Red Hat Ansible Automation Platform 2.3

Upgrades Engagement Journey

For Hong Kong Jockey Club

# Preface

## Confidentiality, Copyright, and Disclaimer

This is a Customer-facing document between Red Hat, Inc. and Hong Kong Jockey Club (“HKJC”).

Copyright ©2023 Red Hat, Inc. All Rights Reserved. No part of the work covered by the copyright herein may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems without permission in writing from Red Hat except as is required to share this information as provided with the aforementioned confidential parties.

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.

## 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 | 2023-06-14 | Raymond Lui | Red Hat Consultant | **First Version of the document** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[**Preface**](#_gzdt39j8e6nr) **2**

[Confidentiality, Copyright, and Disclaimer](#_x29dipxs95a0) 2

[Trademarks](#_k406uvkp5ri6) 2

[Audience](#_9pxxylzgrkin) 2

[Additional Background and Related Documents](#_jzcw3szhsm95) 2

[Scripts and playbooks](#_ucfa9zqebjg2) 2

[**Version history**](#_b8aixy9oaoqn) **3**

[**1. Introduction**](#_cgvwxcn0xpcw) **5**

[1.1. Purpose](#_1gj7vt677mmz) 5

[1.2. Staffing](#_fm2bhgdm5gik) 5

[1.3. Terms and acronyms](#_4wwd1cu6ybzy) 6

[**2. UPGRADES PROCEDURE**](#_eyeft0vuoouz) **7**

[2.1 Pre-Upgrades Steps](#_3p7014z5tfor) 7

[2.2. Run backup before upgrades (if no offline VM snapshot taken)](#_wo4sus4xq9ue) 8

[2.3 Run Ansible Tower Upgrades](#_6ope855q93v0) 8

[2.4 Create and Apply New Ansible Tower License Manifest](#_1tsdbl4ft283) 9

# Introduction

## Purpose

The purpose of this document is to provide the engagement Journey of the upgrades of Red Hat Ansible Tower, from version 3.8.4 to Ansible Automation Platform 2.4, for HKJC.

## Staffing

*Customer project team*

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Function | E-mail address | Phone number |
| Alex Wong | Infrastructure administrator | alex.cs.wong@hkjc.org.hk | +852 9722 09193 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Red Hat project team*

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Function | E-mail address | Phone number |
| Raymond Lui | Consultant | yelui@redhat.com | +852 96027743 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 

## Terms and acronyms

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

|  |  |
| --- | --- |
| Acronym | Description |
| HKJC | Hong Kong Jockey Club |
| RH | Red Hat, Inc |
| RHAT | Red Hat Ansible Tower |
| RHEL | Red Hat Enterprise Linux |
| AD | Active Directory |
| 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 VMware terms, synonymous with “Guest” or “ VM Guest” |

# 

# Upgrades Summary

## Upgrade steps summary

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Name | Site | Category | Action | Description |
| 1 | qcstcfgp01 | ST | Ansible Tower | Upgrade from 3.8.4 to 3.8.6 | Prepare Ansible Tower 3.8.6 Backup |
| 2 | qcstcfgp01 | ST | Ansible Tower | Backup Ansible Tower |
| 3 | qchvcfgp01 | HV | RHEL | Fresh Install RHEL 8.8 | Install Ansible Tower in RHEL 8 and restore tower backup from RHEL7 |
| 4 | qchvcfgp01 ~~+ qccfgsatwin02~~ | HV | Ansible Tower | Fresh Install Ansible Tower 3.8.6 |
| 5 | qchvcfgp01 | HV | Ansible Tower | Restore from ST Ansible Tower 3.8.6 Backup |
| 6 | qchvcfgp01 + ~~qccfgsatwin02 +~~  qchvcfgah01 | HV | AAP2 | Upgrade from Ansible Tower 3.8.6 to AAP 2.2 | Prepare AAP 2.4 backup |
| 7 | qchvcfgp01 + qchvcfgah01 | HV | AAP2 | Upgrade from AAP 2.2 to AAP 2.4 |
| 8 | qchvcfgp01 + qchvcfgah01 | HV | AAP2 | Backup AAP 2.4 |
| 9 | qchvcfgp02 | HV | RHEL | Fresh Install RHEL 9.1 | Install AAP in RHEL 9 and restore AAP backup from RHEL8 |
| 10 | qchvcfgp02 + qchvcfgah01 + qccfgsatwin02 | HV | AAP2 | Fresh Install AAP 2.4 |
| 11 | qchvcfgp02 + qchvcfgah01 + qccfgsatwin02 | HV | AAP2 | Restore backup from AAP 2.4 in RHEL 8.8 |

|  |  |  |  |
| --- | --- | --- | --- |
| Hostname | IP Address | Name before Upgrade | Name After Upgrade |
| qcstcfgp01 | 10.72.17.46 | Ansible Tower | Ansible Automation Controller |
| qchvcfgah01 | 10.72.17.119 | - | Ansible Automation Hub |
| qccfgsatwin02 | 192.168.145.17 | Isolated node | Ansible Execution Node |
| qcstcfgp02 | 10.72.17.46 | Ansible Automation Controller | Ansible Automation Controller |

## Upgrade sources

rhel7.9-x86\_64-dvd.iso

rhel8.8-x86\_64-dvd.iso

rhel9.1-x86\_64-dvd.iso

ansible-tower-setup-bundle-3.8.6-2.tar.gz

ansible-automation-platform-setup-bundle-2.2.2-1.tar.gz

ansible-automation-platform-setup-bundle-2.4-1-x86\_64.tar.gz

## Ports Need To Be Opened In The Firewall For Ansible Automation Platform 2 Services

|  |  |  |
| --- | --- | --- |
| From | To | Port |
| Client | controller | 443/tcp |
| Client | controller | 80/tcp |
| Client | controller | 22/tcp |
| controller | execution node | 27199/tcp |
| controller | execution node | 22/tcp |

Ref: https://access.redhat.com/solutions/6756251

# Upgrades Procedure

## Upgrade Ansible Tower in ST from 3.8.4 to 3.8.6 (qcstcfgp01)

### Pre-Upgrades Steps

1. Upload the ***ansible-tower-setup-bundle-3.8.6-2.tar.gz*** to Ansible Tower.
2. Login Ansible Tower, as root user.
3. Set umask to 0022.

|  |
| --- |
| # umask 0022 |

1. Extract the setup bundle to /opt/ansible.

(Please make sure / has enough spaces.)

|  |
| --- |
| # cd /opt/ansible  # tar zxvf <path of setup bundle>/ansible-tower-setup-bundle-3.8.6-2.tar.gz |

