神州云科
Yunke China

神州云科HDP 6100
备份一体机
安全指南

2023年11月

神州云科HDP 6100备份一体机安全指南

法律声明

本产品可能包括神州云科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。

了解神州云科更多信息，请联系当地代表处或者访问以下官网或微信公众号

神州云科（北京）科技有限公司

DC Yunke（Beijing）Technology Co., Ltd.

官网地址：www.yunke-china.com

总部地址：北京市海淀区上地九街9号数码科技广场

服务电话：4006680103

商标声明：

目录

1

关于神州云科HDP 6100备份一体机安全指南

本章节包括下列主题：

- 关于神州云科HDP 6100备份一体机安全指南

关于神州云科HDP 6100备份一体机安全指南

开发神州云科HDP 6100备份一体机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 操作系统和核心备份软件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。

在神州云科HDP 6100备份一体机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。根据所发现问题的严重性，神州云科会发布安全修补程序或在计划的主要版本或维护版本中提供修复程序。为了减少威胁的风险，在定期维护发布周期中，神州云科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神州云科HDP 6100备份一体机5.0中实施的安全功能，包括以下章节和小节：

神州云科HDP 6100备份一体机用户身份验证

本章介绍神州云科HDP 6100备份一体机中的身份验证功能，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
关于神州云科HDP 6100备份一体机上的用户身份验证	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“关于神州云科HDP 6100备份一体机上的用户身份验证”。

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 18 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 22 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 23 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 23 页的“关于对Kerberos-NIS 用户进行身份验证”。
关于智能卡身份验证	此部分描述配置设备以使用智能卡进行身份验证的前提条件和过程。	请参见第 24 页的“关于使用智能卡和数字证书进行身份验证”。
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 28 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 29 页的“关于用户名和密码规范”。

神州云科HDP 6100备份一体机用户授权

本章描述实施用于授权用户访问神州云科HDP 6100备份一体机的功能，包括以下部分：

表 1-2 关于授权的部分

部分名称	描述	链接
关于神州云科HDP 6100备份一体机上的用户授权	此部分描述神州云科HDP 6100备份一体机的授权过程的关键特性。	请参见第 34 页的“关于神州云科HDP 6100备份一体机的用户授权”。
关于授权神州云科HDP 6100备份一体机用户	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 36 页的“关于授权神州云科HDP 6100备份一体机用户”。
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 38 页的“关于管理员用户角色”。

部分名称	描述	链接
关于备份软件命令行用户角色	此部分描述备份软件命令行用户角色。	请参见第 39 页的“关于备份软件命令行用户角色”。

神州云科HDP 6100备份一体机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神州云科HDP 6100备份一体机的 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
关于神州云科HDP 6100备份一体机上的Symantec Data Center Security	此部分介绍在设备上实现的 SDCS 功能。	请参见第 44 页的“关于神州云科HDP 6100备份一体机上的 Symantec Data Center Security”。
关于神州云科HDP 6100备份一体机入侵防护系统	此部分描述用于保护设备的 IPS 策略。	请参见第 46 页的“关于神州云科HDP 6100备份一体机入侵防护系统”。
关于神州云科HDP 6100备份一体机入侵检测系统	此部分描述用于监视设备的 IDS 策略。	请参见第 47 页的“关于神州云科HDP 6100备份一体机入侵检测系统”。
查看神州云科HDP 6100备份一体机上的SDCS 事件	此部分根据安全级别描述相应的 SDCS 事件。	请参见第 48 页的“查看神州云科HDP 6100备份一体机上的 SDCS 事件”。
在神州云科HDP 6100备份一体机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 50 页的“在神州云科HDP 6100备份一体机上以非受控模式运行SDCS”。
在神州云科HDP 6100备份一体机上以受控模式运行 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 50 页的“在神州云科HDP 6100备份一体机上以受控模式运行 SDCS”。

神州云科HDP 6100备份一体机日志文件

本章列出神州云科HDP 6100备份一体机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	本章概述了神州云科HDP 6100备份一体机中所有可查看的不同日志类型。	请参见第 52 页的“关于神州云科HDP 6100备份一体机日志文件”。
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 54 页的“使用Support 命令查看日志文件”。
使用 Browse 命令查找神州云科HDP 6100备份一体机日志文件	本章描述使用 Browse 命令查看日志文件。	请参见第 55 页的“可使用Browse 命令从何处查找神州云科HDP 6100备份一体机日志文件”。
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 56 页的“收集神州云科HDP 6100备份一体机上的设备日志”。

神州云科HDP 6100备份一体机操作系统安全

表 1-5 操作系统部分

部分名称	描述	链接
关于神州云科HDP 6100备份一体机操作系统安全	此部分描述用于提高神州云科HDP 6100备份一体机整体安全而对操作系统所做的不同更新类型。	请参见第 60 页的“关于神州云科HDP 6100备份一体机操作系统安全”。
神州云科HDP 6100备份一体机操作系统中包含的主要组件	此部分列出神州云科HDP 6100备份一体机的产品和操作系统组件。	请参见第 61 页的“神州云科HDP 6100备份一体机操作系统中包含的主要组件”。
神州云科HDP 6100备份一体机漏洞扫描	此部分列出 神州云科用于验证设备安全的一些安全扫描程序。	

神州云科HDP 6100备份一体机数据安全

本章描述神州云科HDP 6100备份一体机的数据安全实施，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 65 页的“关于数据安全”。

部分名称	描述	链接
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 66 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 67 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 67 页的“关于数据加密 ”。

神州云科HDP 6100备份一体机Web 安全

本章描述神州云科HDP 6100备份一体机的 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	此部分列出神州云科HDP 6100备份一体机网页操作界面的 SSL 认证更新。	请参见第 72 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 73 页的“关于实施 ECA 证书”。

神州云科HDP 6100备份一体机网络安全

本章描述神州云科HDP 6100备份一体机的网络安全实施，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	此部分描述神州云科HDP 6100备份一体机的 IPsec 配置。	请参见第 78 页的“关于 IPsec 通道配置”。
关于神州云科HDP 6100备份一体机端口	此部分描述神州云科HDP 6100备份一体机的端口信息。	请参见第 79 页的“关于神州云科HDP 6100备份一体机端口”。

神州云科HDP 6100备份一体机自动通报安全

本章描述神州云科HDP 6100备份一体机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	此部分描述神州云科HDP 6100备份一体机中的 AutoSupport 功能。	请参见第 83 页的“关于 AutoSupport ”。

部分名称	描述	链接
关于自动通报	此部分描述神州云科HDP 6100备份一体机中的自动通报功能。	请参见第 84 页的“关于自动通报”。
关于 SNMP	此部分描述神州云科HDP 6100备份一体机中的 SNMP 功能。	请参见第 88 页的“关于 SNMP”。

神州云科HDP 6100备份一体机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 以及如何与神州云科HDP 6100备份一体机一同配置。	请参见第 90 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 90 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神州云科HDP 6100备份一体机的 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：

关于神州云科HDP 6100备份一体机上的用户身份验证

通过用户帐户对神州云科HDP 6100备份一体机进行管理。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描述了设备上可用的用户帐户。

表 2-1 神州云科HDP 6100备份一体机帐户类型

帐户名称	描述
admin	**admin** 帐户是神州云科HDP 6100备份一体机上的默认管理员用户。此帐户提供默认管理员用户的完全 Appliance 访问和控制权限。 以下默认登录凭据与新 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：只有本地 **admin** 帐户有权装入或映射 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： ▪ Appliance Management Console ▪ 神州云科HDP 6100备份一体机网页操作界面 ▪ 神州云科HDP 6100备份一体机命令行操作界面 ▪ 备份系统管理控制台
maintenance	**maintenance** 帐户通过神州云科HDP 6100备份一体机命令行操作界面使用（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。

帐户名称	描述
nbasecadmin	**nbasecadmin** 帐户由安全管理员用户用于在备份软件中进行基于角色的访问控制 (RBAC) 以及管理备份和还原操作。当对设备主服务器执行初始配置或升级设备主服务器时，将自动创建此用户。 创建后，将为此帐户分配默认设备密码。当此用户首次登录神州云科HDP 6100备份一体机命令行操作界面时，系统会提示更改该帐户的默认密码。 注意：在更改默认密码之前，此用户无法登录备份软件Web UI。 更改默认密码后，默认情况下，nbasecadmin 用户可以拥有以下访问权限和特权： ▪ 备份软件Web UI 对备份软件Web UI 的访问权限允许此用户为其他备份软件用户设置用户角色、管理所有备份软件安全设置以及执行备份和还原操作。 **nbasecadmin** 用户还可以将备份软件角色分配给设备上的本地用户，也可以分配给 LDAP 服务器或 Active Directory (AD) 服务器上注册的用户。请参见第 42 页的“关于备份软件中的用户授权”。 注意：从软件版本 3.2 开始，您可以为 **nbasecadmin** 用户分配备份和还原权限。如果从早期版本升级，则必须手动为 **nbasecadmin** 用户帐户添加备份和还原权限。有关详细信息，请参见《备份软件Web UI 安全管理指南》。 ▪ 神州云科HDP 6100备份一体机命令行操作界面 登录神州云科HDP 6100备份一体机命令行操作界面来更改该帐户的密码。只能访问 Main > Settings > Password 视图。 此视图对 nbasecadmin 用户以及设备上未分配任何角色的所有设备本地用户可见。当 nbasecadmin 用户登录命令行操作界面时，仅以下菜单项可用： 退出 密码 **nbasecadmin** 用户的访问规则也可以更改为允许更多权限。要访问备份软件Web UI，此用户可以打开浏览器窗口并输入以下 URL：https:<*appliance primary serverhost name*>/webui。 有关 RBAC 和备份软件用户角色管理的更多信息，请参见备份软件*Web UI Security Administrator's Guide*（《备份软件Web UI 安全管理指南》）。

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神州云科HDP 6100备份一体机网页操作界面或神州云科HDP 6100备份一体机命令行操作界面进行访问。

表 2-2 神州云科HDP 6100备份一体机内部帐户类型

帐户名称	描述
sisips	sisips 帐户是一个内部用户，用于实施 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 神州云科支持访问以用于执行维护任务。如果您尝试访问此帐户，则会显示以下消息： Permission Denied !! Access to the root accountrequires overriding the Intrusion Security Policy.
nbcopilotxxxx	支持从主服务器访问介质服务器时进行身份验证。
nbwebsvc	不支持身份验证。

请参见第 36 页的“关于授权神州云科HDP 6100备份一体机用户”。

可在神州云科HDP 6100备份一体机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 描述可添加到神州云科HDP 6100备份一体机的用户的类型。

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 神州云科HDP 6100备份一体机用户类型

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。	▪ 您可以使用神州云科HDP 6100备份一体机网页操作界面的“设置”>“身份验证”>“用户管理”页面添加、删除和管理本地用户。 ▪ 您可以使用神州云科HDP 6100备份一体机命令行操作界面的 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、备份软件命令行角色或 AMSadmin 角色。 注意：无法为现有的本地用户授予备份软件命令行角色。但是，您可以从神州云科HDP 6100备份一体机命令行操作界面使用 Manage >备份软件命令行 > Create 命令创建本地备份软件命令行用户。
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 22 页的“关于对 LDAP 用户进行身份验证”。	▪ 您可以使用神州云科HDP 6100备份一体机网页操作界面的“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。 ▪ 您可以使用神州云科HDP 6100备份一体机命令行操作界 面的 Settings > Security > Authentication > LDAP 命令添加和删除 LDAP 用户和用户组。 ▪ 您可以将管理员或备份软件命令行角色分配给 LDAP 用户或用户组。 注意：在任何给定时间最多可将备 份 软 件命令行 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 23 页的“关于对 Active Directory 用户进行身份验证”。	▪ 您可以使用神州云科HDP 6100备份一体机网页操作界面的“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。 ▪ 您可以使用神州云科HDP 6100备份一体机命令行操作界 面的 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备份软件命令行角色分配给 AD 用户或用户组。 注意：在任何给定时间最多可将备 份 软 件命令行 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 23 页的“关于对 Kerberos-NIS 用户进行身份验证”。	▪ 您可以使用神州云科HDP 6100备份一体机网页操作界面的“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。 ▪ 您可以使用神州云科HDP 6100备份一体机命令行操作界面的 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备份软件命令行角色分配给 NIS 用户或用户组。 注意：在任何给定时间最多可将备 份 软 件 命令行 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《神州云科HDP 6100备份一体机管理指南》。

