Automation Controller Release Notes

Release Automation Controller 4.0.0

Red Hat, Inc.

Oct 24, 2021

CONTENTS

1 Release Notes **2**
- 1.1 Release Notes for 4.0 . . . 2

2 Known Issues **4**
- 2.1 Isolated nodes unsupported in an OpenShift deployment . . . 4
- 2.2 Browsers ignoring the `autocomplete=off` setting . . . 5
- 2.3 Login via HTTP requires workaround . . . 5
- 2.4 Job slicing and limit interactions . . . 5
- 2.5 Default LDAP directory must be configured to use LDAP Authentication . . . 5
- 2.6 Potential security issue using `X_FORWARDED_FOR` in `REMOTE_HOST_HEADERS` . . . 5
- 2.7 Server error when accessing SAML metadata via hostname . . . 5
- 2.8 Live events status indicators . . . 6
- 2.9 VMWare Self-Signed Certs . . . 6
- 2.10 awx-manage inventory_import user . . . 7
- 2.11 Upgrading Tower 3.8 existing Instance Groups on OCP deployments . . . 7
- 2.12 Database on Disk Becomes Corrupted . . . 7
- 2.13 Safari unable to establish connection to web socket . . . 7
- 2.14 Local management not functioning as expected . . . 8
- 2.15 Problems when using SSH customization . . . 8
- 2.16 Reactivating OAuth authentication accounts which have been deleted . . . 8
- 2.17 Using vaulted variables in inventory sourced from a project . . . 9
- 2.18 Saved scheduled and workflow configurations and surveys . . . 9

3 Supported Locales **10**

4 Index **12**

5 Copyright © Red Hat, Inc. **13**

Index **14**

Thank you for your interest in Red Hat Ansible Automation Platform controller. automation controller is a commercial offering that helps teams manage complex multi-tier deployments by adding control, knowledge, and delegation to Ansible-powered environments.

The *Automation Controller Release Notes* provides release notes, known issues, and related reference materials. This document has been updated to include information for the latest release of Automation Controller v4.0.0.

We Need Feedback!

If you spot a typo in this documentation, or if you have thought of a way to make this manual better, we would love to hear from you! Please send an email to: docs@ansible.com

If you have a suggestion, try to be as specific as possible when describing it. If you have found an error, please include the manual's title, chapter number/section number, and some of the surrounding text so we can find it easily. We may not be able to respond to every message sent to us, but you can be sure that we will be reading them all!

Automation Controller Version 4.0.0; July 15, 2021; https://access.redhat.com/

CHAPTER

ONE

RELEASE NOTES

1.1 Release Notes for 4.0

1.1.1 Automation Controller Version 4.0

Introduced

- Support for automation execution environments. All automation now runs in execution environments via containers, either directly via OpenShift, or locally via podman
- New PatternFly 4 based user-interface for increased performance, security, and consistency with other Ansible Automation Platform components

Added

- Added identity provider support for GitHub Enterprise
- Support for RHEL system crypto profiles to nginx configuration
- The ability to disable local system users and only pull users from configured identity providers
- Additional Prometheus metrics for tracking job event processing performance
- New `awx-manage` command for dumping host automation information
- Red Hat Insights as an inventory source
- Ability to set server-side password policies using Django's `AUTH_PASSWORD_VALIDATORS` setting
- Support for Centrify Vault as a credential lookup plugin
- Support for namespaces in Hashicorp Vault credential plugin

Updated

- OpenShift deployment to be done via an Operator instead of a playbook
- Python used by application to Python 3.8
- Nginx used to version 1.18
- PostgreSQL used to PostgreSQL 12, and moved to partitioned databases for performance
- The "container groups" feature to general availability from Tech Preview; now fully utilizes execution environments
- Insights remediation to use new Red Hat Insights inventory source rather than utilizing scan playbooks with arbitrary inventory
- Subscriptions display to count hosts automated on instead of hosts imported

