Red Hat Ansible Automation Platform 2.4

Red Hat Ansible Automation Platform release notes

New features, enhancements, and bug fix information

Red Hat Ansible Automation Platform 2.4 Red Hat Ansible Automation Platform release notes

New features, enhancements, and bug fix information

Legal Notice

Abstract

The release notes for Red Hat Ansible Automation Platform summarize all new features and enhancements, notable technical changes, major corrections from the previous version, and any known bugs upon general availability.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

If you have a suggestion to improve this documentation, or find an error, please contact technical support at https://access.redhat.com to create an issue on the Ansible Automation Platform Jira project using the **docs-product** component.

CHAPTER 1. OVERVIEW OF RED HAT ANSIBLE AUTOMATION PLATFORM

Red Hat Ansible Automation Platform simplifies the development and operation of automation workloads for managing enterprise application infrastructure lifecycles. Ansible Automation Platform works across multiple IT domains including operations, networking, security, and development, as well as across diverse hybrid environments. Simple to adopt, use, and understand, Ansible Automation Platform provides the tools needed to rapidly implement enterprise-wide automation, no matter where you are in your automation journey.

1.1. WHAT IS INCLUDED IN ANSIBLE AUTOMATION PLATFORM

Ansible Automation Platform	Automation controller	Automation hub	Event-Driven Ansible controller	Insights for Ansible Automation Platform
2.4	4.4	4.7 - hosted service	1.0	hosted service

1.2. RED HAT ANSIBLE AUTOMATION PLATFORM LIFE CYCLE

Red Hat provides different levels of maintenance for each Ansible Automation Platform release. For more information, see Red Hat Ansible Automation Platform Life Cycle .

1.3. UPGRADING ANSIBLE AUTOMATION PLATFORM

When upgrading, do not use **yum update**. Use the installation program instead. The installation program performs all of the necessary actions required to upgrade to the latest versions of Ansible Automation Platform, including automation controller and private automation hub.

Additional resources

- For information about the components included in Ansible Automation Platform, see the table in What is included in Ansible Automation Platform .

- For more information about upgrading Ansible Automation Platform, see Red Hat Ansible Automation Platform upgrade and migration guide.

- For procedures related to using the Ansible Automation Platform installer, see Ansible Automation Platform installation guide.

CHAPTER 2. OVERVIEW OF THE ANSIBLE AUTOMATION PLATFORM 2.4 RELEASE

2.1. NEW FEATURES AND ENHANCEMENTS

Ansible Automation Platform 2.4 includes the following enhancements:

- Previously, the execution environment container images were based on RHEL 8 only. With Ansible Automation Platform 2.4 onwards, the execution environment container images are now also available on RHEL 9. The execution environment includes the following container images:

  - ansible-python-base

  - ansible-python-toolkit

  - ansible-builder

  - ee-minimal

  - ee-supported

- The ansible-builder project recently released Ansible Builder version 3, a much-improved and simplified approach to creating execution environments. You can use the following configuration YAML keys with Ansible Builder version 3:

  - additional_build_files

  - additional_build_steps

  - build_arg_defaults

  - dependencies

  - images

  - options

  - version

- Ansible Automation Platform 2.4 and later versions can now run on ARM platforms, including both the control plane and the execution environments.

- Added an option to configure the SSO logout URL for automation hub if you need to change it from the default value.

- Updated the ansible-lint RPM package to version 6.14.3.

- Updated Django for potential denial-of-service vulnerability in file uploads (CVE-2023-24580).

- Updated sqlparse for ReDOS vulnerability (CVE-2023-30608).

- Updated Django for potential denial-of-service in Accept-Language headers (CVE-2023-23969).

- Ansible Automation Platform 2.4 adds the ability to install automation controller, automation hub, and Event-Driven Ansible on IBM Power (ppc64le), IBM Z (s390x), and IBM® LinuxONE (s390x) architectures.

Additional resources

- For more information about using Ansible Builder version 3, see Ansible Builder Documentation and Execution Environment Setup Reference .

2.2. TECHNOLOGY PREVIEW

Technology Preview features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope .

The following are Technology Preview features:

- Starting with Ansible Automation Platform 2.4, the Platform Resource Operator can be used to create the following resources in automation controller by applying YAML to your OpenShift cluster:

  - Inventories

  - Projects

  - Instance Groups

  - Credentials

  - Schedules

  - Workflow Job Templates

  - Launch Workflows

You can now configure the Controller Access Token for each resource with the **connection_secret** parameter, rather than the **tower_auth_secret** parameter. This change is compatible with earlier versions, but the **tower_auth_secret** parameter is now deprecated and will be removed in a future release.

Additional resources

- For the most recent list of Technology Preview features, see Ansible Automation Platform – Preview Features.

- For information about execution node enhancements on OpenShift deployments, see Managing Capacity With Instances .

2.3. DEPRECATED AND REMOVED FEATURES

Deprecated functionality is still included in Ansible Automation Platform and continues to be supported. However, the functionality will be removed in a future release of Ansible Automation Platform and is not recommended for new deployments.

