

Veritas NetBackup™ 高可用性环境管理指南

Windows、UNIX 和 Linux

版本 8.2

VERITAS™

Veritas NetBackup™ 高可用性环境管理指南

法律声明

Copyright © 2019 Veritas Technologies LLC. © Veritas Technologies LLC 版权所有。All rights reserved. 保留所有权利。

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

本产品可能包括 Veritas 必须向第三方支付许可费的第三方软件（以下称“第三程序”）。部分第三程序会根据开源或免费软件许可证提供。软件随附的授权许可协议不会改变这些开源或免费软件许可证赋予您的任何权利或义务。请参考此 Veritas 产品随附的或以下链接提供的第三方法律声明文档：

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

本文档中介绍的产品根据限制其使用、复制、分发和反编译/逆向工程的许可证进行分发。未经 Veritas Technologies LLC 及其许可方（如果存在）事先书面授权，不得以任何方式任何形式复制本文档的任何部分。

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

无论由 Veritas 作为内部服务还是托管服务提供，根据 FAR 12.212 中的定义，授权许可的软件和文档被视为“商业计算机软件”，受 FAR Section 52.227-19 “Commercial Computer Software - Restricted Rights”（商业计算机软件受限权利）和 DFARS 227.7202 等

“Commercial Computer Software and Commercial Computer Software Documentation”（商业计算机软件和商业计算机软件文档）中的适用规定，以及所有后续法规中规定的权利的制约。美国政府仅可根据本协议的条款对授权许可的软件和文档进行使用、修改、发布复制、执行、显示或披露。

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

技术支持

技术支持负责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

请确保您的文档是最新版本。每个文档在第 2 页显示上次更新日期。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：

NB.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，提供的信息和工具有助于自动处理及简化某些耗时的管理任务。根据具体产品，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

第 1 章	预防单一故障点的 NetBackup 保护	6
	关于预防组件故障	6
	关于预防网络链路故障	7
	关于预防存储设备连接故障	8
	关于预防存储设备故障	8
	关于预防介质可用性故障	9
	关于预防主服务器故障	10
	关于预防介质服务器故障	10
	关于预防 LAN 客户端故障	13
	关于预防 SAN 客户端故障	13
	关于预防站点故障	13
	关于在高可用性环境中保护目录库	14
第 2 章	关于使用目录库备份和恢复进行的站点灾难恢复	15
	灾难恢复软件包	15
	关于目录库恢复	16
	关于完全目录库恢复	16
	执行完全目录库还原	17
	在执行完全目录库还原后使 DR 环境一致	20
	关于部分目录库恢复	20
	执行部分目录库还原	21
	在执行部分目录库还原后使 DR 环境一致	22
	关于 DR 域中的磁盘恢复	22
	单域复制 DR 环境中的磁盘恢复	22
	自动映像复制	22
	跨域复制 DR 环境中的磁盘恢复	22
第 3 章	关于使用自动映像和目录库复制进行的站点泄露 保护	24
	关于自动映像复制 (AIR)	24
	关于 NetBackup 目录库复制	24
	关于复制的 NetBackup 目录库的支持条件	25
	关于目录库同步	26

	关于多站点单域复制	26
	关于多站点跨域复制	29
	关于完全目录库复制	31
	关于部分目录库复制	33
第 4 章	使用完全目录库复制部署 NetBackup 主服务器	36
	关于复制注意事项	36
第 5 章	在群集中使用 NetBackup 执行备份和还原	38
	关于在群集中使用 NetBackup 执行备份和还原	38
	在群集中使用 NetBackup 执行用户控制的备份	38
	关于在群集中还原数据	39
	关于群集中支持的 NetBackup 应用程序代理	40
	关于在群集中备份数据库文件	41
	关于用户备份	41
	关于群集中的 NetBackup 客户端	41
索引	43

预防单一故障点的 NetBackup 保护

本章节包括下列主题：

- [关于预防组件故障](#)
- [关于预防站点故障](#)
- [关于在高可用性环境中保护目录库](#)

关于预防组件故障

NetBackup 由许多不同的组件构成，其中每个组件都有可能发生故障，从而中断备份或还原过程。

表 1-1 列出了组件级的故障点和相关保护方法。

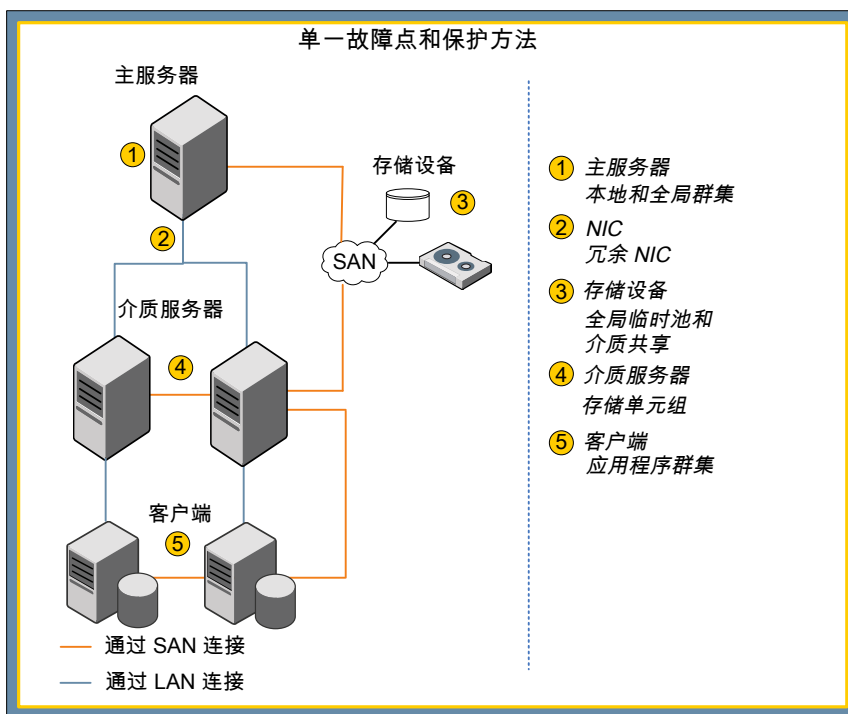
表 1-1 预防组件故障的 NetBackup 保护

故障点	保护方法
网络链路	请参见第 7 页的 “关于预防网络链路故障” 。
存储设备连接	请参见第 8 页的 “关于预防存储设备连接故障” 。
存储设备	请参见第 8 页的 “关于预防存储设备故障” 。
介质可用性	请参见第 9 页的 “关于预防介质可用性故障” 。
主服务器	请参见第 10 页的 “关于预防主服务器故障” 。
介质服务器	请参见第 10 页的 “关于预防介质服务器故障” 。
LAN 客户端	请参见第 13 页的 “关于预防 LAN 客户端故障” 。

故障点	保护方法
SAN 客户端	请参见第 13 页的“关于预防 SAN 客户端故障”。

图 1-1 显示了各个 NetBackup 组件和各单一故障点。使组件高度可用，或者部署多个组件以实现冗余，即可在各组件级消除各单一故障点。

图 1-1 单一故障点和保护方法



关于预防网络链路故障

大部分备份通信通过速度为 100 MB 和 1Gb 的网络连接（传输速率分别为 8 MB/秒和 65 MB/秒）进行传输。要使网络链路高度可用，请部署冗余网络合作。由于成本方面的因素，网络合作往往仅限于备份服务器和任务关键型客户端。非任务关键的客户端使用单一网络连接，可以承受连接故障（以及随后的备份失败）带来的风险。

关于预防存储设备连接故障

到存储设备及其控制器的连接还表示单一故障点。如果出现连接故障，将无法使用设备。

请参见第 8 页的“[关于预防 SAN 连接故障](#)”。

请参见第 8 页的“[关于预防机械手控制连接故障](#)”。

关于预防 SAN 连接故障

尽管 NetBackup SAN 客户端也支持客户端到介质服务器的 SAN 连接，但是 SAN 连接通常存在于备份服务器与备份存储之间。在任何情况下，要保护 NetBackup 不受 SAN 连接故障的影响，应将 SAN 配置为在源组件与目标组件之间提供冗余连接。

大多数 SAN 挂接的磁盘阵列具有冗余的 SAN 连接并且支持动态多路径 (DMP) 软件。此冗余可确保即使有一个路径出现故障也能保持与存储的连接。在许多情况下，DMP 软件还对 SAN 连接的通信量进行负载平衡，以提高流向和来自磁盘存储的数据的传输速率。

许多 SAN 挂接的磁带设备还将提供两个连接以实现冗余，因此依服务器来看它们就像两个独立的设备。多路径选择不是动态的。NetBackup 选择其找到的第一个可用路径，并始终使用该路径。仅当第一个路径损坏时才使用第二个设备路径。

关于预防机械手控制连接故障

在基于磁带的备份环境中，机械手控制连接可能是单一故障点。即使磁带驱动器可用，如果无法将指令发送至磁带库，也将阻止备份和还原操作。

某些磁带库（如 Sun STK ACSLS 或 Quantum ATM）使用在独立于库的服务器上运行的专用控制软件。可以对此类控制服务器构建群集。介质服务器将请求发送至控制服务器，该控制服务器会处理库中槽和驱动器之间的磁带移动。

其他磁带库依赖于从控制指令的 NetBackup 主服务器到库的直接设备连接。如果此设备连接丢失，则无法使用磁带库。SAN 挂接的磁带库支持到机械手控制的多个连接以实现冗余。您可以配置这些连接以预防服务器故障。例如，您可以配置一个到群集主服务器的每个节点的路径。必须确保路径不会同时处于活动状态。如果两个路径同时处于活动状态，则会发出冲突的指令，从而可能导致备份失败或数据丢失。