- Inventory source, credential, and Ansible content collection to reference *controller* instead of *tower*

Deprecated

- None

Removed

- Support for deploying on CentOS (any version) and RHEL 7
- Support for Mercurial projects
- Support for custom inventory scripts stored in controller (use `awx-manage export_custom_scripts` to export them)
- Resource profiling code (`AWX_RESOURCE_PROFILING_*`)
- Support for custom Python virtual environments for execution. Use new `awx-manage` tools for assisting in migration
- Top-level /api/v2/job_events/ API endpoint
- The ability to disable job isolation

CHAPTER

TWO

KNOWN ISSUES

- *Isolated nodes unsupported in an OpenShift deployment*
- *Browsers ignoring the `autocomplete=off` setting*
- *Login via HTTP requires workaround*
- *Job slicing and limit interactions*
- *Default LDAP directory must be configured to use LDAP Authentication*
- *Potential security issue using `X_FORWARDED_FOR` in `REMOTE_HOST_HEADERS`*
- *Server error when accessing SAML metadata via hostname*
- *Live events status indicators*
- *VMWare Self-Signed Certs*
- *awx-manage inventory_import user*
- *Upgrading Tower 3.8 existing Instance Groups on OCP deployments*
- *Database on Disk Becomes Corrupted*
- *Safari unable to establish connection to web socket*
- *Local management not functioning as expected*
- *Problems when using SSH customization*
- *Reactivating OAuth authentication accounts which have been deleted*
- *Using vaulted variables in inventory sourced from a project*
- *Saved scheduled and workflow configurations and surveys*

2.1 Isolated nodes unsupported in an OpenShift deployment

Isolated nodes are not currently supported when deploying automation controller in OpenShift.

2.2 Browsers ignoring the `autocomplete=off` setting

automation controller leverages the `autocomplete=off` attribute on forms to relay to the browser that it should not autocomplete the fields within that form. In some scenarios, however, the browser may ignore this setting and attempt to save and/or autocomplete fields. This tends to happen on forms that appear to contain login fields like username and password, such as the *User* form and some *Settings* forms. Further investigation is underway to deliver options that prevent this behavior.

2.3 Login via HTTP requires workaround

To access controller nodes behind your load balancer (in traditional cluster controller installs) via HTTP, refer to the procedure described in the Troubleshooting section of the *Automation Controller Administration Guide*.

2.4 Job slicing and limit interactions

When passing a limit to a Sliced Job, if the limit causes slices to have no hosts assigned, those slices will fail, causing the overall job to fail.

2.5 Default LDAP directory must be configured to use LDAP Authentication

The ability to configure up to six LDAP directories for authentication requires a value. On the settings page for LDAP, there is a "Default" LDAP configuration followed by five-numbered configuration slots. If the "Default" is not populated, the controller will not try to authenticate using the other directory configurations.

2.6 Potential security issue using `X_FORWARDED_FOR` in `REMOTE_HOST_HEADERS`

If placing controller nodes behind some sort of proxy, this may pose a security issue. This approach assumes traffic is always flowing exclusively through your load balancer, and that traffic that circumvents the load balancer is suspect to `X-Forwarded-For` header spoofing.

2.7 Server error when accessing SAML metadata via hostname

When the controller is accessed via hostname only (e.g. https://my-little-controller), trying to read the SAML metadata from /sso/metadata/saml/ generates a `sp_acs_url_invalid` server error.

A configuration in which uses SAML when accessing the controller via hostname only instead of an FQDN, is not supported. Doing so will generate an error that is captured in the tower.log file and in the browser with full traceback information.

2.8 Live events status indicators

Live events status dots are either seen as a red or orange dot at the top of the automation controller Dashboard when something goes wrong. They are not seen at all when the system is in a healthy state. If you encounter a red or orange live events status indicator, even when your system seems fine, the following suggestions may offer a solution:

- Try manually refreshing/reloading your browser page.
- Try changing web browsers, as Firefox and Safari have been reported to have issues trusting self-signed certificates.
- Try creating a self-signed certificate that matches your DNS and import it into your trust manually.
- Try using an incognito or private browsing session.
- Try disabling your browser plugins to ensure none are blocking the service.