The following functionality was deprecated and removed in Ansible Automation Platform 2.4:

- On-premise component automation services catalog is now removed from Ansible Automation Platform 2.4 onwards.

- With the Ansible Automation Platform 2.4 release, the execution environment container image for Ansible 2.9 (**ee-29-rhel-8**) is no longer loaded into the automation controller configuration by default.

- Although you can still synchronize content, the use of synclists is deprecated and will be removed in a later release. Instead, private automation hub administrators can upload manually-created requirements files from the **rh-certified** remote.

- You can now configure the Controller Access Token for each resource with the **connection_secret** parameter, rather than the **tower_auth_secret** parameter. This change is compatible with earlier versions, but the **tower_auth_secret** parameter is now deprecated and will be removed in a future release.

- Smart inventories have been deprecated in favor of constructed inventories and will be removed in a future release.

2.4. BUG FIXES

Ansible Automation Platform 2.4 includes the following bug fixes:

- Updated the installation program to ensure that collection auto signing cannot be enabled without enabling the collection signing service.

- Fixed an issue with restoring backups when the installed automation controller version is different from the backup version.

- Fixed an issue with not adding user defined galaxy-importer settings to **galaxy-importer.cfg** file.

- Added missing **X-Forwarded-For** header information to nginx logs.

- Removed unnecessary receptor peer name validation when IP address is used as the name.

- Updated the **outdated base_packages.txt** file that is included in the bundle installer.

- Fixed an issue where upgrading the Ansible Automation Platform did not update the nginx package by default.

- Fixed an issue where an **awx** user was created without creating an **awx** group on execution nodes.

- Fixed the assignment of package version variable to work with flat file inventories.

- Added a FQDN check for the automation hub hostname required to run the Skopeo commands.

- Fixed the front end URL for Red Hat Single Sign On (SSO) so it is now properly configured after you specify the **sso_redirect_host** variable.

- Fixed the variable precedence for all component **nginx_tls_files_remote** variables.

- Fixed the **setup.sh** script to escalate privileges if necessary for installing Ansible Automation Platform.

- Fixed an issue when restoring a backup to an automation hub with a different hostname.

CHAPTER 3. AUTOMATION CONTROLLER

Automation controller helps teams manage complex multitiered deployments by adding control, knowledge, and delegation to Ansible-powered environments.

See Automation Controller Release Notes for 4.x for a full list of new features and enhancements.

CHAPTER 4. EVENT-DRIVEN ANSIBLE

Event-Driven Ansible is a new way to enhance and expand automation by improving IT speed and agility while enabling consistency and resilience. Event-Driven Ansible is designed for simplicity and flexibility.

Known issues

- Both contributor and editor roles cannot set the AWX token. Only users with administrator roles can set the AWX token.

- Activation-job pods do not have request limits.

- The onboarding wizard does not request a controller token creation.

- Users cannot filter through a list of tokens under the **Controller Token** tab.

- Only the users with administrator rights can set or change their passwords.

- If there is a failure, an activation with restart policy set to **Always** is unable to restart the failed activation.

- Disabling and enabling an activation causes the restart count to increase by one count. This behavior results in an incorrect **restart** count.

- You must run Podman pods with memory limits.

- Users can add multiple tokens even when only the first AWX token is used.

- A race condition occurs when creating and rapidly deleting an activation causes errors.

- When users filter any list, only the items that are on the list get filtered.

- When ongoing activations start multiple jobs, a few jobs are not recorded in the audit logs.

- When a job template fails, a few key attributes are missing in the event payload.

- Restart policy in a Kubernetes deployment does not restart successful activations that are marked as failed.

- An incorrect status is reported for activations that are disabled or enabled.

- If the **run_job_template** action fails, the rule is not counted as executed.

- RHEL 9.2 activations cannot connect to the host.

- Restarting the Event-Driven Ansible server can cause activation states to become stale.

- Bulk deletion of rulebook activation lists is not consistent, and the deletion can be either successful or unsuccessful.

- When users access the detail screen of a rule audit, the related rulebook activation link is broken.

- Long running activations with loads of events can cause an out of disk space issue. Resolved in installer release 2.4-6.

- Certain characters, such as hyphen (-), forward slash (/), and period (.), are not supported in the event keys. Resolved in installer release 2.4-3.

- When there are more activations than available workers, disabling the activations incorrectly shows them in running state. Resolved in installer release 2.4-3.

- Event-Driven Ansible activation pods are running out of memory on RHEL 9. Resolved in installer release 2.4-3.

- When all workers are busy with activation processes, other asynchronous tasks are not executed, such as importing projects. Resolved in installer release 2.4-3.

CHAPTER 5. AUTOMATION HUB

Automation hub enables you to discover and use new certified automation content, such as Ansible Collections, from Red Hat Ansible and Certified Partners.

New features and enhancements

- This release of automation hub provides repository management functionality. With repository management, you can create, edit, delete, and move content between repositories.

Bug fixes

- Fixed an issue in the collection keyword search which was returning an incorrect number of results.

