Red Hat Ansible Automation Platform 2.2: Engagement Journey

For FWD

Preface

Confidentiality, Copyright, and Disclaimer

This is a Customer-facing document between Red Hat, Inc. and FWD.

This document is not a quote and does not include any binding commitments by Red Hat. If acceptable, a formal quote can be issued upon request, which will include the scope of work, cost, and any customer requirements as necessary.

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Audience

This document is intended for Client technical staff responsible for the environment.

Additional Background and Related Documents

This document does not contain step by step details of installation or other tasks, as they are covered in the relevant documentation on http://access.redhat.com/.
Links to the appropriate documents will be made when required.

The reference documents could be referred as follows:
Ansible Automation Platform Installation:
https://access.redhat.com/documentation/en-us/red_hat_ansible_automation_platform/2.2/html/red_hat_ansible_automation_platform_installation_guide/index

https://docs.ansible.com/automation-controller/latest/html/userguide/index.html
https://docs.ansible.com/automation-controller/latest/html/administration/index.htm
l

https://access.redhat.com/solutions/4618191
https://docs.ansible.com/ansible

Configure SAML Authentication with OKTA:

tower/latest/html/administration/ent_auth.html?extIdCarryOver=true&intcmp=701f20000012k6EAAQ&sc_cid=701f2000001OH7JAAW#saml-authentication-settings

Custom SSL Certificate:
https://access.redhat.com/solutions/5731261
https://access.redhat.com/solutions/3109871

Scripts and playbooks

Any scripts provided are being provided as-is, without any form of support or warranty.
All provided scripts can be modified by the customer at will.

Version history

Version	Date	Contributor	Role	Description
1.0	2022-08-01	Mark Lam	Red Hat Consultant	First Version of the document

Table of Contents

1. INTRODUCTION

1.1. About FWD

FWD is focused on creating fresh customer experiences and making the insurance journey simpler, faster and smoother, with innovative propositions and easy-to-understand products, supported by digital technology. Through this customer-led approach, FWD aims to become a leading pan-Asian insurer by changing the way people feel about insurance.

1.2. Purpose

The purpose of this document is to provide the infrastructure design of Red Hat Ansible Automation Platform 2.2 for FWD. The setup of this platform is the production setup providing the automation management and connection between Red Hat Ansible Automation Platform and FWD's infrastructure servers, in order to utilize Ansible abilities.

Customer project team

1.3. Staffing

Name	Function	E-mail address	Phone number
Wai Kwong	Senior Manager	wai.kwong@fwd.com	+852 92592666
To Hang Chan	Infrastructure Project Manager	tohang.chan@fwd.com	+852 60101789

Red Hat project team

Name	Function	E-mail address	Phone number
Jukey Lee	Project Manager	jukeylee@redhat.com	+852 92716626
Andes Chau	Design Implementation	andeschau@redhat.com	+852 9873 9634
Gary Leung	Implementation	kayleung@redhat.com	+852 9662 0551
Mark Lam	Implementation	palam@redhat.com	+852 92820349

1.4. Terms and acronyms

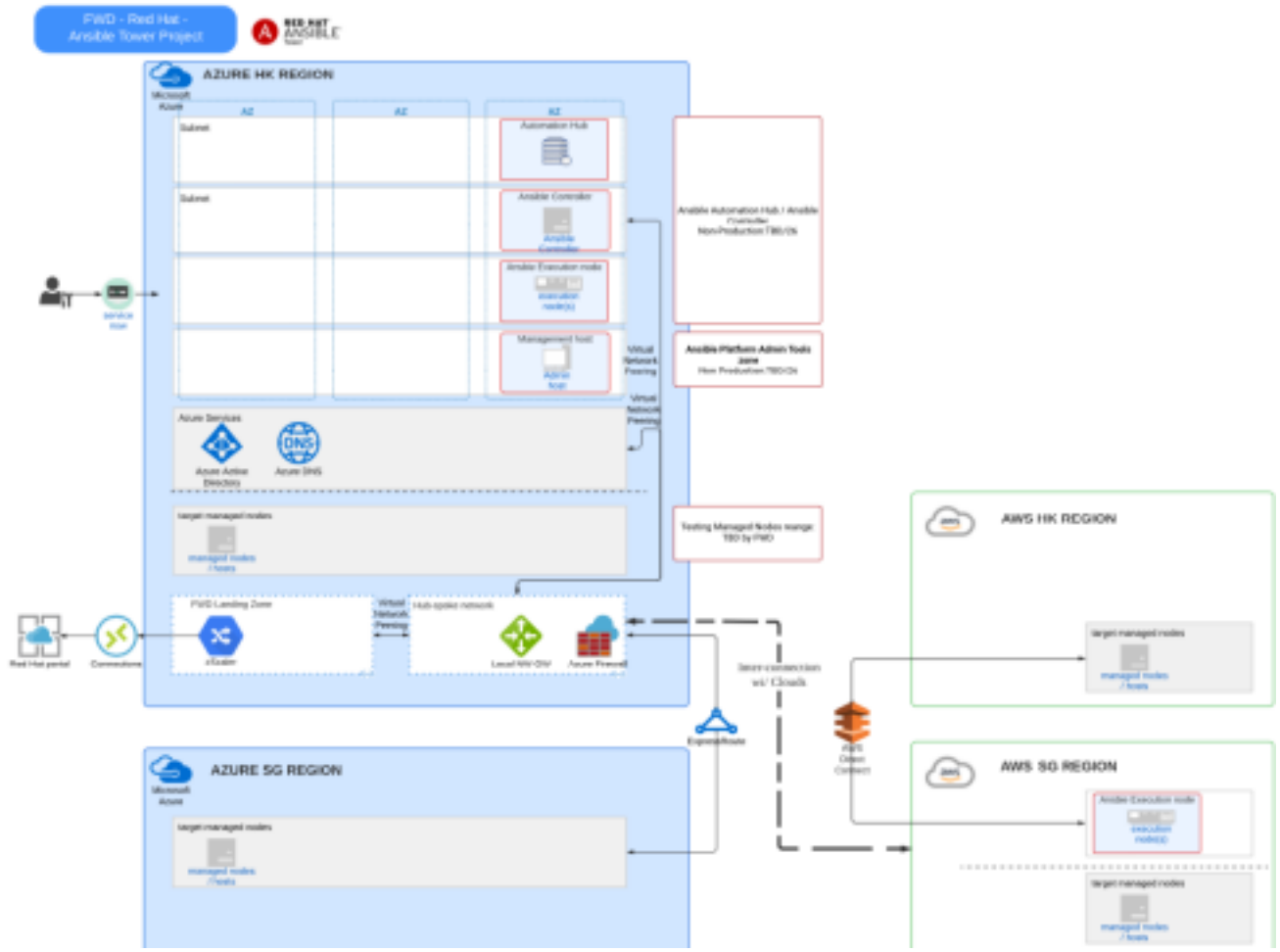
The table below provides a glossary of the terms and acronyms used within this document.

Acronym	Description
FWD	FWD
RH	Red Hat, Inc

RHAT	Red Hat Ansible Tower
RHAAP	Red Hat Ansible Automation Platform
RHEL	Red Hat Enterprise Linux
AD	Active Directory
ALB	Active Load-Balancing, a link-aggregation technique for NICs
API	Application Programming Interface
CA	Certificate Authority
DC	Data Centre
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
FQDN	Fully Qualified Domain Name
Guest	Also see “VM”. This is virtual machine running on a Host.
HA	High-Availability or Highly-Available
Host	The physical hardware or the logical OS which runs virtualisation technology allowing one or more Guest OS’s to run on the hardware owned by the Host
L2	Layer 2, part of the TCI/IP Network Stack
L3	Layer 3, part of the TCI/IP Network Stack
NAT	Network Address Translation
NIC	Network Interface Card. References a virtual or a physical port allowing network access and interface to a Host or Guest VM.
NTP	Network Time Protocol
OS	Operating System
QA	Quality Assurance
SAN	Storage Area Network
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VLAN	Virtual LAN is a networking virtualisation technology
VM	Virtual machine, in OSP terms, synonymous with “Workload” or “Guest”

2. INFRASTRUCTURE ARCHITECTURE DIAGRAM

2.1. Ansible Automation Platform Architecture Diagram



Component	Hostname / IP address
Automation Hub	lgoeasiacappp01.fwdasia.intranet / 10.50.4.4

Ansible Control Node	lgoeasiacappp02.fwdasia.intranet / 10.50.4.5
Ansible Execution Node @ Azure	lgoeasiacappp02.fwdasia.intranet / 10.50.4.20
Ansible Execution Node @ AWS	vm-core-shs-aps1-prd-sgp-rh8-aapexe-01.fwdasia.intrane t / 10.192.0.12
NTP Servers	Azure : 10.50.1.36 AWS: 169.254.169.123
DNS Servers	Azure: 10.50.1.36, 10.51.1.36, 10.11.65.31, 10.11.65.32, 10.24.3.21 AWS: 10.192.0.2

2.1.1 Design Concept

- Ansible Automation Platform is required to connect with Red Hat CDN and Red Hat Subscription Manager site for registration and setting up the package repositories.
- The time synchronization and domain name resolution would be set under all Ansible Automation Platform's' OS (RHEL) Chrony and DNS configurations.
- The Okta authentication would be set under the Ansible Controller setting. SAML Protocol would be used in this setting.
- All Target hosts are the managed objects of Ansible Controller. They are the RHEL servers, and Windows servers within this project.
- The Ansible connection requirements are different depending on the types of target hosts. For most Linux servers, the default connection is using SSH, TCP port 22; for Windows servers, it would be using WinRM, and recommended to use the HTTPS listener, TCP port 5986.
- Users use the web browser to access the Ansible Controller WebUI for its administration and automation execution.
- Private Automation Hub would be deployed as the proxy between Ansible controller and Ansible collection sources in the external networks.

  Ansible collections from Red Hat Cloud's Automation hub and Ansible Galaxy would be synchronized to the Private Automation Hub's Pulp repository.

The AAP Execution Environment images would also be synchronized to this Private Automation Hub's container registry.

- Azure Repos (Git Repository) would be created and used as the Ansible playbooks source control manager. All Ansible playbooks would be stored under the created GIT repositories.

3. NETWORK PORTS REQUIREMENTS

3.1 Network Ports Requirement Table For Red Hat Ansible Automation Platform

The below table is the network ports which commonly need to open on firewall or proxy.

Source (IP address & subnets only)*	**Destination (IP address & subnets only) ***	**Port Number ***	**Business Justifications ***
Automation Hub-HK / Ansible Controller-HK / Execution Node-HK	Azure DNS(s) and Azure NTP EAS: WEASNDSP01 10.50.1.36 SEA: WSEANDSP01 10.51.1.36	UDP/TCP53, UDP/TCP123	Accessible to Azure DNS and NTP servers
Execution Node-SG	AWS DNS(s) and NTP	TBU by FWD	Accessible to AWS DNS and NTP servers
Automation Hub-HK Ansible Controller-HK Execution Node-HK	Azure zScaler proxy gateway whitelist subscription.rhn.redhat.com subscription.rhsm.redhat.com cdn.redhat.com *.akamaiedge.net *.akamaitechnologies.com	HTTPS443	Internet Connectivity for automation module download Registration to the Red Hat Subscription Manager and retrieve the required RPM packages from Red Hat CDN. https://access.redhat.com/solutions/ 65300 The connection could be closed after the installation phase.

Execution Node-SG	AWS zScaler proxy gateway whitelist subscription.rhn.redhat.com subscription.rhsm.redhat.com cdn.redhat.com *.akamaiedge.net *.akamaitechnologies.com	HTTPS443	Internet Connectivity for automation module download Registration to the Red Hat Subscription Manager and retrieve the required RPM packages from Red Hat CDN. https://access.redhat.com/solutions/ 65300 The connection could be closed after the installation phase.
Automation Hub-HK	registry.redhat.io console.redhat.com galaxy.redhat.com	HTTPS443	Download Execution Environments and Ansible Collections into AAP.
Ansible Controller-HK Execution Node-HK (opt) Execution Node-SG (opt)	Email Server	25	AAP nodes connect to SMTP email server Playbooks in Exec Node require to send Email notice
Ansible Controller-HK Execution Node-HK Execution Node-SG	Automation Hub-HK	HTTPS443	Communication between Exec Node & Automation Hub with Controller

Ansible Controller-HK	Automation Hub-HK Execution Node-HK Execution Node-SG	HTTPS443 / TCP22	Communication between Automation Controller and Automation Hub & Execution nodes
Ansible Controller-HK	Execution Node-HK Execution Node-SG	TCP27199	Heartbeat communication
Execution Node-HK Execution Node-SG	Ansible Controller-HK	TCP27199	Heartbeat communication
Jump host-HK	Automation Hub-HK / Ansible Controller-HK / Execution Node-HK / Execution Node-SG	HTTPS443 / TCP22	Admin purpose for communication between Jump node and APP Infra
Ansible Administrator (network subnet)	Ansible Controller-HK	HTTPS443	User Access Web UI interfaces
Execution Node-HK	Testing VMs in AZ-HK Testing VMs in AZ-SG	TCP22 TCP5985 TCP5986	Communication between Execution Node-HK and Testing VMs in AZ
Execution Node-SG	Testing VMs in AWS-HK Testing VMs in AWS-SG	TCP22 TCP5985 TCP5986	Communication between Execution Node-SG and Testing VMs in AWS
Execution Node-HK (Azure)	ServiceNOW uat: https://fwduat.service-now.com ServiceNOW prd: https://fwdprod.service-now.com	TCP443	Execution Node communicate with ServiceNOW API for Production and Non-Production

Execution Node-SG (AWS)	ServiceNOW uat: https://fwduat.service-now.com ServiceNOW prd: https://fwdprod.service-now.com	TCP443	Execution Node communicate with ServiceNOW API
ServiceNOW uat: https://fwduat.service-now.com ServiceNOW prd: https://fwdprod.service-now.com	Ansible Controller-HK: https://aap-control01.fwd.com	TCP443	ServiceNOW API (Production and Non-Production) communicate with Ansible Controller
Automation Hub-HK Ansible Controller-HK Execution Node-HK	AZ-Satellite-HK	TCP443 TCP8443	Communication between AZ-Satellite HK
Execution Node-SG	AWS-Satellite-SG	TCP443 TCP8443	Communication between AWS Satellite-SG

4. HARDWARE AND SOFTWARE REQUIREMENTS

4.1 Ansible Automation Control Node Requirements

The Ansible Automation Controller would be deployed as a VM**.**
The VM hardware requirements are as following table:

Hardware	**Settings**
vCPU	**4 cores (required)**
vMemory	**16GB (required)**

Disk Size	The volume mount table: Filesystem Size Used Avail Use% Mounted on devtmpfs 7.8G 0 7.8G 0% /dev tmpfs 7.8G 436K 7.8G 1% /dev/shm tmpfs 7.8G 49M 7.7G 1% /run tmpfs 7.8G 0 7.8G 0% /sys/fs/cgroup /dev/mapper/rootvg-rootlv 2.0G 282M 1.8G 14% / /dev/mapper/rootvg-usrlv 10G 2.2G 7.9G 22% /usr /dev/sdc1 496M 264M 232M 54% /boot /dev/mapper/rootvg-homelv 1014M 62M 953M 7% /home /dev/mapper/rootvg-varlv 8.0G 2.9G 5.2G 36% /var /dev/mapper/rootvg-tmplv 2.0G 48M 2.0G 3% /tmp /dev/sdc15 495M 5.9M 489M 2% /boot/efi /dev/mapper/rootvg-awxlv 20G 3.7G 17G 19% /var/lib/awx /dev/mapper/pgsqlvg-pgsqllv 100G 860M 100G 1% /var/lib/pgsql /dev/sda1 42M 1.5K 42M 1% /mnt/azure_bek_disk tmpfs 1.6G 0 1.6G 0% /run/user/1000

4.2 Ansible Automation Execution Node Requirements

The Ansible Automation Execution Node would be deployed as a VM**.**

The VM hardware requirements are as following table:

Hardware	**Settings**
vCPU	**4 cores (required)**
vMemory	**16GB (required)** The memory capacity is depending on the number of forks of the Ansible task. For example, if targeting 20 hosts at the same time (set 20 forks), each Ansible fork requires 1GB memory to run, then the total would be 20GB for running the task.

Disk Size@ Azure	The volume mount table: Filesystem Size Used Avail Use% Mounted on devtmpfs 7.8G 0 7.8G 0% /dev tmpfs 7.8G 84K 7.8G 1% /dev/shm tmpfs 7.8G 41M 7.7G 1% /run tmpfs 7.8G 0 7.8G 0% /sys/fs/cgroup /dev/mapper/rootvg-rootlv 2.0G 282M 1.8G 14% / /dev/mapper/rootvg-usrlv 10G 2.0G 8.0G 20% /usr /dev/mapper/rootvg-varlv 13G 7.0G 6.1G 54% /var /dev/mapper/rootvg-tmplv 2.0G 48M 2.0G 3% /tmp /dev/sda1 496M 264M 232M 54% /boot /dev/sda15 495M 5.9M 489M 2% /boot/efi /dev/mapper/rootvg-homelv 21G 189M 21G 1% /home /dev/sdb1 42M 1.5K 42M 1% /mnt/azure_bek_disk tmpfs 1.6G 0 1.6G 0% /run/user/1000
Disk Size@ AWS	Filesystem Size Used Avail Use% Mounted on devtmpfs 3.7G 0 3.7G 0% /dev tmpfs 3.7G 84K 3.7G 1% /dev/shm tmpfs 3.7G 25M 3.7G 1% /run tmpfs 3.7G 0 3.7G 0% /sys/fs/cgroup /dev/nvme0n1p2 50G 6.7G 44G 14% / tmpfs 747M 0 747M 0% /run/user/1001

4.3 Ansible Automation Hub Requirements

The Ansible Automation Execution Node would be deployed as a VM**.**

The VM hardware requirements are as following table:

Hardware	**Settings**
vCPU	**2 cores (required)**
vMemory	**8 GB (required)** .

Disk Size	The volume mount table: Filesystem Size Used Avail Use% Mounted on devtmpfs 3.8G 0 3.8G 0% /dev tmpfs 3.8G 28K 3.8G 1% /dev/shm tmpfs 3.8G 57M 3.8G 2% /run tmpfs 3.8G 0 3.8G 0% /sys/fs/cgroup /dev/mapper/rootvg-rootlv 2.0G 282M 1.8G 14% / /dev/mapper/rootvg-usrlv 10G 2.3G 7.8G 23% /usr /dev/mapper/rootvg-varlv 8.0G 2.9G 5.2G 36% /var /dev/sda1 496M 232M 264M 47% /boot /dev/mapper/rootvg-homelv 1014M 40M 975M 4% /home /dev/mapper/pgsqlvg-pgsqllv 150G 1.5G 149G 1% /var/lib/pgsql /dev/mapper/rootvg-pulplv 40G 2.4G 38G 6% /var/lib/pulp /dev/mapper/rootvg-tmplv 2.0G 47M 2.0G 3% /tmp /dev/sda15 495M 5.9M 489M 2% /boot/efi tmpfs 777M 0 777M 0% /run/user/1000

The software requirements are as the following table:

Software	**Settings**
Operating System	RHEL 8.6
Subscription	Red Hat Ansible Automation Platform Infrastructure Subscription
Repositories	rhel-8-for-x86_64-baseos-rpms rhel-8-for-x86_64-appstream-rpms
Application Bundle	Download the Ansible Automation Platform 2.2 Setup Bundle https://access.redhat.com/downloads/content/480/ver=2.2/rhel--- 8/2.2/x86_64/product-software

5. ANSIBLE AUTOMATION PLATFORM INSTALLATION

5.1 Pre-Installation

5.1.1 RHEL OS Setup

(The following procedures should be run on all AAP controller node, AAP execution nodes, and AT hub node)

Disable Azure/AWS repositories.

```
# sed -i 's/enabled = 1/enabled = 0/g' /etc/yum.repos.d/*.repo
```

Enable repositories for Ansible Automation Platform uses.

```
# subscription-manager repos --disable='*'
# subscription-manager repos
--enable='rhel-8-for-x86_64-baseos-rpms' --
enable='rhel-8-for-x86_64-appstream-rpms'
```

Unset the RHEL 8 minor version control, and update the RHEL 8 OS to the latest version.

```
# subscription-manager release --unset
# mv /etc/yum/vars/releasever ~/.
# dnf clean all
# dnf update -y
```

System reboot after an update.

```
# reboot
```


5.1.2 Configure SSH key-based authentication for fwdadmin user

(The following procedures should be run on AAP controller node only)

Create the SSH key pair.

```
 [root@LGOEASIACAPPP02 ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key
(/root/.ssh/id_rsa): Enter passphrase (empty for no
passphrase):
Enter same passphrase again:
Your    identification    has    been    saved    in
/root/.ssh/id_rsa. Your public key has been saved in
/root/.ssh/id_rsa.pub. The key fingerprint is:
SHA256:mfg1aVX/etkR+qiisULedvAGD8bSzQ1sjRmL/Wx9xeU
root@LGOEASIACAPPP02 The key's randomart image is:
+---[RSA 3072]----+
| . |
| . . ..|
| + * . +o|
| o @ + . E|
| + S X .. .o|
| o O = * .oo+|
| o +.B . .ooo|
| o oo* . . |
| oo+ .. |
+----[SHA256]-----+
```

