Veritas NetBackup™ Appliance 安全指南

3.1.1 版

VERITAS™

Veritas NetBackup Appliance 安全指南

法律声明

Veritas、Veritas 徽标和 NetBackup 是 Veritas Technologies LLC 或其附属机构在美国和其他国家/地区的商标或注册商标。其他名称可能为其各自所有者的商标，特此声明。

本产品可能包括 Veritas 必须向第三方支付许可费的第三方软件（以下称“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。软件随附的授权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。请参考此 Veritas 产品随附的或以下链接提供的第三方法律声明文档：

https://www.veritas.com/about/legal/license-agreements

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 Veritas Technologies LLC 及其许可方（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或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。Veritas Technologies LLC 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 Veritas 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。

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

技术支持

技术支持维护全球的支持中心。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政策进行交付。有关支持产品和服务以及如何联系技术支持的信息，请访问我们的网站：

https://www.veritas.com/support

您可以在下列 URL 上管理 Veritas 帐户信息：

https://my.veritas.com

如有关于现有支持协议有任何问题，请按如下所示给您所在区域的支持协议管理团队发送电子邮件：

全球（日本除外）	CustomerCare@veritas.com
日本	CustomerCare_Japan@veritas.com

文档

可以在 Veritas 网站上获取最新文档：

https://sort.veritas.com/documents

文档反馈

您的反馈对我们非常重要。请提出您对本文档的改进建议，或者就本文档中的错误或疏漏进行报告。请注明所报告文本的文档标题、文档版本和章节标题。请将您的反馈发送至：

APPL.docs@veritas.com

您也可以在以下 Veritas 社区站点中查看相关文档信息或进行提问：

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) 是一个网站，提供的信息和统计可自动处理和简化某些耗时的管理任务。根据您的产品，SORT 会帮助您准备安装和升级、识别您数据中心的风险并提高操作效率。要了解 SORT 为您的产品提供了哪些服务和工具，请参见数据表：

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

目录

1

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

关于 NetBackup appliance 安全指南

开发 NetBackup Appliance 的初衷是以安全性为首要需求。使用业界标准和高级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未经授权的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。根据发现问题的严重性，Veritas 会发布修补程序或在计划的主要版本中提供修复程序。为了减少未知威胁的风险，在定期维护发布周期中，Veritas 会定期更新相应产品中的第三方软件包和模块。

此指南的目标是描述 NetBackup appliance 3.1.1 中实施的安全功能，包括以下章节和小节：

NetBackup 设备用户身份验证

本章介绍 NetBackup 设备中的身份验证功能，包括以下部分：

表 1-1 包含身份验证的部分

部分名称	描述	链接
关于 NetBackup 设备上的用户身份验证	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 13 页的“关于 NetBackup Appliance 上的用户身份验证”。

部分名称	描述	链接
关于配置用户身份验证	此部分描述可在设备上进行身份验证的各种用户类型的配置选项。	请参见第 17 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 20 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 21 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 21 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进行身份验证时要显示的文本提示。	请参见第 22 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 23 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 28 页的“关于 NetBackup appliance 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 29 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 32 页的“关于管理员用户角色”。
关于 NetBackupCLI 用户角色	此部分描述 NetBackupCLI 用户角色。	请参见第 33 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 Data Center Security	此部分介绍在设备上实现的 SDCS 功能。	请参见第 35 页的“关于 NetBackup appliance 上的 Symantec Data Center Security”。
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 37 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 38 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 39 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 41 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 41 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 42 页的“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	此部分描述重新启用用于设备的 IPS 策略的过程。	请参见第 45 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 48 页的“关于 NetBackup appliance 日志文件”。
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 50 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 51 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 52 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 56 页的“关于 NetBackup Appliance 操作系统安全”。
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 57 页的“NetBackup appliance 操作系统中包含的主要组件”。
NetBackup Appliance 漏洞扫描	此部分列出 Veritas 用于验证设备安全的一些安全扫描程序。	请参见第 58 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 59 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 60 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 61 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 61 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 证书	此部分列出 NetBackup Appliance Web Console的 SSL 认证更新。	请参见第 64 页的"关于 SSL 使用情况"。
安装第三方 SSL 证书	此部分列出安装第三方 SSL 证书的过程。	请参见第 65 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 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 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 74 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 75 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 79 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 81 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 81 页的“建议的 IPMI 设置”。

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。

注意：本文档中的任务和过程必须在已配置的设备上执行。在配置设备角色后，才可以成功使用本地用户命令。如果未配置设备角色，则尝试执行的任何本地用户命令（包括但不限于授予用户权限）均会失败。如果尝试在角色配置前运行本地用户命令，则完成角色配置后这些命令也一样会失败。其他命令也可能会出现意外或不需要的行为。要防止发生此情况，最佳做法是避免在配置好设备角色之前尝试任何本地用户命令。

2

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

通过用户帐户对 NetBackup appliance 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。

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 2-1 描述了 Appliance 上可用的用户帐户。

表 2-1 NetBackup appliance 帐户类型

帐户名称	描述
admin	**admin** 帐户是 NetBackup appliance 上的默认管理员用户。此帐户提供默认管理员用户的完全设备访问和控制权限。 以下默认登录凭据与新 NetBackup Appliance 一起提供： ■ 用户名：**admin** ■ 密码：**P@ssw0rd** 当从设备装入或映射共享时，请注意以下要求： ■ Windows：**admin** 帐户和具有管理员角色的 AD 用户有权装入或映射 Windows CIFS 共享。 ■ Linux：只有具有 root 访问权限帐户的用户可以直接发出装入命令以装入 NFS 共享。
AMSadmin	**AMSadmin** 帐户向以下设备接口提供完全访问权限： ■ 设备管理控制台 ■ NetBackup Appliance Web Console ■ NetBackup Appliance Shell Menu ■ NetBackup 管理控制台 有关此帐户的完整详细信息，请参见《Veritas Appliance 管理指南》。
maintenance	**maintenance** 帐户由 Veritas 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。 **注意：**此帐户还用于进行 GRUB 更改以及启用 STIG 选项时用于单用户模式引导。

下面介绍了仅供内部用户使用的帐户。这些帐户不允许系统通过 NetBackup Appliance Web Console或 NetBackup Appliance Shell Menu进行访问。

表 2-2 NetBackup appliance 内部帐户类型

帐户名称	描述
sisips	`sisips` 帐户是一个内部用户，用于实现 SDCS 策略。

帐户名称	描述
root	root 帐户是一个受限制的用户，只能由 Veritas 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： Permission Denied !! Access to the root account requires overriding the Intrusion Security Policy. Please refer to the appliance security guide for overriding instructions. **警告：**虽然您可以覆盖 Intrusion 安全策略 (ISP) 以获取对 root 帐户的访问权限，但不建议进行此操作。覆盖此策略会使系统存在风险，使其更容易受到攻击。请参见第 42 页的"覆盖 NetBackup appliance 入侵防护系统策略"。
nbcopilotxxxx	支持从主服务器访问介质服务器时进行身份验证。
AppComm	不支持身份验证。
nbwebsvc	不支持身份验证。

请参见第 29 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 2-3 描述可添加到 NetBackup Appliance 的用户类型。

注意：在配置设备角色后，才可以成功使用本地用户命令。如果未配置设备角色，则尝试执行的任何本地用户命令（包括但不限于授予用户权限）均会失败。如果尝试在角色配置前运行本地用户命令，则完成角色配置后这些命令也一样会失败。某些命令也可能会出现意外或不需要的行为。要防止发生此类情况，最佳做法是避免在配置好设备角色之前尝试任何本地用户命令。

表 2-3 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，您可以授予或撤消相应的设备访问权限。	■ 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。 **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。
LDAP	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。 请参见第 20 页的“关于对 LDAP 用户进行身份验证”。	■ 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。 **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。
Active Directory	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。 请参见第 21 页的“关于对 Active Directory 用户进行身份验证”。	■ 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。 **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。

用户类型	描述	说明
Kerberos-NIS	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。 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。 请参见第 21 页的"关于对 Kerberos-NIS 用户进行身份验证"。	■ 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。 **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。

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 2-4 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 2-4 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 29 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： ■ `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
LDAP	您可以在“**设置**”>“**身份验证**”>**LDAP** 下执行以下 LDAP 配置任务： ■ 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。 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。 请参见第 29 页的“关于授权 NetBackup Appliance 用户”。	`Settings > Security > Authentication > LDAP` 下提供了以下命令和选项： ■ `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。
Active Directory	您可以在“**设置**”>“**身份验证**”>**Active Directory** 下执行以下 AD 配置任务： ■ 配置新的 Active Directory 配置。 ■ 取消配置现有的 Active Directory 配置。 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。 请参见第 29 页的“关于授权 NetBackup Appliance 用户”。	`Settings > Security > Authentication > ActiveDirectory` 下提供了以下命令和选项： ■ `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	您可以在“**设置**”>“**身份验证**”>**Kerberos-NIS** 下执行以下 Kerberos-NIS 配置任务： ■ 配置新的 Kerberos-NIS 配置。 ■ 取消配置现有的 Kerberos-NIS 配置。 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。 请参见第 29 页的“关于授权 NetBackup Appliance 用户”。	`Settings > Security > Authentication > Kerberos` 下提供了以下命令和选项： ■ `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：

