端 (标准 Windows) 第 157 页的第三方 SSH 客户端 (标准 Windows 以及 Windows on Windows)
	64 位,除 Windows 7 以外	 第 156 页的第三方 Telnet 客户端 (Windows on Windows) 第 157 页的第三方 SSH 客户端 (标准 Windows 以及 Windows on Windows)

表 6 Windows 上 Telnet 和 SSH 配置过程列表 (续)



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,请参阅第 160 页的 用于更改 Windows 注册表的示例文件。

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

要配置操作系统提供的 Telnet 客户端以供 Web 浏览器使用,请遵循以下步骤:

1 (仅适用于 Microsoft Windows 7、Microsoft Vista 或 Microsoft Windows Server 2008) 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 2008:

- 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 设置 URL:Telnet 协议文件类型的文件关联。
 - 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

%1(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。

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 %1

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(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,请遵循以下步骤:

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 设置 URL:Telnet 协议文件类型的文件关联。
 - 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

%1(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。 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>

< 方点> 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,请遵循以下步骤:

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 设置 URL:Telnet 协议文件类型的文件关联。
 - 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

%1(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。

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,请遵循以下步骤:

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);
```

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。

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,请参阅 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,请遵循以下步骤:

- 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。

- 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)。直接将链接键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,请遵循以下步骤:

- 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。

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。直接将链接键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第 153 页的 Windows 操作系统提供的 Telnet 客户端。

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:0000000

[HKEY_CLASSES_ROOT\telnet\shell\open\command] @="\"C:\\Windows\\system32\\rundll32.exe\" \"C:\\Windows\\system32\\url.dll\",TelnetProtocolHandler %1"

示例 nnmputtytelnet.reg

此注册表内容示例适用于第155页的第三方 Telnet 客户端 (标准 Windows)。

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\" %1" 2011年3月

示例 nnmtelnet32on64.reg

此注册表内容示例适用于第 156 页的第三方 Telnet 客户端 (Windows on Windows)。

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:0000000

[HKEY CLASSES ROOT\Wow6432Node\telnet\shell\open\command] @="\"C:\\Program Files\\PuTTY\\putty.exe\" %1"

示例 nnmssh.reg

此注册表内容示例适用于第 157 页的第三方 SSH 客户端 (标准 Windows 以及 Windows on Windows)。

Windows 注册表编辑器版本 5.00

[HKEY_CLASSES_ROOT\ssh] @="URL:ssh Protocol" "EditFlags"=dword:0000002 "FriendlyTypeName"="Secure Shell" "URL Protocol"=""

[HKEY_CLASSES_ROOT\ssh\shell\open\command] @="\"C:\\Windows\\System32\\WScript.exe\" \"c:\\Program Files\\PuTTY\\ssh.js\" %1" 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:

- 第163页的NNMi用户访问信息和配置选项
- 第167页的配置 NNMi 访问目录服务
- 第 174 页的将目录服务访问配置更改为支持 NNMi 安全模型
- 第176页的目录服务查询
- 第 186 页的用于存储 NNMi 用户组的目录服务配置
- 第187页的对目录服务集成进行故障诊断
- 第188页的 ldap.properties 配置文件参考

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。表 7 表示用于存储每个配置选项的 NNMi 用户访问信息的数据库。

表7 存储用户信息的选项

选项	用户名	密码	用户组	用户组成员资格
1	NNMi	NNMi	NNMi	NNMi
2	两者	目录服务	NNMi	NNMi
3	目录服务	目录服务	两者	目录服务

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 与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方式或存储 位置都无关。

选项 1: NNMi 数据库中的所有 NNMi 用户信息

使用配置选项 1, 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 (如图 8 中的注释行所指示)。

图 8 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。不需要阅读本章。

图 8 NNMi 选项 1 的用户登录信息流



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

使用配置选项 2, 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 管理员配置 NNMildap.properties 文件,以针对用户名向 NNMi 描述目录服 务数据库架构。(在图 9 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。

图 9 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*。

图 9 NNMi 选项 2 的用户登录信息流



选项 3: 目录服务中的所有 NNMi 用户信息

使用配置选项 3, 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 管理员配置 NNMildap.properties 文件,以针对用户名和组向 NNMi 描述目 录服务数据库架构。

图 10 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。

因为此选项是选项 2 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*。

图 10 NNMi 选项 3 的用户登录信息流



配置 NNMi 访问目录服务

目录服务访问是在以下文件中配置的:

- Windows: %NNM_SHARED_CONF%\ldap.properties
- UNIX: \$NNM_SHARED_CONF/ldap.properties

有关此文件的信息,请参阅第 188 页的 ldap.properties 配置文件参考。另请参阅第 192 页 的示例。

有关目录服务的常规结构的信息,请参阅第176页的目录服务查询。

对于配置选项 2, 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

对于配置选项3,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

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,请参阅第 186 页的用于存储 NNMi 用户组的目录服务配置。

- 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: 可选。配置与目录服务的安全通信

如果目录服务需要使用安全套接字层 (SSL),请将贵公司的证书导入到 NNMi 信任库中, 如第 132 页的配置与目录服务的 SSL 连接中所述。

任务 3: 配置目录服务中的用户访问

对配置选项2和3完成此任务。遵循适用于您的目录服务的相应过程。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,请参阅第181页的用户标识。)

用于 Microsoft Active Directory 的简单方法

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

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

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

baseCtxDN=CN=Users,DC=<我的主机名>,DC=<我的公司名>,DC=<我的后缀>baseFilter=CN={0}

defaultRole=guest

#rolesCtxDN=CN=Users,DC=<我的主机名>,DC=<我的公司名>,DC=<我的后缀>
roleFilter=member={1}
uidAttributeID=member
userRoleFilterList=admin;level2;level1

3 指定用于访问目录服务的 URL。在以下行中:

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

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

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证。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。因为密码以明文形式存储,因此请指定对目录服务具有只读访问权的用 户名。
- 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,然后在任何文本编辑器中打开此文件。
- 2 指定用于访问目录服务的 URL。在以下行中:

#java.naming.provider.url=ldap://*<我的 ldap 服务器*>:389/ 执行以下操作:

- 取消注释行 (方法是删除 # 字符)。
- 将 < 我的 1 dap 服务器> 替换为目录服务器的完全限定主机名 (例如: myserver.example.com)。

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

- 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。

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)。
 - 如果用户登录正常运行,则继续执行此任务的步骤8。
 - 如果用户登录不能正常执行,则接下来继续执行步骤 6。

在每个测试之后,从 NNMi 控制台注销以清除会话凭证。

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:

- 验证是否正确完成第 168 页的任务 3。
- 遵循第 181 页的用户标识中的详细配置过程。
- 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 数据库中存储 NNMi 用户组成员资格 (配置选项 2),则继续 执行第 173 页的任务 9。
 - 如果计划在目录服务中存储 NNMi 用户组成员资格(配置选项 3),则继续执行接下来的任务 5。

任务 5: (仅配置选项 3) 配置目录服务中的组检索

对配置选项3完成此任务。遵循适用于您的目录服务的相应过程。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,请参阅第183页的用户组标识。)

用于 Microsoft Active Directory 的简单方法

- 1 备份 ldap.properties 文件,然后在任何文本编辑器中打开此文件。
- 2 指定用于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,然后在任何文本编辑器中打开此文件。
- 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: (仅配置选项 3) 将目录服务组映射到 NNMi 用户组

- 1 在 NNMi 控制台中,将预定义 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**管理员**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。
- e 对于每个 guest、 level1 和 level2 行,重复步骤 b 到步骤 d。

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, 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 用户的每个额外的目录服务组,重复步骤 b 和步骤 c。

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: (仅配置选项 3)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。

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)。
 - 如果用户登录正常运行,则继续执行第172页的任务8。
 - 如果用户登录不能正常执行,则接下来继续执行步骤 5。

在每个测试之后,从 NNMi 控制台注销以清除会话凭证。

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:

- 验证是否正确完成第 170 页的任务 5。
- 验证对于每个预定义 NNMi 用户组,是否正确完成了第 171 页的任务 6。
- 遵循第 183 页的用户组标识中的详细配置过程。
- 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: (仅配置选项 3) 配置事件分配的 NNMi 用户组

- 1 备份 ldap.properties 文件,然后在任何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。
- 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(如第184页的表10 中所定义)。
 - 3 保存 ldap.properties 文件。

2011年3月

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 重复执行步骤 1 到步骤 6, 直到可以将事件分配给每个所配置的 NNMi 角色。

任务 9: 清除操作以防止意外访问 NNMi

- 1 可选。更改或注释 ldap.properties 文件中的 defaultRole 参数的值。
- 2 (仅配置选项 2) 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 (仅配置选项 3)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。

将目录服务访问配置更改为支持 NNMi 安全模型

本部分信息描述如何修订 NNMi 8.1x 或 9.0x 中的 ldap.properties 文件以支持每个用 户属于多个 NNMi 用户组。这一修订在以下 两个情况下都是必要的:

- ldap.properties 文件当前启用 NNMi 用户访问配置选项 3(目录服务中的所有 NNMi 用户信息)。
- 已经或将使用自定义安全组配置 NNMi。

在 NNMi 8.1x 和 9.0x 中,为 NNMi 用户分配预定义的 NNMi 角色之一。每个用户可以访问 NNMi 拓扑中的所有对象。

在 NNMi 9.10 中,用预定义 NNMi 用户组代替 NNMi 角色。每个 NNMi 用户必须属于至 少一个预定义 NNMi 用户组,预定义组定义 NNMi 用户可以在 NNMi 控制台中执行的操 作。其他用户组 (如果存在)通过以下方式限制对 NNMi 拓扑对象的访问:

- 如果没有自定义用户组存在,则所有 NNMi 控制台用户都可以访问所有拓扑对象。
- 如果存在一个或多个自定义用户组,则这些用户组中的每一个都可以访问 NNMi 拓扑 中的对象的某个子集。

NNMi 8.1x 和 9.0x 要求每个目录服务组定义包含名为相应 NNMi 角色的组属性。在 ldap.properties 配置文件中,以下参数指定了此组属性:

- roleAttributeID
- roleAttributeIsDN
- roleNameAttributeID

NNMi 9.10 弃用这些参数。它们将在未来版本中不受支持。

在 NNMi 9.10 中,每个用户组必须在 NNMi 控制台中定义。用户组定义包含外部名称,此 名称是该组在目录服务中的可分辨名称。

要更改目录服务访问配置以支持 NNMi 安全模型,请遵循以下步骤:

1 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

- 2 备份 ldap.properties 文件,然后在任何文本编辑器中打开此文件。
 - 有关 1dap.properties 文件的信息,请参阅第 188 页的 ldap.properties 配置文件参考。有关弃用参数的信息,请参阅之前版本的 NNMi 的《NNMi 部署参考》。

- 3 注释或删除以下参数 (如果它们存在):
 - roleAttributeID
 - roleAttributeIsDN
 - roleNameAttributeID

roleAttributeID 参数是告诉 NNMi 用于标识 NNMi 用户组的方法的标记。设置 roleAttributeID时, NNMi 使用 NNMi 8.1x 和 9.0x 方法。不设置 roleAttributeID 时, NNMi 使用 NNMi 9.10 方法。

- 4 在 NNMi 控制台中,将预定义 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**管理员**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。
- e 对于每个 guest、 level1 和 level2 行,重复步骤 b 到步骤 d。

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。

- 5 在目录服务中,标识其他的 NNMi 用户组。根据需要定义新组。
- 6 对于在步骤 5 中添加的每个新组,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, 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 用户的每个新目录服务组,重复步骤 b 和步骤 c。
- 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。
- 7 可选。将用户组映射到安全组。 有关信息,请参阅 NNMi 帮助中的*配置安全*。

目录服务查询

NNMi 使用 LDAP 与目录服务通信。NNMi 发送请求,目录服务返回存储的信息。NNMi 无法改变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
- 目录服务内容
- 由目录服务管理员拥有的信息
- 用户标识
- 用户组标识

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>

- 1dap 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> 是主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。

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 UNIX 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 的组属性是: 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
```

第178页的图11图解了此目录服务域。

图 11 Active Directory 域示例



2011年3月

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 的组属性是: 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
```

图 12 其他目录服务域示例

o=example.com
ou=People
uid=john.doe@example.com
uid=jane.doe@example.com
uid=chris.smith@example.com
ou=Groups
cn=USERS-NNMi-Admin member=john.doe@example.com,ou=People,o=example.com member=chris.smith@example.com,ou=People,o=example.com
cn=USERS-NNMi-Level1 member=john.doe@example.com,ou=People,o=example.com member=jane.doe@example.com,ou=People,o=example.com
on-LISERS NNIM Cupst
cn=USERS-NNMi-Client

由目录服务管理员拥有的信息

表 8 和表 9 列出在配置 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 (配置选项 2),则收集表 8 的信息。
- 如果计划使用目录服务以获取所有 NNMi 访问信息 (配置选项 3),则收集表 8 和表 9 的信息。

表 8 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
主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,并参阅第 132 页的配置与目录服务的 SSL 连接。	
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

表 9 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
表 9 用于从目录服务检索组成员资格的信息(续)

信息	Active Directory 示例	其他目录服务示例
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

用户标识应用于配置选项2和3。

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。

对于配置选项 2,以下信息适用:

- 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。

对于配置选项3,以下信息适用:

- 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。

Active Directory 用户如果 baseFilter 设置为 CN={0}, baseCtxDN 设置为 OU=Users,OU=Accounts,DC=example,标识示例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如果 baseFilter 设置为 uid={0}@example.com, baseCtxDN 设置为 ou=People,识示例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)

如果第168页的任务3中所述的简单方法未能正常运行,则遵循以下步骤:

- 1 从目录服务管理员处获取第 180 页的表 8 中列出的信息。
- 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*:请参阅第 183 页的确 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*:请参阅第 183 页的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。

有关 ldap.properties 文件的信息,请参阅第 188 页的 ldap.properties 配置文件参考。

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 浏览器配置获取此信息。
- Web 浏览器方法:包含第 183 页的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。

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,则取消注释(或添加)以下行: 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。因为密码以明文形式存储,因此请指定对目录服务具有只读访问权的用 户名。
- 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 按第169页的任务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> 是主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不可达的消息,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

用户组标识适用于配置选项3。

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。表 10 将这些组的唯一名称映射到其显示名。

表 10 NNMi	用户组名称映射
-----------	---------

NNMi 控制台中的 NNMi 角色名称	NNMi 配置文件中的用户组唯一名称和文本字 符串
管理员	admin
第2级操作员	level2
第1级操作员	level1
来宾	guest
Web 服务客户端	client

配置目录服务中的用户组检索(详细方法)

如果第170页的任务5中所述的简单方法未能正常运行,则遵循以下步骤:

- 1 从目录服务管理员处获取第180页的表 9 中列出的信息。
- 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*:请参阅第 185 页的确定目录服务如何 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*:请参阅第 185 页的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*:请参阅第 185 页的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。
 - 有关 ldap.properties 文件的信息,请参阅第 188 页的 ldap.properties 配置文件 参考。
- 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。

2011年3月

- 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 按第 172 页的任务 7 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> 是主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中存储 NNMi 用户组(配置选项 3),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。

对目录服务集成进行故障诊断

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 %NnmDataDir%\log\nnm\jbossServer.log(Windows)或/var/opt/OV/log/ nnm/jbossServer.log(UNIX) 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:
 - 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,如第 132 页 的配置与目录服务的 SSL 连接中所述启用 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,增大 nms-ldap.properties 文件中 searchTimeLimit 的值。

javax.naming.TimeLimitExceededException: [LDAP: error code 3
- Timelimit Exceeded]

Idap.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
- UNIX: \$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 \+
 - 要将空格字符()包含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。
 - 要将井号字符(#)包含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。

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

表 11 描述了 ldap.properties 文件中的参数。

初始 ldap.properties 文件可能未包含表 11 中列出的所有参数。添加需要的参数。

衣 II Idap.properties 义件中的参	9参数
----------------------------	-----

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。	
	• 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:	
	<pre>java.naming.provider.url=ldap://ldap1.example.com/ ldap:// ldap2.example.com/</pre>	
	配置此参数将在 NNMi 和目录服务之间启用 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。	

2011年3月

表 11 ldap.properties 文件中的参数(续)

参数	描述
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,请参阅第 132 页的配置与目录服务的 SSL 连接。
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。因为此用户名的密码以明文形式存储于 ldap.properties 文件 中,因此请选择对目录服务具有只读访问权的用户名。 例如: bindDN=region1\\john.doe@example.com
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,请参阅第 181 页的用户标识。
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} (表示为 登录输入的用户名)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,请参阅第 181页的用户标识。

表 11 ldap.properties 文件中的参数(续)

参数	描述		
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。 这些名称是预定义 NNMi 用户组名称的唯一名称(如第 184 页的表 10 中所 定义)。 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-level10perators之类的组,则可以使用类似如下的搜索上下文: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,请参阅第 183 页的用户组标识。 		

表 11 ldap.properties 文件中的参数(续)

参数	描述	
roleFilter	定目录服务组定义中组成员名称的格式。 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 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 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} 表示为登录输入的用户名 (例如 john.doe)。 关于与为登录所输入 (短) 用户名匹配的角色过滤器示例: 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过滤器示例: roleFilter=member={1} 有关详细信息,请参阅第 183 页的用户组标识。 	
uidAttributeID		
	例如: uidAttributeID=member 有关详细信息,请参阅第 183 页的用户组标识。	
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 (如 第 184 页的表 10 中所定义)。 userRoleFilterList=admin; level2; level1	
searchTimeLimit	可选。指定超时值 (毫秒)。默认值是 10000 (10 秒)。如果在 NNMi 用户登录期间遇到超时,请增大此值。 例如: searchTimeLimit=10000	

示例

用于 Active Directory	下面是用于 Active Directory 的 ldap.properties 文件示例:			
的 Idap.properties 文件示例	<pre>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 roleFilter=member={1} uidAttributeID=member userRoleFilterList=admin;level2;level1</pre>			
用于其他目录服务的 Idap.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			

NNMi 安全和 多租户



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模型,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:

- 第194页的限制对象访问的影响
- 第 195 页的 NNMi 安全模型
- 第 200 页的 NNMi 租户模型
- 第 203 页的 NNMi 安全和多租户配置
- 第 210 页的 NNMi 安全、多租户和全局网络管理
- 第 213 页的在 NPS 报告中包含选择界面

限制对象访问的影响

配置 NNMi 安全有以下影响:

- 拓扑资产对象:
 - 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。
 - 一 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有权访问组中至少一个节点的节点组。
 - 对于网络性能服务器 (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,请参阅第 213 页的在 NPS 报告中包含选择界面。
- 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。
 - 一 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。
 - 一 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)。
- 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。
 - 一 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 控制台视图中可见 的某些对象无效的操作。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 共用字符串的节点的 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 安全配置强制该用户的访问权,并相应限制可用拓扑。

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。
- 用于按安全组过滤自定义节点视图和 网络性能服务器 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 第1级操作员
 - NNMi 第2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。

NNMi Web 服务客户端用户组无权访问 NNMi 控制台;但是,它可以授予对所有 NNMi 对象的管理员级别访问。

• 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。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。 所有节点组件都继承该节点的安全组分配。

- 最佳实践 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

图 13 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。

第 198 页的表 12 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。)第 199 页的表 13 列出了此拓扑的几个用户帐户和用户组之间的映射。



表 12 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	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

2011年3月

表 12 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
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

表 13 用户帐户映射示例

用户帐户	用户组	节点访问	说明
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。
	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
	UG2 级别 1	D、 E	的卫点具有弗 1 级操作贝切 问权。
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。
	UG3 级别 2	F、 G	
	UG4 级别 2	H, I, J	
用户 T	NNMi 第2级操作员	无	此用户对拓扑示例中的所有节
	UG1 来宾	A, B, C	 □ 点具有访问权 (特权级别可以 变化)。 □ 此用户具有对节点 D 和 E 的管 理访问权 但看不到雲要管理访
	UG2 管理员	D, E	
	UG3 级别 2	F、 G	一座的内秋, 固有小到而安官哇的 问权的工具的菜单项。如果此
	UG4 级别 1	H、I、J	用户有权访问 NNM1 管理服务器,则此用户可以仅对节点 D 和 E 运行需要管理访问权的命 令行工具。

NNMi 租户模型

NNMi 租户模型可将拓扑搜索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过滤自定义节点资产视图和网络性能服务器报告。
- 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。

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。

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,首次搜索节点并将其添加到 NNMi 数据库时,进行初始搜索租户分配。对于种子节点,可以指定分配到每个节点的租户。NNMi 将所有其他搜索的节点(包含在自动 搜索规则中但不直接播种的节点)分配给默认租户。NNMi 管理员可以在搜索后随时更改节 点的租户。

每个租户定义都包括初始搜索安全组。NNMi 将此初始搜索安全组和初始搜索租户一起分配 给节点。NNMi 管理员可以在搜索后随时更改节点的安全组。

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。

所有节点组件都继承该节点的租户和安全组分配。

最佳实践 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

图 14 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。

第 202 页的表 14 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。)第 202 页的表 15 列出了此拓扑的几个用户帐户和用户组之间的映射。

图 14 多租户拓扑示例



表 14 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
T2 SGb	Н	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

表 15 多租户用户帐户映射示例

用户帐户	用户组	节点访问	说明
用户 L	NNMi 第2级操作员	无	此用户对粉红色椭圆(实线)
	T1 级别 2	A, B, C, D, E	中的卫点具有弟2级操作页切 问权,此椭圆将所有节点分组 为租户1。
用户 M	NNMi 第1级操作员	无	此用户对橙色椭圆(虚线)中
	T2_a 级别 1	F, G	的下点具有第 1 级操作页切向 权,此椭圆将一部分节点分组
	T2_b 级别 1	Н	为租户 2。
用户 N	NNMi 第2级操作员	无	此用户对绿色椭圆(点线)中
	T2_b 级别 2 H 的下点具1 权,此椭圆	的节点具有第2级操作页访问 权,此椭圆将一部分节点分组	
	T2_c 级别 2	I、J	为租户 2。

NNMi 安全和多租户配置

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。

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**自定义节点**资产视图中显示为一列。

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**和自定义节点资产视图中显示为一列。

- **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过滤器。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。
- 最佳实践 由于安全组和租户名称可以更改,请在其他过滤器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 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 台访问 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。

此建议的例外情况是管理级别,因为 NNMi 管理员有权访问所有拓扑对象。要将 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 1 级操作员或 NNMi 第 2 级操作员用户组。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,请参阅第 163 页的通过 LDAP 将 NNMi 与目录服务集成。

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。



安全向导仅针对 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**工作区的**搜索**下。每个**租户**表单描述 一个 NNMi 租户,并显示当前分配到该租户的节点。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,并显示当前分配到该安全组的节点。节点分配 信息是只读的。 2011年3月

•	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。

最佳实践 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 user1 -password password -role level1 nnmsecurity.ovpl -createUserAccount user2 -password 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

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 拓扑对象分配到租户(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 分配到搜索的节点的安全组由与该节点关联的租户的初始搜索安全组的值设置。
- 使用 NNMi 安全模型而不配置 NNMi 租户时,所有节点分配到默认租户。
- 当您播种节点进行 NNMi 搜索时,可以指定该节点所属的租户。 NNMi 通过自动搜索规则搜索节点时, NNMi 将该节点分配到默认租户。搜索之后,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。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,将初始搜索安全组设置为默认安全组或具有受限访问权的租户特定 安全组。此方法确保租户的新节点在一般情况下不可见,除非 NNMi 管理员配置了 访问权。

6 将租户分配到种子,准备搜索。

搜索一组节点之后,可以更改初始搜索安全组的值。使用此方法限制将节点手动重新分 配到安全组。

- 7 搜索完成后,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。
- 8 继续执行第 208 页的步骤 4。

配置安全组

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。

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 分配到搜索的节点的安全组由与该节点关联的租户的初始搜索安全组的值设置。
- 使用 NNMi 安全模型而不配置 NNMi 租户时,所有节点分配到默认租户。

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。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:
 - 为应有权访问 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 按第 208 页的验证配置中所述验证配置。
- 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。



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 验证每个节点是否分配到正确安全组的一个方法是按安全组排序**节点**或**自定义节点**资产视图,然后检查分组。

另一个方法是使用带 -listNodesInSecurityGroup 选项的 nnmsecurity.ovpl 命令。

2011年3月

验证每个用户是否都

有 NNMi 控制台访

问权

验证用户组到安全组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,然的分配后检查分组。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。

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:

- NNMi 管理员
- NNMi 第1级操作员
- NNMi 第2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。

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。

验证用户到用户组的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 分配分组。

> 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 验证每个节点是否分配到正确租户的一个方法是按租户排序**节点**或自定义节点资产视图,然 分配 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,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1级操作员、NNMi 第2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

表 16 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。

表 16 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

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。 2011年3月

最佳实践 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。



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。

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。

最佳实践 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

本部分包含以下主题:

- 第 211 页的初始 GNM 配置
- 第 213 页的 GNM 维护

初始 GNM 配置

在首先配置 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 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 **同步** 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搜索安全组的安全组。

与自定义租户的拓扑 对于有自定义 同步 加到租户的 [

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。
- 初始搜索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 的初始搜索安全组。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。

最佳实践 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)的初始搜索安全组的值,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搜索安全 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

表 17 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。

表 17 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 搜索安全组)。	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

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。



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,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



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
- "全局网络管理"是管理网络的好工具吗?
- 实用的全局网络管理示例
- 查看要求
- 初始准备
- 为全局网络管理配置单点登录
- 在区域管理器上配置转发过滤器
- 用区域管理器连接全局管理器
- 确定从 global1 到 regional1 和 regional2 的连接状态
- 查看 global1 资产
- 断开 global1 和 regional1 之间的通信连接
- 更多信息
- 为全局网络管理配置应用程序故障切换
- 全局网络管理的故障诊断提示
- 全局网络管理和 NNM iSPI 或第三方集成

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 管理服务器搜索和监视网络,以满足搜索 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,而无需其他搜索或监视配置更改。 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*。

"全局网络管理"是管理网络的好工具吗?

请通过以下问题来确定 NNMi 的全局网络管理功能是否能帮助您更好地管理网络。

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上的网络设备吗?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过滤器。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过滤器,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,请参阅第 115 页的许可 NNMi。
我的全局和区域管理器都需要NNMi Advanced 许可证吗? 您必须为要用作全局管理器的 NNMi 管理服务器购买并安装 NNMi Advanced 许可证。用作区域管理器的 NNMi 管理服 务器不需要 NNMi 许可证。

*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?*可以。如果您的信息技术组需要监视位于多个站点的关键设备,可在区域管理器上配置转发过滤器,以确保只将关键设备相关的信息转发到全局管理器。这使您能够明智地使用 NNMi 资源,并控制全局管理器上许可证容量的使用。

我增加了区域管理器的NNMi许可证数,这样许可节点的总数大于全局管理器上NNMi Advanced许可证数。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 可证数不足而跳过的节点?您需要为全局管理器购买并安装足够的NNMiAdvanced许可 证,使其许可证数达到或超过区域管理器上安装的许可证总数。安装足够多的许可证后,执 行以下一项操作:

- 等待所有区域管理器上的所有配置的重新搜索间隔过去,以便重新搜索所有区域中的所有节点。区域管理器重新搜索所有区域中的所有节点之后,它将这些重新搜索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。

第二个选择在网络上造成很大通信量,并占用整组 NNMi 管理器的大量 NNMi 资源。此选 择不像初始 NNMi 搜索那样占用资源,但占用量与执行第一次搜索类似。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 区域管理器的重新搜索。

实用的全局网络管理示例

请参阅第 218 页的图 15。假定贵公司有位于不同地理位置的两个工作场所。公司总部则位于第三个地理区域。3 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。





查看要求

假定公司总部、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, NNMi 管理服务器分别称为 global1、 regional1 和 regional2。假定您已将这些 NNMi 管理服务器配置为搜索和监视位于各自位置的关键交 换机和路由器。无需在其中任何站点重新配置 NNMi 管理服务器搜索,即可使用全局网络 管理功能。

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。 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。下表总结了监视要求:

表 18 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

总的来说,您有 NNMi 管理服务器和 regional1 监视公司总部。有 NNMi 管理服务器、 regional1 和 regional2 监视每个区域位置。您需要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。对于此示例,假定 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:

- 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,如果您需要第二个全局管理器 global2 与 regional1 通信,则 NNMi 允许您配置 global1 和 global2 与 regional1 通信。有关详细信息,请参阅 HP Network Node Manager i Software 系统和设备支持列表。
- 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

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,需要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。

在此部分讨论的示例中, global1 建立与 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
- UNIX: \$NNM CONF/nnm/props/nms-local.properties

下表显示必须可访问的已知端口:

表 19 必须可访问的套接字

	安全性	参数		TCP 端口
# SSL		jboss.http.port	80	
		jboss.bisocket.port	4457	
		jboss.jmsControl.port	4458	
SSL		jboss.https.port	443	
		jboss.sslbisocket.port	4459	
		${\rm jboss.ssljmsControl.port}$	4460	

有关详细信息,请参阅 NNMi 9.10 和已知端口。

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),则需要执行某些额外操作。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 它自己。您需要用具有正确证书的全局网络管理功能配置计划使用的 NNMi 管理服务器。 完成第 129 页的将全局网络管理功能配置为使用自签名证书中显示的步骤。

配置全局网络管理以供应用程序故障切换

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 实体标识它自己。如果您计划将应用程序故障切换用于全局网络管理功能,则需要执行某些 额外配置。完成第 131 页的将带有应用程序故障切换的全局网络管理配置为使用自签名证 书中显示的步骤。

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。全局网络管理功能 和早先 NNM 产品中使用的分布式解决方案不同。全局网络管理功能避免轮询由区域系统 管理的节点,因此您不需要关注网络带宽和计算机资源。

请参阅《NNMi 安装指南》、NNMi 发行说明和 NNMi 系统和设备支持列表,以了解有关 安装 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。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 UNIX (HP-UX/Linux/Solaris) 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诊断*和第 248 页的时钟同步。



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切换功能与自签名证书

如果您计划在应用程序故障切换配置中使用带自签名证书的全局网络管理功能,则需要完成某些额外步骤。请参阅第 131 页的将带有应用程序故障切换的全局网络管理配置为使用 自签名证书。

在全局网络管理中使用自签名证书

如果您计划使用带自签名证书的全局网络管理功能,则需要完成某些额外步骤。请参阅第 129页的将全局网络管理功能配置为使用自签名证书。

在全局网络管理中使用证书颁发机构

如果您计划使用带证书颁发机构的全局网络管理功能,则需要完成某些额外步骤。请参阅第 130页的将全局网络管理功能配置为使用证书颁发机构。

列出要监视的关键设备

创建一张要从 global1 监视的 regional1 和 regional2 所管理设备的列表。您将在转 发过滤器 (随后讨论)中使用此信息。您需要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 上的许可证成本。
- 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 需要的网络通 信量。

查看全局和区域管理器的管理域

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 将您的浏览器指向 global1 的 NNMi 控制台。
- 2 登录。
- 3 单击**资产**工作区。
- 4 您可以在此查看 global1 当前监视的已搜索资产。
- 5 将浏览器指向 regional1 的 NNMi 控制台。
- 6 登录。
- 7 单击**资产**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**资产**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 在搜索字段中键入全局网络管理。
- 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

假定您从全局管理器上的 NNMi 控制台选择了区域管理器管理的节点,则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 遵循第 223 页的为全局网络管理配置单点登录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。需要在从全局管理器连接区域管理器之前完成此步骤。有关详细信息,请参阅第 139 页的对 NNMi 使用单点登录。



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,而您没有如第224页的步骤3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,或如第148页的禁用 SSO 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 上编辑以下文件:
 - Windows: %NNM PROPS%\nms-ui.properties
 - UNIX: \$NNM PROPS/nms-ui.properties
- 2 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

3 将初始化字符串的值从 global1 上的 nms-ui.properties 文件复制到 regional1 和 regional2 上的 nms-ui.properties 文件。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。

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。

如果全局和区域管理器存在于同一管理域中,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,请参阅第 148 页的禁用 SSO。

4 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,且 regional2 在 regional2.company3.com 中。修改 global1、 regional1 和 regional2 上 nms-ui.properties 文件的 protectedDomains 部分:

com.hp.nms.ui.sso.protectedDomains=regional1.company1.com, regional2.company2.com, regional3.company3.com

保存更改。

- 5 在 global1、 regional1 和 regional2 上运行以下命令序列:
 - a ovstop ovjboss
 - b ovstart ovjboss

在应用程序故障切换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 应用程序故障切换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过滤器

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,需要在 regional1 和 regional2 上配置转发过滤器。

配置转发过滤器,限制转发的节点

假定要设置节点组,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。

-

	Ø,	N	etwor	k No	de Mo	anage	r									用户:
Γ	文作	牛 初	图	Τ <u>μ</u>	操作	帮助										
h	0	事件管	理				*	节点	组 一 节 点组 >							
þ	А	拓扑图	3				×	2	\star 🖻 😅	6	P	🗙	E	×	K <	3 1 = 11
l	<u>F</u>	正在出	视				¥	R	新建			чт	添			
	Ŷ	疑难解	譗				*					添加	加到			
		资产					¥					到视	过速	ᆉ		
	0	管理樓	迂				*	状态	名称		•	图讨	器	算状	上次修改状态的时间	说明
	6	事件涼	揽				×					護	列表	态		
	¢,	集成樹	快配	5			¥					列	(未 许			
	Je .	配置					*					70	可)			
		📑 j	通信配:	置				0	global1			~	-	~	2011-5-2 22:31:15	
	B	E 🗀 🗄	索					Ø	Microsoft Window	vs 系统		~	-	-	2011-4-28 22:00:54	任何运行
		=	监视配:	置				Ø	Unnumbered Nod	e Group		~	-	~	2011-5-2 20:21:22	
			自定义	论间器	配置			Ø	VMware ESX 主枝	Л		~	~	-	2011-4-28 22:00:54	VMware
	B	i 🗀 🕯	盰					0	VOIPRouters			~	-	~	2011-4-29 4:04:42	
			陷阱转:	发配置				0	非 SNMP 设备			~	-	-	2011-4-28 22:00:54	在搜索证
			自定义	关联配	置			Ø	交换机			~	~	2	2011-4-28 22:00:54	包括进行
		2	伏态配:	茜 …				0	路由器			~	~		2011-4-28 22:00:54	包括进行
		: 🖬	全局网络	络管理 -				0	网络基础设备			~			2011-4-28 22:00:54	包括那些
		1 🛑 F 1 👝 d	1尸界0 5个时	q				0	虚拟机			~	~		2011_4_28 22:00:54	虚拟机
		9 - 1 3 8 - 1 1	< ±1±					0	重要共占						2011 4 28 22:00:54	手車共ら
		، د. د ا	~~ 设备配:	青文件				-	里女卫凤			*	*	-	2011-4-20 22:00:54	里安卫乐
			节点组													

尽管此示例说明如何创建新的节点过滤器,然后用它创建来自 regional1 和 regional2 的转发过滤器,但您可以使用这些现有过滤器中的任何一个来设置从区域 NNMi 管理服务器 到全局 NNMi 管理服务器的转发过滤器。

可创建不包含自己的设备或过滤器的容器节点组;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**设备过滤器**选项卡。键入 global1 作为过滤器名称,在注释字段中添加有关要创建 的过滤器的所需注释。

Metwork Node Manager		用户名: system NNMi角色: 管理
文件\$ 视图 工具 操作 帮助		
 ▲ 事件管理 > 	节点组 〉 节点组 〉 节点组 〉	
▲ 拓扑图 ×	😕 📴 📋 🎦 🖓 保存并关闭 🥩 🗙	删除节点组 📗 🔛
■ 正在监视 ¥	- 甘古	
▲	* 224	设备过滤器 其他过滤器 其他节点 子节点组
▶ 资产 ×	名称 global1	
 管理模式 > 	F 算 1/33 ✓ 状态 无状态	设备过滤器使您能够按设备类别、供应商、系列或设备配置5 去占组成员。如果配置终个设备过滤器,那次节占必须与至2
	添加到视图过滤器列表 🔽	过滤器 and 相匹配,并通过属于该节点组的任意附加过滤器。
	说明	
▶ 配置 ☆	Pass Procurve swithches to global1	
	可住田边名过近路 甘油过远路 甘油共正的	12 Q 0-0行, 英0行 🛛 🤤
	可使用设备过滤器、其他过滤器、其他节点和子节点组来过滤节点组。如果使用设备过滤器	设备类别 ▲ 设备供应商 设备系列
□ □ 12.5	和其他过滤器,那么节点必须与至少一个设备 过滤器及其他过滤器规范匹配才能属于该节点	
□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	组。指定为其他节点和子节点组的节点 <i>始终</i> 是 该节点组的成员。违策问"帮助",使用节点组	
	表单"。	
▶ 路阱转发配罢	要测试节点组定义,请选择"文件 → 保存",然	
□ 白完义关联翻署	后选择"操作 → 节点组详细信息 → 显示成 员"。	
□ 1/10月111	▼ NNM iSPI性能	
□ 土吗~~河石 巨坯…	供 NNM iSPI Performance for Metrics 和 NNM iSPI for Traffic 使用。	
	漆加到过滤器列表	
🕅 设备配置文件		
■ 节点组		
■ 接口组		
III RAMS 服务器		日本 おお しん
	分析 - 摘要 - 未选择对象	

4 单击新建图标以打开节点设备过滤器表单。



- 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。

文件 视图 工具	操作 帮助
节点设备过滤器 * 🔪	
🦻 🗎 🎦 🖓 保	存并关闭 🧭 💥 删除节点设备过滤器 🗎 🔛
① 只有在保存顶层	表单后才会提交更改!
-	
设备类别	☆ 協和 略 由 哭 →
现象供应案	
() 面供() 2 例	newiett-Packard V
设备系列	HP ProCurve 3500 Fixed-port Switch 💌
设备配置文件	
	· ● 快速查找…
	1 1177

7 查找并选择 HP Procurve 3500yl 交换机的配置文件;然后单击确定。

设备型号 ▲	SNMP 对象 ID	OUI	设备系列	设备供应商
npProCurve3448	.1.3.6.1.4.1.11.2.3.7.11.43		HP ProCurve 3400	😡 Hewlett-Pa
pProCurve3500-24	.1.3.6.1.4.1.11.2.3.7.11.111		BIN HP ProCurve 3500	Hewlett-Pa
npProCurve3500-24-Pot	.1.3.6.1.4.1.11.2.3.7.11.109		BID HP ProCurve 3500	Hewlett-Pa
npProCurve3500-48	.1.3.6.1.4.1.11.2.3.7.11.112		BID HP ProCurve 3500	Hewlett-Pa
npProCurve3500-48-Pot	.1.3.6.1.4.1.11.2.3.7.11.110		BIN HP ProCurve 3500	Hewlett-Pa
npProCurve3500yl	.1.3.6.1.4.1.11.2.3.7.11.114		3500 HP ProCurve 3500	Hewlett-Pa
pProCurve3500yl-48G	.1.3.6.1.4.1.11.2.3.7.11.59		BS00 HP ProCurve 3500	Hewlett-Pa
hpProCurve3500yI-PWR	.1.3.6.1.4.1.11.2.3.7.11.58		3500 HP ProCurve 3500	Hewlett-P
npProCurve4104gl	.1.3.6.1.4.1.11.2.3.7.11.27		HP ProCurve 4100	Hewlett-P
hpProCurve4108gl	.1.3.6.1.4.1.11.2.3.7.11.23		HP ProCurve 4100	Hewlett-P
hpProCurve4202vI-48G	.1.3.6.1.4.1.11.2.3.7.11.56		HP ProCurve 4200	Hewlett-P
npProCurve4202vI-68	.1.3.6.1.4.1.11.2.3.7.11.71		HP ProCurve 4200	Hewlett-P
npProCurve4202vI-68G	.1.3.6.1.4.1.11.2.3.7.11.70		HP ProCurve 4200	🕅 Hewlett-P
hpProCurve4202vI-72	.1.3.6.1.4.1.11.2.3.7.11.57		HP ProCurve 4200	Hewlett-P
hpProCurve4204vI	.1.3.6.1.4.1.11.2.3.7.11.52		HP ProCurve 4200	Hewlett-P
hpProCurve4208vI	.1.3.6.1.4.1.11.2.3.7.11.53		HP ProCurve 4200	Hewlett-P
npProCurve5304xI	.1.3.6.1.4.1.11.2.3.7.11.20		Bin HP ProCurve 5300	Hewlett-P
			107	

8 单击保存并关闭两次。

节点设备过滤器・ ■ ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
 □ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○
 ① 只有在保存顶层表单后才会提交更改!
设备类别 交换机-路由器 ◄
设备供应商 Hewlett-Packard 👻
设备系列 HP ProCurve 3500 Fixed-port Switch 👻
设备配置文件 hpProCurve3500y1-48G V

9 要测试此过滤器,请选择 global1。

10 在下拉菜单中单击显示成员。

	🕼 Network N	ode Manage	r									用户名: s
	文件 视图 工具 ● 事件管理 ▲ 拓扑图 ● 正在监视 ④ 好雜留答	操作 帮助 ☆ 映射 节点组详新	→ 暗息 → ~		2 显示成员 显示所有事件 显示所有未决事件 状态详细信息	 ₫	ý	× 添ね	E 添加	×	0)1-11行
	 法本(新日 資产 管理模式 事件浏览 集成模块配置 保置 		* * * * *	状态	名称		•	加到视图过滤器列表	到过滤器列表床许可	计算状态	上次修改状态的时间	说明
	📑 通信配置…			Ø	global1			~	-	v	2011-5-2 22:31:15	
	🗉 🗀 搜索			Ø	Microsoft Windows 系统	充		~	-	-	2011-4-28 22:00:54	任何运行 Mic
	📔 监视配置…			Ø	Unnumbered Node Grou	ıp		~	-	~	2011-5-2 20:21:22	
	📑 自定义轮询器	器配置		Ø	VMware ESX 主机			~	•	÷	2011-4-28 22:00:54	VMware ESX
1	and an and an and a set of a s											

11 注意, NNMi 已搜索 1 个 HP 3500yl 交换机。这表明您创建的过滤器正在查找您配置为 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过滤器来配置转发过滤器。

Node Groups > Nodes >	>		
🔁 🖾 😂 🥝	ሮ 🦻 🗙 🖾	global1 🚽 📕 🖣	1
Sta Dev Name 🔺	Hostnam I System Location	Device Profile	
🛇 🏰 wansw-1	wansw-1. 10 5 upper east compu	hpProCurve3500yl-480	;

12 从 NNMi 控制台中 regional1 的配置工作区单击全局网络管理。

🍈 Network Node Manage	r
文件 视图 工具 操作 帮助	
♦ 事件管理	×
▲ 拓扑图	×
🔄 正在监视	×
④ 疑难解答	×
资产	×
📀 管理模式	×
🇞 事件浏览	¥
🗳 集成模块配置	×
▶ 配置	*
📑 通信配置	-
∃ 🗀 搜索	
📑 监视配置	
📑 自定义轮询器配置	
速 🧰 事件	
📑 陷阱转发配置	
📑 自定义关联配置…	
📑 状态配置	
▲ 全局网络管理	
🗉 🗀 用户界面	
🗷 🗀 安全性	
📧 🧰 MIB	
📅 设备配置文件	
■ 节点组	
■ 接口组	

13 单击**转发过滤器**选项卡。

文件 视图 工具 操作 帮助 全局网络管理	
 □ □ □ ○ ○	转发过滤器 产点的过滤器
警告:全局网络管理环境中涉及的所有 NNMI 管理服务器 (区域管理器和全局管理器)的系统时钟必须同步。有关详 细信息,请单击 此处 。	可选。将节点组指定为过滤器,该过滤器用于将节点对象数据从该 NNMI管理服务器(区域 管理器)转发到所有已配置为接收来自该区域管理器的节点对象数据的远程 NNMI管理服务 器(全局管理器)。 如果未配置节点组,那么会将所有节点对象数据转发到已连接的全局管理器。
	节点组

14 单击**快速查找**。

文件	视图	工具	操作	帮助
~ 1	DOPPH	122	126115	111 243

全局网络管理 I尋 🖺 🔄 保存并关闭 🥩 🔛		
★ 关于此表单的信息,请参阅"帮助→使用全局网络管理 题写主单"。	转发过滤器 区域管理器连接▼ 节点组过滤器	
警告:全局网络管理环境中涉及的所有 NNMI 管理服务器 (区域管理器和全局管理器)的系统时钟必须同步。有 关详细信息,请单击 此处 。	可选。将节点组指定为过滤器,该过滤器用于将节点对象数据从该NNMI管理服务器 (区域管理器)转发到所有已配置为接收来自该区域管理器的节点对象数据的远程 NNMI管理服务器(全局管理器)。 如果未配置节点组,那么会将所有节点对象数据转发到已连接的全局管理器。	
	市点組	
	▲ 快速查找 ■ 11.#	>

15 选择 global1 过滤器; 然后单击确定。

速查找				
名称				-
global1				
- Microsoft Windows 系统				
Unnumbered Node Group				
VMware ESX 主机				
VOIPRouters				
非 SNMP 设备				
交换机				
路由器				
网络基础设备				
				
重要节点				
更新时间: 11-5-2 10:32:13 下午 CST	总计: 11	选定: 1	过滤器:关闭	自动刷新:关闭

16 单击保存并关闭。

视图 工具 操作 帮助 网络管理 11 图 保存并关闭 32 日 12			
此表单的信息,请参阅"帮助 → 使用全局网络管理 来单"。	转发过滤器 区域管理器连接 ▼节点组过滤器		
20年 。 : 全局の络管理环境中涉及的所有 NNM 管理服务器 过管理器和全局管理器 〉的系统时钟必须同步。有 细信息,请单击此处。	可选。将节点组指定为过滤器,该过滤器用于将节点对象数据从该 NNMI 管理服务器 (区域管理器)转发到所有已配置为接收未自该区域管理器的节点对象数据的远程 NNMI 管理服务器(全局管理器)。 如果未配置节点组,那么会将所有节点对象数据转发到已连接的全局管理器。		
	节点组 🔹 🖬 🗸		

这样就完成了在 regional1 上设置转发过滤器的任务。对 regional2 完成步骤 1 到步骤 16 之后,转到下一部分,将 global1 连接到 regional1 和 regional2。

用区域管理器连接全局管理器

如前面提到的, 假定 regional1 和 regional2 都管理几个常用交换机。假定您希望将这些常用交换机信息从 regional1 转发到 global1。



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 还会忽略有关它从 regional2 接收的这些常用交换机的信息。

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 如前所述,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 中的*时钟 同步问题*。

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 global1 NNMi 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 ╆ 图标创建新的区域管理器。

文件 视图 工具 操作 帮助	
全局网络管理	
😼 📔 🔄 保存并关闭 🛛 🎜 🗎 🔛	
-	转发过滤器
关于此表单的信息,请参阅"帮助 → 使用全局网络管理配置 素单"。	▼
表手。 警告:全局网络管理环境中涉及的所有 NNMi 管理服务器 (区域管理器和全局管理器)的系统时钟必须同步。有关详 细信息,请单击 此处 。	创建区域管理器连接后,该 NNM 管理服务器(全局管理器)接收到其他 NNM 管理服务器 (区域管理器)的所有节点对象数据的副体。考虑登录到区域管理器并配置转发过滤器以限 制该区域管理器为所有已连接的全局管理器提供的节点对象数据里。
	- 図 * 2 2 3 v × 新建 ◎ ◇ 0 - 0 行, 共 0 行 ◎ ◇ 回 名称 注接状态 UUID 描述

- d 添加 regional1 的名称和描述信息。
- e 单击**连接**选项卡。
- f 单击 \star 图标。



g 添加 regional1 的连接信息

有关在该表单中要创建的条目的特定信息,请参阅 NNMi 帮助中的**帮助 -> 使用区域管理器** 连接表单

文件 视图 工具 操作	帮助
区域管理器连接 * 🔪	
☞ 📔 🎦 🔄 保存并关	闭 🛛 🥩 🗶 刪除区域管理器连接 🛛 🔛
(1) 只有在保存顶层表单后	白才会提交更改!
▼ 提供完全限定域名作为远程区 名。有关详细信息,请参阅\$ 接表单"。	区域管理器服务器的主机。 帮助→使用区域管理器连
主机名	regional1. example. hp. co
使用加密	
HTTP(S) 端口	80
用户名	system
用户密码	
排序	20

- h 单击**保存并关闭**两次以保存您的工作。
- 3 完成第 235 页的步骤 g 到第 233 页的步骤 a, 建立从 global1 到 regional2 的连接。

确定从 global1 到 regional1 和 regional2 的连接状态

要检查从 global1 到 regional1 和 regional2 的连接状态,请完成以下步骤:

1 从 global1 NNMi 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 的连接状态,检查它们的状态。注意,连接状态显示为已连接,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态。

NNMi 完成一次有效搜索之后再继续下一部分。有关详细信息,请参阅《NNMi 安装指南》中的检查搜索进度。

查看 global1 资产

NNMi 完成一次有效搜索之后再完成这一部分。有关详细信息,请参阅《NNMi 安装指南》中的检查搜索进度。

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,导航到位于资产工作区中的管理服务器的节点表单。

Metwork Node Manage	er
文件 视图 工具 操作 帮助	
♦ 事件管理	*
▲ 拓扑图	*
🔤 正在監視	*
▲ 反差解答	*
● 資产	*
*	^
■ 端口	
■ 节点组件	
32 ,742	
□□ 管理服务器的市点	
	Ξ
MID VIE	
™ 下儿乐組	×
管理模式	*
🌔 事件浏览	*
🗳 集成模块配置	*
▶ 配量	*

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,资产看上去可能如下:

Metwork Node Manager			用户名: system	NNMi 角色: 管
文件 视图 工具 操作 帮助				
♦ 事件管理	×	管理服务器的节点		
本 拓扑图	×	🖉 📴 🖉 🗟 🔊 🖓 🗶 🔛		
🕎 正在整視	×	regional1 ▼)<设置节点组进	行,共 59 行	\diamond
⚠️ 髮走鲜答	≈	おま 没え 名称 ・ こ选定 regional1	1 程户	系统位置
₤ 養产	*	Procurve1 16.78.56.99	默认租户	SU E CPU RM
		C **** access-server access-server 16.78.56.102	默认租户	5 upper east
■ 項口			默认租户	5 upper east
🏛 第 2 层连接		◎ 弭 c2900sv (其信息从 regional1	认租户	6 Annex Nor
🧰 管理服务器的节点		○ 珥 c2900xl-1 传递到 global1)	默认租户	CO:HPOVCu
🕮 自定义节点		C2950-i1 c2950-i1.fc.ust 16.78.56.105	默认和户	5u computer
🗰 自定义接口 📃		■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	亩:0 试滤器:3	平启 白助
🏧 自定义的 IP 地址		分析		
■ MIB 变量				
····· ··· ·		70 关 😜		
◎ 管理模式	*	未选择对象		
🇞 事件浏览	岽			
🗳 集成模块配置	*			

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 的设备资产。

断开 global1 和 regional1 之间的通信连接

假定您计划永久关闭 global1 或关闭很多天。对此示例,假定 global1 仍然有 regional1 的活动订购。您需要完成某些额外步骤来完成关闭:

1 从 global1 NNMi 控制台单击配置工作区中的全局网络管理。

🧑 Network Node Ma	nager
文件♥ 视图 工具 操作	帮助
♦ 事件管理	*
▲ 拓扑图	*
🛃 正在监视	×
4 疑难解答	×
£ 资产	×
📀 管理模式	*
🇞 事件浏览	*
🗳 集成模块配置	*
▶ 配置	*
📑 诵信配贵	
Image: Imag	
➡ 监视配置…	
📑 自定义轮询器配置…	
📑 陷阱转发配置	
📑 自定义关联配置…	
➡ 状态配置	
■ 全局网络管理	
I □ 用户界面	
📧 🗀 安全性	
🗀 MIB	
🥅 设备配置文件	
☶ 节点组	
ⅲ 接口组	
📅 RAMS 服务器	
	•

2 单击区域管理器连接。

文件 视图 工具 操作 帮助



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 理问题故障诊断* 主题的信息来诊断问题,然后再继续。

文件 视图 工具 操作 帮助 全局网络管理 11日 留 11日 保存并关闭 22 11日	
▼ 关于此素单的信息,请参阅"帮助 → 使用全局网络管理 配置表单"。 警告:全局网络管理环境中涉及的所有 NNM 管理服务 器(区域管理器和全局管理器)的系统时钟必须同步。 有关详细信息,请单击此处。	 接发过滤器 区域管理器连接

4 选择 regional1, 然后单击打开图标。

又件 视图 工具 操作 帮助	
全局网络管理	
🦻 📋 🔄 保存并关闭 🛛 😂 🛛 🔛	
 关于此表单的信息,请参阅帮助→使用全局网络管理配置表单*。 警告:全局网络管理环境中涉及的所有 NNMI 管理服务器 (区域管理器和全局管理器)的系统时钟必须同步。有关详细信息,请单击此处。 	技友过速器 区域管理器连接 ● 创建区域管理器连接后,该 NMM 管理服务器(全局管理器)接收到其他 NMM 管理服务器(区域管理器)的所有节点对象数据的副本。考虑登录到区域管理器并配置转发过滤器以限制该区域管理器为所有已连接的全局管理器提供的节点对象数据量。 ▼ ● ● ● <td< th=""></td<>

5 单击连接,选择 regional1.x.y.z,然后单击删除图标。

文件 视图 工具 操作 帮助 全局网络管理 区域管理器*	
🥪 💾 🎦 🔄 保存并关闭 🥭 🗙 删除区域管理器 🗧	
 ◆基本 名称 regional1 连接状态 UUID 描述 	连接 配置与该区域 NNMI管理服务器的 HTTP 或 HTTPS 通信。 *
	F I 1 regional1 - 80 system

- 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 再次单击保存并关闭。
- 9 在 global1 上的命令行中键入以下命令:

nnmnodedelete.ovpl -rm regional1 -u *NNMi 管理员用户名* -p *NNMi 管理* 员密码

- 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。

文件 视图 工具 操作 帮助				
全局网络管理				
😼 🛅 🔄 保存并关闭 🥩 🔛				
•	转发过滤器 区域管理器连接			
关于此表单的信息,请参阅"帮助 → 使用全局网络管理配置 素单"。	•			
警告: 全局网络管理环境中涉及的所有 NNMI 管理服务器 (区域管理器和全局管理器)的系统时钟必须同步。有关详 细信息,请单击此处。	创建区域管理器连接后,该 NNMI管理服务器(全局管理器)接收到其他 NNMI管理服务器 (区域管理器)的所有节点对象数据的副本。考虑管录到区域管理器并配置转发过滤器以 限制该区域管理器为所有已连接的全局管理器提供的节点对象数据里。			
▼ 図 * 図 の の (本) (+)<				
	名称			
	regional1 已连接 ff1b-160f-feb3-43e8-9335-a017t			
	nmcvm02 未连接 ec150190-410c-47b3-b847-b32			

- e 单击**保存并关闭**以保存删除。
- **12** 对其他连接到 global1 的区域 **NNM**i 管理服务器 (如 regional2),完成步骤 **11** 到 步骤 **1**。

更多信息

搜索和数据同步

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,以及搜索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它。



为维护一致性,当 regional1 和 regional2 搜索设备状态更改时,它们会持续更新 global1,从而使全局和区域服务器上保持相同的节点状态。

任何时候,当 global1 请求 regional1 或 regional2 所管理节点的信息时, regional1 或 regional2 都用请求到的信息响应 global1。global1 不会与节点直接对话。global1 执行搜索操作时,不会有对设备的重复 snmp 查询。

每次 regional1 或 regional2 完成搜索时,global1 都与 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 搜索之间变化会很大,尤其是有多个区域服务器连接到全局服务器时。



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搜索间隔都可调整,并可能导致 globall 和区域管理器之间存在 搜索准确性差异。重新搜索间隔越短,搜索就越准确,而 NNMi 产生的网络通信量也越大。 重新搜索间隔越长,搜索就越不准确,而 NNMi 产生的网络通信量也越少。这意味着您的网 络规模增长越大,可能所需的重新搜索频率就越低。要设置重新搜索间隔,请执行以下步骤

从 global1 或 regional2 NNMi 控制台的配置工作区中单击搜索配置。

🧑 Network Node Manager	
文件 视图 工具 操作 帮助	
♦ 事件管理	*
本 拓扑图	≈
🕎 正在监视	×
全 疑难解答	×
资产	×
📀 管理模式	×
🇞 事件浏览	≈
💞 集成模块配置	≈
▶ 配置	*
 ≧ 通信電置 ② 搜索配置 ☑ 搜索配置 ☑ 批求配置 ☑ 出观配置 ☑ 自定义轮询器配置 ☑ 事件 ☑ 陷阱转发配置 ☑ 自定义关联配置 ☑ 自定义关联配置 ☑ 自定义关联配置 ☑ 自定义关联函置 ☑ 目定义系联面置 ☑ 自定义系联面置 	<u> </u>
 → 二 → → → → → → → → → → → → → → → → → →	-

13 根据所需的区域服务器启动搜索的频率,调整重新搜索间隔。全局服务器将在区域服务器完成搜索之后立即启动搜索。

文件 视图 工具 操	作和助
搜索配置*	
😼 📔 🕙 保存并关闭	🞜 🖴
▼ 全局控制	
重新搜索间隔 1	
删除无响应节点控制	
NNMi将在指定的"无响应"元 表示不删除无响应节点。7	天数之后从 NNMi 数据库删除节点。零 (0) 有关详细信息,请单击 <mark>此处</mark> 。
删除无响应节点的周期 (以天为单位)	
螺旋搜索 Ping 扫描控制	(仅 IPv4)
此控件可以覆盖所有自动	搜索规则的"启用 Ping 扫描"选项。
Ping 扫描	无 👻
扫描间隔 1	00 天 👻
节点名称解析	
第一选择	DNS 简称 🚽
第二选择	DNS 简称 🚽
第三选择	ℙ地址 ▼

14 单击保存并关闭。

设备的状态轮询或配置轮询

假定区域 NNMi 管理服务器 regional2 搜索并管理节点 X, 全局 NNMi 管理服务器 global1 与区域 NNMi 管理服务器 regional2 连接。

图 16 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 的资产工作区中单击节点。
- 2 从节点资产中选择节点 X。
- 3 使用操作 > 轮询 > 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。 您总会看到相同的状态轮询结果。

如果希望 global1 具有节点 X 的最新搜索信息,请执行以下操作从 global1 对节点 X 进行配置轮询。

- 1 从 global1 的资产工作区中单击节点。
- 2 从节点资产中选择节点 X。
- 3 使用操作 > 轮询 > 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。 您总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 的状态更改,并在其本地数据库中更新状态。

NNMi 管理服务器的 regional1 和 regional2 上的 NNMi StatePoller 服务计算它 监视的设备的状态值。global1 从 regional1 和 regional2 接收状态值更新。global1 轮询它搜索的节点,而不轮询由 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 上使用转发过滤器,因为过滤可能影响 global1 上的连通性。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过滤器,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总结。

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切换

您可以将全局和区域管理器配置为使用应用程序故障切换。全局或区域管理器自动检测并连接到活动系统。

在全局管理器上配置应用程序故障切换

要配置 global1, 让它识别应用程序故障切换,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。

🧑 Network Node Manager
文件 视图 工具 操作 帮助
♦ 事件管理 🛛 🕹 🕹
▲ 拓扑图 ×
🔄 正在监视 🛛 😵
登 建难解答 举
资产 *
管理模式 *
🇞 事件浏览 🛛 🕹 😵
🗳 集成模块配置 🛛 🛛 🖇
▶ 配置 ☆
📑 通信配置
📑 监视配置
📑 自定义轮询器配置
🖅 🧰 事件
📑 陷阱转发配置
📑 自定义关联配置
📑 状态配置
🗷 🗀 安全性
📧 🧰 MIB
■ 设备配置文件
■ 节点组
□ 接口组
IIII RAMS 服务器

假定您为 regional1 配置了应用程序故障切换,并将 regional1_backup 配置为辅助服务器。

2 单击区域管理器连接。

3 选择 regional1, 然后单击**打开**图标。

文件视图。工具操作一帮助 全局网络管理。	
■ ● 常体行升天闭 ● ■ ■ ● ******************************	 转发过滤器 区域管理器连接 ● 创建区域管理器连接后,该 NMM 管理服务器(全局管理器) 接收到其他 NMM 管理服务器 (区域管理器) 的所有节点对象数据的副本。考虑登录到区域管理器并配置转发过滤器以限制该区域管理器为所有已连接的全局管理器提供的节点对象数据里。
제(h心, hit-에)()에 ~	
	名称 住後れ念 0000 搁还 regional1 已连接 ff1b-160f-feb3-43e8-9335-a017t 1000000000000000000000000000000000000

4 单击**新建**图标。

文件 视图 工具 操作 帮助	
全局网络管理 区域管理器*	
😼 📔 🎦 🖓 保存并关闭 🛛 🥩 🗙 删除区域管理器 🛛 🔛	
▼基本	连接
名称	•
连接状态	配置与该区域 NNMI管理服务器的 HTTP或 HTTPS通信。
UUID 描述	* 😫 😂 🗙 🔯 🕸 1 - 1 行, 共 1 行 🗇 🔕 🖂
	· · · · · · · · · · · · · · · · · · ·
	デー 密 L
	2 regional1 - 80 system

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。

文件	视图	工具	操作	帮助						
区域管	管理器道	接* 〉								
9	8	3 🛛 保	存并关闭	Ð 🞜	×	删除[≤掝管	理器	连接	
G) 只有7	在保存顶原	■ 表単后:	才会提交	更改	!				
-										
▼提供	完全限的	定域名作》	5.111111111111111111111111111111111111	域管理器	服务	器的主	机名	。有法	关详细	Đ
▼ 提供 信息	完全限9 ,请参问	定域名作; 剤"帮助 →	わ远程区) 使用区5	域管理器 或管理器	服务 连接:	-器的主 表单"。	机名	。有氵	关详纲	Ð
▼ 提供 信息	完全限9 ,请参问	定域名作; 剣"帮助 →	わ远程区) 使用区5	城管理器	漏务 连接:	·器的主 表单"。	机名	。有法	关详维	Ð
▼ 提供信息 主相	完全限 ,请参问 1名	定域名作; 阅"帮助 →	わ远程区) ・使用区!		服务 连接 iona	·器的主 表单"。 11. ba	机名 skup.	。有注 x. y. z	关详组	8
▼ 提信息 主使 T	完全限行 ,请参问 1名 助密	定域名作; 剤"帮助 →	内远程区) ●使用区5		服务 连接 iona	·器的主 表单"。 111. ba	机名 skup.	。有ź	关详纳 ;	=
▼ 提信 主使用 HTT	完全限 ,请参 礼名 加密 P(S)端[定域名作; 剣"帮助 ⊣	内远程区! ・使用区!		漏务 连接: iona	·器的主 表单**。	机名 ckup.	。有ź	关详细	#
▼ 提信 主使 HTT 用 F	完全限 , 请参 し名 別加密 P(S) 端[P名	定域名作; 剤*帮助 →	対远程区 ・使用区5		服务 连接 iona	-器的主 表单"。 11. ba	机名 skup.	。有ź	关详\$	
▼ 提信 主使HTT 用 ー	完全限 ,请参 加密 P(S)端 P 名	定域名作; 剤"帮助 →	内远程区! • 使用区!		服务 连接 ions	·器的主 表单"。 11. ba	机名	。有: x. y. z	关详纲 	∎
▼ 提信 主使HTT 用 戸	完全限》 ,请参 1名 加密 P(S)端 P(S)端 P(S)端 P(S)端 P(S)端 P(S)端 P(S) · 名	定域名作; 剤"帮助 →	勺远程区! → 使用区!		服务 连接 sions	器的主 表单 。	:机名	。有ź		₽
▼ 提信 主使HTT 用 月	完全限参 , する 加密 P(S)端 ロ マ名 マ 密 码	定域名作 剤 [®] 帮助 → コ	勺远程区; ↓ 使用区;			器的主 表单 [*] 。。	·机名	。有 x. y. z	关详组	

6 单击保存并关闭三次以保存您的工作。

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诊断提示

NNMi 帮助中的故障诊断信息

有关全局网络管理故障诊断的信息,请参阅 NNMi 帮助中的 全局网络管理故障诊断 主题。

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 UNIX (HP-UX/Linux/Solaris) 的工具 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 未连接到区域管理器。请参阅"帮助?系统信息,全局网络管理"。

检查全局管理器上的 nnm.0.0.log 文件中的以下消息:

警告:未连接到系统 <服务器名称>,原因是时钟相差 <秒数>。远程时间是 <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:未连接到系统 <服务器名称>,原因是时钟相差 <秒数>。远程时间是 <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 未连接到区域管理器。请参阅"帮助 ? 系统信息, 全局网络管理"。

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搜索

假定您注意到 global1 和 regional2 之间的信息不一致。为解决这个问题,请从 global1 运行 nnmnoderediscover.ovpl 脚本,使 global1 和 regional2 同步。该操作还会使 regional2 用任何新搜索的结果更新 global1。

考虑在第 244 页的图 16 中显示的网络。假定您希望 regional2 将其整组节点(即节 点 X、Y 和 Z)与 global1 同步。运行以下命令以将节点 X、Y 和 Z 与 global1 同 步: nnmnoderediscover.ovpl -u *用户名* -p 密码 -rm regional2。有关详细 信息,请参阅 nnmnoderediscover.ovpl 参考页或 UNIX 联机帮助页。

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 服务中断达较长一段时间,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 上启动新搜索。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,则您需要提交支持呼叫,使用 nnmsubscription.ovpl 脚本从 regional1 和 regional2 数据库清除旧的 global1 数据。

从 NNMi 9.0x 升级到 NNMi 9.10

全局网络管理支持的 NNMi 版本

如果全局管理器与运行 NNMi 9.0x 补丁 2 或更早版本的区域管理器相连,则全局和区域管 理器之间的 SNMP 查询无法正常运行。要对此进行补救,请将区域管理器升级到 NNMi 9.0x 补丁 3 或更高版本。要获得最佳结果,全局管理器与区域管理器应使用相同的版本和 NNMi 补丁级别。HP 支持 NNMi 9.10 全局管理器与 NNMi 9.0x 区域管理器相连。

全局网络管理升级步骤

要升级全局网络管理环境中配置的 NNMi 管理服务器,请按以下顺序升级 NNMi 管理服务器:

- 1 将全局管理器从 NNMi 9.0x 升级到 NNMi 9.10。
- 2 将区域管理器从 NNMi 9.0x 升级到 NNMi 9.10。

在您完成升级过程中,全局网络管理功能会继续工作,但某些新 NNMi 9.10 功能可能要等 到在区域 NNMi 管理服务器上完成升级后,才能在全局 NNMi 管理服务器上正常运行。

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,你可以将某些 NNM iSPI 只部署在 regional1 上、或只部署在 global1,也可以部署在 regional 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。

配置 NNMi Advanced 的 IPv6 功能

必须购买并安装 NNMi Advanced 许可证,才能使用 IPv6 管理功能。本章中所指的 NNMi 是指安装了 NNMi Advanced 许可证的 NNMi。

NNMi 中的 IPv6 管理启用对 IPv6 地址 (包括其接口、节点和子网)的搜索和监视。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
- 先决条件
- 许可
- 受支持配置
- 安装 NNMi
- 激活 IPv6 功能
- 取消激活 IPv6 功能

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 资产搜索
 - 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:
 - 节点搜索
 - 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搜索播种
- 使用 IPv6 第3 层邻居搜索提示进行自动 IPv6 设备搜索
- 使用第2层邻居搜索提示(LLDP(链路层搜索协议)IPv6邻居信息)进行自动 IPv6 设备搜索
- IPv4 和 IPv6 信息的合并显示
 - 节点、接口、地址、子网和关联的资产视图
 - 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、总结和根源分析
- 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
 - 搜索配置
 - 监视配置
 - 节点组和接口组
 - 事件配置
- 对 IPv6 资产和事件的 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 子网连接的搜索
- 将 IPv6 Ping 扫描用于搜索
- 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 链路本地地址作为搜索种子
先决条件

请查看《NNMi 部署参考》、NNMi 发行说明和NNMi 系统和设备支持列表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。

Windows 操作系统上不支持 IPv6。请参阅 NNMi 系统和设备支持列表中有关 IPv6 的受支持操作系统的信息。下面列出其他要求:

- 必须在至少一个网络接口上启用并配置 IPv4。
- 必须启用 IPv6,并且在连接到需要管理的 IPv6 网络的至少一个网络接口上配置全局 单播地址。
- 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 进行搜索和监视的任何设备进行通信。

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 无法搜索"仅 IPv6"设 备,无法使用 IPv6 种子和提示进行搜索,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

如前面所提到的,您必须购买并安装 NNMi Advanced 许可证,才能使用 IPv6 管理功能。 有关获取和安装 NNMi Advanced 许可证的信息,请参阅第 115 页的许可 NNMi。

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。

受支持配置

有关 NNMi 的受支持操作系统配置的更多信息,请参阅 NNMi 系统和设备支持列表。

管理服务器

下表显示"仅 IPv4"和双堆栈 NNMi 管理服务器的功能。

衣 20 官理服务 奋功能		
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 种子的搜索	受支持	受支持
使用 IPv6 种子的搜索	不受支持	受支持
IPv4 地址和子网资产	受支持	受支持
IPv6 地址和子网资产	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
仅 IPv6 被管节点	不受支持	受支持
使用 IPv6 种子的搜索	不受支持	受支持
IPv6 地址和子网资产	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 种子的节点搜索	受支持	受支持
使用 IPv4 种子的节点搜索	受支持	受支持

表 20 管理服务器功能

表 20 管理服务器功能 (续)		
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 地址和子网资产	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,安装脚本包括 IPv6 功能;但是,必须手动启用这些 IPv6 功能。首先,必须购买并应用 NNMi Advanced 许可证,才能启用 IPv6 功能。然后必须手动配置 IPv6 以使之运行,方法是编辑 nms-jboss.properties 文件。

激活 IPv6 功能

需要 IPv6 通信的功能 (例如 "仅 IPv6" 设备的搜索以及 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。

下面所示的过程说明了如何通过执行以下操作来启用 IPv6 功能:

- 安装 NNMi Advanced 许可证
- 启用 nms-jboss.properties 文件中的 IPv6 主交换机

继续操作之前,请查看并验证前面部分所述的所有先决条件。

- 1 使用 NNMi 附带的临时瞬时启动许可证,或安装 NNMi Advanced 许可证。有关获取 和安装 NNMi 许可证的信息,请参阅第 115 页的许可 NNMi。基本 NNMi 许可证不提 供 IPv6 功能。
- 2 编辑 nms-jboss.properties 文件。查看以下位置:
 - UNIX: \$NNM_PROPS/nms-jboss.properties

3 找到以 # Enable NNMi IPv6 Management 开头的文本。

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。

a 要在 NNMi 中启用 IPv6 通信,请取消注释以下属性:

java.net.preferIPv4Stack=false

要取消注释属性,请删除行开头的#!字符。

b 要在 NNMi 中启用总体 IPv6 管理,请取消注释以下属性:

com.hp.nnm.enableIPv6Mgmt=true

- c 保存并关闭 nms-jboss.properties 文件。
- 4 (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 在 IP 版本首选项字段中选择 IPv4、 IPv6 或任何。
 - c 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。
- 6 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: <Process ID #>

_

last message: Initialization complete.

exit status:

additional info:

SERVICE	STATUS
CommunicationModelService	Service is started
CommunicationParametersStatsServ	ice Service is started
EventsCustomExportService	Service is started
ExtensionDeployer	Service is started
IslandSpotterService	Service is started
KeyManager	Service is started
ManagedNodeLicenseManager	Service is started
ModelChangeNotificationAdapter	Service is started

MonitoringSettingsService	Service is started
NMSLogManager	Service is started
NamedPoll	Service is started
NetworkApplication	Service is started
NmsApa	Service is started
NmsDisco	Service is started
NmsEvents	Service is started
NmsEventsConfiguration	Service is started
NmsExtensionNotificationService	Service is started
NmsModel	Service is started
NmsWorkManager	Service is started
NnmTrapService	Service is started
RbaConfig	Service is started
RbaManager	Service is started
SpmdjbossStart	Service is started
StagedIcmp	Service is started
StagedSnmp	Service is started
StatePoller	Service is started
TrustManager	Service is started

7 启用 IPv6 之后, NNMi 视图将立即包含新搜索节点的 IPv6 资产。在下一个搜索周期 中, NNMi 视图显示与以前所搜索节点关联的 IPv6 资产。

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 > 轮 询 > 配置轮询命令。还可以使用 nnmnoderediscover.ovpl 脚本将节点添加到 NNMi 搜索 队列。有关详细信息,请参阅 nnmnoderediscover.ovpl 参考页或 UNIX 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。

取消激活 IPv6 功能

可以使用以下某个方法以管理方式禁用 IPv6 功能:

- 1 关闭 nms-jboss.properties 文件中的 IPv6 主交换机, 然后重新启动 NNMi。
- 2 使 NNMi Advanced 许可证过期,或用基本 NNMi 许可证替换它。

有关更改 NNMi 许可证的信息,请参阅第 115 页的许可 NNMi。

以下部分描述禁用 IPv6 之后的 NNMi 行为和资产清理。

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 地址状态设置为未轮询。如果选择地址,然后使用此地址的操作 > 配置详细信息 > 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 资产

一旦 NNMi 完整搜索了 IPv6 资产,在以下场景中您即可使 NNMi 能够自动清理它:

• 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 资产。NNMi在下一个搜索周期中针对 SNMP 节点删除 IPv6 资产。 NNMi 不删除非 SNMP IPv6 节点。需要从 NNMi 资产手动删除 IPv6 节点。

• NNMi Advanced 许可证过期或某用户删除了许可证。 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搜索的节点。

NNMi 立即从其资产删除所有非 SNMP IPv6 节点。 NNMi 重新搜索所有 SNMP 节 点,并删除所有 IPv6 数据。

NNMi Advanced 许可证过期或某用户删除许可证。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搜索的节点。NNMi 立即删除所有非SNMP IPv6 节点。许可服务将超过许可资产容量的 SNMP 节点标记为非被管状态。NNMi 从管理 SNMP 节点立即删除 IPv6 数据。

对于非被管 SNMP 节点,完成以下步骤:

- a 安装其他许可证容量。
- b 使用位于 NNMi 控制台中的操作 > 管理模式 > 管理命令,更改已由许可服务标为非 被管的节点的管理模式。您还可以使用 nnmmanagementmode.ovpl 脚本管理这些 节点。有关详细信息,请参阅 nnmmanagementmode.ovpl 参考页或 UNIX 联机 帮助页。
- c 使用位于 NNMi 控制台中的操作>轮询>配置轮询命令,使 NNMi 能够搜索它们。还可以使用 nnmnoderediscover.ovpl 脚本搜索这些节点。有关详细信息,请参阅 nnmnoderediscover.ovpl 参考页或 UNIX 联机帮助页。

• NNMi Advanced 许可证过期或某用户删除了许可证; 且您由于疏忽未安装 NNMi 基本许可证。

NNMi 立即删除所有非 SNMP IPv6 节点,并自动取消管理剩余的节点。要对此进行补救,请完成以下步骤:

- a 安装有效许可证。
- b 使用位于 NNMi 控制台中的操作 > 管理模式 > 管理命令,更改已由许可服务标为非 被管的节点的管理模式。您还可以使用 nnmmanagementmode.ovpl 脚本管理这些 节点。有关详细信息,请参阅 nnmmanagementmode.ovpl 参考页或 UNIX 联机 帮助页。
- c 使用位于 NNMi 控制台中的操作 > 轮询 > 配置轮询命令,使 NNMi 能够搜索从非被管更改为被管的节点。也可以使用 nnmnoderediscover.ovpl 脚本搜索这些节点。有关详细信息,请参阅 nnmnoderediscover.ovpl 参考页或 UNIX 联机帮助页。
- d 要创建 IPv6 列表, 然后删除 IPv6 资产, 请使用操作 > 轮询 > 配置轮询命令从每个 被管节点获取配置信息。

清理 IPv6 资产时的已知问题

您可能在以下情况中遇到剩余 IPv6 资产:假定 NNMi 成功使用 SNMP 管理 IPv6 节点,然后节点在下一个搜索之前变得不可访问。由于现有搜索系统的设计,搜索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,需要解决通信问题,然后使用位于 NNMi 控制台中的操作 > 轮询 > 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。

在 Solaris 区域环 境中运行 NNMi

对于支持的 Solaris 操作系统版本, HP Network Node Manager i Software (NNMi) 无需特殊配置即可在 Solaris 区域环境中运行。

本章包含以下主题:

- 在 Solaris 区域中安装 NNMi
- Solaris 区域中的陷阱转发
- 在 Solaris 区域环境中运行 NNMi 应用程序故障切换
- 在 Solaris 区域环境中以 HA 运行 NNMi

在 Solaris 区域中安装 NNMi

如果计划在 Solaris 区域环境中实现 NNMi 应用程序故障切换,请参阅第 262 页的在 Solaris 区域环境中运行 NNMi 应用程序故障切换。

如果计划在高可用性 (HA) 下运行 Solaris 区域,请参阅第 262 页的在 Solaris 区域环境中 以 HA 运行 NNMi。

对于所有其他部署模型,请按照《NNMi 安装指南》中的说明安装 NNMi。

Solaris 区域中的陷阱转发

假定要将 NNMi 接收自被管设备的 SNMP 陷阱转发给另一个应用程序。要执行该操作,请 在**配置**工作区中导航到**陷阱转发配置**。有关详细信息,请参阅 NNMi 帮助。

因为 Solaris 区域环境不支持原始陷阱转发,所以请不要选择**原始陷阱**转发选项。在 Solaris 区域环境中运行 NNMi 时,选择某个其他转发选项。

在 Solaris 区域环境中运行 NNMi 应用程序故障切换

如果要在 Solaris 区域环境中使用 NNMi 应用程序故障切换功能,请在这两个物理系统上的 NNMi 区域中分别安装 NNMi。

按第 267 页的为 NNMi 配置应用程序故障切换中所述配置应用程序故障切换。在整个过程中, "服务器 X"指的是一个区域, "服务器 Y"指的是另一个区域。

在 Solaris 区域环境中以 HA 运行 NNMi

在 Solaris 区域环境中,不需要实现 NNMi 提供的解决方案即可在 HA 群集中运行 NNMi。因为 Veritas Cluster Server (VCS) 是区域感知的,所以请如图 17 中所示配置区域的 HA 资源组。

虚拟 IP 地址 节点 A 节点 B 容器 nnm 配置: 容器 nnm 配置: SHARED_DISK /etc/passwd /etc/group /etc/passwd /etc/group /etc/passwd /etc/passwd /nnm/install/ /etc/init.d/netmat /etc/init.d/netma /nnm/data/ /etc/rc2/ /etc/rc3/ etc/rc3 /opt/OV/ ar/opt/OV/ var/opt/OV/ HA 资源组

图 17 在 Solaris 区域中以 HA 运行的 NNMi

在此环境中运行 NNMi 所需的配置是最少的。 NNMi 安装过程在 nmsdb 组中创建 nmsdbmgr 用户,并将启动配置添加到主机系统。将此设置复制到 HA 群集中的第二个节点。

要安装 NNMi 以在 HA 资源组内的区域中运行,请遵循以下步骤:

- 1 在共享磁盘上, 创建 NNMi 安装文件夹:
 - /nnm/install
 - /nnm/data
- 2 在节点 A 上, 创建并准备名为 nnm 的新区域:
 - 如 Solaris 区域文档中所述创建区域 nnm。
 在区域创建期间记下所有配置参数集。
 - **b** 启动区域 **nnm**。

- c 登录区域 nnm, 然后创建以下符号链接:
 - /opt/OV/, 指向共享磁盘上的 /nnm/install/
 - /var/opt/OV/, 指向共享磁盘上的 /nnm/data/
- d 从区域 nnm 注销, 然后将其关闭。
- 3 在节点 B 上, 创建名为 nnm 的相同新区域, 然后安装 NNMi:
 - a 对区域 nnm 创建与节点 A 上的区域 nnm 相同的属性 (包括 IP 地址)。
 - **b** 启动区域 **nnm**。
 - c 登录区域 nnm, 然后创建以下符号链接:
 - /opt/OV/, 指向共享磁盘上的 /nnm/install/
 - /var/opt/OV/, 指向共享磁盘上的 /nnm/data/
 - d 通过输入以下命令,指示 NNMi 安装程序遵循符号链接:

PKG_NONABI_SYMLINKS=true

e 在 nnm 区域内安装 NNMi。

NNMi 将安装到共享磁盘上的 /nnm/install/ 和 /nnm/data/ 目录中。

- f 将以下文件复制到可从 nnm 区域以外访问的临时位置 (比如共享磁盘):
 - /etc/passwd
 - /etc/group
 - /etc/shadow
 - /etc/init.d/netmgt
- g 从区域 nnm 注销, 然后将其关闭。
- 4 在节点 A 上,复制 NNMi 修改的系统文件,然后启动 NNMi:
 - a 启动区域 **nnm**。
 - b 登录区域 nnm, 然后将文件从步骤 3 中标识的临时位置复制到区域中的正确位置;
 - /etc/passwd
 - /etc/group
 - /etc/shadow
 - /etc/init.d/netmgt

- c 创建以下符号链接(以复制在节点 B 上安装 NNMi 期间创建的配置):
 - /etc/rc0.d/K01netmgt 指向 /etc/init.d/netmgt
 - /etc/rcl.d/K01netmgt 指向 /etc/init.d/netmgt
 - /etc/rc2.d/K01netmgt 指向 /etc/init.d/netmgt
 - /etc/rc3.d/S98netmgt 指向 /etc/init.d/netmgt
 - /etc/rcS.d/K01netmgt 指向 /etc/init.d/netmgt
- d 通过运行以下命令, 启动 NNMi:

ovstart

5 配置 Veritas Cluster Server 以创建包含节点 A 和节点 B 上的区域 nnm 的资源组。 有关详细信息,请参阅 VCS 文档。

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 应用程序故障切换提供灾难恢复。(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。 表 21 对于这两种方法的 NNMi 数据恢复能力方面进行了几项比较。

比较项	NNMi 应用程序故障切换	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
故障切换所需时间	 嵌入式 NNMi 数据库:处理事务日志的时间(正常情况下,无任何 NNM iSPI 的 NNMi 为 10 到 60 分钟)。 Oracle NNMi 数据库:几乎即时。 	正常情况下,无任何 NNM iSPI 的 NNMi 为 5 到 30 分钟。
故障切换的透明性	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,该地址在故障切换时不会更改。
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)

表 21 NNMi 数据恢复能力比较

表 21 NNMi 数据恢复能力比较

比较项	NNMi 应用程序故障切换	在 HA 群集中运行 NNMi
购买的许可证	对于每个功能: 一个生产许可证与初始活动服务器的 IP 地址绑定。 一个非生产许可证与初始备用服务器 的 IP 地址绑定。 	对于每个功能: 一个与 HA 群集中某个物理系统的 IP 地址绑定的生产许可证。 一个与 HA 群集的虚拟 IP 地址绑定的非生产许可证。
安装的许可证	 初始活动服务器上使用生产许可证 密钥。 初始备用服务器上使用非生产许可证 密钥。 	 初始活动服务器上使用非生产许可证 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切换或 HA 配置单独的全局管理器。 可以为应用程序故障切换或 HA 配置单独的区域管理器。 这两个配置分别需要两个物理系统。 如果全局管理器或区域管理器发生故障切换,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切换群集中 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 配置应用程序故障切换
- 在高可用性群集中配置 NNMi





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 管理服务器出现故障时,他们还需要 NNMi 继续指示网络设备故障。NNMi 应 用程序故障切换能够满足此需要,它将 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,从而提供持续的 NNMi 功能。

本章包含以下主题:

- 应用程序故障切换概述
- 应用程序故障切换基本设置
- 为 NNMi 配置应用程序故障切换
- 使用应用程序故障切换功能
- 故障切换后返回原始配置
- NNM iSPI 和应用程序故障切换
- 集成应用程序
- 禁用应用程序故障切换
- 管理任务和应用程序故障切换
- 网络延迟/带宽注意事项

应用程序故障切换概述

应用程序故障切换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切换功能之后, 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 的应用程序故障切换配置:

- 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切换事件的系统; 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; 可在单个 系统上具有多个成员。
- 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切换功能的 nnmcluster 进程和工具。

应用程序故障切换基本设置

要部署应用程序故障切换功能,请在两个服务器上安装 NNMi。本章将这两个 NNMi 管理服务器作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。

为使应用程序故障切换成功, 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 HP-UX 操作系统,则备用服务器也必须运行 HP-UX 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 9.10 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 9.10。两个服务器上的 NNMi 补丁级别也必须相同。
- 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切换功能,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 处于初始搜索的高级阶段,否则不要启用应用程序故障切换。有关详细信息,请参阅第 69 页的评估搜索。

为了让应用程序故障切换正常运行,活动和备用服务器必须能不受限制地通过网络访问彼此。满足此条件后,完成第 270 页的为 NNMi 配置应用程序故障切换中所示的步骤。有关详细信息,请参阅第 605 页的 NNMi 9.10 和已知端口。



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。

为 NNMi 配置应用程序故障切换

上安装 NNMi。



1 如《NNMi 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)



- 2 对服务器 X 上的每个许可证, 如第 115 页的许可 NNMi 中所述获取服务器 Y 的相似非 生产许可证,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。

如果在将 Oracle 作为数据库时使用应用程序故障切换,则备用服务器上的 NNMi 进程应 当已经停止。

4 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)的应用程序故障切换功能。使用以下过程:

编辑在以下步骤中表示取消注释文件中文本块内的行和修改文本。

- a 编辑以下文件:
 - Windows: %NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties
 - UNIX: \$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

在 NNMi 9.0x 中,应用程序故障切换功能支持可自动搜索网络上的群集主机的 UDP 解决方案。从 NNMi 9.10 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 故障切换才能起作用。

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

如果在将 Oracle 作为数据库时使用应用程序故障切换,则 NNMi 忽略 nms-cluster.properties 文件中包含的数据库参数。

5 根据所采取的方法,完成第 124 页的将应用程序故障切换配置为使用自签名证书或第 126 页的将应用程序故障切换配置为使用证书颁发机构中指示的操作。

配置应用程序故障切换功能时,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 5 指示的一组操作

- 6 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
 - UNIX: \$NnmDataDir/shared/nnm/conf/nnmcluster/cluster.keystore

Λ

7 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类似下 面的信息:

State ID: 0000000100000005 Date/Time: 15 Mar 2011 - 09:37:58 (GMT-0600) Cluster name: ThisCluster (key CRC:626,187,650) Automatic failover: Enabled NNM database type: Embedded NNM configured ACTIVE node is: NO ACTIVE NNM current ACTIVE node is: NO ACTIVE Cluster members are: Local? NodeType State OvStatus Hostname/Address _____ ____ _____ n/a * REMOTE ADMIN n/a serverX.xxx.yyy.yourcompany.com/ 16.78.61.68:7800

(SELF) ADMIN 16.78.61.71:7800 n/a

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:

n/a serverY.xxx.yyy.yourcompany.com/

- 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

UNIX: \$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 9.10, 服务器 Y 运行 NNMi 9.10 补丁 1 (可用时)。在运行 nnmcluster 命令之后应该 能看到显示此错误。

8 在服务器 X 上启动 NNMi 群集管理器:

nnmcluster -daemon

- 在 NNMi 管理服务器 X 上运行 nnmcluster -daemon 命令之后, NNMi 群集管 理器通过以下启动例程:
 - 将 NNMi 管理服务器 X 连接到群集。
 - 检测没有其他 NNMi 管理服务器存在。
 - NNMi 管理服务器 X 假定为活动状态。
 - 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 UNIX 联机帮助页。
- 9 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,如
 ACTIVE_NNM_STARTING 或 ACTIVE_某个其他状态中的。不要继续执行步骤 10,除非 您知道服务器 X 是主动节点。
- 10 在服务器 Y 上, 启动 NNMi 群集管理器:

nnmcluster -daemon

在 NNMi 管理服务器 Y 上运行 nnmcluster -daemon 命令之后, NNMi 群集管 理器通过以下启动例程:

- 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,并处于活动状态。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 备用状态的最低需要。屏幕会显示 STANDBY RECV TXLOGS。
- NNMi 管理服务器 Y 进入等待状态,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 UNIX 联机帮助页。

11 如果发生故障切换,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)。如果发生故障切换,则用户可以连接到服务器 Y (备用 NNMi 管理服务器)。 12 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。

使用应用程序故障切换功能

因为两个 NNMi 管理服务器都在运行群集管理器,且有一个主动节点和一个备用节点,所 以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并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切换功能,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 UNIX 联机帮助页。

使用嵌入式数据库的应用程序故障切换行为

图 18 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切换配置。阅读本章的其余内容时,请参考此图。



图 18 应用程序故障切换配置 (嵌入式数据库)

在启动主动和备用节点之后,备用节点检测主动节点,请求来自主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 搜索文件已与活动服务器同步,将不重新传输文件。

主动和备用节点都在运行时,主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。

备用节点从主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。

如果主动节点出于任何原因变为不可用,则通过运行 ovstart 命令以启动 NNMi 服务,可 使备用节点将成为主动节点。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,则备用系统开始搜索和轮询活动。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。

使用 Oracle 数据库的应用程序故障切换行为

图 19 显示使用 Oracle 数据库的两个 NNMi 管理服务器的应用程序故障切换配置。阅读本章的其余内容时,请参考此图。



图 19 应用程序故障切换配置 (Oracle 数据库)

如果主动节点出于任何原因变为不可用,则通过运行 ovstart 命令以启动 NNMi 服务,可 使备用节点将成为主动节点。

如果活动 NNMi 系统失败,则备用系统开始搜索和轮询活动。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。

应用程序故障切换场景

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切换:

- 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 管理服务器都运行于活动状态。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切换的 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

如果运行 ovstop 命令,则 NNMi 不会故障切换到备用节点。HP 设计了 ovstop 命令来 支持临时维护停止。要手动启动故障切换,请用 ovstop 命令加 -failover 选项。有关 详细信息,请参阅 ovstop 参考页或 UNIX 联机帮助页。

ovstop 命令的以下选项应用于在应用程序故障切换群集中配置的 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,并强制故障切换 到备用 NNMi 管理服务器。如果之前禁用了故障切换模式,则重新启用它。此命令等 价于: nnmcluster -enable -shutdown
- ovstop -nofailover: 此命令禁用故障切换模式, 然后停止本地的守护程序模式的 群集进程。不发生故障切换。此命令等价于: nnmcluster -disable -shutdown

• ovstop -cluster: 此命令停止主动节点和备用节点,并从群集删除它们。此命令等 价于: nnmcluster -halt

如果在运行 UNIX 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切换。这可能不是您所希望的结果。要控制维护时段 内的应用程序故障切换,请使用 nnmcluster -acquire 和 nnmcluster -relinquish 命令按您所希望的方式设置主动节点和备用节点,然后再运行 shutdown 命令。有关详细 信息,请参阅 nnmcluster 参考页或 UNIX 联机帮助页。

应用程序故障切换事件

只要 nnmcluster 进程或使用 **nnmcluster** 命令的用户将节点启动为主动, **NNMi** 就生成 以下事件之一:

- *NnmClusterStartup*: 已启动 NNMi 群集,但不存在主动节点。因此,节点是在主动 状态下启动的。此事件的严重度为正常。
- *NnmClusterFailover*: NNMi 群集检测到主动节点故障。备用节点随即启用,并在新的主动节点上启动 NNMi 服务。此事件的严重度为严重。

故障切换后返回原始配置

假定主动节点出现故障,且备用节点用作主动节点。解决以前主动节点的问题之后,在所需 主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 UNIX 联机帮助页。

NNM iSPI 和应用程序故障切换

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) 使用应用程序故障切换功能:

- NNM iSPI 在 NNMi 管理服务器上运行。
- NNM iSPI 使用与 NNMi 相同的嵌入式数据库实例。

NNM iSPI Performance for QA、 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 应用程序故障切换功能,则必须在专用服务器上安装这些 iSPI。在这种情况下,故障切换发生之后, iSPI 自动连接 到新的 NNMi 管理服务器。作为 NNMi 应用程序故障切换配置的一部分,在群集中的每个 NNMi 管理服务器上运行 NNM iSPI Performance for Metrics、NNM iSPI Performance for QA 或 NNM iSPI Performance for Traffic 的支持脚本。

有关详细信息,请参阅 NNM iSPI Performance for Metrics、NNM iSPI Performance for QA 或 NNM iSPI Performance for Traffic 帮助中的*应用程序故障切换支持*。

NNM iSPI 安装信息

要在已经是应用程序故障切换群集一部分的 NNMi 管理服务器上安装 NNM iSPI,请执行 以下操作:

- 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,请参阅第 40 页的最佳实践:保存现有配置。
- 2 作为预防措施,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,请参阅第 349 页的备份范围。
- 3 仅嵌入式数据库:作为预防措施,请在活动 NNMi 管理服务器上运行 nnmcluster -dbsync 命令,并等待命令完成。
- 4 在备用 NNMi 管理服务器上,运行以下命令:

nnmcluster -shutdown

- 5 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
 - UNIX: \$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties
- 6 注释掉 com.hp.ov.nms.cluster.name 选项,并保存文件。
- 7 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。
- 8 如 iSPI 安装指南中所述,在备用 NNMi 管理服务器上安装 NNM iSPI。
- 9 在活动 NNMi 管理服务器上运行 nnmcluster -halt 命令。

- 10 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
 - UNIX: \$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties
- 11 注释掉 com.hp.ov.nms.cluster.name 选项,并保存文件。
- 12 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。
- 13 如 iSPI 安装指南中所述,在活动 NNMi 管理服务器上安装 NNM iSPI。
- 14 在活动和备用 NNMi 管理服务器上编辑以下文件:
 - Windows: %NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties
 - UNIX: \$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties
- 15 取消注释 com.hp.ov.nms.cluster.name 选项,并保存每个文件。
- 16 在活动 NNMi 管理服务器上运行 ovstart 命令。
- 17 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, 如 ACTIVE_NNM_STARTING 或 ACTIVE_某个其他状态中的。不要继续执行步骤 18,除非您知道活动 NNMi 管理服务器是主动节点。
- 18 在备用 NNMi 管理服务器上运行 ovstart 命令。

集成应用程序

当其他 HP 软件或第三方产品与 NNMi 集成时, NNMi 应用程序故障切换对集成的影响取 决于产品如何与 NNMi 通信。有关详细信息,请参阅集成 NNMi 部分中的相应章节。

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 参阅集成 NNMi 部分中的相应章节。
- 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,请遵循以下步骤:
- 1 在服务器 X 上,运行以下命令:

nnmcluster -daemon

服务器 X 加入群集,并假定为备用状态。

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。

禁用应用程序故障切换

假定您配置了应用程序故障切换,使用几天后决定完全禁用它。以下信息解释如何完全禁用 应用程序故障切换。按以下指示完成操作,包括应用程序故障切换群集中配置的活动和备用 NNMi 管理服务器上的操作。

- 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,直到不再看到 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
 - UNIX: \$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
 - UNIX: \$NnmDataDir/shared/nnm/databases/Postgres/postgresql.conf

11 删除每个文件中以 archive_command 和 archive_timeout 开始的以下行。下面是 Windows NNMi 管理服务器上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。