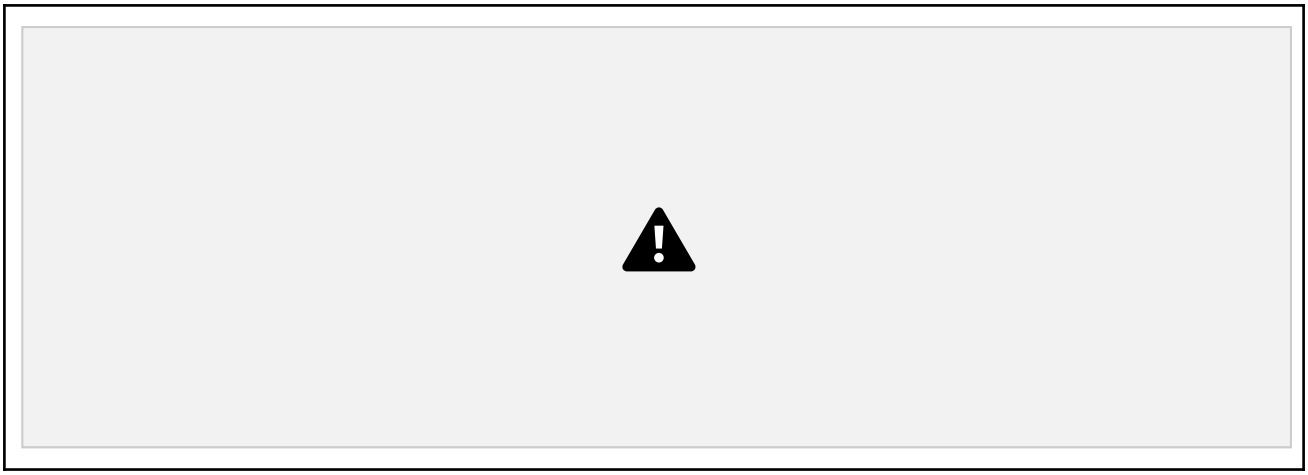
Share the SSH public key to all AAP execution nodes.

```
[fwdadmin@LGOEASIACAPPP02 ~]$ ssh-copy-id
fwdadmin@lgoeasiacapp03.fwdasia.intranet
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be
installed:  "/home/fwdadmin/.ssh/id_rsa.pub"
The authenticity of host 'lgoeasiacappp03 (10.50.4.20)' can't
be  established.
ECDSA key fingerprint is
SHA256:PZ5FDlFy2oCBabVZsw2gG5KDGCKbg5E4D9uIi6KUFOQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
yes /usr/bin/ssh-copy-id: INFO: attempting to log in with the new
key(s), to  filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if
you  are prompted now it is to install the new keys
fwdadmin@lgoeasiacappp03's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh
'fwdadmin@LGOEASIACAPPP03'"
and check to make sure that only the key(s) you wanted were added.
```

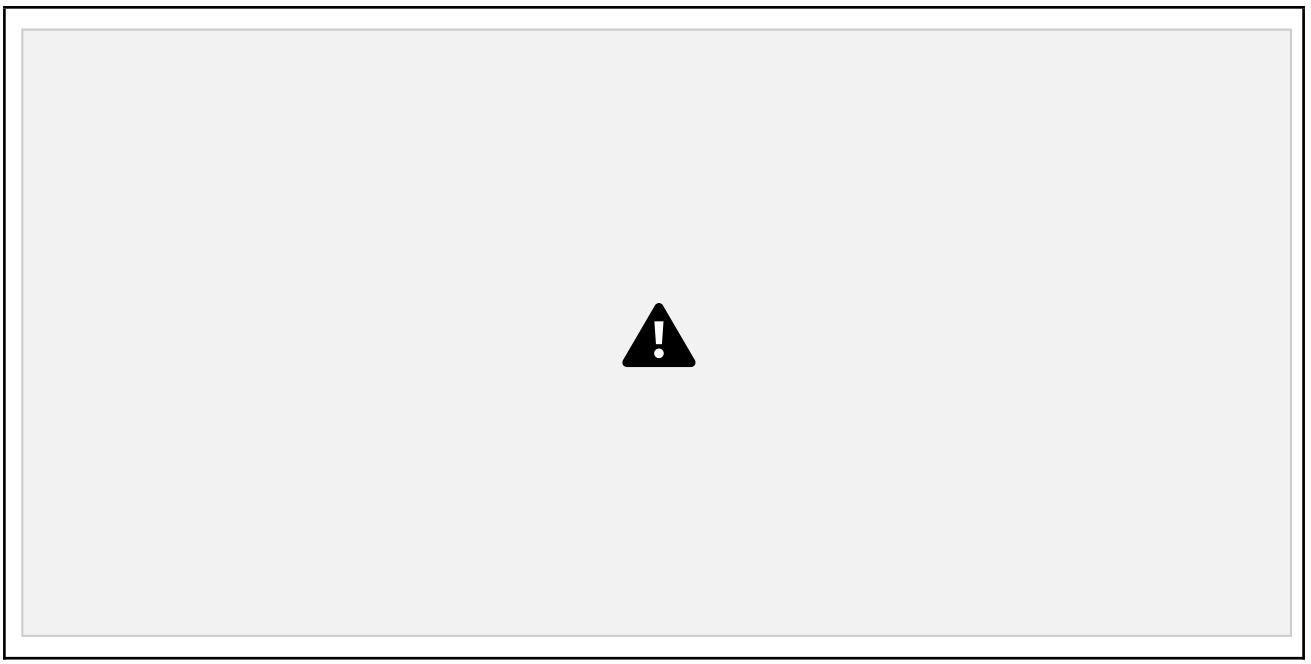

5.1.3 Create the key pairing Registry Service Accounts

(The following procedures should be run on client PC's Browser)

Navigate to the Registry Service Account Management Application (https://access.redhat.com/terms-based registry/) , and log in if necessary.

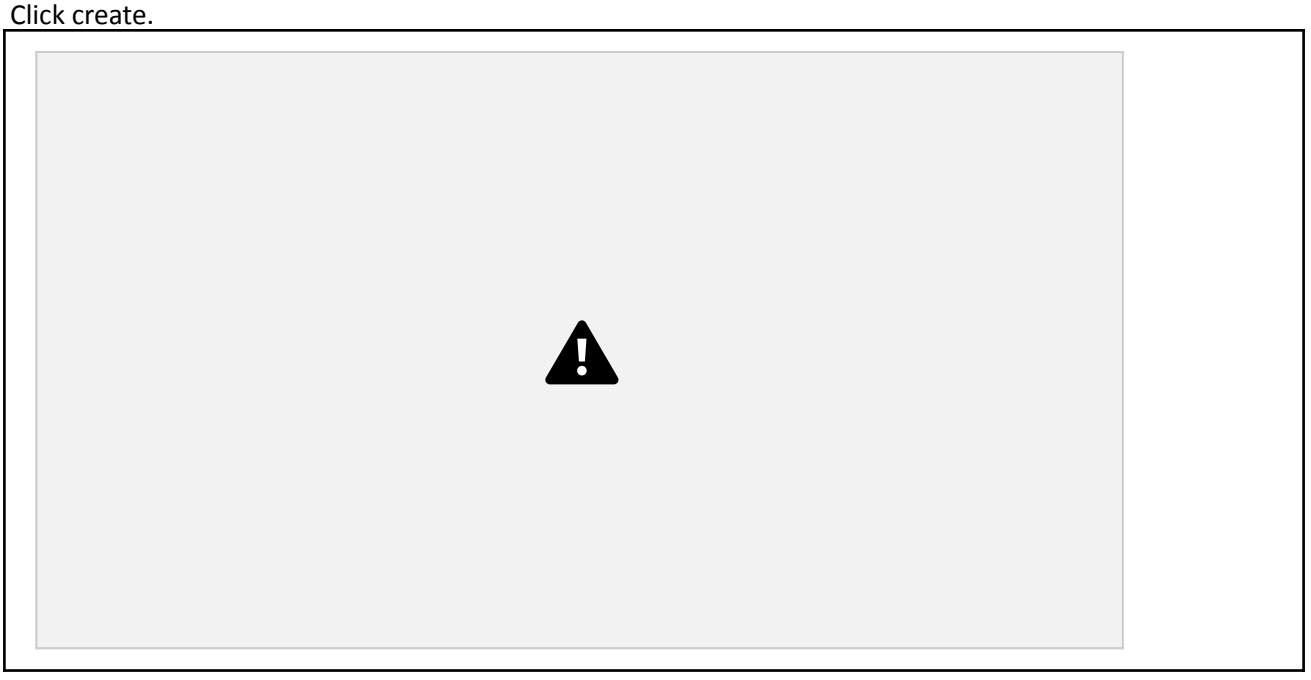


From the Registry Service Accounts page, click the New Service Account button.



Provide a name for the Service Account. It will be prepended with a fixed, random string.

Enter a description.
Click create.

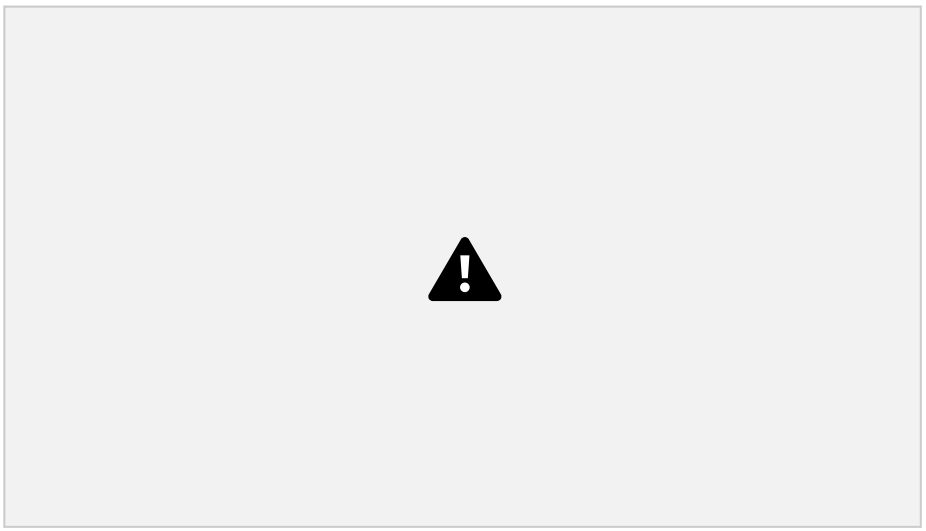


Navigate back to your Service Accounts.

Click the Service Account you created

- Note the username, including the prepended string (i.e. XXXXXXX|username). This is the username which should be used to login to registry.redhat.io.

- Note the password. This is the password which should be used to login to registry.redhat.io.



5.1.4 Automation Hub Setup Answer File Preparation

(The following procedures should be run on AT Hub node only)

Copy the downloaded Ansible Automation Platform 2.2 Setup Bundle - **ansible-automation-platform-setup-bundle-2.2.0-6.1.tar.gz** to /tmp.

Extract Ansible Automation Platform Setup Bundle:

```
[root@LGOEASIACAPPP01 ~]# cd /var

[root@LGOEASIACAPPP01 var]# tar zxvf
/tmp/ansible-automation-platform setup-bundle-2.2.0-6.1.tar.gz
```

Edit the Red Hat Ansible Automation Platform installer inventory file:

```
[root@LGOEASIACAPPP01 ~]# cd
/var/ansible-automation-platform-setup bundle-2.2.0-6.1

[root@LGOEASIACAPPP01
ansible-automation-platform-setup-bundle-2.2.0- 6.1]# vi
inventory
```

Inventory file:

```
[automationhub]

# FQDN and lower-case letter should be used for the inventory
hostname  here.

lgoeasiacapp01.fwdasia.intranet


ansible_connection=local [database]


[all:vars]

# Automation Hub Configuration

#


registry_url='registry.redhat.io'

registry_username='<Red Hat Registry Service Account>'

registry_password='<Red Hat Registry Service Password>'
```

```
automationhub_admin_password='<your password>'


automationhub_pg_host=''

automationhub_pg_port=5432


automationhub_pg_database='automationhub'

automationhub_pg_username='automationhub'

automationhub_pg_password='<your password>'

automationhub_pg_sslmode='prefer'


   # The default install will register node to the Red Hat Insights
                                Service

# if the node is registered with Subscription Manager. Set to False
to  disable.

enable_insights_collection = False


## /tmp size is too low to extract the installation bundle EE

images. ## Setup another temp folder for enough size to extract

the EE images. ee_images_tmp_dir='/var/lib/pulp'


# If set, this will install a custom CA certificate to the system
trust  store.

# custom_ca_cert=<path_to_FWD_internal_CA>/FWD_INTER_CA.cer


# Certificate and key to install in Automation Hub node

#

automationhub_ssl_cert=<path_to_ATHub_cert>/pulp_webserver.c

rt  #

automationhub_ssl_key=<path_to_ATHub_cert>/pulp_webserver.ke

y
```


Variables for AT Hub Installation	Value
registry_username	10069912|ansibleaap

registry_password	eyJhbGciOiJSUzUxMiJ9.eyJzdWIiOiJiZDM4OTdiMmY 2OTU0OGVkYmFmNWQ5Mjk2ZWNiMmUwYyJ9. ms ZgRR8wYfCjF8W1BvMgb9IkydPlzfcyYgSWb4Dm7i z7 nmKJ_GrktgXJrfVasfjsV46sstn6WzpzciFah5L7ZZAn 0 amrPbRNxs4Spu2GgN97vVRFfJ1O2yUlM3XmNgs R1 yQAPfw4jQ95pN9TnHm5RwMfpg65MlH9l3KVM mN F9cyM3J27k5mAjjm6zsiwmHXyEtxF5RkXCduN5ZF gh HHqKtD3kl2nW0r3drLIGN6PXH6klQn8sROVrihki ggk ay53pSvozXf zliaUNr2XHtZj2DDrYDlY8gMvYKF0G77UoT0OlrA wU MAGcY-UFnpYJHncgLdjWAJxWmV LiWhgeOrauznW4n9OjbfTtbSO_m1g2Q81LIjB4Lx 4T uYuZJ5MadH_izNciUTitPFhofbHrVF43942Dfp E_tR9LE9FtzxRCnB2rvFMLEM9vBhLctnkBF682fr1 b9 EaCKWc2cEE5KE4g1cMwT_oHxappv5eIxgghJda_I U DKukjpZjW8MMHyqTdA16S2P6StnxOXOp947kqP z SV5YSrSUSylBnYRYX2RuVwjSv2LyEW8PE2ybZc5C hc Sci5Yg1NylmLULZurCihjW86triHJI5edyNpshnZV_r kV 1uwX6MP MP3CAjiS7VLF6lvZEp7UiUMZ08qEBBet9zBnfSO db Q0vA3IfI
automationhub_admin_password	P@ssw0rd1234
automationhub_pg_password	P@ssw0rd1234

5.1.5 Automation Controller Answer File Preparation

(The following procedures should be run on AAP controller node only)

Copy the downloaded Ansible Automation Platform 2.2 Setup Bundle - **ansible-automation-platform-setup-bundle-2.2.0-6.1.tar.gz** to /tmp.

Extract Ansible Automation Platform Setup Bundle:

```
[root@LGOEASIACAPPP02 var]# cd /var/
[root@LGOEASIACAPPP02 var]# tar zxvf
/tmp/ansible-automation-platform setup-bundle-2.2.0-6.1.tar.gz

[root@LGOEASIACAPPP02 var]# chown -R fwdadmin:fwdadmin
ansible automation-platform-setup-bundle-2.2.0-6.1

[root@LGOEASIACAPPP02 var]# exit
```

Edit the Red Hat Ansible Automation Platform installer inventory file:

```
[fwdadmin@LGOEASIACAPPP02 ~]$ cd
/var/ansible-automation-platform-setup bundle-2.2.0-6.1/


[fwdadmin@LGOEASIACAPPP02
ansible-automation-platform-setup-bundle 2.2.0-6.1]$ cp
inventory inventory.org

[fwdadmin@LGOEASIACAPPP02
ansible-automation-platform-setup-bundle 2.2.0-6.1]$ vi
inventory
```

Inventory file:

```
# Automation Controller Nodes
# There are two valid node_types that can be assigned for this
group. # A node_type=control implies that the node will only be
able to run # project and inventory updates, but not regular
jobs.
# A node_type=hybrid will have the ability to run
everything. # If you do not define the node_type, it
defaults to hybrid. #
# control.example node_type=control
# hybrid.example node_type=hybrid
# hybrid2.example <- this will default to hybrid
[automationcontroller]
lgoeasiacapp02.fwdasia.intranet

[automationcontroller:vars]
peers=execution_nodes
```



```
# Execution Nodes


# There are two valid node_types that can be assigned for this
```

```
group. # A node_type=hop implies that the node will forward jobs to
an  execution node.
# A node_type=execution implies that the node will be able to run
jobs. # If you do not define the node_type, it defaults to execution.
#
# hop.example node_type=hop
# execution.example node_type=execution
# execution2.example <- this will default to execution
[execution_nodes]
lgoeasiacapp03.fwdasia.intranet

[database]


[all:vars]
# Need to run sudo to install
ansible_become=true
ansible_become_method='sudo'

admin_password='<your password>'

pg_host=''
pg_port=5432

pg_database='awx'
pg_username='awx'
pg_password='<your password>'
pg_sslmode='prefer' # set to 'verify-full' for client-side enforced SSL

# Execution Environment Configuration
# Credentials for container registry to pull execution
environment  images from,
# registry_username and registry_password are required
for  registry.redhat.io
registry_url='registry.redhat.io'
registry_username='<Red Hat Registry Service Username>'
registry_password='<Red Hat Registry Service Password>'

# Receptor Configuration
#
receptor_listener_port=27199

# SSL-related variables

# If set, this will install a custom CA certificate to the system
trust  store.
custom_ca_cert=<path_to_FWD_Internal_CA>.cer

# Certificate and key to install in nginx for the web UI and
API
web_server_ssl_cert=<path_to_AAP_controller_new_cert>/tower.cer
t
web_server_ssl_key=<path_to_AAP_controller_new_cert>/tower.key
```

```
# Certificate and key to install in Automation Hub node
# automationhub_ssl_cert=/path/to/automationhub.cert
# automationhub_ssl_key=/path/to/automationhub.key

# Server-side SSL settings for PostgreSQL (when we are installing
it). # postgres_use_ssl=False
# postgres_ssl_cert=/path/to/pgsql.crt
# postgres_ssl_key=/path/to/pgsql.key

# The default install will register node to the Red Hat Insights
Service # if the node is registered with Subscription Manager. Set
to False to  disable.
enable_insights_collection = False

## /tmp size is too low to extract the installation bundle EE
images. ## Setup another temp folder for enough size to extract
the EE images. ee_images_tmp_dir='/var/lib/awx'
```


Variables for Automation Controller Installation	Value
registry_username	10069912|ansibleaap
registry_password	eyJhbGciOiJSUzUxMiJ9.eyJzdWIiOiJiZDM4OTdiMmY 2OTU0OGVkYmFmNWQ5Mjk2ZWNiMmUwYyJ9. ms ZgRR8wYfCjF8W1BvMgb9IkydPlzfcyYgSWb4Dm7i z7 nmKJ_GrktgXJrfVasfjsV46sstn6WzpzciFah5L7ZZA n0 amrPbRNxs4Spu2GgN97vVRFfJ1O2yUlM3XmNgs R1 yQAPfw4jQ95pN9TnHm5RwMfpg65MlH9l3KVM mN F9cyM3J27k5mAjjm6zsiwmHXyEtxF5RkXCduN5Z Fgh HHqKtD3kl2nW0r3drLIGN6PXH6klQn8sROVrihkig gk ay53pSvozXf zliaUNr2XHtZj2DDrYDlY8gMvYKF0G77UoT0OlrA wU MAGcY-UFnpYJHncgLdjWAJxWmV LiWhgeOrauznW4n9OjbfTtbSO_m1g2Q81LIjB4Lx 4T uYuZJ5MadH_izNciUTitPFhofbHrVF43942Dfp E_tR9LE9FtzxRCnB2rvFMLEM9vBhLctnkBF682fr1 b9 EaCKWc2cEE5KE4g1cMwT_oHxappv5eIxgghJda_I U DKukjpZjW8MMHyqTdA16S2P6StnxOXOp947kqP z SV5YSrSUSylBnYRYX2RuVwjSv2LyEW8PE2ybZc5C hc

	Sci5Yg1NylmLULZurCihjW86triHJI5edyNpshnZV_rkV 1uwX6MP MP3CAjiS7VLF6lvZEp7UiUMZ08qEBBet9zBnfSO db Q0vA3IfI
admin_password	P@ssw0rd1234
pg_password	P@ssw0rd1234

5.2 Installation

5.2.1 Install Automation Hub:

(The following procedures should be run on AT Hub node only)

```
[root@LGOEASIACAPPP01~]# cd
/var/ansible-automation-platform-setup bundle-2.2.0-6.1
```

Run the setup.sh script

```
[root@LGOEASIACAPPP01
ansible-automation-platform-setup-bundle-2.2.0- 6.1]#./setup.sh
....
....
...
PLAY RECAP
*********************************************************************
****    lgoeasiacapp01.fwdasia.intranet    :    ok=231    changed=31
unreachable=0   failed=0 skipped=234 rescued=0 ignored=0
localhost : ok=3 changed=1 unreachable=0   failed=0 skipped=1
rescued=0 ignored=0

The setup process completed successfully.
```


5.2.2 Install Automation Controller and Execution Node

(The following procedures should be run on AAP controller node only)

```
[fwdadmin@LGOEASIACAPPP02 ~]$ cd
/var/ansible-automation-platform-setup bundle-2.2.0-6.1/
```

Run the setup.sh with sudo for installing the required system packages on the Automation Controller node first, then it would fail for other tasks.

