

openstack / keystone Public

<> Code Pull requests 1 Actions Security and quality Insights

⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

Commit 37308dd



vishvananda authored and ttx committed on Nov 16, 2012

Ensures User is member of tenant in ec2 validation

It is possible that a user is no longer a member of a tenant when they attempt to use an ec2 token. This checks to make sure that the user still has at least one valid role in the tenant before authenticating them. This should automatically work for the s3 version as well since it is a subclass.

Fixes bug 1064914

Change-Id: Ieb237bae936a7b00ce7ba4d4c59aec6c7a69ec21

· folsom-eol ... 2012.2.1

1 parent [47e4dc8](#) commit 37308dd

1 file changed +10 -7 lines changed

↑ Top ⚙

Filter files...

keystone/contrib/ec2

core.py

1 file changed +10 -7 lines changed

Search within code ⚙

keystone/contrib/ec2/core.py



```
@@ -168,6 +168,16 @@ def authenticate(self, context, credentials=None,
ec2Credentials=None):
```

```

168 168         context=context,
169 169         user_id=user_ref['id'],
170 170         tenant_id=tenant_ref['id'])
171  +
172  +         # TODO(termie): optimize this call at some point and put it into the
173  +         #             the return for metadata
174  +         # fill out the roles in the metadata
175  +         roles = metadata_ref.get('roles', [])
176  +         if not roles:
177  +             raise exception.Unauthorized(message='User not valid for tenant.')
178  +         roles_ref = [self.identity_api.get_role(context, role_id)
179  +                     for role_id in roles]
180  +
181 181         catalog_ref = self.catalog_api.get_catalog(
182 182             context=context,
183 183             user_id=user_ref['id'],
@@ -180,13 +190,6 @@ def authenticate(self, context, credentials=None,
ec2Credentials=None):
180 190             tenant=tenant_ref,
181 191             metadata=metadata_ref))
182 192
183  -         # TODO(termie): optimize this call at some point and put it into the
184  -         #             the return for metadata
185  -         # fill out the roles in the metadata
186  -         roles_ref = []
187  -         for role_id in metadata_ref.get('roles', []):
188  -             roles_ref.append(self.identity_api.get_role(context, role_id))
189  -
190 193         # TODO(termie): make this a util function or something
191 194         # TODO(termie): i don't think the ec2 middleware currently expects a
192 195         #             full return, but it contains a note saying that it

```

Comments 0



Please [sign in](#) to comment.