

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

↑ Top

Filter files...

keystone/contrib/ec2

core.py

Search within code

keystone/contrib/ec2/core.py

```

@@ -168,6 +168,16 @@ def authenticate(self, context, credentials=None,
    ec2Credentials=None):
    context=context,
    user_id=user_ref['id'],
    tenant_id=tenant_ref['id'])
+
+ # TODO(termie): optimize this call at some point and put it into the
+ #               the return for metadata
+ # fill out the roles in the metadata
+ roles = metadata_ref.get('roles', [])
+ if not roles:
+     raise exception.Unauthorized(message='User not valid for tenant.')
+ roles_ref = [self.identity_api.get_role(context, role_id)
+              for role_id in roles]
+
+ catalog_ref = self.catalog_api.get_catalog(
+     context=context,
+     user_id=user_ref['id'],
@@ -180,13 +190,6 @@ def authenticate(self, context, credentials=None,
    ec2Credentials=None):
    tenant=tenant_ref,
    metadata=metadata_ref))
-
- # TODO(termie): optimize this call at some point and put it into the
- #               the return for metadata
- # fill out the roles in the metadata
- roles_ref = []
- for role_id in metadata_ref.get('roles', []):
-     roles_ref.append(self.identity_api.get_role(context, role_id))
-
+ # TODO(termie): make this a util function or something
+ # TODO(termie): i don't think the ec2 middleware currently expects a
+ #               full return, but it contains a note saying that it

```

Comments 0



Please [sign in](#) to comment.