- 设备上只能配置一种用于身份验证的远程用户类型（LDAP、Active Directory (AD) 或 NIS）。例如，如果您当前对设备上的 LDAP 用户进行身份验证，则必须先删除其上的 LDAP 配置，然后再更改为 AD 用户身份验证。
- 在任何给定时间最多可将 NetBackupCLI 角色分配给九 (9) 个用户组。
- 无法为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。
- 您不能向具有与现有设备用户相同的用户名、用户 ID 或组 ID 的设备添加新用户或用户组。
- 不要使用已用于设备本地用户或 NetBackupCLI 用户的组名称或用户名。此外，不要对 LDAP、AD 或 NIS 用户使用设备的默认名称 **admin** 或 **maintenance**。
- 设备不处理 LDAP 或 NIS 配置的 ID 映射。Veritas 建议仅为设备用户保留 1000 到 1999 范围内的用户 ID 和组 ID。

请参见第 13 页的“关于 NetBackup Appliance 上的用户身份验证”。

请参见第 29 页的“关于授权 NetBackup Appliance 用户”。

关于对 LDAP 用户进行身份验证

NetBackup appliance 使用内置的可插入身份验证模块 (PAM) 插件以支持对轻量型目录访问协议 (LDAP) 用户进行身份验证。此功能允许添加属于 LDAP 目录服务的用户并授权用户登录 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

以下内容介绍了在设备上使用 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。

  注意：最佳做法是，不使用已用于设备本地用户或 NetBackupCLI 用户的组名称或用户名。此外，不要为 LDAP 用户使用设备默认名称 **admin** 或 **maintenance**。

- 设备不处理 LDAP 配置的 ID 映射。Veritas 建议仅为设备用户保留 1000 至 1999 范围内的用户 ID 和组 ID。

LDAP 用户身份验证的配置方法

必须将设备配置为可与 LDAP 服务器进行通信，然后才能在设备上注册新的 LDAP 用户和用户组。配置完成后，设备便可访问 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，请使用以下方法之一：

- NetBackup Appliance Web Console中的 **Settings > Authentication > LDAP**。
- NetBackup Appliance Shell Menu中的 `Settings > Security > Authentication > LDAP`。

有关如何在设备上配置和管理 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 使用内置的可插入身份验证模块 (PAM) 插件以支持对 Active Directory (AD) 用户进行身份验证。此功能允许添加属于 AD 服务的用户并授权用户登录 NetBackup appliance。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

以下内容介绍了在设备上使用 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。

注意：最佳做法是，不使用已用于设备本地用户或 NetBackupCLI 用户的组名称或用户名。此外，不要为 AD 用户使用设备默认名称 **admin** 或 **maintenance**。

- 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 服务器配置设备。或者，将设备配置为使用 AD DNS 服务器作为名称服务数据源。

Active Directory 用户身份验证的配置方法

必须将设备配置为可与 AD 服务进行通信，然后才能在设备上注册新的 AD 用户和用户组。配置完成后，设备便可访问 AD 服务器的用户信息以进行身份验证。

使用以下方法之一配置 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和管理 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 使用内置的可插入身份验证模块 (PAM) 插件以支持对网络信息服务 (NIS) 用户进行身份验证。此功能允许添加属于 NIS 目录服务的用户并授权用户登录 NetBackup appliance。UNIX 服务认为 NIS 是安装了架构的另外一种类型的用户目录。

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。

通过 Kerberos 使用 NIS 用户身份验证的先决条件

以下内容介绍了在设备上使用 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。
- 设备不处理 NIS 配置的 ID 映射。Veritas 建议仅为设备用户保留 1000 至 1999 范围内的用户 ID 和组 ID。

  注意：最佳做法是，不使用已用于设备本地用户或 NetBackupCLI 用户的组名称或用户名。此外，不要为 NIS 用户使用设备默认名称 **admin** 或 **maintenance**。

- 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，请始终使用 NTP 服务器在设备、NIS 服务器和 Kerberos 服务器之间同步时间。

通过 Kerberos 进行 NIS 用户身份验证的配置方法

必须将设备配置为与 NIS 服务器和 Kerberos 服务器通信，然后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 域用户信息以进行身份验证。

要配置 Kerberos-NIS 身份验证，请使用以下任一方法：

- 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和管理 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 appliance，可在用户尝试登录该设备时设置显示的文本提示。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、警告消息和公司策略信息。

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 2-5 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（例如 NetBackup Appliance Shell Menu和 SSH）都将显示该提示。但是，可以选择为 NetBackup 管理控制台打开或关闭登录提示。

表 2-5 支持登录提示的设备接口

接口	说明
NetBackup Appliance Shell Menu	用户尝试登录 NetBackup Appliance Shell Menu之前，会出现登录提示。
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 Appliance Web Console	每次通过 Web 浏览器访问设备时都会显示登录提示。仅可以通过单击“**同意**”按钮解除登录提示。
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 I 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》。

或者，在 NetBackup Appliance Web Console中通过路径“**设置**”**>**“**通知**”**>**“**登录提示**”配置登录提示。 有关更多信息，请参阅《NetBackup appliance 管理指南》。

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 2-6 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 2-6 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： ■ 编号 ■ 特殊字符	用户名不能以这些字符开始： ■ 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，提高了设备的安全性。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 2-7 列出了每个用户类型的密码规范。

表 2-7 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	密码必须至少包含八个字符。	密码必须至少包含八个字符。	由 LDAP、AD 或 NIS 策略确定
要求	■ 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。	■ 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

描述	管理员（本地用户）	NetBackupCLI（本地用户）	注册的远程用户
最小密码期限	0 天	0 天 **注意：**您可以使用 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。	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
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，Veritas 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 `passwd` 等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。

密码保护

NetBackup appliance 采用了以下密码保护措施：

- 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）的密码均使用 SHA-512 哈希算法加以保护。每当创建新的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 进行哈希处理。

  注意：在版本 2.6.1.1 之前，设备使用了多种默认密码哈希算法，包括 SHA-512、SHA-256 和 Blowfish。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 Veritas 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，以便他们可以使用新的默认算法。

- 密码历史记录设置为 7，意味着旧密码受到保护并最多记录 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：
  - 密码受 SSH 协议保护的 SSH 登录。
  - 密码受 HTTPS 通信保护的 NetBackup Appliance Web Console 登录

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

关于符合 STIG 规范的密码策略规则

启用 STIG 选项时，NetBackup 设备将自动强制执行较高的安全密码策略以遵从“安全技术操作指南 (STIG)”。

启用 STIG 选项后，在默认策略下创建的所有当前用户的密码仍有效。一旦准备更改任何用户密码，必须遵循符合 STIG 规范的策略规则。

以下内容介绍了符合 STIG 规范的密码策略规则：

- 最少字符数：15
- 最少字数数：1
- 最少小写字符数：1
- 最少大写字符数：1
- 最少特殊字符数：1
- 最多连续重复字符数：2
- 最多同类连续重复字符数：4
- 最少不同类字符数：8

- 密码更改的最少天数：1
- 密码更改的最多天数：60
- 字典中的单词无效或不可接受。
- 最近使用过的七个密码不可重复使用

强制锁定登录

启用 STIG 选项后，它会强制对在 15 分钟内密码连续输入错误三次的任何用户锁定登录。锁定条件有效期为七天。要清除锁定条件，请联系技术支持获取帮助。

请参见第 88 页的“NetBackup Appliance 的 OS STIG 加固”。

3

用户授权

本章节包括下列主题：

关于 NetBackup appliance 的用户授权

通过用户帐户对 NetBackup appliance 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	为分配了管理员角色的用户帐户提供管理 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 32 页的“关于管理员用户角色”。

角色	描述
NetBackupCLI	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。NetBackupCLI 用户没有 NetBackup Appliance Web Console 和 NetBackup Appliance Shell Menu的访问权限。 请参见第 33 页的"关于 NetBackupCLI 用户角色"。
AMSadmin	分配了 AMSadmin 角色的用户帐户具有管理权限，可以访问 AMS 上托管的设备管理器。AMSadmin 用户可在设备管理器上执行所有功能，并集中管理多个设备。AMSadmin 用户无法登录到 AMS 的 NetBackup Appliance Shell Menu。管理员可以创建 AMSadmin 用户。

