

图像签名验证

«

(glancemetadefcatalogapi.html)

»

🐞

(https://bugs.launchpad.net/glance/+filebug?field.title=Image%20Signature%20Verification%20in%20glance&field.comment=%0A%0A%0AThis bug tracker is for errors with the documentation, use the following as a template and remove or add fields as you see fit. Convert [] into [x] to check boxes:%0A%0A- [] This doc is inaccurate in this way: ____%0A- [] This is a doc addition request.%0A- [] I have a fix to the document that I can paste below including example: input and output. %0A%0AIf you have a troubleshooting or support issue, use the following resources:%0A%0A - Ask OpenStack: http://ask.openstack.org%0A - The mailing list: http://lists.openstack.org%0A - IRC: 'openstack' channel on Freenode%0A%0A-----%0ARelease:%2016.0.1.dev1%20on%20'Thu%20Mar%201%2007:26:57%202018,%20commit%20968f4ae'%0ASHA:%20968f4ae9ce244d9372cb3e8f45acea9d557f317d%0ASource:https://docs.openstack.org/glance/queens/user/signature.html&field.tags=)

更新日期：'THU MAR 1 07:26:57 2018，COMMIT 968F4AE'

Glance有能力使用数字签名和非对称密码执行图像验证。要触发此操作，您必须定义特定的图像属性（如下所述），并在本地Barbican安装中存储了使用您的私钥签名的证书。

当图像存在图像属性时，Glance会在存储之前根据这些属性验证上传的图像数据。如果验证失败，上传将失败，图像将被删除。

此外，当从Glance下载图像时，图像属性可能会被其他服务（例如Nova）用于执行数据验证。

要求1

Barbican关键经理 - 请参阅<https://docs.openstack.org/barbican/latest/contributor/devstack.html> (https://docs.openstack.org/barbican/latest/contributor/devstack.html).

配置1

可以修改etc / glance-api.conf以更改bar白的关键端点。默认情况下，barbican会尝试连接到 <http://localhost:5000/v3>的 (<http://localhost:5000/v3>) keystone，但是如果keystone在另一台主机上，则应该更改。

在glance-api.conf中找到以下几行：

```
[ barbican ]
auth_endpoint = http://localhost:5000/v3
```

然后将<http://localhost:5000/v3> (<http://localhost:5000/v3>)替换为keystone的URL，并在其末尾添加/v3。例如，'<https://192.168.245.9:5000/v3>' (<https://192.168.245.9:5000/v3>)'。

etc / glance-api.conf中可以配置的另一个选项是使用哪个密钥管理器。默认情况下，Glance将使用由Castellan密钥管理器接口定义的默认密钥管理器，该接口当前是Barbican密钥管理器。

在glance-api.conf中找到以下几行：

```
[ key_manager ]
backend = barbican
```

然后用所需的密钥管理器类替换该值。

✔ 注意

如果这些行不存在，只需将它们添加到文件的末尾即可。

使用签名验证1

一个图像需要一些属性来启用签名验证，这些属性是：

```
img_signature
img_signature_hash_method
img_signature_key_type
img_signature_certificate_uuid
```

物业img_signature 1

这是你的形象的签名。

✔ 注意

最大字符数限制为255。

物业img_signature_hash_method 1

散列方法是你散列的方法。

目前你可以使用的是：

- SHA-224
- SHA-256
- SHA-384
- SHA-512

物业_signature_key_type 1

这是您可以用于图像的key_types。

目前你可以使用的是：

- RSA-PSS
- DSA
- ECC曲线

- SECT571K1
- SECT409K1
- SECT571R1
- SECT409R1
- SECP521R1
- SECP384R1

✔ 注意

ECC曲线 - 只包含384以上的密钥。不是所有的ECC曲线都可能由后端支持。

物业_signature_certificate_uuid 1

这是您上传到Barbican的证书的UUID。

因此传递给目光的类型是：

- UUID

✔ 注意

支持的证书类型是：

- X_509

使用示例1

按照以下说明创建您的密钥：

```
$ openssl genrsa -out private_key.pem 1024
生成RSA私钥，1024位长模数
..... +++++
.. +++++
e是65537 (0x10001)

$ openssl rsa -pubout -in private_key.pem -out public_key.pem
编写RSA密钥

$ openssl req -new -key private_key.pem -out cert_request.csr
您将被要求输入将合并
到您的证书请求中的信息。

$ openssl x509 -req -days 14 -in cert_request.csr -signkey private_key.pem -out new_cert.crt
签名ok
subject = / C = AU / ST = Some-State / O = Internet Widgits Pty Ltd
获取私钥
```