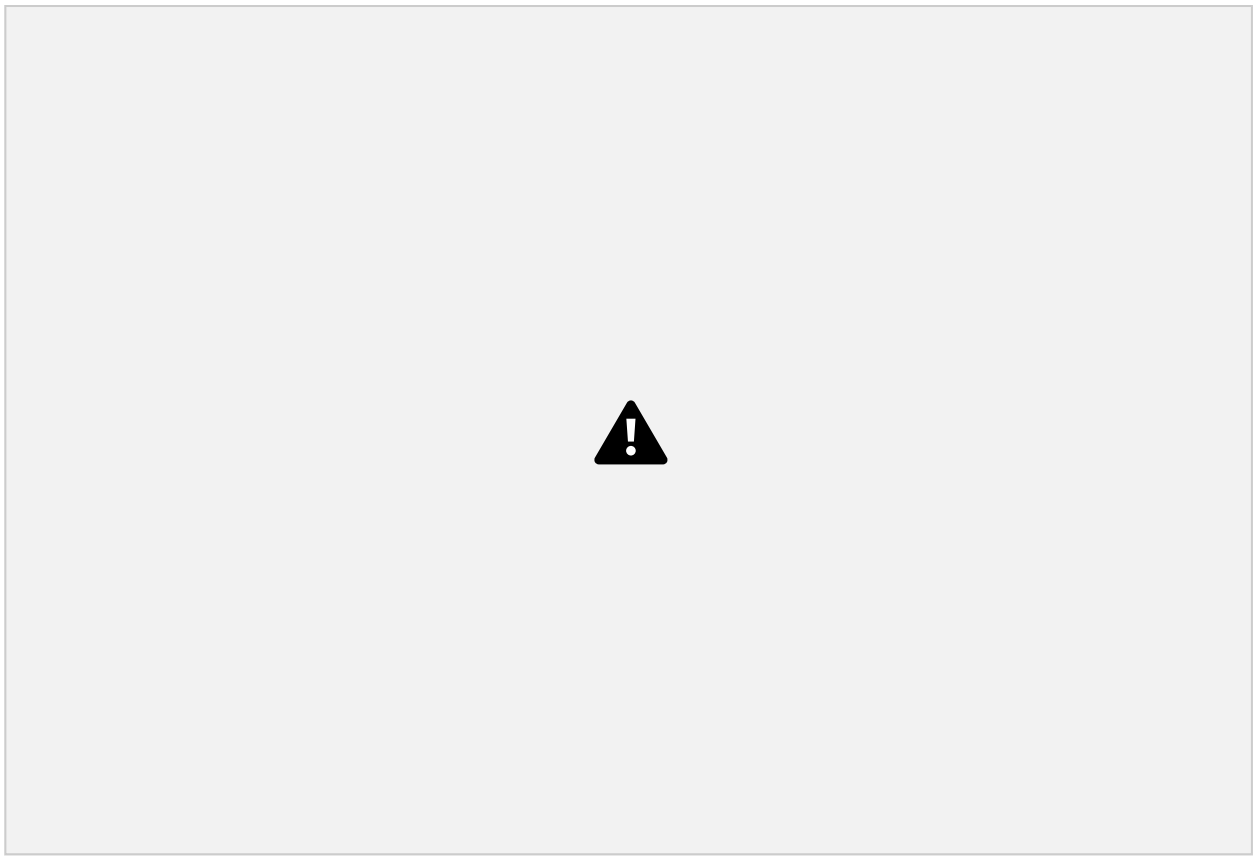
```
[fwdadmin@LGOEASIACAPPP02
ansible-automation-platform-setup-bundle 2.2.0-6.1]$ sudo
./setup.sh
....
....
Transaction Summary
================================================================================
==== ============================================================
Install 20 Packages
....
....
PLAY [Group all valid hosts for AAP installation]
*****************************

TASK [Gathering Facts]
********************************************************* fatal:
[lgoeasiacapp02.fwdasia.intranet]: FAILED! => {"msg": "Invalid
become method specified, could not find matching plugin: ''sudo''.
Use  `ansible-doc -t become -l` to list available plugins."}
fatal: [lgoeasiacapp03.fwdasia.intranet]: FAILED! => {"msg":
"Invalid  become method specified, could not find matching plugin:
''sudo''. Use  `ansible-doc -t become -l` to list available
plugins."}

PLAY RECAP
*****************************************************************
****    lgoeasiacapp02.fwdasia.intranet    :    ok=0    changed=0
unreachable=0  failed=1 skipped=0 rescued=0 ignored=0
lgoeasiacapp03.fwdasia.intranet : ok=0 changed=0 unreachable=0
failed=1 skipped=0 rescued=0 ignored=0
localhost : ok=0 changed=0 unreachable=0  failed=0 skipped=1
rescued=0 ignored=0
```

Run the setup.sh again **without sudo**:

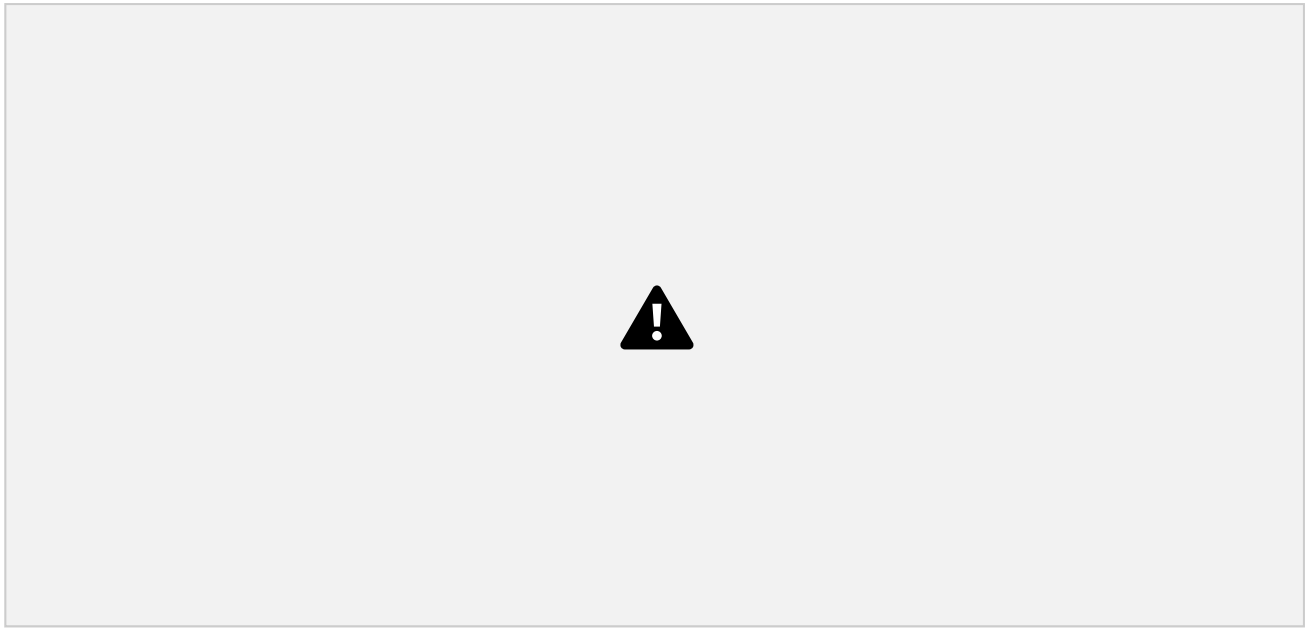
```
ansible-automation-platform-setup-bundle-2.2.0-6.1]$ ./setup.sh
```


Once the installation is completed, using the client PC's browser to browse to the Ansible Automation Controller webUI.

https://10.50.5.4

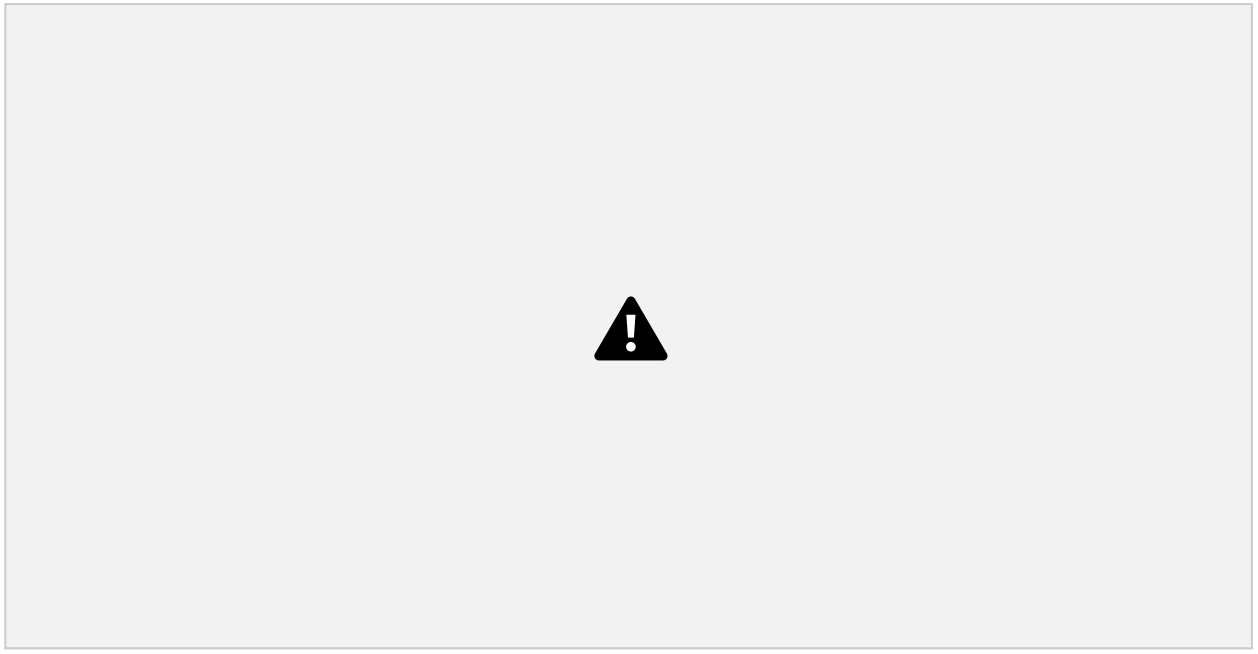


Once login into AAP controller webUI, the subscription setup page would be shown for first login.
Using Red Hat login to active the subscription.
Enter the Red Hat login username and password.
Click Get subscription.

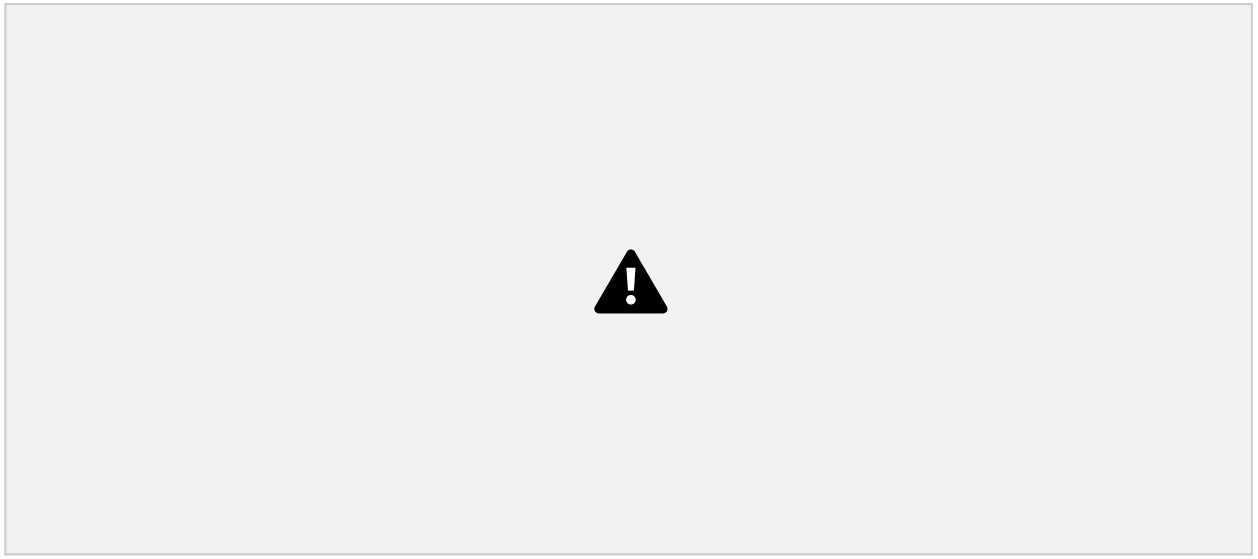


Select the appropriate subscription.

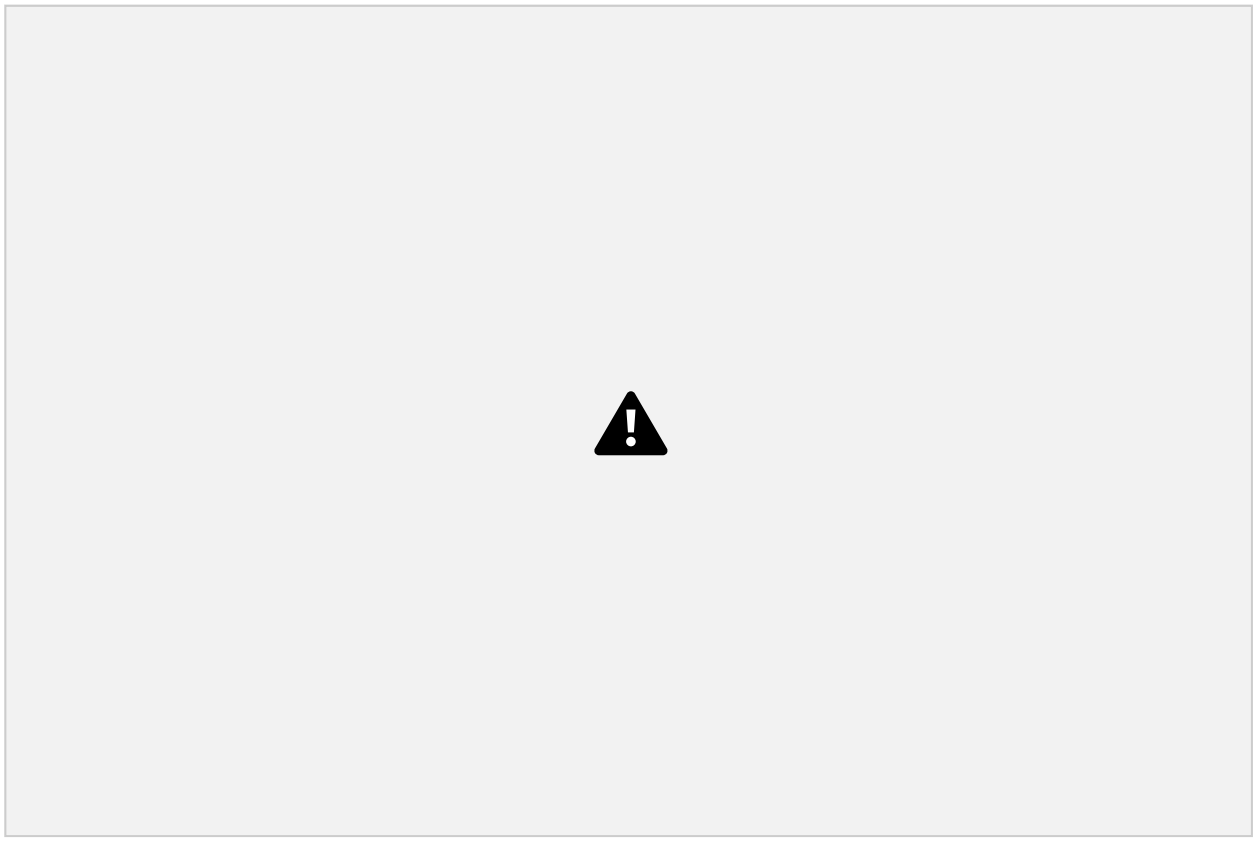
Unselect User analytics and Automation Analytics. Click Next.



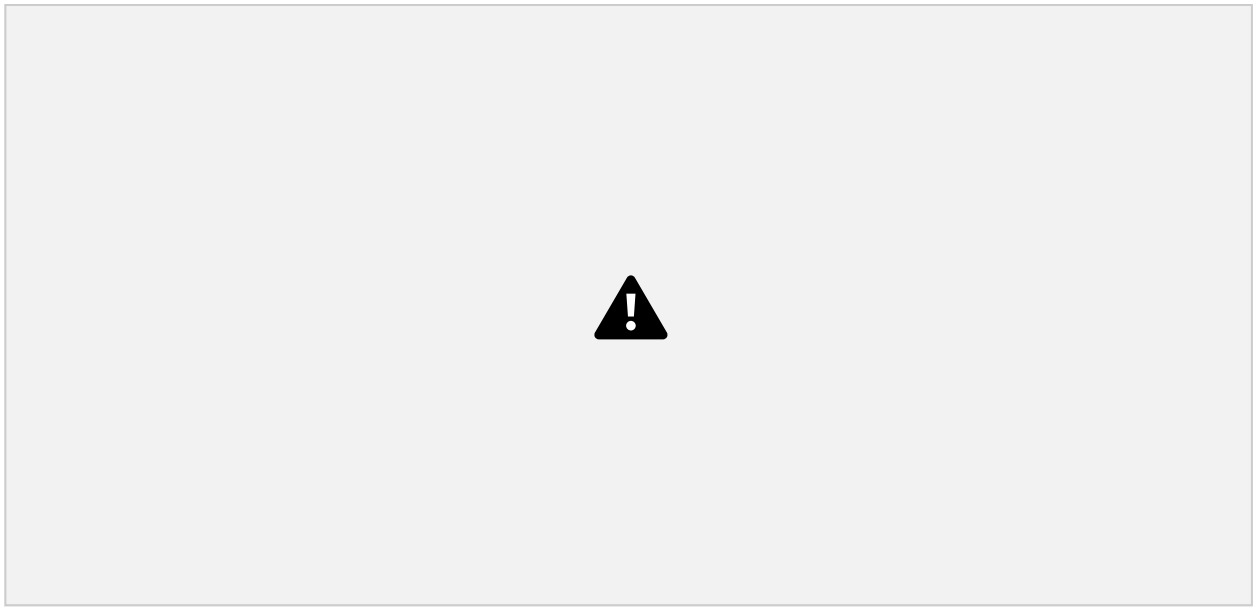
Click Submit.



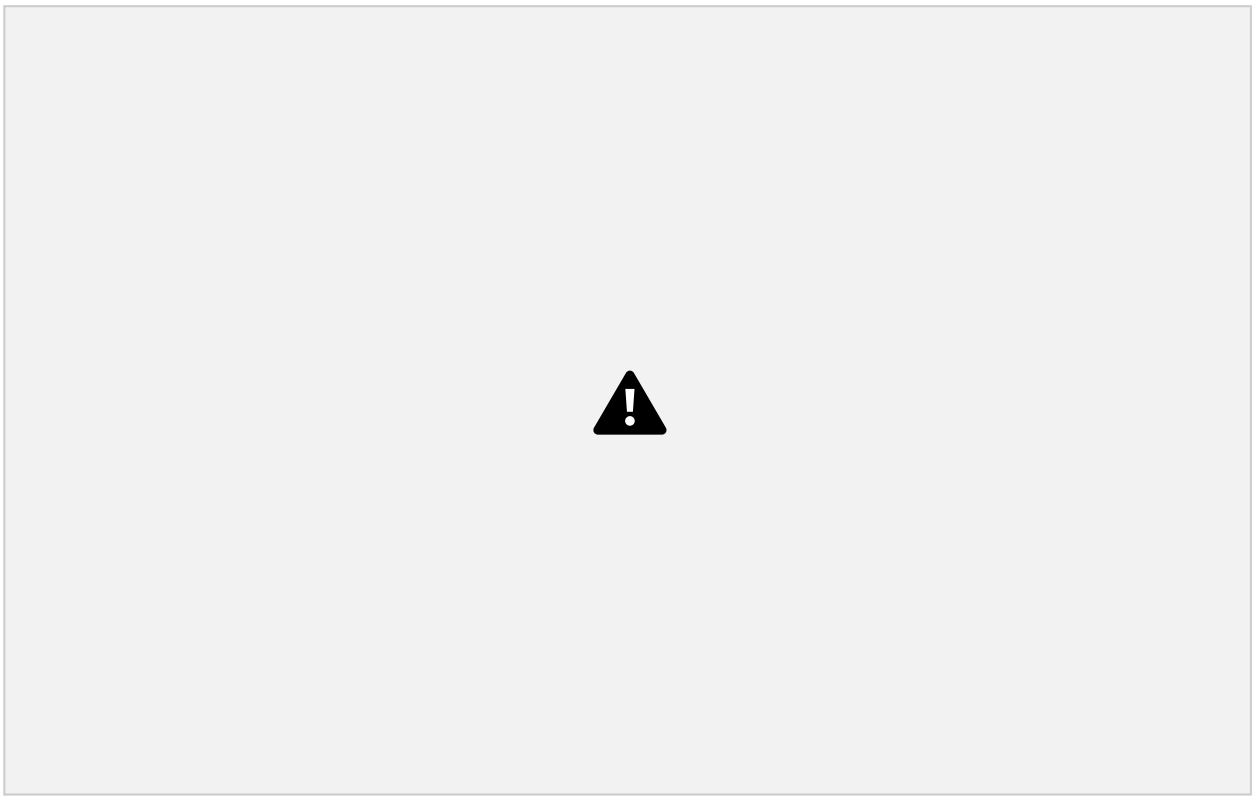
Click Settings from the left navigation bar. Click the Subscription settings to review Subscription Details:



Now the Ansible Automation Platform should show up on its dashboard.



Under the Administration menu from the left navigation bar;
Click Topology View to check the nodes status.



5.2.3 Adding a new Execution Node

(Adding the vm-core-shs-aps1-prd-sgp-rh8-aapexe-01 execution node)

Make sure the **Execution node** updates to the RHEL version same as the Controller node, by registering the

node to the RHSM / Satellite server (using the RHSM provided RHEL 8 repositories), and performing the OS update first.