关于预防存储设备故障

不论是磁带还是磁盘，当存储设备发生故障时，便会将其看作单一故障点。要防止存储设备发生故障，您应该将多台设备作为备份目标。

如果磁带驱动器发生故障，那么仅具有一个磁带驱动器访问权限的介质服务器无法完成磁带的备份。要保护 NetBackup 不受此类故障的影响，请将介质服务器配置为

至少访问两个磁带驱动器。使用可在介质服务器间共享的 SAN 挂接的磁带驱动器。此共享将确保不需要大量冗余设备就可以访问磁带驱动器。通常，一个或两个冗驱动器可提供弹性，并允许在备份进行时执行还原操作。例如，如果将四台介质服务器配置为共享五个磁带驱动器，那么即使有一台驱动器发生故障也仍然可以进行备份。此备份可能会花费更长时间，但可以完成并保证数据安全。如果介质服务器在不同时间运行备份，那么磁带驱动器与服务器的比可能会更低，从而不会冒备份失败的风险。

可以在单个介质服务器上创建 AdvancedDisk 磁盘池，以保护其不受单个磁盘设备故障的影响。

关于预防介质可用性故障

在基于磁带的备份解决方案中，若无合适的磁带介质可用于备份作业，就可能发生故障。借助 NetBackup，通过全局临时池和介质共享可降低此类故障的风险。

表 1-2 介绍了预防介质可用性故障的保护方法。

表 1-2 预防介质可用性故障的 NetBackup 保护

保护方法	描述
全局临时池	<p>对于所有写入磁带的备份作业和复制作业，请使用位于与备份数据具有相同保留条件的特定介质池中的磁带。若无合适的磁带可用，备份将失败。</p> <p>全局临时池是一个 NetBackup 介质池，用于保留可按需自动重新分配到特定介质池的未分配磁带。例如，备份或复制作业处于运行状态，但作业指定的介质池中无合适的磁带可用。此时，未分配的磁带会从全局临时池转移到指定的介质池并用于备份作业。当此磁带失效时，将被自动返回到全局临时池中供重复使用。</p> <p>使用全局临时池可确保所有未分配磁带都可供任何备份作业使用，不论作业指定了哪个介质池。</p>
介质共享	<p>介质共享允许多台介质服务器使用部分已满磁带，直到这些磁带已满为止。这可确保最有效地利用磁带。一次只能有一台介质服务器写入磁带。当该磁带不在使用中时，需要介质池中磁带的其他介质服务器就可以使用它。</p> <p>要启用介质共享，请将“卷池”属性设置为使用“部分已满介质的最大数目”属性。此属性限制介质池中部分已满磁带的数量。除非所有磁带已满，否则无法将空磁带分配到该池。除非某个磁带已满，否则无法将另一个空磁带分配到该池。</p>

关于预防主服务器故障

每个 NetBackup 域的一台主服务器控制该域中的所有备份活动。因此，该主服务器代表了数据保护环境中最明显的单一故障点。没有主服务器，备份和还原就无法进行。要在发生此类故障时保护 NetBackup，主服务器必须采用高可用性配置。

《NetBackup 群集主服务器管理指南》中提供了有关使用这些群集技术安装和配置 NetBackup 的更多信息。

https://www.veritas.com/support/zh_CN/article.DOC5332

在虚拟机上运行的主服务器可以使用虚拟机管理程序的高可用性工具进行保护。有关详细信息，请参考 <http://www.veritas.com/docs/000006177>。

关于预防介质服务器故障

虽然可以使用冗余网络和 SAN 连接配置介质服务器，但是服务器本身仍旧是单一故障点。根据您使用的介质服务器类型的不同，发生介质服务器故障时对 NetBackup 的保护方法也有所不同。

表 1-3 列出了不同的介质服务器类型以及相应的保护方法。

表 1-3 介质服务器类型和保护方法

介质服务器类型	描述
专用介质服务器	只运行介质服务器软件，并专门备份其他系统中的数据。 请参见第 10 页的“关于预防专用介质服务器故障”。
非专用介质服务器	也会运行其他要求备份的应用程序。也会备份其他系统中的数据。 请参见第 11 页的“关于预防非专用介质服务器故障”。
SAN 介质服务器	也会运行其他要求备份的应用程序。不备份其他系统中的数据。 请参见第 11 页的“关于预防 SAN 介质服务器故障”。

关于预防专用介质服务器故障

当一台介质服务器发生故障时，可以使用存储单元组来保护 NetBackup。还可以使用存储单元组在多个介质服务器之间实现负载平衡，以确保最佳的备份和还原性能。

表 1-4 介绍了可用于配置存储单元组的不同模式。

表 1-4 配置存储单元组的模式

模式	描述
故障转移	在故障转移模式下，除非介质服务器已停机，否则始终使用第一个存储单元。多出的作业将会排队，而不是送往下一个存储单元。故障转移模式的工作方式就好像是将两台介质服务器配置为主动群集或被动群集。
优先	在优先模式下，使用列表中的第一个可用存储单元。在此模式下，超出存储单元可处理的作业总数的作业将被送往列表中的下一个存储单元。如果介质服务器停机，所有备份将送往下一个存储单元。
循环	在循环模式下，将针对每个作业轮流使用列表中的不同存储单元。如果每个存储单元都在不同的介质服务器上，则这种模式就能充当一种负载均衡机制。
负载均衡	负载均衡模式仅适用于 Flexible Disk 和介质管理器存储单元类型。在负载均衡模式下，NetBackup 将会对活动以及每个介质上的可用资源执行检查。在执行此检查后，再将备份作业送往负载最轻的介质。

在使用优先和故障转移组配置两个存储单元组时，最佳做法是使用两个介质服务器，如下所述：

- 配置每台介质服务器，以形成一个存储单元。例如，节点 A 包含 STU A，节点 B 包含 STU B。
- 配置两个存储单元组，并让其中的存储单元保持特定的顺序。在此示例中，SUG AB 包含 STU A，后接 STU B。SUG BA 包含 STU B，后接 STU A。
- 然后，可以在 SUG AB 和 SUG BA 之间均衡共享备份策略。

在操作期间，备份通信通常在两个节点间共享，但如果一个节点发生故障，所有备份将自动转到另一个节点。

关于预防非专用介质服务器故障

还可以使用存储单元组来预防非专用介质服务器故障。但是，这样无法阻止给定介质服务器上运行的其他应用程序出现该介质服务器的故障。在某些情况下，非专用介质服务器可以成为支持其他应用程序的群集的一部分。可以使用虚拟存储单元来保护这些应用程序。

关于预防 SAN 介质服务器故障

与常规的介质服务器不同，SAN 介质服务器只能保护自身。SAN 介质服务器像其他常规介质服务器一样直接连接到备份存储，但是它不通过网络或 SAN 链路从其他客户端系统接收数据。

SAN 介质服务器通常部署在支持大型任务关键型应用程序（通常是群集的）的服务器上。由于应用程序可以进行群集，因此您不需要将 SAN 介质服务器本身加入群集。而是应该将 SAN 介质服务器软件安装在群集的每个成员节点上，并在 NetBackup EMM 数据库中为群集使用的每个虚拟名称创建应用程序群集定义。然后，使用群集的虚拟名称作为介质服务器创建一个存储单元。具有给定虚拟名称的关联应用程序使用与同一虚拟名称关联的存储单元进行备份。

使用备用介质服务器还原磁带备份

通常，还原文件时，NetBackup 应该会使用它在创建原始备份时所用的相同介质服务器和客户端。然而，为实现灾难恢复，您可以使用另一台介质服务器将备份还原到不同的客户端。灾难恢复站点上的介质服务器和客户端名称可能与主站点上的名称不同。

NetBackup 允许您配置故障转移还原介质服务器，以便在原始介质服务器不可用的情况下处理还原操作。

配置故障转移还原介质服务器：

- 在 Windows 主服务器上，可以使用 **NetBackup 管理控制台** 配置故障转移还原介质服务器。
转到“主机属性” > “主服务器” > “还原故障转移”。
- 在 UNIX 和 Linux 主服务器上，必须在 `bp.conf` 文件中创建 `FAILOVER_RESTORE_MEDIA_SERVER` 条目。

使用备用介质服务器还原磁盘备份。

NetBackup 可以在多个介质服务器之间共享磁盘存储池。默认情况下，NetBackup 在还原过程中会平衡作业负载，自动将还原任务定向到最不繁忙的一台介质服务器，而不是创建备份的那一台。但是，如果选择用来执行还原的介质服务器已许可为 SAN 介质服务器，或者对需要还原的客户端没有网络访问权限，则此过程可能会出现。

如果您遇到此问题，有以下三个选择：

- 配置强制还原介质服务器设置，如下所示：
 - 在 UNIX 和 Linux 主服务器上，在 `bp.conf` 文件中创建 `FORCE_RESTORE_MEDIA_SERVER` 条目。
 - 在 Windows 主服务器上，可以在 **NetBackup 管理控制台** 中定义此设置。
转到“主机属性” > “主服务器”。
该设置以每台服务器作为基础进行应用。通过该设置，您可以根据用于生成备份的介质服务器，指定用于还原操作的介质服务器。为确保使用同一台介质服务器来进行备份和还原，请为备份服务器和还原服务器指定相同的名称。

- 按如下方式创建 touch 文件
USE_BACKUP_MEDIA_SERVER_FOR_RESTORE:
 - 在 UNIX 和 Linux 主服务器上, 在 /usr/opensv/netbackup/db/config 中创建该文件
 - 在 Windows 主服务器上, 在 <安装路径>\veritas\netbackup\db\config 中创建该文件
 USE_BACKUP_MEDIA_SERVER_FOR_RESTORE 是一项全局设置, 它始终强制还原到生成备份的服务器。

注意: 创建 USE_BACKUP_MEDIA_SERVER_FOR_RESTORE touch 文件后, 将忽略所有 FAILOVER_RESTORE_MEDIA_SERVER 和 FORCE_RESTORE_MEDIA_SERVER 设置。

- 在命令行上使用 bprestore -disk_media_server 命令运行还原。该设置在每个作业级应用。通过该设置, 您可以指定特定还原作业所需的介质服务器。不同于其他两个选项, 该设置是动态的, 可以在需要时应用。