1. Backup the original inventory file.

|  |
| --- |
| # cd ansible-tower-setup-bundle-3.8.6-2/  # cp inventory inventory.org |

1. Copy the Ansible Tower 3.8.4 inventory file to 3.8.6 folder.

|  |
| --- |
| # cp ../ansible-tower-setup-bundle-3.8.4-1/inventory . |

1. Edit the inventory file, as follows:

(Also make sure the admin password and PostgreSQL password are set.)

|  |
| --- |
| # vi inventory  …  …  …  …  [all:vars]  ## Upgrades Tower with upgrade Ansible engine  upgrade\_ansible\_with\_tower=true  ….  …. |

1. Check if Ansible Tower’s License is still in compliance/valid.

|  |
| --- |
| Login into Ansible Tower WebUI, as **admin** user  **Settings** -> **License**  See if it is still in valid license and check expires on date. Upload the valid license before running upgrades. |

### Run backup before upgrades (if no offline VM snapshot taken)

1. Change the backup destination folder, to avoid out of space on / volume.

|  |
| --- |
| # cd /opt/ansible/ansible-tower-setup-bundle-3.8.4-1  # vi /opt/ansible/ansible-tower-setup-bundle-3.8.4-1/roles/backup/defaults/main.yml  ---  backup\_dir: /var/backups/tower/  #backup\_dest: "{{ playbook\_dir }}/"  backup\_dest: /var/backups/ |

1. Run Ansible Tower backup.

|  |
| --- |
| # /opt/ansible/ansible-tower-setup-bundle-3.8.4-1/setup.sh -b |

### Run Ansible Tower Upgrades

1. Run Ansible Tower upgrades.

|  |
| --- |
| # /opt/ansible/ansible-tower-setup-bundle-3.8.6-1/setup.sh |

1. After Ansible Tower upgrades successfully, please restart the services once.

|  |
| --- |
| # ansible-tower-service restart |

1. Check Ansible tower services.

|  |
| --- |
| # ansible-tower-service status |

1. Go to Ansible Tower API ping page to see the status:

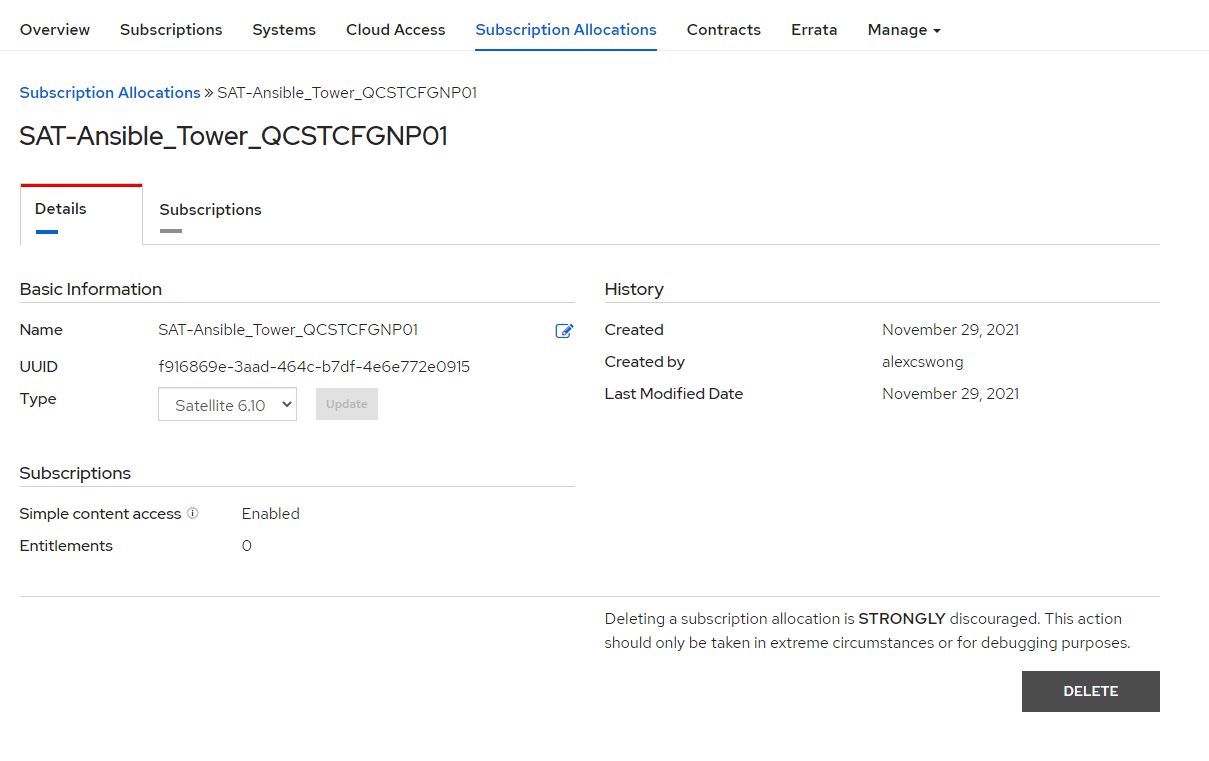
|  |
| --- |
| Go to Ansible Tower API ping page:  https://<ip address>/api/v2/ping  Tower and Isolated node should be shown in the page. |

### Create and Apply New Ansible Tower License Manifest

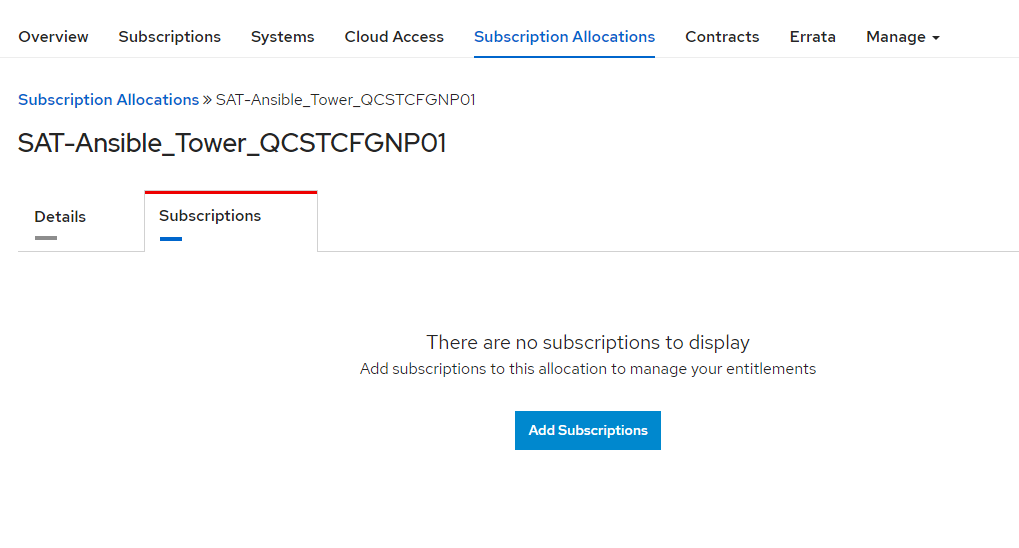
1. Open the browser, and go to <http://access.redhat.com>.
2. Login with “Manage Subscription” permission user.
3. Click to **Subscriptions** on Top right corner:

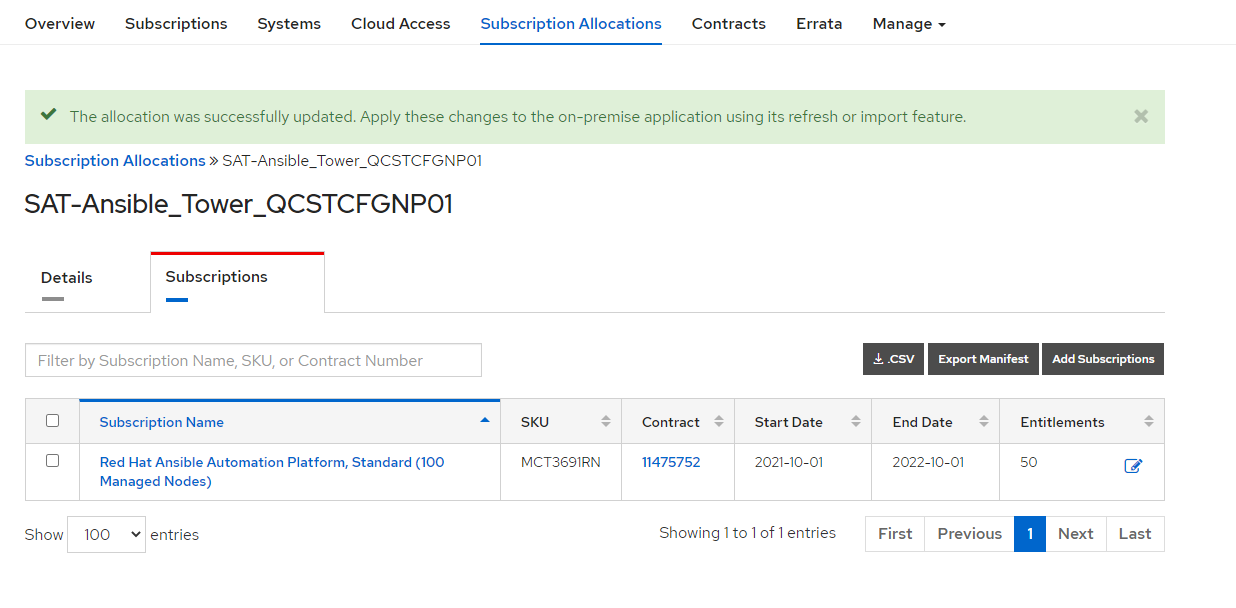


1. Click on the **Subscription Allocations** tab, then create the new allocation (choose the type as Satellite 6.10)



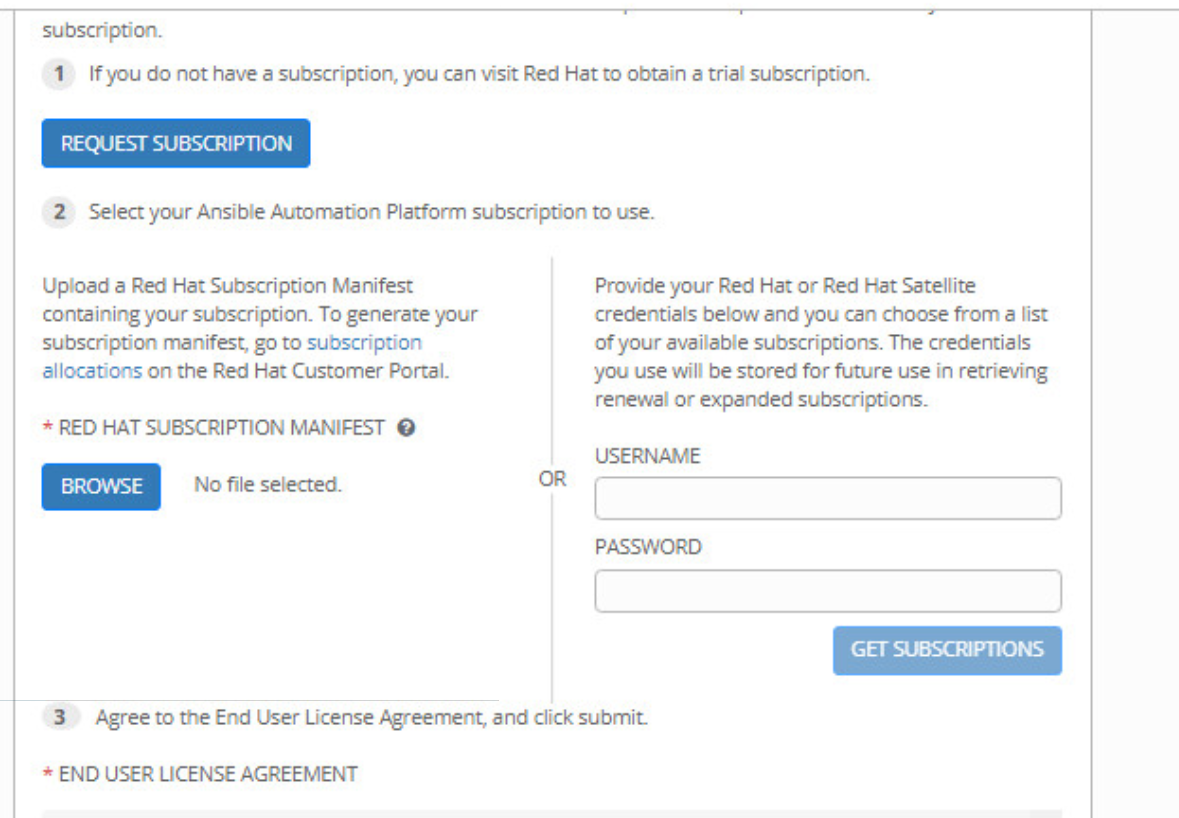
1. Add the **Ansible Automation Platform (Manged Nodes) Subscription**, and allocate the quantity.