- Added the ability to set **OPT_REFERRALS** option for LDAP, so that users can now successfully log in to the automation hub by using their LDAP credentials.

- Fixed an error on the UI when **redhat.openshift** collection's core dependency was throwing a **404 Not Found** error.

- Fixed an error such that the deprecated execution environments are now skipped while syncing with **registry.redhat.io**.

CHAPTER 6. AUTOMATION PLATFORM OPERATOR

Ansible Automation Platform Operator provides cloud-native, push-button deployment of new Ansible Automation Platform instances in your OpenShift environment.

Bug fixes

- Enabled configuration of resource requirements for automation controller **init** containers.

- Added **securityContext** for Event-Driven Ansible Operator deployments to be Pod Security Admission compliant.

- Resolved error **Controller: Error 413 Entity too large** when doing bulk updates.

- Ansible token is now obfuscated in YAML job details.

CHAPTER 7. ANSIBLE AUTOMATION PLATFORM DOCUMENTATION

Red Hat Ansible Automation Platform 2.4 documentation includes significant feature updates as well as documentation enhancements and offers an improved user experience.

New features and enhancements

- With the removal of the on-premise component automation services catalog from Ansible Automation Platform 2.4 onwards, all automation services catalog documentation is removed from the Ansible Automation Platform 2.4 documentation.

- The following documents are created to help you install and use Event-Driven Ansible, the newest capability of Ansible Automation Platform:

  - Getting Started with Event-Driven Ansible

  - Event Driven Ansible User Guide

In addition, sections of the Ansible Automation Platform Planning Guide and the Ansible Automation Platform Installation Guide are updated to include instructions for planning and installing Event-Driven Ansible.

- The automation hub documentation has had significant reorganization to combine the content spread across 9 separate documents into the following documents:

  Getting started with automation hub

  Use this guide to perform the initial steps required to use Red Hat automation hub as the default source for Ansible collections content.

  Managing content in automation hub

  Use this guide to understand how to create and manage collections, content and repositories in automation hub.

  Red Hat Ansible Automation Platform Installation Guide

  Use this guide to learn how to install Ansible Automation Platform based on supported installation scenarios.

- The *Managing Red Hat Certified and Ansible Galaxy collections in automation hub guide* has been moved to the *Red Hat Certified, validated, and Ansible Galaxy content in automation hub* topic in the *Managing content in automation hub* guide.

- The Ansible Automation Platform 2.4 Release Notes are restructured to improve the experience for our customers and the Ansible Community. Users can now view the latest updates based on the Ansible Automation Platform versions, instead of their release timeline.

- The topic Repository management with automation hub is created to help you create and manage custom repositories in automation hub. This topic is found in the *Managing content in automation hub* guide.

CHAPTER 8. ASYNCHRONOUS UPDATES

Security, bug fix, and enhancement updates for Ansible Automation Platform 2.4 are released as asynchronous erratas. All Ansible Automation Platform erratas are available on the Download Red Hat Ansible Automation Platform page in the Customer Portal.

As a Red Hat Customer Portal user, you can enable errata notifications in the account settings for Red Hat Subscription Management (RHSM). When errata notifications are enabled, you receive notifications through email whenever new erratas relevant to your registered systems are released.

> **NOTE**
>
> Red Hat Customer Portal user accounts must have systems registered and consuming Ansible Automation Platform entitlements for Ansible Automation Platform errata notification emails to generate.

The Asynchronous updates section of the release notes will be updated over time to give notes on enhancements and bug fixes for asynchronous errata releases of Ansible Automation Platform 2.4.

Additional resources

- For more information about asynchronous errata support in Ansible Automation Platform, see Red Hat Ansible Automation Platform Life Cycle .

- For information about Common Vulnerabilities and Exposures (CVEs), see What is a CVE? and Red Hat CVE Database .

8.1. RPM RELEASES

Table 8.1. Component versions per errata advisory

Errata advisory	Component versions
RHSA-2024:3781 June 10, 2024	**ansible-automation-platform-installer** 2.4-7 **ansible-automation-platform-setup** 2.4-7 **ansible-core** 2.15.11 - Automation controller 4.5.7 - Automation hub 4.9.2 - Event-Driven Ansible 1.0.7

8.1.1. RHSA-2024:3781 - Security Advisory - June 10, 2024

RHSA-2024:3781

8.1.1.1. General

- Added the **automation-controller-cli** package to the **ansible-developer** RPM repositories (AAP-23368).

With this update, the following CVEs have been addressed:

- CVE-2023-45288 – unlimited number of CONTINUATION frames causes a denial of service (DoS).

  - Packages updated: **receptor: golang: net/http, x/net/http2**.

- CVE-2023-45290 – memory exhaustion in **Request.ParseMultipartForm**.

  - Packages updated: **receptor: golang: net/http**.

- CVE-2023-49083 – null-pointer dereference when loading PKCS7 certificates.

  - Packages updated: **python3-cryptography** and **python39-cryptography**.

- CVE-2023-50447 – arbitrary code execution with the environment parameter.