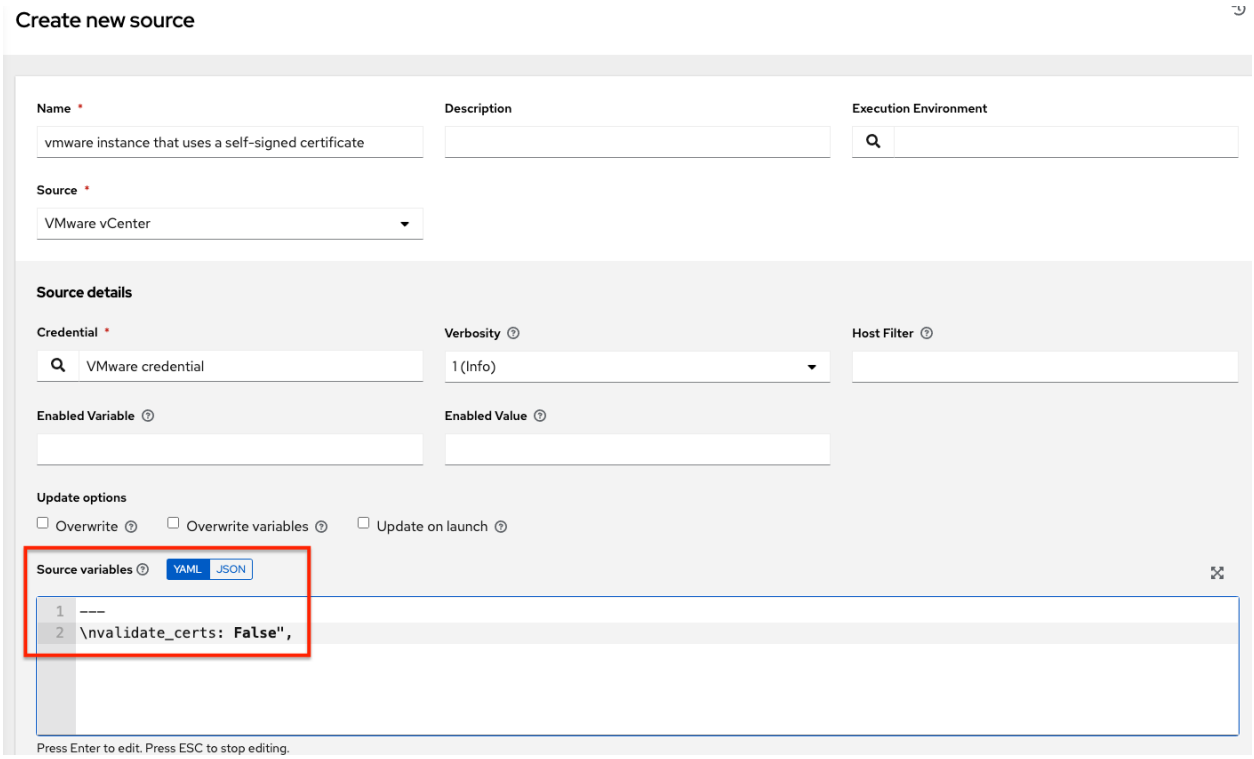
Live event status dots are used for troubleshooting problems with your controller instance. You can collect troubleshooting help by running a `sosreport`. As root, run the command `sosreport` from your system to automatically generate a diagnostic tar file, then contact Ansible's Support team with the collected information for further assistance. For more information on `sosreport`, refer to sosreport in the *Automation Controller Administration Guide*.

