Veritas Alta™ Recovery Vault

安全概要

本指南旨在重点介绍 Veritas Alta Recovery Vault 内建的强大安全功能。

有关 Veritas 产品与解决方案的更多信息，请访问 www.veritas.com/zh/cn/。

白皮书 | 2024 年 1 月

目录

修订历史记录

版本	日期	变更	作者
1.00	2022 年 8 月 29 日	初始版本	Neil Glick
1.01	2022 年 12 月 16 日	品牌重塑	Neil Glick
1.01	2023 年 5 月 16 日	新增 Azure ExpressRoute 内容	Neil Glick
1.03	2023 年 11 月 19 日	新增令牌、AWS Direct Connect 和更新内容	Neil Glick

引言

Veritas Alta Recovery Vault 是基于云构建的数据保管库，可运用虚拟气隙隔离技术以防篡改方式隔离云中的异地数据副本，从而避免应用程序和基础设施中的备份数据成为被攻击的目标。Veritas Alta Recovery Vault 让您省去为隔离备份数据而构建、管理或保护物理站点的麻烦。

在由多个云服务提供商 (CSP) 共同托管的 Veritas 安全租户中，Veritas Alta Recovery Vault 客户可以保护自己的 NetBackup™ 压缩数据和复制数据。大多数存储即服务 (STaaS) 提供商采用责任共担模式，这表示他们不会为客户提供任何数据保护措施。CSP 数据保护责任完全由客户承担。但使用 Veritas Alta Recovery Vault 的客户具有如下优势：

- 所有应用程序数据均可完全备份和恢复
- 快速灵活的数据恢复
- 安全灵活的配置

必要信息

联系 NetBackup 客户经理，这是您使用 STaaS 的第一步。客户经理将收集必要信息，为您配置 Veritas Alta Recovery Vault 存储帐户。您可能需要向 Veritas 提供一些信息，例如：

- 云服务提供商
- 数据中心所在区域
- 存储桶数量
- 存储桶大小（1.2 PB/磁盘卷）
- Veritas 客户代表
- Veritas 合作伙伴名称
- 防篡改支持

注意：Veritas Alta Recovery Vault 仅提供防篡改存储。

防篡改功能/WORM

您可以使用防篡改功能/WORM，对 Veritas Alta Recovery Vault 存储内容执行一次写入、多次读取的操作，并设置映像保留时间。如有威胁行为者/恶意软件入侵，防篡改功能会阻止其对您存储在 Veritas Alta Recovery Vault 中的备份映像执行过期处理，或以任何方式操纵数据。

Veritas Alta Recovery Vault 目前支持治理模式（又称为企业模式）。启用了防篡改功能的治理模式授予用户特殊权限，使其可以关闭保留锁定并删除映像。

注意：必要时，只有云管理员用户有权关闭保留锁定并删除映像。

向 Veritas 发送存储请求时，由 Veritas 创建的 Veritas Alta Recovery Vault 存储桶将启用防篡改功能。此时必须使用启用了防篡改功能的治理模式创建 NetBackup 云存储单元，确保以防篡改方式写入数据。

基于令牌的短期有效身份验证

在 NetBackup 10.2 及更高版本中，您可以使用 Veritas 提供的基于令牌的凭据连接 Azure 中的 Veritas Alta Recovery Vault 云存储。在 NetBackup 零信任模式下，当通过凭据管理机制（使用短期有效的令牌，而不是标准凭据）验证用户或设备的身份时，基于令牌的凭据使安全性提高，大幅缩小了风险窗口。这是一种全新的 SAS 机制，将刷新令牌作为安全登录的输入验证，并在现有令牌到期前定期生成新的访问令牌。这项功能目前仅适用于 Azure 用户。

Azure 用户将获得连接 Veritas Alta Recovery Vault 存储所需的存储帐户和刷新令牌。拥有这些新信息后，您就可以在凭据管理中创建凭据。

基于角色的访问控制 (RBAC)

内置于 NetBackup 的 Veritas Alta Recovery Vault 能够在您的环境中应用基于角色的访问控制 (RBAC)。目前无 NetBackup 访问权限的用户可以通过 RBAC 进行访问。对于目前拥有管理员访问权限的 NetBackup 用户，您也可以根据他们在组织中的角色，限制其访问权限和其他权限。

NetBackup for Veritas Alta Recovery Vault 中包含以下相关角色：

1. **管理员**
    a. 此角色有权在 NetBackup Web 用户界面中执行所有操作。
2. **默认安全管理员**
    a. 此角色有权管理 NetBackup 安全内容，如 RBAC、证书、主机、身份提供商和域、全局安全设置以及其他权限。此角色还能查看 NetBackup 的大部分设置和资产，如工作负载、存储、许可证等方面。
3. **默认存储管理员**
    a. 此角色有权配置并管理磁盘存储和云存储。