关于配置用户身份验证

表 2-4 描述了神州云科HDP 6100备份一体机网页操作界面和神州云科HDP 6100备份一体机命令行操作界面中提供的选项，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	**神州云科HDP 6100备份一体机**网页操作界面	**神州云科HDP 6100备份一体机**命令行操作界面
本地（本机用户）	使用神州云科HDP 6100备份一体机网页操作界面中 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 36 页的“关于授权HDP 6100备份一体机用户”。	在 Settings > Security > Authentication > LocalUser 下可使用以下命令和选项： ▪ 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	**神州云科HDP 6100备份一体机**网页操作界面	**神州云科HDP 6100备份一体机**命令行操作界面
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。 使用神州云科HDP 6100备份一体机网页操作界面中的“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 36 页的“关于授权HDP 6100 备份一体机用户”。	在 Settings > Security > Authentication > LDAP 下可使用以下命令和选项： ▪ 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 用户注册到设备并进行身份验证。* ▪ 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 - 将现有 LDAP 配置导出为 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。

用户类型	**神州云科HDP 6100备份一体机**网页操作界面	**神州云科HDP 6100备份一体机**命令行操作界面
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。 使用神州云科HDP 6100备份一体机网页操作界面中 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 36 页的“关于授权HDP 6100 备份一体机用户”。	在 Settings > Security > Authentication > ActiveDirectory 下可使用以下命令和选项： ▪ Configure - 配置设备以允许 AD 用户注册到设备并进行身份验证。 ▪ 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。
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。 使用神州云科HDP 6100备份一体机网页操作界面中 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 36 页的“关于授权HDP 6100 备份一体机用户”。	在 Settings > Security > Authentication > Kerberos 下可使用以下命令和选项： ▪ Configure - 配置设备以允许 NIS 用户注册到设备并进行身份验证。 ▪ 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。

用户类型	**神州云科HDP 6100备份一体机**网页操作界面	**神州云科HDP 6100备份一体机**命令行操作界面
智能卡身份验证	可以使用智能卡启用身份验证。 ▪ 以备份软件CLI 用户身份运行 vssat addldapdomain 命令。 请参见第 24 页的“关于使用智能卡和数字证书进行身份验证”。	可以使用智能卡启用身份验证。 ▪ 在 Settings > Security > Authentication > LDAP 下使用OpenLDAP 或 ActiveDirectory 配置远程身份验证 ▪ 在 Settings > Security > Certificate AddCACertificate 下添加 CA 证书。 ▪ 在 Network > DNS Add Nameserver 下配置 DNS 以解析 OCSP URI。 ▪ 在 Settings > Security > Authentication > SmartCard 下配置并启用智能卡身份验证。

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备份软件命令行角色分配给九 (9) 个用户组。
- 无法为现有的本地用户授予备份软件命令行角色。但是，您可以从神州云科HDP 6100备份一体机命令行操作界面使用 Manage >备份软件命令行> Create 命令创建本地备份软件命令行用户。
- 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备份软件命令行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。神州云科建议仅为设备用户保留 1000 至 1999 范围内的用户 ID 和组 ID。
- 神州云科HDP 6100备份一体机将常规 CIFS 共享用于一些内部操作，例如存储修补程序和安装文件、将日志上传到支持部门、将日志转发到外部服务器以及上传 OST 插件。
  从设备软件版本 4.0 开始，对于所有本地用户和 Active Directory 用户和用户组（**admin** 用户除外），您必须管理对常规 CIFS 共享的访问权限。使用 Settings > Security > Authentication > CIFSShare 命令管理对常规 CIFS 共享的访问权限。

- 来宾用户：通过创建新的本地用户来替换来宾用户。
- 现有本地用户：更改这些用户的密码。

请参见第 13 页的“关于神州云科HDP 6100备份一体机上的用户身份验证 ”。

关于对 LDAP 用户进行身份验证

神州云科HDP 6100备份一体机使用内置的可插入身份验证模块 (PAM) 插件以支持对轻型目录访问协议 (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 神州云科HDP 6100备份一体机。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：

- LDAP 架构必须符合 RFC 2307 或 RFC 2307bis。
- 必须在 Active Directory 服务器上启用 UNIX 模式。
- 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备份软件命令行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。神州云科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：

- 神州云科HDP 6100备份一体机网页操作界面中的 **Settings > Authentication > LDAP**。
- 从神州云科HDP 6100备份一体机命令行操作界面中执行 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《神州云科HDP 6100备份一体机管理指南》和《神州云科HDP 6100备份一体机命令参考指南》。

关于对 Active Directory 用户进行身份验证

神州云科HDP 6100备份一体机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 神州云科HDP 6100备份一体机。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：

- 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备份软件命令行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：

- 神州云科HDP 6100备份一体机网页操作界面中的“设置”>“身份验证”> **Active Directory** 页面。
- 从神州云科HDP 6100备份一体机命令行操作界面中执行 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《神州云科HDP 6100备份一体机管理指南》和《神州云科HDP 6100备份一体机命令参考指南》。

关于对 Kerberos-NIS 用户进行身份验证

神州云科HDP 6100备份一体机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 神州云科HDP 6100备份一体机。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：

- 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。神州云科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备份软件命令行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：

- 神州云科HDP 6100备份一体机网页操作界面中的“设置”>“身份验证”>

  Kerberos-NIS页面。
- 从神州云科HDP 6100备份一体机命令行操作界面中执行 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《神州云科HDP 6100备份一体机管理指南》和《神州云科HDP 6100备份一体机命令参考指南》。

关于使用智能卡和数字证书进行身份验证

2FA

从 Appliance 版本 3.2 开始，备份软件支持使用备份软件Web UI 的 Active Directory (AD) 或轻型目录访问协议 (LDAP) 域用户进行双重身份验证 (2FA)。

从 Appliance 版本 5.0 开始，神州云科HDP 6100备份一体机支持使用神州云科HDP 6100备份一体机Web UI 的轻型目录访问协议 (LDAP) 域用户进行双重身份验证 (2FA)。

备份软件Web UI 的 2FA

- **nbasecadmin** 用户或任何具有备份软件管理员角色的用户都可以为备份软件Web UI 配置 2FA。
- 即使已在设备上配置 AD 或 LDAP，2FA 配置也要求为备份软件单独配置 AD 或 LDAP。

神州云科HDP 6100备份一体机Web UI 的 2FA

任何具有神州云科HDP 6100备份一体机管理员角色的用户都可以为神州云科HDP 6100 备份一体机Web UI 配置 2FA。2FA 配置要求在设备上配置 LDAP（目录类型为 OpenLDAP 或ActiveDirectory）。

有关如何为 Appliance Web UI 配置、启用或禁用 2FA 的详细信息，请参见以下主题：

请参见第 24 页的“关于使用智能卡和数字证书进行身份验证”。

适用于备份软件Web UI 的智能卡身份验证

备份软件Web UI 支持 Active Directory (AD) 或轻型目录访问协议 (LDAP) 域用户使用数字证书或智能卡（包括 CAC 和 PIV）进行身份验证。此身份验证方法仅支持每个设备主服务器域一个 AD 或 LDAP 域，并且不可用于本地域用户。

注意：应为要使用此身份验证方法的每个设备主服务器域单独执行此配置。

确保在为域用户添加访问规则或配置域以进行智能卡身份验证之前，添加AD或 LDAP 域。使用 vssat 命令添加 AD 或 LDAP 域。

为备份软件添加 AD 或 LDAP 域

1. 以备份软件命令行用户身份登录设备主服务器。
2. 运行 vssat 命令。

   vssat addldapdomain -d *DomainName* -s *server_URL* -u *user_base_DN* -g *group_base_DN* -t *schema_type* -m *admin_user_DN*

   按照以下说明替换上述命令中的变量：

   - *DomainName* 是唯一标识 LDAP 域的符号名称。
   - *server_URL* 是给定域的 LDAP 目录服务器的 URL。LDAP 服务器 URL 必须以 ldap:// 或 ldaps:// 开头。以 ldaps:// 开头表示给定的 LDAP 服务器需要 SSL 连接。例如，ldaps://my-server.myorg.com:636。
   - *user_base_DN* 是 user 容器的 LDAP 可分辨名称。例如，ou=user,dc=mydomain,dc=myenterprise,dc=com。

- *group_base_DN* 是 group 容器的 LDAP 可分辨名称。例如，ou=group,dc=mydomain,dc=myenterprise,dc=com。
- *schema_type* 指定要使用的 LDAP 架构的类型。支持的两个默认架构类型为 rfc2307 或 msad。
- *admin_user_DN*是一个字符串，包含以下用户的 DN：管理用户、具有 user 容器搜索权限的任何用户或 UserBaseDN指定的用户子树。如果包括匿名用户在内的任何用户均可搜索 user 容器，则您可以将此选项配置为空字符串。例如，--admin_user=。此配置允许任何人搜索 user 容器。

3 使用 vssat validateprpl 验证是否已成功添加指定的 AD 或 LDAP 域。请注意，您还可以在 vssat 命令中使用以下选项：

- vssat removeldapdomain，用于从身份验证代理中删除 LDAP 域。
- vssat validategroup，用于检查提供的域中是否存在用户组。
- vssat validateprpl，用于检查提供的域中是否存在用户。

有关 vssat命令的更多详细信息，请参见《神州云科备份软件命令参考指南》

适用于神州云科HDP 6100备份一体机Web UI 的智能卡身份验证

为 Appliance Web UI 执行身份验证之前，请确保执行以下三个步骤。

注意：可以按任意顺序执行这些步骤。

1. 使用 OpenLDAP 或 ActiveDirectory 目录类型配置 LDAP 身份验证。

   Settings > Security > Authentication > LDAP

2. 为将要通过设备进行身份验证的 LDAP 用户添加并授予角色。

   Settings > Security > Authentication > LDAP > Users Add

   Settings > Security > Authorization > Grant

3. 将 CA 链中的所有证书添加到设备。无需添加卡上的中间证书。

Settings > Security > Certificates > AddCACertificate

使用“智能卡”命令菜单，可以配置和显示与 Appliance Web UI 智能卡身份验证相关的参数。您还可以启用或禁用此功能。

Settings > Security > Authentication > SmartCard

表 2-5 智能卡菜单命令

命令	描述
Configure MappingAttribute	Configure 命令可配置设备智能卡身份验证。它具有一个必需配置参数和一个可选配置参数。 MappingAttribute 参数指定是使用智能卡上证书的通用名称 (CN) 还是用户主体名称(UPN) 对用户进行身份验证并确定该用户的角色。输入 CN 或 UPN。这是必需参数。 如果证书中的 CN 与远程数据库、OpenLDAP 或 ActiveDirectory 中的用户记录的 CN 字段匹配，则可以使用 CN。如果证书中的 UPN 与 OpenLDAP 或 ActiveDirectory 中的用户记录的 UPN 字段匹配，则可以使用 UPN。配置 LDAP 后，directoryType 被指定为 OpenLDAP 或 ActiveDirectory。
Configure OCSPURI	OCSPURI 参数（在线证书状态协议）确定智能卡上的证书是否已吊销。这是可选参数。如果证书未吊销，此参数将覆盖证书中的 OCSP URI。URI 是 FQDN 或 IPv4 地址。OCSP URI 不支持 IPv6 地址。 注意：如果使用智能卡进行身份验证失败（即使已执行所有必要步骤），请使用 **SmartCard > Show** 命令并验证参数（包括 OCSP URI，如果存在）是否正确。通过导航到 **Network > DNS Show**，验证是否在“网络”菜单中配置了能够解析 OCSP URI 的名称服务器
Disable	禁用智能卡身份验证。
Enable	启用智能卡身份验证。仅当配置了 LDAP、添加了 CA 证书并配置了智能卡身份验证后，才能启用智能卡身份验证。
Show	显示一个表格，其中显示是否已启用智能卡身份验证、选定的映射属性和 OCSP URI（如果已输入）。