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：从软件版本 3.1 开始，NetBackup appliance 将限制登录尝试次数，并仅当启用 STIG 功能后才强制执行锁定策略。有关详细信息，请参考以下主题：请参见第 26 页的"关于符合 STIG 规范的密码策略规则"。

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	“设置”>“身份验证”>“用户管理”下提供了以下选项 ■ 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。	使用 `Settings > Security > Authentication` 命令可添加、删除和查看设备用户。 请参见第 17 页的“关于配置用户身份验证”。
管理用户权限（角色）	“设置”>“身份验证”>“用户管理” 下提供了以下选项： ■ 授予和撤消用户和用户组的管理员角色。 ■ 授予和撤消用户和用户组的 NetBackupCLI 角色。 ■ 将已注册用户组的成员与管理员角色同步。	`Main > Settings > Security > Authorization` 下提供了以下命令和选项： ■ `Grant` 为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消管理员和 NetBackupCLI 角色。 ■ `SyncGroupMembers` 同步已注册用户组的成员。

有关用户管理的注释

- 无法为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) 用户组和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 用户名和用户组名不能以连字符开始或结束。

- 可以从 NetBackup Appliance Web Console列出具有最多 2000 个用户的组的所有用户。要列出具有超过 2000 个用户的组的所有用户，请使用 NetBackup Appliance Shell Menu中的 `List` 命令。

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 33 页的"关于 NetBackupCLI 用户角色"。
管理员	用户可以访问以下内容： ■ NetBackup Appliance Web Console ■ NetBackup Appliance Shell Menu ■ NetBackup 管理控制台 请参见第 32 页的"关于管理员用户角色"。
AMSadmin	分配了 **AMSadmin** 角色的用户帐户具有管理权限，可以访问 AMS 上托管的设备管理控制台。AMS 用户可在设备管理控制台上执行所有功能，并集中管理多个设备。AMS 用户无法登录到 AMS 的 NetBackup Appliance Shell Menu。管理员可以创建 AMS 用户。

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
Grant AMS Group
Grant AMS Users
```

请参见第 17 页的“关于配置用户身份验证”。

请参见第 29 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。
- 装入或映射共享。存在以下限制：
  - Windows：只有本地 **admin** 用户有权装入或映射 Windows CIFS 共享。
  - Linux：只有具有 root 访问权限帐户的用户可以直接发出装入命令以装入 NFS 共享。

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
NetBackupCLI 用户可以使用 NetBackup Appliance Shell Menu执行以下操作： ■ 运行 NetBackup CLI 并访问 NetBackup 目录和文件。 ■ 使用 `cp-nbu-notify` 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： ■ `/usr/openv/netbackup/bin/*` ■ `/usr/openv/netbackup/bin/admincmd/*` ■ `/usr/openv/netbackup/bin/goodies/*` ■ `/usr/openv/volmgr/bin/*` ■ `/usr/openv/volmgr/bin/goodies/*` ■ `/usr/openv/pdde/pdag/bin/mtstrmd` ■ `/usr/openv/pdde/pdag/bin/pdcfg` ■ `/usr/openv/pdde/pdag/bin/pdusercfg` ■ `/usr/openv/pdde/pdconfigure/pdde` ■ `/usr/openv/pdde/pdcr/bin/*`	以下限制将加在 NetBackupCLI 用户上： ■ 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 `bp.conf` 文件。使用`bpsetconfig`命令设置属性。 ■ `cp-nbu-config` 命令仅支持在 `/usr/openv/netbackup/db/config` 目录中创建和编辑 NetBackup touch 配置文件。 ■ 他们无法使用 `man` 或 `-h` 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

使用以下方法之一可以 NetBackupCLI 用户身份运行命令：

- 受限的 shell。
- 绝对路径 [“sudo”]。例如：bpplist 或 /usr/openv/netbackup/bin/admincmd/bpplist

如何运行特殊指令操作

如果特殊指令文件和命令不在正确的 NetBackup 列表或路径中，则特殊指令操作可能会失败。指定备用还原路径是一个特殊指令操作示例。

需以 NetBackupCLI 用户身份运行 NetBackup 命令以访问特殊指令文件的设备用户必须执行以下操作来确保操作成功：

- 将 /home/nbusers 路径添加到 NetBackup bpcd whitelist。
- 将特殊指令命令添加到 /home/nbusers 目录。

有关将条目添加到 NetBackup bpcd whitelist 的详细信息，请参考下列文档中的 BPCD_WHITELIST_PATH 配置选项：

《NetBackup 管理指南，第 1 卷》

《NetBackup 命令参考指南》

4

入侵防护和入侵检测系统

本章节包括下列主题：

关于 NetBackup appliance 上的 Symantec Data Center Security

注意：在之前的设备发行版中，Symantec Data Center Security (SDCS) 叫作 Symantec Critical System Protection (SCSP)。作为升级到 NetBackup Appliance 2.7.1 及更高版本的一部分，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 appliance 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：

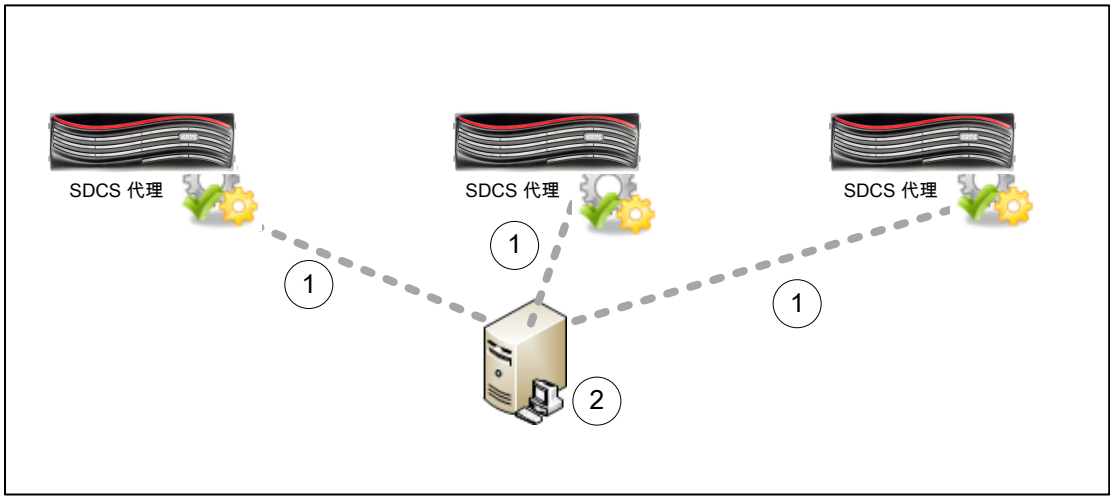
- 加固的 Linux 操作系统组件
  防止或遏制因操作系统漏洞造成恶意软件对基础主机系统完整性的损害。
- 数据保护
  不论系统权限如何，严格限制对设备数据的访问，仅允许需要访问的程序和活动进行访问。
- 加固的设备堆栈
  锁定设备应用程序二进制和配置设置，这样应用程序或可信程序/脚本可严格控制更改。
- 扩展检测和审核功能
  对重要用户或系统操作提供增强的可见性，以确保有效且完整的审核跟踪，该审核跟踪将遵从性法规（例如 PCI）作为补偿控制措施。
- 集中管理模式操作
  允许您使用中央 SDCS 管理器综合查看多个设备以及 SDCS 管理的任意其他企业系统之中的安全性。

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 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
- 连接到 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备份数据，例如 /advanceddisk、/cat、/disk、/usr/openv/kms、/opt/NBUAppliance/db/config/data 等。
- 限制维护用户对 root 帐户的访问。请参见第 42 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。	例如，以下消息提供了与常规事件相关的基本信息。
		
		`general CLISH message`
		
		`Event source: SYSLOG PID: 30315 Complete message: May 21 06:58:55 nb-appliance CLISH[30315]: User admin executed Return`

严重性级别类型	描述	事件示例

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。	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。
		
		`successful SUDO to root`
		`Event source: SYSLOG [sudo facility]`
		`Command: /bin/su From`
		
		`Username: AppComm To Username: root`
		`Port: unknown`

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。	例如，以下事件有助于识别意外活动，如来自本地 IP 地址的入站连接。 `Inbound connection allowed from <IPaddress> to local address.`

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.`

严重性级别类型	描述	事件示例
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 48 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。

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 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 确保 SDCS 控制台可以连接到 SDCS 服务器且服务器可以连接到设备。

如果需要 SDCS 控制台和服务器软件，您可以从 https://my.veritas.com 下载。

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 33 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: 6.7 (build 1060)

Current Policy: NetBackup Appliance Prevention Policy, r123

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：Veritas 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: 6.7 (build 1060)

Current Policy: NetBackup Appliance Prevention Policy, r123

Policy Prevention: Enabled

Policy Override: Allowed

Override State: Overriden

Overide Type: Prevention Overriden except for Self-Protection

Overide 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.
```