存储管理系统或管理员必须先修改 MSDP 存储，才能添加云存储层。如果在搭建 Veritas Alta Recovery Vault 的环境中使用了新的介质服务器，则可能还需要安全管理员进行操作。安全管理员无权查看或修改存储配置。

Veritas Alta Recovery Vault 在 NetBackup 中的通信方式

NetBackup 主服务器、介质服务器和客户端基于 TLS 架构进行通信。此架构以证书形式托管在主服务器上或由外部证书颁发机构托管，符合 X.509 公钥基础架构 (PKI) 标准。这是 Web 上常见的端点验证形式。云服务提供商也将拥有专属证书，进行 TLS 加密通信。NetBackup 数据去重引擎和云存储层采用云服务提供商证书这种相同的信任机制，进行通信和数据传输。我们的云服务提供商软件包反映了我们目前支持的云解决方案。

请按照《NetBackup 安全和加密指南》中的流程，确保与托管 MSDP 的介质服务器进行安全通信。云服务提供商软件包中的证书已获得 NetBackup 信任，可支持 Veritas Alta Recovery Vault 与 AWS 或 Azure 通信。云服务提供商软件包版本需与 NetBackup 版本适配。

在为 MSDP 设置云存储层时，添加存储帐户信息，然后在 “高级” 部分进行其他安全设置。此操作默认启用 SSL，并且在这里也可使用对象锁定切换防篡改模式。

注意：在 NetBackup 10.2 及更高版本中，主服务器可通过端口 443 与 Veritas Alta Recovery Vault 网络服务器通信，而介质服务器可通过端口 443 与云服务提供商（AWS 或 Azure）通信，并通过端口 80 启用证书吊销列表 (CRL)。如果不想在主服务器上启用端口 443可以使用代理服务器。

至于 NetBackup 10.2 以下版本，只有介质服务器通过端口 443 与 CSP 通信，并通过端口 80 启用 CRL。如果不想在介质服务器上启用端口 443 可以使用代理服务器。

注意：您也可以使用本白皮书中讨论的 Azure ExpressRoute 和 AWS Direct Connect。

Veritas Alta Recovery Vault 安全基础原理与架构

Veritas Alta Recovery Vault 使用介质服务器重复数据删除池-云存储层 (MSDP-C)，直接将内存中的重复数据写入云对象存储。

不同于传统 MSDP-C，云对象存储由 Veritas 管理，每个客户都有专属的存储帐户和密钥 (Azure)、访问密钥 ID/密钥，以及 AWS 中为 MSDP-C 创建的 IAM 角色。此外，客户还可选择为对象存储访问权限设置 IP 地址限制。与外部存储桶通信需要启用端口 443 出站，这样 NetBackup API 才能通过 HTTPS 与云服务提供商的存储桶通信。

Veritas Alta Recovery Vault 底层云存储服务由 Microsoft Azure 和 Amazon Web Services (AWS) 等第三方提供。客户在配置 Veritas Alta Recovery Vault 时，可以选择备份数据的托管位置/区域内的云数据中心。Veritas 不会复制或拷贝您的数据。

数据安全

守护您的数据安全是 Veritas 的首要任务。我们会将客户数据列为高度机密数据，在传输时始终加密。传输服务使用 TLS 1.2 协议并使用 AES-256 加密模块，将加密后的数据全部保存在 Azure Blob 或 AWS 存储中。

NetBackup 数据库中存储的所有凭据都会经过哈希处理，并且也可使用 FIPS 140-2 加密模块进行存储。

注意：目前只有 Windows 支持 FIPS 140-2。

在 NetBackup 10.1 及更高版本中，客户可以使用 NetBackup 恶意软件扫描工具或集成的第三方恶意软件扫描程序（使用客户提供的 Microsoft Defender 或 Symantec 的保护引擎集成）对 Veritas Alta Recovery Vault 存储备份进行扫描。对于客户的数据恢复要求，NetBackup 用户可以在备份历史中直接查看恢复中的数据是否有恶意软件感染标识，并发出警报提醒，以避免二次感染。

传输中的数据

NetBackup 管理范围内的传输中数据通道加密 (DTE) 选项可针对数据通道协商适用的 TLS 加密路径。此时无法修改数据，也不会影响重复数据删除率。只有 9.1 或更高版本的 NetBackup 客户端才有这项功能。此功能默认关闭，但可通过全局选项配置，或者为特定客户端进行配置。

- **首选关闭（默认设置）：** 规定在 NetBackup 域中禁用传输中数据加密功能。NetBackup 客户端设置可以覆盖这项设置。
- **首选开启：** 规定仅在 9.1 及更高版本的 NetBackup 客户端中启用传输中数据加密功能。配置传输中数据加密 (DTE) 363 即可启用全局传输中数据加密设置。NetBackup 客户端设置可以覆盖这项设置。
- **强制启用：** 规定在 NetBackup 客户端设置为 “自动” 或 “开启” 时，强制启用传输中数据加密功能。选择此选项后，如果 NetBackup 客户端将传输中数据加密功能设置为 “关闭”，或者主机版本低于 NetBackup 9.1，则视为任务失败。