  - Packages updated: **python3-pillow** and **python39-pillow**.

- CVE-2024-1135 – HTTP Request Smuggling due to improper validation of Transfer-Encoding headers.

  - Packages updated: **python3-gunicorn** and **python39-gunicorn**.

- CVE-2024-21503 – regular expression denial of service (ReDoS) with the **lines_with_leading_tabs_expanded()** function within the **strings.py** file.

  - Packages updated: **python3-black** and **python39-black**.

- CVE-2024-24783 – verify panics on certificates with an unknown public key algorithm.

  - Packages updated: **receptor: golang: crypto/x509**.

- CVE-2024-26130 – NULL pointer dereference with **pkcs12.serialize_key_and_certificates** when called with a non-matching certificate and private key and an **hmac_hash** override.

  - Packages updated: **python3-cryptography** and **python39-cryptography**.

- CVE-2024-27306 – cross-site scripting (XSS) on index pages for static file handling.

  - Packages updated: **python3-aiohttp** and **python39-aiohttp**.

- CVE-2024-27351 – potential ReDoS in **django.utils.text.Truncator.words()**.

  - Packages updated: **automation-controller: Django**.

- CVE-2024-28219 – buffer overflow in **_imagingcms.c**.

  - Packages updated: **python3-pillow** and **python39-pillow**.

- CVE-2024-28849 – possible credential leak.

  - Packages updated: **python3-galaxy-ng: follow-redirects**, **python39-galaxy-ng: follow-redirects**, and **automation-hub: follow-redirects**.

- CVE-2024-30251 – DoS when trying to parse malformed POST requests.

- Packages updated: **python3-aiohttp**, **python39-aiohttp**, and **automation-controller: aiohttp**.

- CVE-2024-32879 - improper handling of case sensitivity in **social-auth-app-django**.

  - Packages updated: **python3-social-auth-app-django** and **python39-social-auth-app-django**.

- CVE-2024-34064 - **xmlattr** filter accepts keys containing non-attribute characters.

  - Packages updated: **python3-jinja2** and **python39-jinja2**.

- CVE-2024-35195 - additional requests to the same host ignore cert verification.

  - Packages updated: **python3-requests** and **python39-requests**.

- CVE-2024-3651 - potential DoS with resource consumption through specially crafted inputs to **idna.encode()**.

  - Packages updated: **python3-idna** and **python39-idna**.

- CVE-2024-3772 - ReDoS with a crafted email string.

  - Packages updated: **python3-pydantic**, **python39-pydantic**, and **automation-controller: python-pydantic**.

- CVE-2024-4340 - parsing a heavily nested list leads to a DoS.

  - Packages updated: **python3-sqlparse** and **python39-sqlparse**.

- CVE-2023-5752 - Mercurial configuration injection in repository revision when installing with **pip**.

  - Packages updated: **automation-controller: pip**.

8.1.1.2. Automation controller

- Fixed a Redis connection leak on automation controller version 4.5.6 (AAP-24286).

- Fixed the **#!** interpreter directive, also known as shebang, for the Python **uwsgitop** script (AAP-22461).

8.1.1.3. Automation hub

- With this update, fetching a list of users for a namespace does not include group members (AAH-3121).

- Fixed an issue that caused a "Calculated digest does not equal passed in digest" error when syncing the community repository (AAH-3111).

- Fixed an issue where syncing a **rh-certified** repository after updating automation hub to the latest version failed (AAH-3218).

8.1.1.4. Event-Driven Ansible

- Added support for the **SAFE_PLUGINS_FOR_PORT_FORWARD** setting for **eda-server** to the installation program (AAP-21620).

- With this update, **eda-server** now opens the ports for a rulebook that has a source plugin that requires inbound connections only if that plugin is allowed in the settings (AAP-17416).

- Fixed an issue where an activation could not be started after reaching a limit of 2048 pods due to a wrong cleanup of volumes (AAP-21065).

- Fixed an issue where some activations failed due a wrong cleanup of volumes (AAP-22132).

- With this release, activation-worker and worker targets now correctly stop worker services independently of other required Event-Driven Ansible services (AAP-23735).

8.1.2. RHSA-2024:1057 - Security Advisory - March 01, 2024

RHSA-2024:1057

8.1.2.1. Automation hub

- Displays the download count for each collection in automation hub (AAP-18298).

8.1.2.2. Event-Driven Ansible

- Added a parameter to control the number of running activations per Event-Driven Ansible worker service (AAP-20672).

- Added **EDA_CSRF_TRUSTED_ORIGINS**, which can be set by user input or defined based on the allowed hostnames that are determined by the installer (AAP-20244).

- Event-Driven Ansible installation now fails when the pre-existing automation controller version is 4.4.0 or older (AAP-20241).

- Added the **podman_containers_conf_logs_max_size** variable for containers.conf to control the max log size for Podman installations. The default value is 10 MiB (AAP-19775).

- Setting the Event-Driven Ansible debug flag to false now correctly disables Django debug mode (AAP-19577).