(The following procedures should be run on AAP controller node only)

Share the SSH public key to the execution nodes.

```
[fwdadmin@LGOEASIACAPPP02 ~]$ ssh-copy-id
fwdadmin@vm-core-shs-aps1-prd sgp-rh8-aapexe-01.fwdasia.intranet
```

Edit the Red Hat Ansible Automation Platform installer inventory file:

```
[fwdadmin@LGOEASIACAPPP02 ~]$ cd
/var/ansible-automation-platform-setup bundle-2.2.0-6.1/


[fwdadmin@LGOEASIACAPPP02
ansible-automation-platform-setup-bundle 2.2.0-6.1]$ cp
inventory inventory.bak

[fwdadmin@LGOEASIACAPPP02
ansible-automation-platform-setup-bundle 2.2.0-6.1]$ vi
inventory
```

Inventory file:

```
# Automation Controller Nodes
# There are two valid node_types that can be assigned for this
group. # A node_type=control implies that the node will only be
able to run # project and inventory updates, but not regular
jobs.
# A node_type=hybrid will have the ability to run
everything. # If you do not define the node_type, it
defaults to hybrid. #
# control.example node_type=control
# hybrid.example node_type=hybrid
# hybrid2.example <- this will default to hybrid
[automationcontroller]
lgoeasiacapp02.fwdasia.intranet

[automationcontroller:vars]
peers=execution_nodes

# Execution Nodes
# There are two valid node_types that can be assigned for this
group. # A node_type=hop implies that the node will forward jobs
to an  execution node.
# A node_type=execution implies that the node will be able to run
jobs.
```

```
# If you do not define the node_type, it defaults to
execution. #
# hop.example node_type=hop
# execution.example node_type=execution
# execution2.example <- this will default to execution
 [execution_nodes]
lgoeasiacapp03.fwdasia.intranet
vm-core-shs-aps1-prd-sgp-rh8-aapexe-01.fwdasia.intranet ← Adding this
line add the execution node

 [database]

 [all:vars]
# Need to run sudo to install
ansible_become=true
ansible_become_method='sudo'

admin_password='<your password>'

pg_host=''
pg_port=5432

pg_database='awx'
pg_username='awx'
pg_password='<your password>'
pg_sslmode='prefer' # set to 'verify-full' for client-side enforced SSL

# Execution Environment Configuration
# Credentials for container registry to pull execution
environment  images from,
# registry_username and registry_password are required
for  registry.redhat.io
registry_url='registry.redhat.io'
registry_username='<Red Hat Registry Service Username>'
registry_password='<Red Hat Registry Service Password>'

# Receptor Configuration
#
receptor_listener_port=27199

# SSL-related variables

# If set, this will install a custom CA certificate to the system
trust  store.
# custom_ca_cert=<path_to_FWD_Internal_CA>.cer

# Certificate and key to install in nginx for the web UI and API
#
web_server_ssl_cert=<path_to_AAP_controller_new_cert>/tower.cert
# web_server_ssl_key=<path_to_AAP_controller_new_cert>/tower.key

# Certificate and key to install in Automation Hub node
# automationhub_ssl_cert=/path/to/automationhub.cert
# automationhub_ssl_key=/path/to/automationhub.key
```

```
# Server-side SSL settings for PostgreSQL (when we are installing
it). # postgres_use_ssl=False
# postgres_ssl_cert=/path/to/pgsql.crt
# postgres_ssl_key=/path/to/pgsql.key

# The default install will register node to the Red Hat Insights
Service # if the node is registered with Subscription Manager. Set
to False to  disable.
enable_insights_collection = False

## /tmp size is too low to extract the installation bundle EE
images. ## Setup another temp folder for enough size to extract
the EE images. ee_images_tmp_dir='/var/lib/awx'
```

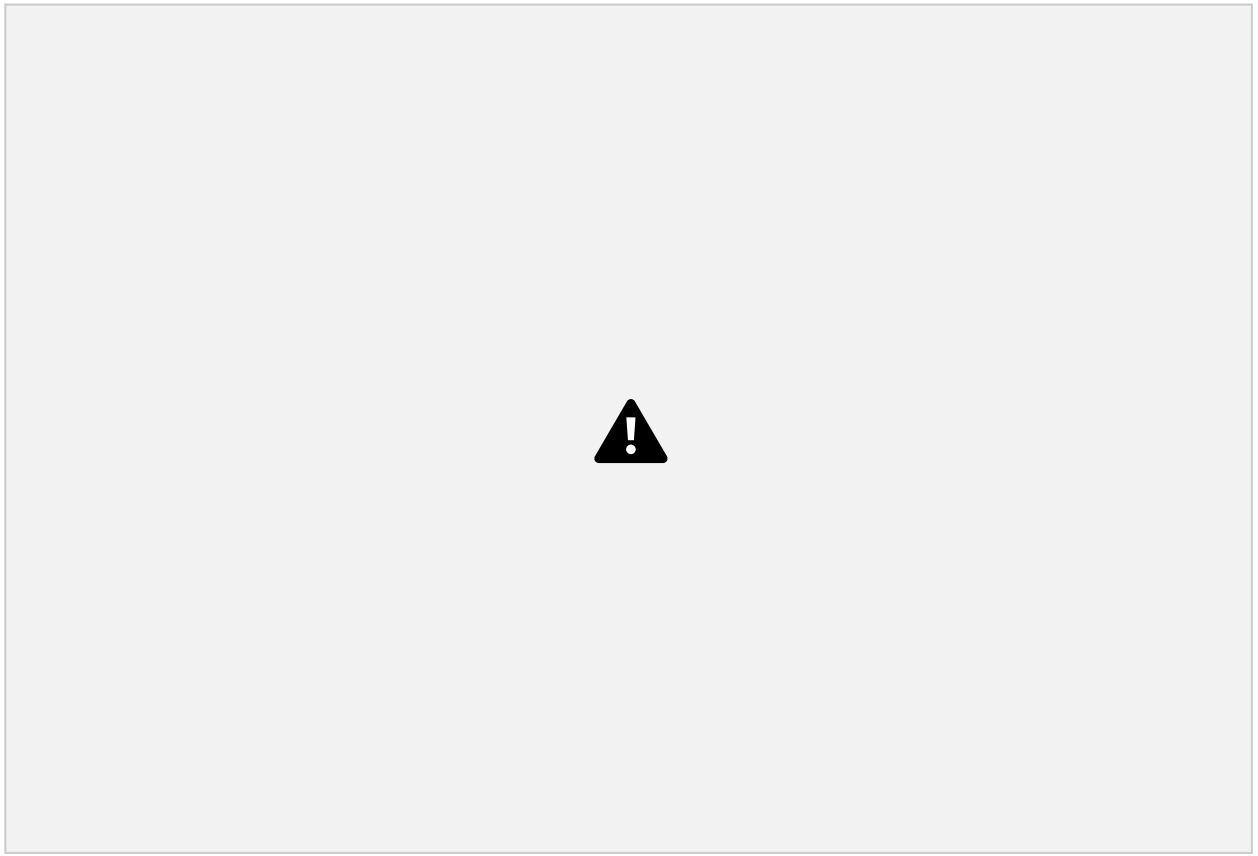
Run the AAP backup first from setup.sh script.

```
 [fwdadmin@LGOEASIACAPPP02
ansible-automation-platform-setup-bundle 2.2.0-6.1]$ ./setup.sh
-b
```

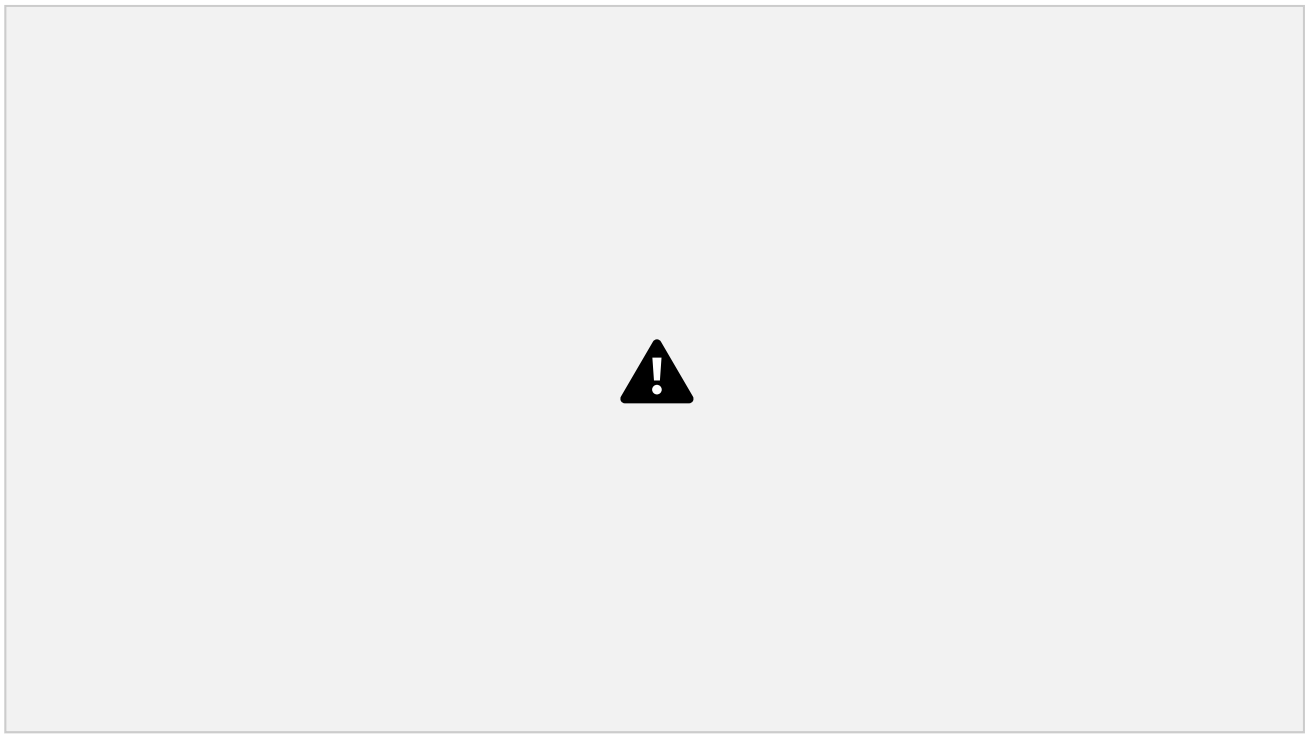
Run the setup.sh script to start configuring the new execution node.

```
 [fwdadmin@LGOEASIACAPPP02
ansible-automation-platform-setup-bundle 2.2.0-6.1]$ ./setup.sh
```


Once the installation is completed, browse to the Ansible Automation Controller webUI.



In the Administration menu from the left navigation bar, Click Topology View to check the nodes status.

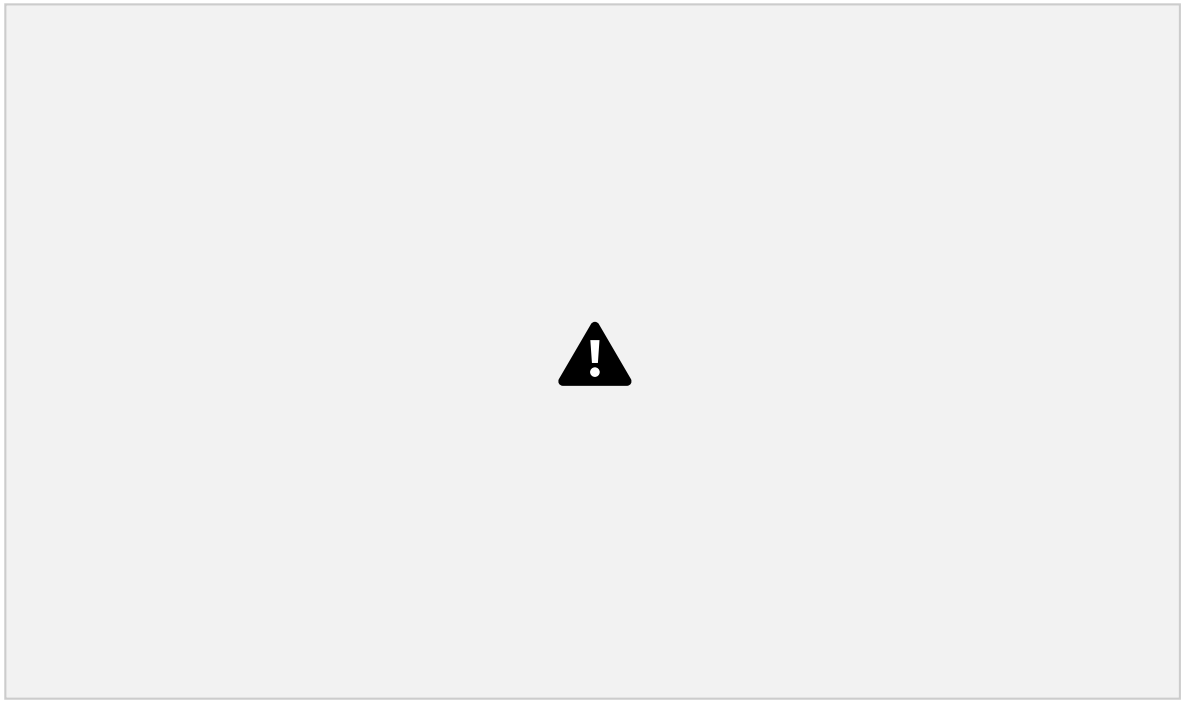


5.3 Post-Installation Settings

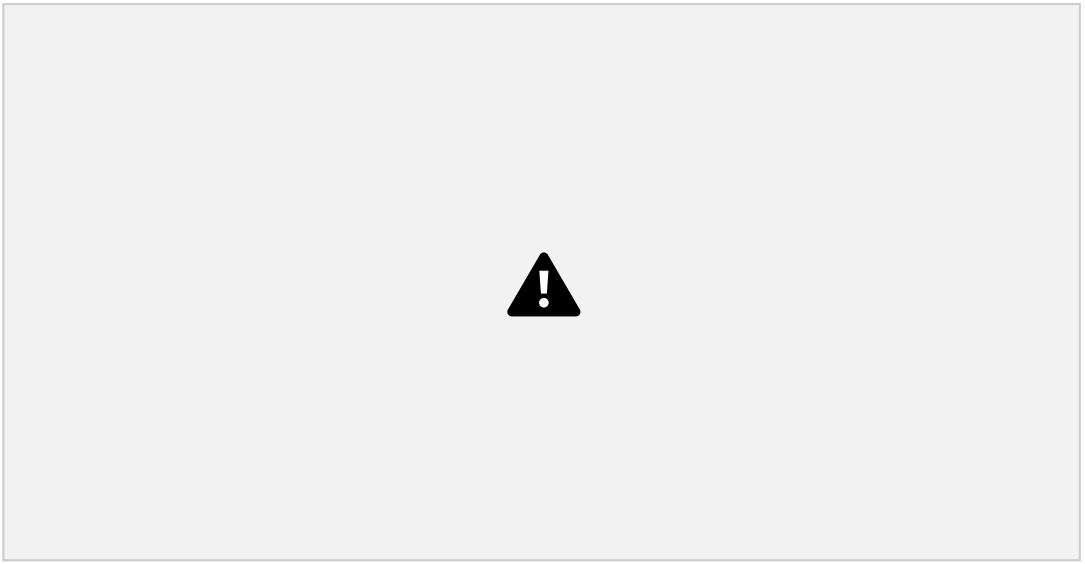
5.3.1 Configure the Ansible Automation Hub

5.3.1.1 Configuring Automation Hub remote registry

1. Login to Automation Hub.



2. Navigate to Remote Registries. Click Add remote registry



3. Type the following in the Edit remote registry window.

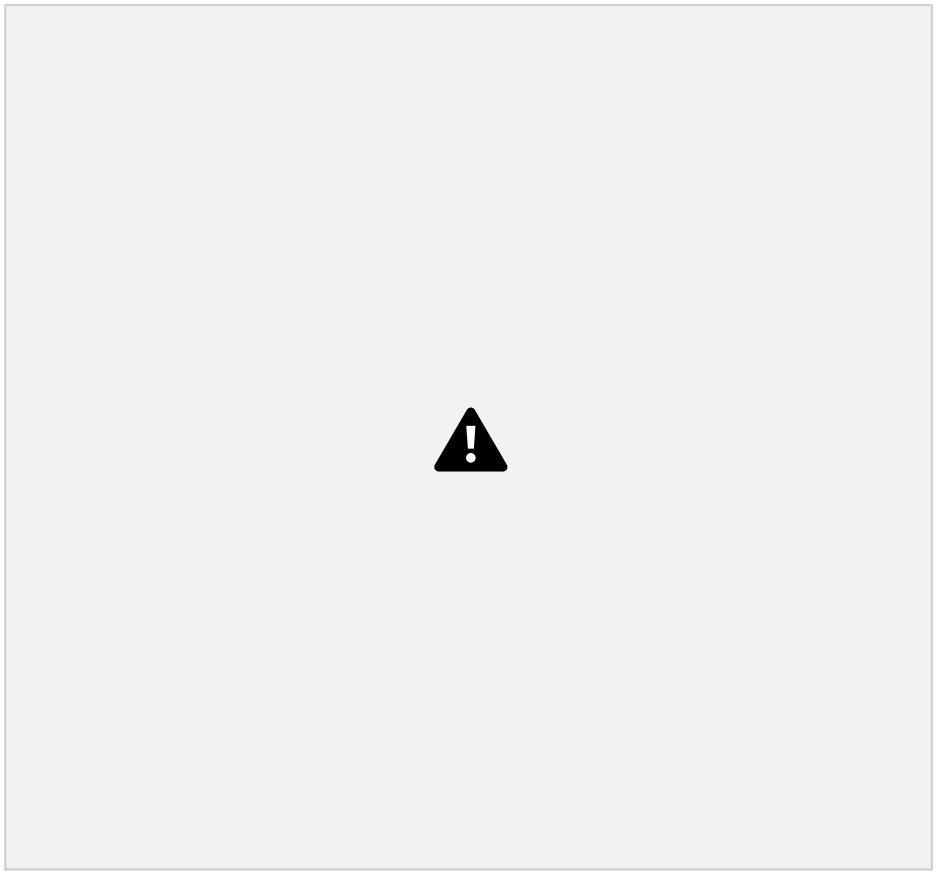
Name: Red Hat Registry IO

URL: https://registry.redhat.io

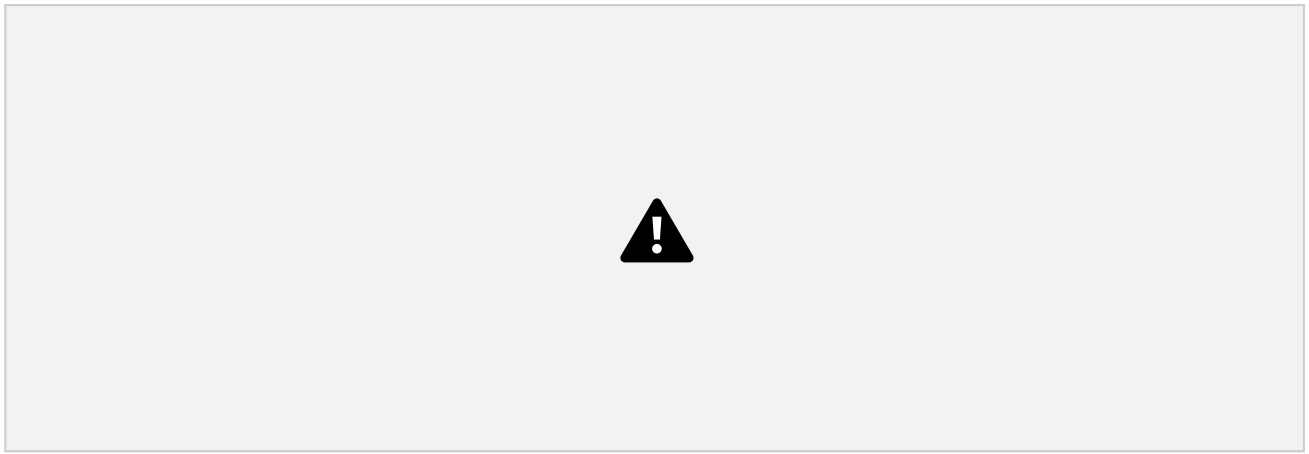
Username: {{ Red Hat Registry Service Account }}

Password: {{ Red Hat Registry Service Password }}

Item	Value
Username	10069912|ansibleaap
Password	eyJhbGciOiJSUzUxMiJ9.eyJzdWIiOiJiZDM4OTdiMmY2OTU0OGVkYmFmNWQ5Mjk2ZWNiMmUwYyJ9.msZgRR8wYfC jF8W1BvMgb9IkydPlzfcyYgSWb4Dm7iz7nmKJ_GrktgXJrfV asfjsV46sstn6WzpzciFah5L7ZZAn0amrPbRNxs4Spu2GgN9 7vVRFfJ1O2yUlM3XmNgsR1yQAPfw4jQ95pN9TnHm5Rw Mfpg65MlH9l3KVMmNF9cyM3J27k5mAjjm6zsiwmHXyEt xF5RkXCduN5ZFghHHqKtD3kl2nW0r3drLIGN6PXH6klQn8 sROVrihkiggkay53pSvozXf zliaUNr2XHtZj2DDrYDlY8gMvYKF0G77UoT0OlrAwUMAGc Y-UFnpYJHncgLdjWAJxWmV LiWhgeOrauznW4n9OjbfTtbSO_m1g2Q81LljB4Lx4TuYuZJ 5MadH_izNciUTitPFhofbHrVF43942Dfp E_tR9LE9FtzxRCnB2rvFMLEM9vBhLctnkBF682fr1b9EaCK Wc2cEE5KE4g1cMwT_oHxappv5eIxgghJda_IUDKukjpZjW 8MMHyqTdA16S2P6StnxOXOp947kqPz SV5YSrSUSylBnYRYX2RuVwjSv2LyEW8PE2ybZc5ChcSci5Y g1NylmLULZurCihjW86triHJI5edyNpshnZV_rkV1uwX6MP -MP3CAjiS7VLF6lvZEp7UiUMZ08qEBBet9zBnfSOdbQ0vA3IfI



4. Save and click the Sync from registry



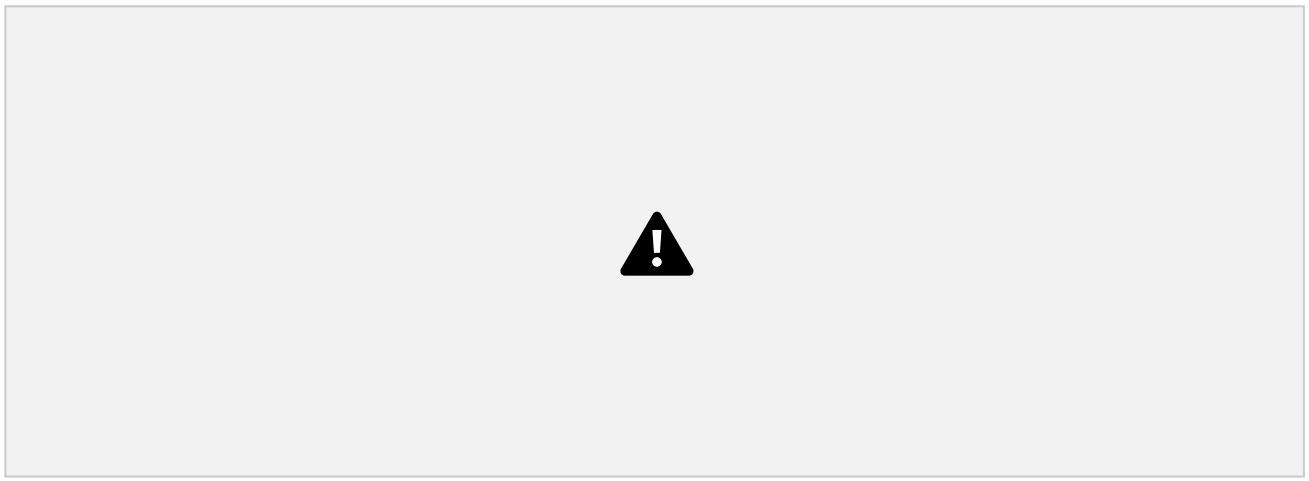
5.3.1.2 Configuring Automation Hub remote repositories to sync content from Red Hat Certified collections

1. Log in to cloud.redhat.com

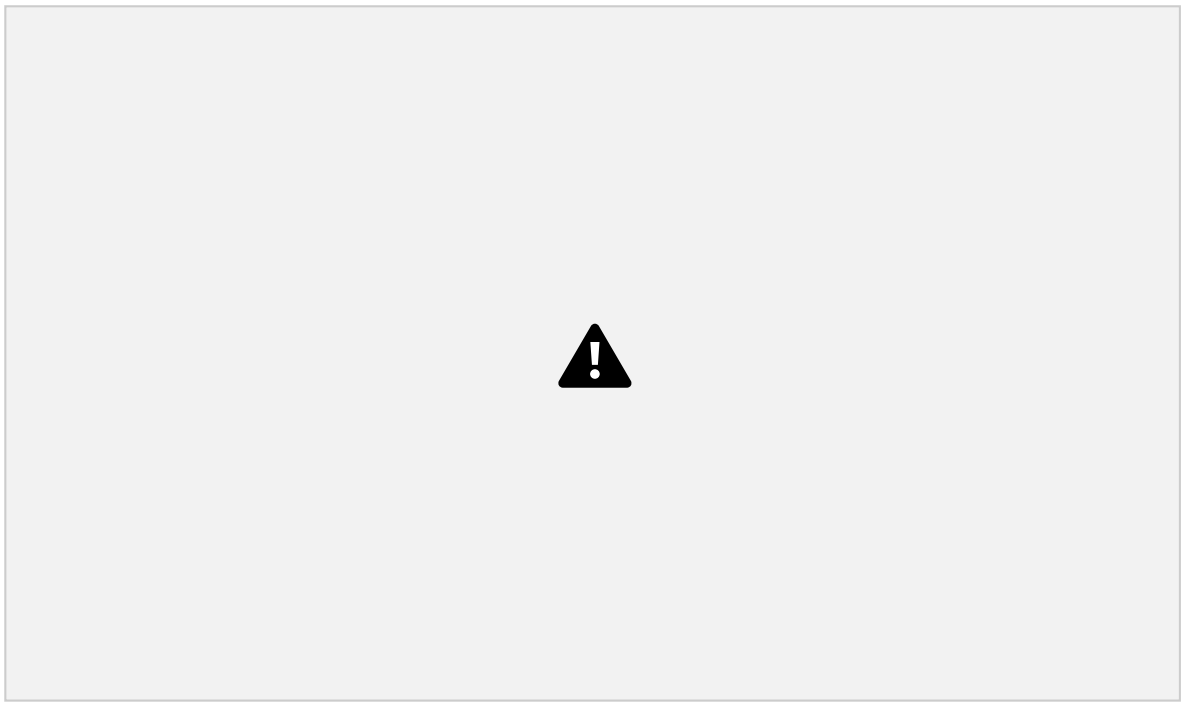
2. Get the token from the https://console.redhat.com/ansible/automation-hub/token URL under the Ansible Automation Platform.

