

远程管理参考手册

Novell. ZENworks® 10 Configuration Management SP3

10.3

2010年3月30日

www.novell.com



法律声明

Novell, Inc. 对本文档的内容或使用不作任何声明或保证，特别是对适销性或用于任何特定目的的适用性不作任何明示或暗示保证。另外，Novell, Inc. 保留随时修改本出版物及其内容的权利，并且没有义务将这些修改通知任何个人或实体。

Novell, Inc. 对任何软件不作任何声明或保证，特别是对适销性或用于任何特定目的的适用性不作任何明示或暗示保证。另外，Novell, Inc. 保留随时修改 Novell 软件全部或部分内容的权利，并且没有义务将这些修改通知任何个人或实体。

依据本协议提供的任何产品或技术信息都将受到美国出口控制和其他国家 / 地区的贸易法律的约束。您同意遵守所有出口控制法规，并同意在出口、再出口或进口可交付产品之前取得所有必要的许可证或分类证书。您同意不出口或再出口至当前美国出口排除列表上所列的实体，或者美国出口法律中规定的任何被禁运的国家 / 地区或支持恐怖主义的国家 / 地区。您同意不将可交付产品用于禁止的核武器、导弹或生物化学武器的最终用途。有关出口 Novell 软件的详细讯息，请访问 [Novell International Trade Services 网页 \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/)。如果您未能获得任何必要的出口许可，Novell 对此不承担任何责任。

版权所有 © 2007-2010 Novell, Inc. 保留所有权利。未经出版商的明确书面许可，不得复制、影印、传送此出版物的任何部分或将其储存在检索系统上。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

联机文档: 要访问该 Novell 产品及其他 Novell 产品的最新联机文档，请参见 [Novell 文档网页 \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/)。

Novell 商标

有关 Novell 商标，请参见 [Novell 商标和服务标记列表 \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html)。

第三方资料

所有第三方商标均属其各自所有者的财产。

目录

关于本指南	9
1 概述	11
1.1 远程管理术语	11
1.2 了解远程管理操作	12
1.2.1 远程控制	12
1.2.2 远程查看	13
1.2.3 远程执行	13
1.2.4 远程诊断	13
1.2.5 文件传送	13
1.2.6 远程唤醒	14
1.3 了解远程管理功能	14
1.3.1 可见信号	14
1.3.2 入侵者检测	14
1.3.3 会话加密	14
1.3.4 哔声	14
1.3.5 键盘和鼠标锁定	14
1.3.6 屏幕消隐	15
1.3.7 异常终止	15
1.3.8 覆盖屏幕保护程序	15
1.3.9 自动终止会话	15
1.3.10 代理启动的连接	15
1.3.11 会话协作	15
1.3.12 远程管理审计	15
1.4 了解远程管理代理	16
2 设置远程管理	17
2.1 配置远程管理设置	17
2.1.1 在区域级别配置远程管理设置	17
2.1.2 在文件夹级别配置远程管理设置	19
2.1.3 在设备级别配置远程管理设置	19
2.2 启用远程管理侦听程序	20
2.3 创建远程管理策略	20
2.4 配置远程操作员权限	25
2.5 配置远程管理口令	26
2.5.1 使用 ZENworks 控制中心设置远程管理口令	26
2.5.2 使用 ZENworks Adaptive Agent 设置远程管理口令	26
2.5.3 使用 ZENworks 控制中心清除远程管理口令	27
2.5.4 使用 ZENworks Adaptive Agent 清除远程管理口令	27
2.6 安装远程管理查看器	27
2.7 升级远程管理查看器	28
2.8 启动远程管理操作	29
2.8.1 从管理控制台启动会话	29
2.8.2 从受管设备启动会话	35
2.9 用于启动远程管理操作的选项	37
2.9.1 用于启动远程操作的命令行选项	37
2.9.2 用于启动远程操作的内部选项	39
2.10 安装远程管理代理	39
2.11 配置远程管理代理	40

2.11.1	Windows 设备上的远程管理代理设置	41
2.11.2	Linux 主服务器或从属服务器上的远程管理代理设置	41
3	管理远程会话	43
3.1	管理远程控制会话	43
3.1.1	使用远程管理查看器中的工具栏选项	43
3.1.2	会话协作	45
3.2	管理远程查看会话	46
3.3	管理远程执行会话	47
3.4	管理远程诊断会话	47
3.5	管理文件传送会话	48
3.6	管理远程管理代理会话	51
3.7	唤醒远程设备	51
3.7.1	前提条件	51
3.7.2	远程唤醒受管设备	51
3.8	提高远程管理性能	52
3.8.1	在管理控制台上	52
3.8.2	在受管设备上	52
4	安全性	53
4.1	鉴定	53
4.1.1	基于权限的远程管理鉴定	53
4.1.2	基于口令的远程管理鉴定	53
4.2	口令强度	54
4.3	端口	54
4.4	Audit	55
4.5	征得受管设备上用户的许可	55
4.6	异常终止	55
4.7	入侵者检测	56
4.7.1	自动取消阻止远程管理服务	56
4.7.2	手动取消阻止远程管理服务	56
4.8	远程操作员标识	56
4.9	浏览器配置	57
4.10	会话安全性	57
4.10.1	SSL 握手	57
4.10.2	重新生成证书	57
5	查错	59
A	密码细节	67
A.1	受管设备密钥对细节	67
A.2	远程操作员密钥对细节	67
A.3	远程管理票据细节	68
A.4	会话加密细节	68
B	最佳实践	69
B.1	关闭远程管理侦听程序	69
B.2	关闭在远程执行操作期间起动的应用程序	69
B.3	在受管设备上识别远程操作员	69
B.4	在已通过“远程桌面连接”连接的设备上执行远程控制会话	70

B.5	确定管理控制台名称	70
B.6	在 Windows Vista、Windows 7、Windows Server 2008 和 Windows Server 2008 R2 设备上使用 Aero 主题	70
B.7	远程控制 Windows Vista 或 Windows Server 2008 设备时启用安全警告序列 (Ctrl+Alt+Del) 按钮	70
B.8	在 Windows XP 设备上通过 RDP 安装远程管理服务	71
B.9	远程管理性能	71
C	文档更新	73
C.1	2010 年 3 月 30 日: SP3 (10.3)	73

关于本指南

本《Novell ZENworks 10 Configuration Management Remote Management 参考手册》包含有关“远程管理”的信息。本指南中信息的组织结构如下：

- ◆ 第 1 章“概述”（第 11 页）
- ◆ 第 2 章“设置远程管理”（第 17 页）
- ◆ 第 3 章“管理远程会话”（第 43 页）
- ◆ 第 4 章“安全性”（第 53 页）
- ◆ 第 5 章“查错”（第 59 页）
- ◆ 附录 A“密码细节”（第 67 页）
- ◆ 附录 B“最佳实践”（第 69 页）
- ◆ 附录 C“文档更新”（第 73 页）

适用对象

本指南的适用对象为 Novell® ZENworks® 管理员。

反馈

我们期待听到您对本手册和本产品中包含的其他文档的意见和建议。请使用联机文档每页底部的“用户意见”功能，或转到 [Novell 文档反馈站点 \(http://www.novell.com/documentation/feedback.html\)](http://www.novell.com/documentation/feedback.html) 并在其中输入您的意见。

其他文档

ZENworks Configuration Management 还有其他两种采用 PDF 和 HTML 格式的支持文档，可供您了解并实施本产品。有关其他文档，请参见 [ZENworks 10 Configuration Management SP3 文档 \(http://www.novell.com/documentation/zcm10/\)](http://www.novell.com/documentation/zcm10/)。

文档约定

在 Novell 文档中，大于号 (>) 用于分隔步骤内的操作和交叉参照路径中的项目。

商标符号 (®、™ 等) 代表一个 Novell 商标。星号 (*) 表示第三方商标。

在书写单一路径名时一些平台使用反斜杠而另一些平台使用正斜杠，但在本文档中路径名一律使用反斜杠。要求使用正斜杠的平台（例如 linux*）用户应根据软件的要求使用正斜杠。

概述

Novell® ZENworks® Configuration Management 可让您通过管理控制台远程管理设备。远程管理允许：

- ◆ 远程控制受管设备
- ◆ 远程运行受管设备上的可执行文件
- ◆ 在管理控制台和受管设备之间传送文件
- ◆ 诊断受管设备发生的问题
- ◆ 远程唤醒断电的受管设备

请查看以下各节：

- ◆ [第 1.1 节“远程管理术语”](#)（第 11 页）
- ◆ [第 1.2 节“了解远程管理操作”](#)（第 12 页）
- ◆ [第 1.3 节“了解远程管理功能”](#)（第 14 页）
- ◆ [第 1.4 节“了解远程管理代理”](#)（第 16 页）

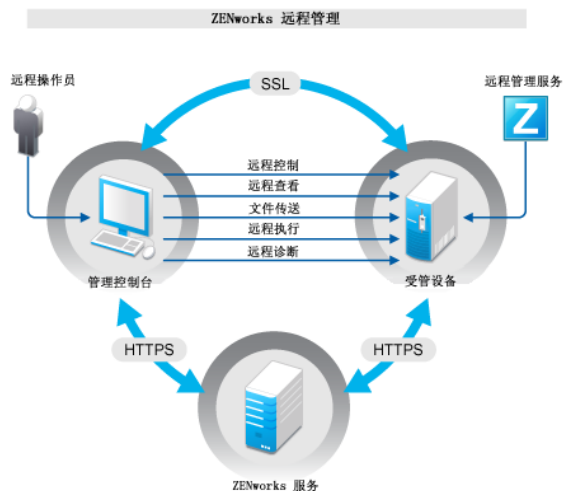
1.1 远程管理术语

术语	说明
受管设备	要对其进行远程管理的设备。要远程管理设备，请确保设备上已安装“远程管理”组件，且“远程管理”服务正在运行。
管理服务器	安装了 ZENworks Configuration Management 服务器的设备。
管理控制台	用于管理设备的界面。要执行远程操作，您必须在控制台上安装“远程管理”查看器。
管理员	可以配置“远程管理”策略和设置，以及将“远程管理”权限授予远程操作员的用户。
远程管理服务	可以让远程操作员在设备上执行远程操作的受管设备组件。
远程管理查看器	可以让远程操作员在受管设备上执行远程操作的管理控制台应用程序。可让远程操作员查看受管设备桌面、传送文件以及执行受管设备上的应用程序。
远程管理侦听程序	管理控制台应用程序，可以让远程操作员接受受管设备用户所发出的远程协助请求。
远程管理代理	可将“远程管理”操作请求从“远程管理查看器”转发给受管设备的代理服务器。当查看器无法直接访问位于专用网络内或使用 NAT（网络地址转换）的防火墙或路由器另一侧的受管设备时，该代理会非常有用。作为先决条件，Windows 受管设备或 Linux 设备（主服务器、从属设备）上必须安装该代理。

1.2 了解远程管理操作

“远程管理”可让管理员无需实地访问即可控制设备，因而节省了您及贵公司的时间和成本。例如，您或您企业的咨询台人员无需访问用户的工作站便可对受管设备出现的问题进行分析和远程修复，从而缩短问题的解决时间，提高工作效率。

图 1-1 远程管理操作



以下各节可帮助您了解各种“远程管理”操作：

- ◆ 第 1.2.1 节“远程控制”（第 12 页）
- ◆ 第 1.2.2 节“远程查看”（第 13 页）
- ◆ 第 1.2.3 节“远程执行”（第 13 页）
- ◆ 第 1.2.4 节“远程诊断”（第 13 页）
- ◆ 第 1.2.5 节“文件传送”（第 13 页）
- ◆ 第 1.2.6 节“远程唤醒”（第 14 页）

1.2.1 远程控制

“远程控制”可让您通过管理控制台远程控制受管设备，以此提供用户协助并帮助解决设备问题。

“远程控制”会在管理控制台和受管设备之间建立连接。通过远程控制连接，您可以执行用户能够在设备上执行的所有操作。有关详细信息，请参见第 3.1 节“管理远程控制会话”（第 43 页）。

1.2.2 远程查看

“远程查看”可让您远程连接受管设备以查看受管设备，但无法对其实施控制。这将帮助您查出用户遇到的问题。例如，可以观察受管设备上的用户如何执行特定任务，以确保用户的执行方式正确。有关详细信息，请参见第 3.2 节“管理远程查看会话”（第 46 页）。

1.2.3 远程执行

“远程执行”可让您以系统特权通过管理控制台运行受管设备上的任何可执行文件。要远程执行应用程序，请在“远程执行”窗口指定可执行文件名。例如，可以执行 `regedit` 命令，在受管设备上打开“注册表编辑器”。有关详细信息，请参见第 3.3 节“管理远程执行会话”（第 47 页）。

1.2.4 远程诊断

“远程诊断”可让您远程诊断和分析受管设备上出现的问题。如此通过让桌面保持正常运行即可提高用户的工作效率。有关详细信息，请参见第 3.4 节“管理远程诊断会话”（第 47 页）。

“诊断”功能会提供可用于诊断和修复受管设备问题的实时信息。受管设备上默认的诊断应用程序包括：

- ◆ 系统信息
- ◆ 计算机管理
- ◆ 服务
- ◆ 注册表编辑器

1.2.5 文件传送

“文件传送”可让您在管理控制台和受管设备上执行各种文件操作，例如：

- ◆ 在管理控制台和受管设备之间复制文件
- ◆ 重命名文件或文件夹
- ◆ 删除文件或文件夹
- ◆ 创建文件夹
- ◆ 查看文件和文件夹的属性
- ◆ 在管理控制台上以关联的应用程序打开文件

有关详细信息，请参见第 3.5 节“管理文件传送会话”（第 48 页）。

重要：“文件传送”程序可让您访问受管设备上的网络驱动器。

1.2.6 远程唤醒

如果网络中某个节点或一组断电节点上的网卡启用了网络唤醒功能，则可通过“网络唤醒”远程唤醒这些节点。有关详细信息，请参见第 3.7 节“唤醒远程设备”（第 51 页）。

1.3 了解远程管理功能

以下各节可帮助您了解各种“远程管理”功能：

- ◆ 第 1.3.1 节“可见信号”（第 14 页）
- ◆ 第 1.3.2 节“入侵者检测”（第 14 页）
- ◆ 第 1.3.3 节“会话加密”（第 14 页）

- ◆ 第 1.3.4 节“哔声”（第 14 页）
- ◆ 第 1.3.5 节“键盘和鼠标锁定”（第 14 页）
- ◆ 第 1.3.6 节“屏幕消隐”（第 15 页）
- ◆ 第 1.3.7 节“异常终止”（第 15 页）
- ◆ 第 1.3.8 节“覆盖屏幕保护程序”（第 15 页）
- ◆ 第 1.3.9 节“自动终止会话”（第 15 页）
- ◆ 第 1.3.10 节“代理启动的连接”（第 15 页）
- ◆ 第 1.3.11 节“会话协作”（第 15 页）
- ◆ 第 1.3.12 节“远程管理审计”（第 15 页）

1.3.1 可见信号

可让您在受管设备桌面上显示可见指示，通知用户该设备正受到远程管理。可见信号会显示远程操作员标识和会话细节，例如远程会话的类型以及会话的开始时间。用户可以终止特定的远程会话，或关闭信号对话框以终止所有远程会话。

1.3.2 入侵者检测

“入侵者检测”功能可大大降低受管设备遭受黑客攻击的风险。如果远程操作员在指定的尝试次数内（默认为 5 次）无法登录受管设备，则会阻止“远程管理”服务并且直到取消阻止该服务之前都不再接受任何远程会话请求。

1.3.3 会话加密

可使用“安全套接层”（TLSv1 协议）确保远程会话的安全。

1.3.4 哔声

在受管设备上有远程会话处于活动状态期间，您可以让受管设备按照“远程管理”策略中的配置，每隔一定时间发出一声哔声。

1.3.5 键盘和鼠标锁定

可让您在远程会话期间锁定受管设备的键盘和鼠标控制，以免受管设备用户中断会话。

注释：在 Windows Vista 受管设备上，如果启用了 Aero 主题，则鼠标和键盘锁定功能将不起作用。

1.3.6 屏幕消隐

可让您在远程会话期间使受管设备显示黑屏，以防止用户查看会话期间远程操作员所执行的操作。此外，受管设备的键盘和鼠标控制也会被锁定。

注释：远程会话期间 Tablet PC 受管设备黑屏会降低会话性能。

1.3.7 异常终止

可让您在远程会话突然断开的情况下锁定受管设备或注销受管设备上的用户。

1.3.8 覆盖屏幕保护程序

可让您在远程会话期间覆盖受管设备上任何设有口令保护的屏幕保护程序。

注释：此功能在 Windows Vista*、Windows Server 2008 和 Windows 7 受管设备上不可用。

1.3.9 自动终止会话

自动终止在指定时间段内一直处于非活动状态的远程会话。

1.3.10 代理启动的连接

可让您允许受管设备上的用户请求远程操作员提供协助。您可以预先配置可供用户选择的远程操作员的列表。有关更多信息，请参见第 2.8.2 节“从受管设备启动会话”（第 35 页）。

注释：目前只有 Windows 系统支持此功能。

1.3.11 会话协作

可让一组远程操作员进行协作，共同执行远程会话。主远程操作员可以邀请其他远程操作员加入会话、将远程控制权限委派给其他远程操作员以解决问题、从其他远程操作员处收回控制权，以及终止远程会话。有关详细信息，请参见第 3.1.2 节“会话协作”（第 45 页）。

