VERITAS The truth in information.

Veritas Backup Exec

安全和加密

VERITAS BACKUP EXEC

Veritas Backup Exec™ 备份解决方案可让您按照自己的方式，自由备份。您可以选择要备份哪些数据、在哪里存储这些备份以及如何购买这款解决方案。您的数据将在每个阶段都保证安全无虞且高度可用，无论是将本地数据备份至云，保护云中的工作负载，从云中恢复，还是连接至本地存储。Backup Exec 可与各类解决方案兼容，包括以后要增加的解决方案，帮助您从容开展业务。

Backup Exec 提供永久授权许可和定期订阅授权许可两种购买方式，您可按所需功能购买铜版、银版或金版许可证。铜版最为经济实惠；银版的功能最常用；金版包含 Backup Exec 的全部功能。您可根据需备份的前端数据量选择购买。无论您选择哪个许可证组合，均可根据自己的需求购买。

Backup Exec 为您提供全面保护，助您远离外部威胁。意外发生时也不必担忧，因为您的全部关键数据都已得到妥善备份，在短时间内即可轻松恢复。

执行摘要

企业及其数据面临的安全和合规风险比以往任何时候都要严峻。企业要在内部安全地存储数据并备份到异地，这需要确保数据始终得到妥善保护。随着新合规条例不断出台，任何数据丢失都可能会影响企业收入，甚至会产生其他监管和合规问题。

实施加密战略，让企业备份成为撑起数据完整性和可用性的重要支柱。

加密需求高涨

数据盗窃、磁带丢失、勒索软件攻击以及客户记录泄露（包含未加密数据）等新闻频频登上媒体头条。这些事件再次提醒我们，企业要加强对关键且敏感数据的保护，包括在备份过程中创建数据副本。

主要优势

- 采用 128/256 位高级加密标准 (AES) 的工业级加密，减轻数据安全风险
- 在 Backup Exec 和云目标之间通过安全套接字层 (SSL) 连接进行数据传输
- 集成式加密密钥管理系统，易于设置和管理
- 安全控制台管理功能增强了 Backup Exec 控制台的安全性。
- 支持支付卡行业数据安全标准 (PCI DSS) 3.1/3.2
- 使用符合 FIPS 140-2 的软件加密
- 支持 TLS 1.2
- 采用 256 位 AES 对称加密算法保护 Backup Exec 数据库敏感内容
- 支持对使用 T10 加密标准的所有存储设备进行硬件加密
- 确保传输中数据和静态数据均得到加密保护，实现全面数据安全
- Backup Exec 内置功能，无需额外付费

数据价值越高，敏感数据的风险越大。部分风险包括：

- 出于安全原因而在异地采用未加密的移动介质保存数据，其实质还不如公司其他数据更安全。
- 磁带和可移动介质被窃是一项重要风险，而且由于介质体积小还不容易追踪。
- 如果磁带丢失或未受保护，数据可能落入第三方手里。
- 此外，企业也无从得知磁带是否被复制或拷贝而用于未经授权的用途。
- 使用磁带进行异地存储，通常是因为便宜而并非因为安全。
- 程序员可以对重定向到他们系统的磁带进行未经授权的恢复。

加密是保护便携式介质中数据的最有效方法。分析师、政府、执法和监管机构一直反复强调加密的重要性并提出各种建议，但许多公司仍未在备份过程中实施加密。这背后的主要原因是加密会增加流程的复杂性，也会延长成功完成备份或恢复流程所需的时间。

加密配合 BACKUP EXEC 使用

Backup Exec 提供加密数据的功能。对数据进行加密可使其免遭未经授权的访问，任何要访问加密数据的人必须拥有您创建的加密密钥才能访问。Backup Exec 提供软件加密，也支持某些使用 T10 标准进行硬件加密的设备。一旦您指定了备份作业的存储设备，Backup Exec 便会配置加密。

Backup Exec 支持两种加密安全级别：128 位和 256 位高级加密标准 (AES) 。256 位 AES 加密的安全级别更高，因为 256 位 AES 的密钥长于 128 位密钥。

