

Symantec NetBackup™ Appliance 安全指南

2.7.1 版

NetBackup 52xx 和 5330



Symantec NetBackup™ Appliance 安全指南

文档版本：2.7.1

法律声明

Copyright © 2015 Symantec Corporation. © 2015 年 Symantec Corporation 版权所有。All rights reserved. 保留所有权利。

Symantec、Symantec 徽标、Checkmark 徽标、Veritas、Veritas 徽标、NetBackup 和 Storage Foundation 是 Symantec Corporation 或其附属机构在美国和其他国家/地区的商标或注册商标。“Symantec”和“赛门铁克”是 Symantec Corporation 在中国的注册商标。其他名称可能为其各自所有者的商标，特此声明。

本 Symantec 产品可能包括 Symantec 必须向第三方支付许可费的第三方软件（“第三方程序”）。部分第三方程序会根据开源或免费软件许可证提供。软件随附的许可协议不会改变这些开源或免费软件许可证赋予您的任何权利或义务。请参见此文档的第三方法律声明附录或此 Symantec 产品随附的 TPIP 自述文件，以获取有关第三方便序的详细信息。

本文档中介绍的产品根据限制其使用、复制、分发和反编译/逆向工程的授权许可协议进行分发。未经 Symantec Corporation（赛门铁克公司）及其特许人（如果存在）事先书面授权，不得以任何方式任何形式复制本文档的任何部分。

本文档按“现状”提供，对于所有明示或暗示的条款、陈述和保证，包括任何适销性、针对特定用途的适用性 or 无侵害知识产权的暗示保证，均不提供任何担保，除非此类免责声明的范围在法律上视为无效。Symantec Corporation（赛门铁克公司）不对任何与性能或使用本文档相关的伴随或后果性损害负责。本文档所含信息如有更改，恕不另行通知。

无论由 Symantec 作为内部服务还是托管服务提供，根据 FAR 12.212 中的定义，授权许可的软件和文档被视为“商业计算机软件”，受 FAR Section 52.227-19 “Commercial Computer Software - Restricted Rights”（商业计算机软件受限权利）和 DFARS 227.7202 “Commercial Computer Software and Commercial Computer Software Documentation”（商业计算机软件和商业计算机软件文档）中的适用规定，以及所有后续法规中规定的权利的制约。美国政府仅可根据本协议的条款对授权许可的软件和文档进行使用、修改、发布复制、执行、显示或披露。

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

技术支持

技术支持维护全球的支持中心。技术支持的主要任务是响应有关产品特性和功能的特定查询。技术支持组还会创建在线知识库的内容。它与公司内部的其他职能部门协同工作，以便及时解答您的问题。

我们提供以下支持服务：

- 一系列支持选项，通过这些选项您可以为任何规模的组织灵活选择正确的服务量。
- 电话和/或基于 Web 的支持，提供快速响应和最新信息
- 升级保证，提供软件升级
- 全球支持，可在地区营业时间甚至每周 7 天、每天 24 小时全天候为您服务
- 超级服务产品，包括帐户管理服务

有关我们的支持服务的信息，请通过以下 URL 访问我们的网站：

www.veritas.com/support

所有支持服务将会根据您的支持协议以及当时最新的企业技术支持策略进行交付。

与技术支持部门联系

持有当前支持协议的客户可以通过以下 URL 访问技术支持信息：

www.veritas.com/support

在与技术支持部门联系之前，请确保您的系统符合产品文档中列出的系统要求。此外，请不要离开出现问题的计算机，以备在必要时重现问题。

在与技术支持部门联系时，请提供以下信息：

- 产品版本级别
- 硬件信息
- 可用内存、磁盘空间和 NIC 信息
- 操作系统
- 版本和修补程序级别
- 网络拓扑结构
- 路由器、网关和 IP 地址信息
- 问题描述：
 - 错误消息和日志文件
 - 在与技术支持人员联系之前执行的故障排除操作

- 最近的软件配置更改和网络更改

授权许可和注册

如果您的产品需要注册或许可证密钥，请访问我们的技术支持网页，URL 如下：

www.veritas.com/support

客户服务

可从以下 URL 获取客户服务信息：

www.veritas.com/support

客户服务可帮助解答非技术性问题，如以下类型的问题：

- 关于产品授权许可或序列化的问题
- 产品注册更新，如地址或名称更改
- 一般产品信息（功能、可用的语言、本地经销商）
- 有关产品更新和升级的最新信息
- 有关升级保证和支持合同的信息
- 有关技术支持选项的建议
- 非技术性的售前问题
- 与 CD-ROM、DVD 或手册相关的问题

支持协议资源

如果您需要就现有支持协议与我们联系，请与您所在区域的支持协议管理团队联系，如下所示：

全球（日本除外）

CustomerCare@veritas.com

日本

CustomerCare_Japan@veritas.com

目录

技术支持	4	
第 1 章	关于 NetBackup Appliance 安全指南	9
	关于 NetBackup Appliance 安全指南	9
	NetBackup Appliance 2.7.1 中的新增安全功能、增强功能和更改	15
第 2 章	用户身份验证	17
	关于 NetBackup Appliance 上的用户身份验证	17
	可在 NetBackup Appliance 上进行身份验证的用户类型	19
	关于配置用户身份验证	21
	通用用户身份验证准则	23
	关于对 LDAP 用户进行身份验证	23
	关于对 Active Directory 用户进行身份验证	24
	关于对 Kerberos-NIS 用户进行身份验证	25
	关于设备登录提示	26
	关于用户名和密码规范	26
第 3 章	用户授权	30
	关于 NetBackup Appliance 上的用户授权	30
	关于授权 NetBackup Appliance 用户	31
	NetBackup Appliance 用户角色权限	33
	关于管理员用户角色	34
	关于 NetBackupCLI 用户角色	34
第 4 章	入侵防护和入侵检测系统	36
	关于 NetBackup 设备上的 Symantec 数据中心安全性	36
	关于 NetBackup Appliance 入侵防护系统	39
	关于 NetBackup Appliance 入侵检测系统	39
	重新查看 NetBackup 设备上的 SDCS 事件	40
	在 NetBackup Appliance 上以非受控模式运行 SDCS	42
	在 NetBackup Appliance 上以受控模式运行 SDCS	42
	覆盖 NetBackup Appliance 入侵防护系统策略	43
	重新启用 NetBackup Appliance 入侵防护系统策略	46

第 5 章	日志文件	49
	关于 NetBackup Appliance 日志文件	49
	关于“收集日志文件”向导	51
	使用 Support 命令查看日志文件	52
	可使用 Browse 命令从何处查找 NetBackup Appliance 日志文件	53
	通过 Datacollect 命令收集设备日志	54
第 6 章	操作系统安全	58
	关于 NetBackup Appliance 操作系统安全	58
	NetBackup Appliance 操作系统中包含的主要组件	59
	NetBackup Appliance 上已禁用的服务帐户	60
	NetBackup Appliance 漏洞扫描	61
第 7 章	数据安全性	62
	关于数据安全	62
	关于数据完整性	63
	关于数据分类	64
	关于数据加密	64
	KMS 支持	64
第 8 章	Web 安全	66
	关于 SSL 认证	66
	IPSec 实现	67
	NBAC 实现	67
	实施第三方 SSL 证书	67
第 9 章	网络安全	69
	关于 IPsec 通道配置	69
	关于 NetBackup Appliance 52xx 端口	71
第 10 章	自动通报安全	73
	关于 AutoSupport	73
	关于自动通报	74
	从 NetBackup Appliance Shell Menu配置自动通报	76
	从 NetBackup Appliance Shell Menu启用和禁用自动通报	77
	从 NetBackup Appliance Shell Menu配置自动通报代理服务 器	77
	了解自动通报工作流程	78
	关于 SNMP	78

	关于管理信息库 (MIB)	79
第 11 章	IPMI 安全	80
	IPMI 配置简介	80
	建议的 IPMI 设置	80
	替换默认 IPMI SSL 证书	82
附录 A	NetBackup Appliance 操作系统中包含的软件包	87
	NetBackup Appliance 操作系统中包含的软件包的列表	87
索引		93

关于 NetBackup Appliance 安全指南

本章节包括下列主题：

- [关于 NetBackup Appliance 安全指南](#)
- [NetBackup Appliance 2.7.1 中的新增安全功能、增强功能和更改](#)

关于 NetBackup Appliance 安全指南

开发 NetBackup 设备的初衷是以安全性为首要需求。使用业界标准和 Symantec 安全产品测试包括设备的 Linux 操作系统和核心 NetBackup 应用程序在内的每个元素是否存在漏洞。这些措施能确保遭受非法访问并导致数据丢失或遭窃的风险降到最低。

在 NetBackup 设备软件及硬件的每个新版本发布之前，都要验证其是否存在漏洞。Symantec 将根据找到的问题的严重级别，使用修补程序或通过预定主要版本来解决这些问题。为了减少未知威胁的风险，Symantec 会定期更新用于相应产品并作为定期维护版本周期的一部分的第三方软件包和模块。

此指南的目标是描述 NetBackup Appliance 的 2.7.1 版本中实施的安全功能，包括以下章节和小节：

NetBackup Appliance 用户身份验证

本章介绍 NetBackup Appliance 中实施的身份验证功能，包括以下部分：

表 1-1 关于身份验证的部分

部分名称	描述	链接
关于 NetBackup Appliance 上的用户身份验证	此部分描述允许访问设备的用户类型、用户帐户和进程。	请参见第 17 页的 “关于 NetBackup Appliance 上的用户身份验证” 。
关于配置用户身份验证	此部分描述可在设备上身份验证的各种用户类型的配置选项。	请参见第 21 页的 “关于配置用户身份验证” 。
关于对 LDAP 用户进行身份验证	此部分描述配置设备以注册 LDAP 用户并对其进行身份验证的先决条件和过程。	请参见第 23 页的 “关于对 LDAP 用户进行身份验证” 。
关于对 Active Directory 用户进行身份验证	此部分描述配置设备以注册 Active Directory (AD) 用户并对其进行身份验证的先决条件和过程。	请参见第 24 页的 “关于对 Active Directory 用户进行身份验证” 。
关于对 Kerberos-NIS 用户进行身份验证	此部分描述配置设备以注册 Kerberos-NIS 用户并对其进行身份验证的先决条件和过程。	请参见第 25 页的 “关于对 Kerberos-NIS 用户进行身份验证” 。
关于设备登录提示	本节描述了登录提示功能，通过它，您可以设置在用户尝试在设备上身份验证时要显示的文本提示。	请参见第 26 页的 “关于设备登录提示” 。
关于用户名和密码规范	此部分描述用户名和密码凭据。	请参见第 26 页的 “关于用户名和密码规范” 。

NetBackup Appliance 用户授权

本章描述实施用于授权用户访问 NetBackup Appliance 的功能，包括以下部分：

表 1-2 关于授权的部分

部分名称	描述	链接
关于 NetBackup Appliance 上的用户授权	此部分描述 NetBackup Appliance 的授权过程的关键特性。	请参见第 30 页的 “关于 NetBackup Appliance 上的用户授权” 。
关于授权 NetBackup Appliance 用户	此部分描述用于授予设备用户多种访问权限的管理选项。	请参见第 31 页的 “关于授权 NetBackup Appliance 用户” 。
关于管理员用户角色	此部分描述管理员用户角色。	请参见第 34 页的 “关于管理员用户角色” 。

部分名称	描述	链接
关于 NetBackupCLI 用户角色	此部分描述 NetBackupCLI 用户角色。	请参见第 34 页的“ 关于 NetBackupCLI 用户角色 ”。

NetBackup Appliance 入侵防护系统和入侵检测系统

本章通过以下各个部分描述适用于 NetBackup Appliance 的 Symantec Data Center Security: Server Advanced (SDCS) 实现：

表 1-3 关于 IPS 和 IDS 策略的部分

部分名称	描述	链接
关于 NetBackup 设备上的 Symantec 数据中心安全性	此部分介绍在设备上实现的 SDCS 功能。	请参见第 36 页的“ 关于 NetBackup 设备上的 Symantec 数据中心安全性 ”。
关于 NetBackup Appliance 入侵防护系统	此部分描述用于保护设备的 IPS 策略。	请参见第 39 页的“ 关于 NetBackup Appliance 入侵防护系统 ”。
关于 NetBackup Appliance 入侵检测系统	此部分描述用于监视设备的 IDS 策略。	请参见第 39 页的“ 关于 NetBackup Appliance 入侵检测系统 ”。
重新查看 NetBackup 设备上的 SDCS 事件	此部分根据安全级别描述相应的 SDCS 事件。	请参见第 40 页的“ 重新查看 NetBackup 设备上的 SDCS 事件 ”。
在 NetBackup Appliance 上以非受控模式运行 SDCS	此部分简要描述设备上的默认安全管理。	请参见第 42 页的“ 在 NetBackup Appliance 上以非受控模式运行 SDCS ”。
在 NetBackup Appliance 上以受控模式运行 SDCS	此部分描述如何在集中 SDCS 环境中进行设备安全管理。	请参见第 42 页的“ 在 NetBackup Appliance 上以受控模式运行 SDCS ”。
覆盖 NetBackup Appliance 入侵防护系统策略	此部分描述覆盖用于设备的 IPS 策略的过程。	请参见第 43 页的“ 覆盖 NetBackup Appliance 入侵防护系统策略 ”。

部分名称	描述	链接
重新启用 NetBackup Appliance 入侵防护系统策略	此部分描述重新启用用于设备的 IPS 策略的过程。	请参见第 46 页的“重新启用 NetBackup Appliance 入侵防护系统策略”。

NetBackup Appliance 日志文件

本章列出 NetBackup Appliance 日志文件和查看日志文件的选项，使用以下部分：

表 1-4 工作日志部分

部分名称	描述	链接
关于处理日志文件	本章概述了 NetBackup Appliance 中所有可查看的不同日志类型。	请参见第 49 页的“关于 NetBackup Appliance 日志文件”。
关于使用“收集日志文件”向导	本章描述 NetBackup Appliance Web Console 中“收集日志文件”向导的使用。	请参见第 51 页的“关于“收集日志文件”向导”。
使用 Support 命令查看日志文件	本章描述使用支持命令查看日志文件的过程。	请参见第 52 页的“使用 Support 命令查看日志文件”。
使用 Browse 命令查找 NetBackup Appliance 日志文件	本章描述使用 Browse 命令查看日志文件。	请参见第 53 页的“可使用 Browse 命令从何处查找 NetBackup Appliance 日志文件”。
通过 Datacollect 命令收集设备日志	本章描述收集设备日志的过程。	请参见第 54 页的“通过 Datacollect 命令收集设备日志”。

NetBackup Appliance 操作系统安全

表 1-5 操作系统部分

部分名称	描述	链接
关于 NetBackup Appliance 操作系统安全	此部分描述用于提高 NetBackup Appliance 整体安全而对操作系统所做的不同更新类型。	请参见第 58 页的“关于 NetBackup Appliance 操作系统安全”。

部分名称	描述	链接
NetBackup Appliance 操作系统中包含的主要组件	此部分列出 NetBackup Appliance 的产品和操作系统组件。	请参见第 59 页的“ NetBackup Appliance 操作系统中包含的主要组件 ”。
NetBackup Appliance 上已禁用的服务帐户	此部分列出设备上禁用的操作系统服务帐户。	请参见第 60 页的“ NetBackup Appliance 上已禁用的服务帐户 ”。
NetBackup Appliance 漏洞扫描	此部分列出 Symantec 用于验证设备安全的一些安全扫描程序。	请参见第 61 页的“ NetBackup Appliance 漏洞扫描 ”。

NetBackup Appliance 数据安全

本章描述 NetBackup Appliance 的数据安全实施，使用以下部分：

表 1-6 数据安全部分

部分名称	描述	链接
关于数据安全	此部分列出提高数据安全需要采取的措施。	请参见第 62 页的“ 关于数据安全 ”。
关于数据完整性	此部分列出提高数据完整性需要采取的措施。	请参见第 63 页的“ 关于数据完整性 ”。
关于数据分类	此部分列出改善数据分类需要采取的措施。	请参见第 64 页的“ 关于数据分类 ”。
关于数据加密	此部分列出改善数据加密需要采取的措施。	请参见第 64 页的“ 关于数据加密 ”。

NetBackup Appliance Web 安全

本章描述 NetBackup Appliance 的 Web 安全实施，使用以下部分：

表 1-7 Web 安全部分

部分名称	描述	链接
关于 SSL 认证	此部分列出 NetBackup Appliance Web Console 的 SSL 认证更新。	请参见第 66 页的“ 关于 SSL 认证 ”。
实施第三方 SSL 证书	此部分列出实施第三方 SSL 证书的过程。	请参见第 67 页的“ 实施第三方 SSL 证书 ”。

NetBackup Appliance 网络安全

本章描述 NetBackup Appliance 的网络安全实施，使用以下部分：

表 1-8 网络安全部分

部分名称	描述	链接
关于 IPsec 通道配置	此部分描述 NetBackup Appliance 的 IPsec 配置。	请参见第 69 页的“ 关于 IPsec 通道配置 ”。
关于 NetBackup Appliance 52xx 端口	此部分描述 NetBackup Appliance 的端口信息。	请参见第 71 页的“ 关于 NetBackup Appliance 52xx 端口 ”。

NetBackup Appliance 自动通报安全

本章描述 NetBackup Appliance 的自动通报安全实施，使用以下部分：

表 1-9 自动通报安全部分

部分名称	描述	链接
关于 AutoSupport	此部分描述 NetBackup Appliance 中的 AutoSupport 功能。	请参见第 73 页的“ 关于 AutoSupport ”。
关于自动通报	此部分描述 NetBackup Appliance 中的自动通报功能。	请参见第 74 页的“ 关于自动通报 ”。
关于 SNMP	此部分描述 NetBackup Appliance 中的 SNMP 功能。	请参见第 78 页的“ 关于 SNMP ”。