2.9 VMWare Self-Signed Certs

If you have a VMware instance that uses a self-signed certificate, then you will need to add the following to the *Source Vars* configuration of the Cloud Group:

```
"source_vars": "---\nvalidate_certs: False",
```

You can set this in inventory source for VMware vCenter as follows:



2.10 awx-manage inventory_import user

In general, the use of `awx-manage` commands is supported when executed by the root or awx user. However, in automation controller 4.0, even when run as the root user, the command `awx-manage inventory_import` fails to authenticate with the private registry where the Red Hat execution environments are hosted. The workaround is to run the command as the `awx` user, given that the images should be pre-pulled by the installer which correctly authenticates.

2.11 Upgrading Tower 3.8 existing Instance Groups on OCP deployments

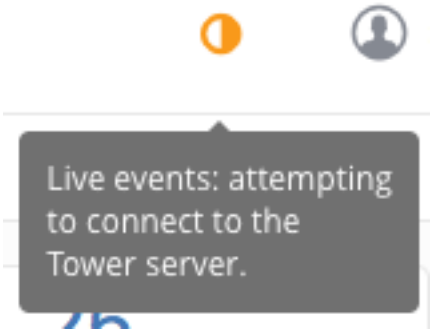
All job execution occurs in Container Groups for automation controller 4.0 deployed on OCP 4. Creating new "normal" Instance Groups is disabled in the user interface, however upon upgrade, nothing happens to regular instance groups. This is a known issue because any resources that attempt to use the normal instance group that contains control plane pods as instances will have 0 capacity and jobs will stay in the pending state indefinitely. The workaround is to delete all of these "normal" instance groups. By default, there is a Container Group where job execution will occur in the same namespace as the Controller pods are deployed. Additional capacity can be provided by configuring other Container Groups on the same or any other OpenShift 4 cluster.

2.12 Database on Disk Becomes Corrupted

If the controller is not cleanly shutdown, it leaves a `/var/lib/awx/beat.db` file on disk. If that happens, the dispatcher won't start, and you must manually delete the `/var/lib/awx/beat.db` file and restart the controller before the dispatcher will start properly.

2.13 Safari unable to establish connection to web socket

The following connection error displays in the controller:



This error is the result of Safari silently refusing to establish a connection to a web socket that is using a self-signed certificate. To resolve this issue, you must set Safari to always trust the website upon first visiting it:

1. Close the current browser and revisit the site. An error message appears stating Safari can't verify the identity of the website.
2. Click **Show Certificate**.
3. Check the **Always trust . . . when connecting to . . .** checkbox to allow Safari to accept the connection.

If you click **Continue** without checking the checkbox, this error will persist.

2.14 Local management not functioning as expected

All playbooks are executed by automation controller in a Linux container called an automation execution environment.

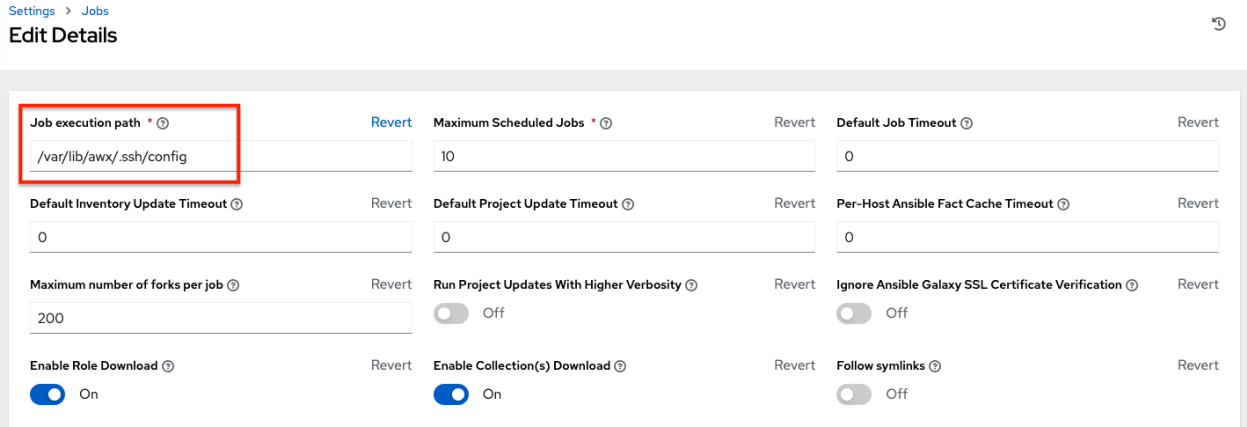
The use of `delegate_to: localhost` or `local_action` to manage the executing host will not function in this environment, as it will still be executing inside the container.

