Red Hat Ansible Automation Platform 2.4

Red Hat Ansible Automation Platform 发行注记

新功能、功能增强和程序错误修复信息

Last Updated: 2024-06-29

Red Hat Ansible Automation Platform 2.4 Red Hat Ansible Automation Platform 发行注记

新功能、功能增强和程序错误修复信息

法律通告

摘要

本指南概述了 Red Hat Ansible Automation Platform 的新功能、功能增强和程序错误修复信息。

目录

对红帽文档提供反馈

如果您对本文档有任何改进建议，或发现了任何错误，请通过 https://access.redhat.com 联系技术支持，以使用 **docs-product** 组件在 Ansible Automation Platform JIRA 项目中创建一个问题。

第 1 章 RED HAT ANSIBLE AUTOMATION PLATFORM 概述

Red Hat Ansible Automation Platform 简化了用于管理企业应用程序基础架构生命周期的自动化工作负载的开发和操作。Ansible Automation Platform 可以在多个 IT 域间工作，包括操作、网络、安全性和跨不同混合环境。Ansible Automation Platform 易于采用、使用和理解，它提供了快速实施企业级自动化所需的工具，无论您处于自动化流程中的什么位置。

1.1. ANSIBLE AUTOMATION PLATFORM 中包含的内容

Ansible Automation Platform	自动化控制器	Automation hub	Event-Driven Ansible 控制器	Insights for Ansible Automation Platform
2.4	4.4	• 4.7 • 托管的服务	1.0	托管的服务

1.2. RED HAT ANSIBLE AUTOMATION PLATFORM 生命周期

红帽为每个 Ansible Automation Platform 发行版本提供不同的维护级别。如需更多信息，请参阅 Red Hat Ansible Automation Platform 生命周期。

1.3. 升级 ANSIBLE AUTOMATION PLATFORM

升级时，请勿使用 **yum update**。使用安装程序替代。安装程序执行升级到最新版本的 Ansible Automation Platform 所需的所有操作，包括自动化控制器和私有自动化中心。

其他资源

- 有关 Ansible Automation Platform 中包含的组件的详情，请查看 Ansible Automation Platform 中包含的 表。
- 有关升级 Ansible Automation Platform 的更多信息，请参阅 Red Hat Ansible Automation Platform 升级和迁移指南。
- 有关使用 Ansible Automation Platform 安装程序的步骤，请参阅 Ansible Automation Platform 安装指南。

第 2 章 ANSIBLE AUTOMATION PLATFORM 2.4 发行版本概述

2.1. 新功能及功能增强

Ansible Automation Platform 2.4 包括以下改进：

- 在以前的版本中，执行环境容器镜像只基于 RHEL 8。使用 Ansible Automation Platform 2.4 以后，执行环境容器镜像现在包括在 RHEL 9 中。执行环境包括以下容器镜像：
  - ansible-python-base
  - ansible-python-toolkit
  - ansible-builder
  - ee-minimal
  - ee-supported
- ansible-builder 项目最近发布了 Ansible Builder 版本 3，这是创建执行环境的一种改进和简化的方法。您可以在 Ansible Builder 版本 3 中使用以下配置 YAML 密钥：
  - additional_build_files
  - additional_build_steps
  - build_arg_defaults
  - dependencies
  - images
  - 选项
  - version
- Ansible Automation Platform 2.4 及更新的版本现在可以在 ARM 平台上运行，包括 control plane 和执行环境。
- 如果需要从默认值中更改，添加了用于自动化中心的 SSO 注销 URL 的选项。
- 将 ansible-lint RPM 软件包更新至 6.14.3 版本。
- 更新了 Django 以在文件上传中潜在的拒绝服务漏洞(CVE-2023-24580)。
- 针对 ReDOS 漏洞更新了 sqlparse (CVE-2023-30608)。
- 更新了 Django for potential denial-of-service in Accept-Language 标头(CVE-2023-23969)。
- Ansible Automation Platform 2.4 添加了在 IBM Power (ppc64le)、IBM Z (s390x)和 IBM® LinuxONE (s390x)架构上安装自动化控制器、自动化中心和 Event-Driven Ansible 的功能。

其他资源

- 有关使用 Ansible Builder 版本 3 的更多信息，请参阅 Ansible Builder 文档 和执行环境设置参考。

2.2. 技术预览

技术预览功能可让用户早期访问将来的产品功能，让用户在开发过程中测试并提供反馈。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