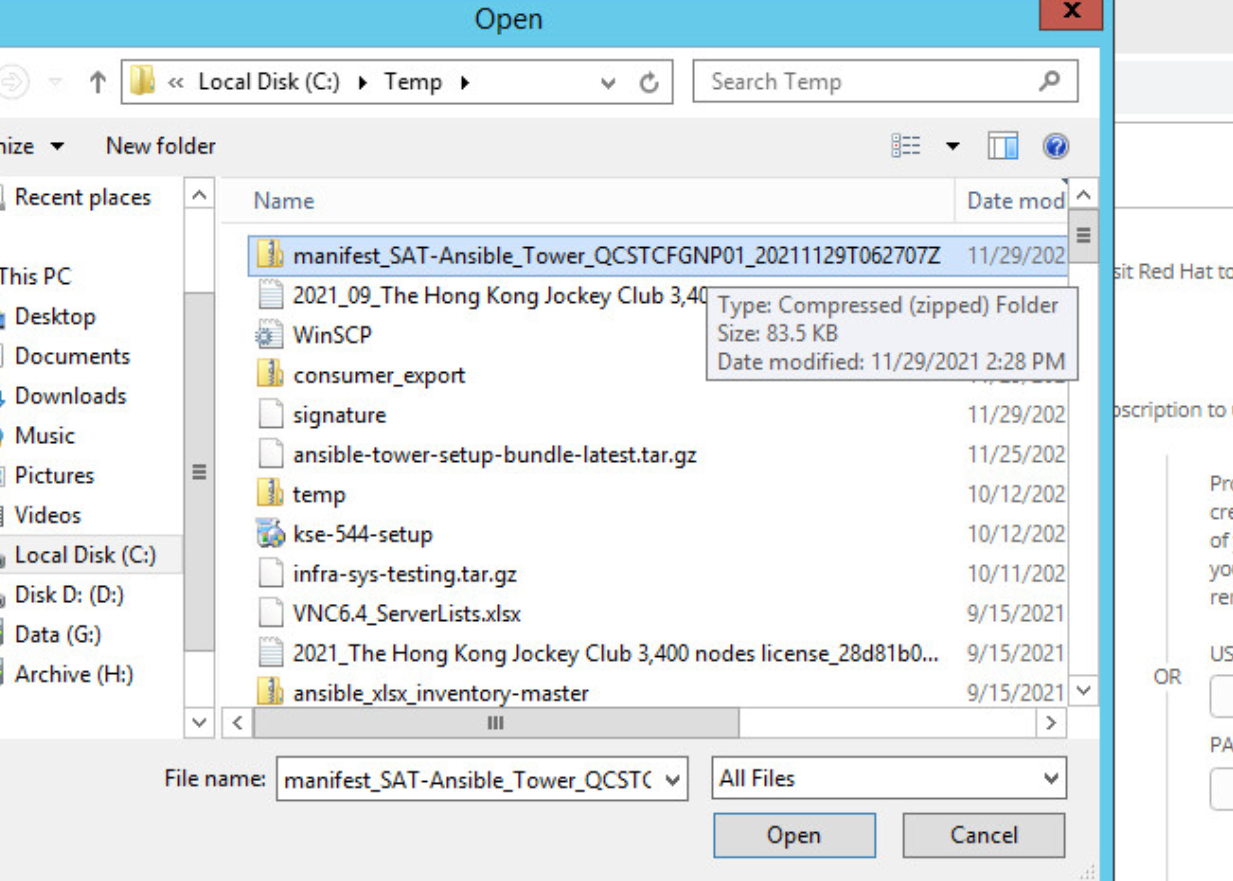




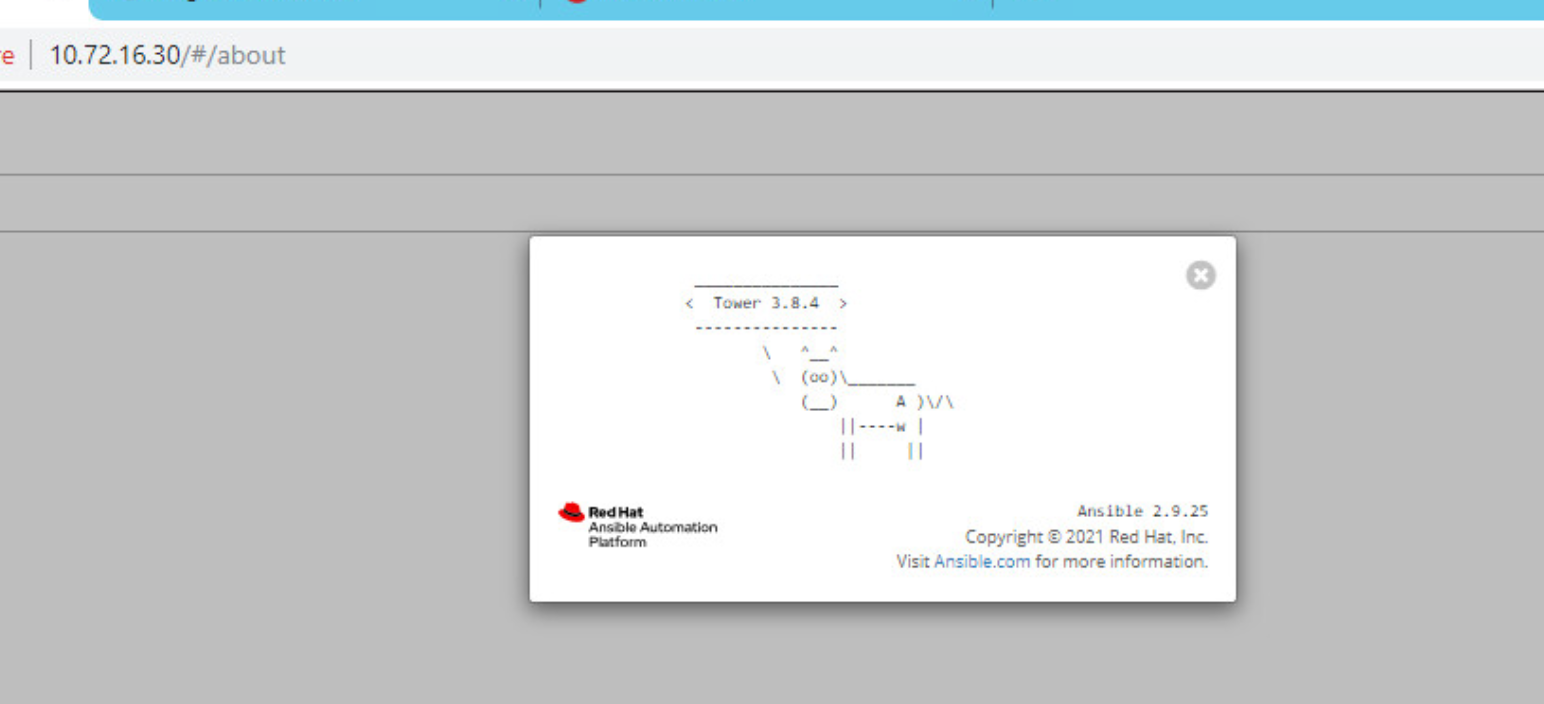
Click **Export Manifest** to download the manifest zip file to the local PC.