- **XDG_RUNTIME_DIR** is now defined when applying Event-Driven Ansible linger settings for Podman (AAP-19265).

- Fixed the Event-Driven Ansible nginx config when using a custom https port (AAP-19137).

- Some features in this release are classified as Developer Preview, including LDAP authentication functionality for Event-Driven Ansible. For more information about these Event-Driven Ansible Developer Preview features, see Event-Driven Ansible - Developer Preview .

8.1.3. RHSA-2024:0733 - Security Advisory - February 07, 2024

RHSA-2024:0733

8.1.3.1. Automation controller

- Fixed an error that caused **rsyslogd** to stop sending events to Splunk HTTP Collector (AAP-19069).

8.1.3.2. Automation hub

- Automation hub now uses system crypto-policies in nginx (AAP-18974).

8.1.3.3. Event-Driven Ansible

- Fixed an error that caused a manual installation failure when pinning Event-Driven Ansible to an older version (AAP-19399).

8.1.3.4. Related RPM and container releases for bundle installer

- RHSA-2024:0322

- RHBA-2023:7863

8.1.4. RHBA-2024:0104 - Bug Fix Advisory - January 11, 2024

RHBA-2024:0104

8.1.4.1. General

- Fixed conditional code statements to align with changes from ansible-core issue #82295 (AAP-19099).

- Fixed an issue which caused the **update-ca-trust** handler to be skipped for execution nodes in controller (AAP-18911).

- Improved the error pages for automation controller (AAP-18840).

- Implemented **libffi** fix to avoid **uWSGI** core dumps on failed import (AAP-18196).

- Fixed an issue with checking the license type following an upgrade caused by earlier incomplete upgrade (AAP-17615).

- Postgres certificates are now temporarily copied when checking the Postgres version for SSL mode **verify-full** (AAP-15374).

8.1.4.2. Related RPM and container releases for bundle installer

- RHSA-2023:7773

- RHBA-2023:7728

- RHBA-2023:7863

8.1.5. RHBA-2023:7460 - Bug Fix Advisory - November 21, 2023

RHBA-2023:7460

8.1.5.1. General

- Fixed an error which caused the incorrect target database to be selected when restoring Event-Driven Ansible from a backup (AAP-18151).

- Postgres tasks that create users in FIPS environments now use **scram-sha-256** (AAP-17516).

- All Event-Driven Ansible services are enabled after installation is complete (AAP-17426).

- Ensure all backup and restore staged files and directories are cleaned up before running a backup or restore. You must also mark the files for deletion after a backup or restore (AAP-16101).

- Updated nginx to 1.22 (AAP-15962).

- Added a task to VMs that will run the **awx-manage** command to pre-create events table partitions before executing **pg_dump** and added a variable for the default number of hours to pre-create (AAP-15920).

8.1.5.2. Event-Driven Ansible

- Fixed the automation controller URL check when installing Event-Driven Ansible without controller (AAP-18169).

- Added a separate worker queue for Event-Driven Ansible activations to not interfere with application tasks such as project updates (AAP-14743).

8.1.5.3. Related RPM and container releases for bundle installer.

- RHSA-2023:7517

- RHBA-2023:7460

- RHBA-2023:6853

- RHBA-2023:6302

- RHBA-2023:7462

8.1.6. RHBA-2023:5347 - Bug Fix Advisory - September 25, 2023

RHBA-2023:5347

8.1.6.1. General

- The installer now properly generates a new **SECRET_KEY** for controller when running **setup.sh** with the **-k** option (AAP-15565).

- Added temporary file cleanup for Podman to prevent **cannot re-exec process** error during job execution (AAP-15248).

- Added new variables for additional nginx configurations per component (AAP-15124).

- The installer now correctly enforces only one Event-Driven Ansible host per Ansible Automation Platform installation (AAP-15122).

- You are now able to sync execution environment images in automation hub to automation controller on upgrade (AAP-15121).

- **awx** user configuration now supports rootless Podman (AAP-15072).

- You can now mount the **/var/lib/awx** directory as a separate filesystem on execution nodes (AAP-15065).

- Fixed the linger configuration for an Event-Driven Ansible user (AAP-14745).

- Fixed the values used for signing installer managed certificates for internal postgres installations (AAP-14236).

- Subject alt names for component hosts will now only be checked for signing certificates when https is enabled (AAP-14235).

- Fixed postgres sslmode for **verify-full** that affected external postgres and postgres signed for 127.0.0.1 for internally managed postgres (AAP-13962).

- Updated the inventory file to include SSL key and cert parameters for provided SSL web certificates (AAP-13854).

- Fixed an issue with the **awx-rsyslogd** process where it starts with the wrong user (AAP-13664).

- Fixed an issue where the restore process failed to stop **pulpcore-worker** services on RHEL 9 (AAP-13297).

- Podman configurations are now correctly aligned to the Event-Driven Ansible home directory (AAP-13289).