DTE 支持 MSDP 存储，而 “使用 SSL” 是 Blob 或存储桶的默认及建议选项。

客户 MSDP 的 NetBackup 安装和 CSP 之间的数据路径应考虑名称解析和防火墙端口允许的 NetBackup 数据去重流量，按照所需传输路径使用端点。有关更多信息，请参阅《NetBackup 网络端口参考指南》。有关此通信段的其他安全问题不在 Veritas 的控制范围内。

已存储的数据

NetBackup 使用 MSDP 重复数据删除功能，对存储在 Veritas Alta Recovery Vault 的数据进行存储优化，并结合使用了数据加密密钥以及密钥加密密钥。其中，密钥加密密钥可以通过 NetBackup 内置的密钥管理服务 (KMS) 或支持密钥管理互操作性协议 (KMIP) 的外部 KMS 进行配置。NetBackup 采用 AES 256 位加密并支持 FIPS 140-2 加密模块。在将数据写入（Azure 支持的）Veritas Alta Recovery Vault 对象存储时，保存的 Azure Blob 数据还会使用 Microsoft Azure 存储加密功能和 Microsoft 托管的密钥，再次进行加密。因此，数据在存储时会经历两次加密操作。

注意： 目前只有 Windows 支持 FIPS 140-2。

在创建存储服务器时，设定为结合使用 MSDP 和 KMS；不支持将 KMS 添加至现有存储服务器。

您可以按需轮换 NetBackup 加密密钥，KMS 外部供应商解决方案也会采取专有控制措施进行密钥轮换。NetBackup KMS 可以在 FIPS 模式下运行，您在此模式下创建的加密密钥也始终符合 FIPS 140-2。

不建议使用 pd.conf 文件启用加密。建议使用 contentrouter.cfg 更改配置。

您可以在创建存储服务器时就启用加密，或者在以下配置文件中配置该选项：

```
[storage location]/etc/puredisk/contentrouter.cfg
```

编辑以下内容：

```
ServerOptions=verify _ so _ references,fast,encrypt
```

外部 KMS 服务器需要使用安全证书来进行身份验证。NetBackup 会在每次操作时向外部 KMS 提交此证书。外部 KMS 负责验证证书，并在确认用户具备所需权限后执行操作。

Azure 使用 Microsoft 托管密钥，通过 Azure 的存储加密对存储中的数据进行加密。AWS 使用 Amazon S3 托管密钥 (SSE-S3)，对存储数据进行加密。

防篡改功能/WORM

您可以使用防篡改功能/WORM，对 Veritas Alta Recovery Vault 存储服务执行一次写入、多次读取的操作，并设置映像保留时间。如有威胁行为者/恶意软件入侵，防篡改功能会阻止其对您存储在 Veritas Alta Recovery Vault 中的备份映像执行过期处理，或以任何方式操纵数据。

Veritas Alta Recovery Vault 目前支持治理模式（又称为企业模式）。启用了防篡改功能的治理模式授予用户特殊权限，可以在关闭保留锁定后删除映像。

注意：只有云管理员用户有权根据需要关闭保留锁定并在之后删除映像。Veritas Alta Recovery Vault 的云管理员是 Veritas。

向 Veritas 发送存储请求时，由 Veritas 创建的 Veritas Alta Recovery Vault 存储桶将启用防篡改功能。此时必须使用启用了防篡改功能的治理模式创建 NetBackup 云存储单元，确保以防篡改方式写入数据。

注意：有关防篡改功能和 msdpcldutil 命令的更多信息，请参阅以下《NetBackup 重复数据删除指南》资源：

- veritas.com/support/zh_CN/doc/25074086-159245004-0/v152917675-159245004
- veritas.com/support/zh_CN/doc/25074086-149019166-0/V149102641-149019166

数据删除

有些数据应长期保留，除非您取消、终止或因欠费而暂停保留服务。

除法律或法院命令另有规定外，在发生上述适用的数据服务停用事件后三十 (30) 天内，停止服务的 Veritas Alta Recovery Vault 客户数据将予以删除，且不可恢复。

若客户数据存储于 Azure 或 AWS，客户自行处理和删除所拥有的数据。Azure 或 AWS 会根据其标准，在删除数据后消除痕迹和进行处置，请见如下参考资料：

Azure：数据删除规定请见《Azure 数据保护》文档第 21 页：
go.microsoft.com/fwlink/p/?LinkID=2114156&clcid=0x409&culture=en-us&country=US

AWS：如何删除 Amazon S3 对象和存储桶？探讨 AWS S3 存储桶数据的不同删除方法：
aws.amazon.com/premiumsupport/knowledge-center/s3-delete-objects-and-buckets/