```
archive_command = 'nnmcluster.exe -archive "%p" "C:/Documents
and Settings/All Users/Application Data/HP/HP BTO Software/
shared/nnm/databases/Postgres_standby/TxWALs_send"/%f'
```

archive timeout = 900

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 只在以前的活动 NNMi 管理服务器上运行 ovstart 命令。在应用程序故障切换配置 中,这是有永久 NNMi 许可证的 NNMi 管理服务器。
- 14 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。在应用程序故障切换配置中,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,请参阅第 115 页的许可 NNMi。
- 15 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
 - UNIX: \$NnmDataDir/shared/nnm/databases/Postgres_standby

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。

- 16 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
 - UNIX: \$NnmDataDir/shared/nnm/databases/Postgres.OLD

管理任务和应用程序故障切换

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切换。

应用程序故障切换和升级到 NNMi 9.10

如果计划升级正在以 NNMi 应用程序故障切换配置运行的 NNMi 9.0x 的较早版本,则支持的升级路径是临时取消应用程序故障切换配置,将每个 NNMi 管理服务器升级到 NNMi 9.10,然后重新配置应用程序故障切换。

要升级配置了应用程序故障切换的 NNMi 管理服务器,请遵循以下步骤:

- 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,请参阅第 40 页的最佳实践:保存现有配置。
- 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,请参阅第 349 页的备份范围。
- 3 *仅嵌入式数据库*:在活动 NNMi 管理服务器上完成以下步骤。完成这些步骤会加速启动第 284 页的步骤 7 中显示的备用 NNMi 管理服务器:
 - **a** 运行 **nnmcluster** 命令。
 - b 在 NNMi 提示之后, 键入 dbsync, 然后按 Enter。检查显示的信息以确保它包括 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 管理服务器完成了前一条消息所指的备份。 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。

- 4 在备用 NNMi 管理服务器上运行 nnmcluster -shutdown 命令。这将关闭备用 NNMi 管理服务器上的所有 nnmcluster 进程。
- 5 要验证备用 NNMi 管理服务器上已无 nnmcluster 节点在运行,*请在备用 NNMi 管理 服务器上完成以下步骤*。
 - a 运行 nnmcluster 命令。
 - b 验证已无 (本地) nnmcluster 节点存在,标记为 (SELF) 的节点除外。可能有一 个或多个 (远程) 节点存在。
 - c 运行 **exit** 或 **quit** 以停止在步骤 a 中启动的交互 nnmcluster 进程。

- 6 在备用NNMi 管理服务器上完成以下步骤,以临时禁用应用程序故障切换:
 - a 编辑以下文件:
 - Windows: %NNM_SHARED_CONF%\props\nms-cluster.properties
 - UNIX: \$NNM SHARED CONF/props/nms-cluster.properties
 - b 注释掉 com.hp.ov.nms.cluster.name 参数。
 - c 保存更改。
- 7 在备用 NNMi 管理服务器上启动然后停止进程。
 - a 在备用 NNMi 管理服务器上运行 ovstart 命令。运行 ovstart 命令会导致备用 NNMi 管理服务器从活动 NNMi 管理服务器导入事务日志。
 - b 在 **ovstart** 命令完成之后,运行 **ovstatus -v** 命令。所有 **NNMi** 服务应当显示 状态 RUNNING。
 - c 在备用 NNMi 管理服务器上运行 ovstop 命令。
- 8 使用位于《NNMi 安装指南》中的说明将备用 NNMi 管理服务器升级到 NNMi 9.10。

必须将已安装在备用 NNMi 管理服务器上的所有 iSPI 升级到支持 NNMi 9.10 的 iSPI 版本。

现在,您已有运行 NNMi 9.0x 的以前的活动 NNMi 管理服务器,以及运行 NNMi 9.10 的以前的备用 NNMi 管理服务器。这两个 NNMi 管理服务器独立运行,没有数据库同步。这意味着有两个 NNMi 管理服务器并行监视网络。不要使这些 NNMi 管理服务器 保持此配置超过几个小时,因为此配置违反以前备用节点上安装的非生产许可证。

要完成升级以纠正此情况,请选择某个时间将以前的主动节点升级到 NNMi 9.10。在完成升级时,让操作员临时使用以前的备用节点监视网络。

此过程的其余部分假定您计划保留以前主动节点的数据库信息,并丢弃以前备用节点的 数据库信息。

- 9 在以前的活动 NNMi 管理服务器上运行 nnmcluster -halt 命令。
- 10 要验证以前的活动 NNMi 管理服务器上已无 nnmcluster 节点在运行,*请在以前的活动 NNMi 管理服务器上完成以下步骤*。
 - a 运行 nnmcluster 命令。
 - b 验证已无 (本地) nnmcluster 节点存在,标记为 (SELF) 的节点除外。可能有一 个或多个 (远程) 节点存在。
 - c 运行 **exit** 或 **quit** 以停止在步骤 a 中启动的交互 nnmcluster 进程。

- 11 在以前的活动 NNMi 管理服务器 上完成以下步骤,以临时禁用应用程序故障切换:
 - a 编辑以下文件:
 - Windows: %NNM_SHARED_CONF%\props\nms-cluster.properties
 - UNIX: \$NNM_SHARED_CONF/props/nms-cluster.properties
 - b 注释掉 com.hp.ov.nms.cluster.name 参数。

使用位于《NNMi 安装指南》的说明将以前的活动 NNMi 管理服务器升级到 NNMi 9.10。

必须将已安装在以前的活动 NNMi 管理服务器上的所有 iSPI 升级到支持 NNMi 9.10 的 iSPI 版本。

现在有两个服务器再运行 NNMi 9.10,但因为数据库不同步,它们仍然是独立的。

- 12 在以前的活动 NNMi 管理服务器上完成以下步骤:
 - **a** 运行 **ovstop** 命令。
 - b 编辑以下文件:
 - Windows: %NNM SHARED CONF%\props\nms-cluster.properties
 - UNIX: \$NNM SHARED CONF/props/nms-cluster.properties
 - c 输入 com.hp.ov.nms.cluster.name 参数的值。
 - d 取消注释 com.hp.ov.nms.cluster.name 参数。
 - e 保存更改。
- 13 在以前的活动 NNMi 管理服务器上运行 ovstart 或 nnmcluster -daemon 命令。 它现在是主动节点。
- 14 指示操作员开始使用主动节点来监视网络。

以前的备用 NNMi 管理服务器丢弃维护时段内发生的从第 284 页的步骤 9 到第 285 页 的步骤 13 的所有数据库活动。

- 15 在以前的备用 NNMi 管理服务器上完成以下步骤:
 - **a** 运行 **ovstop** 命令。
 - b 编辑以下文件:
 - Windows: %NNM_SHARED_CONF%\props\nms-cluster.properties
 - UNIX: \$NNM SHARED CONF/props/nms-cluster.properties
 - c 取消注释 com.hp.ov.nms.cluster.name 参数。
 - d 保存更改。
- 16 在以前的备用 NNMi 管理服务器上运行 ovstart 或 nnmcluster -daemon 命令。

此 NNMi 管理服务器成为备用节点,并从主动节点接收数据库的副本。

- 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切换功能;并完成了 上述升级过程,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。
- 18 如果正在使用 Linux NNMi 管理服务器,则在活动和备用 NNMi 管理服务器上运行以下命令:

chmod 777 /var/opt/OV/shared/perfSpi/datafiles/nnm_details.xml

应用程序故障切换和 NNMi 补丁

两个 NNMi 管理服务器必须运行相同的 NNMi 版本和补丁级别。要向活动和备用 NNMi 管理服务器添加补丁,请使用以下某个过程:

- 为应用程序故障切换应用补丁(关闭活动和备用服务器)
 当您不在乎网络监视中断时,请使用此过程。
- 为应用程序故障切换应用补丁 (保留一个活动 NNMi 管理服务器) 当您需要避免任何网络监视中断时,请使用此过程。

为应用程序故障切换应用补丁 (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。要将补丁应用于配置了应用程序故障切换的 NNMi 管理服务器,请遵循以下步骤:

- 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,请参阅第 40 页的最佳实践:保存现有配置。
- 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,请参阅第 349 页的备份范围。
- 3 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, 键入 dbsync, 然后按 Enter。检查显示的 信息以确保它包括以下消息:

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 管理服务器完成了前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。

- 4 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。
- 5 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 验证已无 nnmcluster 节点存在,标记未 (SELF) 的节点除外。
 - c 运行 **exit** 或 **quit** 以停止在步骤 a 中启动的交互 nnmcluster 进程。
- 6 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
 - UNIX: \$NNM_SHARED_CONF/props/nms-cluster.properties
 - b 注释掉 com.hp.ov.nms.cluster.name 参数。
 - c 保存更改。
- 7 遵循 NNMi 补丁附带的说明将该补丁应用于活动 NNMi 管理服务器。
- 8 在活动 NNMi 管理服务器上,取消注释 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
 - UNIX: \$NNM SHARED CONF/props/nms-cluster.properties
 - **b** 取消注释 com.hp.ov.nms.cluster.name 参数。
 - c 保存更改。
- 9 在活动 NNMi 管理服务器上运行 ovstart 命令。
- 10 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。
- 11 运行 **nnmcluster** -**dbsync** 命令以创建新备份。
- 12 在备用 NNMi 管理服务器上,如第 287 页的步骤 a 到第 287 页的步骤 c 中所示,注释 掉 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.name 参数。
- 13 将 NNMi 补丁应用于备用 NNMi 管理服务器。
- 14 在备用 NNMi 管理服务器上,如第 287 页的步骤 a 到第 287 页的步骤 c 中所示,取消 注释 nms-cluster.properties 文件中的 com.hp.ov.nms.cluster.name 参数。
- 15 在备用 NNMi 管理服务器上运行 ovstart 命令。

- 16 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切换功能;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。
- 17 如果正在使用 Linux NNMi 管理服务器,则在活动和备用 NNMi 管理服务器上运行以下命令:

chmod 777 /var/opt/OV/shared/perfSpi/datafiles/nnm_details.xml

为应用程序故障切换应用补丁 (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。

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 补丁应用于配置了应用程序故障切换的 NNMi 管理服务器,请遵循以下步骤:

- 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,请参阅第 40 页的最佳实践:保存现有配置。
- 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,请参阅第 349 页的备份范围。
- 3 要同步两个数据库,请在任一 NNMi 管理服务器上运行以下命令: nnmcluster -dbsync

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。

- 4 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 -display
 等待活动 NNMi 管理服务器回复到 ACTIVE_NNM_RUNNING,备用 NNMi 管理服务器
 回复到 STANDBY READY,然后再继续操作。
- 5 要禁用群集,请在活动 NNMi 管理服务器上运行以下命令: nnmcluster -disable
- 6 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
- 7 继续之前,确保以下进程和服务终止:
 - postgres
 - ovjboss
- 8 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。
- 9 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

UNIX: \$nnmDataDir/shared/nnm/conf/props/nms-cluster.properties

- 10 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
- 11 在备用 NNMi 管理服务器上安装 NNMi 补丁。
- 12 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
- 13 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。
- 14 在备用 NNMi 管理服务器上,取消注释 nms-cluster.properties 文件中的群集名称。
- 15 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
- 16 在活动 NNMi 管理服务器上安装 NNMi 补丁。
- 17 在活动 NNMi 管理服务器上,取消注释 nms-cluster.properties 文件中的条目。
- 18 使用以下命令启动活动 NNMi 管理服务器:

 nnmcluster -daemon
- **19** 要启用群集,请在活动 NNMi 管理服务器上运行以下命令: nnmcluster -enable
- 20 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 -display 等待活动 NNMi 管理服务器完成从备用 NNMi 管理服务器检索数据库的操作。
- 21 在活动 NNMi 管理服务器显示 STANDBY_READY 之后,在活动 NNMi 管理服务器上运行以下命令: nnmcluster -acquire
- 22 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切换功能;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。
- 23 如果正在使用 Linux NNMi 管理服务器,则在活动和备用 NNMi 管理服务器上运行以下命令:

chmod 777 /var/opt/OV/shared/perfSpi/datafiles/nnm_details.xml

应用程序故障切换和重新启动 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切换 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切换功能。

应用程序故障切换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切换时,要从原始备份恢复 NNMi 数据 库,请遵循以下步骤:

- 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
 - UNIX: \$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
 - UNIX: \$NnmDataDir/shared/nnm/conf/ props\nms-cluster.properties
 - b 将数据库恢复正常。请参阅第 352 页的恢复 NNMi 数据。
 - 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注释群集名称:
 - Windows: %NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties
 - UNIX: \$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。要验证此步骤已完成,请运行 nnmcluster -display 命令,并查找 STANDBY_READY 消息。

网络延迟 / 带宽注意事项

NNMi 应用程序故障切换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、数据库事务日志及其他 NNMi 配置文件。通过 WAN(广域网)实现 NNMi 应用程序故障切换时,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 应用程序故障切换的带宽需要,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。

类似地,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主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切换的数据传输需要,NNMi即可避免虚假的故障切换通知。

HP 验证多子网 NNMi 应用程序故障切换时,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,不会有虚假故障切换。

应用程序故障切换和 NNMi 嵌入式数据库

应用程序故障切换适用于 NNMi 9.10 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切换的网络需要。相比于使用嵌入式数据库进行应用程序故障切换,使用 Oracle 进行应用程序故障切换 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 序故障切换相关的 NNMi 通信量信息。 将 NNMi 配置为使用嵌入式数据库进行应用程序故障切换后, NNMi 执行以下操作:

- 1 主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 应用程序故障切换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 当备用节点变为主动的时,NNMi启动,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,数据库变为可用的,且备用节点启动剩余的 NNMi 进程。
- 8 原始备用节点现在变为主动的,进程在步骤1重新开始。

应用程序故障切换环境中的网络通信量

在应用程序故障切换环境中, NNMi 从主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切换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主动节点上的那些文件同步。
- 其他事件,如参数更改(启用/禁用故障切换等),节点加入或退出群集。

前两项产生应用程序故障切换使用的网络通信量的 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:

- 搜索新节点。
- 搜索有关节点、接口、VLAN 及其他被管对象的属性。
- 状态轮询和状态更改。
- 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 发网络上设备的状态轮询,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切换。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。应用程序故障切换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 16 MB 文件压缩到大约 8 MB。请记住,在数据库活动频繁时期,应用程序故障切换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。

应用程序故障切换通信量测试

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。这归因于于 每次故障切换事件添加的额外 5000 个节点的搜索相关的数据库活动。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,并等待搜索稳定下来。4小时后,测试人员引发故障切换(备用节点变为主动的,以前的主动节点变为备用的)。故障切换后,测试人员立即添加大约5000个节点,再等待4小时以使NNMi搜索进程稳定,随后引发下一次故障切换(故障回复到以前的主动节点)。测试人员重复此循环若干次,使故障切换之间的时间有所变化(4小时,然后6小时,然后再2小时)。每次故障切换事件后,测试人员都测量以下数据:

- 数据库备份 ZIP 文件 (节点第一次变为主动时创建)的大小。
- 事务日志: 文件总数和磁盘空间利用率。
- 在引发故障切换前一刻, NNMi 数据库中的节点数和接口数。
- 完成故障切换的时间。它包括从主动节点上运行初始 ovstop 命令到备用节点完全主动 且 NNMi 开始运行的时间。

表 22 汇总了结果:

表 22 应用程序故障切换测试结果

小时	DB.zip	Tx 日志	Tx 日志	节点	接口	故障切换时
	大小 (MB)	Tx 日志	(GB)			间(分钟)
4	6.5	50	.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 将文件从主动节点传输到备用节点时, 平均传输速率约为5GB/4小时, 连续吞吐量约为350KB/ 秒或2.8MB/ 秒。

此数据不包括任何其他应用程序故障切换通信量,比如检测信号、文件一致性检查或其他 应用程序故障切换通信。此数据还排除了网络 I/O 的开销,比如数据包报头。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。

由 NNMi 应用程序故障切换环境生成的通信量有很大突发性。应用程序故障切换每五分钟 识别一次主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。

每次主动和备用节点交换角色(备用节点变为主动的,主动节点变为备用的)时,新的主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切换时间,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,不需要在故障切换时导入。

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切换结 合使用时,在故障切换之后网络可能如何运作。



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切换时功能和数据的连续性的一组硬件和软件。

NNMi 支持配置为在 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。

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。如果需要,可以在这些说明指定 NNMi 提供的命令的 位置替换特定于 HA 产品的命令。

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:

- 第 298 页的 HA 概念
- 第 303 页的验证配置 NNMi 以 HA 运行的先决条件
- 第 305 页的配置 HA
- 第 314 页的共享 NNMi 数据
- 第 317 页的在 HA 群集中许可 NNMi
- 第 318 页的维护 HA 配置
- 第 322 页的从 HA 群集取消配置 NNMi
- 第 326 页的对以 HA 运行的 NNMi 应用补丁
- 第 327 页的将以 HA 运行的 NNMi 从 NNMi 9.0x 升级到 NNMi 9.10
- 第 331 页的对 HA 配置进行故障诊断
- 第 341 页的 HA 配置参考

HA 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。图 20 显示示例群集体系结构。



图 20 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。

在诸如 HP Serviceguard、Veritas Cluster Server、Microsoft Failover Clustering 或 Microsoft Cluster Services 的当前群集环境中,应用程序表示为资源的复合体,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。资源将构造 HA 资源组,它表示在群集 环境中运行的应用程序。图 21 显示示例 HA 资源组。

图 21 典型 HA 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 产品对于 HA 资源 组使用不同的名称。表 23 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 系统和设备支持列表。)

表 23 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
Microsoft Failover Clustering	MSFC	资源组
HP Serviceguard	SG	包
Veritas Cluster Server	VCS	服务组
Red Hat Cluster Suite	RHCS	服务

HA 术语

表 24 列出并定义了某些常用 HA 术语。

表 24 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。

表 24 常用 HA 术语 (续)

术语	描述
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。 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	在主群集节点之后添加到 HA 配置的任何系统都已针对 HA 作了完全配置。
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 资源组故障切换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 HA 群集场景

对于 NNMi 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。

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

图 22 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,则按类似于图 22 中的节点 B 的方式配置其他节点。

图 22 NNMi HA 群集的基本场景



有关如何实施此场景的信息,请参阅第 305 页的为 HA 配置 NNMi 和第 311 页的为 HA 配置 NNM iSPI。

独立服务器场景上的 NNMi和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,如图 23 中所示。NNMi HA 资源组与仅针对 NNMi 的场景所述的内容相同。



图 23 NNMi 以及在独立服务器上安装 NNM Performance iSPI 的 HA

有关如何实施此场景的信息,请参阅第 305 页的为 HA 配置 NNMi 和第 311 页的为 HA 配置 NNM iSPI。

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 数据库应当在单独的服务器上,如图 24 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。





有关如何实施此场景的信息,请参阅第 312 页的在 Oracle 环境中配置 NNMi 以 HA 运行 和第 311 页的为 HA 配置 NNM 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,如图 25 中所示。

NNMi 以及在独立服 务器上安装 NNM Performance iSPI 的 场景

带 Oracle 数据库的

图 25 带 Oracle 数据库的 NNMi 以及在独立服务器上安装 NNM Performance iSPI 的 HA



有关如何实施此场景的信息,请参阅第 312 页的在 Oracle 环境中配置 NNMi 以 HA 运行 和第 311 页的为 HA 配置 NNM iSPI。

联机帮助页

对于 HA 配置, NNMi 联机帮助页包含以下主题:

- 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 HA 运行的先决条件

以 HA 运行 NNMi 的成功配置取决于很多因素:

- 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 系统和设备支持列表中的信息,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。

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(或虚拟机图像)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)。

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。

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

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 系统和设备支持列表 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 MSFC)
 - 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 的正确版本和补丁级别。
- 8 如有必要,请安装 HA 产品。

在 Solaris 区域环境中,在全局区域中安装 HA 产品。

- 9 如第 315 页的手动准备共享磁盘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 群集提供检查应用程序检测信号和启动故障切换之类的功能。HA 群集配置必须至 少包含以下各项:

- (仅 UNIX) ssh 和/或 remsh
- (仅 Windows) 可进行 DNS 解析的 HA 群集虚拟 IP 地址
- 可进行 DNS 解析的 HA 群集虚拟主机名
- 唯一且特定于 NNMi 的资源组。

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。

- MSFC: 使用 Failover Cluster Management for Windows 2008 的创建群集向导。
- ServiceGuard:
 - 添加节点的 .rhosts 条目或 .ssh 条目。
 - — 配置 HA 产品 (cmgetconf、 cmcheckconf、 cmapplyconf)。请参阅 HA 产 品的最新文档,了解设置群集的信息。
- 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,请参阅第 332 页的 HA 资源测试。

配置 HA

本部分描述用于为 NNMi 执行新的 HA 配置的过程。它包含以下主题:

- 第 305 页的为 HA 配置 NNMi 证书
- 第 305 页的为 HA 配置 NNMi
- 第 311 页的为 HA 配置 NNM iSPI
- 第 312 页的在 Oracle 环境中配置 NNMi 以 HA 运行



如果在 Solaris 区域环境中运行 NNMi,则无须执行本章中描述的配置过程。请参阅第 262 页 的在 Solaris 区域环境中以 HA 运行 NNMi。

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。

为 HA 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 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,则需要执行额外的操作。获取新证书之后,完成第 128 页的为高可用性配置新证书中所示的步骤。可以在配置 NNMi 以 HA 运行之前或之后完成此过程。

为 HA 配置 NNMi

配置 NNMi 以 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,如第 308 页的在主群集节点上配置 NNMi 中的步骤 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, 如第 308 页的在主群集节点上配置 NNMi 中的步骤 10 到 步骤 15 所述。
 - 在辅助节点上同样执行此任务,如第 310 页的在辅助群集节点上配置 NNMi 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。



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。

故障切换期间 NNMi 控制台无响应。故障切换完成之后, NNMi 用户必须登录才能继续其 NNMi 控制台会话。

NNMi HA 配置信息

HA 配置脚本采集有关 NNMi HA 资源组的信息。表 25 列出配置主节点所需的信息。开始 配置过程之前,采集此信息。

表 25	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。 例如: nnmtest1	
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。 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 本可能将系统置于不稳定状态。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 NNMi	
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 • HP-UX: lan0 • Linux: eth0 • Solaris: bge0	

表 25 NNMi HA 主节点配置信息

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 SAN 或 NFS。运行HA 配置脚本之后,按第 315 页的手动准备共享磁盘中所述配置共享磁盘。
文件系统类型	 (仅 UNIX)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(参阅第 317页的有关 Windows 服务器上的共享磁盘配置的说明);SAN HP-UX:vxfs Linux:ext2、ext3和vxfs(用于 VCS和 RHCS) Solaris:vxfs 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,然后指定共享文件系统类型为无。
磁盘组	(仅 UNIX) NNMi 共享文件系统的磁盘组名称。此名称基于 HA 资源组的名称。例如: nnmtest1-dg
卷组	(仅 UNIX) NNMi 共享文件系统的卷组名称。此名称基于 HA 资源组的名称。例如: nnmtest1-vol
安装点	用于安装 NNMi 共享磁盘的目录位置。安装点必须在系统之间保持一致。(即 每个节点必须使用相同的安装点名称。)例如: • Windows: S:\ 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。 • UNIX: /nnmmount

在主群集节点上配置 NNMi

在主群集节点上完成以下过程。



如果要将 Oracle 用作主 NNMi 数据库,请先参阅第 312 页的在 Oracle 环境中配置 NNMi 以 HA 运行。

如果在 Solaris 区域环境中运行 NNMi,则无须执行本章中描述的配置过程。请参阅第 262 页 的在 Solaris 区域环境中以 HA 运行 NNMi。

- 1 如果尚未执行此操作,请完成第 303 页的验证配置 NNMi 以 HA 运行的先决条件的 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),然后验证 NNMi 是否正常运行。
- 3 如果希望在此 NNMi 管理服务器上运行任何 NNM iSPI, 请先参阅第 311 页的为 HA 配置 NNM iSPI, 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, 以备份所有 NNMi 数据。例如:

nnmbackup.ovpl -type offline -scope all -target nnmi_backups

有关此命令的详细信息,请参阅第 347 页的 NNMi 备份和恢复工具。

- 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:
 - MSFC: 使用磁盘管理配置磁盘安装点并格式化磁盘。
 - Serviceguard:

使用诸如 pvcreate、vgcreate 和 lvcreate 的 LVM 命令初始化磁盘, 创建卷组 和逻辑卷。

• *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:

使用诸如 pvcreate、vgcreate 和 lvcreate 的 LVM 命令初始化磁盘, 创建卷组 和逻辑卷。

对于 UNIX 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:

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。

- Windows: 使用 Windows 资源管理器和磁盘管理。
- UNIX:
 - 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 555。例如:

ls -l /nnmmount

7 停止 NNMi:

ovstop -c

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>

• UNIX:

\$NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM \ -to <HA 安装点>

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,请参阅第 336页的在取消配置所有群集节点之后,对 NNMi 重新启用 HA。

9 (仅 UNIX) 卸载共享磁盘, 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)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。

- 12 配置 NNMi HA 资源组:
 - Windows:

%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM

• UNIX:

\$NnmInstallDir/misc/nnm/ha/nnmhaconfigure.ovpl NNM

第306页的表25描述此命令请求的信息。

13 (仅 UNIX) 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, 您为共享文件系统类型指定的值是什么(如第 306 页的表 25 中的共享 文件系统类型和文件系统类型所述)?
 - 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,按第 315 页的手动准备共享磁盘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>

• UNIX:

\$NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM \
<资源组>

如果 NNMi 未正确启动,请参阅第 331 页的对 HA 配置进行故障诊断。

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,请完成第 308 页的在主群集节点上配置 NNMi 的过程。
- 2 如果尚未执行此操作,请完成第 303 页的验证配置 NNMi 以 HA 运行的先决条件的 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),然后验证 NNMi 是否正常工作。
- 4 安装第 308 页的在主群集节点上配置 NNMi 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)。

该安装点必须使用您在在主群集节点上配置 NNMi 过程的步骤 6 中创建的相同安装点 名称。

- 7 (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。
- 8 配置 NNMi HA 资源组:
 - Windows: %NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM
 - UNIX: \$NnmInstallDir/misc/nnm/ha/nnmhaconfigure.ovpl NNM

命令请求此信息时,提供 HA 资源组名称。

- 9 验证配置是否已成功:
 - Windows:

```
%NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl \
-group <资源组> -nodes
```

• UNIX:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
-group <资源组> -nodes
```

命令输出列出指定 HA 资源组的所有已配置节点。

10 (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。

为 HA 配置 NNM iSPI

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 Performance iSPI (NNM iSPI Performance for Metrics、NNM iSPI Performance for QA 和 NNM iSPI Performance for Traffic)可以安装在 NNMi 管理服务器或独立服务器上,但不能同时安装在这两种服务器上。

- 如果 NNM Performance iSPI 将安装在 NNMi 管理服务器上,请先安装这些产品,然 后配置 NNMi 以 HA 运行。
- 如果 NNM Performance iSPI 将安装在独立服务器上,请先配置 NNMi 以 HA 运行, 然后再安装这些产品。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。

NNM iSPI for MPLS、 NNM iSPI for IP Multicast 和 NNM iSPI for IP Telephony

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。先安装这些产品,然后配置 NNMi 以 HA 运行。

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 导出功能是随 NNMi 自动安装的。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 遵循以下步骤:

- 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 计划和 安装指南》。

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。



卸载 NNM iSPI NET 诊断服务器将删除所有现有报告。

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 HA 运行

本部分详细概述了配置带 Oracle 数据库的 NNMi 以 HA 运行的过程。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。

Oracle 上的 NNMi 依赖性

Oracle 和 NNMi 都以 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 HA 运行

- 1 如果计划以 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)。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 (如第 308 页的在主群集节点上配置 NNMi 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)。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 (如第 310 页的在辅助群集节点上配 置 NNMi 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。

共享 NNMi 数据

以 HA 运行的 NNMi 实施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。



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。

NNMi 共享磁盘上的数据

本部分列出当 NNMi 以 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
- UNIX:
 - \$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 日志记录目录。
 - %NnmDataDir%\shared\nnm\databases\eventdb pmd 事件数据库。
 - %NnmInstallDir%\nonOV\jboss\nms\server\nms\data
 由 ovjboss 使用的事务存储。
- UNIX:
 - \$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 日志记录目录。
 - \$NnmDataDir/shared/nnm/databases/eventdb pmd 事件数据库。
 - \$NnmInstallDir/nonOV/jboss/nms/server/nms/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。

配置文件的复制

NNMi HA 实施使用文件复制在 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 命令 nnmdatareplicator.ovpl 管理文件复制。此命令将在故 障切换过程中将 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。

有关数据复制过程的信息,请参阅 nnm-ha 联机帮助页。

手动准备共享磁盘

如果共享磁盘的格式是经过 HP 测试的(如第 306 页的表 25 中所列),则 HA 配置脚本将 准备共享磁盘,您可以忽略本部分的内容。

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。

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,请遵循以下步骤:

- 1 如第 315 页的配置 SAN 或已实际连接的磁盘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:
 - 第 316 页的在 ov.conf 文件中设置 HA 变量
 - 第 316 页的将共享磁盘移到 NNMi HA 资源组中

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 遵循以下步骤:

- 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 用第 306 页的表 25 中列出的磁盘格式对磁盘进行格式化。

5 确保 SAN 已安装。

对于 UNIX 操作系统,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切换。

在 ov.conf 文件中设置 HA 变量

NNMi 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/installDir/nonOV/jboss/nms/server/ nms/data
- HA MOUNT POINT=<HA 安装点>
- HA_CUSTOMPOLLER_DIR=<HA 安装点>/NNM/dataDir/shared/nnm/databases/ custompoller

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>
```

• UNIX:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
-config NNM -set <变量> <値>
```

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: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。

- MSFC: 使用故障切换管理将资源添加到资源组。
- ServiceGuard:

/etc/cmcluster/<资源组>/<资源组>.cntl

- 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

根据 Microsoft 知识库文章 237853, 具有 Windows Server 2008 的群集不支持动态磁盘。 要确保正确的磁盘配置,请查看以下网站上的信息:

- http://support.microsoft.com/kb/237853
- http://www.petri.co.il/ difference_between_basic_and_dynamic_disks_in_windows_xp_2000_2003.htm

在 HA 群集中许可 NNMi

对于以 HA 运行的 NNMi, NNMi 非生产许可证与 NNMi HA 资源组的虚拟 IP 地址相关 联。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。

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 如第 115 页的许可 NNMi 中所述为每个订购产品获取并安装永久非产品许可证密钥。 提示输入 NNMi 管理服务器的 IP 地址时,提供 NNMi HA 资源组的虚拟 IP 地址。
- 2 使用主动节点上 LicFile.txt 文件的新信息更新共享磁盘上的 licenses.txt 文件。 执行以下某个操作:
 - 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 目录的 licenses.txt 中。

在主动节点上, LicFile.txt 文件位于以下位置:

- Windows: %AUTOPASS_HOME%\data\LicFile.txt
 要确定 %AUTOPASS HOME% 值,请检查计算机的系统环境变量。
- UNIX: /var/opt/OV/HPOvLIC/LicFile.txt

在共享磁盘上, licenses.txt 文件的示例位置如下:

- Windows: S:\NNM\licenses.txt
- UNIX: /nnmount/NNM/licenses.txt

维护 HA 配置

维护模式

需要将 NNMi 补丁或更新应用到 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切换。 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。



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切换。

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
- UNIX: \$NnmDataDir/hacluster/<资源组>/maintenance

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 资源组从维护模式中除去

使 HA 资源组脱离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 资源组故障切换到被动群集节点。

要将 HA 资源组从维护模式中除去,请遵循以下步骤:

1 验证 NNMi 是否在正确运行:

ovstatus -c

所有 NNMi 服务应当显示状态正在运行。

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 于维护模式中描述了此文件。

在 HA 群集中维护 NNMi

启动和停止 NNMi

NNMi 正以 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。对于正常运行,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UNIX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 (HP-UX 或 Linux 上的 NIS, Solaris 上的 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:

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 地址的永久非生产许可证密钥。

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 (如第 318 页的将 HA 资源组置于维护模式中所述)。

Δ

- 3 停止 NNMi HA 资源组:
 - Windows:

```
%NnmInstallDir%\misc\nnm\ha\nnmhastoprg.ovpl NNM \
<资源组>
```

• UNIX:

\$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
- UNIX: \$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 UNIX 联机帮助页。

- 6 更改群集配置以使用新 IP 地址:
 - MSFC:

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。

• Serviceguard:

在主动 HA 群集节点上,编辑 /etc/cmcluster/<*资源组*>/<*资源组*>.cntl 文件, 以将 IP[0]=<旧 IP 地址> 替换为 IP[0]=<新 IP 地址>。(如果将 NNMi HA 资源 组移到了不同的子网,还要将 SUBNET[0]=<旧子网掩码> 替换为 SUBNET[0]=<新 子网掩码>。) 然后使用 cmapplyconf 更新所有其他系统。

• *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 如第 115 页的许可 NNMi 中所述安装 NNMi HA 资源组的新虚拟 IP 地址的永久非生 产许可证密钥。

2011年3月

- 8 使用主动节点上 LicFile.txt 文件的新信息更新共享磁盘上的 licenses.txt 文件。 执行以下某个操作:
 - 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 目录的 licenses.txt 中。

在主动节点上, LicFile.txt 文件位于以下位置:

• *Windows*: %AUTOPASS HOME%\data\LicFile.txt

要确定 %AUTOPASS HOME% 值,请检查计算机的系统环境变量。

• UNIX: /var/opt/OV/HPOvLIC/LicFile.txt

在共享磁盘上, licenses.txt 文件的示例位置如下:

- Windows: S:\NNM\licenses.txt
- UNIX: /nnmount/NNM/licenses.txt
- 9 启动 NNMi HA 资源组:
 - Windows:

%NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM \
<资源组>

• UNIX:

\$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 服务应当显示状态正在运行。

11 使 NNMi HA 资源组脱离维护模式(如第 318 页的将 HA 资源组从维护模式中除去中所述)。

停止 NNMi 而不执行故障切换

需要执行 NNMi 维护时,可以在主动群集节点上停止 NNMi,而不故障切换到当前被动节 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 (如第 318 页的将 HA 资源组置于维护模式中 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切换的方式停止 NNMi,则遵循以下步骤以重新启动 NNMi 和 HA 监视:

1 启动 NNMi:

ovstart -c

2 验证该 NNMi 是否已正确启动:

ovstatus -c

所有 NNMi 服务应当显示状态正在运行。

3 使 NNMi HA 资源组脱离维护模式(如第 318 页的将 HA 资源组从维护模式中除去中 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。

从 HA 群集取消配置 NNMi

从 HA 群集取消配置 NNMi

从 HA 群集除去 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,或者可以从该节点卸载 NNMi。

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 群集中完全除去 NNMi,请在群集中的所有节点上 取消配置 HA 功能。

要在 HA 群集中完全取消配置 NNMi,请遵循以下步骤:

- 1 确定 HA 群集中的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

• UNIX:

\$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。

2011年3月

- 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
```

• UNIX:

\$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
-config NNM -get NNM ADD ON PRODUCTS

命令输出以格式 <iSPI PM 名称>[主机名列表]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>

• UNIX:

\$NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM \ <资源组>

此命令除去对共享磁盘的访问,但不取消配置磁盘组或卷组。

5 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:

如果不打算重新配置 NNMi HA 资源组,就不需要保存这些文件的副本,此时就可以 删除它们。

- *MSFC*:在Windows Explorer 中,删除 %NnmDataDir%\hacluster\<*资源组*>\ 文件夹。
- Serviceguard:

```
rm -rf /var/opt/OV/hacluster/<资源组>
rm -rf /etc/cmcluster/<资源组>
```

- *VCS*:
 - rm -rf /var/opt/OV/hacluster/<资源组>
- RHCS:
 - rm -rf /var/opt/OV/hacluster/<资源组>

6 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

• UNIX:

```
$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。

- 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>

• UNIX:

\$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,从HA群集中取消配置 NNMi:
 - Windows:

%NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM \ <资源组>

• UNIX:

\$NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM \ <*咨源组*>

此命令除去对共享磁盘的访问,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:

如果不打算重新配置 NNMi HA 资源组,就不需要保存这些文件的副本,此时就可以 删除它们。

- *MSFC*:在Windows Explorer 中, 删除 %NnmDataDir%\hacluster\<资源组>\文件夹。
- Serviceguard:

rm -rf /var/opt/OV/hacluster/*<资源组>* rm -rf /etc/cmcluster/*<资源组*>

• *VCS*:

rm -rf /var/opt/OV/hacluster/<资源组>
• RHCS:

rm -rf /var/opt/OV/hacluster/<资源组>

- 10 卸载共享磁盘。
 - 如果要在某个时间重新配置 NNMi HA 群集,则可以使磁盘保留其当前状态。
 - 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(如第 325 页的不以 HA运行带现有数据库的 NNMi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,请遵循以下步骤:

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 (UNIX),检查 ovspmd 过程的状态。

2 在当前节点(将要不以 HA 运行 NNMi 的节点)上,验证 NNMi 是否未在运行:

ovstop

Λ

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 UNIX) 激活磁盘组:

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 Windows 资源管理器。
 - UNIX: mount /dev/vgnnm/lvnnm /nnmmount
- 5 将 NNMi 文件从共享磁盘复制到该节点:
 - Windows:

%NnmInstallDir%\misc\nnm\ha\nnmhadisk.ovpl NNM \ -from <HA 安装点>

• UNIX:

\$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。
 - UNIX: umount /nnmmount
- 7 (仅 UNIX) 取消激活磁盘组:

vgchange -a n *<磁盘组*>

8 如第 115 页的许可 NNMi 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

要对 NNMi 应用补丁,请在 HA 维护模式中工作。遵循以下步骤:

- 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
```

• UNIX:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
-group <资源组> -activeNode
```

2 在主动节点上,使 NNMi HA 资源组进入维护模式(如第 318 页的将 HA 资源组置于维护模式中所述)。

包括 NORESTART 关键字。

3 在所有被动节点上,使 NNMi HA 资源组进入维护模式(如第 318 页的将 HA 资源组 置于维护模式中所述)。

包括 NORESTART 关键字。

- 4 在主动节点上,遵循以下步骤:
 - a 停止 NNMi:

ovstop -c

- b 通过执行磁盘副本,备份共享磁盘。
- c *可选*。使用 nnmbackup.ovpl 命令或另一个数据库命令, 以备份所有 NNMi 数据。 例如:

```
nnmbackup.ovpl -type offline -scope all -target nnmi_backups
```

有关此命令的详细信息,请参阅第 347 页的 NNMi 备份和恢复工具。

- d 对该系统应用相应的 NNMi 和 NNM iSPI 补丁。
- e 启动 NNMi:

ovstart -c

f 验证 NNMi 是否正确启动:

ovstatus -c

所有 NNMi 服务应当显示状态正在运行。

Λ

- 5 在每个被动节点上,对该系统应用相应的补丁。
- 不要在辅助(备份)群集节点上运行 ovstart 或 ovstop 命令。
- 6 在所有被动节点上,使 NNMi HA 资源组脱离维护模式(如第 318 页的将 HA 资源组 从维护模式中除去中所述)。
- 7 在主动节点上,使 NNMi HA 资源组脱离维护模式(如第 318 页的将 HA 资源组从维 护模式中除去中所述)。

将以 HA 运行的 NNMi 从 NNMi 9.0x 升级到 NNMi 9.10

执行适合您环境的步骤:

- 第 327 页的在 Windows、Linux 或 Solaris 操作系统上升级带有嵌入式数据库的 NNMi
- 第 329 页的在 HP-UX 操作系统上升级带有嵌入式数据库的 NNMi
- 第 330 页的在所有受支持的操作系统上升级带 Oracle 的 NNMi

在 Windows、 Linux 或 Solaris 操作系统上升级带有嵌入式数据库 的 NNMi

从 NNMi 9.10 起,在 Linux 操作系统上不再支持 Serviceguard。如果 NNMi 当前正在以 Serviceguard HA 运行,则无法执行本部分的过程。请改为从 HA 取消配置 NNMi(如第 322 页的从 HA 群集取消配置 NNMi 中所述),在所有节点上升级 NNMi,然后将 NNMi 配置为在受支持的 HA 产品下运行(如第 305 页的为 HA 配置 NNMi 中所述)。或者,可 以配置 NNMi 执行 NNMi 应用程序故障切换,如第 297 页的在高可用性群集中配置 NNMi 中所述。

在 Windows、Linux 或 Solaris 操作系统上,要从以 HA 运行的 NNMi 9.0x 升级到以 HA 运行的 NNMi 9.10,请升级被动节点,从主动节点故障切换到被动节点,然后升级下一个 节点。遵循以下步骤:

- 1 确保 NNMi 9.0x 配置在所有 HA 节点之间是一致的,方法是依次强制故障切换到每个 被动节点。
- 2 确定 NNMi 9.0x 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

• UNIX:

\$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \ -group *<资源组*> -activeNode

此过程的其余部分将当前主动节点称为服务器 X,将当前被动节点称为服务器 Y。

- 3 在服务器 Y 上,升级 NNMi:
 - a 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

 UNIX: \$NnmDataDir/hacluster/<资源组>/maintenance 文件可以为空。

- b 如第 391 页的升级自 NNMi 9.0x 中所述将 NNMi 升级为当前版本。
- c 验证升级是否正确完成。
- d 将所有加载项 NNM iSPI 升级到版本 9.10。

有关信息,请参阅每个 NNM iSPI 的文档。

如果您的环境包含独立的 NNM iSPI,则还必须将这些产品升级到版本 9.10 以使运行正常。可以在完成此过程之后执行这些升级。

- e 删除维护文件:
 - Windows: %NnmDataDir%\hacluster\<资源组>\maintenance
 - UNIX: \$NnmDataDir/hacluster/<资源组>/maintenance
- 4 如果 HA 群集包括多个被动节点,则对每个被动节点重复步骤 3。
- 5 在服务器 X 上,升级 NNMi:

NNMi 在故障切换到服务器 Y 期间数据库升级时,会有大约 20 到 60 分钟时间处于不可用状态。可以将此步骤安排在便于进行系统维护的时间执行。

a 强制故障切换到服务器 Y。

这时,共享磁盘上的 NNMi 数据库升级到新 NNMi 产品版本的格式。

- b 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
 - UNIX: \$NnmDataDir/hacluster/<资源组>/maintenance 文件可以为空。
- c 如第 391 页的升级自 NNMi 9.0x 中所述将 NNMi 升级为当前版本。
- d 验证升级是否正确完成。
- e 将所有加载项 NNM iSPI 升级到版本 9.10。

有关信息,请参阅每个 NNM iSPI 的文档。

- f 删除维护文件:
 - Windows: %NnmDataDir%\hacluster\<资源组>\maintenance
 - UNIX: \$NnmDataDir/hacluster/<资源组>/maintenance

6 可选。从服务器 Y 强制故障切换到服务器 X,以便升级之前为主动的节点仍然是主动 节点。

在 HP-UX 操作系统上升级带有嵌入式数据库的 NNMi

在 HP-UX 操作系统上, NNMi 的升级包括将 Postgres 数据库从 32 位版本迁移到 64 位版本。由于这个原因, NNMi 必须在升级过程中停止操作。



NNMi 在此升级过程中将有大约 30 到 60 分钟时间不可用。

在 HP-UX 操作系统上,要从以 HA 运行的 NNMi 9.0x 升级到以 HA 运行的 NNMi 9.10, 升级主动节点以更新嵌入式数据库,然后在 NNMi 仍在维护模式中时升级被动节点。遵循 以下步骤:

- 1 确保 NNMi 9.0x 配置在所有 HA 节点之间是一致的,方法是依次强制故障切换到每个 被动节点。
- 2 确保所有节点都在运行 NNMi 9.0x 补丁 2 (9.01) 或 NNMi 9.0x 的更高版本。

如有必要,将每个系统升级到最新的 NNMi 9.0x 合并补丁。按照《NNMi 部署参考》 最新 NNMi 9.0x 版本中的"在高可用性群集中配置 NNMi"一章的"将以 HA 运行 的 NNMi 从 NNMi 8.1x 升级到 NNMi 9.01"部分中的说明操作。

3 确定 NNMi 9.0x HA 群集中的哪个节点是主动节点:

\$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \ -group <资源组> -activeNode

此过程的其余部分将当前主动节点称为服务器 X,将当前被动节点称为服务器 Y。

4 在服务器 X 上,通过创建以下维护文件,禁用 HA 资源组监视:

\$NnmDataDir/hacluster/<资源组>/maintenance

文件可以为空。

- 5 在服务器 X 上, 升级 NNMi:
 - a 如第 391 页的升级自 NNMi 9.0x 中所述将 NNMi 升级为当前版本。 数据库升级在此步骤中发生。
 - b 要验证升级是否正确完成,请输入以下命令:

ovstart

所有 NNMi 服务应当显示状态正在运行。

c 将所有加载项 NNM iSPI 升级到版本 9.10。

有关信息,请参阅每个 NNM iSPI 的文档。

如果您的环境包含独立的 NNM iSPI,则还必须将这些产品升级到版本 9.10 以使运行正常。可以在完成此过程之后执行这些升级。

- 6 在服务器 Y 上,升级 NNMi:
 - a 如第 391 页的升级自 NNMi 9.0x 中所述将 NNMi 升级为当前版本。
 - b 验证升级是否正确完成。
 - c 将所有加载项 NNM iSPI 升级到版本 9.10。

有关信息,请参阅每个 NNM iSPI 的文档。

- 7 如果 HA 群集包括多个被动节点,则对每个被动节点重复步骤 6。
- 8 在服务器 X 上, 删除维护文件:

\$NnmDataDir/hacluster/<资源组>/maintenance

在所有受支持的操作系统上升级带 Oracle 的 NNMi

要在 Oracle 环境中升级以 HA 运行的 NNMi,请执行第 327 页的在 Windows、Linux 或 Solaris 操作系统上升级带有嵌入式数据库的 NNMi 中描述的步骤。

对 HA 配置进行故障诊断

本部分包括以下主题:

- 第 331 页的常见配置错误
- 第 332 页的 HA 资源测试
- 第 333 页的常规 HA 故障诊断
- 第 335 页的特定于 NNMi 的 HA 故障诊断
- 第 340 页的特定于 NNM iSPI 的 HA 故障诊断

常见配置错误

以下列出了某些常见的 HA 配置错误:

- 磁盘配置不正确
 - VCS:如果探查不到资源,则配置一定存在某种错误。如果探查不到磁盘,则操作 系统可能不再能访问此磁盘。
 - 手动测试磁盘配置,并根据 HA 文档确认此配置是适当的。
- 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。
- MSFC: 网络配置错误

如果网络通信量流经多个 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)。
- 故障切换或 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切换。

MSFC: 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。如果资源组在系统上处于联机状态并不久便发生 故障切换,可以通过维护模式在系统上保持资源组,以查明实际故障点。

• 不查看群集日志 (群集日志可显示很多常见错误)。

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 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,请遵循以下步骤:

- 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,如测试。

- 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切换到被动群集节点,以验证 HA 群集是否能够正确进行故障 切换。
 - c 从新的主动群集节点故障切换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切换,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 如第 315 页的配置 SAN 或已实际连接的磁盘中所述配置共享磁盘。
- 6 测试与共享磁盘的连接:
 - a 如第 316 页的将共享磁盘移到 NNMi HA 资源组中中所述,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切换到被动群集节点,以验证 HA 群集是否能够正确进行故障 切换。

- c 从新的主动群集节点故障切换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切换,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。

常规 HA 故障诊断

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
- 资源托管子系统进程意外停止 (Windows Server 2008 R2)
- 产品启动超时 (Solaris)
- 主动群集节点上的日志文件未更新
- 无法在特定群集节点上启动 NNMi HA 资源组

错误:参数个数不正确

产品 Perl 模块的名称对于大多数 NNMi 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 2008 R2)

在运行 Windows Server 2008 R2 操作系统的计算机上启动 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 2008 R2,可访问 http://support.microsoft.com/kb/978527 以查看此 文章。

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 (Solaris)

一个或多个 /var/adm/messages* 文件包含与以下示例类似的消息:

VCS 错误 V-16-1-13012 线程(...) 资源(<*资源组*>-app): 联机过程未在预期时间内完成。

此消息表示产品未在 Veritas 超时值的时限中完全启动。 NNMi 提供的 HA 配置脚本将此 超时定义为 15 分钟。

要在 Solaris 操作系统上更改 Veritas 超时值,请按顺序运行以下命令:

```
/opt/VRTSvcs/bin/haconf -makerw
/opt/VRTSvcs/bin/hares -modify <资源组>-app OnlineTimeout <秒数>
/opt/VRTSvcs/bin/haconf -dump -makero
```

主动群集节点上的日志文件未更新

此情况是正常的。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, 查看位于由 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 命令不能正确地启动、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态。
 - 查看事件查看器日志中是否有任何错误。
- Serviceguard :

查看 <资源组>.cntl.log 文件和 syslog 文件中是否有错误。最常见的问题是使系统处于无法添加资源的状态,例如:某磁盘组配置错误,因此无法激活它。

/etc/cmcluster/<*资源组*>/*<资源组*>.cntl.log

- VCS:
 - 运行 /opt/VRTSvcs/bin/hares -state 以查看资源状态。
 - 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。
 资源按代理类型参考,例如: IP*.log、Mount*.log和 Volume*.log。
- RHCS:

查看 <资源组>.cntl.log 文件和 syslog 文件中是否有错误。最常见的问题是使系统处于无法添加资源的状态,例如:某磁盘组配置错误,因此无法激活它。

/etc/cmcluster/*<资源组*>/*<资源组*>.cntl.log

2011年3月

如果找不到问题根源,通过使用 HA 产品命令,可以手动启动 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。
 - Serviceguard: 运行 /usr/sbin/cmmodnet 以添加 IP 地址。
 - 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>
```

• UNIX:

```
$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 NNMi 的 HA 故障诊断

本部分中的主题仅适用于 NNMi 的 HA 配置。它们包括:

- 在取消配置所有群集节点之后,对 NNMi 重新启用 HA
- NNMi 未以 HA 正确启动
- 故障切换之后看不到对 NNMi 数据的更改
- nmsdbmgr 在配置 HA 后未启动
- pmd 在配置 HA 后未启动
- NNMi 仅在一个 HA 群集节点上正确运行 (Windows)
- 磁盘故障切换未执行
- 无法访问共享磁盘 (Windows)
- 共享磁盘不包含当前数据
- 故障切换之后辅助节点找不到共享磁盘文件

在取消配置所有群集节点之后,对 NNMi 重新启用 HA

所有 NNMi 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>
```

• UNIX:

```
$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,请参阅第 341 页的 NNMi HA 配置文件。

NNMi 未以 HA 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
 - UNIX: \$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 服务应当显示状态正在运行。如果不是这种情况,则诊断未正确启动的进程。

- 4 完成故障诊断之后,删除维护文件:
 - Windows: %NnmDataDir%\hacluster\<资源组>\maintenance
 - UNIX: \$NnmDataDir/hacluster/<资源组>/maintenance

故障切换之后看不到对 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=<<u>虚拟主机名</u>>
- 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/installDir/nonOV/jboss/nms/server/ nms/data
- HA LOCALE=C

有关 ov.conf 文件的位置,请参阅第 341 页的 NNMi HA 配置文件。

nmsdbmgr 在配置 HA 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 命令之后启动 NNMi 而造成的。在此案例中, ov.conf 文件中的 HA POSTGRES DIR 条目指定共享磁盘上的嵌入式数据库的位置,但此位置对 NNMi 不可用。

要解决此问题,请遵循以下步骤:

- 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
 - UNIX: \$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>

• UNIX:

\$NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM \ -to <HA 安装点>



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,请参阅第 336页的在取消配置所有群集节点之后,对 NNMi 重新启用 HA。

- 3 启动 NNMi HA 资源组:
 - Windows:

%NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM \
<资源组>

• UNIX:

\$NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM \ <资源组>

4 启动 NNMi:

ovstart

5 验证 NNMi 是否正确启动:

```
ovstatus -c
```

所有 NNMi 服务应当显示状态正在运行。

- 6 完成故障诊断之后,删除维护文件:
 - Windows: %NnmDataDir%\hacluster\<资源组>\maintenance
 - UNIX: \$NnmDataDir/hacluster/<资源组>/maintenance

pmd 在配置 HA 后未启动

此情况通常是在配置错误(例如未正确设置共享磁盘)之后发生的。 ovjboss 进程未完全 启动时, pmd 进程将失败。

查看以下日志文件:

- Windows: %HA MOUNT POINT%\NNM\dataDir\log\nnm\jbossServer.log
- UNIX: \$HA MOUNT POINT/NNM/dataDir/log/nnm/jbossServer.log

NNMi 仅在一个 HA 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 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确运行。

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。

磁盘故障切换未执行

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 不启动故障切换。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

以无文本方式响应 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, 请遵循第 315 页的手动准备共享磁 盘中的步骤操作。

故障切换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,请遵循以下步骤:

- 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
 - UNIX: \$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>
```

• UNIX:

\$NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM \ -to <HA 安装点>



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,请参阅第 336 页的在取消配置所有群集节点之后,对 NNMi 重新启用 HA。

- 5 启动 NNMi HA 资源组:
 - Windows:

%NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM \
<资源组>

• UNIX:

\$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 服务应当显示状态正在运行。

- 8 完成故障诊断之后,删除维护文件:
 - Windows: %NnmDataDir%\hacluster\<资源组>\maintenance
 - UNIX: \$NnmDataDir/hacluster/<资源组>/maintenance

特定于 NNM iSPI 的 HA 故障诊断

有关对以 HA 运行的 NNM iSPI 进行故障诊断的信息,请参阅该 NNM iSPI 的文档。



NNMi HA 配置文件

表 26 列出 NNMi 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
- UNIX: \$NnmDataDir/shared/nnm/conf

文件名	描述
ov.conf	由 nnmhaclusterinfo.ovpl 命令更新,以描述 NNMi HA 实施。 NNMi 进程读取 此文件以确定 HA 配置。
nnmdatareplicator.conf	由 nnmdatareplicator.ovpl 命令使用,以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。

表 26 NNMi HA 配置文件

NNMi 提供的 HA 配置脚本

表 27 和表 28 列出 NNMi 附带的 HA 配置脚本。表 27 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
- UNIX: \$NnmInstallDir/misc/nnm/ha

表 27 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。

表 27 NNMi HA 配置脚本 (续)

脚本名称	描述	
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。	
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。	

表 28 中列出的 NNMi 提供的脚本由第 341 页的表 27 中列出的脚本使用。不要直接运行 表 28 中列出的脚本。

表 28 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 Serviceguard 配置,由 < 资源组 >.cntl 使用。 对于 VCS 配置,由 VCS 用于启动、停止和监视脚本。(nnmhargconfigure.ovpl 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 HA 配置日志文件

以下日志文件适用于 NNMi 管理服务器上的 NNMi 和加载项 NNM iSPI 的 HA 配置:

- Windows 配置:
 - %NnmDataDir%\tmp\HA_nnmhaserver.log
 - -- %NnmDataDir%\log\haconfigure.log
- UNIX 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\jbossServer.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。
- HP-UX 运行时:
 - /etc/cmcluster/<资源组>/<资源组>.cntl.log
 这是资源组的日志文件。
 - /var/adm/syslog/syslog.log
 - /var/adm/syslog/OLDsyslog.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/jbossServer.log

• Linux 或 Solaris VCS 运行时:

资源	日志文件	
< <i>资源组</i> >-app	 /var/VRTSvcs/log/Application_A.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/jbossServer.log /var/adm/messages* 	
< <i>资源组</i> >-dg < <i>资源组</i> >-volume < <i>资源组</i> >-mount	 /var/VRTSvcs/log/DiskGroup_A.log /var/VRTSvcs/log/Volume_A.log /var/VRTSvcs/log/Mount_A.log /var/adm/messages* 	
< <i>资源组</i> >-ip	/var/VRTSvcs/log/IP_A.log/var/adm/messages*	

对于与 HA 资源相关的特定于操作系统的问题,请查看 /var/adm/messages* 文件。对于 <*资源组*>-app,请查看 关于无法启动进程的消息。

- RCHS 的 *Linux* 运行时:
 - /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/jbossServer.log

维护 NNMi

本部分包含以下各章:

- NNMi 备份和恢复工具
- 维护 NNMi
- NNMi 日志记录
- 更改 NNMi 管理服务器
- 在 Xen 虚拟化环境中运行 NNMi

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
- 备份 NNMi 数据
- 恢复 NNMi 数据
- 备份和恢复策略
- 只备份和恢复嵌入式数据库

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 丢弃 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 UNIX 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 数据库中部分或所有表复制到指定目标目录。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。



Α

如果您的 NNMi 实施使用 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或不包括来自您的网络环境中安装的任何 NNM iSPI 的数据。详 细信息请查看每个 NNM iSPI 附带的文档。

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 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%, UNIX 上为 \$NNM DB)。可用 nnmbackup.ovpl 定期备份 NNMi 数据库。

备份类型

NNMi 备份命令支持两类备份:

发生在 NNMi 运行时的联机备份。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 备份命令提供用来定义备份多少 NNMi 的几个范围。

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,为表 29 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 控制台的资产工作区中的信息。因为网络 拓扑依赖用于搜索该拓扑的配置,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,为表 29 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,是在表 29 中列出的文件系统内的 NNMi 配置信息和表 30 中列出的 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。

表 29 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
%NnmInstallDi%r\nonOV\jboss\nms\server\nms\conf \$NnmInstallDir/nonOV/jboss/nms/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
 Windows Server 2008: <	许可证信息
%NnmDataDir%\NNMVersionInfo \$NnmDataDir/NNMVersionInfo	NNMi 版本信息文件
%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 应用程序故障切换或高可用性环境中与另 一个 NNMi 管理服务器共享的文件。

2011年3月

表 30 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。

▶ 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,从原始 NNMi 管理服务器卸载 NNMi。

- 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态。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。

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。

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)
- 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。

最佳实践 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。

1

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)
- 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,请参阅第 115 页的许可 NNMi。

备份和恢复策略

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 的状态正确。例如:

```
nnmbackup.ovpl -force -type online -scope all -archive
    -target nnmi backups\periodic
```

如果需要在硬件故障之后恢复 NNMi 数据,则遵循以下步骤:

- 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级别。
- 3 恢复 NNMi 数据:
 - 如果恢复 NNMi 管理服务器满足第 352 页的相同系统恢复中列出的要求,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,但满足第 353 页的不同 系统恢复中列出的要求,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(如第349页的备份范围中所述)。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

要将这备份恢复到同一 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,并确保符合在第 353 页的不同系统恢复中列出的要求。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 实施使用 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 命令只执行联机备份。至少 nmsdbmgr 服务必须正在运行。

最佳实践 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 UNIX 联机帮助页。

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:

- 第358页的管理自定义轮询器采集导出
- 第359页的管理事件操作
- 第 362 页的使用 trapFilter.conf 文件阻止事件
- 第 363 页的配置与 NNMi 控制台的仅 HTTPS 通信
- 第 363 页的修改 NNMi 标准化属性
- 第 365 页的修改并发 SNMP 请求数
- 第 365 页的 NNMi 自监视
- 第 366 页的抑制对特定节点使用搜索协议
- 第 369 页的抑制对大型交换机使用 VLAN 索引
- 第 371 页的了解对 NAT 环境中的管理地址的 ICMP 轮询

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,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*。

CustomPoller 功能需要您在处理文件时将文件从导出目录中删除。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: %NNM_DATA%\shared\nnm\databases\custompoller\export
- UNIX: \$NNM_DATA/shared/nnm/databases/custompoller/export

要更改 NNMi 写入自定义轮询器文件的目录,请遵循以下步骤:

- 1 编辑以下文件:
 - Windows: %NNM PROPS%\nms-custompoller.properties
 - UNIX: \$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,请遵循以下步骤.

- 1 编辑以下文件:
 - Windows: %NNM_PROPS%\nms-custompoller.properties
 - UNIX: \$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 对每个 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,请遵循以下步骤:

- 1 编辑以下文件:
 - Windows: %NNM PROPS%\nms-custompoller.properties
 - UNIX: \$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。

设置并发操作数目

在 Solaris NNMi 管理服务器上增大并发操作数目会导致 NNMi 性能下降。

要修改 NNMi 可以运行的并发操作数目,请遵循以下步骤:

- 1 编辑以下文件:
 - Windows: %NNM_PROPS%\shared\nnmaction.properties
 - UNIX: \$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
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,请遵循以下步骤:

- 1 编辑以下文件:
 - Windows: %NNM PROPS%\shared\nnmaction.properties
 - UNIX: \$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

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

要修改在 Windows NNMi 管理服务器上运行操作服务器的用户名,请更改 HP NNM Action Server 服务的 LogOn 属性。
要修改运行操作服务器的用户名(适用于 HP-UX、Solaris 和 Linux NNMi 管理服务器), 请遵循以下步骤:

- 1 编辑以下文件: \$NNM PROPS/shared/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 使系统运行操作服务器 (而不是默认值),请将该行作如下更改:

com.hp.ov.nms.events.action.userName=system

确保删除位于行开头的 #! 字符。

3 保存更改。

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。

对于 Solaris NNMi 管理服务器,如果 NNMi 运行状况信息显示操作队列大小正在增长,则减少最大内存大小以改进性能。

要修改这些限制,请遵循以下步骤:

- 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。

使用 trapFilter.conf 文件阻止事件

假定流经 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。

如果发生这种情况,NNMi 会生成 TrapStorm 事件,指示此事件被阻止。NNMi 还可能生成主要运行状况消息,指示事件比率较高并将阻止事件。

为对此进行补救,可以尝试使用 nnmtrapd.conf 文件阻止事件进入 NNMi 中以减少事件 流量。但是,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 UNIX 联机帮助页。

与使用 nnmtrapd.conf 文件相比,有更好的解决方案可以解决此问题。NNMi 可提供用于 阻止 NNMi 事件管道中较早事件的过滤机制,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。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 UNIX 联机帮助页。

配置与 NNMi 控制台的仅 HTTPS 通信

阻止对 NNMi 控制台的 HTTP 访问的最有效方法是将 NNMi 管理服务器放置到防火墙后面,防火墙只允许对受保护系统进行 HTTPS 访问。

对于使用 Web 服务与 NNMi 通信并且仅支持 HTTP 的那些集成,用于阻止 HTTP 访问的 防火墙配置可能导致出现问题。请参阅集成产品的文档,以了解它是否支持 HTTPS。

作为安全性不高的方法,可通过完成以下步骤,将 NNMi 控制台访问请求从 HTTP 端口重 定向到 HTTPS 端口:

- 1 编辑以下文件:
 - Windows: %NNM_PROPS\nms-ui.properties
 - UNIX: \$NNM_PROPS/nms-ui.properties
- 2 搜索字符串 https 以找到包含以下行的文本块:
- #! com.hp.ov.nms.ui.https.only=false
- 3 取消注释并编辑以下行,以呈现以下内容:

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

4 重新启动 ovjboss:

```
ovstop ovjboss
ovstart ovjboss
```

对于一些交叉启动回到 NNMi 的应用程序,设置此属性以针对 NNMi 控制台将 HTTP 请求重定向为 HTTPS 会导致问题。如果遇到这些问题,则禁用此 HTTPS 重定向。

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、排序和过滤操作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 搜索之前进行这些更改。HP 建议您在部署期间(但在运行初始搜索之前)对这一部分中的 设置进行调整。

如果运行初始搜索后又决定更改标准化属性,则可以运行 nnmnoderediscover.ovpl -all 脚本以启动完整搜索。有关详细信息,请参阅 nnmnoderediscover.ovpl 参考页或 UNIX 联机帮助页。

可以更改以下属性:

- 将搜索的节点名标准化为 UPPERCASE、 LOWERCASE 或 OFF。
- 将搜索的主机名标准化为 UPPERCASE、 LOWERCASE 或 OFF。

要更改标准化属性,请遵循以下步骤:

- 1 编辑以下文件:
 - Windows: %NNM PROPS%\nms-topology.properties
 - UNIX: \$NNM PROPS/nms-topology.properties
- 2 要配置 NNMi 以标准化搜索的名称,请查找类似以下内容的行:

#!com.hp.ov.nms.topo.NAME_NORMALIZATION=OFF

a 取消注释属性:

com.hp.ov.nms.topo.NAME_NORMALIZATION=OFF

要取消注释属性,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 以标准化搜索的主机名,请查找类似以下内容的行:

#!com.hp.ov.nms.topo.NAME_NORMALIZATION=OFF

a 取消注释属性:

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。

在初始搜索之后更改标准化属性

在初始搜索之后更改标准化属性将导致 NNMi 与属性更改不一致,直到进行下一次搜索。 要对此进行补救,请在更改 NNMi 标准化属性之后运行 nnmnoderediscover.ovpl -all 脚本以启动完整搜索。

在 NNMi 完成完整搜索之后,下面所示的行为应该恢复正常。这些示例并不是穷尽的,目 的是为更改 NNMi 标准化属性时要考虑的事项提供几个示例。

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,这将导致搜索速度加快。但是,如果将值设置得太高,会增加丢弃 响应的风险,并使搜索的准确度降低。

如果需要修改此限制,则遵循以下步骤:

- 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 取消注释属性: com.hp.ov.nms.comm.snmp.maxConcurrentRequests=3

要取消注释属性,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。
- 在 NNMi 管理服务器上运行 ovstart 命令。

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。
- 要获取详细自监视报告,请选择工具 > NNMi 系统运行状况报告
- 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。通过完成以下步骤,可以禁用此警告消息:

- 1 编辑以下文件:
 - Windows: %NNM_PROPS\nms-ui.properties
 - UNIX: \$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 取消注释并编辑以下行,以呈现以下内容:

com.hp.nms.ui.health.disablewarning==true

- 4 重新启动 ovjboss:
 - a ovstop ovjboss
 - b ovstart ovjboss

抑制对特定节点使用搜索协议

NNMi 使用几个协议来搜索网络设备之间的第2层连接。有很多已定义的搜索协议。例如, Link Layer Discovery Protocol (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 Discovery Protocol (CDP)。

可以配置 NNMi 以抑制针对指定设备的搜索协议采集。有些特殊情况可以通过抑制搜索协议采集来补救。

下面是一些示例:

• Enterasys 设备:使用 SNMP 从一些 Enterasys 设备上的 Enterasys Discovery Protocol (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,如抑制使用搜索协议采集中 所示。



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)来搜索第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,如抑制使用搜索协议采集中所示。

抑制使用搜索协议采集

如果需要抑制此采集,请遵循以下步骤:

- 1 创建以下文件:
 - Windows: %NnmDataDir%\shared\nnm\conf\disco\disco.SkipXdpProcessing
 - UNIX: \$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 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.



抑制一个或多个节点的搜索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。

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。

如果在任何 Enterasys 设备上运行了 set snmp 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 使用搜索协议时,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 UNIX 联机帮助页。

管理对 NAT 环境中的管理地址的 ICMP 轮询

本部分的信息未包含在 HP NNMi 9.0x 补丁 2 的《NNMi 部署参考》的已出版版本中。可 以与需要使用该新功能的客户共享此信息。

在网络地址转换 (NAT) 环境中,防火墙阻止 NNMi 与使用 NAT 节点上的 IP 地址 (专用 IP 地址)的 NAT 节点进行通信。要对此进行补救,请使用 NAT 地址 (公共 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。要让 NNMi 搜索 NAT 环境中的节点,必须将 NAT 地址作为搜索种子添加到 NNMi。NNMi 使用此 NAT 地 址进行 SNMP 通信,即使该地址不在节点的 ipAddressTable 中。

应用NNMi 9.0x 补丁2 之后,可以配置新NNMi 功能以便对节点的SNMP 地址进行 ICMP 轮询。结果将是更为可靠准确的分析。使用此新功能可避免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

要在 NAT 环境中启用 ICMP 管理地址轮询,请执行以下操作:

- 1 启用 ICMP 管理地址轮询。请参阅 NNMi 帮助中的"默认监视"。
- 2 如下设置系统属性:
 - a 切换到以下目录:

Windows: %NNM PROPS%

UNIX: \$NNM PROPS

- b 创建以下属性文件:*我的属性文件*.properties。用任何文件名代替*我的属性文件*,但是必须使用.properties文件扩展名。
- c 将以下行添加到我的属性文件.properties 文件:

com.hp.ov.nnm.useSnmpAgentManagementAddressState = true

d 重新启动 NNMi 管理服务器。

ovstop -c

ovstart -c

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。

对 NNMi 的更改方式

完成第 368 页的启用对 NAT 环境中的管理地址的 ICMP 轮询中显示的步骤之后, NNMi 发生如下更改:

- "代理 ICMP 状态"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 状态的显示位置。 NNMi 还更改它确定 SNMP 代理状态 的方式。

表 33 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 地址状态轮询操作。表 33 中加阴影的第一行显示默认配置。

表 31

ICMP 管理地址 轮询	ICMP 故障轮询	代理 ICMP 状态	IP 地址状态
已启用	已禁用	已轮询	未轮询

表 31

ICMP 管理地址 轮询	ICMP 故障轮询	代理 ICMP 状态	IP 地址状态
已启用	已启用	己轮询	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

表 34 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。

表:	32
----	----

正在响应	正在响应	正常
响应	未响应	轻微
未响应	响应	紧急
未响应	未响应	紧急

启用管理地址 ICMP 轮询的情况下, APA 现在会在生成总结和事件时考虑管理地址 ICMP 响应和 SNMP 代理响应。

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 层搜索。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,如第 370 页的抑制使用 VLAN 索引中所示。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 进行文件,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 索引在所有设备上采集整个 FDB 表。

抑制使用 VLAN 索引

如果需要禁用此 vlan 索引,请遵循以下步骤:

- 1 创建以下文件:
 - Windows: %NnmDataDir%\shared\nnm\conf\disco\disco.NoVLANIndexing
 - UNIX: \$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。



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。

ovjboss 服务在启动时读取 disco.NoVLANIndexing 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。

有关详细信息,请参阅 disco.Disco.NoVLANIndexing 参考页或 UNIX 联机帮助页。

了解对 NAT 环境中的管理地址的 ICMP 轮询

在网络地址转换 (NAT) 环境中,防火墙阻止 NNMi 与使用 NAT 节点上的 IP 地址 (专用 IP 地址)的 NAT 节点进行通信。要对此进行补救, NNMi 使用 NAT 地址 (公共 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。要让 NNMi 搜索 NAT 环境中的节点,必须将 NAT 地址作为搜索种子添加到 NNMi。NNMi 使用此 NAT 地 址进行 SNMP 通信,即使该地址不在节点的 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。

对 NAT 环境中的管理地址的 ICMP 轮询

NNMi 自动启用对所有节点的 ICMP 管理地址轮询,包括驻留在 NAT 环境中的节点。 NNMi 以如下方式在 NAT 环境中工作。

- "管理地址状态"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 状态的显示位置。 NNMi 还更改它确定 SNMP 代理状态 的方式。

表 33 显示 NNMi 为 ICMP 管理地址轮询和 ICMP 故障轮询设置执行的管理地址 ICMP 和 IP 地址状态轮询操作。表 33 中加阴影的第一行显示默认配置。

ICMP 管理地址 轮询	ICMP 故障轮询	管理 ICMP 地址 状态	IP 地址状态
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

表 33 ICMP 配置和生成的状态轮询

表 34 显示由 APA 针对 SNMP 代理和 ICMP 响应确定的对 SNMP 代理状态的更改和生成的事件。通过对管理地址进行 ICMP 轮询, APA 会在生成总结和事件时考虑管理地址 ICMP 响应和 SNMP 代理响应。

SNMP 代理响应	管理地址 ICMP 响应	SNMP 代理状态	生成的事件
正在响应	正在响应	正常	无
正在响应	未响应	轻微	有以下两种可能性,具体取决于其他网 络问题: ·无
			-AddressNotResponding
未响应	响应	紧急	- SNMPAgentNotResponding
未响应	未响应	紧急	有以下两种可能性,具体取决于其他网络问题: - 无 - NodeDown

表 34 确定 SNMP 代理状态和生成的事件

.

NNMi 日志记录

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,可以查阅呈现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\
- UNIX: \$NnmDataDir/log/nnm

NNMi 以 name.%g.%u.log 的格式存储这些日志文件。

- name 是日志文件的基本名称,对于大多数 NNMi 功能而言就是 nnm。
- %g 与存档的日志文件相关。如果日志文件名的 %g 部分是零(0),则说明 NNMi 会主动 将日志记录写到 name.0.%u.log 文件中。还应当看到 name.0.%u.log.lck 文件。
- %u 通常为零(0),除非父 ovjboss 进程在日志记录会话期间失败。

可通过以下任一方式将日志文件转换成存档日志文件:

- ovjboss 进程重新启动。
- 日志文件的大小超过配置的限制。

如果 ovjboss 重新启动,或者日志文件大小超过配置的限制,则上个活动日志文件将存档。 例如,文件 nnm.0.0.log 存档为文件 nnm.1.0.log。然后, NNMi 开始将日志记录写到 新的 nnm.0.0.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: 表示潜在问题的事件,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。
- CONFIG: 静态配置信息,以及 INFO 日志记录级别中包含的所有消息。

日志文件属性

通过在 logging.properties 文件中调整 NNMi 日志文件处理程序的.limit 属性,可以 控制每个服务的日志文件的大小。还可以通过在 logging.properties 文件中调整 NNMi 日志文件处理程序的.count 属性,控制存档文件数目。

logging.properties 文件在以下位置中:

- Windows: %NnmDataDir%\shared\nnm\conf\ovjboss
- UNIX: \$NnmDataDir/shared/nnm/conf/ovjboss

有关日志记录的详细信息,请参考 logging.properties 参考页或 UNIX 联机帮助页。

更改日志记录文件属性

通过调整以下日志记录参数,可以配置 NNMi 日志文件的数目和大小:

- .count
- .limit

例如,要创建数目更少而大小更大的 nnm.%g.%u.log 文件,请遵循以下步骤:

- 1 备份 logging.properties 文件,然后在任何文本编辑器中打开此文件。
- 2 通过更改以下行,将日志文件的数目减少到10,将:

com.hp.ov.nms.admin.log.NnmMainFileHandler.count = 20

更改为:

```
com.hp.ov.nms.admin.log.NnmMainFileHandler.count = 10
```

3 通过更改以下行,增加对搜索进程记录的信息量,将:

com.hp.ov.nms.admin.log.NnmMainFileHandler.limit = 50000000
更改为:

com.hp.ov.nms.admin.log.NnmMainFileHandler.limit = 100000000

- 4 通过运行以下命令,重新启动 ovjboss:
 - a ovstop ovjboss
 - b ovstart ovjboss

或者,也可以运行 NNMi support 目录中的 nnmrereadlogging.ovpl 命令:

- Windows: %NnmInstallDir%\support
- UNIX: \$NnmInstallDir/support

文件管理

应当定期监视 %NnmDataDir%\log\nnm(Windows) 或 \$NnmDataDir/log/nnm (UNIX) 中的日志文件,因为它们的大小将不断增长。删除过大的存档文件。

更改 NNMi 管理 服务器

可以在另一个系统上复制 HP Network Node Manager i Software (NNMi) 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
- 移动 NNMi 配置和嵌入式数据库
- 移动 NNMi 配置
- 恢复 NNMi 公钥证书
- 更改独立 NNMi 管理服务器的 IP 地址
- 更改 NNMi 管理服务器的主机名或域名
- 更改 Oracle 数据库实例连接信息
- 更改 NNMi 用于连接 Oracle 数据库实例的密码

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),请参阅集成 NNMi 部分的相应章节。

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
```

确保在新系统上符合第 353 页的不同系统恢复中列出的要求,然后运行与以下示例类似的 命令:

nnmrestore.ovpl -source nnmi backups\offline\newest backup



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,请使用第 379 页的移动 NNMi 配置中描述的过程,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。



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 UNIX 联机帮助页。



nnmconfigexport.ovpl 命令不保留 SNMPv3 凭证。有关详细信息,请参阅 nnmconfigexport.ovpl 参考页或 UNIX 联机帮助页。

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



如果 NNMi 管理服务器参与 NNMi 应用程序故障切换或是高可用性 (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,但不在随后重新安装之前删除(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
- 任务 2: 备份当前 nnm.keystore 文件
- 任务 3: 尝试找到原始 nnm.keystore 文件
- 任务 4:如果可用,则恢复原始 nnm.keystore 文件

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。

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
 - UNIX: \$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>"
 - UNIX: \$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
 - UNIX: \$NnmDataDir/shared/nnm/certificates
 - b 检查密钥库的内容:
 - Windows: %NnmInstallDir%\nonOV\jdk\b\bin\keytool -list \ -keystore nnm.keystore
 - UNIX: \$NnmInstallDir/nonOV/jdk/b/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 比较此 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)。
 - 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。
 - 如果指纹不完全匹配,请重复任务 3: 尝试找到原始 nnm.keystore 文件。

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。

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 ovjboss 进程:

ovstop ovjboss

- 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
 - UNIX: \$NnmDataDir/shared/nnm/certificates
- 3 启动 ovjboss 进程:

ovstart ovjboss

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,请遵循以下步骤:

- 1 转到 http://www.webware.hp.com。
- 2 单击 Manage Licenses (管理许可证)。
- 3 登录;执行相应步骤获得新许可证密钥,以完成移动过程。
- 4 用新 IP 地址配置 NNMi 管理服务器。
- 5 配置 DNS 服务器以识别 NNMi 管理服务器的新 IP 地址。
- 6 重新启动 NNMi 管理服务器。
- 7 在命令提示符处,输入以下命令:

```
nnmlicense.ovpl NNM -g
```

- 8 在 Autopass: License Management (Autopass: 许可证管理) 对话框中, 单击 Remove License Key (删除许可证密钥)。
- 9 选择要删除的许可证密钥。
- 10 选择 Remove Licenses permanently (永久删除许可证)。
- 11 单击 Remove (删除); 然后关闭对话框。
- 12 将在步骤 3 中获得的新许可证密钥复制到名为 license.txt 的文本文件中。
- 13 在命令提示符处,输入以下命令:

nnmlicense.ovpl NNM -f license.txt

许可注意事项

有关获取和安装 NNMi 许可证密钥的信息,请参阅第 115 页的许可 NNMi。

更改 NNMi 管理服务器的主机名或域名



如果 NNMi 管理服务器参与 NNMi 应用程序故障切换或是高可用性 (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,请完成以下任务:

- 任务 1: 准备系统
- 任务 2: 创建新 NNMi 公钥证书
- 任务 3: 更改 NNMi 管理服务器的完全限定域名
- 任务 4: 用新证书更新 HTTPS 配置
- 任务 5: 重新启动、更新和刷新系统
- 任务 6: 备份 NNMi

任务 1: 准备系统

1 遵循标准过程以执行完整的 NNMi 备份。

明确标注此备份,就像之前更改 NNMi 管理服务器名称一样。

2 重命名系统。

如有必要,请重新启动系统。 ovjboss 进程可能未完全启动。

- 3 如果 NNMi 的 IP 地址也将更改, 请完成第 382 页的更改独立 NNMi 管理服务器的 IP 地址中的步骤。
- 4 停止 ovjboss:

ovstop ovjboss

- 5 切换到包含 NNMi 证书的目录:
 - Windows: %NnmDataDir%\shared\nnm\certificates
 - UNIX: \$NnmDataDir/shared/nnm/certificates
- 6 出于备份目的,保存以下文件的副本:
 - nnm.keystore
 - nnm.truststore

任务 2: 创建新 NNMi 公钥证书

在 nnm.keystore 文件中创建此 NNMi 管理服务器的新证书。当下次 ovjboss 进程成功启动时, NNMi 将更新数据库权限以使用此新证书。

- 1 切换到包含 NNMi 证书的目录:
 - Windows: %NnmDataDir%\shared\nnm\certificates
 - UNIX: \$NnmDataDir/shared/nnm/certificates

从 certificates 目录中运行此过程中的所有命令。

2 通过运行以下命令,在密钥库中生成新公钥/私钥对(证书):

```
    Windows:
        %NnmInstallDir%\nonOV\jdk\b\bin\keytool -genkey \
            -alias "<唯一别名>" -keyalg rsa
            -dname "cn=<主机名>, dc=<按组成部分表示的域名>" \
            -keypass "nnmkeypass" -validity 36500 \
            -keystore nnm.keystore -storepass "nnmkeypass"
```

- UNIX:
 - \$NnmInstallDir/nonOV/jdk/b/bin/keytool -genkey \
 -alias "<唯一別名>" -keyalg rsa
 - -dname "cn=<主机名>, dc=<按组成部分表示的域名>" \ -keypass "nnmkeypass" -validity 36500 \ -keystore nnm.keystore -storepass "nnmkeypass"

将 <别名> 替换为唯一值,如 NNMi 管理服务器的新主机名,例如: newnnmi

将 <主机名> 替换为 NNMi 管理服务器的新完全限定域名,例如: newnnmi.servers. example.com

将 dc=<*按组成部分表示的域名*> 替换为 NNMi 管理服务器所驻留的新域的各个组成部分。例如,对于 NNMi 管理服务器 newnnmi.servers.example.com,请指定: dc=servers, dc=example, dc=com

有关 keytool 命令的详细信息,请在 **java.sun.com** 上搜索 "Key and Certificate Management Tool"(密钥和证书管理工具)。

任务 3: 更改 NNMi 管理服务器的完全限定域名

要设置 NNMi 以使用 NNMi 管理服务器的新完全限定域名,请使用 nnmsetofficialfqdn.ovpl 命令。例如:

nnmsetofficialfqdn.ovpl newnnmi.servers.example.com

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

任务 4: 用新证书更新 HTTPS 配置

通过编辑以下文件,配置 Tomcat 服务器:

\$jboss.home.dir/server/nms/deploy/jboss-web.deployer/server.xml

\$jboss.home.dir 的默认值是:

- Windows: %NnmInstallDir%\nonOV\jboss\nms
- UNIX: \$NnmInstallDir/nonOV/jboss/nms

如果 NNMi Web 服务器使用 HTTPS 协议,请执行以下步骤以更新 HTTPS 配置:

- 1 在任何文本编辑器中打开 server.xml 文件。
- 2 在取消注释的 https 连接器块中,更改 keyAlias 参数的值以匹配在任务 2: 创建新 NNMi 公钥证书中为新证书使用的别名值。
- 3 保存 server.xml 文件。

有关 server.xml 文件和示例 https 连接器块的详细信息,请参阅第 86 页的更新 server.xml 文件。

任务 5: 重新启动、更新和刷新系统

1 启动 ovjboss:

ovstart ovjboss

- 2 更新 NNMi 管理服务器与专用服务器上运行的任何 NNM iSPI 之间的连接,以使用 NNMi 管理服务器的新完全限定域名。
- 3 更新 NNMi 管理服务器与任何集成的应用程序之间的连接,以使用 NNMi 管理服务器 的新完全限定域名。

如有必要,更新所集成应用程序的单点登录配置以信任新 NNMi 证书。

4 如果 NNMi 数据库包含任何加密的数据(比如 SNMPv3 密码短语),则此数据是用旧 安全密钥加密的。新安全密钥无法解密该数据。请联系支持代表以获得删除和重新创建 这些配置项的帮助。

任务 6: 备份 NNMi

遵循标准过程以执行完整的 NNMi 备份。



如果 NNMi 恢复自更改 NNMi 管理服务器名称之前所作的备份,则将覆盖 nnm.keystore 文件,从而使 NNMi 数据库不可访问。如果需要从旧备份恢复 NNMi 数据,请联系支持代表以获得帮助。

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
- 任务 2: 更新 NNMi 配置

任务 1: 更新 Oracle 数据库实例

1 停止 ovjboss:

ovstop ovjboss

- 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

Λ

- 1 备份数据库连接配置文件:
 - a 切换到以下目录:
 - Windows: %NnmInstallDir%\nonOV\jboss\nms\server\nms\
 - UNIX: \$NnmInstallDir/nonOV/jboss/nms/server/nms/
 - b 在 nms 目录中, 创建名为 deploy.save 的目录。
 - c 将 nms-ds.xml 文件从 deploy 目录复制到 deploy.save 目录。

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,就像对 deploy.save 目录执行的操作一样。

- 2 编辑数据库连接配置文件:
 - **a** 切换到 deploy 目录。

- b 在任何文本编辑器中,打开 nms-ds.xml 文件。
- c 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 主机名:数据库端口:数据库实例名

d 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。
 (此数据库实例必须已存在!)
- e 保存 nms-ds.xml 文件。
- 3 启动 ovjboss:

ovstart ovjboss

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 关闭 NNMi:

ovstop

- 2 运行 nnmchangedbpw.ovpl 命令并遵循提示操作。
- 3 启动 NNMi:

ovstart

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

在 Xen 虚拟化环 境中运行 NNMi

Xen 是 Linux 的 OpenSource 虚拟化环境。Xen 具有一个低级别管理程序,允许您创建运行 Windows 或 Linux 之 类操作系统的虚拟机。它还允许快照,并提供类似于 VMWare 的其他功能。

如果在安装 NNMi 之前 Xen 已经存在,则 NNMi 安装过程将自动解决 Xen 虚拟接口问题。

本章包含以下主题:

• 在正在运行的 NNMi 管理服务器上安装 Xen 之后的问题

在正在运行的 NNMi 管理服务器上安装 Xen 之后的问题

假定在服务器上安装了 NNMi 9.10,并且 NNMi 在生产环境中正常运行。如果在此 NNMi 管理服务器上安装 Xen,则 Xen 更改 NNMi 管理服务器上的网络路由表,以便所有数据包(包括发送到环回地址的数据包)遍历 Xen 虚拟接口。如果在 NNMi 管理服务器上运行 ifconfig -a 命令,则看见 Xen 的虚拟地址显示为 virbr0。在 NNMi 管理服务器上安装 Xen 的结果是当多个 NNMi 进程需要使用 NNMi 管理服务器的环回地址通信时, NNMi 可能停止正常运行。现在是 virbr0 虚拟接口而不是 NNMi 管理服务器的环回地址响应,这导致 NNMi 中发生通信问题。



不要在 Xen 内部运行的虚拟机上运行 NNMi,因为那不是支持的配置。

要对此进行补救,请执行以下操作:

1 使用 kill 命令停止所有 NNMi 进程。



必须使用 kill 命令。由于 virbr0 虚拟接口问题,您不可以再使用 ovstop 命令与 NNMi 进程管理器 (ovspmd)进行通信。

- 2 运行 **ifconfig virbr0** 命令,显示 virbr0 接口的 **IP** 地址。此过程的其余部分将显示的 **IP** 地址引用为 *IP_Address*。
- 3 编辑以下文件: \$NNM SHARED CONF/ovspmd.auth
- 4 在文本的末尾添加行,包括步骤 2 中的 IP 地址和 + 号。使用以下示例: IP_Address +
- 5 如果计划将 NNMi 用于嵌入式数据库,则执行以下操作:
 - a 编辑以下文件: \$NNM_DATA/shared/nnm/databases/Postgres/ pg_hba.conf。
 - b 添加包含步骤 2 中的 IP 地址的以下行: host all all IP_Address/32 trust
- 6 使用 ovstart c 命令启动 NNMi 进程。 NNMi 管理服务器应当正常运行。

升级自 NNMi 9.0x

有关从 NNM 6.x/7.x 升级到 NNMi 9.10 的信息,请参阅《NNMi 升级参考》。

可以按照表 35 中显示的信息升级 NNMi。为获得最佳结果,请先升级到 NNMi 9.0x 补丁 3 或更高版本,然后再升级到 NNMi 9.10。表 35 中显示的信息假定您已在 NNMi 管理服务器上安装 NNMi 9.0x 或更高版本。

表 35 支持的 NNMi 升级

NNMi 版本	升级到 NNMi 9.10
NNMi 9.0x	受支持
NNMi 9.0x 补丁 1	受支持
NNMi 9.0x 补丁 2 (NNMi 9.01)	受支持
NNMi 9.0x 补丁 3 或更新版本	受支持

如果计划升级正在以 NNMi 应用程序故障切换配置运行的 NNMi 9.0x 的较早版本,则支持的升级路径是临时取消应用程序故障切换配置,将 NNMi 管 理服务器升级到 NNMi 9.10,然后重新配置应用程序故障切换。有关详细信息,请参阅第 283 页的应用程序故障切换和升级到 NNMi 9.10。

如果计划升级正在以高可用性 (HA) 运行的 NNMi 9.0x 的更早版本,请参阅第 327 页的将以 HA 运行的 NNMi 从 NNMi 9.0x 升级到 NNMi 9.10。

如果计划升级在全局网络管理环境中配置的 NNMi 管理服务器,请参阅第 249 页的从 NNMi 9.0x 升级到 NNMi 9.10。

如果计划将 Linux NNMi 管理服务器从 NNMi 9.0x 升级到 NNMi 9.10,则必须先将 HP 公钥导入 Linux RPM 数据库,然后再安装 NNMi 9.10。为此,请将浏览器指向以下位置,并按照说明操作: https://h20392.www2.hp.com/portal/swdepot/

displayProductInfo.do?productNumber=HPLinuxCodeSigning

您可能会遇到几种升级场景。本部分包含以下各章:

• 从现有版本升级 NNMi 管理服务器,它描述以下升级场景:

— 在相同硬件和操作系统上从 NNMi 9.0x 升级到 NNMi 9.10。

- 升级到不同 NNMi 管理服务器,它描述以下升级场景:
 - 在相同版本的操作系统上从 NNMi 9.0x 升级到 NNMi 9.10。
- 将 NNMi 从 Windows 2003 移到 Windows 2008。 NNMi9.10 不支持 Windows 2003。在升级到 NNMi 9.10 之前,必须将操作系统更改为 Windows 2008。
- 迁移 NNMi Oracle 数据。解释将 NNMi 管理服务器使用的 Oracle 数据从一个 Oracle 数据库实例移到另一个实例所执行的步骤。
- 其他升级信息。解释 NNMi 9.10 不同于 NNMi 的更早版本的一些方面。

从现有版本升级 NNMi 管理服务器

本章描述将现有 NNMi 管理服务器升级到 NNMi 9.10 的过程。

本章包含以下主题:

• 将现有 NNMi 管理服务器升级到 NNMi 9.10

将现有 NNMi 管理服务器升级到 NNMi 9.10

在继续之前,请先阅读《NNMi 安装指南》中的 NNMi 9.10 *安装前清单*一章以及第 403 页的其他升级信息。《NNMi 安装指南》具有重大更改。例如,如果使用 Oracle 数据库实例 而不是嵌入式数据库,则应当设置 FLASHBACK ANY TABLE 权限,因为这使得 NNMi 能够在迁移期间创建恢复点。

在继续之前,阅读要升级到的 NNMi 软件的 HP Network Node Manager i Software 系统 和设备支持列表。可以从 http://h20230.www2.hp.com/selfsolve/manuals 上获得此文档 的副本。必须有 HP Passport 用户 ID 才能访问此网站。

以下步骤解释如何将 NNMi 管理服务器升级到 NNMi 9.10。以下步骤假定已在 NNMi 管理服务器上运行 NNMi 9.0x。

- 1 使用 nnmbackup.ovpl 脚本备份 NNMi 管理服务器。将此作为预防措施,因为只有发 生迁移失败等可能性很小的事件时才会用到此备份。有关详细信息,请参阅 nnmbackup.ovpl 参考页或 UNIX 联机帮助页。
- 2 仅针对Oracle 数据库:如果NNMi管理服务器使用Oracle数据库,请Oracle数据库管理员备份NNMi数据。如上面提及的那样,请Oracle数据库管理员设置 FLASHBACK ANY TABLE 权限,这样NNMi就能在迁移期间创建恢复点

3 *仅针对 Oracle 数据库*:使用 nnmconfigexport.ovpl 脚本从 NNMi 管理服务器备份 配置信息。将此作为预防措施,因为只有发生迁移失败等可能性很小的事件时才会用到 此备份。有关详细信息,请参阅 *nmconfigexport.ovpl* 或 *nnmconfigimport.ovpl* 参考 页或者 UNIX 联机帮助页。

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。

4 使用《NNMi 安装指南》中的说明在 NNMi 管理服务器上安装 NNMi 9.10。

仅针对 Oracle 数据库:如果 Oracle 数据库管理员不设置 FLASHBACK ANY TABLE 权限,则在安装完成之后,将看见有关该缺失权限的警告。可以忽略此警告。

5 验证信息已从 NNMi 管理服务器成功迁移。

Δ

升级到不同 NNMi 管理服务器

本章描述在维护现有 NNMi 管理服务器的配置时,在新系统上升级到 NNMi 9.10 的过程。

本章包含以下主题:

• 升级到不同 NNMi 管理服务器

升级到不同 NNMi 管理服务器

在继续之前,请先阅读《NNMi 安装指南》中的 NNMi 9.10 *安装前清单*一章以及第 403 页的其他升级信息。《NNMi 安装指南》具有重大更改。例如,如果使用 Oracle 数据库实例 而不是嵌入式数据库,则应当设置 FLASHBACK ANY TABLE 权限,因为这使得 NNMi 能够在迁移期间创建恢复点。

以下步骤说明如何将数据从现有 NNMi 管理服务器复制到目标 NNMi 管理服务器。以下步骤假定已在现有 NNMi 管理服务器上运行 NNMi 9.0x。



如果要更改 Oracle 数据库服务器,请在升级到 NNMi 9.10 之前或之后完成此过程。有关 信息,请参阅第 401 页的迁移 NNMi Oracle 数据。

- 作为预防措施,使用 nnmbackup.ovpl 脚本备份现有(源) NNMi 9.0x 管理服务器。为 此备份标注 NNMi 9.0x。有关详细信息,请参阅 nnmbackup.ovpl 参考页或 NNMi 9.0x 的 UNIX 联机帮助页。
- 2 如果现有(源)NNMi管理服务器使用 Oracle 数据库,则请 Oracle 数据库管理员备份 NNMi 9.0x 数据。如上面提及的那样,请 Oracle 数据库管理员设置 FLASHBACK ANY TABLE 权限,这样 NNMi 就能在迁移期间创建恢复点。

3 使用《NNMi 安装指南》中的说明在源 NNMi 管理服务器上安装 NNMi 9.10 和最新的合并补丁(如果有)。

仅针对 Oracle 数据库:如果 Oracle 数据库管理员不设置 FLASHBACK ANY TABLE 权限,则在安装完成之后,将看见有关该缺失权限的警告。可以忽略此警告。

- 4 验证 NNMi 9.10 正在源 NNMi 管理服务器上正常运行。
- 5 使用 nnmbackup.ovpl 脚本在源 NNMi 管理服务器上备份 NNMi 9.10。为此备份标 注 NNMi 9.10。您将需要此备份以将数据复制到目标 NNMi 管理服务器。有关详细信 息,请参阅 nnmbackup.ovpl 参考页或 NNMi 9.10 的 UNIX 联机帮助页。
- 6 使用《NNMi 安装指南》中的说明在目标 NNMi 管理服务器上安装 NNMi 9.10 和最新的合并补丁(如果有)。要迁移来自步骤 5 的数据,目标 NNMi 管理服务器必须正在运行相同的操作系统版本。 NNMi 不支持将数据迁移到在不同操作系统上运行的NNMi 管理服务器。
- 7 使用 nnmrestore.ovpl 脚本将 NNMi 数据库信息复制到目标服务器。有关详细信息, 请参阅 nnmrestore.ovpl 参考页或 UNIX 联机帮助页。
- 8 获取新许可证并将其安装到目标 NNMi 管理服务器上。

有关信息,请参阅第 115 页的许可 NNMi。

9 验证从现有 NNMi 管理服务器成功迁移目标 NNMi 管理服务器的信息。
将 NNMi 从 Windows 2003 移 到 Windows 2008

NNMi 9.10 不支持 Windows 2003。在迁移到 NNMi 9.10 之前,必须将操作系统更改为 Windows 2008。

如果已在 Windows 2003 Server 上运行 NNMi 9.0x 补丁 3 或更高版本,并且需要将操作系统更改为 Windows 2008,请使用本章中的信息。

本章包含以下主题:

将 NNMi 从 Windows 2003 更改为 Windows 2008

将 NNMi 从 Windows 2003 更改为 Windows 2008

要完成以下步骤,必须在 Windows 2003 Server 上运行 NNMi 9.0x 补丁 3 或更高版本。 要检查 NNMi 版本号,请记下帮助 -> 关于 HP Network Node Manager i Software 窗口中的当前补丁级别。验证版本是否是 9.01.003 或更高版本。如果版本早于此版本号,请不要继续。 在继续之前,需要安装 NNMi 9.0x 补丁 3 或更高版本。

要将运行 NNMi 9.0x 补丁 3 或更高版本的 NNMi 管理服务器从 Windows 2003 更改为 Windows 2008,请按照以下步骤操作:

- 1 识别将在此过程期间使用的三个服务器:
 - 服务器 A 是运行 Windows 2003 的当前 NNMi 管理服务器。
 - 服务器 B将保存 NNMi 备份文件。
 - 服务器 C 将成为运行 Windows 2008 的新 NNMi 管理服务器。此 NNMi 管理服务 器可以与当前服务器 A 使用相同硬件。

确保新 NNMi 管理服务器上的 hosts 文件包含以下条目: 127.0.0.1 localhost



2 在服务器 A上,运行 nnmbackup.ovpl -type online -scope all -target 临时位置命令,以完成完整 NNMi 备份。

有关要使用哪些命令选项的详细信息,请参阅第 347 页的 NNMi 备份和恢复工具和 nnmbackup.ovpl 参考页,或 UNIX 联机帮助页。

- 3 在服务器 A上,将步骤 2 中完成的备份复制到服务器 B上。
- 4 在服务器 C上, 安装 Windows 2008。



也可以不使用服务器 C, 而是在服务器 A 上重新格式化磁盘并安装 Windows 2008。 如果选择此方案,则用服务器 A 代替服务器 C 完成剩余步骤。

- 5 在服务器 c 上, 安装 NNMi 9.0x 补丁 3 或更高版本。必须安装在步骤 2 中完成备份期 间 NNMi 服务器 A 所使用的补丁级别。
- 6 在服务器 C 上安装 NNMi 期间,安装脚本分配的端口可能与服务器 B 配置中的不同。 在服务器 C 上配置恢复期间,这可能产生端口冲突。要对此进行补救,请执行以下操作:
 - a 在服务器 C上,导航到以下目录: %\$NNM CONF%\nnm\props\
 - b 在服务器 C上,将 nms-local.properties 文件复制到临时位置中的 nms-local. properties.save。
 - c 在服务器 B上,将 NNMi 备份复制到服务器 C上。
 - d 在服务器 C上,运行 nnmrestore.ovpl -force -source 临时位置命令以完 成完整 NNMi 恢复。

有关要使用哪些命令选项的详细信息,请参阅第 347 页的 NNMi 备份和恢复工具和 nnmrestore.ovpl 参考页,或 UNIX 联机帮助页。

使用与您在步骤2中完成的备份相匹配的命令选项

《NNMi 部署参考》

e 在服务器 C上,将临时位置中的 nms-local.properties.save 文件与位于以下 目录中的 nms-local.properties 文件进行比较: %NNM_CONF%\nnm\props\

更改上述目录中的 nms-local.properties,解决任何端口冲突。确保保留在服务器 C 上安装 NNMi 期间选择的 jboss.http.port (NNMi Web 服务器端口)和 jboss.https.port (NNMi HTTPS Web 服务器端口)值。

f 重新启动 ovjboss:

ovstop ovjboss

ovstart ovjboss

- 7 NNMi 将其许可证密钥与服务器的 IP 地址相关联。如果服务器 C 的 IP 地址与服务器 A 的 IP 地址不同,请获得并安装新的 NNMi 许可证密钥。请参阅第 382 页的 更改独 立 NNMi 管理服务器的 IP 地址。
- 8 在服务器 C上,安装 NNMi 9.10。

迁移 NNMi Oracle 数据

如果计划将 NNMi 中的 Oracle 数据移到 Oracle 11G 中,本章中的信息将说明完成此工作要执行的步骤。

迁移 NNMi Oracle 数据

假定 NNMi 按以下某种配置运行:

- NNMi 9.0x (带最新补丁),连接到 Oracle 10G 数据库,需要升级到 NNMi 9.10。
- NNMi 9.0x (带最新补丁),连接到 Oracle 11G 数据库,需要升级到 NNMi 9.10。 需要完成的 Oracle 数据库实例迁移可以包括以下需求的组合:
- 在 NNMi 9.10 上运行的现有 Oracle 实例可能正在运行 Oracle 10G 或 11G。
- 在 NNMi 9.10 上运行的新 Oracle 实例必须正在运行 Oracle 11G。
- 新 Oracle 实例可以位于原始服务器上或在其他服务器和主机上。

要完成 NNMi Oracle 数据的迁移,请完成以下步骤:

- 1 以根或管理员身份运行以下命令以停止 NNMi: ovstop?。
- 2 使用 Oracle 工具将 NNMi 数据从现有 Oracle 服务器移动或复制到新服务器。请参考 Oracle 文档,以了解其他信息。
- 此 Oracle 数据迁移可以是在同一服务器上从 Oracle 10 就地升级到 Oracle 11。Oracle 提供数据库迁移工具,用于将 Oracle 10 数据转换为 Oracle 11 格式。
 - 3 *仅当新 Oracle 服务器与之前 Oracle 服务器的主机名不同时,才完成此步骤*。在 NNMi 管理服务器上,通过完成以下步骤,重新配置 NNMi 以指向新 Oracle 服务器:

a 编辑如下所示的数据源配置文件:

准确完成以下步骤很重要,否则 jboss 不会正确连接到 Oracle 11G 数据库。

- Windows: %NNM JBOSS%\server\nms\deploy\nms-ds.xml
- UNIX: \$NNM JBOSS/server/nms/deploy/nms-ds.xml
- b 更改以下属性以反映新服务器

旧值: <connection-url>jdbc:oracle:thin:@ 现有FQDN: 现有ORACLE 端口: 现 有SID </connection-url>

新值: <connection-url>jdbc:oracle:thin:@ 新FQDN: 新端口: 新SID </connection-url>

4 完成以下某个操作:

如果从 NNMi 9.0x 升级到 NNMi 9.10,请立即按照《HP Network Node Manager i Software 安装指南》中的安装说明执行该迁移。

如果已在使用 NNMi 9.10,请按照这些步骤以重新启动 NNMi,并完成 Oracle 数据库 移动 / 迁移:

- a 在 NNMi 管理服务器上运行以下命令以重新启动 NNMi: ovstart -c
- b 在 NNMi 管理服务器上运行以下命令以检查所有服务是否都已启动并正确运行: ovstatus -v

其他升级信息

本章描述 NNMi 9.10 相比较早的 NNMi 版本的一些更改。本章包含以下主题:

- 配置差异
- MIB
- 功能差异

配置差异

- 用户组替换 NNMi 角色以将用户权限限制在 NNMi 控制台中。用户帐户可以映射到多 个用户组。
 - 为登录 NNMi 控制台,每个用户帐户必须映射到至少一个 NNMi 提供的用户组。
 这些组等价于以前版本中的 NNMi 角色的功能。
 - 在多租户环境中,每个用户帐户可以映射到用于访问拓扑对象子集的一个或多个自 定义用户组。

有关详细信息,请参阅第 193 页的 NNMi 安全和多租户。

- 用于从目录服务检索用户信息的 NNMi 集成现在可以检索每个用户的多个组名称。
 - 对于配置选项2(仅目录服务中的用户名和密码),具有目录服务的现有集成继续 工作,而无需修改ldap.properties配置文件。
 - 对于配置选项3(目录服务中的所有用户信息),应用以下信息:
 - 在单租户环境 (所有 NNMi 控制台 用户可以访问所有拓扑对象)中,具有目录服务的现有集成继续工作,而无需修改 ldap.properties 配置文件。

如果在目录服务中添加任何新 NNMi 用户组,则必须将 ldap.properties 配置文件更新到新模型,才能从目录服务检索到用户信息。

- 在多租户环境中,将 ldap.properties 配置文件更新到新模型,以便从目录 服务检索到用户信息。
- 有关更新 ldap.properties 配置文件的信息,请参阅第 174 页的 将目录服务 访问配置更改为支持 NNMi 安全模型。
- NNMi 9.10 弃用以下 ldap.properties 配置文件参数。它们在未来版本中不受 支持:
 - roleAttributeID
 - roleAttributeIsDN
 - roleNameAttributeID
- 在升级到 NNMi 9.10 之后,将应用以下安全和多租户配置:
 - 一 所有节点分配到默认租户和默认安全组。
 - 所有用户都有权访问 NNMi 拓扑中的所有节点和所有事件。

此默认配置与 NNMi 9.0x 中可用的对象访问匹配。有关自定义对象访问的信息,请参 阅第 193 页的 NNMi 安全和多租户。

- 如果 HP NNMi 桯 P NA 集成是在 NNMi 9.0x 管理服务器上配置的,则升级到 NNMi 9.10 的过程将禁用该配置。有关详细信息,请参阅第 450 页的 从 NNMi 9.0x 升级的集成配置。
- 在升级到 NNMi 9.10 之后, NNMi 不再为登录或从 NNMi 控制台注销的每个用户生成日志条目。通过编辑 logging.properties 文件,可以更改此行为。有关详细信息,请参阅第 363 页的。
 在完成升级到 NNMi 9.10 之后,在以下位置查找用于 NNMi 9.0x 的 logging.properties 文件的副本:
 - Windows: %NNM DATA%\shared\nnm\conf\ovjboss\logging.properties.old
 - UNIX: \$NNM DATA/shared/nnm/conf/ovjboss/logging.properties.old

应用程序故障切换

对于应用程序故障切换功能, NNMi 9.0x 支持 UDP 或 TCP 解决方案。NNMi 9.10 仅支 持 TCP 解决方案。如果对 NNMi 9.0x 使用了 UDP 应用程序故障切换解决方案,并且要升 级到 NNMi 9.10,那么升级脚本将应用程序故障切换配置转换成 TCP 解决方案。必须将群 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。有关详细信息,请参阅第 270 页的为 NNMi 配置应用程序故障切换。

为使应用程序故障切换功能正确工作,活动服务器和备用服务器必须能够相互进行不受限制的网络访问。NNMi 9.10包括某些端口更改,因此可能需要修改防火墙配置。有关详细信息,请参阅第 605 页的 NNMi 9.10 和已知端口。

MIB

如果将其他 MIB 加载到不与标准兼容或依赖于其他 MIB 文件的 NNMi 更早版本中,则它 们可能无法成功迁移。如果 MIB 迁移不成功,则陷阱配置继续工作,但是您可能无法像迁 移之前那样浏览该 MIB。

如果怀疑某些 MIB 未迁移,则检查以下目录中的 failed 子目录,其中包含未迁移 MIB 文件、失败详细信息以及名称与未迁移 MIB 文件关联的日志文件:

- Windows: %NNM_DATA%\tmp\nnm9xMibMigrate
- UNIX: \$NNM DATA/tmp/nnm9xMibMigrate

使用在以上目录中包含的文件来确定 MIB 未迁移的原因, 然后重新加载这些 MIB。

功能差异

要查看有关 NNMi 9.10 中所含新功能的信息,请参阅 NNMi 发行说明中的本版本的新增 功能部分。

集成 NNMi

本部分包含以下各章:

- CiscoWorks LAN 管理解决方案
- Clarus Systems ClarusIPC Plus⁺
- HP Asset Manager
- HP Business Service Management 拓扑
- HP Universal CMDB
- HP Business Availability Center My BSM
- HP Network Automation
- HP ProCurve Manager Plus
- HP RAMS MPLS WAN
- HP SiteScope
- HP Systems Insight Manager
- nGenius Performance Manager
- NNMi Northbound Interface
- HP BSM Operations Management
- HP Operations Manager
- HP NNMi Integration Module for Netcool Software
- xMatters (以前称作 AlarmPoint)

CiscoWorks LAN 管理解决方案

Cisco Systems CiscoWorks LAN 管理解决方案 (CiscoWorks LMS) 是一套集成管理工具,用于对 Cisco 网络进行 配置、管理、监视和故障诊断。

本章包含以下主题:

- HP NNMi-CiscoWorks LMS 集成
- 启用 HP NNMi-CiscoWorks LMS 集成
- 使用 HP NNMi-CiscoWorks LMS 集成
- 更改 HP NNMi-CiscoWorks LMS 集成配置
- 禁用 HP NNMi-CiscoWorks LMS 集成
- 对 HP NNMi-CiscoWorks LMS 集成进行故障诊断
- HP NNMi-CiscoWorks LMS 集成配置表单参考

HP NNMi-CiscoWorks LMS 集成

HP NNMi-CiscoWorks LMS 集成提供了用于从 NNMi 控制台访问 CiscoWorks LMS 工具的操作。

价值

HP NNMi-CiscoWorks LMS 集成将 CiscoWorks LMS 信息添加到 NNMi, 以便 NNMi 用户可以检测并调查 Cisco 设备的潜在网络问题。

集成产品

本章中的信息适用于以下产品:

CiscoWorks LMS

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

• NNMi 9.10

NNMi 和 CiscoWorks LMS 必须安装在不同的计算机上。NNMi 管理服务器和 CiscoWorks LMS 服务器计算机可以使用相同或不同的操作系统。

有关 NNMi 的受支持硬件平台和操作系统的最新信息,请参阅 NNMi 系统和设备支持列表。

有关 CiscoWorks LMS 的受支持硬件平台和操作系统的最新信息,请参阅您所用版本的对 应文档。例如:

• CiscoWorks LMS 版本 3.1:

http://www.cisco.com/en/US/docs/net_mgmt/ ciscoworks_lan_management_solution/3.1/install/guide/prereq.html

• CiscoWorks LMS 版本 3.2:

http://www.cisco.com/en/US/docs/net_mgmt/ ciscoworks_lan_management_solution/3.2/install/guide1/prereq.html

文档

本章描述如何配置 NNMi 以与 CiscoWorks LMS 通信以及如何从 NNMi 控制台使用集成。

启用 HP NNMi-CiscoWorks LMS 集成

在 NNMi 管理服务器上,通过执行以下步骤,配置 NNMi 和 CiscoWorks LMS 之间的连接:

- 在 NNMi 控制台中, 打开 HP NNMi-CiscoWorks LMS 集成配置表单 (集成模块配置 > CiscoWorks LMS)。
- 2 选中启用集成复选框以激活表单上的其余字段。
- 3 输入用于连接到 NNMi 管理服务器的信息。有关这些字段的信息,请参阅第 413 页的 NNMi 管理服务器连接。
- 4 键入用于连接到 CiscoWorks LMS 服务器的信息。有关这些字段的信息,请参阅第 414 页的 CiscoWorks LMS 服务器连接。

2011年3月

5 单击表单底部的**提交**。

将会出现新窗口,其中显示状态消息。如果消息指出连接到 NNMi 管理服务器时发生问题,则单击**返回**,然后按照错误消息文本的建议调整值。

- 6 加载 CiscoWorks LMS 所管理设备的事件定义:
 - a 切换到以下目录:
 - Windows: %NnmInstallDir%\newconfig\HPOvNmsEvent
 - UNIX: \$NnmInstallDir/newconfig/HPOvNmsEvent
 - b 通过输入以下命令,导入 CiscoWorks LMS 事件定义:

```
nnmconfigimport.ovpl -f nnm-cisco-incidentConfig.xml \
-u <用户名> -p <密码>
```

- 7 以下操作可选,建议执行。为 CiscoWorks LMS 所管理设备生成的陷阱加载 MIB 定义 文件:
 - a 从设备介质或 Cisco 网站获取相应的 MIB 文件:

tools.cisco.com/Support/SNMP/do/SearchOID.do?local=en&step=1

- b 切换到存储 MIB 文件的目录。
- c 使用 nnmloadmib.ovpl 命令加载被管环境的适合 MIB 文件。例如:

nnmloadmib.ovpl -load cpqhost.mib -u <用户名> -p <密码>

d 通过输入以下命令,验证 MIB 是否正确加载:

nnmloadmib.ovpl -list -u <用户名> -p <密码>

使用 HP NNMi-CiscoWorks LMS 集成

HP NNMi-CiscoWorks LMS 集成提供从 NNMi 控制台到 CiscoWorks LMS 的链接。集成不提供产品之间的单点登录。必须输入 CiscoWorks LMS 用户凭证,才能查看 CiscoWorks LMS 页。

启用 HP NNMi-CiscoWorks LMS 集成会将以下操作添加到 NNMi 控制台:

- CiscoWorks Device Center 在所选节点的上下文中打开 CiscoWorks Device Center。
- CiscoWorks CiscoView 在所选节点的上下文中打开 CiscoWorks CiscoView。

更改 HP NNMi-CiscoWorks LMS 集成配置

- 1 在 NNMi 控制台中,打开 HP NNMi-CiscoWorks LMS 集成配置表单 (集成模块配置 > CiscoWorks LMS)。
- 2 对值进行相应修改。有关此表单上的字段的信息,请参阅第 413 页的 HP NNMi-CiscoWorks LMS 集成配置表单参考。
- 3 验证表单顶部的**启用集成**复选框是否已选中,然后单击表单底部的**提交**。
- 更改会立即生效。不需要重新启动 ovjboss。

禁用 HP NNMi-CiscoWorks LMS 集成

- 1 在 NNMi 控制台中,打开 HP NNMi-CiscoWorks LMS 集成配置表单 (集成模块配置 > CiscoWorks LMS)。
- 2 清除表单顶部的**启用集成**复选框,然后单击表单底部的**提交**。集成操作不再可用。



更改会立即生效。不需要重新启动 ovjboss。

对 HP NNMi-CiscoWorks LMS 集成进行故障诊断

CiscoWorks LMS 操作不运行

如果已经验证 HP NNMi-CiscoWorks LMS 集成配置表单中的值,并且仍然不能从 NNMi 控制台打开 CiscoWorks LMS 页,请执行以下操作:

- 1 清除 Web 浏览器缓存。
- 2 从 Web 浏览器清除所有保存的表单或密码数据。
- 3 完全关闭 Web 浏览器窗口,然后重新打开它。
- 4 在 HP NNMi-CiscoWorks LMS 集成配置表单中重新输入值。
- 5 验证 CiscoWorks LMS 是否正在运行。

陷阱中的 "MIB 缓存中找不到 OID" 消息

如果 NNMi 中未加载 CiscoWorks LMS 所管理设备生成的陷阱的 MIB 定义文件,则您会 看到与以下文本类似的错误:

<mib 缓存中找不到值为1的Cia .1.3.6.1.4.1.11.5.7.5.2.1.1.1.7.0>

要解决这些错误,请如第 411 页的步骤 7 中所述加载 MIB。

HP NNMi-CiscoWorks LMS 集成配置表单参考

HP NNMi-CiscoWorks LMS 集成配置表单包含用于配置 NNMi 和 CiscoWorks LMS 之间的 通信的参数。此表单是通过集成模块配置工作区提供的。



只有具有管理员角色的 NNMi 用户才可以访问 HP NNMi-CiscoWorks LMS 集成配置表单。

HP NNMi-CiscoWorks LMS 集成配置表单采集以下常规方面的信息:

- NNMi 管理服务器连接
- CiscoWorks LMS 服务器连接

要应用对集成配置的更改,请在 HP NNMi-CiscoWorks LMS 集成配置表单上更新值,然后单击提交。

NNMi 管理服务器连接

表 36 列出用于连接到 NNMi 管理服务器的参数。这就是您用于打开 NNMi 控制台的信息。通过查看调用 NNMi 控制台会话的 URL,可以确定这些值中的大部分。与 NNMi 管理员协作,为配置表单的这一部分确定合适的值。

表 36 NNMi 管理服务器信息

字段	描述
启用 NNMi SSL	连接协议规范。 如果将 NNMi 控制台配置为使用 HTTPS,则选中 NNMi SSL 已启用复选框。这是默认配置。 如果将 NNMi 控制台配置为使用 HTTP,则清除 NNMi SSL 已启用复选框。
NNMi 主机	NNMi 管理服务器的完全限定域名。此字段已预填充了用于访问 NNMi 控制台的主机 名。验证此值是否是由在 NNMi 管理服务器上运行的 nnmofficialfqdn.ovpl -t 命 令返回的名称。
NNMi 端口	用于连接到 NNMi 控制台的端口。此字段预填充了 jboss 应用程序服务器用于与 NNMi 控制台通信的端口,如以下文件中所指定: • Windows: %NnmDataDir%\conf\nnm\props\nms-local.properties • UNIX: \$NnmDataDir/conf/nnm/props/nms-local.properties 对于非 SSL 连接,使用 jboss.http.port 的值,它的默认值为 80 或 8004 (具体取决 于安装 NNMi 时是否存在另一个 Web 服务器)。 对于 SSL 连接,使用 jboss.https.port 的值,它的默认值为 443。

表 36 NNMi 管理服务器信息 (续)

字段	描述
NNMi 用户	用于连接到 NNMi 控制台的用户名。此用户必须具有 NNMi 管理员或 Web 服务客户端 角色。
NNMi 密码	指定 NNMi 用户的密码。

CiscoWorks LMS 服务器连接

表 37 列出了用于连接到 CiscoWorks LMS 服务器以打开 CiscoWorks LMS 页的参数。与 CiscoWorks LMS 管理员协作,为配置表单的这一部分确定合适的值。

表 37 CiscoWorks LMS 管理服务器信息

CiscoWorks LMS 服 务器参数	描述
启用 CiscoWorks LMS SSL	用于连接到 CiscoWorks LMS 的连接协议规范。
	• 如果将 CiscoWorks LMS 配置为使用 HTTPS,则选中 启用 CiscoWorks LMS SSL 复选框。这是默认配置。
	• 如果将 CiscoWorks LMS 配置为使用 HTTP,则清除 启用 CiscoWorks LMS SSL 复选框。
CiscoWorks LMS 主机	CiscoWorks LMS 服务器的完全限定域名。
CiscoWorks LMS 端口	用于连接到 CiscoWorks LMS Web 服务的端口。 如果正在使用默认 CiscoWorks LMS 配置,则使用端口 1741(对于与 CiscoWorks LMS 的非 SSL 连接)或端口 443(对于与 CiscoWorks LMS 的 SSL 连接)。

Clarus Systems ClarusIPC Plus⁺



Clarus Systems ClarusIPC Plus⁺ 提供声音服务测试; IP 电话功能的远程诊断; 基于调用详细记录 (CDR) 的警报 和跟踪; 以及在新的部署、升级和持续操作的过程中针对 Cisco Unified Communications Manager IP 电话系统报 告配置。

Clarus Systems 提供 ClarusIPC Plus⁺ 与 HP Network Node Manager i Software (NNMi) 的集成。HP 提供 ClarusIPC Plus⁺ 与 NNM iSPI for IP Telephony 的集成。这些集成是互斥的。

本章描述以下可用集成:

- HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成
- HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成

HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成

本部分包含以下主题:

- 第 416 页的关于 HP NNMi-Clarus Systems Clarus IPC Plus⁺ 集成
- 第 416 页的启用 HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成
- 第 417 页的使用 HP NNMi-Clarus Systems Clarus IPC Plus⁺ 集成
- 第 417 页的禁用 HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成
- 第 417 页的对 HP NNMi-Clarus Systems Clarus IPC Plus⁺ 集成进行故障诊断

关于 HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成

Clarus Systems 提供并支持 HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成。在此集成中, ClarusIPC Plus⁺ 将关于 IP 电话服务测试结果的 SNMP 陷阱、基于所设 CDR 策略的警报或基于 Unified Communications Manager 配置更改策略的警报转发到 NNMi, 后者随后会生成关于 IP 电话配置和设备的状态的事件。 NNMi 提供整个网络的整合视图。

集成实现了在 NNMi 控制台中通过这些事件访问若干 ClarusIPC Plus+ 工具。

价值

HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成通过提供从 NNMi 控制台到 ClarusIPC Plus⁺ 工具的访问以进行 IP 电话配置更改跟踪和报告,从而整合 IP 电话设备管理。

集成产品

本章中的信息适用于以下产品:

• ClarusIPC Plus⁺

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

• 仅 Windows 操作系统上的 NNMi 9.10

文档

集成安装包中所含的《ClarusIPC Plus+ HP NNMi Software 集成指南》完整描述了 HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成。

ClarusIPC Plus⁺ 文档套件包含详细描述 ClarusIPC Plus⁺ 功能的更多文档。文档套件可 从以下地址的 Clarus Systems 网站下载:

www.support.clarussystems.com

启用 HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成

要获取 HP NNMi–Clarus Systems ClarusIPC Plus⁺ 集成安装包, 请联系 Clarus Systems 支持。

有关启用集成的信息,请参阅集成安装包中所含的《ClarusIPC Plus+ HP NNMi Software 集成指南》。

使用 HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成

启用 HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成会将若干 URL 操作添加到 NNMi 控制台。有关这些 URL 操作的信息,请参阅《ClarusIPC Plus+ HP NNMi Software 集成 指南》。



ClarusIPC Plus⁺ 需要使用 Microsoft Internet Explorer Web 浏览器。在 Internet Explorer 中打开 NNMi 控制台,然后启动将打开 ClarusIPC Plus⁺ 窗口的 URL 操作。

禁用 HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成

有关禁用 HP NNMi–Clarus Systems ClarusIPC Plus⁺ 集成的信息,请联系 Clarus Systems 支持。

对 HP NNMi-Clarus Systems ClarusIPC Plus⁺ 集成进行故障诊断

有关优化和扩展集成的信息以及任何当前已知问题,请参阅《ClarusIPC Plus+ HP NNMi Software 集成指南》。

HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成

本部分包含以下主题:

- 第 418 页的关于 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成
- 第 419 页的启用 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成
- 第 419 页的使用 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成
- 第 419 页的禁用 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成
- 第 420 页的对 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成进行故障诊断

关于 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成

HP 提供并支持 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成。使用此集成,操作员可以访问关于 IP 电话服务测试和诊断的 ClarusIPC Plus⁺ 功能、 Cisco Unified Communications Manager 配置更改报告以及 CDR 监视策略。ClarusIPC Plus⁺ 将关于 IP 电话服务测试结果的 SNMP 陷阱、基于所设 CDR 策略的警报或基于 Unified Communications Manager 配置更改策略的警报转发到 NNMi,后者随后会生成 关于 IP 电话配置和设备的状态的事件。NNM iSPI for IP Telephony 提供以下各项功能:

- 用于启动 ClarusIPC Plus⁺ 配置更改报告、策略、测试计划和测试结果的工作区和菜单
- 在所选 IP 电话的上下文中,访问用于 IP 电话的 ClarusIPC Plus⁺ 远程诊断工具
- 在 NNMi 事件视图中的所选警报事件的上下文中,访问 ClarusIPC Plus⁺ 测试结果、 测试详细信息和 CDR 策略详细信息。

此集成允许从 NNMi 控制台访问的 ClarusIPC Plus⁺ 工具数量多于无 NNM iSPI for IP Telephony 的集成。

价值

HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成为 NNM iSPI for IP Telephony 添加了高级 IP 电话服务测试和诊断、 CDR 监视以及配置更改跟踪和报告功能。

集成产品

本部分中的信息适用于以下产品:

ClarusIPC Plus⁺

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

- 有 NNM iSPI Network Engineering Toolset Software 许可证的 NNMi 9.10
- NNM iSPI for IP Telephony 9.10

文档

iSPI 附带的 NNM iSPI for IP Telephony 帮助中完整描述了 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成。

该帮助(PDF 格式)及更多 NNM iSPI for IP Telephony 文档可从以下地址获取:

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

启用 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成

- 1 准备 NNMi 管理服务器:
 - a 如果在 NNMi 管理服务器上安装了 HP NNMi-Clarus Systems ClarusIPC Plus⁺
 集成(由 Clarus Systems 提供),请先卸载该集成,然后再启用 NNM iSPI for
 IP Telephony 和 ClarusIPC Plus⁺ 的集成。

有关如何卸载 Clarus IPC Plus⁺ 集成包的信息,请联系 Clarus Systems 支持。

- b 在 NNMi 管理服务器上,安装以下各项:
 - 最新的 NNMi 合并补丁 (如果有)
 - 最新的 NNM iSPI for IP Telephony 合并补丁 (如果有)

补丁可从以下地址获取:

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

2 在 NNMi 管理服务器上,如 NNM iSPI for IP Telephony 帮助中所述启用 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成。

使用 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成

启用 HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus⁺ 集成会将若干 工作区、事件类型和 URL 操作添加到 NNMi 控制台。有关这些 URL 操作的信息,请参阅 NNM iSPI for IP Telephony 帮助。



ClarusIPC Plus⁺ 需要使用 Microsoft Internet Explorer Web 浏览器。在 Internet Explorer 中打开 NNMi 控制台,然后启动将打开 ClarusIPC Plus⁺ 窗口的 URL 操作。

禁用 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集成

有关禁用 HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus⁺ 集成的信息,请参阅 NNM iSPI for IP Telephony 帮助。

对 HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus⁺ 集 成进行故障诊断

有关优化和扩展集成的信息以及任何当前已知问题,请参阅 NNM iSPI for IP Telephony 帮助。

有关对 ClarusIPC Plus⁺ 的问题进行故障诊断的帮助,请联系 Clarus Systems 支持。

HP Asset Manager

HP Asset Manager 是用于跟踪和维护公司资产(包括 IT 资产)的资产管理平台。Asset Manager 提供以下功能:

- 管理软件许可证符合性、权利和成本
- 搜索、提供、管理和改进物理及虚拟 IT 资产的使用
- 有效使用分布式来源的资产、资产和服务数据
- 自动管理设备、空间、散热和电源

有关购买 Asset Manager 的信息,请联系 HP 销售代表。

本章包含以下主题:

- HP NNMi-HP Asset Manager 集成
- 使用 HP NNMi-HP Asset Manager 集成

HP NNMi-HP Asset Manager 集成

当 HP Network Node Manager i Software 与 HP Asset Manager 集成时, 会用 NNMi 数据库中的设备信息自动填充 Asset Manager 资产组合。

价值

HP NNMi-HP Asset Manager 集成提供以下好处:

- 减少流向所管理设备的网络通信量。NNMi 搜索设备,并且 Asset Manager 与 NNMi 拓扑同步。
- 向 Asset Manager 提供完整的网络资产。通过 NNMi 螺旋搜索,使此资产保持最新。
- 简化网络管理配置。仅在 NNMi 中存储网络搜索配置。

集成产品

本章中的信息适用于以下产品:

• 带 HP Connect-It 的 Asset Manager

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

• NNMi 9.10

NNMi 和 Asset Manager 必须安装在不同的计算机上。NNMi 管理服务器和 Asset Manager 计算机可以使用相同的或不同的操作系统。

文档

http://h20230.www2.hp.com/selfsolve/manuals 上用于 Connect-It 和 Integration Connector 产品类别的《HP Connect-It 连接器指南》中完整描述了 HP NNMi-HP Asset Manager 集成。

使用 HP NNMi-HP Asset Manager 集成

启用 HP NNMi-HP Asset Manager 集成的步骤将在 Asset Manager 服务器上执行。

启用 HP NNMi-HP Asset Manager 集成会用 NNMi 节点、接口和 IP 地址信息填充 Asset Manager 资产组合。

有关启用、使用和禁用 HP NNMi-HP Asset Manager 集成以及对它进行故障诊断的信息, 请参阅 《HP Connect-It 连接器指南》。

HP Business Service Management 拓扑

HP Business Service Management (BSM) 软件提供的工具用于在生产过程中管理应用程序的可用性,监视系统性能,监视基础结构性能,以及在问题出现时主动解决问题。

有关购买 BSM 的信息,请联系 HP 销售代表。

本章包含以下主题:

- HP NNMi-HP BSM 拓扑集成
- 启用 HP NNMi-HP BSM 拓扑集成
- 使用 HP NNMi-HP BSM 拓扑集成
- 更改 HP NNMi-HP BSM 拓扑集成配置
- 禁用 HP NNMi-HP BSM 拓扑集成
- 对 HP NNMi-HP BSM 拓扑集成进行故障诊断
- 应用程序故障切换和 HP NNMi-HP BSM 拓扑集成
- HP NNMi-HP BSM 拓扑集成配置表单参考

HP NNMi-HP BSM 拓扑集成

HP NNMi-HP BSM 拓扑集成用 NNMi 拓扑填充 BSM 运行时服务模型 (RTSM)。BSM 将 NNMi 拓扑中的每个设备存储为一个配置项 (CI)。BSM 用户以及集成的应用程序可以 了解网络设备之间的关系。

此外,集成将所填充 CI 的标识符存储到 NNMi 数据库中。由 NNMi 所管理设备的 CI 的 使用情况包括:

- MyBSM 门户中的 NNMi 组件。
- 路径状况视图在 BSM Real User Monitor (RUM) 中可用。
- HP NNMi-HP BSM Operations Management 集成可以将有关 NNMi 所管理设备的 事件与 BSM CI 相关联。有关详细信息,请参阅第 526 页的配置项标识符。
- HP NNMi-HPOM 集成的代理实施可以将有关 NNMi 所管理设备的事件与 BSM CI 相关联。有关详细信息,请参阅第 546 页的配置项标识符。

价值

HP NNMi-HP BSM 拓扑集成将 NNMi 设置为网络设备状态和关系信息的权威性源。该集成是与 BSM 进行其他集成的基础。它不提供从 NNMi 控制台访问 BSM 用户界面的功能。

集成产品

本章中的信息适用于以下产品:

• BSM



有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

• NNMi 9.10

NNMi 和 BSM 必须安装在不同的计算机上。 NNMi 管理服务器和 BSM 网关服务器计算 机可以使用相同或不同的操作系统。

有关受支持的硬件平台和操作系统的最新信息,请参阅这两种产品的支持列表。

文档

本章描述如何配置 NNMi 以与 BSM 通信。

BSM 文档套件详细描述了 BSM 功能。 BSM 产品介质包含该文档套件。

启用 HP NNMi-HP BSM 拓扑集成

▲ NNMi 无法同时与 HP BSM 拓扑和 HP Universal CMDB (UCMDB) 集成。如果在此 NNMi 管理服务器上配置 HP NNMi-HP UCMDB 集成,则在启用 HP NNMi-HP BSM 拓扑集成之前,禁用该配置。如果您需要这两个数据库中的 NNMi 信息,则以任意顺序执 行以下 两个操作:

- 如本章所述配置 HP NNMi-HP BSM 拓扑集成。
- 配置 BSM 与 UCMDB 的集成,如 UCMDB 产品介质上所含的《UCMDB 数据流管理 指南》中所述。对于 UCMDB 产品,还可从以下地址获取本手册: http://h20230.www2.hp.com/selfsolve/manuals

在 NNMi 管理服务器上,通过执行以下步骤,配置 NNMi 和 BSM 之间的连接:

- 1 可选。更新接口的 RTSM,将接口显示标签设置为接口名称优先于 MAC 地址:
 - a 在 BSM 用户界面中,打开 CI Type Manager 页(管理 > RTSM 管理 > 建模 > CI Type Manager)。
 - b 在 CI 类型窗格中,选择接口 (配置项 > 基础结构元素 > 节点元素 > 接口)。
 - c 在编辑窗格中默认标签选项卡上的 CI 类型属性下,选择 InterfaceName。
 - d 在 CI 类型标签定义格式下,将格式设置为:

接口名称 | MAC 地址

- 2 *可选*。RTSM 使用域名系统 (DNS) 名称协调相同节点的多个 CI。如果 HP Operations Manager 还与 RTSM 同步,则根据其 DNS 名称设置 NNMi 以命名节点:
 - a 在 NNMi 控制台中, 打开搜索配置表单 (配置 > 搜索配置)。
 - b 在**节点名称解析**下,执行以下操作:
 - 将第一选择设置为 DNS 全称。
 - 将第二选择设置为 DNS 简称。
- 3 在 NNMi 控制台中,打开 HP NNMi-HP BSM 拓扑集成配置表单(集成模块配置 > HP BSM 拓扑)。
- 4 选中**启用集成**复选框以激活表单上的其余字段。
- 5 输入用于连接到 NNMi 管理服务器的信息。有关这些字段的信息,请参阅第 429 页的 NNMi 管理服务器连接。
- 6 输入用于连接到 BSM 网关服务器的信息。有关这些字段的信息,请参阅第 430 页的 BSM 网关服务器连接。
- 7 *可选*。输入用于描述应当在 BSM 中保留哪些 NNMi 节点的信息。有关这些字段的信息,请参阅第 430 页的 BSM 拓扑过滤器。

8 单击表单底部的提交。

将会出现新窗口,其中显示状态消息。如果消息指出连接到 NNMi 管理服务器时发生问题,则单击**返回**,然后按照错误消息文本的建议调整值。

使用 HP NNMi-HP BSM 拓扑集成

HP NNMi-HP BSM 拓扑集成在 BSM RTSM 中填充以下 CI 类型:

• InfrastructureElement>节点

NNMi 拓扑中的节点。可以如第 430 页的 BSM 拓扑过滤器中所述对该组节点作出限制。

- InfrastructureElement > NodeElement > HardwareBoard 与集成填充在 BSM 中的节点 CI 相关联的卡。
- InfrastructureElement > NodeElement > Interface 与集成填充在 BSM 中的节点 CI 相关联的接口。
- InfrastructureElement > NodeElement > PhysicalPort
 与集成填充在 BSM 中的节点 CI 相关联的端口。
- InfrastructureElement > NetworkEntity > IpAddress 与集成填充在 BSM 中的节点 CI 相关联的接口的 IP 地址。
- InfrastructureElement > NetworkEntity > IpSubnet
 NNMi 拓扑中的所有子网。
- InfrastructureElement > NetworkEntity > Layer2Connection
 具有集成作为节点 CI 填充在 BSM 中的至少两个连接端的 NNMi 第 2 层连接。

对于在 BSM RTSM 中创建的每个 CI,集成在 NNMi 数据库中存储 RTSM 标识符。

默认情况下, NNMi不会搜索端节点。更新 NNMi 搜索和监视配置以包含要出现在 BSM 中的端节点。

作为单向通信,HPNNMi-HPBSM 拓扑集成将 NNMi 信息和更新转发到 BSM RTSM。 因为 NNMi 不会了解或控制 BSM CI 信息的使用方式,因此集成依赖于 BSM 过期删除策 略来删除设定的某段时间内未更新的 CI。

HP NNMi-HP BSM 拓扑集成使其他产品在与 BSM 集成时能够使用 NNMi 拓扑信息。没有与此集成的直接用户交互。

更改 HP NNMi-HP BSM 拓扑集成配置

- 在 NNMi 控制台中, 打开 HP NNMi-HP BSM 拓扑集成配置表单(集成模块配置 > HP BSM 拓扑)。
- 2 对值进行相应修改。有关此表单上的字段的信息,请参阅第 429 页的 HP NNMi-HP BSM 拓扑集成配置表单参考。
- 3 验证表单顶部的**启用集成**复选框是否已选中,然后单击表单底部的**提交**。
- 更改会立即生效。不需要重新启动 ovjboss。

禁用 HP NNMi-HP BSM 拓扑集成

- 在 NNMi 控制台中,打开 HP NNMi-HP BSM 拓扑集成配置表单(集成模块配置 > HP BSM 拓扑)。
- 2 清除表单顶部的启用集成复选框,然后单击表单底部的提交。集成 URL 操作不再可用。



更改会立即生效。不需要重新启动 ovjboss。

对 HP NNMi-HP BSM 拓扑集成进行故障诊断

本部分包含以下主题:

- 第 427 页的接口标签在 BSM 用户界面中显示为 MAC 地址
- 第 428 页的 RTSM 中被管节点的 CI 有重复

有关对 RTSM 连接进行故障诊断的信息,请参阅 BSM 文档套件。

接口标签在 BSM 用户界面中显示为 MAC 地址

默认情况下,对于接口标签, RTSM 优先使用 MAC 地址而非接口名称。要在 BSM 用户界 面中显示接口名称,请按第425页的步骤1中所述编辑接口模型。

RTSM 中被管节点的 CI 有重复

如果 HP Operations Manager 还与 RTSM 同步,则可能在 RTSM 中看到被管节点的 CI 有重复。HPOM 搜索的节点是 CI 类型计算机,而 NNMi 搜索的节点是 CI 类型节点。此 重复不会影响产品性能。

如果希望 RTSM 将来自 HPOM 和每个被管节点的 NNMi 的拓扑信息合并到一个 CI,请按第 425 页的步骤 2 中所述将 NNMi 设置为根据节点的 DNS 名称命名节点。RTSM 保留 每个节点的较早 CI。

应用程序故障切换和 HP NNMi-HP BSM 拓扑集成

如果 NNMi 管理服务器参与 NNMi 应用程序故障切换,则在故障切换发生之后, HP NNMi–HP BSM 拓扑集成将使用新的 NNMi 管理服务器主机名重新配置 BSM 服务器。故障切换对于集成用户应该是透明的。

集成不支持 BSM 服务器的故障切换。

HP NNMi-HP BSM 拓扑集成配置表单参考

HP NNMi-HP BSM 拓扑集成配置表单包含用于配置 NNMi 和 BSM 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。



只有具有管理员角色的 NNMi 用户才可以访问 HP NNMi-HP BSM 拓扑集成配置表单。

HP NNMi-HP BSM 拓扑集成配置表单采集以下方面的信息:

- 第 429 页的 NNMi 管理服务器连接
- 第 430 页的 BSM 网关服务器连接
- 第 430 页的 BSM 拓扑过滤器

要应用集成配置更改,请在 HP NNMi-HP BSM 拓扑集成配置表单上更新值,然后单击提交。

NNMi 管理服务器连接

表 38 列出用于连接到 NNMi 管理服务器的参数。这就是您用于打开 NNMi 控制台的信息。通过查看调用 NNMi 控制台会话的 URL,可以确定这些值中的大部分。与 NNMi 管理员协作,为配置表单的这一部分确定合适的值。

表 38 NNMi 管理服务器信息

字段	描述
启用 NNMi SSL	连接协议规范。 如果将 NNMi 控制台配置为使用 HTTPS,则选中 NNMi SSL 已启用 复选框。这是默 认配置。 如果将 NNMi 控制台配置为使用 HTTP,则清除 NNMi SSL 已启用 复选框。 集成根据此规范选择连接到 NNMi 控制台的端口。
NNMi 主机	NNMi 管理服务器的正式完全限定域名。此字段为只读。
NNMi 用户	用于连接到 NNMi Web 服务的用户名。此用户必须具有 NNMi 管理员或 Web 服务客户端角色。
NNMi 密码	指定 NNMi 用户的密码。

BSM 网关服务器连接

表 39 列出用于连接到 BSM 网关服务器以与 BSM RTSM 通信的参数。与 BSM 管理员协作,为配置的这一部分确定合适的值。

表 39 BSM 网关服务器信息

BSM 网关服务器参数	描述
启用 BSM SSL	用于连接到 BSM 的连接协议规范。 如果将 BSM 配置为使用 HTTPS,则选中启用 BSM SSL 复选框。这是默认配置。 如果将 BSM 配置为使用 HTTP,则清除启用 BSM SSL 复选框。
BSM 主机	BSM 网关服务器的完全限定域名。
BSM 端口	用于连接到 BSM 的端口。 如果正在使用默认 BSM 配置,则使用端口 80 (对于与 BSM 的非 SSL 连接)。
BSM 用户	BSM RTSM 管理员的用户名。
BSM 密码	BSM RTSM 管理员的密码。 BSM 管理员可以通过使用以下 URL 更改 BSM RTSM 管理员的密码: http:// <bsm 主机名="">:21212/ucmdb-ui/applet/applet.jsp</bsm>

BSM 拓扑过滤器

默认情况下, HP NNMi 朒 P BSM 拓扑集成将 NNMi 拓扑中所有节点和接口的相关信息 传达给 BSM。如果要集成仅在 BSM 中保留一部分 NNMi 拓扑信息,请按本部分所述指定 一个可选节点组或两个都指定。

用于过滤 NNMi 拓扑信息的场景如下:

- 定义型 在 NNMi 中,创建一个节点组以明确定义要包含在 BSM 拓扑中的每个 NNMi 节点。此方法要求您非常熟悉网络拓扑。
 - 例如,可创建名为 BSM_Topology 的节点组以包含以下类型的设备:
 - 被管环境中的应用程序服务器
 - 连接应用程序服务器的路由器和交换机

在这种情况下,将节点组(例如, BSM_Topology)指定为拓扑过滤器节点组。不要指 定其他连接节点组。

集成将转发指定拓扑过滤器节点组(例如, BSM_Topology)中每个节点的相关信息, 并忽略 NNMi 拓扑中的所有其他节点。

• 添加型 — 在 NNMi 中,标识(或创建)一个节点组以定义受监视网络的核心基础结构,然后创建另一个节点组以定义所需的端节点。

2011年3月

例如,可创建以下 NNMi 节点组:

- BSM_Core 组,包含网络基础结构设备节点组及其他主要连接设备
- BSM_End_Nodes 组,包含被管网络中的应用程序服务器

在这种情况下,将第一个节点组 (例如, BSM_Core)指定为拓扑过滤器节点组。而 且,将第二个节点组 (例如, BSM_End_Nodes)指定为其他连接节点组。

集成将转发拓扑过滤器节点组(例如,BSM_Core)中每个节点的相关信息。然后,集成将按以下方式检查其他连接节点组(例如,BSM_End_Nodes)中的每个节点:

- 如果节点连接到拓扑过滤器节点组中的一个或多个节点,则集成将该节点的相关信息转发到 BSM。
- 如果节点未连接到拓扑过滤器节点组中的任何节点,则集成将忽略该节点。

表 40 列出用于指定 BSM 拓扑过滤器的可选参数,并提供有关为这些参数输入值的信息。

表 40 BSM 拓扑过滤器信息

BSM 拓扑过滤器参数	描述
拓扑过滤器节点组	NNMi 节点组, 包含要在 BSM 中填充的该组主要节点。集成用此节点组中每个节点的相关信息填充 RTSM。
	在 NNMi 的 节点组 表单的名称字段中,输入节点组的确切名称(不带引号或额外字符)。
	如果不指定拓扑过滤器节点组,则 HP NNMi-HP BSM 拓扑集成向 RTSM 填充 NNMi 拓扑中的所有节点和接口。在这种情况下,集成忽略其他连接节点组字段的值。
其他连接节点组	NNMi 节点组,包含要在 BSM 中填充的其他节点的提示。集成仅用此节点组中(通过 NNMi 拓扑)连接到拓扑过滤器节点组中一个或多个节点的那些节点的相关信息填充 RTSM。
	在 NNMi 的 节点组 表单的名称字段中,输入节点组的确切名称(不带引号或额外字符)。
	如果指定了拓扑过滤器节点组和某个其他连接节点组,则 HP NNMi-HP BSM 拓扑集成 将转发拓扑过滤器节点组中的节点和接口的相关信息,以及该其他连接节点组中的所连接 节点的相关信息。
	如果指定拓扑过滤器节点组,但不指定其他连接节点组,则 HP NNMi-HP BSM 拓扑集成仅转发拓扑过滤器节点组中的节点和接口的相关信息。
	如果不指定拓扑过滤器节点组,则 HP NNMi-HP BSM 拓扑集成向 RTSM 填充 NNMi 拓扑中的所有节点和接口。在这种情况下,集成忽略其他连接节点组字段的值。
HP Universal CMDB

HP Universal CMDB (UCMDB) 通过与 HP 搜索和依赖性映射 (DDM) 的本机集成,自动保留关于基础结构和应用 程序关系的准确且最新的信息。UCMDB 有助于以下任务:

- 在基础结构和应用程序的更改发生之前,对更改影响建模以显示更改的波动效果。
- 通过搜索的更改历史记录,跟踪实际的计划更改和未计划更改。
- 通过知晓现有数据存储库,获得环境的共享授权视图。

有关购买 UCMDB 的信息,请联系 HP 销售代表。

本章包含以下主题:

- HP NNMi-HP UCMDB 集成
- 使用 HP NNMi-HP UCMDB 集成

HP NNMi-HP UCMDB 集成

HP NNMi-HP UCMDB 集成与 UCMDB 共享 NNMi 拓扑信息。UCMDB 将 NNMi 拓 扑中的每个设备存储为配置项 (CI)。UCMDB 将搜索和依赖性映射 (DDM) 模式应用到 CI,以便让 NNMi 拓扑预测设备故障的影响。可以通过 UCMDB 用户界面或 NNMi 控制 台获取此影响分析。

此外,集成将所填充 CI 的标识符存储到 NNMi 数据库中。由 NNMi 所管理设备的 CI 的 使用情况包括:

- HP NNMi 桯 P BSM Operations Management 集成可以将关于 NNMi 所管理设备的 事件与 UCMDB CI 关联。有关详细信息,请参阅第 526 页的配置项标识符。
- HP NNMi 脑 POM 集成的代理实施可以将关于 NNMi 所管理设备的事件与 UCMDB CI 关联。有关详细信息,请参阅第 546 页的配置项标识符。

价值

HP NNMi-HP UCMDB 集成将 NNMi 设置为网络设备关系的权威性源。集成提供从 NNMi 控制台对 UCMDB 影响分析和 CI 详细信息的访问。

集成产品

本章中的信息适用于以下产品:

• UCMDB

1

有关受支持版本的列表,请参阅NNMi系统和设备支持列表。

• NNMi 9.10

NNMi 和 UCMDB 不能安装在同一台计算机上。这两个产品必须按以下任一配置安装在不同计算机上:

- 不同操作系统。例如, NNMi 管理服务器是 Linux 系统, 而 UCMDB 服务器是 Windows 系统。
- 相同操作系统。例如, NNMi 管理服务器是 Windows 系统, 而 UCMDB 服务器是另 一个 Windows 系统。

有关受支持的硬件平台和操作系统的最新信息,请参阅这两种产品的支持列表。

文档

UCMDB 产品介质上所含的《搜索和集成内容指南》的"Network Node Manager i (NNMi) 与 HP Universal CMDB 集成"一章中完整描述了 HP NNMi-HP UCMDB 集成。

使用 HP NNMi-HP UCMDB 集成



NNMi 不能同时与 HP Business Service Management (BSM) 拓扑和 HP UCMDB 集成。 如果在此 NNMi 管理服务器上配置了 HP NNMi-HP BSM 拓扑集成,请先禁用该配置, 然后再启用 HP NNMi-HP UCMDB 集成。如果您需要这两个数据库中的 NNMi 信息,则 以任意顺序执行以下 两个操作:

- 如第 423 页的 HP Business Service Management 拓扑中所述配置 HP NNMi-HP BSM 拓扑集成。
- 配置 BSM 与 UCMDB 的集成,如 UCMDB 产品介质上所含的《UCMDB 数据流管理 指南》中所述。对于 UCMDB 产品,还可从以下地址获取本手册: http://h20230.www2.hp.com/selfsolve/manuals

有关启用、使用和禁用 HP NNMi–HP UCMDB 集成以及对它进行故障诊断的信息,请参 阅 "Network Node Manager i (NNMi) 与 HP Universal CMDB 集成"。

HP Business Availability Center My BSM

HP Business Availability Center (BAC) 软件提供的工具用于在生产中管理应用程序的可用性、监视系统性能、监视基础结构性能以及在出现问题时主动解决问题。BAC 包括 My BSM 门户,用于查看报告和实时产品性能信息。(在 BAC V8.00 之前,该门户称为 My BAC。)

本章包含以下主题:

- HP NNMi-HP BAC My BSM 集成
- My BSM 的默认 NNMi 模块
- 配置演示 **Portlet**
- 创建自定义 NNMi Portlet
- 为 HP NNMi-HP BAC My BSM 集成配置单点登录
- 对 HP NNMi-HP BAC My BSM 集成进行故障诊断
- HP NNMi-HP BAC My BSM 配置表单参考

HP NNMi-HP BAC My BSM 集成

HP NNMi-HP BAC My BSM 集成用于在 My BSM 门户中查看 NNMi。集成提供了模板,用于将 NNMi 和 NNM iSPI for Performance Portlet 添加到 My BSM 门户中。要查看快速门户演示,可以使用 NNMi 控制台中的配置工具针对环境自定义这些模板。

My BSM 管理员可以使用 My BSM 标准管理界面进一步自定义默认 Portlet 的配置和访问 权限。 My BSM 管理员还可以使用 My BSM 管理界面为 NNMi 和 NNMi Smart Plug-in (NNM iSPI) 的其他视图创建自定义 Portlet,并在一个门户页上组合多个 NNMi 管理服务 器的视图。

价值

HP NNMi-HP BAC My BSM 集成扩展了通过 My BSM 门户提供的信息。

集成产品

本章中的信息适用于以下产品:

• BAC

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

要与 BAC V9.x 集成,请使用 BAC 组件库。

• NNMi 9.10

有关受支持的硬件平台和操作系统的最新信息,请参阅这两种产品的支持列表。

文档

本章描述如何从 NNMi 控制台配置 My BSM 的默认 NNMi Portlet。 《使用 My BAC 指南》包含在 BAC 7.x 产品介质上,描述如何配置和维护 My BAC。 《使用 My BSM 指南》包含在 BAC 8.x 产品介质上,描述如何配置和维护 My BSM。

My BSM 的默认 NNMi 模块

NNMi 为 NNMi 控制台中的配置提供以下 My BSM 模块:

- NNMi 演示模块在 NOC_Demo_Portal.xml 模板文件中定义。此模块显示表 41 中描述 的某些关键网络状态信息。
- NNMi 和 NNM iSPI for Performance 演示模块在 NOC_Demo_Portal_iSPIPerf.xml 模板文件中定义。此模块将某些 NNM iSPI for Performance 报告添加到 NNMi 演示 模块的网络状态信息中。第 437 页的表 42 描述了此模块。

表 41 NNMi 演示模块内容

页	Portlet	Portlet 描述
概述图	关键操作图	指定节点组的 NNMi 拓扑图。
网络状态 / 设备运行状况	节点组状态	等价于 NNMi 控制台中对指定节点组执行 操作 > 状态详细信息菜单命令的结果。
	网络状态	等价于 NNMi 控制台中的 节点组 资产视图。

表 42 NNMi 和 NNM iSPI for Performance 演示模块内容

页	Portlet	Portlet 描述
概述图	关键操作图	指定节点组的 NNMi 拓扑图。
网络状态 / 设备运行状况	节点组状态	等价于 NNMi 控制台中对指定节点组执行 操作 > 状态详细信息菜单命令的结果。
	网络状态	等价于 NNMi 控制台中的 节点组 资产视图。
	内存利用率排名前 N 名	实时 NNM iSPI for Performance 组件运行状况报告,显示内存利用率排名前 10 名的节点。
	CPU 利用率排名前 N 名	实时 NNM iSPI for Performance 组件运行状况 报告,显示 CPU 利用率排名前 10 名的节点。
NNM iSPI for Performance 异常	组件异常数排名前 N 名的设备	实时 NNM iSPI for Performance 组件运行状况仪表板,显示 CPU 使用异常数排名前 5 名的节点和内存使用异常数排名前 5 名的节点。

配置演示 Portlet

本部分描述 My BSM 演示模块的初始配置。My BSM 管理员可以完全自定义 Portlet 内容 和对 Portlet 的用户权限。

- 1 在 NNMi 管理服务器上, 创建模块配置 XML 文件:
 - a 在 NNMi 控制台中,打开 HP NNMi-HP BAC My BSM 配置表单(集成模块配置> HP BAC 我的 BSM)。
 - b 选择一个要自定义的已命名 XML 文件:
 - 如果未在环境中安装 NNM iSPI for Performance,则选择 NOC_Demo_Portal.xml 文件。
 - 如果已在环境中安装 NNM iSPI for Performance,则选择 NOC Demo Portal iSPIPerf.xml 文件。
 - c 单击**加载**。
 - d 在 HP NNMi-HP BAC My BSM 配置表单的每一页上,根据需要编辑提供的文本,然 后单击下一步。有关这些字段的信息,请参阅第 444 页的 HP NNMi-HP BAC My BSM 配置表单参考。
 - e 浏览所有 HP NNMi-HP BAC My BSM 配置表单页后,请单击完成,然后将 XML 文件 保存到计算机上的已知位置。
 - f 关闭 HP NNMi-HP BAC My BSM 配置表单。
- 2 将模块配置导入 BAC 中:
 - a 在 BAC **管理**选项卡上,在 My BSM (或 My BAC)下面,单击导入 Portlet 和模块 (某个用于管理 Portlet 定义的选项)。
 - b 在导入 My BSM 对象页(或导入 My BAC 对象页)上,单击浏览,然后选择从 NNMi 控制台保存的 XML 文件。
 - c 选中替换相同 Portlet 定义复选框。
 - d 选中替换相同模块复选框。
 - e 单击导入。

导入状态窗口显示操作的结果。如果导入未成功,则验证是否已同时选中这两个复选框,然后重试导入。

- 3 在 My BSM 或 My BAC 中查看模块:
 - 验证每个 Portlet 是否显示预期的信息。
 - 使用 My BSM 或 My BAC 管理工具来定义哪些用户可以访问新 Portlet、重新组 织页和编辑 Portlet 定义等。

创建自定义 NNMi Portlet

创建显示 NNMi 或 iSPI 信息的新 Portlet 的最简单方法如下:

- 1 在 My BSM 管理界面中,复制现有的 NNMi Portlet 定义。
- 2 在新 Portlet 定义中更改 URL 以指向要在门户中显示的信息。

当编辑 Portlet 定义时,请遵循演示 Portlet 中使用的 HTML 代码结构。有关 HTML 代码结构的描述,请参阅第 440 页的 Portlet 定义 HTML 参考。

有关如何创建用于直接启动 NNMi 控制台窗口的 URL 的信息,请参阅 NNMi 控制台中的

确定 Portlet URL

NNMi 控制台窗口 的 URL

NNM iSPl for 确定用于启动 NNM iSPl for Performance 报告的 URL 的过程取决于使用什么 Web 浏览 Performance 报告 器查看报告。 的 URL



用于访问报告的 URL 在任何 Web 浏览器中都相同。

帮助 > NNMi 文档库 > 在别处将 NNMi 与 URL 集成。

在 Mozilla Firefox 中,要确定用于启动 NNM iSPI for Performance 报告的 URL,请遵循以下步骤:

- 1 运行 NNM iSPI for Performance 报告。
- 2 *可选。*在报告顶部单击显示选项,然后自定义报告视图。
- 3 在报告顶部单击显示 URL。

报告的 URL 显示在报告横幅和自定义链接下面。可以复制此 URL 以在 Portlet 定义 中使用。

4 可选。单击隐藏 URL,从视图中隐藏报告 URL。

在 Microsoft Internet Explorer 中,要确定用于启动 NNM iSPI for Performance 报告的 URL,请遵循以下步骤:

- 1 运行 NNM iSPI for Performance 报告。
- 2 *可选*。在报告顶部单击显示选项,然后自定义报告视图。
- 3 在报告顶部单击添加书签。
- 4 在添加收藏窗口中,单击添加。
- 5 在收藏夹列表中,右键单击在步骤 4 中创建的收藏,然后单击**属性**。
 - URL 字段显示报告的 URL。可以从此字段中复制此 URL 以在 Portlet 定义中使用。

Portlet 定义 HTML 参考

以下规则适用于 BAC 中的 HTMLPortlet 类型:

- 使用单引号('),而不是标准的双引号(")。
- 对每个 iframe 开始标记 (<iframe>) 使用相应的 iframe 结束标记 (</iframe>), 因为 某些 Web 浏览器无法正确识别空元素 <iframe/> 标记。
- 在 iframe 定义中,为 id 指定以下其中一个值:

ID 值	描述
nnmi-portlet	显示 NNMi URL 的 iframe 的 ID。此 ID 对于用户提供一致配置。
nnmi-auth	管理单点登录 NNM iSPI for Performance 的 iframe 的 ID。 用于加载 NNM iSPI for Performance Portlet 的 JavaScript 函数将解释此 ID 值。
ispiperf-portlet	显示 NNM iSPI for Performance 报告 URL 的 iframe 的 ID。用于加载 NNM iSPI for Performance Portlet 的 JavaScript 函数将解释此 ID 值。

NNMi Portlet HTML 显示 NNMi URL 的 BAC Portlet 只包含一个识别要显示的 NNMi URL 的单个 iframe 元 结构 素。结构如下:

```
紊。结构如下:
```

```
<html>
<head></head>
<body>
<iframe id='nnmi-portlet' src='<NNMi_URL>'></iframe>
</body>
</html>
```

将 <NNMi URL> 替换为用于启动 NNMi 控制台窗口的 URL。

例如,以下代码定义显示路由器节点组状态的 Portlet。在此示例中,高度和宽度值是此 Portlet 的建议值。可以根据需要更改这些值。

```
<html>
<head></head>
<body>
<iframe id='nnmi-portlet'
src='http://nnmi.example.com:8004/nnm/launch
?cmd=runTool
&tool=nodegroupstatus
&nodegroup=Routers
&menus=false'
width='100%'
height='425px'>
</iframe>
</body>
</html>
```

2011年3月

NNM iSPI for Performance Portlet HTML 结构

显示 NNM iSPI for Performance 报告 URL 的 BAC Portlet 包含以下元素:

- 在 Portlet 标题中,有 loadIspiPerf() JavaScript 函数的声明。此声明定义要显示 的 NNM iSPI for Performance 报告。
- 一个 iframe 元素,处理从 NNMi 到 NNM iSPI for Performance 的单点登录。
- 第二个 iframe 元素,显示 Portlet 标题的 loadIspiPerf() 函数声明中命名的 NNM iSPI for Performance 报告。

显示 NNM iSPI for Performance 报告 URL 的 BAC Portlet 的结构如下:

```
<ht.ml>
<head>
<script id='ispiperf-load'>function loadIspiPerf()
{
 var ispiperf url='<报告 URL>';
 document.getElementById('ispiperf-portlet').src =
   ispiperf url;
}
</script>
</head>
<body onload='loadIspiPerf();'>
<iframe id='nnmi-auth'
  src='http:</NNMi 主机>:</NNMi 端口>/nnm/launch?cmd=isRunning'>
</iframe>
<iframe id='ispiperf-portlet'></iframe>
</body>
</html>
```

将 < 报告 URL> 替换为用于启动 NNM iSPI for Performance 报告的 URL。将 < NNMi 主机> 和 < NNMi 端口> 分别替换为 NNMi 管理服务器的完全限定域名和访问 NNMi 的端口号。

例如,以下代码定义显示前 N 个节点的节点运行状况报告的 Portlet。在此示例中,高度和 宽度值是此 Portlet 的建议值。可以根据需要更改这些值。

```
<html>
<head>
<script id='ispiperf-load'>function loadIspiPerf()
 var ispiperf url=
    'http://nnmi.example.com:8004/ssoservlet/protected
    /reports
      ?reportURL=http://ispiperf.example.com:9300/PerfSpi
      /PerfSpi
        ?package=NodeHealth
          &report=Top%20N%20Live
          &element=All%20Nodes/Components&timeperiod=
          &dow=
          &hod=
          &metric=CPU%20Utilization%20(Avg%25)
          &namespaceID=ErsAuthenticationProvider
          &ssoDomain=example.com';
```

```
document.getElementById('ispiperf-portlet').src =
    ispiperf url;
}
</script>
</head>
<body onload='loadIspiPerf();'>
<iframe id='nnmi-auth'
 src='http://nnmi.example.com:8004/nnm/launch
    ?cmd=isRunning'
 width='100%'
 height='1px'>
</iframe>
<iframe id='ispiperf-portlet'
 width='100%'
 height='750px'>
</iframe>
</body>
</html>
```

为 HP NNMi-HP BAC My BSM 集成配置单点登录

使用相同初始化字符串值并且还共享通用网络域名的所有 HP 企业应用程序都可以使用单点登录。有关配置 BAC My BSM 单点登录的信息,请参阅第 143 页的配置 NNMi 和 HP BSM 或 HP BAC 之间的单点登录。

对 HP NNMi-HP BAC My BSM 集成进行故障诊断

NNMi Portlet 作为登录页显示

验证单点登录配置:

- 使用 My BSM 的登录用户名登录 NNMi 控制台。
 如果登录未成功,则请求 NNMi 管理员为 My BSM 用户配置一个帐户。
- 2 确保 BAC 和 NNMi 使用第 442 页的为 HP NNMi-HP BAC My BSM 集成配置单点 登录中所述的相同初始化字符串。

另请参阅第443页的单点登录未正常运行。

NNMi Portlet 未正确加载

在 My BSM 管理界面中,验证 Portlet URL 中的 NNMi 管理服务器主机名和端口号。

NNM iSPI for Performance Portlet 未正确加载

在 My BSM 管理界面中, 验证 Portlet URL 中的 NNM iSPI for Performance 服务器主机 名、端口号和单点登录域。

NNM iSPI for Performance Portlet 显示 AsynchWait_Requests 错误

当 BAC 门户页加载 NNM iSPI for Performance Portlet 时,它从 NNM iSPI for Performance Cognos 数据库请求信息。当一个页面包含多个 NNM iSPI for Performance Portlet 时,来自单个 Web 浏览器会话的对 Cognos 数据库的同时请求会导致 AsynchWait_Requests 错误。重新加载门户页。

单点登录未正常运行

所有 NNMi 和 NNM iSPI for Performance Portlet 都未加载。Web 浏览器可能关闭,同时显示内容类似如下的消息:

由于 LW-SSO 主机已退出,因此无法显示请求的页。

验证参与单点登录集成的所有应用程序服务器是否都设置为最大时差为 15 分钟的同一 GMT 时间。

保存 Portlet 定义时, My BSM 报告 HTML 验证错误

必须在 BAC 配置文件中配置设置,然后才能在 My BSM 中保存新 Portlet。

编辑 <HP Business Availability Center 根目录>\HPBAC\ conf\dashboard.properties 文件,在其中添加以下行:

Block-URL-Injections=false

HP NNMi-HP BAC My BSM 配置表单参考

表 43 列出 HP NNMi-HP BAC My BSM 配置表单页上包含的字段。与 NNM iSPI for Performance 管理员协商以确定 NNM iSPI for Performance 字段的正确值。文本字段可 以包含任何字符。 NNMi 不验证配置的值。验证 My BSM 门户中的新 Portlet。

表 43 模块配置信息

字段	描述
名称	门户模块的名称。此文本有助于在 My BSM 门户中导航。
描述	描述门户模块的文本。此文本显示在 My BSM 管理界面中。
页面标题	门户页的名称。此文本有助于在门户中导航。
Portlet 标题	Portlet 在门户中的显示名称。
Portlet 类型	My BSM 配置所需的字段。此字段当前为只读。
NNMi 计算机	用于访问 NNMi 管理服务器的 URL。此字段中预填充了主机名和端口号以便为当前 NNMi 控制台会话连接到 NNMi 管理服务器。 • 如果希望 Portlet 访问默认 NNMi 管理服务器,请保留默认设置。 • 如果希望 Portlet 访问其他 NNMi 管理服务器,请手动输入正确的 URL。
NNMi 节点组	当前 NNMi 控制台会话的 NNMi 管理服务器上的节点组列表。 如果 Portlet 访问默认 NNMi 管理服务器,请从列表中选择节点组。 如果 Portlet 访问其他 NNMi 管理服务器,请手动输入正确的节点组名称。
iSPI for Performance 计算机	用于访问 NNM iSPI for Performance 服务器的 URL。此字段中预填充了用于从当前 NNMi 控制台会话连接到 NNM iSPI for Performance 服务器的主机名和端口号。 • 如果希望 Portlet 访问默认 NNM iSPI for Performance 服务器,请保留默认设置。 • 如果希望 Portlet 访问其他 NNM iSPI for Performance 服务器,请手动输入正确的 URL。

2011年3月

表 43 模块配置信息(续)

字段	描述
SSO 域	用于单点登录 NNM iSPI for Performance 的域。
禁用 iSPI for Performance Portlet 复选框	禁用 iSPI for Performance Portlet 复选框在定义 Portlet 对 NNM iSPI for Performance 的访问的配置表单页上提供。 如果在此页第一次显示时选中此复选框,则不在 NNMi 管理服务器上配置 NNM iSPI for Performance。因此,与 NNM iSPI for Performance 相关的字段未设置。 清除此复选框以启用字段,以便可以手动输入用于访问 NNM iSPI for Performance 的 信息。

HP Network Automation

HP Network Automation 软件 (NA) 通过以流程支持的自动化,跨全球分布的多供应商网络跟踪、管理并自动执行 配置和软件更改。

有关购买 NA 的信息,请联系 HP 销售代表。

本章包含以下主题:

- HP NNMi-HP NA 集成
- 启用 HP NNMi-HP NA 集成
- 使用 HP NNMi-HP NA 集成
- 更改 HP NNMi-HP NA 集成
- 禁用 HP NNMi-HP NA 集成
- 对 HP NNMi-HP NA 集成进行故障诊断
- HP NNMi-HP NA 集成配置表单参考
- HP NNMi-HP NA 集成配置表单参考
- NA 参考中的 NNMi 集成配置

HP NNMi-HP NA 集成

HP NNMi-HP NA 集成将 NA 配置更改检测功能与 NNMi 网络监视功能相结合,可以在问题发生时为您提供详细信息。



NNMi 与 Cisco Network Compliance Manager (NCM) 集成的工作方式和 HP NNMi– HP NA 集成相同。本章内容还适用于 HP NNMi–Cisco NCM 集成。 此集成提供以下功能:

- 使 NNMi 与 NA 拓扑同步,以降低所提供设备的拥有成本并提高管理覆盖率。
- 某些 NNMi 事件发生时,自动运行 NA 设备诊断。
- NA应用设备配置更新而导致设备服务中断时,阻止 NNMi发出不必要的警报。
- 使用用于访问被管设备的信息更新 NNMi 配置。

此外,您无需退出 NNMi 控制台即可连接到 NA 以查看有关 NA 所管理设备和配置更改事件的信息。当您处于 NA 中时,可以执行您具有所需凭证的任何 NA 功能。

HP NNMi-HP NA 集成将菜单项添加到 NNMi 控制台,用于打开与 NA 的连接以及查看 由 NA 管理的设备的配置信息。这些工具提供以下功能:

- 查看详细设备信息,包括供应商、型号、模块、操作系统版本和最新诊断结果。
- 查看设备配置更改和配置历史。
- 比较配置 (通常是最近的与最早的配置),以了解更改内容、更改原因以及更改人员。
- 查看设备符合性信息。
- 从 NNMi 节点运行 NA 诊断和命令脚本。
- 检测具有不匹配速度或双工配置的连接。

这些功能不可用于 NA 中未配置的网络设备以及禁用了更改检测的 NA 设备。

价值

HP NNMi-HP NA 集成在已在运行 NNMi 和 NA 的环境中提供以下功能和好处:

- 报警集成 NNMi 集成将 NA 配置更改信息传达给 NNMi 控制台,使您能够快速确定 配置更改是否可能已经导致网络问题。从 NNMi 内部,您可以快速访问 NA 功能以查 看特定配置更改和设备信息,确定执行更改的人员,并回滚到之前配置以恢复网络操 作。因为大部分网络中断由设备配置错误导致,所以此功能可以改进解决网络故障的问 题确定和响应时间。
- 从 NNMi 访问 NA 配置历史 在 NNMi 控制台中,设备级别菜单用于访问 NA 功能 以查看配置更改。对于 NA 数据库中的任何设备,此功能并排显示配置更改,使您可以 方便地查看。您还可以查看配置历史。
- 操作效率 网络操作人员可以在单个屏幕中监视和调查来自两个数据源的信息。

集成产品

本章中的信息适用于以下产品:

• NA

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

• NNMi 9.10

此集成不再需要 NNM iSPI NET 许可证。

集成限于与一个 NNMi 管理服务器连接的一个 NA 服务器。NNMi 和 NA 必须处于同一网 段 (也叫 NA 域)中。

NNMi 和 NA 可以安装在相同或不同的计算机上。



要使 NNMi 和 NA 在同一台计算机上正常运行,必须先安装 NNMi 再安装 NA。

这两个产品可以按以下任一配置安装在不同计算机上:

- 不同操作系统。例如, NNMi 管理服务器是 Linux 系统, 而 NA 服务器是 Windows 系统。
- 相同操作系统。例如, NNMi 管理服务器是 Windows 系统, 而 NA 服务器是另一个 Windows 系统。

有关受支持的硬件平台和操作系统的最新信息,请参阅这两种产品的支持列表。

文档

本章描述如何配置和使用集成。

启用 HP NNMi-HP NA 集成

启用 HP NNMi — HP NA 集成就会将 NNMi 管理服务器设置为托管环境中的主定义拓 扑。在 NNMi 中,创建包含节点的一个节点组,以便与 NA 资产同步。此集成会将此节点 组的内容与 NA 默认站点分区同步,如第 453 页的 NNMi 和 NA 之间的拓扑同步中所述。

本部分描述以下过程:

- 第 450 页的从 NNMi 9.0x 升级的集成配置
- 第 451 页的新集成配置

从 NNMi 9.0x 升级的集成配置

在 NNMi 版本 9.10 之前, NA 提供了 NNMi 连接器工具, 用于在 NNMi 和 NA 之间建立 通信。 NNMi 现在提供此功能; NA 提供的 NNMi 连接器不再使用。

如果 HP NNMi—HP NA 集成是在 NNMi 9.0x 管理服务器上配置的,则升级到 NNMi 9.10 的过程将禁用此集成(但保留配置值)。NA 数据库中的对象仍然包含 NNMi UUID,并且 将在您从升级后的 NNMi 管理服务器启用集成时与当前 NNMi 拓扑同步。

此集成现在提供 NNMi 控制台与 NA 用户界面之间的单点登录。

要对 NNMi 9.10 管理服务器启用 HP NNMi-HP NA 集成,请遵循以下步骤:

- 1 验证 NA 是否已升级到受支持版本,如 NNMi 系统和设备支持列表的"集成"部分 所列。
- 2 从 NNMi 管理服务器卸载 NNMi 连接器:
 - Windows: 打开控制面板, 单击**添加或删除程序**, 然后删除 HP NA HP Network Node Manager 连接器。
 - *Linux 或 Solaris*:运行以下命令:

\$NAINSTALLDIR/UninstallConnector/Uninstall\ NA

\$NAINSTALLDIR 的默认值是 /opt/NA。

- 3 从系统删除残余的 integration.jar 文件:
 - a 停止 NA ManagementEngine 服务:
 - Windows: 打开服务控制面板 (开始 > 设置 > 控制面板 > 管理工具 > 服务)。在服务列表中,右键单击 TrueControl ManagementEngine,然后单击停止。
 - *Linux 或 Solaris*:运行以下命令:

/etc/init.d/truecontrol stop

- b 手动从以下位置删除 integration.jar 文件:
 - *Windows*: %NAINSTALLDIR%\server\ext\jboss\server\default\ integration.jar
 - *Linux 或 Solaris*: \$NAINSTALLDIR/server/ext/jboss/server/default/ integration.jar
- c 重新启动 NA ManagementEngine 服务:
 - *Windows*:打开**服务**控制面板 (**开始 > 控制面板 > 管理工具 > 服务**)。在服务列 表中,右键单击 TrueControl ManagementEngine,然后单击启动。
 - *Linux 或 Solaris*:运行以下命令:

/etc/init.d/truecontrol restart

4 *可选*。如第 145 页的配置 NNMi 和 HP NA 之间的单点登录中所述, 配置 NNMi 和 NA 之间的单点登录。

- 5 在 NNMi 控制台中, 配置从 NNMi 到 NA 的连接:
 - a 打开 HP NNMi-HP NA 集成配置表单 (集成模块配置 > HP NA)。
 - b 选中**启用集成**复选框以激活表单上的其余字段。

HP NNMi-HP NA 集成配置表单包含来自 NNMi 9.0x 配置的值。此表单上的新字段 设置为其默认值。

c 输入新集成配置字段(**拓扑过滤器节点组、拓扑同步间隔**和**在 NA 中搜索设备驱动程序**) 的值。

有关这些字段的信息,请参阅第466页的集成行为。

d 单击表单底部的提交。

将会出现新窗口,其中显示状态消息。如果消息指出连接到 NA 服务器时发生问题,则单击**返回**,然后按照错误消息文本的建议调整用于连接到 NA 服务器的值。

6 如果 NNMi 控制台操作菜单上的 NA 菜单项不可用,请退出 NNMi 控制台再重新 登录。

新集成配置

要启用 HP NNMi-HP NA 集成,请遵循以下步骤:

- 1 *可选*。如第 145 页的配置 NNMi 和 HP NA 之间的单点登录中所述, 配置 NNMi 和 NA 之间的单点登录。
- 2 *可选*。如果希望此集成搜索已同步拓扑中的设备上的驱动程序,请在 NNMi 拓扑中指 定节点的 SNMP 配置。在 NA 用户界面中,遵循以下步骤:
 - **α** 打开**设备密码规则**页 (**设备 > 设备工具 > 设备密码规则**)。
 - b 创建指定如何与 NNMi 拓扑中的节点通信的一个或多个密码规则。
- 3 在 NNMi 控制台中, 配置从 NNMi 到 NA 的连接:
 - a 打开 HP NNMi-HP NA 集成配置表单 (集成模块配置 > HP NA)。
 - b 选中**启用集成**复选框以激活表单上的其余字段。
 - c 输入用于连接到 NNMi 管理服务器的信息。有关这些字段的信息,请参阅第 465 页 的 NNMi 管理服务器连接。
 - d 输入用于连接到 NA 服务器的信息。有关这些字段的信息,请参阅第 465 页的 NA 服务器连接。

- e 输入剩余字段的值: 有关这些字段的信息,请参阅第466页的集成行为。
- f 单击表单底部的**提交**。

将会出现新窗口,其中显示状态消息。如果消息指出连接到 NA 服务器时发生问题,则单击**返回**,然后按照错误消息文本的建议调整用于连接到 NA 服务器的值。

- 4 可选。在 NA 用户界面中,改变此集成提供的 NA 功能的默认设置:
 - a 打开管理设置 第三方集成页 (管理 > 管理设置 > 第三方集成)。
 - b 验证是否为**第三方集成**选择了**已启用**。
 - c 更改以下任何字段的选择:
 - 任务完成后重新搜索主机
 - 服务中断事件
 - 如果设备任务失败
 - 如果任务完成之后,设备符合性检查失败
 - 传播 SNMP 共用字符串

有关这些字段的信息,请参阅第 467 页的 NA 参考中的 NNMi 集成配置。

- d 单击页面底部的保存。
- 5 *可选*。如果希望集成检测具有不匹配速度或双工配置的连接,请填充 NA 拓扑中 NNMi 设备的接口 MAC 地址。在 NA 用户界面中,遵循以下步骤:
 - a 对于 NNMi 拓扑中的每个节点,验证在 NA 资产中的相应设备上是否设置了 NNMUuid 属性。

集成拓扑同步过程设置 NNMUuid 属性。在 NA 中的设备页的设备详细信息部分列 出此属性。

b 在**设备密码规则**页(**设备 > 设备工具 > 设备密码规则**)上,创建指定如何与 NNMi 拓 扑中的节点通信的一个或多个密码规则。

如果在第451页的步骤2中创建了密码规则,则不需要再次创建。

c 在新建任务 — 搜索驱动程序页 (设备 > 设备 > 搜索驱动程序)上,为从 NNMi 拓 扑导入的设备搜索驱动程序。

如果您已将集成配置为搜索驱动程序,则集成已完成此步骤。

- d 为从 NNMi 拓扑导入的设备创建快照 (设备 > 设备任务 > 拍摄快照)。 如果您已将集成配置为搜索驱动程序,则集成已完成此步骤。
- e 对从 NNMi 拓扑导入的设备运行 NA 拓扑数据采集诊断 (设备 > 设备 > 运行 诊断)。

f 验证与 NNMi 拓扑同步的每个设备的每个接口是否都有一个 MAC 地址。

在设备页上,单击视图 > 设备详细信息 > MAC 地址,以显示该设备的 MAC 地址。

6 如果 NNMi 控制台操作菜单上的 NA 菜单项不可用,请退出 NNMi 控制台再重新 登录。

使用 HP NNMi-HP NA 集成

HP NNMi-HP NA 集成将功能添加到 NNMi 和 NA。本部分包含以下主题:

- 第 453 页的 NNMi 和 NA 之间的拓扑同步
- 第 455 页的由集成提供的 NNMi 功能
- 第 458 页的由集成提供的 NA 功能

NNMi 和 NA 之间的拓扑同步

HP NNMi-HP NA 集成将所指定 NNMi 同步节点组中的节点的拓扑与 NA 默认站点分区 中的设备进行动态同步。集成通过比较主机名和 IP 地址(如有必要),将 NNMi 节点与 NA 设备进行匹配。集成将 NA ID 添加到同步后的每个 NNMi 节点,将 NNMi UUID 添 加到同步后的每个 NA 设备。

HP NNMi-HP NA 集成配置表单上的拓扑过滤器节点组参数指定 NNMi 同步节点组。

此同步按以下方式发生:

- 在 HP NNMi-HP NA 集成配置表单上首次启用集成时,集成在 NNMi 同步节点组和 NA 默认站点分区之间执行完整拓扑同步。
 - 如果同步节点组中的任何 NNMi 节点不在 NA 中,则集成会将这些节点添加到 NA 默认站点分区。
 - 如果同步节点组中的任何 NNMi 节点已经存在于 NA 中,但不在 NA 默认站点分 区中,集成会将这些设备移动到 NA 默认站点分区。
 - 如果 NA 默认站点分区中的任何设备不在 NNMi 同步节点组中,则集成会向 NNMi 发送这些设备的搜索提示。 NNMi 自动搜索规则配置确定是否搜索这些节点。 NNMi 节点组配置确定哪些节点组包括 NA 提示的设备。
 - NA 默认站点分区可能包含不在 NNMi 同步节点组中的节点。同步完成之后,NNMi 同步节点组中的所有节点都在 NA 默认站点分区中。

- 初始同步之后,集成按如下方式维护拓扑同步:
 - 将新节点添加到 NNMi 同步节点组时,集成在 NA 默认站点分区中创建此设备。
 - 将新设备添加到 NA 默认站点分区时,集成将搜索提示发送到 NNMi。
 - 从 NNMi 删除同步的节点时,集成将取消管理 NA 中的相应设备。NA 中不非被管 设备的设备历史仍然可用。
 - 从 NA 删除同步的设备时,集成将从 NNMi 拓扑删除相应节点。
 - 同步节点从 NNMi 同步节点组移出到不同节点组时,不立即影响 NA 资产。但是,如果稍后从 NNMi 删除此节点,集成将取消管理 NA 中的相应设备。同样,如果稍后从 NA 删除此节点,集成将从 NNMi 拓扑删除相应节点。
 - 集成在两个产品之间定期执行完整拓扑同步。除了集成不向 NNMi 发送在 NA 资产中但不在 NNMi 拓扑中的设备的额外搜索提示外,此定期同步的过程与首次启用集成时发生的过程相同。

HP NNMi-HP NA 集成配置表单上的拓扑同步间隔参数指定定期拓扑同步的频率。

定期同步注意事项

选择拓扑同步间隔时,请考虑以下准则:

- 拓扑同步是防故障机制。如果 NNMi 管理服务器与 NA 服务器之间的连接非常可靠,则拓扑同步间隔可以大一些。
- 对于不超过 500 的同步节点,建议的最小拓扑同步间隔是 24 小时。每增加 500 个同步 节点,考虑另增 24 (或更多)小时。

定期拓扑同步与 NNMi 螺旋搜索进行负载平衡,其节奏是为了避免 NNMi 管理服务器负载 过高。在搜索活动活跃期间,不进行拓扑同步。

支持 HP Blade System Virtual Connect 设备

HP Blade System Virtual Connect 设备可以组合起来形成一个由一台主设备和一台或多 台备用和从属设备组成的 Virtual Connect 域。集成应向 NA 资产只传递有关充当域主设 备或独立设备的 Virtual Connect 设备的信息。 要限制与 NA 资产同步的 Virtual Connect 设备,请遵循以下步骤:

- 1 根据使用以下任何功能的其他过滤器创建一个或多个 NNMi 节点组:
 - com.hp.nnm.capability.node.hpvcStandalone
 - com.hp.nnm.capability.node.hpvcPrimary
 - com.hp.nnm.capability.node.hpvcStandby
 - com.hp.nnm.capability.node.hpvcSlave
- 2 为步骤1中创建的所有节点组创建一个父节点组。

在此父节点组中,还包括所有其他应与 NA 资产同步的设备。

3 用父节点组的名称更新 HP NNMi-HP NA 集成配置表单上的拓扑过滤器节点组参数。有关 详细信息,请参阅第 466 页的集成行为。

由集成提供的 NNMi 功能

HP NNMi-HP NA 集成对从 NNMi 到 NA 的通信提供以下功能:

- 第 455 页的从 NNMi 控制台启动 NA 视图
- 第 456 页的将 NA 诊断和命令脚本配置为事件操作
- 第 457 页的查看用于访问 NA 的事件操作的结果
- 第457页的识别具有不匹配状态的第2层连接

从 NNMi 控制台启动 NA 视图

HP NNMi-HP NA 集成提供从 NNMi 控制台到 NA 的链接。

启用 HP NNMi-HP NA 集成会将以下项添加到 NNMi 控制台中的操作菜单:

- 显示 HP NA 诊断结果 显示已对 NNMi 事件中的设备安排的 NA 任务的列表。选择任务以查看任务结果。有关详细信息,请参阅第 457 页的查看用于访问 NA 的事件操作的结果。
- **重新运行 HP NA 诊断** 运行为 NNMi 事件中的设备配置的任何 NA 操作。有关详细信息,请参阅第 457 页的查看用于访问 NA 的事件操作的结果。
- **显示不匹配的连接** 显示具有可能的速度差异或双工配置差异的所有第 2 层连接的表。 有关详细信息,请参阅第 457 页的识别具有不匹配状态的第 2 层连接。
- 查看 HP NA 设备信息 为在 NNMi 中选择的设备打开当前 NA 设备详细信息页。

• 查看 HP NA 设备配置 — 为在 NNMi 中选择的设备打开 NA 当前配置页。

如果对设备禁用实时更改检测,则显示的信息为在上个设备轮询间隔捕获的配置 NA。 如果在该捕获之后进行了配置更改,则**当前配置**页上的信息可能不是实际的当前配置。

- 查看 HP NA 设备配置差异 为在 NNMi 中选择的设备打开 NA 比较设备配置页。
- 查看 HP NA 设备配置历史 为在 NNMi 中选择的设备打开 NA 设备配置历史页。
- 查看 HP NA 策略符合性报告 为在 NNMi 中选择的设备打开 NA 策略、规则和符合性搜索结果页。
- 以 Telnet 方式连接 HP NA 设备 打开 Telnet 窗口以连接到 NNMi 中选择的设备。
- 以 SSH 方式连接 HP NA 设备 打开 SSH 窗口以连接到 NNMi 中选择的设备。
- **启动 HP NA** 打开 NA 用户界面。
- 启动 HP NA 命令脚本 在 NA 中打开新建任务 运行命令脚本页。针对 NNMi 控制台中 选择的节点或事件预填充该页。
- 启动 HP NA 诊断 在 NA 中打开新建任务 运行诊断页。针对 NNMi 控制台中选择的节 点或事件预填充该页。

有关使用 NA 功能的信息,请参阅《HP Network Automation 用户指南》。

将 NA 诊断和命令脚本配置为事件操作

启用 HP NNMi-HP NA 集成会修改某些现有 NNMi 事件以包含用于在每次发生关联事件 时访问 NA 诊断的事件操作。表 44 列出了经过修改的事件。

NNMi 事件	NA 诊断
OSPFNbrStateChange	显示邻居
OSPFVirtIfStateChange	显示邻居
OSPFIfStateChange	显示邻居 显示接口
InterfaceDown	显示接口
CiscoChassisChangeNotification	显示模块

表 44 NNMi 配置了 NA 诊断的事件

可以将用于访问 NA 的操作添加到任何其他 NNMi 事件,并且可以修改默认事件操作。在 事件的操作选项卡上,添加命令类型为 ScriptOrExecutable 的新生命周期转换操作。在命 令框中,输入带有相应参数的 naruncmdscript.ovpl 或 narundiagnostic.ovpl。有关 示例,请参阅表 44 中所列事件的操作配置。

查看用于访问 NA 的事件操作的结果

已配置 NA 操作的某类型的事件发生时, NNMi 启动所配置的操作,并且将诊断或命令脚本的任务 ID 存储为该事件的属性。出现任务 ID 时将启用操作菜单上的显示 HP NA 诊断结果 和重新运行 HP NA 诊断项。

要在事件发生时查看操作结果,请在 NNMi 事件视图中选择事件,然后选择**操作 > 显示** HP NA 诊断结果。

要查看所配置操作的当前结果,请在 NNMi 事件视图中选择事件,然后选择操作 > **重新运行** HP NA 诊断。

如果多次运行该任务,则 NNMi 在事件表单的自定义属性选项卡上列出最近的任务 ID。显示 HP NA 诊断结果操作显示已为事件运行的所有任务,使您可以比较各次运行的结果。

识别具有不匹配状态的第2层连接

如果启用了 HP NNMi-HP NA 集成,则 NNMi 将定期查询 NA 以获取 NNMi 拓扑中每个 第 2 层连接的两端接口的速度和双工设置。另外,NNMi 查询 NA 以获取添加到 NNMi 拓扑的任何新连接的接口速度和双工设置,并且在 NNM iSPI Performance for Metrics 正在 运行的情况下,还会查询具有可能指示不匹配连接的性能阈值异常的任何连接的接口速度 和双工设置。NNMi 使用不匹配检测算法确定这些值是否可能导致不匹配连接。

仅当 NA 资产中包含构成第 2 层连接的两个接口的 MAC 地址时, NNMi 才会执行不匹配 分析。如果 NA 接口记录不包含有效 MAC 地址,请运行 NA 拓扑数据采集诊断以更新 MAC 地址字段。有关详细信息,请参阅第 452 页的步骤 5。

操作 > 显示不匹配连接命令显示 NNMi 怀疑可能包含速度不匹配和 / 或双工不匹配的第 2 层 连接的表,如图 26 所示。

图 26 不匹配连接表示例

😭 🕸 🔛 HP NA Mismatched Connections		🟠 🔻 🖾 👻 🖶 Page 🔻
File View Tools Actions Help		
Layer 2 Connection	Speed Comparison (configured/negotiated : configured/negotiated)	Duplex Comparison (configured/negotiated : configured/negotiated)
Small Subnets-mplsp04[V1137],mplspe07[Fa0/1]	MATCH (100/100 : auto-negotiated/100)	POSSIBLE_MISMATCH (full/full : auto-negotiated/half)

对于每个可疑连接,表中列出了连接的两端接口的速度和双工值,并对数据进行了说明。可能的说明如下:

- MATCH 表示速度值和双工值最可能使第 2 层连接正常运行。
- POSSIBLE_MISMATCH 表示速度值和 / 或双工值可能冲突,导致连接不佳或无效。

• MISMATCH 表示速度值和 / 或双工值的冲突可能性高,导致连接不佳或无效。

HP NNMi-HP NA 集成配置表单上的 HP NA 连接检查间隔参数指定连接查询的频率。

由集成提供的 NA 功能

HP NNMi-HP NA 集成对从 NA 到 NNMi 的通信提供以下功能:

- 第458页的发送设备配置更改通知
- 第458页的维护准确的设备信息
- 第459页的在设备配置期间禁用网络管理
- 第460页的传播设备共用字符串更改
- 第 460 页的 NA 事件规则

发送设备配置更改通知

设备添加到 NA 资产以及 NA 资产中设备上的配置更改时, NA 会将 SNMP 陷阱发送到 NNMi。 NNMi 操作员可以在事件视图中看到这些陷阱, 如有必要, 可以调查更改。

集成将 NASnmpTrapv1 和 NASnmpTrapv2 SNMP 陷阱事件配置添加到 NNMi。

维护准确的设备信息

对于某些设备配置任务,任务完成之后,NA 会触发 NNMi 重新搜索设备。

NA 管理设置 - 第三方集成页上的任务完成后重新搜索主机字段指定用于触发 NNMi 重新搜索设备的设备配置任务。默认选择是:

- 更新设备软件
- 部署密码
- 重新启动设备
- 搜索驱动程序

可以选择以下任一或所有额外任务:

- 运行命令脚本
- 运行诊断
- 删除 ACL
- 配置 Syslog
- 运行 ICMP 测试
- 拍摄快照
- 同步启动和运行

• 操作系统分析

要禁用此功能,请从任务列表清空所有选择。

在设备配置期间禁用网络管理

对于某些设备配置任务, NA 触发 NNMi 以在配置过程中将设备设为禁用状态。此管理状态将抑制 NNMi 监视设备以防发生不需要的事件。在配置设备之前, NA 会将服务中断事件发送到 NNMi。在设备配置成功之后, NA 会将"服务中"事件发送到 NNMi, 后者将除去设备的禁用状态,并恢复定期状态轮询。

NA 管理设置 - 第三方集成页上的服务中断事件字段指定用于触发 NNMi 以在任务期间将设备 设置为禁用状态的设备配置任务。默认选择是:

- 更新设备软件
- 部署密码
- 重新启动设备

可以选择以下任一或所有额外任务:

- 运行命令脚本
- 运行诊断
- 删除 ACL
- 配置 Syslog
- 搜索驱动程序
- 运行 ICMP 测试
- 拍摄快照
- 同步启动和运行
- 操作系统分析

要禁用此功能,请从任务列表清空所有选择。

如果设备配置不能令人满意地完成,则要执行的操作取决于集成配置。

- NA 管理设置 第三方集成页上的如果设备任务失败设置指定在设备配置不成功的情况下, 集成在 NNMi 中是应该除去还是保留禁用状态。
- NA 管理设置 第三方集成页上的如果任务完成后设备符合性检查失败设置指定在设备配置 不相符的情况下,集成在 NNMi 中是应该除去还是保留禁用状态。

这些设置应用于在服务中断事件字段中选择的所有设备任务。无法按每个任务设置恢复行为。

传播设备共用字符串更改

启用 SNMP 共用字符串传播时,集成行为如下:

• 如果 NA 用于访问同步设备的 SNMPv1 或 SNMPv2c 共用字符串发生更改,则 NA 向 NNMi 通知更改, NNMi 随后更新与该设备的通信设置。

NNMi 立即开始对设备使用新共用字符串。

- 仅当用于管理设备的共用字符串发生更改时, NA 将更新发送到 NNMi。 NA 将新共用 字符串部署到设备时, NNMi 不接收更新。
 - 如果将新设备添加到 NA 默认站点分区,则 NA 向 NNMi 告知 NA 用于管理设备的
- SNMPv1 和 SNMP v2c 共用字符串。 集成不会将 SNMPv3 用户从 NA 传播到 NNMi。

NA 管理设置 - 第三方集成页上的**传播 SNMP 共用字符串**设置指定集成是否应当将 **SNMP** 共用 字符串从 **NA** 转发到 **NNMi**。默认情况下,不执行共用字符串传播。

NA 事件规则

NA 事件规则定义 NA 如何与 NNMi 管理服务器通信。

不要在 NA 中修改或删除这些事件规则。

集成在 NA 中定义以下事件规则:

• 通过 SNMP 陷阱进行的 NA/NNMi 集成

新设备添加到 NA 资产或者更改设备配置时,此 NA 事件会向 NNMi 发送 SNMP 陷阱。有关详细信息,请参阅第 458 页的发送设备配置更改通知。

• 为添加设备进行的 NA/NNMi 拓扑同步

将新设备添加到默认站点分区时,此 NA 事件将设备提示发送到 NNMi。有关详细信息,请参阅第 453 页的 NNMi 和 NA 之间的拓扑同步。

• 为删除设备进行的 NA/NNMi 拓扑同步

从 NA 资产删除设备时,此 NA 事件发送请求,以从 NNMi 拓扑删除设备。有关详细 信息,请参阅第 453 页的 NNMi 和 NA 之间的拓扑同步。

• NA/NNMi 集成重新搜索主机

NA 资产中的设备配置更改时,此 NA 事件请求设备的最新 NNMi 状态。有关详细信息,请参阅第 458 页的维护准确的设备信息。

• NA/NNMi 集成服务中断

启动任务时,此 NA 事件在 NNMi 中将设备设置为服务中断状态。在任务完成之后,此事件在 NNMi 中将设备设回服务中状态。有关详细信息,请参阅第 459 页的在设备 配置期间禁用网络管理。

• NA/NNMi 集成 Snmp 共用字符串传播

NA 资产中设备的"上次使用的设备密码更改"更改时,此 NA 事件将 NA 正用于管理 设备的共用字符串发送到 NNMi。有关详细信息,请参阅第 460 页的传播设备共用字 符串更改。

更改 HP NNMi-HP NA 集成

- 1 在 NA 用户界面中,打开管理设置 第三方集成页 (管理 > 管理设置 > 第三方集成)。
 - a 对值进行相应修改。有关此表单上的字段的信息,请参阅以下参考内容:
 - 第458页的维护准确的设备信息
 - 第459页的在设备配置期间禁用网络管理
 - 第460页的传播设备共用字符串更改
 - b 单击页面底部的**保存**。
- 2 在 NNMi 控制台中,打开 HP NNMi-HP NA 集成配置表单 (集成模块配置 > HP NA)。
 - a 对值进行相应修改。有关此表单上的字段的信息,请参阅第 464 页的 HP NNMi-HP NA 集成配置表单参考。
 - b 验证表单顶部的**启用集成**复选框是否已选中,然后单击表单底部的**提交**。

更改会立即生效。不需要重新启动 ovjboss。

禁用 HP NNMi-HP NA 集成

- 1 在 NNMi 控制台中,打开 HP NNMi-HP NA 集成配置表单 (集成模块配置 > HP NA)。
- 2 清除表单顶部的**启用集成**复选框,然后单击表单底部的提交。集成操作不再可用。
- 更改会立即生效。不需要重新启动 ovjboss。

对 HP NNMi-HP NA 集成进行故障诊断

本部分包含以下主题:

- 第462页的测试集成
- 第 464 页的 NNMi 拓扑中缺少 NA 设备

测试集成



如果集成在过去一直成功运行,则可能是配置的某个方面(例如 NNMi 或 NA 用户密码) 最近有更改。请尝试按第 464 页的 HP NNMi-HP NA 集成配置表单参考中所述更新集成 配置,然后完整地执行此过程。

- 1 在 NNMi 控制台中,打开 HP NNMi-HP NA 集成配置表单 (集成模块配置 > HP NA)。 有关此表单上的字段的信息,请参阅第 464 页的 HP NNMi-HP NA 集成配置表单 参考。
- 2 要检查集成状态,请单击 HP NNMi-HP NA 集成配置表单底部的提交(不进行任何配置 更改)。
 - 成功后,此步骤将启动 NNMi 和 NA 之间的完整拓扑同步。

将会出现新窗口,其中显示状态消息。

如果消息表明连接到 NA 服务器时发生问题,则说明 NNMi 和 NA 无法通信。继续执行此过程的步骤 3。

3 要验证 NA 凭证的准确性和访问级别,请使用 NA 用户的凭证从 HP NNMi-HP NA 集成配置表单登录到 NA 用户界面。

如果无法登录到 NA 用户界面,请联系 NA 管理员以验证登录凭证。

4 要验证与 NA 服务器的连接是否已正确配置,请在 NNMi 管理服务器上的 Web 浏览器 中,输入以下 URL:

http://<NA 服务器>:<NA 端口>/soap

其中的这些变量与 HP NNMi-HP NA 集成配置表单上的值相关,如下所示:

- 必须清除启用 NA SSL 复选框,以指示与 NA 服务器的连接使用 http 协议。
- <*NA 服务器*>是 **NA 主机**的值。
- <*NA 端口*>是 **NA 端口**的值。

如果 NA Web 服务正在指定服务器和端口上运行,则 NA 服务器会以类似于以下内容 的消息作出响应:

NAS SOAP API: 仅处理 HTTP POST 请求

- 如果显示预期的消息,则继续执行步骤 5。
- 如果看到错误消息,则说明与 NA 服务器的连接未正确配置。请联系 NA 管理员以 验证用于连接到 NA Web 服务的信息。继续对 NA 连接进行故障诊断,直到您看到 预期的消息。
- 5 验证与 NNMi 的连接是否已正确配置:

如果在此过程的步骤 1 中已使用此步骤中所述信息连接到 NNMi 控制台,则不需要重新连接到 NNMi 控制台。继续执行步骤 6。

a 在 NA 服务器上的 Web 浏览器中,输入以下 URL:

http://<NNMi 服务器>:<端口>/nnm/

其中的这些变量与 HP NNMi-HP NA 集成配置表单上的值相关,如下所示:

- <NNMi 服务器> 是 NNMi 主机的值。
- <端□> 是 NNMi 端口的值。
- b 提示时,输入具有管理员角色的 NNMi 用户的凭证。

应当看见 NNMi 控制台。如果 NNMi 控制台未出现,请联系 NNMi 管理员以验证 用于连接到 NNMi 的信息。继续对 NNMi 连接进行故障诊断,直到 NNMi 控制台 出现。

无法作为具有 Web 服务客户端角色的用户登录到 NNMi 控制台。

- 6 请联系 NNMi 管理员以验证具有 Web 服务客户端角色的 NNMi 用户和相应的 NNMi 密码的值。
- 7 使用在此过程的步骤 4 和步骤 5 中用于成功连接的值更新 HP NNMi-HP NA 集成配置表 单。另外,在此表单上重新输入步骤 6 的 NNMi 用户和密码。

有关详细信息,请参阅第464页的HPNNMi-HPNA集成配置表单参考。

- 8 单击表单底部的提交。
- 9 如果状态消息仍然表明连接到 NA 服务器时发生问题,请执行以下操作:
 - a 清除 Web 浏览器缓存。
 - b 从 Web 浏览器清除所有保存的表单或密码数据。
 - c 完全关闭 Web 浏览器窗口, 然后重新打开它。
 - d 重复此过程的步骤 7 和步骤 8。
- 10 通过启动第 453 页的使用 HP NNMi-HP NA 集成中列出的某个操作,测试配置。

NNMi 拓扑中缺少 NA 设备

如果 NNMi 同步节点组中不显示 NA 默认站点分区的设备,请遵循以下步骤:

- 检查 NNMi 节点资产,以确定是否该设备在拓扑中,但在其他节点组中。
 如果是这样,请更新 NNMi 同步节点组的定义以包括该设备。
- 2 检查 NNMi IP 地址资产,以确定 NA 中使用的 IP 地址是否在 NNMi 中列出。

如果 IP 地址包括在 NNMi 中,请确定托管该 IP 地址的节点。此节点应与 NA 设备同步。 NNMi 可能会对此节点使用其他管理地址,而不是 NA 作为搜索提示发送的 IP 地址。

3 (可选)重新启用集成。

只有在启用了集成和向 NA 默认站点分区添加了新设备时, NA 才会发送搜索提示。如果在网络中断期间或在正确包括 NNMi 同步节点组和自动搜索规则之前向 NA 添加了设备,请重新启用集成以使 NA 重新发送搜索提示。

应用程序故障切换和 HP NNMi-HP NA 集成

如果 NNMi 管理服务器参与 NNMi 应用程序故障切换,则在故障切换发生之后, HP NNMi-HP NA 集成将使用新的 NNMi 管理服务器主机名重新配置 NA 服务器。故障 切换对于集成用户应该是透明的。

集成不支持 NA 服务器的故障切换。

HP NNMi-HP NA 集成配置表单参考

在 NNMi 控制台中, HP NNMi-HP NA 集成配置表单包含用于配置从 NNMi 到 NA 的通信的参数。此表单是通过集成模块配置工作区提供的。



只有具有管理员角色的 NNMi 用户才可以访问 HP NNMi-HP NA 集成配置表单。

HP NNMi-HP NA 集成配置表单采集以下常规方面的信息:

- NNMi 管理服务器连接
- NA 服务器连接
- 集成行为

要应用对集成配置的更改,请在 HP NNMi-HP HA 集成配置表单上更新值,然后单击提交。

NNMi 管理服务器连接

表 45 列出用于从 NA 连接到 NNMi 管理服务器的参数。通过查看调用 NNMi 控制台会话的 URL,可以确定这些值中的大部分。与 NNMi 管理员协作,为配置表单的这一部分确定 合适的值。

表 45 NNMi 控制台中的 NNMi 管理服务器信息

字段	描述
NNMi 主机	 NNMi 管理服务器的正式完全限定域名。此字段为只读。 注:集成通过确定以下文件中 jboss.http.port 的值,选择用于连接到 NNMi 控制台的端口: Windows: %NnmDataDir%\conf\nnm\props\nms-local.properties UNIX: \$NnmDataDir/conf/nnm/props/nms-local.properties
NNMi 用户	用于连接到 NNMi 控制台的用户名。此用户必须具有 NNMi Web 服务客户端角色。 注:此用户名的密码将以明文形式传递。 最佳实践:创建和使用具有 Web 服务客户端角色的 NNMiIntegration 用户帐户。
NNMi 密码	指定 NNMi 用户的密码。

NA 服务器连接

表 46 列出用于连接到 NA 服务器上的 Web 服务的参数。与 NA 管理员协作,为配置表单的这一部分确定合适的值。

表 46 NNMi 控制台中的 NA 服务器信息

HP NA 服务器参数	描述
NA 主机	NA 服务器的完全限定域名或 IP 地址。

表 46 NNMi 控制台中的 NA 服务器信息 (续)

HP NA 服务器参数	描述
NA 端口	用于连接到 NA Web 服务的端口。 默认 NA 端口如下: • 80 — 用于连接到与 NNMi 不同的另一台计算机上的 NA • 8080 — 用于连接到与 NNMi 相同的计算机上的 NA 提示: NA URL 显示 SSL 端口,此端口不适用于集成通信。输入正确的非 SSL 端口。
NA 用户	具有 NA 管理员角色的有效 NA 用户帐户名。 注:此用户名的密码将以明文形式传递。 最佳实践:创建和使用 NAIntegration 用户帐户。
NA 密码	指定 NA 用户的密码。

集成行为

表 47 列出用于配置 HP NNMi 脑 P NA 集成行为的 NNMi 控制台参数。

表 47 NNMi 控制台中的集成行为信息

参数	描述
拓扑过滤器节点组	包含用于与 NA 拓扑同步的一组节点的 NNMi 节点组。集成用此节点组中每个节点的相关信息填充 NA 默认站点分区。 从此 NNMi 管理服务器上的节点组列表中选择此节点组。 如果未指定节点组,则集成将整个 NNMi 拓扑与 NA 默认站点分区同步。
拓扑同步间隔 (小时)	NNMi 执行与 NA 的完整拓扑同步的频率, 如第 453 页的 NNMi 和 NA 之间的拓扑同步 中所述。连接检查的默认间隔是 24 小时。
	要禁用定期拓扑同步,请将此值设置为 0。
在 NA 中搜索设备驱 动程序	NA配置规范。
	如果选中在 NA 中搜索设备驱动程序复选框,则作为与 NNMi 拓扑同步的结果, NA 会自动 搜索已添加到 NA 的设备的驱动程序。
	默认设置已清除。在这种情况下,可以手动启动设备驱动程序搜索。
NA 连接检查间隔 (小时)	NNMi 对 NA 验证 NNMi 拓扑中所有第2层连接的接口数据的频率,如第457页的识别 具有不匹配状态的第2层连接中所述。连接检查的默认间隔是24小时。
	要禁用定期连接检查,请将此值设置为 0。

NA 参考中的 NNMi 集成配置

在 NA 用户界面中, 管理设置 - 第三方集成页的 NNMi 集成部分包含用于配置从 NA 到 NNMi 的通信的参数。在 HP NNMi-HP NA 集成配置表单上启用集成时,会设置管理设置 - 第三方集成页上的字段。访问管理设置 - 第三方集成页更改 NNMi 设备重新搜索触发、服务中断触发和 SNMP 共用字符串传播的集成行为。

管理设置 - 第三方集成页可从**管理 > 管理设置 > 第三方集成**进行访问。要应用集成配置更改,请 更新此页上的值,然后单击**保存**。

只有具有管理员角色的 NA 用户才可以访问管理设置 - 第三方集成页。

集成通信

表 48 列出用于从 NA 服务器连接到 NNMi Web 服务的参数。集成将以 NNMi 控制台中的 HP NNMi-HP NA 集成配置表单上的信息配置这些参数。

表 48 NA 用户界面中的集成连接信息

字段	描述
NA 用户	HP NNMi-HP NA 集成配置表单上指定的 NA 用户帐户名。
NA 分区	HP NNMi-HP NA 集成配置表单上指定的 NA 分区。
NNMi 主机	HP NNMi-HP NA 集成配置表单上指定的 NNMi 管理服务器名称。
NNMi HTTP 端口	由集成确定的 NNMi 控制台端口。
NNMi 用户	HP NNMi-HP NA 集成配置表单上指定的 NNMi 用户名。
NNMi 密码	HP NNMi-HP NA 集成配置表单上指定的 NNMi 用户密码。

其他集成行为

表 49 列出用于配置 HP NNMi-HP NA 集成行为的 NA 用户界面参数。

表 49 NA 用户界面中的集成行为信息

字段	描述
任务完成后重新搜索 主机	使集成触发 NNMi 设备搜索的 NA 任务。默认选择是: 更新设备软件 部署密码 重新启动设备 搜索驱动程序 有关详细信息,请参阅第 458 页的维护准确的设备信息。
服务中断事件	使集成将设备设置为禁用状态的 NA 任务。默认选择是: 更新设备软件 部署密码 重新启动设备 有关详细信息,请参阅第 459 页的在设备配置期间禁用网络管理。
如果设备任务失败	服务中断事件的设备任务失败恢复规范。默认设置是将设备返回到 NNMi 中的服务。 有关详细信息,请参阅第 459 页的在设备配置期间禁用网络管理。
如果任务完成之后, 设备符合性检查失败	服务中断事件的设备符合性检查失败恢复规范。默认设置是将设备返回到 NNMi 中的服务。 有关详细信息,请参阅第 459 页的在设备配置期间禁用网络管理。
传播 SNMP 共用 字符串	共用字符串传播规范。默认设置已禁用。 有关详细信息,请参阅第460页的传播设备共用字符串更改。
HP ProCurve Manager Plus

HP ProCurve Manager Plus (PCM Plus) 是用于映射、配置和监视 HP ProCurve 设备的网络管理平台。 PCM Plus 提供以下功能:

- 统一管理整个网络中的有线和无线以太网
- 配置、更新和监视 HP ProCurve 设备并对它进行故障诊断
- 基于策略的管理和多设备管理
- 预先发出带有自动警报响应的警报
- 高级通信量监视功能

有关购买 PCM Plus 的信息,请联系 HP 销售代表。

本章包含以下主题:

- HP NNMi-HP ProCurve Manager Plus 集成
- 使用 HP NNMi-HP ProCurve Manager Plus 集成

HP NNMi-HP ProCurve Manager Plus 集成

通过在 PCM Plus 环境中包含 HP Network Node Manager i Software (NNMi),使用 PCM Plus 监视和管理其 ProCurve 设备的网络管理员将进一步了解这些设备。

HP NNMi-HP ProCurve Manager Plus 集成提供以下功能:

- 将 NNMi 数据库中的 IPv4 ProCurve 设备信息与 PCM Plus 进行同步。(目前, PCM Plus 不支持 IPv6 ProCurve 设备。)
- 在这两个应用程序之间,对 SNMPv2 共用字符串和 SNMPv3 基于用户的安全模型 (USM)设置进行同步,以便与被管 ProCurve 设备进行通信。

价值

HP NNMi-HP ProCurve Manager Plus 集成提供以下好处:

- 当 NNMi 为 NNMi 和 PCM Plus 搜索 ProCurve 设备时,减少流向 ProCurve 设备的 网络通信量。
 - NNMi 将更丰富的 ProCurve 设备信息转发到 PCM Plus。
 - 简化的 PCM Plus 网络图仅包含已知 ProCurve 设备。
- 在 NNMi 中整合了 ProCurve 设备事件处理。
- 减少支持 ProCurve 设备的最大可用性所需的成本。

集成产品

本章中的信息适用于以下产品:

• PCM Plus

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

• NNMi 9.10

NNMi 和 PCM Plus 必须安装在不同的计算机上。NNMi 管理服务器和 PCM Plus 计算机可以使用相同或不同的操作系统。

PCM Plus 远程代理不能安装在 NNMi 管理服务器上。



文档

www.procurve.com/pcm-manuals 提供的《HP ProCurve Manager 网络管理员指南》 的 "附录 A"中完整描述了 HP NNMi–HP ProCurve Manager Plus 集成。

使用 HP NNMi-HP ProCurve Manager Plus 集成

启用 HP NNMi-HP ProCurve Manager Plus 集成的步骤将在 PCM Plus 服务器(配置) 和 NNMi 管理服务器 (安装 PCM Plus 陷阱定义)上执行。

启用 HP NNMi-HP ProCurve Manager Plus 集成会针对 PCM Plus 转发到 NNMi 的所 有应用程序事件,将 ICMEVT_PCMPLUS_EVENTS_ALL 事件配置添加到 NNMi。此事 件具有 SNMP 对象 ID .1.3.6.1.4.1.11.2.3.7.11.0.63000000。

有关启用、使用和禁用 HP NNMi-HP ProCurve Manager Plus 集成并对它进行故障诊断 的信息,请参阅《HP ProCurve Manager 网络管理员指南》的"附录 A"。

HP RAMS MPLS WAN

HP RAMS MPLS WAN 集成使 HP Route Analytics Management System (RAMS) 能够支持如下所述的企业: 企业的多个站点在 WAN 上通过 ISP 连接,这些 ISP 在其各自网络中使用多协议标签交换 (MPLS)。

有关购买 HP RAMS 的信息,请联系 HP 销售代表。

本章包含以下主题:

- HP NNMi-HP RAMS MPLS WAN 集成
- 使用 HP NNMi-HP RAMS MPLS WAN 集成

HP NNMi-HP RAMS MPLS WAN 集成

HP NNMi-HP RAMS MPLS WAN 集成提供用于从 NNMi 控制台访问 MPLS WAN 信息的功能。

价值

HP NNMi-HP RAMS MPLS WAN 集成增加了通过不同网络云查看连通性的功能,这样 NNMi 用户就可以检测和查看 WAN 上连接的多个站点。

集成产品

本章中的信息适用于以下产品:

• RAMS

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

• 有 NNMi Advanced 许可证的 NNMi 9.10

有关支持 NNMi 的硬件平台和操作系统的信息,请参阅 NNMi 系统和设备支持列表。

文档

将 Route Analytics Management Systems (RAMS) 用于 NNMi Advanced (NNMi 帮助 中) 中完整描述了 HP NNMi-HP RAMS MPLS WAN 集成。

使用 HP NNMi-HP RAMS MPLS WAN 集成

启用 HP NNMi-HP RAMS MPLS WAN 集成的步骤将在 NNMi 管理服务器上执行。

有关启用、使用和禁用 HP NNMi-HP RAMS MPLS WAN 集成并对它进行故障诊断的信息, 请参阅 将 Route Analytics Management Systems (RAMS) 用于 NNMi Advanced (NNMi 帮助中)。

HP SiteScope

HP SiteScope 是一款无代理监视解决方案,用于跟踪分布式 IT 基础结构的可用性和性能,例如:服务器、操作系统、网络设备、网络服务、应用程序和应用程序组件。SiteScope 可提供实时信息,用于验证基础结构操作、报告问题并在其成为紧急问题之前解决瓶颈。

有关购买 SiteScope 的信息,请联系 HP 销售代表。

本章描述以下集成:

- 第 475 页的 HP NNMi-HP SiteScope 事件集成
- 第 479 页的 HP NNMi-HP SiteScope 系统度量集成

有关 NNM iSPI for IP Telephony-HP SiteScope 集成的信息,请参阅 NNM iSPI for IP Telephony 帮助中的*配置 与 SiteScope 的集成*。

HP NNMi-HP SiteScope 事件集成

本部分包含以下主题:

- 第 476 页的关于 HP NNMi-HP SiteScope 事件集成
- 第 477 页的启用 HP NNMi-HP SiteScope 事件集成
- 第 477 页的使用 HP NNMi-HP SiteScope 事件集成
- 第 478 页的更改 HP NNMi-HP SiteScope 事件集成
- 第 478 页的禁用 HP NNMi-HP SiteScope 事件集成
- 第 478 页的对 HP NNMi-HP SiteScope 事件集成进行故障诊断

关于 HP NNMi-HP SiteScope 事件集成

借助于 HP NNMi-HP SiteScope 事件集成,SiteScope 服务器可以在符合配置的 SiteScope 监视器警报条件时,将 SNMP 陷阱发送到 NNMi 管理服务器。NNMi 再将监视器警报陷 阱转换成 NNMi 事件。从这些事件中,NNMi 控制台用户可以在该监视器的上下文中启动 SiteScope。

价值

通过在 NNMi 中提供 SiteScope 事件配置, HP NNMi-HP SiteScope 事件集成简化了就 SiteScope 监视的设备和应用程序的状态对 SNMP 陷阱进行说明的过程。

系统只为 SiteScope 中配置的警报生成这些陷阱。集成使这些陷阱在 NNMi 控制台中可以 事件的形式被看到。如果 SiteScope 指示警报条件不再存在 (变为正常),则 NNMi 会自 动关闭这些警报事件。

集成产品

本部分中的信息适用于以下产品:

SiteScope

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

• NNMi 9.10

NNMi 和 SiteScope 可以安装在相同或不同的计算机上。

有关受支持的硬件平台和操作系统的最新信息,请参阅这两种产品的支持列表。

支持的 SiteScope 监视器

如 SiteScope 中所配置, HP NNMi-HP SiteScope 事件集成接收从任何 SiteScope 监视器 类型的 SiteScope 服务器发送的 SNMP 陷阱。SiteScope 警报配置必须包括 NNMi 管理服 务器并将其作为陷阱目标。

SiteScope 陷阱配置确定是将 SiteScope 服务器还是被管主机设置为陷阱源。如果不在 NNMi 中管理陷阱源,则事件配置表单上的丢弃未解析的 SNMP 陷阱复选框设置确定 NNMi 如何处 理该陷阱。有关详细信息,请参阅 NNMi 帮助中的*处理未解析的传入陷阱*。

文档

此部分描述如何配置和使用集成。

SiteScope 产品介质上包含的《HP SiteScope Using SiteScope 指南》描述了如何配置 SiteScope 监视器,以及如何配置 SiteScope 以将事件数据发送到 NNMi。

启用 HP NNMi-HP SiteScope 事件集成

要启用 HP NNMi-HP SiteScope 事件集成,请将一台或多台 SiteScope 监视器配置为将 SNMP 陷阱发送到 NNMi。高级别步骤如下:



默认情况下 NNMi 事件类型是启用的。

- 1 在 SiteScope 用户界面中, 创建将 HP SiteScope 事件陷阱发送到 NNMi 管理服务器 的 SNMP 首选项。
- 2 在 SiteScope 用户界面中, 创建将 SNMP 陷阱首选项设置为警报操作目标的警报。(在 此警报中, 为每个可能监视状态创建警报操作。)

有关详细信息,请参阅《HP SiteScope Using SiteScope 指南》的*使用Network Node Manager i (NNMi)*章节中的"如何配置 SiteScope 以将事件数据发送到 NNMi"。

使用 HP NNMi-HP SiteScope 事件集成

NNMi 为 SiteScope 监视器警报陷阱定义了两个事件类型:

- SiteScopeAlertEvent1 将 SNMPv1 格式的陷阱转换成 NNMi 事件。
- SiteScopeAlertEvent2 将 SNMPv2c 格式的陷阱转换成 NNMi 事件。

这些事件类型的配置是相同的。SiteScope SNMP 陷阱首选项确定 SiteScope 向 NNMi 发送 SNMPv1 格式还是 SNMPv2c 格式的陷阱。

在事件配置中,事件严重度设置如下:

- 默认事件状态是紧急,它映射到 SiteScope 事件严重度错误、不可用或无数据。
- 当 SiteScope 事件严重度是警告时,事件强化会将事件状态设置为警告。
- 当 SiteScope 事件严重度是良好时,事件强化会将事件状态设置为正常。

每个 SiteScopeAlertEvent 陷阱都包含一个 URL,用于在该监视器的上下文中启动 SiteScope。此 URL 在**事件**表单**自定义属性**选项卡上的 .1.3.6.1.4.1.11.15.1.2.1.4 自定义事 件属性 (CIA) 中提供。此 URL 将传递加密凭证,用于以 Integration Viewer 用户的身份 登录 SiteScope。

对于每个 SiteScopeAlertEvent 事件, NNMi 都会通过比较陷阱负载中包含的数据,对 SiteScopeAlertEvent 陷阱执行成对处理。每个陷阱都包含一个事件关键 varbind (OID .1.3.6.1.4.1.11.15.1.3.1.7)。如果陷阱还包含事件关闭关键模式 varbind (OID .1.3.6.1.4.1.11.15.1.3.1.8), NNMi 会将事件关闭关键模式 varbind 的值与现有事件中的事件关键 varbind 的值进行比较。 NNMi 会关闭匹配的现有事件,并将它们关联到传入陷阱下。NNMi 会在每个已关闭事件中添加 cia.reasonClosed CIA 和关联说明。此外, NNMi 还会自动关闭状态正常的每个 SiteScopeAlertEvent 事件。

SiteScope SNMP 陷阱出现在系统和应用程序系列中。

有关 SiteScopeAlertEvent 陷阱的内容的详细信息,请参阅随附 NNMi 提供的 HP-SITESCOPE-MIB。

更改 HP NNMi-HP SiteScope 事件集成

要更改 HP NNMi-HP SiteScope 事件集成,请执行以下任一步骤:

- 在 NNMi 控制台中,编辑 SiteScopeAlertEvent1 和 SiteScopeAlertEvent2 SNMP 陷 阱的事件配置。
- 在 SiteScope 用户界面中,更改监视器警报配置。

禁用 HP NNMi-HP SiteScope 事件集成

要禁用 HP NNMi-HP SiteScope 事件集成,请执行以下任一步骤或这两个步骤:

- 在 NNMi 控制台中,清除 SiteScopeAlertEvent1 和 SiteScopeAlertEvent2 SNMP 陷
 阱配置表单上的已启用复选框。
- 在 SiteScope 用户界面中,执行以下某个操作:
 - 从警报操作目标删除监视器和组。
 - 禁用或删除与 SiteScope 监视器关联的 SNMP 陷阱警报。

对 HP NNMi-HP SiteScope 事件集成进行故障诊断

本部分包含以下主题:

- 第 478 页的 NNMi 事件视图中不显示 SiteScopeAlertEvent 事件
- 第 479 页的无法从 SiteScope 事件中的 URL 正确打开 SiteScope

NNMi 事件视图中不显示 SiteScopeAlertEvent 事件

如果 NNMi 事件视图未包含所有预期的 SiteScopeAlertEvent 事件,请遵循以下步骤:

- 在 NNMi 控制台中,检查 SiteScopeAlertEvent1 和 SiteScopeAlertEvent2 事件 配置:
 - 验证是否已启用 SiteScopeAlertEvent1 和 SiteScopeAlertEvent2 事件类型。
 - 如果配置了接口或节点设置,则验证它们是否未阻止期望的 SiteScope 陷阱。
- 2 在 NNMi 控制台中,检查过滤器中是否有事件视图。

将当前过滤器与 SiteScopeAlertEvent1 和 SiteScopeAlertEvent2 事件配置进行比较。验证过滤器是否未阻止这些事件类型。

3 如果已选中**事件配置**表单上的**丢弃未解析的 SNMP 陷阱**复选框,则验证与 SiteScope 监视 器关联的节点是否在 NNMi 拓扑中。

SiteScope 陷阱配置确定是将 SiteScope 服务器还是被管主机设置为陷阱源。

4 在 SiteScope 用户界面中,验证 HP SiteScope 事件陷阱的 SNMP 陷阱首选项的配置。

- 5 在 SiteScope 用户界面中,验证每个预期的监视器警报是否将 SNMP 陷阱首选项设置 为警报操作目标。
- 6 在 SiteScope 用户界面中,向 NNMi 发送测试陷阱。

无法从 SiteScope 事件中的 URL 正确打开 SiteScope

如果无法从**事件**表单**自定义属性**选项卡上的 .1.3.6.1.4.1.11.15.1.2.1.4 CIA 中的 URL 正确 启动 SiteScope,请遵循以下步骤:

- 1 验证对 SiteScope 用户界面的访问权:
 - a 在新浏览器窗口中,直接打开 SiteScope 用户界面。

如果 SiteScope 用户界面无法正确工作,请验证浏览器配置是否匹配*HP SiteScope 发行说明*中描述的要求。

- b 将 URL 从 .1.3.6.1.4.1.11.15.1.2.1.4 CIA 复制到浏览器地址字段中。删除登录凭 证。在 SiteScope 登录窗口中, 输入 SiteScope 登录信息。
- 验证 SiteScope Integration Viewer 用户凭证是否在 URL 中。将 URL 从 .1.3.6.1.4.1.11.15.1.2.1.4 CIA 复制到浏览器地址字段中。(保留登录凭证。)

如果此测试失败,请向 SiteScope 管理员询问 Integration Viewer 用户的状态。如果最 近更改了 Integration Viewer 用户的密码,则在更改密码之前就存在的 SiteScope 的 URL 不会工作。

HP NNMi-HP SiteScope 系统度量集成

本部分包含以下主题:

- 第 479 页的关于 HP NNMi-HP SiteScope 系统度量集成
- 第 481 页的启用 HP NNMi-HP SiteScope 系统度量集成
- 第 484 页的使用 HP NNMi-HP SiteScope 系统度量集成
- 第 487 页的更改 HP NNMi-HP SiteScope 系统度量集成
- 第 487 页的禁用 HP NNMi-HP SiteScope 系统度量集成
- 第 488 页的对 HP NNMi-HP SiteScope 系统度量集成进行故障诊断
- 第 492 页的 HP NNMi-HP SiteScope 系统度量集成配置表单引用

关于 HP NNMi-HP SiteScope 系统度量集成

HP NNMi-HP SiteScope 系统度量集成在 NNM iSPI Performance for Metrics 网络性能服务器 (NPS) 中填充由 SiteScope 监视器采集的系统度量数据。集成将按如下方式处理数据

1 SiteScope 将监视器数据采集到 XML 文件中,并在 SiteScope 数据集成首选项的报告 间隔将采集的数据传递到 NNMi。

- 2 NNMi 在 SiteScope 数据中增加 NNMi 节点 UUID。
- 3 NNMi 将此增加的数据放置在为 NPS 检索配置的位置。
- 4 NPS 以 NPS 累计间隔使用增加的数据。
- 图 27 显示 HP NNMi-HP SiteScope 系统度量集成的数据流。

图 27 HP NNMi-HP SiteScope 系统度量集成数据流



价值

HP NNMi-HP SiteScope 系统度量集成在 NPS 中启用 SiteScope 采集的度量的报告。

集成产品

本部分中的信息适用于以下产品:

SiteScope

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

- NNMi 9.10
- NNM iSPI Performance for Metrics 版本 9.10

此集成需要 NNM iSPI Performance for Metrics 许可证。

NNMi、NNM iSPI Performance for Metrics 和 SiteScope 可以安装在相同或不同的计算 机上。

有关受支持的硬件平台和操作系统的最新信息,请参阅所有产品的支持列表。

支持的 SiteScope 监视器

HP NNMi-HP SiteScope 系统度量集成理解来自 SiteScope 监视器的以下类型的数据:

- CPU 利用率监视器
- 磁盘空间监视器
- 内存监视器
- Microsoft Windows 资源监视器的进程所监视的对象
- UNIX 资源监视器的进程所监视的对象

监视的节点必须在 NNMi 中管理。集成将丢弃不在 NNMi 拓扑中的节点和非被管节点的数据。

文档

此部分描述如何配置 NNMi 以与 SiteScope 和对 SiteScope 采集的数据可用的 NPS 报告 通信。

SiteScope 产品介质上包含的《HP SiteScope Using SiteScope 指南》描述了如何配置 SiteScope 监视器。

启用 HP NNMi-HP SiteScope 系统度量集成

图 28 显示 HP NNMi-HP SiteScope 系统度量集成的配置点。

图 28 HP NNMi-HP SiteScope 系统度量集成配置点



要启用 HP NNMi-HP SiteScope 系统度量集成,请遵循以下步骤:

- 1 在 NNMi 控制台中, 启用集成并用 SiteScope 系统度量集成包配置 NPS:
 - a *可选*。创建集成用于连接到 NNMi 控制台的具有 Web 服务客户端角色的 NNMi 用户。

也可以通过具有 Web 服务客户端角色的现有用户进行集成。

- b 打开 HP NNMi-HP SiteScope 系统度量集成配置表单(集成模块配置 > HP SiteScope 系统度量)。
- c 选中启用集成复选框。
- d 输入用于连接到 NNMi 管理服务器的信息。有关这些字段的信息,请参阅 第 492 页的 HP NNMi-HP SiteScope 系统度量集成配置表单引用。
- e 单击表单底部的**提交**。

此窗口将显示状态消息。如果消息指示 NNMi 凭证有问题,则单击**返回**,然后按照 错误消息文本的建议调整值。

- f 从结果窗口中,将数据集成 URL 复制到临时位置。配置 SiteScope 时,将使用 此值。
- 2 在 SiteScope 用户界面中, 配置 SiteScope 服务器以与 NNMi 进行 SSL 通信:
 - a 从首选项工作区,打开证书管理页,然后单击导入证书 <u>涞</u>。
 - b 在源选择下面,提供用于识别 NNMi 管理服务器到 SiteScope 的信息:
 - 验证是否已选中**主机**,然后输入 NNMi 管理服务器的完全限定域名。
 - 如有必要,更改端口号,以与 NNMi 管理服务器上的 HTTPS 端口匹配。 有关详细信息,请参阅第 492 页的 NNMi 端口。
 - c 单击**加载**。

NNMi 证书信息将显示在加载的证书下。请注意证书别名。

d 选择 NNMi 证书,然后单击导入。

在证书管理页上将列出 NNMi 证书。

- 3 在 SiteScope 用户界面中,创建将用于标识 NNMi 目标的搜索 / 过滤标记。
 - a 从首选项工作区,打开搜索/过滤标记页,然后单击新建标记 😕 。
 - b 输入标记名称 (例如, NNMi_upload) 和至少一个值。

- 4 在 SiteScope 用户界面中, 配置 SiteScope 和 NNMi 之间的连接:
 - a 从首选项工作区,打开集成首选项页,单击新建集成 🙀 ,然后单击数据集成。
 - b 在常规设置下,输入名称 (例如, NNMi_receiver)和可选描述。
 - c 在数据集成首选项设置下,包含以下设置:
 - 在接收器 URL 字段中,粘贴在此过程的步骤 1 末尾保存的 URL (例如: https://nnmi_server.example.com:443/sitescope-adapter/ sitescopereceiver)。
 - 选中 GZIP 压缩复选框。
 - 清除**包含其他数据**和**重定向时出错**复选框。(这些是默认设置。)
 - 选中**当请求时进行身份认证**复选框。(这是默认设置。)
 - 清除**禁用集成**复选框。(这是默认设置。)

对于所有其他设置,可以接受默认配置。

- d 在 Web 服务器安全设置下面,输入步骤 1 中在集成配置表单上指定的 NNMi 用户的 用户名和密码。
- e 在报告标记下面,选择在步骤3中创建的搜索/过滤标记(例如,NNMi_upload)。
- 5 在 SiteScope 用户界面中, 配置在 NPS 中生成 SiteScope 报告的监视器:
 - a 根据需要,创建新监视器或标识受支持类型的现有监视器:
 - CPU 利用率监视器
 - 磁盘空间监视器
 - 内存监视器
 - Microsoft Windows 资源监视器的进程所监视的对象
 - UNIX 资源监视器的进程所监视的对象
 - b 将在步骤 3 中创建的搜索 / 过滤标记 (例如, NNMi_upload) 添加到应将数据传递 到 NNMi 的监视器中。

集成只能处理 NNMi 拓扑中被管节点的数据。因此,仅将此标记应用于 NNMi 拓扑中的节点上的监视器。

c 建议。采集将数据传递给一个监视器组中的 NNMi 的监视器。

使用 HP NNMi-HP SiteScope 系统度量集成

HP NNMi-HP SiteScope 系统度量集成在 NPS 中提供以下 SiteScope 监视器报告:

- 日历
- 图表详细信息
- 热图
- 被管资产
- 最大变化
- 高峰期
- 阈值套筒
- 前 N 名
- 前 N 名图表

要访问 SiteScope 系统度量报告,请遵循以下步骤:

- 1 在 NNMi 控制台中,单击操作 > 报告 报表菜单。
- 2 在 NPS 的报告工作区中,打开 SiteScope 系统度量 > SiteScope > System_Metrics 文件夹。

最佳实践 以下提示适用于 SiteScope 系统度量报告:

- 对于某些报告(比如前N名,),侧重于一种类型的SiteScope监视器的报告比侧重于多个监视器类型的报告更易解释。在拓扑过滤器中,为ComponentType属性选择单个值。
- 如果未设置"节点名称"属性,则报告包含所选类型的所有监视器的数据。要限制一个 或多个特定节点的报告数据,请相应地设置"节点名称"属性。如果已设置 ComponentType 属性,则"节点名称"选择列表仅显示具有所选监视器类型的节点。
- 如需有关 Windows 资源监视器的报告,过滤掉 _Total on 和 Idle on 数据可能很有用。为此,在拓扑过滤器中,将 ComponentName 属性设置为不等于 _Total on 和 Idle on。

表 50 列出由集成添加的分组选项。

表 50 可用报告分组选项

选项名称	描述
Windows 进程 – 创建进程	标识父进程(创建被测量进程)的进程 ID (PID) 的整数值。
Windows 进程 – ID 进程	标识被测量进程的进程 ID (PID) 的整数值。

选项名称	描述
Unix 进程 – PID	标识被测量进程的进程 ID (PID) 的整数值。
Unix 进程 – 用户	标识被测量进程的 UNIX 用户 ID (uid) 的整 数值。
限定的组件名称	标识度量名称以及在其上采集此度量的节点的 字符串值。限定的组件名称的形式是 < <i>度量名称</i> > on < <i>节点长名称</i> >(例如:disk percent full on device.example.com)。 限定的组件名称是建议的分组选择。

表 50 可用报告分组选项 (续)