NetBackup Appliance IPMI 安全

本章描述用于保护 IPMI 配置的准则，使用以下部分：

表 1-10 IPMI 安全部分

部分名称	描述	链接
IPMI 配置简介	此部分描述 IPMI 以及如何与 NetBackup Appliance 一同配置。	请参见第 80 页的“ IPMI 配置简介 ”。
列出建议的 IPMI 设置	此部分列出用于安全配置的建议 IPMI 设置。	请参见第 80 页的“ 建议的 IPMI 设置 ”。

附录

表 1-11 安全指南中列出的附录

部分名称	描述	链接
附录 A: NetBackup Appliance 操作系统中包括的软件包	此附录列出 NetBackup Appliance 操作系统中包括的操作系统软件包。	请参见第 87 页的“ NetBackup Appliance 操作系统中包含的软件包的列表 ”。

目标读者

本指南的目标读者为包括安全管理员、备份管理员、系统管理员和安排维护 NetBackup Appliance 的 IT 技术人员在内的用户。

NetBackup Appliance 2.7.1 中的新增安全功能、增强功能和更改

对于 NetBackup Appliance 2.7.1，通过添加以下功能改进了安全实施：

- 从 NetBackup 设备软件版本 2.7.1 开始，Red Hat Enterprise Linux (RHEL) 操作系统代替 SUSE Linux Enterprise Server (SLES)。您当前使用的任何现有 NetBackup 5220、5230 或 5330 设备（软件版本 2.6.1.2 及先前版本）均可升级至版本 2.7.1。

注意：由于某些硬件、固件和性能限制，NetBackup 5200 Appliance 不支持升级至版本 2.7.1。

- Symantec Critical System Protection (SCSP) 功能及其关联的策略已更新到 6.5 版本并重命名为 Symantec Data Center Security: Server Advanced (SDCS)。该功能自动设置为非受控模式（默认）。将此功能设置为受控模式需要您将设备连接至 SDCS 服务器。
 在 SDCS 6.5 中，您不能再覆盖和禁用 IPS 策略超过 8 小时。这是 SDCS 软件的限制，而非设备平台的限制。

注意：作为升级到 NetBackup Appliance 2.7.1 的一部分，设备 SDCS 代理将设置为非受控模式。如果升级前某个设备运行在受控模式中，则确保在升级完成之后将该设备重置回受控模式。

此外，还必须在 SDCS 管理服务器上更新设备 IPS 和 IDS 策略。不能使用较早的策略来管理运行 2.7.1 或更新软件版本的设备。新策略可从 NetBackup Appliance Web Console 的“监视” > “SDCS 事件”页面中下载。此外，请注意，升级到 NetBackup Appliance 2.7.1 后，IPS 和 IDS 策略的所有可能的自定义规则或支持例外均不可用。

- 从 NetBackup Appliance 软件版本 2.6.1.1 开始，客户可访问的所有本地设备用户（本地用户、NetBackupCLI 用户、管理员用户和维护用户）的密码哈希均使用 SHA-512 加密算法。每当创建新本地设备用户或更改现有本地设备用户的密码时，密码将使用 SHA-512 进行加密。

注意：在版本 2.6.1.1 之前，设备会使用多种默认密码加密算法，包括 SHA-512、SHA-256 和 Blowfish。将设备升级到 2.6.1.1 或更高版本后，尽管新的默认算法为 SHA-512，但会保留现有密码哈希。虽然先前的算法仍然可用且安全，但 Symantec 建议在升级到 NetBackup Appliance 软件版本 2.6.1.1 或更高版本后，最终更改所有本地设备用户的密码，以便可以使用新的默认算法。

- 从 NetBackup Appliance 2.7.1 开始，Internet Explorer 9.x 不再是设备管理支持的 Web 浏览器。若您正在使用 IE 8.x 或 9.x 访问 NetBackup Appliance Web Console 或 IPMI 控制台，您必须升级至 IE 10.0 或更高版本。
参阅《NetBackup Appliance 管理指南》Appliance 章节支持的 Web 浏览器以了解更多详细信息。

用户身份验证

本章节包括下列主题：

- [关于 NetBackup Appliance 上的用户身份验证](#)
- [关于配置用户身份验证](#)
- [关于对 LDAP 用户进行身份验证](#)
- [关于对 Active Directory 用户进行身份验证](#)
- [关于对 Kerberos-NIS 用户进行身份验证](#)
- [关于设备登录提示](#)
- [关于用户名和密码规范](#)

关于 NetBackup Appliance 上的用户身份验证

[表 2-1](#) 描述了 NetBackup Appliance 上可用的用户帐户。

表 2-1 NetBackup Appliance 帐户类型

帐户类型	描述
用户	<p>NetBackup Appliance 通过用户帐户进行管理。您可以创建本地用户帐户，也可以注册属于远程目录服务的用户和用户组。每个用户帐户必须使用用户名和密码进行身份验证以访问设备。对于本地用户，用户名和密码在设备上管理。对于已注册的远程用户，用户名和密码由远程目录服务管理。</p> <p>为使新用户帐户能够登录并访问设备，必须首先对其授权一个角色。默认情况下，新用户帐户未分配角色，因此在您为其授予角色之前无法登录。</p> <p>您可以对用户或用户组授予以下角色：</p> <ul style="list-style-type: none"> ■ 管理员 分配了管理员角色的用户帐户具有管理 NetBackup Appliance 的管理权限。管理员用户能够登录、查看和在 NetBackup Appliance Web Console 与 NetBackup Appliance Shell Menu 上执行所有功能。这些用户帐户有权登录到设备，并以超级用户权限运行 NetBackup 命令。 请参见第 34 页的“关于管理员用户角色”。 ■ NetBackupCLI 分配了 NetBackupCLI 角色的用户帐户可以执行所有 NetBackup 命令、查看日志、编辑 NetBackup touch 文件以及编辑 NetBackup 通知脚本。NetBackupCLI 用户的唯一限制是必须使用超级用户权限运行 NetBackup 命令并且在 NetBackup 软件目录之外没有访问权限。这些用户登录后，他们将转到可以运行 NetBackup 命令的受限 shell。 请参见第 34 页的“关于 NetBackupCLI 用户角色”。
admin	<p>admin 帐户是 NetBackup Appliance 上的默认管理员用户。</p> <p>以下默认登录凭据与新 NetBackup Appliance 一起提供：</p> <ul style="list-style-type: none"> ■ 用户名：admin ■ 密码：P@ssw0rd
Maintenance	<p>Maintenance 帐户由 Symantec 支持通过 NetBackup Appliance Shell Menu 使用（在以管理员身份登录之后）。此帐户专用于执行维护活动或对设备进行故障排除。</p>
AppComm	<p>AppComm 帐户用于内部进程通信。</p>
sisips	<p>sisips 帐户是一个内部用户，用于实现 SDCS 策略。</p>

帐户类型	描述
root	<p>root 帐户是一个受限制的用户，只能由 Symantec 支持访问并用于执行维护任务。如果您尝试访问此帐户，则会显示以下消息：</p> <pre>Permission Denied !! Access to the root account requires overriding the Symantec Intrusion Security Policy.</pre> <p>Please refer to the appliance security guide for overriding instructions.</p> <p>警告： 请注意，您可以覆盖 Symantec 入侵安全策略 (ISP) 以获取对 root 帐户的访问权限。但是，不建议进行此操作，此操作会使系统处于风险中并且使系统易受到攻击。请参见第 43 页的“覆盖 NetBackup Appliance 入侵防护系统策略”。</p>

请参见第 17 页的“关于 NetBackup Appliance 上的用户身份验证”。

请参见第 31 页的“关于授权 NetBackup Appliance 用户”。

可在 NetBackup Appliance 上进行身份验证的用户类型

您可以在设备上直接添加本地用户，也可以从 LDAP 服务器、Active Directory (AD) 服务器或 NIS 服务器注册用户。注册远程用户的好处是允许您利用现有的目录服务进行用户管理和身份验证。表 2-2 描述可添加到 NetBackup Appliance 的用户类型。

表 2-2 NetBackup Appliance 用户类型

用户类型	描述	说明
“本地”（本机用户）	本地用户将被添加到设备数据库，而并不引用到基于外部目录的服务器，例如 LDAP 服务器。添加用户后，您可以授予或撤销相应的设备访问权限。	<ul style="list-style-type: none"> ■ 您可以使用 NetBackup Appliance Web Console 的“设置” > “身份验证” > “用户管理”页面添加、删除和管理本地用户。 ■ 您可以使用 NetBackup Appliance Shell Menu 的 Settings > Security > Authentication > LocalUser 命令添加和删除本地用户，以及更改用户密码。 ■ 您无法添加本地用户组。 ■ 本地用户可以具有管理员角色，也可以具有 NetBackupCLI 角色。 <p>注意： 无法对现有的本地用户授予 NetBackupCLI 角色。但是，您可以使用 NetBackup Appliance Shell Menu 的 Manage > NetBackupCLI > Create 命令创建本地 NetBackupCLI 用户。</p>

用户类型	描述	说明
LDAP	<p>LDAP（轻量型目录访问协议）用户或用户组位于外部 LDAP 服务器上。将设备配置为与 LDAP 服务器进行通信之后，可以向设备注册这些用户和用户组。注册（添加）用户后，您可以授予或撤消相应的设备访问权限。</p> <p>请参见第 23 页的“关于对 LDAP 用户进行身份验证”。</p>	<ul style="list-style-type: none"> ■ 您可以使用 NetBackup Appliance Web Console 的“设置”>“身份验证”>“用户管理”页面添加、删除和管理 LDAP 用户和用户组。 ■ 您可以使用 NetBackup Appliance Shell Menu 的 Settings > Security > Authentication > LDAP 命令添加和删除 LDAP 用户和用户组。 ■ 您可以将管理员或 NetBackupCLI 角色分配给 LDAP 用户或用户组。 <p>注意：在任何给定时间最多可将 NetBackupCLI 角色分配给九 (9) 个用户组。</p>
Active Directory	<p>Active Directory (AD) 用户或用户组位于外部 AD 服务器上。将设备配置为与 AD 服务器进行通信之后，可以向设备注册这些用户和用户组。注册（添加）用户后，您可以授予或撤消相应的设备访问权限。</p> <p>请参见第 24 页的“关于对 Active Directory 用户进行身份验证”。</p>	<ul style="list-style-type: none"> ■ 您可以使用 NetBackup Appliance Web Console 的“设置”>“身份验证”>“用户管理”页面添加、删除和管理 AD 用户和用户组。 ■ 您可以使用 NetBackup Appliance Shell Menu 的 Settings > Security > Authentication > ActiveDirectory 命令添加和删除 AD 用户和用户组。 ■ 您可以将管理员角色或 NetBackupCLI 角色分配给 AD 用户或用户组。 <p>注意：在任何给定时间最多可将 NetBackupCLI 角色分配给九 (9) 个用户组。</p>
Kerberos-NIS	<p>NIS（网络信息服务）用户或用户组位于外部 NIS 服务器上。与 LDAP 和 AD 实施不同，将设备配置为与 NIS 域进行通信需要 Kerberos 身份验证。必须将现有 Kerberos 服务与您的 NIS 服务器进行关联，然后才能配置设备以注册 NIS 用户。</p> <p>将设备配置为与 NIS 服务器和 Kerberos 服务器进行关联之后，可以向设备注册 NIS 用户和用户组。向设备注册（添加）用户后，您可以授予或撤消相应的设备访问权限。</p> <p>请参见第 25 页的“关于对 Kerberos-NIS 用户进行身份验证”。</p>	<ul style="list-style-type: none"> ■ 您可以使用 NetBackup Appliance Web Console 的“设置”>“身份验证”>“用户管理”页面添加、删除和管理 NIS 用户和用户组。 ■ 您可以使用 NetBackup Appliance Shell Menu 的 Settings > Security > Authentication > Kerberos 命令添加和删除 NIS 用户和用户组。 ■ 您可以将管理员角色或 NetBackupCLI 角色分配给 NIS 用户或用户组。 <p>注意：在任何给定时间最多可将 NetBackupCLI 角色分配给九 (9) 个用户组。</p>

有关配置新用户的详细说明，请参考《NetBackup Appliance 管理指南》。

关于配置用户身份验证

表 2-3 描述了 NetBackup Appliance Web Console 和 NetBackup Appliance Shell Menu 中提供的选项，用于配置设备对不同类型的用户进行身份验证并授予这些用户访问权限。

表 2-3 用户身份验证管理

用户类型	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
“本地”（本机用户）	使用 NetBackup Appliance Web Console 中的“设置”>“身份验证”>“用户管理”选项卡可添加本地用户。 请参见第 31 页的 “关于授权 NetBackup Appliance 用户” 。	Settings > Security > Authentication > LocalUser 下提供了以下命令和选项： <ul style="list-style-type: none"> ■ Clean - 删除所有本地用户。 ■ List - 列出已添加到设备的所有本地用户。 ■ Password - 更改本地用户的密码。 ■ Users - 添加或删除一个或多个本地用户。

用户类型	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
<p>LDAP</p>	<p>您可以在“设置” > “身份验证” > LDAP 下执行以下 LDAP 配置任务：</p> <ul style="list-style-type: none"> ■ 添加新的 LDAP 配置。 ■ 从 XML 文件导入已保存的 LDAP 配置。 ■ 添加、编辑和删除 LDAP 服务器的配置参数。 ■ 识别并挂接 LDAP 服务器的 SSL 证书。 ■ 添加、编辑和删除 LDAP 服务器的属性映射。 ■ 将当前 LDAP 配置（包括用户）导出为 XML 文件。可以在其他设备上导入此文件以配置 LDAP。 ■ 禁用并重新启用 LDAP 配置。 ■ 取消配置 LDAP 服务器。 <p>使用 NetBackup Appliance Web Console 中的“设置” > “身份验证” > “用户管理”选项卡可添加 LDAP 用户和用户组。</p> <p>请参见第 31 页的“关于授权 NetBackup Appliance 用户”。</p>	<p>Settings > Security > Authentication > LDAP 下提供了以下命令和选项：</p> <ul style="list-style-type: none"> ■ Attribute - 添加或删除 LDAP 配置属性。 ■ Certificate - 设置、查看或禁用 SSL 证书。 ■ ConfigParam - 设置、查看和禁用 LDAP 配置参数。 ■ Configure - 配置设备以允许 LDAP 用户使用设备注册并进行身份验证。* ■ Disable - 禁用设备的 LDAP 用户身份验证。 ■ Enable - 启用设备的 LDAP 用户身份验证。 ■ Export - 导出现有 LDAP 配置为 XML 文件。 ■ Groups - 添加或删除一个或多个 LDAP 用户组。仅 LDAP 服务器上已存在的用户组可以添加到设备。 ■ Import - 从 XML 文件导入 LDAP 配置。 ■ List - 列出已添加到设备中的所有 LDAP 用户和用户组。 ■ Map - 添加、删除或显示 NSS 映射属性或对象类。 ■ Show - 查看 LDAP 配置详细信息。 ■ Status - 查看设备上的 LDAP 身份验证状态。 ■ Unconfigure - 删除 LDAP 配置。 ■ Users - 添加或删除一个或多个 LDAP 用户。仅能向设备添加 LDAP 服务器上已存在的用户组。
<p>Active Directory</p>	<p>您可以在“设置” > “身份验证” > Active Directory 下执行以下 AD 配置任务：</p> <ul style="list-style-type: none"> ■ 配置新的 Active Directory 配置。 ■ 取消配置现有的 Active Directory 配置。 <p>使用 NetBackup Appliance Web Console 中的“设置” > “身份验证” > “用户管理”选项卡可添加 Active Directory 用户和用户组。</p> <p>请参见第 31 页的“关于授权 NetBackup Appliance 用户”。</p>	<p>Settings > Security > Authentication > ActiveDirectory 下提供了以下命令和选项：</p> <ul style="list-style-type: none"> ■ Configure - 配置设备以允许 AD 用户使用设备注册并进行身份验证。 ■ Groups - 添加或删除一个或多个 AD 用户组。仅 AD 服务器上已存在的用户组可以添加到设备。 ■ List - 列出已添加到设备中的所有 AD 用户和用户组。 ■ Status - 查看设备上的 AD 身份验证状态。 ■ Unconfigure - 删除 AD 配置。 ■ Users - 添加或删除一个或多个 AD 用户。仅 AD 服务器上已存在的用户可以添加到设备。

用户类型	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Kerberos-NIS	<p>您可以在“设置” > “身份验证” > Kerberos-NIS 下执行以下 Kerberos-NIS 配置任务：</p> <ul style="list-style-type: none"> ■ 配置新的 Kerberos-NIS 配置。 ■ 取消配置现有的 Kerberos-NIS 配置。 <p>使用 NetBackup Appliance Web Console 中的“设置” > “身份验证” > “用户管理”选项卡可添加 Kerberos-NIS 用户和用户组。</p> <p>请参见第 31 页的“关于授权 NetBackup Appliance 用户”。</p>	<p>Settings > Security > Authentication > Kerberos 下提供了以下命令和选项：</p> <ul style="list-style-type: none"> ■ Configure - 配置设备以允许 NIS 用户使用设备注册并进行身份验证。 ■ Groups - 添加或删除一个或多个 NIS 用户组。仅 NIS 服务器上已存在的用户组可以添加到设备。 ■ List - 列出已添加到设备中的所有 NIS 用户和用户组。 ■ Status - 查看设备上的 NIS 和 Kerberos 身份验证状态。 ■ Unconfigure - 删除 NIS 和 Kerberos 配置。 ■ Users - 添加或删除一个或多个 NIS 用户。仅 NIS 服务器上已存在的用户可以添加到设备。