以下是技术预览功能：

- 从 Ansible Automation Platform 2.4 开始，通过将 YAML 应用到 OpenShift 集群，可以使用 Platform Resource Operator 在自动化控制器中创建以下资源：
  - 清单
  - 项目
  - 实例组
  - 凭证
  - 调度
  - 工作流任务模板
  - 启动工作流

现在，您可以使用 **connection_secret** 参数而不是 **tower_auth_secret** 参数为每个资源配置 Controller Access Token。这个更改与早期版本兼容，但 **tower_auth_secret** 参数现已弃用，并将在以后的发行版本中删除。

其他资源

- 有关技术预览功能的最新列表，请参阅 Ansible Automation Platform - 技术预览功能 。
- 如需有关在 OpenShift 部署上执行节点增强的详情，请参阅使用实例管理容量。

2.3. 弃用和删除的功能

弃用的功能仍然包含在 Ansible Automation Platform 中，并被支持。但是，这个功能将在以后的 Ansible Automation Platform 发行版本中删除，且不建议在新部署中使用。

Ansible Automation Platform 2.4 中已弃用并删除以下功能：

- 内部组件自动化服务目录现在从 Ansible Automation Platform 2.4 开始中删除。
- 在 Ansible Automation Platform 2.4 发行版本中，Ansible 2.9 的执行环境容器镜像(**ee-29-rhel-8**)默认不再加载到自动化控制器配置中。
- 虽然您仍然可以同步内容，但使用同步列表已弃用，并将在以后的版本中删除。相反，私有自动化中心管理员可以从 **rh-certified** remote 中上传手动创建的要求文件。
- 现在，您可以使用 **connection_secret** 参数而不是 **tower_auth_secret** 参数为每个资源配置 Controller Access Token。这个更改与早期版本兼容，但 **tower_auth_secret** 参数现已弃用，并将在以后的发行版本中删除。
- 智能清单已弃用，而是使用构建的清单，并将在以后的发行版本中删除。

2.4. 程序错误修复

Ansible Automation Platform 2.4 包括以下程序错误修复：

- 更新了安装程序，以确保在没有启用集合签名服务的情况下无法启用集合自动签名。
- 修复了在安装的自动化控制器版本与备份版本不同时恢复备份的问题。
- 修复了没有将用户定义的 galaxy-importer 设置添加到 **galaxy-importer.cfg** 文件中的问题。
- 在 nginx 日志中添加了缺少的 **X-Forwarded-For** 标头信息。
- 当 IP 地址用作名称时，删除了不必要的 receptor peer 名称验证。
- 更新了捆绑包安装程序中包含的 过时的 **base_packages.txt** 文件。
- 修复了升级 Ansible Automation Platform 默认不会更新 nginx 软件包的问题。
- 修复了在执行节点上没有创建 **awx** 组的情况下创建 **awx** 用户的问题。
- 修复了软件包版本变量的分配，以用于平面文件清单。
- 添加了运行 Skopeo 命令所需的自动化中心主机名的 FQDN 检查。
- 修复了 Red Hat Single Sign On (SSO)的前端 URL，以便在指定 **sso_redirect_host** 变量后正确配置。
- 修复了所有组件 **nginx_tls_files_remote** 变量的变量优先级。
- 修复了 **setup.sh** 脚本，以便在安装 Ansible Automation Platform 需要时升级特权。
- 修复了在将备份恢复到具有不同主机名的自动化中心时的问题。

第 3 章 自动化控制器

自动化控制器通过增加控制、知识、协调基于 Ansible 的环境，帮助团队管理复杂的多层部署。

如需了解新功能和功能增强的完整列表，请参阅 4.x 的自动化控制器发行注记。

第 4 章 EVENT-DRIVEN ANSIBLE

Event-Driven Ansible 是一种新方法，通过提高 IT 速度和灵活性来增强和扩展自动化，同时实现一致性和弹性。Event-Driven Ansible 专为简洁性和灵活性而设计。