表 51 列出由集成添加的度量。对于每个度量,可以选择报告实际值。对于多个度量,也可 以报告阈值信息。有关对报告的值进行说明的信息,请参阅每个操作系统的文档。

监视器类型	可用度量	
CPU 利用率 ¹	• CPU 利用率	
磁盘空间	可用磁盘空间 (MB)已用磁盘百分比	
内存 ²	 内存页面 / 秒 已用虚拟内存百分比 可用虚拟内存 (MB) 已用交换内存百分比 可用交换内存 (MB) 已用物理内存百分比 可用物理内存 (MB) 	

表 51 可用的 SiteScope 系统度量

表 51 可用的 SiteScope 系统度量(续)

监视器类型	可用度量
Microsoft Windows 资源	• Windows 进程 – 特权时间百分比
	• Windows 进程 – 处理器时间百分比
	• Windows 进程 – 用户时间百分比
	• Windows 进程 – 创建进程 ID
	• Windows 进程 – 经过时间
	• Windows 进程 – 句柄计数
	• Windows 进程 – ID 进程
	• Windows 进程 – IO 数据字节 / 秒
	• Windows 进程 – IO 数据操作 / 秒
	• Windows 进程 – IO 其他数据字节 / 秒
	• Windows 进程 – IO 其他操作 / 秒
	• Windows 进程 – IO 读取字节 / 秒
	• Windows 进程 – IO 读取操作 / 秒
	• Windows 进程 – IO 写入字节 / 秒
	• Windows 进程 – IO 写入操作 / 秒
	• Windows 进程 – 页面错误
	• Windows 进程 – 页面文件字节
	• Windows 进程 – 页面文件字节峰值
	• Windows 进程 – 池非分页字节
	• Windows 进程 – 池分页字节
	• Windows 进程 – 优先级基数
	• Windows 进程 – 专用字节
	• Windows 进程 – 线程计数
	• Windows 进程 – 虚拟字节
	• Windows 进程 – 虚拟字节峰值
	• Windows 进程 – 上作集
	• Windows 进程 – 专用工作集
	• Windows 进程 – 丄作集峰值
UNIX 资源 ³	• Unix 进程 – CPU 百分比
	• Unix 进程 – 成员大小
	• Unix 进程 – 运行中成员
	• Unix 进程 – PID
	• Unix 进程 – 用户

1 SiteScope 汇总在 HP-UX 和 AIX 操作系统上采集的 CPU 利用率数据作为此系统而不 是每个特定 CPU 的单个平均值。因为集成不会将平均值发送到 NPS,所以 CPU 利用率 数据对 HP-UX 和 AIX 操作系统不可用。

2 SiteScope 不会采集所有操作系统的所有这些度量。

3 对于 HP-UX 操作系统上的 UNIX 资源监视器, SiteScope 仅采集 CPU 百分比、正在运行的数目和进程 ID。内存大小和用户数据对 HP-UX 节点不可用。

更改 HP NNMi-HP SiteScope 系统度量集成

可以通过以下方式更改 HP NNMi-HP SiteScope 系统度量集成:

- 将连接从 NNMi 更改为 NPS
- 将连接从 SiteScope 更改到 NNMi

将连接从 NNMi 更改为 NPS

要更改用于连接到 NPS 的信息,请遵循以下步骤:

- 在 NNMi 控制台中,打开 HP NNMi-HP SiteScope 系统度量集成配置表单 (集成模块配置 > HP SiteScope 系统度量)。
- 2 对值进行相应修改。有关此表单上的字段的信息,请参阅第 492 页的 HP NNMi-HP SiteScope 系统度量集成配置表单引用。
- 3 验证表单顶部的**启用集成**复选框是否已选中,然后单击表单底部的提交。

更改会立即生效。效果是更新显示在 HP NNMi-HP SiteScope 系统度量集成配置表单上的数据集成 URL。如果此 URL 更改,将如第 483 页的步骤 4 中所述更新 SiteScope 数据集成首选项。

将连接从 SiteScope 更改到 NNMi

要更改 SiteScope 数据接收器的信息,请遵循以下步骤:

- 1 在 SiteScope 界面中,打开用于定义 SiteScope 和 NNMi 之间的连接的数据集成 (从 首选项 > 集成首选项)。
- 2 对值进行相应修改。有关此表单上的字段的信息,请参阅 SiteScope 帮助。
- 3 验证是否已清除禁用集成复选框,然后单击表单底部的确定。 更改会立即生效。

禁用 HP NNMi-HP SiteScope 系统度量集成

要完全禁用 HP NNMi-HP SiteScope 系统度量集成,请完成以下两个步骤:

- 禁用从 NNMi 到 NPS 的连接
- 禁用从 SiteScope 到 NNMi 的连接

禁用从 NNMi 到 NPS 的连接

要使 NNMi 停止处理 SiteScope 监视器数据,请遵循以下步骤:

- 1 在 NNMi 控制台中,打开 HP NNMi-HP SiteScope 系统度量集成配置表单(集成模块配置> HP SiteScope 系统度量)。
- 清除表单顶部的启用集成复选框,然后单击表单底部的提交。
 更改会立即生效。

禁用从 SiteScope 到 NNMi 的连接

要使 SiteScope 停止将监视器数据发送到 NNMi 管理服务器,请遵循以下步骤:

- 1 在 SiteScope 界面中,打开用于定义 SiteScope 和 NNMi 之间的连接的数据集成 (从 首选项 > 集成首选项)。
- 2 选中**禁用集成**复选框,然后单击表单底部的**确定**。

更改会立即生效。

对 HP NNMi-HP SiteScope 系统度量集成进行故障诊断

与 SiteScope 数据处理相关的消息 (包括 XML 解析错误和不在 NNMi 拓扑中的节点的监视器数据)都会记录到 NNMi 管理服务器上的 nnm.0.0.log (和更早的)文件中。如果在 NNMi 管理服务器上遇到问题,请检查这些日志文件中是否有以字符串 com.hp.ov.nnm.sitescope.im或 com.hp.ov.nms.im.sitescope 开头的类的"严重"和 "警告"消息。有关详细信息,请参阅第 373 页的 NNMi 日志记录。

SiteScope 日志文件采集有关数据集成的问题的消息。在 SiteScope 日志文件中查看数据传输错误,这些错误很可能由一个或多个以下配置问题造成:

- 证书错误; NNMi 证书未正确加载到 SiteScope 中。
- 用户名和密码验证错误; NNMi 控制台中的 HP NNMi-HP SiteScope 系统度量集成配置 表单上的 NNMi 用户和 / 或 NNMi 密码不正确。
- 集成模块支持错误;已清除 NNMi 控制台中的 HP NNMi-HP SiteScope 系统度量集成配置表单上的启用集成复选框。

有关 SiteScope 日志文件的详细信息,请参阅 SiteScope 文档。

此部分包含以下主题:

- 第489页的验证集成数据流
- 第 490 页的验证集成配置的 NNMi 端
- 第 491 页的防火墙后面的 NAT 环境中的节点无报告数据

2011年3月

验证集成数据流

来自 SiteScope 的系统度量集成将 SiteScope 数据示例作为 *.gz 文件放置在 NNMi 管理服务器上的以下目
XML 文件XML 文件录中:

- Windows:
 - %NnmDataDir%\shared\perfspi\datafiles\metric\working\sitescope
- UNIX: \$NnmDataDir/shared/perfspi/datafiles/metric/working/sitescope

默认情况下,系统度量集成每分钟在此目录中放置一个新文件, NNMi 每5分钟使用一次 这些文件。

SiteScope 数据集成首选项的报告间隔确定 SiteScope 将数据示例发送到系统度量集成的 频率。客户不可配置 NNMi 使用率。

如果 sitescope 目录留空时间超过 2 分钟,则 SiteScope 将不会传送文件。在这种情况下,请执行以下操作:

1 在 SiteScope 用户界面中,验证是否已按第 483 页的步骤 4 中所述启用并配置数据集成首选项。

还需验证报告间隔字段的值。

2 在 SiteScope 用户界面中,验证是否至少有一个监视器配置包含与数据集成首选项关联 的搜索 / 过滤标记。

如果文件在 sitescope 目录中累计,则 NNMi 将不使用这些文件。在这种情况下,在 NNMi 控制台中,验证是否正确配置 HP NNMi-HP SiteScope 系统度量集成。有关详细 信息,请参阅第 490 页的验证集成配置的 NNMi 端。

来自 NNMi 的 CSV 文件

NNMi 将供 **NPS** 使用的 SiteScopeMetrics_*.csv.gz 文件放置在 **NNMi** 管理服务器 上的以下目录中:

- Windows: %NnmDataDir%\shared\perfspi\datafiles\metric\final
- UNIX: \$NnmDataDir/shared/perfspi/datafiles/metric/final

NNMi 大约每5分钟在此目录中放置一个新文件, NPS 大约每5分钟使用一次这些文件。

客户不可配置 NNMi 放置率。 NPS 累计率将决定 NPS 使用此目录中的文件的频率。 NNM iSPI Performance for Metrics 设置 NPS 累计率,客户不可配置此累计率。

如果 final 目录留空时间超过 10 分钟,则 NNMi 将不会传送文件。在这种情况下,在 NNMi 控制台中,验证是否正确配置 HP NNMi-HP SiteScope 系统度量集成。有关详细信息,请参阅第 490 页的验证集成配置的 NNMi 端。

如果文件在 final 目录中累计,则 NPS 将不使用这些文件。在这种情况下,请参阅 NPS 故障诊断文档。

- **报告** 在文件通过 final 目录之后的 2 小时内,如果 NPS 用户界面中未显示 SiteScope 报告,则 表示未正确配置集成。在这种情况下,请重新启动 SiteScope、NNMi ovjboss 进程和 NPS:
 - 1 重新启动 SiteScope:
 - Windows:
 - 打开**服务**控制面板 (**开始 > 控制面板 > 管理工具 > 服务**)。
 - 在服务列表中,右键单击 SiteScope,然后单击启动。
 - Linux 或 Solaris:
 - 在安装 SiteScope 的服务器上打开终端窗口。
 - 使用以下语法运行 start 命令 shell 脚本:

<安装路径>/SiteScope/start

- 2 通过运行以下命令,重新启动 ovjboss:
 - a ovstop ovjboss
 - b ovstart ovjboss
- 3 重新启动 NPS。

验证集成配置的 NNMi 端

在 NNMi 控制台中,打开 HP NNMi-HP SiteScope 系统度量集成配置表单 (集成模块配置 > HP SiteScope 系统度量)。

有关此表单上的字段的信息,请参阅第 492 页的 HP NNMi-HP SiteScope 系统度量集成配置表单引用。

2 要检查集成的状态,请在 HP NNMi–HP SiteScope 系统度量集成配置表单中,单击表单底部的提交(不进行任何配置更改)。

此窗口将显示状态消息。

3 验证与 NNMi 的连接是否已正确配置:

如果在此过程的步骤 1 中已使用此步骤中所述信息连接到 NNMi 控制台,则不需要重新连接到 NNMi 控制台。继续执行步骤 4。

a 在Web 浏览器中,输入以下 URL:

< 协议>://<NNMi 服务器>:< 端口>/nnm/

其中的这些变量与 HP NNMi-HP SiteScope 系统度量集成配置表单上的值相关,如下 所示:

- 如果选中 NNMi SSL 已启用复选框,则 < 协议 > 是 https。
- 如果清除 NNMi SSL 已启用复选框,则 < 协议 > 是 http.
- <NNMi 服务器 > 是 NNMi 主机的值。
- <端□>是 NNMi 端口的值。

b 提示时,输入具有管理员角色的 NNMi 用户的凭证。

此时应当看到 NNMi 控制台。如果 NNMi 控制台未出现,请联系 NNMi 管理员以 验证用于连接到 NNMi 的信息。继续对 NNMi 连接进行故障诊断,直到 NNMi 控 制台出现。



- 无法作为具有 Web 服务客户端角色的用户登录到 NNMi 控制台。
- c 请联系 NNMi 管理员以验证具有 Web 服务客户端角色的 NNMi 集成用户的 NNMi 用户和 NNMi 密码的值。

密码在 NNMi 控制台中是隐藏的。如果您不能确定为 NNMi 用户名指定的密码,可以请 NNMi 管理员重置密码。

4 使用在此过程的步骤 3 中用于成功连接的值更新 HP NNMi-HP SiteScope 系统度量集成配置表单。

有关详细信息,请参阅第 492 页的 HP NNMi-HP SiteScope 系统度量集成配置表单引用。

- 5 单击表单底部的提交。
- 6 如果状态消息仍指示存在问题,请执行以下操作:
 - a 清除 Web 浏览器缓存。
 - b 从 Web 浏览器清除所有保存的表单或密码数据。
 - c 完全关闭 Web 浏览器窗口,然后重新打开它。
 - d 重复此过程的步骤 4 和步骤 5。
- 7 按第 489 页的验证集成数据流中所述观察 SiteScope 监视器数据的传输以测试配置。

防火墙后面的 NAT 环境中的节点无报告数据

在网络地址转换 (NAT) 环境中,如果在防火墙后面部署 SiteScope 服务器,而具有重复 IP 地址的节点的报告数据在防火墙以外,则 NNMi 无法确定正在监视哪个节点。在这种情况下,集成不会向 NPS 提供这些节点的 SiteScope 数据,因此 NPS 报告未包含此信息。

HP NNMi-HP SiteScope 系统度量集成配置表单引用

HP NNMi-HP SiteScope 系统度量集成配置表单包含用于配置 NNMi 和 SiteScope 之间的通信的参数。此表单是通过集成模块配置工作区提供的。



只有具有管理员角色的 NNMi 用户才可以访问 HP NNMi-HP SiteScope 系统度量集成配置 表单。

HP NNMi-HP SiteScope 系统度量集成配置表单采集信息以识别 NNMi 管理服务器。

要应用集成配置更改,请更新 HP NNMi–HP SiteScope 系统度量集成配置表单上的值,然后单击提交。

表 52 列出用于连接到 NNMi 管理服务器的参数。这就是您用于打开 NNMi 控制台的信息。通过查看调用 NNMi 控制台会话的 URL,可以确定这些值中的大部分。与 NNMi 管理员协作,为配置表单的这一部分确定合适的值。

表 52 NNMi 管理服务器信息

字段	描述
启用 NNMi SSL	连接协议规范。 如果将 NNMi 控制台配置为使用 HTTPS,则选中 NNMi SSL 已启用 复选框。 如果将 NNMi 控制台配置为使用 HTTP,则清除 NNMi SSL 已启用 复选框。
NNMi 主机	NNMi 管理服务器的完全限定域名。此字段已预填充了用于访问 NNMi 控制台的主机 名。验证此值是否是由在 NNMi 管理服务器上运行的 nnmofficialfqdn.ovpl -t 命 令返回的名称。
NNMi 端口	用于连接到 NNMi 控制台的端口。此字段预填充了 jboss 应用程序服务器用于与 NNMi 控制台通信的端口,如以下文件中所指定: • Windows: %NnmDataDir%\conf\nnm\props\nms-local.properties • UNIX: \$NnmDataDir/conf/nnm/props/nms-local.properties 对于非 SSL 连接,使用 jboss.http.port 的值,它的默认值为 80 或 8004 (具体取决 于安装 NNMi 时是否存在另一个 Web 服务器)。 对于 SSL 连接,使用 jboss.https.port 的值,它的默认值为 443。
NNMi 用户	用于连接到 NNMi 控制台的用户名。此用户必须具有 Web 服务客户端角色。
NNMi 密码	指定 NNMi 用户的密码。

HP Systems Insight Manager

HP Systems Insight Manager (SIM) 提供 HP 服务器和存储设备的系统管理。 SIM 功能包括系统搜索和标识、单个事件视图、资产数据采集和报告。

SIM 有助于以下任务:

- 对跨服务器和存储基础结构的复杂问题进行故障诊断。
- 维护服务器和存储资产信息。
- 在执行对基础结构和应用程序的更改之前,对更改影响建模。
- 通过搜索的更改历史记录,跟踪实际的计划更改和未计划更改。
- 通过知晓现有数据存储库,获得环境的共享授权视图。
- 培训跨各个专业领域的网络管理人员。
- 将网络管理的重点从日常维护转移到未来业务需要。

有关购买 SIM 的信息,请联系 HP 销售代表。

本章包含以下主题:

- HP NNMi-HP SIM 集成
- 启用 HP NNMi-HP SIM 集成
- 使用 HP NNMi-HP SIM 集成
- 更改 HP NNMi-HP SIM 集成配置
- 禁用 HP NNMi-HP SIM 集成
- 对 HP NNMi-HP SIM 集成进行故障诊断
- HP NNMi-HP SIM 集成配置表单参考

HP NNMi-HP SIM 集成

HP NNMi-HP SIM 集成提供用于从 NNMi 控制台访问若干 SIM 工具的操作。

价值

HP NNMi-HP SIM 集成将网络设备信息添加到 NNMi,以便 NNMi 用户可以检测并调查 HP ProLiant 服务器和存储设备的潜在网络问题。

集成产品

本章中的信息适用于以下产品:

• SIM

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

• NNMi 9.10

NNMi 和 SIM 必须安装在不同的计算机上。 NNMi 管理服务器和 SIM 服务器计算机可以 使用相同或不同的操作系统。

有关 NNMi 的受支持硬件平台和操作系统的最新信息,请参阅 NNMi 系统和设备支持列表。

有关 SIM 的受支持硬件平台和操作系统的最新信息,请参阅位于以下地址的 QuickSpecs:

www.hp.com/go/sim

文档

本章描述如何配置 NNMi 以与 SIM 通信和如何从 NNMi 控制台使用集成。

SIM 文档套件详细描述 SIM 功能。文档套件可从位于以下地址的 SIM 信息库下载:

www.hp.com/go/sim

启用 HP NNMi-HP SIM 集成

在 NNMi 管理服务器上,通过执行以下步骤,配置 NNMi 和 SIM 之间的连接:

- 1 在 NNMi 控制台中,打开 HP NNMi-HP SIM 集成配置表单(集成模块配置 > HP SIM)。
- 2 选中启用集成复选框以激活表单上的其余字段。
- 3 输入用于连接到 NNMi 管理服务器的信息。有关这些字段的信息,请参阅第 498 页的 NNMi 管理服务器连接。
- 4 输入用于连接到 SIM 服务器的信息。有关这些字段的信息,请参阅第 499 页的 SIM 服务器连接。
- 5 单击表单底部的提交。

将会出现新窗口,其中显示状态消息。如果消息指出连接到 NNMi 管理服务器时发生问题,则单击返回,然后按照错误消息文本的建议调整值。

- 6 加载 SIM 所管理设备的事件定义:
 - a 切换到以下目录:
 - Windows: %NnmInstallDir%\newconfig\HPOvNmsEvent
 - UNIX: \$NnmInstallDir/newconfig/HPOvNmsEvent
 - b 通过输入以下命令,导入 SIM 事件定义:

nnmconfigimport.ovpl -f nnm-sim-incidentConfig.xml \ -u <*用户名*> -p <密码>

- 7 以下操作可选,建议执行。为 SIM 所管理设备生成的陷阱加载 MIB 定义文件:
 - a 切换到以下目录:
 - Windows: %NNM_SNMP_MIBS%\Vendor\Hewlett-Packard\SystemsInsightManager
 - UNIX: \$NNM_SNMP_MIBS/Vendor/Hewlett-Packard/SystemsInsightManager
 - b 使用 nnmloadmib.ovpl 命令加载被管环境的适合 MIB 文件。例如:

nnmloadmib.ovpl -load cpqhost.mib -u <用户名> -p <密码>

- 对于 HP ProLiant 设备陷阱,加载 cpqhost.mib 文件,然后加载
 SystemsInsightManager 目录中其余的 cpq*.mib 文件。
- 一 对于 HP Virtual Connect 设备陷阱,将 vc*.mib 文件和 fa-mib40.mib 文件加载到 NNMi 中。
- c 通过输入以下命令,验证 MIB 是否正确加载:

nnmloadmib.ovpl -list -u <用户名> -p <密码>

使用 HP NNMi-HP SIM 集成

HP NNMi-HP SIM 集成将提供从 NNMi 控制台到位于某个设备上的 SIM 代理或者直接 到 SIM 的链接。集成不提供产品之间的单点登录。必须输入 SIM 用户凭证才能查看 SIM 页。

启用 HP NNMi-HP SIM 集成会将以下操作添加到 NNMi 控制台:

- HP System Management Homepage 为 NNMi 控制台中选择的节点打开 HP System Management 设备主页。
- HP Systems Insight Manager 主页 打开 SIM 主页。
- HP Systems Insight Manager 为在 NNMi 控制台中选择的节点打开 SIM 系统页。

更改 HP NNMi-HP SIM 集成配置

- 1 在 NNMi 控制台中,打开 HP NNMi-HP SIM 集成配置表单 (集成模块配置 > HP SIM)。
- 2 对值进行相应修改。有关此表单上的字段的信息,请参阅第 498 页的 HP NNMi-HP SIM 集成配置表单参考。
- 3 验证表单顶部的**启用集成**复选框是否已选中,然后单击表单底部的提交。



更改会立即生效。不需要重新启动 ovjboss。

禁用 HP NNMi-HP SIM 集成

- 1 在 NNMi 控制台中, 打开 HP NNMi-HP SIM 集成配置表单 (集成模块配置 > HP SIM)。
- 2 清除表单顶部的**启用集成**复选框,然后单击表单底部的提交。集成操作不再可用。



更改会立即生效。不需要重新启动 ovjboss。

对 HP NNMi-HP SIM 集成进行故障诊断

SIM 操作不运行

如果已经验证了 HP NNMi-HP SIM 集成配置表单中的值,并且仍然不能从 NNMi 控制台打开 SIM 页,则执行以下操作:

- 1 清除 Web 浏览器缓存。
- 2 从 Web 浏览器清除所有保存的表单或密码数据。
- 3 完全关闭 Web 浏览器窗口, 然后重新打开它。
- 4 在 HP NNMi-HP SIM 集成配置表单中重新输入值。

因为 NNMi 无法以静默方式验证与 SIM 服务器的连接,因此 HP NNMi-HP SIM 集成配置表单状态消息仅适用于 NNMi 管理服务器连接信息。

5 通过在 Web 浏览器中打开 SIM 主页,验证 SIM 是否正在运行。

陷阱中的 "MIB 缓存中找不到 OID" 消息

如果 NNMi 中未加载 SIM 所管理设备所生成陷阱的 MIB 定义文件,则您会看到与以下文本类似的错误:

<mib 缓存中找不到值为1的Cia.1.3.6.1.4.1.11.5.7.5.2.1.1.1.7.0>

要解决这些错误,请如第 495 页的步骤 7 中所述加载 MIB。

HP NNMi-HP SIM 集成配置表单参考

HP NNMi-HP SIM 集成配置表单包含用于配置 NNMi 和 SIM 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。



只有具有管理员角色的 NNMi 用户才可以访问 HP NNMi-HP SIM 集成配置表单。

HP NNMi-HP SIM 集成配置表单采集以下常规方面的信息:

- NNMi 管理服务器连接
- SIM 服务器连接

要应用对集成配置的更改,请在 HP NNMi-HP SIM 集成配置表单上更新值,然后单击提交。

NNMi 管理服务器连接

表 53 列出用于连接到 NNMi 管理服务器的参数。这就是您用于打开 NNMi 控制台的信息。通过查看调用 NNMi 控制台会话的 URL,可以确定这些值中的大部分。与 NNMi 管理员协作,为配置表单的这一部分确定合适的值。

寿	53	NNMi	答理眼	么	哭	信	自
ᅑ	J J	INTATAT	百垤加	97	' 6 67'	16	应

字段	描述
启用 NNMi SSL	连接协议规范。 如果将 NNMi 控制台配置为使用 HTTPS,则选中 NNMi SSL 已启用复选框。这是默认配置。 如果将 NNMi 控制台配置为使用 HTTP,则清除 NNMi SSL 已启用复选框。
NNMi 主机	NNMi管理服务器的完全限定域名。此字段已预填充了用于访问 NNMi 控制台的主机名。 验证此值是否是由在 NNMi管理服务器上运行的 nnmofficialfqdn.ovpl -t 命令返 回的名称。
NNMi 端口	用于连接到 NNMi 控制台的端口。此字段预填充了 jboss 应用程序服务器用于与 NNMi 控制台通信的端口,如以下文件中所指定: • Windows: %NnmDataDir%\conf\nnm\props\nms-local.properties • UNIX: \$NnmDataDir/conf/nnm/props/nms-local.properties 对于非 SSL 连接,使用 jboss.http.port 的值,它的默认值为 80 或 8004(具体取决 于安装 NNMi 时是否存在另一个 Web 服务器)。 对于 SSL 连接,使用 jboss.https.port 的值,它的默认值为 443。

2011年3月

表 53 NNMi 管理服务器信息 (续)

字段	描述
NNMi 用户	用于连接到 NNMi 控制台的用户名。此用户必须具有 NNMi 管理员或 Web 服务客户端 角色。
NNMi 密码	指定 NNMi 用户的密码。

SIM 服务器连接

表 54 列出用于连接到 SIM 服务器以打开 SIM 页的参数。与 SIM 管理员协作,为配置的 这一部分确定合适的值。

表 54 SIM 服务器信息

SIM 服务器参数	描述
启用 SIM SSL	用于连接到 SIM 的连接协议规范。 如果配置 SIM 使用 HTTPS,则选中启用 HP SIM SSL 复选框。这是默认配置。 如果配置 SIM 使用 HTTP,则清除启用 HP SIM SSL 复选框。
SIM 主机	SIM 服务器的完全限定域名。
SIM 端口	用于连接到 SIM 的端口。 如果正在使用默认 SIM 配置,则使用端口 50000 (对于与 SIM 的 SSL 连接)。

nGenius Performance Manager

	් ස් 🖾	R Phone Users - 6 (VolP_)	(_EN0.04)	් ස් 🗵
Utilization - H0_0FWX3 From 15 min samples	-	Ehone Users MulP_IT_EN	o inte	
	VPN_User	Active ' Phone Number	User Name	Heat
	Weber	4 8708184318	Sapkal, Rahul	18216813585
	E (MTP	2 919794555187	Inching Collectors	192 108 130 196
	EPSec-ESP	A 1013	Nagalaflamesh	192 168 121 47
	Cons Line	2 2445	Paulta Main	101.102.101.20
	290LU			
Link Usage over Time - 10 Bioston)				188
81%	=	~~~~	\sim	
	12-40-00 12-40-00 15 Mar 1, 2000, Eastern Tax	1900 12900 12000 dae fine		10 0 0 0 0
ext up to up	C-40-00 C-40-00 S War C 2000, Eastern Far	NOR ONO ORIO	1.05.08 12.10.08	
Control of the second for this pel Control of the second for t	Union Union s West, 2000, Fasters for Wester, a rd 67 (2)	Data Source Headlo on	10000 10100 Lastinour - 10107 51 Time - 1 (fould) Blocks - fould	10 10 10 10 10 10 10 10 10 10 10 10 10 1
Control	U-000 U-000 S Ref (1000, Eather the Meter) of S ² S Reg Tran Drawatiety	1000 0.000 0.000 and Time Data Bourse Health one (Fig	1200-00 12:00-00 Lastinitur - 11/107 5.1 Time - 1 (Roder) Billioton - Rober 5 nin suniden	19 100 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
the design of the second dor the poll the seco	the set of	These Canada Calenda And Tana	120500 12:0000 (Lastiniour - 11010)7 51 (Time - 1 (Roder) (Riteator: Roder 6 no societos	
execution control of the set of	United of the second se	The Chief Constant	Caldeas Canada (Caldining - 11/10/7 6.1 (Time - 1 (Rodel) (Rington - Roder 8 no nordels	
Control Control Control Control Control Control Control Control Control Control Control Control Control Control Contro Control Control Control Contro Control Co	12-00 12 -00 10 12 We 1 - 1000. Earlies for We 1 - 1000. Earlies for 0 - 10 - 00 - 00 0 - 10 - 000 - 00 0 - 10 - 000 - 000 0 - 10 - 000 - 000 0 - 000	Della Source Health one and Time	10668 13458 (Lastineyr - 151027 6 1 Time - 1 (Roder) Hitston - Ruse 5 no notides	5 PHEOD 5 PHEOD 5 PHEOD 5 PHEOD 6 Pheodem Rev 6 Pheodem Rev 7 Pheodem Rev
$\label{eq:constraints} \begin{array}{c} & & & & \\ & & & & \\ & & & & \\ & & & & $	12-000 12-000 5 We 1,000, Eathers Ho We 1,000, Eathers Ho 0-000 at 0-000	55:00 0.05:00 0.00:00 • Data Source Health one of the source of	10050 1000 (Latineur - 10107 51 Time 1 (Rode) (Ristato, Australia Seconsolution Seconsolution	S FREED S FREE

NetScout Systems nGenius Performance Manager 能使复杂网络清晰化以供用于以下用途:

- 应用程序识别和监视
- 对数据包和流量进行分析和故障诊断
- 响应时间分析
- 报告和容量计划
- 集中管理
- 报警和事件标识

nGenius Performance Manager 借助深入数据包检查和基于流量的技术,使用户能够了解跨越多种数据的实时操作信息:

- 高级别的关键性能指标 (KPI), 比如响应时间、错误或抖动
- 应用程序流数据,比如利用率、会话或排名靠前的会话者
- 数据包级别的分析,比如解码和反弹图

nGenius Performance Manager 从各类网络数据源采集性能数据,以便能够监视所有网络基础结构、拓扑和应用程序的使用模式。nGenius Performance Manager 随后在一系列实时和历史视图及报告中显示这些结果,提供的信息如下:

- 应用程序性能
- 网络资源的用户和滥用者
- 资源所占用的网络容量

有关购买 nGenius Performance Manager 的信息,请联系 HP 销售代表。

本章包含以下主题:

- HP NNMi-nGenius Performance Manager 集成
- 启用 HP NNMi-nGenius Performance Manager 集成
- 使用 HP NNMi-nGenius Performance Manager 集成
- 禁用 HP NNMi-nGenius Performance Manager 集成
- 对 HP NNMi-nGenius Performance Manager 集成进行故障诊断

HP NNMi-nGenius Performance Manager 集成

通过在 HP Network Node Manager i Software (NNMi)环境中包含 nGenius Performance Manager,使用 NNMi 监视和管理其网络设备的网络管理员通过 nGenius 设备可在应用 程序级别了解这些设备。

HP NNMi-nGenius Performance Manager 集成提供以下功能:

- 在 NNMi 事件视图中显示 nGenius Performance Manager 服务器报警和探测器 报警。
- 通过在 nGenius Performance Manager 中启动上下文视图来调查事件的原因。
- 在 NNMi 图视图中显示带 NetScout 图标的 nGenius Probe。
- 从 NNMi 控制台启动 nGenius Performance Manager 快速视图。
- 从 NNMi 控制台启动 nGenius Performance Manager 应用程序。
- 为 NNMi 事件视图中提供的 nGenius Performance Manager 事件启动 NNMi 第 2 层 和第 3 层邻居视图。
- 为 NNMi 事件视图中提供的 nGenius Performance Manager 事件启动 NNMi 路径视 图图。
- 对于 nGenius Performance Manager 生成的每个报警,将"清除陷阱"报警转发到 NNMi。

价值

HP NNMi-nGenius Performance Manager 集成提供以下好处:

- 减少支持最大网络可用性所需的成本。
- 在单个控制台中合并网络管理基础结构。
- 通过集成的故障和应用程序感知的性能数据,提高员工生产力和效率。
- 通过对流量和数据包级别的详细信息进行上下文相关的向下钻取来识别性能问题,从而 减低 **MTTR**。

集成产品

本章中的信息适用于以下产品:

nGenius Performance Manager

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

- nGenius Performance Manager 附带的 nGenius K2 版本
- CDM 代理固件
- nGenius InfiniStream Appliance
- NNMi 9.10

NNMi 和 nGenius Performance Manager 服务器必须安装在不同的计算机上。 NNMi 管 理服务器和 nGenius Performance Manager 服务器计算机可以使用相同或不同的操作系统。

文档

在以下文档中完整描述了 HP NNMi 杗 Genius Performance Manager 集成:

将 nGenius Performance Manager 与HP Network Node Manager i Software 集成 (NetScout 部件号 733-0194 修订版 A,可从 http://www.netscout.com 获取)

启用 HP NNMi-nGenius Performance Manager 集成

nGenius Performance Manager 服务器上的以下位置提供了 nGenius Performance Manager 与 HP Network Node Manager 的集成实用程序的安装文件:

- Windows: %nGenius Install%\rtm\bin\nGeniusNNM8.zip
- UNIX: \$nGenius Install/rtm/bin/nGeniusNNM8.zip

以具有管理特权或根特权的用户身份在 NNMi 管理服务器上安装集成实用程序。实用程序 将 nGenius 服务器的与 NNMi 集成相关的所有配置数据导入到 NNMi 中。

用于安装 nGenius Performance Manager 集成实用程序的高级别步骤如下。有关详细信息,请参阅将 nGenius Performance Manager 与 HP Network Node Manager i Software *集成*。

- 1 解压缩安装文件,并在 nGenius Performance Manager 中配置 NNMi 支持。
- 2 在 NNMi 中配置 NetScout 事件 (报警)。
- 3 配置 nGenius Probe 以将 SNMP 陷阱发送到端口 395。
- 4 可选。配置探测器路由器映射。

使用 HP NNMi-nGenius Performance Manager 集成

有关使用 HP NNMi-nGenius Performance Manager 集成的信息,请参阅 将 nGenius Performance Manager 与 HP Network Node Manager i Software 集成。

禁用 HP NNMi-nGenius Performance Manager 集成

有关禁用 HP NNMi-nGenius Performance Manager 集成的信息,请参阅将nGenius Performance Manager 与HP Network Node Manager i Software 集成。

对 HP NNMi-nGenius Performance Manager 集成进行故障诊断

有关对 HP NNMi-nGenius Performance Manager 集成进行故障诊断的信息,请联系 NetScout Systems 客户支持。联系信息可从以下地址获取:

http://www.netscout.com/support
NNMi Northbound Interface



HP Network Node Manager i Software (NNMi) 提供 NNMi Northbound Interface,用于将 NNMi 事件转发到 可以接收 SNMPv2c 陷阱的任何应用程序。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 Interface,对每个应用程序都单独进行配置。

NNMi 支持使用 NNMi Northbound Interface 与以下产品集成:

- HP Business Service Management (BSM) 平台的 Operations Management 功能;有关信息,请参阅第 521 页的 HP BSM Operations Management。
- HP Operations Manager (HPOM) 活动消息浏览器;有关信息,请参阅第 539 页的 HP NNMi—HPOM 集成 (代理实施)。
- IBM Tivoli Netcool/OMNIbus; 有关信息,请参阅第 577页的 HP NNMi Integration Module for Netcool Software。

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 Interface
- 启用 NNMi Northbound Interface
- 使用 NNMi Northbound Interface
- 更改 NNMi Northbound Interface
- 禁用 NNMi Northbound Interface
- 对 NNMi Northbound Interface 进行故障诊断
- 应用程序故障切换和 NNMi Northbound Interface
- NNMi Northbound Interface 目标表单参考

NNMi Northbound Interface

NNMi Northbound Interface 将 NNMi 管理事件作为 SNMPv2c 陷阱转发到 northbound 应用程序。northbound 应用程序可过滤、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 Interface 可以将事件生命周期状态更改通知、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 Interface 还可以将 NNMi 接收的 SNMP 陷阱转发到 northbound 应 用程序。 NNMi Northbound Interface 不会将 NNM 6.x 或 7.x 管理工作站生成的事件转 发到 northbound 应用程序。

价值

NNMi Northbound Interface 通过第三方或自定义的事件合并器实现事件合并。NNMi Northbound Interface 用可用于将 NNMi 与其他应用程序集成的信息强化事件。

受支持版本

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 系统和设备支持列表。

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 Interface 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 Interface 的一个配置,定义与 northbound 应 用程序的陷阱接收组件的连接,并指定该 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 Interface

Λ

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 Interface,请遵循以下步骤:

- 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 Interface 目标表单(集成模块配置 > Northbound Interface),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,请参阅第 515 页的 Northbound 应用程序连接参数。

- d 指定关于将哪些内容发送到 northbound 应用程序的发送选项和事件过滤器。 有关这些字段的信息,请参阅第 516 页的 NNMi Northbound Interface 集成 内容。
- e 单击表单底部的提交。

将会出现新窗口,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 > 在别处将 NNMi 与 URL 集成。

使用 NNMi Northbound Interface

启用 NNMi Northbound Interface 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 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,请参阅第 516 页的 NNMi Northbound Interface 集成内容。

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态时, NNMi 将它发送到 northbound 应用程序。

所转发管理事件的 OID 是 NNMi 控制台中**管理事件配置**表单上的 SNMP 对象 ID。 NNMi 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,则当关联事件更改为已注册生命周期状态时,NNMi 将每个传入 SNMPv1、v2c 或 v3 格式的陷阱转发到 northbound 应用程序。NNMi 妥善保留原始陷阱 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 NNMi 无法正确地重新构造陷阱并追加 NNMi 事件数据;因此 NNMi 不转发此陷阱。

对于第三方 SNMP 陷阱,注意以下事项:

- 因为 NNMi 从其 SNMP 陷阱事件中重新构造陷阱,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 管理服务器显示为陷阱源。要确定原始陷阱源,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,请参阅第93页的陷阱和事件转发。

事件生命周期状态更改通知

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态更改为 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态值。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。

 状态更改陷阱 如果 northbound 目标包含生命周期状态已更改通知,则当 NNMi 中事件的生命周期状态 更改为进行中、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态更改:

• 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)

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

下表列出生命周期状态的可能整数值。

事件关联通知

如果 northbound 目标包含事件关联通知,则当 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,则当在 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。

事件转发过滤器

如果 northbound 目标包含事件过滤器,则过滤器中的对象标识符 (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:

- 如果事件过滤器阻止转发某一关联的父事件,则 NNMi 不将关联通知陷阱发送到 northbound 应用程序。
- 如果事件过滤器阻止转发某一关联的子事件,则转发关联通知陷阱不包含该子事件的UUID。(如果关联通知陷阱不包含任何子事件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。如果事件过滤器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 Interface

要更改 NNMi Northbound Interface 配置参数,请遵循以下步骤:

- 在 NNMi 控制台中,打开 HP NNMi-Northbound Interface 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。 有关此表单上的字段的信息,请参阅第 515 页的 NNMi Northbound Interface 目标表 单参考。
- 4 验证表单顶部的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 Interface

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,请遵循以下步骤:

- 在 NNMi 控制台中,打开 HP NNMi-Northbound Interface 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 不要选中表单顶部的启用复选框,然后单击表单底部的提交。 更改会立即生效。

对 NNMi Northbound Interface 进行故障诊断

如果 NNMi Northbound Interface 没有按预期工作,则遵循以下步骤,直到问题得到 解决:

- 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 Interface 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 将事件生命周期状态设置为已注册,然后单击 🔛 保存。
 - c 将事件生命周期状态设置为已关闭,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 目标以与不同的 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诊断信息。

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*搜索的节点*是 NNMi 拓扑中节点的主机名或 IP 地址, NNMi 节点 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 Interface 正在正常运行。
 - 如果 northbound 应用程序未接收陷阱,则配置新 northbound 目标以与不同的 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诊断信息。

如果重复测试失败,则联系 HP 支持以获取帮助。

应用程序故障切换和 NNMi Northbound Interface

如果 NNMi 管理服务器将参与 NNMi 应用程序故障切换,则此主题中的信息适用于任何实现 NNMi Northbound Interface 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。在应用程序故障切换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 Interface 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 Interface。

在 HP NNMi-Northbound Interface 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 Interface 确定当前 NNMi 管理服务器的正确名称或 IP 地址。这样,Northbound Interface 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 Interface。在 HP NNMi-Northbound Interface 目标 表单上,选择**其他**选项用于**主机**标识。

NNMi Northbound Interface 目标表单参考

HP NNMi–Northbound Interface 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 Interface 目标表单上,单击新建;或选择目标,然后单击编辑。)



只有具有管理员角色的 NNMi 用户才可以访问 HP NNMi-Northbound Interface 目标表单。

HP NNMi-Northbound Interface 目标表单包含以下方面的信息:

- 第 515 页的 Northbound 应用程序连接参数
- 第 516 页的 NNMi Northbound Interface 集成内容
- 第 518 页的 NNMi Northbound Interface 目标状态信息

要应用集成配置更改,请更新 HP NNMi–Northbound Interface 目标表单上的值,然后单击 提交。

Northbound 应用程序连接参数

表 55 列出用于配置 northbound 应用程序连接的参数。

表 55 Northbound 应用程序连接信息

字段	描述
主机	运行 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 管理与 NNMi 管理服务器上的 northbound 应用程序的连接,并且 主机 字段变成只读的。 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 字段变成只读的。
	• 其他 在 圭机 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 圭机 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。
	注:如果 NNMi 管理服务器参与 NNMi 应用程序故障切换,请参阅第 513 页的应用程序 故障切换和 NNMi Northbound Interface,以了解有关应用程序故障切换对集成的影响 的信息。

表 55 Northbound 应用程序连接信息(续)

字段	描述
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。 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 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)。
共用字符串	northbound 应用程序用于接收陷阱的只读共用字符串。 如果 northbound 应用程序配置需要在所接收的 SNMP 陷阱中有共用字符串,则输入 该值。 如果 northbound 应用程序配置不需要特定共用字符串,则使用默认值 public。

NNMi Northbound Interface 集成内容

表 56 列出用于配置 NNMi Northbound Interface 将哪些内容发送到 northbound 应用程序的参数。

表 56 NNMi Northbound Interface 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。
	 两者 NNMi 将 NNMi 生成的管理事件和 NNMi 从被管设备接收到的 SNMP 陷阱一并转 发到 northbound 应用程序。 这是默认配置。
	一旦启用 northbound 目标, NNMi 就开始转发事件。 有关详细信息,请参阅第 508 页的事件转发。

表 56	NNMi Northbound Interface	内容配置信息	(续)
------	---------------------------	--------	-----

字段	描述
生命周期状态更改	 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态的每个事件,NNMi 会将"事件已关闭"陷阱发送到 northbound 应用程序。 这是默认配置。 状态已更改 对于生命周期状态更改为进行中、已完成或已关闭的每个事件,NNMi 将"事件生命 周期状态已更改"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态的每个事件,NNMi 会将"事件已关闭"陷阱发送到 northbound 应用程序。另外,对于生命周期状态更改为进行中、已完成或已关闭的每 个事件,集成将"事件生命周期状态已更改"陷阱发送到 northbound 应用程序。 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改"陷阱。
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事件关联关系发送陷阱。 组 NNMi 对于列出关联到父事件的所有子事件的每个关联发送一个陷阱。 有关详细信息,请参阅第 509 页的事件关联通知。
删除	 事件删除规范。 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,请参阅第 510 页的事件删除通知。

表 56 NNMi Northbound Interface 内容配置信息(续)

字段	描述
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。
事件过滤器	对象标识符 (OID) 的列表,集成据此过滤发送到 northbound 应用程序的事件。每个过滤 器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 将所有事件发送到 northbound 应用程序。 这是默认配置。 • 包含 NNMi 仅发送与过滤器中识别出的 OID 相匹配的特定事件。 • 排除 NNMi 发送所有事件,不包括与过滤器中识别出的 OID 相匹配的特定事件。 指定事件过滤器: • 要添加过滤器条目,请在下部的文本框中输入文本,然后单击 添加 。 • 要删除过滤器条目,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,请参阅第 510 页的事件转发过滤器。

NNMi Northbound Interface 目标状态信息

表 57 列出 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。

表 57 NNMi Northbound Interface 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。
	此旧对丁元 normbound 日你吧。

2011年3月

字段	描述
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 Interface 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。

表 57 NNMi Northbound Interface 目标状态信息(续)

HP BSM Operations Management



HP Business Service Management (BSM) 平台的 Operations Management 功能提供全面事件管理、主动性能监视以及自动警报、报告和制图功能,用于管理操作系统、中间件和应用程序基础结构。BSM Operations Management 能够将来源广泛的事件整合到单个视图中。

有关购买 BSM 的信息,请联系 HP 销售代表。

本章包含以下主题:

- 第 521 页的 HP NNMi—HP BSM Operations Management 集成
- 第 523 页的启用 HP NNMi—HP BSM Operations Management 集成
- 第 526 页的使用 HP NNMi-HP BSM Operations Management 集成
- 第 528 页的更改 HP NNMi—HP BSM Operations Management 集成
- 第 530 页的禁用 HP NNMi—HP BSM Operations Management 集成
- 第 530 页的对 HP NNMi—HP BSM Operations Management 集成进行故障 诊断
- 第 534 页的 HP NNMi—HPOM 代理目标表单参考 (BSM Operations Management 集成)

HP NNMi—HP BSM Operations Management 集成

HP NNMi—HP BSM Operations Management 集成将 NNMi 管理事件作为 SNMPv2c 陷阱转发到 NNMi 管理服务器上的 HP BSM Integration Adapter。BSM Integration Adapter 过滤 NNMi 陷阱,并且将它们转发到 BSM Operations Management 事件浏览器。

HP NNMi—HP BSM Operations Management 集成还可以将 NNMi 接收到的 SNMP 陷阱转发到 Integration Adapter。集成不会将 NNM 6.x 或 7.x 管理工作站生成的事件转发到 Integration Adapter。

HP NNMi—HP BSM Operations Management 集成还允许从 BSM Operations Management 事件浏览器内访问 NNMi 控制台。

-

本章描述 NNMi 和 BSM Operations Management 事件浏览器之间的直接集成。或者, 可以将 NNMi 与 HP Operations Manager (HPOM) 集成,后者随即将事件转发到 BSM Operations Management 事件浏览器。

HP NNMi—HP BSM Operations Management 集成是 NNMi Northbound Interface 的 特定实施,如第 505 页的 NNMi Northbound Interface 中所述。

HP NNMi—HP BSM Operations Management 集成由以下组件组成:

- nnmi-hpom 代理集成模块
- nnmopcexport.ovpl 工具

价值

HP NNMi 程 P BSM Operations Management 集成在 BSM Operations Management 事 件浏览器中提供关于网络管理、系统管理和应用程序管理方面的事件合并,以便 BSM Operations Management 事件浏览器的用户可以检测并调查潜在网络问题。

集成的主要功能如下:

- 从 NNMi 转发到 BSM Integration Adapter 的自动事件。转发的事件出现在 BSM Operations Management 事件浏览器中。
- 从 BSM Operations Management 事件浏览器访问 NNMi 控制台。
 - 在所选事件的上下文中打开 NNMi 事件表单。
 - 在所选事件和节点的上下文中打开 NNMi 视图 (例如, 第2层邻居视图)。
 - 在所选事件和节点的上下文中启动 NNMi 工具 (例如,状态轮询)。

集成产品

本章中的信息适用于以下产品:

• 带有 HP Operations Manager i 许可证的 BSM

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

• 仅 Windows 或 Linux 操作系统上的 NNMi 9.10

NNMi 和 BSM 必须安装在不同的计算机上。 NNMi 管理服务器和 BSM 服务器计算机可以使用相同的或不同的操作系统。

BSM Integration Adapter 需要许可证,并且必须在安装 NNMi 之后 安装在 NNMi 管理服务器计算机上。

有关受支持的硬件平台和操作系统的最新信息,请参阅所有产品的支持列表。

文档

本章描述如何配置 NNMi 以与 BSM Operations Management 事件浏览器通信。

BSM 文档描述如何安装和使用从 BSM Operations Management 事件浏览器访问 NNMi 控制台的 BSM Integration Adapter 和应用程序。

- 《HP BSM Integration Adapter 安装和配置指南》
- 《HP BSM Integration Adapter 用户指南》
- HP BSM Integration Adapter 帮助
- 《HP BSM Operations Management 可扩展性指南》

启用 HP NNMi—HP BSM Operations Management 集成

建议让有经验的 BSM Integration Adapter 用户完成启用 HP NNMi—HP BSM Operations Management 集成的过程。



NNMi 与 HP Business Service Management (BSM) 拓扑数据库集成时, HP NNMi— HP BSM Operations Management 集成可以将关于 NNMi 所管理设备的事件与 BSM 配 置项 (CI) 关联。标准 NNMi Northbound Interface 未提供此信息。有关详细信息,请参 阅第 526 页的配置项标识符。

要启用 HP NNMi—HP BSM Operations Management 集成, 遵循以下步骤:

- 1 在 NNMi 管理服务器上,为 NNMi 转发的陷阱生成 SNMP 陷阱策略文件:
 - a 验证 NNMi 服务是否正在运行:

ovstatus -c

所有 NNMi 服务应当显示状态正在运行。

b 通过输入以下命令, 生成 SNMP 陷阱策略文件:

nnmopcexport.ovpl -u <用户名> -p <密码> \ -template "NNMi Management Events" -application "NNMi" \ -omi_policy -omi_hi

<用户名>和 <密码>的值对应于具有管理员角色的 NNMi 控制台用户。

此命令在当前目录中创建两个文件:

Λ

- *<UUID>_data* 文件是 SNMP 陷阱策略文件,其中 *<UUID>* 是全局唯一标 识符。
- <UUID>_header.xml 文件向 BSM Integration Adapter 标识 <UUID>_data 文件。

不要编辑或重命名这些输出文件,因为这样做会导致 BSM Integration Adapter 不能使用它们。

SNMP 陷阱策略文件将每个管理事件和 SNMP 陷阱配置的策略条件包含到当前 NNMi 事件配置中。有关自定义此命令的输出的信息,请参阅 nnmopcexport.ovpl 参考页或 UNIX 联机帮助页。

有关默认策略条件和自定义条件的信息,请参阅第 526 页的使用 HP NNMi-HP BSM Operations Management 集成。

- 2 在 NNMi 管理服务器上, 配置 BSM Integration Adapter:
 - a 如《HP BSM Integration Adapter 安装和配置指南》中所述,安装并配置 BSM Integration Adapter。

HP Operations agent from HPOM 和 BSM Integration Adapter 不能在一个系统上同时运行。如有必要,在安装 BSM Integration Adapter 之前,卸载 HP Operations Agent。

b 使用 BSM Integration Adapter 用户界面可以导入在此过程的步骤 1 中创建的头 文件和策略文件。

有关详细信息,请参阅 HP BSM Integration Adapter 帮助中的*管理策略 > 导入 策略*。

c 使用 BSM Integration Adapter 用户界面可以激活新策略。

有关详细信息,请参阅 HP BSM Integration Adapter 帮助中的管理策略>激活 和取消激活策略。

3 标识可用于 NNMi 和 BSM Integration Adapter 之间的 SNMP 通信的端口。

BSM Integration Adapter 将在此端口上侦听 NNMi 转发到此端口的 SNMP 陷阱。启用集成时,在此过程的步骤 4 (对于 BSM Integration Adapter)和步骤 5 (对于 NNMi)中都使用此端口号。

SNMP 通信端口不同于您在使用 ia-config.bat (Windows) 或 ia-config.sh (Linux) 命令配置 BSM Integration Adapter 时为 Apache Tomcat 服务器指定的 HTTP 端口。

因为 BSM Integration Adapter 安装在 NNMi 管理服务器上,因此此端口号必须与 NNMi 接收 SNMP 陷阱的端口不同。

- a 在 NNMi 控制台中,从配置工作区打开通信配置表单。
- b 在默认 SNMP 设置区域中,记下 SNMP 端口的值。

- c 选择与通信配置表单上的 SNMP 端口值不同的端口。较好的做法是使用与 162 类似 的端口号,162 是用于接收 SNMP 陷阱的标准 UDP 端口。例如,如果端口 162 不可用,则试用端口 5162。
- d 在 NNMi 管理服务器上,运行命令 netstat -a,然后在输出中搜索在步骤 c 中选择的端口。如果该端口号未出现在输出中,则它可能对 BSM Integration Adapter 是可用的。
- 4 在 NNMi 管理服务器上,通过输入以下命令,对 BSM Integration Adapter 内的代理 配置用于从 NNMi 接收 SNMP 陷阱的自定义端口:
 - Windows NNMi 管理服务器:
 - a 配置代理:

```
ovconfchg -ns eaagt -set SNMP_TRAP_PORT <自定义端口> \
-set SNMP_SESSION_MODE NNM_LIBS
```

b 重新启动代理:

ovc -restart opctrapi

- Linux NNMi 管理服务器:
 - a 配置代理:

```
ovconfchg -ns eaagt -set SNMP_TRAP_PORT <自定义端口> \
-set SNMP_SESSION_MODE NO_TRAPD
```

b 重新启动代理:

ovc -restart opctrapi

对于<自定义端口>,使用在此过程的步骤3中识别的端口。

- 5 在 NNMi 管理服务器上, 配置转发到 BSM Integration Adapter 的 NNMi 事件:
 - a 在 NNMi 控制台中, 打开 HP NNMi-HPOM 集成选择表单(集成模块配置 > HPOM)。
 - b 单击 HPOM 代理实施,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。)

- c 在 HP NNMi-HPOM 代理目标表单上,选中已启用复选框以激活表单上的其余字段。
- d 输入用于连接到 NNMi 管理服务器上的 BSM Integration Adapter 的信息。陷阱 目标端口是在此过程的步骤 3 中识别的端口。

有关这些字段的信息,请参阅第 534 页的 BSM Integration Adapter 连接。

e 指定发送选项。对于 NNMi 控制台访问字段,选择 HTTP 选项。

有关这些字段的信息,请参阅第 535 页的 BSM Operations Management 集成 内容。

f 单击表单底部的提交。

将会出现新窗口,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。

6 可选。在 BSM 服务器上,安装并配置 HPOprInf 基础结构内容包。

有关信息,请参阅《HP BSM Operations Management 可扩展性指南》。

使用 HP NNMi-HP BSM Operations Management 集成

HP NNMi-HP BSM Operations Management 集成提供 NNMi 管理事件和 SNMP 陷阱 到 BSM Operations Management 事件浏览器的单向传送。 NNMi SNMP 陷阱策略确定 BSM Operations Management 事件浏览器如何处理和显示传入陷阱。例如,可以更改策略条件以在事件标题中包括陷阱自定义属性的值。

NNMi 仅将每个管理事件或 SNMP 陷阱的一个副本发送到 BSM Integration Adapter。 此行为不同于 NNM 6.x/7.x 与 HPOM 集成的行为。

在 BSM Operations Management 事件浏览器中查看转发的 NNMi 事件。 BSM Operations Management 事件浏览器中的菜单命令用于在所选事件的上下文中访问 NNMi 视图。嵌入到每个事件中的信息支持此交叉导航:

- 事件中的 nnmi.server.name 和 nnmi.server.port 自定义属性标识 NNMi 管理服务器。
- nnmi.incident.uuid 自定义属性标识 NNMi 数据库中的事件。

在 BSM Operations Management 事件浏览器中,原始陷阱源出现在**其他信息**选项卡上的 对象字段中以及 nnm.source.name 自定义属性中。

配置项标识符

在 HP Business Service Management (BSM) 和 HP Universal CMDB 软件 (UCMDB) 中,配置项 (CI) 是 IT 环境中的组件的数据库表示。CI 可以是某种业务、业务流程、应用 程序、服务器硬件或服务。

NNMi 与 BSM 拓扑数据库或 UCMDB 集成时, NNMi 与 BSM 或 UCMDB 共享 NNMi 所管理设备的 CI 信息。在这种情况下, HP NNMi 桯 P BSM Operations Management 集成可以将关于 NNMi 所管理设备的事件与 BSM 或 UCMDB CI 关联。SNMP 陷阱策略条件启用此关联。

有关与 BSM 和 UCMDB 集成的信息,请参阅:

- 第 423 页的 HP Business Service Management 拓扑
- 第 433 页的 HP Universal CMDB

运行状况指示器

因为 NNMi SNMP 陷阱策略文件是使用带 -omi_hi 选项的 nnmopcexport.ovpl 创建的,因此该策略文件会在适用时将运行状况指示器与 SNMP 陷阱策略文件中的每个标准 NNMi 管理事件相关联。(并非所有管理事件类型都有运行状况指示器。)运行状况指示器 是在 EtiHint 自定义属性中提供的。

有关特定的运行状况指示器,请参阅 SNMP 陷阱策略文件。

默认策略条件

默认集成行为将根据集成内容而有所不同,如下所述:

- NNMi "管理事件"事件
 - NNMi SNMP 陷阱策略文件包含在生成文件时 NNMi 事件配置中定义的所有 NNMi 管理事件配置的条件。
 - 从 NNMi 管理事件创建的事件显示在 BSM Operations Management 事件浏览器中。
 - 这些陷阱包含第 526 页的配置项标识符中所述的 CI 信息。
 - 从这些陷阱创建的事件包含第 527 页的运行状况指示器中所述的运行状况指示器。
- 第三方 SNMP 陷阱
 - NNMi SNMP 陷阱策略文件包含在生成文件时 NNMi 事件配置中定义的所有 SNMP 陷阱配置的条件。
 - 从第三方陷阱创建的事件显示在 BSM Operations Management 事件浏览器中。
 - 这些陷阱包含第 526 页的配置项标识符中所述的 CI 信息。
 - 从这些陷阱创建的事件不包含运行状况指示器。
 - 如果配置了集成以转发所有接收的 SNMP 陷阱,并且 BSM Operations Management 事件浏览器直接从 NNMi 管理的设备接收 SNMP 陷阱,则 BSM Operations Management 事件浏览器接收到重复的设备陷阱。可以设置策略以将 来自 NNMi 的 SNMP 陷阱与 BSM Operations Management 事件浏览器直接从 所管理设备接收的那些陷阱相关联。
- EventLifecycleStateClosed 陷阱
 - BSM Integration Adapter 记录从这些陷阱创建的事件。通常,它们不显示在 BSM Operations Management 事件浏览器中。
 - NNMi SNMP 陷阱策略文件使得 BSM Integration Adapter 确认与 BSM
 Operations Management 事件浏览器中的已关闭 NNMi 事件相对应的事件。

- LifecycleStateChangeEvent 陷阱
 - NNMi SNMP 陷阱策略文件不包含有关处理这些陷阱的条件。 BSM Integration Adapter 不将这些陷阱转发到 BSM Operations Management 事件浏览器。
- EventDeleted 陷阱
 - NNMi SNMP 陷阱策略文件不包含有关处理这些陷阱的条件。BSM Integration Adapter 不将这些陷阱转发到 BSM Operations Management 事件浏览器。
- 关联通知陷阱
 - BSM Integration Adapter 记录从这些陷阱创建的事件。它们不显示在 BSM Operations Management 事件浏览器中。
 - BSM Integration Adapter 处理 NNMi 关联陷阱以复制 BSM Operations Management 事件浏览器中的 NNMi 事件关联。

自定义策略条件

使用 BSM Integration Adapter 用户界面可以自定义默认策略条件。有关详细信息,请参 阅 HP BSM Integration Adapter 帮助中的*开发 SNMP 拦截器策略 > 配置 SNMP 规则*。

更多信息

有关 HP NNMi 程 P BSM Operations Management 集成的详细信息,请参阅以下参考:

- 有关集成发送到 BSM Integration Adapter 的陷阱类型的描述,请参阅第 508 页的使用 NNMi Northbound Interface。
- 有关 NNMi 发送到 BSM Integration Adapter 的陷阱的格式信息,请参阅 hp-nnmi-nbi.mib 文件。
- 有关使用 HP NNMi—HP BSM Operations Management 集成的详细信息,请参阅 《HP BSM Operations Management 可扩展性指南》。

更改 HP NNMi—HP BSM Operations Management 集成

本部分包含以下主题:

- 第 529 页的更新新 NNMi 陷阱的 SNMP 陷阱策略条件
- 第529页的更改配置参数

更新新 NNMi 陷阱的 SNMP 陷阱策略条件

自配置集成以来,如果已将新 SNMP 陷阱事件配置添加到 NNMi,请遵循以下步骤:

1 在 NNMi 管理服务器上,使用 nnmopcexport.ovpl 命令以创建新陷阱的 SNMP 陷阱 策略文件。

对于 -template 选项,请指定与现有 SNMP 陷阱策略文件的名称不同的名称。

使用-omi policy和-omi hi选项。

可以将文件内容限制为特定作者或 OID 前缀值。有关详细信息,请参阅 nnmopcexport.ovpl 参考页或 UNIX 联机帮助页。

2 使用 BSM Integration Adapter 用户界面可以导入和激活新的头文件和策略文件。

或者,可以为所有 NNMi 管理事件和 SNMP 陷阱重新创建 SNMP 陷阱策略文件。如果采用此方法,请从 BSM Integration Adapter 用户界面删除旧策略。

如果 BSM Integration Adapter 配置对一个 NNMi 事件包含多个策略条件,则会有重复 消息显示在 BSM Operations Management 事件浏览器中。

更改配置参数

要更改集成配置参数,请遵循以下步骤:

- 1 在 NNMi 控制台中,打开 HP NNMi-HPOM 集成选择表单 (集成模块配置 > HPOM)。
- 2 单击 HPOM 代理实施。
- 3 选择目标,然后单击**编辑**。
- 4 对值进行相应修改。

有关此表单上的字段的信息,请参阅第 534 页的 HP NNMi—HPOM 代理目标表单参考(BSM Operations Management 集成)。

5 验证表单顶部的**启用集成**复选框是否已选中,然后单击表单底部的**提交**。 更改会立即生效。

禁用 HP NNMi—HP BSM Operations Management 集成

禁用目标时,不会发生 SNMP 陷阱排队。

要停止将 NNMi 事件转发到 BSM Integration Adapter,请遵循以下步骤:

- 1 在 NNMi 控制台中,打开 HP NNMi-HPOM 集成选择表单 (集成模块配置 > HPOM)。
- 2 单击 HPOM 代理实施。
- 3 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。

4 清除表单顶部的**启用集成**复选框,然后单击表单底部的**提交**。

更改会立即生效。

(可选)如 HP BSM Integration Adapter 帮助中所述,取消激活或删除 SNMP 陷阱策略。

对 HP NNMi—HP BSM Operations Management 集成进行故障 诊断

本部分包含以下主题:

- 第 530 页的 BSM Operations Management 事件浏览器不包含转发的事件
- 第 533 页的 BSM Operations Management 事件浏览器仅包含某些转发的事件

BSM Operations Management 事件浏览器不包含转发的事件



- Windows: < 驱动器 >\Program Files\HP\HP BTO Software\bin
- Linux: /opt/OV/bin

如果 BSM Operations Management 事件浏览器不包含来自 NNMi 的任何事件,则遵循 以下步骤:

- 1 在 NNMi 管理服务器上,验证代理配置:
 - Windows NNMi 管理服务器:

%OVBIN%\ovconfget eaagt

• *Linux* NNMi 管理服务器:

\$OVBIN/ovconfget eaagt

命令输出应包含以下信息:

• Windows:

SNMP_SESSION_MODE=NNM_LIBS SNMP TRAP PORT=<自定义端口>

• Linux:

SNMP_SESSION_MODE=NO_TRAPD SNMP TRAP PORT=<自定义端口>

< *自定义端口*> 的值不应是 162,而应当与 HP NNMi–HPOM 代理目标表单上的端口字段的值相匹配。

- 2 通过考虑步骤1的结果,评估代理配置:
 - 如果代理配置是您所预期的,则继续执行此过程的步骤3。
 - 如果 SNMP_SESSION_MODE 参数设置不正确,则重复执行第 525 页的步骤 4,直到 ovconfget 命令返回预期结果。
 - 如果 < 自定义端口> 的值是 162 或者与 HP NNMi-HPOM 代理目标表单上的端口字段的值不匹配,请相应地重复执行第 524 页的步骤 3 到第 525 页的步骤 5,直到 ovconfget 命令返回预期结果。
- 3 在 NNMi 管理服务器上,验证代理是否正在运行:
 - Windows NNMi 管理服务器:

%OVBIN%\opcagt -Status

• *Linux* NNMi 管理服务器:

\$OVBIN/opcagt -status

命令输出应当包含与以下示例类似的 opctrapi 条目:

opctrapi OVO SNMP Trap Interceptor AGENT, EA (4971) Running 如果输出不是预期结果,则重新启动代理:

ovc -restart opctrapi

- 4 在 NNMi 管理服务器上,验证代理是否正在预期的 SNMP 陷阱端口上侦听:
 - a 运行以下命令:
 - Windows: netstat -an | findstr <自定义端口>
 - Linux: netstat -an | grep <自定义端口>

其中 < 自定义端口 > 是此过程的步骤 1 中 SNMP TRAP PORT 的值。

b 验证输出是否包含状态 LISTENING 或 LISTEN。

如果输出不是预期结果,则重新启动代理:

```
ovc -restart opctrapi
```

- 5 在 NNMi 管理服务器上,验证 NNMi 的 SNMP 陷阱策略文件是否已部署到 NNMi 管理服务器上的 BSM Integration Adapter:
 - Windows NNMi 管理服务器:

%OVBIN%\ovpolicy -list

• *Linux* NNMi 管理服务器:

\$OVBIN/ovpolicy -list

命令输出应当包含与以下示例类似的条目:

Туре	Name	Status	Version
			0001 0000
trapi	"NNMI Management Events"	enabled	0001.0000
Name 字段	的值是第523页的步骤1中通过带	帯-template	选项的
nnmopces	xport.ovpl 创建的 SNMP 陷阱贫	策略文件的名称	К.