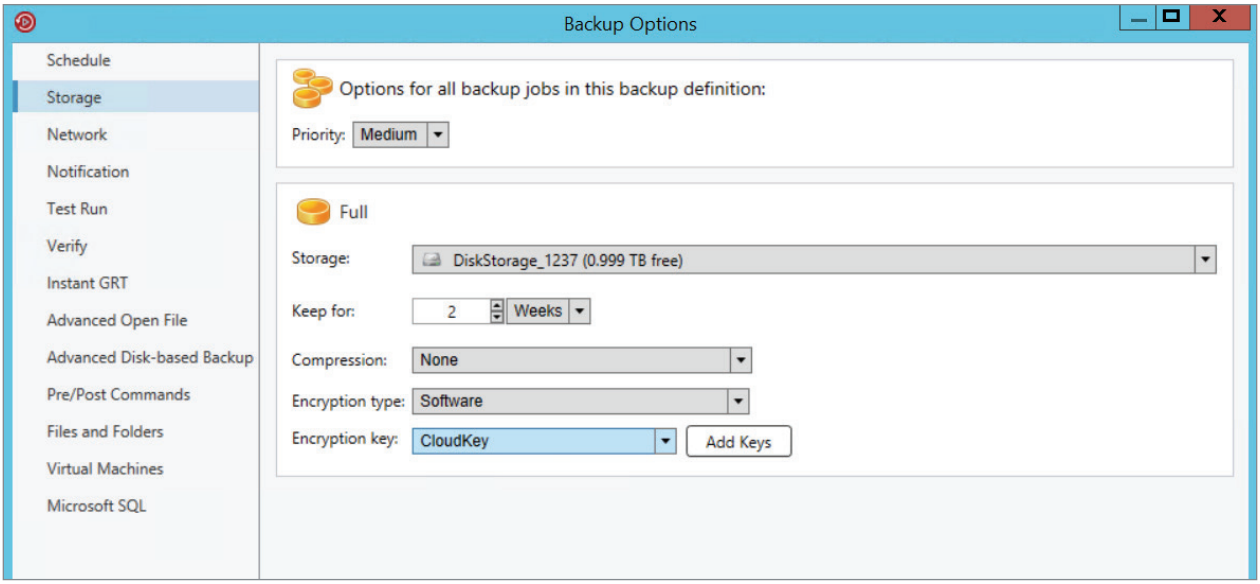

图 1：备份选项下的加密密钥选项

当然，128 位 AES 加密可以更快速地处理备份作业。使用 T10 标准的硬件加密需要 256 位 AES。运行复制备份作业时，已加密的任何备份集不会重新加密。但是，您可以对没有加密的备份集进行加密。

如要深入了解 Backup Exec 用于软件加密的高级加密标准 (AES)，请参阅如下文档：
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

软件加密

安装 Backup Exec 时，安装程序会在 Backup Exec 服务器和使用 Backup Exec 代理的任何远程计算机上安装加密软件。Backup Exec 可以在使用 Backup Exec 代理的计算机上对数据进行加密，然后将加密数据传输到 Backup Exec 服务器。然后，Backup Exec 将加密数据集逐一写入公共云存储目标（AWS、Azure、Google 等）、磁带或磁盘存储。

Backup Exec 可以对下列类型的数据进行加密：

- 用户数据，如文件和 Microsoft Exchange 数据库。
- 元数据，如文件名、属性和操作系统信息。
- 磁带上的编录文件和目录信息。

Backup Exec 不会加密 Backup Exec 元数据或磁盘上的编录文件和目录信息。对备份作业进行加密时，可以使用软件压缩。Backup Exec 首先压缩文件，然后进行加密。但是，如果同时使用加密压缩和软件压缩，备份作业将需要更长的时间才能完成。

Veritas 建议在软件加密时避免使用硬件压缩，硬件压缩可在加密之后执行。在加密过程中，数据会变得随机化。对于已随机化的数据，压缩功能无法有效地工作。

符合联邦信息处理标准 (FIPS) 140-2 的软件加密

Backup Exec 允许您启用符合 FIPS 140-2 标准的软件加密。如果选择该选项，则您必须使用 256 位 AES 加密密钥。此选项仅适用于 Windows 计算机。

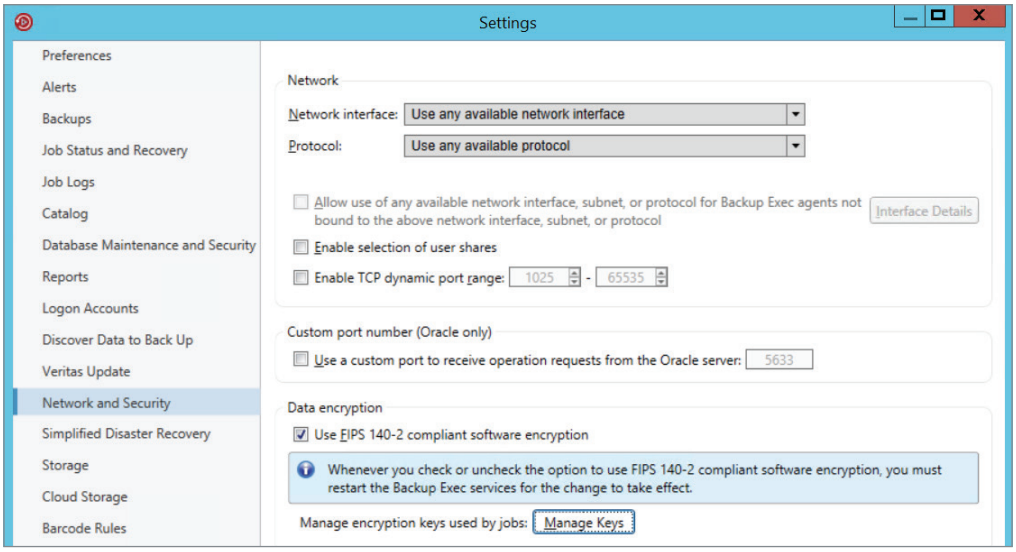

图 2：“网络与安全”下符合 FIPS 140-2 的软件加密选项

某些政府机构（美国及美国以外国家/地区）以及与政府合作的承包商（例如军火承包商）通常需要遵守 FIPS 140-2，以确保加密的正确实施且未被篡改。

有关 FIPS 的详细信息，请参阅以下文章：http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

您可在“关于 Veritas Backup Exec”对话框中查看 OpenSSL/FIPS 版本，如图 3 所示。

硬件加密

Backup Exec 支持对使用 T10 加密标准的所有存储设备进行硬件加密。使用硬件加密时，将数据从主机计算机传输到存储设备，然后在设备上进行加密。Backup Exec 可管理访问加密数据的加密密钥。