1. Login to Ansible Tower WebUI, and upload the Manifest zip file.





1. Tick to agree to the agreement, and then OK to apply the License Manifest.
2. Ansible Tower Dashboard should be now shown.
3. Click on the **i** button on the Top right to check the Ansible Tower and Ansible Version.



## Backup Ansible Tower 3.8.6 in ST (qcstcfgp01)

### Run backup for Ansible Tower

1. Change the backup destination folder, to avoid out of space on / volume.

|  |
| --- |
| # cd /opt/ansible/ansible-tower-setup-bundle-3.8.6-2  # vi /opt/ansible/ansible-tower-setup-bundle-3.8.6-2/roles/backup/defaults/main.yml  ---  backup\_dir: /var/backups/tower/  #backup\_dest: "{{ playbook\_dir }}/"  backup\_dest: /var/backups/ |

1. Run Ansible Tower backup.

|  |
| --- |
| # /opt/ansible/ansible-tower-setup-bundle-3.8.6-2/setup.sh -b |

1. Verify backup file and this file will be used for restore Ansible Tower in HV.

|  |
| --- |
| # cd /var/backups  # ls  tower-backup-latest.tar.gz |

## Fresh Install RHEL 8.8 (qchvcfgp01)

1. Ref doc: [RHEL 8 Bare Metal Quick Install | Red Hat Developer](https://developers.redhat.com/rhel8/install-rhel8#overview)
2. Software selection: Minimal Install
3. Disks/partition:
   1. Storage Configuration: Custom
   2. Manual Partitioning

|  |  |
| --- | --- |
| Mount Point | Desired Capacity |
| / | 40 GiB |
| /boot | 1024 MiB |
| /boot/efi | 600 Mib |
| /var | 40 GiB |
| /tmp | 14 GiB |
| /home | 20 GiB |
| /var/log | 20 GiB |
| /var/log/audit | 10 GiB |

1. Begin Installation
2. Create admin user and set the root password
   1. Username: redhat
3. Convert to RHEL 8.8 Template in vCenter

## Fresh Install Ansible Tower 3.8.6 (qchvcfgp01)

### Installation Steps

1. Use the RHEL 8.8 Template from vCenter
2. Extract the setup bundle to /opt/ansible.

(Please make sure / has enough spaces.)

|  |
| --- |
| # cd /opt/ansible  # tar zxvf <path of setup bundle>/ansible-tower-setup-bundle-3.8.6-2.tar.gz |

1. Copy the ST Ansible Tower 3.8.6 inventory file to HV Ansible Tower 3.8.6. And copy to setup bundler directory to replace the default inventory file.

|  |
| --- |
| # cp <inventory from ST Ansible Tower> /opt/ansible/ansible-tower-setup-bundle-3.8.6-2/inventory |

1. Update hostname

|  |
| --- |
| # hostnamectl set-hostname <hostname.fqdn> |

1. Assign sudo right to user “redhat”

Add the entry line as below.

|  |
| --- |
| # visudo  .  .  .  # wheel ALL=(ALL) NOPASSWD: ALL  redhat ALL=(ALL) NOPASSWD: ALL  .  .  . |

1. Change the setup bundler owner to redhat user

|  |
| --- |
| # chown -R redhat: /opt/ansible/ansible-tower-setup-bundle-3.8.6-2 |

1. Change to user “Redhat”

|  |
| --- |
| # su - redhat |

1. Generate ssh-key

|  |
| --- |
| $ ssh-keygen |

1. Copy ssh key to own machine (qchvcfgp01)

|  |
| --- |
| $ ssh-copy-id [redhat@10.72.17.46](mailto:redhat@10.72.17.46) |

1. Prepare repository

|  |
| --- |
| vi /etc/yum.repos.d/rhel88.repo |
| [dvd-BaseOS]  name=DVD for RHEL - BaseOS  baseurl=file:///media/rheldvd/BaseOS  enabled=1  gpgcheck=0  [dvd-AppStream]  name=DVD for RHEL - AppStream  baseurl=file:///media/rheldvd/AppStream  enabled=1  gpgcheck=0 |

1. Attached RHEL8.8 ISO in vCenter. And mount rhel 8.8 dvd iso

|  |
| --- |
| mkdir /media/rheldvd  mount /dev/sr0 /media/rheldvd |

1. Run Ansible Tower Installation.

|  |
| --- |
| $ ANSIBLE\_SUDO=True /opt/ansible/ansible-tower-setup-bundle-3.8.6-2/setup.sh |

1. Check Ansible tower services.

|  |
| --- |
| # ansible-tower-service status |

1. Go to Ansible Tower API ping page to see the status:

|  |
| --- |
| Go to Ansible Tower API ping page:  https://<ip address>/api/v2/ping  Tower and Isolated node should be shown in the page. |

## Restore from ST Ansible Tower 3.8.6 Backup (qchvcfgp01)

### Restore Steps

1. Copy the ST Ansible Tower backup file to HV Ansible Tower
2. Change to user “redhat”

|  |
| --- |
| # su - redhat |

1. Restore the backup

(Please make sure / has enough spaces.)

|  |
| --- |
| $ cd /opt/ansible/ansible-tower-setup-bundle-3.8.6-2  $ ANSIBLE\_SUDO=True /opt/ansible/ansible-tower-setup-bundle-3.8.6-2/setup.sh -e ‘<path of backup>/tower-backup-latest.tar’ -r |

1. Check Ansible tower services.

|  |
| --- |
| # ansible-tower-service status |

1. Go to Ansible Tower API ping page to see the status:

|  |
| --- |
| Go to Ansible Tower API ping page:  https://<ip address>/api/v2/ping  Tower and Isolated node should be shown in the page. |

## Upgrade from Ansible Tower 3.8.6 to AAP 2.2 (qchvcfgp01 + qchvcfgah01 )

### In Automation Hub (qchvcfgah01)

1. Use the RHEL 8.8 Template from vCenter
2. Update hostname

|  |
| --- |
| # hostnamectl set-hostname <hostname.fqdn> |

1. Assign sudo right to user “redhat”

Add the entry line as below.