配置基于角色的访问控制

为备份软件添加 AD 和 LDAP 域后，可以使用 nbasecadmin 用户登录到备份软件Web UI，并为备份软件Web UI 配置基于角色的访问控制。有关为神州云科HDP 6100备份一体机用户配置 RBAC 的更多信息，请参见《备份软件Web UI 安全管理指南》。

为备份软件Web UI 配置使用智能卡或数字证书进行身份验证

您可以使用 nbasecadmin 用户登录到备份软件Web UI，并配置使用智能卡或数字证书进行身份验证。有关执行配置所需的以下过程的步骤，请参考《备份软件Web UI 安全管理指南》：

- 配置备份软件Web UI 以使用智能卡或数字证书对用户进行身份验证。
- 编辑智能卡身份验证的配置。
- 添加用于智能卡身份验证的 CA 证书。
- 删除用于智能卡身份验证的 CA 证书。

关于设备登录提示

通过 神州云科HDP 6100备份一体机，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。

备份软件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，备份软件不会使用提示。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备份软件，以便每当用户尝试登录到备份软件管理控制台时都会显示该横幅。

表 2-6 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（例如神州云科HDP 6100备份一体机命令行操作界面和 SSH）都将显示该提示。但是，可以选择为备份软件管理控制台打开或关闭登录提示。

表 2-6 支持登录提示的设备接口

接口	说明
神州云科HDP 6100备份一体机命令行操作界面	用户尝试登录神州云科HDP 6100备份一体机命令行操作界面之前，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。

接口	说明
神州云科HDP 6100备份一体机网页操作界面	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。
备份软件管理控制台（可选）	每当用户尝试使用备份软件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，该提示功能属于备份软件。

使用神州云科HDP 6100备份一体机命令行操作界面中的 Settings > Notifications > LoginBanner 配置登录提示。有关更多信息，请参考《神州云科HDP 6100备份一体机命令参考指南》。

或者，在神州云科HDP 6100备份一体机网页操作界面中通过路径“设置”>“通知”>“登录提示”配置登录提示。有关详细信息，请参考《神州云科HDP 6100备份一体机管理指南》。

关于用户名和密码规范

神州云科HDP 6100备份一体机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 2-7列出了每个用户类型的用户名规范。

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

表 2-7 用户名规范

描述	管理员（本地用户）	**备份软件命令行**（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

描述	管理员（本地用户）	**备份软件命令行**（本地用户）	注册的远程用户
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

神州云科HDP 6100备份一体机密码策略已更新，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 2-8列出了每个用户类型的密码规范。

表 2-8 密码规范

描述	管理员（本地用户）	**备份软件命令行**（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）	**备份软件命令行**（本地用户）	注册的远程用户
最小密码期限	0 天	0 天 注意：您可以通过神州云科HDP 6100备份一体机命令行操作界面使用Settings > Security > Authentication > LocalUser 命令管理用户的密码期限。 有关更多信息，请参考《神州云科HDP 6100备份一体机 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
密码过期	不适用，因为密码不过期	使用 Settings > Security > Authentication > LocalUser 命令管理备份软件命令行用户密码。	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

警告：设备不支持 Maintenance 帐户密码，如 passwd。系统升级后，这些类型的密码将被重写。使用神州云科HDP 6100备份一体机命令行操作界面更改 Maintenance 帐户密码。

密码保护

神州云科HDP 6100备份一体机采用了以下密码保护措施：

- 客户可访问的所有本地设备用户（本地用户、备份软件命令行用户、管理员用户和Maintenance 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：如果从低于 2.6.1.1 的神州云科HDP 6100备份一体机软件版本升级，神州云科建议在升级后，最终更改所有本地设备用户的密码，以便他们可以使用最新的默认 SHA-512 哈希算法。

- 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 通信保护的神州云科HDP 6100备份一体机网页操作界面登

录。有关详细的密码说明，请参考《神州云科HDP 6100备份一体机管理指

南》。

关于符合 STIG 规范的密码策略规则

启用 STIG 选项时，备份软件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实施指南 (STIG)。

启用 STIG 选项后，在默认策略下创建的所有当前用户密码仍有效。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

注意：界面上显示的密码策略未翻译为其他语言。在日语和中文界面上，密码策略以英语显示。

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，请使用 Settings > Security > Authentication > AccountStatus > UnlockAccounts 命令。

启用了 STIG 的设备上的 maintenance 帐户密码更改

从 Appliance 版本 3.1.2 开始，在以下情况下，STIG 密码期限策略会将 maintenance 帐户密码更改延迟一段时间：

- 在启用 STIG 选项后，延迟 24 小时。
- 在将启用了 STIG 的设备升级到 3.1.2 或更高版本后，延迟 24 小时。

在发生其中任一事件的 24 小时内，尝试更改 maintenance 帐户密码的所有操作都会失败。要在发生这些事件后更改 maintenance 帐户密码，请确保至少等待 24 小时。

请参见第 99 页的“神州云科HDP 6100备份一体机的操作系统 STIG 加固”。

3

用户授权

本章节包括下列主题：

关于神州云科HDP 6100备份一体机的用户授权

通过用户帐户对神州云科HDP 6100备份一体机进行管理。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　　神州云科HDP 6100备份一体机用户角色

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神州云科HDP 6100备份一体机的管理权限。管理员用户能够登录、查看和在神州云科HDP 6100备份一体机网页操作界面与神州云科HDP 6100备份一体机命令行操作界面上执行所有功能。这些用户帐户有权登录到设备，并以超级用户权限运行备份软件命令。 请参见第 38 页的“关于管理员用户角色”。

角色	描述
备份软件命令行	分配了备份软件命令行角色的用户帐户只能运行有限的一组备份软件CLI 命令，并且对备份软件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备份软件。 备份软件命令行用户没有神州云科HDP 6100备份一体机网页操作界面和神州云科HDP 6100备份一体机命令行操作界面的访问权限。 请参见第 39 页的“关于备份软件命令行用户角色”。
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 的神州云科HDP 6100备份一体机命令行操作界面。管理员可以创建 AMSadmin 用户。

以下列表介绍了神州云科HDP 6100备份一体机授权的一些特性：

- 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备 份 软 件 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 的神州云科HDP 6100备份一体机网页操作界面 对神州云科HDP 6100备份一体机命令行操作界面进行网络访问。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，神州云科HDP 6100备份一体机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 32 页的“关于符合 STIG 规范的密码策略规则”。

注意：从神州云科HDP 6100备份一体机版本 3.1.2 开始，已从 VxOS 中删除 telnet 软件 包，以便在神州云科HDP 6100备份一体机上启用了 STIG 功能时符合 STIG 规范。APPSOL-80036 and APPSOL89038, Jay Vasa - Sangria Teamtelnet协议不安全或未加密。使用未加密的传输介质可能会允许未经授权的用户窃取凭据。ssh 软件包提供加密会话和更高的安全性，且包含在 VxOS 中。

关于授权神州云科HDP 6100备份一体机用户

表 3-2 描述了为通过神州云科HDP 6100备份一体机网页操作界面和 神州云科HDP 6100备份一体机
命令行操作界面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	**神州云科HDP 6100备份一体机** 网页操作界面	**神州云科HDP 6100备份一体机** 命令行操作界面
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 18 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备份软件命令行角色。 ▪ 将已注册用户组的成员与管理员角色同步。	在 Main > Settings > Security > Authorization 下可使用以下命令和选项： ▪ Grant 为已添加到设备的特定用户和用户组授予管理员和备份软件命令行角色。 ▪ List 列出已添加到设备中的所有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备份软件命令行角色。 ▪ 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备份软件命令行角色。但是，您可以从神州云科HDP 6100备份一体机命令行操作界面使用 Manage >备份软件命令行> Create 命令创建本地备份软件命令行用户。
- 在任何给定时间最多可将备 份 软 件 命令行角色分配给九个用户组。

- Active Directory (AD) 用户组和用户名称支持在这些名称中使用连字符。连字符必须出现在用户名或用户组名的第一个字符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。
- 可以从神州云科HDP 6100备份一体机网页操作界面列出具有最多 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，请使用神州云科HDP 6100备份一体机命令行操作界面中的 List 命令。

神州云科HDP 6100备份一体机用户角色权限

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
备份软件命令行	用户只能访问备份软件CLI。 请参见第 39 页的“关于备份软件命令行用户角色”。
管理员	用户可以访问以下内容： ▪ 神州云科HDP 6100备份一体机网页操作界面 ▪ 神州云科HDP 6100备份一体机命令行操作界面 ▪ 备份软件管理控制台 请参见第 38 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 Appliance Management Console。AMS 用户可在 Appliance Management Console 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 的神州云科HDP6100备份一体机命令行操作界面。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，也可以授予备 份 软 件 命令行用户访问神州云科HDP 6100备份一体机命令行操作界面的权限：

- 具有备 份 软 件 命令行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备 份 软 件 命令行角色的组中。

注意：授予用户备份软件命令行和神州云科HDP 6100备份一体机命令行操作界面的权限时，需要一个额外步骤。用户必须从备份软件CLI 输入 switch2admin 命令才能访问神州云科HDP 6100备份一体机命令行操作界面。

授予用户和用户组权限的方法如下：

- 在神州云科HDP 6100备份一体机网页操作界面的“设置”>“身份验证”>“用户管理”页面上，单击“授予权限”链接。
- 从神州云科HDP 6100备份一体机命令行操作界面，在 Settings > Security > Authorization 视图中使用以下命令：

  Grant Administrator GroupGrant

  Administrator UsersGrant备份软

  件命令行Group Grant备份软件命

  令行Users Grant AMS Group

  Grant AMS Users

请参见第 18 页的“关于配置用户身份验证”。

请参见第 36 页的“关于授权神州云科HDP 6100备份一体机用户”。

关于管理员用户角色

神州云科HDP 6100备份一体机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 神州云科HDP 6100备份一体机。

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 使用神州云科HDP 6100备份一体机命令行操作界面或通过 HTTPS 使用神州云科HDP 6100备份一体机网页操作界面来访问设备。

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。

- 本地用户以及分配有管理员角色的 LDAP 或 Active Directory (AD) 用户和用户组可以访问备份软件Java 控制台。

关于备份软件命令行用户角色

备份软件命令行用户可以执行所有备份软件命令、查看日志、编辑备份软件touch 文件以及编辑备份软件通知脚本。备份软件命令行用户的唯一限制是必须使用超级用户权限运行备份软件命令并且在备份软件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备份软件命令的受限 shell。
备份软件命令行用户共享一个主目录，并且没有神州云科HDP 6100备份一体机网页操作界面或神州云科HDP 6100备份一体机命令行操作界面的访问权限。

从设备版本 5.0 开始，备份软件命令行用户只能以超级用户身份运行某些命令，并且需要遵循备份软件CLI 授权机制来对此类命令进行身份验证以及运行此类命令。有关各种备份软件命令和命令参数所需的确切权限的更多信息，请参考《备份软件命令参考指南》。

在任何给定时间最多可将备 份 软 件 命令行 角色分配给九个用户组。要创建本地备份软件命令行用户，请从神州云科HDP 6100备份一体机命令行操作界面使用 Manage > 备份软件命令行> Create命令。有关详细信息，请参见《神州云科HDP 6100备份一体机命令参考指南》。