Backup Exec 仅支持可实施 T10 加密的设备。

您可通过如下链接找到兼容设备列表：https://www.veritas.com/support/en_US/article.000017788。

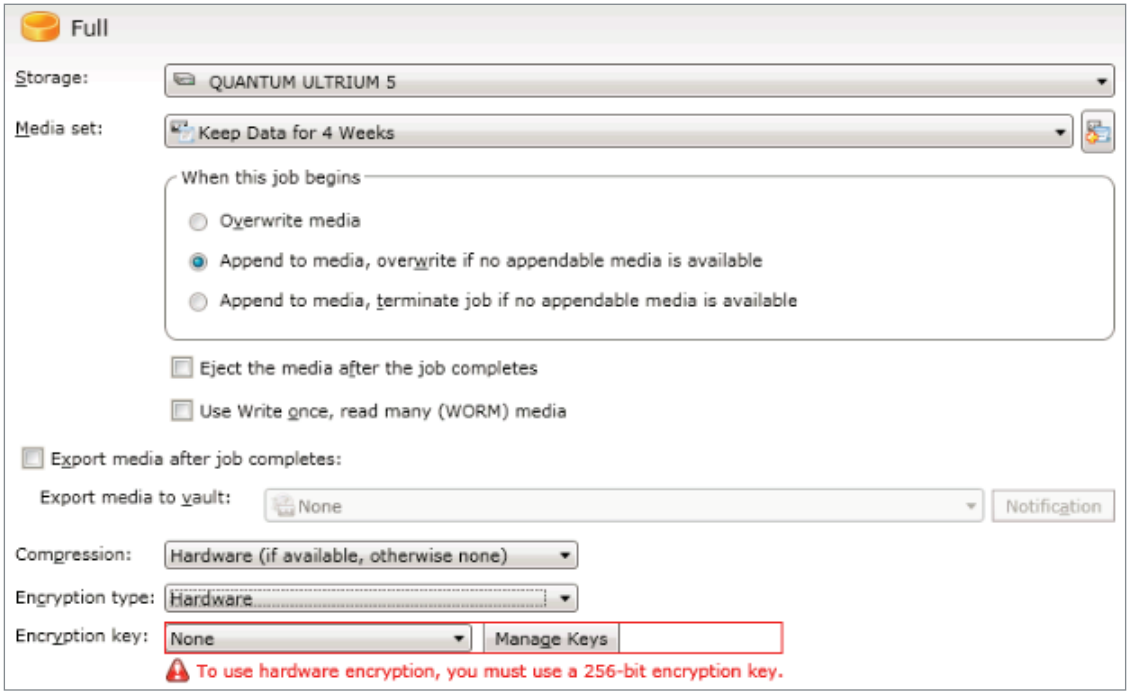

图 3：硬件加密

注意：使用 T10 标准的硬件加密需要 256 位 AES。除非使用至少 16 个字符的密码短语，否则 Backup Exec 不允许启用硬件加密。

加密密钥

必须创建加密密钥才能在 Backup Exec 中使用加密功能。当用户创建加密密钥时，Backup Exec 会基于已登录用户的安全标识符，生成新的标识符来标记该密钥。创建密钥的用户将成为密钥的所有者。

如果对合成备份加密，则所有关联备份都必须使用同一个加密密钥。创建基准备份后，请勿再更改加密密钥。为基准备份选择的加密密钥将自动应用到所有关联备份。

选择要还原的加密数据时，Backup Exec 会检验数据库中是否存在该数据的加密密钥。如果任何密钥都不存在，则 Backup Exec 会提示您重新创建缺失的密钥。如果在安排了要运行的作业之后删除密钥，作业运行将失败。

如果在运行编录作业时，Backup Exec 找不到加密密钥，Backup Exec 将会发送警报。如果您知道密码短语，则可以重新创建缺失的加密密钥。Simplified Disaster Recovery 支持使用以前加密的备份集恢复计算机。如果您有在备份期间加密的 Simplified Disaster Recovery 备份，“恢复此计算机”向导会提示您输入每个加密备份集的密码短语，以便完成恢复。

受限密钥和通用密钥

Backup Exec 提供以下类型的加密密钥：

加密密钥类型	说明
通用密钥	在备份作业期间，任何人都可以使用该密钥来加密数据，以及还原加密的数据。
受限密钥	在备份作业期间，任何人都可以使用该密钥加密数据，但非密钥所有者的用户必须知道密码短语。如果非密钥所有者的用户尝试还原加密的数据，Backup Exec 将提示该用户提供密码短语。如果您无法提供密钥的正确密码短语，将无法还原数据。