1.3.12 远程管理审计

可让您对在受管设备上执行的每个远程会话生成审计记录。审计日志在受管设备上维护，并可供用户查看。

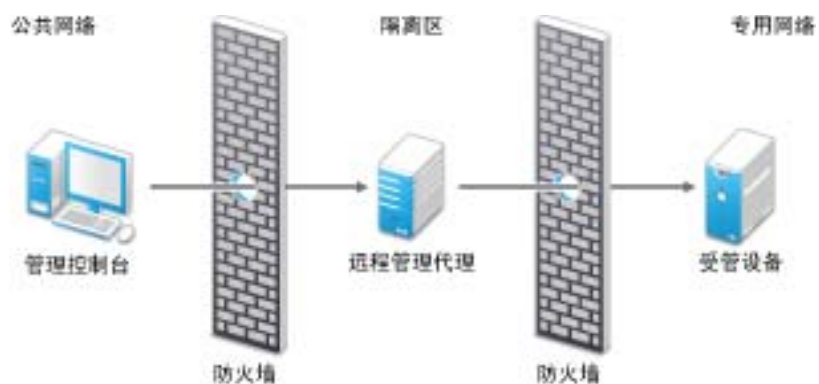
1.4 了解远程管理代理

您无法在位于专用网络内或使用 NAT（网络地址转换）的防火墙或路由器另一侧的受管设备上执行任何远程管理操作。这是因为 NAT 防火墙会对外部网络隐藏设备 IP 地址，并以此阻止到该设备的连接请求。要远程管理此类设备，必须通过远程管理代理来路由远程操作。

有关从管理控制台启动远程会话时通过代理路由远程操作的详细信息，请参见[从设备环境启动远程管理会话](#)（第 30 页）中的[通过代理路由](#)。

有关从设备环境启动远程会话时通过代理路由远程操作的详细信息，请参见[从用户环境启动远程管理会话](#)（第 32 页）中的[通过代理路由](#)。

图 1-2 远程管理代理



必须在位于隔离区 (DMZ) 中的设备上安装该代理。安装代理的设备应该可以从拥有管理控制台的公用网络进行访问，且应该能访问专用网中的设备。有关安装远程管理代理的信息，请参见第 2.10 节“安装远程管理代理”（第 39 页）。

默认情况下，远程管理代理会在端口 5750 上侦听从远程管理查看器传入的远程管理请求，并将该请求转发给设备。

设置远程管理

以下几节提供了在生产环境中部署 Novell® ZENworks® 10 Configuration Management 的“远程管理”组件的相关信息：

- ◆ 第 2.1 节“配置远程管理设置”（第 17 页）
- ◆ 第 2.2 节“启用远程管理侦听程序”（第 20 页）
- ◆ 第 2.3 节“创建远程管理策略”（第 20 页）
- ◆ 第 2.4 节“配置远程操作员权限”（第 25 页）
- ◆ 第 2.5 节“配置远程管理口令”（第 26 页）
- ◆ 第 2.6 节“安装远程管理查看器”（第 28 页）
- ◆ 第 2.7 节“升级远程管理查看器”（第 29 页）
- ◆ 第 2.8 节“启动远程管理操作”（第 29 页）
- ◆ 第 2.9 节“用于启动远程管理操作的选项”（第 37 页）
- ◆ 第 2.10 节“安装远程管理代理”（第 39 页）
- ◆ 第 2.11 节“配置远程管理代理”（第 40 页）

2.1 配置远程管理设置

“远程管理”设置是一组规则，决定着“远程管理”服务在受管设备上的行为或执行情况。设置包括对远程会话期间的端口配置、会话设置及性能设置。这些设置可应用于“区域”级别、“文件夹”级别和“设备”级别。

以下几节提供了在不同级别配置“远程管理”设置的信息。

- ◆ 第 2.1.1 节“在区域级别配置远程管理设置”（第 17 页）
- ◆ 第 2.1.2 节“在文件夹级别配置远程管理设置”（第 19 页）
- ◆ 第 2.1.3 节“在设备级别配置远程管理设置”（第 19 页）

2.1.1 在区域级别配置远程管理设置

默认情况下，在区域级别配置的“远程管理”设置会应用于所有受管设备。

- 1 在“ZENworks 控制中心”中，单击 *配置*。
- 2 在“管理区域设置”面板中，单击 *设备管理*，然后单击 *远程管理*。
- 3 选择在 *端口上运行远程管理服务* 并指定端口，以使“远程管理”服务在该端口上运行。
“远程管理”服务默认会在端口 5950 上侦听。
- 4 选择“会话设置”的选项：

字段	细节
<i>在远程会话开始时查找查看器 DNS 名称</i>	<p>启用“远程管理”服务，在远程会话开始时查找管理控制台的 DNS 名称。</p> <p>该名称保存于审计日志中，在远程会话期间会作为会话信息的一部分显示。如果没有选择此选项，或“远程管理”服务找不到控制台名称，控制台名称会显示为未知。</p> <p>如果网络未启用反向 DNS 查找功能，建议您禁用此设置，以免在远程会话开始时发生明显延迟。</p>
<i>无用户登录受管设备时，允许远程会话</i>	<p>当策略允许远程操作但没有用户登录设备时，可让远程操作员远程管理设备。默认情况下此选项是选中的。</p>

5 选择下列选项以提高远程会话的性能：

字段	细节
<i>取消壁纸</i>	<p>在远程会话期间隐藏受管设备上的墙纸。这样可以避免将墙纸的位图数据反复发送到“远程管理”控制台，从而提高远程会话的性能。</p>
<i>启用优化驱动程序</i>	<p>启用优化驱动程序，默认情况下，每台受管设备上都安装有此程序。如果选择此选项，则远程会话期间“远程管理”控制台仅会截获并更新受管设备上屏幕发生更改的部分，从而提高远程会话的性能。</p>

6（可选）配置远程管理代理以在受管设备上执行远程操作。

如果受管设备位于专用网络或使用 NAT（网络地址转换）的防火墙或路由器的另一侧，设备的远程管理操作就可以通过远程管理代理进行路由。必须单独安装代理。有关安装远程管理代理的信息，请参见第 2.10 节“安装远程管理代理”（第 39 页）。

任务	细节
添加远程管理代理	<ol style="list-style-type: none"> 单击添加显示“添加代理设置”对话框。 填写以下字段： <ul style="list-style-type: none"> 代理：指定远程管理代理的 IP 地址或 DNS 名称。 IP 地址范围：指定要通过远程管理代理远程管理的设备的 IP 地址。可以通过以下一种方式指定 IP 地址范围： <ul style="list-style-type: none"> ◆ 使用 CIDR（无类别域间路由）表示法指定 IP 地址范围。使用 CIDR 时，点分十进制的 IP 地址会解析成 4 个 8 位字节的 32 位二进制数。斜杠 (/n) 后面的数字是前缀长度，也就是从地址左侧算起的共享起始位数。/n 数字的范围可以在 0 到 32 之间，常用的有 8、16、24 和 32。示例： <p>123.45.678.12/16：指定以 123.45 开头的所有 IP 地址。</p> <p>123.45.678.12/24：指定以 123.45.678 开头的所有 IP 地址。</p> ◆ 以起始 IP 地址 - 结束 IP 地址格式指定 IP 地址范围。例如： <p>123.45.678.12 - 123.45.678.15：指定从 123.45.678.12 到 123.45.678.15 范围内的所有 IP 地址。</p>
删除远程管理代理	<ol style="list-style-type: none"> 选择要删除的代理。 单击“删除”，然后单击确定。

7 (可选) 将应用程序添加到 *诊断应用程序* 列表, 以配置“远程诊断”会话期间要在受管设备上起动的应用程序。默认情况下, 该列表包含以下应用程序:

- ◆ 系统信息
- ◆ 计算机管理
- ◆ 服务
- ◆ 注册表编辑器

下表列出了自定义 *诊断应用程序* 列表时可执行的任务:

任务	细节
添加应用程序	<ol style="list-style-type: none">1. 单击 <i>添加</i>。2. 指定受管设备上的应用程序名称和应用程序路径。3. 单击 <i>确定</i>。
删除应用程序	<ol style="list-style-type: none">1. 选择要删除的应用程序。2. 单击“删除”, 然后单击 <i>确定</i>。
还原为默认应用程序	<ol style="list-style-type: none">1. 单击 <i>还原</i>, 然后单击 <i>确定</i>。

8 单击 *应用*, 然后单击 *确定*。

这些更改将于设备刷新后生效。

2.1.2 在文件夹级别配置远程管理设置

默认情况下, 在区域级别配置的“远程管理”设置将应用于所有受管设备。不过, 您可以针对文件夹内的设备修改这些设置:

- 1 在“ZENworks 控制中心”中, 单击 *设备*。
 - 2 单击要配置“远程管理”设置的文件夹 (细节)。
 - 3 单击 *设置*, 然后单击 *设备管理 > 远程管理*。
 - 4 单击 *覆盖*。
 - 5 根据需要编辑“远程管理”设置。
 - 6 要应用这些更改, 请单击 *应用*。
- 或
- 要还原在区域级别配置的系统设置, 请单击 *还原*。
- 7 单击 *确定*。

这些更改将于设备刷新后生效。

2.1.3 在设备级别配置远程管理设置

默认情况下, 在区域级别配置的“远程管理”设置将应用于所有受管设备。不过, 您可以针对受管设备更改这些设置:

- 1 在“ZENworks 控制中心”中, 单击 *设备*。
- 2 单击 *服务器* 或 *工作站* 以显示受管设备列表。

- 3 单击要配置“远程管理”设置的设备。
- 4 单击 *设置*，然后单击 *设备管理 > 远程管理*。
- 5 单击 *覆盖*。
- 6 根据需要编辑“远程管理”设置。
- 7 要应用这些更改，请单击 *应用*。
或
要在设备上还原之前配置的系统设置，请单击 *还原*。
如果设备上的“远程管理”设置于文件夹级别配置，则设置会还原为已配置的文件夹级别设置；否则会还原为默认区域级别设置。
- 8 单击 *确定*。

这些更改将于设备刷新后生效。

2.2 启用远程管理侦听程序

要让远程管理侦听程序侦听受管设备的连接：

- 1 在“ZENworks 控制中心”中，单击 *设备*。
- 2 在左侧窗格的 *设备任务* 中，单击 *远程管理侦听程序*。
- 3 在“远程管理侦听程序”对话框中，为远程连接指定侦听端口。默认端口号为 5550。
- 4 单击 *确定*。

“ZENworks Remote Management 侦听程序”图标随即出现在通知区域。

2.3 创建远程管理策略

您可以使用“远程管理”策略配置受管设备上的“远程管理”会话的行为和执行。该策略包括各项“远程管理”操作设置，例如“远程控制”、“远程查看”、“远程执行”、“远程诊断”以及“文件传送”，它还可让您控制安全性设置。

默认情况下，在受管设备上为 ZENworks Adaptive Agent 部署了“远程管理”组件后，此设备中即创建了安全的远程管理策略。可以使用默认策略来远程管理设备。要覆盖默认策略，您可以以显式方式创建设备的“远程管理”策略。

- 1 在“ZENworks 控制中心”内，单击 *策略* 选项卡。
- 2 在 *策略* 列表中，单击 *新建*，然后单击 *策略* 显示“选择策略类型”页。
- 3 选择 *远程管理策略*，单击 *下一步* 显示“定义细节”页，然后填写字段：
策略名称：提供策略的唯一名称。策略不能与驻留在同一文件夹中的任何其他项目（组、文件夹等）同名。
文件夹：键入名称，或浏览并选择要存放策略的“ZENworks 控制中心”文件夹。默认为 / 策略，但您也可以创建其他文件夹来组织策略。
说明：提供策略内容的简短说明。该说明显示在“ZENworks 控制中心”中的策略摘要页上。
- 4 单击 *下一步* 显示“远程管理一般设置”页。要接受默认设置，则继续下一步，否则请使用下表中指定的信息来更改默认设置。

字段	细节
允许用户请求远程会话	允许受管设备上的用户请求远程操作员执行远程会话。远程操作员必须确保“远程管理侦听程序”正在运行。
登录到受管设备的新用户要求许可权限时，终止远程会话	当登录到远程受管设备的新用户请求许可权限时，会终止正在进行的远程会话。
为受管设备上的用户显示远程会话审计信息	允许受管设备上的用户通过 ZENworks 图标查看远程会话的审计信息。
显示 ZENworks 图标中的远程管理属性	允许受管设备上的用户查看 ZENworks 图标中与“远程管理”策略相关的属性。
编辑	在远程会话开始前，编辑向受管设备上的用户显示的讯息： <ol style="list-style-type: none"> 1. 单击 <i>编辑</i> 显示“编辑讯息”对话框。 2. 编辑该讯息。 3. 单击 <i>确定</i>。
恢复默认值	恢复默认讯息： <ol style="list-style-type: none"> 1. 单击 <i>恢复默认值</i> 将还原为默认讯息。
添加远程侦听程序	添加远程侦听程序： <ol style="list-style-type: none"> 1. 单击 <i>添加</i>。 2. 在“添加远程侦听程序”对话框中，指定管理控制台的 DNS 名称或 IP 地址，以及“远程管理侦听程序”侦听远程会话请求时使用的端口号。 3. 单击 <i>确定</i>。
删除远程侦听程序	删除远程侦听程序： <ol style="list-style-type: none"> 1. 选择要删除的远程侦听程序。 2. 单击 <i>删除</i>。

- 5 单击 *下一步* 显示“远程控制设置”页。要接受默认设置，则继续下一步，否则请使用下表中指定的信息来更改默认设置。

字段	细节
允许远程控制受管的设备	允许在受管设备上启动“远程控制”会话。选择该选项会启用该页上的后续选项。取消选择该选项会禁用设备上的“远程控制”操作。
启动远程控制前先征得受管设备上用户的许可	可让您在启动“远程控制”会话前先征得受管设备上用户的许可。
在远程控制期间，向受管设备上的用户发出可见的信号	在“远程控制”会话期间，会在受管设备桌面的右上角显示可见信号。通过该信号，受管设备上的用户便会知道有“远程控制”会话正在进行。
在远程控制期间，每隔 [] 秒向受管设备上的用户发出哔哔声	“远程控制”会话期间，会在受管设备上发出哔哔声。经过指定的秒数后，定期发出哔哔声。
允许受管设备在远程控制期间显示黑屏	令受管设备在“远程控制”会话期间显示黑屏。选择此选项还会锁定受管设备的键盘和鼠标控制。

字段	细节
<i>在远程控制期间允许锁定受管设备的鼠标和键盘</i>	可让您在“远程控制”会话期间，锁定受管设备的鼠标和键盘。
<i>在远程控制期间允许自动解除锁定屏保</i>	在受管设备上启动“远程控制”会话之前，可让您通过“远程控制查看器”来解除锁定受口令保护的屏保。
<i>自动终止远程控制会话 - 当处于非活动状态长达 [] 分钟</i>	如果受管设备上的“远程控制”会话在指定期间一直处于非活动状态，则终止该会话。

- 6 单击下一步显示“远程查看设置”页。要接受默认设置，则继续下一步，否则请使用下表中指定的信息来更改默认设置。

字段	细节
<i>允许远程查看受管设备</i>	允许在受管设备上启动“远程查看”会话。选择该选项会启用该页上的后续选项。取消选择该选项会禁用设备上的“远程查看”操作。
<i>启动远程查看前先征得受管设备上用户的许可</i>	可让您在启动“远程控制”会话前先征得受管设备上用户的许可。
<i>在远程查看期间，向受管设备上的用户发出可见的信号</i>	在“远程查看”会话期间，受管设备桌面的右上角会显示可见信号。通过该信号，受管设备上的用户便会知道有“远程查看”会话正在进行。
<i>在远程查看期间，每隔 [] 秒向受管设备上的用户发出哔哔声</i>	进行“远程查看”会话期间，在受管设备上发出哔哔声。经过指定的秒数后，定期发出哔哔声。

- 7 单击下一步显示“远程诊断设置”页。要接受默认设置，则继续下一步，否则请使用下表中指定的信息来更改默认设置。

字段	细节
<i>允许远程诊断受管设备</i>	允许在受管设备上启动“远程诊断”会话。选择该选项会启用该页上的后续选项。取消选择该选项会禁用设备上的“远程诊断”操作。
<i>启动远程诊断前先征得受管设备上用户的许可</i>	确保在启动“远程诊断”会话前远程操作员先征得受管设备上用户的许可。
<i>在远程诊断期间，向受管设备上的用户发出可见的信号</i>	在“远程诊断”会话期间，受管设备桌面的右上角会显示可见信号。通过该信号，受管设备上的用户便会知道有“远程诊断”会话正在进行。
<i>在远程诊断期间，每隔 [] 秒向受管设备上的用户发出哔哔声</i>	“远程诊断”会话期间，在受管设备上发出哔哔声。经过指定的秒数后，定期发出哔哔声。
<i>允许受管设备在远程诊断期间显示黑屏</i>	可让受管设备在“远程诊断”会话期间显示黑屏。在“远程诊断”会话期间，受管设备的键盘和鼠标会一直处于锁定状态。选择此选项还会禁用受管设备上的可见信号。
<i>重引导前显示警告讯息 [] 秒</i>	启动“远程诊断”会话时，在受管设备上显示警告讯息，提示用户保存所有现有应用程序。“远程诊断”会话期间，此警告讯息会持续显示一段指定的时间，以防止用户因远程操作员启动系统重引导而丢失尚未保存的数据。

