Veritas NetBackup™ Appliance AutoSupport 2.0 参考指南

3.1 版

文档版本 **1**

VERITAS™

Veritas NetBackup™ Appliance AutoSupport 2.0 参考指南

文档版本：2.7.3

法律声明

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

http://www.veritas.com

。

法律声明

Copyright © 2016 Veritas Technologies LLC. © 2016 年 Veritas Technologies LLC 版权所有。All rights reserved. 保留所有权利。

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

介绍

本章节包括下列主题：

AutoSupport 概述

Veritas AutoSupport 是通过对 Veritas Appliance 硬件和软件进行主动型监视来改善支持体验的一套基础架构、进程和系统。AutoSupport 也提供自动报错和支持案例创建功能。

通过集成自动化、Internet 访问和案例管理，Veritas 可以改进支持流程，为我们的支持工程师提供工具以快速地解决问题。Veritas 中的 AutoSupport 基础架构将分析来自每个设备的“自动通报”数据，为硬件故障提供主动型客户支持和事件响应。该功能减少了需要管理员初始化支持案例的情况。它还使 Veritas 能够更好地理解客户对设备的配置和使用方式，以及最需要改进的地方。AutoSupport 还能够将“自动通报”数据和存储在 Veritas 中的其他站点配置数据相关联，用于技术支持和错误分析。借助 AutoSupport，Veritas 极大地改善了客户支持体验。

本文档介绍了 AutoSupport 的许多方面，其中包括架构（工作原理）、操作（配置方法）、安全和数据隐私以及技术详细信息（数据）。本文档主要介绍 NetBackup 52xx Appliance 和 NetBackup 53xx Appliance。

AutoSupport 2.0 支持的平台

AutoSupport 2.0 支持以下 NetBackup appliance 平台：

- NetBackup 5220 Appliance（软件 2.7.1 或更高版本）
- NetBackup 5230 Appliance（软件 2.7.1 或更高版本）
- NetBackup 5240 Appliance（软件 2.7.3 或更高版本）
- NetBackup 5330 Appliance（软件 2.7.1 或更高版本）

- NetBackup 5340 Appliance（软件 3.1 或更高版本）

其他信息

有关 Veritas Appliances 的更多信息以及其他相关文档，请访问 Veritas 网站上的以下信息商店：

- NetBackup Appliance 主页
- Veritas 技术支持页面
- Veritas Appliance 服务页面

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。

注意：自动通报不是必需的，但它是主动客户支持和故障事件响应的关键步骤。

下表提供了有关禁用自动通报时出现的情况的更多详细信息。

表 1-1 当禁用自动通报时，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。 ■ 设备会向配置的电子邮件地址生成以下三种电子邮件警报： 　■ 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。 ■ 从软件版本 2.7.1 开始，Veritas 会在 Veritas AutoSupport 服务器超过 28 小时没有从您的设备收到任何自动通报数据软件包时，发送有关传输故障的电子邮件警报。 ■ 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。

2

架构

本章节包括下列主题：

AutoSupport 2.0 架构简介

在 Appliance 2.7.1 版本中，实现了一个同时适用于客户端和服务器的新架构，以增强 AutoSupport 提升客户支持体验的能力。我们已经创建了一个新客户端框架，可在警报管理、组件监视和软件监视中提供模块化特性。它还支持将来的高级诊断功能。

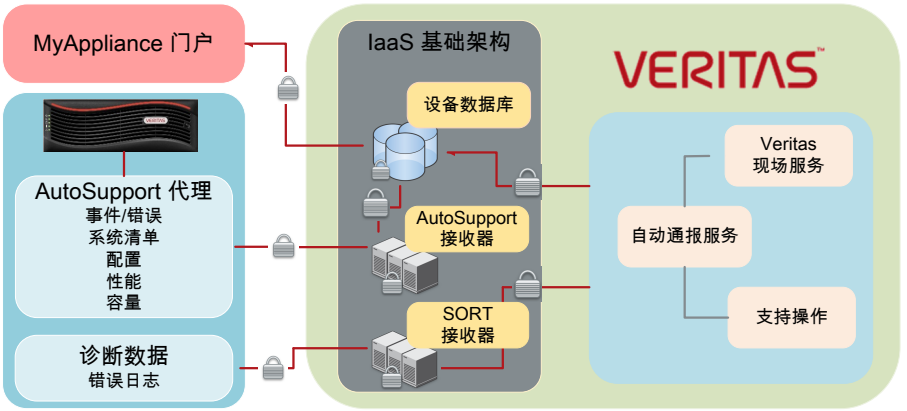
实现了同时适用于客户端和服务器的 AutoSupport 2.0 架构，以增强 AutoSupport 提升客户支持体验的能力。Veritas AutoSupport 引入了一个框架，可在警报管理、组件监视和软件监视中提供模块化特性。它还支持将来的高级诊断功能。

AutoSupport 组件

AutoSupport 技术包含三个主要组件：AutoSupport 客户端代理、AutoSupport 接收程序和 MyAppliance 门户。

下图概述了基本的 AutoSupport 架构。

图 2-1 AutoSupport 2.0 架构



关于 AutoSupport 客户端代理

AutoSupport 客户端代理会不断地监视设备硬件和软件组件。它收集问题诊断数据、系统运行状况数据以及清单数据，并通过 CallHome 基础架构将这些数据安全地传输给 Veritas，以响应关键事件。Veritas Support 使用数据帮助执行诊断和故障排除。