关于预防 LAN 客户端故障

NetBackup 客户端软件包 (包括应用程序代理) 不能识别群集, 而且必须分别安装在作为 NetBackup 客户端进行保护的群集的每个节点上。在备份群集应用程序时, 请在备份策略中指定与应用程序关联的虚拟服务器名称作为客户端名称。这样可确保在备份操作过程中选择正确的群集节点。

关于预防 SAN 客户端故障

与 SAN 介质服务器类似, SAN 客户端不会通过网络将备份通信发送到介质服务器。但是, 与 SAN 介质服务器直接将备份数据发送到存储设备不同, SAN 客户端通过 SAN 连接将备份数据发送到一个远程介质服务器。

SAN 客户端通常用来保护群集的应用程序。采用这种部署方式时, 为了在发生 SAN 客户端故障时保护 NetBackup, 请在 EMM 中将 SAN 客户端配置为应用程序群集。此配置也可以确保在启动备份后, 控制备份的介质服务器始终能够与群集的活动节点建立光纤传输连接。

关于预防站点故障

本地群集为每个站点提供了本地故障转移。但是, 这些配置不提供对重大灾难 (例如导致整个地区断电的特大洪水、飓风和地震) 的防护。整个群集都可能受到此类断电的影响。在这些情况下, 全局群集或广域群集通过将应用程序迁移到距离较远的远程群集来确保数据可用性。

全局群集体系结构支持部署两个或多个相隔较远距离的数据中心、群集和子网。具有已复制主服务器群集的全局群集可以监视和管理每个站点上的复制作业和群集。在站点断电的情况下，它会控制将复制角色切换到辅助站点。它会运行关键应用程序并将客户端通信从一个群集重定向到其他群集。

自动映像复制是 NetBackup 的一项功能，它允许在各个 NetBackup 域之间复制基于单个磁盘的备份。由于在目标域的 NetBackup 目录库中会自动记录备份，因此在使用自动映像复制时无需对复杂的目录库恢复过程进行目录库复制。有关更多信息，请参考《NetBackup 管理指南，第 I 卷》。

https://www.veritas.com/support/zh_CN/article.DOC5332

关于在高可用性环境中保护目录库

NetBackup 目录库包含有关现有备份以及备份策略的信息，例如，备份的内容、备份的时间、备份的位置以及备份保存时间。这样，目录库便成了单一故障点，因而需要保护。使用 RAID 存储可以在一定程度上防止存储故障。复制也可以防止存储故障和站点泄露。目录库的常规备份可以防止数据损坏和意外的数据丢失。

请参见第 14 页的表 1-5。介绍了保护 NetBackup 目录库的各种方法。

表 1-5 高可用性环境中的 NetBackup 目录库保护

保护方法	描述
目录库备份	<p>目录库备份可保护主服务器上的 NetBackup 目录库免于硬件故障和数据损坏，应定期进行目录库备份，最好每天一次。目录库备份是基于策略的，因此它具有常规备份策略的所有预定灵活性。由于策略允许进行增量式备份，因此可以显著缩短大型目录库的目录库备份时间。但是，应注意，从增量式备份进行恢复可能需要较长时间，因为需要进行还原。</p> <p>写入磁带的目录库备份仅使用目录库备份卷池中的介质。</p> <p>有关更多信息，请参考《NetBackup 管理指南，第 I 卷》。</p>
目录库复制	<p>目录库复制是创建和管理目录库数据库的复制版本的过程。目录库复制将会复制一个数据库，并同步一系列副本，使一个副本发生的更改可以在其他所有副本上反映出来。</p> <p>将目录库复制到灾难恢复站点或辅助站点上的某个备用主服务器，可以确保在灾难恢复站点上快速完成目录库恢复。只要复制链路不中断，连续复制就能确保目录库保持最新状态。</p> <p>注意：复制不能防止目录库损坏或者映像的意外删除或失效。您必须定期执行预定的目录库备份。</p> <p>请参见第 24 页的“关于 NetBackup 目录库复制”。</p> <p>请参见第 16 页的“关于目录库恢复”。</p>

关于使用目录库备份和恢复进行的站点灾难恢复

本章节包括下列主题：

- [灾难恢复软件包](#)
- [关于目录库恢复](#)
- [关于 DR 域中的磁盘恢复](#)

灾难恢复软件包

为了提高安全性，在每个目录库备份期间均会创建灾难恢复软件包。灾难恢复软件包文件具有 `.drpkg` 扩展名。

该灾难恢复软件包存储主服务器主机的身份。**NetBackup** 需要此软件包才能在发生灾难后重新获取主服务器的身份。恢复主机身份后，您可以执行目录库恢复。

灾难恢复软件包包含以下信息：

- **NetBackup CA 签名证书**以及主服务器证书和 **NetBackup 证书颁发机构 (CA) 证书**的私钥
- 域中主机的有关信息
- 安全设置
- 外部 CA 签名证书
Windows 证书存储库中的外部 CA 签名证书（如果适用）
- 外部 CA 签名证书特定的 **NetBackup** 配置选项

注意：必须为灾难恢复软件包设置密码，目录库备份才能成功。

关于目录库恢复

用户在站点灾难恢复期间遇到的主要问题是，灾难恢复 (disaster recovery, DR) 站点不是生产站点的镜像映像。要执行 DR 操作，需要生产主服务器的 NetBackup 目录库的副本。NetBackup 目录库备份和恢复过程主要用于从目录库存储或主服务器故障中恢复，而不是从站点泄露中恢复。默认情况是 NetBackup 还原整个目录库，包括 EMM 数据库。EMM 数据库包含介质服务器、备份设备和存储单元的详细信息。主服务器使用该信息指导备份和还原。主服务器还使用该信息调查介质服务器，以建立备份设备的状态。在不包含这些介质服务器的 DR 环境中，主服务器的性能可能会受到影响。此外，由于轮询操作无法连接并且超时，执行还原操作的能力可能会受到影响。

注意：在群集设置中，如果使用外部 CA 签名证书进行主机通信，请确保虚拟名称和群集节点的证书颁发机构 (CA) 使用情况相同。例如，如果节点仅使用外部 CA 签名证书，请确保虚拟名称也使用外部 CA 签名证书。如果虚拟名称和群集节点的 CA 使用情况不一致，则目录库备份和目录库恢复可能会失败。

使用以下方法在介质服务器和客户端的布局与主产品站点的介质服务器和客户端的布局不同的 DR 站点上恢复 NetBackup 环境。两种方法各有各的优点和缺点。

- 在完全目录库恢复方法中，将会恢复整个目录库，然后可以删除或禁用不需要的配置元素。
请参见第 16 页的[“关于完全目录库恢复”](#)。
- 在部分目录库恢复中，不会还原 EMM 和 BMR 数据库。
请参见第 20 页的[“关于部分目录库恢复”](#)。

可通过 DR 工具的性质及其与生产工具的相似程度来确定适合恢复的最佳方法。

当您创建灾难恢复计划时，请确保其与以下各节中讨论的方法一致：

- 请参见第 30 页的[“计划跨域复制灾难恢复域”](#)。
- 请参见第 17 页的[“执行完全目录库还原”](#)。
- 请参见第 21 页的[“执行部分目录库还原”](#)。

关于完全目录库恢复

完全目录库恢复主要用于在生产站点中的数据发生损坏或存储丢失时恢复目录库。我们建议对单一域配置执行完全目录库恢复。如果 DR 站点中的介质服务器的数量及其名称都与生产站点中的相同，则使用完全目录库恢复。

与部分目录库恢复相比，完全目录库恢复具有以下优点：

- 还原关系数据库组件，其中包括存储单元定义、介质分配和历史记录。
- 保留主站点中的磁带信息，其中包括介质池和其他分配信息。

- 还原 BMR 数据。
- 使用生产站点中使用的相同策略和磁带可使备份在 DR 站点运行。

对于完全目录库恢复，存在以下限制：

- 目录库恢复不会恢复主机证书。要恢复 NetBackup 主服务器标识或主机证书及其他信息，应恢复灾难恢复软件包。
请参见第 15 页的“灾难恢复软件包”。
- 恢复关系数据库组件时，恢复前 DR 站点中设置的设备配置和服务器配置会丢失。恢复后，必须再次对其进行设置。存在于关系数据库中的有关生产服务器和设备的信息可能不存在于 DR 站点。要确保在 DR 环境中平稳运行，必须禁用这些服务器条目，并且应删除与其关联的设备。
- 完全目录库恢复会重写关系数据库中的设备配置和服务器配置。还原目录库后，必须重新发现 DR 域服务器和设备配置。

执行完全目录库还原

使用完全目录库恢复可将整个目录库备份恢复到 DR 主服务器。停用 DR 环境中不存在的介质服务器以避免占用不必要的池。因为 DR 站点中的设备配置可以不同于生产站点中的设备配置，所以会删除所有设备记录。运行设备发现以更新 EMM 数据库。必须先执行以下过程才能启动还原操作。此外，请在您的 DR 计划中记录该过程。

准备进行完全目录库还原

- 1 在 UNIX 和 Linux 主服务器上，创建 `bp.conf` 和 `vm.conf` 文件的副本。
- 2 运行 `bprecover` 命令以恢复整个目录库。

注意：DR 主服务器与生产主服务器必须具有相同的名称和拓扑结构。如果生产主服务器是一个群集，则 DR 主服务器也必须是一个群集。成员节点的数量和节点的名称可以不同。

注意：如果使用的是在单独介质服务器上创建的目录库备份，则目录库恢复需要具有相同名称的介质服务器。

- 3 运行 `bprecover` 命令之后，需为灾难恢复软件包设置密码，以便后续目录库成功备份。

请参见第 15 页的“灾难恢复软件包”。

4 在目录库恢复期间，没有恢复群集节点的安全证书。仅恢复虚拟名称证书。

如果使用 **NetBackup** 证书进行主机通信 要成功进行主机通信，发生灾难后，必须在所有群集节点上部署 **NetBackup** 证书（基于主机名的证书和基于主机 ID 的证书）。有关更多详细信息，请参考 [NetBackup 安全和加密指南](#) 中的“安装灾难恢复后在群集主服务器上生成证书”一章。