5

日志文件

本章节包括下列主题：

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	访问方法	日志详细信息
NetBackup Appliance Web Console	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 39 页的“重新查看 NetBackup 设备上的 SDCS 事件”。	设备审核日志

起始位置	访问方法	日志详细信息
NetBackup Appliance Shell Menu	可以使用 `Main > Support > Logs > Browse` 命令打开 `LOGROOT/>` 提示符。您可以使用 `ls` 和 `cd` 遍历该设备的日志目录。 请参见第 50 页的"使用 Support 命令查看日志文件"。	■ 设备配置日志 ■ 设备命令日志 ■ 设备调试日志 ■ 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
NetBackup Appliance Shell Menu	可以使用 `Main > Support > Logs > VxLogView Module` *`ModuleName`* 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。 请参见第 50 页的"使用 Support 命令查看日志文件"。	设备统一日志： ■ `All` ■ `CallHome` ■ `Checkpoint` ■ `Commands` ■ `Common` ■ `Config` ■ `CrossHost` ■ `Database` ■ `Hardware` ■ `HWMonitor` ■ `Network` ■ `RAID` ■ `Seeding` ■ `SelfTest` ■ `Storage` ■ `SWUpdate` ■ `Trace` ■ `FTMS` ■ `FTDedup` ■ `TaskService` ■ `AuthService`
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 52 页的"通过 Datacollect 命令收集设备日志"。	设备存储设备日志

起始位置	访问方法	日志详细信息
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

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 Menu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 `OS` 目录，则提示符将显示为 `LOGROOT/OS/>`。在此提示符下，您可以使用 `ls` 命令以显示 `OS` 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 51 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. 可以使用 `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。
2. 如果需要，可以使用 `Main > Support > Logs > Share Open` 命令复制统一日志。使用桌面映射、共享和复制日志。

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 Veritas 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 日志不再由 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 48 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`
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` ■ `<DIR> netbackup` ■ `<DIR> openv` ■ `<DIR> volmgr`

操作系统 (OS) 安装日志	`<DIR> OS`
	`boot.log`
	`boot.msg`
	`boot.omsg`
	`messages`

设备日志	日志文件位置
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 ■ <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 48 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 Veritas 支持团队共享这些设备日志，以解决设备相关问题。

DataCollect 命令可收集以下日志：

- 版本信息
- 磁盘性能日志
- 命令输出日志
- iSCSI 日志

注意：可以在 /var/log/messages 和 /var/log/iscsiuio.log 中找到 iSCSI 日志。

- CPU 信息
- 内存信息
- 操作系统日志
- 修补程序日志
- 存储日志
- 文件系统日志
- 测试硬件日志

- AutoSupport 日志
- 硬件信息
- Sysinfo 日志

通过 DataCollect 命令收集设备日志

1 登录到 NetBackup Appliance Shell Menu。

2 从 `Main > Support` 视图中，键入以下命令以收集设备日志。

```
DataCollect
```

设备会在 `/tmp/DataCollect.zip` 文件中生成设备日志。

3 使用 `Main > Support > Logs > Share Open` 命令将 `DataCollect.zip` 复制到本地文件夹。

4 可以将 `DataCollect.zip` 文件发送到 Veritas 支持团队以解决问题。

请参见第 48 页的“关于 NetBackup appliance 日志文件”。

日志转发功能概述

通过日志转发功能，可以将设备日志发送至外部日志管理服务器。自软件 3.0 版起，NetBackup 设备支持转发 syslog。syslog 是一种操作系统日志，以事件形式提供了用户和系统级别活动。使用此功能有助于增强安全性以及实现常规合规计划，例如，HIPPA、SOX 和 PCI。当前支持的日志管理服务器有 HP ArcSight 和 Splunk。

NetBackup Appliance 使用 Rsyslog 客户端转发日志。除了 HP ArcSight 和 Splunk 外，也可以使用其他支持 Rsyslog 客户端的日志管理服务器从设备接收 syslog。请参考日志管理服务器文档，验证 Rsyslog 客户端支持。

安全日志传输

要确保日志从设备安全地传输到日志管理服务器，可以使用 TLS（传输层安全）选项。NetBackup appliance 当前仅支持对日志转发进行 TLS 匿名身份验证。

要启用 TLS，设备和日志管理服务器各自需要不同的准备工作，如下所示：

- 设备要求
  配置和启用日志转发功能之前，设备需要具备以下使用 X.509 文件格式的证书和私钥文件：
  - `ca-server.pem`
    派生日志管理服务器证书的根 CA 证书。
  - `nba-rsyslog.pem`
    设备与日志管理服务器进行通信所用的证书，还包括任何中间 CA 证书。
  - `nba-rsyslog.key`

与 syslog 管理服务器进行通信所用证书对应的私钥。

您可以通过 NFS 或 CIFS 共享将这些文件上载到设备。

- HP ArcSight 服务器的配置要求
  必须在 HP ArcSight 服务器上设置带有 TLS 设置的 Rsyslog 服务器，才能从设备接收加密日志。然后，配置 Rsyslog 服务器以将解密后的日志转发到 HP ArcSiight 服务器。请参见 www.rsyslog.com 网站以获得设置和配置指南。
- Splunk 服务器的配置要求
  必须先在这些服务器上配置 TLS，然后在设备上配置日志转发功能。有关相应的 TLS 配置详细信息，请参考 Splunk 文档。

配置

此功能必须使用以下 Main > Settings > LogFowarding 命令选项从 shell 菜单进行配置：

- LogForwarding Enable
  配置功能。
- LogForwarding Disable
  删除配置和禁用功能。
- LogForwarding Interval
  设置日志转发频率。从 0（持续）、15、30、45 或 60 分钟中选择。
- LogForwarding Share
  打开或关闭设备上的 NFS 或 CIFS 共享，以获取所需证书和私钥文件。共享路径如下：
  NFS：<appliance.name>:/inst/logforwarding.
  CIFS：\\<appliance.name>\logforwarding
- LogForwarding Show
  显示当前配置和状态。

输入 LogForwarding > Enable 命令后，会出现提示以指导您完成配置，如下表所述：

表 5-3 LogForwarding > Enable 命令提示

提示	描述
服务器名称或 IP	输入外部日志管理服务器的名称或 IP 地址。
服务器端口	输入外部日志管理服务器上的相应端口号。
协议	选择 UDP 或 TCP。
间隔	设置日志转发频率。

提示	描述
启用 TLS	选择启用 TLS 以向日志管理服务器安全传输日志。当前，仅支持 X.509 文件格式。 必须将以下证书和私钥文件上载到设备才能使用 TLS： ■ `ca-server.pem` ■ `nba-rsyslog.pem` ■ `nba-rsyslog.key`

有关完整的配置和命令信息，请参考以下文档：

《NetBackup Appliance 管理指南》

《NetBackup Appliance 命令参考指南》

6

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 使用 Veritas 操作系统 (VxOS)，这是一个自定义的 Linux 操作系统。每个 NetBackup Appliance 软件版本均包含最新版本的 VxOS 和 NetBackup 软件。除了常规的安全修补程序和更新以外，VxOS 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。
- 基于国家标准与技术研究院 (NIST) 和 RHEL 制定的安全标准加固 VxOS。Symantec Data Center Security (SDCS) 增强了安全性。
- 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 VxOS 并保护备份数据。
- 使用行业认可的漏洞扫描程序对设备进行常规扫描。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 Veritas 支持联系获取已知的解决方案。
- 删除或禁用了未使用的服务帐户。
- VxOS 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。VxOS 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。
- VxOS 中禁用了 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 VxOS 中找到的所有全局可写入文件的权限。
- 搜索并修复了 VxOS 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。
- 从软件版本 3.1 开始，SMBv1 协议已禁用并替换为 SMBv2 协议。SMBv1 协议易受勒索软件（如 `WannaCry`、`Petya`）攻击，不再视为安全。SMBv2 如今是 NetBackup Appliance 的最低支持协议。

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 (VxOS) 的主要软件组件。

表 6-1 设备版本 3.1.1 VxOS 中包含的主要软件组件。

软件组件	版本
Red Hat Enterprise Linux (RHEL)	7.4
Veritas InfoScale	**注意：** 对 Veritas InfoScale 安装进行了修改和调整，以在设备上实现最佳性能。
Symantec Data Center Security: Server 6.7 Advanced (SDCS)	6.7 HF2
Java Runtime Environment (JRE)	8u162
Apache Tomcat	8.0.48
RabbitMQ	3.6.8
MongoDB	3.2.9

软件组件	版本
Intel IPMI Utils	2.9.5-1

NetBackup appliance 漏洞扫描

Veritas 使用行业认可的漏洞扫描程序定期对 NetBackup appliance 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。对于高严重性漏洞，Veritas 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 列出了用于此发行版的软件产品。

