

Barbican服务管理工具

说明

barbican-manage 是一个用来控制密钥管理服务数据库和硬件安全模块（HSM）插件驱动的工具。使用场景包括迁移机密数据库或者在HSM中生成主加密密钥（MKEK）。此命令应该只能由具有管理员权限的用户使用。

操作

执行barbican-manage命令的标准格式如下：

barbican-manage <category> <command> [<args>]

不带参数执行**barbican-manage** 将列出可用命令类别的列表。目前，支持2种类别：db和hsm。

袋类别参数执行命令将列出该类别的命令列表：

- **barbican-manage db --help**
- **barbican-manage hsm --help**
- **barbican-manage --version** 显示barbican服务的版本信息。

接下来介绍barbican-manage的可用类别和参数。

Barbican数据库

barbican-manage db revision [--db-url] [--message] [--autogenerate]

创建新的数据库版本文件。

barbican-manage db upgrade [--db-url] [--version]

升级到指定版本的数据库

barbican-manage db history [--db-url] [--verbose]

显示数据库变更历史。

barbican-manage db current [--db-url] [--verbose]

显示数据库当前版本。

barbican-manage db clean [--db-url] [--verbose] [--min-days] [--clean-unassociated-projects] [--soft-delete-expired-secrets] [--log-file]

清除数据库中的软删除。更详细的文档请查看[数据清理](#)。

barbican-manage db sync_secret_stores [--db-url] [--verbose] [--log-file]

使用barbican.conf文件中的配置同步机密存储数据表。在启用多机密存储和新机密存储启用时有用。

Barbican PKCS11/HSM

barbican-manage hsm gen_mkek [--library-path] [--passphrase] [--slot-id] [--label] [--length]

在HSM中生成新的主加密密钥。主加密密钥将用来加密所有项目密钥。它的标签必须是唯一的。

barbican-manage hsm gen_hmac [--library-path] [--passphrase] [--slot-id] [--label] [--length]

在HSM中创建新的主HMAC密钥。此密钥用来生成加密项目密钥的加密密钥的认证标签。它的标签必须是唯一的。

barbican-manage hsm rewrap_pkek [--dry-run]

在HSM中旋转到新的MKEK和/或HMAC密钥后重新打包项目密钥的加密密钥。执行上述命令时，新的MKEK和HMAC密钥应该以生成。在执行上述命令前，用户应在/etc/barbican/barbican.conf文件中重新配置MKEK和HMAC的标签。