字段	细节
<i>自动终止远程诊断会话 - 当处于非活动状态长达 [] 分钟</i>	如果“远程诊断”会话在指定期间一直处于非活动状态，则终止该会话。

- 8 单击下一步显示“远程执行设置”页。要接受默认设置，则继续下一步，否则请使用下表中指定的信息来更改默认设置。

字段	细节
<i>允许在受管设备上远程执行程序</i>	允许在受管设备上远程执行程序。选择该选项会启用该页上的后续选项。取消选择该选项会禁用设备上的“远程执行”操作。
<i>启动远程执行前先征得受管设备上用户的许可</i>	确保在启动“远程执行”会话前远程操作员先征得受管设备上用户的许可。
<i>在远程执行期间，向受管设备上的用户发出可见的信号</i>	在“远程执行”会话期间，会在受管设备桌面的右上角显示可见信号。通过该信号，受管设备上的用户便能知道有“远程执行”会话正在进行。
<i>自动终止远程诊断会话 - 当处于非活动状态长达 [] 分钟</i>	如果“远程执行”会话在指定期间一直处于非活动状态，则终止该会话。

- 9 单击下一步显示“文件传送设置”页。要接受默认设置，则继续下一步，否则请使用下表中指定的信息来更改默认安全性设置。

字段	细节
<i>允许在受管设备上传送文件</i>	允许在管理控制台和受管设备之间进行文件传送。选择该选项会启用该页上的后续选项。取消选择该选项会禁用设备上的“文件传送”操作。
<i>启动文件传送前先征得受管设备上用户的许可</i>	确保在启动“文件传送”会话前远程操作员先征得受管设备上用户的许可。
<i>在文件传送期间，向受管设备上的用户发出可见的信号</i>	在“文件传送”会话期间，会在受管设备桌面的右上角显示可见信号。通过该信号，受管设备上的用户便能知道有“文件传送”会话正在进行。
<i>允许从受管设备上下载文件</i>	允许远程操作员打开受管设备上的文件，并将其传送到管理控制台。如果不选择此选项，远程操作员只能将文件从管理控制台传送到受管设备。
<i>文件传送根目录</i>	指定“文件传送”会话期间，远程操作员可以看到的受管设备目录。远程操作员只能与此目录及其子目录互传文件。默认目录为“我的电脑”，也就是说，远程操作员可以查看和传送受管设备整个文件系统中的文件。

- 10 单击下一步显示“安全性设置”页。要接受默认设置，则继续下一步，否则请使用下表中指定的信息来更改默认安全性设置。

口令鉴定

字段	细节
启用基于口令的鉴定	允许远程操作员使用口令鉴定到受管设备。选择该选项可配置口令类型设置。
最短口令长度	可让您指定口令的最小长度。默认情况下为 6 个字符。
会话口令	选择此选项会在启动新的远程会话之前，提示受管设备上的用户设置口令。由于口令不会储存在受管设备上，且仅在当前会话期间有效，因此建议选择此选项。
永久口令	选择该选项可设置 ZENworks 口令和 VNC 口令。由于 ZENworks 口令比 VNC 口令更为安全可靠，因此建议设置 ZENworks 口令。该口令可以由管理员通过“远程管理”策略或由受管设备用户通过 ZENworks 图标进行设置。选择该选项将启用后续选项。 要让用户能够通过 ZENworks 图标设置口令，请选择 <i>允许用户覆盖受管设备上的默认口令</i> 选项。
ZENworks 口令	清除 ZENworks 口令： <ol style="list-style-type: none">1. 单击 <i>清除密码</i>。2. 单击 <i>应用</i>，然后单击 <i>确定</i>。 设置 ZENworks 口令： <ol style="list-style-type: none">1. 单击 <i>设置口令</i>。2. 输入口令。口令的最大长度为 255 个字符。3. 单击 <i>应用</i>，然后单击 <i>确定</i>。
VNC 口令	清除 VNC 口令： <ol style="list-style-type: none">1. 单击 <i>清除密码</i>。2. 单击 <i>应用</i>，然后单击 <i>确定</i>。 设置 VNC 口令： <ol style="list-style-type: none">1. 单击 <i>设置口令</i>。2. 输入口令。口令的最大长度为 8 个字符。3. 单击 <i>应用</i>，然后单击 <i>确定</i>。

入侵者检测

字段	细节
启用入侵者检测	选择此选项会针对试图在受管设备上启动远程会话的无效或未授权尝试，启用检测操作。选择该选项将启用“入侵者检测”区域中的后续选项。
暂停接受连接 - 当达到 [] 次连续的无效尝试	指定远程操作员连续进行无效尝试的最大次数，超过该次数后受管设备上的“远程管理”服务就会被阻止。默认为 5 次。
自动开始接受连接 - 当达到 [] 分钟	指定要过多少分钟之后，“远程管理代理”才会自动接受与受管设备的连接。要手动取消阻止“远程管理”服务，请双击 ZENworks Adaptive Agent 图标后，单击 <i>安全性设置</i> ，然后单击 <i>如果当前连接因入侵者检测而被阻止则启用接受连接</i> 。默认值为 10 分钟。

会话安全性

字段	细节
启用会话加密	可使用 SSL 加密（TLSv1 协议）为会话加密。选择该选项将启用“会话安全”区域中的后续选项。
当远程管理控制台没有 SSL 证书时允许连接	从“ZENworks 控制中心”启动远程会话时，自动为远程操作员生成证书。该证书会在鉴定期间用到。选择此选项会允许可能没有 SSL 证书的“远程管理”控制台从“ZENworks 控制中心”外部起动的连接。
查看器证书链中最多允许[]层	Novell 基于权限和基于口令的鉴定模式都会对 SSL 加密通道产生一定影响。建立此通道需要查看器提供证书。此证书可能经由某个中间证书授权者或根证书授权者签名，因而创建了证书链。 此属性定义了查看器证书链中允许的最大层数。如果采用了 ZENworks 内部证书授权者（默认安装），则在从“ZENworks 控制中心”启动远程会话的同时，会自动创建一个 2 层的查看器证书链。

异常终止

字段	细节
锁定设备	当远程会话异常终止时锁定受管设备。
注销用户	当远程会话异常终止时注销受管设备上的用户。

- 11 单击 *下一步* 以显示“摘要”页面。
- 12 单击 *完成* 立即创建策略，或选择 *定义附加属性* 指定其他信息，例如策略指派、实施、状态，以及策略所属的组。

2.4 配置远程操作员权限

您可以为远程操作员指派权限以在受管设备上执行远程会话。“远程操作员”可拥有设备特定权限以及用户特定权限。

- 1 在“ZENworks 控制中心”中，单击 *配置*。
- 2 在“管理员”面板中，单击要为其指派“远程管理”权限的管理员名称。
- 3 在“指派的权限”面板中，单击 *添加*，然后单击 *远程管理权限*，随即显示“远程管理权限”对话框。
- 4 选择要为其指派权限的设备或用户。

下表包含“远程管理”权限的信息：

远程管理权限	细节
远程控制	为远程操作员指派远程控制设备的权限。
远程查看	为远程操作员指派远程查看设备的权限。
远程诊断	为远程操作员指派远程诊断设备的权限。

远程管理权限	细节
远程执行	为远程操作员指派在设备上远程执行应用程序的权限。
传送文件	为远程操作员指派在设备上传入或传出文件的权限。
取消阻止远程管理服务	为远程操作员指派取消阻止“远程管理服务”（因入侵者检测而锁定）的权限。

注释：“远程管理”权限仅适用于基于权限的鉴定。但如果远程管理策略允许，远程管理操作员可以使用基于口令的鉴定执行远程管理操作。

5 单击 *确定*。

2.5 配置远程管理口令

以下各节提供了为受管设备上的“远程管理”服务配置“远程管理”口令的信息：

- ◆ 第 2.5.1 节“使用 ZENworks 控制中心设置远程管理口令”（第 26 页）
- ◆ 第 2.5.2 节“使用 ZENworks Adaptive Agent 设置远程管理口令”（第 27 页）
- ◆ 第 2.5.3 节“使用 ZENworks 控制中心清除远程管理口令”（第 27 页）
- ◆ 第 2.5.4 节“使用 ZENworks Adaptive Agent 清除远程管理口令”（第 27 页）

2.5.1 使用 ZENworks 控制中心设置远程管理口令

管理员可于创建“远程管理”策略期间或之后，在“安全性设置”页中设置“远程管理”口令。

如果要在创建“远程管理”策略时设置口令，请参见第 2.3 节“创建远程管理策略”（第 20 页）。

编辑“远程管理”策略中设置的口令。

- 1 在“ZENworks 控制中心”中，单击 *策略*。
- 2 单击“远程管理”策略，然后单击 *设置* 选项卡。
- 3 在“安全性设置”面板中选择口令，然后以新口令替换该口令。
- 4 单击 *应用*。
- 5 提升“摘要”页或“常见任务”中此策略的版本，以更新受管设备上对口令所做的更改。

如果要在创建“远程管理”策略后设置口令，请执行以下操作：

- 1 在“ZENworks 控制中心”中，单击 *策略*。
- 2 单击“远程管理”策略，然后单击 *设置* 选项卡。
- 3 在“安全性设置”面板中，选择 *启用基于口令的鉴定*，然后选择 *持续*。
- 4 单击 *设置* 口令并指定口令。如果在创建“远程管理”策略时就已设置了口令，则可以编辑口令。要编辑口令，请选择口令并用新口令将其替换。

- 5 单击 *应用*。
- 6 提升“摘要”页或“常见任务”中此策略的版本，以更新受管设备上对口令所做的更改。

2.5.2 使用 ZENworks Adaptive Agent 设置远程管理口令

如果在受管设备上有效的“远程管理”策略中启用了 *允许用户覆盖受管设备上的默认口令* 选项，则受管设备上的用户就可以为“远程管理”服务设置口令。该口令的优先级高于“远程管理”策略中设置的口令。

在受管设备上设置口令：

- 1 双击 *ZENworks Adaptive Agent* 图标以显示 ZENworks Adaptive Agent 窗口。
- 2 在左侧窗格中，浏览到 *远程管理*，然后单击 *安全性*。
- 3 在右侧窗格中，单击 *设置口令* 以设置下列口令：
 - **ZENworks 口令（推荐）**：用于 ZENworks 鉴定。该标识符最长为 255 个字符。
 - **VNC 口令**：用于 VNC 鉴定以与开源 VNC 查看器相互操作。该标识符最长为 8 个字符。
- 4 单击 *确定*。

2.5.3 使用 ZENworks 控制中心清除远程管理口令

使用策略清除设置的“远程管理”口令：

- 1 在“ZENworks 控制中心”中，单击 *策略*。
- 2 单击“远程管理”策略，然后单击 *设置选项卡*。
- 3 在“安全性设置”面板中，选择 *清除口令*，然后单击 *应用*。
- 4 提升“摘要”页或“常见任务”中此策略的版本，以更新受管设备上策略的更改。

清除由受管设备用户设置的“远程管理”口令：

- 1 在“ZENworks 控制中心”中，单击 *策略*。
- 2 单击“远程管理”策略，然后单击 *设置选项卡*。
- 3 在“安全性设置”面板中，取消选择 *允许用户覆盖受管设备上的默认口令* 选项，然后单击 *应用*。
- 4 提升“摘要”页或“常见任务”中此策略的版本，以更新受管设备上策略的更改。

2.5.4 使用 ZENworks Adaptive Agent 清除远程管理口令

受管设备上的用户可以重设置自己先前设置的“远程管理”口令。

- 1 双击 *ZENworks Adaptive Agent* 图标以显示 ZENworks Adaptive Agent 窗口。
- 2 在左侧窗格中，浏览到 *远程管理*，然后单击 *安全性*。
- 3 在右侧窗格中，单击 *清除口令* 以清除下列口令。
- 4 单击 *确定*。

由于没有用户设置的口令，因此将启用策略中配置的口令。

2.6 安装远程管理查看器

“远程管理查看器”是能让远程操作员在受管设备上执行远程操作的管理控制台应用程序。能让远程操作员查看受管设备桌面、传送文件以及执行受管设备上的应用程序。

要安装“远程管理查看器”，请在受管设备上执行远程管理操作时，单击“ZENworks 控制中心”中显示的 *安装远程管理查看器* 链接。只有在第一次于设备上执行远程管理操作时以及设备上尚未安装该查看器的情况下，此链接才会显示。

如果设备上已安装有旧版“远程管理查看器”，则会显示 *升级远程管理查看器* 链接。单击此链接可升级设备上所安装的查看器版本。

注释：要在 SUSE® Linux Enterprise Server 11 (SLES 11) 或 SUSE Linux Enterprise Desktop 11 (SLED 11) 上安装远程管理查看器，必须安装相关的 *glitz* 包。您必须从 [openSUSE® 网站 \(http://software.opensuse.org/112/en\)](http://software.opensuse.org/112/en) 安装适当的 *glitz* 包。

在 Windows 上：

- 1 在“ZENworks 控制中心”中，单击 *配置*。
- 2 在左侧导航窗格中，单击 *下载 ZENworks 工具*。
- 3 在“ZENworks 下载”页的左侧导航窗格中，单击 *管理工具*。
- 4 单击 *novell-zenworks-rm-viewer-<版本>.msi*。
- 5（视情况而定）如果使用 Internet Explorer* 启动“ZENworks 控制中心”，请执行以下操作之一：
 - ◆ 单击 *运行安装查看器*。
 - ◆ 单击 *保存* 将文件保存到某个临时位置。双击该文件以安装查看器。
- 6（视情况而定）如果您使用 Firefox 启动“ZENworks 控制中心”，请单击 *保存文件* 将文件保存到临时位置，然后双击文件以安装查看器。

在 Linux 上：

- 1 在“ZENworks 控制中心”中，单击 *配置*。
- 2 在左侧导航窗格中，单击 *下载 ZENworks 工具*。
- 3 在“ZENworks 下载”页的左侧导航窗格中，单击 *管理工具*。
- 4 单击 *novell-zenworks-rm-viewer-<版本>.noarch.rpm*。
- 5 决定要立即安装查看器，还是先保存查看器 RPM 文件以供日后再进行安装。
 - ◆ 要立即安装查看器，请单击 *打开方式* 以使用 *zen-installer* 打开“远程管理查看器”，指定根口令，然后单击 *确定*。
 - ◆ 要将查看器 RPM 文件保存到默认的下载目录以便您可以稍后再进行安装，请单击 *保存到磁盘*。要安装 RPM，请执行以下操作之一：
 - ◆ 单击查看器 RPM 文件，指定根口令，然后单击 *确定*。
 - ◆ 以超级用户或根用户身份运行以下命令：

```
rpm -ivh novell-zenworks-rm-viewer-<版本>.noarch.rpm
```

2.7 升级远程管理查看器

如果您执行远程管理操作所在的 Windows 受管设备上安装有旧版的“远程管理查看器”，则“ZENworks 控制中心”中会显示[升级远程管理查看器](#)链接。单击此链接可升级设备上所安装的查看器版本。

要将 Linux 设备上的远程管理查看器从 Novell ZENworks 10 Configuration Management SP2 (10.2) 升级为 Novell ZENworks 10 Configuration Management SP3 (10.3) 或更高版本，请以超级用户或根用户身份运行以下命令：

```
rpm -Uvh --no-postun novell-zenworks-rm-viewer-<版本>.noarch.rpm
```

或者，卸载旧版 `novell-zenworks-rm-viewer-10.x.x.rpm`，然后安装新版。有关安装查看器的详细信息，请参见第 2.6 节“[安装远程管理查看器](#)”（第 28 页）。

2.8 启动远程管理操作

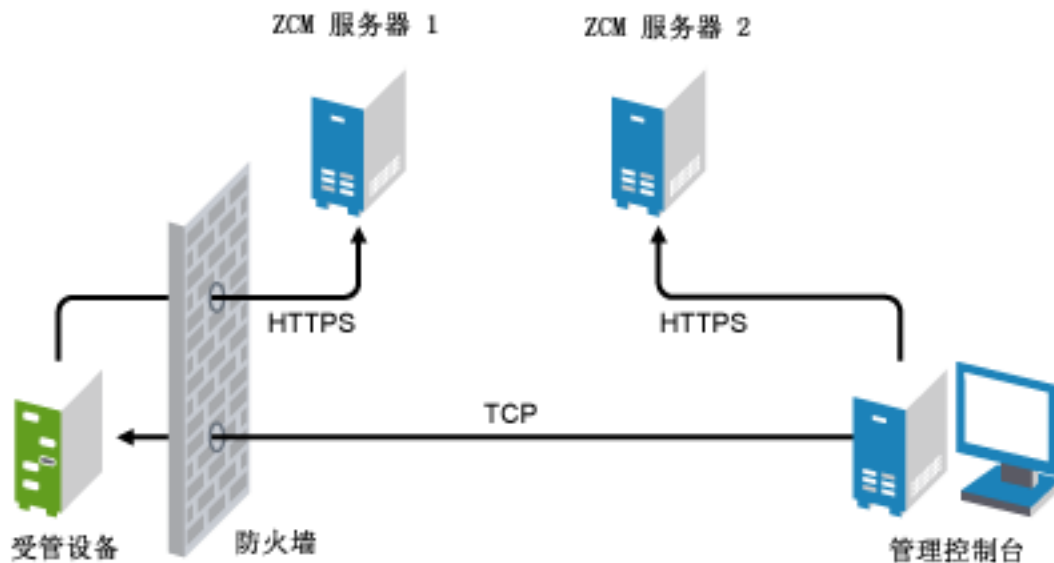
远程管理操作的启动方式有以下几种：

- ◆ 第 2.8.1 节“[从管理控制台启动会话](#)”（第 29 页）
- ◆ 第 2.8.2 节“[从受管设备启动会话](#)”（第 35 页）

2.8.1 从管理控制台启动会话

在这种方式中，远程会话由管理控制台上的管理员启动。管理控制台通常放置于企业网络内，受管设备则可以置于企业网络内部或外部。下图说明了从管理控制台启动的受管设备上的远程会话。

图 2-1 控制台启动的会话



当受管设备引导时，会自动启动“远程管理代理”。部署设备后，此设备中即创建了默认的“远程管理”策略。使用默认策略时只能通过基于权限鉴定的模式来远程管理设备。如果要创建新的“远程管理”策略，则新策略会覆盖默认策略。