设备硬件监视

“自动通报”功能可监视以下硬件组件：

- CPU
- 磁盘
- 风扇
- 电源
- 环境遥测数据
  - 系统温度
  - 系统电压
  - 风扇速度
  - BBU 充电状态
- RAID 控制器
- RAID 卷组
- 系统温度

- 系统板组件由集成平台管理界面 (IPMI) 和基板管理控制器 (BMC) 芯片组成
- 存储子系统（扩展架和互连）

设备软件监视

软件监视功能基于监视代理的设备型号。

AutoSupport 客户端代理将监视以下特定于应用程序配置和性能的数据。

- 容量利用率
- 固件
- MSDP 性能
- 应用程序版本
- 操作系统软件包
- 修补程序和紧急工程二进制文件 (EEB)

关于 Veritas Appliance 监视基础架构

Veritas Appliance 监视基础架构由两个独立的接收服务器组成：AutoSupport 接收器和 SORT 数据接收器。

Veritas 利用位于美国大陆的托管型基础架构即服务 (IaaS) 设备来承载此基础架构，并具有高度冗余性。

Veritas CallHome Services (CHS) 团队位于三个分布适宜的地理位置：美国、爱尔兰和新加坡，以提供最快的全球事件响应和 24 小时监视。

Veritas Support 包括 Veritas CallHome Services、Veritas Enterprise Support Operations 和 Veritas Field Services，所有这些服务都在全球提供，以实现“全天候式”支持。

当设备将事件数据传输给 Veritas 时，此数据被发送至 Veritas Appliance 监视基础架构服务器。如果发生心跳故障事件，会向 CHS 团队发出警报。设备也会将 `DataCollect` 软件包传输至 SORT 接收器，并打开一个事件票证以追踪状态。CHS 工程师会对事件分类，并确定要执行的步骤。然后，CHS 工程师将问题上报给 Support Operations，或向 Veritas Field Services 分派硬件维修单。

关于 MyAppliance 门户

MyAppliance Web 门户提供集中式注册和支持体验，以及供 Veritas 设备使用的信息存储。您还可以访问最佳做法和其他知识库文章，以及注册和维护设备的管理联系人和位置信息。

注意：无需在MyAppliance门户中注册设备，但它是支持服务流程中的关键步骤。注册后，Veritas可以在已确定设备故障的情况下联系到相应人员，并向正确地点派遣现场服务人员以进行维修。

自动通报数据传输

为了实施支持服务，AutoSupport 客户端代理将传输日常数据，以提供主动性监视和高级诊断服务。这些数据收集和传输分为 4 个主要类别：

- 事件数据
- 配置和清单数据
- 遥测和性能数据
- 诊断数据

以下部分说明了其中每个类别，以及它们的传输时间间隔和基本属性：

事件数据状况

时间间隔：

- 在检测事件（例如硬件或软件故障）之后立即

基本属性：

- 设备模式（主服务器或介质服务器）
- 设备状态（正常或不正常）
- 序列号
- 故障时长
- 固件版本

仅限于故障组件的扩展属性：

- 电池电压级别、充电状态等

系统清单和配置数据

时间间隔：

- 每 24 小时一次

基本属性：

- 所有硬件组件的清单，其中包括：
  - 制造商
  - 型号

  - 序列号
  - 类型
  - 位置
  - 固件
  - 组件供应商提供的特定于组件的其他元数据或属性
- 包括由用户定义的配置状态在内的配置数据：
  - 存储配置
  - 网络信息
  - 功能启用/禁用标志
- 遥测和性能数据：
  - 存储利用率
  - 某些组件的扩展属性，例如，电池电压、充电状态、热传感器数据、风扇速度和电源电压。

DataCollect 软件包

时间间隔：

- 每三天
- 如果在间歇时段检测到故障状态，系统会在 30 分钟内组装 `DataCollect` 软件包，并重置为期三天传输的频率。

完整的诊断和硬件配置清单：

- 操作系统诊断：
  - 系统消息日志 (`/var/log/messages`)
  - `dmesg` 日志
  - 引导日志
  - 磁盘分区利用率（`df -h` 输出）
  - 内存状态信息
  - `iostat` 磁盘性能日志
  - `vmstat` 卷性能日志
  - `vxfsstat` 文件系统性能日志
- IPMI 和机箱硬件：
  - IPMI 警报状态日志

- IPMI 传感器数据
- CPU 诊断数据
- 现场可更换单元 (FRU) 机箱日志

- RAID 控制器：
  - RAID 适配器日志
  - RAID 电池备份单元状态日志
  - LUN 配置数据
- 存储子系统：
  - 磁盘组信息
  - 扩展架诊断
  - 阵列诊断
  - 物理磁盘日志
  - SMART 磁盘诊断
- 修补程序管理：
  - 修补程序安装日志

3

“自动通报”安全功能

本章节包括下列主题：

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传输的所有 AutoSupport 数据，以及在客户端内部不同组件之间传输的数据通信：

