管理安全证书

Active IQ Unified Manager 9.14

NetApp
November 12, 2024

目录

管理安全证书

您可以在 Unified Manager 服务器中配置 HTTPS ，以便通过安全连接监控和管理集群。

查看 HTTPS 安全证书

您可以将 HTTPS 证书详细信息与浏览器中检索到的证书进行比较，以确保浏览器与 Unified Manager 的加密连接不会被截获。

- 您需要的内容 *

您必须具有操作员，应用程序管理员或存储管理员角色。

通过查看证书，您可以验证重新生成的证书的内容，或者查看可用于访问 Unified Manager 的使用者替代名称（ SAN ）。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * HTTPS 证书 * 。

   HTTPS证书将显示在页面顶部

如果您需要查看有关安全证书的详细信息，而不是 HTTPS 证书页面上显示的内容，则可以在浏览器中查看连接证书。

下载 HTTPS 证书签名请求

您可以下载当前 HTTPS 安全证书的证书签名请求，以便将文件提供给证书颁发机构进行签名。CA签名证书有助于防止中间人攻击、并提供比自签名证书更好的安全保护。

- 您需要的内容 *

您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * HTTPS 证书 * 。
2. 单击 * 下载 HTTPS 证书签名请求 * 。
3. 保存 `<hostname>.csr`文件。

您可以将文件提供给证书颁发机构进行签名、然后安装签名证书。

安装 CA 签名并返回的 HTTPS 证书

您可以在证书颁发机构签名并返回安全证书后上传并安装该证书。您上传和安装的文件必须是现有自签名证书的签名版本。CA签名证书有助于防止中间人攻击、并提供比自签名证书更好的安全保护。

- 您需要的内容 *

您必须已完成以下操作：

- 已下载证书签名请求文件并由证书颁发机构签名
- 已以PEM格式保存证书链
- 包括链中的所有证书，从 Unified Manager 服务器证书到根签名证书，包括存在的任何中间证书

您必须具有应用程序管理员角色。

如果创建了 CSR 的证书的有效期超过 397 天，则 CA 会将有效期缩短为 397 天，然后再签署并返回此证书

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * HTTPS 证书 * 。
2. 单击 * 安装 HTTPS 证书 * 。
3. 在显示的对话框中，单击 * 选择文件 ...* 以找到要上传的文件。
4. 选择文件，然后单击 * 安装 * 以安装此文件。

有关信息，请参见 "安装使用外部工具生成的 HTTPS 证书"。

证书链示例

以下示例显示了证书链文件的显示方式：

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

安装使用外部工具生成的 **HTTPS** 证书

您可以安装自签名或 CA 签名的证书，这些证书是使用 OpenSSL ， BoringSSL ， LtsEncrypt 等外部工具生成的。

您应将私钥与证书链一起加载，因为这些证书是外部生成的公共 - 私有密钥对。允许的密钥对算法为 "`RSA` "

和 "`EC` " 。"* 安装 HTTPS 证书 * " 选项位于 "General " 部分的 "HTTPS Certificates" 页面中。上传的文件应采用以下输入格式。

1. 属于Active IQ Unified Manager 主机的服务器的专用密钥
2. 与私钥匹配的服务器证书
3. CA 的证书将反向添加到根证书，用于对上述证书进行签名

使用**EC**密钥对加载证书的格式

允许的曲线为 "`prime256v1` " 和 " `secp384r1` " 。具有外部生成的 EC 对的证书示例：

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

使用**RSA**密钥对加载证书的格式

属于主机证书的RSA密钥对允许的密钥大小为2048、3072和4096。外部生成的*RSA密钥对*的证书：

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

上传证书后，您应重新启动 Active IQ Unified Manager 实例，以使更改生效。

上传外部生成的证书时检查

系统会在上传使用外部工具生成的证书时执行检查。如果任何检查失败，则证书将被拒绝。此外，还会对产品中的 CSR 生成的证书以及使用外部工具生成的证书进行验证。

- 输入中的私钥将根据输入中的主机证书进行验证。
- 系统会根据主机的 FQDN 检查主机证书中的公用名（ Common Name ， CN ）。
- 主机证书的公用名（ Common Name ， CN ）不应为空或空白，不应设置为 localhost 。
- 有效开始日期不应是未来的，证书的有效到期日期不应是过去的。
- 如果存在中间 CA 或 CA ，则证书的有效期开始日期不应是未来的，而有效期到期日期不应是过去的。