数据处理

Veritas 在制定的策略中阐明了通过适当的控制措施进行信息分类的方法。《Veritas 信息分类与处理方法》明确规定了数据分类、标记和保护要求。信息的分类依据包括自身价值、法律要求、敏感级别、对组织的重要性，以及针对不同信息类别制定的信息处理协议。Veritas 参考上述因素，将数据划分为公共数据、机密数据或高度机密数据。

客户数据被视为高度机密数据，只有部分员工和承包商能够根据最小权限规则进行处理。最小权限规则是指，只有获得管理层特别授权的人员才能访问数据。此访问权限将授予单独用户帐户，用于执行其角色需承担的有限工作责任。

代表 Veritas 按照合同规定提供服务的各方必须遵守 Veritas 制定的安全策略标准。《Veritas 提供商安全要求》阐明了签约期间针对 MS Azure 等第三方提供商制定的安全控制与合规性措施。所有相关方还可以登录 veritas.com/zh/cn/company/privacy，查看提供商（分包商）数据处理条款选项卡下的合同条款：

veritas.com/content/dam/Veritas/docs/policies/DATA%20PROCESSING%20TERMS%20FOR%20PROVIDERS%20(with%20new%20SCCs).pdf

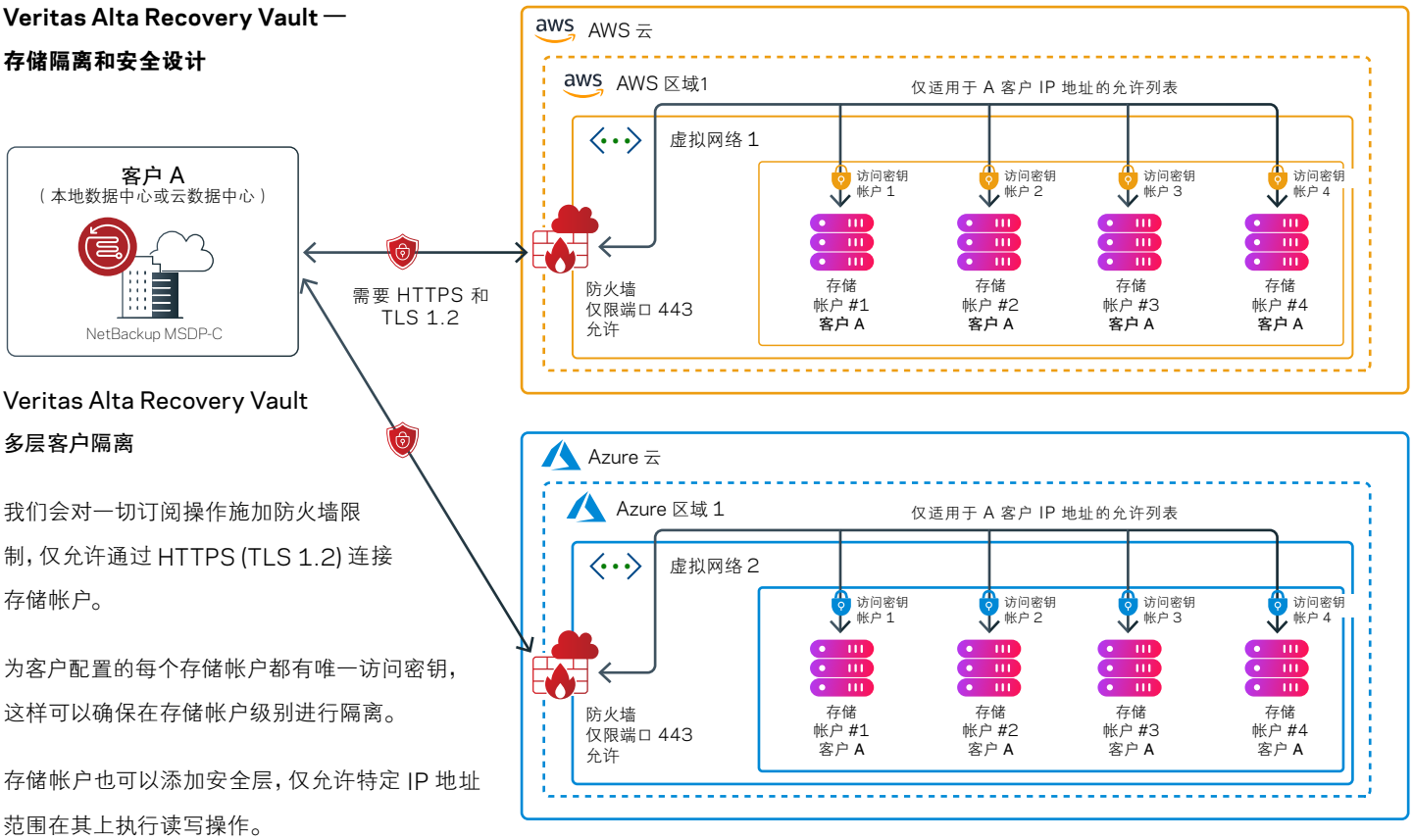
网络/硬件要求

NetBackup 通过 NetBackup MSDP-C 服务器将数据写入 Veritas Alta Recovery Vault。介质服务器上的 MSDP 角色需要满足以下硬件要求：