8.1.6.2. Related RPM and container releases for bundle installer

- RHSA-2023:5208

- RHBA-2023:5271

- RHBA-2023:5316

8.2. INSTALLER RELEASES

Table 8.2. Component versions per installation bundle

Installation bundle	Component versions
2.4-7 June 12, 2024	**ansible-automation-platform-setup** 2.4-7 **ansible-core** 2.15.11 - Automation controller 4.5.7 - Automation hub 4.9.2 - Event-Driven Ansible 1.0.7

8.2.1. RHBA-2024:3871 - bundle installer release 2.4-7 - June 12, 2024

RHBA-2024:3871

8.2.1.1. Related RPM releases

- RHSA-2024:3781 - Security Advisory - June 10, 2024

8.2.1.2. Related container releases

- RHBA-2024:3782 - Bug Fix Advisory - June 10, 2024

8.2.2. RHBA-2024:2074 - bundle installer release 2.4-6.2 - April 25, 2024

RHBA-2024:2074

8.2.2.1. General

- Resolved a race condition that occurred when there were many nearly simultaneous uploads of the same collection. (AAH-2699)

8.2.2.2. Automation controller

- Fixed a database connection leak that occurred when the **wsrelay** main **asyncio** loop crashes. (AAP-22938)

8.2.3. RHBA-2024:1672 - bundle installer release 2.4-6.1 - April 4, 2024

RHBA-2024:1672

8.2.3.1. General

- Fixed an issue where worker nodes became unavailable and stuck in a running state (AAP-21828).

- automation-controller: axios: Exposure of confidential data stored in cookies (CVE-2023-45857)

- python-django: Potential regular expression denial-of-service in **django.utils.text.Truncator.words()** (CVE-2024-27351)

- receptor: golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads (CVE-2024-1394)

- automation-controller: python-aiohttp: HTTP request smuggling (CVE-2024-23829)

- python-aiohttp: HTTP request smuggling (CVE-2024-23829)

- automation-controller: aiohttp: **follow_symlinks** directory traversal vulnerability (CVE-2024-23334)

- python3x-aiohttp: aiohttp: **follow_symlinks** directory traversal vulnerability (CVE-2024-23334)

- python-aiohttp: aiohttp: **follow_symlinks** directory traversal vulnerability (CVE-2024-23334)

- automation-controller: Django: denial of service in **intcomma** template filter (CVE-2024-24680)

- automation-controller: jinja2: HTML attribute injection when passing user input as keys to **xmlattr** filter (CVE-2024-22195)

- automation-controller: python-cryptography: NULL-dereference when loading PKCS7 certificates (CVE-2023-49083)

- receptor: golang: net/http/internal: Denial of service by resource consumption through HTTP requests (CVE-2023-39326)

- automation-controller: python-aiohttp: Issues in HTTP parser with header parsing (CVE-2023-47627)

- automation-controller: GitPython: Blind local file inclusion (CVE-2023-41040)

- automation-controller: python-twisted: Disordered HTTP pipeline response in **twisted.web** (CVE-2023-46137)

8.2.3.2. Automation controller

- The update execution environment image no longer fails with jobs that use the previous image (AAP-21733).

- Replaced string validation of English literals with error codes to allow for universal validation and comparison (AAP-21721).

- The dispatcher now appropriately ends child processes when the dispatcher terminates (AAP-21049).

- Fixed a bug where schedule prompted variables and survey answers were reset in edit mode when changing one of the basic form fields (AAP-20967).

- The upgrade from Ansible Tower 3.8.6 to Ansible Automation Platform 2.4 no longer fails after a database schema migration (AAP-19738).

- Fixed a bug in OpenShift Container Platform deployments that caused the controller task container to restart (AAP-21308).

8.2.4. RHBA-2024:1158 - bundle installer release 2.4-6 - March 6, 2024

RHBA-2024:1158

8.2.4.1. General

- python-django: Django: denial-of-service in intcomma template filter (CVE-2024-24680)

- pycryptodomex: pycryptodome: Side-channel leakage for OAEP decryption in PyCryptodome and pycryptodomex (CVE-2023-52323)

- python-pygments: pygments: ReDoS in pygments (CVE-2022-40896)

- python3x-jinja2: jinja2: HTML attribute injection when passing user input as keys to xmlattr filter (CVE-2024-22195)

- python-jinja2: jinja2: HTML attribute injection when passing user input as keys to xmlattr filter (CVE-2024-22195)

- python3x-aiohttp: CRLF injection if user controls the HTTP method using aiohttp client (CVE-2023-49082)

- python-aiohttp: aiohttp: CRLF injection if user controls the HTTP method using aiohttp client (CVE-2023-49082)

- python3x-aiohttp: aiohttp: HTTP request modification (CVE-2023-49081)

- python-aiohttp: aiohttp: HTTP request modification (CVE-2023-49081)

- python3x-aiohttp: python-aiohttp: Issues in HTTP parser with header parsing (CVE-2023-47627)

- python-aiohttp: Issues in HTTP parser with header parsing (CVE-2023-47627)

- python3x-pillow: python-pillow: Uncontrolled resource consumption when text length in an **ImageDraw** instance operates on a long text argument (CVE-2023-44271)

- python-pillow: Uncontrolled resource consumption when text length in an **ImageDraw** instance operates on a long text argument (CVE-2023-44271)

8.2.4.2. Event-Driven Ansible

- event_driven: Ansible Automation Platform: Insecure WebSocket used when interacting with Event-Driven Ansible server (CVE-2024-1657).

