

Atlas Multi-Region Configuration User Guide

Cloud Execution Environment

USER GUIDE

Copyright

© Ericsson AB 2016, 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Target Groups	2
1.2	Prerequisites	2
1.3	Risks	2
1.4	Limitations	2
2	Configure with Local Authentication	3
3	Configure with Centralized Authentication	6
3.1	Register Endpoints	6
3.2	Change Keystone Information for All Services	8
3.2.1	Edit Configuration Files on vCIC Host	8
3.2.2	Edit Configuration Files on Compute Host	11
3.2.3	Edit Configuration Files on Atlas	11
3.3	Post-Configuration Activities	11



1 Introduction

This document describes the procedures for enabling multiple Cloud Execution Environment (CEE) regions in Atlas.

CEE can be operated in a multi-region configuration. Atlas is a deployment tool, that provides a common dashboard for a group of sites or regions.

There are two main deployment configurations for multiple regions, based on the use of the OpenStack Keystone authentication service:

- Local authentication
- Centralized authentication

Table 1 Deployment Configuration Options for Multiple Regions

Deployment Configuration	Description
Local Authentication	<div> <div> <div>Atlas region 1</div> <div> <div>Region 1</div> <div> <div>Glance</div> <div>Cinder</div> <div>Nova</div> <div>Neutron</div> <div>Heat</div> <div>Keystone</div> </div> </div> </div> <div> <div>Atlas region 2</div> <div> <div>Region 2</div> <div> <div>Glance</div> <div>Cinder</div> <div>Nova</div> <div>Neutron</div> <div>Heat</div> <div>Keystone</div> </div> </div> </div> </div> <p>Each CEE region has a dedicated, local Keystone service. The Atlas VM is running locally.</p>
Centralized Authentication	<div> <div> <div>Atlas region 1</div> <div> <div>Region 1</div> <div> <div>Glance</div> <div>Cinder</div> <div>Nova</div> <div>Neutron</div> <div>Heat</div> </div> </div> </div> <div> <div>Atlas region 2</div> <div> <div>Region 2</div> <div> <div>Glance</div> <div>Cinder</div> <div>Nova</div> <div>Neutron</div> <div>Heat</div> </div> </div> </div> </div> <p>The CEE regions have a common, centralized Keystone service. The Atlas VM is running separately in each region.</p>

Both configurations have a different representation in the Atlas GUI.



1.1 Target Groups

This document is aimed at skilled professionals from the following groups:

- Cloud administrators
- Users who want to configure a CEE environment

1.2 Prerequisites

Before starting this procedure, ensure that the following conditions are met:

- CEE and Atlas are deployed and running in multiple regions
- Atlas administrator credentials are available
- The public IP address of Keystone in RegionOne

Public IP address of Keystone in RegionOne is accessible from RegionTwo nodes (vCIC, compute and Cinder). Compute and Cinder nodes of RegionTwo cannot be reached directly, as they do not have a public IP address assigned for access. These nodes can only be accessed indirectly from RegionOne.

1.3 Risks

Multi-region configuration is associated with the following risks:

- Connections can break down between RegionOne and RegionTwo.
- Services may need to be highlighted when configuration is done during traffic.

1.4 Limitations

Multi-region configuration has the following limitations:

Local authentication only impacts the regions having contact with Atlas. If central authentication changes the region configuration to use Keystone in RegionOne, this impacts HA. Redundant links may be needed.



2 Configure with Local Authentication

In this configuration each CEE region has a dedicated Keystone service running locally, and there is also an Atlas VM (Virtual Machine) running in each region.

To enable available regions in Atlas, proceed with the following steps:

Note: If `ssl` is enabled, use `https` instead of `http`.

1. Log on as an Atlas administrator, for example, `atlasadm@atlas`:
2. Open `local_settings.py` by using the command:

```
atlasadm@atlas:~$ sudo nano /usr/lib/python2.7/⇒
dist-packages/openstack_dashboard/local/local_settings.py
```

3. Find the following lines:


```
AVAILABLE_REGIONS = [
    ('http://region1.example.com:5000/v2.0', Region1),
    ('http://region2.example.com:5000/v2.0', Region2),
]
```
4. Modify `Region1` and `Region2` with the specific region names.
5. Modify `region1.example.com` and `region2.example.com` with the region specific Keystone host IP addresses.