注意：无法为现有的本地用户授予备份软件命令行角色。

表 3-4列出了备份软件命令行用户的权限和限制。

表 3-4 设备备份软件命令行用户的权限和限制

权限	限制
备份软件命令行用户可以使用神州云科HDP 6100备份一体机命令行操作界面执行以下操作： ▪ 运行备份软件CLI 并访问备份软件目录和文件。 ▪ 使用 cp-nbu-notify 命令修改或创建备份软件通知脚本。 ▪ 对包含备份软件CLI 的以下目录运行以下命令： ▪ /opt/VRTSpbx/bin/* ▪ /opt/VRTS/bin/* ▪ /usr/openv/db/bin/* ▪ /usr/openv/mqbroker/bin/goodies/* ▪ /usr/openv/mqbroker/bin/install/* ▪ /usr/openv/netbackup/bin/* ▪ /usr/openv/netbackup/bin/admincmd/* ▪ /usr/openv/netbackup/bin/goodies/* ▪ /usr/openv/netbackup/bin/goodies/support/* ▪ /usr/openv/netbackup/bin/support/* ▪ /usr/openv/pdde/pdcr/bin/* ▪ /usr/openv/pdde/vpfs/bin/* ▪ /usr/openv/volmgr/bin/* ▪ /usr/openv/volmgr/bin/goodies/* ▪ /usr/openv/pdde/pdcr/bin/crcontrol ▪ /usr/openv/pdde/pdag/bin/mtstrmd ▪ /usr/openv/pdde/pdag/bin/pdcfg ▪ /usr/openv/pdde/pdag/bin/pdusercfg ▪ /usr/openv/pdde/pdconfigure/pdde	以下限制将加在备份软件命令行用户上： ▪ 备份软件命令行用户对备份软件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 目录中创建和编辑备份软件touch 配置文件。 ▪ 无法使用 man或-h命令查看任何其他命令的帮助。 ▪ 不能使用绝对路径执行任何命令。所有命令必须仅使用短名称执行。 ▪ 无法运行大多数系统命令，只有少数只读系统命令除外，例如在只读模式下工作的 cat、date、whoami、ls、which、grep、sort、cut、jq和vi 命令。

如何以备份软件**命令行**用户身份运行备份软件命令

以备份软件命令行用户身份登录，并在命令提示符处键入 Command以进入受限 Shell 环境。然后，可以从该 Shell 运行备份软件命令。不允许使用绝对路径运行备份软件命令。例如，您可以运行 bplist，但无法从命令 Shell 运行 /usr/openv/netbackup/bin/admincmd/bpplist。

可能需要额外的授权才能运行某些备份软件命令。您将看到不同的授权提示，具体取决于您尝试运行的备份软件命令。

以下列表介绍了成功执行备份软件命令的典型情况：

▪ 授权提示：需要 **Web** 登录
某些备份软件命令可能需要 Web 登录。您将看到以下提示：

A web login is required. Run the 'bpnbat -login -loginType WEB|WEBUI|APIKEY' command to login. EXIT STATUS 5930: The requestcould not be authorized.

要对此类请求进行身份验证，必须以备份软件管理员身份登录备份软件Web 管理服务并运行以下命令：

myappliance.NBCLIUSER> bpnbat -login -logintype WEB

下面显示了一个示例 WEB 登录：

Authentication Broker: *ApplianceHostname*

Authentication Port: 0

Authentication Type: unixpwd

LoginName: *Username* Password:

Password

Operation completed successfully.

- 授权提示：需要 **Web UI** 登录

  某些备份软件命令可能需要使用访问令牌进行批准。要对此类请求进行身份验证，请通过运行以下命令生成访问代码：

  # bpnbat -login -logintype webui -requestApproval

  记下命令窗口中显示的访问代码。

  以备份软件命令行 (CLI) 管理员用户身份登录备份软件Web UI，并通过输入先前生成的访问代码来批准 CLI 访问请求。有关访问密钥和批准请求的更多信息，请参考《备份软件安全和加密指南》。

- 授权提示：需要超级用户权限

  某些备 份 软 件 命令可能需要超级用户权限。您将看到以下提示：

  EXIT STATUS 140: user id was not superuser

  要对此类请求进行身份验证，请使用 sudo 提升权限并使用绝对路径运行备份软件命令。例如：

  # sudo /usr/openv/netbackup/bin/nbkmscmd -discoverNbkms

  如果在使用了绝对路径和sudo之后，身份验证消息仍然存在，可以使用前面介绍的 WEB 登录方法并运行以下命令对请求进行身份验证：

  # sudo /usr/openv/netbackup/bin/bpnbat -login -loginType WEB

常规注意事项：

- 前面介绍的身份验证案例是典型情况。某些备份软件命令可能需要其他身份验证方法。有关各种备份软件命令和命令参数所需的确切权限的更多信息，请参考《备份软件命令参考指南》。
- 默认情况下，某些备份软件命令以 root 身份运行。通过运行以下命令，可以验证特定命令是否需要 root 权限：

  nbucliuser-!> alias | grep备份软件*command*

  例如，默认情况下，nbkms 命令以 root 身份运行：

```
nbucliuser-!> alias | grep nbkms
alias nbkms='sudo -n /usr/openv/netbackup/bin/nbkms'
```

- 默认情况下，某些备份软件命令由当前备份软件命令行用户运行。但是，有些备份软件命令参数需要 root 权限。在这种情况下，可以使用“sudo <absolute path of command> <parameters>”运行命令。

  如果您看到提示“sudo: 需要密码”，则表示该命令不能以 root 身份运行。此类情况下，请联系神州云科技术支持获取帮助。

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备份软件列表或路径中，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。

需以备份软件命令行用户身份运行备份软件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 路径添加到备份软件bpcd allowed list。
- 将特殊指令命令添加到 /home/nbusers 目录。

关于备份软件中的用户授权

可以使用 **nbasecadmin** 帐户登录备份软件Web UI 并将备份软件角色分配给设备上的本地用户，也可以分配给 LDAP 服务器或 Active Directory (AD) 服务器上注册的用户。通过备份软件基于角色的访问控制(RBAC) 中分配的角色，设备用户可以在备份软件中执行特定任务，同时限制对非基本资产和功能的访问权限。有关 RBAC 和备份软件用户角色管理的更多信息，请参见备份软件*Web UI Security Administrator’s Guide*（《备份软件Web UI 安全管理指南》）。

如果要升级在版本 3.1.2 或 3.2 上运行的设备，则升级后，将撤销备份软件RBAC 定义的所有非管理角色。必须使用备份软件中引入的新 RBAC 模型重新配置现有 RBAC 配置。

可以使用 RBAC 迁移工具将现有的备份管理员和安全管理员角色迁移到备份软件 RBAC 模型。RBAC 迁移工具执行以下操作：

- 迁移现有安全管理员角色及其添加的主体。
- 删除现有的备份管理员角色，并将其用户重新分配给管理员角色。

在升级后，必须重新配置当前配置的任何工作负载管理员角色和自定义角色。可以使用备份软件RBAC 角色实用程序添加最新角色定义。

4

入侵防护和入侵检测系统

本章节包括下列主题：

关于神州云科HDP 6100备份一体机上的 Symantec Data Center Security

注意：升级后，设备 SDCS 代理会自动设置为非受控模式。如果升级前某个设备在受控模式中运行，请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。升级后，不能使用之前的旧版策略来管理运行更高软件版本的设备。新策略可从神州云科HDP 6100备份一体机网页操作界面的“监视”>“SDCS 事件”页面中下载。另外请注意，升级后，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

自定义的神州云科HDP 6100备份一体机入侵防护系统 (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：

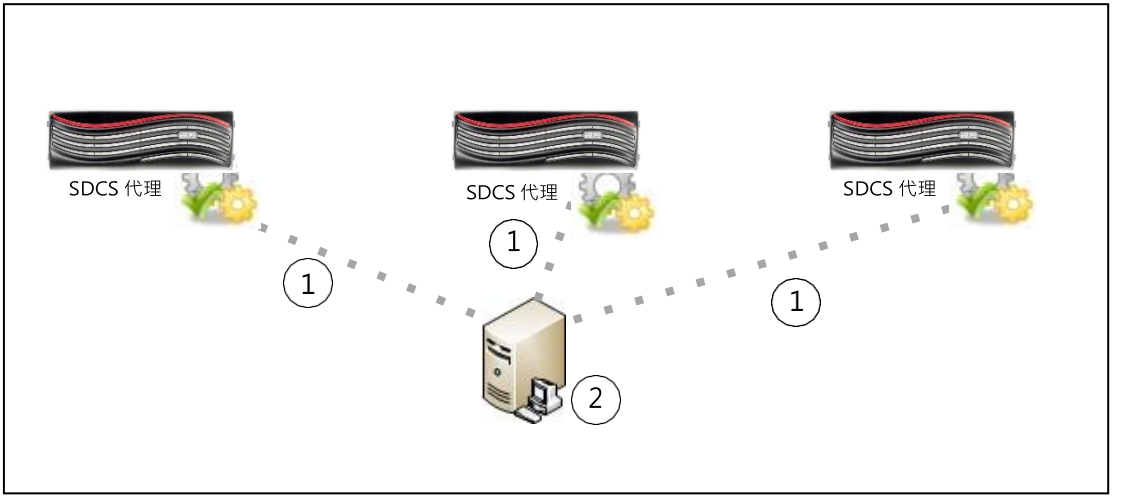
- 加固的 Linux 操作系统组件
  防止或遏制因操作系统漏洞造成恶意软件对基础主机系统完整性的损害。
- 数据保护
  不论系统权限如何，严格限制对设备数据的访问，仅允许需要访问的程序和活动进行访问。
- 加固的设备堆栈
  锁定设备应用程序二进制和配置设置，这样应用程序或可信程序/脚本可严格控制更改。
- 扩展检测和审核功能
  对重要用户或系统操作提供增强的可见性，以确保有效且完整的审核跟踪，该审核跟踪将遵从性法规（例如 PCI）作为补偿控制措施。
- 集中管理模式操作
  允许您使用中央 SDCS 管理器综合查看多个设备以及 SDCS 管理的任意其他企业系统之中的安全性。

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，神州云科HDP 6100备份一体机处于非受控模式。在非受控模式下，可通过神州云科HDP 6100备份一体机网页操作界面 监视 SDCS 事件。通过 **Monitor > SDCS Events** 页面，监视所记录的事件。使用神州云科HDP 6100备份一体机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 代理与每个神州云科HDP 6100备份一体机进行配置。

图 4-1显示了处于受控模式的 SDCS。

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：

- 下载神州云科HDP 6100备份一体机IPS 和 IDS 策略
- 使用 SDCS 管理控制台应用上述策略
- 连接神州云科HDP 6100备份一体机和服务器
- 监视适用于连接至该服务器之所有神州云科HDP 6100备份一体机的事件。

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《*神州云科HDP 6100备份一体机*安全指南》。

关于神州云科HDP 6100备份一体机入侵防护系统

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
  - NFS 的 rpcd
    - 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。

关于神州云科HDP 6100备份一体机入侵检测系统

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

- 备份软件服务启动和停止
- 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
- 所有神州云科HDP 6100备份一体机网页操作界面和神州云科HDP 6100备份一体机命令行操作界面活动的审核，包括 maintenance、root 和备份软件命令行用户的 shell 操作。

查看神州云科HDP 6100备份一体机上的 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 tosystem.