通用用户身份验证准则

对设备上的用户进行身份验证时请使用以下准则：

- 同一时间只能在设备上配置一种用于身份验证的远程用户类型（如 LDAP、Active Directory (AD) 和 NIS）。例如，如果当前在设备上进行身份验证的是 LDAP 用户，则在切换为对 AD 用户进行身份验证之前，必须在该设备上取消配置 LDAP。
- 在任何给定时间最多可将 NetBackupCLI 角色分配给九 (9) 个用户组。
- 无法对现有的本地用户授予 NetBackupCLI 角色。但是，您可以使用 NetBackup Appliance Shell Menu 的 Manage > NetBackupCLI > Create 命令创建本地 NetBackupCLI 用户。
- 您无法向设备添加其用户名、用户 ID 或组 ID 与该设备上现有用户均相同的新用户或用户组。

请参见第 17 页的[“关于 NetBackup Appliance 上的用户身份验证”](#)。

请参见第 31 页的[“关于授权 NetBackup Appliance 用户”](#)。

关于对 LDAP 用户进行身份验证

NetBackup Appliance 使用内置的可插入验证模块 (PAM) 插件支持对轻量级目录访问协议 (LDAP) 用户进行身份验证。此功能允许添加属于 LDAP 目录服务的用户和授权这些用户登录到 NetBackup Appliance。UNIX 服务认为 LDAP 是安装了架构的另外一种类型的用户目录。

使用 LDAP 用户身份验证的先决条件

以下列表包含了在设备上使用 LDAP 用户身份验证的先决条件和要求：

- 必须安装 NetBackup Appliance 2.6 或更高版本才能配置 LDAP 用户身份验证。
- LDAP 架构必须符合 RFC 2307 或 RFC 2307bis。
- 必须开放以下防火墙端口：
 - LDAP 389
 - LDAP OVER SSL/TLS 636
 - HTTPS 443
- 确保 LDAP 服务器可用，并已设置了要向设备注册的用户和用户组。

配置 LDAP 用户身份验证

在设备上注册新的 LDAP 用户和用户组之前，需要配置设备以与 LDAP 服务器通信。完成配置后，设备即可访问 LDAP 服务器的用户信息以进行身份验证。

要配置 LDAP 用户身份验证，可以使用以下任一选项：

- NetBackup Appliance Web Console 中的“设置” > “身份验证” > LDAP。
- NetBackup Appliance Shell Menu 中的 Settings > Security > Authentication > LDAP。

有关如何在设备上配置 LDAP 用户身份验证的详细说明，请参考《NetBackup Appliance 管理指南》和《NetBackup Appliance 命令参考指南》。

关于对 Active Directory 用户进行身份验证

NetBackup Appliance 使用内置的可插入验证模块 (PAM) 插件以支持 Active Directory (AD) 用户的身份验证。此功能允许添加属于 AD 服务的用户并向其授予登录到 NetBackup Appliance 的权限。UNIX 服务认为 AD 是安装了架构的另外一种类型的用户目录。

使用 Active Directory 用户身份验证的先决条件

以下列表包含在设备上使用 AD 用户身份验证的先决条件和要求：

- 必须安装 NetBackup Appliance 2.6.0.3 或更高版本才能配置 AD 用户身份验证。
- 确保 AD 服务可用，并已设置了要向设备注册的用户和用户组。
- 确保使用已授权的域用户凭据来通过设备配置 AD 服务器。
- 通过可将 DNS 请求转发给 AD DNS 服务器的 DNS 服务器配置 NetBackup Appliance。或者，将设备配置为使用 AD DNS 服务器作为名称服务数据源。

配置 Active Directory 用户身份验证

必须将设备配置为与 AD 服务进行通信，才能在设备上注册新的 AD 用户和用户组。配置完成后，设备就能立即访问 AD 服务器的用户信息进行身份验证。您可以使用下列选项配置 AD 身份验证：

- NetBackup Appliance Web Console 中的“设置” > “身份验证” > **Active Directory** 页面。
- NetBackup Appliance Shell Menu 中的 `Settings > Security > Authentication > ActiveDirectory` 命令。

有关如何在设备上配置 AD 用户身份验证的详细说明，请参考《*NetBackup Appliance 管理指南*》和《*NetBackup Appliance 命令参考指南*》。

关于对 Kerberos-NIS 用户进行身份验证

NetBackup Appliance 使用内置的可插入验证模块 (PAM) 插件支持网络信息服务 (NIS) 用户的身份验证。此功能允许添加属于 NIS 目录服务的用户并向用户授予登录到 NetBackup Appliance 的权限。UNIX 服务认为 NIS 是安装了架构的另外一种类型的用户目录。

与 LDAP 和 Active Directory (AD) 的实施不同，将设备配置为对 NIS 用户进行身份验证需要 Kerberos 身份验证。您必须具有与 NIS 域关联的现有 Kerberos 服务才能将设备配置为注册 NIS 用户。

使用具有 Kerberos 的 NIS 用户身份验证的先决条件

以下列表包括了在设备上使用 NIS 用户身份验证的先决条件和要求：

- 必须安装 NetBackup Appliance 2.6.1.1 或更高版本才能使用 Kerberos 配置 NIS 用户身份验证。
- 确保 NIS 域可用，并已设置了要向设备注册的用户和用户组。
- 确保 Kerberos 服务器可用，并已正确配置为与 NIS 域进行通信。
- 由于 Kerberos 的严格时间要求，Symantec 强烈建议使用 NTP 服务器在设备、NIS 服务器和 Kerberos 服务器三者之间同步时间。

配置具有 Kerberos 的 NIS 用户身份验证

您需要将设备配置为可以与 NIS 服务器和 Kerberos 服务器通信，才能在设备上注册新的 NIS 用户和用户组。配置完成后，设备便可访问 NIS 域的用户信息进行身份验证。可以使用下列选项配置 Kerberos-NIS 身份验证：

- NetBackup Appliance Web Console 中的“设置” > “身份验证” > **Kerberos-NIS** 页面。

- NetBackup Appliance Shell Menu 中的 Settings > Security > Authentication > Kerberos 命令。

有关如何在设备上配置 Kerberos-NIS 用户身份验证的详细说明，请参考《NetBackup Appliance 管理指南》和《NetBackup Appliance 命令参考指南》。

关于设备登录提示

通过 NetBackup 设备，可设置当用户尝试登录该设备时显示的文本提示。您可以使用登录提示向用户传达各种消息。登录提示的典型用途包括法律声明、警告消息和公司政策信息。

NetBackup 管理控制台也支持登录提示。默认情况下，设置设备的登录提示时，NetBackup 不会使用提示。但是，在设备登录横幅配置期间，您可以选择将该横幅传播到 NetBackup，以便每当用户尝试登录到 NetBackup 管理控制台时都会显示该横幅。

表 2-4 介绍了支持登录提示的设备接口。设置登录提示后，每个支持提示的设备接口都将显示该提示，例如 NetBackup Appliance Shell Menu 和 SSH。但是，可以选择为 NetBackup 管理控制台打开或关闭登录提示。

表 2-4 支持登录提示的设备接口

接口	说明
SSH	在 SSH 会话中指定用户名后（但在请求输入密码前），将显示登录提示。
IPMI 控制台会话	在 IPMI 控制台会话中指定用户名后（但在请求输入密码前），将显示登录提示。
NetBackup 管理控制台（可选）	每当用户尝试使用 NetBackup 管理控制台登录到该设备时，系统都会显示该登录横幅。此功能使用已存在的登录提示功能，该提示功能属于 NetBackup。有关更多信息，请参考《NetBackup 管理指南，第 1 卷》。

使用 NetBackup Appliance Shell Menu 中的 Settings > Notifications > LoginBanner 配置登录提示。有关更多信息，请参考《NetBackup Appliance 命令参考指南》。

关于用户名和密码规范

NetBackup Appliance 用户帐户的用户名必须符合所选身份验证系统接受的格式。

表 2-5 列出了每个用户类型的用户名规范。

注意： Manage > NetBackupCLI > Create 命令用于创建具有 NetBackupCLI 角色的本地用户。所有本地用户和密码规范均适用于这些用户。

表 2-5 用户名规范

描述	管理员（本地用户）	NetBackupCLI（本地用户）	注册的远程用户
最大长度	没有适用的限制	没有适用的限制	由 LDAP、AD 或 NIS 策略确定
最小长度	2 个字符	2 个字符	由 LDAP、AD 或 NIS 策略确定
限制	用户名不能以这些字符开始： <ul style="list-style-type: none"> ■ 编号 ■ 特殊字符 	用户名不能以这些字符开始： <ul style="list-style-type: none"> ■ 编号 ■ 特殊字符 	由 LDAP、AD 或 NIS 策略确定
包含空格	用户名不能包含空格。	用户名不能包含空格。	由 LDAP、AD 或 NIS 策略确定

密码规范

NetBackup Appliance 密码策略已更新，增强了设备的安全性。设备用户帐户的密码必须符合所选身份验证系统接受的格式。[表 2-6](#) 列出了每个用户类型的密码规范。

表 2-6 密码规范

描述	管理员（本地用户）	NetBackupCLI（本地用户）	注册的远程用户
最大长度	没有适用的限制	没有适用的限制	由 LDAP、AD 或 NIS 策略确定
最小长度	7 个（带限制）或 8 个字符 密码必须至少包含八个字符。	7 个（带限制）或 8 个字符 密码必须至少包含八个字符。	由 LDAP、AD 或 NIS 策略确定

描述	管理员 (本地用户)	NetBackupCLI (本地用户)	注册的远程用户
要求	<ul style="list-style-type: none"> ■ 一个大写字母 ■ 一个小写字母 (a-z) ■ 一个数字 (0-9) ■ 字典中的单词被视为安全强度较弱的密码, 且不可接受。 ■ 最近使用过的七个密码不能重复使用, 且新密码不能类似于之前的密码。 	<ul style="list-style-type: none"> ■ 一个大写字母 ■ 一个小写字母 (a-z) ■ 一个数字 (0-9) ■ 字典中的单词被视为安全强度较弱的密码, 且不可接受。 ■ 最近使用过的七个密码不能重复使用, 且新密码不能类似于之前的密码。 	由 LDAP、AD 或 NIS 策略确定
包含空格	密码不能包含空格。	密码不能包含空格。	由 LDAP、AD 或 NIS 策略确定
最小密码期限	0 天	0 天 注意: 您可以使用中使用的 NetBackup Appliance Shell Menu 中的 Manage > NetBackupCLI > PasswordExpiry 命令管理用户的密码期限。有关更多信息, 请参考《NetBackup Appliance 命令参考指南》。	由 LDAP、AD 或 NIS 策略确定
最大密码期限	99999 天 (不过期)	99999 天 (不过期)	由 LDAP、AD 或 NIS 策略确定
密码历史记录	最近使用过的七个密码不能重复使用, 且新密码不能类似于之前的密码。	无 最近使用过的七个密码不能重复使用, 且新密码不能类似于之前的密码。	由 LDAP、AD 或 NIS 策略确定
密码到期	不适用, 因为密码不过期	使用 Manage > NetBackupCLI > PasswordExpiry 命令管理 NetBackupCLI 用户密码。	由 LDAP、AD 或 NIS 策略确定
密码锁定	无	无	由 LDAP、AD 或 NIS 策略确定

描述	管理员 (本地用户)	NetBackupCLI (本地用户)	注册的远程用户
锁定持续时间	无	无	由 LDAP、AD 或 NIS 策略确定

注意： 为了提高设备环境安全性，Symantec 建议您在初次登录到设备后更改默认的 admin 和 maintenance 帐户密码。您可以使用 NetBackup Appliance Web Console 的“设置” > “密码”页面或 NetBackup Appliance Shell Menu 的 Settings > Password 命令更改密码。

警告： NetBackup Appliance 不支持使用诸如 yppasswd root 或 passwd root 的命令设置维护帐户密码。系统升级后，以此方式设置的密码将被重写。您应该使用 NetBackup Appliance Shell Menu 更改维护帐户密码。

密码加密

NetBackup Appliance 采用了以下密码加密措施：

- 从 NetBackup Appliance 软件版本 2.6.1.1 开始，客户可访问的所有本地设备用户（本地用户、NetBackupCLI 用户、管理员用户和维护用户）的密码哈希均使用 SHA-512 加密算法。每当创建新本地设备用户或更改现有本地设备用户的密码时，密码将使用 SHA-512 进行加密。

注意： 在版本 2.6.1.1 之前，设备会使用多种默认密码加密算法，包括 SHA-512、SHA-256 和 Blowfish。将设备升级到 2.6.1.1 或更高版本后，尽管新的默认算法为 SHA-512，但会保留现有密码哈希。虽然先前的算法仍然可用且安全，但 Symantec 建议在升级到 NetBackup Appliance 软件版本 2.6.1.1 或更高版本后，最终更改所有本地设备用户的密码，以便可以使用新的默认算法。

- 密码历史记录设置为 7 意味着将加密和记录旧密码多达 7 次。如果尝试将旧密码用作新密码，设备将显示令牌处理错误。
- 转换中的密码包含：
 - 通过 SSH 协议保护密码的 SSH 登录。
 - 通过 HTTPS 通信保护密码的 NetBackup Appliance Web Console 登录。

有关密码的详细说明，请参考《NetBackup Appliance 管理指南》。

用户授权

本章节包括下列主题：

- [关于 NetBackup Appliance 上的用户授权](#)
- [关于授权 NetBackup Appliance 用户](#)
- [关于管理员用户角色](#)
- [关于 NetBackupCLI 用户角色](#)

关于 NetBackup Appliance 上的用户授权

NetBackup Appliance 通过用户帐户进行管理。您可以创建本地用户帐户，也可以注册属于远程目录服务的用户和用户组。为使新用户帐户能够登录并访问设备，必须首先对其授权一个角色。默认情况下，新用户帐户未分配角色，因此在您为其授予角色之前无法登录。

表 3-1 NetBackup Appliance 用户角色

角色	描述
管理员	分配了管理员角色的用户帐户具有管理 NetBackup Appliance 的管理权限。管理员用户能够登录、查看和在 NetBackup Appliance Web Console 与 NetBackup Appliance Shell Menu 上执行所有功能。这些用户帐户有权登录到设备，并以超级用户权限运行 NetBackup 命令。 请参见第 34 页的“ 关于管理员用户角色 ”。

角色	描述
NetBackupCLI	<p>分配了 NetBackupCLI 角色的用户帐户只能运行有限的一组 NetBackup CLI 命令，并且对 NetBackup 软件目录之外的目录没有访问权限。这些用户登录到设备后会将其定位到受限的 Shell 菜单，他们可从此菜单管理 NetBackup。</p> <p>NetBackupCLI 用户没有 NetBackup Appliance Web Console 和 NetBackup Appliance Shell Menu 的访问权限。</p> <p>请参见第 34 页的“关于 NetBackupCLI 用户角色”。</p>

以下列表介绍了 NetBackup Appliance 授权的一些特性：

- 通过密码保护登录以防止意外访问设备的能力。
- 仅对已授权设备用户和 NetBackup 进程提供对共享数据的访问。
- 设备中存储的数据本身无法防止知道设备管理员凭据的恶意用户对其进行意外修改或删除。
- 仅允许通过 SSH 或通过 HTTPS 的 NetBackup Appliance Web Console 对 NetBackup Appliance Shell Menu 进行网络访问。您也可以直接将监视器和键盘连接到设备并使用管理凭据登录。
- 所有设备上均禁止访问 FTP、Telnet 和 rlogin。

注意：NetBackup Appliance 当前不限制登录尝试次数，也不强制执行锁定策略。这些功能将在将来的版本中实现。

关于授权 NetBackup Appliance 用户

表 3-2 描述了为通过 NetBackup Appliance Web Console 和 NetBackup Appliance Shell Menu 对新用户和现有用户或用户组进行授权而提供的选项：

表 3-2 用户授权管理

任务	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
管理用户	<p>“设置” > “身份验证” > “用户管理” 下提供了以下选项</p> <ul style="list-style-type: none"> ■ 查看已添加到设备的所有用户。 ■ 展开并查看属于单个用户组的所有用户。 ■ 添加和删除本地用户。 ■ 添加和删除 LDAP/AD/Kerberos-NIS 用户和用户组。 	<p>使用 Settings > Security > Authentication 命令可添加、删除和查看设备用户。</p> <p>请参见第 21 页的“关于配置用户身份验证”。</p>
管理用户权限（角色）	<p>“设置” > “身份验证” > “用户管理” 下提供了以下选项：</p> <ul style="list-style-type: none"> ■ 授予和撤销用户和用户组的管理员角色。 ■ 授予和撤销用户和用户组的 NetBackupCLI 角色。 ■ 将已注册用户组的成员与管理员角色同步。 	<p>Main > Settings > Security > Authorization 下提供了以下命令和选项：</p> <ul style="list-style-type: none"> ■ Grant 对已添加到设备的特定用户和用户组授予管理员和 NetBackupCLI 角色。 ■ List 列出已添加至设备的用户和用户组及其指定角色。 ■ Revoke 对已添加到设备的特定用户和用户组撤销管理员和 NetBackupCLI 角色。 ■ SyncGroupMembers 同步已注册用户组的成员。

有关用户管理的注释

- 无法对现有的本地用户授予 NetBackupCLI 角色。但是，您可以使用 NetBackup Appliance Shell Menu 的 Manage > NetBackupCLI > Create 命令创建本地 NetBackupCLI 用户。
- 在任何给定时间最多可将 NetBackupCLI 角色分配给九 (9) 个用户组。
- Active Directory (AD) 用户组 and 用户名称支持在这些名称中使用连字符。连字符必须位于用户名或用户组名称的第一个和最后一个字符之间。AD 用户名和用户组名称不能以连字符开始或结束。

NetBackup Appliance 用户角色权限

用户角色确定授予用户操作系统或更改系统配置的访问权限。本主题中描述的用户角色特定于 LDAP、Active Directory (AD) 和 NIS 用户。

以下内容描述了设备用户角色及其关联权限：

表 3-3 用户角色和权限

用户角色	权限
NetBackupCLI	用户只能访问 NetBackup CLI。 请参见第 34 页的“关于 NetBackupCLI 用户角色”。
管理员	用户可以访问以下内容： <ul style="list-style-type: none"> ■ NetBackup Appliance Web Console ■ NetBackup Appliance Shell Menu ■ NetBackup 管理控制台 请参见第 34 页的“关于管理员用户角色”。