- MSDP 池（仅块存储）的硬件要求：严格遵循 NetBackup 8.2 的 MSDP 指导。保持 NetBackup 备份一体机的最大容量为 960 TB，BYO MSDP 的最大容量为 400 TB。
- 存储池（仅对象存储）的硬件要求：1 PB 最大容量和 196 GB 内存。对于每个云逻辑存储单元 (LSU)，本地存储可用容量默认设置为 1 TB，文件系统的整体利用率不应超过 90%。
- 对象和块混合存储的硬件要求：与存储池（仅本地存储）的硬件要求类似。总容量上限为 1.2 PB。
- 操作系统：可在运行于 Red Hat Linux Enterprise 或 CentOS 平台的存储服务器上配置云 LSU。客户端和负载均衡服务器无平台限制。

Veritas Alta Recovery Vault 网络容量很大程度将取决于异地发送的数据量及数据传输至云服务提供商所需的速度。Veritas Alta Recovery Vault 必须启用端口 443 传出数据，从而可以通过 HTTPS 与云服务提供商进行通信。

Veritas Alta Recovery Vault — 存储隔离和安全设计



Veritas Alta Recovery Vault 多层客户隔离

我们会对一切订阅操作施加防火墙限制，仅允许通过 HTTPS (TLS 1.2) 连接存储帐户。

为客户配置的每个存储帐户都有唯一访问密钥，这样可以确保在存储帐户级别进行隔离。

存储帐户也可以添加安全层，仅允许特定 IP 地址范围在其上执行读写操作。

图 1. Veritas Alta Recovery Vault — 存储隔离和安全设计

Azure 和 AWS 的 IP 地址范围

如有客户想将 AWS 和/或 Azure IP 地址范围加入允许列表，以连接 Microsoft 或 Amazon，请参阅以下网站：

Azure：microsoft.com/en-us/download/confirmation.aspx?id=56519

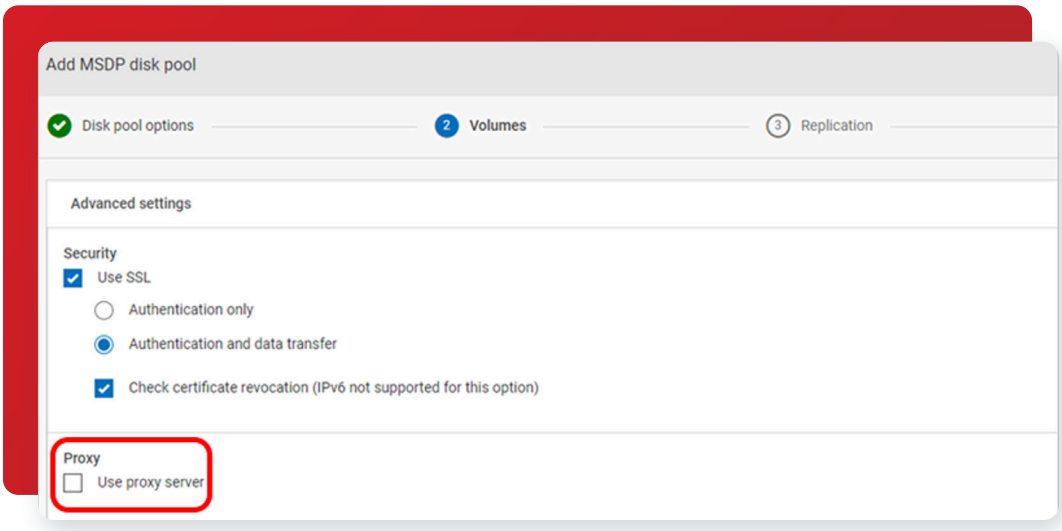
AWS：docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html

替代网络连接

Veritas 发现标准连接方式可能无法满足所有客户需求。因此，Veritas 支持以下替代连接方法（除了通过出站端口 443 进行 HTTPS 连接）。

代理服务器

当端口 443 和端口 80 无法启用时，可以改用代理服务器。有关更多信息，请参阅《NetBackup 重复数据删除指南》。



Azure ExpressRoute 的 Microsoft 对等互连

如果要在 Azure 中使用 Azure ExpressRoute 连接到 Veritas Alta Recovery Vault 存储，客户应该使用 Azure ExpressRoute 的 Microsoft 对等互连，而非 Azure 专用对等互连。具体区别请参见 Microsoft 官网说明：docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings。