如果 ZENworks 管理区域设置分布在两个或两个以上启用 NAT 的专用网络中，而这些专用网络又通过公用网络互相连接，则必须在这些专用网络的网关上部署 DNS_ALG。DNS_ALG 可确保由 ZENworks 组件启动的 DNS 查找查询能够返回映射主机名的正确私有地址，并可让管理控制台与受管设备之间能够进行通讯。有关 DNS_ALG 的详细信息，请参见 DNS ALG RFC - 2694 (<http://www.ietf.org/rfc/rfc2694>)。

如果要通过使用设备的 DNS 名称对设备进行远程管理，请确保网络中已部署动态 DNS 服务。

远程操作员可以采用以下任意一种方式启动会话：

- ◆ [在 ZENworks 控制中心启动远程管理操作（第 30 页）](#)
- ◆ [以独立模式启动远程管理操作（第 34 页）](#)
- ◆ [使用命令行选项启动远程管理操作（第 34 页）](#)

在 ZENworks 控制中心启动远程管理操作

您可以从设备环境或用户环境启动各种“远程管理”操作：

- ◆ [从设备环境启动远程管理会话（第 30 页）](#)
- ◆ [从用户环境启动远程管理会话（第 32 页）](#)

从设备环境启动远程管理会话

启动设备上的远程管理会话

- 1 在“ZENworks 控制中心”内，单击 *设备* 选项卡。
- 2 单击 *服务器* 或 *工作站*，然后选择要远程管理的设备。单击 *操作*，然后选择要执行的“远程管理”操作。

或

在左侧窗格的 *设备任务* 中，选择要执行的“远程管理”操作。

可执行的远程操作如下：

- ◆ **远程控制：**显示“远程管理”对话框，可让您在受管设备上执行“远程控制”、“远程查看”或“远程执行”操作。
 - ◆ **远程诊断：**显示“远程诊断”对话框，可让您在受管设备上执行“远程诊断”操作。
 - ◆ **传送文件：**显示“文件传送”对话框，可让您在受管设备上执行文件传送操作。
- 3 在显示的对话框中填写选项。下表包含各种可用选项的信息：

字段	细节
设备	指定要远程管理的设备的主机名或 IP 地址。
操作	选择要在受管设备上执行的远程操作的类型。此选项仅在“远程管理”对话框中可用。
应用程序	选择要在设备上启动以执行远程诊断的应用程序。此选项仅在“远程诊断”对话框中可用。
鉴定	选择鉴定到受管设备时使用的方式。鉴定方式有： <ul style="list-style-type: none"> ◆ 基于权限的鉴定 ◆ 基于口令的鉴定
端口	指定“远程管理”服务侦听时使用的端口号。默认情况下，端口号为 5950。
会话模式	<p>选择下列其中一种会话模式：</p> <ul style="list-style-type: none"> ◆ 协作：可让您以协作模式启动“远程控制”会话和“远程查看”会话。默认会选择此模式进行“远程控制”操作。如果您最先在受管设备上启动“远程控制”会话，就可获得主远程操作员的特权，包括： <ul style="list-style-type: none"> ◆ 邀请其他远程操作员加入远程会话。 ◆ 将“远程控制”权限委派给某个远程操作员。 ◆ 收回委派给远程操作员的控制权限。 ◆ 终止“远程会话”。 <p>之后启动的会话都是“远程查看”会话。</p> <hr/> <p>注释：Linux 尚不支持协作模式。</p> <hr/> <ul style="list-style-type: none"> ◆ 共享：允许多个远程操作员同时控制受管设备。 ◆ 排它：可让您在受管设备上启动排它性远程会话。某个会话以排它模式启动后，该受管设备上便无法再启动其他远程会话。默认会选择此模式进行“远程查看”操作。 <p>此选项仅在“远程管理”对话框中可用。</p>
会话加密	使用 SSL 加密（TLSv1 协议）可确保远程会话受到保护。
启用超速缓存	启用远程管理会话数据超速缓冲功能可以提高性能。此选项适用于“远程控制”、“远程查看”和“远程诊断”操作。目前只有 Windows 系统支持此选项。
启用动态带宽优化	启用可用网络带宽检测，并适当调整会话设置以提高性能。此选项适用于“远程控制”、“远程查看”和“远程诊断”操作。
启用日志记录	将会话和调试信息记录在 novell-zenworks-vncviewer.txt 文件中。如果是通过 Internet Explorer 启动“ZENworks 控制中心”(ZCC)，该文件默认会保存在桌面上，如果是通过 Mozilla* FireFox* 启动 ZCC，则该文件会保存在 mozilla 的安装目录中。

字段	细节
通过代理路由	<p>可让受管设备的远程管理操作通过远程管理代理进行路由。如果受管设备位于专用网络或使用 NAT（网络地址转换）的防火墙或路由器的另一侧，设备的远程管理操作就可以通过远程管理代理进行路由。目前只有 Windows 系统支持此选项。</p> <p>填写以下字段：</p> <p>代理：指定远程管理代理的 DNS 名称或 IP 地址。默认情况下，此字段中将填入在代理设置面板中配置的用于在设备上执行远程操作的代理。您可以指定其他代理。</p> <p>代理人端口：指定远程管理代理侦听时使用的端口号。默认端口号为 5750。</p> <hr/> <p>注释：“远程管理审计”将显示运行远程管理代理的设备的 IP 地址，而非管理控制台的 IP 地址。</p>
使用以下密钥对进行标识	<p>如果部署了内部证书颁发机构 (CA)，则下列选项将不会显示。如果部署了外部 CA，请填写以下字段：</p> <p>私有密钥：单击浏览浏览并选择远程操作员的私有密钥。</p> <p>证书：单击浏览浏览并选择私有密钥对应的证书。此证书必须链接到为区域配置的证书授权者。</p> <p>受支持的密钥和证书格式为 DER、PEM 和 PFX。如果使用的是 PFX 格式，则相同文件中必须同时有密钥和证书。您应为密钥和证书提供此文件作为输入。</p> <p>启用超速缓存路径：启用要在管理控制台上超速缓存的主键和证书路径。</p> <p>目前只有 Windows 系统支持此选项。</p>

4 单击 *确定* 启动选定的远程操作。

从用户环境启动远程管理会话

如果要在用户登录的受管设备上执行远程会话以协助该用户，请执行以下操作：

- 1 在“ZENworks 控制中心”中，单击 *用户* 选项卡。
- 2 单击 *用户来源*。
- 3 选择用户以远程管理其所登录的设备。
- 4 单击 *操作*，然后选择要执行的“远程管理”操作。

可执行的操作如下：

- ◆ **远程控制：**显示“远程管理”对话框，可让您在受管设备上执行“远程控制”、“远程查看”或“远程执行”操作。
 - ◆ **远程诊断：**显示“远程诊断”对话框，可让您在受管设备上执行“远程诊断”操作。
 - ◆ **传送文件：**显示“文件传送”对话框，可让您在受管设备上执行文件传送操作。
- 5 在显示的对话框中填写选项。下表包含各种可用选项的信息：

字段	细节
设备	指定要远程管理的设备的主机名或 IP 地址。
操作	选择要在受管设备上执行的远程操作的类型。此选项仅在“远程管理”对话框中可用。
应用程序	选择要在设备上启动以执行远程诊断的应用程序。此选项仅在“远程诊断”对话框中可用。
鉴定	选择鉴定到受管设备时使用的方式。鉴定方式有： <ul style="list-style-type: none"> ◆ 基于权限的鉴定 ◆ 基于口令的鉴定
端口	指定“远程管理”服务侦听时使用的端口号。默认情况下，端口号为 5950。
会话模式	<p>选择下列其中一种会话模式：</p> <ul style="list-style-type: none"> ◆ 协作：可让您以协作模式启动“远程控制”会话和“远程查看”会话。默认会选择此模式进行“远程控制”操作。如果您最先在受管设备上启动“远程控制”会话，就可获得主远程操作员的特权，包括： <ul style="list-style-type: none"> ◆ 邀请其他远程操作员加入远程会话。 ◆ 将“远程控制”权限委派给某个远程操作员。 ◆ 收回委派给远程操作员的控制权限。 ◆ 终止“远程会话”。 <p>之后启动的会话都是“远程查看”会话。</p> <hr/> <p>注释：Linux 尚不支持协作模式。</p> <hr/> <ul style="list-style-type: none"> ◆ 共享：允许多个远程操作员同时控制受管设备。 ◆ 排它：可让您在受管设备上启动排它性远程会话。某个会话以排它模式启动后，该受管设备上便无法再启动其他远程会话。默认会选择此模式进行“远程查看”操作。 <p>此选项仅在“远程管理”对话框中可用。</p>
会话加密	使用 SSL 加密（TLSv1 协议）可确保远程会话受到保护。
启用超速缓存	启用远程管理会话数据超速缓冲功能可以提高性能。此选项适用于“远程控制”、“远程查看”和“远程诊断”操作。目前只有 Windows 系统支持此选项。
启用动态带宽优化	启用可用网络带宽检测，并适当调整会话设置以提高性能。此选项适用于“远程控制”、“远程查看”和“远程诊断”操作。
启用日志记录	将会话和调试信息记录在 novell-zenworks-vncviewer.txt 文件中。如果是通过 Internet Explorer 启动“ZENworks 控制中心”(ZCC)，该文件默认会保存在桌面上，如果是通过 Mozilla* FireFox* 启动 ZCC，则该文件会保存在 mozilla 的安装目录中。

字段	细节
通过代理路由	<p>可以让受管设备的远程管理操作通过远程管理代理进行路由。如果受管设备位于专用网络或使用 NAT（网络地址转换）的防火墙或路由器的另一侧，设备的远程管理操作就可以通过远程管理代理进行路由。目前只有 Windows 系统支持此选项。</p> <p>填写以下字段：</p> <p>代理：指定远程管理代理的 DNS 名称或 IP 地址。默认情况下，此字段中将填入在代理设置面板中配置的用于在设备上执行远程操作的代理。您可以指定其他代理。</p> <p>代理人端口：指定远程管理代理侦听时使用的端口号。默认端口号为 5750。</p> <hr/> <p>注释：“远程管理审计”将显示运行远程管理代理的设备的 IP 地址，而非管理控制台的 IP 地址。</p>
使用以下密钥对进行标识	<p>如果部署了内部证书颁发机构 (CA)，则下列选项将不会显示。如果部署了外部 CA，请填写以下字段：</p> <p>私有密钥：单击浏览浏览并选择远程操作员的私有密钥。</p> <p>证书：单击浏览浏览并选择私有密钥对应的证书。此证书必须链接到为区域配置的证书授权者。</p> <p>受支持的密钥和证书格式为 DER、PEM 和 PFX。如果使用的是 PFX 格式，则相同文件中必须同时有密钥和证书。您应为密钥和证书提供此文件作为输入。</p> <p>启用超速缓存路径：启用要在管理控制台上超速缓存的主键和证书路径。</p> <p>目前只有 Windows 系统支持此选项。</p>

6 单击 *确定* 启动选定的远程操作。

以独立模式启动远程管理操作

在独立模式下启动远程管理操作之前，请先安装远程管理查看器。有关安装此查看器的信息，请参见第 2.6 节“[安装远程管理查看器](#)”（第 28 页）。

以独立模式启动“远程管理操作”：

- 1 双击 nzmViewer.exe 文件启动“ZENworks Remote Management 客户程序”。
 - 2 在显示的“ZENworks Remote Management 连接”窗口中，以 *IP 地址* ~ *端口* 格式指定受管设备的 DNS 名称或 IP 地址以及端口号。例如，10.0.0.0~1000。
 - 3 采用下列其中一种格式指定远程管理代理的 DNS 名称或 IP 地址以及端口号：
 - ◆ *IP 地址* ~ *端口*。例如 10.0.0.0~5750。
 - ◆ *IP 地址* ~ *端口*。例如 10.0.0.0~50。
 - 4 单击 *连接*。
- 一旦鉴定成功，远程会话即会启动。默认启动的是“远程控制”会话。

使用命令行选项启动远程管理操作

在通过命令行启动远程管理操作之前，请先安装远程管理查看器。有关安装此查看器的信息，请参见第 2.6 节“[安装远程管理查看器](#)”（第 28 页）。

使用命令行选项启动“远程管理”操作：

1 在命令提示符处，更改查看器的安装目录。默认情况下，查看器会安装到 <用户的 Application Data 文件夹>\Novell\ZENworks\Remote Management\bin 目录中。

2 执行以下命令：

```
nzrViewer [/选项<参数 (如果有)>][受管设备的IP 地址][~ 端口]
```

受管设备的默认端口为 5950。

有关可用命令行选项的信息，请参见第 2.9.1 节“用于启动远程操作的命令行选项”（第 37 页）。

3 单击连接。

一旦鉴定成功，远程会话即会启动。如果在命令行中未指定远程操作类型，则默认情况会启动“远程控制”会话。

但是，使用命令行选项启动远程管理操作有以下限制：

- ◆ 如果您不想在 nzrViewer 命令中为 SSL 鉴定指定 key、cert 和 CAcert 命令行选项，请确保在远程管理策略的安全性设置中启用了当远程管理控制台没有 SSL 证书时允许连接选项。但是，不建议使用此选项，因为这样会使设备的安全性降低。
- ◆ 如果受管设备是“管理区域”的一部分，请确保查看器所提供的证书有效、已签名并且已链接到 CA，否则 SSL 鉴定将失败。

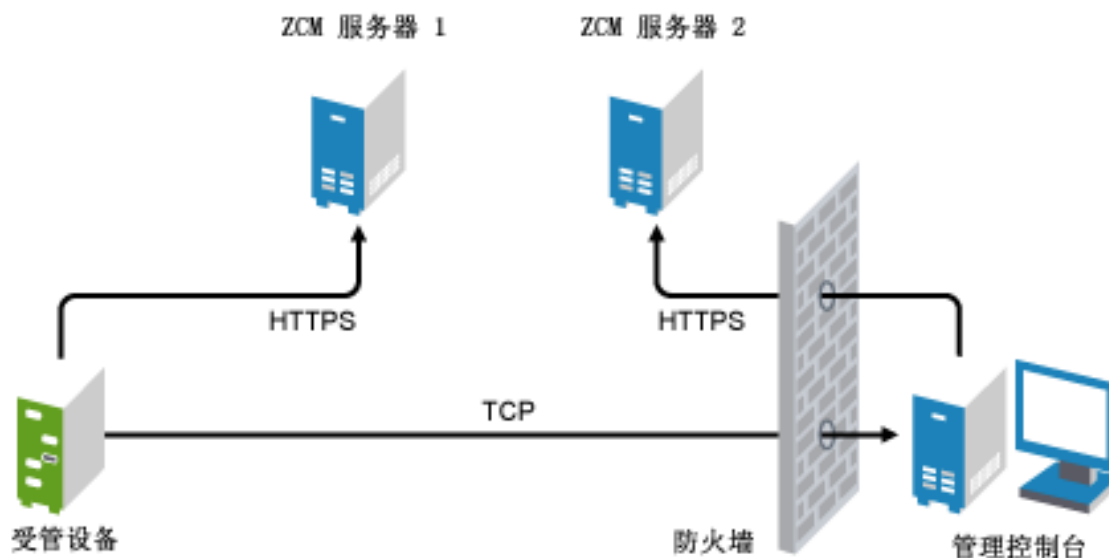
注释：从“ZENworks 控制中心”(ZCC) 启动远程会话时，ZCC 会自动生成证书并将其传送到查看器以启动会话。证书有效期只有 4 天。

- ◆ 受管设备使用查看器提供的证书来识别远程操作员。如果查看器未提供证书，将无法识别用户，此时在权限讯息、可见信号和审核日志中会将该用户记录为未知。

2.8.2 从受管设备启动会话

在此情况下，远程会话由受管设备上的用户启动。这种方式在管理控制台无法与受管设备连接的情况下非常有用。下图说明了由受管设备的用户启动的远程会话。

图 2-2 代理启动的会话



在以下情况下，受管设备的用户可以请求远程管理员在设备上执行远程会话：

- ◆ 远程操作员已启动“远程管理侦听程序”以侦听用户发出的远程会话请求。
- ◆ 在“远程管理”策略中启用了允许用户请求远程会话选项。
- ◆ 管理控制台的防火墙中必须已打开“远程管理侦听程序”侦听远程连接所使用的端口。默认端口为 5550。

请求会话：

- 1 双击通知区域中的 ZENworks 图标。
- 2 在左侧窗格中，浏览到 *远程管理*，然后单击 *常规*。
- 3 单击 *请求远程管理会话* 显示“请求会话”对话框。

请求“远程管理”会话的功能由管理员控制，也就是说可以禁用该选项，特别是当您的公司或部门没有专门的咨询台人员可随时充当远程操作员时。如果 *请求远程管理会话* 选项没有显示为链接文本，则表明该选项已被禁用。

- 4 在 *侦听远程操作员* 列表中，选择您要进行远程会话的远程操作员。

或

如果没有列出远程操作员，请在 *请求连接* 字段中提供该操作员的连接信息。

- 5 在 *操作* 字段中，选择您要打开的操作类型（“远程控制”、“远程查看”、“远程诊断”、“文件传送”或“远程执行”）。

有关每个操作的信息，请参见第 1.2 节“了解远程管理操作”（第 12 页）。

- 6 单击 *请求启动会话*。

如果想让公共网络与专用网络建立连接，请部署“DNS 应用层网关”(DNS_ALG)。有关 DNS_ALG 的详细信息，请参考 RFC 2694 (<http://www.ietf.org/rfc/rfc2694>)。