角色可以应用于单个用户，也可以应用于包含多个用户的组。

无法同时授予两个用户角色权限。但是，在以下情况下，也可以授予 NetBackupCLI 用户访问 NetBackup Appliance Shell Menu 的权限：

- 具有 NetBackupCLI 角色的用户也位于分配了管理员角色的组中。
- 具有管理员角色的用户也位于分配了 NetBackupCLI 角色的组中。

注意：授予用户 NetBackupCLI 和 NetBackup Appliance Shell Menu 的权限时，需要一个额外步骤。用户必须从 NetBackup CLI 输入 `switch2admin` 命令才能访问 NetBackup Appliance Shell Menu。

授予用户和用户组权限的方法如下：

- 在 NetBackup Appliance Web Console 的“设置” > “身份验证” > “用户管理”页面上，单击“授予权限”链接。
- 在 NetBackup Appliance Shell Menu 的 Settings > Security > Authorization 视图中使用以下命令：

```
Grant Administrator Group
Grant Administrator Users
Grant NetBackupCLI Group
Grant NetBackupCLI Users
```

请参见第 21 页的“关于配置用户身份验证”。

请参见第 31 页的“关于授权 NetBackup Appliance 用户”。

关于管理员用户角色

NetBackup Appliance 提供访问控制机制以防止未经授权对设备上的备份数据进行访问。这些机制包括管理用户帐户，该机制提供了较高权限来修改设备配置、监视设备等。仅分配了管理员角色的用户有权配置和管理 NetBackup Appliance。

只能为授权的系统管理员提供管理员角色，以防止对设备配置或扩展磁盘存储中包含的备份数据进行未授权的不当修改。管理员可通过 SSH 使用 NetBackup Appliance Shell Menu 或通过 HTTPS 使用 NetBackup Appliance Web Console 来访问设备。

管理员作为超级用户可以执行以下所有任务：

- 执行设备初始配置。
- 监视硬件、存储和 SDCS 日志。
- 管理存储配置、附加服务器、许可证等
- 更新配置设置，如“日期和时间”、“网络”、“通知”等。
- 还原设备。
- 淘汰设备。
- 为设备应用修补程序。

本地、LDAP、Active Directory (AD) 或 NIS 用户需要具有管理员用户角色权限才能访问和管理设备。添加新用户或用户组之后，使用 NetBackup Appliance Web Console 中的“设置” > “身份验证” > “用户管理”页面可对其授予管理员用户权限。

关于 NetBackupCLI 用户角色

NetBackupCLI 用户可以执行所有 NetBackup 命令、查看日志、编辑 NetBackup touch 文件以及编辑 NetBackup 通知脚本。NetBackupCLI 用户的唯一限制是必须使用超级用户权限运行 NetBackup 命令并且在 NetBackup 软件目录之外没有访问权限。这些用户登录后，他们将转到可以运行 NetBackup 命令的受限 shell。NetBackupCLI 用户共享一个主目录，并且没有 NetBackup Appliance Web Console 或 NetBackup Appliance Shell Menu 的访问权限。

表 3-4 列出了 NetBackupCLI 用户的权利和限制。

表 3-4 设备 NetBackupCLI 用户的权利和限制

权利	限制
<p>NetBackupCLI 用户可以使用 NetBackup Appliance Shell Menu 执行以下操作：</p> <ul style="list-style-type: none"> ■ 运行 NetBackup CLI 并访问 NetBackup 目录和文件。 ■ 使用 <code>cp-nbu-notify</code> 命令修改或创建 NetBackup 通知脚本。 注意：从 2.6.0.2 及更高版本已解除通知脚本限制。 ■ 对包含 NetBackup CLI 的以下目录运行以下 NetBackup 命令： <ul style="list-style-type: none"> ■ <code>/usr/opensv/netbackup/bin/*</code> ■ <code>/usr/opensv/netbackup/bin/admincmd/*</code> ■ <code>/usr/opensv/netbackup/bin/goodies/*</code> ■ <code>/usr/opensv/volmgr/bin/*</code> ■ <code>/usr/opensv/volmgr/bin/goodies/*</code> ■ <code>/usr/opensv/pdde/pdag/bin/mtstcmd</code> ■ <code>/usr/opensv/pdde/pdag/bin/pdcfg</code> ■ <code>/usr/opensv/pdde/pdag/bin/pdusercfg</code> ■ <code>/usr/opensv/pdde/pdconfigure/pdde</code> ■ <code>/usr/opensv/pdde/pdcr/bin/*</code> 	<p>以下限制将加在 NetBackupCLI 用户上：</p> <ul style="list-style-type: none"> ■ NetBackupCLI 用户对 NetBackup 软件目录之外没有访问权限。 ■ 也无法使用编辑器直接编辑 <code>bp.conf</code> 文件。使用 <code>bpsetconfig</code> 命令设置属性。 ■ <code>cp-nbu-config</code> 命令仅支持在 <code>/usr/opensv/netbackup/db/config</code> 目录中创建和编辑 NetBackup touch 配置文件。 ■ 他们无法使用 <code>man</code> 或 <code>-h</code> 命令查看其他任何命令的帮助。

如何以 NetBackupCLI 用户身份运行 NetBackup 命令：

以 NetBackupCLI 用户身份运行命令有以下两种方式：

- 使用受限的 shell
- 使用绝对路径 [“sudo”]，例如：`bppllist` 或 `/usr/opensv/netbackup/bin/admincmd/bppllist`

入侵防护和入侵检测系统

本章节包括下列主题：

- [关于 NetBackup 设备上的 Symantec 数据中心安全性](#)
- [关于 NetBackup Appliance 入侵防护系统](#)
- [关于 NetBackup Appliance 入侵检测系统](#)
- [重新查看 NetBackup 设备上的 SDCS 事件](#)
- [在 NetBackup Appliance 上以非受控模式运行 SDCS](#)
- [在 NetBackup Appliance 上以受控模式运行 SDCS](#)
- [覆盖 NetBackup Appliance 入侵防护系统策略](#)
- [重新启用 NetBackup Appliance 入侵防护系统策略](#)

关于 NetBackup 设备上的 Symantec 数据中心安全性

注意：在之前的设备发行版中，Symantec 数据中心安全性 (SDCS) 叫作 Symantec Critical System Protection (SCSP)。作为升级到 NetBackup Appliance 2.7.1 的一部分，设备 SDCS 代理将设置为非受控模式。如果升级前某个设备运行在受控模式中，则确保在升级完成之后将该设备重置回受控模式。

此外，还必须在 SDCS 管理服务器上更新设备 IPS 和 IDS 策略。不能使用较早的策略来管理运行 2.7.1 或更新软件版本的设备。新策略可从 NetBackup Appliance Web Console 的“监视” > “SDCS 事件”页面中下载。此外，请注意，升级到 NetBackup Appliance 2.7.1 后，IPS 和 IDS 策略的所有可能的自定义规则或支持例外均不可用。

Symantec Data Center Security: Server Advanced (SDCS) 是 Symantec 提供的安全解决方案，用于在数据中心为服务器提供保护。SDCS 软件包含在设备中，在设

备软件安装期间能够自动配置。SDCS 使用基于主机的入侵防护和检测技术，提供基于策略的防护并帮助保证设备的安全。使用最小权限遏制方法并且还能帮助安全管理员集中管理您数据中心中的多个设备。SDCS 代理在启动时运行，并强制执行自定义的 NetBackup 设备入侵防护系统 (IPS) 和入侵检测系统 (IDS) 策略。有关设备的整体 SDCS 解决方案提供下列功能：

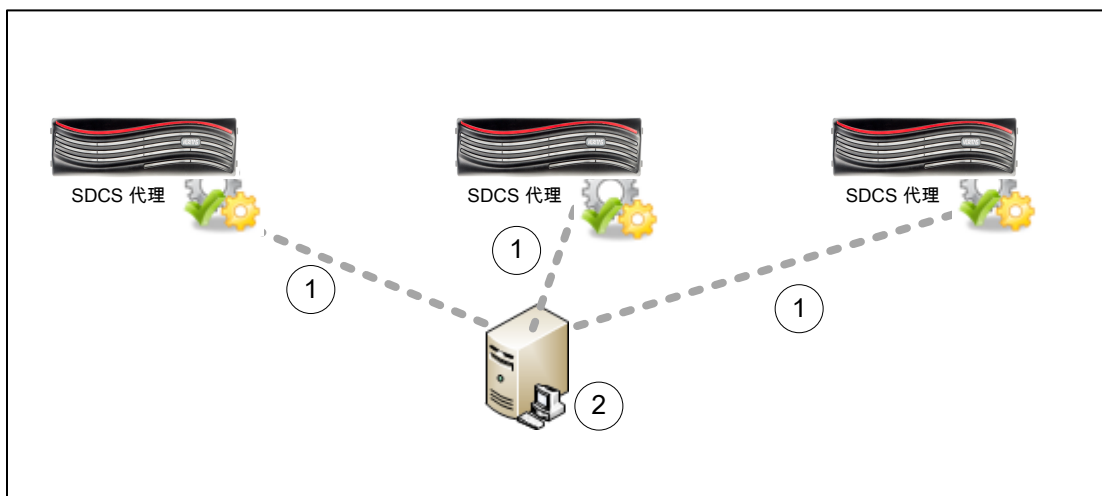
- 加固的 Linux 操作系统组件
防止或遏制因操作系统漏洞造成恶意软件对基础主机系统完整性的损害。
- 数据保护
不论系统权限如何，严格限制对设备数据的访问，仅允许需要访问的程序和活动进行访问。
- 加固的设备堆栈
锁定设备应用程序二进制和配置设置，这样应用程序或可信程序/脚本可严格控制更改。
- 扩展检测和审核功能
对重要用户或系统操作提供增强的可见性，以确保有效且完整的审核跟踪，该审核跟踪将遵从性法规（例如 PCI）作为补偿控制措施。
- 集中管理模式操作
允许您使用中央 SDCS 管理器综合查看多个设备以及 SDCS 管理的任意其他企业系统之中的安全性。

允许设备 SDCS 实现处于非受控模式或处于受控模式。默认情况下，SDCS 在一个未处理的模式运行使用基于主机的入侵防护和检测技术，并且帮助巩固设备。当连接至 SDCS 服务器时，NetBackup 设备处于非受控模式。在受控模式下，可通过 NetBackup Appliance Web Console 监视 SDCS 事件。通过 **Monitor > SDCS Events** 页面，监视所记录的事件。使用 NetBackup 设备 IDS 和 IPS 策略对事件进行监视。这些策略在初始配置时将自动运用。单击 **Filter Logs** 来过滤和查看具体事件。

在受控模式下，设备的 SDCS 代理继续保护设备，同时连接至外部 SDCS 服务器，以便进行集中管理和日志分析。在受控模式下，设备连接至 SDCS 服务器，并且通过 SDCS 管理控制台对事件进行监视。在这种模式下，使用一台单一 SDCS 服务器便可同时监视多个设备。用于将事件发送至 SDCS 服务器的 SDCS 代理与每个 NetBackup 设备进行配置。

图 4-1 对处于受控模式的 SDCS 进行说明。

图 4-1 处于受控模式的 SDCS 实现



为了设置受控模式，您可安装 SDCS 服务器，管理控制台，然后将设备连接至 SDCS 服务器。

通过 **Monitor > SDCS Events** 页面来完成以下操作：

- 下载 SDCS 服务器和控制台
- 安装服务器和控制台
- 下载 NetBackup 设备 IPS 和 IDS 策略
- 使用 SDCS 管理控制台应用上述策略
- 连接 NetBackup 设备和服务器
- 监视适用于连接至该服务器之所有 NetBackup 设备的事件。

通过 **Monitor > SDCS Events > Connect to SDCS server** 来完成以下操作：

- 添加 SDCS 服务器详细信息
- 下载身份验证证书
- 连接至 SDCS 服务器

有关设备 SDCS 实现的完整信息，参考《*NetBackup Appliance 安全指南*》。

关于 NetBackup Appliance 入侵防护系统

设备入侵防护系统 (IPS) 由一个自定义的 Symantec Data Center Security (SDCS) 策略组成，该策略在系统启动时自动运行。IPS 策略是一个内联策略，可以在操作系统对不需要的资源访问行为采取措施之前主动阻止这些行为。

以下列表包含 IPS 策略的一些功能：

- 实时严格限制设备操作系统进程和常见应用程序，例如：
 - `nscd` - 缓存 DNS 请求以减少远程 DNS 查找的次数。
 - `cron`
 - `syslog-ng`
 - `klogd`
 - `rpcd (NFS)`
 - `rpc.idmapd`
 - `rpc.mountd`
 - `rpc.statd`
 - `rpcbind`
- SDCS 代理本身的自我保护，确保 SDCS 的安全和监视功能不受到影响。
- 锁定对系统二进制文件的访问，只有已标识和受信任的应用程序、用户和用户组才能访问。
- 具有限制作用，保护系统并防止应用程序安装软件（例如 `sbin`）或更改系统配置设置（例如 `hosts` 文件）。
- 禁止应用程序执行重要的系统调用，例如 `mknod`、`modctl`、`link`、`mount` 等。
- 禁止未授权的用户或应用程序访问已备份的数据，例如 `/advanceddisk`、`/cat`、`/disk`、`/usr/opensv/kms`、`/opt/NetBackup/db/config/data` 等。
- 限制维护用户对 `root` 帐户的访问。请参见第 43 页的“[覆盖 NetBackup Appliance 入侵防护系统策略](#)”。

关于 NetBackup Appliance 入侵检测系统

设备入侵检测系统 (IDS) 由一个自定义的 Symantec Data Center Security (SDCS) 策略组成，该策略在系统启动时自动运行。IDS 策略是一个实时策略，用于监视重大系统事件和关键配置更改，并对感兴趣的事件选择性地采取补救措施。

以下列表包含 IDS 策略监视的一些事件：

- 用户登录、注销和失败的登录尝试
- Sudo 命令
- 用户添加、用户删除和密码更改
- 用户组添加、用户组删除和成员修改
- 系统自动启动选项更改
- 对所有系统目录和文件的修改，包括核心系统文件、核心系统配置文件、安装程序和通用的后台驻留程序文件
- NetBackup 服务启动和停止
- 检测到的来自 UNIX Rootkit 文件/目录检测、UNIX Worm 文件/目录检测、恶意模块检测、可疑权限更改检测等的系统攻击
- 所有 NetBackup Appliance Web Console 和 NetBackup Appliance Shell Menu 活动的审核，包括 maintenance、root 和 NetBackupCLI 用户的 shell 操作。

重新查看 NetBackup 设备上的 SDCS 事件

可以使用 **Monitor > SDCS Events** 页面查看 Symantec Data Center Security (SDCS) 日志。这些审核日志有助于检测设备上的安全缺口和异常活动。审核日志中的事件包括以下详细信息：

- 时间 - 显示已记录事件的时间戳。
- 人员 - 显示事件发生时登录的用户。
- 内容 - 显示事件的描述和涉及的资源。
- 方式 - 显示进程名称、进程 ID、操作权限以及沙盒详细信息。
- 严重性 — 显示事件的严重性。
- 强制操作 - 显示是允许还是拒绝了事件。

使用 [表 4-1](#) 中说明的严重性级别类型检索和表示 SDCS 事件

表 4-1 SDCS 事件严重性级别类型

严重性级别类型	描述	事件示例
信息	严重性级别为“信息”的事件包含有关正常系统操作的信息。	<p>例如，以下消息提供了与常规事件相关的基本信息。</p> <pre> general CLISH message Event source: SYSLOG PID: 30315 Complete message: May 21 06:58:55 nb-appliance CLISH[30315]: User admin executed Return </pre>
通知	严重性级别为“通知”的事件包含有关正常系统操作的信息。	<p>有助于确认事件是否成功执行的事件记录为“通知”。例如，以下消息有助于用户了解事件是否已成功执行。</p> <pre> successful SUDO to root Event source: SYSLOG [sudo facility] Command: /bin/su From Username: AppComm To Username: root Port: unknown </pre>
警告	严重性级别为“警告”的事件表示已经由 SDCS 处理的意外活动或问题。这些警告消息可能表示在目标计算机上的服务或应用程序未正确运行所应用的策略。调查策略冲突之后，可以配置该策略，如果需要，可以允许服务或应用程序访问特定资源。	<p>例如，以下事件有助于识别意外活动，如来自本地 IP 地址的人站连接。</p> <pre> Inbound connection allowed from <IPaddress> to local address. </pre>

严重性级别类型	描述	事件示例
重度	严重性级别为“重度”的事件比“警告”级别的影响大，比“严重”级别的影响小。	例如，以下事件可帮助识别未授权的访问。 General luser message Event source:SYSLOG Complete message: Feb 5 21:57 luser Unauthorized user by luser Denying access to system.
严重	严重性级别为“严重”的事件表示可能需要管理员干预来更正的活动或问题。	例如，以下事件有助于识别以意外方式影响设备的严重事件。 Group Membership for "group1" CHANGED from 'admin1' to 'admin2'

更多有关 SDCS 审核日志检索的信息，请参考 *NetBackup 设备管理指南*。

有关设备操作系统日志的信息，例如 `syslogs` 以及其他设备日志，请参见第 49 页的“关于 NetBackup Appliance 日志文件”。

在 NetBackup Appliance 上以非受控模式运行 SDCS

设备 Symantec Data Center Security (SDCS) 实现在非受控模式或受控模式中运行。非受控模式是配置设备的默认模式。在非受控模式下，不使用外部 SDCS 服务器即可保护设备并对其进行审核。即使在非受控模式下，也会应用 IDS 和 IPS 策略，在设备启动时便可对其提供保护。