Note: `AVAILABLE_REGIONS` contains a list of tuples, which define multiple regions. The tuple format is:
`('http://{ keystone_host }:5000/v2.0', '{{ region_name }}')`.

Your Keystone version can vary. For Keystone API v3, use the following format:

```
('http://{ keystone_host }:5000/v3, '{{ region_name }}')
```

If the regions are specified, the appropriate region can be selected in the Atlas logon form.



Figure 1 Logon Page with Region Selection

Once logged on to the system, switch between regions using the region switcher dropdown in the site header:

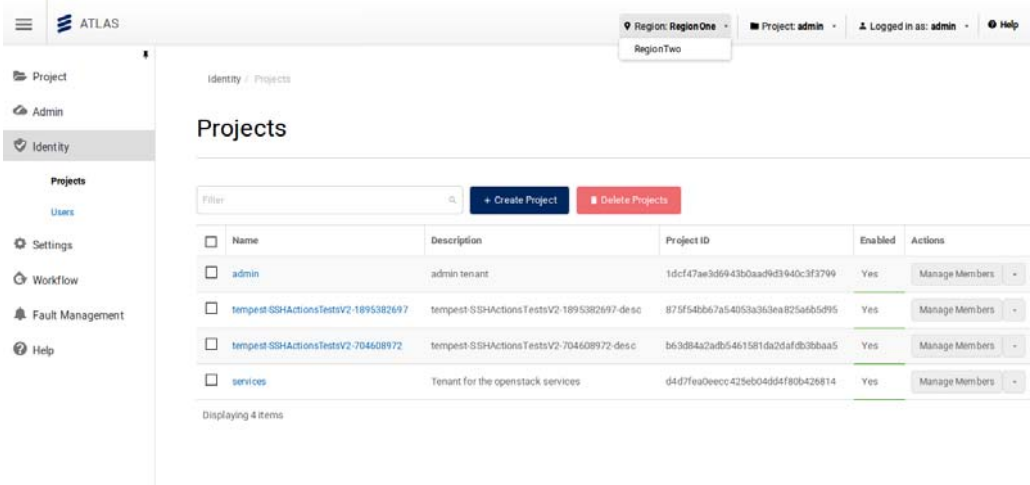


Figure 2 Region Switcher Dropdown in the Overview Page

Note: Changing region takes the user to the login page.



3 Configure with Centralized Authentication

For centralized authentication, the CEE instances (regions) have a common, centralized Keystone service. The Atlas VMs run separately, one in each region.

This configuration example assumes that the centralized Keystone service is hosted in RegionOne. This Keystone has information about available service endpoints in RegionOne.

Note: If `ssl` is enabled, use `https` instead of `http`.

1. Check the service endpoint information:

```
root@cic-1:~# openstack endpoint list
```

An example of the output is the following:

ID	Region	Service Name	Service Type
8213ca63bb53485bb4cd8dab85fa1690	RegionOne	swift	object-store
7cb3df2268d941b19f4915b4482e5e5f	RegionOne	swift_s3	s3
6c6632e2bb4f4a03a812f98eeabb3043	RegionOne	ceilometer	metering
9ae30aa4e69948d2b395dbbc3d30d0ab	RegionOne	novav3	computev3
1a1d5268acad4fd7b7d34b3f2b5affcd	RegionOne	cinder	volume
1b3b41bac63645a2b29539ea02071adf	RegionOne	glance	image
9c9f9cfe08ed4ba485070aa4a0f3a5b19	RegionOne	watchmen	fm
b1037aa470d742b0b0cc1b273df63597	RegionOne	cinderv2	volumev2
68992f32dab341eb87c97342a64040ff	RegionOne	nova_ec2	ec2
99c9c2dc703b44dd996658be31580e33	RegionOne	neutron	network
b40fed3b363c4302a3027def69810784	RegionOne	heat	orchestration
1c13ddf09a8c43a7bf0dd9960975fb63	RegionOne	nova	compute
5d84215d6ba74d97b3506c335ad740fe	RegionOne	mistral	workflowv2
e6e3915e18454429bdfb3449688bd75e	RegionOne	heat-cfn	cloudformation
430ed2cea5024ff883e2e11c3f7b7787	RegionOne	keystone	identity
e4471e2fab8340e58c7bf33e4baf4281	RegionOne	ovft	translator
ecc6471ef2284f62ac70979f52d00874	RegionOne	pmapi	pm

Example 1 Service Endpoint Information

2. Make Keystone in RegionOne aware of the endpoints located in RegionTwo by registering the endpoints, see Section 3.1 on page 6.
3. Change the `keystone_authtoken` information for all services in RegionTwo, see Section 3.2 on page 8.