密码短语

加密密钥需要类似于密码的密码短语。密码短语通常比密码长，由若干字符或文本组成。理想的密码短语字符数应介于 8 到 128 个之间。128 位 AES 加密的最小字符数为 8。256 位 AES 加密的最小字符数为 16。Veritas 建议您使用多于最小字符数的密码短语。

注意：使用 T10 标准的硬件加密需要 256 位 AES。除非使用至少 16 个字符的密码短语，否则 Backup Exec 不允许启用硬件加密。

此外，理想的密码短语包含大写和小写字母、数字以及特殊字符的组合。应避免在密码短语中引用文学作品中的语句。

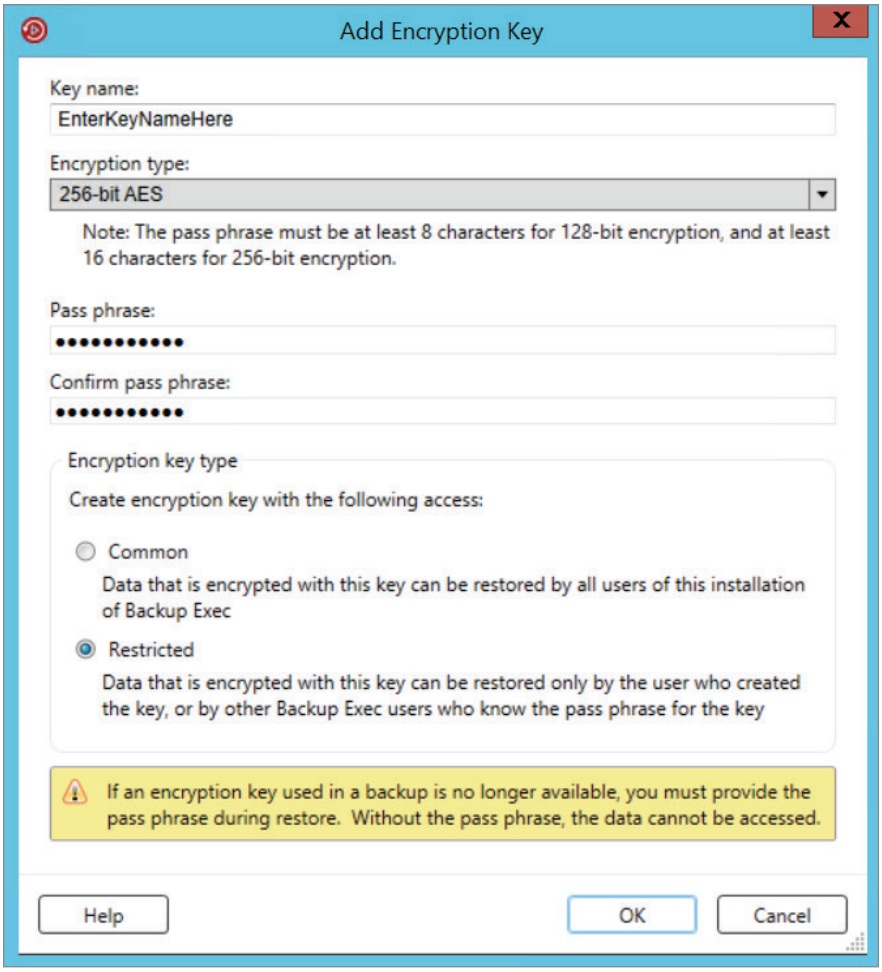

图 4：添加加密密钥

密码短语只能包含可打印的 ASCII 字符，即字符 32 到 126。ASCII 字符 32 是空格字符，可使用键盘上的空格键输入。ASCII 字符 33 到 126 包括：

!" #$%&' ()*+,-./0123456789:;<=>?@
ABCDEFGHIJKLMNOPQRSTUVWXYZ

[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

加密密钥管理

当用户创建加密密钥时，Backup Exec 会基于已登录用户的安全标识符，生成新的标识符来标记该密钥。创建密钥的用户将成为密钥的所有者。

Backup Exec 将密钥存储在 Backup Exec 数据库中。但是，Backup Exec 不会存储密钥的密码短语。每个密钥的所有者负责记住密钥的密码短语。

对于密钥保护，Veritas 建议：

- 将密码短语以书面形式记录下来。保存在一个安全的物理位置，与加密备份集分开保存。
- 备份 Backup Exec 数据库。数据库保存了密钥的记录。

注意：如果未备份 Backup Exec 数据库并且忘记了密码短语，将无法从加密的介质还原数据。在这种情况下，Veritas 也无法还原加密的数据。

在某一 Backup Exec 服务器上创建的密钥是特定于该 Backup Exec 服务器的。不能在 Backup Exec 服务器之间移动密钥。但是，可以使用现有的密码短语在其他 Backup Exec 服务器上创建新密钥。密码短语始终会生成相同的密钥。此外，如果不小心删除了密钥，也可以使用密码短语重新创建。