表 6-2 软件扫描软件和版本

安全扫描程序	版本
Nessus™	6.10.5（内部版本 #90）
QualysGuard™	9.9.13-1
Trustwave App Scanner™	OWASP ZAP 2.6.0

7

数据安全性

本章节包括下列主题：

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。
- 使用“自动通报”功能，利用 HTTPS 协议和端口 443 连接到 Veritas AutoSupport 服务器以上传硬件和软件信息。Veritas 技术支持可使用此信息解决可能报告的任何问题。此信息在 Veritas 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 目录库和 KMS 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，Veritas 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：

- 通过使用安全通道以加密格式传输数据。通过客户端加密和主从复制即可进行这些配置。如果不使用这些选项，则数据从设备中传输时，将使用网络基础架构来保护传输中的数据。
- 从 NetBackup appliance 版本 3.0（NetBackup 版本 8.0）开始，MSDP 提供 AES 加密。如果您的环境使用加密 MSDP，则新的传入数据会使用 AES 128 位（默认）或 AES 256 位加密。有关更多信息，请参见以下 NetBackup 文档：
  《Veritas NetBackup Deduplication 指南》
  《Veritas NetBackup 安全和加密指南》
- 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 61 页的“KMS 支持 ”。

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。对于设备版本 2.6 和更高版本，主服务器和介质服务器设备支持 KMS。在设备主服务器上恢复 KMS 的唯一一种受支持的方法是重新生成数据加密密钥。

以下内容介绍了 KMS 密钥功能：

- 无需额外的许可证。
- 是基于主服务器的对称密钥管理服务。
- 可以作为主服务器进行管理，并将磁带设备与之连接或与另一个 NetBackup appliance 连接。
- 按照 T10 标准（例如 LTO4 或 LTO5）管理磁带驱动器的对称密码密钥。
- 设计为使用基于卷池的磁带加密。
- 可用于具有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的设备中，只有当设备配置为介质服务器时才支持KMS。需要非设备主服务器才能使用连接到设备的设备管理 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列出了包含密钥相关信息的关联的 KMS 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	该文件对 KMS 至关重要，因为它包含数据加密密钥。	/usr/openv/kms/db/KMS_DATA.dat
主机主密钥	该文件包含使用 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	此加密密钥使用 AES 256 加密并保护 KMS_DATA.dat 密钥文件中的单个记录。当前，使用同一密钥保护密钥为所有记录加密。	/usr/openv/kms/key/KMS_KPKF.dat

配置 KMS

按照以下过程在设备上配置并启用KMS。您必须以NetBackupCLI用户身份登录到该设备来执行此过程。

在设备上配置并启用 KMS

1 以 NetBackupCLI 用户身份登录到该设备。

2 使用 nbkms 命令创建空数据库，如下所示：

```
[nbcli@myappliance~]# nbkms -createemptydb
```

3 启动 nbkms。例如：

```
[nbcli@myappliance~]# nbkms
```

4 创建密钥组。例如：

```
[nbcli@myappliance~]# nbkmsutil -createkg -kgname test_keygroup
```

5 创建活动密钥。例如：

```
[nbcli@myappliance~]# nbkmsutil -createkey -kgname test_keygroup
-keyname test_key
```

8

Web 安全

本章节包括下列主题：

- 关于 SSL 使用情况
- 实施第三方 SSL 证书

关于 SSL 使用情况

安全套接字层 (SSL) 协议可创建设备 Web 服务器与设备 Web 控制台和其他本地服务器之间的加密连接。通过此类型的连接，可在不发生个人身份信息窃取、数据篡改或消息伪造等问题的情况下更安全地传输信息。要在设备 Web 服务器上启用 SSL，需要能够识别设备主机的 SSL 证书。

设备使用自签名证书进行客户端和主机验证。设备证书是使用 2048 位 RSA 公钥生成的，该公钥已使用 SHA256 算法进行了哈希处理并使用 RSA 加密签名。为确保安全通信，设备仅使用 TLS v1.2 和更高版本的协议。

注意：通过将默认的自签名证书替换为 CA 颁发的自定义证书可避免“**无法信任 SSL 证书**”或“**SSL 自签名证书**”等警告。

为了在设备与各种外部服务器（例如 LDAP 和 Syslog）之间实现安全通信，也支持 SSL 证书。

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。 这些证书用于 SSL 加密和身份验证。

要实施已创建的第三方证书，请参见以下主题：

请参见第 65 页的“实施第三方 SSL 证书”。

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。要在设备中实施第三方证书，您必须以根帐户身份登录。

注意：如果您需要此过程相关的帮助，请与 Veritas 技术支持联系。

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。并且，不管您选择什么类型的 PKCS，keystore 文件必须包含以下关键字：

SubjectAlternativeName [

DNSName: hostnames and IP addresses

其中 *hostnames* 是设备的完全限定域名，*IP address* 对应于设备的完全限定域名。

]

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： 转换证书

PKCS 格式

PKCS#12 格式

准备 keystore 文件

执行下列操作：

- 要将 PEM 格式的 x509 证书和私钥转换为 PKCS# 12，请键入以下命令：

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

  有关 `openssl` 用法的更多信息，请参考 https://www.openssl.org/。

  注意：确保使用密码保护 PKCS #12 文件。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

- 要将 pkcs12 文件转换为 Java Keystore，请键入以下命令：

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

  注意：为 -deststorepass 和 -destkeypass 选项指定相同的密码。否则，在 Web 服务器启动时可能会遇到异常。对于密码，仅支持字母数字字符。默认密码为 *appliance*。

  为 -alias 选项指定 **tomcat**。否则，在 Web 服务器启动时可能会遇到异常。

  注意：有关 `keytool` 用法的更多信息，请参考以下链接：

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

2 键入以下命令以关闭数据库和相关服务：

```
/opt/IMAppliance/scripts/infraservices.sh database stop

systemctl stop nginx

/opt/IMAppliance/scripts/infraservices.sh database stop

/opt/IMAppliance/scripts/infraservices.sh webserver stop
```

3 将现有的 keystore 文件替换为以下目录中的新 keystore 文件：

```
/opt/apache-tomcat/security/
```

4 将权限设置为新的 keystore 文件：

```
chmod 700 /opt/apache-tomcat/security

chmod 600 /opt/apache-tomcat/security/keystore

chown -R tomcat:tomcat /opt/apache-tomcat/security
```

5 如果在前面的步骤中使用自己的非默认密码，则键入以下命令以更新 Web 服务器配置：

```
/opt/apache-tomcat/vrts/scripts/tomcat_instance.py update
--keystore --password <your password>
```

6 在 `/etc/rc.d/init.d/as-functions` 文件中更新 **Tomcat_Keystore** 和 **Tomcat_Keystore_Passwd** 设置。

7 将证书导入到 `mongo_server_part_pam` 文件，并从 `/etc/vxos-ssl/cert.conf` 中获取 server-Cert，然后将证书导入到其中。

```
/usr/bin/openssl pkcs12 -in server.p12 -out <server_cert> -passin
pass:

<keyPassword> -passout pass: <keyPassword>
```

8 将证书导入到 `client_part_pam` 文件，并从 `/etc/vxos-ssl/cert.conf` 中获取 `client_cert`，然后将证书导入到其中：

```
/usr/bin/openssl pkcs12 -nokeys -in server.p12 -out <server_cert>
-passin pass:

<keyPassword> -passout pass: <keyPassword>
```

9 如果自定义的密码与 `/etc/vxos-ssl/cert.conf` 中的 `pem_password` 不同，则修改 `/etc/vxos-ssl/cert.conf` 以使用自定义的密码。

10 键入以下命令以重新启动 nginx：

```
/usr/sbin/update-nginx-conf.sh
service nginx stop
service nginx start
```

11 键入以下命令以重新启动 Web 服务：

```
/opt/IMAppliance/scripts/infraservices.sh database start
/opt/IMAppliance/scripts/infraservices.sh webserver start
```

12 键入以下命令以重新启动 AutoSupport 服务：

```
service as-alertmanager stop
service as-analyzer stop
service as-transmission stop
service as-alertmanager start
service as-analyzer start
service as-transmission start
```

9

网络安全

本章节包括下列主题：

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 Verisign 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《NetBackup Appliance 命令参考指南》。

关于 NetBackup appliance 端口

除 NetBackup 软件使用的端口之外，NetBackup Appliance 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。使用 `https://<appliance-name>` 登录 Web 控制台，其中 appliance-name 是设备的完全限定域名 (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
443	HTTPS	带内管理 GUI
5900	KVM	CLI 访问、ISO 和 CDROM 重定向
623	KVM	（可选，打开时使用）
2049	NFS	NFS
445		CIFS（用于日志/安装共享）