- AES-128/256/384加密
- RSA-1024/2048 加密
- SHA-256/384 证书身份验证
- 通过 443/tcp 端口由 HTTPS PUT 进行的 TLS 加密传输

注意：软件版本为 2.6.1.x 的 NetBackup Appliance 仅支持 SHA-1 证书身份验证。技术文章 000108230 对此问题进行了记录。按照文档中的说明升级您的设备，以实现对 SHA-256 证书身份验证的“自动通报”支持。

“自动通报”数据的传输方式

所有从设备传输到 Veritas 的数据都是由 HTTPS PUT 通过端口 443/tcp 以 TLS 加密传输方式完成的。

注册数据会发送至 https://api.appliance.veritas.com

“自动通报”数据会发送至 https://receiver.appliance.veritas.com。

`DataCollect` 软件包会发送至 https://sort.veritas.com。

注意：如果您在设备上配置代理服务器，则代理必须接受上述 URL 的连接，这样 AutoSupport 平台才能工作。

基础架构包括一组具有混合的静态和动态 IP 池的端点，用于负载平衡和高可用性。注册和自动通报数据具有静态 IP 池，而 `DataCollect` 软件包传输端点具有动态 IP 池。Veritas 强烈建议在代理和/或防火墙级别使用 DNS 或完全限定的主机名解析置备，以减少可能的服务中断的机会。

请确保在设备、代理和/或防火墙上启用到以上 URL 的出站 443/TCP TLS 套接字连接。

有关自动通报数据传输基础架构的更多信息，请参见 Veritas 支持网站上的以下技术文章：

https://www.veritas.com/support/en_US/article.000126756

如何接收和存储“自动通报”数据

所有传输到 Veritas 的数据都存储在位于美国大陆的托管型 IaaS 基础架构中。

只有获授权的特定支持和工程人员才能通过已经过验证、审核或控制的方式访问这些数据。

“自动通报”数据的维护和存储时间长度

Veritas 会在每台计算机的生命周期内维护为该计算机收集的数据，此时间通常是 5-7 年。超过此时间后，数据可能会被汇总和匿名，以进一步用作内部研发。

数据隐私

Veritas AutoSupport 将收集一些可能会被客户视为敏感数据的有限的配置数据，例如，设备主机名和 IP 地址。收集此类数据仅仅是为了向 Veritas 技术支持人员提供

用于故障排除的更多环境信息。Veritas 将以客户的观点来对待此类数据，并采取严格的安全实践来保护这些数据。

有关 Veritas 如何管理客户隐私的更多信息，请访问 https://www.veritas.com/about/privacy/。

4

配置 AutoSupport 客户端设置

本章节包括下列主题：

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

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

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

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

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

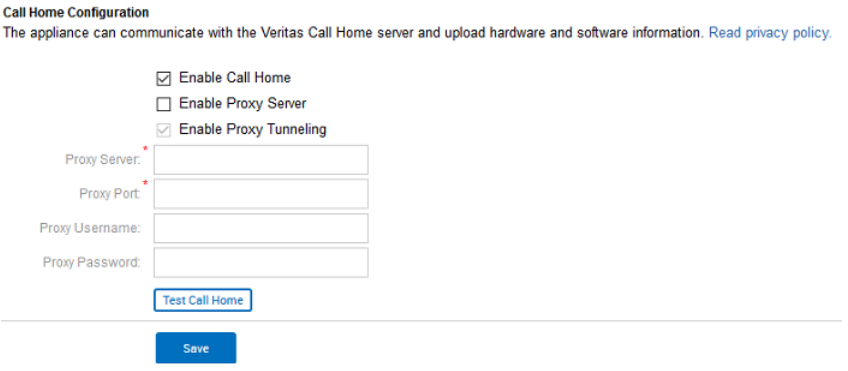
从 NetBackup Appliance Web Console 启用和禁用“自动通报”功能

以下过程说明了如何使用 NetBackup Appliance Web Console 启用和禁用 NetBackup Appliance 上的“自动通报”功能。

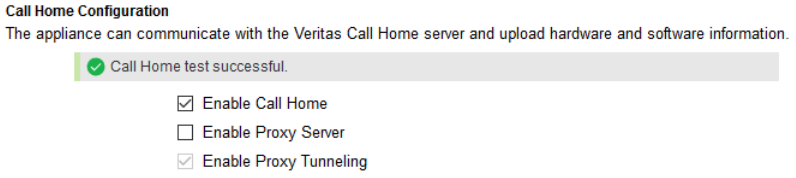
从 NetBackup Appliance 网页操作界面中配置 52xx 设备上的“自动通报”功能

1 登录到 NetBackup Appliance 网页操作界面，并导航至“设置”>“通知”>“警报配置”页面。

2 选中“**启用自动通报**”复选框。



3 要测试“自动通报”功能，请单击屏幕下方的“测试自动通报”。系统会尝试将心跳软件包推送到 Veritas。成功之后，将出现以下消息：



4 单击“保存”。

设置 > 通知 > 警报配置

“**设置**”>“**通知**”>“**警报配置**”页面为您提供了可启用 SNMP、SMTP 和自动通报警报通知的一个位置。页面将划分为三个部分。每个部分专用于提供 **SNMP**、**SMTP**和“**自动通报**”警报通知的详细信息。