如果管理员是设备的唯一所有者并主要涉及备份管理，建议使用非受控模式。

您可以从 NetBackup Appliance Web Console (“**监视**” > “**SDCS 事件**”) 和 NetBackup Appliance Shell Menu (`Main_Menu > Monitor > SDCS`) 监视 SDCS 事件。从这些接口

在 NetBackup Appliance 上以受控模式运行 SDCS

允许设备 SDCS 实现处于非受控模式或处于受控模式。在受控模式下，使用外部 SDCS 服务器与一个或多个设备上的 SDCS 代理进行通信并对其进行管理。SDCS 服务器使用的 IPS 和 IDS 策略与受控模式下使用的策略相同。您可以从 NetBackup Appliance Web Console 中下载 SDCS 服务器、控制台和策略。

仅建议安全管理员或者非常熟悉 SDCS 的现有 SDCS 客户使用受控模式。

使用受控模式的优势:

- 帮助提供单独的工具供“备份管理员”角色和“安全管理员”角色使用。
- 使用单一 SDCS 服务器和控制台提供多个设备的集中式安全管理。
- 提供存档和导出日志的功能。
- 为监视、报告和设置警报提供公用控制台。
- 在 Symantec 基线的基础上扩展 IPS 和 IDS 策略以符合您的数据中心标准。

在 SDCS 受控模式下配置设备

- 1 如果尚未在环境中下载和安装 SDCS，可以直接从 NetBackup Appliance Web Console 下的“监视”>“SDCS 事件”中下载服务器软件包和控制台软件包。您需要确保控制台可以连接到 SDCS 服务器且服务器可以连接到设备。
- 2 从设备下载 IPS 和 IDS 策略并使用 SDCS 控制台导入它们。您可以直接从 NetBackup Appliance Web Console 下的“监视”>“SDCS 事件”中下载这些策略。
- 3 将设备连接到 SDCS 服务器。您可以通过 NetBackup Appliance Web Console 下的“监视”>“SDCS 事件”或 NetBackup Appliance Shell Menu 下的 Monitor > SDCS 连接到 SDCS 服务器。
- 4 使用 SDCS 控制台将 IPS 和 IDS 策略应用到已连接的设备。

覆盖 NetBackup Appliance 入侵防护系统策略

要阻止访问根帐户，设备要求您首先禁用入侵防护系统 (IPS) 策略。例如，如果不禁用 IPS 策略，Support > Maintenance 下的 elevate 命令会失败。

警告：由于禁用 IPS 策略会使系统处于风险中并且使系统易受到攻击，因此不建议执行此操作。

您可以使用 NetBackupCLI 用户角色运行 NetBackup 命令，而无需覆盖 IPS 策略。请参见第 34 页的“关于 NetBackupCLI 用户角色”。

注意：覆盖 IPS 策略仅禁用设备入侵防护系统。设备入侵检测系统 (IDS) 日志记录仍然启用，且仍然记录维护帐户下的每个活动。

覆盖设备 IPS 策略

- 1 以管理员身份登录到 NetBackup Appliance Shell Menu。
- 2 输入 `Support > Maintenance` 命令以启动维护模式登录提示。输入维护用户帐户密码以登录到维护模式。

```
app123.Support> Maintenance
<!-- Maintenance Mode --!>
maintenance's password:
```

- 3 在维护模式下，键入以下命令以覆盖 IPS 策略：

```
/opt/Symantec/sdcssagent/IPS/sisipsoverride.sh
```

显示以下消息：

```
Symantec Critical Protection Policy Override

Agent Version: 6.5.0 (build 355)

Current Policy: NetBackup Appliance Prevention Policy, r33

Policy Prevention: Enabled

Policy Override: Allowed

Override State: Not overridden

To override the policy and disable protection,
enter your login password.

Password:
```

- 4 输入维护用户帐户密码。将显示以下选项：

```
Choose the type of override that you wish to perform:
```

1. Override Prevention except for Self Protection
2. Override Prevention Completely

```
Choice?
```

5 输入 **1** 覆盖除自我保护之外的防护。

注意：Symantec 建议您使用选项 1。选择“选项 1”只允许对 NetBackup Appliance Shell Menu 进行修改，而不允许对 SDCS 代理进行修改。

将显示以下选项：

```
Choose the amount of time after which to automatically re-enable:
```

1. 15 minutes
2. 30 minutes
3. 1 hour
4. 2 hours
5. 4 hours
6. 8 hours

6 根据调试支持案例所需的时间，输入合适的数字（1 到 7）。

设备将显示以下消息：

```
Enter a comment. Press Enter to continue.
```

7 输入相关注释，解释覆盖原因。例如：

```
Enter a comment. Press Enter to continue.
```

**Disabling the security policy for
debugging support case no - XYZ**

设备将覆盖该策略并显示以下消息：

```
Please wait while the policy is being overridden.
```

```
.....
```

```
The policy was successfully overridden.
```

```
maintenance - !> elevate
```

您现在应该拥有访问 root 帐户进行设备调试的权限了。

重新启用 NetBackup Appliance 入侵防护系统策略

可以使用以下过程从维护模式重新启用入侵安全策略 (IPS)。

重新启用 Symantec Intrusion 安全策略：

- 1 以管理员身份登录到 NetBackup Appliance Shell Menu。
- 2 输入 `Support > Maintenance` 命令以启动维护模式登录提示。输入维护用户帐户密码以登录到维护模式。

```
app123.Support> Maintenance
<!-- Maintenance Mode --!>
maintenance's password:
```

- 3 在“维护”模式下，键入以下命令以重新启用 IPS 策略：

```
/opt/Symantec/sdcssagent/IPS/sisipsoverride.sh
```

显示以下消息：

```
Symantec Critical Protection Policy Override
```

```
Agent Version: 6.5.0 (build 355)
```

```
Current Policy: NetBackup Appliance Prevention Policy, r33
```

```
Policy Prevention: Enabled
```

```
Policy Override: Allowed
```

```
Override State: Overriden
```

```
Override Type: Prevention Overriden except for Self-Protection
```

```
Override User: maintenance
```

```
Previous Comment: This is an example.
```

```
Auto re-enable in: 13 minutes, 31 seconds
```

Do you wish to:

1. Re-enable the Policy.
2. Extend the Override Time.

- 4 输入 **1** 以重新启用 IPS 策略。

显示以下消息：

```
Enter a comment. Press Enter to continue.
```

- 5 输入相关注释，例如：

```
Enter a comment. Press Enter to continue.
```

The policy is re-enabled.

设备将重新启用该策略并显示以下消息：

```
Please wait while the policy is being re-enabled.
```

```
.....
```

```
The policy was successfully re-enabled.
```

日志文件

本章节包括下列主题：

- [关于 NetBackup Appliance 日志文件](#)
- [关于“收集日志文件”向导](#)
- [使用 Support 命令查看日志文件](#)
- [可使用 Browse 命令从何处查找 NetBackup Appliance 日志文件](#)
- [通过 Datacollect 命令收集设备日志](#)

关于 NetBackup Appliance 日志文件

日志文件可帮助您识别和解决您设备可能遇到的所有问题。

NetBackup Appliance 能够捕获与硬件、软件、系统和性能相关的数据。日志文件可捕获设备运行等信息、取消配置的卷或阵列等问题、温度或电池问题以及其他详细信息。

[表 5-1](#) 描述了可用于访问设备日志文件的方法。

表 5-1 查看日志文件

起始位置...	使用...	日志详细信息
NetBackup Appliance Web Console	<p>可以使用 NetBackup Appliance Web Console 中的“收集日志文件”向导从设备收集日志文件。</p> <p>请参见第 51 页的“关于“收集日志文件”向导”。</p>	<ul style="list-style-type: none"> ■ “NetBackup 复制日志”工具 (nbcplogs) 创建的日志 ■ 设备日志 (包括高可用性、硬件和事件日志) ■ 操作系统日志 ■ 与介质服务器重复数据删除池 (MSDP) 相关的所有日志 ■ 与 NetBackup Appliance Web Console 相关的所有日志 ■ 有关 NetBackup 和操作系统的诊断信息 ■ 硬件和存储设备日志
NetBackup Appliance Web Console	<p>可以使用 NetBackup Appliance Web Console 中的“监视” > “SDCS 审核视图”屏幕检索设备的审核日志。请参见第 40 页的“重新查看 NetBackup 设备上的 SDCS 事件”。</p>	设备审核日志
NetBackup Appliance Shell Menu	<p>可以使用 Main > Support > Logs > Browse 命令打开 LOGROOT/> 提示符。可以使用诸如 ls 和 cd 等命令处理设备日志目录和获取各种日志。</p> <p>请参见第 52 页的“使用 Support 命令查看日志文件”。</p>	<ul style="list-style-type: none"> ■ 设备配置日志 ■ NetBackup 日志、卷管理器日志以及 openv 目录中包含的 NetBackup 日志 ■ 设备操作系统 (OS) 安装日志 ■ NetBackup 管理 Web 用户界面日志和 NetBackup Web 服务器日志 ■ NetBackup 52xx 设备的设备日志

起始位置...	使用...	日志详细信息
NetBackup Appliance Shell Menu	可以使用 Main > Support > Logs > VxLogView Module <i>ModuleName</i> 命令访问设备 VxUL (统一) 日志。您也可以使用 Main > Support > Share Open 命令和桌面映射、共享和复制 VxUL 日志。	设备统一日志: <ul style="list-style-type: none"> ■ All ■ CallHome ■ Checkpoint ■ Commands ■ Common ■ Config ■ CrossHost ■ Database ■ Hardware ■ HWMonitor ■ Network ■ RAID ■ Seeding ■ SelfTest ■ Storage ■ SWUpdate ■ Trace
NetBackup Appliance Shell Menu	可以使用 Main > Support > DataCollect 命令收集存储设备日志。 请参见第 54 页的“ 通过 Datacollect 命令收集设备日志 ”。	设备存储设备日志
NetBackup-Java 应用程序	如果 NetBackup-Java 应用程序出现问题, 则可以使用本节中的脚本收集与技术支持联系所需的信息。	与 NetBackup-Java 应用程序相关的日志

关于“收集日志文件”向导

可以使用 NetBackup Appliance Web Console 中的“收集日志文件”向导从设备收集日志文件。通过该向导, 可以收集 NetBackup、设备、操作系统、NBSU (NetBackup 支持实用程序)、DataCollect 及其他项目的不同类型的日志文件。

可从任意 NetBackup Appliance 收集日志文件。

生成日志文件后, 可将这些文件通过电子邮件发送给收件人、下载到您的计算机或上载到 Symantec 支持。

有关设备诊断中心的信息，请参考下列内容：

请参见第 49 页的[“关于 NetBackup Appliance 日志文件”](#)。

使用 Support 命令查看日志文件

您可以使用以下部分查看日志文件信息。

使用 Support > Logs > Browse 命令查看日志：

- 1 通过在 NetBackup Appliance Shell 菜单中使用 Main_Menu > Support > Logs，然后运行 Browse 命令，进入浏览模式。此时将出现 LOGROOT/> 提示符。
- 2 要显示设备上的可用日志目录，请在 LOGROOT/> 提示符下键入 ls。
- 3 要查看任何日志目录中的可用日志文件，请使用 cd 命令将目录更改为您选择的日志目录。提示符将更改以显示您所在的目录。例如，如果您将目录更改为 GUI 目录，则提示符将显示为 LOGROOT/GUI/>。在此提示符下，您可以使用 ls 命令以显示 GUI 日志目录中的可用日志文件。
- 4 要查看文件，请使用 less <FILE> 或 tail <FILE> 命令。文件使用 <FILE> 来标记，目录使用 <DIR> 来标记。

请参见第 53 页的[“可使用 Browse 命令从何处查找 NetBackup Appliance 日志文件”](#)。

使用 Support > Logs 命令查看 NetBackup Appliance 统一 (VxUL) 日志：

- 1 使用 Support > Logs > VXLogView 命令查看 NetBackup Appliance 统一 (VxUL) 日志。在 Shell 菜单中输入命令，并使用下列选项之一：
 - Logs VXLogView JobID *job_id*
用于显示特定工作 ID 的调试信息。
 - Logs VXLogView Minutes *minutes_ago*
用于显示特定时段的调试信息。
 - Logs VXLogView Module *module_name*
用于显示特定模块的调试信息。可用模块名称包括：All、CallHome、Checkpoint、Common、Config、Database、Hardware、HWMonitor、Network、RAID、Seeding、SelfTest、Storage、SWUpdate、Commands、CrossHost 和 Trace。
用于显示特定模块的调试信息。可用模块名称包括：All、CallHome、Checkpoint、Common、Config、Database、FTMS、Hardware、

HWMonitor、Network、RAID、Seeding、SelfTest、Storage、SWUpdate、Commands、CrossHost 和 Trace。

- 2 如果需要，可以使用 Main > Support > Share Open 命令复制统一日志。使用桌面映射、共享和复制日志。

注意：NetBackup Appliance 统一日志与 NetBackup 统一日志不相同，例如 nbpem 或 nbjm。NetBackup Appliance 有自己的统一日志集。要收集 NetBackup 统一日志，使用收集日志向导并选择 **NetBackup**。

您也可以使用 Main_Menu > Support > Logs 命令执行以下操作：

- 将日志文件上载到 Symantec 技术支持。
- 设置日志级别。
- 导出或删除 CIFS 和 NFS 共享。

注意：NetBackup Appliance VxUL 日志不再被 cron 作业或预定任务存档。此外，日志回收已启用，且日志文件的默认数量已设置为 50。

有关如何使用上述命令的更多信息，请参考《NetBackup Appliance 命令参考指南》。

请参见第 49 页的“关于 NetBackup Appliance 日志文件”。

可使用 Browse 命令从何处查找 NetBackup Appliance 日志文件

表 5-2 提供了可以使用 Support > Logs > Browse 命令访问的日志和日志目录的位置。

表 5-2 NetBackup Appliance 日志文件位置

设备日志	日志文件位置
配置日志	<DIR> APPLIANCE config_nb_factory.log
自检报告	<DIR> APPLIANCE selftest_report

设备日志	日志文件位置
主机更改日志	<DIR> APPLIANCE hostchange.log
NetBackup 日志、卷管理器日志以及 openv 目录中包含的 NetBackup 日志	<DIR> NBU <ul style="list-style-type: none"> ■ <DIR> netbackup ■ <DIR> openv ■ <DIR> volmgr
操作系统 (OS) 安装日志	<DIR> OS boot.log boot.msg boot.omsg messages
NetBackup 重复数据删除 (PDDE) 配置脚本日志	<DIR> PD pdde-config.log
NetBackup 管理 Web 用户界面日志和 NetBackup Web 服务器日志	<DIR> WEBGUI <ul style="list-style-type: none"> ■ <DIR> gui ■ <DIR> webserver
设备日志	/tmp/DataCollect.zip 可以使用 Main > Support > Logs > Share Open 命令将 DataCollect.zip 复制到您的本地文件夹。

请参见第 49 页的[“关于 NetBackup Appliance 日志文件”](#)。

通过 Datacollect 命令收集设备日志

可以使用 Main > Support **Shell** 菜单中的 Datacollect 命令收集设备日志。可以和 Symantec 支持团队共享这些设备日志，以解决设备相关问题。

现在，DataCollect 命令连同操作系统、IPMI 和存储日志一起收集以下日志：

- 修补程序日志
- 文件系统日志
- 测试硬件日志
- CPU 信息

- 磁盘性能日志
- 内存信息
- 硬件信息

通过 Datacollect 命令收集设备日志

- 1 登录到管理 NetBackup Appliance Shell 菜单。
- 2 打开 Support 菜单。要打开 Support 菜单，请使用以下命令：

```
Main > Support
```

设备会显示支持菜单中的所有子任务。

3 输入 DataCollect 命令以收集存储设备日志。

设备会启动以下过程：

```

appliancel23.Support > DataCollect
Gathering release information
Gathering dmidecode logs
Gathering ipmitool sel list logs
Gathering fwtermlog logs
Gathering AdpEventLog logs
Gathering smartctl logs
Gathering disk performance logs
Gathering ipmiutil command output
Gathering cpu information
Gathering memory information
Gathering sdr logs
Gathering adpallinfo logs
Gathering encinfo logs
Gathering cfgdsply logs
Gathering ldpdinfo logs
Gathering pdlist logs
Gathering fru logs
Gathering adpbucmd logs
Gathering os logs
Gathering adpalilog logs
Gathering dfinfo logs
Gathering vxprint logs
Gathering Test Hardware logs
Gathering patch logs

```

```

All logs have been collected in /tmp/DataCollect.zip
Log file can be collected from the appliance shared folder
- \\appliancel23\logs\APPLIANCE
Share can be opened using Main->Support->Logs->Share Open

```

```

=====End of DataCollect=====
All logs have been collected in /tmp/DataCollect.zip

```

设备会在 /tmp/DataCollect.zip 文件中生成设备日志。

- 4 使用 Main > Support > Logs > Share Open 命令将 DataCollect.zip 复制到本地文件夹。
- 5 可以将 DataCollect.zip 文件发送到 Symantec 支持团队，以便解决问题。

请参见第 49 页的[“关于 NetBackup Appliance 日志文件”](#)。

操作系统安全

本章节包括下列主题：

- [关于 NetBackup Appliance 操作系统安全](#)
- [NetBackup Appliance 操作系统中包含的主要组件](#)
- [NetBackup Appliance 上已禁用的服务帐户](#)
- [NetBackup Appliance 漏洞扫描](#)

关于 NetBackup Appliance 操作系统安全

NetBackup Appliance 运行 Symantec 提供的自定义 Linux 操作系统 (OS)。每个 NetBackup Appliance 软件版本均包含最新的设备操作系统和 NetBackup 软件。除了常规的安全修补程序和更新以外，设备操作系统还包含以下安全功能和增强功能：