+ NetBackup Integrated storage manager

* Veritas Remote Management - 远程控制台

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 Veritas 发送自动通报通知 下载 SDCS 证书
162**	SNMP	下载设备更新
22	SFTP	将日志上载到 Veritas
25	SMTP	电子邮件警报
389	LDAP	
636	LDAP	
514	rsyslog	日志转发

** 可以在设备配置中更改此端口号以匹配远程服务器。

表 9-4 列出了 NetBackup Appliance 的 Out of Band Management 端口。

表 9-4 Out of Band Management 端口

80	HTTP	带外管理（ISM+ 或 RM*）
443	HTTP	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	CDROM
5127		USB 或软盘
2049	NFS	NFS
445		CIFS（用于日志/安装共享）

+ NetBackup Integrated storage manager

* Veritas Remote Management - 远程控制台

注意：端口 7578、5120 和 5123 用于未加密模式。端口 7582、5124 和 5127 用于加密模式。

《NetBackup 网络端口参考指南》中提供了所有适用端口的完整列表。

10

自动通报安全

本章节包括下列主题：

关于 AutoSupport

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

MyAppliance 门户是注册设备和编辑注册详细信息的统一地址。

支持基础架构旨在允许 Veritas 支持通过以下方式为您提供帮助：

- 通过主动监视，Veritas 支持可自动创建案例、修复问题并分派任何可能存在风险的设备部件。
- Veritas 中的 AutoSupport 基础架构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，Veritas 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 Veritas 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，如第二联系人、电话、机架位置等，可以访问 https://my.veritas.com。

数据安全标准

从设备传输到 Veritas 的所有数据都通过行业标准的高度加密方法进行处理。以下数据安全标准适用于在客户端和服务器之间发送的所有 AutoSupport 数据，以及在客户端内部不同组件之间进行的数据通信：

- 适用于服务器身份验证的 RSA 2048 位密钥
- 适用于数据加密的 AES 128/256 位密钥
- 适用于消息身份验证的 SHA1、SHA2（256/384 位）哈希

关于自动通报

设备可与 Veritas AutoSupport 服务器连接并上载硬件和软件信息。Veritas 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 Veritas 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 小时定期将信息（或自动通报数据）上载到 Veritas AutoSupport 服务器。

如果确定设备存在问题，您可能希望与 Veritas 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	故障例程
自动通报已启用	当发生故障时，会依次出现以下警报： ■ 设备将所有受监视的硬件和软件信息上载到 Veritas 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。 ■ 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	未将任何数据发送到 Veritas AutoSupport 服务器。您的系统不会向 Veritas 报告错误以加快解决问题的速度。

以下列表提供了发送到 Veritas 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

- 53xx 主存储扩展架 - 磁盘、风扇、电源、温度、备用电池（BBU）、控制器、卷和卷组的状态
- 53xx 扩展存储扩展架 - 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 77 页的“从 NetBackup Appliance Shell Menu配置自动通报”。

请参见第 74 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：

- 从设备 Shell 菜单启用和禁用“自动通报”功能
- 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。

要了解有关 `Main > Settings > Alerts > CallHome` 命令的详细信息，请参阅《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 75 页的“关于自动通报”。

从设备 Shell 菜单启用和禁用“自动通报”功能

您可以从 NetBackup Appliance Shell Menu和 Access 3340 Appliance Shell 菜单启用或禁用“自动通报”功能。默认情况下启用自动通报。

从 shell 菜单启用或禁用自动通报

1 登录到 shell 菜单。

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` 命令的更多信息，请参阅《NetBackup Appliance 命令参考指南》或 *Access 3340 Appliance Getting Started Guide*（《Access 3340 Appliance 快速入门指南》）。

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 Veritas 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 Veritas 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 Veritas 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 Veritas 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日志。
- 然后，将日志上载到 Veritas AutoSupport 服务器以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 75 页的“关于自动通报”。

请参见第 74 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。

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 由一些以小数点隔开的数字组成（例如，1.3.6.1.4.1.48328.1）。

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 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**”页面中的“**查看 SNMP MIB 文件**”。

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

11

IPMI 安全

本章节包括下列主题：

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 Veritas Remote Management 工具。Veritas 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，请遵循下列建议：

- 不使用空用户名或密码创建帐户。
- 将管理用户的数量限制在一个。
- 禁用任何匿名用户。
- 要缓解 CVE-2013-4786 漏洞：

- 使用强密码帮助阻止离线字典攻击和暴力强制攻击。建议的密码长度为 16-20 个字符。
- 尽快更改默认用户密码 (`sysadmin`)。
- 使用访问控制列表 (ACL) 或隔离的网络来限制对 IPMI 接口的访问。

登录

对 IPMI 用户应用登录设置时，请使用下列建议：

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 启用“**强制 HTTPS**”以确保 IPMI 连接始终使用 HTTPS。
Web 会话超时	1800

LDAP 设置

Veritas 建议启用 LDAP 身份验证。

SSL 上载

Veritas 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

为了帮助防止未经过身份验证进行 IPMI 用户操作或活动，应禁用特定密码。要进一步获取帮助，请与技术支持联系并通知技术支持代表参考编号为 000127964 的文章。

以太网连接设置

对 IPMI 使用专用的以太网连接，避免共享物理服务器连接。

- 使用静态 IP。
- 避免使用 DHCP。

替换默认 IPMI SSL 证书

Veritas 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 字母代码）[AU]：	输入您所在国家/地区的名称。例如，US。
省/市/自治区名称（全名）[Some-State]：	输入您所在省/市/自治区的名称。例如，OR。
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）[Internet Widgits Pty Ltd]：	输入您组织的名称。例如，Veritas。
组织单元名称（如部门）[]：	输入您组织单元的名称。
常见名称（如您的姓名）[]：	输入 `hostname.your.company`。
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=Veritas/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 Veritas 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 Veritas Remote Management（IPMI Web 界面）界面，以验证所显示的是否为新证书。

12

STIG 和 FIPS 一致性

本章节包括下列主题：

NetBackup Appliance 的 OS STIG 加固

安全技术实施指南 (STIG) 提供了用于提高信息系统和软件的安全性的技术指导，从而帮助防止计算机受到恶意攻击。这种安全性类型也称为加固。

从软件版本 3.1 开始，为了提高安全性，您可以启用 OS STIG 加固规则。这些规则基于国防信息系统局 (DISA) 的以下配置文件：

Red Hat Enterprise Linux 7 Server 的 STIG - 0.1.31 版

要启用这些规则，请使用以下命令：

`Main_Menu > Settings > Security > Stig Enable`，后跟维护密码。

请注意有关启用 STIG 的以下几点：

- 启用该选项时，将显示强制执行的规则列表。命令输出还显示不强制执行的任何规则的例外情况。
- 此命令不支持单个规则控制。
- 对于高可用性 (HA) 设置中的设备（节点）中，必须在每个节点上手动启用此功能以确保转换后正常运行。
- 启用该选项后，需要执行恢复出厂设置才可禁用关联的规则。
- 如果已配置轻型目录访问协议 (LDAP)，建议您先将其设置为使用传输层安全性 (TLS)，然后再启用该选项。

注意：如果在设备上启用了 STIG 功能，且需要在该设备上升级或安装 EEB，请勿计划在 4:00am - 4:30am 时段进行此类安装。按照此最佳做法，可以避免中断 AIDE 数据库和所有受监视文件的自动更新，而中断其自动更新可能会导致设备发出多个警报消息。

下面介绍了在启用该选项后强制执行的加固规则。每个规则均由通用配置枚举器 (CCE) 标识符、简短规则描述和安全内容自动化协议 (SCAP) 扫描程序严重性级别进行标识。软件版本 3.1 可处理扫描程序严重性级别为高和中的规则。

启用该选项后强制执行的规则

- CCE-27127-0：启用虚拟地址空间的随机布局。
  扫描程序严重性级别：中
- CCE-26900-1：禁止对 SUID 程序进行核心转储。
  扫描程序严重性级别：低
- CCE-27050-4：限制对内核消息缓冲区的访问。
  扫描程序严重性级别：低
- CCE-80258-7：禁用 kdump 内核崩溃分析程序。
  扫描程序严重性级别：中
- CCE-27220-3：构建并测试 AIDE 数据库。
  扫描程序严重性级别：中
- CCE-26952-2：配置 AIDE 的定期执行。
  扫描程序严重性级别：中
- CCE-27303-7：修改系统登录提示。
  扫描程序严重性级别：中
- CCE-27082-7：设置 SSH 客户端动态帐户。
  扫描程序严重性级别：中
- CCE-27314-4：启用 SSH 警告提示。
  扫描程序严重性级别：中
- CCE-27437-3：确保 auditd 收集有关使用特权命令的信息。
  扫描程序严重性级别：中
- CCE-27309：设置引导加载程序密码。
  扫描程序严重性级别：高
- CCE-80374-2：配置 AIDE 扫描结果的通知。
  扫描程序安全级别：中
- CCE-80375-9：将 AIDE 配置为对访问控制列表 (ACL) 进行验证。
  扫描程序严重性级别：中