在“**警报配置**”下是“**通知间隔**”字段。您必须为 SNMP 和 SMTP 配置输入两个后续通知之间的时间间隔（分钟）。时间间隔应是 15 的倍数，且不得为 0。

配置 SNMP

表 4-1 列出了 **SNMP**（简单网络管理协议）部分中的字段。

表 4-1 SNMP 服务器配置设置

字段	描述
启用 SNMP 警报	选中此复选框可启用 SNMP 警报配置。
SNMP 服务器	输入 SNMP 服务器主机名。您可以输入主机名或 IP 地址来定义该计算机。IP 地址可以是 IPv4 或 IPv6 地址。仅允许使用全局范围 IPv6 地址和唯一本地 IPv6 地址。 在设备中生成的警报通知或陷阱通知将发送到此 SNMP 管理器。 **注意：** NetBackup appliance 支持市场上的所有 SNMP 服务器。但是，ManageEngine™ SNMP 服务器和 HP OpenView SNMP 服务器已通过 2.6 版的测试和认证。
SNMP 端口	输入 SNMP 服务器端口号。如果您不为此变量输入任何值，则默认端口为 162。 **注意：** 您的防火墙必须允许此设备通过此端口访问 SNMP 服务器。
SNMP 团体	输入接收警报或陷阱的团体。例如，备份报告部门。 可以输入在 SNMP 服务器上配置的值。例如，您的公司名称。如果您不希望披露公司名称，Veritas 提供了系统定义的值，其中包括：`admin_group`、`public` 和 `private`。如果您不输入任何值，则默认值为 `public`。

SNMP MIB 文件充当用于汇编和解译 SNMP 邮件的数据字典。如果配置了 SNMP，则必须将 MIB 文件导入到监视软件中，以便该软件可以解释 SNMP 陷阱。您可以从“服务器配置”窗格检查 SNMP MIB 文件的详细信息。要检查有关 SNMP MIB 文件的详细信息，请单击“**查看 SNMP MIB 文件**”。SNMP MIB 文件将打开。

有关如何在配置后发送测试 SNMP 陷阱的信息，请参见 Veritas 支持网站上的以下技术文章：

www.veritas.com/docs/TECH208354

配置 SMTP

SMTP 邮件服务器协议用于传出电子邮件。您可以从 NetBackup Appliance Web Console（“设置”>“警报配置”>“SMTP 服务器配置”）配置 SMTP。

您也可以在设备的 Shell 菜单中使用以下命令对 SMTP 服务器进行配置并添加一个新的电子邮件帐户：

`Main_Menu > Settings > Alerts > Email SMTP Add` *`Server`* `[Account] [Password]`，其中 *`Server`* 是用于发送电子邮件的目标 SMTP 服务器的主机名。`[Account]` 和 `[Password]` 是可选参数，用于确定帐户名和帐户密码（如果需要进行身份验证）。

有关详细信息，请参见设备的相关客户文档。

表 4-2 列出了 NetBackup Appliance Web Console的 **SMTP** 部分中的字段。

表 4-2 SMTP 服务器配置设置

字段	描述
SMTP 服务器	输入 SMTP（简单邮件传输协议）服务器主机名。使用该 SMTP 服务器发送设备中生成的警报通知。IP 地址可以是 IPv4 或 IPv6 地址。仅允许使用全局范围 IPv6 地址和唯一本地 IPv6 地址。
软件管理员的电子邮件地址	输入软件管理员的电子邮件 ID 以接收特定于 Veritas NetBackup Appliance 软件的软件警报。指定的电子邮件 ID 接收以下软件条件的警报： ■ 主机信息，如： 　■ 磁盘信息。 　■ 总体备份状态。 　■ 每个客户端最近七次备份的结果。 ■ 您的目录库备份灾难恢复文件的电子邮件。 ■ 修补程序安装成功报告。
硬件管理员的电子邮件地址	输入硬件管理员的电子邮件 ID 以接收特定于 Veritas NetBackup 硬件设备的硬件警报。例如，输入 hardwareadmin@usergroup.com。
电子邮件测试	测试电子邮件将发送到上述配置的电子邮件地址。如果未收到测试电子邮件，请按照错误提示检查网络连接、SMTP 设置和电子邮件设置，或与系统管理员联系，以获取更多帮助。
发件人电子邮件	输入电子邮件 ID 以接收设备发送的任何警报或报告的答复。
SMTP 帐户	输入用户名以访问 SMTP 帐户。
密码	输入上述 SMTP 用户帐户的密码。

您可以将此服务器配置为向代理服务器或 Veritas 自动通报服务器发送电子邮件报告。

以下内容介绍了支持的代理服务器：

- Squid
- Apache
- TMG

注意：还支持代理配置中的 NTLM 身份验证。

从 NetBackup appliance 2.6.1.1 开始，由设备生成的所有电子邮件通知现在均使用相同的 SMTP 设置。这些电子邮件包括硬件监控通知和 NetBackup 作业通知。配置设置位于 NetBackup Appliance Web Console中的“**设置**”>“**通知**”>“**警报配置**”下或 NetBackup Appliance Shell Menu中的 `Main_Menu > Settings > Alerts` 下。这些设置覆盖您之前可能已用于发送 NetBackup 作业通知的任何先前的 SMTP 设置。