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，请参考神州云科HDP 6100备份一体机管理指南。

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 52 页的“关于神州云科HDP 6100备份一体机日志文件”。

在神州云科HDP 6100备份一体机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。

您可以从神州云科HDP 6100备份一体机网页操作界面（“监视”>“SDCS 事件”）和神州云科HDP 6100备份一体机命令行操作界面 (Main_Menu > Monitor > SDCS) 监视 SDCS 事件。

在神州云科HDP 6100备份一体机上以受控模式运行 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。您可以从神州云科HDP 6100备份一体机网页操作界面中下载 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.yunke-china.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。您可以直接从神州云科HDP 6100备份一体机网页操作界面下的“监视”>“SDCS 事件”中下载这些策略。

3 将设备连接到 SDCS 服务器。您可以通过神州云科HDP 6100备份一体机网页操作界面下的“监视”>“SDCS 事件”或神州云科HDP 6100备份一体机命令行操作界面下的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。

5

日志文件

本章节包括下列主题：

关于神州云科HDP 6100备份一体机日志文件

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。

神州云科HDP 6100备份一体机能够捕获与硬件、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

开始时间	访问方法	日志详细信息
神州云科HDP 6100备份一体机网页操作界面	可以使用神州云科HDP 6100备份一体机网页操作界面中的“监视”>“SDCS 审核视图”屏幕 检索设备的审核日志。请参见第 48 页的“查看神州云科HDP 6100备份一体机上的 SDCS 事件”。	设备审核日志

开始时间	访问方法	日志详细信息
神州云科HDP 6100备份一体机命令行操作界面	您可以使用 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 54 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 ▪ 备份软件日志、卷管理器日志以及 openv 目录中包含的备份软件日志 ▪ 设备操作系统 (OS) 安装日志 ▪ 备份软件管理 Web 用户界面日志和备份软件Web 服务器日志 ▪ 备份软件52xx Appliance 的设备日志
神州云科HDP 6100备份一体机命令行操作界面	您可以使用 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 54 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 ▪ FTDedupTarget ▪ TaskService ▪ AuthService
神州云科HDP 6100备份一体机命令行操作界面	您可以使用 Main > Support > DataCollect 命令收集存储设备日志。 请参见第56页的“收集 HDP 6100备份一体机上的设备日志。”	设备存储设备日志

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。

要使用 Support > Logs > Browse 命令查看日志，请执行以下操作：

1 通过在神州云科HDP 6100备份一体机命令行操作界面中使用 Main_Menu > Support > Logs，然后运行 Browse 命令进入浏览模式。此时将显示 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 55 页的“可使用 Browse 命令从何处查找神州云科HDP 6100备份一体机日志文件”。

要使用 Support > Logs 命令查看神州云科HDP 6100备份一体机统一 (VxUL) 日志，请执行以下操作：

1 可以使用 Support > Logs > VXLogView 命令查看神州云科HDP 6100备份一体机统一 (VxUL) 日志。在命令行操作界面中输入命令，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

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 神州云科技术支持。
- 设置日志级别。

- 导出或删除 CIFS 和 NFS 共享。

注意：神州云科HDP 6100备份一体机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《神州云科HDP 6100备份一体机命令参考指南》。

请参见第 52 页的“关于神州云科HDP 6100备份一体机日志文件”。

可使用 Browse 命令从何处查找 神州云科HDP 6100备份一体机 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 神州云科HDP 6100备份一体机日志文件位置

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
备份软件日志、Volume Manager 日志以及 openv 目录中包含的备份软件日志	<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
操作系统 (OS) 审核日志	<DIR> APPLIANCE audit.log
备份软件重复数据删除 (PDDE) 配置脚本日志	<DIR> PD pdde-config.log
备份软件管理 Web 用户界面日志和 备份软件Web 服务器日志	<DIR> WEBGUI ▪ <DIR> gui ▪ <DIR> webserver
设备日志	/tmp/DataCollect.zip（软件版本 3.1.2 及更低版本） /log/DataCollect.zip（软件版本 3.2 及更高版本） 可以使用 Main > Support > Logs > Share Open 命令将 DataCollect.zip复制到本地文件夹。

请参见第 52 页的“关于神州云科HDP 6100备份一体机日志文件”。

收集神州云科HDP 6100备份一体机上的设备日志

可以使用 Main > Support命令行操作界面中的 DataCollect命令收集设备日志。可以和 神州云科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 登录到神州云科HDP 6100备份一体机命令行操作界面。

2 从 Main > Support 视图中，键入以下命令以收集设备日志：

DataCollect

对于 Appliance 软件版本 3.1.2 及更低版本，Appliance 在 /tmp/DataCollect.zip 文件中生成设备日志。

对于高于 3.1.2 但低于 5.0 的 Appliance 软件版本，Appliance 在 /log/DataCollect.zip 文件中生成设备日志。

对于 Appliance 软件版本 5.0 及更高版本 ，Appliance 在 /log/data-collect/sosreport*.tar.xz 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 神州云科支持团队以解决问题。

请参见第 52 页的“关于神州云科HDP 6100备份一体机日志文件”。

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，神州云科HDP 6100备份一体机支持转发 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。

从软件版本 5.0 开始，将审核 Appliance 命令行操作界面和 Appliance 网页操作界面访问日志。

神州云科HDP 6100备份一体机使用 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。神州云科HDP 6100备份一体机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 共享将这些文件上传到设备。
- 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

必须使用以下 Main > Settings > LogFowarding 命令选项从命令行操作界面配置此功能：

- 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。
  如果设备上启用了 STIG，则无法手动配置日志转发间隔。
- 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/share

CIFS：\\<appliance.name>\general_share

注意：您也可以从 Appliance 网页操作界面中的“管理”>“文件管理器”菜单上传证书文件。

- 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 命令提示符

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。
Interval (时间间隔)	设置日志转发频率。
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传到设备才能使用 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：

《神州云科HDP 6100备份一体机管理指南》

《神州云科HDP 6100备份一体机命令参考指南》

6

操作系统安全

本章节包括下列主题：

关于神州云科HDP 6100备份一体机操作系统安全

神州云科HDP 6100备份一体机使用 神州云科操作系统 (VxOS)，这是一个自定义的 Linux 操作系统。每个神州云科HDP 6100备份一体机软件版本均包含最新版本的 VxOS 和备份软件软件。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 神州云科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)。用法限于 ssh、scp 和 sftp。

注意：从神州云科HDP 6100备份一体机版本 3.1.2 开始，已从 VxOS 中删除 telnet 软件包，以便在神州云科HDP 6100备份一体机上启用了 STIG 功能时符合 STIG 规范。APPSOL-80036 and APPSOL89038, Jay Vasa - Sangria Teamtelnet 协议不安全或未加密。使用未加密的传输介质可能会允许未经授权的用户窃取凭据。ssh 软件包提供加密会话和更高的安全性，且包含在 VxOS 中。

- 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。
- 神州云科HDP 6100备份一体机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，但神州云科HDP 6100备份一体机的 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 如今是神州云科HDP 6100备份一体机的最低支持协议。

神州云科HDP 6100备份一体机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 Appliance 版本 4.0 的 VxOS 中包含的主要软件组件

软件组件	版本
Red Hat Enterprise Linux (RHEL)	

软件组件	版本
神州云科InfoScale	注意：对 神州云科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 6.8 Advanced (SDCS)	
Java Runtime Environment (JRE)	
Apache Tomcat	
RabbitMQ	
MongoDB	
Intel IPMI Utils	

禁用用户对神州云科HDP 6100备份一体机操作系统的访问

根据组织的安全策略，可以选择永久禁用用户对神州云科HDP 6100备份一体机操作系统(VxOS) 的访问。可以通过将 VxOS 的安全级别配置为 High 禁用用户对 VxOS 的访问。请注意，将在设备中永久强制实施以下限制：

- 用户无法访问 maintenance shell。Support > Maintenance 菜单在命令行操作界面中不可用。

  注意：仅可以授予 神州云科支持人员访问 maintenance shell 的权限，以对问题进行故障排除并管理与操作系统相关的任务。请参见第 63 页的“管理对 maintenance shell 的支持访问”。

- 用户无法创建和删除备份软件命令行用户。Manage > 备份软件命令行菜单在命令行操作界面中不可用。
- 用户无法授予或撤销备份软件命令行角色。Authorization > Grant备份软件命令行菜单在命令行操作界面中不可用。
- 具有备份软件命令行角色的用户无法登录到 Appliance。

永久禁用用户对 VxOS 的访问

1 要查看 VxOS 的当前安全级别，请使用以下命令：

Main_Menu > Settings > Security > SecurityLevel Show

VxOS 可在下列任一安全级别运行：

安全级别	描述
Optimal	按照标准 神州云科安全策略授予对 VxOS 的访问权限。这是默认安全配置。
High	永久禁止所有用户访问 VxOS。
Maintenance	通过 maintenance shell 为 神州云科支持人员临时授予 VxOS 的访问权限。维护活动完成后，安全级别将自动恢复为High。

2 要永久禁用用户对 VxOS 的访问，请将安全级别配置为 High。使用以下命令：

Main_Menu > Settings > Security > SecurityLevel High

注意：切换到 High 安全级别后，除非对设备执行恢复出厂设置，否则无法恢复到默认 (Optimal) 安全级别。

管理对 maintenance shell 的支持访问

如果将 VxOS 的安全级别配置为 High，则 Support > Maintenance 菜单中的 maintenance shell 将被禁用。但是，要对问题进行故障排除并管理操作系统任务，可以允许 神州云科支持人员启用和访问 maintenance shell。

使用 Main_Menu > Support > System 菜单中的命令管理对 maintenance shell 的支持访问。有关更多信息，请参见《神州云科HDP 6100备份一体机命令参考指南》。

表 6-2 用于管理对 maintenance shell 的支持访问的命令

命令	描述
Support > System > Generate-otp	使用此命令生成十位数的一次性密码 (OTP)，该密码在两小时内保持活动状态。 可与 神州云科支持人员共享 OTP。
Support > System > Show-otp	使用此命令可查看当前处于活动状态的OTP。

命令	描述
Support > System > Unlock	神州云科支持人员使用此命令启用 maintenance shell (Support > Maintenance)。除了活动的 OTP 之外，神州云科支持人员还需要客户案例 ID 和支持密码，才能成功运行 Unlock 命令并访问 maintenance shell。 注意：VxOS 已临时配置为 Maintenance 安全级别。
Support > System > Lock	使用此命令可禁用 maintenance shell。神州云科支持人员将无法访问 maintenance shell，并且会注销任何活动会话。 注意：VxOS 恢复为 High 安全级别。

7

数据安全性

本章节包括下列主题：

关于数据安全

神州云科HDP 6100备份一体机支持策略驱动机制以保护客户端和备份软件服务器上的数据。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神州云科HDP 6100备份一体机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。
- 神州云科HDP 6100备份一体机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。
- 仅授权的用户和备份软件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 神州云科 AutoSupport 服务器以上传硬件和软件信息。神州云科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 神州云科安全操作中心保留 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时间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
  - 备份软件软件
  - 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（例如备份软件目录库和 KMS 数据库）可能需要进行额外配置。

神州云科HDP 6100备份一体机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，神州云科建议在备份软件主机之间部署 VPN（虚拟专用网络）解决方案，例如 IPSec。

关于数据完整性

神州云科HDP 6100备份一体机中的“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备份软件控制台的磁盘报告 UI（“**备份软件**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要求，可使配置有不同要求的数据备份变得轻松自如。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。神州云科HDP 6100备份一体机支持与备份软件相同的数据分类属性。

备份软件“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转到黄金级别数据分类的存储单元。

备份软件提供以下默认数据分类：

- 白金
- Gold（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才会采用。如果列表显示“无数据分类”，策略将使用“策略存储”列表中显示的存储选择。如果选择了数据分类，则策略创建的所有映像都将带有该分类 ID 的标记。

关于数据加密

神州云科HDP 6100备份一体机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。
- 从神州云科HDP 6100备份一体机版本 3.0（备份软件版本 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，请参见以下备份软件文档：
  《神州云科备份软件重复数据删除指南》
  《神州云科备份软件安全和加密指南》
- 支持使用备份软件密钥管理服务 (KMS)（与备份软件Enterprise Server 7.1 集成）加密。请参见第 67 页的“KMS 支持 ”。