- CCE-80376-7：将 AIDE 配置为对扩展属性进行验证。
  扫描程序严重性级别：中
- CCE-27375-5：配置磁盘空间不足时的 `auditd_space_left_action`。
  扫描程序严重性级别：中
- CCE-27341-7：将 `auditd` 配置为使用 `audispd_syslog_plugin`。
  扫描程序安全级别：中
- CCE-27353-2：记录修改系统自主访问控制的事件 (`fremovexattr`)。
  扫描程序严重性级别：中
- CCE-27410-0：记录修改系统自主访问控制的事件 (`lremovexattr`)。
  扫描程序严重性级别：中
- CCE-27367-2：记录修改系统自主访问控制的事件 (`removexattr`)。
  扫描程序严重性级别：中
- CCE-27204-7：记录修改登录和注销事件的尝试次数。
  扫描程序严重性级别：中
- CCE-27347-4：确保 `auditd` 收集未经授权的文件访问尝试次数。
  扫描程序严重性级别：中
- CCE-27447-2：确保 `auditd` 收集有关成功导出到介质的信息。
  扫描程序严重性级别：中
- CCE-27206-2：确保 `auditd` 收集用户执行的文件删除事件。
  扫描程序严重性级别：中
- CCE-27129-6：确保 `auditd` 收集有关内核模块加载和卸载的信息。
  扫描程序严重性级别：中
- CCE-27333-4：设置最多连续重复字符数的密码规则。
  扫描程序严重性级别：中
- CCE-27512-3：设置相同字符类的最多连续重复字符数的密码规则。
  扫描程序严重性级别：中
- CCE-27214-6：设置最少数字字符数的密码强度。
  扫描程序严重性级别：中
- CCE-27293-0：设置最小长度的密码规则。
  扫描程序严重性级别：中
- CCE-27200-5：设置最少大写字符数的密码强度。
  扫描程序严重性级别：中
- CCE-27360-7：设置最少特殊字符数的密码强度。
  扫描程序严重性级别：中

- CCE-27345-8：设置最少小写字符数的密码强度。
  扫描程序严重性级别：中
- CCE-26631-2：设置最少不同字符数的密码强度。
  扫描程序严重性级别：中
- CCE-27115-5：禁止通过 `modprobe` 加载 USB 存储驱动程序。
  扫描程序严重性级别：中
- CCE-27350-8：设置因密码尝试失败而拒绝访问的次数。
  扫描程序严重性级别：中
- CCE-80353-6：为失败的密码尝试配置 root 帐户。
  扫描程序严重性级别：中
- CCE-26884-7：为失败的密码尝试设置锁定时间。
  扫描程序严重性级别：中
- CCE-27297-1：设置对失败的密码尝试进行计数的间隔。
  扫描程序严重性级别：中
- CCE-27002-5：设置最短密码期限。
  扫描程序严重性级别：中
- CCE-27051-2：设置最长密码期限。
  扫描程序安全级别：中
- CCE-27081-9：限制每个用户允许的并行登录会话数。
  扫描程序严重性级别：低

始终强制执行的规则

以下规则始终强制执行，无法禁用。这些规则的加固符合“NIST 专刊 800-123”中所述的规范。有关更多信息，请参考以下内容：

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

- CCE-80165-4：配置用于忽略 ICMP 广播回显请求的内核参数。
  扫描程序严重性级别：中
- CCE-80156-3：禁用默认情况下用于发送 ICMP 重定向的内核参数。
  扫描程序严重性级别：中
- CCE-80156-3：禁用用于发送所有接口的 ICMP 重定向的内核参数。
  扫描程序严重性级别：中
- CCE-27212-0：为在审核后台驻留程序之前启动的进程启用审核。
  扫描程序严重性级别：中
- CCE-26957-1：确保已安装 Red Hat GPG 密钥。
  扫描程序严重性级别：高

- CCE-27096-7：确保已安装 AIDE 软件包。
  扫描程序严重性级别：中
- CCE-27351-6：安装 screen 软件包。
  扫描程序严重性级别：中
- CCE-27268-2：限制串行端口以 root 身份登录。
  扫描程序严重性级别：低
- CCE-27318-5：限制虚拟控制台以 root 身份登录。
  扫描程序严重性级别：中
- CCE-27471-2：禁止在没有密码的情况下进行 SSH 访问。
  扫描程序严重性级别：高
- CCE-27286-4：防止在没有密码的情况下登录到帐户。
  扫描程序严重性级别：高
- CCE-27511-5：禁用 **Ctrl-Alt-Del** 重新启动激活。
  扫描程序严重性级别：高
- CCE-27320-1：仅允许 SSH 协议版本 2。
  扫描程序严重性级别：高
- CCE-27294-8：不允许直接以 root 身份登录。
  扫描程序严重性级别：中
- CCE-80157-1：禁用用于 IP 转发的内核参数。
  扫描程序严重性级别：中
- CCE-80158-9：配置用于接受所有接口的 ICMP 重定向的内核参数。
  扫描程序严重性级别：中
- CCE-80163-9：配置默认情况下用于接受 ICMP 重定向的内核参数。
  扫描程序严重性级别：中
- CCE-27327-6：禁用蓝牙内核模块。
  扫描程序严重性级别：中
- CCE-80179-5：配置用于接受所有接口的源路由数据包的内核参数。
  扫描程序严重性级别：中
- CCE-80220-7：禁用 GSSAPI 身份验证。
  扫描程序严重性级别：中
- CCE-80221-5：禁用 Kerberos 身份验证。
  扫描程序严重性级别：中
- CCE-80222-3：启用严格模式检查。
  扫描程序严重性级别：中

- CCE-80224-9：禁用压缩或将压缩设置为延迟。
  扫描程序严重性级别：中
- CCE-27455-5：只使用 FIPS 批准的 MAC。
  扫描程序严重性级别：中
- CCE-80378-3：验证拥有 `/etc/cron.allow` 的用户。
  扫描程序严重性级别：中
- CCE-80379-1：验证拥有 `/etc/cron.allow` 的组。
  扫描程序严重性级别：中
- CCE-80372-6：禁用对用户已知主机的 SSH 支持。
  扫描程序严重性级别：中
- CCE-80373-4：禁用对 `rhosts` RSA 身份验证的 SSH 支持。
  扫描程序严重性级别：中
- CCE-27363-1：不允许使用 SSH 环境选项。
  扫描程序严重性级别：中
- CCE-26989-4：确保 `gpgcheck` 已全局激活。
  扫描程序严重性级别：高
- CCE-80349-4：确保安装的操作系统已经过认证。
  扫描程序严重性级别：高
- CCE-27175-9：UID 只显示 0（进行更好地描述）。
  扫描程序严重性级别：高
- CCE-27498-5：禁用自动装入程序。
  扫描程序严重性级别：中
- CCE-80134-0：用户拥有所有文件。
  扫描程序严重性级别：中
- CCE-80135-7：组拥有所有文件权限。
  扫描程序严重性级别：中
- CCE-27211-2：`sysctl_kernal_exec_shield`。
  扫描程序严重性级别：中
- CCE-27352-4：验证是否隐藏所有帐户密码哈希。
  扫描程序严重性级别：中
- CCE-27104-9：设置密码哈希算法 `systemauth`。
  扫描程序严重性级别：中
- CCE-27124-7：设置密码哈希算法 `logindefs`。
  扫描程序严重性级别：中

- CCE-27053-8：设置密码哈希算法 libusercon。
  扫描程序严重性级别：中
- CCE-27078-5：禁用预链接软件。
  扫描程序严重性级别：低
- CCE-27116-3：在支持的 32 位 x86 系统上安装 PAE 内核。
  扫描程序严重性级别：低
- CCE-27503-2：/etc/password 中引用的所有 GID 必须在 /etc/group 中进行定义。
  扫描程序严重性级别：低
- CCE-27160-1：密码 pam retry。
  扫描程序严重性级别：低
- CCE-27275-7：显示登录尝试次数。
  扫描程序严重性级别：低
- CCE-80350-2：在 sudo 上删除 no_authenticate。
  扫描程序严重性级别：中
- CCE-26961-3：确保 /etc/default/grub 中未禁用 SELinux。
  扫描程序严重性级别：中

请参见第 94 页的“非强制 STIG 加固规则”。

非强制 STIG 加固规则

本主题介绍 NetBackup Appliance 上当前未强制执行的“安全技术操作指南 (STIG)”规则。出于以下原因（包括但不限于），可能不会强制执行此列表中的规则：

- 为未来设备软件版本计划强制执行规则。
- 备用方法可用于提供满足或超过规则中所述方法的保护。
- NetBackup Appliance 上未使用或不支持该规则中所述的方法。