Upload your certificate. This only has to be done once as you can use the same **Secret href** for many images until it expires.

```
$ openstack secret store --name test --algorithm RSA --expiration 2016-06-29 --secret-type certificate --payload-content-type "application/octet-stream"
+-----+
| Field      | Value |
+-----+-----+
| Secret href | http://127.0.0.1:9311/v1/secrets/cd7cc675-e573-419c-8fff-33a72734a243 |
+-----+-----+

$ cert_uuid=cd7cc675-e573-419c-8fff-33a72734a243
```

Get an image and create the signature:

```
$ echo This is a dodgy image > myimage

$ openssl dgst -sha256 -sign private_key.pem -sigopt rsa_padding_mode:pss -out myimage.signature myimage

$ base64 -w 0 myimage.signature > myimage.signature.b64

$ image_signature=$(cat myimage.signature.b64)
```

Note

Using Glance v1 requires '-w 0' due to not supporting multiline image properties. Glance v2 does support multiline image properties and does not require '-w 0' but may still be used.

Create the image:

```
$ glance image-create --name mySignedImage --container格式裸--disk格式qcow2 --property img_signature ="$ image_signature"--property img_signatu
```

注意

如果验证不成功，则创建映像可能会失败。这将导致图像被删除。

其他链接1

- <https://etherpad.openstack.org/p/mitaka-glance-image-signing-instructions> (<https://etherpad.openstack.org/p/mitaka-glance-image-signing-instructions>)
- https://wiki.openstack.org/wiki/OpsGuide/User-Facing_Operations (https://wiki.openstack.org/wiki/OpsGuide/User-Facing_Operations)

field.title=Image%20Signature%20Verification%20in%20glance&field.comment=%0A%0A%0AThis bug tracker is for errors with the documentation, use the following as a template and remove or add fields as you see fit. Convert [] into [x] to check boxes:%0A%0A- [] This doc is inaccurate in this way: ____%0A- [] This is a doc addition request.%0A- [] I have a fix to the document that I can paste below including example: input and output. %0A%0AIf you have a troubleshooting or support issue, use the following resources:%0A%0A - Ask OpenStack: <http://ask.openstack.org> - The mailing list: <http://lists.openstack.org> - IRC: 'openstack' channel on Freenode%0A%0A-----%0ARelease:%2016.0.1.dev1%20on%20Thu%20Mar%202017%2026:57%202018,%20commit%20968f4ae'%0ASHA:%20968f4ae9ce244d9372cb3e8f45acea9d557f317d%0ASo [https://docs.openstack.org/glance/queens/user/signature.html&field.tags=\)](https://docs.openstack.org/glance/queens/user/signature.html&field.tags=))

更新日期：'THU MAR 1 07:26:57 2018，COMMIT 968F4AE'



[\(https://creativecommons.org/licenses/by/3.0/\)](https://creativecommons.org/licenses/by/3.0/)
除另有说明外，本文档受 [Creative Commons Attribution 3.0许可的授权](https://creativecommons.org/licenses/by/3.0/) (<https://creativecommons.org/licenses/by/3.0/>)。查看所有 [OpenStack法律文件](http://www.openstack.org/legal) (<http://www.openstack.org/legal>)。