To manage the local host where execution is running, you will need to use the ssh connection plugin to connect from the container to the local host.

2.15 Problems when using SSH customization

The Job Isolation functionality in automation controller limits the directories available for playbooks to the project that is in use. If you are attempting to customize SSH behavior by using a custom SSH configuration in the awx user's home directory, this directory must be added to the list of directories exposed to the container.

For example, to add a custom SSH config in `/var/lib/awx/.ssh/config` and make it available for controller jobs, you can specify the path in the **Job Execution Isolation Path** field accessed from the **Jobs** tab of the Settings screen:



2.16 Reactivating OAuth authentication accounts which have been deleted

Once a user who logs in using social authentication has been deleted, the user will not be able to login again or be recreated until the system administrator runs a `cleanup_deleted` action with `days=0` to allow users to login again. Once `cleanup_deleted` has been run, the controller must be restarted using the `automation-controller-service restart` command. Accounts which have been deleted prior to having the `cleanup_deleted` action run will receive a "Your account is inactive" message upon trying to login.

2.17 Using vaulted variables in inventory sourced from a project

When using inventory from a source control project, individual vaulted variable values are supported. Vaulted files are not currently supported.

2.18 Saved scheduled and workflow configurations and surveys

If a configuration of a job template is scheduled or added to a workflow with answers from a prompted survey, changing the Job Template survey to supply different variable names may cause the saved configuration to not function. The workaround is to delete the saved schedule configuration/workflow node, and recreate it with answers from the updated survey.

CHAPTER

THREE

SUPPORTED LOCALES

Ansible Tower supports the following locales for UTC-friendly date and time information.

Tower automatically sets the locale preference based on the user's browser settings. For Safari, Internet Explorer, and older versions of Chrome as well as FireFox, this is handled automatically.

For newer versions of Chrome (v32 and later) and FireFox (v32 and later), Tower uses the language preferences set from your browser's language settings. The browser lists the user's preferred languages and selects the first in the array as the user's top choice, which Tower uses as the preferred locale. This means that you can change your browser's language and change your Tower locale preferences (although you may need to reload/refresh Tower in your browser to see this change.)

- `az` – Cyrillic
- `bg` – Bulgarian
- `bs` – Bosnian
- `ca` – Catalan
- `cs` – Czech
- `da` – Danish
- `de` – German
- `el` – Greek
- `en-gb` – English (United Kingdom)
- `es` – Spanish
- `et` – Estonian
- `eu` – Basque
- `fa` – Persian
- `fi` – Finnish
- `fo` – Faroese
- `fr` – French
- `gl` – Galician
- `he` – Hebrew
- `hr` – Croatian
- `hu` – Hungarian
- `id` – Indonesian

- `is` – Icelandic
- `it` – Italian
- `ja` – Japanese
- `ka` – Georgian
- `lt` – Lithuanian
- `lv` – Latvian
- `mk` – Macedonian
- `nb` – Norwegian
- `nl` – Dutch
- `pl` – Polish
- `pt-br` – Portuguese (Brazil)
- `pt` – Portuguese
- `ro` – Romanian
- `ru` – Russian
- `sk` – Slovak
- `sl` – Slovenian
- `sq` – Albanian
- `sr` – Serbian
- `sv` – Swedish
- `th` – Thai
- `tr` – Turkish
- `uk` – Ukrainian
- `vi` – Vietnamese
- `zh-cn` – Chinese (simplified)
- `zh-tw` – Chinese (traditional)

CHAPTER

FOUR

INDEX

- genindex

CHAPTER

FIVE

COPYRIGHT © RED HAT, INC.