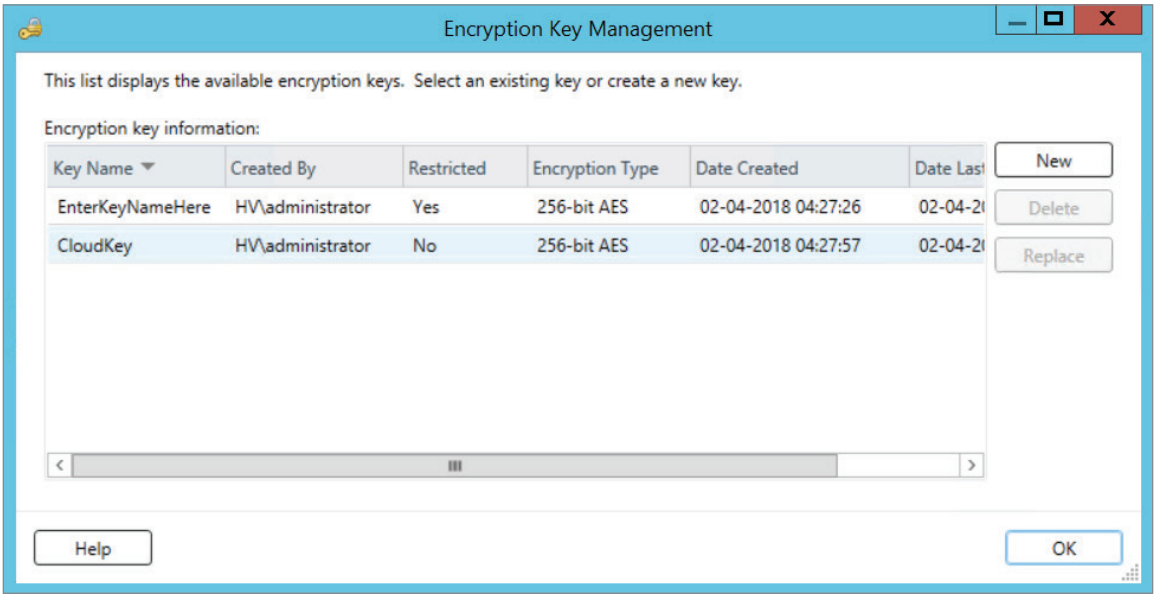

图 5：加密密钥管理

如果 Backup Exec 服务器上的 Backup Exec 数据库已损坏并且被新数据库取代，您必须手动重新创建存储在原始数据库中的所有加密密钥。

如果将数据库从一台 Backup Exec 服务器移到另一台 Backup Exec 服务器，则只要新 Backup Exec 服务器满足以下条件，加密密钥就保持不变：

- 与原始 Backup Exec 服务器具有相同的用户帐户。
- 与原始 Backup Exec 服务器在同一个域中。

跟踪加密密钥的更改

Backup Exec 内置全面审核日志记录功能，可跟踪对 Backup Exec 设置做出的大部分配置更改，包括对加密密钥的更改。审核日志功能可通过 Backup Exec 控制台的“工具/审核日志”菜单进行访问（参见图 5）。

Backup Exec 审核日志跟踪：

- 新加密密钥的创建
- 加密密钥的删除
- 加密密钥的修改
- 做出更改的用户的名称
- 更改的日期/时间
- 更改说明

审核日志显示活动的日期和时间、活动的执行者、活动内容以及活动说明。

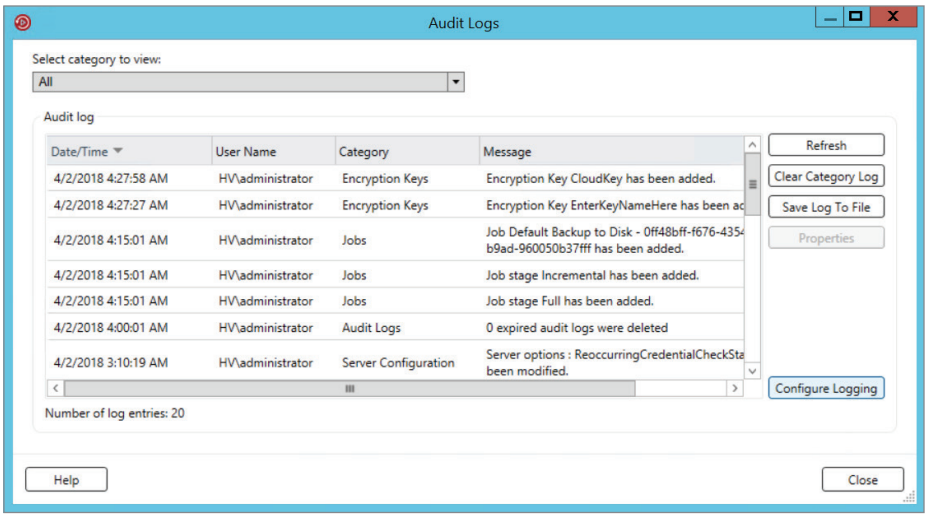

图 6：审核日志

BACKUP EXEC 数据库加密密钥

Backup Exec 加密敏感信息后将其存储在 Backup Exec 数据库中。安装或升级 Backup Exec 时，它会自动创建一个数据库加密密钥。使用数据库加密密钥加密的信息有：登录帐户凭据、用于加密备份作业的密钥等。数据库加密密钥存储在 Backup Exec 安装目录的 Data 文件夹中。