KMS 支持

神州云科HDP 6100备份一体机支持备份软件密钥管理服务 (KMS)（与备份软件 Enterprise Server 7.1 集成）管理的加密。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神州云科HDP 6100备份一体机连接。
- 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。
- 可由备份软件CLI 管理员使用神州云科HDP 6100备份一体机命令行操作界面或 KMS 命令行界面 (CLI) 进行管理。

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 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

要在设备主服务器上配置 KMS，必须以备份软件命令行用户身份登录。

在继续之前，请确保为备份软件命令行用户分配了配置和启用 KMS 所需的 RBAC 权限。使用备份软件管理员帐户（如 **nbasecadmin**）登录到备份软件Web UI，并将“默认安全管理员”角色分配给备份软件命令行用户。

有关管理基于角色的访问控制的步骤，请参见《备份软件Web UI 管理指南》。

注意：如果需要，您可以创建一个新的备份软件命令行用户来配置和启用 KMS。有关备份软件命令行用户的更多信息，请参见第 39 页的“关于备份软件命令行用户角色”。

以下内容介绍了如何在设备上配置并启用 KMS。

在设备上配置并启用 KMS

1 以备份软件命令行用户身份登录设备主服务器。

2 使用如下所示的 Command 命令进入受限 Shell 环境：

```
[nb-appliance.NBCLIUSER>]# Command
```

3 使用以下步骤对 CLI 访问进行身份验证：

- 通过运行以下命令生成访问代码：

  ```
  #bpnbat -login -logintype webui -requestApproval
  ```

  记下命令窗口中显示的访问代码。

- 以备份软件命令行 (CLI) 管理员用户身份登录备份软件Web UI，并通过输入先前生成的访问代码来批准 CLI 访问请求。
  请求获得批准后，您将在受限 Shell 命令窗口中看到一条确认消息。

有关访问密钥和批准请求的更多信息，请参考《备份软件安全和加密指南》。

4 使用 nbkms 命令创建空数据库，如下所示：

```
[nbucliuser-!>]# nbkms -createemptydb
```

5 启动 nbkms。例如：

```
[nbucliuser-!>]# nbkms
```

6 创建密钥组。例如：

```
[nbucliuser-!>]# nbkmsutil -createkg -kgname KMSKeyGroupName
```

7 创建活动密钥。例如：

```
[nbucliuser-!>]# nbkmsutil -createkey -kgname KMSKeyGroupName
-keyname KMS KeyName
```

为 MSDP 启用 KMS 加密

验证是否已在主服务器上配置并运行 KMS。然后，可在与主服务器关联的所有介质服务器上为 MSDP 启用 KMS 加密。

在继续之前，请确保为备份软件命令行用户分配了配置和启用 KMS 所需的 RBAC 权限。使用备份软件管理员帐户（如 **nbasecadmin**）登录到备份软件Web UI，并将“默认安全管理员”角色分配给备份软件命令行用户。

有关如何管理基于角色的访问控制的步骤，请参见《备份软件Web UI 管理指南》。

注意：如果需要，您可以创建一个新的备份软件命令行用户来配置和启用 KMS。有关备份软件命令行用户的更多信息，请参见第 39 页的“关于备份软件命令行用户角色”。

以下内容介绍了如何在设备上为 MSDP 启用 KMS 加密。

为 MSDP 启用 KMS 加密

1 以备份软件命令行用户身份登录设备介质服务器。

2 按照所示顺序更改以下选项：

- nbucliuser-!> pdcfg
  --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg
  --section=KMSOptions --option=KMSType --value=0
- nbucliuser-!> pdcfg
  --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg
  --section=KMSOptions --option=KMSServerName --value=<*primaryserver hostname*
- nbucliuser-!> pdcfg
  --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg
  --section=KMSOptions --option=KMSKeyGroupName --value=msdp
- nbucliuser-!> pdcfg
  --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg
  --section=KMSOptions --option=KeyName --value=<*KMS KeyName*>
- nbucliuser-!> pdcfg
  --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg
  --section=KMSOptions --option=KMSEnable --value=true
- nbucliuser-!> pdcfg --write=
  /msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg
  --section=ContentRouter --option=ServerOptions
  --value=verify_so_references,fast,encrypt
  在与主服务器关联的所有介质服务器上重复执行此步骤。

3 通过登录到备份软件Web 应用程序在系统中提供身份信息。运行以下命令：

sudo /usr/openv/netbackup/bin/bpnbat -login -loginType WEB

Authentication Broker: *ApplianceHostname*

Authentication Port: 0

Authentication Type: unixpwd

LoginName: *Username* Password:

Password

4 确保已向备份软件Web 服务注册 KMS。

```
sudo /usr/openv/netbackup/bin/nbkmscmd -discoverNbkms
```

5 使用以下命令停止并重新启动备份软件服务：

- bp.kill_all
- bp.start_all

6 要验证是否在介质服务器上为 MSDP 启用了 KMS 加密，请在服务器上运行备份作业，然后运行以下命令：

```
crcontrol --getmode
```

8

Web 安全

本章节包括下列主题：

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 Appliance 网页操作界面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。

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

自签名证书

设备使用自签名证书进行客户端和主机验证。在角色配置期间，内部 CA 颁发的主机证书将部署到主服务器和介质服务器上。自签名证书是使用 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。

ECA 证书

神州云科HDP 6100备份一体机还支持由外部证书颁发机构 (ECA) 颁发的主机证书。您可以使用 ECA 来替代内部 CA，以提供主机验证和安全，从而满足组织的各项标准。

有关神州云科HDP 6100备份一体机中使用的不同类型的外部证书，请参考下表。

表 8-1 ECA 证书类型

证书类型	描述
主机证书	设备主机证书基于 X.509 或 PKCS#7 标准。证书以 DER（二进制）或 PEM（文本）格式进行编码。神州云科建议您使用长度至少为 2048 位的 RSA 公钥和私钥。 注意：确保 **SubjectAlternativeName** 证书扩展名包含所有设备主机名和 IP 地址，通过这些主机名和 IP 地址可以访问该设备。包括完全限定主机名和短名称。
主机私钥（对应于主机证书）	设备主机私钥必须采用 PKCS#8 标准，并且以 PEM 格式进行编码。
（可选）中间 CA 证书	中间 CA 证书是从设备主机证书到根 CA 证书的证书链。仅当主机证书由根 CA 以外的 CA 颁发时，才需要这些证书。
根 CA 证书	其中包括设备证书链及其对等方的根 CA 证书。如果与设备进行交互的主机具有来自不同 CA 的证书，则必须在名为 cacerts.pem 的文件中准备好所有这些中间 CA 证书和根 CA 证书。

关于实施 ECA 证书

神州云科HDP 6100备份一体机的 Web 服务使用 PKCS＃12 标准，并要求证书文件采用 X.509 (.pem) 格式。如果证书文件采用 .der、.DER 或 .p7b 格式，神州云科HDP 6100备份一体机则会自动将文件转换为接受的格式。

证书要求

为防止在导入证书时出现错误，请确保外部证书文件满足以下要求。

- 证书文件采用.pem文件格式，并以“-----BEGIN CERTIFICATE ----------” 开头。
- 证书文件中证书的使用者备用名称(SAN) 字段包含主机名和FQDN。如果在HA环境中使用证书，则 SAN 字段必须包含 VIP、主机名和 FQDN。
- 使用者名称和公用名称字段不为空。
- 每个主机的使用者字段唯一。
- 使用者字段最多包含 255 个字符。
- 在证书中设置服务器和客户端身份验证属性。
- 证书的使用者和 SAN 字段中只使用 ASCII 7 字符。
- 私钥文件采用 PKCS#8 PEM 格式，并以 -----BEGIN ENCRYPTED PRIVATEKEY----- 或 -----BEGIN PRIVATE KEY---------- 开头。

证书签名请求 (CSR)

虽然可选，但您可以使用 Settings > Security > Certificate > CertificateSigningRequest > Create命令生成 CSR。将 CSR 内容从命令行复制到 ECA 门户，以获取所需的外部证书文件。

```
Example:
Enter specified value or use the default value.
Common Name (eg, your name or your server's hostname) [Defaultnbapp2ao]:
Organizational Unit Name (eg, section) []:Appliance Organization Name
(eg, company) [Default Company Ltd]:神州云科Locality Name (eg, city)
[Default City]:Beijing
State or Province Name (full name) []:BeijingCountry
Name (2 letter code) [XX]:CH
Email Address []:support@yunke-china.com
Please enter the following 'extra' attributesto be
sent with your certificate request.
--------
A challenge password []:123456 An
optional company name []:VRTS
Subject Alternative Name (DNS Names and/or IP Addresses comma
separated):nbapp2ao,nbapp2ao.engba.yunke-china.com
Subject Alternative Name (email comma separated): Certificate
Signing Request Name [Default nbapp2ao.csr]:Validity period (in
days) [Default 365 days]:
Ensure that the Distinguished Name (DN) is specified as a string consisting of
a sequence of key=value pairs separated by a comma:
Then the generated certificate signing request will be shown on thescreen.
```

注册 ECA

从版本 4.1 开始，可以使用 Settings > Security > Certificate > Import 命令在神州云科HDP 6100备份一体机和备份软件上注册 ECA。

执行以下步骤以导入主机证书、主机私钥和信任存储区，以在备 份 软 件 和神州云科HDP 6100备份一体机上注册 ECA。备份软件和神州云科HDP 6100备份一体机层都使用相同的主机证书、主机私钥和信任存储区。

1 以管理员用户身份登录设备。

2 从神州云科HDP 6100备份一体机命令行操作界面 中，运行 Settings > Security > Certificate > Import 命令。现在可以访问以下 NFS 和 CFS 共享位置：

- NFS：/inst/share

- CFS：*<ApplianceName>*\general_share

3 将证书文件、信任存储区文件和私钥文件上传到任一共享位置，并输入文件的路径。

4 选择如何访问证书吊销列表 (CRL)。CRL 包括 ECA 已吊销且不应信任的外部证书的列表。选择以下任一选项：

- 使用证书文件中提供的 CRL 位置。
- 提供 CRL 文件 (.crl) 在本地网络中的位置。
- 请勿使用 CRL。

5 确认要在设备上注册证书文件的位置。

此处提供了如何导入证书的详细示例。

- 标识应导入的证书。

```
After certificate uploaded, /inst/share/ may look like that:
/inst/share # ls
cacerts.pem  cert_chain.pem  crl  key.pem
/inst/share # ls crl
NBAECA.crl  NBAECA_INTERMEDIATE.crl  NBRootCA.crl
```

- 导入证书。

```
Enter the certificate:
Enter the following details for external certificate configuration:Enter the
certificate file path: cert_chain.pem
Enter the trust store file path: cacerts.pemEnter the
private key path: key.pem
Enter the password for the passphrase file path or skip securityconfiguration (default:
NONE):
Should a CRL be honored for the external certificate?
1) Use the CRL defined in the certificate.
2) Use the specific CRL directory.
3) Do not use a CRL.
q) Skip security configuration.CRL
option (1): 2
Enter the CRL location path: crl
Then confirm input information and answer the subsequent questions.
```

- 注册后，证书文件将存储在 /usr/openv/var/hostcert 目录中。

对 Copilot 的支持

在使用外部证书部署的设备上使用 Copilot 功能之前，请确保满足以下条件：

- 设备的证书文件（在 /etc/vxos-ssl/servers/certs/ 中）与主服务器的证书文件（在 /usr/openv/var/global/appliance_certificates/ 中）相同。
- 设备的证书文件（在 /etc/vxos-ssl/servers/certs/ 中）以 *<FQDN_hostname>*-self.cert.pem 格式命名。在每