发现错误？报告错误 ([https://bugs.launchpad.net/glance/+filebug?field.title=Image%20Signature%20Verification%20in%20glance&field.comment=%0A%0A%0Athis%20bug%20tracker%20is%20for%20errors%20with%20the%20documentation%2C%20use%20the%20following%20as%20a%20template%20and%20remove%20or%20add%20fields%20as%20you%20see%20fit%2C%20convert%20%5B%5D%20into%20%5BX%5D%20to%20check%20boxes%3A%0A%0A-%20%5B%5D%20this%20doc%20is%20inaccurate%20in%20this%20way%3A%20____%0A-%20%5B%5D%20this%20is%20a%20doc%20addition%20request.%0A-%20%5B%5D%20i%20have%20a%20fix%20to%20the%20document%20that%20i%20can%20paste%20below%20including%20example%3A%20input%20and%20output.%0A%0Aif%20you%20have%20a%20troubleshooting%20or%20support%20issue%2C%20use%20the%20following%20resources%3A%0A%0A-%20ask%20openstack%3A%20http%3A%2F%2Fask.openstack.org%0A-%20the%20mailing%20list%3A%20http%3A%2F%2Flists.openstack.org%0A-%20irc%3A%20openstack%20channel%20on%20freenode%0A%0A-----%0Arelease%3A%202016.0.1.dev1%20on%20thu%20mar%202017%2026%3A57%202018%2C%20commit%20968f4ae'%0Asha%3A%20968f4ae9ce244d9372cb3e8f45acea9d557f317d%0ASource%3A%20https%3A%2F%2Fdocs.openstack.org/glance/queens/user/signature.html&field.tags=\)](https://bugs.launchpad.net/glance/+filebug?field.title=Image%20Signature%20Verification%20in%20glance&field.comment=%0A%0A%0Athis%20bug%20tracker%20is%20for%20errors%20with%20the%20documentation%2C%20use%20the%20following%20as%20a%20template%20and%20remove%20or%20add%20fields%20as%20you%20see%20fit%2C%20convert%20%5B%5D%20into%20%5BX%5D%20to%20check%20boxes%3A%0A%0A-%20%5B%5D%20this%20doc%20is%20inaccurate%20in%20this%20way%3A%20____%0A-%20%5B%5D%20this%20is%20a%20doc%20addition%20request.%0A-%20%5B%5D%20i%20have%20a%20fix%20to%20the%20document%20that%20i%20can%20paste%20below%20including%20example%3A%20input%20and%20output.%0A%0Aif%20you%20have%20a%20troubleshooting%20or%20support%20issue%2C%20use%20the%20following%20resources%3A%0A%0A-%20ask%20openstack%3A%20http%3A%2F%2Fask.openstack.org%0A-%20the%20mailing%20list%3A%20http%3A%2F%2Flists.openstack.org%0A-%20irc%3A%20openstack%20channel%20on%20freenode%0A%0A-----%0Arelease%3A%202016.0.1.dev1%20on%20thu%20mar%202017%2026%3A57%202018%2C%20commit%20968f4ae'%0Asha%3A%20968f4ae9ce244d9372cb3e8f45acea9d557f317d%0ASource%3A%20https%3A%2F%2Fdocs.openstack.org/glance/queens/user/signature.html&field.tags=)))

问题吗？ (<http://ask.openstack.org>)



OpenStack文档

一瞥16.0.1.dev1

(../index.html)

用户指南 (index.html)

- 图像标识符 (identifiers.html)
- 图像状态 (statuses.html)
- 任务状态 (statuses.html#task-statuses)
- 磁盘和容器格式 (formats.html)
- 常见图像属性 (common-image-properties.html)
- 元数据定义概念 (metadefs-concepts.html)
- 使用Glance的Image Public API (glanceapi.html)
- 使用Glance的客户端工具 (glanceclient.html)

使用Glance的元数据定义目录公共API (glancemetadefcatalogapi.html)

图像签名验证

管理指南 (../admin/index.html)

安装 (../install/index.html)

一览配置选项 (../configuration/index.html)

命令行界面 (../cli/index.html)

一览贡献指南 (../contributor/index.html)

词汇表 (../glossary.html)

页面内容

要求

组态

使用签名验证

属性img_signature

属性img_signature_hash_method

属性img_signature_key_type

属性img_signature_certificate_uuid

使用示例

其他链接

OpenStack的

- 项目 (<http://openstack.org/projects/>)
- OpenStack安全 (<http://openstack.org/projects/openstack-security/>)
- 常见问题 (<http://openstack.org/projects/openstack-faq/>)
- 博客 (<http://openstack.org/blog/>)
- 新闻 (<http://openstack.org/news/>)

社区

- 用户组 (<http://openstack.org/community/>)
- 活动 (<http://openstack.org/community/events/>)
- 工作 (<http://openstack.org/community/jobs/>)
- 公司 (<http://openstack.org/foundation/companies/>)
- 有助于 (<http://docs.openstack.org/infra/manual/developers.html>)

文档

- OpenStack手册 (<http://docs.openstack.org>)
- 入门 (<http://openstack.org/software/start/>)
- API文档 (<http://developer.openstack.org>)
- 维基 (<https://wiki.openstack.org>)

品牌与法律

- 标志和指南 (<http://openstack.org/brand/>)
- 商标政策 (<http://openstack.org/brand/openstack-trademark-policy/>)
- 隐私政策 (<http://openstack.org/privacy/>)
- OpenStack CLA (https://wiki.openstack.org/wiki/How_To_Contribute#Contributor_License_Agreement)

保持联系

(<https://twitter.com/openstack>) (<https://www.youtube.com/user/OpenStackFoundation>)

OpenStack项目是在Apache 2.0许可 (<http://www.apache.org/licenses/LICENSE-2.0>)下提供的。Openstack.org由 Rackspace云计算提供支持 (<http://rackspace.com>)。