如果使用外部证书进行主机通信 要成功进行主机通信，必须在发生灾难后将所有群集节点配置为使用外部证书。有关更多详细信息，请参考 [NetBackup 安全和加密指南](#)。

5 在域中所有主机上清除白名单缓存并重新启动服务。

6 停用所有备份策略以防止备份自动启动。

- 可使用 **NetBackup 管理控制台** 手动执行此操作。
- 或运行 `bpplinfo <policy> -modify -inactive CLI`。

7 关闭 **NetBackup**。

8 在 UNIX 和 Linux 主服务器上，将从目录库备份中还原的 `bp.conf` 和 `vm.conf` 文件替换为在步骤 1 中创建的副本。

9 启动新主服务器上的 **NetBackup** 关系数据库管理器、**NetBackup PBX** 和 **EMM** 服务。

- 在 UNIX 和 Linux 主服务器上，运行下列命令：
 - `/usr/opensv/netbackup/bin/nbdbms_start_stop start`
 - `start /opt/VRTSpx/bin/pbx_exchange`
 - `/usr/opensv/netbackup/bin/nbemm`
- 在 Windows 主服务器上，启动下列 Windows 服务：
 - **NetBackup 关系数据库管理器**
 - **Veritas Private Branch Exchange**
 - **NetBackup 企业介质管理器**

注意：因为 **NetBackup** 命令不会停止和启动 PBX，所以 PBX 进程可能已经在运行。

有关 **NetBackup** 关系数据库管理器服务的更多信息，请参见 [NetBackup 故障排除指南](#)。

- 10 停用不属于 DR 环境的介质服务器。运行以下命令：

```
nbeimmcmd -updatehost -machinename <Media Server> -machinestateop  
set_admin_pause -machinetype media -masterserver <Master Server>
```

- 11 从 EMM 数据库删除所有磁带设备。运行以下命令：

```
nbeimmcmd -deletealldevices -allrecords
```

- 12 如果您的环境中具有 NAT 客户端，则需要执行此步骤。

如果配置了 **NetBackup Messaging Broker**（或 `nbmqbroker`）服务，则目录库还原后，需要使用 `configureMQ -enableCluster` 命令使群集监视该服务。

有关该命令的更多信息，请参考 [NetBackup 命令参考指南](#)。

- 13 重新启动 **NetBackup**。

- 14 使用“**设备配置**”向导创建新的磁带驱动器和库配置。

- 15 如果在步骤 9 中使用了条形码掩码规则，请确保在此处设置相同的规则。必要时添加这些规则。

- 16 使用 **NetBackup 管理控制台** 验证是否所有恢复介质都已设置为非机械手。

- 17 ■ 如果仍需将某些恢复介质设置为非机械手，请执行以下操作：

- 选择机械手介质，右键单击它并选择“**移动**”。
- 将机械手字段更改为“**独立**”。
- 单击“**确定**”保存更改。

- 18 将所有恢复介质都设置为非机械手后，在“**清点所有磁带库**”字段中确保介质位于正确的库中。

现在即可启动在生产数据中心备份的客户端数据的还原和恢复操作。

如果为 **NetBackup Web** 服务器配置了外部 CA 签名证书，则必须在活动节点上运行 `configureWebServerCerts` 命令，以确保在故障转移后使用外部证书。

有关命令的更多信息，请参见 [NetBackup 命令参考指南](#)。

对于所有群集节点，执行以下操作：

- 在节点上的配置文件中定义外部证书配置选项（`ECA_CERT_PATH`、`ECA_CRL_PATH` 等）。
- 在节点上运行 `nbcertcmd -enrollCertificate`。
有关更多详细信息，请参考《[NetBackup 安全和加密指南](#)》。

在执行完全目录库还原后使 DR 环境一致

如果在生产站点中出现了重大事件，则在基本恢复完成之后会从 DR 站点运行一段时间。如果 DR 环境可正常运行，则可选择执行下列附加任务以使 DR 环境一致。

使 DR 环境一致

- 1 如果未在恢复 DR 软件包后立即执行目录库恢复，为了使 DR 环境保持一致，请执行以下操作：
 - 如果使用 NetBackup CA 签名证书进行主机通信，请在所有节点上运行以下命令：
 - `nbcertcmd -getcacertificate`
 - `nbcertcmd -getcertificate`
 - 如果使用外部 CA 签名证书进行主机通信，请验证是否正确定义了所有节点的外部证书配置选项，然后在所有节点上运行以下命令：
 - `nbcertcmd -enrollCertificate`
- 2 修改备份策略（包括目录库备份策略），以使用 DR 站点上提供的存储单元并启用它们。
- 3 删除不再需要的备份策略。
- 4 删除与介质服务器相关且不属于 DR 环境的存储单元。
- 5 修改所有使用已删除的存储单元的存储生命周期策略。

关于部分目录库恢复

我们建议对多域配置执行部分目录库恢复。当 DR 站点中的服务器布局与具有较少介质服务器和不同库类型的生产站点中的服务器布局不同时，应使用部分目录库恢复。部分目录库恢复是无需导入的恢复方法的一种变体。它具有很多相同的限制。有关更多信息，请转到以下链接：

部分目录库恢复仅恢复平面文件组件而不恢复关系数据库。因此，DR 站点的现有基础架构（服务器、设备等）的详细信息在恢复过程中不会丢失。这也意味着不会恢复与备份关联的介质服务器信息。介质服务器必须手动添加到数据库且处于未分配状态。确保介质服务器位于在其中不会意外被重写的池中。

与完全目录库恢复相比，部分目录库恢复具有以下优点：

- 无需删除或重新发现配置的任何元素。恢复过程不会影响 DR 环境的常规配置。
- 不影响服务器拓扑结构。DR 站点的主服务器拓扑结构不需要在生产站点反映拓扑结构。因此，可将群集主服务器的目录库备份还原至 DR 站点中的独立主服务器。

- 如果这两个环境中使用的客户端名称、备份策略名称和磁带标签范围是唯一的，DR 站点可以是生产站点。并且，必须能够对其他生产备份域执行部分恢复。

对于部分目录库恢复，不能从 DR 站点的主站点恢复磁带信息。确保磁带没有被意外重写。这些磁带不能轻易用于 DR 站点的备份。

执行部分目录库还原

使用部分目录库方法时，假定还原操作不需要对磁带进行分配或要求磁带位于指定介质池中。此外，还假定磁带存在于 EMM 中，且 NetBackup 可装入和读取用于还原的磁带。必须先执行下列步骤才能启动还原操作：

准备进行部分目录库还原

- 1 在 UNIX 和 Linux 主服务器上，创建 `bp.conf` 和 `vm.conf` 文件的副本。
- 2 仅恢复 NetBackup 目录库映像和配置文件。
 - 如果使用 **NetBackup 管理控制台**，在出现提示时，请选择“部分目录库恢复”选项。
 - 或运行 `bprecover -wizard` 命令。

注意：DR 主服务器与生产主服务器必须具有相同的名称。

注意：如果使用的是在单独介质服务器上创建的目录库备份，则目录库恢复需要具有相同名称的介质服务器。

- 3 运行 `cat_export -all -staging` 从复制的关系数据库备份中导出元数据。
- 4 运行命令 `cat_import -all` 将导出的元数据导入到活动的关系数据库。或者，根据主服务器平台，将 `bp.conf` 文件或注册表中的参数 `LIST_FS_IMAGE_HEADERS` 设置为 `YES`。这将导致下一个目录库清理作业自动导入导出的元数据。
- 5 停用所有备份策略以防止备份自动启动。
 - 可使用 **NetBackup 管理控制台** 手动执行此操作。
 - 或运行 `bpplinfo <policy> -modify -inactive CLI`。
- 6 关闭 NetBackup。
- 7 在 UNIX 和 Linux 主服务器上，将从目录库备份中还原的 `bp.conf` 和 `vm.conf` 文件替换为在步骤 1 中创建的副本

- 8 启动 NetBackup:
- 9 清点所有磁带库以确保磁带已添加到非临时介质池中。此池可阻止磁带以后被活动的备份策略意外重写。

现在即可启动在生产数据中心备份的客户端数据的还原和恢复操作。

在执行部分目录库还原后使 DR 环境一致

如果在生产站点中出现了重大事件，则在基本恢复完成之后会从 DR 站点运行一段时间。如果 DR 环境可正常运行，则可选择执行下列附加任务以使 DR 环境一致。

使 DR 环境一致

- 1 修改并启用备份策略，目录库备份策略是 DR 站点所需的策略。
- 2 删除不再需要的策略。

关于 DR 域中的磁盘恢复

随着 OpenStorage 和其他 AdvancedDisk 类型的引入，重复数据删除磁盘会优先于磁带存储作为备份存储介质。使用磁盘存储，您可以将磁盘设备的内容复制到辅助位置上的其他磁盘设备中。通过此复制，无需再将物理备份介质传输到灾难恢复站点。

单域复制 DR 环境中的磁盘恢复

在同一 NetBackup 域中复制备份时，可以使用存储生命周期策略来优化重复数据删除磁盘的复制。这是在灾难恢复站点（与生产站点受同一个主服务器控制）创建重复备份映像副本的有效方法。然而，优化的重复数据删除仅对单域复制有效。

自动映像复制

自动映像复制将复制备份的概念扩展到了单独的域，从而允许将各个备份副本发送到一个 DR 域。由于使用自动映像复制创建的备份副本在 DR 域中会自动编录，因此在 DR 域内无需执行更多恢复步骤。有关自动映像复制的更多信息，请参考 [NetBackup 管理指南，第 I 卷](#)。