2.9 用于起动远程管理操作的选项

您在通过命令行起动远程管理操作时，可以指定一些选项来控制远程会话的行为。例如，指定 `remotecontrol` 选项可在设备上起动远程控制操作，指定 `notoolbar` 选项可隐藏查看窗口中的工具栏。

当您在设备上起动远程管理操作时，远程管理会在内部使用一些特定选项。例如，`zenrights` 选项可将鉴定模式指定为 ZENworks 权限鉴定。在设备上使用命令行起动远程管理操作时，不得指定这些内部选项。有关内部使用选项的详细信息，请参见第 2.9.2 节“用于起动远程操作的内部选项”（第 39 页）。

有关远程管理选项的详细信息，请查看以下几节：

- ◆ 第 2.9.1 节“用于起动远程操作的命令行选项”（第 37 页）
- ◆ 第 2.9.2 节“用于起动远程操作的内部选项”（第 39 页）

2.9.1 用于起动远程操作的命令行选项

使用下列命令行选项控制远程操作：

表 2-1 用于起动远程操作的命令行选项

命令行选项	参数	说明
<code>listen</code>	端口	启用侦听程序以侦听指定端口上的远程会话请求。默认端口号为 5550。
<code>restricted</code>		隐藏工具栏和系统菜单。
<code>viewonly</code>		起动受管设备上的“远程查看”操作。
<code>remotecontrol</code>		起动受管设备上的“远程控制”操作。
<code>ftponly</code>		起动受管设备上的“文件传送”操作。
<code>remoteexecute</code>		起动受管设备上的“远程执行”操作。
<code>diagnostics</code>	应用程序名称	起动受管设备上的“远程诊断”操作。如果指定了应用程序名称参数，则会起动受管设备上的该应用程序。
<code>filecompressionlevel</code>	级别	提供优化文件压缩进程的方式，以提高文件传送操作的速度和文件压缩质量。压缩级别为从 0 至 9： <ul style="list-style-type: none">◆ 0 表示不压缩◆ 1 表示速度最快◆ 9 表示压缩质量最佳 如果未指定压缩级别，则会使用默认压缩级别 6，以使速度和压缩质量都得到优化。
<code>noencrypt</code>		以未加密模式起动远程会话。
<code>fullscreen</code>		以全屏模式起动受管设备上的远程操作。
<code>notoolbar</code>		隐藏查看窗口中的工具栏。
<code>exclusive</code>		以排它模式起动远程会话。

命令行选项	参数	说明
8bit		指定用于显示会话数据的颜色深度。
shared		启用共享连接，可让您与其他也在使用桌面的客户机共享桌面。此选项默认处于“真”状态。
collaborate		以协作模式起动远程会话。Linux 尚不支持此选项。
noshared		启用取消共享连接，可使已连接的其他客户机断开连接或拒绝您的连接，具体取决于服务器配置。
swapmouse		切换鼠标按钮。
nocursor		只显示受管设备鼠标指针，而不显示本地鼠标指针。
dotcursor		将本地鼠标指针显示为一个点。此选项默认处于“真”状态。
smalldotcursor		将本地鼠标指针显示为一个点。
normalcursor		将本地鼠标指针显示为默认形状。
belldeiconify		允许传送响铃特性，可使查看器发出哔声。此选项还会使系统在接收到响铃特性后，将最小化的 vncviewer 最大化。
emulate3		具备双按钮鼠标的用户可以通过同时按两个按钮来模拟中间按钮。此选项默认处于“真”状态。
noemulate3		不模拟三按钮鼠标。
nojpeg		禁用质量不佳的 JPEG 压缩。不建议使用此选项，因为解码器的效率可能会下降。如果一定要使图片质量完美无瑕，则可能需要使用此选项。
nocursorshape		禁用光标形状更新以处理远程光标移动。使用光标形状更新会减轻随远程光标移动而导致的延迟现象，从而可以大幅提高宽带使用率。
noremotecursor		不显示远程光标。
fitwindow		隐藏查看窗口中的滚动条。
scale	<i>比例</i>	根据指定的缩放比例缩放查看窗口。
emulate3timeout	<i>毫秒</i>	指定模拟三按钮鼠标的超时时间。
disableclipboard		禁用将数据复制到剪贴板的功能。
delay		在检索下一次更新之前，显示显示区域并等待指定时间。
loglevel	<i>n</i>	指定信息日志记录的级别。
console		在控制台窗口中记录信息。
logfile	<i>文件名</i>	记录信息的日志文件名。
config	<i>文件名</i>	用于加载预定义配置设置的配置文件名。
key	<i>文件名</i>	储存私用密钥的文件名。与受管设备进行 SSL 握手期间可使用此密钥。

重要： key 和 cert 选项必须搭配使用。如果将这些选项与 nZrViewer 命令搭配使用，则必须禁用“远程管理”策略安全性设置中的当远程管理控制台没有 SSL 证书时允许连接选项。

命令行选项	参数	说明
cert	文件名	<p>储存与私用密钥对应的证书的文件名。</p> <hr/> <p>重要： key 和 cert 选项必须搭配使用。如果将这些选项与 nzmViewer 命令搭配使用，则必须禁用“远程管理”策略安全性设置中的当远程管理控制台没有 SSL 证书时允许连接选项。</p>
CAcert	文件名	储存根证书的文件名。用于在 SSL 握手期间校验受管设备证书的证书。
encoding	编码名称	指定用于会话的所需编码。各种编码类型包括 Raw、CopyRect、RRE、CoRRE、HexTile、Zlib 和 Tight。
compresslevel	n	指定从 0 到 9 的压缩级别以压缩远程会话数据。级别 1 使用的 CPU 时间最少但压缩率极低，而级别 9 的压缩质量最佳但速度很慢，服务器的 CPU 耗时较多。如果网络连接速度缓慢，请使用高级别，如果是在高速 LAN 下工作，请使用低级别。不建议您使用压缩级别 0。
quality	n	指定从 0 至 9 的 JPEG 质量级别。质量级别 0 表示图片质量很差但压缩率高，而级别 9 表示图片质量很好但压缩率相对较低。
zenpasswd		指定使用的鉴定模式为“ZENworks 口令鉴定”。
locale		指定用于显示资源的区域设置。默认使用英语。此选项的值包括：英语、法语、德语、西班牙语、葡萄牙语、日语、意大利语、简体中文和繁体中文。
proxy	proxy_server	<p>指定采用下列其中一种格式的远程管理代理的 DNS 名称或 IP 地址以及端口号：</p> <ul style="list-style-type: none"> ◆ IP 地址 ~ 端口。例如 10.0.0.0~5750。 ◆ IP 地址 ~ 端口。例如 10.0.0.0~50。 <p>代理的默认端口为 5750。</p>

2.9.2 用于起动远程操作的内部选项

下表列出了远程管理内部使用选项：通过命令行起动远程管理操作时，不得使用这些选项。

表 2-2 用于起动远程操作的内部选项

选项	描述
zenrights	将 ZENworks 权限鉴定指定为鉴定模式。
pipe	指定鉴定信息。

2.10 安装远程管理代理

如果受管设备位于专用网络或使用 NAT（网络地址转换）的防火墙或路由器的另一侧，设备的远程管理操作就可以通过远程管理代理进行路由。代理可安装在 Windows 受管设备上或在 Linux 设备（主服务器或从属服务器）上。默认情况下，远程管理代理的侦听端口为 5750。

有关远程管理代理的详细信息，请参见第 1.4 节“了解远程管理代理”（第 15 页）。

有关要在设备上安装代理时 Windows 受管设备或 Linux 设备必须满足的系统要求的信息，请参见《ZENworks 10 Configuration Management 安装指南》中的“系统要求”。

要安装代理，请执行下列步骤：

在 Windows 上：

- 1 在设备上打开 Web 浏览器并转到 ZENworks 下载页面：
`https:// 服务器 /zenworks-setup`
其中，*服务器*是“ZENworks 服务器”的 DNS 名称或 IP 地址。
- 2 在左侧导航窗格中，单击 *管理工具*。
- 3 单击 `novell-zenworks-rm-repeater-< 版本 >.msi`，将文件保存到某个临时位置。
*版本*是 ZENworks 产品的版本。
- 4 执行以下命令以安装代理应用程序：
`msiexec /i novell-zenworks-rm-repeater-< 版本 >.msi TARGETDIR="ZENworks 安装目录”。`

在 Linux 上：

- 1 在设备上打开 Web 浏览器并转到 ZENworks 下载页面：
`https:// 服务器 /zenworks-setup`
其中，*服务器*是“ZENworks 服务器”的 DNS 名称或 IP 地址。
- 2 在左侧导航窗格中，单击 *管理工具*。
- 3 单击 `novell-zenworks-rm-repeater-< 版本 >.noarch.rpm`。
- 4 决定是要立即安装代理，还是先保存代理 RPM 文件，以后再安装。
 - ◆ 要立即安装代理，请单击 *打开方式*，使用 `zen-installer` 打开远程管理代理，指定根口令，然后单击 *确定*。
 - ◆ 要将代理 RPM 文件保存到默认下载目录以便以后再安装，请单击 *保存到磁盘*。要安装 RPM，请执行以下操作之一：
 - ◆ 单击代理 RPM 文件，指定根口令，然后单击 *确定*。
 - ◆ 以超级用户或根用户身份运行以下命令：
`rpm -ivh novell-zenworks-rm-repeater-< 版本 >.noarch.rpm`

根据设计，远程管理代理会在安装完成后自动运行。您可以选择通过修改设备的默认设置来自定义该代理的行为。有关远程管理代理设置的详细信息，请参见第 2.11 节“配置远程管理代理”（第 40 页）。

2.11 配置远程管理代理

在设备上安装远程管理代理后，设备在默认情况下会配置特定设置。您可以选择编辑这些设置。

- ◆ 第 2.11.1 节“Windows 设备上的远程管理代理设置”（第 41 页）
- ◆ 第 2.11.2 节“Linux 主服务器或从属服务器上的远程管理代理设置”（第 41 页）

2.11.1 Windows 设备上的远程管理代理设置

在 Windows 设备上，可从 HKLM\SOFTWARE\Novell\ZCM\Remote Management\Proxy 获得远程管理代理的注册表设置。

ClientPort: 指定代理用于侦听来自远程管理查看器的所有远程会话请求的端口号。默认值是 5750。

SessionEncryption: 指定是否加密代理与远程管理查看器之间的初始数据流。默认值为 True。当代理与受管设备建立起连接后，此设置便不再适用，而要由远程管理策略和远程操作员的自选设置来控制会话加密。不过此设置仍应保留为 True，否则系统会允许除远程管理查看器以外的未经鉴定的外部程序与专用网内的设备建立连接。

SSLClientAuthentication: 指定代理是否应接受来自缺少有效证书的查看器的连接请求。可用的值为 True 和 False。默认值为 True。

2.11.2 Linux 主服务器或从属服务器上的远程管理代理设置

在 Linux 主服务器或从属服务器上，可从 /etc/opt/novell/zenworks/repeater/nzrepeater.ini 文件中获得远程管理代理的设置。部分设置如下：

viewerport: 指定远程管理代理用于侦听来自远程管理查看器的任何远程会话请求的端口号。默认值是 5750。

runasuser: 指定代理将模拟的用户。远程管理代理只需具备用户特权即可执行远程操作。默认值为 zenworks。不过，您也可以指定其他用户。

strictimpersonation: 指定当指定为 runasuser 的用户不存在时，是否将以 root 身份继续运行远程会话。可用的值为 True 或 False。默认值为 False，表示当指定为 runasuser 的用户不存在时，将以 root 身份继续运行远程会话。

sslauth: 指定是启用还是禁用 SSL 鉴定。可用的值为 0 或 1。默认值为 1，表示启用 SSL 鉴定。

警告： 建议不要禁用 SSL 鉴定，否则外部程序无需经过鉴定便可访问网络设备。

verifyViewerCert: 指定是否需要验证远程管理查看器的证书。此设置只有在启用了 SSL 鉴定的情况下方适用。可用的值为 0 或 1。默认值为 1，表示必须验证远程管理查看器的证书。在从独立查看器启动会话时，远程操作员可能没有链接到根证书颁发机构所需的证书。在这种情况下，代理无法连接到服务器。

loggingenabled: 指定是否在设备上记录讯息。可用的值为 True 或 False。默认值为 True。

有关注册表设置的信息，请参见 /etc/opt/novell/zenworks/repeater/nzrepeater.ini 文件。

管理远程会话

以下几节提供的信息可帮助您有效地管理 Novell® ZENworks® 10 Configuration Management 的远程会话：

- ◆ 第 3.1 节“管理远程控制会话”（第 43 页）
- ◆ 第 3.2 节“管理远程查看会话”（第 46 页）
- ◆ 第 3.3 节“管理远程执行会话”（第 47 页）
- ◆ 第 3.4 节“管理远程诊断会话”（第 47 页）
- ◆ 第 3.5 节“管理文件传送会话”（第 48 页）
- ◆ 第 3.6 节“管理远程管理代理会话”（第 51 页）
- ◆ 第 3.7 节“唤醒远程设备”（第 51 页）
- ◆ 第 3.8 节“提高远程管理性能”（第 52 页）





3.1 管理远程控制会话

“远程管理”可让您远程控制受管设备。通过远程控制连接，远程操作员不仅能够查看受管设备，进而能够控制该设备，这有助于协助用户解决受管设备上发生的问题。有关启动“远程控制”会话的信息，请参见第 2.8 节“启动远程管理操作”（第 29 页）。

3.1.1 使用远程管理查看器中的工具栏选项

下表提供了“远程控制”会话期间“远程管理”查看器内各种可用工具栏选项的相关说明。另外还列出了可用的快捷键。

表 3-1 远程管理查看器中的工具栏选项

选项	快捷键	功能
 连接选项	Ctrl+Alt+Shift+P	可让您配置各种会话参数，例如用于提高会话性能的格式和编码、日志记录以及本地和远程光标控制。
 连接信息	Ctrl+Alt+Shift+I	提供受管设备的主机名、端口、屏幕分辨率和协议版本。
 全屏	Ctrl+Alt+Shift+F	可让您在全屏模式和正常模式之间切换。
 请求屏幕刷新	Ctrl+Alt+Shift+H	刷新查看窗口。

选项	快捷键	功能
发送 	Ctrl-Alt-Del	将 Ctrl+Alt+Del 击键发送到受管设备。 在 Windows 7 设备上，当前禁用对 Ctrl+Alt+Del 功能的模拟。
发送 	Ctrl-Esc	调用受管设备上的“开始”菜单。
发送 	Alt 键按下 / 放开	单击此选项并按键盘上的 ALT 键可将 Alt 击键发送给受管设备。
黑屏 / 取消黑屏 	Ctrl+Alt+Shift+B	在受管设备上呈现黑屏或显示屏幕。设备屏幕出现黑屏时，设备用户将无法看到远程操作员在设备上执行的各项操作。受管设备的键盘和鼠标控制也会被锁定。 只有在受管设备的有效“远程管理”策略中启用了允许受管设备显示黑屏选项时，此选项才会启用。
锁定 / 解除锁定键盘和鼠标 	Ctrl+Alt+Shift+L	锁定受管设备的键盘和鼠标控制，或解除其锁定。设备的鼠标和键盘控制锁定时，受管设备上的用户便无法使用这些控制。 只有在受管设备的有效“远程管理”策略中启用了允许锁定受管设备的鼠标和键盘选项时，此选项才会启用。
传送文件 	Ctrl+Alt+Shift+T	起动一个与受管设备间互传文件的会话。 只有在受管设备的有效“远程管理”策略中启用了允许在受管设备上传送文件选项时，此选项才会启用。有关“文件传送”的详细信息，请参见第 3.5 节“管理文件传送会话”（第 48 页）。
协作 		在受管设备上起动“ZENworks Remote Management 协作会话”，可让您邀请多个远程操作员加入远程管理会话。您还可以将“远程控制”权限委托给其他远程操作员，让他帮助您解决问题。目前只有 Windows 系统支持此选项。 有关“会话协作”的详细信息，请参见第 3.1.2 节“会话协作”（第 45 页）。
远程执行 	Ctrl+Alt+Shift+U	在受管设备上起动“远程执行”会话，这样您就可以远程起动受管设备上的任意可执行文件。 只有在受管设备的有效“远程管理”策略中启用了允许在受管设备上远程执行程序选项时，此选项才会启用。
覆盖 ScreenSaver 	Ctrl+Alt+Shift+O	在远程会话期间覆盖受管设备上任何设有口令保护的屏幕保护程序。 只有在受管设备的有效“远程管理”策略中启用了在远程控制期间允许自动解除锁定屏保选项时，此选项才会启用。
断开连接 	Alt+F4	结束远程会话。


3.1.2 会话协作

如果远程操作员已启动“远程管理侦听程序”以侦听远程会话请求，“会话协作”功能可让您邀请多个远程操作员加入“远程管理”会话。您还可以将“远程控制”权限委托给某个远程操作员，让他来帮助您解决问题，之后再收回委托给该操作员的控制权限。目前只有Windows系统支持此选项。

如果由您最先在受管设备上启动“远程控制”会话，则可获得主远程操作员的特权。“会话协作”可用于：

- ◆ 邀请多个远程操作员加入“远程控制”会话。
- ◆ 将远程控制权限委托给某个远程操作员，让他帮助您解决问题，之后再收回委托给该操作员的控制权限。
- ◆ 终止远程会话。

启动“会话协作”：

- 1 以协作模式在受管设备上启动“远程控制”会话。
有关启动“远程控制”会话的详细信息，请参见第2.8节“启动远程管理操作”（第29页）。
- 2 在“远程管理”查看器工具栏中，单击显示“会话协作”窗口。