3. Click Get token. On the Token management page, click Load token

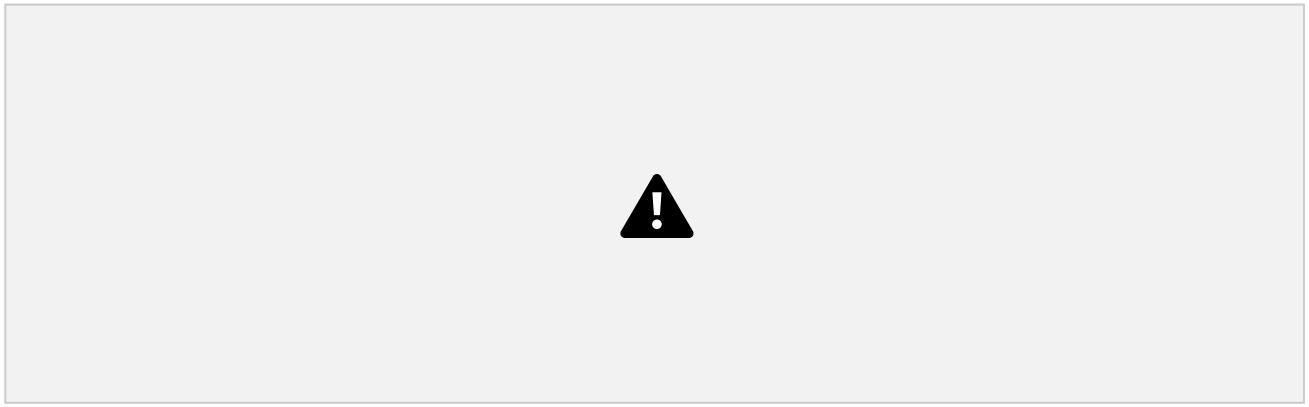
.



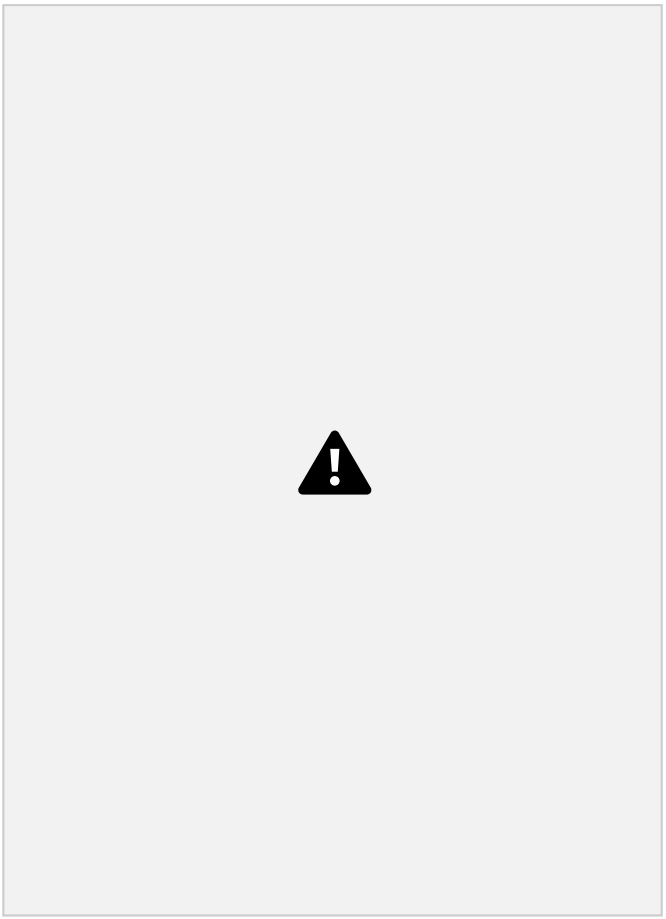
4. Log in to Automation Hub.



5. Edit the Remote Repo Management, as below.



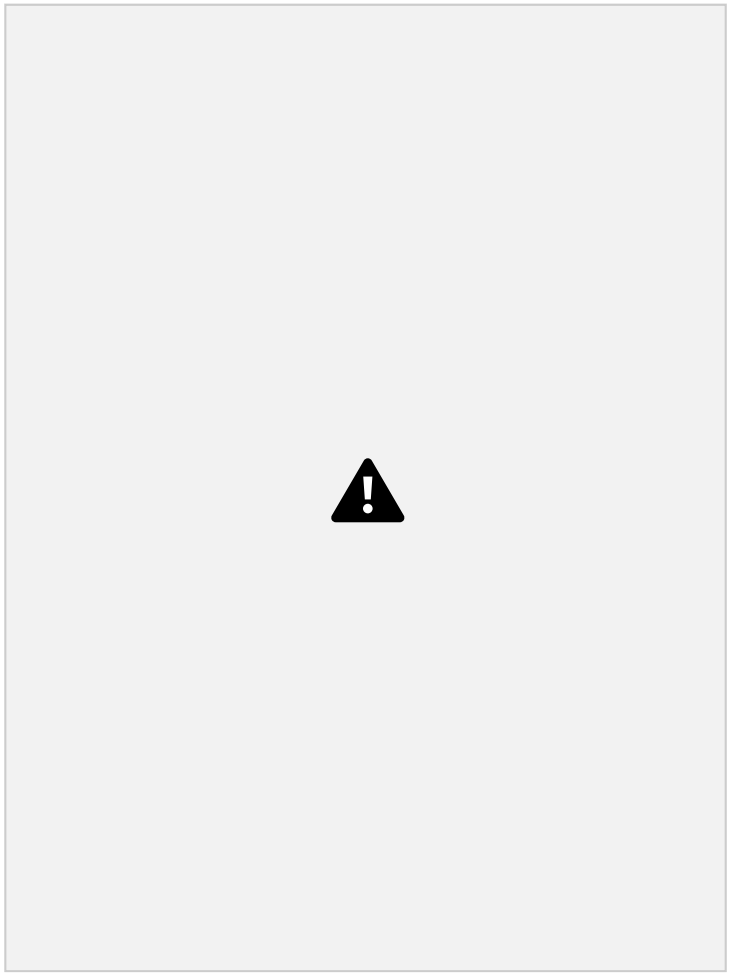
6. Type token and the username and password in the below Edit Remote window.



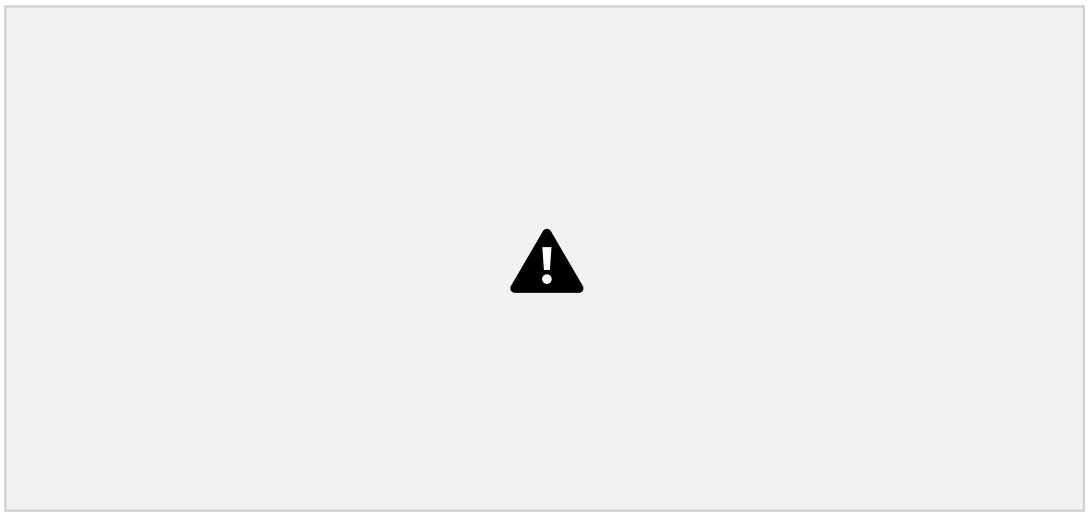
Item	Value
Token	eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJhZDUyMjdhMy1iY2ZkLTRjZjAtYTdiNi0zOTk4MzVhMDg1NjYifQ.eyJpYXQiOjE2NTQ3NDg2OTEsImp0aSI6IjY1NWJkZmQ4LTE0MTAtNGQwNi04OTFmLWU5ZTVlMTUwM2YwYSIsImlzcyI6Imh0dHBzOi8vc3NvLnJlZGhhdC5jb20vYXV0aC9yZWFsbXMvcmVkaGF0LWV4dGVybmFsIiwiYXVkIjoiaHR0cHM6Ly9zc28ucmVkaGF0LmNvbS9hdXRoL3JlYWxtcy9yZWRoYXQtZXh0ZXJuYWwiLCJzdWIiOiJmOjUyOGQ3NmZmLWY3MDgtNDNlZC04Y2Q1LWZlMTZmNGZlMGNlNjpmd2R3aW50ZWxhZG1pbiIsInR5cCI6Ik9mZmxpbmUiLCJhenAiOiJjbG91ZC1zZXJ2aWNlcyIsIm5vbmNlIjoiN2Y5MzkzMGYtN2I0My00MzJjLWE5ZDEtOTg0MGY2MDQ3NzhkIiwic2Vzc2lvbl9zdGF0ZSI6IjMzZThmNGY3LTY3YzMtNDcyZS04ODk5LTk5

	N Dc4MjY2MzA5NyIsInNjb3BlIjoib3BlbmlkIG9mZmxpbm VfY WNjZXNzIiwic2lkIjoiMzNlOGY0ZjctNjdjMy00NzJlLTg4OT kt OTk0NzgyNjYzMDk3In0.J3OPPzcZCX5TTkY6m7DK7LgLo Y m9BgX2WRtl7DQaFME

7. Click Show advanced options change the Download concurrency to 1

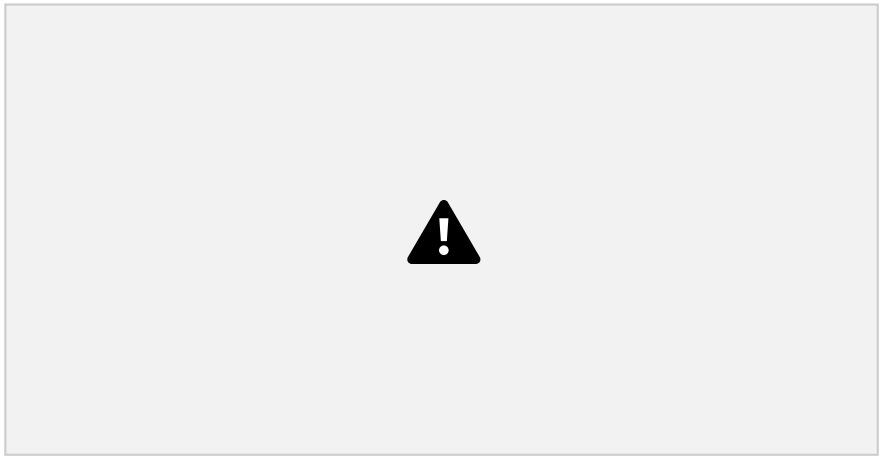


8. Save and click the Sync for the repo synchronization.

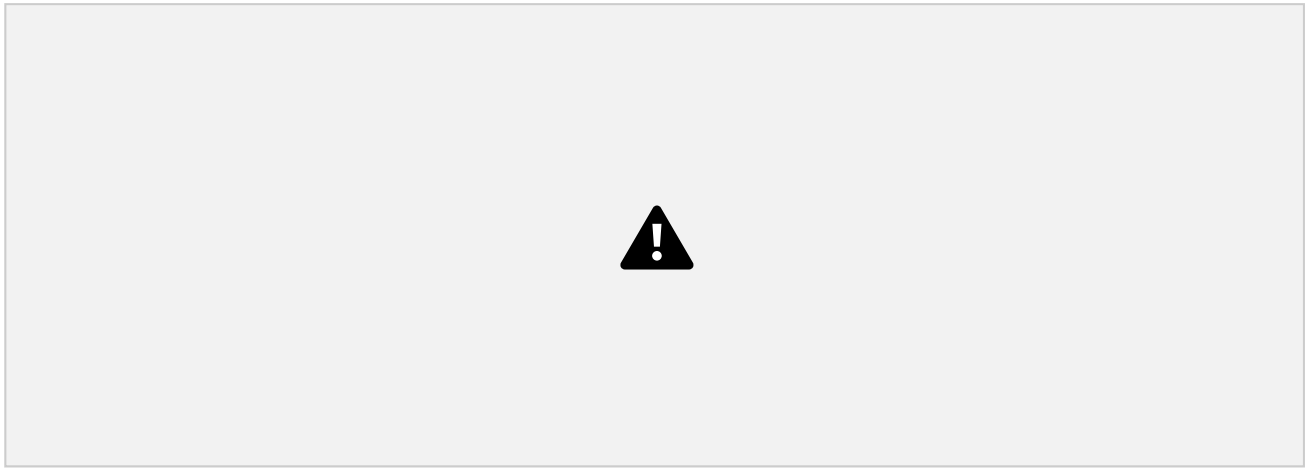


5.3.1.3 Configuring Automation Hub remote repositories to sync content from Ansible Galaxy collections

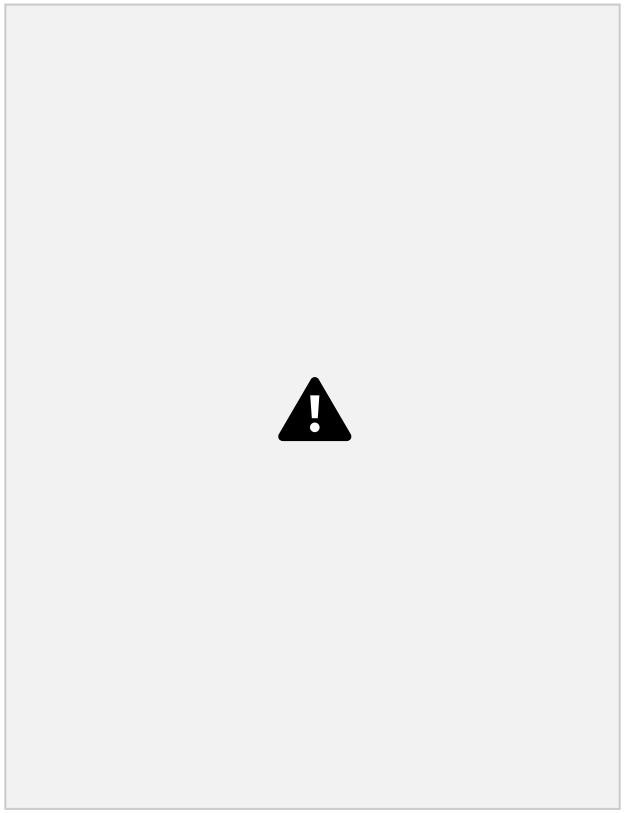
1. Navigate to Collections -> Repository Management. Click the Remotes tab.

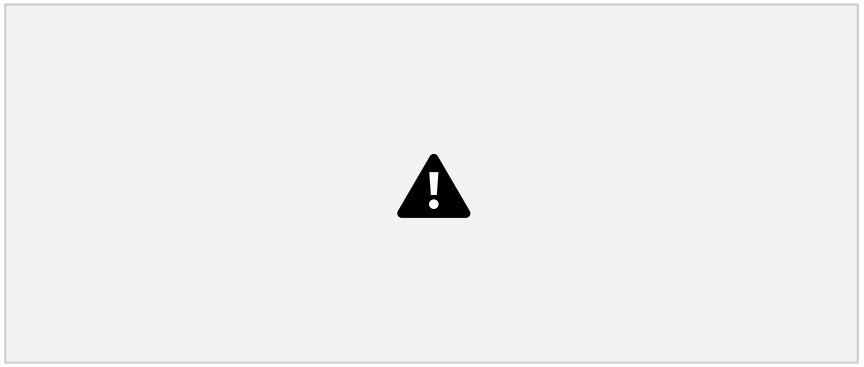


2. In the community remote, click More actions and click Edit.

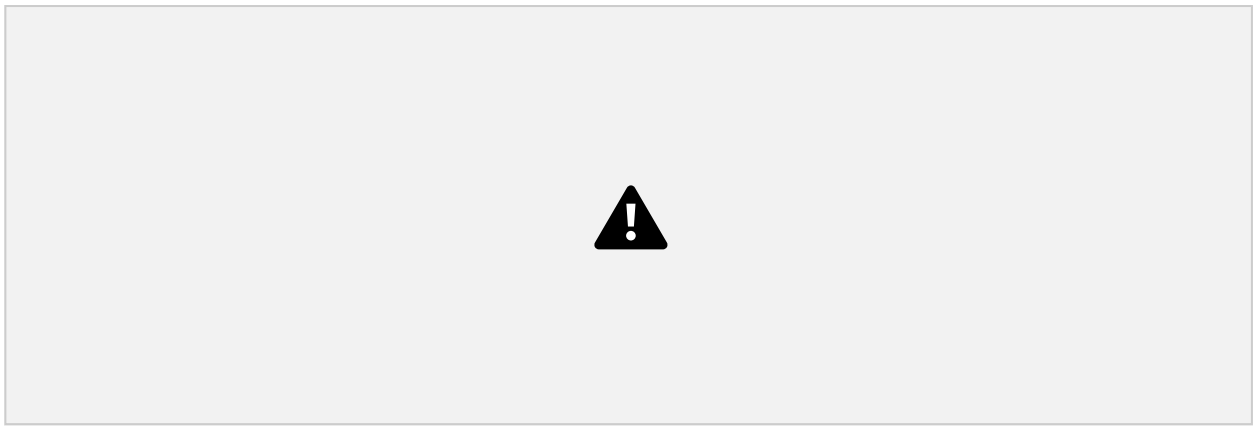


3. In the modal, click Browse and locate the requirements.yml file on your local machine.





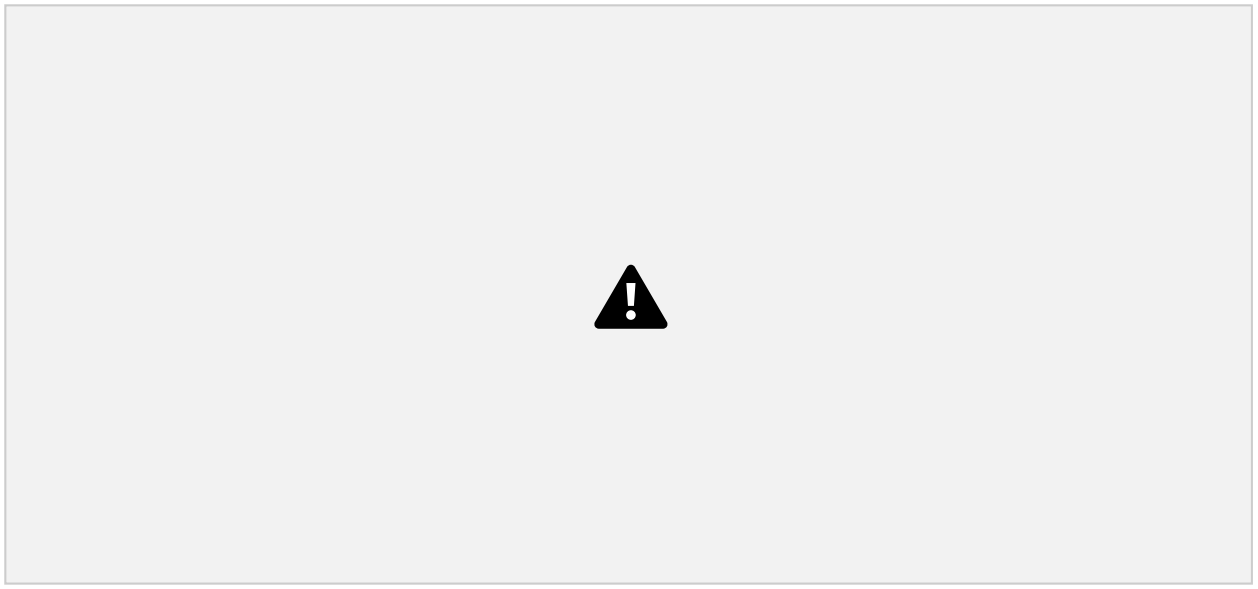
4. Click Save and click the Sync to sync collections from Ansible Galaxy and Automation Hub.