8.2.5. RHBA-2023:6831 - bundle installer release 2.4-2.4 - November 08, 2023

RHBA-2023:6831

8.2.5.1. General

- python3-urllib3/python39-urllib3: Cookie request header is not stripped during cross-origin redirects (CVE-2023-43804)

8.2.5.2. Automation controller

- automation-controller: Django: Denial-of-service possibility in django.utils.text.Truncator (CVE-2023-43665)

- Customers using the **infra.controller_configuration** collection (which uses **ansible.controller** collection) to update their Ansible Automation Platform environment no longer receive an HTTP 499 response (AAP-17422).

8.2.6. RHBA-2023:5886 - bundle installer release 2.4-2.3 - October 19, 2023

RHBA-2023:5886

8.2.6.1. General

- receptor: golang: net/http, x/net/http2: rapid stream resets can cause excessive work (CVE-2023-44487) (CVE-2023-39325)

- receptor: golang: crypto/tls: slow verification of certificate chains containing large RSA keys (CVE-2023-29409)

8.2.6.2. Automation controller

- receptor: HTTP/2: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack) (CVE-2023-44487)

8.2.7. RHBA-2023:5812 - bundle installer release 2.4-2.2 - October 17, 2023

RHBA-2023:5812

8.2.7.1. General

- ansible-core: malicious role archive can cause ansible-galaxy to overwrite arbitrary files (CVE-2023-5115)

- python3-django/python39-django: Denial-of-service possibility in django.utils.text.Truncator (CVE-2023-43665)

8.2.7.2. Automation controller

- Added a new **Subscription Usage** page to the controller UI to view historical usage of licenses (AAP-16983).

- automation-controller: Django: Potential denial of service vulnerability in django.utils.encoding.uri_to_iri() (CVE-2023-41164)

8.2.8. RHBA-2023:5653 - bundle installer release 2.4-2.1 - October 10, 2023

RHBA-2023:5653

8.2.8.1. General

- Updated ansible-lint to include an offline mode, which is enabled by default, to prevent outbound network calls (AAH-2606).

8.2.8.2. Automation controller

- Fixed settings lookup to no longer leave some services in a **supervisord FATAL** unresponsive state (AAP-16460).

- Replaced the SQL commands for creating a partition with the use of **ATTACH PARTITION** to avoid exclusive table lock on event tables (AAP-16350).

- Fixed settings to allow simultaneous use of **SOCIAL_AUTH_SAML_ORGANIZATION_ATTR** and **SOCIAL_AUTH_SAML_ORGANIZATION_MAP** for a given organization (AAP-16183).

- Fixed Content Security Policy (CSP) to enable Pendo retrieval (AAP-16057).

- Updated the Thycotic DevOps Secrets Vault credential plugin to allow for filtering based on **secret_field** (AAP-15695).

8.2.9. RHBA-2023:5140 - bundle installer release 2.4-1.4 - September 12, 2023

RHBA-2023:5140

8.2.9.1. Automation controller

- Fixed a bug that caused a deadlock on shutdown when Redis was unavailable (AAP-14203).

- The login form no longer supports autocomplete on the password field due to security concerns (AAP-15545).

- automation-controller: cryptography: memory corruption via immutable objects (CVE-2023-23931)

- automation-controller: GitPython: Insecure non-multi options in clone and clone_from is not blocked (CVE-2023-40267)

- python3-gitpython/python39-gitpython: Insecure non-multi options in clone and clone_from is not blocked (CVE-2023-40267)

8.2.10. RHBA-2023:4782 - bundle installer release 2.4-1.3 - August 28, 2023

RHBA-2023:4782

8.2.10.1. Automation controller

- automation-controller: python-django: Potential regular expression denial of service vulnerability in EmailValidator/URLValidator (CVE-2023-36053)

- automation-controller: python-django: Potential denial-of-service vulnerability in file uploads (CVE-2023-24580)

- Changing credential types by using the drop-down list in the **Launch prompt** window no longer causes the screen to disappear (AAP-11444).

- Upgraded python dependencies which include upgrades from Django 3.2 to 4.2.3, psycopg2 to psycopg3, and additional libraries as needed. Also added a new setting in the UI exposing the **CSRF_TRUSTED_ORIGIN** settings (AAP-12345).

- Fixed slow database UPDATE statements on the job events table which could cause a task manager timeout (AAP-12586).

- Fixed an issue where adding a new label to a job through the **Prompt On Launch** option would not add the label to the job details (AAP-14204).

- Added **noopener** and **noreferrer** attributes to controller UI links that were missing these attributes (AAP-14345).

- Fixed the broken **User Guide** link in the **Edit Subscription Details** page (AAP-14375).