- 更新和调整过的基于 Red Hat Enterprise Linux (RHEL) 的操作系统平台，该平台可以在兼容和可靠的硬件平台上打包和安装所有必要的软件组件。
- Symantec Data Center Security: Server Advanced (SDCS) 入侵防护与入侵检测软件，该软件通过隔离并沙盒化每个进程和所有系统文件加固了设备操作系统并保护备份数据。
- 使用行业认可的漏洞扫描程序对 NetBackup Appliance 进行常规扫描。发现的所有漏洞均会在定期发布的设备软件中使用紧急工程二进制文件 (EEB) 进行修补。如果在版本计划之间的空档期确定了安全威胁，请与 Symantec 支持联系获取已知的解决方案。
- 删除或禁用了非用户和未使用的服务帐户。
- 设备操作系统包含已编辑的内核参数以保护设备免受诸如拒绝服务 (DoS) 等攻击。例如，sysctl 设置 net.ipv4.tcp_syncookies 已添加到 /etc/sysctl.conf 配置文件以实现 TCP SYN Cookie。

- 禁用了不必要的 `runlevel` 服务。设备操作系统使用 `runlevels` 确定应运行的服务，并允许在系统上执行特定工作。
- 禁用了 `FTP`、`telnet` 和 `rlogin` (`rsh`)。限制为使用 `ssh`、`scp` 和 `sftp`。
- 通过将 `AllowTcpForwarding no` 和 `X11Forwarding no` 添加到 `/etc/ssh/sshd_config`，从而禁用了对 `SSH` 的 `TCP` 转发。
- 设备操作系统上禁用了 `IP` 转发并且不允许在 `TCP/IP` 堆栈上路由。此功能可以防止某个子网上的主机将设备当作路由器使用以访问另一个子网上的主机。
- `NetBackup Appliance` 不允许网络接口上的 `IP` 别名（配置多个 `IP` 地址）。此功能可以防止对同一 `NIC` 端口上多个网段的访问。
- `UMASK` 值确定了新创建文件的文件权限。它指定了不应默认提供给新创建文件的权限。虽然大多数 `UNIX` 系统中 `UMASK` 的默认值是 `022`，但 `NetBackup Appliance` 的 `UMASK` 设置为 `077`。
- 搜索并修复了设备操作系统中找到的所有全局可写入文件的权限。
- 搜索并修复了设备操作系统中找到的所有孤立的和不属于任何人的文件和目录的权限。

NetBackup Appliance 操作系统中包含的主要组件

表 6-1 列出了设备操作系统主要软件组件的列表：

表 6-1 NetBackup Appliance 操作系统 2.7.1 版中包含的主要软件组件的列表

软件组件	版本
Red Hat Enterprise Linux (RHEL)	6.6 注意： 设备操作系统合并了 RHEL 6.7 中的若干软件包和更新。
Symantec NetBackup	7.7.1
Symantec Storage Foundation	6.2 注意： Symantec Storage Foundation 安装已修改并调整以实现设备的最佳性能。
Symantec Data Center Security: Server Advanced (SDCS)	6.5
Symantec Perl	5.16.1.27
Java Runtime Environment (JRE)	1.8.0_51

软件组件	版本
Apache Tomcat	8.0.24
RabbitMQ	3.5.0-1
Intel IPMI Utils	2.9.5-1
Intel IPMI Tools	1.8.11-28

NetBackup Appliance 上已禁用的服务帐户

下面列出的服务帐户已经在 NetBackup Appliance 操作系统中禁用：

- Batch jobs daemon
- bin
- daemon
- DHCP server daemon
- FTP account
- User for haldaemon
- User for OpenLDAP
- Mailer daemon
- Manual pages viewer
- User for D-BUS
- Name server daemon
- News system
- nobody
- NTP daemon
- PolicyKit
- Postfix Daemon
- SSH daemon
- Novell Customer Center User
- UNIX-to-UNIX CoPy system
- wwwrun WWW daemon Apache
- NBE Web service ntbecmpi

NetBackup Appliance 漏洞扫描

Symantec 使用行业认可的漏洞扫描程序对 NetBackup Appliance 定期进行测试。对设备构成安全威胁的任何新漏洞均会稍后在常规软件版本中进行修补。对于高度严重的漏洞，Symantec 可选择在紧急工程二进制文件 (EEB) 中发布修补程序，以尽快解决潜在的安全威胁。表 6-2 列出了用于扫描 NetBackup Appliance 软件版本 2.7.1 的软件产品。

表 6-2 用于扫描 NetBackup Appliance 的软件

安全扫描程序	版本
Nessus™	5.2.7
QualysGuard™	7.14.37-1
Trustwave App Scanner™	8.0.0

数据安全

本章节包括下列主题：

- [关于数据安全](#)
- [关于数据完整性](#)
- [关于数据分类](#)
- [关于数据加密](#)

关于数据安全

NetBackup Appliance 支持策略驱动机制以保护客户端和 NetBackup 服务器上的数据。通过以下措施的实施避免了数据泄漏并加强了防护，从而提高了数据安全性：

- 实时入侵检测机制可审核对 NetBackup Appliance 上存储的机密数据的访问。
- 记录并实时跟踪所有还原。
- 仅授权设备用户和进程访问备份的数据。
- NetBackup Appliance 确保在进行备份时重复数据删除池 (MSDP) 中的所有备份数据均使用循环冗余校验 (CRC) 数字签名进行标记。维护任务会持续重新计算 CRC 数字签名并将其与原始签名进行比较，从而检测重复数据删除池中是否存在任何不需要的篡改或损坏。
- 通过密码保护登录到设备防止了对设备存储的意外访问。
- 仅授权的用户和 NetBackup 进程能够访问共享数据。
请参见第 60 页的“[NetBackup Appliance 上已禁用的服务帐户](#)”。
- 使用自动通报功能，利用 HTTPS 协议和端口 443 连接到 Symantec AutoSupport 服务器以上传硬件和软件信息。Symantec 支持可使用此信息解决可能报告的任何问题。此信息在 Symantec 安全操作中心保留 90 天，之后将被清除。

- 支持“检查点”，允许您轻松将整个系统回滚到某个即时点以撤消任意错误配置。检查点会捕获以下组件：
 - 设备操作系统
 - 设备软件
 - NetBackup 软件
 - 主服务器上的磁带介质配置
 - 网络配置
 - LDAP 配置（如果存在）
 - 光纤通道配置
 - 任何先前应用的修补程序

注意：关键组件（例如 NetBackup 目录库、KMS 数据库或 NBAC 数据库）可能需要进行额外配置。

NetBackup Appliance 软件没有任何内置的传输/会话安全性，除非是 HTTP（Web 服务）协议。如果设备软件在不可信的网络环境中运行，Symantec 建议在 NetBackup 主机之间部署 VPN（虚拟专用网络）解决方案，例如 IPsec。

关于数据完整性

NetBackup Appliance 中的“重复数据删除池”存储提供了以下数据完整性检查以确保成功还原数据：

对存储在重复数据删除池中的备份数据持续进行端到端验证

任何可能导致数据损坏的意外数据修改都可自动检测到并尽可能进行纠正。任何不可恢复的数据损坏问题都将通过 NetBackup 控制台的磁盘报告 UI（“NetBackup 管理控制台”>“报告”>“磁盘报告”）报告给存储管理员。

对存储在重复数据删除池中的备份数据持续进行循环冗余校验 (CRC) 验证

在重复数据删除池中会计算为备份作业创建的每个对象的 CRC 值。后台进程会持续验证 CRC 签名以确保备份数据不会被篡改并且可以在需要时成功还原。重复数据删除池设计会自然地将任意损坏数据从池中未损坏分区隔离，防止损坏在整个重复数据删除池中传播。

关于数据分类

数据分类表示一组备份需求，使为不同需求的数据配置备份更加容易。例如，黄金级别分类的备份必须转到黄金级别数据分类的存储生命周期策略。NetBackup Appliance 支持与 NetBackup 相同的数据分类属性。

NetBackup “数据分类” 属性指定了存储备份的存储生命周期策略的分类。例如，黄金级别分类的备份必须存储到黄金级别数据分类的存储单元。

NetBackup 提供以下默认数据分类：

- 白金
- 黄金
- 银
- 铜

此属性是可选的，仅在要将备份写入存储生命周期策略时适用。如果列表显示“无数据分类”，则策略会使用“策略存储”列表中显示的存储选择。如果选择了数据分类，则会用分类 ID 标记策略所创建的所有映像。

关于数据加密

NetBackup Appliance 提供以下加密方法来保护静态数据和使用中的数据：

- 以加密格式且使用安全通道传输数据。通过客户端加密和复制即可进行这些配置。如果不使用这些选项，则数据不在 NetBackup Appliance 中时我们依赖网络基础架构来保护使用中的数据。
- 在 MSDP 中提供 blowfish 128 位加密并且允许使用唯一密钥加密每个块，从而进一步增强安全性。
- 支持使用 NetBackup 密钥管理服务 (KMS) (与 NetBackup Enterprise Server 7.1 集成) 加密。请参见第 64 页的“KMS 支持”。
- 支持 NetBackup Access Control (NBAC) 功能，该功能将 NetBackup Product Authentication 和 NetBackup Product Authorization 合并到了 NetBackup Appliance 主服务器中。

KMS 支持

NetBackup Appliance 支持由 NetBackup 密钥管理服务 (KMS) 管理的加密，而 NetBackup 密钥管理服务已集成在 NetBackup Enterprise Server 7.1 中。配置为主服务器或媒体服务器的 2.6 或更高版本的 NetBackup Appliance 支持 KMS。在设备主服务器上恢复 KMS 的唯一一种支持方法是重新生成数据加密密钥。

KMS 具有以下关键特征：

- 无需额外的许可证。
- 是基于主服务器的对称密钥管理服务。
- 可使用与之连接或与另一个 NetBackup Appliance 连接的磁带设备将其作为主服务器进行管理。
- 其按照 T10 标准（例如 LTO4 或 LTO5）管理磁带驱动器的对称密码密钥。
- 其设计为使用基于卷池的磁带加密。
- 可用于内置硬件加密功能的磁带硬件。
- 可由 NetBackup CLI 管理员使用 NetBackup Appliance Shell Menu 或 KMS 命令行界面 (CLI) 进行管理。

注意：在版本低于 2.6 的 NetBackup Appliance 中，只有当设备配置为媒体服务器时才支持 KMS。需要非设备主服务器才能使用连接到 NetBackup Appliance 的设备管理 KMS。

关于 KMS 下使用的密钥

KMS 将从密码生成密钥或自动生成密钥。表 7-1 列出了与 KMS 关联并包含密钥相关信息的文件。

表 7-1 KMS 文件

KMS 文件	描述	位置
密钥文件或密钥数据库	此为最重要的 KMS 文件。其包含数据加密密钥。	/usr/openv/kms/db/KMS_DATA.dat
主机主密钥	它包含使用 AES 256 加密并保护 KMS_DATA.dat 密钥文件的加密密钥。	/usr/openv/kms/key/KMS_HMKF.dat
密钥保护密钥	此为使用 AES 256 加密并保护 KMS_DATA.dat 密钥文件中单个记录的加密密钥。目前，加密所有记录均使用同一个密钥保护密钥。	/usr/openv/kms/key/KMS_KEYF.dat

Web 安全

本章节包括下列主题：

- [关于 SSL 认证](#)
- [实施第三方 SSL 证书](#)

关于 SSL 认证

“安全套接字层”协议会在您的设备 Web 服务器和您的 LDAP 服务器或本地服务器之间创建加密连接，使信息传输免遭窃取、数据篡改或者消息伪装的问题。要在您的 NetBackup Appliance Web Console 上启用 SSL，您需要能够识别您的 SSL 证书并将其安装到设备的 Web 服务器上。

Symantec Product Authentication Service 发行自签名 SSL 证书。NetBackup Appliance 使用自签名证书层次结构。用于生成 SSL 证书密钥的关键算法是 SHA1withRSA。所有低强度密码（例如 SSLv2 和 Diffie-Hellman）均已禁用。

还可以为 LDAP PAM 身份验证模块设置 SSL 证书，从而在 NetBackup Appliance LDAP PAM 模块和 LDAP 服务器之间建立安全连接。

第三方证书

您可以手动添加和实施第三方证书来获得 Web 服务支持。设备使用 Java KeyStore 作为安全证书的存储库。Java KeyStore (JKS) 是一个安全证书存储库，与 SSL 加密中用于实例的授权证书或公钥证书一样。

注意：实施第三方证书的过程随使用的 PKCS（公钥密码标准）的类型不同而变化。有关使用 PKCS# 7 和 PKCS# 12 标准格式实施第三方证书的更多信息，请参见《Symantec NetBackup™ Appliance 管理指南》的“实施第三方 SSL 证书”一节。

IPSec 实现

什么是 IPSec?

设备证书是由 Versign CA 颁发的 x509 证书。设备证书颁发给主设备、介质设备和 PureDisk NBU 设备。其目的是在传输模式中使用 IPSec 通道来保护 NBU 设备之间的通信安全。设备与非设备之间的所有其他通信将是非 IPSec。

在使用设备证书置备且已为 IPSec 启用的主设备与介质设备之间，通信需双方身份验证且具有保密性。这使主服务器与介质服务器之间的交互得到保护。在客户端与介质设备之间，通信不进行身份验证，且很明显不会影响实际的数据移动速度。注意：如果客户端是另一个介质服务器，那么这一点也很明显，因为我们并未在这两个介质服务器之间设置 IPSec 策略。在这里，我们仅重点强调了主设备与介质设备之间的通信，但通过设置适当的安全策略并定义关联，可以轻松扩展以涵盖任何设备。简单地说，安全策略指明实体之间需要何种安全性，而安全关联则定义其具体组成。

何时适用

应用程序不支持 TLS

主机验证

不需要使用 KPI

VPN

如何保护设备?

我们阐述的安全关联是指两台设备之间的一种特定的安全连接。

NBAC 实现

实施第三方 SSL 证书

您可以手动添加和实施第三方证书来获得 Web 服务支持。设备使用 Java KeyStore 作为安全证书的存储库。Java KeyStore (JKS) 是一个安全证书存储库，与 SSL 加密中用于实例的授权证书或公钥证书一样。如果要实施第三方证书，请使用下列过程：

实施第三方 SSL 证书：

- 1 为 Web 服务准备 keystore 文件。该过程会因您所用的 PKCS（公钥密码标准）类型而异，下表介绍了使用 PKCS# 7 和 PKCS# 12 标准格式的步骤

PKCS 格式	准备 keystore 文件
---------	----------------

PKCS#7 或 X.509 格式	您可以使用下列链接：
-------------------	------------

	https://knowledge.verisign.com/support/ssl-certificates-support/index.html
--	---

PKCS 格式 准备 keystore 文件

- PKCS#12 格式 1 使用以下命令将 PEM 格式的 x509 证书和密钥转换为 PKCS#12:

```
openssl pkcs12 export -in server.crt -inkey  
server.key -out server.p12 -name some-alias  
-CAfile ca.crt -caname root
```

有关 openssl 用法的详细信息, 请参考
<http://www.openssl.org/>。

注意: 请确保在 PKCS #12 文件上设置密码。如果未对该文件应用此密码, 则在尝试导入该文件时可能会遇到空引用异常

- 2 使用以下命令将 pkcs12 文件转换为 Java Keystore:

```
keytool -importkeystore -deststorepass  
changeit -destkeypass changeit -destkeystore  
server.keystore -srckeystore server.p12  
-srcstoretype PKCS12 -srcstorepass some-  
password -alias some-alias
```

有关 keytool 用法的详细信息, 请参考

<http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html>

- 2 使用以下命令关闭 web 服务:

```
/etc/init.d/nbappws stop
```

- 3 将现有的 keystore 文件替换为新的 keystore 文件。默认文件名是

```
/opt/SYMCnbappws/Security/keystore。
```

- 4 在配置文件中更正下列信息:

- 更改 /opt/SYMCnbappws/config/server.xml 中的 keystoreFile 和 keystorePass 设置。
- 更改 /opt/SYMCnbappws/webserver/conf/server.xml 中的 keystoreFile 和 keystorePass 设置。
- 更改 /opt/SYMCnbappws/bin/startgui.sh 中的 javax.net.ssl.trustStore 和 javax.net.ssl.trustStorePassword 设置。

- 5 使用以下命令启动 Web 服务:

```
/etc/init.d/nbappws start
```

网络安全

本章节包括下列主题：

- [关于 IPsec 通道配置](#)
- [关于 NetBackup Appliance 52xx 端口](#)

关于 IPsec 通道配置

NetBackup Appliance 使用 IPsec 通道来保护两台设备之间的通信安全，从而帮助保护传输中的数据。NetBackup Appliance 与非设备（例如 NetBackup 主服务器）之间的所有其他通信均不使用 IPsec。

IPsec 安全在 IP 级别发挥作用并且允许保护两台主机之间的 IP 通信。主设备和介质设备均置备了设备证书，之后会启用这些证书以配置 IPsec 通道。这使主服务器与介质服务器之间的交互得到保护。所使用的这些设备证书是由 Versign CA 发行的 x509 证书。