“会话协作”窗口列出了设备的有效“远程管理”策略中所添加的远程操作员。每个远程操作员都是单独的一项，并且前面显示一个彩色圆圈：

- ◆ 灰色圆圈表示远程操作员尚未加入会话。
- ◆ 红色圆圈表示远程操作员已加入会话并处于“远程查看”模式。
- ◆ 绿色圆圈表示远程操作员已加入会话并被委托了会话中的“远程控制”权限。

有关添加远程操作员的详细信息，请参见第2.3节“创建远程管理策略”（第20页）。

下表列出了主远程操作员可在会话协作期间执行的操作：

表3-2 会话协作窗口选项

任务	步骤	其他细节
邀请远程操作员加入远程会话	<ol style="list-style-type: none">1. 选择会话协作窗口中列出的远程操作员。2. 单击邀请。	<p>如果远程操作员接受请求并加入会话，则其对应的灰色圆圈将变为红色。</p> <p>默认情况下，新会话会从“远程查看”模式开始。</p>
将远程控制权限委托给远程操作员	<ol style="list-style-type: none">1. 选择要委托“远程控制”权限的远程操作员。2. 单击委托。	<p>现在所选远程操作员即处于“远程控制”模式，其对应的红色圆圈变为绿色。</p> <p>主远程操作员会自动切换到“远程查看”模式。</p>

任务	步骤	其他细节
收回委托给远程操作员的远程控制权限	1. 单击 <i>收回控制</i> 。	远程操作员即切换到“远程查看”模式，其对应的绿色圆圈变为红色。 主远程操作员会自动切换到“远程控制”模式。
终止远程会话	1. 选择要终止其“远程会话”的远程操作员。 2. 单击 <i>终止</i> 。	如果所选远程操作员处于“远程控制”模式，您将收回“远程控制”权限。 “远程操作员”的会话终止后，其对应的圆圈将变为灰色。
邀请外部远程操作员	1. 单击 <i>邀请外部</i> 邀请“会话协作”窗口中未列出的远程操作员加入远程会话。 2. 指定远程操作员的设备的 DNS 名称或 IP 地址以及端口号。例如，10.0.0.0 ~1000。 3. 单击 <i>邀请</i> 。	





如果主远程操作员断开了与远程会话的连接，所有远程操作员都会终止会话。

3.2 管理远程查看会话

“远程查看”可让您远程连接受管设备，进而查看该受管设备的桌面。有关启动“远程查看”会话的信息，请参见第 2.8 节“启动远程管理操作”（第 29 页）。

下表提供了“远程查看”会话期间“远程管理”查看器内各种可用工具栏选项的相关说明。

表 3-3 远程管理查看器中的工具栏选项

选项	快捷键	功能
 连接选项	Ctrl+Alt+Shift+P	可让您配置各种会话参数，例如用于提高会话性能的格式和编码、日志记录以及本地和远程光标控制。
 连接信息	Ctrl+Alt+Shift+I	提供受管设备的主机名、端口、屏幕分辨率和协议版本。
 全屏	Ctrl+Alt+Shift+F	可让您在全屏模式和正常模式之间切换。
 请求屏幕刷新	Ctrl+Alt+Shift+H	刷新查看窗口。

选项	快捷键	功能
断开连接	Alt+F4	结束远程会话。



3.3 管理远程执行会话

“远程执行”可让您使用系统特权远程运行受管设备上的可执行文件。要执行受管设备上的应用程序，请启动“远程执行”会话。

1 启动“远程执行”会话。

有关启动“远程执行”会话的信息，请参见第 2.8 节“启动远程管理操作”（第 29 页）。

2 指定可执行文件名。

如果该应用程序不在受管设备的系统路径中，则请指定其完整路径。如果未指定要在受管设备上执行的文件的扩展名，“远程执行”将追加 .exe 扩展名。

3 单击执行。

如果定义的路径中所指定的应用程序在受管设备上不可用，则远程执行该应用程序的操作可能会失败。



警告：默认情况下，会使用系统特权在受管设备上以服务方式运行“远程管理”模块。因此，“远程执行”会话期间起动的所有应用程序也会使用系统特权运行。出于安全考虑，强烈建议您在使用应用程序后将其关闭。

3.4 管理远程诊断会话

“远程管理”可让您远程诊断和分析受管设备上出现的问题。这有助于缩短解决问题的时间，且无需技术人员亲临故障设备的现场就可以协助用户排除故障。这样，通过保证桌面的正常运行提高了用户的工作效率。

启动受管设备上的“远程诊断”会话时，您只能访问“远程管理”设置中专为该设备配置的诊断应用程序来诊断并解决设备上的问题。会话期间，诊断应用程序在工具栏中显示为图标。默认情况下，“远程管理”设置中配置了以下诊断应用程序：

表 3-4 远程管理查看器中的工具栏选项

选项	快捷键	功能
 连接选项	Ctrl+Alt+Shift+P	可让您配置各种会话参数，例如用于提高会话性能的格式和编码、日志记录以及本地和远程光标控制。
 连接信息	Ctrl+Alt+Shift+I	提供受管设备的主机名、端口、屏幕分辨率和协议版本。









选项	快捷键	功能
全屏 	Ctrl+Alt+Shift+F	可让您在全屏模式和正常模式之间切换。
请求屏幕刷新 	Ctrl+Alt+Shift+H	刷新查看窗口。
传送文件 	Ctrl+Alt+Shift+T	<p>起动一个与受管设备间互传文件的会话。</p> <p>只有在受管设备的有效“远程管理”策略中启用了允许在受管设备上传送文件选项时，此选项才会启用。有关“文件传送”的详细信息，请参见第 3.5 节“管理文件传送会话”（第 48 页）。</p>
断开连接 	Alt+F4	结束远程会话。

表 3-5 远程诊断应用程序

图标	应用程序
	系统信息
	计算机管理
	服务
	注册表编辑器

您可以配置“远程诊断”会话期间要在受管设备上起动的应用程序。有关配置诊断应用程序的详细信息，请参见第 2.1 节“配置远程管理设置”（第 17 页）。





3.5 管理文件传送会话

“远程管理”可让您在管理控制台与受管设备之间传送文件。有关起动“文件传送”会话的信息，请参见第 2.8 节“启动远程管理操作”（第 29 页）。

在“文件传送”窗口中，“本地计算机”窗格会显示管理控制台上的所有文件及文件夹，而“远程计算机”窗格会显示在“远程管理”策略的**文件传送根目录**选项中指定的目录下的所有文件及文件夹。如果策略中未指定**文件传送根目录**，或受管设备没有任何与其关联的策略，您可以在远程设备的整个文件系统中执行文件传送操作。

下表说明了可用于从“文件传送”窗口中处理文件的“文件传送”控件和选项。Linux 尚不支持**操作菜单**选项。不过，您可以单击工具栏中适当的图标来执行此操作。

表 3-6 文件传送窗口选项

任务	快捷键	步骤	其他细节
新建本地文件夹	Alt+L	<ol style="list-style-type: none"> 单击操作 > 新建本地文件夹。 <p>或</p> <p>在“本地计算机”窗格中单击 。</p> <ol style="list-style-type: none"> 按照屏幕上的提示操作。 	
新建远程文件夹	Alt+W	<ol style="list-style-type: none"> 单击操作 > 新建远程文件夹。 <p>或</p> <p>在“远程计算机”窗格中单击 。</p> <ol style="list-style-type: none"> 按照屏幕上的提示操作。 	
打开文件		<ol style="list-style-type: none"> 双击文件，在关联的应用程序中将其打开。 	
重命名文件或文件夹	Alt+N	<ol style="list-style-type: none"> 选择要重命名的文件或文件夹。 单击操作 > 重命名。 <p>或</p> <p>单击 。</p> <ol style="list-style-type: none"> 按照屏幕上的提示操作。 	
删除文件或文件夹	Alt+D	<ol style="list-style-type: none"> 选择要删除的文件或文件夹。 单击操作 > 删除。 <p>或</p> <p>单击 。</p> <ol style="list-style-type: none"> 按照屏幕上的提示操作。 	可以使用 Shift 或 Ctrl 键选择多个文件。

任务	快捷键	步骤	其他细节
刷新本地文件夹	Alt+E	1. 单击 操作 > 刷新本地文件夹 。 或 在“本地计算机”窗格中单击 	
刷新远程文件夹	Alt+M	1. 单击 操作 > 刷新远程文件夹 。 或 在“远程计算机”窗格中单击 	
对本地文件进行排序		1. 单击 操作 > 本地排序 。 2. 选择排序类型。可以按照名称、大小或日期对文件进行排序。	也可以通过单击对应的列标题对文件进行排序。
对远程文件进行排序		1. 单击 操作 > 远程排序 。 2. 选择排序类型。可以按照名称、大小或日期对文件进行排序。	也可以通过单击对应的列标题对文件进行排序。
上载文件 / 文件夹		1. 选择要上载到远程计算机的文件。 2. 在“远程计算机”窗格中选择目标文件夹。 3. 单击 操作 > 上载 。 或 单击 	只有当焦点在本地计算机上时， 操作 > 上载 选项才可用。 可以使用 Shift 或 Ctrl 键选择多个文件。
下载文件 / 文件夹	Alt+O	1. 选择要下载到本地计算机的文件。 2. 在“本地计算机”窗格中选择目标文件夹。 3. 单击 操作 > 下载 。 或 单击 	只有当焦点在远程计算机上时， 操作 > 下载 选项才可用。 可以使用 Shift 或 Ctrl 键选择多个文件。
取消文件传送	Alt+C	1. 单击 操作 > 取消文件传送 。	也可以通过单击“取消”按钮取消文件传送操作。
显示文件属性	Alt+P	1. 选择文件。 2. 单击 操作 > 属性 。 或 单击 	可以使用 Shift 或 Ctrl 键选择多个文件。 显示选定文件或文件夹的累积大小。
前往父文件夹		1. 单击  移至父文件夹。	

3.6 管理远程管理代理会话

若受管设备位于专用网中或位于使用 NAT（网络地址转换）的防火墙或路由器的另一端，则可以使用远程管理代理在该受管设备上执行远程管理操作。

有关远程管理代理的详细信息，请参见第 1.4 节“了解远程管理代理”（第 15 页）。

有关安装远程管理代理的详细信息，请参见第 2.10 节“安装远程管理代理”（第 39 页）。

有关配置远程管理代理的详细信息，请参见第 2.11 节“配置远程管理代理”（第 40 页）。

3.7 唤醒远程设备

如果网络中某个节点或一组断电节点上的网卡启用了网络唤醒功能，“网络唤醒”可让您远程唤醒这些节点。

如果设备具有多个 NIC（网络接口卡），那么只有为正在广播网络唤醒包的设备所在子网配置了这些 NIC 的其中一个或几个时，才能成功唤醒该设备。

- ◆ 第 3.7.1 节“前提条件”（第 51 页）
- ◆ 第 3.7.2 节“远程唤醒受管设备”（第 51 页）

3.7.1 前提条件

唤醒受管设备之前，必须满足以下前提条件：

- ◆ 确保受管设备上的网卡支持网络唤醒。此外，确保已在受管设备的 BIOS 设置中启用了网络唤醒选项。
- ◆ 确保受管设备已在“ZENworks 管理区域”中注册。
- ◆ 确保远程节点处于软断电状态。在软断电状态下，CPU 会断电且网络接口卡耗电最少。和硬断电状态不同，软断电状态下，计算机在关闭时依然保持电源连接。

3.7.2 远程唤醒受管设备

要执行远程唤醒：

- 1 在“ZENworks 控制中心”中，单击 *设备*。
- 2 单击 *服务器* 或 *工作站* 以显示受管设备列表。
- 3 选择要唤醒的设备。
- 4 单击 *快速任务* > *唤醒* 以显示“唤醒”对话框。
- 5 选择以下其中一个选项指定向受管设备发送唤醒请求的服务器：
 - ◆ **自动检测服务器：** ZENworks 会自动检测离受管设备最近的“主服务器”。如果服务器和远程设备位于不同的子网，请确保连接它们的路由器配置为在 UDP 端口 1761 上转发面向子网的广播。
 - ◆ **使用以下设备：** 单击 *添加* 选择与要唤醒的设备处于同一子网的代理设备。
如果路由器配置为在 UDP 端口 1761 上转发面向子网的广播，则不需要代理。

- 6 (可选) 选择以下其中一个选项指定用于发送唤醒广播的 IP 地址:
 - ◆ **自动检测 IP 地址:** ZENworks 会自动检测用于将唤醒广播发送到受管设备的子网的默认广播地址。
 - ◆ **使用以下 IP 地址:** 指定用于将唤醒广播发送到受管设备的 IP 地址, 然后单击添加。
- 7 在 *重试次数* 选项中, 指定唤醒设备的尝试次数。默认为 1 次。
- 8 在 *重试的时间间隔* 选项中, 指定两次重试之间的时间段。默认为 2 分钟。
- 9 单击 *确定*。

*重试次数*和“*重试的时间间隔*”选项的默认值配置于区域级别。您可以在设备级别覆盖这些值。

3.8 提高远程管理性能

远程会话期间, 链接速度这一“远程管理”性能的快慢因网络流量而异。要改进响应时间, 请尝试以下一个或多个策略:

- ◆ [第 3.8.1 节“在管理控制台上”](#) (第 52 页)
- ◆ [第 3.8.2 节“在受管设备上”](#) (第 52 页)

3.8.1 在管理控制台上

在控制台的“ZENworks Remote Management 连接”窗口中, 单击 *选项* 并设置以下值:

- ◆ 最大化慢速链接的“远程管理”性能:
 - ◆ 选择 *使用 8 位颜色* 选项。
 - ◆ 将 *自定义压缩级别* 设置为级别 6。
- ◆ 选择 *阻止鼠标移动事件* 选项。
- ◆ 启用“远程管理设置”中的 *隐藏墙纸* 选项。

3.8.2 在受管设备上

- ◆ “远程管理”会话的速度取决于受管设备的处理能力。建议您使用 Pentium* III、700 MHz (或更新)、256 MB RAM 或更高。
- ◆ 不要设置墙纸图案。

以下几节提供了您在使用 Novell® ZENworks® 10 Configuration Management 的“远程管理”组件时所应了解的与安全性相关的信息：

- ◆ 第 4.1 节“鉴定”（第 53 页）
- ◆ 第 4.2 节“口令强度”（第 54 页）
- ◆ 第 4.3 节“端口”（第 54 页）
- ◆ 第 4.4 节“Audit”（第 55 页）
- ◆ 第 4.5 节“征得受管设备上用户的许可”（第 55 页）
- ◆ 第 4.6 节“异常终止”（第 55 页）
- ◆ 第 4.7 节“入侵者检测”（第 56 页）
- ◆ 第 4.8 节“远程操作员标识”（第 56 页）
- ◆ 第 4.9 节“浏览器配置”（第 57 页）
- ◆ 第 4.10 节“会话安全性”（第 57 页）

4.1 鉴定

远程操作员要远程管理的设备上必须安装“远程管理”服务。该服务会在受管设备引导时自动启动。如果远程操作员启动了受管设备上的远程会话，则只有操作员已获得在受管设备上执行远程操作的授权，该服务才会启动远程会话。

受管设备上的“远程管理”服务会使用以下鉴定模式，以防未经授权的用户访问受管设备：

- ◆ 第 4.1.1 节“基于权限的远程管理鉴定”（第 53 页）
- ◆ 第 4.1.2 节“基于口令的远程管理鉴定”（第 53 页）

4.1.1 基于权限的远程管理鉴定

在基于权限的鉴定中，系统会为远程操作员指派权限，以在受管设备上启动远程会话。默认情况下，无论本地用户或 ZENworks 用户是否已登录设备，ZENworks 管理员和超级管理员均有权在所有受管设备上执行远程操作。

如果尚无用户登录受管设备，或登录受管设备的用户未登录 ZENworks，则远程操作员无需任何排它权限即可在受管设备上执行远程会话。但如果有 ZENworks 用户登录受管设备，则远程操作员需要排它的“远程管理”权限方可在受管设备上执行远程操作。因为基于权限的鉴定安全可靠，所以强烈建议您使用此模式。

设备上需要安装 ZENworks Adaptive Agent 才能使用基于权限的鉴定。在设备上只安装“远程管理”服务是不够的。

在独立模式下或从命令行启动远程管理操作时，不支持此鉴定模式。

4.1.2 基于口令的远程管理鉴定

在基于口令的鉴定中，系统会提示远程操作员输入口令，以启动受管设备上的远程会话。

口令鉴定模式有以下两种类型：

- ◆ **ZENworks 口令：**此为基于“安全远程密码”(SRP)协议(6a版)的口令模式。ZENworks 口令的最大长度为 255 个字符。
- ◆ **VNC 口令：**此为传统的 VNC 口令鉴定模式。VNC 口令的最大长度为 8 个字符。此口令模式有内在缺陷，即仅在与开源组件交互操作时才可使用。

如果您要使用基于口令的鉴定，强烈建议使用 ZENworks 口令模式，因为这种模式比 VNC 口令模式更为安全可靠。

这些口令模式可以通过下列模式运行：

- ◆ **会话模式：**通过此模式设置的口令仅对当前会话有效。受管设备上的用户必须在远程会话开始时设置口令，然后再通过电话等带外方式将该口令传送给远程操作员。起动受管设备的远程会话后，远程操作员须在随之显示的会话口令对话框中输入正确的口令。如果远程操作员在对话框显示后的两分钟内未输入正确的口令，出于安全考虑会关闭会话。如果您要使用基于口令的鉴定，强烈建议您采用这种鉴定模式，因为该口令仅对当前会话有效且不会保存于受管设备上。
- ◆ **持续模式：**在这种模式下，如果在“远程管理”策略的安全性设置中选择了 *允许用户覆盖受管设备上的默认口令* 选项，管理员便可通过“远程管理”策略设置口令，或者受管设备用户可通过 ZENworks 图标设置口令。