以前，Microsoft 使用配置了 ExpressRoute 的对等互连发送公共 IP 地址的所有前缀。但现在，客户需要先配置路由筛选器（一种边界网关协议 (BGP) 社区值，用于筛选想要接收的前缀），将其配置为客户所选存储区域（如美国东部或美国西部 2 区），以执行 Veritas Alta Recovery Vault Azure 存储操作。

有关客户想要接收的地址前缀，请查看 Microsoft 关于设置路由筛选器的指南：
learn.microsoft.com/en-us/azure/expressroute/how-to-routefilter-portal

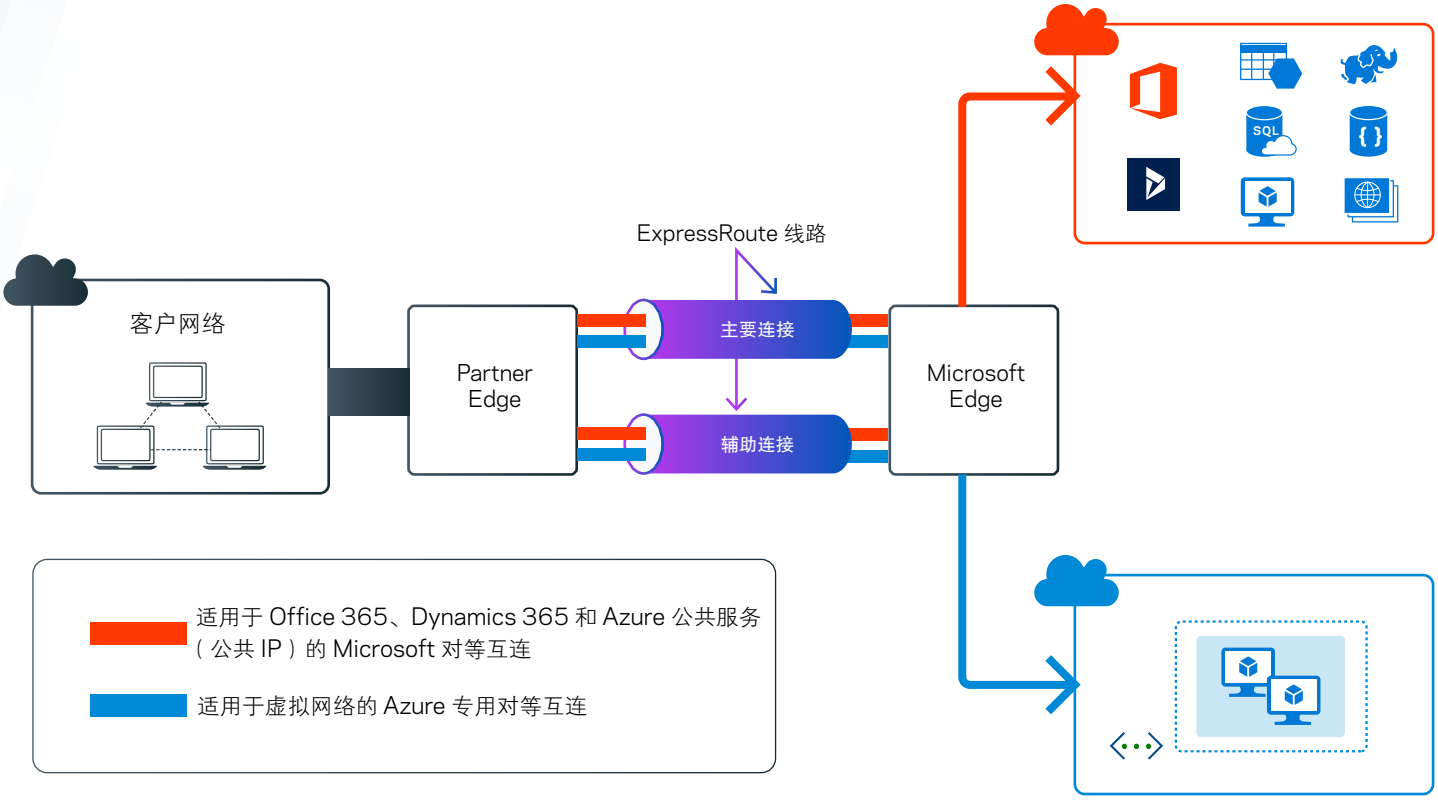


图 2. 与 Veritas Alta Recovery Vault 兼容的 Microsoft ExpressRoute 配置

有关 AWS Direct Connect 测评的更多信息，请参见《Veritas Alta Recovery Vault ExpressRoute 概述指南》。