输入中的私钥不应加密。如果存在任何已加密的私钥，则系统会拒绝这些私钥。

示例1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

示例2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

示例3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

如果证书安装失败、请参见知识库(KB)文章：https://kb.netapp.com/mgmt/AIQUM/IQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager无法安装外部生成的证书"^]

证书管理的页面说明

您可以使用 HTTPS 证书页面查看当前安全证书并生成新的 HTTPS 证书。

HTTPS 证书页面

您可以通过"HTTPS证书"页面查看当前安全证书、下载证书签名请求、生成新的自签名HTTPS证书或安装新的HTTPS证书。

如果您尚未生成新的自签名HTTPS证书、则此页面上显示的证书是在安装期间生成的证书。

命令按钮

命令按钮可用于执行以下操作：

- * 下载 HTTPS 证书签名请求 *

  下载当前安装的 HTTPS 证书的认证请求。您的浏览器会提示您保存 <hostname>.csr 文件，以便您可以将此文件提供给证书颁发机构进行签名。

- * 安装 HTTPS 证书 *

  用于在证书颁发机构签名并返回安全证书后上传并安装该证书。新证书将在您重新启动管理服务器后生效。

- * 重新生成 HTTPS 证书 *

  用于生成新的自签名HTTPS证书、此证书将替换当前安全证书。新证书将在重新启动 Unified Manager 后生效。

重新生成 **HTTPS** 证书对话框

通过重新生成 HTTPS 证书对话框，您可以自定义安全信息，然后使用该信息生成新的 HTTPS 证书。

当前证书信息将显示在此页面上。

通过 "`使用当前证书属性重新生成` " 和 "`更新当前证书属性` " 选项，您可以使用当前信息重新生成证书或使用新信息生成证书。

- * 公用名 *

  必填。要保护的完全限定域名(FQDN)。

  在 Unified Manager 高可用性配置中，使用虚拟 IP 地址。

- * 电子邮件 *

  可选。用于联系您的组织的电子邮件地址；通常是证书管理员或IT部门的电子邮件地址。

- * 公司 *

  可选。通常是贵公司的法定名称。

- * 部门 *

  可选。公司中部门的名称。

- * 城市 *

  可选。公司所在的城市位置。

- * 状态 *

  可选。您公司所在的州或省/自治区/直辖市(非缩写)。

- * 国家 / 地区 *

  可选。公司的国家/地区位置。这通常是国家/地区的双字母ISO代码。

- * 备用名称 *

  必填。除了现有本地主机或其他网络地址之外、还可以用于访问此服务器的其他非主域名。使用英文逗号分隔每个备用名称。

  如果要从证书的 " 备用名称 " 字段中删除本地标识信息，请选中 "`exclude local Identifying information （ e.go localhost ）` " 复选框。如果选中此复选框，则 " 备用名称 " 字段仅会使用您在字段中输入的内容。如果留空，则生成的证书将根本没有备用名称字段。

- * 密钥大小（密钥算法： RSA ） *

  密钥算法设置为 RSA 。您可以选择以下密钥大小之一： 2048 ， 3072 或 4096 位。默认密钥大小设置为

2048 位。

- * 有效期 *

  默认有效期为 397 天。如果您已从先前版本升级，则可能会看到先前的证书有效期未更改。

有关详细信息，请参见 "正在生成HTTPS证书"。