Ansible, Ansible Automation Platform, Red Hat, and Red Hat Enterprise Linux are trademarks of Red Hat, Inc., registered in the United States and other countries.

If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original version.

Third Party Rights

Ubuntu and Canonical are registered trademarks of Canonical Ltd.

The CentOS Project is copyright protected. The CentOS Marks are trademarks of Red Hat, Inc. ("Red Hat").

Microsoft, Windows, Windows Azure, and Internet Explore are trademarks of Microsoft, Inc.

VMware is a registered trademark or trademark of VMware, Inc.

Rackspace trademarks, service marks, logos and domain names are either common-law trademarks/service marks or registered trademarks/service marks of Rackspace US, Inc., or its subsidiaries, and are protected by trademark and other laws in the United States and other countries.

Amazon Web Services", "AWS", "Amazon EC2", and "EC2", are trademarks of Amazon Web Services, Inc. or its affiliates.

OpenStack™ and OpenStack logo are trademarks of OpenStack, LLC.

Chrome™ and Google Compute Engine™ service registered trademarks of Google Inc.

Safari® is a registered trademark of Apple, Inc.

Firefox® is a registered trademark of the Mozilla Foundation.

All other trademarks are the property of their respective owners.

INDEX

A

Ansible Azure dependencies
    known issues, 4
authentication (*reactive user*)
    known issues, 4
awx-manage inventory_import user
    known issues, 4

B

browser auto-complete
    known issues, 4
bundled installer
    known issues, 4

D

database corruption
    known issues, 4

G

green dot
    live event statuses, 4

H

host comparisons
    known issues, 4

I

issues, known, 4

J

job isolation
    known issues, 4

K

known issues, 4
    Ansible Azure dependencies, 4
    authentication (*reactive user*), 4
    awx-manage inventory_import user, 4
    browser auto-complete, 4
    bundled installer, 4
    database corruption, 4
    host comparisons, 4
    job isolation, 4
    LDAP authentication, 4
    live event statuses, 4
    local management, 4
    login problems with social authentication, 4
    login via http, 4
    lost isolated jobs, 4
    OAuth account recreation, 4
    proxy support, 4
    self-signed certs (*VMWare*), 4
    session limit, 4
    sosreport, 4
    ssh customization, 4
    traceback error, 4
    Ubuntu, 4
    upgrades, 4
    upgrading tower 3.8 exisiting instance groups on OCP deployments, 4
    user cannot log in using authentication, 4
    VMWare self-signed certs, 4
    web sockets in safari, 4
    YAML traceback error, 4

L

LDAP authentication
    known issues, 4
live event statuses
    green dot, 4
    known issues, 4
    red dot, 4
local management
    known issues, 4
locales supported, 10
login problems with social authentication
    known issues, 4
login via http
    known issues, 4
lost isolated jobs

known issues, 4

O

OAuth account recreation
known issues, 4

P

proxy support
known issues, 4

R

red dot
live event statuses, 4
release notes
v4.0, 2

S

self-signed certs (*VMWare*)
known issues, 4
session limit
known issues, 4
sosreport
known issues, 4
ssh customization
known issues, 4

T

traceback error
known issues, 4

U

Ubuntu
known issues, 4
upgrades
known issues, 4
upgrading tower 3.8 exisiting instance groups on OCP deployments
known issues, 4
user cannot log in using authentication
known issues, 4

V

v4.0
release notes, 2
VMWare self-signed certs
known issues, 4

W

web sockets in safari
known issues, 4

Y

YAML traceback error
known issues, 4