Microsoft 虚拟网络对等互连

Veritas 不建议将 Microsoft 虚拟网络对等互连应用于 Veritas Alta Recovery Vault。因为使用虚拟网络对等互连备份并恢复数据的成本过高。在同一区域内进行虚拟网络对等互连的成本最低，对入站和出站流量的收费为 0.01 美元/GB，且此费用由对等网络两端共同支付。Veritas 和最终用户在不同区域间的数据传输成本增长 3.5 到 16 倍，具体因所在区域而异。

此外，使用虚拟网络对等互连时，要求 IP 地址不能重叠，并且 Veritas Alta Recovery Vault 必须是多租户环境。因为很多客户使用相同 Veritas Azure 订阅来连接存储，这可能与未来客户的 IP 地址范围重叠，导致我们无法支持未来客户的请求。

AWS Direct Connect 托管连接

Veritas Alta Recovery Vault 经测评认证，可以通过托管连接方式使用 AWS Direct Connect。AWS Direct Connect 通过标准的以太网光纤电缆将您的内网链接至 AWS Direct Connect 位置。电缆两端分别连接着您和 AWS Direct Connect 的路由器。成功建立连接后，您就可以绕过网络上的互联网服务提供商，创建直通公共 AWS 服务（如 Amazon S3）或 Amazon VPC 的虚拟接口。从 AWS Direct Connect 位置还可以访问关联区域内的 AWS 服务。您也可以使用公共区域或 AWS GovCloud (US) 中的单一连接，访问其他公共区域内的公共 AWS 服务。

传输数据时，网络流量仍位于 AWS 全局网络，不会进入公共互联网，有效避免流量限制或意外增加延迟。新建连接时，您可以选择 AWS Direct Connect 合作伙伴提供的托管连接或者 AWS 专有连接，然后部署到全球 100 多个 AWS Direct Connect 位置。有关更多信息，请访问 aws.amazon.com/directconnect。

下图简要概述了 AWS Direct Connect 如何连接您的网络。

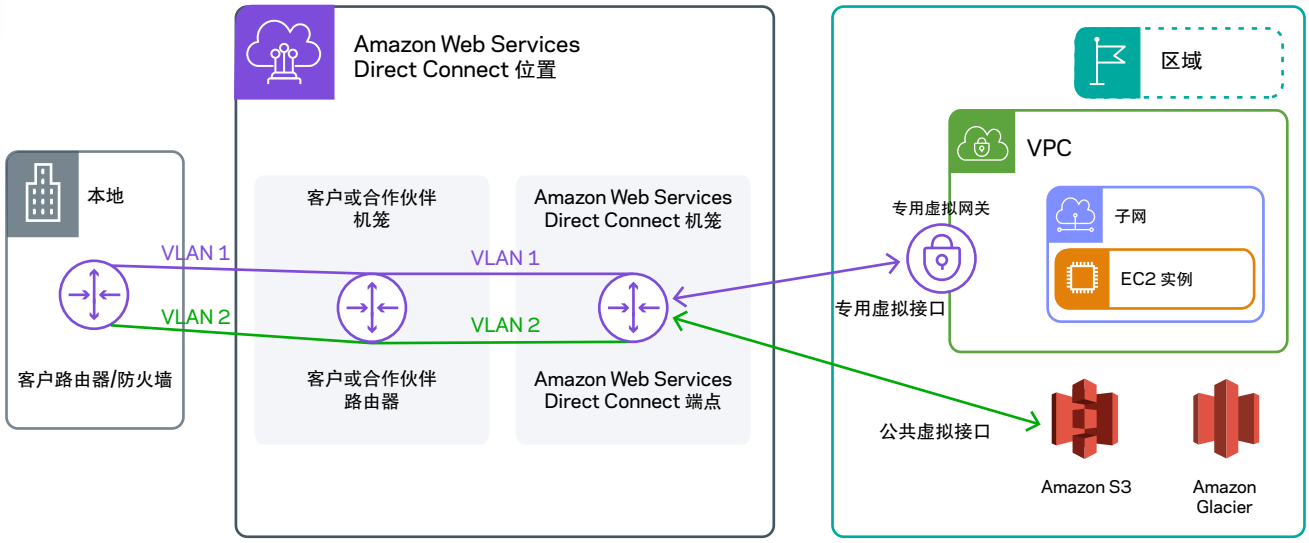


图 3. AWS Direct Connect 连接概述

有关 AWS Direct Connect 测评的更多信息，请参见《Veritas Alta Recovery Vault Direct Connect 概述指南》。

常见问题解答

问：现有卷可以启用 WORM 吗？

答：您在现有卷上无法启用 WORM，但可以新建 WORM 磁盘卷。Veritas Alta Recovery Vault 仅支持 WORM。

问：除创建新卷外，我们是否还需要 Veritas 配置团队提供其他 WORM 支持措施？

答：要配置 WORM，您需要配置团队提供支持 WORM 功能的证书。

问：对于需要使用 Veritas Alta Recovery Vault 防篡改存储 (WORM) 的客户，是否要将 NetBackup 9.1.01 升级至 NetBackup 10？

