
Automation Controller Release Notes

Release Automation Controller 4.1.2

Red Hat, Inc.

Feb 10, 2023

CONTENTS

1	Release Notes	2
1.1	Automation Controller Version 4.1.2	2
1.2	Automation Controller Version 4.1.1	3
1.3	Automation Controller Version 4.1	3
1.4	Automation Controller Version 4.0.1	4
1.5	Automation Controller Version 4.0	4
2	Known Issues	6
2.1	Launching the ansible-runner component not working as expected	7
2.2	Deleted default orgs produces duplicate Ansible-Galaxy credentials	7
2.3	Isolated nodes unsupported in an OpenShift deployment	7
2.4	Browsers ignoring the autocomplete=off setting	7
2.5	Login via HTTP requires workaround	7
2.6	Job slicing and limit interactions	7
2.7	Misuse of job slicing can cause errors in job scheduling	8
2.8	Default LDAP directory must be configured to use LDAP Authentication	8
2.9	Potential security issue using X_FORWARDED_FOR in REMOTE_HOST_HEADERS	8
2.10	Server error when accessing SAML metadata via hostname	8
2.11	Live events status indicators	8
2.12	VMWare Self-Signed Certs	9
2.13	awx-manage inventory_import user	9
2.14	Upgrading Tower 3.8 existing Instance Groups on OCP deployments	10
2.15	Database on Disk Becomes Corrupted	10
2.16	Safari unable to establish connection to web socket	10
2.17	Local management not functioning as expected	11
2.18	Problems when using SSH customization	11
2.19	Database server installed on nodes	11
2.20	Reactivating OAuth authentication accounts which have been deleted	11
2.21	Using vaulted variables in inventory sourced from a project	12
2.22	Saved scheduled and workflow configurations and surveys	12
3	Supported Locales	13
4	Index	15
5	Copyright © Red Hat, Inc.	16
	Index	17

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 v4.1.2.

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 4.1.2; April 12, 2022; <https://access.redhat.com/>

RELEASE NOTES

1.1 Automation Controller Version 4.1.2

Automation Controller fixes:

- Upgraded Django version to 3.2 LTS
- System (management) jobs are now able to be canceled
- Rsyslog no longer needs manual intervention to send out logs after hitting a 40x error
- Credential lookup plugins now respect the `AWX_TASK_ENV` setting
- Fixed the controller to list valid subscriptions from Satellite when having multiple quantities from the same SKU
- Updated Receptor version to 1.2.1, which includes several fixes

Execution Environment fixes:

- The host trusted cert store is now exposed to execution environments by default. See [Isolation functionality and variables](#) for detail.
- Mounting the `/etc/ssh` or `/etc/` to isolated jobs now works in podman
- User customization of execution environment mount options and mount paths are now supported
- Fixed SELinux context on `/var/lib/awx/.local/share/containers` and ensure `awx` as podman storage
- Fixed failures to no longer occur when the `semanage fcontext` has been already set for the expected directory

Automation Controller UI fixes:

- Fixed the ability to create manual projects in Japanese and other supported non-English languages
- Fixed the controller UI to list the roles for organizations when using non-English web browsers
- Fixed the job output to display all job type events, including source control update events over websockets
- Fixed the `TypeError` when running a command on a host in a smart inventory
- Fixed the encrypted password in surveys to no longer show up as plaintext in the Edit Order page

Installation fixes specific to Automation Controller:

- Fixed duplicate Galaxy credentials with no default organization
- Running the `./setup.sh -b` out of the installer directory no longer fails to load group vars
- The installer no longer fails when IPV6 is disabled
- Fixed unnecessary `become_user:root` entries in the installation

- Modified database backup and restore logic to compress dump data
- Creating default execution environments no longer fails when password has special characters
- Fixed installations of execution environments when installing without internet access
- Upgrading to AAP 2.1 no longer breaks when the Django superuser is missing
- Rekey now allowed with existing key

1.2 Automation Controller Version 4.1.1

- Added the ability to specify additional nginx headers
- Fixed analytics gathering to collect all the data the controller needed to collect
- Fixed the controller to no longer break subsequent installer runs when deleting the demo organization