- Turned off auto-complete on the remaining controller UI forms that were missing that attribute (AAP-14442).

- The **Add** button on the credentials page is now accessible for users with the correct permissions (AAP-14525).

- Fixed an unexpected error that occurred when adding a new host while using a manifest with size 10 (AAP-14675).

- Applied environment variables from the **AWX_TASK_ENV** setting when running credential lookup plugins (AAP-14683).

- Interrupted jobs (such as canceled jobs) no longer clear facts from hosts if the job ran on an execution node (AAP-14878).

- Using a license that is missing a **usage** attribute no longer returns a 400 error (AAP-14880).

- Fixed sub-keys under **data** from HashiCorp Vault Secret Lookup responses to check for secrets, if found (AAP-14946).

- Fixed Ansible facts to retry saving to hosts if there is a database deadlock (AAP-15021).

8.2.10.2. Event-Driven Ansible

- automation-eda-controller: token exposed at importing project (CVE-2023-4380)

- python3-cryptography/python39-cryptography: memory corruption via immutable objects (CVE-2023-23931)

- python3-requests/python39-requests: Unintended leak of Proxy-Authorization header (CVE-2023-32681)

- Contributor and editor roles now have permissions to access users and set the AWX token (AAP-11573).

- The onboarding wizard now requests controller token creation (AAP-11907).

- Corrected the filtering capability of the **Rule Audit** screens so that a search yields results with the **starts with** function (AAP-11987).

- Enabling or disabling rulebook activation no longer increases the restarts counter by 1 (AAP-12042).

- Filtering by a text string now displays all applicable items in the UI, including those that are not visible in the list at that time (AAP-12446).

- Audit records are no longer missing when running activations with multiple jobs (AAP-12522).

- The event payload is no longer missing key attributes when a job template fails (AAP-12529).

- Fixed the Git token leak that occurs when importing a project fails (AAP-12767).

- The restart policy in Kubernetes (k8s) now restarts a successful activation that is incorrectly marked as failed (AAP-12862).

- Activation statuses are now reported correctly, whether you are disabling or enabling them (AAP-12896).

- When the **run_job_template** action fails, ansible-rulebook prints an error log in the activation output and creates an entry in rule audit so the user is alerted that the rule has failed (AAP-12909).

- When a user tries to bulk delete rulebook activations from the list, the request now completes successfully and consistently (AAP-13093).

- The **Rulebook Activation** link now functions correctly in the **Rule Audit Detail** UI (AAP-13182).

- The ansible-rulebook now only connects to the controller if the rulebook being processed has a **run_job_template** action (AAP-13209).

- Fixed a bug where some audit rule records had the wrong rulebook link (AAP-13844).

- Fixed a bug where only the first 10 audit rules had the right link (AAP-13845).

- Before this update, project credentials could not be updated if there was a change to the credential used in the project. With this update, credentials can be updated in a project with a new or different credential (AAP-13983).

- The **User Access** section of the navigation panel no longer disappears after creating a decision environment (AAP-14273).

- Fixed a bug where filtering for audit rules did not work properly on OpenShift Container Platform (AAP-14512).

8.2.11. RHBA-2023:4621 – bundle installer release 2.4-1.2 – August 10, 2023

RHBA-2023:4621

8.2.11.1. Automation controller

- automation controller: Html injection in custom login info (CVE-2023-3971)

- Organization admin users are no longer shown an error on the Instances list (AAP-11195).

- Fixed the workflow job within the workflow approval to display the correct details (AAP-11433).

- Credential name search in the ad hoc commands prompt no longer requires case-sensitive input (AAP-11442).

- The **Back to list**button in the controller UI now maintains previous search filters (AAP-11527).

- **Topology view** and **Instances** are only available as sidebar menu options to System Administrators and System Auditors (AAP-11585).

- Fixed the frequency of the scheduler to run on the correct day of the week as specified by the user (AAP-11776).

- Fixed an issue with slow database UPDATE statements when using nested tasks (include_tasks) causing task manager timeout (AAP-12586).

- Added the ability to add execution and hop nodes to VM-based controller installations from the UI (AAP-12849).

- Added the **awx-manage** command for creating future events table partitions (AAP-12907).

- Re-enabled Pendo support by providing the correct Pendo API key (AAP-13415).

- Added the ability to filter teams by using partial names in the dialog for granting teams access to a resource (AAP-13557).

- Fixed a bug where a weekly rrule string without a BYDAY value would result in the UI throwing a TypeError (AAP-13670).

- Fixed a server error that happened when deleting workflow jobs ran before event partitioning migration (AAP-13806).

- Added API reference documentation for the new bulk API endpoint (AAP-13980).

- Fixed an issue where related items were not visible in some cases. For example, job template instance groups, organization galaxy credentials, and organization instance groups (AAP-14057).

8.2.12. RHBA-2023:4288 - bundle installer release 2.4-1.1 - July 26, 2023

RHBA-2023:4288

8.2.12.1. Automation hub

- Fixed issue by using **gpg** key with passphrase for signing services (AAH-2445).