跨域复制 DR 环境中的磁盘恢复

如果使用的磁盘技术不支持自动映像复制，一个替代方法是仅复制整个存储，然后结合使用目录库恢复和 `nbcatsync` 实用程序在灾难恢复位置填充目录库。

`nbcatsync` 实用程序有利于复制，即使在 EMM 数据库和映像数据库的元数据组件中记录的磁盘介质 ID 不同。`nbcatsync` 实用程序使映像数据库元数据中的磁盘介质 ID 和灾难恢复域的 EMM 数据库中的介质 ID 相符。在生产站点进行的常规备份

和目录库备份将写入复制的磁盘存储。目录库备份的灾难恢复文件将发送至灾难恢复域。

所有主服务器平台均支持 `nbcatsync` 实用程序。可以对 NetBackup 支持的所有“高级磁盘”类型使用该实用程序。

在发生灾难时，要在跨域复制环境中恢复磁盘，请在 DR 域的主服务器上执行下列步骤：

- 1 使目录库备份的 DR 文件中的磁盘介质 ID 信息与 DR 域的 EMM 数据库中的磁盘介质 ID 信息相符。为此，请运行以下命令：

```
nbcatsync -sync_dr_file <DR file name>
```

- 2 通过运行以下命令，从复制的目录库备份中执行部分目录库恢复：

```
bprecover -wizard
```

- 3 运行命令 `cat_export -all -staging` 从复制的关系数据库备份导出元数据。

- 4 运行命令 `cat_import -all` 将导出的元数据导入到活动的关系数据库。

- 5 使与映像记录（通过部分目录库恢复所恢复）关联的磁盘介质 ID 与 DR 域中存在的磁盘介质 ID 相符。为此，请运行以下命令：

```
nbcatsync -backupid <restored catalog backup ID>
```

关于使用自动映像和目录库复制进行的站点泄露保护

本章节包括下列主题：

- [关于自动映像复制 \(AIR\)](#)
- [关于 NetBackup 目录库复制](#)

关于自动映像复制 (AIR)

自动映像复制功能允许在 NetBackup 域之间复制备份，并在复制备份的同时在目标域中自动创建目录库条目。Veritas 推荐使用自动映像复制（而不是实时目录库复制）作为在灾难恢复站点填充 NetBackup 目录库的方法。有关自动映像复制的更多信息，请参考 [NetBackup 管理指南](#) 中的相关部分。该文档讨论了在网络环境不适合使用自动映像复制的情况下复制目录库数据的替代方法。

关于 NetBackup 目录库复制

要决定 NetBackup 数据保护策略，需要决定 DR 站点应属于同一 NetBackup 域，还是单独的 NetBackup 域。

可采用以下方式通过目录库复制配置 NetBackup：

- 多站点单域复制
请参见第 26 页的“[关于多站点单域复制](#)”。
- 多站点跨域复制
请参见第 29 页的“[关于多站点跨域复制](#)”。

关于复制的 NetBackup 目录库的支持条件

为进行复制而设置的 NetBackup 环境的支持方式与任何其他 NetBackup 服务器的支持方式相同。如果复制的目录库卷出现故障且无法在合理的时间内恢复，NetBackup 支持部门建议您执行当非复制目录库发生不可恢复的磁盘故障时所执行的操作。您应从主要主服务器上的最新可用目录库备份中还原目录库。

注意：在任何数据复制解决方案中，都可能会丢失数据。要保护 NetBackup 目录库，不能仅依赖于复制技术，因为复制技术存在失败的风险。由于 NetBackup 主服务器上的数据要复制到辅助热备用 NetBackup 服务器，因此这些数据可能会发生损坏。所以，必须经常备份 NetBackup 服务器目录库。

警告：复制可能会对应用程序性能造成负面影响。由于提交对 NetBackup 目录库的更改需要额外的时间，因此可能会影响总体备份时间。使用复制应自担风险。对于由于您未能正确安装、配置和监视复制解决方案而造成的任何复制失败，Veritas 不承担任何责任。

NetBackup 目录库复制的支持条件如下：

- 使用的复制技术必须始终维护着一个一致的写排序数据副本。
- 如果能够维护写顺序保真，则允许使用异步复制技术。
- 不支持使用预定复制技术，如每小时快照。
- NetBackup 主服务器必须位于作为单个实体进行控制的同一台虚拟服务器上。
- 主要主服务器和辅助主服务器的类型、规范和操作系统必须类似，并且使用相同的虚拟主机名。
- 不论是在与主要主服务器相同的域中，还是在其他域中，辅助主服务器都不得兼具任何其他 NetBackup 功能。例如，如果未将辅助主服务器用作主服务器，则不能将其用作介质服务器。也不能将其用作其他 NetBackup 域的主服务器。可以复制目录库，但不能合并。
- 将群集环境而非群集环境均配置为使用独立于服务器物理主机名和 IP 地址的 NetBackup 主服务器虚拟主机名和 IP 地址。使用独立的虚拟主机名和 IP 地址，可以通过 DNS 路由来控制活动主服务器节点。此外，也会阻止域中的主要主服务器和辅助主服务器同时处于活动状态。对于群集环境，通过群集配置可自动满足此项要求。对于非群集环境，必须在安装过程中指定虚拟主机名。
- 确保主要主服务器和辅助主服务器使用相同版本的 NetBackup 和相关组件。验证是否为复制指定了没有包括在路径中的操作系统、NetBackup 二进制文件、EEB 和配置文件。
- 无法在群集服务器与非群集主服务器之间执行备份。服务器对必须同属于群集服务器或非群集服务器。

- 在主站点和辅助站点上，NetBackup 目录库装入点必须相同。
- 目录库数据仅在服务器之间复制，并且这些数据必须同位于要进行复制的单个卷或卷集中。对于群集主服务器，将复制群集公用卷。
对于非群集主服务器，有关必须链接到要进行复制的卷集的路径的详细信息，
- 确保虚拟名称或 DNS 别名不会同时解析为主主机和辅助主机。
- 目录库复制依然要求进行目录库备份。从主要主服务器定期备份 NetBackup 目录库，以免受到在主站点目录库引入并复制到辅助站点的意外映像过期或其他不一致情况的影响。
- 如果在 NetBackup 域之间复制目录库（而不是复制到可访问主域介质服务器的辅助服务器），则在灾难恢复域中只能还原写入磁带和复制的 BasicDisk 存储的备份。
- 通过将目录库复制到辅助主服务器，您可以在主要主服务器发生短期中断期间还原数据。在跨域复制配置中，请确保故障转移后备份可以运行。以后目录库应该能够故障恢复至主服务器，而不会造成数据丢失。如果您计划在长时间中断期间在 DR 站点上执行备份，然后在不丢失有关在 DR 站点上所创建备份的信息的情况下移回主站点，请考虑此支持条件。
- 验证 NetBackup 是否使用辅助站点上的复制副本启动。该用法不属于支持要求。
- 在辅助站点上，必须可以同时访问目录库和备份映像。
用户需要了解与备份映像有效副本的可用性有关的过程。用户还应定义启用要从辅助站点的映像还原的 NetBackup 服务器的过程。本文档不介绍这些过程。
- 用户负责安装、配置和监视其数据复制解决方案。用户必须确保复制技术始终维护着一个一致的 NetBackup 目录库卷写排序副本。
- 不支持 Microsoft 已分配文件系统复制 (DFSR) 技术，因为它不能保证正在复制的文件的写排序一致性。
有关更多信息，请参见 https://www.veritas.com/support/en_US/article.100043283

关于目录库同步

与在站点间移动磁带相比，复制几乎是瞬间完成的活动。DR 域中的复制目录库数据比 DR 域中可用的磁带更新，这些磁带是之前从生产域调度的。在执行还原操作期间，仅选择那些在从生产域调度磁带之前所创建的备份进行还原。

关于多站点单域复制

多站点单域适用于两个站点的客户端和介质服务器位于公共主服务器控制下的情况。由于两个服务器属于同一个域，因此它们可以看到相同的介质服务器和客户端，NetBackup 目录库在辅助主服务器上完全有效。

在多站点单域模式中，NetBackup 目录库在站点间进行复制。在主站点出现问题的情况下，主服务器将故障转移到辅助站点上的备用节点。两个站点上都创建了备份（根据配置采用内联复制或复制）。因此，单一站点丢失并不代表真正的灾难，多个应用程序服务器丢失才是真正的灾难。由于备份域跨越两个站点，因此单一站点丢失会导致备份和存储能力下降，而不会损坏备份环境。多站点单域模式使用主服务器群集和存储复制的组合。此组合可以将主服务器快速便捷地重定位至辅助位置。

可以采用以下方式配置多站点单域模式：

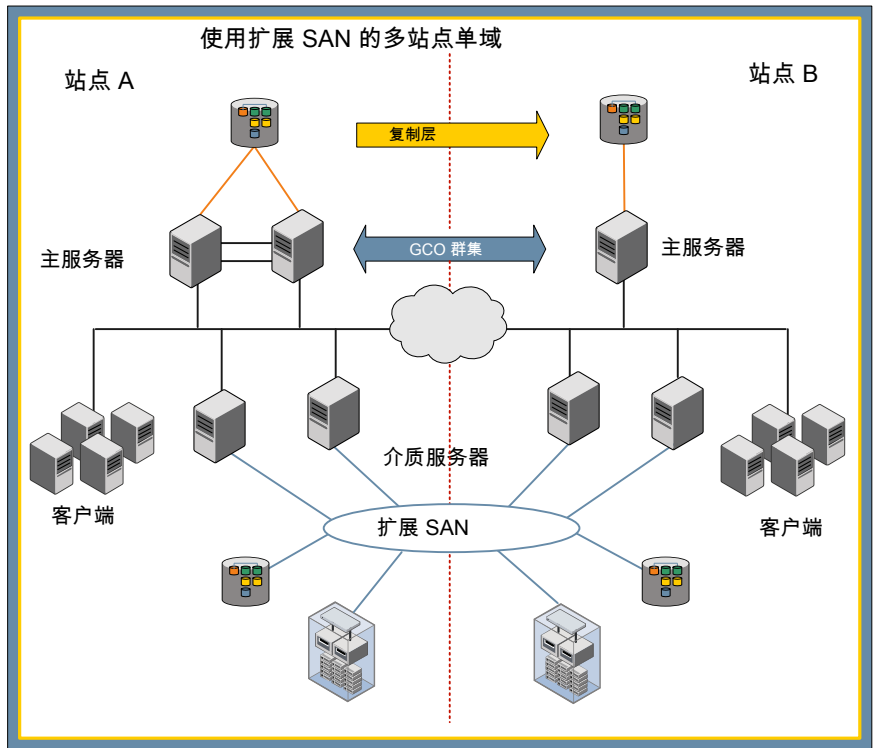
- 使用扩展 SAN 的多站点单域
请参见第 27 页的“[关于使用扩展 SAN 的多站点单域](#)”。
- 使用优化复制的多站点单域
请参见第 28 页的“[关于使用优化复制的多站点单域](#)”。