1.3 Automation Controller Version 4.1

Introduced

- Connected Receptor nodes to form a control plane and execution mesh configurations
- The special `controlplane` instance group to allow for the task manager code to target an OpenShift Controller node to run the project update
- The ability to render a configured mesh topology in a graph in the installer
- Controller 4.1 execution nodes can be remote
- Node types for Controller 4.1 (`control`, `hybrid`, `execution`, `hop`, `control`, `hybrid`, `execution`, `hop`) installed for different sets of services and provide different capabilities, allowing for scaling nodes that provide the desired capability such as job execution or serving of web requests to the API/UI.

Added

- The ability for the platform installer to allow users to install execution nodes and express receptor mesh topology in the inventory file. The platform installer will also be responsible for deprovisioning nodes.
- Work signing to the receptor mesh so that control plane nodes have the exclusive authority to submit receptor work to execution nodes over the mesh
- Support for pre-population of execution environment name, description, and image from query parameters when adding a new execution environment in the Controller User Interface
- Ability to trigger a reload of the topology configuration in Receptor without interrupting work execution
- Using Public Key Infrastructure (PKI) for securing the Receptor mesh
- Added importing execution environments from Automation Hub into the controller to improve the platform experience

Updated

- The controller to support new controller control plane and execution mesh
- Task manager will only run project updates and system jobs on nodes with `node_type` of “control” or “hybrid”
- Task manager will only run jobs, inventory updates, and ad hoc commands on nodes with `node_type` of “hybrid” or “execution”

- Heartbeat and capacity check to work with Receptor execution nodes
- Reaper to work with the addition of execution nodes
- Controller User Interface to not show control instances as an option to associate with instance groups
- The Associate pop-up screen to display host names when adding an existing host to a group
- Validators for editing miscellaneous authentication parameters
- Advanced search key options to be grouped
- SAML variables default values
- Survey validation on Prompt on Launch
- Login redirect

Deprecated

- None

Removed

- The ability to delete the default instance group through the User Interface

1.4 Automation Controller Version 4.0.1

- Upgraded Django version to 3.2 LTS
- Updated receptor to version 1.2.1

1.5 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

KNOWN ISSUES

- *Launching the ansible-runner component not working as expected*
- *Deleted default orgs produces duplicate Ansible-Galaxy credentials*
- *Isolated nodes unsupported in an OpenShift deployment*
- *Browsers ignoring the `autocomplete=off` setting*
- *Login via HTTP requires workaround*
- *Job slicing and limit interactions*
- *Misuse of job slicing can cause errors in job scheduling*
- *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*
- *Database server installed on nodes*
- *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 Launching the ansible-runner component not working as expected

A change was made to the way the ansible-runner component is launched (the executable inside of the execution environment that the controller launches to run a playbook), introduced a backward incompatibility. It is highly recommended to always rebuild on top of the base execution environments that corresponds to the platform version you are using. This should be the ideal way to upgrade in general.

2.2 Deleted default orgs produces duplicate Ansible-Galaxy credentials

Despite being able to run subsequent installs when deleting the default organization, it does not automatically remove or fix duplicate Ansible-Galaxy credentials. Refer to the KCS article on [How to remove duplicated Ansible-Galaxy credentials from the database](#) for further detail.

2.3 Isolated nodes unsupported in an OpenShift deployment

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

2.4 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.

2.5 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*.

2.6 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.

2.7 Misuse of job slicing can cause errors in job scheduling

Job slicing is intended to scale job executions horizontally. Enabling job slicing on a job template divides an inventory to be acted upon in the number of slices configured at launch time and then starts a job for each slice.

It is expected that the number of slices will be equal to or less than the number of controller nodes. Setting an extremely high number of job slices (e.g., thousands), while allowed, can cause performance degradation as the job scheduler is not designed to schedule simultaneously thousands of workflow nodes, which are what the sliced jobs become.

2.8 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.

2.9 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.

2.10 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.

2.11 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*.