个关联的设备上运行以下命令：

```
rm /etc/vxos-ssl/servers/certs/<FQDN_hostname>-self.cert.pem

cp /etc/vxos-ssl/servers/certs/server.pem
/etc/vxos-ssl/servers/certs/<FQDN_hostname>-self.cert.pemtpconfig -

delete -nb_appliance <Short_hostname>

/opt/NBUAppliance/scripts/copilot_users.pl --add
```

添加和删除证书

可以使用 **Certificate** 命令管理神州云科HDP 6100备份一体机上的外部证书。

您可以使用 **Settings** > **Security** > **Certificate** > **Add CACertificate** 命令将服务器CA、HTTPS 代理 CA 或 LDAP CA 证书添加到证书颁发机构列表。确保粘贴 PEM 或 P7B 格式的 CA 证书内容。设备会将此 CA 证书附加到证书颁发机构列表中。在附加 CA 证书之前，设备会验证该 CA 证书是否已在这个设备上使用。如果是，设备则会退出并显示一条消息。新添加的 CA 证书将更新到系统范围的信任存储区、Tomcat 密钥存储库和备份软件信任存储区。

- 系统范围的信任存储区：
  CA 证书将添加到系统范围的信任存储区中。将 CA 证书复制到 /etc/pki/ca-trust/source/anchors/，并将 CA 证书添加到 /etc/pki/ca-trust/extracted 下的所有位置。其中包括 /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem、/etc/pki/ca-trust/extracted/pem/email-ca-bundle.pem、objsign-ca-bundle.pem tls-ca-bundle.pem 和 /etc/pki/ca-trust/extracted/java/cacerts。
- Tomcat 密钥存储库：
  CA 证书将添加到 Tomcat 信任存储区 /opt/apache-tomcat/security/keystore。
- 备份软件信任存储区：
  如果通过备份软件启用 ECA，CA 将附加到 /usr/openv/var/hostcert/trustStorePath/cacerts.pem 文件的末尾。调用 configureWebServerCerts 以更新备份软件Web 服务信任存储区。其中包括 /usr/openv/var/global/wsl/credentials/externalcacreds/nbwebservice.bcfks

和
/usr/openv/var/global/wsl/credentials/tpcredentials/nbwebservice.bcfks。

您可以使用 **Settings** > **Security** > **Certificate** > **Remove CACertificate** 命令将服务器 CA 证书从证书颁发机构列表中删除。将列出可用的 CA 证书，您可以选择要删除的证书。系统范围的信任存储区、Tomcat 密钥存储库和备份软件信任存储区将更新以删除 CA 证书。

- 系统范围的信任存储区：
  /etc/pki/ca-trust/source/anchors 下的 CA 证书文件将删除，而且系统范围的信任存储区会更新。其中包括
  /etc/pki/ca-trust/extracted/pem/email-ca-bundle.pem、/etc/pki/ca-trust/extracted/pem/objsign-ca-bundle.pem、/etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem 和
  /etc/pki/ca-trust/extracted/java/cacerts。
- Tomcat 密钥存储库：
  CA 证书将从 Tomcat 密钥存储库中删除。
- 备份软件信任存储区：
  从备份软件相关密钥存储库中删除 CA 证书。/usr/openv/var/hostcert/trustStorePath/cacerts.pem 文件中的 CA 将删除，备份软件Web 服务信任存储区中的 CA 也会删除。其中包括
  /usr/openv/var/global/wsl/credentials/externalcacreds/nbwebservice.bcfks 和
  /usr/openv/var/global/wsl/credentials/tpcredentials/nbwebservice.bcfks。

9

网络安全

本章节包括下列主题：

关于 IPsec 通道配置

神州云科HDP 6100备份一体机使用 IPsec 通道来保护两个设备之间的通信安全，从而帮助保护传输中的数据。神州云科HDP 6100备份一体机与非设备（例如备份软件主服务器）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个设备之间的 IP 通信。主服务器设备和介质服务器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 DigiCert 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设备进行检测。只有此检查完成后才能配置和启用 IPsec 通道。

请与 神州云科支持联系，以在设备上配置 IPsec 功能。

关于神州云科HDP 6100备份一体机端口

除备份软件软件使用的端口之外，神州云科HDP 6100备份一体机还提供带内和带外管理。带外管理通过独立网络连接、远程管理模块 (RMM) 和智能平台管理界面 (IPMI) 实现。可以视情况在防火墙中打开这些端口，以允许从远程笔记本电脑或 KVM（键盘、视频监视器、鼠标）访问管理服务。

有关在进行初始配置之前和之后默认打开的 Appliance 端口的列表，请参考以下主题：

请参见第 80 页的“关于神州云科HDP 6100备份一体机防火墙”。

注意：只能使用 HTTPS 通过默认端口 443 访问神州云科HDP 6100备份一体机网页操作界面。使用 https://*<appliance-name>* 登录网页操作界面，其中 appliance-name 是 Appliance 的完全限定域名 (FQDN)，也可以是 IP 地址。

表 9-1列出了允许将警报和通知发送到指定服务器的 Appliance 出站端口。

表 9-1 出站端口

端口	服务	描述
443	HTTPS	向 神州云科发送自动通报通知 下载 SDCS 证书
161	SNMP 轮询	下载 Appliance 更新
162**	SNMP	下载 Appliance 更新
22	SFTP	将日志上载到网站
25	SMTP	电子邮件警报
389	LDAP	
636	LDAP	
514	rsyslog	日志转发

** 可以在 Appliance 配置中更改此端口号以匹配远程服务器。

注意：要查看远程管理模块 (RMM) 端口的列表，请参见以下主题：

请参见第 92 页的“RMM 端口”。

《备份软件网络端口参考指南》中提供了所有适用端口的完整列表。

关于神州云科HDP 6100备份一体机防火墙

从神州云科HDP 6100备份一体机版本 3.1.2 开始，防火墙策略为设备提供增强的网络安全。此功能将防火墙默认区域从“可信”更改为“公共”。为了提供最大的安全性，在以下操作期间，特定传入连接将自动打开，而其他连接将自动阻止：

- 初始配置
- 角色配置（在初始配置期间）
- 添加或删除节点（高可用性配置）
- 升级

例外规则有助于确保主服务器和介质服务器之间的连接在所述操作期间保持打开状态，并使不必要的端口保持阻止状态。

以下各表介绍了在进行初始配置之前和之后设备上打开的端口。

表 9-2 显示了在完成设备初始配置之前，默认打开的神州云科HDP 6100备份一体机端口。

表 9-2 出厂时默认打开的神州云科HDP 6100备份一体机端口（在设备初始配置之前）

端口	协议	用法
22	TCP	SSH
111	TCP/UDP	Sunrpc、Portmapper
137	UDP	NetBIOS 名称服务 (Samba)
138	UDP	NetBIOS 数据报服务 (Samba)
139	TCP	NetBIOS 会话服务 (Samba)
162	TCP/UDP	SNMP
443	TCP	HTTPS
445	TCP	Samba
867	TCP	NFS 装入
2049	TCP/UDP	NFS
20048	UDP	mountd

端口	协议	用法
27017	TCP/UDP	Mongo 注意：此端口仅在您添加合作伙伴节点以完成高可用性 (HA) 设置或从 HA 设置中删除节点时打开。添加或删除节点后，将关闭此端口。

表 9-3 显示了在完成设备初始配置之后，默认打开的备份软件端口。

表 9-3 神州云科HDP 6100备份一体机上打开的备份软件端口（在设备初始配置之后）

1025-5000	TCP	神州云科NDMP、SERVER_PORT_WINDOW
1556	TCP	神州云科PBX
5637	TCP/UDP	备份软件Cloud Storage Server 配置、对云的重复数据删除
7394	TCP	神州云科粒度恢复技术 (GRT)
8443	TCP	备份软件VMware
10000	TCP/UDP	神州云科NDMP 代理
10082	TCP/UDP	MSDP、Deduplication Engine (spoold)、HA、迁移
10102	TCP/UDP	MSDP、Deduplication Manager (spad)、HA、迁移
13701-13723	TCP	神州云科粒度恢复技术 (GRT)
13720	TCP	支持 271 介质角色配置
13724	TCP	vnetd
13781	TCP	RabbitMQ
13782	TCP	神州云科vnet_async

同步或查看设备上打开的备份软件端口

已添加以下命令，用于同步或查看设备上当前打开的备 份 软 件 端口：

Main > Settings > Security > Ports > ModifyNBUPortRange

请注意有关使用此命令的以下事项：

- 必须为设备配置了主服务器或介质服务器角色，然后才能运行此命令。

- 在运行此命令之前，必须首先在备份软件Java 控制台中使用SERVER_PORT_WINDOW 命令修改打开的备份软件端口。然后，运行此命令以同步设备端口与打开的备份软件端口。

注意：ModifyNBUPortRange 命令不允许更改分配的默认备份软件VMware 端口 8443。默认情况下，VMware 要求将端口 8443 用于备份一体机。

Main > Settings > Security > Ports > Show

有关这些命令的详细信息，请参见《神州云科HDP 6100备份一体机命令参考指南》。

10

“自动通报”安全功能

本章节包括下列主题：

关于 AutoSupport

通过 AutoSupport 功能，可以在 神州云科支持网站上注册该设备和您的联系人详细信息。神州云科支持使用此信息解决您报告的任何问题。这些信息允许 神州云科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。

https://netInsights.yunke-china.com 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 神州云科支持通过以下方式为您提供帮助：

- 通过主动监视，神州云科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。
- 神州云科中的 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，神州云科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。

数据安全标准

从设备传输到 神州云科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 神州云科AutoSupport 服务器连接并上载硬件和软件信息。神州云科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 连接到神州云科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。

AutoSupport 使用自动通报收集的数据为设备提供主动式监视。如果启用了自动通报，设备会按照默认间隔（24 小时）将信息或数据上传到 神州云科AutoSupport 服务器。

如果确定设备存在问题，您可能希望与 神州云科支持联系。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。

要从神州云科HDP 6100备份一体机网页操作界面获取设备的序列号，请转到“监视器”>“硬件”>“运行状况详细信息”页面。要使用命令行操作界面确定设备的序列号，请转到 Monitor > Hardware 命令。有关 Monitor > Hardware 命令的更多信息，请参考《神州云科HDP 6100备份一体机命令参考指南》。

使用“设置”>“通知”页面从神州云科HDP 6100备份一体机网页操作界面配置自动通报。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 神州云科 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 神州云科AutoSupport 服务器。您的系统不会向 神州云科报告错误以加快解决问题的速度。

以下列表提供了发送到 神州云科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
- 神州云科HDP 6100备份一体机软件版本
- 备份软件版本
- 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 86 页的“从神州云科HDP 6100备份一体机命令行操作界面配置自动通报”。请参见第 83 页的“关于 AutoSupport ”。

从神州云科HDP 6100备份一体机命令行操作界面配置自动通报

您可以从“设置”>“通知”页面配置自动通报详细信息。

可以从神州云科HDP 6100备份一体机命令行操作界面配置以下自动通报设置：

- 从 Appliance 命令行操作界面启用和禁用自动通报
- 从神州云科HDP 6100备份一体机命令行操作界面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，请参考《神州云科HDP 6100备份一体机命令参考指南》。

有关导致警报的硬件问题列表，请参见下列主题：

请参见第 84 页的“关于自动通报”。

从 Appliance 命令行操作界面启用和禁用自动通报

可以从 Appliance 命令行操作界面启用或禁用自动通报。默认情况下启用自动通报。

注意：为了使自动通报正常运行，您需要注册设备。神州云科NetInsights 控制台版本不再支持 MyAppliance 门户，并且将停用该门户。应通过使用 神州云科 Account Manager 凭据登录到 NetInsights 门户 (https://netInsights.yunke-china.com) 来完成设备注册。有关更多信息，请参见《神州云科Appliance AutoSupport 参考指南》和
《神州云科NetInsights 控制台安装使用指南》。