关于使用扩展 SAN 的多站点单域

要配置使用扩展 SAN 的多站点单域，每个站点的介质服务器必须配置有对两个站点的备份设备的 SAN 访问权限。通过此访问权限，介质服务器可以在站点间写入和复制备份。此配置对站点间的距离在 50 英里以内的情况凑效，但是随着距离和延迟的增加，此配置的效率也会降低。

图 3-1 显示了如何通过使用扩展 SAN 的多站点单域配置复制全局群集。

图 3-1 使用扩展 SAN 的多站点单域

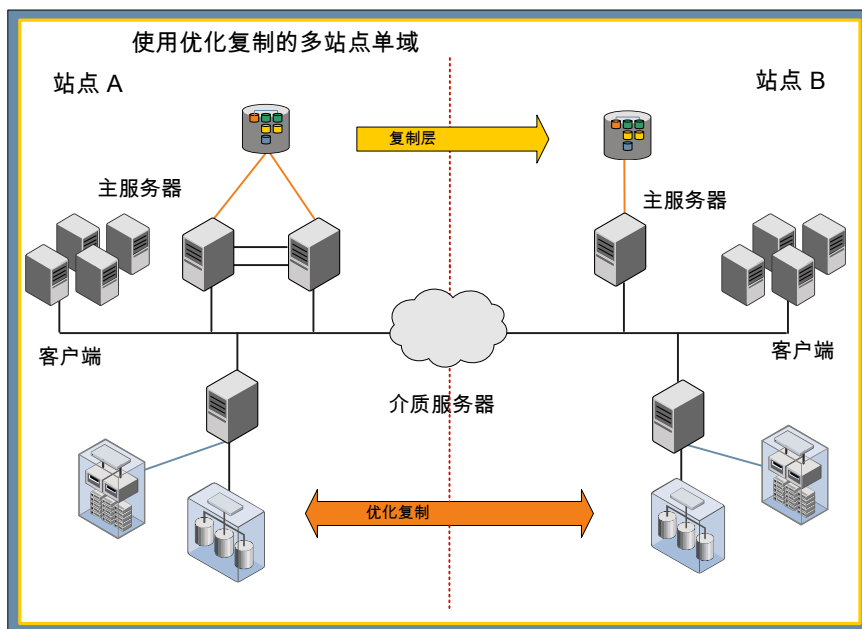


关于使用优化复制的多站点单域

要配置使用优化复制的多站点单域，必须将扩展 SAN 替换为执行优化复制的 OpenStorage 设备之间的连接。在此配置中，由于站点间交换的数据卷更小，因此地理分隔可以更大。使用存储生命周期策略中的分层复制功能，可在某个站点的 OpenStorage 设备中创建备份。然后，可以将备份复制到其他站点的 OpenStorage 设备，最后，再将复制的副本复制到磁带进行长期存储。

图 3-2 显示了如何通过使用优化复制的多站点单域来配置复制全局群集。

图 3-2 使用优化复制的多站点单域



关于多站点跨域复制

多站点跨域复制适用于 DR 站点是单独 NetBackup 域而不是生产域的情况。DR 站点具有不同的介质服务器和设备。

仅磁带和 BasicDisk 存储支持多站点跨域复制。AdvancedDisk 类型具有特定的介质服务器或设备配置要求，不允许在灾难恢复域中对其进行访问。

关于多站点跨域和 BasicDisk 存储

可以复制存储在域间非分段作业 BasicDisk 存储上的映像。必须通过 DR 域中介质服务器上的同一装入点装入复制目标。此外，请设置 `FAILOVER_RESTORE_MEDIA_SERVER` 参数以确保选择了正确的介质服务器。例如，可以通过生产域中介质服务器 `prdmed1` 上的装入点 `/BD1` 将 BasicDisk 存储单元复制到 DR 域。如果将 DR 主服务器上的 `bp.conf` 文件编辑为设置 `FAILOVER_RESTORE_MEDIA_SERVER = prdmed1 drmed1`，则 `/BD1` 可装入到介质服务器 `drmed1` 上。此设置仅适用于未充当分段作业存储单元、不受分段作业存储单元或其他磁盘类型支持的 BasicDisk 存储单元。

计划跨域复制灾难恢复域

要使用 DR 域中辅助主服务器上的复制目录库数据，请确保主服务器、介质服务器、网络连接和 NetBackup 软件正常运行。

Veritas 建议您记录 DR 配置步骤，特别是当 DR 域没有按常规配置时。如果域是由专业 DR 服务公司提供的工具，本文档尤其重要。准备 DR 计划时，请参考以下步骤：

计划跨域复制灾难恢复域

- 1 在 DR 域中的主服务器、介质服务器和客户端上安装与生产域所使用的版本相同的 NetBackup。

注意：如果生产域具有使用旧版本 NetBackup 的介质服务器，请不要在 DR 域中的介质服务器上安装旧版本。请为 DR 域中的主服务器和介质服务器使用相同的版本。

如果使用完全目录库复制方法，且生产域中的主服务器已群集，则 DR 域中必须也存在群集主服务器。群集的成员节点不需要与生产域中的那些节点相同。如果使用部分目录库复制方法，则不需要 DR 域中存在群集主服务器。

- 2 使用测试备份策略测试客户端和服务器之间的网络连接和身份验证。测试后禁用这些策略。
- 3 磁带驱动器和库必须连接到介质服务器。DR 域中使用的磁带驱动器必须与生产域的磁带是“读兼容”的。必须在 NetBackup 中将它们配置为同一介质类型。
- 4 设置 `FAILOVER_RESTORE_MEDIA_SERVER` 参数，以允许将备份写入到生产域的介质服务器，从而能够使用 DR 域中的介质服务器还原备份。
- 5 如果使用部分复制方法，请创建未被任何备份策略使用的非临时介质池。配置条形码规则，确保备份磁带自动添加到该池。
- 6 如果 DR 域和生产域使用不同的库类型，请确保条形码掩码以相同的方式工作。根据需要删除尾随字符。可配置规则来管理此操作。
- 7 请确保以下条件成立：
 - 如果出于 DR 目的使用原始备份磁带，必须将其装入 DR 域中的磁带库。
 - 如果出于 DR 目的将备份复制到辅助磁带，请将场外磁带装入磁带库。同时，将创建包含相应副本号的 `ALT_RESTORE_COPY_NUMBER` 文件。

注意：Veritas 建议先以物理方式对磁带设置写锁定，然后再将其放入 DR 域的库。此锁定可降低有效备份被意外重写的风险。

关于完全目录库复制

在完全目录库复制中，会将目录库的所有部分都复制到辅助主服务器。在完全目录库复制中，将保留来自生产域、介质池和其他分配的磁带信息。通过使用与生产域中所用的相同的策略和磁带，可在 DR 域中运行备份。可以反向复制，从而简化切换回生产域的过程。但是，复制关系数据库组件意味着生产域的设备配置和服务器配置已复制到 DR 域。无法使用此配置信息，必须在恢复之后才能发现 DR 域中的该配置。

因此，不建议在跨域复制中使用完全目录库复制。

使用完全目录库复制恢复目录库

通过完全目录库复制，可将完整的目录库备份恢复到 DR 主服务器。应停用 DR 环境中不存在的介质服务器以避免占用不必要的池。由于 DR 站点的设备配置可能与生产站点不同，将删除所有设备记录。而且，将运行设备发现以更新 EMM 数据库。

此方法假设 NetBackup 已安装在 DR 域中的辅助主服务器和介质服务器上但没有运行。并且，已将辅助主服务器和介质服务器配置为互相进行通信。

启动还原之前，请执行以下过程，为完全目录库还原做准备。必须在 DR 计划中记录此过程：

- 1 确保主站点和辅助站点间的复制已停止。
如果主要主服务器不可用或复制链接已禁用，则复制会停止。
- 2 将复制卷装入到辅助主服务器上的相应装入点。
- 3 启动新主服务器上的 NetBackup 关系数据库管理器、NetBackup PBX 和 EMM 服务。
 - 在 UNIX 和 Linux 主服务器上，运行以下命令：
 - `/usr/opensv/netbackup/bin/nbdbms_start_stop start`
 - `/opt/VRTSspb/bin/pbx_exchange`
 - `/usr/opensv/netbackup/bin/nbemmm -maintenance`
 - 在 Windows 主服务器上，启动以下 Windows 服务：
 - NetBackup 关系数据库管理器
 - Veritas Private Branch Exchange
 - NetBackup 企业介质管理器

注意：由于 PBX 进程不由 NetBackup 的启动和关闭命令停止和启动，因此 PBX 进程可能已在运行。

- 4 停用不属于 DR 环境的介质服务器。运行以下命令：

```
nbemmcmd -updatehost -machinename <Media Server> -machinestateop  
set_admin_pause -machinetype media -masterserver <Master Server>
```

- 5 如果 DR 域中的任何介质服务器与生产域中的介质服务器同名，则从 EMM 数据库删除所有磁带设备。运行以下命令：

```
nbemmcmd -deletealldevices -allrecords
```