|  |
| --- |
| # visudo  .  .  .  # wheel ALL=(ALL) NOPASSWD: ALL  redhat ALL=(ALL) NOPASSWD: ALL  .  .  . |

1. Prepare repository

|  |
| --- |
| vi /etc/yum.repos.d/rhel88.repo |
| [dvd-BaseOS]  name=DVD for RHEL - BaseOS  baseurl=file:///media/rheldvd/BaseOS  enabled=1  gpgcheck=0  [dvd-AppStream]  name=DVD for RHEL - AppStream  baseurl=file:///media/rheldvd/AppStream  enabled=1  gpgcheck=0 |

1. Attached RHEL8.8 ISO in vCenter. And mount rhel 8.8 dvd iso

|  |
| --- |
| mkdir /media/rheldvd  mount /dev/sr0 /media/rheldvd |

### In Ansible Automation Controller (qchvcfgp01)

1. Change to user “redhat”

|  |
| --- |
| # su - redhat |

1. Copy ssh key to Automation Hub (qchvcfgah01)

|  |
| --- |
| $ ssh-copy-id redhat@10.72.17.119 |

1. Extract the setup bundle to /opt/ansible.

(Please make sure / has enough spaces.)

|  |
| --- |
| # cd /opt/ansible  # tar zxvf <path of setup bundle>/ansible-automation-platform-setup-bundle-2.2.2-1.tar.gz |

1. Backup the original inventory file.

|  |
| --- |
| # cd ansible-automation-platform-setup-bundle-2.2.2-1/  # cp inventory inventory.ori |

1. Copy the Ansible Tower 3.8.6 inventory file to 2.2.2 folder.

|  |
| --- |
| # cp ../ansible-tower-setup-bundle-3.8.6-2/inventory . |

1. Update the inventory as follow:

|  |
| --- |
| # vi inventory |
| # 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]  10.72.17.46  [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  [automationhub]  10.72.17.119  [automationcatalog]  [database]  # Single Sign-On  # If sso\_redirect\_host is set, that will be used for application to connect to  # SSO for authentication. This must be reachable from client machines.  #  # ssohost.example sso\_redirect\_host=<host/ip>  [sso]  [all:vars]  admin\_password='xxxxxx'  pg\_host=''  pg\_port=5432  pg\_database='awx'  pg\_username='awx'  pg\_password='xxxxxx'  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  #  # When deployed with Automation Hub:  # - The installer will push execution environment images to Automation Hub and  # configure Automation Controller to pull images from the Hub regisitry.  # - To make Hub to be the only registry to pull execution environment images from,  # set 'ee\_from\_hub\_only' to True. This is set to True by default when bundle  # installer is used.  registry\_url='registry.redhat.io'  registry\_username=''  registry\_password=''  # ee\_from\_hub\_only =  # Receptor Configuration  #  receptor\_listener\_port=27199  # Automation Hub Configuration  #  automationhub\_admin\_password='xxxxxx'  automationhub\_pg\_host='10.72.17.46'  automationhub\_pg\_port=5432  automationhub\_pg\_database='automationhub'  automationhub\_pg\_username='automationhub'  automationhub\_pg\_password='xxxxxx'  automationhub\_pg\_sslmode='prefer'  # Set to True to overwrite existing admin password.  #  # automationhub\_force\_change\_admin\_password = False  # The main automation hub URL that clients will connect to (e.g. https://<load balancer host>).  # If not specified, the first node in the [automationhub] group will be used when needed.  #  # automationhub\_main\_url = ''  # By default when one uploads collections to Automation Hub  # an admin needs to approve it before it is made available  # to the users. If one wants to disable the content approval  # flow, the following setting should be set to False.  #  # automationhub\_require\_content\_approval = True  # At import time collections can go through a series of checks.  # Behaviour is driven by galaxy-importer.cfg configuration.  # Example are ansible-doc, ansible-lint, flake8, ...  #  # The following parameter allow one to drive this configuration.  # This variable is expected to be a dictionary.  #  # automationhub\_importer\_settings = None  # The default install will deploy a TLS enabled Automation Hub.  # If for some reason this is not the behavior wanted one can  # disable TLS enabled deployment.  #  # automationhub\_disable\_https = False  # The default install will deploy a TLS enabled Automation Hub.  # Unless specified otherwise the HSTS web-security policy mechanism  # will be enabled. This setting allows one to disable it if need be.  #  # automationhub\_disable\_hsts = False  # The default install will not create a signing service by default. If set to true  # a signing service will be created.  # automationhub\_create\_default\_collection\_signing\_service = False  # If a collection signing service is enabled, one must provide the following two variables  # to ensure collections can be properly signed. Note: those MUST be absolute paths  # automationhub\_collection\_signing\_service\_key = /absolute/path/to/key/to/sign  # automationhub\_collection\_signing\_service\_script = /absolute/path/to/script/that/signs  # If a collectiion signing service is enabled, collections won't be signed automatically by default  # the following parameter will have them signed by default  #  # automationhub\_auto\_sign\_collections = False  # If upgrading from Ansible Automation Platform 2.0 or earlier, you must either:  # - provide an existing Automation Hub token as 'automationhub\_api\_token' or  # - set 'generate\_automationhub\_token' to True to generate a new token  # Generating a new token will invalidate the existing token.  #  # automationhub\_api\_token=''  # generate\_automationhub\_token=  # Automation Hub LDAP configuration  #  # For Automation Hub to connect to LDAP directly the following variables  # need to be configured. The list of all possible configuration can be found here:  # https://django-auth-ldap.readthedocs.io/en/latest/reference.html#settings  # Extra parameter will need to be passed through an ansible ldap\_extra\_settings dictionnary.  #  # automationhub\_authentication\_backend = "ldap"  #  # automationhub\_ldap\_server\_uri = "ldap://ldap:10389"  # automationhub\_ldap\_bind\_dn = "cn=admin,dc=ansible,dc=com"  # automationhub\_ldap\_bind\_password = "GoodNewsEveryone"  # automationhub\_ldap\_user\_search\_base\_dn = "ou=people,dc=ansible,dc=com"  # automationhub\_ldap\_group\_search\_base\_dn = "ou=people,dc=ansible,dc=com"  # Automation Services Catalog Configuration  #  automationcatalog\_pg\_host=''  automationcatalog\_pg\_port=5432  automationcatalog\_pg\_database='automationservicescatalog'  automationcatalog\_pg\_username='automationservicescatalog'  automationcatalog\_pg\_password=''  # For an alternative front end url needed for SSO configuration with Automation  # Services Catalog, provide the URL.  # automationcatalog\_main\_url=''  # Automation Services Catalog requires either Controller to be installed  # with Automation Controller or a URL to an active and routable Controller  # server must be provided with the below variable.  # automation\_controller\_main\_url=''  # Automation Services Catalog requires SSO and SSO admin credentials for  # authentication. SSO admin credentials are also required for set Catalog specific  # roles needed for the application. If SSO is not provided in inventory for  # configuration, then the SSO host needs to be defined with the below.  # sso\_host=''  # Automation Services Catalog will generate a token, but a specific OAuth token  # can be provided with the following. Note that the variable  # "automation\_controller\_main\_url" must be assigned a routable address from  # the Automation Service Catalog host.  # automationcatalog\_controller\_token=''  # Automation Controller credentials can also be provided to generate a token  # for a working Controller environment. Note that the variable  # "automation\_controller\_main\_url" must be assigned a routable address from  # the Automation Service Catalog host. Generating a token will also create  # an application in Automation Controller for stateful management of the token.  # automationcatalog\_controller\_username=''  # automationcatalog\_controller\_password=''  # The default install will enable analytics collection for Services Catalog.  # Set to False to disable.  # automationcatalog\_enable\_analytics\_collection = True  # The default install will use RHSM certificate to send Services Catalog analytics  # collection data. To use username and password instead, provide the  # console.redhat.com credentials.  # insights\_username=''  # insights\_password=''  # If connection to Automation Controller requires SSL validation to be off,  # provide the variable below. By default, the value is true.  #  # automationcatalog\_controller\_verify\_ssl=False  # The default install will deploy a TLS enabled Automation Hub.  # If for some reason this is not the behavior wanted one can  # disable TLS enabled deployment.  #  # automationcatalog\_disable\_https = False  # The default install will deploy a TLS enabled Automation Hub.  # Unless specified otherwise the HSTS web-security policy mechanism  # will be enabled. This setting allows one to disable it if need be.  #  # automationcatalog\_disable\_hsts = False  # SSL-related variables  # If set, this will install a custom CA certificate to the system trust store.  # custom\_ca\_cert=/path/to/ca.crt  # Certificate and key to install in nginx for the web UI and API  # web\_server\_ssl\_cert=/path/to/tower.cert  # web\_server\_ssl\_key=/path/to/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  # Keystore file to install in SSO node  # sso\_custom\_keystore\_file='/path/to/sso.jks'  # The default install will deploy SSO with sso\_use\_https=True  # Keystore password is required for https enabled SSO  sso\_keystore\_password=''  # Single-Sign-On configuration  sso\_console\_admin\_password=''  # 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 = True  [aap\_valid\_hosts]  10.72.17.46 |