5.3.1.4 Configuring Automation Hub Execution Environments

1. Click Execution Environments from the left navigation bar.

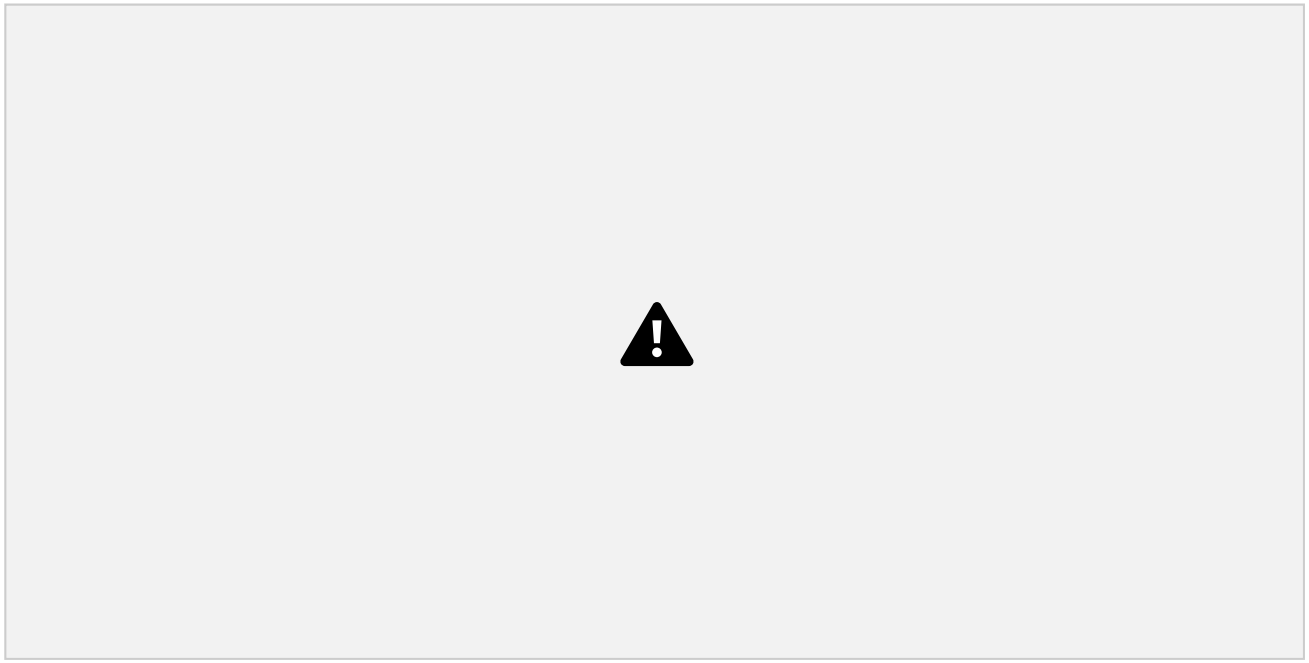
2. Add an execution environment by selecting the Add button.



3. Fill in the following fields to add the new execution environment.

Name	Upstream name	Registry	Add tag(s) to include
ee-supported-rhel8-registry redhat-io	ansible-automation-platform 22/ee-supported-rhel8	Red Hat Registry IO	latest
ee-29-rhel8-registry-redhat-io	ansible-automation-platform 22/ee-29-rhel8	Red Hat Registry IO	latest
ee-minimal-rhel8-registry-redhat io	ansible-automation-platform 22/ee-minimal-rhel8	Red Hat Registry IO	latest
ee-212-rhel8-registry-redhat-io	ansible-automation-platform 21/ee-supported-rhel8	Red Hat Registry IO	latest

4. Click ‘Sync from registry’ on the new execution environment.



5.3.1.5 Creating the Automation Hub API token

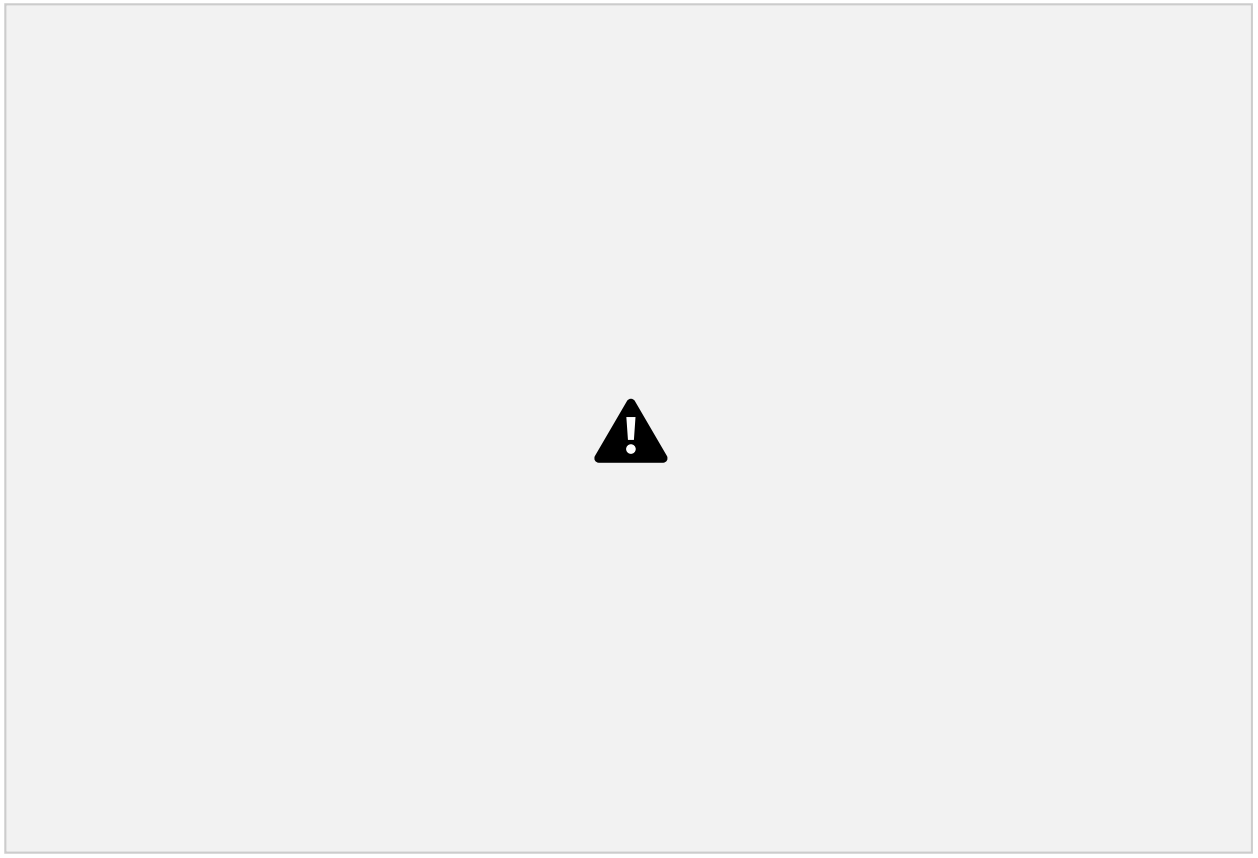
1. Click API token management from the left navigation bar.
2. Click Load Token.
3. Click the copy icon to copy the API token to the clipboard.
4. Paste the API token into a file and store in a secure location.

Item	Value
Automation Hub API token	106d737d32f6f27c6f3ffd5ad3c32a517c9237dc

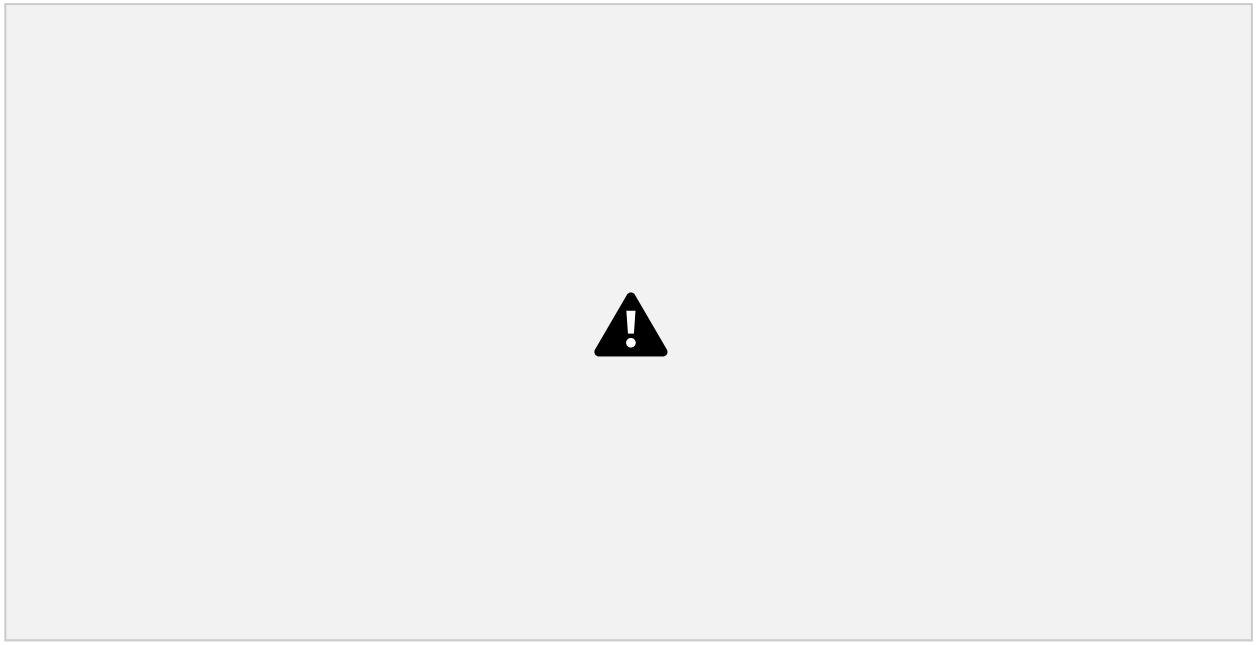
5.3.2 Configure the Ansible Automation Controller

5.3.2.1 Add Automation Hub credential

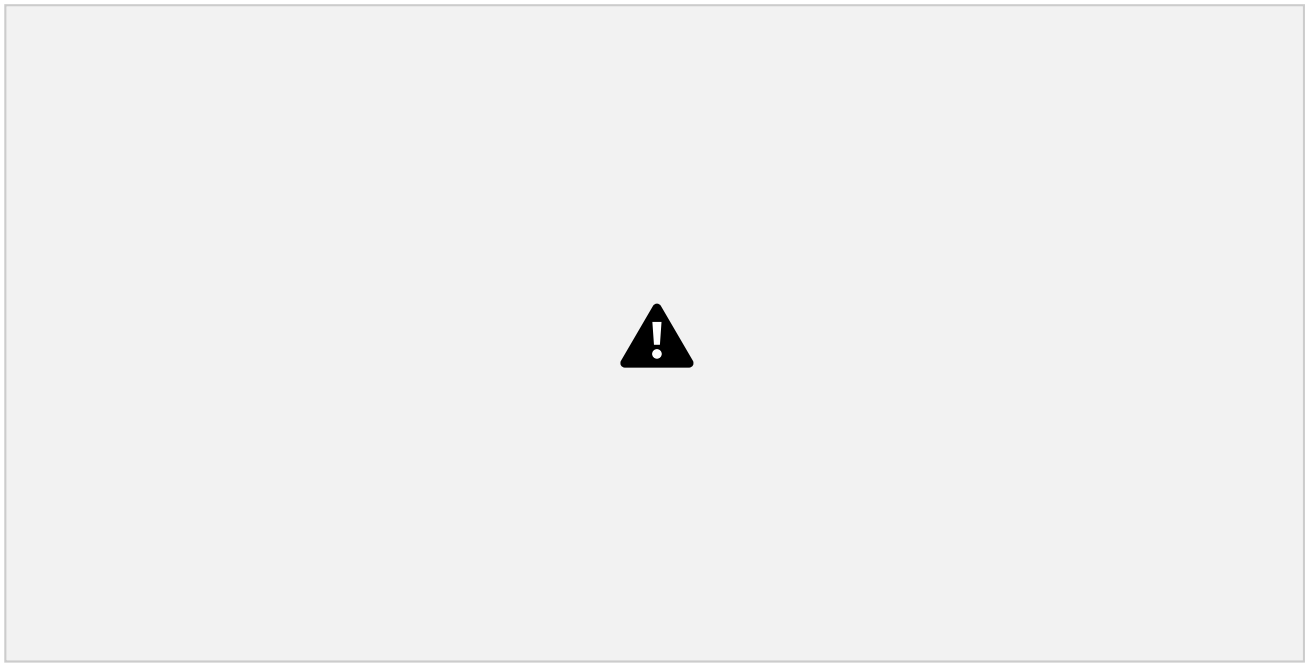
1. Login to Ansible Automation Controller



2. Click Credentials from the left navigation bar. And click the Add buttons.



3. Fill in the following fields in the Create New Credential window.



Name	ATHub Registry
Organization	FWD Group
Credential Type	Container Registry
Authentication URL	lgoeasiacapp01.fwdasia.intranet
Username	admin

Password or Token	{{ Automation Hub API Token }}

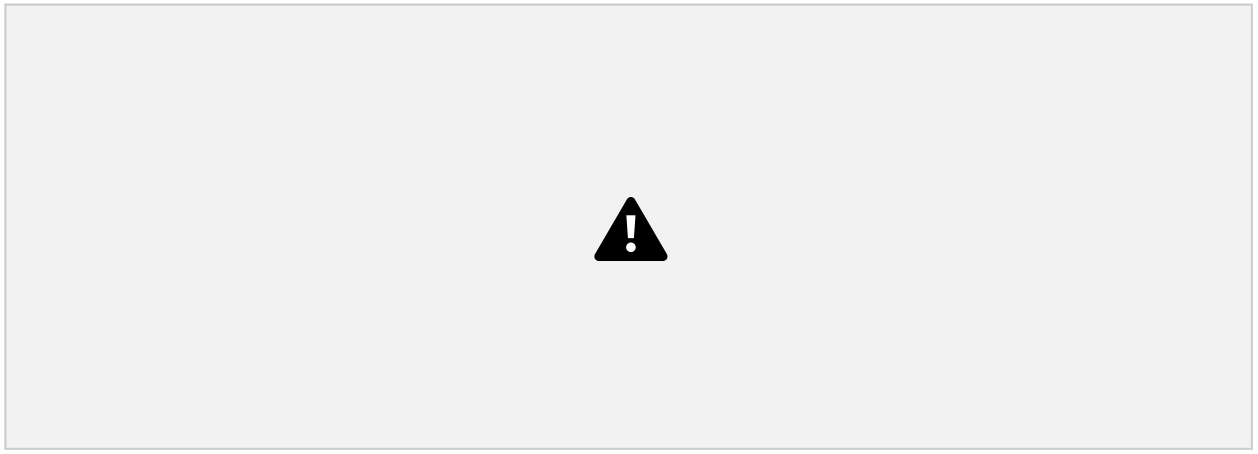
Name	ATHub RH-Certified Collections
Organization	FWD Group
Credential Type	Ansible Galaxy/Automation Hub API Token
Authentication URL	https://aap hub01.fwdasia.intranet/api/galaxy/content/ rh certified/
Auth Server URL	
Password or Token	{{ Automation Hub API Token }}

Name	ATHub Community Collections
Organization	FWD Group
Credential Type	Ansible Galaxy/Automation Hub API Token
Authentication URL	https://aap hub01.fwdasia.intranet/api/galaxy/content/com mu nity/
Auth Server URL	
Password or Token	{{ Automation Hub API Token }}

Item	**Value**
Automation Hub API token	106d737d32f6f27c6f3ffd5ad3c32a517c9237dc

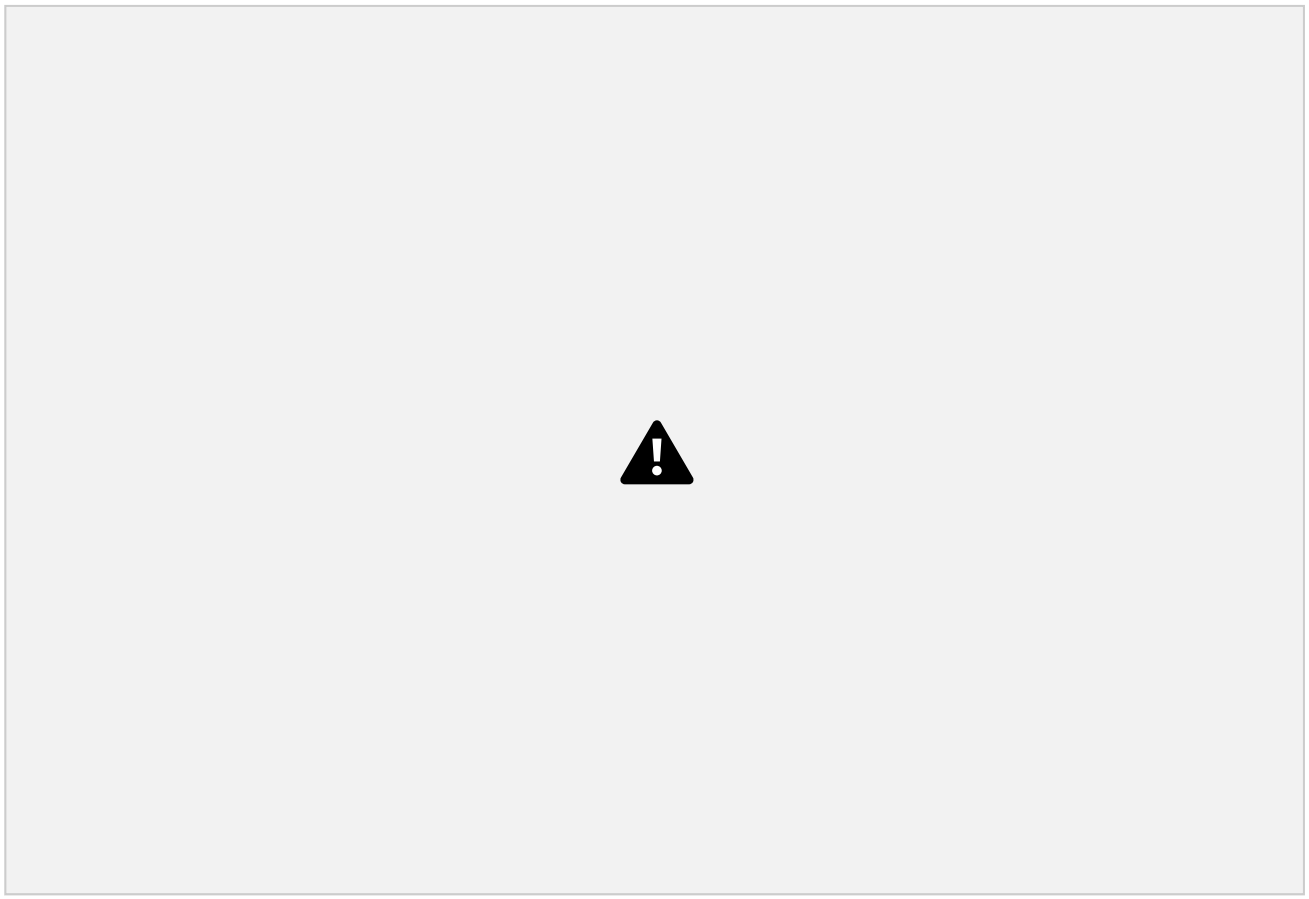
5.3.2.2 Configuring the Organizations

1. Click Organizations from the left navigation bar. Select the default and click the Edit buttons.



2. Change the name from Default to FWD Group.

3. In the Galaxy Credentials select the following credentials.

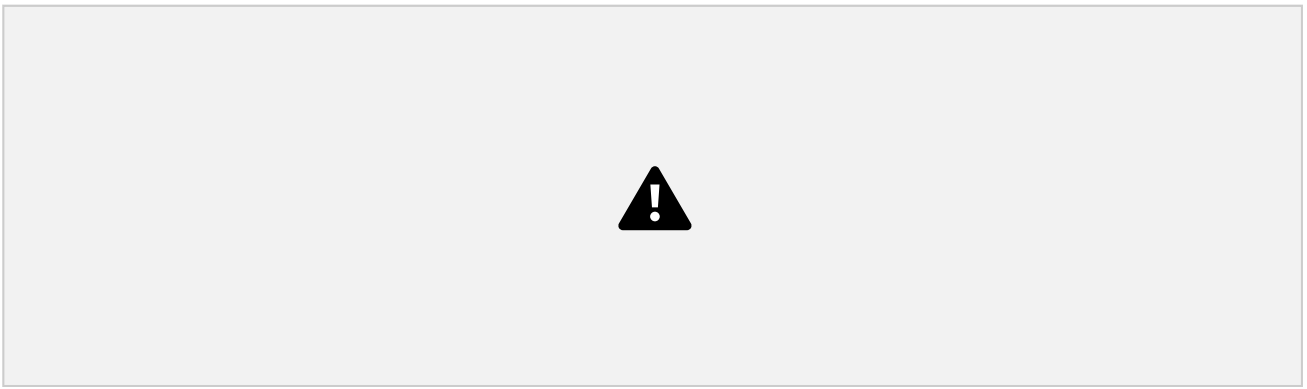


4. Click Save

5. Click Add.

6. Fill in the following fields in the Create New Organization window. And Click Save.

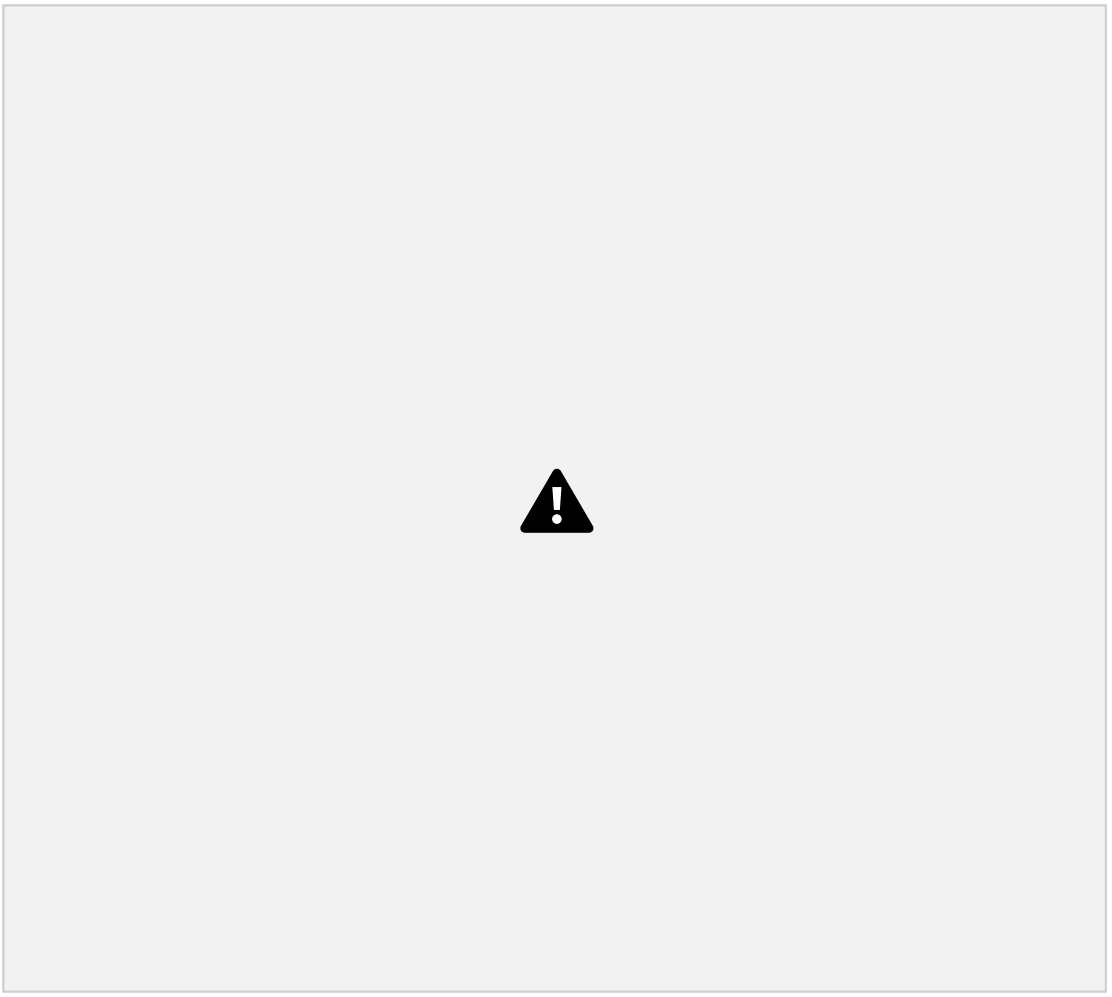
Name	FWD HKG
Description	FWD HKGroup
Galaxy Credentials	ATHub RH-Certified Collections ATHub Community Collections