3.1 Register Endpoints

To make Keystone in RegionOne aware of the endpoints located in RegionTwo, the endpoints must be registered in RegionOne. The endpoints are registered by specifying a public URL, an internal URL, an admin URL, a region name, and a service type. This is done for all services.

The `openstack endpoint list` command in RegionTwo can be used to check the URL information.



The following example shows the URLs associated with an endpoint in RegionTwo:

```
root@cic-1:~# openstack endpoint show $(openstack endpoint list
| awk '/ compute / {print $2'})
```

Field	Value
adminurl	http://192.168.2.21:8774/v2/\$(tenant_id)s
enabled	True
id	1c13ddf09a8c43a7bf0dd9960975fb63
internalurl	http://192.168.2.21:8774/v2/\$(tenant_id)s
publicurl	https://public.fuel.local:8774/v2/\$(tenant_id)s
region	RegionOne
service_id	932a7ee62cd945dbb5008a968e007524
service_name	nova
service_type	compute

Example 2 Checking URLs Associated with Endpoints in RegionTwo

The output shows the information required to proceed with registering a new endpoint: `internalurl`, `adminurl`, and `publicurl`.

The following example shows how to register a new Nova endpoint from RegionTwo in Keystone, in RegionOne:

```
openstack endpoint create =>
--publicurl 'http://10.33.190.100:8774/v2/$(tenant_id)s' =>
--internalurl 'http://192.168.2.20:8774/v2/$(tenant_id)s' =>
--adminurl 'http://10.33.190.100:8774/v2/$(tenant_id)s' =>
--region 'RegionTwo'
compute
```

Example 3 Register a New Endpoint in RegionOne

Repeat for each compute host.

Repeat the endpoint registration in RegionOne, for all the registered services, except for the identity service, by replacing `compute`, with a corresponding service type:



```
root@cic-1:~# openstack service list
```

ID	Name	Type
035b75af797643208bd5bf1e4cb54a6e	novav3	computev3
0eee0ed8c08b432b8f03dfe79e730097	mistral	workflowv2
2342cc8ca0f84528a884f7a109ee1afb	cinder	volume
477b9f0648ea4537b1fd54d4168fe24e	swift_s3	s3
6d8bfea5c1f84aa986a9fbad3365ad76	heat-cfn	cloudformation
7c4820d08ae64e0381ad2d52946cbf77	heat	orchestration
8766816cca9e47628cd27f5aab3cc819	ovft	translator
8aa622cc8ad84185af81c18e284e40ae	ceilometer	metering
932a7ee62cd945dbb5008a968e007524	nova	compute
999a96816f02478e8b889e38aa624aef	nova_ec2	ec2
a42da7ba5d774b2ba0b17bf85394f727	swift	object-store
c65b20036edd4291812d8edf5853172a	pmapi	pm
e19a9e6195994fe6b4a40d58ca64c9e1	keystone	identity
e51ea728a9ce4419af6c71aff344bf84	cinderv2	volumev2
e7e7ec0e976b40d19475fce90a815d82	neutron	network
e962e686dc42496d86f3e72ea483ce93	glance	image
f4734e3f29ea47f3b045e0de5b84dc0f	watchmen	fm

Example 4 OpenStack Service List

At the end of this example, Keystone has received registered endpoints for both RegionOne and RegionTwo.

3.2 Change Keystone Information for All Services

Change the keystone_auth token information for all services in RegionTwo. This requires editing the configuration files for each of the following registered services: Nova, Neutron, Cinder, Glance, Heat, OVFT, Ceilometer, Swift, and Watchmen. Locate entries with authentication information in the configuration files of RegionOne. Copy that information to the configuration files in RegionTwo.

Note: Instead of using the internal IP address, use the public IP address of Keystone from RegionOne; for example, use 10.33.168.100 instead of 192.168.2.20.

The configuration file edits must be made first on the vCIC host, then on the compute host.

3.2.1 Edit Configuration Files on vCIC Host

This section describes how to edit the configuration files on the vCIC host.