1. Ensure the owner of the setup bundler is redhat user

|  |
| --- |
| # sudo chown -R redhat: /opt/ansible/ansible-automation-platform-setup-bundle-2.2.2-1 |

1. Run Ansible Tower Installation.

|  |
| --- |
| $ ANSIBLE\_SUDO=True /opt/ansible/ansible-automation-platform-setup-bundle-2.2.2-1/setup.sh |

## Upgrade from AAP 2.2 to AAP 2.4 (qchvcfgp01 + qchvcfgah01 )

### In Ansible Automation Controller (qchvcfgp1)

1. Change to user “redhat”

|  |
| --- |
| # su - redhat |

1. Extract the setup bundle to /opt/ansible.

(Please make sure / has enough spaces.)

|  |
| --- |
| # cd /opt/ansible  # tar zxvf <path of setup bundle>/ansible-automation-platform-setup-bundle-2.4-1-x86\_64.tar.gz |

1. Backup the original inventory file.

|  |
| --- |
| # cd ansible-automation-platform-setup-bundle-2.4-1-x86\_64/  # cp inventory inventory.ori |

1. Copy the AAP 2.2 inventory file to AAP 2.4 folder.

|  |
| --- |
| # cp ../ansible-automation-platform-setup-bundle-2.2.2-1/inventory . |

1. Ensure the owner of the setup bundler is redhat user

|  |
| --- |
| # sudo chown -R redhat: /opt/ansible/ansible-automation-platform-setup-bundle-2.4-1-x86\_64 |

1. Run Ansible Tower Installation.

|  |
| --- |
| $ ANSIBLE\_SUDO=True /opt/ansible/ansible-automation-platform-setup-bundle-2.4-1-x86\_64/setup.sh |

Using Kerberos for Windows in Ansible Automation Platform 2

**Edit /etc/krb5.conf.d/WIN.BETTING.HKJC.ORG.HK.conf in execution node (eg: QCCFGSATWIN02)**

# cat /etc/krb5.conf.d/WIN.BETTING.HKJC.ORG.HK.conf

[libdefaults]

rdns = false

default\_realm = DEMOLAB.LOCAL

[realms]

DEMOLAB.LOCAL = {

kdc = ms-ad.demolab.local

admin\_server = ms-ad.demolab.local

}

Configuring automation controller

configure **Settings -> Job Settings**and edit the “path to expose to isolated jobs”, adding the Kerberos directory

Paths to expose to isolated jobs

"/etc/krb5.conf.d:/etc/krb5.conf.d:O"

"/etc/pki/ca-trust:/etc/pki/ca-trust:O",

"/usr/share/pki:/usr/share/pki:O"

Reinstall execution nodes with different hostname:

https://access.redhat.com/solutions/6616271

|  |
| --- |
| [root@QCCFGSATWIN02 redhat]# cat inventory  # 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]  10.72.17.46  [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]  [execution\_nodes:children]  instance\_group\_sat\_win  [execution\_nodes:vars]  node\_state='iso\_migrate'  node\_type=execution  [instance\_group\_sat\_win]  192.168.145.17  [instance\_group\_sat\_win:vars]  node\_state='iso\_migrate'  [automationhub]  10.72.17.119  [automationcatalog]  [database]  # Single Sign-On  # If sso\_redirect\_host is set, that will be used for application to connect to  # SSO for authentication. This must be reachable from client machines.  #  # ssohost.example sso\_redirect\_host=<host/ip>  [sso]  [all:vars]  admin\_password='redh@t123'  pg\_host=''  pg\_port=5432  pg\_database='awx'  pg\_username='awx'  pg\_password='redh@t123'  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  #  # When deployed with Automation Hub:  # - The installer will push execution environment images to Automation Hub and  # configure Automation Controller to pull images from the Hub regisitry.  # - To make Hub to be the only registry to pull execution environment images from,  # set 'ee\_from\_hub\_only' to True. This is set to True by default when bundle  # installer is used.  registry\_url='registry.redhat.io'  registry\_username=''  registry\_password=''  # ee\_from\_hub\_only =  # Receptor Configuration  #  receptor\_listener\_port=27199  # Automation Hub Configuration  #  automationhub\_admin\_password='redh@t123'  automationhub\_pg\_host='10.72.17.46'  automationhub\_pg\_port=5432  automationhub\_pg\_database='automationhub'  automationhub\_pg\_username='automationhub'  automationhub\_pg\_password='redh@t123'  automationhub\_pg\_sslmode='prefer'  # Set to True to overwrite existing admin password.  #  # automationhub\_force\_change\_admin\_password = False  # The main automation hub URL that clients will connect to (e.g. https://<load balancer host>).  # If not specified, the first node in the [automationhub] group will be used when needed.  #  # automationhub\_main\_url = ''  # By default when one uploads collections to Automation Hub  # an admin needs to approve it before it is made available  # to the users. If one wants to disable the content approval  # flow, the following setting should be set to False.  #  # automationhub\_require\_content\_approval = True  # At import time collections can go through a series of checks.  # Behaviour is driven by galaxy-importer.cfg configuration.  # Example are ansible-doc, ansible-lint, flake8, ...  #  # The following parameter allow one to drive this configuration.  # This variable is expected to be a dictionary.  #  # automationhub\_importer\_settings = None  # The default install will deploy a TLS enabled Automation Hub.  # If for some reason this is not the behavior wanted one can  # disable TLS enabled deployment.  #  # automationhub\_disable\_https = False  # The default install will deploy a TLS enabled Automation Hub.  # Unless specified otherwise the HSTS web-security policy mechanism  # will be enabled. This setting allows one to disable it if need be.  #  # automationhub\_disable\_hsts = False  # The default install will not create a signing service by default. If set to true  # a signing service will be created.  # automationhub\_create\_default\_collection\_signing\_service = False  # If a collection signing service is enabled, one must provide the following two variables  # to ensure collections can be properly signed. Note: those MUST be absolute paths  # automationhub\_collection\_signing\_service\_key = /absolute/path/to/key/to/sign  # automationhub\_collection\_signing\_service\_script = /absolute/path/to/script/that/signs  # If a collectiion signing service is enabled, collections won't be signed automatically by default  # the following parameter will have them signed by default  #  # automationhub\_auto\_sign\_collections = False  # If upgrading from Ansible Automation Platform 2.0 or earlier, you must either:  # - provide an existing Automation Hub token as 'automationhub\_api\_token' or  # - set 'generate\_automationhub\_token' to True to generate a new token  # Generating a new token will invalidate the existing token.  #  # automationhub\_api\_token=''  # generate\_automationhub\_token=  # Automation Hub LDAP configuration  #  # For Automation Hub to connect to LDAP directly the following variables  # need to be configured. The list of all possible configuration can be found here:  # https://django-auth-ldap.readthedocs.io/en/latest/reference.html#settings  # Extra parameter will need to be passed through an ansible ldap\_extra\_settings dictionnary.  #  # automationhub\_authentication\_backend = "ldap"  #  # automationhub\_ldap\_server\_uri = "ldap://ldap:10389"  # automationhub\_ldap\_bind\_dn = "cn=admin,dc=ansible,dc=com"  # automationhub\_ldap\_bind\_password = "GoodNewsEveryone"  # automationhub\_ldap\_user\_search\_base\_dn = "ou=people,dc=ansible,dc=com"  # automationhub\_ldap\_group\_search\_base\_dn = "ou=people,dc=ansible,dc=com"  # Automation Services Catalog Configuration  #  automationcatalog\_pg\_host=''  automationcatalog\_pg\_port=5432  automationcatalog\_pg\_database='automationservicescatalog'  automationcatalog\_pg\_username='automationservicescatalog'  automationcatalog\_pg\_password=''  # For an alternative front end url needed for SSO configuration with Automation  # Services Catalog, provide the URL.  # automationcatalog\_main\_url=''  # Automation Services Catalog requires either Controller to be installed  # with Automation Controller or a URL to an active and routable Controller  # server must be provided with the below variable.  # automation\_controller\_main\_url=''  # Automation Services Catalog requires SSO and SSO admin credentials for  # authentication. SSO admin credentials are also required for set Catalog specific  # roles needed for the application. If SSO is not provided in inventory for  # configuration, then the SSO host needs to be defined with the below.  # sso\_host=''  # Automation Services Catalog will generate a token, but a specific OAuth token  # can be provided with the following. Note that the variable  # "automation\_controller\_main\_url" must be assigned a routable address from  # the Automation Service Catalog host.  # automationcatalog\_controller\_token=''  # Automation Controller credentials can also be provided to generate a token  # for a working Controller environment. Note that the variable  # "automation\_controller\_main\_url" must be assigned a routable address from  # the Automation Service Catalog host. Generating a token will also create  # an application in Automation Controller for stateful management of the token.  # automationcatalog\_controller\_username=''  # automationcatalog\_controller\_password=''  # The default install will enable analytics collection for Services Catalog.  # Set to False to disable.  # automationcatalog\_enable\_analytics\_collection = True  # The default install will use RHSM certificate to send Services Catalog analytics  # collection data. To use username and password instead, provide the  # console.redhat.com credentials.  # insights\_username=''  # insights\_password=''  # If connection to Automation Controller requires SSL validation to be off,  # provide the variable below. By default, the value is true.  #  # automationcatalog\_controller\_verify\_ssl=False  # The default install will deploy a TLS enabled Automation Hub.  # If for some reason this is not the behavior wanted one can  # disable TLS enabled deployment.  #  # automationcatalog\_disable\_https = False  # The default install will deploy a TLS enabled Automation Hub.  # Unless specified otherwise the HSTS web-security policy mechanism  # will be enabled. This setting allows one to disable it if need be.  #  # automationcatalog\_disable\_hsts = False  # SSL-related variables  # If set, this will install a custom CA certificate to the system trust store.  # custom\_ca\_cert=/path/to/ca.crt  # Certificate and key to install in nginx for the web UI and API  # web\_server\_ssl\_cert=/path/to/tower.cert  # web\_server\_ssl\_key=/path/to/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  # Keystore file to install in SSO node  # sso\_custom\_keystore\_file='/path/to/sso.jks'  # The default install will deploy SSO with sso\_use\_https=True  # Keystore password is required for https enabled SSO  sso\_keystore\_password=''  # Single-Sign-On configuration  sso\_console\_admin\_password=''  # 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 = True  [aap\_valid\_hosts]  10.72.17.46 |