在建立 IPsec 通道前设备会执行以下验证检查：

- 使用 x509 证书验证证书的真实性。
- 验证设备证书是否与 IP 对应。
- 验证并更新双向通信中的安全关联。

在设别了设备证书后将对主机进行检测。只有此检查完成后才能配置和启用 IPsec 通道。

管理 IPsec 配置

可以从 NetBackup Appliance Shell Menu 使用以下命令来管理 IPsec 通道：

表 9-1 IPsec 命令

命令	描述
Network > Security > Configure	可使用此命令配置任何两个主机之间的 IPsec。可以通过主机名定义主机。也可以通过用户 ID 和密码来标识主机。
Network > Security > Delete	可使用此命令为本地系统上的一系列远程主机删除 IPsec 策略。可使用此命令为本地系统上的一系列远程主机删除 IPsec 策略。为本地系统上的一系列远程主机删除 IPsec 策略。使用 Hosts 变量可定义一个或多个主机名。使用逗号分隔多个主机名。
Network > Security > Export	使用此命令可导出 IPsec 凭据。EnterPasswd 字段用于回答问题“是否要输入密码?”。您必须在此字段中输入 yes 或 no。此外，您必须指定一个路径，用于定义要放置所导出凭据的位置。 注意： IPsec 凭据将在重映像过程中删除。凭据对于每个设备而言是唯一的，包含在原始出厂映像中。用于重映像设备的 USB 驱动器上不包含 IPsec 凭据。
Network > Security > Import	使用此命令可导入 IPsec 凭据。 EnterPasswd 字段用于回答问题“是否要输入密码?”。您必须在此字段中输入 yes 或 no。此外，您必须指定用于定义导入凭据位置的路径。
Network > Security > Provision	使用此命令可为本地系统上的一系列远程主机置备 IPsec 策略。使用 Hosts 变量可定义一个或多个主机名。使用逗号分隔多个主机名。
Network > Security (IPsec) > Refresh	使用此命令可重新加载 IPsec 配置。[Auto] 选项定义是否刷新所有引用主机上的配置。您可以输入 [Auto] 或 [NoAuto]。默认值为 [NoAuto]。
Network > Security > Show	为本地主机或提供的主机显示 IPsec 策略。[[Verbose]] 选项用于定义输出是否详细。您可以在此字段中输入的值为 [VERBOSE] 或 [NOVERBOSE]。默认值为 [NOVERBOSE]。[[HostInfo]] 选项可以包含以下信息，以逗号分隔。主机名、用户 ID (可选) 和密码 (可选)。
Network > Security > Unconfigure	使用此命令可取消任意两台主机间的 IPsec 配置。Host1Info 变量可以包含以下信息，以逗号分隔。主机名、用户 ID (可选) 和密码 (可选)。[Host2info] 变量可以包含主机名、用户 ID (可选) 和密码 (可选)。

可使用 NetBackup Appliance Shell Menu 中的 Main > Network > Security 命令配置两台主机之间的 IPSec 通道。有关配置 IPSec 通道的更多信息，请参见《Symantec NetBackup™ Appliance 命令参考指南》。

关于 NetBackup Appliance 52xx 端口

除 NetBackup 使用的端口之外，52xx 设备还提供带内和带外管理。带外管理通过独立网连接、远程管理模块 (RMM) 和智能平台管理接口 (IPMI) 进行。根据需要打开通过防火墙的这些端口可允许从远程便携式计算机或 KVM (键盘、显示器和鼠标) 访问管理服务。

警告：现在只能使用 HTTPS 通过默认端口 443 访问 NetBackup Appliance Web Console；通过 HTTP 的端口 80 已禁用。请使用 `https://<appliance-name>` 登录到 Web 控制台，其中 `appliance-name` 是设备的完全限定的域名 (FQDN)，也可以是 IP 地址。

表 9-2 列出了开放用于 NetBackup Appliance 的入站通信的端口。

表 9-2 入站端口

端口	Service	描述
22	ssh	带内管理 CLI
80	HTTP	带内管理 GUI
443	HTTPS	带内管理 GUI
80	HTTP	带外管理 (ISM+ 或 RM*)
443	HTTPS	带外管理 (ISM+ 或 RM*)
5900	KVM	CLI 访问、ISO 和 CDRom 重定向
623	KVM	(可选, 打开时使用)
7578	RMM	CLI 访问
5120	RMM	ISO 和 CD-ROM 重定向
5123	RMM	软盘重定向
7582	RMM	KVM
5124	HTTPS	CD ROM

端口	Service	描述
5127		USB 或软盘
2049	HTTPS	NFS++
445		CIFS (用于日志/安装共享)

+ NetBackup Integrated storage manager

* Symantec Remote Management - 远程控制台

++ NFS 服务关闭后，漏洞扫描程序不会将这些端口作为威胁。

注意：端口 7578、5120 和 5123 用于未加密模式。端口 7528、5124 和 5127 用于加密模式。

表 9-3 列出了允许将警报和通知发送到指定服务器的设备出站端口。

表 9-3 出站端口

端口	Service	描述
443	HTTPS	向 Symantec 发送自动通报通知
162**	SNMP	出站陷阱和警报
443	HTTPS	下载 SDCS 证书

** 可以在设备配置中更改此端口号以匹配远程服务器。

《Symantec NetBackup 网络端口参考指南》中提供了所有适用端口的完整列表。

自动通报安全

本章节包括下列主题：

- [关于 AutoSupport](#)
- [关于自动通报](#)
- [关于 SNMP](#)

关于 AutoSupport

通过 AutoSupport 功能，可以在 Symantec 技术支持网站上注册该设备和您的联系人详细信息。Symantec 技术支持可使用此信息解决您报告的任何问题。这些信息允许 Symantec 支持能够最大限度地减少停机时间，并提供一种更主动的支持方法。

使用以下其中一种方法提供设备的注册详细信息：

- 安装设备之前登录 [MyAppliance 门户](#)
- “注册” 页面上的设备初始配置
- 通过导航到 “设置” > “通知” > “注册” 页面显示的 NetBackup Appliance Web Console
- 通过运行 `Settings > Alerts > CallHome Registration` 命令显示的 NetBackup Appliance Shell Menu。有关此命令的更多信息，请参考《[NetBackup Appliance 命令参考指南](#)》。

可以通过输入以下基本信息进行注册：

- 名称：您的姓名、公司名称
- 地址，即设备的物理位置：市/县、街道、省/市/自治区、邮政编码
- 联系人信息：电话号码、电子邮件地址

技术支持基础设施旨在允许 Symantec 支持通过以下方式为您提供帮助：

- 通过主动监视，Symantec 支持可以自动创建案例、修正问题并派送任何可能面临危险的设备部件。
- Symantec 中的 AutoSupport 基础设施将分析来自设备的自动通报数据。此分析可针对硬件故障提供主动的客户支持，从而减少需要备份管理员启动支持案例的情况。
- 通过 AutoSupport 功能，Symantec 支持可以开始了解客户如何配置并使用其设备，以及在哪里做出改进最为有利。
- 发送并接收设备的状态和警报通知。
- 使用自动通报接收硬件和软件状态。
- 提供对问题的更多见解，并识别由于现有问题可能进一步出现的任何问题。
- 查看自动通报数据的报告以分析硬件故障模式，并查看使用趋势。该设备每隔 30 分钟发送一次运行状况数据。

您在注册设备时提供的信息可帮助 Symantec 支持启动针对您报告的任何问题的解决过程。但是，如果要提供其他详细信息，例如，辅助联系人、电话、机架位置等，可以访问 <https://my.symantec.com>。

关于自动通报

设备可与 Symantec AutoSupport 服务器连接并上载硬件和软件信息。Symantec 支持可使用此信息解决可能报告的任何问题。设备使用 HTTPS 协议并使用端口 443 连接到 Symantec AutoSupport 服务器。设备的此功能称为“自动通报”。该功能在默认情况下处于启用状态。

设备中的 AutoSupport 使用由自动通报收集的数据为设备提供主动监视。如果启用了自动通报，默认情况下设备会每隔 24 小时定期将硬件和软件信息（或自动通报数据）上载到 Symantec AutoSupport 服务器。

如果确定某块硬件存在问题，您可能希望与 Symantec 支持联系。技术支持工程师可以使用设备的序列号并根据自动通报数据评估硬件状态。要从 NetBackup Appliance Web Console 查看设备的序列号，请转到“监视器”>“硬件”>“运行状况详细信息”页面。要使用 shell 菜单确定设备的序列号，请转到 Monitor > Hardware 命令。有关 Monitor > Hardware 命令的更多信息，请参考《NetBackup Appliance 命令参考指南》。

使用“设置”>“通知”页面从 NetBackup Appliance Web Console 配置自动通报。单击“警报配置”，然后在“自动通报配置”窗格中输入详细信息。

表 10-1 介绍了在该功能处于启用或禁用状态时如何报告硬件故障。

表 10-1 当启用或禁用自动通报时，会出现什么情况

监视状态	硬件故障例程
自动通报已启用	<p>当发生硬件故障时，会依次出现以下警报：</p> <ul style="list-style-type: none"> ■ 设备将所有受监视的硬件和软件信息上载到 Symantec AutoSupport 服务器。此表后面的列表提供了所有相关信息。 ■ 设备会向配置的电子邮件地址生成 3 种电子邮件警报。 <ul style="list-style-type: none"> ■ 一旦检测到错误，就会通过电子邮件向您发送一条错误消息，以通知您出现硬件故障。 ■ 一旦错误得到解决，就会通过电子邮件向您发送一条已解决消息，以通知您任何硬件故障已得到解决。 ■ 通过电子邮件发送 24 小时摘要，以汇总最近 24 小时尚未解决的所有错误。 ■ 设备还可生成 SNMP 陷阱。
自动通报已禁用	<p>数据没有发送到 Symantec AutoSupport 服务器。您的系统不会向 Symantec 报告硬件错误以加快解决问题的速度。</p>

以下列表提供了发送到 **Symantec AutoSupport** 服务器进行分析的所有受监视信息。

- CPU
- 磁盘
- 风扇
- 电源
- RAID 组
- 温度
- 适配器
- PCI
- 光纤通道 HBA
- 网卡
- 分区信息
- MSDP 统计数据
- 存储连接
- 存储状态
- 52xx 存储扩展架 - 磁盘、风扇、电源和温度的状态

- 5330 主存储架 - 磁盘、风扇、电源、温度、备用电池（BBU）、控制器、卷和卷组的状态
- 5330 扩展存储架 - 磁盘、风扇、电源和温度的状态
- NetBackup Appliance 软件版本
- NetBackup 版本
- 设备型号
- 设备配置
- 固件版本
- 设备、存储和硬件组件序列号

请参见第 76 页的“从 NetBackup Appliance Shell Menu 配置自动通报”。

请参见第 73 页的“关于 AutoSupport”。

从 NetBackup Appliance Shell Menu 配置自动通报

您可以从“设置” > “通知”页面配置自动通报详细信息。

可以从 NetBackup Appliance Shell Menu 配置以下自动通报设置：

- 从 NetBackup Appliance Shell Menu 启用和禁用自动通报
- 从 NetBackup Appliance Shell Menu 配置自动通报代理服务器
- 通过运行 `Settings > Alerts > CallHome > Test` 命令来测试自动通报是否正常运行。

如果启用了自动通报，则可以使用 `Settings > Alerts > CallHome Registration` 命令为设备配置联系人详细信息，方法是输入以下信息：

- 负责设备的第一联系人的姓名。
- 联系人的地址。
- 联系人的电话号码。
- 联系人的电子邮件地址。

要了解有关 `Main > Settings > Alerts > CallHome` 命令的详细信息，请参见《Symantec NetBackup Appliance 命令参考指南》。

有关导致警报的硬件问题列表，请参见下列主题：

请参见第 74 页的“关于自动通报”。

从 NetBackup Appliance Shell Menu 启用和禁用自动通报

您既可以从 NetBackup Appliance Web Console 也可以从 NetBackup Appliance Shell Menu 启用或禁用自动通报。默认情况下启用自动通报。

从 NetBackup Appliance Shell Menu 启用或禁用自动通报

- 1 登录到 NetBackup Appliance Shell Menu。
- 2 要启用自动通报，请运行 `Main > Settings > Alerts > CallHome Enable` 命令。
- 3 要禁用自动通报，请运行 `Main > Settings > Alerts > CallHome Disable` 命令。

有关 `Main > Settings > Alerts > CallHome` 命令的详细信息，请参阅《Symantec NetBackup Appliance 命令参考指南》。

从 NetBackup Appliance Shell Menu 配置自动通报代理服务器

如果需要，可以为自动通报配置代理服务器。如果设备环境在环境与外部 Internet 访问之间存在代理服务器，则必须在设备上启用代理设置。代理设置包括代理服务器和端口。该代理服务器必须接受来自 Symantec AutoSupport 服务器的 https 连接。默认情况下，将禁用此选项。

从 NetBackup Appliance Shell Menu 添加自动通报代理服务器

- 1 登录到 NetBackup Appliance Shell Menu。
- 2 要启用代理设置，请运行 `Main > Settings > Alerts > CallHome Proxy Enable` 命令。
- 3 要添加代理服务器，请运行 `Main > Settings > Alerts > CallHome Proxy Add` 命令。

- 系统将提示您输入代理服务器的名称。代理服务器名称是代理服务器的 TCP/IP 地址或完全限定域名。
- 输入代理服务器的名称后，系统将提示您输入该代理服务器的端口号。
- 接着，您将需要回答以下问题：

```
Do you want to set credentials for proxy server? (yes/no)
```

- 回答 `yes` 后，系统将提示您输入代理服务器的用户名。
- 输入用户名后，系统将提示您为该用户输入密码。输入所需信息后，将显示以下消息：

```
Successfully set proxy server
```

- 4 要禁用代理设置，请运行 `Main > Settings > Alerts > CallHome Proxy Disable` 命令。

接着，您也可以使用 `NetBackup Appliance Shell Menu` 为设备启用或禁用代理服务器隧道。要执行此操作，请运行 `Main > Settings > CallHome Proxy EnableTunnel` 和 `Main > Settings > Alerts > CallHome Proxy DisableTunnel` 命令。通过代理服务器隧道，您可以通过不信任的网络提供安全路径。

了解自动通报工作流程

本节对自动通报用于将数据从设备上传到 Symantec AutoSupport 服务器的机制进行说明。

自动通报将端口号为 443 的 HTTPS（安全和加密协议）用于与 Symantec AutoSupport 服务器的所有通信。为了使自动通报正常工作，请确保您的设备可通过互联网直接访问或通过代理服务器访问 Symantec AutoSupport 服务器。AutoSupport（主动监视设备的机制）使用自动通报数据分析和解决设备可能遇到的所有问题。

所有通信都由设备启动。您的设备需能够访问 <https://receiver.appliance.veritas.com>。

设备的自动通报功能使用以下工作流程与 AutoSupport 服务器进行通信：

- 每 24 小时访问一次以下网站的端口：<https://receiver.appliance.veritas.com>。
- 对以下网站执行自检操作：<https://receiver.appliance.veritas.com>。
- 如果此设备遇到错误状态，则会随当前日志一起收集三天前的所有硬件日志。
- 然后，将日志上载到 Symantec AutoSupport 服务器作进一步的分析并获取支持。这些错误日志也将存储在设备上。可从 `/log/upload/<date>` 文件夹访问这些日志。
- 如果三天后错误状态仍然存在，则将重新上传日志。

请参见第 74 页的“关于自动通报”。

请参见第 73 页的“关于 AutoSupport”。

关于 SNMP

简单网络管理协议 (SNMP) 是一种应用程序层协议，可以简化网络设备之间管理信息的交换。根据配置情况，它会使用传输控制协议 (TCP) 或用户数据报协议 (UDP) 进行传输。网络管理员可以使用 SNMP 来管理网络性能，查找和解决网络问题，以及针对网络增长进行规划。

SNMP 基于管理器模型和代理模型。此模型由管理器、代理、管理信息数据库、管理对象和网络协议组成。

管理器提供网络管理员与管理系统之间的接口。代理提供管理器与受管理的物理设备之间的接口。

管理器和代理使用管理信息库 (MIB) 和相对较小的一组命令来交换信息。MIB 是一种树型组织结构，树枝上的叶子表示各个变量，如点状态或描述。数字标签或对象标识符 (OID) 用于区分 MIB 和 SNMP 消息中具有唯一性的各个变量。

NetBackup Appliance 2.7.1 支持 SNMP v2。

关于管理信息库 (MIB)

每个 SNMP 元素都管理特定的对象，而各个对象都有特定的特性。每个对象和特性都有一个与其关联的唯一对象标识符 (OID)。每个 OID 由以小数点隔开的数字组成（例如，1.3.6.1.4.1.2682.1）。

这些 OID 形成了一个树型结构。MIB 将每个 OID 与可读的标签以及与对象相关的各种其他参数相关联。然后，MIB 用作数据字典，该字典用于汇编和解释 SNMP 消息。此信息保存为 MIB 文件。

您可以从 NetBackup Appliance Web Console 的“设置” > “通知” > “警报配置”页面检查 SNMP MIB 文件的详细信息。要配置设备 SNMP 管理器以接收与硬件监视相关的陷阱，请单击“SNMP 服务器配置”窗格中的“查看 SNMP MIB 文件”。

您还可以在 NetBackup Appliance Shell 菜单中使用 `Settings > Alerts > SNMP ShowMIB` 命令查看 SNMP MIB 文件。

IPMI 安全

本章节包括下列主题：

- [IPMI 配置简介](#)
- [建议的 IPMI 设置](#)
- [替换默认 IPMI SSL 证书](#)

IPMI 配置简介

可以配置设备的 IPMI 子系统。当意外断电导致连接的系统关闭时，智能平台管理接口 (IPMI) 子系统是非常有益的。此子系统独立于操作系统运行，并可使用位于此设备后面板上的远程管理端口进行连接。

可以使用 BIOS 设置配置 IPMI 子系统和 Symantec Remote Management 工具。Symantec Remote Management 工具提供了一个使用远程管理端口的界面。使您可以从远程位置监视和管理设备。

建议的 IPMI 设置

此部分列出了建议的 IPMI 设置以确保安全的 IPMI 配置。

Users

创建 IPMI 用户时请务必记住以下建议：

- 不允许帐户的用户名或密码为空。
- 建议设置一个管理员用户。
- 建议禁用匿名用户。
- 建议删除供应商帐户并创建您自己的用户名和密码。
- 建议为每个用户设置 16-20 个字符的密码以避免暴力强制攻击

登录

创建 IPMI 用户适用的登录设置时请务必记住以下建议：

表 11-1 登录安全设置

设置	建议值
失败的登录尝试	3
用户锁定时间（分钟）	60 秒
强制 HTTPS	是 必须选中“强制 HTTPS”复选框以确保 IPMI 连接始终使用 HTTPS。
Web 会话超时	1800