图 7：主屏幕上的数据库加密密钥

对于以下每种情形，都必须提供 Backup Exec 数据库加密密钥：

- 对 Backup Exec 服务器执行手动灾难恢复
- 使用 Simplified Disaster Recovery (SDR) 对 Backup Exec 服务器执行灾难恢复
- 将 Backup Exec 从一台计算机迁移到另一台计算机
- 解决 Backup Exec 服务器上的数据库加密密钥损坏或缺失的任何情况

Veritas 建议将 Backup Exec 数据库加密密钥导出到一个安全的位置，以便以后需要时进行访问。确保数据库加密密钥导出的位置满足以下条件：

- 位于某个驱动器盘号下的物理卷，或 UNC 路径指定的网络共享（不支持映射到驱动器盘号的网络共享）
- 具有足够的磁盘空间
- 可从 Backup Exec 服务器进行访问
- Backup Exec 有写入权限

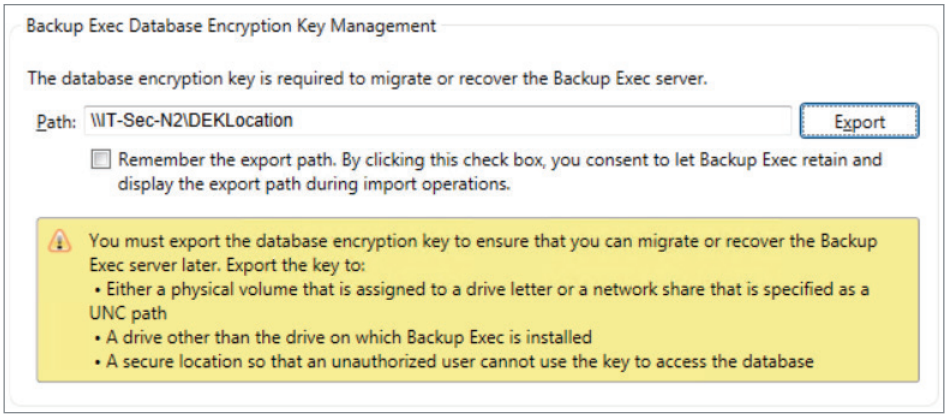

图 8：Backup Exec 数据库加密密钥管理

与 BACKUP EXEC 数据库的安全 SQL 连接

Backup Exec 数据库包含有关企业的敏感信息，例如用户帐户凭据和已备份数据等。保护 Microsoft SQL Server 与 Backup Exec 数据库的连接是防范网络被非法访问的重要一步。Microsoft 建议，只要 SQL Server 与应用程序之间的数据传输通过网络，就使用 SSL 加密。

在以下情形中，Backup Exec 服务与 SQL 实例之间的数据传输会通过网络：

- 将 Backup Exec 数据库配置为集中式数据库，其位于 CASO 环境内的中央管理服务器上。对于此情况的某些变化形式，数据传输也可能通过网络，例如当您使用受控 Backup Exec 服务器或使用共享存储时。
- 您可能对 Backup Exec 数据库使用远程 SQL 实例，这样 Backup Exec 服务就必须通过网络访问数据库。

如果您使用名为 BKUPEXEC 的本地默认 SQL Express 实例，则 Backup Exec 将自动启用 SSL 加密。如果您配置 Backup Exec 使用其他任何 SQL Server 实例，则必须自行配置加密。

SQL Server 使用证书加密数据。您可以生成自己的证书，也可以让 SQL Server 使用自动生成的自签名证书。默认情况下，Backup Exec 使用 SQL Server 自动生成的自签名证书。但是，Veritas 建议您创建并使用自己的证书以增强安全性。

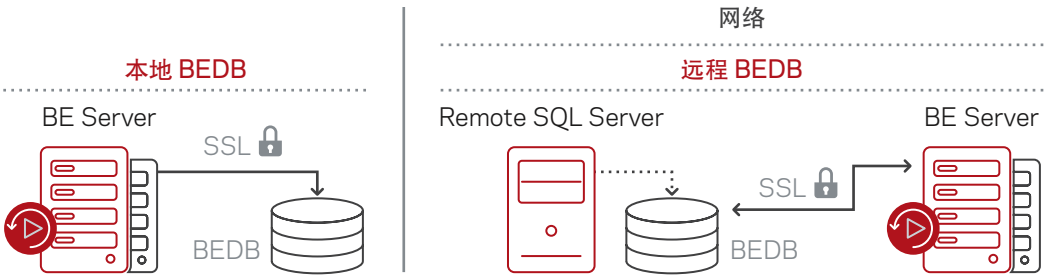

图 9：安全 SQL 连接

注意：使用加密可能影响 SQL Server 和 Backup Exec 数据库之间的通信性能。因为这会在网络中加入一次额外的往返过程，并且加密和解密数据需要时间。