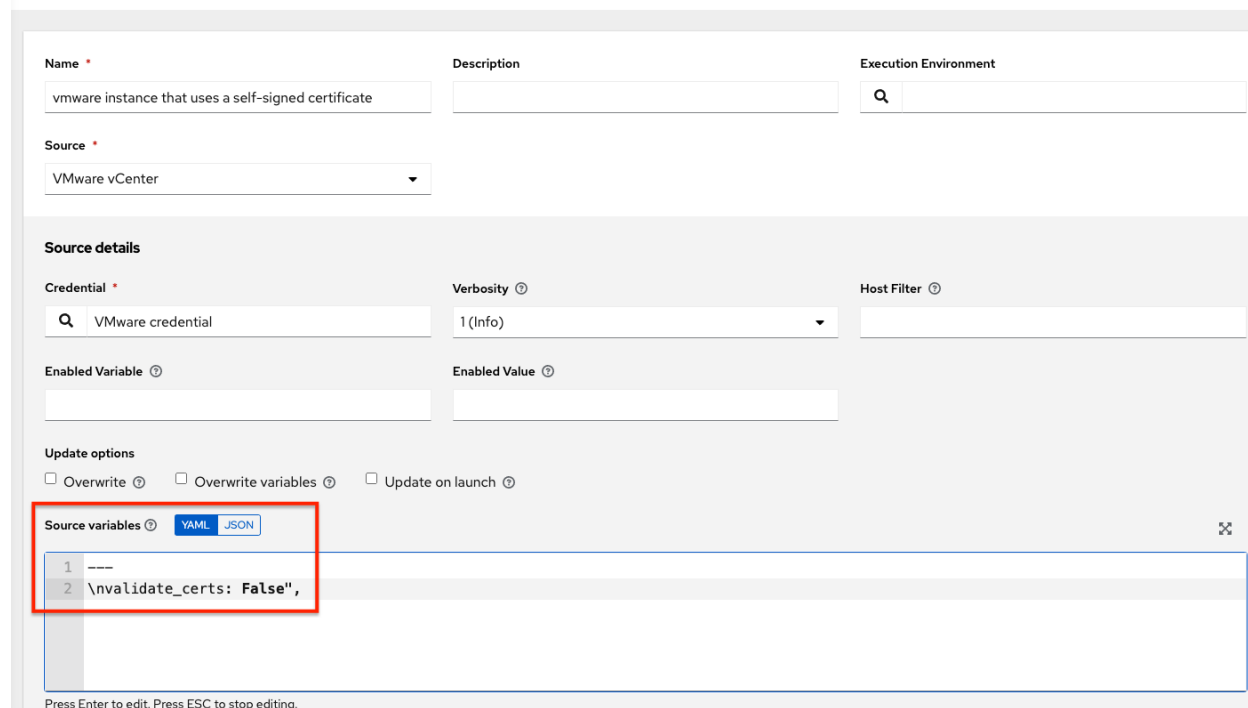
2.12 VMWare Self-Signed Certs

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:

Create new source



The screenshot shows the 'Create new source' form in the Automation Controller UI. The form includes fields for Name, Description, Execution Environment, Source (VMware vCenter), Credential (VMware credential), Verbosity (1 (Info)), Host Filter, Enabled Variable, and Enabled Value. The 'Source variables' section is highlighted with a red box, showing a list of variables with the second line containing the text: `\nvalidate_certs: False",`

2.13 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.

2.14 Upgrading Tower 3.8 existing Instance Groups on OCP deployments

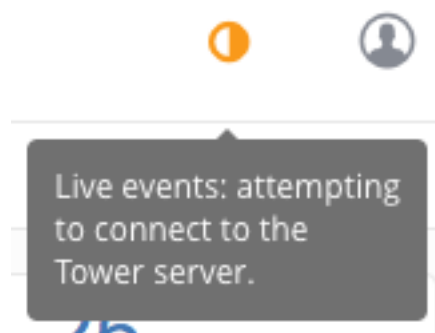
All job execution occurs in Container Groups for automation controller 4.0 deployed on OCP 4. Creating new “normal” Instance Groups is disabled in the user interface, however upon upgrade, nothing happens to regular instance groups. This is a known issue because any resources that attempt to use the 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.