Nova

Copy the values of the following entries for /etc/nova/nova.conf from RegionOne to RegionTwo:

```
neutron_admin_password=VYNe6HWY
neutron_admin_auth_url=http://10.33.168.100:35357/v2.0
```



```
auth_uri=http://10.33.168.100:5000/  
auth_host=10.33.168.100  
admin_password=t83EqF0T
```

Note: Check the parameters against the latest version of `config.yaml`.

Neutron

Copy the values of the following entries for `/etc/neutron/neutron.conf` from RegionOne to RegionTwo:

```
nova_admin_password =t83EqF0T  
nova_admin_auth_url =http://10.33.168.100:35357/v2.0  
auth_host = 10.33.168.100  
admin_password = VYNe6HWY  
auth_url=http://10.33.168.100:35357/v2.0
```

Copy the values of the following entries for `/etc/neutron/api-paste.ini` from RegionOne to RegionTwo:

```
auth_url=http://10.33.168.100:35357/v2.0  
auth_host=10.33.168.100  
admin_password=VYNe6HWY
```

Copy the values of the following entries for `/etc/neutron/dhcp_agent.ini` from RegionOne to RegionTwo:

```
auth_url=http://10.33.168.100:35357/v2.0  
admin_password=VYNe6HWY
```

Copy the values of the following entries for `/etc/neutron/metadata_agent.ini` from RegionOne to RegionTwo:

```
auth_url = http://10.33.168.100:35357/v2.0  
admin_password = VYNe6HWY
```

Cinder

Copy the values of the following entries for `/etc/cinder/cinder.conf` from RegionOne to RegionTwo:

```
auth_host=10.33.168.100  
admin_password=d7nzpGJW
```

Copy the values of the following entries for `/etc/cinder/api-paste.ini` from RegionOne to RegionTwo:



```
auth_uri=http://10.33.168.100:5000/  
service_host=10.33.168.100  
auth_host=10.33.168.100  
admin_password=d7nzpGJW
```

Glance

Copy the values of the following entries for `/etc/glance/glance-api.conf` from RegionOne to RegionTwo:

```
swift_store_auth_address = http://10.33.168.100:5000/v2.0/  
auth_host = 10.33.168.100  
admin_password = DQxrXv0S  
auth_uri=http://10.33.168.100:5000/
```

Copy the values of the following entries for `/etc/glance/glance-cache.conf` from RegionOne to RegionTwo:

```
auth_url = http://10.33.168.100:5000/v2.0  
admin_password = DQxrXv0S  
swift_store_auth_address = http://10.33.168.100:5000/v2.0/
```

Copy the values of the following entries for `/etc/glance/glance-registry.conf` from RegionOne to RegionTwo:

```
auth_host = 10.33.168.100  
admin_password = DQxrXv0S  
auth_uri=http://10.33.168.100:5000/
```

Swift

Copy the values of the following entries for `/etc/swift/proxy-server.conf` from RegionOne to RegionTwo:

```
auth_host = 10.33.168.100  
auth_uri = http://10.33.168.100:35357  
admin_password = dBvMkLy5
```

Watchmen

Copy the values of the following entries for `/etc/watchmen-api.conf` from RegionOne to RegionTwo:

```
auth_url=http://10.33.168.100:35357/v2.0/
```

Copy the values of the following entries for `/etc/watchmen-cli.conf` from RegionOne to RegionTwo:

```
auth_url=http://10.33.168.100:35357/v2.0/
```



3.2.2 Edit Configuration Files on Compute Host

This section describes how to edit the configuration files on the compute host.

Nova

Copy the values of the following entries for `/etc/nova/nova.conf` from RegionOne to RegionTwo:

```
neutron_admin_password=VYNe6HWY
```

```
neutron_admin_auth_url=http://10.33.168.100:35357/v2.0
```

Neutron

Copy the values of the following entries for `/etc/neutron/neutron.conf` from RegionOne to RegionTwo:

```
auth_host = 10.33.168.100
```

```
admin_password = VYNe6HWY
```

```
auth_url=http://10.33.168.100:35357/v2.0
```

3.2.3 Edit Configuration Files on Atlas

Update `/etc/hosts` with the public IP address of Keystone in RegionOne:

```
10.33.168.100 cic-pub-api cic-int-api cic-adm-api
```

OVFT

Copy the values of the following entries for `/etc/ovft/ovft.conf` from RegionOne to RegionTwo:

```
auth_uri = http://10.33.168.100:5000/v2.0
```

```
auth_host = 10.33.168.100
```

Heat

Copy the values of the following entries for `/etc/ovft/ovft.conf` from RegionOne to RegionTwo:

```
auth_uri = http://10.33.168.100:5000/v2.0
```

```
auth_host = 10.33.168.100
```

Note: This configuration must also be done for Atlas in RegionTwo.