有关安全套接字层 (SSL) 和加密与 SQL Server 的连接的详细信息，请参考 Microsoft 知识库。

如果您对 SQL Server 使用自己的证书，则必须遵循 Microsoft 的要求。证书可以是自签名的，也可以由证书颁发机构颁发。证书颁发机构既可以是您组织中的当地机构，也可以是已知的第三方机构。

有关 Microsoft 证书要求的更多信息，请参阅以下 Microsoft 文章：加密与 SQL Server 之间的连接。

配置加密之前，必须将要使用的证书导入承载 Backup Exec 数据库的计算机的本地证书存储中。

有关如何在服务器上导入和安装证书的更多信息，请参阅以下 Microsoft 文章：操作方法：启用与数据库引擎（SQL Server 配置管理器）之间的加密连接。

导入证书时，您应使用运行 SQL Server 服务的同一用户帐户

使用 SSL 的网络安全层 (NSL)

Backup Exec 提供的 SSL 可支持代理和 Backup Exec 服务器，为跨 WAN、公有云或私有云传输备份数据的公司提供额外的安全保护。更高的安全性有助于您确保通过公共互联网发送的备份数据安全无虞。

证书现在与 SSL 结合使用，以确保远程代理和 Backup Exec 介质服务器之间通过 WAN、LAN 或其他基于互联网传输的任何通信都是安全的。

Backup Exec 在交换任何敏感信息之前，在 Backup Exec 远程代理和 Backup Exec 服务器之间建立信任，以避免发生任何中间人 (MiTM) 问题。这可最大限度降低在代理和 Backup Exec 服务器之间通过网络传输数据的风险。

MiTM 漏洞可能会导致权限升级，致使攻击者在通过身份验证后执行 NDMP 命令。攻击者要想利用漏洞成功入侵，就必须是网络上的授权用户，即使不是授权用户，也要位于网络的授权系统上。

Backup Exec 使用 TLS 1.2（传输层安全）协议在 Backup Exec 服务器和受保护服务器上的代理（支持 Backup Exec 服务器、Agent for Windows 和 Agent for Linux）之间通过 NDMP 建立 SSL 连接控制。

为提高安全性，客户在 NDMP 上对 Backup Exec 服务器和代理之间的连接启用 SSL 控制并使用强密码。TLS 连接可与安全扫描程序配合运行，客户可放心使用 Backup Exec。TLS 1.2 支持 AES-GCM 密码套件，该套件不容易存在密码块链接或 CBC 和 RC4 缺陷。

此外，Backup Exec 使用 SHA-2 证书在 Backup Exec 服务器和代理之间进行 SSL 通信。Backup Exec 服务器、中央管理服务器、受控 Backup Exec 服务器、Agent for Windows 和 Agent for Linux 均支持 SHA-2 SSL 证书。SHA-2 证书的安全性更高。

每个 Backup Exe 服务器都可以成为自己的证书颁发机构 (CA)，不必使用由真实 CA（例如付费的 Verisign）签署的中间证书。它能够签署证书，然后将其部署到远程代理。一旦使用这些证书在 Backup Exec 服务器和远程代理之间建立信任，就可以防御中间人 (MITM) 攻击 Backup Exec 服务器和远程代理之间用于通信的 NDMP 连接。

加密+压缩

如果您对备份作业使用软件压缩和软件加密，Backup Exec 首先压缩文件，然后再加密。这会导致备份速度变慢。

如果您对备份作业使用硬件压缩和软件加密，则数据在压缩之前会被加密。加密导致数据变得随机化，因此无法正确压缩。Veritas 建议在软件加密时避免使用硬件压缩。

BACKUP EXEC 中的安全控制台管理

安全控制台管理功能增强了 Backup Exec 用户界面控制台的安全性。

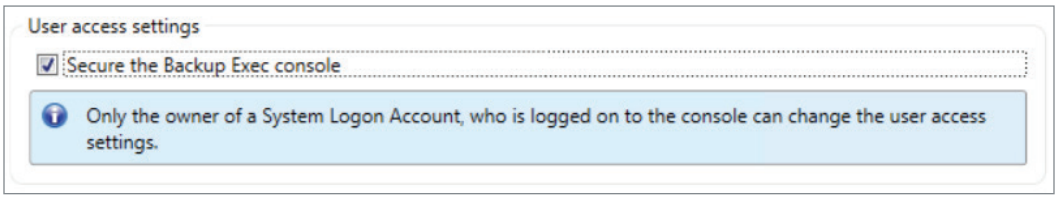

图 10：Backup Exec 中的安全控制台管理

在安全管理控制台中，Backup Exec 提供如下功能：

身份验证

启用安全控制台管理复选框将启用身份验证。因此，当 BE 用户界面启动时，Backup Exec 将不再尝试自动使用已登录的 Windows 用户帐户登录，而是每次用户想要登录 Backup Exec 控制台时都需要输入身份验证凭据。

会话锁定

启用安全控制台管理复选框将启用会话锁定功能。因此，BE 用户界面会话将被锁定，需要重新进行身份验证才能解锁 BE 用户界面。

将防火墙与 BACKUP EXEC 配合使用

在防火墙环境中，Backup Exec 具有以下优点：

- 用于执行备份的网络连接端口数保持在最小数量。
- Backup Exec 服务器和远程系统上的开放端口是动态变化的，因此在浏览、备份和还原操作过程中有着高度的灵活性。
- 可以设置特定的防火墙端口范围，并在这些范围内指定用于执行备份和还原的网络；可以划分特定范围来隔离数据通信并实现高可靠性。

Backup Exec 20.1 版本增强了现有数据入站的防火墙规则，允许用户仅访问所需端口并限制对所有其他端口的访问。这有助于最大限度降低安全漏洞或违规事件发生的概率。

最佳做法

根据常规的最佳做法，Veritas 强烈建议：

- 仅限特权用户访问管理系统。
- 如有必要，仅限受信任/授权的系统进行远程访问。
- 在适用情况下实行最小特权原则，以限制漏洞造成的破坏范围。
- 使用最新的供应商补丁更新所有操作系统和应用程序。
- 采取多层保护，确保安全。采取的保护措施应至少包括运行防火墙和反恶意软件应用程序，对数据的入站和出站进行多点检测，以确保安全。
- 部署基于网络和主机的入侵检测系统，监控网络流量，及时发现异常或可疑的活动迹象。这可有助于检测与潜在漏洞相关的攻击或恶意活动。

- 通过执行以下操作创建强密码短语：
  - 使用的字符数应多于要求的最小字符数。
  - 使用大写和小写字母、数字以及特殊字符的组合。
  - 避免在密码短语中引用文学作品。
  - 安全地保存密码短语。
- 在 FIPS 模式下运行 Backup Exec 服务并使用符合 FIPS 要求的 256 位 AES 加密。
- 如果将数据备份到基于磁盘的存储时不使用软件加密，则使用文件系统加密来阻止未经授权的访问。

向 VERITAS 报告漏洞

Veritas 非常重视产品安全，始终致力于保护产品的正常运行。Veritas Technologies 坚持以主动方式保护软件开发，并在软件开发过程的各个阶段实施安全审查。此外，除保证自身产品、服务的安全外，Veritas 还不遗余力地确保客户数据安全，承诺不断改进其软件的安全流程。

本文档概述了 Veritas Backup Exec 中的安全和加密功能。本文档只是简要的功能概述，并不代表 Backup Exec 软件中安全和加密功能的全部内容。

如果您在 Backup Exec 或任何其他 Veritas 产品中发现了安全问题，请联系 Veritas 授权经销商/合作伙伴或 Veritas 技术支持。

总结

借助 Backup Exec 的全新加密和安全功能，企业可轻松保护关键和敏感数据，远离未经授权的访问和安全威胁。工业级 128 位/256 位 AES OpenSSL 强加密功能，结合 Backup Exec 软件的易用性和灵活性，可帮助您随时随地加密任何所需内容。部署 Backup Exec 的企业可放心地将关键数据存储在任何地方，无论是云平台、虚拟环境还是实体环境。

了解更多详情

Backup Exec 网页	www.backupexec.com
Backup Exec 管理指南	www.backupexec.com/admin
Backup Exec 资源	www.backupexec.com/resources
Backup Exec 兼容性	www.backupexec.com/compatibility
Backup Exec 技术支持	www.backupexec.com/support
Backup Exec 培训	www.backupexec.com/training
Backup Exec 用户论坛	www.backupexec.com/forum
Backup Exec 博客	www.backupexec.com/blogs
Backup Exec 的 60 天试用软件	www.backupexec.com/trybe
Backup Exec 订阅	www.backupexec.com/subscription
Backup Exec 促销	www.backupexec.com/save
PartnerNet	https://partnernet.veritas.com/
查找 Backup Exec 合作伙伴	http://veritas.force.com/public

关于 VERITAS

Veritas Technologies 是全球数据保护及数据管理领域的领导者。超过八万家企业级客户，包括 87% 的全球财富 500 强企业，均依靠 Veritas 化解 IT 复杂度并简化数据管理流程。Veritas 多云数据服务平台可提供自动化的数据保护，无论何处都能协调数据冗灾恢复，确保关键业务数据及应用的 7x24 实时稳定运行，同时也为企业提供数据洞察，实现数据合规。Veritas 在可靠性、扩展性以及灵活按需部署方面拥有很好的声誉，支持超过 800 种数据源，100 多种操作系统，1400 多种存储设备以及 60 类云平台。欲了解更多详细信息，请访问 www.veritas.com 或者关注 Veritas 官方微信平台：VERITAS_CHINA（VERITAS 中文社区）。

Veritas 中国总部
华睿泰科技（北京）有限公司
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/cn

如需了解特定国家或地区的办事处地址
和联系电话，请访问我们的网站：
veritas.com/zh/cn/about/contact.html

VERITAS™

The truth in information.

V0651 03/18