以下内容介绍了当前未强制执行的 STIG 规则：

- CCE-26876-3：确保为所有 yum 软件包存储库启用了 gpgcheck。
  扫描程序严重性级别：高
- CCE-27209-6：验证并更正 rpm 的文件权限。
  扫描程序严重性级别：高
- CCE-27157-7：使用 rpm 验证文件哈希。
  扫描程序严重性级别：高
- CCE-80127-4：安装 McAfee Antivirus

扫描程序严重性级别：高

- CCE-26818-5：安装入侵检测软件。
  扫描程序严重性级别：高
- CCE-27334-2：确保强制执行 SELinux 状态。
  扫描程序严重性级别：高
- CCE-80226-4：启用经过加密的 X11 转发。
  扫描程序严重性级别：高
- CCE-27386-2：确保不使用默认的 SNMP 密码。
  扫描程序严重性级别：高
- CCE-80126-6：安装资产配置遵从性模块 (ACCM)。
  扫描程序严重性级别：中
- CCE-80369-2：安装策略审核员 (PA) 模块。
  扫描程序严重性级别：中
- CCE-27277-3：禁止通过 `modprobe` 加载 USB 存储驱动程序。
  扫描程序严重性级别：中
- CCE-27349-0：为传入数据包设置默认的 `firewalld` 区域。
  扫描程序严重性级别：中
- CCE-80170-4：安装 `libreswan` 软件包。
  扫描程序严重性级别：中
- CCE-80223-1：启用特权分离。
  扫描程序严重性级别：中
- CCE-80347-8：确保为本地软件包启用 `gpgcheck`。
  扫描程序严重性级别：高
- CCE-80348-6：确保为存储库元数据启用 `gpgcheck`。
  扫描程序严重性级别：高
- CCE-80358-5：安装 `dracut_fips` 软件包。
  安全扫描程序级别：中
- CCE-80359-3：在 `GRand Unified Bootloader` 版本 2 (GRUB2) 中启用 FIPS 模式。
  扫描程序严重性级别：中
- CCE-27557-8：设置交互式会话超时以终止空闲会话。
  扫描程序严重性级别：中
- CCE-80377-5：将 AIDE 配置为用于验证哈希的 FIPS 140-2。
  扫描程序严重性级别：中

- CCE-80351-0：确保用户对权限提升 (`sudo_NOPASSWD`) 重新进行身份验证。
  扫描程序严重性级别：中
- CCE-27355-7：设置帐户不活动后的到期日期。
  扫描程序严重性级别：中
- CCE-80207-4：启用智能卡登录。
  扫描程序严重性级别：中
- CCE-27370-6：配置磁盘空间不足时的 `auditd_admin_space_left_action`。
  安全扫描程序级别：中
- CCE-27295-5：只使用经过批准的密码。
  扫描程序严重性级别：中
- CCE-26548-8：禁止通过 `bootloader` 配置实现 USB 的内核支持。
  扫描程序严重性级别：低
- CCE-27128-8：对分区进行加密。
  扫描程序严重性级别：高
- CCE-26895-3：确保已安装软件修补程序。
  扫描程序安全级别：高
- CCE-27279-9：配置 SE Linux 策略。
  扫描程序严重性级别：高
- CCE-27399-5：卸载 `ypserv` 软件包。
  扫描程序严重性级别：高
- CCE-80128-2：启用服务钉。
  扫描程序严重性级别：中
- CCE-80129-0：更新病毒扫描定义。
  扫描程序严重性级别：中
- CCE-27288-0：确保 SE Linux 已限制所有后台驻留程序。确保 SE Linux 已限制所有后台驻留程序。
  扫描程序严重性级别：中
- CCE-27326-8：确保 SE Linux 已对任何设备文件进行标记。/确保 SE Linux 已对所有设备文件进行标记。
  扫描程序严重性级别：中
- CCE-80354-4：设置 UEFI 引导加载程序密码。
  扫描程序严重性级别：中
- CCE-80171-2：验证任何已配置的 `IPSec` 隧道连接。
  扫描程序严重性级别：中
- CCE-26960-5：禁止从引导固件中的 USB 设备引导。

扫描程序严重性级别：低

- CCE-27194-0：分配密码以防止对引导固件配置进行更改。
  扫描程序严重性级别：低

请参见第 88 页的“NetBackup Appliance 的 OS STIG 加固”。

NetBackup Appliance 的 FIPS 140-2 一致性

联邦信息处理标准 (FIPS) 规定了美国和加拿大政府对计算机系统的安全和互操作性要求。国家标准与技术研究院 (NIST) 发布了 FIPS 140 系列出版物，用于调整验证加密模块的要求和标准。FIPS 140-2 标准规定了对加密模块的安全要求，适用于硬件和软件组件。它还阐述了获准的对称和非对称密钥加密、消息身份验证和哈希安全功能。

有关 FIPS 140-2 标准及其验证程序的更多信息，请单击以下链接：

https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf

https://csrc.nist.gov/projects/cryptographic-module-validation-program

NetBackup 加密模块已通过 FIPS 验证。NetBackup MSDP 使用此模块，且从 NetBackup Appliance 版本 3.1.1 开始，您可以使用以下命令为 NetBackup MSDP 启用 FIPS 140-2 标准：

`Main Menu > Settings > Security > FIPS > Enable`，后跟维护密码。

注意：启用或禁用此功能会自动终止当前正在进行的所有作业，并重新启动 NetBackup 服务。最佳做法建议首先手动停止所有作业，然后再启用或禁用此功能。

有关 FIPS 命令的完整信息，请参见《NetBackup Appliance 命令参考指南》。

注意：当前不支持在高可用性 (HA) 设置中的设备（节点）上使用 FIPS 功能。

附录 A

安全版本内容

本附录包括下列主题：

NetBackup Appliance 安全版本内容

以下列表包含已修复且现在包括在此版本 NetBackup Appliance 软件中的已知安全问题：

Spectre 和 Meltdown 漏洞

NetBackup Appliance 版本 3.1.1 包括特定于以下变体的修复：

- 变体 1 - Spectre，CVE-2017-5753
- 变体 3 - Meltdown，CVE-2017-5754

这些修复解决了本地用户可以安装并运行二进制文件来访问其他进程的内存这一潜在威胁。

为了缓解这些漏洞带来的危害，Veritas 建议您尽快将所有 NetBackup Appliance 升级到版本 3.1.1。有关这些漏洞的更多详细信息，请参见以下文章：

https://www.veritas.com/support/en_US/article.100041496

下面介绍了 3.1.1 版中已解决的其他漏洞：

- Apache Struts 漏洞
  CVE-2017-5638
- 针对 KRACK 的 WPA2 软件包更新：
  CVE-2017-13077
  CVE-2017-13078
  CVE-2017-13080
  CVE-2017-13082
  CVE-2017-13086

CVE-2017-13088

- DNS 软件包更新
  CVE-2017-14491
  CVE-2017-14492
  CVE-2017-14493
  CVE-2017-14494
  CVE-2017-14495
  CVE-2017-14496
- Java 漏洞
  CVE-2017-10309
  CVE-2017-10274
  CVE-2017-10293
  CVE-2017-10281
  CVE-2017-10347
  CVE-2017-10348
  CVE-2017-10349
  CVE-2017-10350
  CVE-2017-10357
  CVE-2017-10345
  VE-2017-10346
  CVE-2017-10285
- 其他
  CVE-2017-8030
  CVE-2017-8046
  CVE-2017-15288
  CVE-2017-5645
  CVE-2017-17485
  CVE-2017-1000253
  CVE-2017-7555
  CVE-2016-10164
  CVE-2017-2625
  CVE-2017-2626
  CVE-2016-10200
  CVE-2017-2647
  CVE-2017-8797
  CVE-2015-8839
  CVE-2015-8970
  CVE-2016-9576
  CVE-2016-7042

CVE-2016-7097
CVE-2016-8645
CVE-2016-9576
CVE-2016-9588
CVE-2016-9806
CVE-2016-10088
CVE-2016-10147
CVE-2017-2596
CVE-2017-2671
CVE-2017-5970
CVE-2017-6001
CVE-2017-6951
CVE-2017-7187
CVE-2017-7616
CVE-2017-7889
CVE-2017-8890
CVE-2017-9074
CVE-2017-9075
CVE-2017-9076
CVE-2017-9077
CVE-2017-9242
CVE-2014-7970
CVE-2014-7975
CVE-2016-6213
CVE-2016-9604
CVE-2016-9685
CVE-2016-10165
CVE-2016-8399
CVE-2016-9841
CVE-2017-1000111
CVE-2017-1000112
CVE-2017-10274
CVE-2017-10281
CVE-2017-10295
CVE-2017-7558
CVE-2017-10355
CVE-2017-7542
CVE-2017-10356
CVE-2017-10388
CVE-2017-7184

CVE-2017-12617

索引

R

S

T

W

Y

Z