- 6 验证 BSM Integration Adapter 是否正在接收陷阱:
 - a 验证 BSM Integration Adapter 是否可以将事件发送到 BSM Operations Management 事件浏览器。
 - b 启用对 BSM Integration Adapter 的跟踪,以确定陷阱是否到达 BSM Integration Adapter。
- 7 验证 NNMi 是否正在将管理事件转发到 BSM Integration Adapter。

有关信息,请参阅第 512 页的对 NNMi Northbound Interface 进行故障诊断。

BSM Operations Management 事件浏览器仅包含某些转发的事件

如果一个或多个 NNMi 事件未显示在 BSM Operations Management 事件浏览器中,则 遵循以下步骤:

- 1 在 NNMi 管理服务器上,验证 SNMP 陷阱策略是否未抑制陷阱。
- 2 在 BSM 服务器上,验证 BSM Operations Management 是否正在运行。

如果 BSM 服务器关闭,则 BSM Integration Adapter 将接收到的陷阱进行排队。 BSM Operations Management 事件浏览器变为可用时, BSM Integration Adapter 会转发排队的陷阱。

如果 BSM Integration Adapter 关闭,则转发的陷阱将丢失。NNMi不重新发送陷阱。

3 在 NNMi 管理服务器上,验证 NNMi 进程是否正在运行:

ovstatus -c

发送到处于关闭状态的 NNMi 的任何陷阱都将丢失。

HP NNMi—HPOM 代理目标表单参考 (BSM Operations Management 集成)

HP NNMi-HPOM 代理目标表单包含用于配置 NNMi 和 BSM Integration Adapter 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-HPOM 集成选择表单上,单击 HPOM 代理实施。单击新建,或选择目标,然后单击编辑。)



只有具有管理员角色的 NNMi 用户才可访问 HP NNMi—HPOM 代理目标表单。

HP NNMi-HPOM 代理目标表单采集以下方面的信息:

- 第 534 页的 BSM Integration Adapter 连接
- 第 535 页的 BSM Operations Management 集成内容
- 第 537 页的 BSM Integration Adapter 目标状态信息

要应用集成配置更改,请更新 HP NNMi-HPOM 代理目标表单上的值,然后单击提交。

BSM Integration Adapter 连接

表 58 列出用于配置 BSM Integration Adapter 连接的参数。

表 58 BSM Integration Adapter 连接信息

字段	描述
主机	NNMi 管理服务器的完全限定域名(首选)或 IP 地址,此管理服务器是 BSM Integration Adapter 接收来自 NNMi 的 SNMP 陷阱的系统。
	集成支持用以下方法标识 BSM Integration Adapter 主机:
	 NNMi FQDN NNMi 管理与 NNMi 管理服务器上的 BSM Integration Adapter 的连接,并且主机 字段变成只读的。 这是默认和建议的配置。
	• 使用环回 不使用此选项。
	• 其他 不使用此选项。
	注:如果 NNMi 管理服务器参与 NNMi 应用程序故障切换,请参阅第 513 页的应用程序 故障切换和 NNMi Northbound Interface,以了解有关应用程序故障切换对集成模块的 影响的信息。

表 58 BSM Integration Adapter 连接信息 (续)

字段	描述
端口	BSM Integration Adapter 接收 SNMP 陷阱的 UDP 端口。 输入特定于 BSM Integration Adapter 的端口号。此值是在第 524 页的步骤 3 中识别的端口。 要确定端口,请在 NNMi 管理服务器上运行 ovconfget eaagt 命令。陷阱端口是 SNMP_TRAP_PORT 变量的值。 注:此端口号必须不同于 NNMi 接收 SNMP 陷阱的端口,它是在 NNMi 控制台上的通 信配置表单的 SNMP 端口字段中设置的。
共用字符串	BSM Integration Adapter 用于接收陷阱的只读共用字符串。 对于 HP NNMi—HP BSM Operations Management 集成,使用默认值 public。

BSM Operations Management 集成内容

表 59 列出用于配置 NNMi 将哪些内容发送到 BSM Integration Adapter 的参数。

Kee Doni operations management XXX 11 ha	ement 集成内容配置信息	Managem	Operations	BSM	表 59
--	----------------	---------	-------------------	-----	------

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 BSM Integration Adapter。
	• 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 BSM Integration Adapter。
	 两者 NNMi 将 NNMi 生成的管理事件和 NNMi 从被管设备接收到的 SNMP 陷阱一并转 发到 BSM Integration Adapter。 这是默认配置。
	一旦启用目标, NNMi 就开始转发事件。
	有关详细信息,请参阅第 508 页的事件转发。

表 59 BSM Operations Management 集成内容配置信息(续)

字段	描述
生命周期状态更改	 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态的每个事件,NNMi会将"事件已关闭"陷阱发送到 BSM Integration Adapter。 这是默认配置。 状态已更改 对于生命周期状态更改为进行中、已完成或已关闭的每个事件,NNMi会将"事件生 命周期状态已更改"陷阱发送到 BSM Integration Adapter。
	 两者 对于更改为已关闭生命周期状态的每个事件,NNMi会将"事件已关闭"陷阱发送到BSM Integration Adapter。另外,对于生命周期状态更改为进行中、已完成或已关闭的每个事件,集成会将"事件生命周期状态已更改"陷阱发送到BSM Integration Adapter。 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改"陷阱。 有关详细信息,请参阅第 509 页的事件生命周期状态更改通知。
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 BSM Integration Adapter。 这是默认配置。 单个 NNMi 为从 NNMi 原因分析产生的每个父子事件关联关系发送陷阱。 组 NNMi 对于列出关联到父事件的所有子事件的每个关联发送一个陷阱。 有关详细信息,请参阅第 509 页的事件关联通知。
删除	 事件删除规范。 不发送 从 NNMi 中删除事件时, NNMi 不会通知 BSM Integration Adapter。 这是默认配置。 发送 对于 NNMi 中删除的每个事件, NNMi 会向 BSM Integration Adapter 发送一个删 除陷阱。 有关详细信息,请参阅第 510 页的事件删除通知。
NNMi 控制台访问	URL 中的连接协议规范,用于从 BSM Operations Management 事件浏览器浏览到 NNMi 控制台。 NNMi 发送到 BSM Integration Adapter 的陷阱在 NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2) 中包含此 NNMi URL。 集成需要与 NNMi 控制台进行 HTTP 连接。选择 HTTP 选项。

表 59 BSM Operations Management 集成内容配置信息 (续)

字段	描述	
事件过滤器	对象标识符 (OID) 的列表,集成据此过滤发送到 BSM Integration Adapter 的事件。每 个过滤器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 将所有事件发送到 BSM Integration Adapter。 这是默认配置。 	
	• 包含 NNMi 仅发送与过滤器中识别出的 OID 相匹配的特定事件。	
	 排除 NNMi 发送所有事件,不包括与过滤器中识别出的 OID 相匹配的特定事件。 指定事件过滤器: 要添加过滤器条目,请在下部的文本框中输入文本,然后单击添加。 要删除过滤器条目,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,请参阅第 510 页的事件转发过滤器。 	

BSM Integration Adapter 目标状态信息

表 60 列出 BSM Integration Adapter 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。

表 60 BSM Integration Adapter 目标状态信息

字段	描述
陷阱目标 IP 地址	BSM Integration Adapter 目标主机名解析而得的 IP 地址。 此值对于此目标唯一。
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 BSM Integration Adapter 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 Interface 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 BSM Integration Adapter 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。

HP Operations Manager



HP Operations Manager (HPOM) 提供全面事件管理、主动性能监视及自动警报、报告和制图,用于管理操作系统、中间件和应用程序基础结构。 HPOM 能够将来源广泛的事件整合到单个视图中。

有关购买 HPOM 的信息,请联系 HP 销售代表。

本章描述以下可用集成:

- HP NNMi—HPOM 集成 (代理实施)
- HP NNMi—HPOM 集成 (Web 服务实施)

HP NNMi-HPOM 集成 (代理实施)

HP NNMi—HPOM 集成的代理实施是 HPOM 与 NNMi 集成的首选解决方案。

如果 HP NNMi—HPOM 集成的代理实施和 Web 服务实施都将消息转发到相同 HPOM 管理服务器,则您在 HPOM 活动消息浏览器中可能看不到这两种实施的所有消息。由于这个 原因, HP 不支持从某一个 NNMi 管理服务器到同一 HPOM 管理服务器并发运行 HP NNMi—HPOM 集成的这两种实施。

本部分包含以下主题:

- 第 540 页的关于 HP NNMi-HPOM 集成 (代理实施)
- 第 541 页的启用 HP NNMi-HPOM 集成 (代理实施)
- 第 546 页的使用 HP NNMi-HPOM 集成 (代理实施)
- 第 548 页的更改 HP NNMi-HPOM 集成配置 (代理实施)
- 第 549 页的禁用 HP NNMi-HPOM 集成 (代理实施)

- 第 550 页的对 HP NNMi-HPOM 集成 (代理实施)进行故障诊断
- 第 553 页的 HP NNMi-HPOM 代理目标表单参考 (代理实施)

关于 HP NNMi-HPOM 集成 (代理实施)

HP NNMi-HPOM 集成的代理实施将 NNMi 管理事件作为 SNMPv2c 陷阱转发到 NNMi 管理服务器上的 HP Operations Agent。代理将过滤 NNMi 陷阱,并且将它们转发到 HPOM 活动消息浏览器。代理配置确定哪个 HPOM 管理服务器将接收转发事件。

HP NNMi-HPOM 集成还可以将 NNMi 接收的 SNMP 陷阱转发到代理。集成不会将 NNM 6.x 或 7.x 管理工作站生成的事件转发到代理。

HP NNMi-HPOM 集成还实现了从 HPOM 内部访问 NNMi 控制台。

HP NNMi-HPOM 集成的代理实施是 NNMi Northbound Interface 的特定实施,如第 505 页的 NNMi Northbound Interface 中所述。

HP NNMi-HPOM 集成的代理实施由以下组件组成:

- nnmi-hpom 代理集成模块
- nnmopcexport.ovpl 工具

价值

HP NNMi 脑 POM 集成在 HPOM 活动消息浏览器中提供关于网络管理、系统管理和应用 程序管理方面的事件合并,这样 HPOM 用户就可以检测和调查潜在的网络问题。

集成的主要功能如下:

- 从 NNMi 转发到 HP Operations Agent 的自动事件。转发的事件显示在 HPOM 活动 消息浏览器中。
- 从 HPOM 访问到 NNMi 控制台。
 - HPOM 用户可以在所选消息的上下文中打开 NNMi 事件表单。
 - HPOM 用户可以在所选消息和节点的上下文中启动 NNMi 视图(例如,第2层邻 居视图)。
 - HPOM 用户可以在所选消息和节点的上下文中启动 NNMi 工具 (例如,状态 轮询)。
集成产品

本部分中的信息适用于以下产品:

- HPOM for Windows (也称为 OMW)
- HPOM for UNIX (也称为 OMU)
- HPOM for Linux (也称为 OML)

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

• NNMi 9.10

NNMi和 HPOM 必须安装在不同的计算机上。NNMi管理服务器和 HPOM 管理服务器计算机可以使用相同或不同的操作系统。

HP Operations Agent 需要许可证,并且必须在安装 NNMi *之后* 安装在 NNMi 管理服务 器计算机上。

有关受支持的硬件平台和操作系统的最新信息,请参阅所有产品的支持列表。

文档

本章描述如何配置 NNMi 以与 HPOM 通信。

HPOM 文档描述如何安装和使用从 HPOM 活动消息浏览器访问 NNMi 控制台的 HPOM 应用程序。

- 有关 HPOM for Windows,请参阅 HPOM 帮助中关于 HP NNMi Adapter 的信息。
- 有关 HPOM for UNIX 版本 9.xx,请参阅《HP Operations Manager for UNIX 管理 员参考》中的将NNMi 集成到HPOM 部分。
- 有关 HPOM for UNIX 版本 8.3x,请参阅《HP NNMi—HPOM Integration for HP Operations Manager 用户指南》。
- 有关 HPOM for Linux,请参阅《HP Operations Manager for Linux 管理员参考》 中的*将 NNMi 集成到 HPOM* 部分。

启用 HP NNMi-HPOM 集成 (代理实施)

建议让有经验的 HPOM 管理员完成启用 HP NNMi 脑 POM 集成的代理实施的过程。

NNMi 与 HP Business Service Management (BSM) 拓扑数据库集成时, HP NNMi— HPOM 集成的代理实施可以将关于 NNMi 所管理设备的事件与 BSM 配置项 (CI) 相关 联。标准 NNMi Northbound Interface 未提供此信息。有关详细信息,请参阅第 546 页 的配置项标识符。 要启用 HP NNMi-HPOM 集成的代理实施,请遵循以下步骤:

- 1 在 NNMi 管理服务器上,生成 SNMP 陷阱策略文件:
 - a 验证 NNMi 服务是否正在运行:

```
ovstatus -c
```

所有 NNMi 服务应当显示状态正在运行。

b 通过输入以下命令, 生成 SNMP 陷阱策略文件:

```
nnmopcexport.ovpl -u <用户名> -p <密码> \
-template "NNMi Management Events" -application "NNMi" \
-file NNMi_policy.dat
```

<用户名>和<密码>的值对应于具有管理员角色的 NNMi 控制台用户。

如果 HPOM 将 NNMi 事件转发到 HP OMi 事件浏览器或 BSM Operations Management 事件浏览器,还请使用 -omi_hi 选项将运行状况指示器添加到管理 事件策略条件。有关详细信息,请参阅第 546 页的运行状况指示器。

SNMP 陷阱策略文件将每个管理事件和 SNMP 陷阱配置的策略条件包含到当前 NNMi 事件配置中。有关自定义此命令的输出的信息,请参阅 nnmopcexport.ovpl 参考页或 UNIX 联机帮助页。

有关默认策略条件和自定义条件的信息,请参阅第 546 页的使用 HP NNMi-HPOM 集成(代理实施)。

- 2 在 HPOM 管理服务器上, 配置 HPOM 以从 NNMi 接收消息:
 - a 在 HPOM 控制台中,添加 NNMi 管理服务器的节点。
 - b 在 NNMi 管理服务器上安装 HP Operations Agent。
 - c 将在此过程的步骤 1 中创建的 NNMi_policy.dat 文件从 NNMi 管理服务器传输 到 HPOM 管理服务器。
 - d 将 NNMi policy.dat 文件导入到 HPOM 中。
 - HPOM for Windows: 使用 ImportPolicies 命令。
 - HPOM for UNIX 版本 9.x: 使用 opcpolicy 命令。
 - HPOM for UNIX 版本 8.x: 使用 opctempl 命令。
 - HPOM for Linux: 使用 opcpolicy 命令。
 - e 将 NNMi 管理事件策略部署到 NNMi 被管节点。
 - f 在 HPOM 控制台中,添加外部节点以捕获所有转发的 NNMi 事件。
 - 对于初始测试,将节点过滤器设置为 <*>.<*>.<*>(对于 IP 过滤器)或 <*> (对于名称过滤器)。在验证集成之后,限制外部节点过滤器以匹配网络。



如果不为 NNMi 事件源节点设置 HPOM 被管节点,则 HPOM 管理服务器丢弃关于该节点的所有事件。

有关详细信息,请参阅以下参考:

- HPOM for Windows:
 - HPOM 帮助中的 导入 OVO for UNIX 模板
 - HPOM 帮助中的配置外部节点
- *HPOM for UNIX*:
 - 《HP Operations Manager for UNIX HTTPS Agent 概念和配置指南》
 - 《HP Operations Manager for UNIX 概念指南》
 - 《HP Operations Manager for UNIX 管理员参考》
 - 《HP Operations Manager for UNIX 开发人员工具包开发人员参考》
 - opcnode(1M)、opcbbcdist(1M)、opcragt(1M)、opccfgupl(1M)、opcpolicy(1M)(版本 9.xx)和 opctempl(1M)(版本 8.3x)联机帮助页
- HPOM for Linux:
 - 《HP Operations Manager for Linux HTTPS Agent 概念和配置指南》
 - 《HP Operations Manager for Linux 概念指南》
 - 《HP Operations Manager for Linux 管理员参考》
 - 《HP Operations Manager for Linux 开发人员工具包开发人员参考》
 - opcnode(1M)、opcbbcdist(1M)、opcragt(1M)、opccfgupl(1M)和
 opcpolicy(1M) 联机帮助页
- 3 识别可用于 NNMi 和 HP Operations Agent 之间的 SNMP 通信的端口。

HP Operations Agent 将在此端口上侦听 NNMi 转发到此端口的 SNMP 陷阱。启用 集成时,此过程的步骤 4 (对于 HP Operations Agent)和步骤 5 (对于 NNMi)中都使用此端口号。

因为 HP Operations Agent 安装在 NNMi 管理服务器上,所以此端口号必须与 NNMi 接收 SNMP 陷阱的端口不同。

- a 在 NNMi 控制台中,从配置工作区打开通信配置表单。
- b 在默认 SNMP 设置区域中,记下 SNMP 端口的值。
- c 选择与**通信配置**表单上的值不同的端口。较好的做法是使用与 162 类似的端口号, 162 是用于接收 SNMP 陷阱的标准 UDP 端口。例如,如果端口 162 不可用,则 试用端口 5162。
- d 在 NNMi 管理服务器上,运行命令 netstat -a,然后在输出中搜索在步骤 c 中选择的端口。如果该端口号未出现在输出中,则它可能对 HP Operations Agent 是可用的。

- 4 在 NNMi 管理服务器上,通过输入以下命令,对 HP Operations Agent 配置用于从 NNMi 接收 SNMP 陷阱的自定义端口:
 - Windows NNMi 管理服务器:
 - 配置代理:

ovconfchg -ns eaagt -set SNMP_TRAP_PORT <自定义端口> \ -set SNMP_SESSION_MODE NNM_LIBS

— 重新启动代理:

ovc -restart opctrapi

- UNIX NNMi 管理服务器:
 - 配置代理:

ovconfchg -ns eaagt -set SNMP_TRAP_PORT *<自定义端口>* \ -set SNMP_SESSION_MODE NO_TRAPD

— 重新启动代理:

ovc -restart opctrapi

对于<自定义端口>,使用在此过程的步骤3中识别的端口。

- 5 在 NNMi 管理服务器上, 配置转发到 HP Operations Agent 的 NNMi 事件:
 - a 在 NNMi 控制台中, 打开 HP NNMi-HPOM 集成选择表单(集成模块配置 > HPOM)。
 - b 单击 HPOM 代理实施,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。)

- c 在 HP NNMi-HPOM 代理目标表单上,选中已启用复选框以激活表单上的其余字段。
- d 输入用于连接到 NNMi 管理服务器上的 HP Operations Agent 的信息。陷阱目标 端口是在此过程的步骤 3 中识别的端口。

有关这些字段的信息,请参阅第 553 页的 HP Operations Agent 连接。

- e 指定发送选项。对于 NNMi 控制台访问字段,选择 HTTP 选项。 有关这些字段的信息,请参阅第 554 页的 HPOM 集成内容。
- f 单击表单底部的提交。

将会出现新窗口,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。 2011年3月

- 6 *可选*。在 HPOM 中,将 NNMi 事件的自定义消息属性添加到活动消息浏览器。遵循相 应的步骤:
 - HPOM for Windows:
 - 在浏览器中,右键单击任何列标题,然后单击选项。
 - 在**输入自定义消息属性**列表中,选择属性,然后单击**添加**。
 - HPOM for UNIX 或 HPOM for Linux:
 - 在 Java GUI 消息浏览器中,右键单击任何列标题,然后单击自定义消息浏览器列。
 - 在自定义选项卡上,从可用自定义消息属性中进行选择,然后单击确定。

```
注意以下信息:
```

- NNMi 事件的大多数自定义消息属性以文本 nnm 开头。
- 对于 HP NNMi-HPOM 集成的代理实施, NNMi 事件最具相关性的属性如下:

```
nnm.name
```

```
nnm.server.name
```

有关其他相关的 CMA 的信息,请参阅第 546 页的使用 HP NNMi-HPOM 集成 (代理实施)。

- 要更改自定义消息属性出现在消息浏览器中的顺序,请将列标题拖到新位置。
- 7 可选。在 HPOM 管理服务器上, 启用 NNMi 视图的根据上下文启动功能。
 - *HPOM for Windows*:将 NNMi 源节点与 HP NNMi Web 工具组关联。 有关信息,请参阅 HPOM 帮助中的*启用"按节点"工具组中的工具*。
 - HPOM for UNIX: 安装这组基本的 NNMi 应用程序,还可以选择安装其他 NNMi 应用程序。

HPOM 版本 9.00 或更高版本将自动安装基本 NNMi 应用程序。

有关信息,请参阅《HP Operations Manager for UNIX 管理员参考》(版本 9.xx) 或《HP NNMi—HPOM Integration for HP Operations Manager 用户指南》(版 本 8.3x)中关于安装和配置 HP NNMi—HPOM 集成的部分。

• *HPOM for Linux*: HPOM 自动安装基本 NNMi 应用程序。可选择安装其他 NNMi 应用程序。

有关信息,请参阅《HP Operations Manager for Linux 管理员参考》中关于安装和配置 HP NNMi-HPOM 集成的部分。

使用 HP NNMi-HPOM 集成 (代理实施)

HP NNMi-HPOM 集成的代理实施提供 NNMi 管理事件和 SNMP 陷阱到 HP Operations Agent 的单向传送。SNMP 陷阱策略条件确定 HPOM 如何处理和显示传入陷阱。例如,可以更改策略条件以在消息文本中包括陷阱自定义消息属性 (CMA) 的值。

NNMi 仅将每个管理事件或 SNMP 陷阱的一个副本发送到 HP Operations Agent。此行 为不同于 NNM 6.x/7.x 与 HPOM 集成的行为。

在 HPOM 活动消息浏览器中查看转发的 NNMi 事件。HPOM 菜单命令用于在所选消息的 上下文中访问 NNMi 视图。嵌入到每个消息中的信息支持此交叉导航:

- 消息中的 nnmi.server.name 和 nnmi.server.port CMA 标识 NNMi 管理服务器。
- nnmi.incident.uuid CMA 标识 NNMi 数据库中的事件。

原始陷阱源显示在 HPOM 活动消息浏览器的对象列中以及 nnm.source.name CMA 中。 (在 HP NNMi-HPOM 集成的 Web 服务实施中,原始陷阱源仅显示在 nnm.source.name CMA 中。)

配置项标识符

在 HP Business Service Management (BSM) 和 HP Universal CMDB 软件 (UCMDB) 中,配置项 (CI) 是 IT 环境中的组件的数据库表示。 CI 可以是某种业务、业务流程、应用 程序、服务器硬件或服务。

NNMi 与 BSM 拓扑数据库或 UCMDB 集成时, NNMi 与 BSM 或 UCMDB 共享 NNMi 所管理设备的 CI 信息。在这种情况下, HP NNMi-HPOM 集成的代理实施可以将关于 NNMi 所管理设备的事件与 BSM 或 UCMDB CI 关联。SNMP 陷阱策略条件启用此关联。

有关与 BSM 和 UCMDB 集成的信息,请参阅:

- 第 423 页的 HP Business Service Management 拓扑
- 第 433 页的 HP Universal CMDB

运行状况指示器

如果 NNMi SNMP 陷阱策略文件是使用带 -omi_hi 选项的 nnmopcexport.ovpl 创建的,则该策略文件会在适用时将运行状况指示器与 SNMP 陷阱策略文件中的每个标准 NNMi 管理事件相关联。(并非所有管理事件类型都有运行状况指示器。)运行状况指示器 是在 EtiHint CMA 中提供的。

有关特定的运行状况指示器,请参阅 SNMP 陷阱策略文件。

默认策略条件

默认集成行为将根据集成内容而有所不同,如下所述:

- NNMi "管理事件"事件
 - NNMi SNMP 陷阱策略文件包含在生成文件时 NNMi 事件配置中定义的所有 NNMi 管理事件配置的条件。
 - 从 NNMi 管理事件创建的消息显示在 HPOM 活动消息浏览器中。
 - 这些陷阱包含第 546 页的配置项标识符中所述的 CI 信息。
 - 从这些陷阱创建的消息可能包含第 546 页的运行状况指示器中所述的运行状况指示器。
- 第三方 SNMP 陷阱
 - NNMi SNMP 陷阱策略文件包含在生成文件时 NNMi 事件配置中定义的所有 SNMP 陷阱配置的条件。
 - 从第三方陷阱创建的消息显示在 HPOM 活动消息浏览器中。
 - 这些陷阱包含第 546 页的配置项标识符中所述的 CI 信息。
 - 从这些陷阱创建的消息不包含运行状况指示器。
 - 如果将集成配置为转发所有接收的 SNMP 陷阱,并且 HPOM 管理服务器直接从 NNMi 管理的设备接收 SNMP 陷阱,则 HPOM 接收重复设备陷阱。可以设置策略 以将来自 NNMi 的 SNMP 陷阱与 HPOM 直接从所管理设备接收的那些陷阱关联。
- EventLifecycleStateClosed 陷阱
 - HP Operations Agent 记录从这些陷阱创建的消息。通常,它们不显示在 HPOM 活动消息浏览器中。
 - NNMi SNMP 陷阱策略文件使得 HP Operations Agent 确认与 HPOM 活动消息浏览器中的已关闭 NNMi 事件相对应的消息。
- LifecycleStateChangeEvent 陷阱
 - NNMi SNMP 陷阱策略文件不包含有关处理这些陷阱的条件。HP Operations agent 不将这些陷阱转发到 HPOM 活动消息浏览器。
- EventDeleted 陷阱
 - NNMi SNMP 陷阱策略文件不包含有关处理这些陷阱的条件。HP Operations agent 不将这些陷阱转发到 HPOM 活动消息浏览器。

- 关联通知陷阱
 - HP Operations Agent 记录从这些陷阱创建的消息。它们不显示在 HPOM 活动消息浏览器中。
 - 这些陷阱对于 HPOM 活动消息浏览器没有影响。

自定义策略条件

要自定义默认策略条件,请在 HPOM 管理服务器上编辑条件,然后将策略重新部署到 NNMi 管理服务器上的 HP Operations Agent。有关详细信息,请参阅以下参考:

- *HPOM for Windows*: HPOM 帮助中的 *SNMP 拦截器策略*(版本 9.0x)或*策略开发*(版本 8.1x)
- HPOM for UNIX: 《HP Operations Manager for UNIX 概念指南》
- HPOM for Linux: 《HP Operations Manager for Linux 概念指南》

更多信息

有关 HP NNMi 朒 POM 集成的代理实施的详细信息,请参阅以下参考:

- 关于集成发送到 HP Operations Agent 的陷阱类型的描述,请参阅第 508 页的使用 NNMi Northbound Interface。
- 有关 NNMi 发送到 HP Operations Agent 的陷阱的格式信息,请参阅 hp-nnmi-nbi.mib 文件。
- 有关使用 HP NNMi-HPOM 集成的详细信息,请参阅 HPOM 文档。
 - HPOM for Windows: 请参阅 HPOM 帮助中的 NNMi Adapter 的代理实施。
 - HPOM for UNIX: 请参阅《HP Operations Manager for UNIX 管理员参考》(版本 9.xx)或《HP NNMi—HPOM Integration for HP Operations Manager 用户 指南》(版本 8.3x)中有关安装和配置 HP NNMi–HPOM 集成的部分。
 - HPOM for Linux: 请参阅《HP Operations Manager for Linux 管理员参考》中 关于安装和配置 HP NNMi-HPOM 集成的部分。

更改 HP NNMi-HPOM 集成配置 (代理实施)

更新新 NNMi 陷阱的 SNMP 陷阱策略条件

自配置集成以来,如果已将新 SNMP 陷阱事件配置添加到 NNMi,请遵循以下步骤:

1 在 NNMi 管理服务器上,使用 nnmopcexport.ovpl 命令以创建新陷阱的 SNMP 陷阱 策略文件。

对于 -template 选项,请指定与现有 SNMP 陷阱策略文件的名称不同的名称。

可以将文件内容限制为特定作者或 OID 前缀值。有关详细信息,请参阅 nnmopcexport.ovpl 参考页或 UNIX 联机帮助页。

- 2 将新 SNMP 陷阱策略文件从 NNMi 管理服务器传输到 HPOM 管理服务器, 然后导入 到 HPOM 中。
- 3 在 HPOM 管理服务器上,将新策略部署到 NNMi 被管节点。

或者,可以为所有 NNMi 管理事件和 SNMP 陷阱重新创建 SNMP 陷阱策略文件。如果采取此方法,则将新策略文件导入到 HPOM 中会覆盖任何现有策略自定义。

更改配置参数

要更改集成配置参数,请遵循以下步骤:

- 1 在 NNMi 控制台中,打开 HP NNMi-HPOM 集成选择表单 (集成模块配置 > HPOM)。
- 2 单击 HPOM 代理实施。
- 3 选择目标,然后单击**编辑**。
- 4 对值进行相应修改。

有关此表单上的字段的信息,请参阅第 553 页的 HP NNMi-HPOM 代理目标表单参考 (代理实施)。

5 验证表单顶部的**启用集成**复选框是否已选中,然后单击表单底部的**提交**。 更改会立即生效。

禁用 HP NNMi-HPOM 集成 (代理实施)

禁用目标时,不会发生 SNMP 陷阱排队。

要停止将 NNMi 事件转发到 HP Operations Agent,请遵循以下步骤:

- 1 在 NNMi 控制台中,打开 HP NNMi-HPOM 集成选择表单 (集成模块配置 > HPOM)。
- 2 单击 HPOM 代理实施。
- 3 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。

- 4 清除表单顶部的启用集成复选框,然后单击表单底部的提交。 更改会立即生效。
- (可选)如 HPOM 文档中所述,取消激活或删除 SNMP 陷阱策略。

对 HP NNMi-HPOM 集成 (代理实施)进行故障诊断

HPOM 活动消息浏览器不接收任何转发事件

在以下过程中,对于 HP Operations Agent 命令, OVBIN 环境变量引用 bin 目录,该目录 默认为以下值:

- Windows: <驱动器>\Program Files\HP\HP BTO Software\bin
- UNIX: /opt/OV/bin

如果 HPOM 活动消息浏览器不包含来自 NNMi 的任何事件,则遵循以下步骤:

- 1 在 NNMi 管理服务器上,验证 HP Operations Agent 配置:
 - Windows NNMi 管理服务器:

%OVBIN%\ovconfget eaagt

• UNIX NNMi 管理服务器:

\$OVBIN/ovconfget eaagt

命令输出应包含以下信息:

- Windows: SNMP_SESSION_MODE=NNM_LIBS
- UNIX: SNMP_SESSION_MODE=NO_TRAPD
- SNMP TRAP PORT=<自定义端口>

<自定义端口>的值不应是162,而应当与 HP NNMi-HPOM 代理目标表单上的端口字段的值相匹配。

- 2 通过考虑步骤 1 的结果, 评估 HP Operations Agent 配置:
 - 如果 HP Operations Agent 配置是您所预期的,则继续执行此过程的步骤 3。
 - 如果 SNMP_SESSION_MODE 参数设置不正确,则重复执行第 544 页的步骤 4,直到 ovconfget 命令返回预期结果。
 - 如果 < *自定义端□*> 的值是 162 或者与 HP NNMi-HPOM 代理目标表单上的端口字段 的值不匹配,请相应地重复执行第 543 页的步骤 3 到第 544 页的步骤 5,直到 ovconfget 命令返回预期结果。
- 3 在 NNMi 管理服务器上,验证 HP Operations Agent 是否正在运行:
 - Windows NNMi 管理服务器:

%OVBIN%\opcagt -status

• UNIX NNMi 管理服务器:

\$OVBIN/opcagt -status

命令输出应当包含与以下示例类似的 opctrapi 条目:

opctrapi OVO SNMP Trap Interceptor AGENT, EA (4971) Running

如果输出不是预期结果,则重新启动 HP Operations Agent:

ovc -restart opctrapi

- **4** 在 NNMi 管理服务器上,验证 HP Operations Agent 是否正在预期的 SNMP 陷阱端 口上侦听:
 - a 运行以下命令:
 - Windows: netstat -an | findstr <自定义端口>
 - UNIX: netstat -an | grep <自定义端口>

其中 <自定义端口> 是此过程的步骤 1 中 SNMP TRAP PORT 的值。

b 验证输出是否包含状态 LISTENING 或 LISTEN。

如果输出不是预期结果,则重新启动 HP Operations Agent:

```
ovc -restart opctrapi
```

5 在 HPOM 管理服务器上,验证 NNMi 管理服务器节点的外部节点过滤器。

HPOM 管理服务器必须配置为接受来自 NNMi 管理的设备的事件。如果 NNMi 源节 点未配置为被管节点或者包含在外部节点过滤器中,则 HPOM 将忽略来自该节点的所 有转发事件,如第 542 页的步骤 2 中所述。

- 6 在 NNMi 管理服务器上,验证 NNMi 的 SNMP 陷阱策略文件是否已部署到 NNMi 管 理服务器上的 HP Operations Agent:
 - Windows NNMi 管理服务器:

%OVBIN%\ovpolicy -list

• UNIX NNMi 管理服务器:

\$OVBIN/ovpolicy -list

命令输出应当包含与以下示例类似的条目:

Туре	Name	Status	Version
trapi	"NNMi Management Events"	enabled	0001.0000

Name 字段的值是第 542 页的步骤 1 中通过带 -template 选项的 nnmopcexport.ovpl 创建的 SNMP 陷阱策略文件的名称。

- 7 验证 HP Operations Agent 是否正在接收陷阱:
 - a 验证 HP Operations Agent 是否可以将消息发送到 HPOM 管理服务器。
 - b 启用对 HP Operations Agent 的跟踪以确定陷阱是否到达 HP Operations Agent。

有关对 HP Operations Agent 进行故障诊断的信息,请参阅以下参考:

- HPOM for Windows: HPOM 帮助
- HPOM for UNIX:《HP Operations Manager for UNIX HTTPS Agent 概念和配置指南》
- HPOM for Linux:《HP Operations Manager for Linux HTTPS Agent 概念和配置指南》

8 验证 NNMi 是否正在将管理事件转发到 HP Operations Agent。

有关信息,请参阅第 512 页的对 NNMi Northbound Interface 进行故障诊断。

HPOM 活动消息浏览器不接收某些转发事件

如果一个或多个 NNMi 事件未显示在 HPOM 活动消息浏览器中,则遵循以下步骤:

- 1 在 NNMi 管理服务器上,验证 SNMP 陷阱策略是否未抑制陷阱。
- 2 在 HPOM 管理服务器上,验证 NNMi 管理服务器节点的外部节点过滤器。

HPOM 管理服务器必须配置为接受来自 NNMi 管理的设备的事件。如果 NNMi 源节 点未配置为被管节点或者包含在外部节点过滤器中,则 HPOM 将忽略来自该节点的所 有转发事件,如第 542 页的步骤 2 中所述。

3 在 HPOM 管理服务器上,验证 HPOM 是否正在运行。

如果 HPOM 管理服务器关闭,则 HP Operations Agent 将接收的陷阱进行排队。当 HPOM 管理服务器变为可用时, HP Operations Agent 转发排队的陷阱。

如果 HP Operations Agent 关闭,则转发的陷阱将丢失。 NNMi 不重新发送陷阱。

4 在 NNMi 管理服务器上,验证 NNMi 进程是否正在运行:

ovstatus -c

发送到处于关闭状态的 NNMi 的任何陷阱都将丢失。

HP NNMi-HPOM 代理目标表单参考 (代理实施)

HP NNMi-HPOM 代理目标表单包含用于配置 NNMi 和 HP Operations Agent 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-HPOM 集成选择表单上,单击 HPOM 代理实施。单击新建,或选择目标,然后单击编辑。)



HP NNMi-HPOM 代理目标表单采集以下方面的信息:

- 第 553 页的 HP Operations Agent 连接
- 第 554 页的 HPOM 集成内容
- 第 556 页的 HP Operations Agent 目标状态信息

要应用集成配置更改,请更新 HP NNMi-HPOM 代理目标表单上的值,然后单击提交。

HP Operations Agent 连接

表 61 列出用于配置 HP Operations Agent 连接的参数。

字段	描述
主机	NNMi 管理服务器的完全限定域名(首选)或 IP 地址,此管理服务器是 HP Operations Agent 接收来自 NNMi 的 SNMP 陷阱的系统。
	集成支持用以下方法标识 HP Operations Agent 主机:
	 NNMi FQDN NNMi 管理与 NNMi 管理服务器上的 HP Operations Agent 的连接,并且主机字段 变成只读的。 这是默认和建议的配置。
	• 使用环回 不使用此选项。
	• 其他 不使用此选项。
	注:如果 NNMi 管理服务器参与 NNMi 应用程序故障切换,请参阅第 513 页的应用程序 故障切换和 NNMi Northbound Interface,以了解有关应用程序故障切换对集成模块的 影响的信息。

表 61 HP Operations Agent 连接信息

表 61 HP Operations Agent 连接信息(续)

字段	描述
端口	HP Operations Agent 接收 SNMP 陷阱的 UDP 端口。
	输入特定于 HP Operations Agent 的端口号。此值是在第 543 页的步骤 3 中识别的端口。
	要确定端口,请在 NNMi 管理服务器上运行 ovconfget eaagt 命令。陷阱端口是 SNMP_TRAP_PORT 变量的值。
	注:此端口号必须不同于 NNMi 接收 SNMP 陷阱的端口,它是在 NNMi 控制台上的通信 配置表单的 SNMP 端口字段中设置的。
共用字符串	HP Operations Agent 用于接收陷阱的只读共用字符串。 对于 HP NNMi—HPOM 集成,使用默认值 public。

HPOM 集成内容

表 62 列出用于配置 NNMi 将哪些内容发送到 HP Operations Agent 的参数。

表 62	HPOM	集成内容配置信息
------	------	----------

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 HP Operations Agent。 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 HP Operations Agent。 两者 NNMi 将 NNMi 生成的管理事件和 NNMi 从被管设备接收到的 SNMP 陷阱一并转 发到 HP Operations Agent。 这是默认配置。 一旦启用目标, NNMi 就开始转发事件。
	有关详细信息,请参阅第 508 页的事件转发。

表 62 HPOM 集成内容配置信息(续)

字段	描述
生命周期状态更改	 事件更改通知规范。 增强已关闭 对于每个更改为已关闭生命周期状态的事件,NNMi都将事件关闭陷阱发送到 HP Operations Agent。 这是默认配置。 状态已更改 对于生命周期状态更改为进行中、已完成或已关闭的每个事件,NNMi将"事件生命 周期状态已更改"陷阱发送到 HP Operations Agent。 两者 对于每个更改为已关闭生命周期状态的事件,NNMi都将事件关闭陷阱发送到 HP Operations Agent。对于生命周期状态更改为进行中、已完成或已关闭的每个事 件,集成将"事件生命周期状态已更改"陷阱发送到 HP Operations Agent。 注:在此例中,每次事件更改为已关闭生命周期状态可改"陷阱发送到 HP Operations Agent。 "事件已关闭"陷阱和"事件生命周期状态已更改"陷阱。 有关详细信息,请参阅第 509 页的事件生命周期状态更改通知。
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 HP Operations Agent。这是默认配置。 单个 NNMi 为从 NNMi 原因分析产生的每个父子事件关联关系发送陷阱。 组 NNMi 对于列出关联到父事件的所有子事件的每个关联发送一个陷阱。 有关详细信息,请参阅第 509 页的事件关联通知。
删除	 事件删除规范。 不发送 从 NNMi 中删除事件时, NNMi 不会通知 HP Operations Agent。 这是默认配置。 发送 对于 NNMi 中删除的每个事件, NNMi 会向 HP Operations Agent 发送一个删除陷阱。 有关详细信息,请参阅第 510 页的事件删除通知。
NNMi 控制台访问	URL 中的连接协议规范,用于从 HPOM 消息浏览器浏览到 NNMi 控制台。NNMi 发送 到 HP Operations Agent 的陷阱在 NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2) 中包 含此 NNMi URL。 集成需要与 NNMi 控制台进行 HTTP 连接。选择 HTTP 选项。

表 62 HPOM 集成内容配置信息(续)

描述
对象标识符 (OID) 的列表, 集成根据这些 OID 对发送到 HP Operations Agent 的事件进行过滤。每个过滤器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 将所有事件发送到 HP Operations Agent。 这是默认配置。
• 包含 NNMi 仅发送与过滤器中识别出的 OID 相匹配的特定事件。
• 排除 NNMi 发送所有事件,不包括与过滤器中识别出的 OID 相匹配的特定事件。
指定事件过滤器: ● 更添加过滤器条用 请左下郊的立木框由绘λ立木 然后的丰 添加
 要刪除过滤器条目,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,请参阅第 510 页的事件转发过滤器。

HP Operations Agent 目标状态信息

表 63 列出 HP Operations Agent 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。

表 63 HP Operations Agent 目标状态信息

字段	描述
陷阱目标 IP 地址	HP Operations Agent 目标主机名解析而得的 IP 地址。 此值对于此 HP Operations Agent 目标是唯一的。
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 HP Operations Agent 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 Interface 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 HP Operations Agent 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。

HP NNMi—HPOM 集成 (Web 服务实施)

HP NNMi—HPOM 集成的代理实施是 HPOM 与 NNMi 集成的首选解决方案。

如果 HP NNMi—HPOM 集成的代理实施和 Web 服务实施都将消息转发到相同 HPOM 管理服务器,则您在 HPOM 活动消息浏览器中可能看不到这两种实施的所有消息。由于这个原因, HP 不支持从某一个 NNMi 管理服务器到同一 HPOM 管理服务器并发运行 HP NNMi—HPOM 集成的这两种实施。

本部分包含以下主题:

- 第 557 页的关于 HP NNMi-HPOM 集成 (Web 服务实施)
- 第 559 页的启用 HP NNMi-HPOM 集成 (Web 服务实施)
- 第 563 页的使用 HP NNMi-HPOM 集成 (Web 服务实施)
- 第 564 页的更改 HP NNMi-HPOM 集成配置 (Web 服务实施)
- 第 565 页的禁用 HP NNMi-HPOM 集成 (Web 服务实施)
- 第 565 页的对 HP NNMi-HPOM 集成 (Web 服务实施)进行故障诊断
- 第 570 页的 HP NNMi-HPOM Web 服务集成配置表单参考

关于 HP NNMi-HPOM 集成 (Web 服务实施)

HP NNMi-HPOM 集成的 Web 服务实施将 NNMi 事件转发到 HPOM 活动消息浏览器。 集成在 NNMi 和 HPOM 之间同步事件。它还实现了从 HPOM 内部访问 NNMi 控制台。

HP NNMi-HPOM 集成支持 "多对多"格局。每个 NNMi 管理服务器可以将事件转发到 多个 HPOM 管理服务器。同样,每个 HPOM 管理服务器可以从多个 NNMi 管理服务器接 收事件。集成会解释事件的唯一标识符以确定源 NNMi 管理服务器。

HP NNMi-HPOM 集成由以下部分组成:

• HP NNMi-HPOM 集成模块

HP NNMi-HPOM 集成模块将事件从 NNMi 转发到 HPOM。它是在 NNMi 管理服务 器上安装和配置的。

• HP Operations Manager 事件 Web 服务

HPOM 使用 HP Operations Manager 事件 Web 服务 (IWS) 接收从 NNMi 转发的事件。

• 用于根据上下文访问 NNMi 控制台的 HPOM 应用程序

HPOM 提供了用于访问 NNMi 控制台中的表单、视图和工具的应用程序。例如,可以 直接从 HPOM 活动消息浏览器打开 NNMi 事件。特定应用程序确定 NNMi 控制台打 开时所处的上下文。需要先配置这些应用程序,然后才能使用。

价值

HP NNMi-HPOM 集成在 HPOM 活动消息浏览器中提供关于网络管理、系统管理和应用 程序管理方面的事件合并,这样 HPOM 用户就可以检测和调查潜在的网络问题。

集成的主要功能如下:

- 从 NNMi 转发到 HPOM 的自动事件。
 - 转发的事件显示在 HPOM 活动消息浏览器中。
 - 可以创建过滤器来限制 NNMi 转发哪些事件。
- 下表描述了 NNMi 和 HPOM 之间的事件更新的同步。

触发	结果
在 HPOM 中,消息已确认。	在 NNMi 中,相应事件的生命周期状态 设置为"已关闭"。
在 HPOM 中,消息未确认。	在 NNMi 中,相应事件的生命周期状态 设置为"已注册"。
在 NNMi 中, 事件的生命周期状态设置为 "已关闭"。	在 HPOM 中,相应消息已确认。
在 NNMi 中, 事件的生命周期状态从"已 关闭"更改为任何其他状态。	在 HPOM 中,相应消息未确认。

- 从 HPOM 访问 NNMi 控制台。
 - HPOM 用户可以在所选消息的上下文中打开 NNMi 事件表单。
 - HPOM 用户可以在所选消息和节点的上下文中启动 NNMi 视图(例如,第2层邻 居视图)。
 - HPOM 用户可以在所选消息和节点的上下文中启动 NNMi 工具(例如,状态轮询)。
 - 当 HPOM 正在整合来自多个 NNMi 管理服务器的 NNMi 事件时,集成会解释每 个事件的唯一标识符以访问正确的 NNMi 管理服务器。

集成产品

本部分中的信息适用于以下产品:

- HPOM for Windows (也称为 OMW)
- HPOM for UNIX (也称为 OMU)
- HPOM for Linux (也称为 OML)

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

• NNMi 9.10

NNMi和 HPOM 必须安装在不同的计算机上。NNMi管理服务器和 HPOM 管理服务器计算机可以使用相同或不同的操作系统。

有关受支持的硬件平台和操作系统的最新信息,请参阅这两种产品的支持列表。

文档

本章描述如何配置 NNMi 以与 HPOM 通信。

HPOM 文档描述如何配置 HPOM 以与 NNMi 通信。它还描述如何使用 HP NNMi-HPOM 集成。

- 有关 HPOM for Windows,请参阅 HPOM 帮助中关于 HP NNMi Adapter 的信息。
- 有关 HPOM for UNIX 版本 9.xx,请参阅《HP Operations Manager for UNIX 管理员参考》中的将NNMi 集成到HPOM部分。
- 有关 HPOM for UNIX 版本 8.3x,请参阅《HP NNMi—HPOM Integration for HP Operations Manager 用户指南》。
- 有关 HPOM for Linux,请参阅《HP Operations Manager for Linux 管理员参考》 中的*将 NNMi 集成到 HPOM* 部分。

启用 HP NNMi-HPOM 集成(Web 服务实施)

这一部分描述用于启用 HP NNMi-HPOM 集成的过程。对于要包含在集成中的每个 NNMi 管理服务器和每个 HPOM 管理服务器,完成过程中针对所用 HPOM 版本的相应步骤。

HPOM for Windows

- 1 在 NNMi 管理服务器上,配置转发到 HPOM 的 NNMi 事件:
 - a 在 NNMi 控制台中, 打开 HP NNMi-HPOM 集成选择表单(集成模块配置 > HPOM)。
 - b 单击 Web 服务实施。
 - c 在 HP NNMi-HPOM Web 服务集成配置表单上,选中启用集成复选框以激活表单上的 其余字段。

d 输入用于连接到 NNMi 管理服务器的信息。



集成需要与 NNMi 控制台进行 HTTP 连接。使 NNMi SSL 已启用复选框保持未选中 状态。

有关这些字段的信息,请参阅第 570 页的 NNMi 管理服务器连接。

e 输入用于连接到 HPOM 管理服务器的信息。

有关这些字段的信息,请参阅第 571 页的 HPOM 管理服务器连接。

- f 输入以下字段的值:
 - 仅转发
 - 保留期 (分钟)
 - 事件过滤器

有关这些字段的信息,请参阅第572页的集成行为。

g 如果要 NNMi 将事件转发到多个 HPOM 管理服务器,则单击**添加其他 HPOM 服务** 器,然后在 HPOM 字段中输入下一个 HPOM 管理服务器的信息。

第一个服务器的信息显示在其他 HPOM 服务器列表中。

h 单击表单底部的提交。

将会出现新窗口,其中显示状态消息。如果有消息指出连接到 HPOM 服务器时发 生问题,请重新打开 HP NNMi-HPOM Web 服务集成配置表单(或在消息窗口中按 ALT+向左箭头),然后根据错误消息文本的建议调整用于连接到 HPOM 管理服务 器的值。

- 2 在 HPOM 中, 配置用于连接到 NNMi 管理服务器的 NNMi Adapter, 如 HPOM 帮助的 *配置 NNMi 服务器名称和端口*中所述。
- 3 在 HPOM 中,对于在转发到此 HPOM 管理服务器的 NNMi 事件中将指定为源节点的 每个 NNMi 节点,添加一个被管节点。还要为将事件转发到此 HPOM 管理服务器的每 个 NNMi 管理服务器添加一个被管节点。

或者,也可以创建一个外部节点以捕获所有转发的 NNMi 事件。对于初始测试,将节 点过滤器设置为 <*>.<*>.<*>(对于 IP 过滤器)或 <*>(对于名称过滤器)。 在验证集成之后,限制外部节点过滤器以匹配网络。

有关详细信息,请参阅 HPOM 帮助中的 配置 NNMi 服务器 节点。



如果不为 NNMi 事件源节点设置 HPOM 被管节点,则 HPOM 管理服务器丢弃关于该 节点的所有事件。

- 4 可选。在 HPOM 中,将 NNMi 事件的自定义消息属性添加到活动消息浏览器:
 - a 在浏览器中,右键单击任何列标题,然后单击选项。
 - b 在**输入自定义消息属性**列表中,选择属性,然后单击**添加**。
 - NNMi 事件的自定义消息属性以文本 nnm 开头。
 - 对于 HP NNMi-HPOM 集成的 Web 服务实施, NNMi 事件最具相关性的属 性如下:

```
nnm.assignedTo
nnm.category
nnm.emittingNode.name
nnm.source.name
```

- 要更改自定义消息属性出现在消息浏览器中的顺序,请将列标题拖到新位置。
- 5 *可选*。在 HPOM 中,通过将 NNMi 源节点与 HP NNMi Web 工具组关联,可启用 NNMi 视图的根据上下文启动。

有关详细信息,请参阅 HPOM 帮助中的*启用"按节点"工具组中的工具*。

HPOM for UNIX 和 HPOM for Linux

- 1 仅针对 HPOM for UNIX 版本 8.3x。准备 HPOM for UNIX 管理服务器:
 - a 在 HPOM for UNIX 管理服务器上,安装 HP Operations Manager 事件 Web 服务(IWS),如《HP Operations Manager 事件 Web 服务集成指南》中所述。
 - b 在 HPOM for UNIX 管理服务器上,安装最新的 HPOM 合并补丁,可从以下地址获取:

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

- 2 在 NNMi 管理服务器上, 配置转发到 HPOM 的 NNMi 事件:
 - a 在 NNMi 控制台中, 打开 HP NNMi-HPOM 集成选择表单(集成模块配置 > HPOM)。
 - b 单击 Web 服务实施。
 - c 在 HP NNMi-HPOM Web 服务集成配置表单上,选中启用集成复选框以激活表单上的 其余字段。
 - d 输入用于连接到 NNMi 管理服务器的信息。



有关这些字段的信息,请参阅第 570 页的 NNMi 管理服务器连接。

• 输入用于连接到 HPOM 管理服务器的信息。有关这些字段的信息,请参阅第 571 页的 HPOM 管理服务器连接。

- f 输入以下字段的值:
 - 仅转发
 - 保留期 (分钟)
 - 事件过滤器

有关这些字段的信息,请参阅第572页的集成行为。

g 如果要 NNMi 将事件转发到多个 HPOM 管理服务器,则单击**添加其他 HPOM 服务** 器,然后在 HPOM 字段中输入下一个 HPOM 管理服务器的信息。

第一个服务器的信息显示在其他 HPOM 服务器列表中。

h 单击表单底部的**提交**。

将会出现新窗口,其中显示状态消息。如果有消息指出连接到 HPOM 服务器时发 生问题,请重新打开 HP NNMi-HPOM Web 服务集成配置表单(或在消息窗口中按 ALT+ 向左箭头),然后根据错误消息文本的建议调整用于连接到 HPOM 管理服务 器的值。

- i 单击表单底部的**提交**。
- 3 在 HPOM 中,对于在转发到此 HPOM 管理服务器的 NNMi 事件中将指定为源节点的 每个 NNMi 节点,添加一个被管节点。还要为将事件转发到此 HPOM 管理服务器的每 个 NNMi 管理服务器添加一个被管节点。

或者,也可以创建一个外部节点以捕获所有转发的 NNMi 事件。对于初始测试,将节 点过滤器设置为 <*>.<*>.<*>.<*>(对于 IP 过滤器)或 <*>(对于名称过滤器)。 在验证集成之后,限制外部节点过滤器以匹配网络。

有关详细信息,请参阅《HP Operations Manager for UNIX 管理员参考》或《HP Operations Manager for Linux 管理员参考》。

如果不为 NNMi 事件源节点设置 HPOM 被管节点,则 HPOM 管理服务器丢弃关于该 节点的所有事件。

- 4 可选。在 HPOM 中,将 NNMi 事件的自定义消息属性添加到活动消息浏览器:
 - a 在 Java GUI 消息浏览器中,右键单击任何列标题,然后单击自定义消息浏览器列。
 - b 在自定义选项卡上,从可用自定义消息属性中进行选择,然后单击确定。
 - NNMi 事件的自定义消息属性以文本 nnm 开头。
 - 对于 HP NNMi-HPOM 集成的 Web 服务实施, NNMi 事件最具相关性的属 性如下:

nnm.assignedTo nnm.category nnm.emittingNode.name nnm.source.name

— 要更改自定义消息属性出现在消息浏览器中的顺序,请将列标题拖到新位置。

- 5 可选。在 HPOM 管理服务器上,准备用于访问 NNMi 控制台的 HPOM 应用程序。
 - a 必需。安装该组基本 NNMi 应用程序。

HPOM 版本 9.00 或更高版本将自动安装基本 NNMi 应用程序。

b 可选。安装其他 NNMi 应用程序。

有关信息,请参阅《HP Operations Manager for UNIX 管理员参考》(版本 9.xx)、 《HP NNMi—HPOM Integration for HP Operations Manager 用户指南》(版本 8.3x)或《HP Operations Manager for Linux 管理员参考》中关于安装和配置 HP NNMi—HPOM 集成的部分。

使用 HP NNMi-HPOM 集成 (Web 服务实施)

用法示例

图 29 显示 NNMi 控制台中的接口故障事件。源对象和消息列中的信息一同用于描述该情境。

SNMP 陷阱 🔁 😅 🤄 🌮 🗙 🔛 2 前一个小时 🚽 <设置节点组过滤器> → 🛛 🔯 🕥 0-0 行, 共 0 行 \Diamond 生命周期状态 上次发生时间 严重度 源节点 源对象 类别 ▲ 系列 关联属性 消息 5 8 9/25/08 4:29 PM ovccrt1 Et1/0 * V. Cisco Agent Inte 图 30 显示由 HPOM for Windows 接收的 NNMi 事件。图 31 显示由 HPOM for UNIX 接 收的 NNMi 事件。 nnm.source.name 和文本列等同于 NNMi 控制台中的源对象和消息列。 如第 561 页的步骤 4 (对于 HPOM for Windows) 以及第 562 页的步骤 4 (对于 HPOM for UNIX 和 HPOM for Linux)所述,必须显示 nnm.source.name 自定义消息属性列。 图 30 HPOM for Windows 中的转发事件

图 29 NNMi 控制台中的接口故障事件

everity	Received	Node	Application	Object 🛆 🛛	Text	nnm.source.name
Critical	26/08/2008 16:2	ovccrt1	NNMi	Interface	Cisco Agent Interface Down (linkDo	Et1/0

图 31 HPOM for UNIX 中的转发事件

/ Severity	Time Received	Node	Application	Object	Message Text	1	nnm.source.name
ritical	08:56:39 09/2	ovcort1	NNMi	Interface	Cisco Agent Interface Down (linkDown Trap) on interf	5	Et1/0

正常情况: MSI 条件未知

HPOM 服务器通过 MSI (不是常规陷阱策略)接收转发的 NNMi 事件。在 HPOM 消息浏览器中,消息源的格式是 MSI 后跟 MSI 接口的名称。条件名称对应于消息中的 condition_id 字段,此字段由于没有关联的策略而未设置。

- *HPOM for Windows*:策略类型为空。
- HPOM for UNIX 或 HPOM for Linux: 消息源格式为: MSI: <MSI 接口>:条件未知。

更多信息

有关使用 HP NNMi-HPOM 集成的详细信息,请参阅 HPOM 文档。

- HPOM for Windows: 请参阅 HPOM 帮助中有关 HP NNMi Adapter 的主题。
- HPOM for UNIX: 请参阅《HP Operations Manager for UNIX 管理员参考》(版本 9.xx)或《HP NNMi—HPOM Integration for HP Operations Manager 用户指南》 (版本 8.3x)中有关安装和配置 HP NNMi-HPOM 集成的部分。
- *HPOM for Linux*: 请参阅《HP Operations Manager for Linux 管理员参考》中关于 安装和配置 HP NNMi-HPOM 集成的部分。
- 在 HPOM 消息浏览器中,所转发 NNMi 事件的详细信息是作为自定义消息属性提供的。

更改 HP NNMi-HPOM 集成配置 (Web 服务实施)

- 1 在 NNMi 控制台中,打开 HP NNMi-HPOM 集成选择表单 (集成模块配置 > HPOM)。
- 2 单击 Web 服务实施。
- 3 对值进行相应修改。
 - 如果您了解事件过滤器及其他 HPOM 服务器列表中条目的语法,则可以直接修改 条目。
 - 如果不知道列表项的语法,则删除该条目,然后重新输入它。

有关此表单上的字段的信息,请参阅第 570 页的 HP NNMi-HPOM Web 服务集成配置表单参考。

4 验证表单顶部的启用集成复选框是否已选中,然后单击表单底部的提交。 更改会立即生效。

禁用 HP NNMi-HPOM 集成 (Web 服务实施)

对于所有 HPOM 管理服务器

要停止将 NNMi 事件转发到所有 HPOM 管理服务器,请遵循以下步骤:

- 1 在 NNMi 控制台中,打开 HP NNMi-HPOM 集成选择表单(集成模块配置 > HPOM)。
- 2 单击 Web 服务实施。
- 3 清除表单顶部的启用集成复选框,然后单击表单底部的提交。 更改会立即生效。

如有必要,对所有 NNMi 管理服务器重复此过程。

对于一个 HPOM 管理服务器

要停止将 NNMi 事件转发到仅一个 HPOM 管理服务器,请遵循以下步骤:

- 1 在 NNMi 控制台中,打开 HP NNMi-HPOM 集成选择表单 (集成模块配置 > HPOM)。
- 2 单击 Web 服务实施。

Λ

- 3 在**其他 HPOM 服务器**列表中,编辑文本以删除条目,以使 HPOM 管理服务器断开与集成的连接。
 - 单击**清除**将删除列表中的所有 HPOM 服务器。
- 4 单击表单底部的提交。 更改会立即生效。

对 HP NNMi-HPOM 集成 (Web 服务实施)进行故障诊断

HPOM 不接收任何转发事件

- 如果集成在过去一直成功运行,则可能是配置的某个方面(例如 NNMi 或 HPOM 用户密码)最近有更改。您可能希望在全程执行这整个过程之前,如第 564 页的更改 HP NNMi– HPOM 集成配置(Web 服务实施)中所述更新集成配置。
 - 1 在 NNMi 控制台中,打开 HP NNMi-HPOM 集成选择表单 (集成模块配置 > HPOM)。
 - 2 单击 Web 服务实施。

有关此表单上的字段的信息,请参阅第 570 页的 HP NNMi-HPOM Web 服务集成配置表单参考。

3 在 HP NNMi-HPOM Web **服务集成配置**表单中检查集成的状态,方法是在表单的底部单击 **提交** (不进行任何配置更改)。

将会出现新窗口,其中显示状态消息。

- 如果消息指示成功,问题很可能是由于 HPOM 未配置为接受来自 NNMi 所管理设备的事件。对于未配置为 HPOM 中的被管节点的 NNMi 源节点, HPOM 将忽略来自该节点的任何转发事件,如第 560 页的步骤 3 (对于 HPOM for Windows)和第 562 页的步骤 3 (对于 HPOM for UNIX 和 HPOM for Linux)中所述。验证 HPOM 配置,然后如此过程的步骤 10 所述测试集成。
- 如果消息表明连接到 HPOM 服务器发生问题,则说明 NNMi 和 HPOM 无法通信。继续执行此过程的步骤 4。
- 4 通过登录到 HPOM 控制台并显示 HPOM 活动消息浏览器,验证 HPOM 凭证的准确 性和访问级别:
 - *HPOM for Windows*: 以 HPOM 用户身份从 HP NNMi-HPOM Web 服务集成配置表单登录计算机,然后启动 HPOM 控制台。

用户名格式为 <Windows 域>\<用户名>。

• *HPOM for UNIX* 或 *HPOM for Linux* 用 HPOM 用户凭证从 HP NNMi-HPOM Web 服务集成配置表单登录 HPOM 控制台。

如果无法登录到 HPOM 控制台,请联系 HPOM 管理员以验证登录凭证。

- 5 验证与 HPOM 管理服务器的连接是否配置正确:
 - a 在 Web 浏览器中, 输入以下 URL:

<协议>://<omserver>:<端口>/opr-webservice//Incident.svc?wsdl

其中的这些变量与 HP NNMi—HPOM Web 服务集成配置表单上的值相关,如下所示:

- 如果选中**启用 HPOM SSL** 复选框,则 < 协议> 是 https。
- 如果不选中**启用 HPOM SSL**复选框,则 < 协议> 是 http。
- *<omserver>*是 HPOM 主机的值。
- *<端□*> 是 HPOM 端口的值。
- b 系统提示时,从 HP NNMi-HPOM Web **服务集成配置**表单输入 HPOM **用户**的凭证。

生成的网页是用于描述 IWS 的 XML 文件。

- 如果显示 XML 文件,则说明与 HPOM 管理服务器的连接已正确配置。继续执行步骤 6。
- 如果看到错误消息,则说明与 HPOM 管理服务器的连接未正确配置。请联系 HPOM 管理员以验证用于连接到 HPOM Web 服务的信息。继续对 HPOM 连 接进行故障诊断,直到您看到 XML 文件。

6 验证与 NNMi 的连接是否已正确配置:

如果在此过程的步骤 1 中已使用此步骤中所述信息连接到 NNMi 控制台,则不需要重新连接到 NNMi 控制台。继续执行步骤 7。

- a 在 Web 浏览器中, 输入以下 URL:
 - < 协议>://<NNMi 服务器>:< 端口>/nnm/

其中的这些变量与 HP NNMi—HPOM Web 服务集成配置表单上的值相关,如下所示:

— 如果选中NNMi SSL 已启用 复选框,则 <协议> 是 https。

如果选中 NNMi SSL 已启用 复选框,通过输入以下命令验证 KeyManager 进程是否正在运行:

ovstatus -v ovjboss

— 如果清除NNMi SSL 已启用 复选框,则 <协议> 是 http.