注意：此步骤可解决介质服务器上可能发生的设备配置冲突。如果 DR 域中的介质服务器与生产域中的介质服务器名称不同，则跳过此步骤。

- 6 重新启动 NetBackup。
- 7 （可选）您可停用所有备份策略，以阻止备份自动启动。
- 您可使用 **NetBackup 管理控制台** 手动停用备份策略。
 - 或运行 `bppllist<policy> -set -inactive CLI`。
- 8 通过在每台介质服务器上启动 NetBackup，在 EMM 中注册组成 DR 环境的介质服务器。
- 9 使用“设备配置向导”创建新的磁带驱动器和库配置。
- 10 使用 **NetBackup 管理控制台** 验证是否所有恢复介质都已设置为非机械手。
- 11 如果仍需将某些恢复介质设置为非机械手，请执行以下操作：
- 选择机械手介质，右键单击它并选择“移动”。
 - 将机械手字段更改为“独立”。
 - 单击“确定”保存更改。
- 12 将所有恢复介质都设置为非机械手后，在“清点所有磁带库”字段中确保介质位于正确的库中。

现在即可启动在生产数据中心备份的客户端数据的还原和恢复操作。

通过完全目录库复制使 DR 环境一致

如果在生产站点中出现了重大事件，则在基本恢复完成之后会从 DR 站点运行一段时间。如果 DR 环境可正常运行，则可选择执行下列附加任务以使 DR 环境一致。

使 DR 环境一致

- 1 修改并启用 DR 域中需要的目录库备份策略和其他所有备份策略。
- 2 删除不再需要的策略。
- 3 删除与不属于 DR 环境的介质服务器关联的存储单元。

关于部分目录库复制

在部分目录库复制中，仅复制映像数据库、策略和客户端配置，不复制关系数据库组件。因此，可以在灾难恢复域中预配置介质服务器和设备。在故障转移到辅助主服务器时，不需要重新发现介质服务器和设备。

由于在部分目录库复制中，不复制 NetBackup 目录库的关系数据库组件，故障转移到灾难恢复主服务器后还需要执行附加步骤，才能还原备份。

为部分目录库复制准备环境

运行还原操作所需的目录库映像元数据存储的关系数据库中，因此必须定期备份关系数据库并与平面文件信息一起复制。

- 1 更改源（生产）主服务器上的配置，以确保关系数据库的分段作业区域位于复制的存储上。这可以通过以下方法实现：
 - 在复制的存储上创建一个适当的目录。
 - 运行以下命令，将此目录用作分段作业区域。
- 2 通过在预定脚本中运行以下命令，每天多次（最好每小时一次）将关系数据库备份到分段作业区域。

```
nbdb_admin -vxdbs_nb_staging <directory>
```

```
nbdb_backup -online <directory>-truncate_tlog
```

使用部分目录库复制恢复环境

如果缺少源主服务器（或者在灾难恢复测试期间），请按照以下步骤操作：

- 1 确保主站点和辅助站点间的复制已停止。
如果主要主服务器不可用或者复制链接已禁用，则复制将停止。
- 2 将复制卷装入到辅助主服务器上的相应装入点。
- 3 在目标（灾难恢复）主服务器上使用 `nbdb_admin -vxdbs_nb_staging <directory>` 命令将关系数据库的分段作业区域指向复制的存储上的位置。
- 4 运行命令 `cat_export -all -staging` 从复制的关系数据库备份导出元数据。
- 5 运行命令 `cat_import -all` 将导出的元数据导入到活动的关系数据库。

- 6 启动辅助主服务器上的 NetBackup。
- 7 如果已复制备份策略，请停用所有备份策略来阻止备份自动启动。
 - 您可使用 **NetBackup 管理控制台** 手动停用备份策略。
 - 或运行 `bppllist<policy> -set -inactive` 命令。
- 8 请确保已定义正确的 `FAILOVER_RESTORE_MEDIA_SERVER` 设置，以引导辅助站点上的介质服务器的还原操作。
- 9 要从磁带还原备份，必须通过将磁带放入磁带库并对库运行清点，将磁带添加到灾难恢复主服务器的目录库。为防止磁带被意外重写，灾难恢复主服务器应具有这样一个条形码规则：将磁带添加到不是全局临时池且未由任何备份策略所使用的卷池。理想情况下，还应以物理方式对磁带设置写锁定。
- 10 对于基于磁盘的备份，必须通过运行磁盘存储服务器向导，将存储服务器和磁盘池添加到灾难恢复主服务器。

有了磁盘存储之后，请运行以下命令来协调磁盘介质 ID：

```
nbcatsync -backupid <catalog backup ID> -prune_catalog
```

<catalog backup ID> 的值是最新目录库备份的备份 ID，可以在目录库备份的灾难恢复文件中找到。在添加磁带并协调磁盘介质 ID 之后，即可启动还原操作。

通过部分目录库复制使灾难恢复环境一致

如果在生产站点中发生了重大事件，请在恢复完成之后从灾难恢复站点运行一段时间。如果灾难恢复环境可正常运行，则可选择执行下列附加任务以使灾难恢复环境一致。

通过部分目录库复制使灾难恢复环境一致

- 1 修改并启用灾难恢复域中需要的目录库备份策略和所有其他备份策略。
- 2 删除不再需要的策略。

有关管理具有部分目录库复制的磁带的注意事项

在灾难恢复域中没有分配来自生产域的磁带。必须手动将磁带添加到数据库，并将其放置在无法意外重写它们的池中。也可以使用条形码规则和机械手清点命令的组合来完成此操作。

由于磁带未在灾难恢复主服务器上分配，当备份失效时不会将其释放到全局临时池，因此必须手动回收这些磁带。

小心： 确保仅当磁带不包含有效备份时，将磁带手动移动到全局临时池，在此过程中需要多加小心。

检查此项的最简单方法是，通过运行命令 `bpimagelist -d "01/01/1970 00:00:00" -media -l` 和 `vmquery -pn <private pool name> -b` 创建两个列表，然后对列表进行比较。在第二个列表中找到但是未在第一个列表中找到的磁带不包含有效映像，可以通过运行命令 `vmchange -p <scratch pool number> -m <media id>` 将其移动到临时池。

使用完全目录库复制部署 NetBackup 主服务器

本章节包括下列主题：

- [关于复制注意事项](#)

关于复制注意事项

要部署具有目录库复制功能的 NetBackup，必须针对实际部署的规划考虑下列因素。

表 4-1 复制注意事项

注意事项	描述
主服务器注意事项	<p>Veritas 不建议将一台主服务器既用作主服务器又用作介质服务器。如果不同站点上的存储设备互不兼容，可能会导致存储单元定义出现问题，并导致备份失败。</p> <p>目录库复制不能替代目录库备份，必须定期进行目录库备份。</p>
联网注意事项	<p>在多站点单域配置中，主服务器控制两个站点上的介质服务器。元数据必须在站点之间传递。此元数据通信通过标准 I/P 链路在站点之间发送。同一链路可用作全局群集控制的心跳链路。Veritas 建议必须在站点之间提供至少 10 MB/秒且理想情况下为 100 MB/秒的链路，以处理该通信。</p> <p>如果使用基于主机的复制，复制层需要额外的 I/P 带宽。其他带宽也必须考虑。</p>

注意事项	描述
DNS 注意事项	<p>如果辅助站点上的主服务器节点与主站点上的主服务器节点位于不同的子网上，则故障转移过程中需要更改 DNS。可通过使用群集故障转移过程自动启动 DNS 更改。也可以手动启动该过程。在完全传播更改之前，备份系统不会正常运行，这会影响站点故障转移中的恢复时间。</p> <p>注意：要使群集服务组自动传播 DNS 更改，DNS 资源必须在 NetBackup 启动后联机。</p>
主要主服务器和辅助主服务器注意事项	<p>使用目录库复制时，为了执行故障转移，主要主服务器和辅助主服务器必须使用同一拓扑。</p> <p>主要主服务器和辅助主服务器节点必须都为群集或非群集节点。</p> <p>注意：群集主服务器不要求每个站点具有相同的节点数。</p> <p>有关其他详细信息，请参考 http://www.veritas.com/docs/000090837。</p>

在群集中使用 NetBackup 执行备份和还原

本章节包括下列主题：

- [关于在群集中使用 NetBackup 执行备份和还原](#)
- [关于群集中支持的 NetBackup 应用程序代理](#)

关于在群集中使用 NetBackup 执行备份和还原

本主题提供了说明如何在群集中执行用户控制的备份和还原数据的链接。此外，有关执行备份和还原的特定说明可以在其他 NetBackup 指南中找到。有关 NetBackup 代理和选件的相关信息，请参见 [NetBackup 备份、存档和还原快速入门指南](#) 以及《[NetBackup 管理指南](#)》。

无论是在群集环境中还是在非群集环境中，备份和还原进程都是相同的。有关备份和存档进程以及还原进程的更多信息，请参见 [NetBackup 故障排除指南](#)。

在群集中使用 NetBackup 执行用户控制的备份

在群集中执行用户控制的备份时，您可以使用客户端的节点名称或虚拟名称来执行备份。如果选择虚拟名称，则可以从任何群集节点中还原备份。您还可以配置自动备份。

在 Windows 客户端上执行用户控制的备份

- 1 打开“备份、存档和还原”控制台。
- 2 在“文件”菜单上，单击“指定 NetBackup 计算机”。
- 3 从“源客户端”列表中，选择（或者添加）需要的节点或虚拟名称。

在 UNIX/Linux 客户端上执行用户控制的备份

- 1 打开“备份、存档和还原”控制台。
- 2 在“登录”对话框中，输入客户端的名称（节点名称或虚拟客户端名称）。

您必须登录到需要的节点或虚拟客户端上。在 Java 界面中，您无法指定非本地的客户端。

关于在群集中还原数据

对于所有文件还原操作，要了解执行还原时使用的步骤，请参见 [NetBackup 备份、存档和还原入门指南](#)。将文件还原到共享磁盘驱动器时，请将这些文件还原为虚拟服务器名称。