已知问题

- 贡献者和编辑器角色无法设置 AWX 令牌。只有具有管理员角色的用户才能设置 AWX 令牌。
- activation-job pod 没有请求限制。
- join 向导不会请求控制器令牌创建。
- 用户无法通过 **Controller Token** 选项卡下的令牌列表进行过滤。
- 只有具有管理员权限的用户才能设置或更改其密码。
- 如果失败，重启策略设置为 **Always** 的激活无法重启失败的激活。
- 禁用并启用激活会导致重启计数增加。这个行为会导致 **重启** 计数不正确。
- 您必须使用内存限制运行 Podman pod。
- 即使只使用第一个 AWX 令牌，用户可以添加多个令牌。
- 创建和快速删除激活时出现竞争条件会导致错误。
- 当用户过滤任何列表时，只会过滤列表上的项目。
- 当持续激活启动多个作业时，不会在审计日志中记录几个作业。
- 当作业模板失败时，事件有效负载中缺少几个关键属性。
- Kubernetes 部署中重启策略不会重启标记为失败的成功激活。
- 为禁用或启用的激活报告不正确的状态。
- 如果 **run_job_template** 操作失败，则该规则不会被计算为执行。
- RHEL 9.2 激活无法连接到主机。
- 重启 Event-Driven Ansible 服务器可能会导致激活状态过时。
- 批量删除规则手册激活列表不一致，删除操作可能会成功或失败。
- 当用户访问规则审计的详细信息屏幕时，相关的规则手册激活链接将被破坏。
- 长时间运行事件负载的激活可能会导致磁盘空间不足。在安装程序发行版本 2.4-6 中解决。
- 事件键不支持某些字符，如连字符 (-)、正斜杠 (/) 和句点 (.)。在安装程序版本 2.4-3 中解决。
- 当激活超过可用 worker 时，禁用激活会错误地显示它们处于运行状态。在安装程序版本 2.4-3 中解决。
- Event-Driven Ansible 激活 pod 在 RHEL 9 上运行内存不足。在安装程序版本 2.4-3 中解决。

- 当所有 worker 忙碌激活进程时，不会执行其他异步任务，如导入项目。在安装程序版本 2.4-3 中解决。

第 5 章 AUTOMATION HUB

通过自动化中心，您可以从 Red Hat Ansible 和认证合作伙伴发现并使用新的认证自动化内容，如 Ansible Collections。

新功能及功能增强

- 此自动化中心发行版本提供存储库管理功能。通过存储库管理，您可以在存储库之间创建、编辑、删除和移动内容。

程序错误修复

- 修复了 collection 关键字搜索中返回一个错误的结果数的问题。
- 添加了为 LDAP 设置 **OPT_REFERRALS** 选项的功能，以便用户现在可以使用其 LDAP 凭据成功登录到自动化中心。
- 修复了当 **redhat.openshift** 集合的核心依赖项抛出 **404 Not Found** 错误时，UI 中的错误。
- 修复了一个错误，以便在与 **registry.redhat.io** 同步时跳过已弃用的执行环境。

第 6 章 AUTOMATION PLATFORM OPERATOR

Ansible Automation Platform Operator 在 OpenShift 环境中提供新的 Ansible Automation Platform 实例的云原生、按钮式部署。

程序错误修复

- 为自动化控制器 **init** 容器启用资源要求配置。
- 为 Event-Driven Ansible Operator 部署添加了 **securityContext**，以兼容 Pod Security Admission。
- 解决的错误 **控制器：在进行批量更新时，错误 413 Entity 太大**。
- Ansible 令牌现在在 YAML 作业详情中模糊处理。

第 7 章 ANSIBLE AUTOMATION PLATFORM 文档

Red Hat Ansible Automation Platform 2.4 文档包括重要的功能更新以及文档改进，并提供更好的用户体验。

新功能及功能增强

- 从 Ansible Automation Platform 2.4 开始删除了内部组件自动化服务目录后，所有自动服务目录文档都会从 Ansible Automation Platform 2.4 文档中删除。
- 以下文档是帮助您安装和使用 Event-Driven Ansible (Ansible Automation Platform 的最新功能)：
  - Event-Driven Ansible 入门
  - 事件驱动器 Ansible 用户指南

此外，Ansible Automation Platform 规划指南 和 Ansible Automation Platform 安装指南的章节 已更新，以包含规划和安装 Event-Driven Ansible 的说明。