答：Azure 客户必须升级到 NetBackup 10 才能使用 WORM。AWS 客户可以继续使用 9.X 版本。

问：《Veritas Alta Recovery Vault for NetBackup 技术说明》(veritas.com/support/zh_CN/article.100051821) 提示要限制 I/O 流。对此能否提供限制设置指导？

答：如不取消“有限 I/O”流选择，则默认值为“无限”，这可能会影响性能。建议从较低值开始逐步增加。先设置为 2，观察性能并进行调整。不要等到连接饱和再增加流数，那将无济于事。

问：Veritas Alta Recovery Vault 是否提供适合数据复制的网络带宽？

答：NetBackup 使用 MSDP-C 将数据写入 Veritas Alta Recovery Vault。客户可以和任何其他 MSDP-C 目标一样采用相同网络选项。

问：如果要使用 Azure 中的 Veritas Alta Recovery Vault 防篡改存储，除了升级至 NetBackup 10 软件外，是否还要将设备软件更新至版本 5？

答：是的。有关必要 EEB 的更多信息，请参阅《Veritas Alta Recovery Vault 部署指南》和访问 Veritas 下载中心。

- veritas.com/content/support/zh_CN/doc/NetBackupRecoveryVaultGuide
- veritas.com/content/support/zh_CN/downloads

问：Veritas Alta Recovery Vault 能否在不做出重大变更的情况下，与现有环境集成？

答：可以。您应能够在不中断当前环境的情况下，将数据分层存储至 Veritas Alta Recovery Vault。

问：是否存在与你们所提供服务相关的文档？比如 SLA 文档和性能文档等？

答：服务描述中介绍了正常运行时间 SLA，如下：

Veritas SLA 为服务提供的正常运行时间应达到 99.9% 或更高。

正常运行时间是指 Veritas 事件管理系统报告的客户能够访问服务的时间。访问权限是指客户能够按照本服务说明成功登录并使用服务功能。

正常运行时间为百分比值，每个自然月都会计算。每月正常运行时间百分比为自然月达成的正常运行时间的总分钟数除以自然月总分钟数。

我们使用 Azure 和 AWS 原生存储，其性能足以满足用户的预期要求。我们对存储采取的是带外管理，不会产生额外开支。

问：我们是采用推送模式将数据从 NetBackup 推送至 Veritas Alta Recovery Vault，还是采用拉取模式，通过端口 443 将数据从 Veritas Alta Recovery Vault 拉取至 NetBackup？

答：所有数据移动均由原生 NetBackup 操作驱动。对于 NetBackup 而言，Veritas Alta Recovery Vault 是标准的对象存储目标。

总结

Veritas Alta Recovery Vault 可为您的所有数据源提供专门的异地存储库，兼具灵活性与安全性。Veritas Alta Recovery Vault 可与 NetBackup 无缝集成，简化云存储即服务，带来无限扩展可能，同时丝毫不降低安全性或合规性。

资料来源

- 《Veritas Alta Recoery Vault for NetBackup 技术说明》
- 《NetBackup 安全和加密指南》
- 《NetBackup 重复数据删除指南》
- 《NetBackup 备份计划和性能优化指南》
- Azure 位置

- ExpressRoute 线路和对等互连
- 下载 Azure IP 地址范围和服务标签
- 虚拟网络定价
- ExpressRoute 和虚拟网络 VPN 哪个更适合我?
- AWS 位置
- AWS IP 地址范围
- AWS Direct Connect 是什么
- 《Veritas Alta Recovery Vault 部署指南》
- 适用于 Azure Blob、文件、表和队列存储的默认加密方式
- Veritas 下载中心

关于 Veritas

Veritas Technologies 是安全多云数据管理领域的领导者。超过八万家企业级客户，包括 91% 的全球财富 100 强企业，均依靠 Veritas 确保其数据的安全性、可恢复性和合规性。Veritas 在规模化的可靠性方面享有盛誉，可为企业提供抵御勒索软件攻击等网络威胁所需的韧性。我们支持 800 多个数据源、100 多个操作系统以及 1400 多个存储目标，这样的执行能力在业界尚无出其右者。凭借云级备份技术支持，Veritas 正在实现其自治数据管理的战略愿景，帮助您减少运营开销，为您带来更高价值。如需了解更多详细信息，请访问 www.veritas.com/zh/cn/ 或关注 Veritas 官方微信平台：VERITAS_CHINA（VERITAS 中文社区）。

VERITAS

北京市朝阳区东大桥路 9 号
侨福芳草地大厦 A 座 10 层
04-05 单元 100020
咨询服务热线：400-120-4816
www.veritas.com/zh/cn

关于全球联系信息，请访问：
www.veritas.com/zh/cn/company/contact/

V1537 01/24