5.3.2.3 Configuring Automation Controller Execution Environments

1. Click Execution Environments from the left navigation bar.

2. Add an execution environment by selecting the Add button.



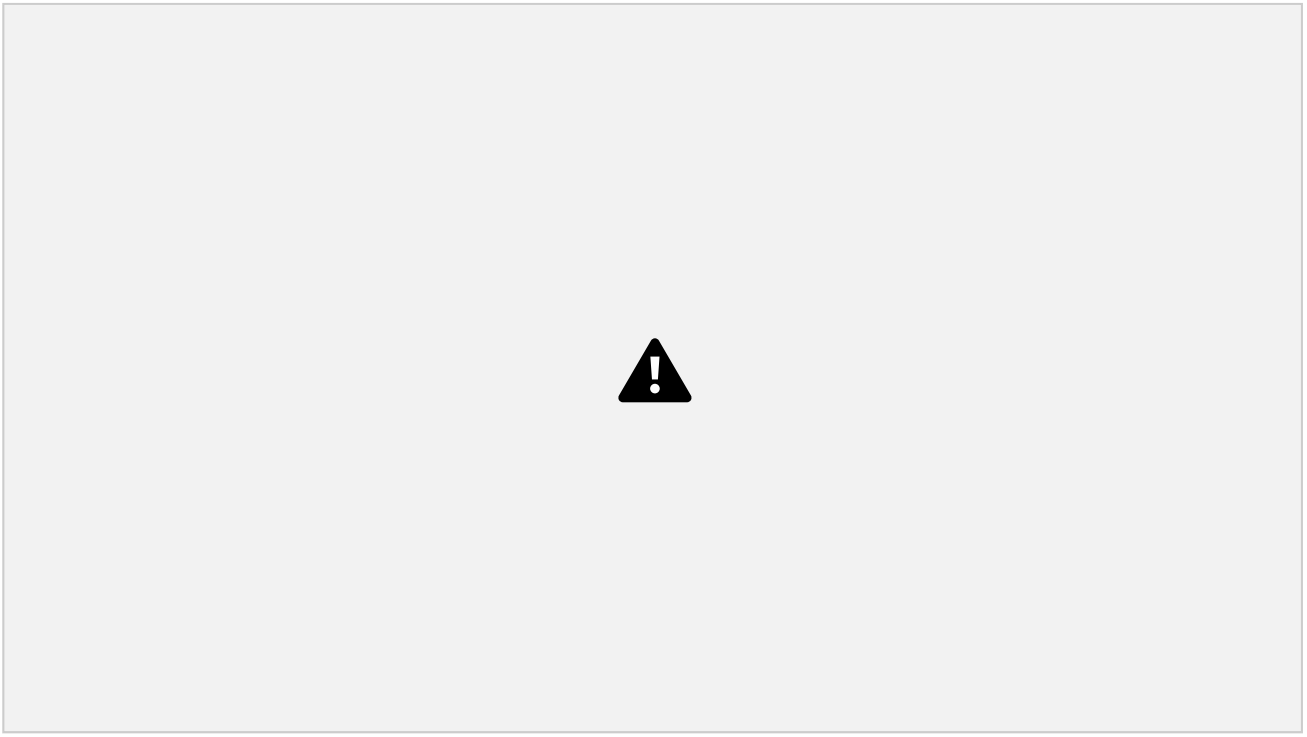
3. Fill in the following fields to add the new execution environment.

Name	ATHub Default EE
Image	aap-hub01.fwdasia.intranet/l/ee-supported rhel8:latest
Pull	Only pull the image if not present running
Description	Default EE from ATHub
Organization	
Registry credential	ATHub Registry

Name	ATHub 2.9EE
Image	aap-hub01.fwdasia.intranet/ee-29-rhel8-registry redhat-io:latest
Pull	Only pull the image if not present running

Description	EE 2.9 from ATHub
Organization	
Registry credential	ATHub Registry

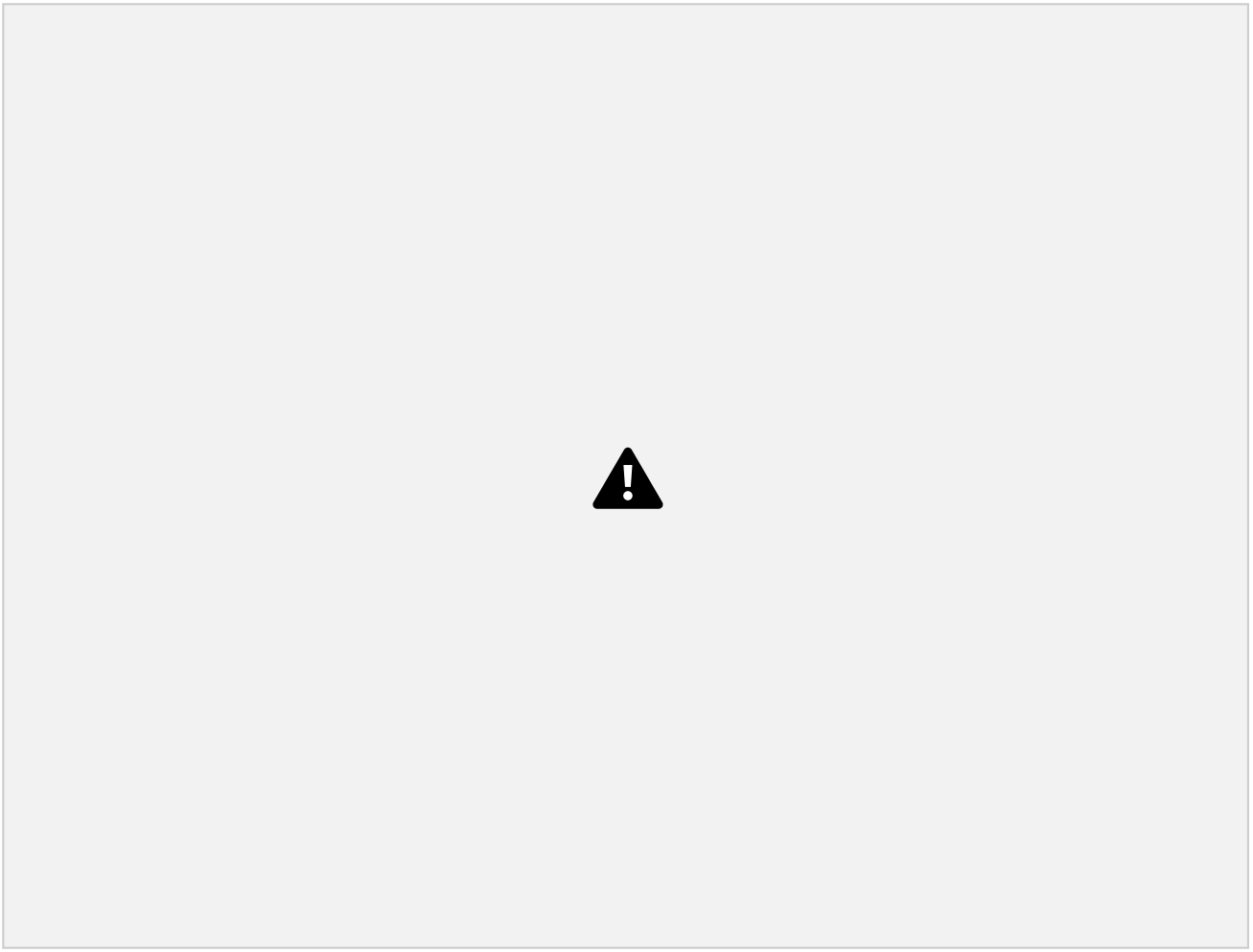
Name	ATHub 212 EE
Image	aap-hub01.fwdasia.intranet/ee-212-rhel8-registry redhat-io:latest
Pull	Only pull the image if not present running
Description	EE 212 from ATHub
Organization	
Registry credential	ATHub Registry



5.3.2.4 Add a Source Control credential for Github

1. Click Credentials from the left navigation bar. And click the Add button.

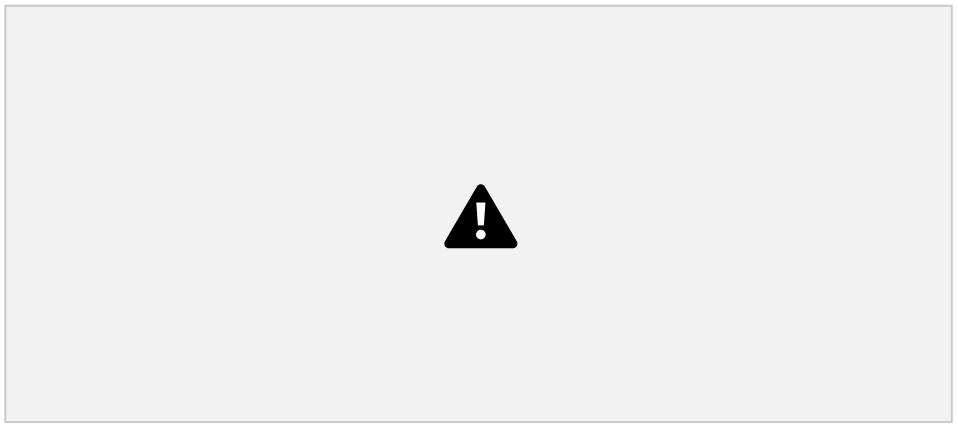
2. Fill in the following fields in the Create New Credential window. And click Save.



Name	Git SCM Login
Organization	FWD Group
Credential Type	Source Control
SCM Private Key	{{ Private Key }}

5.3.2.5 Configuring the Instance Groups

1. Click Instance Groups from the left navigation bar.
2. Click Add and select Add instance group.

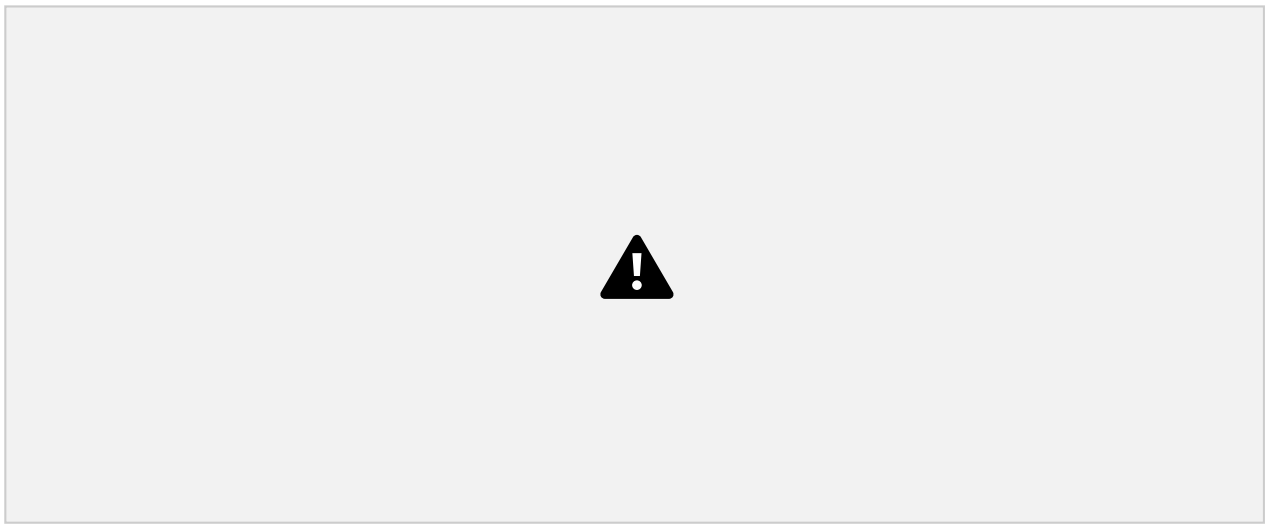


3. Fill in the following fields to add the Create new instance group window.

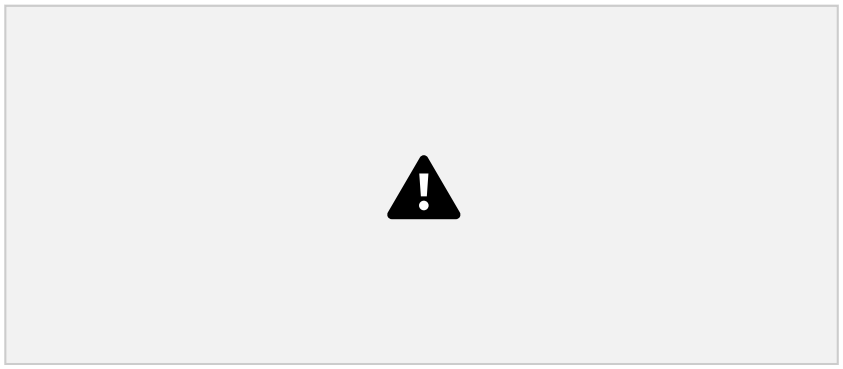
Name	AWS-Subnet 10.192.0.0/28

Name	Azure-Subnet 10.50.4.16/28

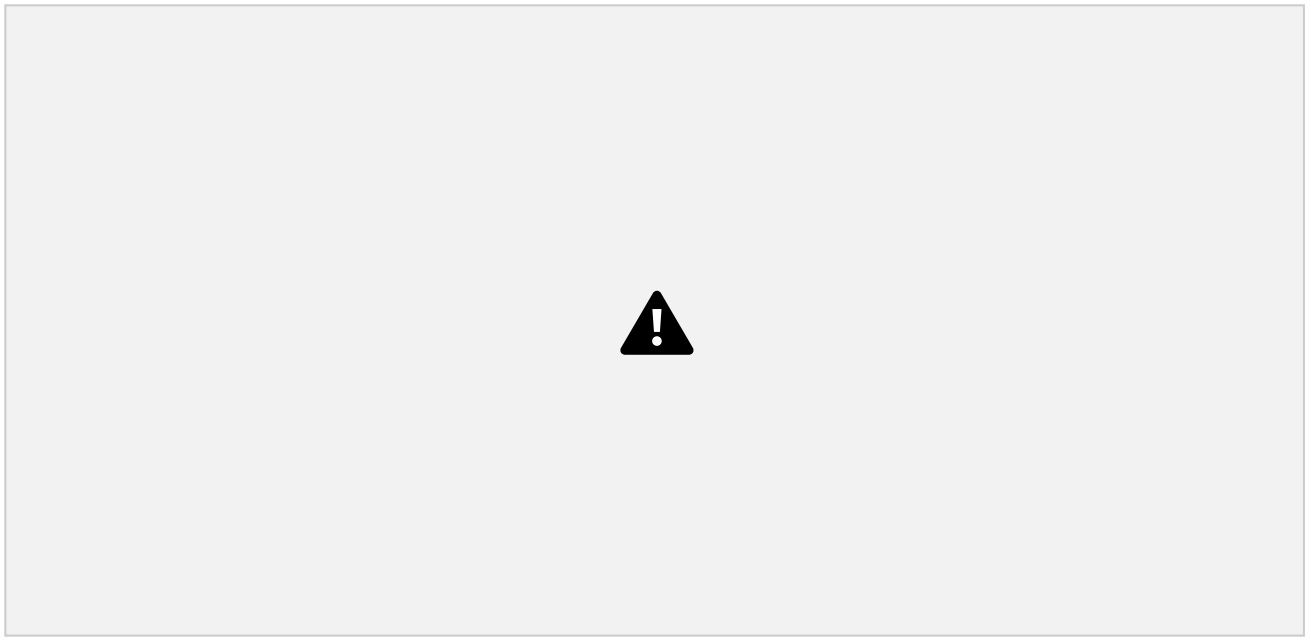
4. Click Save



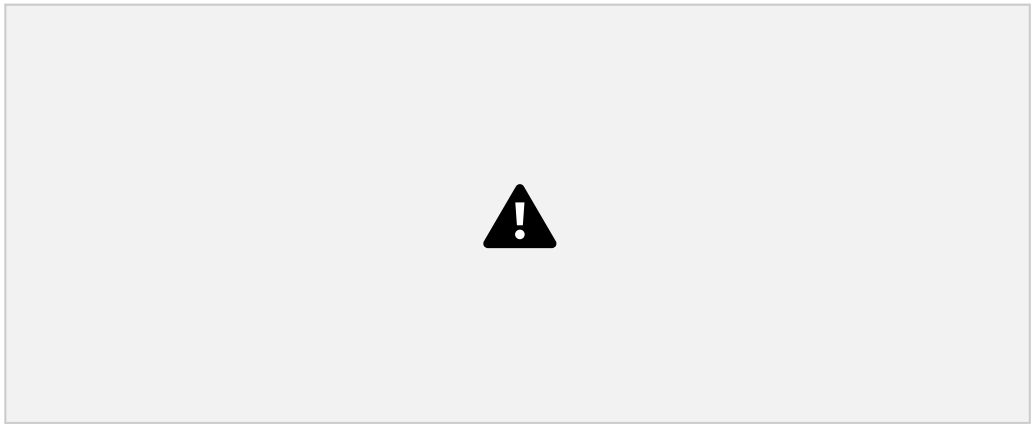
5. Click **AWS-Subnet 10.192.0.0/28**. click Instances and click Associate



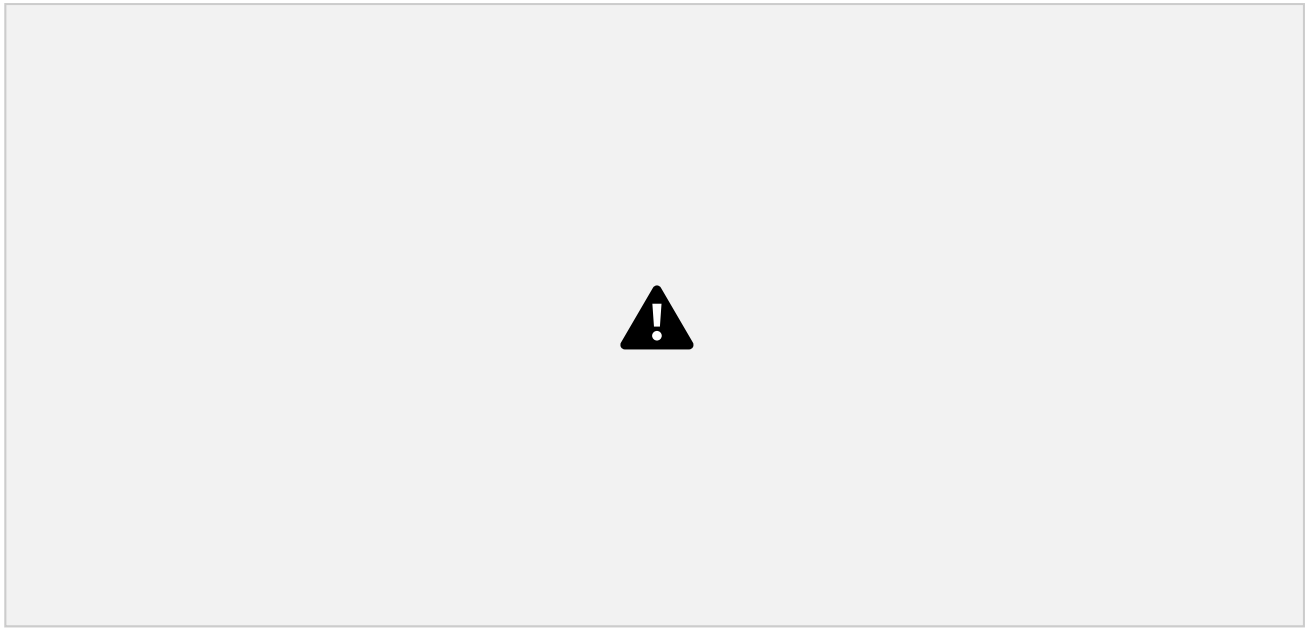
6. Select **vm-core-shs-aps1-prd-sgp-rh8-appexe-01.fwdasia.intranet** and click Save.