注意：如果在升级到 NetBackup appliance 2.6.1.1 之前已经配置了设备 SMTP 设置，则可能需要重新保存配置，以使 NetBackup 能够使用设置。在 NetBackup Appliance Web Console中，转至“**设置**”>“**通知**”>“**警报配置**”并单击“**保存**”。或者在 NetBackup Appliance Shell Menu中，转至 `Main_Menu > Settings > Alerts` 并重新提交 `SMTP` 和 `SenderID` 设置。

配置自动通报

表 4-3 列出了“**自动通报配置**”部分中的字段。

表 4-3 自动通报配置设置

字段	描述
启用自动通报	选中此复选框可启用自动通报警报配置。
启用代理服务器	选中此复选框可启用代理。
启用代理隧道	如果您的代理服务器支持 SSL 隧道，请选中此复选框。
代理服务器	输入代理服务器的名称。
代理端口	输入代理服务器的端口号。
代理用户名	输入登录代理服务器的用户名。
代理密码	输入登录代理服务器的用户名的密码。

当启用自动通报时，可以通过单击自动通报配置设置下的“**测试自动通报**”选项测试自动通报是否正在正确运行。

注意：只有当启用自动通报时，NetBackup Appliance Web Console上的“**测试自动通报**”选项才处于活动状态。

以下内容介绍了支持的代理服务器：

- Squid
- Apache
- TMG

NTLM 是“自动通报”代理设置支持的身份验证方法。

配置警报配置设置

本节介绍了使用“**设置**”>“**通知**”>“**警报配置**”页面配置SNMP、SMTP 和自动通报服务器设置的过程。

配置 SNMP、SMTP **和自动通报服务器设置**

1 登录到 NetBackup Appliance Web Console。

2 单击“**设置**”>“**通知**”>“**警报配置**”。

此时系统将显示“**警报配置**”页面。

“**警报配置**”页面分为三个部分，用于启用**SNMP**、**SMTP** 和**自动通报**以及提供相关详细信息。

3 对于**SNMP**、**SMTP** 和“**自动通报**”警报配置，请在“**通知间隔**”字段中输入两次后续通知之间的时间间隔（分钟）。

4 在提供的字段中输入 SNMP 设置。表 4-1 中提供了 SNMP 参数的说明。

5 在提供的字段中输入 SMTP 设置。表 4-2 中提供了 SMTP 参数的说明。

设备使用全局服务器设置将电子邮件通知发送到您指定的 SMTP 服务器。

6 在提供的字段中输入自动通报设置。表 4-3 中提供了自动通报参数的说明。

7 单击“**保存**”以保存 SNMP、SMTP 和自动通报设置。

5

配置 MyAppliance 门户

本章节包括下列主题：

配置 MyAppliance 门户

MyAppliance 门户已经与 MyVeritas 门户集成，可以通过 https://my.appliance.veritas.com 或 https://my.veritas.com 直接访问。在任一情况下，如果您没有用户帐户，可以在门户上单击“**立即注册**”，以注册新的 Veritas 帐户管理器 (VAM) 用户帐户。VAM 凭据还允许您访问 MyVeritas、MySupport、客户关怀以及其他 Veritas 门户网站。

在验证 VAM 凭据之后，可导航至“**设备**”选项卡以访问 MyAppliance Web 门户。您可以在此处注册设备，查看和编辑已注册的现有设备，以及检查心跳数据。

有关 MyAppliance 门户的更多信息，请访问 https://my.appliance.veritas.com。

注册设备

设备注册集中在 MyAppliance 门户中。

要使 Veritas 能够帮助您最大程度地提高设备可用性以及提供主动型监视服务，必须注册您的设备。注册过程为 Veritas 提供准确的联系人详细信息和具体的站点信息，这有助于加快实现支持、现场服务和客户故障通知。