— <*NNMi 服务器*>是 NNMi 主机的值。

使用 NNMi 管理服务器的完全限定域名或 IP 地址。不要使用 localhost。

— <端口> 是 NNMi 端口的值。

要验证 NNMi 的 HTTP 或 HTTPS 端口,请检查 nms-local.properties 文件 (如第 570 页的表 64 中所述)。

b 提示时,输入具有管理员角色的 NNMi 用户的凭证。

此时应当看到 NNMi 控制台。如果 NNMi 控制台未出现,请联系 NNMi 管理员以 验证用于连接到 NNMi 的信息。继续对 NNMi 连接进行故障诊断,直到 NNMi 控 制台出现。



- c 验证 NNMi 用户和 NNMi 密码的值。
 - 如果 HP NNMi-HPOM Web 服务集成配置表单上列出的 NNMi 用户具有管理员角 色,并且您曾经使用此用户名成功连接到 NNMi 控制台,请在 HP NNMi-HPOM Web 服务集成配置表单上重新输入相应密码。
 - 如果 HP NNMi-HPOM Web 服务集成配置表单上列出的 NNMi 用户具有 Web 服务 客户端角色,请联系 NNMi 管理员以验证 NNMi 用户和 NNMi 密码的值。

密码在 NNMi 控制台中是隐藏的。如果您不能确定为 NNMi 用户名指定的密码,可以请 NNMi 管理员重置密码。

7 使用在此过程的步骤 5 和步骤 6 中用于成功连接的值更新 HP NNMi-HPOM Web 服务集成配置表单。

有关详细信息,请参阅第 570 页的 HP NNMi-HPOM Web 服务集成配置表单参考。

- 8 单击表单底部的提交。
- 9 如果状态消息仍然表明连接到 HPOM 服务器发生问题,请执行以下操作:
 - a 清除 Web 浏览器缓存。
 - b 从 Web 浏览器清除所有保存的表单或密码数据。
 - c 完全关闭 Web 浏览器窗口, 然后重新打开它。
 - d 重复此过程的步骤 7 和步骤 8。
- 10 通过在 NNMi 管理服务器上生成事件并确定它是否到达 HPOM 管理服务器,以此测 试配置。

或者,将 NNMi 管理事件的生命周期状态更改为打开。(如果生命周期状态当前已为打 开,则将生命周期状态更改为已关闭,然后再改回打开。)

HPOM 不接收某些转发事件

验证 HPOM 节点和事件过滤器。

HPOM 管理服务器必须配置为接受来自 NNMi 管理的设备的事件。对于未配置为 HPOM 中的被管节点的 NNMi 源节点, HPOM 将忽略来自该节点的任何转发事件,如第 560 页 的步骤 3 (对于 HPOM for Windows)和第 562 页的步骤 3 (对于 HPOM for UNIX 和 HPOM for Linux)中所述。

如果将 NNMi 源节点配置为 HPOM 中的被管节点,则在 HP NNMi-HPOM Web 服务集成配置表单上验证事件过滤器配置。然后,通过在 NNMi 管理服务器上生成事件并确定它是否到达 HPOM 管理服务器,以此测试过滤器。

NNMi HPOM 消息浏览器中不提供事件信息

来自 NNMi 事件的重要信息作为自定义消息属性传递到 HPOM。如第 561 页的步骤 4(对于 HPOM for Windows) 以及第 562 页的步骤 4(对于 HPOM for UNIX 和 HPOM for Linux) 中所述,为 NNMi 事件添加一个或多个自定义消息属性。

NNMi 和 HPOM 不同步

如果任一管理服务器不再可访问,则 NNMi 事件视图和 HPOM 活动消息浏览器中的事件可能不再匹配。 HP NNMi-HPOM 集成可以重新同步这些事件 (如此处所述)。

 如果 HPOM 管理服务器对于 HP NNMi-HPOM 集成模块不再可用,则集成模块将定 期检查该 HPOM 管理服务器是否可用,并将在可以重新建立连接时恢复事件转发。可 以与 HPOM 管理服务器建立连接时,集成模块将转发 HPOM 管理服务器关闭期间可 能已错过的事件。 • 如果 NNMi 管理服务器在 HPOM 用户确认或取消确认转发事件时不可用,则 NNMi 不接收状态更改。 NNMi 和 HPOM 可能对此事件显示不同状态。

集成不能通过防火墙运行

确保 NNMi 管理服务器可以通过主机和端口直接处理 HPOM IWS。

HP NNMi-HPOM Web 服务集成配置表单参考

HP NNMi-HPOM Web 服务集成配置表单包含用于配置 NNMi 和 HPOM 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—HPOM 集成选择表单上,单击 Web 服务实施。)

只有具有管理员角色的 NNMi 用户才可以访问 HP NNMi-HPOM Web 服务集成配置表单。

HP NNMi—HPOM Web 服务集成配置表单采集以下常规方面的信息:

- 第 570 页的 NNMi 管理服务器连接
- 第 571 页的 HPOM 管理服务器连接
- 第572页的集成行为
- 第 573 页的事件过滤器

要应用对集成配置的更改,请在 HP NNMi-HPOM Web 服务集成配置表单上更新值,然后单击 提交。

NNMi 管理服务器连接

表 64 列出用于连接到 NNMi 管理服务器的参数。这就是您用于打开 NNMi 控制台的信息。通过查看调用 NNMi 控制台会话的 URL,可以确定这些值中的大部分。与 NNMi 管理员协作,为配置表单的这一部分确定合适的值。

表 64 NNMi 管理服务器连接信息

字段	描述
NNMi SSL 己启用	用于连接到 NNMi 控制台的连接协议规范。 集成需要与 NNMi 控制台进行 HTTP 连接。使 NNMi SSL 已启用复选框保持未选中状态。
NNMi 主机	NNMi 管理服务器的完全限定域名。此字段已预填充了用于访问 NNMi 控制台的主机 名。验证此值是否是由在 NNMi 管理服务器上运行的 nnmofficialfqdn.ovpl -t 命 令返回的名称。
NNMi 端口	用于连接到 NNMi 控制台的端口。此字段预填充了 jboss 应用程序服务器用于与 NNMi 控制台通信的端口,如以下文件中所指定: • Windows: %NnmDataDir%\conf\nnm\props\nms-local.properties • UNIX: \$NnmDataDir/conf/nnm/props/nms-local.properties 使用 jboss.http.port 的值,它的默认值为 80 或 8004 (具体取决于安装 NNMi 时是 否存在另一个 Web 服务器)。

表 64 NNMi 管理服务器连接信息 (续)

字段	描述
NNMi 用户	用于连接到 NNMi Web 服务的用户名。此用户必须具有 NNMi 管理员或 Web 服务客户端角色。 注:此用户名的密码将以明文形式传递。 最佳实践:创建和使用具有 Web 服务客户端角色的 NNMiIntegration 用户帐户。
NNMi 密码	指定 NNMi 用户的密码。

HPOM 管理服务器连接

表 65 列出用于连接到 HPOM 管理服务器上的 Web 服务的参数。与 HPOM 管理员协作, 为配置的这一部分确定合适的值。

表 65 HPOM 管理服务器连接信息

HPOM 服务器参数	描述
启用 HPOM SSL	连接协议规范。 • 如果将 HPOM 配置为使用 HTTPS,则选中 启用 BSM SSL 复选框。这是默认配置。 • 如果将 HPOM 配置为使用 HTTP,则清除 启用 BSM SSL 复选框。
HPOM 主机	HPOM 管理服务器的完全限定域名。 通过使用 nslookup 或 ping 命令,验证此名称是否可以从 NNMi 管理服务器进行解析。 如果 DNS 发生问题,请使用 HPOM 管理服务器的 IP 地址。如果可能,请使用 traceroute 命令,以验证从 NNMi 管理服务器到 HPOM 管理服务器的网络路径。
HPOM 端口	 用于连接到 HPOM Web 服务的端口。要确定指定哪个端口号,请在 HPOM 管理服务器 上执行以下操作: <i>HPOM for Windows</i>:检查 IIS Manager 中的端口设置(可以从开始菜单访问,例如 开始 > 管理工具 > Internet Information Services (IIS) Manager)。 <i>HPOM for UNIX</i> 或 HPOM for <i>Linux</i>:运行以下命令:ovtomcatbctl -getconf 此字段已使用值 443 预填充,它是与 HPOM for Windows 进行 SSL 连接时使用的默认端 口。要与 HPOM for UNIX 或 HPOM for Linux 进行 SSL 连接,默认端口是 8443 或 8444。

表 65 HPOM 管理服务器连接信息(续)

HPOM 服务器参数	描述
HPOM 用户	具有 HPOM 管理员角色的有效 HPOM 用户帐户名。必须允许此用户查看 HPOM 活动 消息浏览器和 HPOM 事件 Web 服务 WSDL。
	<i>仅针对 Windows</i> :在 Windows 操作系统上, HPOM 通过 Microsoft Internet 信息服务 (IIS) 验证用户凭证。用格式 < <i>Windows 域</i> >\< <i>用户名></i> 指定 Windows 用户。 最佳实践:
	 HPOM for Windows: 指定属于 HP-OVE-ADMINS 用户组的用户。(在 Microsoft 管理 控制台的"本地用户和组"区域中验证组成员资格,此管理控制台可通过控制面板 > 管 理工具 > 计算机管理打开。) HPOM for UNIX 或 HPOM for Linux: 使用 opc_adm 用户帐户。
HPOM 密码	指定 HPOM 用户的密码。

集成行为

表 66 列出描述集成行为的参数。与 NNMi 管理员协作,为配置的这一部分确定合适的值。

表 66 集成行为信息

字段	描述
仅转发	HP NNMi-HPOM 集成模块的行为规范。默认情况下,集成模块将事件转发到 HP NNMi- HPOM Web 服务集成配置表单上标识的 HPOM 管理服务器,并从这些 HPOM 管理服务器 接收事件确认。可以禁用事件确认的接收。 • 对于单向通信(将事件转发到 HPOM 但是忽略来自 HPOM 的事件确认),请选中仅 转发复选框。 • 对于双向通信,将仅转发复选框保留为未选中。这是默认行为。
保留期(分钟)	将配置事件转发到 HPOM 之前将等待的分钟数。如果在此时间内事件关闭(例如, SNMPLinkUp 事件会取消 SNMPLinkDown 事件),则 HPOM 不会接收到该事件。如 果要 NNMi 立即转发事件,则输入值 0。 默认值是 5 分钟。
事件过滤器	基于 NNMi 事件属性的用于限制事件转发的过滤器。默认过滤器 (nature=ROOTCAUSE origin=MANAGEMENTSOFTWARE) 指定由 NNMi 生成的所有根源事件。可以修改过滤器以更改将哪些事件转发到 HPOM。 注: 事件过滤器字段中的所有文本 (属性名称和值)都区分大小写。 有关详细信息,请参阅事件过滤器。

事件过滤器

事件过滤器是**事件过滤器**列表中的所有条目的一种组合。具有相同属性值的过滤器条目将扩展过滤器 (逻辑 OR)。具有不同属性值的过滤器条目将限制过滤器 (逻辑 AND)。所有 过滤器条目一起作用;您*不能*创建格式为 (a AND b) OR c 的过滤器。有关过滤器条目的 示例,请参阅第 574 页的事件过滤器示例。

要创建事件过滤器,请遵循以下步骤:

- 1 在 NNMi 控制台中,打开 HP NNMi-HPOM 集成选择表单 (集成模块配置 > HPOM)。
- 2 单击 Web 服务实施。

Λ

3 要删除过滤器条目,在事件过滤器列表中,编辑文本以删除条目。

单击**清除**将删除列表中的所有过滤器条目。

- 4 要添加事件过滤器条目:
 - a 从名称列表中选择一个属性。有关受支持属性,请参阅步骤 c 中的表。
 - b 选择要执行的比较操作。受支持的运算符如下:
 - =
 - ___!=
 - <
 - <=
 - >
 - >=
 - c 输入比较值。下表列出每个属性的受支持属性和可接受值。

属性	可能值
名称	在 NNMi 控制台中检查事件配置以确定可用事件名称。
性质	 ROOTCAUSE SECONDARYROOTCAUSE SYMPTOM SERVICEIMPACT STREAMCORRELATION INFO NONE

属性	可能值
来源	 MANAGEMENTSOFTWARE MANUALLYCREATED SYMPTOM REMOTELYGENERATED SNMPTRAP SYSLOG OTHER
系列	 com.hp.nms.incident.family.Address com.hp.nms.incident.family.Interface com.hp.nms.incident.family.Node com.hp.nms.incident.family.OSPF com.hp.nms.incident.family.HSRP com.hp.nms.incident.family.AggregatePort com.hp.nms.incident.family.Board com.hp.nms.incident.family.Connection com.hp.nms.incident.family.Correlation
类别	 com.hp.nms.incident.category.Fault com.hp.nms.incident.category.Status com.hp.nms.incident.category.Config com.hp.nms.incident.category.Accounting com.hp.nms.incident.category.Performance com.hp.nms.incident.category.Security com.hp.nms.incident.category.Alert
严重度	 NORMAL WARNING MINOR MAJOR CRITICAL

5 重复步骤 4, 直到定义完所有过滤器条目。

6 单击表单底部的提交。

事件过滤器示例

将 NodeDown 事件从 NNMi 转发到 HPOM

name=NodeDown

将 NodeDown 和 InterfaceDown 事件从 NNMi 转发到 HPOM

name=NodeDown name=InterfaceDown

将 CiscoLinkDown 事件从 NNMi 转发到 HPOM

name=CiscoLinkDown

转发严重度为 MAJOR 或 MINOR 的 NNMi 管理事件

```
origin=MANAGEMENTSOFTWARE
severity=MAJOR
severity=MINOR
```

转发严重度至少为 MINOR 且性质为 ROOTCAUSE 或 SERVICEIMPACT 的 NNMi 事件

```
severity>=MINOR
nature=ROOTCAUSE
nature=SERVICEIMPACT
```

事件过滤器限制

因为所有过滤器条目将结合起来为 NNMi 管理服务器创建一个事件过滤器,因此应用以下限制:

- 声明的严重度应用于所有事件。例如,要转发严重度为 MINOR 或更高的 NodeDown 事件以及严重度为 MAJOR 的 InterfaceDown 事件,请将过滤器严重度设置为 >=MINOR, 并且使用 HPOM 逻辑过滤掉那些不需要的 InterfaceDown 消息。
- 事件过滤器不提供使事件转发仅限于特定源节点的机制。HPOM 被管节点(或外部节 点)配置将限制 HPOM 接受的转发事件。
HP NNMi Integration Module for Netcool Software



IBM Tivoli Netcool/OMNIbus 能够将来源广泛的事件整合到单个视图中。

本章包含以下主题:

- HP NNMi Integration Module for Netcool Software
- 启用 HP NNMi Integration Module for Netcool Software
- 使用 HP NNMi Integration Module for Netcool Software
- 更改 HP NNMi Integration Module for Netcool Software
- 禁用 HP NNMi Integration Module for Netcool Software
- 对 HP NNMi Integration Module for Netcool Software 进行故障诊断
- HP NNMi Integration Module for Netcool Software 目标表单参考

HP NNMi Integration Module for Netcool Software

HP NNMi Integration Module for Netcool Software 将 NNMi 管理事件作为 SNMPv2c 陷阱转发到 NNMi 管理服务器上的 Netcool/OMNIbus SNMP 探测器。探测器过滤 NNMi 陷阱并将它们转发到 Netcool/OMNIbus 服务器。

虽然集成也可以将 NNMi 从被管设备接收到的 SNMP 陷阱转发到探测器,但是建议您改用 NNMi SNMP 陷阱转发机制。有关详细信息,请参阅 hp-nnmi-nbi.mib 文件。

集成不会将 NNM 6.x 或 7.x 管理工作站生成的事件转发到探测器。

集成提供了用于扩展 Netcool 事件查看器的菜单项,以在所选事件的上下文中启动 NNMi 表单和视图。

NNMi Integration Module for Netcool Software 是 NNMi Northbound Interface 的特 定实施,如第 505 页的 NNMi Northbound Interface 中所述。

NNMi Integration Module for Netcool Software 由以下组件组成:

- nnmi-northbound 集成模块
- 配置文件,用于将 NNMi 陷阱转换成 Netcool/OMNIbus 事件以及在 Netcool/Webtop 事件列表和 Netcool/OMNIbus 事件列表中创建新菜单

价值

NNMi Integration Module for Netcool Software 将网络级别故障和性能信息添加到 Netcool/OMNIbus,以便 Netcool/OMNIbus 用户可以检测并调查潜在网络问题。

集成的主要功能如下:

- 从 NNMi 转发到 Netcool/OMNIbus 的自动管理事件。转发的管理事件出现在 Netcool/ Webtop 事件列表和 Netcool/OMNIbus 事件列表中。
- 从 Netcool/Webtop 和 Netcool/OMNIbus 访问 NNMi 控制台。
 - Netcool 用户可以在所选事件和拓扑对象的上下文中打开 NNMi 表单(例如,节点表单)。
 - Netcool 用户可以在所选事件和节点的上下文中打开 NNMi 视图 (例如,第2层 邻居视图)。
 - Netcool 用户可以在所选事件的上下文中打开 NNMi 事件表单。

集成产品

本章中的信息适用于以下产品:

- Netcool/OMNIbus

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

- Netcool/OMNIbus SNMP Probe
- 有 NNMi Integration Module for Netcool Software 许可证的 NNMi 9.10

从 NNMi 9.00 起, 安装 NNMi 为 NNMi Integration Module for Netcool Software 启用临时的瞬时启动许可证密钥。要在瞬时启动许可证密钥过期之后使用集成,请获取 并安装 NNMi Integration Module for Netcool Software 的永久许可证密钥。

NNMi 和 Netcool/OMNIbus 必须安装在不同的计算机上。 NNMi 管理服务器和 Netcool/ OMNIbus 服务器计算机可以使用相同或不同的操作系统。

Netcool/OMNIbus SNMP Probe 必须安装在 NNMi 管理服务器计算机上。

有关受支持的硬件平台和操作系统的最新信息,请参阅 NNMi 支持列表和 Netcool/ OMNIbus 产品文档。

文档

本章描述如何配置 NNMi Integration Module for Netcool Software 以将 NNMi 管理事件 转发到 Netcool/OMNIbus SNMP Probe。它还描述如何使用集成功能。

有关 Netcool/OMNIbus 的信息,请参阅该应用程序的文档。

启用 HP NNMi Integration Module for Netcool Software

NNMi Integration Module for Netcool Software 包含用于配置 Netcool/OMNIbus SNMP Probe 和 Netcool 事件查看器的文件。因为 Netcool 具有很高的可配置性,所以 Netcool 端的配置说明可能并不完全适用于您的 Netcool 系统。建议让有经验的 Netcool 管 理员完成启用集成的过程。

要启用 NNMi Integration Module for Netcool Software,请遵循以下步骤:

- 1 收集用于配置 Netcool 的信息:
 - a 在任何计算机上,作为具有管理员角色的 NNMi 用户登录到 NNMi 控制台。
 - b 在 NNMi 控制台中,打开 HP NNMi Integration Module for Netcool Software 配置操 作表单 (集成模块配置 > Netcool)。
 - c 通过以下方法下载 Netcool/OMNIbus SNMP Probe 的规则包含文件:右键单击 nnmi.include.rules 链接,然后将文件保存到计算机上的已知位置。

nnmi.include.rules 文件定义规则,用于解释 NNMi 管理事件的 SNMPv2c 陷阱。

- 有关 NNMi 发送到 Probe 的陷阱内容和格式的信息,请参阅 hp-nnmi-nbi.mib 文件。
- 有关自定义 nnmi.include.rules 文件的信息,请参阅 Netcool/OMNIbus 文档。
- d *可选*。下载用于配置 Netcool/Webtop 事件列表以启动 NNMi 视图的信息。执行以下两个操作:
 - 右键单击 nnmi_launch.cgi 链接,然后将文件保存到计算机上的已知位置。
 - 右键单击 nnmi_launch_cfg.txt 链接,然后将文件保存到计算机上的已知位置。
- e *可选*。下载用于配置 Netcool/OMNIbus 事件列表以启动 NNMi 视图的信息。执行 以下某个操作:
 - Windows Netcool/OMNIbus 服务器:
 - 右键单击 nnmi_confpack.zip 链接,然后将文件保存到计算机上的已知位置。
 - UNIX Netcool/OMNIbus 服务器:

右键单击 nnmi_confpack.gz 链接,然后将文件保存到计算机上的已知位置。

- 2 在 NNMi 管理服务器上安装 Netcool/OMNIbus SNMP Probe。
 - a 配置 Probe 在可用 UDP 端口上接收 SNMP 陷阱。
 - 记下此端口号以配置 NNMi 中的集成。
 - 验证 Probe 端口是否不同于 NNMi 接收 SNMP 陷阱的端口(该端口是在 NNMi 控制台中的通信配置表单上配置的)。
 - b 将步骤 1c 中的 nnmi.include.rules 文件复制到 NNMi 管理服务器。
 - c 备份主规则文件,然后在任何文本编辑器中打开该文件。
 - d 在 Netcool 企业陷阱交换机块中,对 nnmi.include.rules 文件添加 include 指 令,然后保存主规则文件。
 - e 重新启动 Probe, 然后检查 Probe 日志文件以验证重新加载规则文件时是否未发 生任何问题。

有关安装和配置 Probe 的详细信息,请参阅 Probe 文档。

- 3 配置 NNMi 事件转发:
 - a 在任何计算机上,作为具有管理员角色的 NNMi 用户登录到 NNMi 控制台。
 - b 在 NNMi 控制台中,打开 HP NNMi Integration Module for Netcool Software 配置操 作表单 (集成模块配置 > Netcool)。
 - c 单击**启用 / 禁用** NNMi Integration Module for Netcool Software, 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。)
 - d 在 HP NNMi Integration Module for Netcool Software 目标表单上,选中启用复选框以 激活表单上的其余字段。
 - e 输入用于连接到 Netcool/OMNIbus SNMP Probe 的信息。

有关这些字段的信息,请参阅第 585 页的 Netcool/OMNIbus SNMP Probe 连接。

f 指定发送选项。

有关这些字段的信息,请参阅第586页的集成内容。

g 单击表单底部的**提交**。

将会出现新窗口,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。

- 4 可选。配置 Netcool/Webtop 事件列表以启动 NNMi 视图。
 - a 将步骤 1d 中的 nnmi_launch.cgi 文件复制到 Netcool/Webtop 服务器上的 cgi-bin 目录。
 - b 遵循步骤 1d 中的 nnmi_launch_cfg.txt 文件中的说明,准备 CGI 文件并配置 Netcool/Webtop 菜单。
- 5 可选。配置 Netcool/OMNIbus 事件列表以启动 NNMi 视图。
 - a 将步骤 1e 中的 nnmi_confpack.* 存档文件复制到正在运行 Netcool/OMNIbus ObjectServer 实例的计算机。

- b 将 nnmi_confpack.* 存档文件解压到临时位置。
- c 从临时位置,运行以下命令:
 - Windows Netcool/OMNIbus 服务器:

```
%OMNIBUSHOME%\bin\nco_confpack -import \
-package nnmi.confpack \
-user <对象服务器管理员用户名> \
-server <对象服务器名称>
```

— UNIX Netcool/OMNIbus 服务器:

```
$OMNIBUSHOME/bin/nco_confpack -import \
-package nnmi.confpack \
-user <对象服务器管理员用户名> \
-server <对象服务器名称>
```

d 仅针对 UNIX: 验证 \$OMNIBROWSER 是否设置为 Mozilla Firefox 浏览器的位置。

使用 HP NNMi Integration Module for Netcool Software

启用 NNMi Integration Module for Netcool Software 时, NNMi 将 SNMPv2c 陷阱发送 到 Netcool/OMNIbus SNMP Probe。在 Netcool/Webtop 事件列表和 Netcool/OMNIbus 事件列表中查看从 NNMi 转发的内容。

有关集成模块可以转发到 Probe 的陷阱类型的信息,请参阅第 508 页的使用 NNMi Northbound Interface。有关这些陷阱的内容和格式的信息,请参阅 hp-nnmi-nbi.mib 文件。有关陷阱转发机制的比较,请参阅第 93 页的陷阱和事件转发。

NNMi 仅将每个管理事件陷阱(或接收的 SNMP 陷阱)的一个副本发送到 Netcool/ OMNIbus SNMP Probe。NNMi 不会将陷阱排队。NNMi 转发陷阱时,如果 Probe 不可 用,该陷阱将丢失。

集成模块提供了从 Netcool 事件查看器到 NNMi 控制台的链接。输入 NNMi 用户凭证以查 看 NNMi 控制台视图。

在 第 579 页的启用 HP NNMi Integration Module for Netcool Software 中,步骤 4 和步骤 5 将以下菜单项添加到 Netcool 事件查看器:

- 源对象 对于 Netcool/OMNIbus 所选事件中的对象, 打开 NNMi 表单。
- **节点** 对于 Netcool/OMNIbus 所选事件中的节点, 打开 NNMi 节点表单。
- L2 邻居 对于 Netcool/OMNIbus 所选事件中的节点,打开其 NNMi 第 2 层邻居视图。
- L3 邻居 对于 Netcool/OMNIbus 所选事件中的节点, 打开其 NNMi 第 3 层邻居视图。

• 事件详细信息 — 对于 Netcool/OMNIbus 中的所选事件, 打开 NNMi 事件表单。

- 在 UNIX Netcool/OMNIbus 服务器上:
 - Mozilla Firefox 必须是默认 Web 浏览器,才能支持从 Netcool/OMNIbus 事件列表启动 NNMi 视图。
 - \$OMNIBROWSER 环境变量必须设置为 Mozilla Firefox 浏览器的位置。

更改 HP NNMi Integration Module for Netcool Software

要更改 NNMi Integration Module for Netcool Software 配置参数,请遵循以下步骤:

- 在 NNMi 控制台中,打开 HP NNMi Integration Module for Netcool Software 配置操作表
 单 (集成模块配置 > Netcool)。
- 2 单击**启用 / 禁用 NNMi Integration Module for Netcool Software**。
- 3 选择目标,然后单击**编辑**。

4

- 对值进行相应修改。 有关此表单上的字段的信息,请参阅 第 585 页的 HP NNMi Integration Module for Netcool Software 目标表单参考。
- 5 验证表单顶部的**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 HP NNMi Integration Module for Netcool Software

禁用目标时,不会发生 SNMP 陷阱排队。

要停止将 NNMi 管理事件转发到 Netcool/OMNIbus SNMP Probe,请遵循以下步骤:

- 在 NNMi 控制台中,打开 HP NNMi Integration Module for Netcool Software 配置操作表
 单 (集成模块配置 > Netcool)。
- 2 单击 启用 / 禁用 NNMi Integration Module for Netcool Software。
- 3 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。

- 4 在 HP NNMi Integration Module for Netcool Software 目标表单上,清除表单顶部的启用复选框,然后单击表单底部的提交。
 更改会立即生效。
- 5 要保留系统资源,禁用目标时请关闭 Netcool/OMNIbus SNMP Probe。

要永久禁用集成,还要执行以下操作:

- 如 Probe 文档中所述卸载 Netcool/OMNIbus SNMP Probe。
- 从 Netcool/Webtop 和 Netcool/OMNIbus 事件列表配置中删除 NNMi 菜单项。

对 HP NNMi Integration Module for Netcool Software 进行故障诊断

Netcool/OMNIbus 不接收任何转发的 NNMi 管理事件

如果 Netcool 事件查看器不包含来自 NNMi 的任何陷阱,则遵循以下步骤:

- 1 验证 Netcool/OMNIbus SNMP Probe 是否正在接收陷阱:
 - a 验证 Probe 是否可以将消息发送到 Netcool/OMNIbus 服务器。
 - b 验证 Probe 主规则文件是否包含 nnmi.include.rules 文件的内容。
 - c 验证主规则文件的语法。
 - d 检查 Probe 日志文件以验证加载规则文件时是否未发生任何问题。
 - e 检查 Probe 日志文件以确定 NNMi 陷阱是否到达 Probe。
 - f 检查 Probe 日志文件以确定 Probe 是否处理或丢弃传入陷阱。

有关对 Probe 进行故障诊断的信息,请参阅 Netcool/OMNIbus 文档。

2 验证 NNMi 是否正在将管理事件转发到 Netcool/OMNIbus SNMP Probe。 有关信息,请参阅第 512 页的对 NNMi Northbound Interface 进行故障诊断。

Netcool/OMNIbus 不接收某些转发的 NNMi 管理事件

如果一个或多个 NNMi 管理事件陷阱未显示在 Netcool 事件查看器中,则遵循以下步骤:

验证 Netcool/OMNIbus SNMP Probe 主规则文件是否包含 nnmi.include.rules 文件的内容。

2 验证 Netcool/OMNIbus 是否正在运行。

如果 Netcool/OMNIbus 服务器关闭,则 Netcool/OMNIbus SNMP Probe 会将接收的 陷阱排队。 Netcool/OMNIbus 服务器可用时, Probe 将转发排队的陷阱。

NNMi 依赖于 Probe 对陷阱进行排队和转发。如果 Probe 关闭,则转发的陷阱将丢失。

3 验证 NNMi 进程是否正在运行。

启动第2层连接的 NNMi 表单时出错

如果 NNMi 管理事件中的源对象是第 2 层连接,则非管理员角色的 NNMi 用户无法通过 Netcool 事件查看器的**源对象**菜单项直接打开 NNMi 表单。请改为在 Netcool 事件查看器中 使用**第 2 层邻居**菜单项连接到 NNMi,然后在第 2 层邻居视图中双击该连接。

HP NNMi Integration Module for Netcool Software 目标表单参考

HP NNMi Integration Module for Netcool Software 目标表单包含用于配置 NNMi 和 Netcool/ OMNIbus SNMP Probe 之间通信的参数。如果 NNMi 管理服务器上已安装有效的 NNMi Integration Module for Netcool Software 许可证,则可以通过**集成模块配置**工作区使用此 表单。(在 HP NNMi Integration Module for Netcool Software 配置操作表单中,单击启用/禁用 NNMi Integration Module for Netcool Software。单击新建,或选择目标,然后单击编辑。)



只有具有管理员角色的 NNMi 用户才可以访问 HP NNMi Integration Module for Netcool Software 目标表单。

HP NNMi Integration Module for Netcool Software 目标表单采集以下方面的信息:

- 第 585 页的 Netcool/OMNIbus SNMP Probe 连接
- 第 586 页的集成内容
- 第589页的目标状态信息

要应用集成配置更改,请更新 HP NNMi Integration Module for Netcool Software 目标表单上的值,然后单击提交。

Netcool/OMNIbus SNMP Probe 连接

表 67 列出用于配置 Netcool/OMNIbus SNMP Probe 连接的参数。

表 67 Netcool/OMNIbus SNMP Probe 连接信息

字段	描述
主机	NNMi 管理服务器的完全限定域名(首选)或 IP 地址,此服务器是 Netcool/OMNIbus SNMP Probe 接收来自 NNMi 的 SNMP 陷阱的系统。
	集成支持用以下方法标识 Probe 主机:
	 NNMi FQDN NNMi 管理与 NNMi 管理服务器上的 Probe 的连接,并且主机字段变成只读的。 这是默认和建议的配置。
	• 使用环回 NNMi 管理与 NNMi 管理服务器上的 Probe 的连接,并且 主机 字段变成只读的。
	• 其他 不使用此选项。
	注:如果 NNMi 管理服务器参与 NNMi 应用程序故障切换,请参阅第 513 页的应用程序 故障切换和 NNMi Northbound Interface,以了解有关应用程序故障切换对集成的影响 的信息。

表 67 Netcool/OMNIbus SNMP Probe 连接信息(续)

字段	描述
端口	Netcool/OMNIbus SNMP Probe 接收 SNMP 陷阱的 UDP 端口。 输入特定于 Probe 的端口号。 要确定端口,请检查 NNMi 管理服务器上的 Probe 的 mttrapd.properties 文件。 注:此端口号必须不同于 NNMi 接收 SNMP 陷阱的端口,它是在 NNMi 控制台上的通 信配置表单的 SNMP 端口字段中设置的。
共用字符串	Netcool/OMNIbus SNMP Probe 用于接收陷阱的只读共用字符串。 如果 Probe 配置需要在所接收的 SNMP 陷阱中有特定的共用字符串,则输入该值。 如果 Probe 配置不需要特定的共用字符串,则使用默认值 public。

集成内容

表 68 列出用于配置 NNMi Integration Module for Netcool Software 将哪些内容发送到 Netcool/OMNIbus SNMP Probe 的参数。

表 68	NNMi Integration	Module for	Netcool Softwar	e 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 Netcool/OMNIbus SNMP Probe。 这是默认配置。
	 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 Probe。
	 两者 NNMi 将 NNMi 生成的管理事件和 NNMi 从被管设备接收到的 SNMP 陷阱一并转 发到 Probe。
	一旦启用目标, NNMi 就开始转发事件。
	有关详细信息,请参阅第 508 页的事件转发。

表 68	NNMi Integration Module for Netcool Software	内容配置信息	(续)
------	--	--------	-----

字段	描述
生命周期状态更改	 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态的每个事件,NNMi 会将"事件已关闭"陷阱发送到 Netcool/OMNIbus SNMP Probe。 这是默认配置。 状态已更改 对于生命周期状态更改为进行中、已完成或已关闭的每个事件,NNMi 将"事件生命 周期状态已更改"陷阱发送到 Probe。 两者 对于更改为已关闭生命周期状态的每个事件,NNMi 会将"事件已关闭"陷阱发送到 Probe。另外,对于生命周期状态的每个事件,NNMi 会将"事件已关闭"陷阱发送到 Probe。另外,对于生命周期状态更改为进行中、已完成或已关闭的每个事件,集成会 将"事件生命周期状态已更改"陷阱发送到 Probe。 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改"陷阱。 有关详细信息,请参阅第 509 页的事件生命周期状态更改通知。
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 Netcool/OMNIbus SNMP Probe。 这是默认配置。 单个 NNMi 为从 NNMi 原因分析产生的每个父子事件关联关系发送陷阱。 组 NNMi 对于列出关联到父事件的所有子事件的每个关联发送一个陷阱。 有关详细信息,请参阅第 509 页的事件关联通知。
删除	 事件删除规范。 不发送 从 NNMi 中删除事件时, NNMi 不会通知 Netcool/OMNIbus SNMP Probe。 这是默认配置。 发送 对于从 NNMi 中删除的每个事件, NNMi 会向 Probe 发送一个删除陷阱。 有关详细信息,请参阅第 510 页的事件删除通知。

表 68 NNMi Integration Module for Netcool Software 内容配置信息 (续)

字段	描述
NNMi 控制台访问	URL 中的连接协议规范,用于从 Netcool 事件查看器浏览到 NNMi 控制台。NNMi 发送到 Netcool/OMNIbus SNMP Probe 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,如果所有 Netcool 用户都在内部网上,则可以将从 Netcool 事件查看器对 NNMi 控制台的访问设置为通过 HTTP。要更改用于从 Netcool 事件查看 器连接到 NNMi 控制台的协议,请相应选择 HTTP 选项或 HTTPS 选项。
事件过滤器	 对象标识符(OID)的列表,集成据此过滤发送到 Netcool/OMNIbus SNMP Probe 的事件。每个过滤器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 将所有事件发送到 Probe。这是默认配置。 包含 NNMi 仅发送与过滤器中识别出的 OID 相匹配的特定事件。 排除 NNMi 发送所有事件,不包括与过滤器中识别出的 OID 相匹配的特定事件。 指定事件过滤器: 要添加过滤器条目,请在下部的文本框中输入文本,然后单击添加。 要删除过滤器条目,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,请参阅第 510 页的事件转发过滤器。

目标状态信息

表 69 列出 NNMi Integration Module for Netcool Software 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。

表 69 NNMi Integration Module for Netcool Software 状态信息

字段	描述
陷阱目标 IP 地址	Netcool/OMNIbus SNMP Probe 目标主机名解析而得的 IP 地址。 此值对于此 Probe 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 Netcool/OMNIbus SNMP Probe 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 Interface 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 Netcool/OMNIbus SNMP Probe 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。

xMatters (以前称 作 AlarmPoint)



xMatters 是 xMatters, inc. 的交互式警报平台,设计用于捕获和强化重要事件,将这些事件发送给使用任何通信设备的适当人员,使此人员能够解决、呈报问题或召集其他人来解决问题。

xMatters 可通过集成而成为自动化引擎或智能应用程序(如 HP Network Node Manager i Software,简称 NNMi)的语音口和接口。当 NNMi 检测到需要注意的事件时, xMatters 会安排致电或者将页面、即时消息或电子 邮件消息发送给相应的人员、供应商或客户。

xMatters 还是持久性的,它通过多个设备、通信媒体和人员呈报问题,直到有人对此负责或解决事件。xMatters 允 许收到通知的人员与 NNMi 进行即时双向通信。在 NNMi 管理服务器上会立即处理响应,从而能远程解决事件。

xMatters 移动访问 (带所有 xMatters 企业许可证)扩展了 xMatters 平台的功能,允许对关键应用程序进行移动 Web 访问。

有关购买 xMatters 和 xMatters 移动访问的信息,请联系 HP 销售代表或发送电子邮件至 sales@xmatters.com。

本章描述以下可用集成:

- HP NNMi-xMatters 集成
- HP NNMi-xMatters 移动访问集成

HP NNMi-xMatters 集成

关于 HP NNMi-xMatters 集成

通过将 xMatters 包括在 NNMi 环境中,使用 NNMi 监视和管理其网络设备的网络操作人员可获得个人通信工具和 NNMi 之间的智能警报和双向通信功能。

HP NNMi-xMatters 集成通过 NNMi 事件类型的配置支持事件通知(从 NNMi 到 xMatters)。它还支持确认原始事件、改变其优先级及添加信息批注的入站操作(从 xMatters 到 NNMi)。

每个 NNMi 管理服务器都可以与 xMatters 和 / 或 xMatters 移动访问集成。

价值

使用 HP NNMi-xMatters 集成,可以通过语音、电子邮件、呼机或其他设备直接通知相应的技术人员。事件解决者接收有关故障的信息,并能实时作出决策,如确认、忽略、批注或更改事件优先级。

收件人在其远程设备上选择响应之后, xMatters 会实时更新 NNMi 事件。该过程的好处立 竿见影 – 比起工作人员察觉故障或失灵后了解电话接听者,再人工通知适当人员,该过程 要快得多。能以简单操作从任何设备更新事件,使事件解决者能快速处理很多问题,并向其 他团队成员通知事件的当前状态。

处理期间, xMatters 记录每个通知、响应和操作。此外, xMatters 用状态信息自动批注原 始 NNMi 事件。

xMatters 产品具有基于 Web 的自助服务用户界面,用于将负责人员分配到每个作业。 xMatters 还包括允许被管和自订购 NNMi 事件的可选增强订购面板。



xMatters lite 作为 xMatters 的受限版本可用于 NNMi 选定版本。用于 HP NNMi 的 xMatters lite 功能集较小,并已针对 NNMi 集成做了预配置。 xMatters lite 是初次使用 xMatters 产品系列的较好途径。 xMatters lite 非常适合不需要语音或分布式加载功能的 小型生产环境。

集成产品

本章中的信息适用于以下产品:

• xMatters

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

- AlarmPoint Java Client
- NNMi 9.10

对于任何 xMatters 产品与 NNMi 的集成, NNMi 集成支持许可证不是必需的。

文档

HP NNMi-xMatters 集成附带的《用于 HP Network Node Manager i-series 的 AlarmPoint 集成指南》中完整描述了此集成。

xMatters 文档套件详细描述了 xMatters 功能。文档套件可从以下 xMatters 客户支持站 点下载:

https://connect.xmatters.com

《用于 HP NNMi 的 AlarmPoint Express 快速入门指南》介绍了 xMatters 功能集。此指 南描述如何安装、配置和维护 HP NNMi-xMatters lite 集成。

启用 HP NNMi-xMatters 集成

如果您计划对 NNMi 实施这两种 xMatters 集成,建议您在启用 HP NNMi-xMatters 移动访问集成之前,先启用 HP NNMi-xMatters 集成。

用于安装和配置 xMatters-NNMi 集成的高级步骤如下。有关详细信息,请参阅《用于 HP Network Node Manager i-series 的 AlarmPoint 集成指南》。

- 1 在 NNMi 管理服务器上安装 AlarmPoint Java Client。
- 2 安装 AlarmPoint Java Client 的特定于 NNMi 的集成脚本。
- 3 在 xMatters Web 服务器和应用程序服务器上安装 Web 服务库。
- 4 *可选*。在 xMatters Web 服务器上安装 NNMi 的 xMatters 订购面板。
- 5 使用 xMatters Developer IDE 安装 NNMi 的 xMatters 操作脚本。
- 6 将集成语音文件安装到 xMatters 应用程序服务器。
- 7 在 xMatters 中配置事件域 (及可选的订购域)。
- 8 配置具有 Web 服务客户端角色的 NNMi 用户。
- 9 配置应触发 xMatters 脚本的 NNMi 事件类型。

10 验证集成可以注入 xMatters 通知的 NNMi 事件参数, 并且该 xMatters 响应能正确更 新 NNMi 事件。

使用 HP NNMi-xMatters 集成

NNMi 和 xMatters 的交互方式为将通知传递给用户并将响应注入回 NNMi 中。NNMi 检测到网络中有问题 (例如, NonSNMPNodeUnresponsive 事件)时,发生以下过程:

- 1 NNMi 使用描述问题 (例如受影响的计算机和情况) 的参数调用 AlarmPoint 客户端 (APClient)。
- 2 APClient 将信息提交到 AlarmPoint Agent (APAgent)。
- 3 APAgent 确保将问题详细信息传递到 xMatters,后者又会通知相应的收件人。
- 4 收件人通过采取表 70 中列出的某个操作来响应通知。收件人的确认、批注或优先级更 改通过 Web 服务调用更新 NNMi。

操作	描述
确认	用户取得事件的所有权,避免进一步通知其他用户。 例外就是订购 FYI 通知,这些通知报告服务中断。直到问题解决 后这些通知才会停止。
忽略	停止通知当前用户。
提高优先级	在 NNMi 中将事件优先级提高一级。(仅语音)
降低优先级	在 NNMi 中将事件优先级降低一级。(仅语音)
将优先级设置为最高	将事件的优先级设置为最高。(仅电子邮件、BES 和浏览器)
将优先级设置为高	将事件的优先级设置为高。(仅电子邮件、BES 和浏览器)
将优先级设置为中	将事件的优先级设置为中。(仅电子邮件、BES 和浏览器)
将优先级设置为低	将事件的优先级设置为低。(仅电子邮件、BES 和浏览器)
批注	允许用户将消息追加到 NNMi 事件的"说明"字段。(仅对非HTML 电子邮件)

表 70 对所接收事件通知的可能响应

禁用 HP NNMi-xMatters 集成

要禁用集成,请删除由集成的可执行存档安装的组件。

有关删除 xMatters 部署的信息,请参阅 《用于 HP Network Node Manager i-series 的 AlarmPoint 集成指南》。

对 HP NNMi-xMatters 集成进行故障诊断

有关优化和扩展集成的信息以及任何当前已知问题,请参阅《用于 HP Network Node Manager i-series 的 AlarmPoint 集成指南》。

HP NNMi-xMatters 移动访问集成

关于 HP NNMi-xMatters 移动访问集成

通过在 NNMi 环境中包括 xMatters 移动访问,网络操作人员可在移动设备的 Web 浏览器 中与 NNMi 事件交互。

每个 NNMi 管理服务器都可以与 xMatters 和 / 或 xMatters 移动访问集成。

价值

使用 HP NNMi-xMatters 移动访问集成, NNMi 操作员可以在移动设备上使用 Web 浏览 器与 NNMi 事件实时交互:

- 查询 NNMi 的当前事件
- 查看事件的详细信息
- 修改属性,如事件的状态、生命周期状态或分配的 NNMi 操作员

集成产品

本章中的信息适用于以下产品:

- xMatters 移动访问
- -

有关受支持版本的列表,请参阅 NNMi 系统和设备支持列表。

- xMatters 集成代理
- NNMi 9.10

对于任何 xMatters 产品与 NNMi 的集成, NNMi 集成支持许可证不是必需的。

文档

HP NNMi-xMatters 移动访问集成附带的《用于 HP Network Node Manager i-series Software 的 AlarmPoint Mobile Gateway 集成指南》中完整描述了此集成。

xMatters 文档套件详细描述了 xMatters 功能。文档套件可从以下 xMatters 客户支持站 点下载:

https://connect.xmatters.com

启用 HP NNMi-xMatters 移动访问集成

如果您计划对 NNMi 实施这两种 xMatters 集成,建议您在启用 HP NNMi-xMatters 移动访问集成之前,先启用 HP NNMi-xMatters 集成。请参阅第 593 页的启用 HP NNMi-xMatters 集成。

用于安装和配置 NNMi 集成的 xMatters 移动访问的高级步骤如下。有关详细信息,请参 阅《用于 HP Network Node Manager i-series Software 的 AlarmPoint Mobile Gateway 集成指南》。

如果为 NNMi 的更早版本配置了 HP NNMi 朅 larmPoint 集成,则可以将 NNMi 9.0x 升 级到 NNMi 9.10 而不会影响集成配置。验证 xMatters 版本是否是 4.0 或更高版本。

- 1 在 xMatters 服务器上安装 xMatters Integration Agent。
- 2 在 xMatters Integration Agent 和 Web 服务器上安装 Web 服务库。
- 3 在 xMatters Web 服务器上安装 xMatters 移动访问。
- 4 安装 NNMi 集成服务。
- 5 创建具有 Web 服务客户端角色的 NNMi 用户。
- 6 在 xMatters 中配置事件域 (如果尚未配置 HP NNMi-xMatters 集成) 和集成服务。
- 7 验证 xMatters 移动访问和 NNMi 之间的交互性。

使用 HP NNMi-xMatters 移动访问集成

使用 HP NNMi-xMatters 移动访问集成,可对移动 Web 浏览器中的事件执行以下操作:

- 添加说明
- 更新优先级
- 更新生命周期状态
- 更新"分配给"操作员
- 查看多数事件详细信息(由 xMatters 移动访问管理员提供)
- 显示源对象和节点的快速视图。

有关使用集成的详细信息,请参阅《用于 HP Network Node Manager i-series Software 的 AlarmPoint Mobile Gateway 集成指南》和《xMatters (alarmpoint)移动访问指南》。

禁用 HP NNMi-xMatters 移动访问集成

要禁用集成,请删除由集成的可执行存档安装的组件。

有关删除 xMatters 移动访问部署的信息,请参阅《用于 HP Network Node Manager i-series Software 的 AlarmPoint Mobile Gateway 集成指南》。

对 HP NNMi-xMatters 移动访问集成进行故障诊断

有关优化和扩展集成的信息以及任何当前已知问题,请参阅《用于 HP Network Node Manager i-series Software 的 AlarmPoint Mobile Gateway 集成指南》。



本部分包含以下附录:

- NNMi 环境变量
- NNMi 9.10 和已知端口
- 建议的配置更改

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
- 其他可用环境变量

本文档中使用的环境变量

本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 2008:
 - %NnmInstallDir%: < 驱动器 >\Program Files\HP\HP BTO Software
 - %NnmDataDir%:<*驱动器*>\ProgramData\HP\HP BTO Software

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。

如果首先安装了 NNMi 8.00,则系统对这些环境变量使用不同的值,如第 604 页的中 所述。

• UNIX:

- \$NnmInstallDir: /opt/OV
- \$NnmDataDir: /var/opt/OV



在 UNIX 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,您可将这些环境变量用作 NNMi 管理服务器上用户登录 配置的一部分根据。这些变量形式为 NNM_*。有关该 NNMi 环境变量扩展列表的信息,请参阅第 601 页的其他可用环境变量。

其他可用环境变量

NNMi 管理员定期访问某些 NNMi 文件位置。 NNMi 提供的脚本可用于设置很多环境变量,

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\HP\HP BTO Software\bin\nnm.envvars.bat"
- UNIX: /opt/OV/bin/nnm.envvars.sh

运行操作系统命令之后,可以使用表 71 (Windows) 或表 72 (UNIX) 中显示的 NNMi 环境 变量,以获得常用的 NNMi 文件位置。

表 71 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\nnm\ bin\java.exe
%NNM_JAVA_DIR%	C:\Program Files (x86)\HP\HP BTO Software\java
%NNM_JAVA_PATH_SEP%	;
%NNM_JBOSS%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jboss\nms
%NNM_JBOSS_DEPLOY%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jboss\nms\ server\nms\deploy
%NNM_JBOSS_LOG%	C:\Program Files (x86)HP\HP BTO Software\nonOV\jboss\nms\ server\nms\log
%NNM_JBOSS_ROOT%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jboss\nms
%NNM_JBOSS_SERVERCONF%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jboss\nms\ server\nms
%NNM_JRE%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jdk\nnm
%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
%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_SUPPORT%	C:\Program Files (x86)\HP\HP BTO Software\support

表 71 Windows 操作系统的环境受重新认证直(:系统的坏境受重新认位直 (缤)
-----------------------------	------------------

变量	Windows (示例)
%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

表 72 UNIX 操作系统的环境变量默认位置

变量	HP-UX
\$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/nnm/bin/java
\$NNM_JAVA_DIR	/opt/OV/java
\$NNM_JAVA_PATH_SEP	:
\$NNM_JBOSS	/opt/OV/nonOV/jboss/nms
\$NNM_JBOSS_DEPLOY	/opt/OV/nonOV/jboss/nms/server/nms/deploy
\$NNM_JBOSS_LOG	/opt/OV/nonOV/jboss/nms/server/nms/log
\$NNM_JBOSS_ROOT	/opt/OV/nonOV/jboss/nms
\$NNM_JBOSS_SERVERCONF	/opt/OV/nonOV/jboss/nms/server/nms
\$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_SUPPORT	/opt/OV/support
\$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 9.10 和已知端口

表 73 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.port.4 参考页或 UNIX 联机帮助页。



为使应用程序故障切换成功,打开 TCP 端口 7800-7810。为了让应用程序故障切换功能正常运行,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。

表 73 在 NNMi 管理服务器上使用的端口

端口	类型	名称	目的	更改配置
80	TCP	jboss.http.port	默认 HTTP 端口 - 用于 Web UI 和 Web 服务	修改 nms-local.properties 文件 还可以在安装期间更改此配置
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 <i>nnmtrapconfig.ovpl</i> 参考页 或 UNIX 联机帮助页。
443	TCP	jboss.https.port	默认安全 HTTPS 端口 (SSL) - 用于 Web UI 和 Web 服务	修改 nms-local.properties 文件
1098	TCP	jboss.rmi.port	RMI 命名服务的默认端口	修改 nms-local.properties 文件
1099	ТСР	jboss.jnp.port	默认启动 JNP 服务端口 (JNDI 提供程序)	修改 nms-local.properties 文件
3873	ТСР	jboss.ejb3.port	默认 EJB3 远程连接器端口	修改 nms-local.properties 文件
4444	TCP	jboss.jrmp.port	默认 RMI 对象端口 (JRMP 调用程序)	修改 nms-local.properties 文件
4445	тср	jboss.pooled.port	默认 RMI 池调用程序端口	修改 nms-local.properties 文件

表 73 在 NNMi 管理服务器上使用的端口(续)

端口	类型	名称	目的	更改配置	
4446	тср	jboss.socket.port	默认 RMI 远程服务器连接器 端口	修改 nms-local.properties 文件	
4457	ТСР	jboss.bisocket.port	默认消息传送双套接字连接器	修改 nms-local.properties 文件	
4458	TCP	jboss.jmsControl.port	默认 JMS 控制端口;用于全局 网络管理通信	修改 nms-local.properties 文件	
4459	TCP	jboss.sslbisocket.port	默认消息传送双套接字连接器; 用于保护全局网络管理通信	修改 nms-local.properties 文件	
4460	TCP	jboss.ssljmsControl.port	默认 JMS 控制端口;用于保护 全局网络管理通信	修改 nms-local.properties 文件	
5432	TCP		Postgres 端口	不可配置	
7800- 7810	ТСР		用于应用程序故障切换的 JGroups 端口	修改 nms-cluster.properties 文件	
8083	тср	jboss.ws.port	默认 jboss Web 服务端口	修改 nms-local.properties 文件	
8886	ТСР	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	

表 74 显示 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,则需要在防火墙 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。

表 74	用于 NNMi	管理服务器及其他系统之间通信的端口
------	---------	-------------------

端口	类型	目的	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
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

2011年3月

表 74 用于 NNMi 管理服务器及其他系统之间通信的端口(续)

端口	类型	目的	客户端,服务器
162	UDP	SNMP 陷阱端口;陷阱转发、Northbound Interface 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。	客户端
		Windows 上 HP OM 的默认 HTTPS 端口	
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	默认消息传送双套接字连接器,用于全局网络管理通信。连接从全局管理器 到区域管理器。	客户端,服务器
4458	TCP	默认 JMS 控制端口,用于全局网络管理通信。连接从全局管理器到区域管理器。	客户端,服务器
4459	ТСР	默认消息传送双套接字连接器,用于保护全局网络管理通信。连接从全局管 理器到区域管理器。	客户端,服务器
4460	TCP	默认 JMS 控制端口,用于保护全局网络管理通信。连接从全局管理器到区域管理器。	客户端,服务器
7800- 7810	TCP	用于应用程序故障切换的 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 的默认 HTTP 端口。	客户端
		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 for Performance 的默认 HTTP 端口	客户端
50000	TCP	连接到 SIM 的默认 HTTPS 端口	客户端

如果将 NNMi 配置为使用 ICMP 故障轮询或 Ping 扫描进行搜索,则将防火墙配置为使 ICMP 数据包通过防火墙。

NNMi-HP OM 集成的 Web 服务途径不能通过防火墙工作,但使用 Northbound Interface 的 NNMi-HP OM 集成能通过防火墙工作。

如果计划使用全局网络管理功能,则表 75 显示了必须能从全局 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 回全局 NNMi 管理服务器的套接字。

表 75 全局网络管理要求可访问套接字

	安全性	参数		TCP 端口
# SSL		jboss.http.port	80	
		jboss.bisocket.port	4457	
		jboss.jmsControl.port	4458	
SSL		jboss.https.port	443	
		${ m jboss.sslbisocket.port}$	4459	
		${\rm jboss.ssljmsControl.port}$	4460	

建议的配置更改

某些改进性能的常见操作及如何完成它们。

消息和解决方案

消息: 数据库池具有数字个可用连接。

解决方案:这是一则警告,表示数据库池利用率过高。如果这只显示一段较短时间,则它可能 表示 NNMi 负载高。如果它频繁出现,则可能表示有性能问题。

消息: 数据库连接池耗尽。应当立即重新启动 NNM。

解决方案:这是严重错误,表明数据库池已由于某些原因失败,并且 NNMi 无法访问数据库。 需要重新启动 ovjboss 或联系支持人员以解决问题。

消息: 检测到数字个数据库连接缺失。应在稍后重新启动 NNM 以校正此问题。

解决方案:这是一则警告,表明 NNMi 在数据库池中检测到不一致。在方便时重新启动 ovjboss 以解决此问题。

消息:该磁盘位置*位置名称*只有*数字*%可用。

解决方案: NNMi 使用的磁盘位置空间不足时, NNMi 显示此警告。

消息: 平均系统负载为数字。

解决方案:系统负载超过阈值后,NNMi显示此警告。如果该消息在主要活动期间偶尔显示,则可以忽略。但是,如果它经常显示,您需要调查系统是否无法承载环境规模,或者系统上是否有其他进程在大量消耗资源。

消息: 系统的交换空间少, 剩余数字 MB。

解决方案: NNMi 检测到系统在交换空间过低状况下运行后, NNMi 显示此消息。应增加可用 交换空间或减少交换空间的使用。 消息: NNMi 进程目前正在使用允许的打开文件数的数字%。

解决方案:此消息表示 NNMi 即将用完文件句柄。预期 1000 个以内的文件可一次打 开,但某些环境可能要求一次打开更多。但是,如果打开文件的句柄数持续增长,则可 能表示产品中有缺陷。

消息: NNMi CPU 利用率为 100%。

解决方案: 这表示 ovjboss 进程在相当长的时间内占用了系统上 100% 的 CPU。对于 短时间的高负载,这可能是预期的,但如果此警告经常出现,则可能是系统没有能力处 理此负载。

消息: 全局管理器 主机名 有 数字 条未决消息等待传递。

解决方案: 它表示连接到此系统的全局管理器关闭或无法足够快地接收消息。如果全局 管理器只是关闭以供维护,则应在它重新联机时恢复,但是如果此数字超过几十万,则 可能需要手动清除它(联系支持人员)。

消息: 与区域管理器区域名称的连接断开。

解决方案: 与区域管理器的通信中断时出现的警告消息。如果此消息显示时间较短,则 无须担心; 但如果该消息显示了较长时间,则可能需要进行故障诊断。此状况存在时, 全局管理器不会从区域接收任何状态更改。

消息: 对于嵌入式数据库, 目前最多有数字个 (共数字个) 连接打开。

解决方案:此消息警告您,嵌入式数据库 NNMi 使用的连接正接近其打开连接数限制。 这可能表示系统负载过高,或安装了太多 SPI。建议在此数字达到最大值之前,执行关 闭 SPI 之类的操作。

消息:内存区域区域名称利用率为数字%。

消息:系统在采集器名称采集器中花费了数字%的总运行时间。

解决方案:这两条消息表示 ovjboss 内存不足。应根据为该环境规模推荐的设置检查 指定区域的内存设置,并且如果系统有可用内存,则增加该区域的内存。

问题和解决方案

问题: NNMi 不能始终正确解释和显示 SNMP 数据及 MIB 字符串。

解决方案: 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 陷阱及其他 octetstring 数据的乱码字符串,如 sysDescription、sysContact 及其他数据。解决方案是使用正确字符集解释此数据。

对于由于使用不正确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:

- a 编辑以下文件:
 - Windows: %NNM PROPS%\nms-jboss.properties
 - UNIX: \$NNM_PROPS/nms-jboss.properties
- **b** 从如下开始的行删除注释 (#!字符): #!com.hp.nnm.sourceEncoding=
- c 使用在 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。
- d 保存更改。
- e 从命令提示符,运行 ovstop ovjboss。
- f 从命令提示符,运行 ovstart ovjboss。
- g 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 编辑以下文件:
 - Windows: %NNMDATADIR%\shared\nnm\conf\nnmvbnosrcenc.conf
 - UNIX: \$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 从命令提示符,运行 ovstop ovjboss。
- e 从命令提示符,运行 ovstart ovjboss。
- f 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。

问题: 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

解决方案: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,就会发生这种情况。解决方案是删除无效的许可证密钥:

1 在命令提示符下,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 NMM 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,请参阅第 115 页的许可 NNMi。

问题: 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。NNMi 显示由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,它才构成一个问题。

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搜索配置。
- 4 单击"自动搜索规则"选项卡。
- 5 创建新的自动搜索规则。
- 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。切勿选中搜索包含的节 点复选框。
- 7 为此规则添加新的 IP 地址范围。
- 8 对于表示 ESXi 服务器以及在其上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。

这些步骤不会删除任何现有节点;但是,它将阻止未来对所排除 IP 地址范围内的节点的搜索。
问题: NNMi 图显示 Linux 服务器而不是 ESXi 服务器和节点。

解决方案: 已经在已启用 Net-SNMP 代理的 Linux 服务器上部署了 VMWARE。如果 希望 NNMi 搜索并显示 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。

问题: 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 才能搜索和映射 ESXi 服务器 及节点。也许您卸载或禁用了 ESXi SNMP 代理。为纠正此问题,请安装或启用 ESXi SNMP 代理。有关详细信息,请访问 http://www.vmware.com。

问题: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。

解决方案: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。
- 为以下节点组在节点组图设置 -> 连通性 -> 节点组连通性部分中选择以下任一选择或这两个选择:
 - 节点到节点组
 - 节点组到节点组

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 -> 连通性 -> 节点组连通性部分中的节点到节点组和 / 或节点组到节点组。

词汇表

Α

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。在基于规则的搜索中,NNMi 在搜索的节点上使用 ARP 缓存条目(以及其他技术)查找可对照当前搜索规则检查的其他节点。请参阅搜索提示。

B

播种搜索

请参阅基于列表的搜索。

D

地址提示

请参阅搜索提示。

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通性的信息。

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通性的信息。

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。

断开的接口

从 NNMi 的角度理解, 断开的接口就是未连接到 NNMi 所搜索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。

对象标识符

SNMP 中用于标识 MIB 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,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.

G

高可用性

在本指南中是指一种硬件和软件配置,用来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,也能保持应用程序的运行。可将 NNMi 配置为支持若干商业上可用的 HA 解决方案之一。与应用程序故障切换相对照。

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 的示例情形: 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不能再响应状态轮询查询。 NNMi 用 RCA 确定状态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

属性*关联性质*设置为*根源*的 NNMi 事件。NNMi 使用 根源分析 (RCA) 建立根源事件,作为找到相关问题症状 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。用于确认公钥属于某个人或组织的证书。NNMi使用 SSL 证书,这些证书包含公钥和私钥,用于客户端-服务器通信的身份验证和加密。

共用字符串

SNMPv1 和 SNMPv2c 实现中使用的一种类似密码的 机制,用于 SNMP 代理对 SNMP 查询的验证。SNMP 数据包中以明文形式传递共用字符串,使得它容易受到 数据包嗅探的攻击。SNMPv3 提供用于身份验证的更强 安全机制。

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态。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。故障轮询是状态轮询的子集。

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指向被管设备的特征。 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。

规则

请参阅搜索规则。

Η

HA

请参阅高可用性。

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搜索、监视事件和网络故障管理。主要从 NNMi 控制台访问。

活动服务器

在应用程序故障切换或高可用性配置中当前运行 NNMi 进程的服务器。

I

ICMP

请参阅 Internet 控制消息协议。

Internet 控制消息协议

Internet 协议组 (TCP/IP) 的核心协议之一。 ICMP Ping 由 NNMi 和状态轮询的 SNMP 查询一起使用。

iSPI

请参阅 NNM iSPI。

J

基于规则的搜索

通常称为*自动搜索*, NNMi 可以使用基于规则的搜索, 根据用户指定的搜索规则来查找 NNMi 应添加到其数 据库的节点。NNMi 从已搜索节点的数据中查找搜索提 示,然后根据指定搜索规则检查这些候选项。在 NNMi 控制台的**搜索配置**部分的自动搜索规则下,配置搜索规则。与基于列表的搜索相对照。

基于列表的搜索

基于种子列表的进程,它搜索并返回*仅关于指定为种子的节点*的详细网络信息。基于列表的搜索为特定查询和 任务维护有限的网络资产。与基于规则的搜索相对照。 另请参阅搜索过程和螺旋搜索。

2011年3月

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 络管理信息的主导性协议。 NNMi 支持三个最常见的 SNMP 版本: SNMPv1、SNMPv2c 和 SNMPv3。

角色

请参阅用户角色。

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,在此期间次要故障被抑制或关联 在主故障下。

接口

用于将节点连接到网络的物理端口。

接口组

NNMi 的主要过滤技术之一,将接口分组,以便将设置应用于组或按组过滤可见性。接口组可用于以下任一或 全部操作:配置监视、过滤表视图,以及自定义图视图。 另请参阅节点组。

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 的主要过滤技术之一,将节点分组,以便将设置应用到组或按组过滤可见性。节点组可用于以下任一或全部操作:配置监视、过滤表视图,以及自定义图视图。 另请参阅接口组。

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。

Κ

控制器

在 NNMi 应用程序故障切换中,用于具有主群集状态的群集成员的 JGroups 术语。控制器总是群集的最早成员。

控制台

请参阅 NNMi 控制台。

L

L2

请参阅第2层。

L3

请参阅第3层。

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。

螺旋搜索

NNMi的持续改进的网络拓扑信息,包括有关 NNMi管理的网络中资产、包含、关系和连通性的信息。另请参阅搜索过程、基于规则的搜索和基于列表的搜索。

Μ

MIB

请参阅管理信息库。

Ν

NNM 6.x/7.x 事件

用于从早先的 NNM 管理工作站转发到 NNMi 的事件 的 NNMi 术语。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

ICMP 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

请参阅 HP Network Node Manager i Software。

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。

0

OID

请参阅对象标识符。

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。

Ρ

Ping 扫描

一种网络探查技术,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。在基于规则的搜索中启用时, 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放源关系数据库。NNMi 对其多数表还可以配置为使用 Oracle 而非 PostgreSQL。

Q

嵌入式数据库

NNMi 附带的数据库。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。

区域

NNMi 中的设备分组,用于配置超时值和访问凭证之类的通信设置。

全局网络管理部署中的 NNMi 管理服务器,它提供设备 搜索、轮询和陷阱接收,并将信息转发到全局管理器。

全局管理器

区域管理器

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 障切换。

R

RCA

请参阅根源分析。

S

SNMP

请参阅简单网络管理协议。

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 代理针对内部状态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。

sysObjesctID

请参阅系统对象 ID。

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过滤 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。

搜索规则

用户定义的 IP 地址和 / 或系统对象 ID (RCA) 的范围, 用于限制基于规则的搜索过程。在 NNMi 控制台的搜索 配置部分的自动搜索规则下,配置搜索规则。另请参阅基 于规则的搜索。

搜索过程

NNMi 采集有关网络节点的信息以使其能处于被管状态的过程。初始搜索作为两阶段的过程运行,返回设备资产信息,然后返回网络连通性信息。

初始搜索之后,搜索过程持续进行。在基于列表的搜索 中,这意味着如果种子列表中的设备的配置更改,则将 会更新设备。在基于规则的搜索中,如果新设备匹配当 前搜索规则,也会添加它们。对设备或设备组的搜索也 可以根据需要从 NNMi 控制台或命令行启动。

另请参阅螺旋搜索、基于规则的搜索和基于列表的 搜索。

搜索提示

NNMi 使用 SNMP ARP 缓存查询搜索的 IP 地址; CDP、EDP 或其他搜索协议查询;或 Ping 扫描。 NNMi 进一步查询作为搜索提示的 IP 地址,然后根据 基于规则的搜索中当前的搜索规则检查结果。

搜索种子

请参阅种子。

Τ

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。

Х

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 MIB 对象的一部分,搜索期间由 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。与用户帐户相对照。

陷阱

请参阅 SNMP 陷阱。

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切换或负载平衡需要,将连续的网络通信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。

Y

应用程序故障切换

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。用户角色确定哪 些用户帐户可以访问 NNMi 控制台,以及哪些工作区和 操作对每个用户帐户可用。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,提供给用户或用户组用于访问 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,包括由于状态轮询、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 出有关它们的总结,并生成根源事件。

Ζ

帐户

请参阅用户帐户。

种子

通过充当网络搜索过程的起点,帮助 NNMi 搜索网络的 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 规则的搜索,否则 NNMi 的搜索过程限于指定的种子的 基于列表的搜索。

主动群集节点

请参阅活动服务器。

状态

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**状态**。与状态相对照。

状态

在 NNMi 中,表示其总体状况的被管对象属性。状态 由播种搜索根据被管对象的未决总结来计算。与状态相 对照。

状态轮询

由 NNMi 的状态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。

自动搜索

请参阅基于规则的搜索。

总结

在 NNMi 中由播种搜索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。

感谢您的反馈!

如果在此系统上配置了电子邮件客户端,默认情况下单击*此处*时将打开电子邮件窗口。 如果没有电子邮件客户端可用,请将以下信息复制到 Web 邮件客户端中的新邮件中,然后 将此邮件发送到 ovdoc-nsm@hp.com。

产品名称和版本: NNMi 9.10

文档标题: 《NNMi 部署参考》 反馈:



