Image Signature Verification

« (glancemetadefcatalogapi.html) » (../admin/index.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%0ASour
https://docs.openstack.org/glance/queens/user/signature.html&field.tags=)

UPDATED: 'THU MAR 1 07:26:57 2018, COMMIT 968F4AE'

Glance has the ability to perform image validation using a digital signature and asymmetric cryptography. To trigger this, you must define specific image properties (described below), and have stored a certificate signed with your private key in a local Barbican installation.

When the image properties exist on an image, Glance will validate the uploaded image data against these properties before storing it. If validation is unsuccessful, the upload will fail and the image will be deleted.

Additionally, the image properties may be used by other services (for example, Nova) to perform data verification when the image is downloaded from Glance.

Requirements¶

Barbican key manager - See https://docs.openstack.org/barbican/latest/contributor/devstack.html (https://docs.openstack.org/barbican/latest/contributor/devstack.html)

Configuration¶

The etc/glance-api.conf can be modified to change keystone endpoint of barbican. By default barbican will try to connect to keystone at http://localhost:5000/v3 (http://localhost:5000/v3) but if keystone is on another host then this should be changed.

In glance-api.conf find the following lines:

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

Then replace http://localhost:5000/v3 (http://localhost:5000/v3) with the URL of keystone, also adding /v3 to the end of it. For example, 'https://192.168.245.9:5000/v3 (https://192.168.245.9:5000/v3)'.

Another option in etc/glance-api.conf which can be configured is which key manager to use. By default Glance will use the default key manager defined by the Castellan key manager interface, which is currently the Barbican key manager.

In glance-api.conf find the following lines:

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

Then replace the value with the desired key manager class.

> **Note**
>
> If those lines do not exist then simply add them to the end of the file.

Using the Signature Verification¶

An image will need a few properties for signature verification to be enabled, these are:

```
img_signature
img_signature_hash_method
img_signature_key_type
img_signature_certificate_uuid
```

Property img_signature¶

This is the signature of your image.

> **Note**
>
> The max character limit is 255.

Property img_signature_hash_method¶

Hash methods is the method you hash with.

Current ones you can use are:

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

Property img_signature_key_type¶

This is the key_types you can use for your image.

Current ones you can use are:

- RSA-PSS
- DSA
- ECC-CURVES

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

> **Note**
>
> ECC curves - Only keysizes above 384 are included. Not all ECC curves may be supported by the back end.

Property img_signature_certificate_uuid¶

This is the UUID of the certificate that you upload to Barbican.

Therefore the type passed to glance is:

- UUID

> **Note**
>
> The supported certificate types are:
>
> - X_509

Example Usage¶

Follow these instructions to create your keys:

```
$ openssl genrsa -out private_key.pem 1024
Generating RSA private key, 1024 bit long modulus
...............................................++++++
..++++++
e is 65537 (0x10001)

$ openssl rsa -pubout -in private_key.pem -out public_key.pem
writing RSA key

$ openssl req -new -key private_key.pem -out cert_request.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.

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

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/oct
+---------------+-----------------------------------------------------------------------+
| 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-format bare --disk-format qcow2 --property img_signature="$image_signature" --property
```

> **Note**
>
> Creating the image can fail if validation does not succeed. This will cause the image to be deleted.

Other Links¶

- 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)

« (glancemetadefcatalogapi.html) » (../admin/index.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%0ASo
https://docs.openstack.org/glance/queens/user/signature.html&field.tags=)

UPDATED: 'THU MAR 1 07:26:57 2018, COMMIT 968F4AE'

FOUND AN ERROR? REPORT A BUG (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:%20HTTPS:/,
HTTPS://DOCS.OPENSTACK.ORG/GLANCE/QUEENS/USER/SIGNATURE.HTML&FIELD.TAGS=)

QUESTIONS? (HTTP://ASK.OPENSTACK.ORG)

OpenStack Documentation ▾

glance 16.0.1.dev1

Page Contents

OpenStack

- Projects (http://openstack.org/projects/)
- OpenStack Security (http://openstack.org/projects/openstack-security/)
- Common Questions (http://openstack.org/projects/openstack-faq/)
- Blog (http://openstack.org/blog/)
- News (http://openstack.org/news/)

Community

- User Groups (http://openstack.org/community/)
- Events (http://openstack.org/community/events/)
- Jobs (http://openstack.org/community/jobs/)
- Companies (http://openstack.org/foundation/companies/)
- Contribute (http://docs.openstack.org/infra/manual/developers.html)

Documentation

- OpenStack Manuals (http://docs.openstack.org)
- Getting Started (http://openstack.org/software/start/)
- API Documentation (http://developer.openstack.org)
- Wiki (https://wiki.openstack.org)

Branding & Legal

- Logos & Guidelines (http://openstack.org/brand/)
- Trademark Policy (http://openstack.org/brand/openstack-trademark-policy/)
- Privacy Policy (http://openstack.org/privacy/)
- OpenStack CLA (https://wiki.openstack.org/wiki/How_To_Contribute#Contributor_License_Agreement)

Stay In Touch

(https://twitter.com/OpenStack)(https://www.facebook.com/openstack)(https://www.linkedin.com/company/openstack)(https://www.youtube.com/user/OpenStackFoundation)