如果受管设备用户和策略都设置了口令，则用户设置的口令优先于策略中配置的口令。

管理员可禁止受管设备用户设置口令，甚至可以重设置用户设置的口令，这样便可确保鉴定期间始终使用策略中配置的口令。有关重设置由受管设备用户设置的口令的详细信息，请参见第 2.5.3 节“使用 ZENworks 控制中心清除远程管理口令”(第 27 页)。

4.2 口令强度

使用安全口令。请注意以下使用指南：

- ◆ **长度：**建议最小长度为 6 个字符。安全口令至少要有 8 个字符，如果再长一些则更好。ZENworks 口令和 VNC 口令的最大长度分别为 255 个字符和 8 个字符。
- ◆ **复杂性：**安全口令由字母和数字组合而成。该口令包含的字母应区分大小写，且至少要有 1 个数字字符。在口令中添加数字，特别是添加在口令的中间而非开头或结尾时，可以增强口令强度。&、*、\$ 及 > 等特殊字符可大大增强口令强度。请勿在口令中使用字典中收录的特定名词或单词之类的可识别单字，以及电话号码、生日、周年纪念日、地址或邮政代码等个人信息。

4.3 端口

默认情况下，“远程管理”服务会在端口 5950 上运行，而“远程管理侦听程序”会在端口 5550 上运行。防火墙已配置为允许“远程管理”服务使用的任何端口，但您需要将防火墙配置为允许“远程管理侦听程序”所使用的端口。

默认情况下，远程管理代理的侦听端口为 5750。

4.4 Audit

ZENworks Configuration Management 会维护受管设备上执行的所有远程会话的日志。此日志存放在受管设备上，可供用户及管理员查看。管理员可查看设备上执行的所有远程会话的日志。用户可在登录后查看设备上执行的所有远程会话的日志。

查看审计日志：

- 1 在受管设备的通知区域双击 ZENworks 图标。
- 2 在左侧窗格中，浏览到 *远程管理*，然后单击 *安全性*。
- 3 单击 *显示审计信息* 以显示设备上执行的远程操作的审计信息。

字段	说明
<i>ZENworks 用户</i>	远程会话开始时登录至受管设备的 ZENworks 用户的名称。
<i>远程操作员</i>	执行该操作的远程操作员的用户名。
<i>控制台计算机</i>	执行远程操作的设备的主机名。
<i>控制台 IP</i>	执行远程操作的设备的 IP 地址。
注释： 如果设备的远程管理操作通过“远程管理”代理路由，则会显示运行该代理的设备的 IP 地址。	
<i>操作</i>	所执行操作的类型有：“远程控制”、“远程执行”、“远程查看”、“远程诊断”、“文件传送”。
<i>开始时间</i>	远程操作的开始时间。
<i>结束时间</i>	远程操作的结束时间。
<i>状态</i>	远程操作的状态有：“成功”、“正在运行”或“失败”。系统还会显示导致操作失败的原因。

4.5 征得受管设备上用户的许可

管理员可以配置“远程管理”策略，以在启动设备上的远程操作前，先让远程操作员征得受管设备上用户的许可。

远程操作员启动受管设备上的远程会话时，“远程管理”服务会检查设备上的有效策略中是否针对该远程操作启用了 *征得受管设备上用户的许可* 选项。如果该选项已启用但无用户登录到设备，远程会话仍会执行。不过，如果选项已启用且有用户已登录到受管设备，则系统便会向该用户显示“远程管理”策略中配置的讯息，请求其允许启动设备上的远程会话。只有当用户授予许可权限之后，会话才可以启动。

4.6 异常终止

如果远程会话突然中断，异常终止功能可让您锁定受管设备，也可以让您注销受管设备上的用户，具体取决于对“远程管理”策略中的安全性设置的配置。在以下情况中，远程会话会异常终止：

- ◆ 网络出现故障，“远程管理”查看器和“远程管理”服务之间无法通信。

- ◆ 任务管理器突然关闭“远程管理”查看器。
- ◆ 受管设备或管理控制台已禁用网络。

某些情况下，“远程管理”服务可能需要一分钟的时间才能判断会话是否异常终止。

4.7 入侵者检测

“入侵者检测”功能可大大降低受管设备遭受黑客攻击的风险。如果远程操作员在指定的尝试次数内（默认为 5 次）无法登录受管设备，则将阻止“远程管理”服务并且直到取消阻止之前都不再接受任何远程会话请求。管理员可选择以手动或自动方式取消阻止“远程管理”服务。

4.7.1 自动取消阻止远程管理服务

达到“远程管理”策略的*自动开始接受连接 - 当达到[] 分钟*选项中所指定的持续时间后，会自动取消阻止“远程管理”服务。默认值时间为 10 分钟。您可以在“远程管理”策略的安全性设置中更改默认时间。

4.7.2 手动取消阻止远程管理服务

您可以从受管设备或“ZENworks 控制中心”中手动取消阻止“远程管理”服务。

要从“ZENworks 控制中心”取消阻止“远程管理”服务，远程操作员必须拥有对受管设备的“取消阻止远程管理服务”权限。

- 1 在“ZENworks 控制中心”中，单击 *设备*。
- 2 单击 *服务器或工作站* 以显示受管设备列表。
- 3 选择要取消阻止的设备。
- 4 单击 *操作*，然后单击 *取消阻止远程管理*。
- 5 单击 *确定*。

从受管设备取消阻止“远程管理”服务：

- 1 在受管设备的通知区域双击 ZENworks 图标。
- 2 在左侧窗格中，浏览到 *远程管理*，然后单击 *安全性*。
- 3 单击 *当前连接因入侵者检测而受阻时允许接受连接*。

4.8 远程操作员标识

远程操作员从“ZENworks 控制中心”起动远程会话时，系统会自动生成帮助受管设备识别远程操作员的证书。不过，如果远程操作员以独立模式起动会话，系统将不会生成证书，并且在审计日志、“可见信号”及“请求用户许可”对话框中均会将远程操作员视为 *未知用户*。“安全套接层”(SSL) 握手期间，“远程管理”服务会使用管理控制台提供的证书来检索远程操作员的身份。除了 VNC 口令鉴定，其他所有类型的鉴定中都会发生 SSL 握手。

如果设备上的有效策略中已启用 *向受管设备上的用户发出可见信号* 选项，则设备上的“远程管理”服务会在可见信号对话框中显示远程操作员的细节。还会在“远程管理审计”日志中记录有关远程操作员的信息。

4.9 浏览器配置

如果在 Windows Vista 设备上使用 Internet Explorer 启动“ZENworks 控制中心”，请关闭浏览器安全性设置中的保护模式（工具 > Internet 选项 > 安全），然后重新启动浏览器。

4.10 会话安全性

ZENworks Configuration Management 会使用“安全套接层”(SSL) 保护远程会话的安全。但通过基于口令的 VNC 鉴定起动的远程会话得不到安全保护。无论“远程管理”策略中是否配置了会话加密，SSL 握手时，鉴定过程都是通过安全通道进行的。

如果“远程管理”策略中的*启用会话加密*选项被禁用，且远程操作员在启动受管设备上的远程会话时禁用了*会话加密*选项，那么当鉴定完成之后，远程会话会切换到非安全模式。不过，建议您继续以安全模式进行会话，因为会话的性能并不会受很大影响。

4.10.1 SSL 握手

在受管设备上安装 ZENworks Adaptive Agent 后，“远程管理”服务会生成有效期为 10 年的自我签名证书。

远程操作员启动受管设备上的远程会话时，“远程管理”查看器会提示远程操作员校验受管设备证书。证书中显示了受管设备的名称、证书授权者、证书有效期及指纹等细节。出于安全考虑，远程操作员必须比对证书的指纹与受管设备用户通过带外方式传送的指纹，以校验受管设备的身份凭证。然后，远程操作员可执行下列其中一个操作：

- ◆ **永久接受证书：**如果管理控制台的登录用户永久接受证书，则由该用户启动的后续远程会话中便不再显示该证书。
- ◆ **暂时接受证书：**如果管理控制台的登录用户暂时接受证书，则证书只是对于当前会话是接受的，下次启动与受管设备的连接时，系统仍会提示用户校验该证书。
- ◆ **拒绝证书：**如果管理控制台的登录用户拒绝证书，远程会话便会终止。

4.10.2 重新生成证书

在以下情况下，受管设备可重新生成新的自我签名证书：

- ◆ 受管设备的名称已更改
- ◆ 证书生效日期迟于当前日期，证书当前无效
- ◆ 证书已过期
- ◆ 证书即将过期
- ◆ 证书遗失

默认情况下，每隔 10 年才会重新生成一次证书。

以下几节说明使用 Novell® ZENworks® 10 Configuration Management 的“远程管理”组件时可能会遇到的情况。

- ◆ 无法覆盖受管设备上的屏幕保护程序（第 60 页）
- ◆ 如果在远程管理会话期间注销 Windows 2000* Professional 计算机然后再重新登录，计算机上设置的墙纸可能无法恢复。（第 60 页）
- ◆ 无法在以极低的颜色质量运行的受管设备上启动远程会话（第 60 页）
- ◆ 无法启动远程管理查看器（第 60 页）
- ◆ 在 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 受管设备上，异常会话终止可能会失败（第 61 页）
- ◆ 如果管理控制台的防火墙中未打开侦听程序绑定的端口，“远程管理侦听程序”将无法接受来自受管设备的远程会话请求（第 61 页）
- ◆ 对在使用远程管理组件时出现的错误讯息进行查错（第 61 页）
- ◆ 如何在启动了“ZENworks 控制中心”的设备上启用“远程管理”调试日志（第 61 页）
- ◆ 安装新版镜像驱动程序（第 62 页）
- ◆ 受管设备无法为会话启动 Novell 加密模式。请确保受管设备与此系统的 UTC 时间同步。如果此问题持续出现，请与 Novell 技术服务联系（第 62 页）
- ◆ 通过“远程执行”在 64 位受管设备上启动的应用程序（如 Regedit）将无权访问某些注册表项（第 62 页）
- ◆ 远程控制 Windows 设备时，黑屏选项可能无法正常工作（第 62 页）
- ◆ 在 Windows 2000 Professional 受管设备上启动远程管理会话时，设备会重引导（第 63 页）
- ◆ 在安装了 Internet Explorer 7 浏览器的设备上启动了“远程管理”查看器的多个实例（第 63 页）
- ◆ 从远程控制 Windows Vista、Windows Server 2008 或 Windows Server 2008 R2 设备时无法使用 Ctrl-Alt-Del 图标（第 63 页）
- ◆ “远程管理”咬接中未选择默认会话模式（第 63 页）
- ◆ 在安装了 Internet Explorer 7 浏览器的 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 设备上，“安装远程管理查看器”链接保持启用状态（第 63 页）
- ◆ “远程管理”查看器的安装可能失败（第 64 页）
- ◆ 无法在 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 设备上启动远程管理查看器（第 64 页）
- ◆ 在“远程控制”会话期间，单击“远程管理”查看器中的 Ctrl+Alt+Del 图标可能会显示没有任何控制项的“安全警告序列”窗口（第 64 页）
- ◆ 远程控制或查看设备时，设备的桌面可能不会显示（第 64 页）
- ◆ 无法从远程将文件传送到 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 设备上的限制文件夹（第 65 页）

- ◆ 无法在 SUSE Linux Enterprise Server 11 设备上通过 Mozilla Firefox 启动远程会话（第 65 页）
- ◆ 如果通过 Internet Explorer 8 启动 ZENworks 控制中心，则不会显示“升级远程管理查看器”链接（第 65 页）

无法覆盖受管设备上的屏幕保护程序

源： ZENworks 10 Configuration Management；远程管理。

解释： 如果“远程控制”会话启动之前已激活受管设备上受口令保护的屏幕保护程序，“远程管理”服务会尝试覆盖屏幕保护程序，以使远程操作员可以查看用户桌面。远程操作员也可以在远程会话期间单击“远程管理”查看器工具栏上的*覆盖屏幕保护程序*图标，以覆盖屏幕保护程序。

可能的原因： 远程会话处于非活动状态而激活了屏幕保护程序。

操作： 单击“远程管理”查看器工具栏上的*覆盖屏幕保护程序*图标。您可能需要单击该图标数次才能将其覆盖。

可能的原因： 在 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 设备上，不支持覆盖“屏幕保护程序”功能。

操作： 无。

可能的原因： 如果受管设备接收到鼠标移动事件，屏幕保护程序就有可能中断。

操作： 选中 ZENworks Remote Management 查看器选项窗口中的*阻止鼠标移动事件*选项，可防止将鼠标移动事件发送到受管设备。

可能的原因： 受管设备上的屏幕保护程序中断，因而激活了受管设备上的图形标识和鉴定 (GINA)。

操作： 再次登录到受管设备。

如果在远程管理会话期间注销 Windows 2000* Professional 计算机然后再重新登录，计算机上设置的墙纸可能无法恢复

源： ZENworks 10 Configuration Management；远程管理。

操作： 无。

无法在以极低的颜色质量运行的受管设备上启动远程会话

源： ZENworks 10 Configuration Management；远程管理。

解释： 您可能无法启动以极低颜色质量（低于每像素 8 位 (bpp)）运行的受管设备上的“远程控制”、“远程查看”或“远程诊断”会话。

操作： 使用以下流程将设备的颜色质量提高至 16 bpp 或更高：

1. 右击桌面。
2. 单击*属性*。
3. 在“显示属性”窗口中，单击*设置*。
4. 选择适当的颜色质量，然后单击*确定*。

无法启动远程管理查看器

源： ZENworks 10 Configuration Management；远程管理。

可能的原因： 如果“远程管理”查看器可执行文件已删除或重命名，“远程管理”查看器将无法启动。

操作： 从 https://ZENworks_服务器IP_地址/zenworks-remote-management 下载最新版的 novell-zenworks-rm-viewer.msi，重新安装“远程管理”查看器。

在 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 受管设备上，异常会话终止可能会失败

源： ZENworks 10 Configuration Management；远程管理。

解释： 在远程会话期间，如果用户在 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 受管设备上禁用网络连接，则 ZENworks 可能不会将其检测为异常终止，因此便不会锁定该设备或注销受管设备上的用户。

操作： 无。

如果管理控制台的防火墙中未打开侦听程序绑定的端口，“远程管理侦听程序”将无法接受来自受管设备的远程会话请求

源： ZENworks 10 Configuration Management；远程管理。

操作： 在管理控制台防火墙中，打开侦听程序端口。

对在使用远程管理组件时出现的错误信息进行查错

源： ZENworks 10 Configuration Management；远程管理。

操作： 要对使用“远程管理”组件时遇到的错误信息进行查错，请将下列日志文件发送给 [Novell 支持 \(http://support.novell.com\)](http://support.novell.com)：

- ◆ WinVNCApp.log 和 WinVNC.log 文件（适用于 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 设备）
- ◆ WinVNC.log 文件（适用于其他受管设备）

访问日志文件：

1. 打开“注册表编辑器”。
2. 转至 HKLM\Software\Novell\ZCM\Remote Management\Agent。
3. 创建名为 DebugMode 的 DWORD，将值设为 2。
4. 创建名为 DebugLevel 的 DWORD，将十六进制值设为 a（相当于十进制值 10）。
5. 重新启动远程管理服务。

系统会在 ZENworks 安装目录\logs 下创建以下“远程管理”日志文件：

- ◆ WinVNC.log
- ◆ WinVNCApp.log

如何在启动了“ZENworks 控制中心”的设备上启用“远程管理”调试日志

源： ZENworks 10 Configuration Management；远程管理。

操作： 要启用该日志，请参见 [Novell 支持知识库 \(http://support.novell.com/search/kb_index.jsp\)](http://support.novell.com/search/kb_index.jsp) 中的 TID 3418069。

安装新版镜像驱动程序

源： ZENworks 10 Configuration Management ； 远程管理。

可能的原因： 在 Windows 2003 64 位受管设备上安装 ZENworks Adaptive Agent 时，镜像驱动程序并未安装到该设备上。但“ZENworks 控制中心”会记录讯息安装新版镜像驱动程序。

虽然仍可在该设备上执行远程会话，但其性能会降低。

操作： 忽略该讯息。

可能的原因： 如果对通过“远程桌面连接”(RDP) 连接的设备进行远程控制，“ZENworks 控制中心”会记录讯息安装新版镜像驱动程序。

虽然仍可在该设备上执行远程会话，但其性能会降低。

操作： 忽略该讯息。

受管设备无法为会话启动 Novell 加密模式。请确保受管设备与此系统的 UTC 时间同步。如果此问题持续出现，请与 Novell 技术服务联系

源： ZENworks 10 Configuration Management ； 远程管理。

可能的原因： 受管设备已升级或注册，但在受管设备的注册表中可能尚未更新此信息。

操作： 当升级或注册受管设备时，请执行以下操作：

1. 以新细节更新注册表中新 CA 证书的域名：

注册表项： HKLM\Software\Novell\ZCM

值： CASubject

2. 将新区域的 CA 证书导入到可信根证书存储区。
3. 从可信根证书存储区去除旧区域的 CA 证书。

可能的原因： 受管设备已移至新的管理区域。

操作： 请从新的管理区域管理该设备。

通过“远程执行”在 64 位受管设备上起动的应用程序（如 Regedit）将无权访问某些注册表项

源： ZENworks 10 Configuration Management ； 远程管理。

可能的原因： 通过“远程执行”在 64 位受管设备上起动的应用程序会于 Windows On Windows (WOW) 环境中运行。

操作： 使用“远程诊断”起动应用程序。

远程控制 Windows 设备时，黑屏选项可能无法正常工作

源： ZENworks 10 Configuration Management ； 远程管理。

可能的原因： Windows 的旧式驱动程序不支持黑屏这一电源选项。

操作： 必须安装系统特定的图形驱动程序。

在 Windows 2000 Professional 受管设备上启动远程管理会话时，设备会重引导

源： ZENworks 10 Configuration Management；远程管理。

可能的原因： 设备上未安装视频驱动程序。

操作： 必须安装系统特定的视频驱动程序。

在安装了 Internet Explorer 7 浏览器的设备上启动了“远程管理”查看器的多个实例

源： ZENworks 10 Configuration Management；远程管理。

可能的原因： 如果管理控制台上安装了下载加速器软件（如 FlashGet），那么当您在安装了 Internet Explorer 7 浏览器的设备上启动“远程管理”操作时，设备上会启动查看器的多个实例。