注册后，您还可以访问设备的其他报告功能，如：

- 关于所有已注册的设备的概述信息

- 容量和利用率详细信息
- 能够更新联系人信息和站点信息

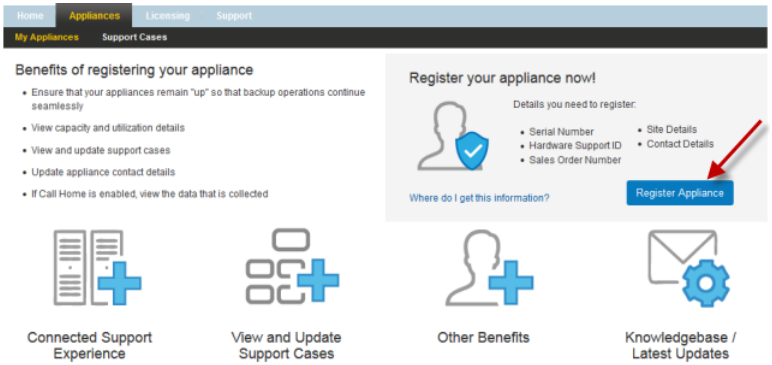
注册之后，您将收到关于您设备的产品更新及其他重要信息的提醒。

如果您的设备可以直接访问或通过代理访问 Internet，则会自动填写注册详细信息。如果设备未置备，则会显示验证和更新设备注册信息的消息。

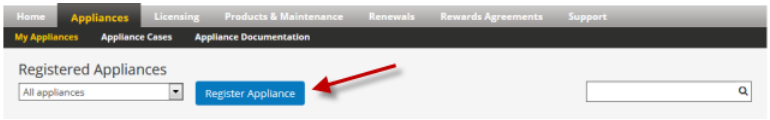
从 MyAppliance 门户中注册设备

1 登录至 MyAppliance 门户，然后使用以下方法之一开始注册过程：

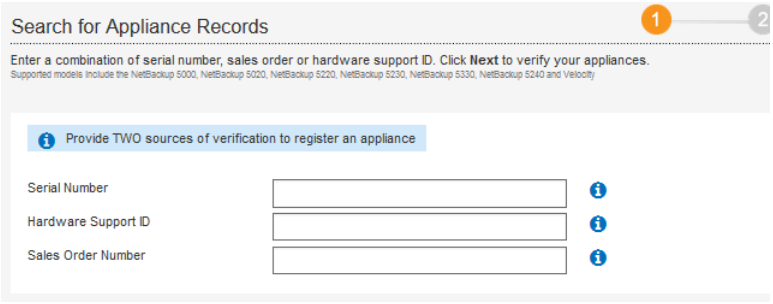
- 如果您是首次访问该门户，则会出现一个信息页面。单击“**注册设备**”。



- 如果之前已在帐户中注册设备，请导航到“**设备**”>“**我的设备**”页面，然后单击“**注册设备**”。

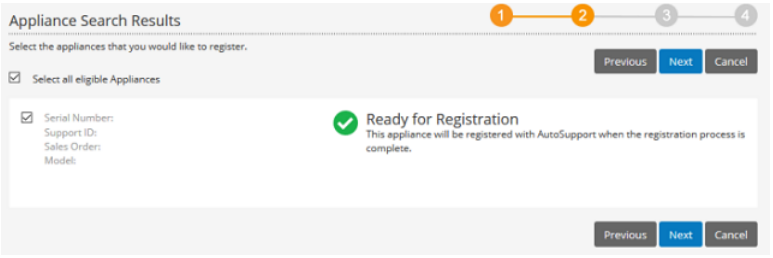


2 输入验证源。注册设备时只需要两个源。



3 单击“**下一步**”启动搜索。

4 选择要注册的设备。



5 单击“**下一步**”输入“**注册新设备**”页面。

注意：要进行注册，必须输入任何带星号的突出显示字段。只有在输入必需的信息之后，才移到下一步。

---

6 在基本信息列中，输入您的公司名称。

7 在“**设备位置**”列中，单击“**添加新站点**”按钮，以创建新站点。

8 在弹出对话框中，输入站点名称、站点地址和其他信息。

9 在“**选择站点**”字段中，选择已创建的站点。

10 在“**联系信息**”列中，单击“**添加新联系人**”按钮以创建新的主要联系人。

11 在弹出对话框中，输入联系人的姓名、电子邮件地址、电话号码和其他信息。

12 在“**选择联系人**”字段中，选择已创建的联系人。

注意：默认情况下，“**接收自动通报传输故障警报**”选项处于选中状态，以便在 Veritas 超过 28 小时没有收到有效的自动通报数据传输的情况下发出警报。警报每隔 24 小时重复一次，直到收到有效的数据传输。

该选项仅供具有 2.7.1 和更高版本软件的 NetBackup 设备使用。

如果启用了垃圾邮件过滤，则将过滤设置配置为允许来自以下发件人 ID 的电子邮件：appliance.veritas.com。

如果您不再希望在发生自动通报传输故障时从 Veritas 接收警报，请取消选中该选项。

---

13 验证信息，然后单击“**提交**”。

将弹出通知，告知您设备已注册成功。

手动更新设备信息

注册设备时，应将包括主机名和版本在内的信息更新到门户。如果未显示此类设备信息，请尝试以下操作手动进行更新。

1 验证您的设备能否直接访问或通过代理访问 Veritas 服务器。

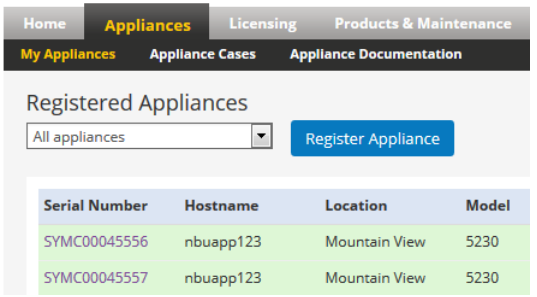
2 使用 NetBackup Appliance Shell Menu中的 `Settings > Alerts > CallHome Test` 命令验证是否已启用自动通报。

3 使用 NetBackup Appliance Shell Menu中的 `Support > Collect Inventory` 命令手动更新设备信息。

获取心跳软件包和 DataCollect 软件包的副本

获取心跳软件包的副本

1 登录到 MyAppliance 门户，然后从已注册系统的列表中选择所需设备。

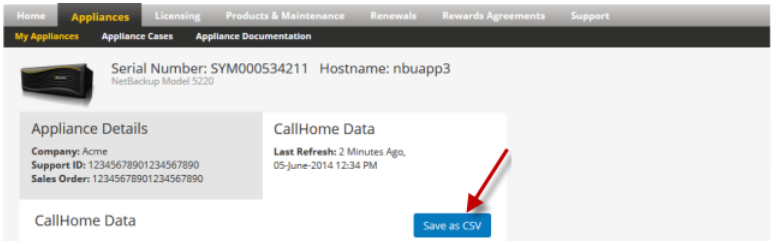


2 单击序列号可管理设备。

在“设备管理”页面中，您可以查看两个选项卡，包括“**设备详细信息**”和“**自动通报数据**”。

3 单击“**自动通报数据**”选项卡以查看心跳数据。“**上次刷新时间**”字段显示上次心跳数据传输的时间戳。

您还可以单击“**另存为 CSV**”，将数据副本导出为以逗号分隔的值列表。



获取 DataCollect 软件包的副本

1 登录到 Appliance Shell Menu，然后运行 `Support > DataCollect` 命令。数据收集过程需要几分钟时间。完成后，会返回以下消息：

```
All logs have been collected in /tmp/DataCollect.zip
```

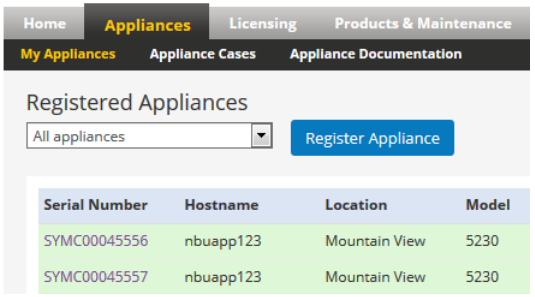
2 使用 `Support > Logs > Share Open` 命令检索软件包文件。

取消注册设备

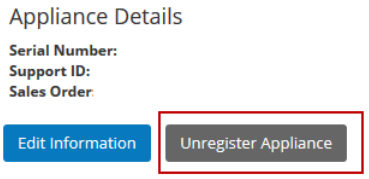
如果已从环境中解除授权或删除某个设备，则您可以从 MyAppliance 门户的“**设备**”>“**我的设备**”页面中取消注册该设备。

取消注册设备

1 从“**设备**”>“**我的设备**”页面中，单击要取消注册的设备。



2 在显示的设备“**详细信息**”页面中，单击“**取消注册设备**”。



3 将出现一个确认弹出窗口。单击“**确认取消注册**”。

6

NetBackup 产品改进计划

本章节包括下列主题：

关于 NetBackup 产品改进计划

NetBackup 产品改进计划允许 NetBackup 定期收集部署和使用情况数据。所收集的信息可帮助确定客户对 NetBackup 的部署和使用方式。例如，所收集的数据可帮助确认最常用的功能以及这些常用功能的使用方式。通过使用汇总的数据，NetBackup 开发和支持服务团队可以计划针对易用性、性能、安装过程和许多其他产品方面的产品改进。

默认情况下，NetBackup 设备可使用默认 AutoSupport“自动通报”功能参加产品改进计划。如果禁用“自动通报”功能，将同时禁用针对产品遥测数据的扩展收集功能。

所收集和传输的数据包括以下部署信息和使用情况信息：

部署信息：

- 每个服务器的硬件和软件配置详细信息：
  - IP 地址、IP 类型
  - 完全限定域名 (FQDN)

    - 别名、主机名、主机 ID、平台和架构
- CPU 名称、类型、时钟速度等
- 时区
- 环境语言
- 操作系统版本级别
- 内存大小
- 授权的 NetBackup 软件版本
- 授权的 NetBackup 软件功能和已安装软件包
- 已安装的其他 Veritas 软件包
- NetBackup Appliance 部署信息

使用情况信息：

- 按策略类型和平台分类的客户端计数
- 按 NetBackup 版本和平台分类的介质服务器计数
- 按策略类型分类的策略计数
- 按介质保留级别分类的介质计数
- 按操作类型分类的存储生命周期策略 (SLP) 计数

Veritas 对 NetBackup 产品改进计划数据的使用方式

通过产品改进计划收集的信息将通过安全渠道定期自动异步传输到 Veritas。

Veritas 将所收集的信息用于内部统计产品部署分析，以实现以下目标：

- 确定和分析汇总安装库中的趋势和比较。
- 了解 NetBackup 授权软件产品硬件和软件部署配置。
- 改进 Veritas 产品和服务。
- 加强技术支持问题研究。

NetBackup 产品改进计划数据的传输方式

NetBackup 产品改进计划通过端口 443/tcp 使用安全套接字层 (SSL) 进行通信。系统需要能够访问主机 https://telemetry.veritas.com。

通信流示例

1 测试访问权限，打开用于访问 https://telemetry.veritas.com 的端口

2 在 /data/uploader/nbupload.conf 上执行 HEAD 请求

3 在 /data/uploader/nbupload.conf 上执行 GET 请求

4 在 /uploader/submit/nb 上执行 POST 操作

客户端系统初始化所有通信。当设备请求的数据托管在遥测系统上时，某些通信是双向通信。

例如，GET 请求能够动态更新收集程序参数，而不需要安装或更新标准的软件包或版本。这些动态更新只限于收集程序更新，该过程不会向客户端部署任何其他代码。最典型的更新是收集程序参数中的变更，例如命令标志或添加运行 NetBackup 命令以收集其他配置和运行时间信息。

