使用机密存储插件

综述

默认情况下，Barbican被配置为在部署中使用一个激活的机密存储插件。这意味着所有新的机密都将使用相同的插件机制（例如，相同的存储后端）来存储。

在OpenStack Newton发行时，加入了支持配置多存储插件后端的功能。作为改变的一部分，客户端可以在项目级别选择首选插件后端来存储它们的机密。

启用多Barbican后端

在特殊的部署/使用情景下，可能需要多个后端支持；通过修改配置即可启用。

为此，Barbican部署时可能在服务配置中添加多个机密存储后端。项目管理员可以预先选择一个后端作为该项目下创建的机密的首选。在该项目下任何新建的机密都将使用首选后端来进行存储。如果没有选择项目级别的存储后端，则新密钥将使用全局机密存储后端。

多插件配置定义如下：

```
[secretstore]
# Set to True when multiple plugin backends support is needed
enable_multiple_secret_stores = True
stores_lookup_suffix = software, kmip, pkcs11, dogtag

[secretstore:software]
secret_store_plugin = store_crypto
crypto_plugin = simple_crypto

[secretstore:kmip]
secret_store_plugin = kmip_plugin
global_default = True

[secretstore:dogtag]
secret_store_plugin = dogtag_plugin

[secretstore:pkcs11]
secret_store_plugin = store_crypto
crypto_plugin = p11_crypto
```

当 *enable_multiple_secret_stores*启用（为真）时，列出的配置部分 *stores_lookup_suffix*列出可供查找的插件名称。此部分名称使用'secretstore：{one_of_suffix}'模式构建。其中一个插件必须明确标识为全局默认值，即 *global_default = True*。只要在服务配置中定义了匹配的部分，那么对所使用的后缀和标签的排序就无关紧要了。

多后端在以下类型的使用场景中非常有用。

- 在部署时，部署者可以使用低安全性机密存储来存储它们的开发/测试资源，例如仅使用软件加密的后端，但可能要使用HSM支持的机密存储用于生产环境。
- 在部署中，对于客户端需要对存储密钥进行高并发访问的某些用例，HSM可能不是一个很好选择。同样的，水平扩展它们以提供更高的可扩展性将带来高昂的成本。
- HSM设备通常具有有限的存储容量，因此部署必须主动监视器存储的密钥大小以保证在限制约束下。由于插件的存储方式不同，这在KMIP的后端比PKCS#11后端更适用。
- barbican作为IaaS服务或平台组件运行，其中某些客户端服务具有安装的合规性要求（例如FIPS），因此这些服务将使用HSM支持的插件，而其他的可能存储密钥到仅软件加密的插件就可以了。