还原单个数据库文件时，将这些文件还原为与已安装数据库应用程序的客户端相对应的虚拟服务器名称。

注意：由于在群集环境中一台计算机可以有多个虚拟名称，因此可在多个客户端名称的上下文中备份文件。如果仔细规划备份策略，则可以避免此问题。但是，可能需要浏览多个客户端名称以查找备份映像。并且您可能需要执行多个还原，以便还原所需的所有文件。

“备份、存档和还原”控制台在客户端名称的上下文中运行。您必须执行重定向还原，以便还原共享磁盘上使用虚拟服务器名称备份的文件。只有当在 NetBackup 主服务器上执行必要的配置时，NetBackup 才允许进行重定向还原操作。有关如何进行重定向还原的信息，请参见 [NetBackup 管理指南，第 I 卷](#)。

有时候可能需要在主服务器上创建适当的 altnames 目录条目。当 NetBackup 尝试从客户端还原文件时，操作可能失败并显示此错误消息：

```
131 client is not validated to use this server
```

如果您看到此消息，则必须设置 altnames 目录以使操作成功。例如，可以将所需的网络接口参数设置为客户端的有效网络名称。但是该名称可能与该客户端的 NetBackup “客户端名称”参数不匹配。群集中的 NetBackup 客户端经常发生这种情况。或者，您可以执行服务器控制的还原，而无需设置 altnames 目录。

请参见第 39 页的“在 [NetBackup 群集中执行用户控制的还原](#)”。

在 NetBackup 群集中执行用户控制的还原

例如，假设群集虚拟服务器名称为 TOE，群集节点名称为 TIC 和 TAC。共享磁盘上的文件必须由客户端列表中包含 TOE 的 NetBackup 策略来备份。

要在共享磁盘上对文件执行服务器控制的还原，请将源客户端和目标客户端均设置为 TOE。服务器控制的还原无需知道还原时共享磁盘控制哪个节点。

在 NetBackup 群集中执行文件的用户控制还原

- 1 在主服务器上创建以下文件。

对于 UNIX 或 Linux 服务器:

```
/usr/opensv/netbackup/db/altnames/tic  
/usr/opensv/netbackup/db/altnames/tac
```

对于 Windows 服务器:

```
shared_drive_install_path\NetBackup\db\altnames\tic  
shared_drive_install_path\NetBackup\db\altnames\tac
```

- 2 在这两个文件中, 将虚拟服务器名称 TOE 添加在文件中的某行。
- 3 确定共享磁盘控制的节点 (TIC 或 TAC)。
- 4 在该节点上启动“备份、存档和还原”界面, 并选择虚拟服务器名称 (TOE) 作为源客户端和服务端。
 - 在 Windows 计算机的“文件”菜单中, 单击“指定 NetBackup 计算机”。
 - 在 UNIX 或 Linux 计算机的“操作”菜单中, 单击“NetBackup 计算机”。
- 5 通过使用虚拟服务器名称 (TOE) 从共享磁盘中浏览已备份的文件, 并根据需要还原它们。

关于群集中支持的 NetBackup 应用程序代理

在群集环境中仅支持某些数据库代理和 NetBackup 选件。

有关如何在群集中安装和配置数据库代理和选件的信息, 请参考相应代理或选件的管理指南。

在群集中备份数据库文件

数据库应用程序作为虚拟服务器安装在群集上。要保护这些虚拟服务器的数据, 请在群集的每个节点上安装适当的 NetBackup 数据库代理。对于 NetBackup for Windows, 数据库代理与 NetBackup 服务器和 NetBackup 客户端一起安装。还需为该数据库代理创建一个备份策略。在为群集中的应用程序或数据库配置策略时, 请始终使用应用程序或数据库的虚拟服务器名称作为策略的客户端名称。有关特定数据库代理的完整的安装和配置说明, 请参见相应代理的 NetBackup 文档。

用户备份

在群集的单个节点上运行的用户备份通常作为节点的备份运行, 而不作为 NetBackup 虚拟服务器运行。您可能会发现使用预定备份来保护群集中的数据比使用用户备份要容易得多。

群集中的 NetBackup 客户端 您可以选择在群集中仅安装 NetBackup 客户端。在此配置中，您可以通过网络将群集中的数据备份到一个单独的 NetBackup 服务器。在这种情况下，磁带设备、介质等 NetBackup 特定配置任务与群集自身的设置和维护分开执行。但是，NetBackup 客户端本身不能进行故障转移。

将 NetBackup 客户端安装在 WSFC、VCS、SunCluster、Service Guard 群集或 HACMP 群集上

在群集中安装 NetBackup 客户端的方法与在非群集的环境中相同。有关如何安装 NetBackup 客户端的信息，请参见《Veritas NetBackup 安装指南》。在 Windows 系统上，当尝试备份群集上的数据时可能会遇到与名称解析有关的问题。（此数据可以是本地数据或共享数据。）请考虑将每个客户端“所需的网络接口”参数设置为安装有 NetBackup 客户端的节点的完全限定名称。

关于在群集中备份数据库文件

数据库应用程序作为虚拟服务器安装在群集上。要保护这些虚拟服务器的数据，请在群集的每个节点上安装适当的 NetBackup 数据库代理对于 NetBackup for Windows，数据库代理与 NetBackup 服务器和 NetBackup 客户端一起安装。还需为该数据库代理创建一个备份策略。在为群集中的应用程序或数据库配置策略时，请始终使用应用程序或数据库的虚拟服务器名称作为策略的客户端名称。有关特定数据库代理的完整的安装和配置说明，请参见相应代理的 NetBackup 文档。

关于用户备份

在群集的单个节点上运行的用户备份通常作为节点的备份运行，而不作为 NetBackup 虚拟服务器运行。您可能会发现使用预定备份来保护群集中的数据比使用用户备份要容易得多。

关于群集中的 NetBackup 客户端

您可以选择在群集中仅安装 NetBackup 客户端。在此配置中，您可以通过网络将群集中的数据备份到一个单独的 NetBackup 服务器。在这种情况下，磁带设备、介质等 NetBackup 特定配置任务与群集自身的设置和维护分开执行。但是，NetBackup 客户端本身不能进行故障转移。

将 NetBackup 客户端安装在 MSCS、VCS、SunCluster、Service Guard 群集或 HACMP 群集上

在群集中安装 NetBackup 客户端的方法与在非群集的环境中相同。有关如何安装 NetBackup 客户端的信息，请参见《Symantec NetBackup 安装指南》。在 Windows 系统上，当尝试备份群集上的数据时可能会遇到与名称解析有关的问题。（此数据

可以是本地数据或共享数据。) 请考虑将每个客户端“所需的网络接口”参数设置为安装有 NetBackup 客户端的节点的完全限定名称。

索引

B

保护方法

- LAN 客户端 13
- SAN 介质服务器
 - 应用程序群集 11
- SAN 客户端 13
- SAN 连接
 - 动态多路径 8
- 存储设备
 - 冗余驱动器 8
- 非专用介质服务器
 - 存储单元组 11
- 机械手控制连接
 - 控制服务器群集 8
 - 冗余连接 8
- 介质可用性
 - 介质共享 9
 - 全局临时池 9
- 网络链路
 - 冗余网络合作 7
- 站点
 - 全局群集 13
- 主服务器
 - 群集 10
- 专用介质服务器
 - 存储单元组 10

备份

- 用户控制的 38
- 备份数据库文件 41
- 部分目录库复制 33
- 部分目录库恢复 20
 - 还原部分目录库 21

C

存储设备保护

- 冗余驱动器 8

D

- 多站点单域复制 26
 - 扩展 SAN 27

- 优化复制 28
- 多站点跨域复制
 - BasicDisk 存储 29

F

- 非专用介质服务器保护
 - 存储单元组 11
- 复制注意事项 36
 - DNS 注意事项 37
 - 联网注意事项 36
 - 主服务器注意事项 36

G

故障点

- LAN 客户端 13
- SAN 介质服务器 11
- SAN 客户端 13
- 存储设备 8
 - 存储设备连接 8
 - SAN 连接 8
 - 机械手控制连接 8
- 非专用介质服务器 11
- 介质服务器 10
- 介质可用性 9
- 网络链路 7
- 站点 13
 - 主服务器 10
 - 专用介质服务器 10
 - 组件 6
- 光盘恢复 22

H

- 还原部分目录库 21
- 还原整个目录库 17
- 机械手控制连接保护
 - 控制服务器群集 8
 - 冗余连接 8

J

- 介质服务器
 - 还原备份 12
- 介质可用性保护
 - 介质共享 9
 - 全局临时池 9

L

- LAN 客户端保护 13

M

- 目录库保护
 - 联机目录库备份 14
 - 目录库复制 14
 - 另请参见 目录库复制
- 目录库备份
 - 灾难恢复软件包 15
- 目录库复制
 - 部分目录库复制 33
 - 多站点单域 26
 - 多站点跨域复制 29
 - 目录库同步 26
 - 完全目录库复制 31
 - 支持条件 25
 - 注意事项. 请参见 复制注意事项
- 目录库恢复 16
 - 部分目录库恢复 20
 - 完全目录库恢复 16
- 目录库同步 26

Q

- 群集中的 NetBackup 客户端 41

S

- SAN 介质服务器保护
 - 应用程序群集 11
- SAN 客户端保护 13
- SAN 连接保护
 - 动态多路径 8

W

- 完全目录库复制 31
 - 还原整个目录库 31
- 完全目录库还原 31
- 完全目录库恢复 16
 - 还原整个目录库 17

网络链路保护

- 冗余网络合作 7

X

- 选项 40

Y

- 用户备份 41
- 用户控制的备份 38

Z

- 灾难恢复软件包 15
- 在群集中还原数据 39
- 站点保护
 - 全局群集 13
- 主服务器保护
 - 群集 10
- 专用介质服务器保护
 - 存储单元组 10