数据隐私

Veritas NetBackup 产品改进计划既不会跟踪个人验证信息，也不会传输有关受软件保护的特定数据的信息。要了解我们收集或处理哪些关于您的信息，以及当您使用 Veritas NetBackup Appliance 时我们是如何处理这些信息的，请参见 Veritas NetBackup Appliance 隐私声明。

如果您要检查发送至 Veritas 的数据，此数据位于设备的 root 文件系统中：

/var/symantec/telemetry/telemetry<timestamp><randomstring>/DATA/nb-install/1/telemetry_data.json

例
如，/var/symantec/telemetry/telemetry20140224103 1WdH/DATA/nb-install/1/telemetry_data.json

也可以使用 MyAppliance 门户检查发送至 Veritas 的“自动通报”数据。

请参见第 28 页的“获取心跳软件包和 DataCollect 软件包的副本”。

启用或禁用 NetBackup 产品改进计划

默认情况下，在安装 NetBackup 集成设备后，NetBackup 产品改进计划会自动启用。可通过两种方式禁用产品改进计划：

- 通过禁用“自动通报”功能
  默认情况下，NetBackup 产品改进计划与“自动通报”启用功能相关联。要启用或禁用产品改进计划，请启用或禁用“自动通报”功能。

注意：建议不要禁用“自动通报”功能，因为这不仅会影响设备向 Veritas 报告错误状况的能力，也会延迟故障情形中的修复时间。

- 通过编辑 bpsetconfig 文件
  要编辑 bpsetconfig 文件，请以 NetBackupCLI 用户身份登录 NetBackup Appliance Shell Menu，并运行以下命令：
  /usr/openv/netbackup/bin/bpsetconfig -set TELEMETRY_UPLOAD=NO
  该属性存储在 /usr/openv/netbackup/bp.conf 中

注意：由于 NetBackup 产品改进计划也与“自动通报”启用功能相关联，因此在任何时候禁用或启用“自动通报”功能都会将 TELEMETRY_UPLOAD 值重置为出厂默认状态。

NetBackup 产品改进计划代理配置

NetBackup 产品改进计划支持各种代理配置。

为设备上的产品改进计划配置代理

1 请以 NetBackupCLI 用户身份登录至 NetBackup Appliance 命令行操作界面，并运行以下命令：

```
/usr/openv/netbackup/bin/nbtelemetry
```

2 使用以下命令完成配置：

`--proxy-server=SERVER:PORT`	指定要在上传过程中使用的代理服务器。 例如，http://proxy.example.com:8080。
`--proxy-username=USERNAME`	指定要在上传过程中用于代理服务器中的用户名称（如果需要）。
`--proxy-password=PASSWORD`	指定要在上传过程中与用户名称一起使用的密码（如果需要）。

3 完成代理配置后，请确保代理服务器设置允许来自以下 URL 的连接：

- https://receiver.appliance.veritas.com（设备注册日期）
- https://sort.veritas.com（DataCollect 软件包）

附录 A

常见问题

本附录包括下列主题：

常见问题

哪些 Veritas 设备可支持 Veritas AutoSupport 功能？

目前已在下列设备上实现 Veritas AutoSupport 功能：

- Veritas NetBackup 50xx 重复数据删除设备，软件版本 D1.2 或更高版本
- Veritas NetBackup 52xx 和 5330 Appliance，软件版本 2.7.1 或更高版本
- Veritas Backup Exec 3600 Appliance，软件版本 2.0.189 或更高版本

注意：可将较早软件版本上运行的设备升级到特定于设备的最新软件版本，以获取主动型硬件监视功能。

Veritas AutoSupport 是免费服务吗？

是的。Veritas AutoSupport 包含在与设备一起购买的维护服务中，不需要额外的费用。Veritas AutoSupport 旨在改进注册和提升设备客户的支持体验。AutoSupport 的长期任务是向 Veritas 设备提供高可靠性，可用性和可维护性。

AutoSupport 是否允许执行远程更改，或监视设备上的任何进程、操作或功能？

当前设备版本不提供任何远程访问功能或配置更改功能。

设备在连接到 AutoSupport 服务时是否会验证任何证书吊销列表 (CRL)？

Veritas 不会验证客户端的证书，因为它们是自签名证书。

AutoSupport 服务证书是否由受信任的证书颁发机构颁发?

Veritas VeriSign™ 对 AutoSupport 所使用的 URL 采用由 Symantec VeriSign™ Root Authority 颁发的证书。

设备是否支持本地根证书颁发机构，这样就可以拦截并扫描设备，然后阻止 HTTPS 流的内容?

否。Veritas 设备不支持任何本地证书颁发机构。

“自动通报”进程是否可以提交任何存储在 NetBackup 目标卷上的数据?

否。“自动通报”数据收集程序仅会查看卷的性能元数据，不会检查存储在卷上的数据的内容。

您能确保文件不会从设备上复制或传输出去吗?

此系统旨在清除指定目录结构中的要在 `DataCollect` 进程中打包的文件。文件也可复制到目录结构，然后传输到 Veritas。但是，该进程的计时非常精准，因此数据在传输前不会存储。

“自动通报”是否仅限于出站的连接?

是的。“自动通报”是仅限于出站的连接。