操作： 暂时禁用下载加速器的加载项：

1. 启动 Internet Explorer 7 浏览器。
2. 单击 **工具 > 管理加载项**。
3. 单击 **启用或禁用加载项**，然后禁用下载加速器的加载项。
4. 启动“远程管理”操作。

操作： 尝试使用 Firefox 浏览器来执行该操作。

从远程控制 Windows Vista、Windows Server 2008 或 Windows Server 2008 R2 设备时无法使用 Ctrl-Alt-Del 图标

源： ZENworks 10 Configuration Management；远程管理。

解释： 如果在禁用了“用户帐户控制”(UAC)的 Windows Vista、Windows Server 2008 或 Windows Server 2008 R2 设备上启动“远程控制”操作，*Ctrl-Alt-Del* 图标会变灰。

操作： 启用 UAC。

“远程管理”咬接中未选择默认会话模式

源： ZENworks 10 Configuration Management；远程管理。

解释： 如果使用 Internet Explorer 打开“ZENworks 控制中心”并在设备上执行“远程管理”操作，则“远程管理”咬接中不会选择默认会话模式。不过，如果您不选择任何会话模式，则“远程控制”操作会以默认协作模式启动，“远程查看”操作会以默认排它模式启动。

操作： 选择执行“远程”操作的会话模式。

在安装了 Internet Explorer 7 浏览器的 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 设备上，“安装远程管理查看器”链接保持启用状态

源： ZENworks 10 Configuration Management；远程管理。

解释： 在安装了 Internet Explorer 7 浏览器的 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 设备上，如果没有启动 ActiveX* 控制项，则可能会无法安装 *远程管理查看器*。

操作： 执行以下操作打开 Vista 设备上的“用户帐户控制”(UAC)：

1. 单击开始 > 设置 > 控制面板 > 用户帐户 > > 用户帐户 > 打开或关闭“用户帐户控制”。
2. 选择使用用户帐户控制(UAC) 帮助保护您的计算机。
3. 单击确定。

操作： 如果您不想在 Windows Vista 设备上启动 UAC，则应升级到 Windows Vista SP1。

“远程管理”查看器的安装可能失败

源： ZENworks 10 Configuration Management；远程管理。

解释：“远程管理”查看器的安装可能会失败。此错误是 MSI 框架的固有错误。

操作： 执行下列任一步骤：

- ◆ 使用“添加 / 删除程序”卸装远程管理查看器，然后重新安装
- ◆ 使用“Microsoft Windows Installer 清理实用程序”清除应用程序，然后重新安装。此实用程序可从 [Microsoft 支持 \(http://support.microsoft.com/kb/290301\)](http://support.microsoft.com/kb/290301) 下载

无法在 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 设备上启动远程管理查看器

源： ZENworks 10 Configuration Management；远程管理。

解释： 在 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 设备上，即使成功完成了安全性提示中的步骤，远程管理查看器仍会失败。

操作： 将运行 ZENworks 控制中心的服务器添加到受信任的站点列表中，然后重试。

在“远程控制”会话期间，单击“远程管理”查看器中的 Ctrl+Alt+Del 图标可能会显示没有任何控制项的“安全警告序列”窗口

源： ZENworks 10 Configuration Management；远程管理。

操作： 单击远程管理查看器中的 *Ctrl+Alt+Del* 图标，然后按 Esc 键退出“安全警告序列”(SAS) 窗口。然后，再次单击“远程管理”查看器中的 *Ctrl+Alt+Del* 图标。

远程控制或查看设备时，设备的桌面可能不会显示

源： ZENworks 10 Configuration Management；远程管理。

解释： 如果远程控制或远程查看执行了 RDP 会话的设备，您可能会看到黑屏，而不是设备的桌面。

操作： 要查看设备的桌面：

- 1 手动解除桌面锁定。

2 运行以下命令在设备的控制台会话上重新启动 RDP 会话:

```
mstsc / console
```

无法从远程将文件传送到 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 设备上的限制文件夹

源: ZENworks 10 Configuration Management ; 远程管理。

解释: 如果启动“文件传送”操作, 从远程将文件传送到启用了“用户帐户控制”(UAC) 的 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 设备上的限制文件夹, 操作将会失败。

操作: 执行以下操作关闭 Windows Vista 设备上的用户帐户控制 (UAC):

- 1 单击 *开始* > *设置* > *控制面板* > *用户帐户* > > *用户帐户* > *打开或关闭“用户帐户控制”*。
- 2 取消选择 *使用用户帐户控制 (UAC) 帮助保护您的计算机*。
- 3 单击 *确定*。

操作: 执行以下操作关闭 Windows 7 设备上的用户帐户控制 (UAC):

- 1 单击 *开始* > *控制面板* > *用户帐户* > > *更改用户帐户控制设置*。
- 2 将滚动条向 *从不通知* 方向滑动最小值, 此时显示的说明为“从不通知我”。
- 3 单击 *确定*。
- 4 重新启动设备。

无法在 SUSE Linux Enterprise Server 11 设备上通过 Mozilla Firefox 启动远程会话

源: ZENworks 10 Configuration Management ; 远程管理。

解释: 适用于 Firefox 的“远程管理”插件安装在 /usr/lib/firefox 目录中, 它同时也是 Firefox 的默认安装目录。如果将 Firefox 安装在 SLES 11 设备上的其他目录, 则无法在设备上通过 Firefox 启动远程会话。

操作: 将 nsZenworksPluginSample.so 文件从 /usr/lib/firefox/plugins 目录复制到 Firefox 插件目录。

如果通过 Internet Explorer 8 启动 ZENworks 控制中心, 则不会显示“升级远程管理查看器”链接

源: ZENworks 10 Configuration Management ; 远程管理。

解释: 如果从 ZENworks Configuration Management SP2 升级到 ZENworks Configuration Management SP3, 并通过 Internet Explorer 8 启动 ZENworks 控制中心, 则 ZENworks 控制中心中不会显示 *升级远程管理查看器* 链接。

操作: 要查看 *升级远程管理查看器* 链接, 请执行下列步骤:

- 1 启动 Internet Explorer 8 浏览器。
- 2 单击 *工具* > *Internet 选项* 以显示“Internet 选项”对话框。
- 3 单击 *安全选项卡*。

- 4 单击 *自定义级别* 选项。
- 5 确保启用了下列设置：
 - ◆ *运行 ActiveX 控件和插件*
 - ◆ *对没有标记为安全的 ActiveX 控件进行初始化和脚本运行*
- 6 重新启动浏览器。

密码细节

A

以下几节包含使用 Novell® ZENworks® 10 Configuration Management 的“远程管理”组件时生成的各种证书的详细信息。

- ◆ 第 A.1 节“受管设备密钥对细节”（第 67 页）
- ◆ 第 A.2 节“远程操作员密钥对细节”（第 67 页）
- ◆ 第 A.3 节“远程管理票据细节”（第 68 页）
- ◆ 第 A.4 节“会话加密细节”（第 68 页）

A.1 受管设备密钥对细节

证书生成者：远程管理服务

证书生成工具：OpenSSL v0.9.8e（Novell 版）

证书签名者：自我签名

证书签名工具：OpenSSL v0.9.8e（Novell 版）

证书校验者：远程管理查看器

证书校验工具：OpenSSL v0.9.8e（Novell 版）

操作者：远程管理服务

目的：通过远程管理查看器建立安全会话

私用密钥类型：RSA

密钥强度：1024 位

签名算法：RSA-SHA256

有效期：10 年

A.2 远程操作员密钥对细节

只有在部署了“内部 CA”之后此证书才生效。

证书生成者：作为 ZENworks 控制中心宿主的 ZENworks 服务器

证书生成工具：Bouncy Castle 库 (bcprov-jdk15-134.jar)

证书签名者：作为 ZENworks 控制中心宿主的 ZENworks 服务器

证书签名工具：Bouncy Castle 库 (bcprov-jdk15-134.jar)

证书校验者：远程管理服务

证书校验工具：OpenSSL v0.9.8e（Novell 版）

使用者：远程管理查看器和远程管理服务

用途：建立安全会话并识别远程操作员

私用密钥类型：RSA

密钥强度：1024 位

签名算法：RSA-SHA1

有效期：4 天

A.3 远程管理票据细节

此证书仅对“权限鉴定”有效。

票据生成者：作为 ZENworks 控制中心宿主的 ZENworks 服务器

票据生成工具：Bouncy Castle 库 (bcprov-jdk15-134.jar)

证书签名者：作为 ZENworks 控制中心宿主的 ZENworks 服务器

票据签名工具：Bouncy Castle 库 (bcprov-jdk15-134.jar)

证书校验者：远程管理 Web 服务（在 ZENworks 服务器上）

证书校验工具：Bouncy Castle 库 (bcprov-jdk15-134.jar)

使用者：远程管理查看器和远程管理 Web 服务

用途：鉴定远程操作员并校验执行操作的权限

签名算法：RSA-SHA1

有效期：2 分钟

A.4 会话加密细节

会话建立于：远程管理服务与远程管理查看器之间

加密协议：SSL (TLSv1)

会话加密算法：AES256-SHA

SSL 鉴定模式：双向 / 服务器

最佳实践

B

以下几节介绍了使用 Novell® ZENworks® 10 Configuration Management 的“远程管理”组件时可遵循的最佳实践。

- ◆ 第 B.1 节“关闭远程管理侦听程序”（第 69 页）
- ◆ 第 B.2 节“关闭在远程执行操作期间起动的应用程序”（第 69 页）
- ◆ 第 B.3 节“在受管设备上识别远程操作员”（第 69 页）
- ◆ 第 B.4 节“在已通过“远程桌面连接”连接的设备上执行远程控制会话”（第 70 页）
- ◆ 第 B.5 节“确定管理控制台名称”（第 70 页）
- ◆ 第 B.6 节“在 Windows Vista、Windows 7、Windows Server 2008 和 Windows Server 2008 R2 设备上使用 Aero 主题”（第 70 页）
- ◆ 第 B.7 节“远程控制 Windows Vista 或 Windows Server 2008 设备时启用安全警告序列 (Ctrl+Alt+Del) 按钮”（第 70 页）
- ◆ 第 B.8 节“在 Windows XP 设备上通过 RDP 安装远程管理服务”（第 71 页）
- ◆ 第 B.9 节“远程管理性能”（第 71 页）

B.1 关闭远程管理侦听程序

远程操作员起动“远程管理侦听程序”侦听受管设备用户发出的远程会话请求时，ZENworks 会提供票据，以使远程操作员鉴定到受管设备。票据的生命周期为两天。

即使在远程操作员注销“ZENworks 控制中心”或将其关闭后，“远程管理侦听程序”仍会继续运行。如果票据依然有效，任何其他远程操作员都可使用侦听程序侦听受管设备用户发出的远程会话请求。出于安全考虑，注销系统或关闭浏览器前请先关闭“远程管理侦听程序”。

要关闭“远程管理侦听程序”，请右键单击通知区域中的 *ZENworks Remote Management 侦听程序* 图标，然后单击 *关闭侦听守护程序*。

B.2 关闭在远程执行操作期间起动的应用程序

默认会使用系统特权在受管设备上以服务方式运行“远程管理”模块。因此，“远程执行”会话期间起动的所有应用程序也会以系统特权运行。出于安全考虑，强烈建议您在使用应用程序后将其关闭。

B.3 在受管设备上识别远程操作员

远程操作员通过“ZENworks 控制中心”在受管设备上起动远程会话时，如果使用了内部 CA，ZENworks 会自动生成证书，帮助受管设备识别远程操作员。但是，如果使用的是外部 CA，则远程操作员需要手动提供链接至所部署的外部 CA 且经 SSL 客户机鉴定认可的证书。有关使用外部 CA 的详细信息，请参见第 2.8 节“启动远程管理操作”（第 29 页）中的使用以下密钥对进行标识。

如果远程操作员未提供证书就在受管设备上启动了远程操作，则在审计日志、“可见信号”及“请求用户许可”对话框中均会将该远程操作员的名称记录为 *未知用户*。要确保远程操作员提供证书，请取消选择“远程管理”策略中的 *当远程管理控制台没有 SSL 证书时允许连接*。

B.4 在已通过“远程桌面连接”连接的设备上执行远程控制会话

要对已通过“远程桌面连接”(RDP) 连接的设备进行远程控制，请确保以下事项之一：

- 受管设备上正在进行 RDP 会话
- 受管设备上的 RDP 会话中止后，已手动解除该设备的锁定。

B.5 确定管理控制台名称

如果“远程管理”策略中启用了 *在远程会话开始时查找查看器 DNS 名称* 选项，则受管设备会在远程会话开始时尝试确定管理控制台名称。如果网络没有启用反向 DNS 查找，选择该选项可能会导致远程会话开始时发生明显延迟。要防止延迟，请禁用策略中的 *在远程会话开始时查找查看器 DNS 名称*。

B.6 在 Windows Vista、Windows 7、Windows Server 2008 和 Windows Server 2008 R2 设备上使用 Aero 主题

为提高远程会话的性能，“远程管理”使用镜像驱动程序来检测屏幕的更改。如果镜像驱动程序与 Aero 桌面主题不兼容，则尝试在已启用 Aero 主题的设备上装载镜像驱动程序时，会将设备切换到默认桌面主题。这可能会影响用户体验，因此不建议在要进行远程管理的设备上使用 Aero 主题。

如果想在受管设备的远程会话期间保留 Aero 主题，请禁用设备上的映像驱动程序。要禁用映像驱动程序，请在设备上取消选择 *启用优化驱动程序*。有关“启用优化驱动程序”设置的详细信息，请参见 [在区域级别配置远程管理设置](#)。

但是，在受管设备上启用 Aero 主题可能会降低设备上的远程会话的性能。

B.7 远程控制 Windows Vista 或 Windows Server 2008 设备时启用安全警告序列 (Ctrl+Alt+Del) 按钮

要在远程控制 Windows Vista 或 Windows Server 2008 设备时启用“远程管理查看器”工具栏中的  (Ctrl+Alt+Del) 图标，请确保受管设备上启用了“用户帐户控制”(UAC)。

B.8 在 Windows XP 设备上通过 RDP 安装远程管理服务

在受管设备上安装“远程管理服务”期间，ZENworks 会自动在设备上安装名为 DFMirage 的镜像驱动程序。如果要在 Windows XP 设备上通过“远程桌面连接”(RDP) 会话安装“远程管理”服务，请确保设备上已安装 [Microsoft 支持网站 \(http://support.microsoft.com/kb/952132\)](http://support.microsoft.com/kb/952132) 提供的增补程序。

B.9 远程管理性能

远程会话期间，“远程管理”在快速或慢速链接上的性能取决于网络流量的大小。要获得更佳响应时间，请参见第 3.8 节“提高远程管理性能”（第 52 页）。

文档更新

C

本节提供本 Novell® ZENworks® 10 Configuration Management SP3 的《ZENworks Remote Management 参考手册》文档中内容更改的相关信息。该信息可帮助您了解关于文档更新的最新信息。

本产品的文档采用 HTML 和 PDF 两种格式，可从 Web 上获得。HTML 和 PDF 文档始终为最新版本，本节中列出的更改也包含于其中。

如需了解正在使用的 PDF 文档是否为最新版本，可以查看 PDF 文档封面上提供的发布日期。

本文档做了以下更新：

- ◆ [第 C.1 节“2010 年 3 月 30 日：SP3 \(10.3\)”](#)（第 73 页）

C.1 2010 年 3 月 30 日：SP3 (10.3)

对以下几节进行了更新：

位置	更改
远程管理代理 （第 11 页）	更新了本节。
第 1.3 节“了解远程管理功能” （第 14 页）	更新了本节。
第 2.5 节“配置远程管理口令” （第 26 页）	更新了本节。
第 2.9 节“用于起动远程管理操作的选项” （第 37 页）	添加了本节。
第 2.10 节“安装远程管理代理” （第 39 页）	更新了本节，添加了对在 Linux 上安装远程管理代理的支持。
第 2.11 节“配置远程管理代理” （第 40 页）	添加了本节。
第 3.7 节“唤醒远程设备” （第 51 页）	更新了本节，添加了有关唤醒配有多个 NIC 的设备的信息。
第 3.6 节“管理远程管理代理会话” （第 51 页）	添加了本节。
第 5 章“查错” （第 59 页）	添加了以下内容： <ul style="list-style-type: none">◆ 无法在 SUSE Linux Enterprise Server 11 设备上通过 Mozilla Firefox 起动远程会话（第 65 页）◆ 如果通过 Internet Explorer 8 起动 ZENworks 控制中心，则不会显示“升级远程管理查看器”链接（第 65 页）

位置	更改
第 5 章“查错”（第 59 页）	添加了以下情景： 无法远程将文件传送到 Windows Vista 或 Windows 7 设备上的限制文件夹
第 B.6 节“在 Windows Vista、Windows 7、Windows Server 2008 和 Windows Server 2008 R2 设备上使用 Aero 主题”（第 70 页）	更新了本节。