2.15 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.

2.16 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.

2.17 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.

2.18 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:

Settings > Jobs Edit Details

Job execution path ⓘ /var/lib/awx/.ssh/config	Maximum Scheduled Jobs ⓘ 10	Default Job Timeout ⓘ 0
Default Inventory Update Timeout ⓘ 0	Default Project Update Timeout ⓘ 0	Per-Host Ansible Fact Cache Timeout ⓘ 0
Maximum number of forks per job ⓘ 200	Run Project Updates With Higher Verbosity ⓘ ☐ Off	Ignore Ansible Galaxy SSL Certificate Verification ⓘ ☐ Off
Enable Role Download ⓘ ☒ On	Enable Collection(s) Download ⓘ ☒ On	Follow symlinks ⓘ ☐ Off

2.19 Database server installed on nodes

All nodes in the cluster get a database server even if the nodes do not have a database. This is unexpected and may take up space.

2.20 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.

2.21 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.

2.22 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.

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)

INDEX

- `genindex`

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.

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.

A

- Ansible Azure dependencies
 - known issues,6
- ansible-runner
 - known issues,6
- authentication (*reactive user*)
 - known issues,6
- awx-manage inventory_import user
 - known issues,6

B

- browser auto-complete
 - known issues,6
- bundled installer
 - known issues,6

D

- database corruption
 - known issues,6
- deleted default orgs
 - known issues,6
- duplicate Ansible-Galaxy credentials
 - known issues,6

G

- green dot
 - live event statuses,6

H

- host comparisons
 - known issues,6

I

- issues, known,6

J

- job isolation
 - known issues,6

K

- known issues,6
 - Ansible Azure dependencies,6

- ansible-runner,6
- authentication (*reactive user*),6
- awx-manage inventory_import user,6
- browser auto-complete,6
- bundled installer,6
- database corruption,6
- deleted default orgs,6
- duplicate Ansible-Galaxy
 - credentials,6
- host comparisons,6
- job isolation,6
- LDAP authentication,6
- live event statuses,6
- local management,6
- login problems with social
 - authentication,6
- login via http,6
- lost isolated jobs,6
- OAuth account recreation,6
- proxy support,6
- SAML issues,6
- self-signed certs (*VMWare*),6
- session limit,6
- sosreport,6
- ssh customization,6
- traceback error,6
- Ubuntu,6
- upgrades,6
- upgrading tower 3.8 existing
 - instance groups on OCP
 - deployments,6
- user cannot log in using
 - authentication,6
- VMWare self-signed certs,6
- web sockets in safari,6
- YAML traceback error,6

L

- LDAP authentication
 - known issues,6
- live event statuses
 - green dot,6

- known issues,6
- red dot,6
- local management
 - known issues,6
- locales supported,13
- login problems with social authentication
 - known issues,6
- login via http
 - known issues,6
- lost isolated jobs
 - known issues,6

O

- OAuth account recreation
 - known issues,6

P

- proxy support
 - known issues,6

R

- red dot
 - live event statuses,6
- release notes
 - v4.0,2
 - v4.0.1,2
 - v4.1,2
 - v4.1.1,2
 - v4.1.2,2

S

- SAML issues
 - known issues,6
- self-signed certs (*VMWare*)
 - known issues,6
- session limit
 - known issues,6
- sosreport
 - known issues,6
- ssh customization
 - known issues,6

T

- traceback error
 - known issues,6

U

- Ubuntu
 - known issues,6
- upgrades
 - known issues,6
- upgrading tower 3.8 existing instance
 - groups on OCP deployments

- known issues,6
- user cannot log in using authentication
 - known issues,6

V

- v4.0
 - release notes,2
- v4.0.1
 - release notes,2
- v4.1
 - release notes,2
- v4.1.1
 - release notes,2
- v4.1.2
 - release notes,2
- VMWare self-signed certs
 - known issues,6

W

- web sockets in safari
 - known issues,6

Y

- YAML traceback error
 - known issues,6