7. Click **AZure-Subnet 10.50.4.16/28**. click Instances and click Associate

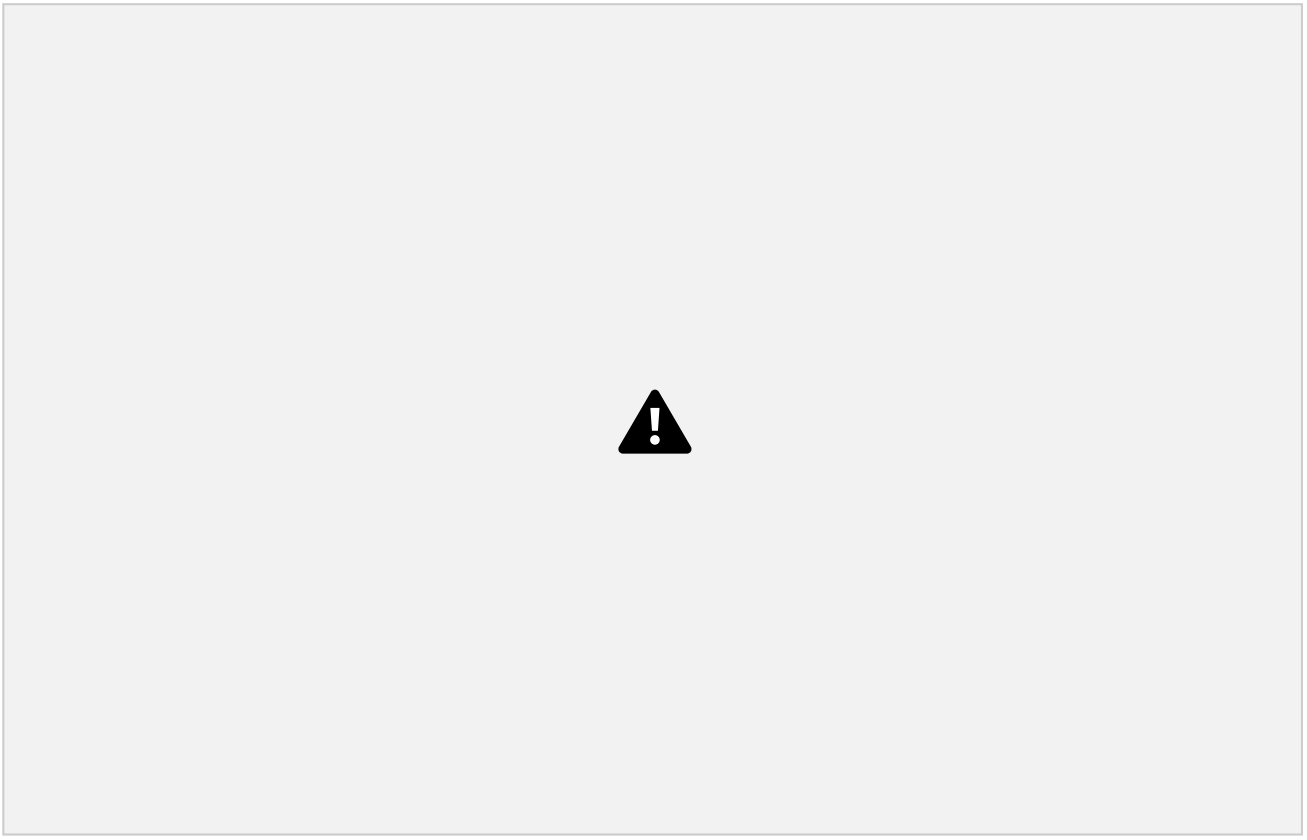


8. Select **lgeasiacppp03.fwdasia.intranet** and click Save



5.3.2.6 Create project for security hardening and OS patch

1. Click Projects from the left navigation bar. And click the Add button.

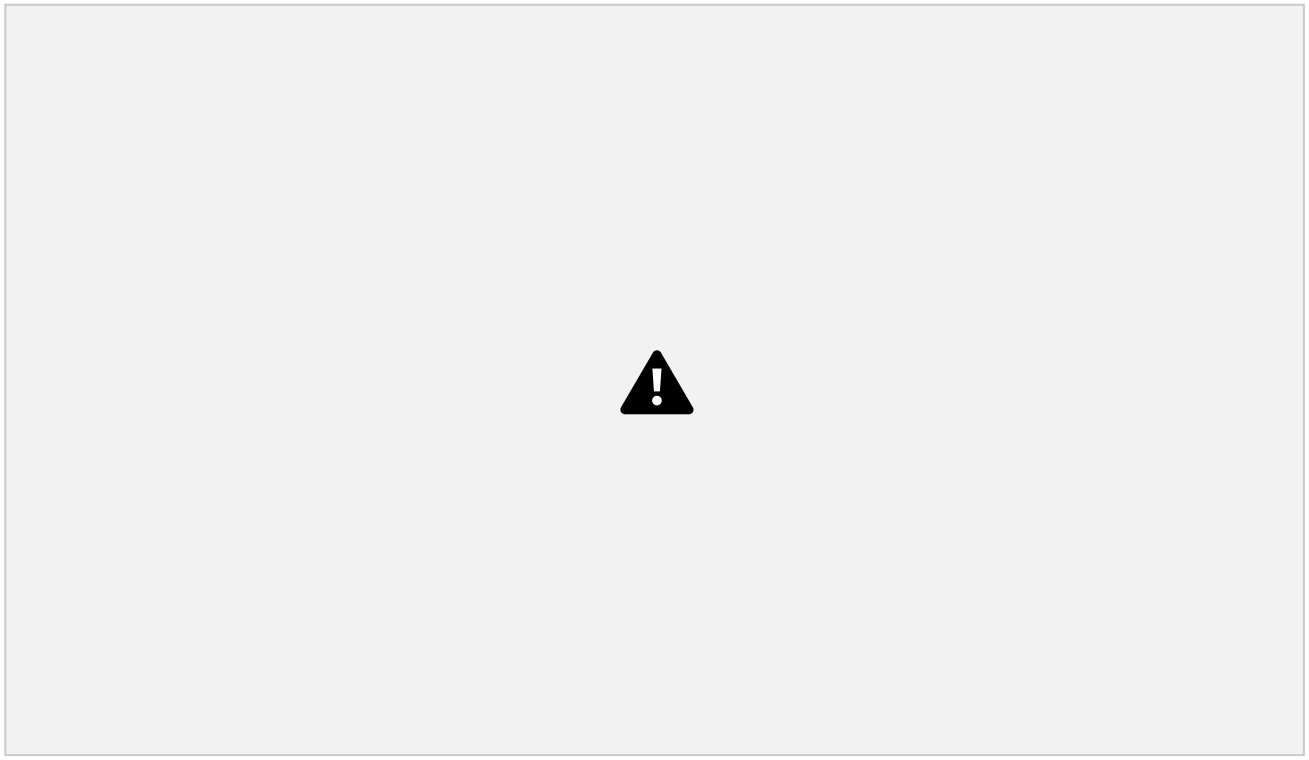


2. Fill in the following fields in the Create New Project window. Click Save.

Name	ansible-security-hardening
Organization	FWD Group
Source Control Type	Git
Source Control URL	git@ssh.dev.azure.com:v3/FWDGODevOps/GT_ Aut omation/ansible-security-hardening
Source Control Credential	Git SCM Login

Name	ansible-os-patch
Organization	FWD Group
Source Control Type	Git
Source Control URL	git@ssh.dev.azure.com:v3/FWDGODevOps/GT_ Aut omation/ansible-os-patch
Source Control Credential	Git SCM Login

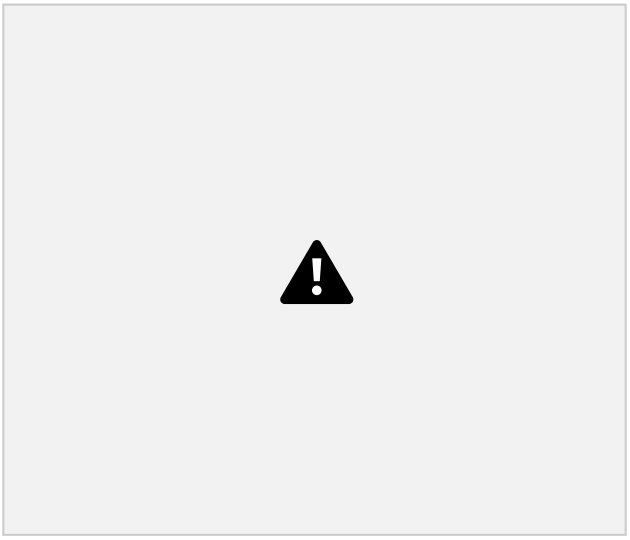
3. Click the Sync Project icon.



5.3.2.7 Configure SAML Authentication with OKTA

1. Click Settings from the left navigation bar and click Miscellaneous System settings

2. Click Edit. Change the Base URL of the service to
https://aap-control01.fwd.com



3. Click Save

4. Click Settings from the left navigation bar and click SAML settings.

5. Click Edit.

6. Fill in the following fields in the Edit Details. And Click Save.

SAML Service Provider Entity ID	`https://aap-control01.fwd.com`
SAML Service Provider Public Certificate	`{{ aap-control01 - Public Certificate }}` **- Cannot use Chain-Certificate**

SAML Service Provider Private Key	{{ aap-control01 - Private Key }}
SAML Service Provider Organization Info	{ "en-US": { "url": "https://aap control01.fwd.com", "displayname": "Ansible Automation Platform Controller", "name": "aap_control01" } }
SAML Service Provider Technical Contact	{ "emailAddress": "fwdadmin@fwd.com", "givenName": "FWD admin" }
SAML Service Provider Support Contact	{ "emailAddress": "fwdadmin@fwd.com", "givenName": "FWD admin" }
SAML Enabled Identity Providers	{ "okta": { "attr_user_permanent_id": "userName", "url": "https://uat esso.fwd.com/app/fwdsso staging_aapcontroller_1/exk7r15uqmN2N 6Io p4x7/sso/saml", "entity_id": "http://www.okta.com/exk7r15uqmN2N6Io p4x 7", "attr_username": "userName", "attr_first_name": "firstName", "attr_last_name": "lastName", "x509cert": "<Okta x509cert>", "attr_email": "email" } }
SAML Organization Map	null
SAML Organization Attribute Mapping	{}

SAML Team Map	null

SAML Team Attribute Mapping	<pre>{
	"team_org_map": [
	{
	"team_alias": "Admin",
	"organization": "FWD Group",
	"team": "ANSIBLE_GRP_ADM"
	},
	{
	"team_alias": "Operator",
	"organization": "FWD Group",
	"team": "ANSIBLE_GRP_OPR"
	},
	{
	"team_alias": "Admin",
	"organization": "FWD HKG",
	"team": "ANSIBLE_HKG_ADM"
	},
	{
	"team_alias": "Operator",
	"organization": "FWD HKG",
	"team": "ANSIBLE_HKG_OPR"
	}
	],
	"saml_attr": "AnsibleGroup",
	"remove": true
	}</pre>

SAML User Flags Attribute Mapping	<pre>{
	"is_superuser_attr":
	"AnsibleGroup",
	"is_superuser_value":
	"ANSIBLE_ALL_ADM"
	}</pre>

SAML Security Config	<pre>{
	"requestedAuthnContext":
	false }</pre>

SAML Service Provider extra configuration data	<pre>null</pre>
SAML IDP to extra_data attribute mapping	<pre>null</pre>

I. Appendix

Procedure for Generating and Applying the AAP Controller Certificate

(The following procedures should be run on AAP controller node only)

Backup the original AAP controller certificate and key:

```
# mkdir -p ~/tower_cert/original_cert_backup
#cp /etc/tower/tower.cert
~/tower_cert/original_cert_backup/. # cp
/etc/tower/tower.key ~/tower_cert/original_cert_backup/.
```

Create CA request for new certificate:

```
# mkdir -p ~/tower_cert/new_cert
# cd ~/tower_cert/new_cert
# vi tower.cnf
 [req]
distinguished_name = req_distinguished_name
req_extensions = req_ext
prompt = no

 [req_distinguished_name]
C = HK
ST = HongKong
L = HongKong
O = FWD
OU = FWD
CN = aap-control01.fwd.com

 [req_ext]
subjectAltName = @alt_names

 [alt_names]
DNS.1 = aap-control01.fwd.com

# openssl req -new -key /etc/tower/tower.key -out tower.csr
-config  tower.cnf
```

<Copy the tower.key and tower.csr to FWD team to generate the new cert>

<After new cert zip file was copied to AAP controller>

```
# mkdir -p ~/tower_cert/test
# cd ~/tower_cert/test
# unzip <new_cert>.zip
# cd ~/tower_cert/new_cert
# cp ~/tower_cert/test/<new_cert_folder>/<new_cert>.crt
tower.cert # cp
~/tower_cert/test/<new_cert_folder>/DigiCertCA.crt .
```

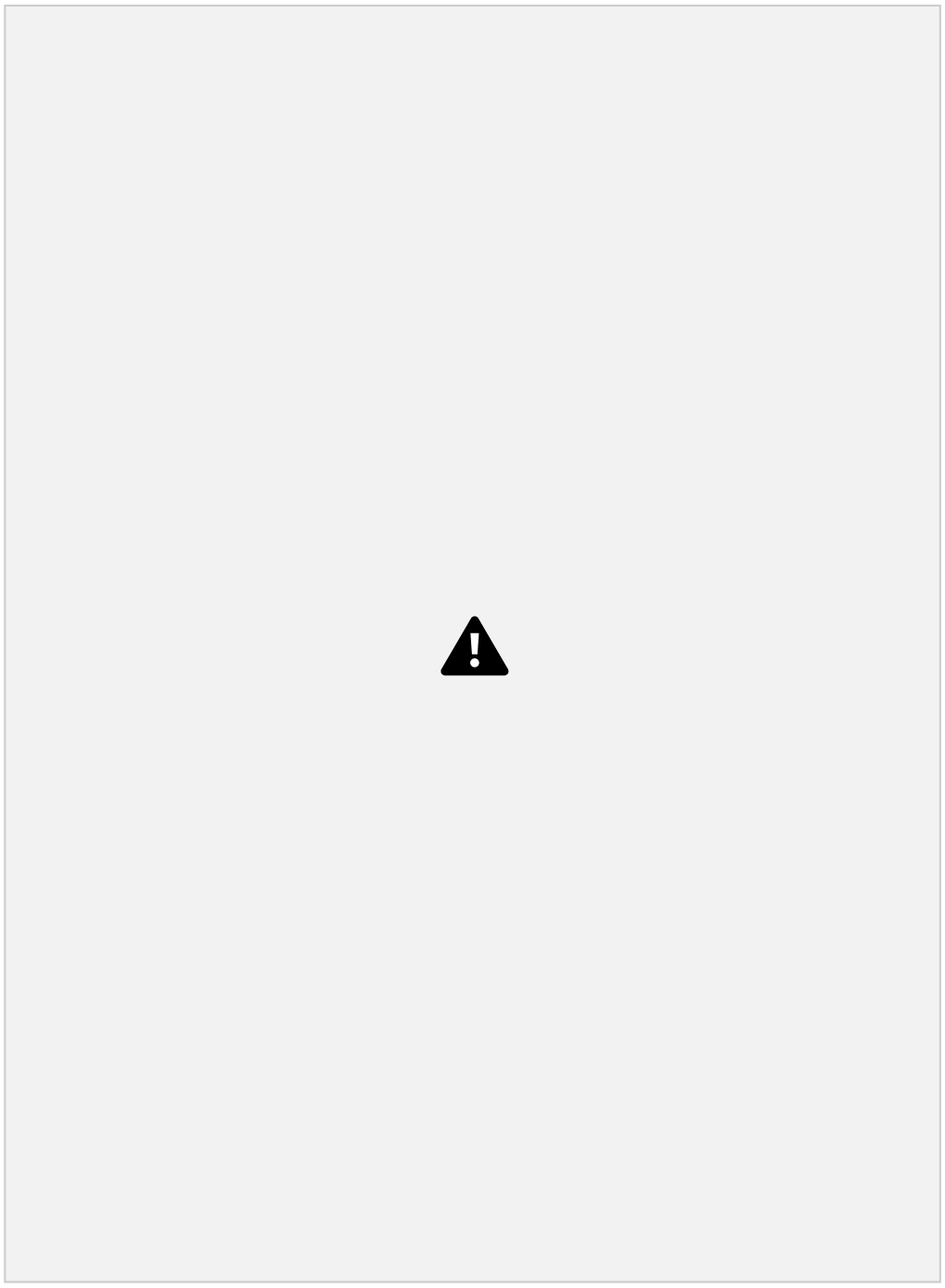
Create the Chain-Certification:

```
# cat DigiCertCA.crt >> tower.cert
# openssl x509 -in tower.cert -text -noout
```

`` check the cert`` ***Replace the New certification on AAP controller:***

```
# automation-controller-service stop
# cp ~/tower_cert/new_cert/tower.cert
/etc/tower/tower.cert # chown root:awx
/etc/tower/tower.cert
# automation-controller-service start
```

Browse to https://10.50.4.5



Procedure for Generating and Applying the Automation Hub Certificate

(The following procedures should be run on AT hub node only)

Backup the original AT Hub certificate and key:

```
# mkdir -p ~/athub_cert/original_cert_backup

#cp /etc/pulp/certs/pulp_webserver.crt
~/athub_cert/original_cert_backup/.

# cp /etc/pulp/certs/pulp_webserver.key
~/athub_cert/original_cert_backup/.
```

Create CA request for new certificate:

```
# mkdir -p ~/athub_cert/new_cert
# cd ~/athub_cert/new_cert
# vi pulp_webserver.cnf
 [req]
distinguished_name = req_distinguished_name
req_extensions = req_ext
prompt = no

 [req_distinguished_name]
C = HK
ST = HongKong
L = HongKong
O = FWD
OU = FWD
CN = lgoeasiacappp01.fwdasia.intranet

 [req_ext]
subjectAltName = @alt_names

 [alt_names]
DNS.1 = aap-hub01.fwdasia.intranet
DNS.2 = lgoeasiacappp01.fwdasia.intranet

# openssl req -new -key /etc/pulp/certs/pulp_webserver.key
-out  pulp_webserver.csr -config pulp_webserver.cnf
```

<Copy the pulp_webserver.key and pulp_webserver.csr to FWD team to generate the new cert>

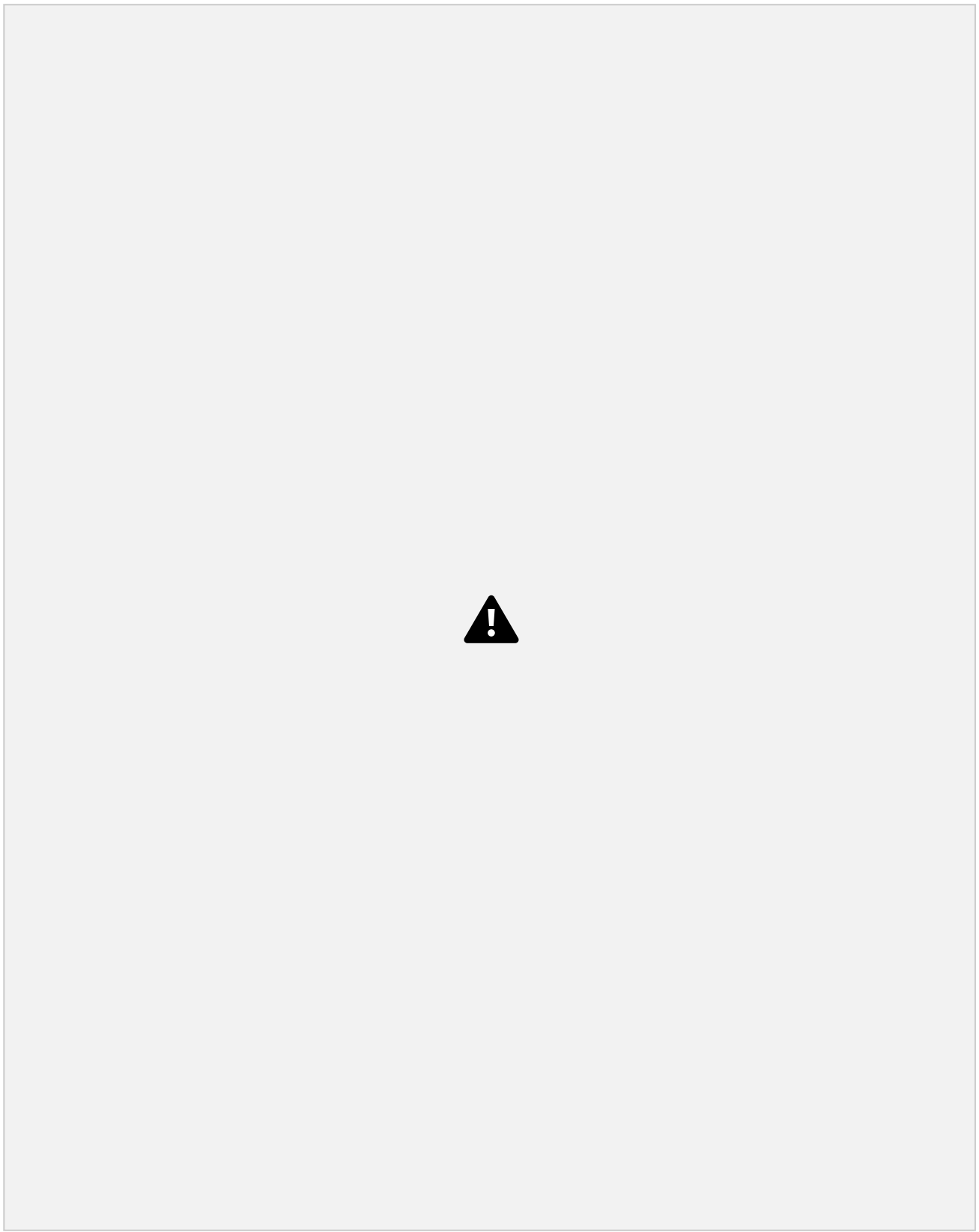
<After new pkcs7 certificate .p7b was copied to AT Hub node> Convert P7B cert to PEM cert:

```
# cp <path>/LGOEASIACAPPP01.p7b ~/athub_cert/new_cert/.
# cd ~/athub_cert/new_cert
# openssl pkcs7 -print_certs -in LGOEASIACAPPP01.p7b
-out  pulp_webserver.crt
# openssl x509 -in pulp_webserver.crt -text -noout
```

`` check the cert ***Replace the New certification on AT hub node:***

```
# systemctl stop pulp* nginx.service redis.service
# cp ~/athub_cert/new_cert/pulp_webserver.crt
/etc/pulp/certs/pulp_webserver.crt

# restorecon -v /etc/pulp/certs/pulp_webserver.crt
# systemctl start pulp* nginx.service redis.service
```


Browse to https://10.50.4.4



Procedure for Adding the Trust of FWD CA

(The following procedures should be run on all AAP controller node, AAP execution nodes, and AT hub node)

```
<Copy the "FWD internal CA.zip" to all AAP controller node,
AAP  execution nodes and AT hub node>

# unzip 'FWD internal CA.zip'

Convert P7B cert to PEM cert:
# openssl pkcs7 -print_certs -in FWD_Intermediate_root.p7b
-out  FWD_CA.cert
# openssl x509 -in FWD_CA.cert -text -noout ?? check the

cert # cp FWD_CA.cert

/usr/share/pki/ca-trust-source/anchors/ # update-ca-trust
```