LDAP 设置

Symantec 建议尽可能在您的环境中启用 LDAP 身份验证。

SSL 上载

Symantec 建议导入新的或自定义的 SSL 证书。

远程会话

表 11-2 远程会话安全设置

设置	建议值
KVM 加密	AES
介质加密	启用

密码建议

- 请勿在 IPMI 通道上将密码设置为零

警告：如果通道上启用了密码 0，则将允许任何人执行任意 IPMI 操作而无需身份验证，实际上完全破坏了 IPMI 的安全性。请无论如何都要将其禁用。

- 请仅使用密码 3、8 和 12。

以太网连接设置

建议设置一个 IPMI 专用的以太网连接，这意味着您应当避免共享服务器的物理连接。

- 使用静态 IP
- 避免 DHCP

禁用没有使用的服务

未来版本的 IPMI 中将具有从 Symantec Remote Management 控制台或命令行界面禁用 SSH 和 HTTP 服务的功能。

有关更多信息，请参见

<http://www.intel.com/content/www/us/en/servers/ipmi/ipmi-home.html>。

替换默认 IPMI SSL 证书

Symantec 建议将用于访问 IPMI Web 界面的默认 IPMI SSL 证书替换为由受信任内部或外部证书颁发机构签署的证书（采用 PEM 格式）或自签名证书。可以使用以下过程在 Linux 计算机上创建最小的自签名证书，并将其导入到 IPMI Web 界面：

要在 Linux 计算机上创建最小的自签名证书并将其导入到 IPMI Web 界面，请执行以下操作：

- 1 运行以下命令以生成名为 `ipmi.key` 的私钥：

```
$ openssl genrsa -out ipmi.key 2048
```

```
Generating RSA private key, 2048 bit long modulus
```

```
.....+++
```

```
.+++
```

```
e is 65537 (0x10001)
```

- 2 使用 `ipmi.key` 生成名为 `ipmi.csr` 的证书签名请求，每个字段用其相应的值填充：

注意：要避免浏览器中出现额外的警告，请将 CN 设置为 IPMI 界面的完全限定域名。将要输入的是所谓的可分辨名称或 DN。

```
$ openssl req -new -key ipmi.key -out ipmi.csr
```

请参考以下准则以输入要合并到证书请求中的信息：

国家/地区名称（2 字母 输入您所在国家/地区的名称。例如，US。
代码）[AU]：

省/市/自治区名称（全 输入您所在省/市/自治区的名称。例如，OR。
名）[Some-State]：

区域名称（如城市）[]： 输入您所在区域的名称。例如，Springfield。

组织名称（如公司） 输入您组织的名称。例如，Symantec。
[Internet Widgits Pty
Ltd]：

组织单元名称（如部 输入您组织单元的名称。
门）[]：

常见名称（如您的姓 输入 `hostname.your.company`。
名）[]：

电子邮件 []： 输入您的电子邮件地址。例如，`email@your.company`。

质询密码 []： 输入相应的质询密码，该密码是要随证书请求一起发送的额外属性。

可选公司名称 []： 输入相应的可选公司名称，该名称是要随证书请求一起发送的额外属性。

注意：输入 . 以将任何字段留空。

- 3 使用 `ipmi.key` 签署 `ipmi.csr`，然后创建名为 `ipmi.crt` 的证书，其有效期为 1 年：

```
$ openssl x509 -req -in ipmi.csr  
  
-out ipmi.crt -signkey ipmi.key  
  
-days 365  
  
Signature ok  
  
subject=/C=US/ST=OR/L=Springfield  
  
/O=Symantec/OU=Your OU/  
  
CN=hostname.your.company/  
  
emailAddress=email@your.company
```

```
Getting Private key
```

- 4 连接 `ipmi.crt` 和 `ipmi.key` 以创建名为 `ipmi.pem` 的证书（采用 PEM 格式）。

```
$ cat ipmi.crt ipmi.key > ipmi.pem
```

- 5 将 `ipmi.pem` 复制到可访问设备的 IPMI Web 界面的主机。
- 6 登录到 Symantec Remote Management（IPMI Web 界面）。
- 7 单击“配置” > SSL。
设备将显示“SSL 上载”页面。
- 8 从“SSL 上载”页面中，单击“选择文件”以导入证书。
- 9 选择 `ipmi.pem`，然后单击“上载”。
- 10 可能会显示警告，指出 SSL 证书已存在，按“确定”以继续。
- 11 要导入密钥，请重新单击“选择文件”（请注意按钮旁边显示的是“新私钥”）。
- 12 选择 `ipmi.pem`，然后单击“上载”。

- 13 将显示一条确认消息，指出已成功上载证书和密钥，按“确定”以重新启动 Web 服务。
- 14 关闭再重新打开 Symantec Remote Management (IPMI Web 界面) 界面，以验证所显示的是否为新证书。

NetBackup Appliance 操作系统中包含的软件包

本附录包括下列主题：

- [NetBackup Appliance 操作系统中包含的软件包的列表](#)

NetBackup Appliance 操作系统中包含的软件包的列表

设备操作系统 (OS) 基于 Red Hat Enterprise Linux (RHEL) 的 Symantec 自定义版本。为提升安全性、性能和稳定性，Symantec 仅包含了设备运行所必需的 RHEL 软件包。[表 A-1](#) 包含设备 OS 中所含 RHEL 软件包的列表。

表 A-1 NetBackup Appliance 操作系统中包含的软件包的列表

abrt	gtk	libxml	python-libs
abrt-addon-ccpp	gzip	libxml2-python	python-lxml
abrt-addon-kerneloops	hal	libXpm	python-paramiko
abrt-addon-python	hal-info	libXpm-devel	python-pycurl
abrt-cli	hal-libs	libXrandr	python-rhsm
abrt-libs	hdparm	libXrender	python-slip
abrt-python	hicolor-icon-theme	libxslt	python-slip-dbus
abrt-tui	hunspell	libXt	python-tdb
acl	hunspell-en	lm_sensors	python-tevent4
acpid	hwdata	lm_sensors-devel	python-urlgrabber
aic94xx	ifplugd	lm_sensors-libs	ql2100-firmware
alsa-lib	info	lockdev	ql2200-firmware
atk	initscripts	logrotate	ql23xx-firmware
atmel-firmware	iotop	lrzsz	ql2400-firmware
attr	ipmitool	lsof	ql2500-firmware
audit	iproute	lsscsi	quota
audit-libs	iptables	ltrace	rarian
audit-libs	iptables-ipv6	lua	rarian-compatible
augeas-libs	iputils	lvm	rdate
authconfig	ipw2100	lvm2-libs	readahead
avahi-glib	ipw2200	lzo	readline
avahi-libs	irqbalance	m2crypto	redhat-indexhtml
b43-fwcutter	iscsi-initiator-utils	m4	redhat-logos
b43-openfwf	isomd5sum	mailcap	redhat-release-server
basesystem	ivtv-firmware	mailx	redhat-rpm-config
bash	iw	make	redhat-support-lib-python
bc	iwl100-firmware	MAKEDEV	redhat-support-tool
bfa-firmware	iwl1000-firmware	man	rfskill
bind-libs	iwl13945-firmware	man-pages	rhn-check
bind-utils	iwl4965-firmware	man-pages-overrides	rhn-client-tools
binutils	iwl5000-firmware	mdadm	rhn-setup
biosdevname	iwl5150-firmware	microcode_ctl	rhnlib
blktrace	iwl6000-firmware	mingetty	rhnsl
bridge-utils	iwl6000g2a-firmware	minicom	rng-tools
btparser	iwl6050-firmware	mlocate	rootfiles
busybox	jasper	module-init-tools	rpcbind
bzip2	jasper-libs	mozilla-filesystem	rpm
bzip2-libs	json-c	mpfr	rpm-build
ca-certificates	kbd	mtools	rpm-devel
cairo	kbd-misc	mtr	rpm-libs
cas	kernel	mysql-libs	rpm-python
checkpolicy	kernel-devel	nano	rsh
chkconfig	kernel-firmware	ncurses	rsh-server
cifs-utils	kernel-headers	ncurses-base	rsync
cloog-ppl	kexec-tools	ncurses-libs	rsyslog
cmatrix	keyutils	net-snmp	rt61pci-firmware

compat-glibc	keyutils-libs	net-snmp-devel	rt73usb-firmware
compat-glibc-headers	keyutils-libs-devel	net-snmp-libs	samba
compat-libstdc++	kmmod-megasr	net-snmp-perl	samba-client
ConsoleKit	kpartx	net-snmp-python	samba-common
ConsoleKit-libs	krb5-devel	net-snmp-utils	samba-winbind
ConsoleKit-x11	krb5-libs	net-tools	samba-winbind-clients
coreutils	krb5-pkinit-openssl	newt	satyr
coreutils-libs	krb5-workstation	newt-python	sblim-cmpi-samba
cpio	ksh	nfs-utils	sblim-tools-libra
cpp	latrace	nfs-utils-lib	scl-utils
cpuspeed	ledmon	nmap	screen
cracklib	less	nscd	sed
cracklib-dicts	Lib_Utils	nspr	selinux-policy
crash	libacl	nss	selinux-policy-targeted
crash-trace-command	libaio	nss-pam-ldapd	setserial
crda	libaio-devel	nss-softokn	setup
createrepo	libattr	nss-softokn-freebl	setuptools
cronie	libblkid	nss-sysinit	sg3_utils
cronie-anacron	libcap	nss-tools	sg3_utils-libs
crontabs	libcap-ng	nss-util	sgml-common
cryptsetup-luks	libcom_err	ntp	sgpio
cryptsetup-luks-libs	libcom_err-devel	ntpdate	shadow-utils
cups-libs	libcurl	ntsysv	shared-mime-info
curl	libdaemon	numactl	slang
cvs	libdrm	OpenIPMI	smartmontools
cyrus-sasl	libedit	OpenIPMI-libs	snappy
cyrus-sasl-lib	liberation-fonts-common	openldap	sos
cyrus-sasl-plain	liberation-sans-fonts	openldap-clients	sqlite
dash	libertas-usb8388-firmware	openssl	startup-notification
db4	libevent	openssh	strace
db4-utils	libffi	openssh-clients	subscription-manager
dbus	libfprint	openssh-server	sudo
dbus-glib	libgcc	openssl	syslinux
dbus-libs	libgcrypt	openssl-devel	syslinux-nonlinux
dbus-python	libglade	openssl098e	sysstat
deltarpm	libgomp	ORBit	system-config-firewall
desktop-file-utils	libgpg-error	p11-kit	system-config-firewall-base
device-mapper	libgssglue	p11-kit-trust	system-config-firewall-tui
device-mapper-event	libgudev	pam_krb5	system-config-kdump
device-mapper-event-libs	libICE	pam_ldap	system-config-network-tui
device-mapper-libs	libIDL	pam_passwdqc	systemtap
device-mapper-persistent-data	libidn	pam	systemtap-client
dhclient	libjpeg-turbo	pango	systemtap-devel
dhcp-common	libldb	parted	systemtap-initscript
diffutils	libldb-devel	passwd	systemtap-runtime
dmidecode	libnih	patch	systemtap-sdt-devel

dmraid	libnl	pciutils	systemtap-server
dmraid-events	libpcap	pciutils-libs	sysvinit-tools
docbook-dtdds	libpciaccess	pcmciautils	tar
dos2unix	libpng	pcre	tcl
dosfstools	libproxy	perl	tcp_wrappers
dracut	libproxy-bin	perl-Compress-Raw-Bzip2	tcp_wrappers-devel
dracut-kernel	libproxy-python	perl-Compress-Raw-Zlib	tcp_wrappers-libs
e2fsprogs	libreport	perl-Compress-Zlib	tcpdump
e2fsprogs-libs	libreport-cli	perl-HTML-Parser	tcsh
ed	libreport-compat	perl-HTML-Tagset	telnet
efibootmgr	libreport-filesystem	perl-IO-Compress-Base	time
eggdbus	libreport-plugin-kernel	perl-IO-Compress-Bzip	tmpwatch
eject	libreport-plugin-logger	perl-IO-Compress-Zlib	tog-pegasus
elfutils	libreport-plugin-mailx	perl-libs	tog-pegasus-libs
elfutils-devel	libreport-plugin-report	perl-Module-Pluggable	trace-cmd
elfutils-libelf	libreport-plugin-rhtsup	perl-Module-Pluggable	traceroute
elfutils-libelf-devel	libreport-plugin-ureport	perl-Module-Pluggable	tzdata
elfutils-libs	libreport-python	perl-Pod-Escapes	udev
ethtool	libselinux	perl-Pod-Simple	unzip
expat	libselinux-devel	perl-URI	upstart
expect	libselinux-python	perl-version	usbutils
file	libselinux-utils	perl-XML-Parser	usermode
file-devel	libsemanage	perl-XML-XPath	ustr
file-libs	libsepol	pinentry	util-linux-ng
filesystem	libsepol-devel	pininfo	valgrind
findutils	libSM	pixman	vconfig
fipscheck	libss	pkgconfig	vim-common
fipscheck-lib	libssh	plymouth	vim-enhanced
fontconfig	libstdc++	plymouth-core-libs	vim-filesystem
fontpackages-filesystem	libtalloc	plymouth-scripts	vim-minimal
fprintd	libtalloc-devel	pm-utils	virt-what
fprintd-pam	libtar	policycoreutils	vlock
freetype	libtasn	polkit	w3m
gamin	libtbb	popt	wget
gawk	libtbb-devel	popt-devel	which
gc	libtevent	portreserve	wireless-tools
gcc	libtevent-devel	postfix	words
GConf	libthai	ppl	xcb-util
gd	libtiff	prelink	xdg-utils
gdb	libtirpc	procps	xinetd
gdbm	libtool-ltdl	psacct	xml-common
gdk-pixbuf	libtool-ltdl-devel	psmisc	xmlrpc-c
genisoimage	libudev	pth	xmlrpc-c-client
gettext	libusb	pycairo	xmlsec
glib	libusb	pygobject	xmlsec1-openssl
glibc	libuser	pygpgme	xorg-x11-drv-ati-firmware

glibc-common	libutempter	pygtk	xorg-x11-proto-devel
glibc-devel	libuuid	pygtk2-libglade	xulrunner
glibc-headers	libX11	pykickstart	xz
glibc-utils	libX11-common	pyldb	xz-devel
gmp	libX11-devel	pyOpenSSL	xz-libs
gnome-doc-utils-style	libXau	pytalloc	xz-lzma-compat
gnome-user-docs	libXau-devel	python	yelp
gnome-vfs	libxcb	python-argparse	yp-tools
gnupg	libxcb-devel	python-crypto	ypbind
gnutls	libXcomposite	python-dateutil	yum
gpgme	libXcursor	python-decorator	yum-metadata-parser
gpm-libs	libXdamage	python-deltarpm	yum-plugin-security
grep	libXext	python-dmidecode	yum-rhn-plugin
groff	libXfixes	python-ethtool	yum-utils
grub	libXft	python-gudev	zd1211-firmware
grubby	libXi	python-iniparse	zip
	libXinerama	python-iwlib	zlib
			zlib-devel

索引

A

- Active Directory 用户
 - 配置身份验证 22
- AutoSupport
 - 客户注册 73

B

- Browse 命令
 - 设备日志文件 53
- 本地用户
 - 配置身份验证 21

C

- 操作系统
 - 安全亮点 58
 - 软件包 87
 - 已禁用服务 60
 - 主要组件 59

D

- datacollect
 - 设备日志 54
- 登录提示
 - NetBackup 26
 - 关于 26
 - 设备 26
- 第三方 SSL 证书 67

G

- 管理信息库 (MIB) 79

I

- IPMI SSL 证书 82
- IPMI 安全
 - 建议 80
- IPS 策略
 - 覆盖 43
 - 重新启用 46

IPsec

- 网络安全 69

J

- 简单网络管理协议 (SNMP) 78

K

- Kerberos
 - 对 NIS 进行身份验证 25

L

- LDAP 用户
 - 配置身份验证 22

M

- 密码
 - 加密 26
 - 凭据 26

N

- NetBackupCLI
 - 命令 35
- NIS 用户
 - 配置身份验证 23

Q

- 权限
 - 用户角色 33

R

- root 43
- 日志文件
 - 简介 49
- 入侵防护系统
 - 关于 39
- 入侵检测系统
 - 关于 39

S

Symantec Data Center Security

IDS 策略 39

IPS 策略 39

Symantec 数据中心安全性

非受控模式 36, 42

关于 36

受控模式 36, 42

设备安全性

关于 9

新增功能和增强功能 15

设备日志文件

Browse 命令 53

身份验证

AD 19

LDAP 19

NIS

Kerberos 19

本地用户 19

收集日志

datacollect 54

命令 52

日志类型 52

日志文件位置 52

收集日志文件 51

授权 30

NetBackupCLI 用户 34

管理员 34

数据安全性 62

数据分类 64

数据加密 64

KMS 支持 64

数据完整性 63

CRC 验证 63

端到端验证 63

T

替换

IPMI SSL 证书 82

通知 74

W

网络安全

IPsec 69

X

向导

收集日志文件 51

Y

用户 17

Active Directory 22

admin 17

AppComm 17

Kerberos-NIS 23

LDAP 22

Maintenance 17

NetBackupCLI 17

root 17

sisips 17

本地 21

管理角色

权限 32

管理员 17

授权 31

添加 32

用户角色权限

NetBackup Appliance 33

用户名凭据 26

用户身份验证

配置 21

准则 23

用户组

管理角色

权限 32

添加 32

Z

支持 AD 的用户

配置服务器 24

先决条件 24

支持 LDAP 的用户

配置服务器 23

先决条件 23

支持 NIS 的用户

配置服务器 25

先决条件 25

自动通报

工作流程 78

警报 74

自动通报代理服务器

配置 77