3.3 Post-Configuration Activities

Restart all the services to apply the configurations. This must be performed for all hosts, both vCIC and compute.

After the multi-region environment is configured, the Atlas UI shows the following information for RegionOne:

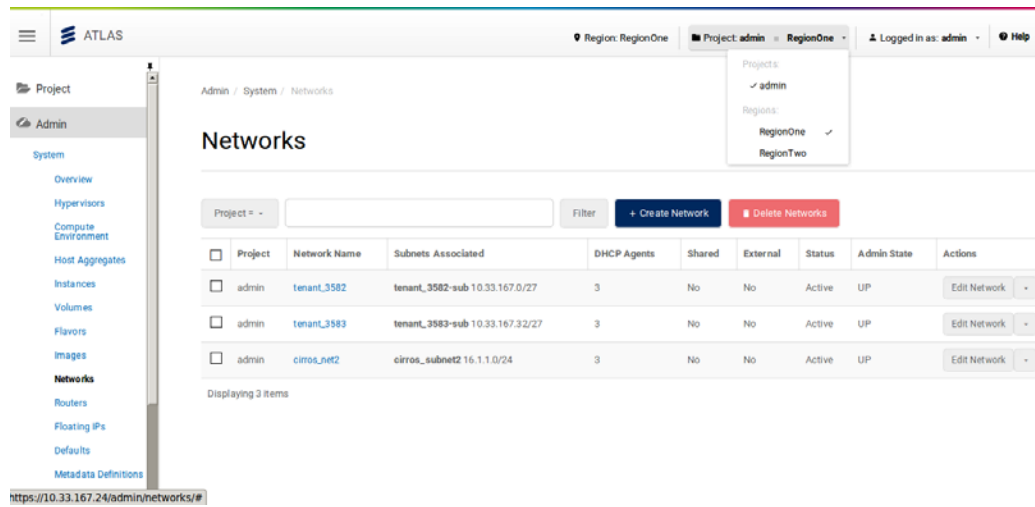


Figure 3 Networks Page, RegionOne after Multi-Region Configuration

Note: Changing region takes the user directly to the network page in RegionTwo.

For RegionTwo, the Atlas UI shows the following information after the multi-region environment is configured:

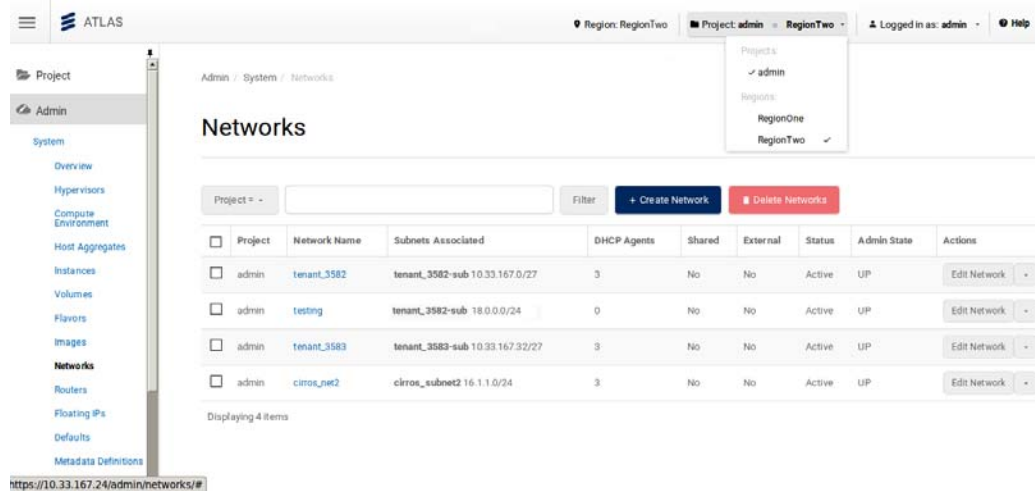


Figure 4 Networks Page, RegionTwo after Multi-Region Configuration

Note: Changing region takes the user directly to the network page in RegionTwo.