从命令行操作界面启用或禁用自动通报

1 登录到命令行操作界面。

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。

有关神州云科HDP 6100备份一体机Main > Settings > Alerts > CallHome 命令的更多信息，请参考《神州云科HDP 6100备份一体机命令参考指南》。

从神州云科HDP 6100备份一体机命令行操作界面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 神州云科AutoSupport 服务器的 https 连接。默认情况下，该选项处于禁用状态。

从神州云科HDP 6100备份一体机命令行操作界面添加自动通报代理服务器

1 登录到神州云科HDP 6100备份一体机命令行操作界面。

2 要启用代理设置，请运行 Main > Settings > Alerts > CallHome ProxyEnable 命令。

3 要添加代理服务器，请运行 Main > Settings > Alerts > CallHome ProxyAdd 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。默认情况下，HTTP 协议用于与代理服务器进行通信。

注意：如果要使用 HTTPS 协议，请在代理服务器名称前输入 **https://**。要确保与代理服务器成功通信，请通过运行 Settings > Security > Certificate > AddCACertificate 命令添加代理服务器使用的最新 CA 证书。

- 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 ProxyDisable 命令。

接着，您也可以使用神州云科HDP 6100备份一体机命令行操作界面为设备启用或禁用代理服务器隧道。为此，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 神州云科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 神州云科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 神州云科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。

设备将启动所有通信。在设备上，请确保启用代理和/或防火墙，以将出站 443/TCP TLS 套接字连接到以下站点：https://api.appliance.yunke-china.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://api.appliance.yunke-china.com。
- 对以下网站执行自检操作：https://api.appliance.yunke-china.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 神州云科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 84 页的“关于自动通报”。

请参见第 83 页的“关于 AutoSupport ”。

关于 SNMP

简单网络管理协议 (SNMP) 是一种应用层协议，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，以及规划网络的增长。

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变量。

神州云科HDP 6100备份一体机3.1 及更高版本支持 SNMP V2。

神州云科HDP 6100备份一体机4.0 及更高版本支持 SNMP V2 和 SNMP V3。

关于管理信息库 (MIB)

每个 SNMP 元素都管理特定的对象，而各个对象都有其具体的特性。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，可汇编和解释 SNMP 消息。此信息保存为 MIB 文件。

您可以从 Web 控制台的“设置”>“通知”>“警报配置”页面查看 SNMP MIB 文件的详细信息。要将设备 SNMP 管理器配置为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 Appliance 命令行操作界面中使用 Settings > Alerts > SNMP ShowMIB 命令查看 SNMP MIB 文件。

11

远程管理模块(RMM) 安全性

本章节包括下列主题：

IPMI 配置简介

您可以为设备配置智能平台管理接口(IPMI) 子系统。在由于意外断电而关闭所连接的系统时，IPMI 子系统很有帮助。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 神州云科Remote Management 工具。神州云科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。

用户

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。
  - 在不使用 IPMI 协议端口 (623) 时将其关闭，以缓解与 IPMI 协议关联的安全风险 (CVE-2013-4786)。有关详细信息，请参见 https://nvd.nist.gov/vuln/detail/CVE-2013-4786。

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

KCS 策略控制模式

对于使用 BIOS 版本 2.01.0010 或更高版本更新的神州云科HDP 6100备份一体机型号 5250、5340 和 5350，登录到 IPMI 控制台时会显示以下消息：

```
KCS Policy Control Mode is Allow All.
This setting is intended for BMC provisioning and isconsidered
insecure for deployment.
```

您可以放心地忽略此消息，因为 KCS 策略设置仅影响操作系统级别的 IPMI 命令的带内访问。这些命令只能由 root 级别用户访问。此默认策略设置与以前 神州云科产品版本的设置相匹配。

LDAP 设置

神州云科建议启用通过 OpenLDAP 进行 LDAP 身份验证。IPMI 子系统与 Active Directory 不兼容。

SSL 上传

神州云科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	Stunnel 注意：BMC 固件 01.51.11142 中的 KVM 加密已删除对 AES 和 RC4 算法的支持。
介质加密	启用

您也可以使用 iKVM over HTML5 登录到 Appliance 命令行操作界面。

注意：HTML5 选项仅适用于具有固件 (BIOS) 版本 00.01.0016 或更高版本的 Appliance。

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。

RMM 端口

配置远程管理模块时，会显示以下端口。

表 11-3 RMM 端口

端口	服务	描述	5240 上的默认状态	5340、5250 和 5350 上的默认状态
80	HTTP	带外管理（ISM+ 或 RM*）	已禁用	已禁用

端口	服务	描述	5240 上的默认状态	5340、5250 和 5350 上的默认状态
443	HTTP	带外管理（ISM+ 或 RM*）	已启用	已启用
5120	RMM	ISO & CD-ROM 重定向	已启用	已禁用
5124	RMM（安全）	CDROM	已禁用	已启用
22 或 66	SSH	CLI 访问	已禁用	已禁用
(UDP) 623	IPMI over LAN	带外管理（ISM+ 或 RM*）	已禁用	已禁用
特定于 *5340*、*5250* 和 *5350* 的端口				
5900	KVM	CLI 访问、ISO & CDROM 重定向	N/A	已禁用
5902	KVM（安全）	CLI 访问、ISO & CDROM 重定向	N/A	已启用
623	RMM	软盘重定向	N/A	已禁用
627	RMM（安全）	软盘重定向	N/A	已启用
特定于 *5240* 的端口				
7578	KVM	CLI 访问	已启用	N/A
7582	KVM（安全）	CLI 访问	已禁用	N/A
5123	RMM	软盘重定向	已启用	N/A
5127	RMM（安全）	USB 或软盘	已禁用	N/A

+备份软件集成存储管理器

* 神州云科Remote Management - 远程控制台

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

在远程管理模块上启用 SSH

安装期间，在远程管理模块上自动阻止端口 20 (ssh) 用于 IPMI。可按照以下步骤操作以启用 SSH。

在远程管理模块上启用 SSH

1 登录 神州云科Remote Management 模块。

2 在“配置”选项卡上的左侧窗格中，选择“安全设置”。

3 在“可选网络服务”中，选中 **SSH** 旁边的“启用”复选框。

4 单击“保存”。

替换默认 IPMI SSL 证书

神州云科建议将用于访问 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，DigitalChina。
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=DCYunke/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 神州云科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 关闭再重新打开神州云科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：

神州云科HDP 6100备份一体机的操作系统 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，您可以启用操作系统 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 - V3R3

要启用这些规则，请使用以下命令：

Main_Menu > Settings > Security > Stig Enable，后接 maintenance 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。

- 在设备上启用 STIG 规则之前，您可以拥有无限制的并行 SSH 会话和 10 个网页操作界面会话。启用 STIG 规则后，最多并行 SSH 会话和网页操作界面会话数限制为各 10 个。使用 Security > Sessions命令可设置并行会话数的限制。设置限制后，在执行恢复出厂设置之前，无法将其更改为无限制。

注意：如果在 Appliance 上启用了 STIG 功能，且需要升级 Appliance 或在该 Appliance 上安装 EEB，请勿计划在凌晨 4:00 - 4:30 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 Appliance 发出多个警报消息。

从 4.1 版本开始，所有 STIG 规则列表均在 神州云科支持站点上以单独的文档提供。目前提供了两个检查清单，一个用于操作系统，另一个用于应用程序安全 STIG。有关如何获取这些文档的说明，请转到 神州云科下载中心上的“最新版本”页面，导航到“**神州云科HDP 6100备份一体机**操作系统”并单击“了解详细信息”。

神州云科HDP 6100备份一体机符合 FIPS 140-2 标准

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。

注意：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

---

Java 的 FIPS 验证

从神州云科HDP 6100备份一体机4.1 开始，默认情况下，所有基于 Java 的服务均启用 FIPS 140-2 标准。FIPS 验证通过使用 SafeLogic 的 CryptoComply 模块来实现。

MSDP、备份软件和 VxOS 的 FIPS 验证

从神州云科HDP 6100备份一体机版本 5.0 开始，您可以为 MSDP、备份软件和 VxOS 启用 FIPS 140-2 标准。MSDP、备份软件和 VxOS 使用的备份软件加密模块已通过 FIPS 验证。

为 VxOS 启用 FIPS 后，sshd 将使用以下获得 FIPS 批准的密码：

- aes128-ctr

- aes192-ctr

- aes256-ctr

为VxOS 启用 FIPS 后，较旧的 SSH 客户端可能会阻止对 Appliance 的访问。检查以确保 SSH 客户端支持列出的密码，并在必要时升级到最新版本。默认密码设置通常不符合 FIPS 标准，这意味着可能需要在 SSH 客户端配置中手动选择这些设置。

您可以使用以下命令为备份软件MSDP、备份软件和 VxOS 启用 FIPS 140-2 标准：

- Main Menu > Settings > Security > FIPS Enable MSDP，后接 maintenance 密码。
  启用或禁用MSDP选项会终止当前正在进行的所有作业，并重新启动备份软件服务。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。

  注意：如果已从早期版本的神州云科HDP 6100备份一体机升级，请确保仅在现有数据转换为使用符合 FIPS 标准的算法后启用 MSDP。要检查数据转换的当前状态，请使用 crcontrol --dataconvertstate 命令。如果在状态设置为“已完成”前启用 MSDP，可能会导致数据还原失败。

- Main Menu > Settings > Security > FIPS Enable NetBackup，后接 maintenance 密码。
  启用或禁用备份软件选项会终止当前正在进行的所有作业，并重新启动备份软件服务。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。
- Main Menu > Settings > Security > FIPS Enable VxOS，后接 maintenance 密码。
  启用或禁用VxOS选项会重新启动设备，并断开所有登录用户与其会话的连接。最佳做法建议首先向所有用户进行提前通知，然后再启用或禁用此功能。
- Main Menu > Settings > Security > FIPS Enable All，后接 maintenance 密码。
  启用或禁用 All 选项会重新启动设备，并断开所有登录用户与其会话的连接。最佳做法建议首先向所有用户进行提前通知，然后再启用或禁用此功能。

注意：在神州云科HDP 6100备份一体机高可用性 (HA) 设置中，只有在完成 HA 设置配置后，才能在两个节点上启用 FIPS 功能。两个节点上的 FIPS 配置必须匹配。如果在完成 HA 设置之前在任一节点上启用了 FIPS，则必须在完成 HA 设置之前在该节点上禁用 FIPS。

有关 FIPS 命令的完整信息，请参见《神州云科HDP 6100备份一体机命令参考指南》。

关于符合 FIPS 的密码

从神州云科HP 6100备份一体机4.1.2 开始，设备将限制使用符合 FIPS 的密码与 Kerberos、AD 和 LDAP 服务器进行通信，以提高设备的安全性。

如果您已将设备配置为使用 Kerberos 服务器，则仅使用以下符合 FIPS 的密码与 Kerberos 服务器进行通信。

- aes256-cts-hmac-sha1-96
- aes128-cts-hmac-sha1-96

如果您已将设备配置为使用 LDAP 服务器，则仅使用 TLS v1.2 和以下符合 FIPS 的密码与 LDAP 服务器进行通信。

- ecdhe-rsa-aes128-gcm-sha256
- ecdhe-rsa-aes256-gcm-sha384
- dhe-rsa-aes128-gcm-sha256
- dhe-rsa-aes256-gcm-sha384

如果您已将设备配置为使用 AD 服务器，则仅使用以下符合 FIPS 的密码与 AD 服务器进行通信。

- aes256-cts-hmac-sha1-96
- aes128-cts-hmac-sha1-96

安全版本内容

本附录包括下列主题：

神州云科HDP 6100备份一体机安全版本内容

以下列表包含已修复且现在包括在此版本神州云科HDP 6100备份一体机软件中的已知安全问题：

索引