- Automation hub 文档有显著的重新组织，将发布在 9 个独立文档中的内容组合到以下文档中：

  Automation hub 入门

  使用本指南执行使用 Red Hat Automation Hub 作为 Ansible 集合内容的默认源所需的初始步骤。

  管理自动化 hub 中的内容

  使用本指南了解如何在 Automation Hub 中创建和管理集合、内容和存储库。

  Red Hat Ansible Automation Platform 安装指南

  使用本指南来了解如何根据支持的安装场景安装 Ansible Automation Platform。

- *Automation Hub 指南中的管理红帽认证的集合和 Ansible Galaxy 集合* 已移到 Automation *Hub 指南中的红帽认证、验证和 Ansible Galaxy 内容 文档中*。
- Ansible Automation Platform 2.4 发行注记被重组，以改进我们的客户和 Ansible 社区的体验。用户现在可以根据 Ansible Automation Platform 版本查看最新的更新，而不是根据版本时间表查看最新的更新。
- 创建使用 自动化中心的主题仓库管理，以帮助您在自动化中心中创建和管理自定义存储库。本主题包括在 *Automation hub 指南中的管理内容*。

第 8 章 异步更新

Ansible Automation Platform 2.4 的安全更新、程序错误修正、功能增强更新将会以异步勘误的形式发布。所有 Ansible Automation Platform 勘误都包括在客户门户网站的 Download Red Hat Ansible Automation Platform 页面中。

作为红帽客户门户网站用户，您可以在 Red Hat Subscription Management (RHSM)的帐户设置中启用勘误通知。当勘误通知被启用后，每当您注册的系统相关的勘误发行时，您会收到电子邮件通知。

注意

红帽客户门户网站用户帐户必须注册并消耗 Ansible Automation Platform 权利，以便生成 Ansible Automation Platform 勘误通知电子邮件。

发行注记的 Asynchronous updates 部分的内容将会持续更新，以提供 Ansible Automation Platform 2.4 的异步勘误信息。

其他资源

- 如需有关 Ansible Automation Platform 中异步勘误支持的更多信息，请参阅 Red Hat Ansible Automation Platform 生命周期。
- 有关常见漏洞和暴露(CVE)的详情，请查看 什么是 CVE？ 和 Red Hat CVE 数据库。

8.1. RPM 发行版本

表 8.1. 每个勘误公告的组件版本

勘误公告	组件版本
RHSA-2024:3781 2024 年 6 月 10 日	• **ansible-automation-platform-installer** 2.4-7 • **ansible-automation-platform-setup** 2.4-7 • **ansible-core** 2.15.11 • 自动化控制器 4.5.7 • Automation hub 4.9.2 • event-Driven Ansible 1.0.7

8.1.1. RHSA-2024:3781 - 安全公告 - 2024 年 6 月 10 日

RHSA-2024:3781

8.1.1.1. General

- 将 **automation-controller-cli** 软件包添加到 **ansible-developer** RPM 存储库(AAP-23368)。

在这个版本中，解决了以下 CVE：

- CVE-2023-45288 - 无限数量的 CONTINUATION 帧会导致拒绝服务(DoS)。

    - 软件包已更新： **receptor: golang: net/http, x/net/http2**.

- CVE-2023-45290 - **Request.ParseMultipartForm** 中的内存耗尽。
    - 软件包已更新： **receptor: golang: net/http**.
- CVE-2023-49083 - 加载 PKCS7 证书时 null-pointer dereference。
    - 软件包已更新： **python3-cryptography** 和 **python39-cryptography**.
- CVE-2023-50447 - 使用 environment 参数执行任意代码。
    - 软件包已更新： **python3-pillow** 和 **python39-pillow**.
- CVE-2024-1135 - HTTP 请求交换，因为未验证 Transfer-Encoding 标头。
    - 软件包已更新： **python3-gunicorn** 和 **python39-gunicorn**。
- CVE-2024-21503 - 在 string **.py** 文件中带有 lines_with_leading_tabs_expanded （） **函数的 lines_with_leading_tabs_expanded** （） 函数的正则表达式拒绝服务(ReDoS)。
    - 软件包已更新： **python3-black** 和 **python39-black**.
- CVE-2024-24783 - 验证带有未知公钥算法的证书上的 panics。
    - 软件包更新： **receptor: golang: crypto/x509**.
- CVE-2024-26130 - 当使用不匹配证书和私钥和 **hmac_hash** 覆盖调用时，使用 **pkcs12.serialize_key_and_certificates** 调用的 NULL 指针解引用。
    - 软件包已更新： **python3-cryptography** 和 **python39-cryptography**.
- CVE-2024-27306 - 在用于静态文件处理的索引页面上的跨站点脚本(XSS)
    - 软件包已更新： **python3-aiohttp** 和 **python39-aiohttp**。
- CVE-2024-27351 - **django.utils.text.Truncator.words （）** 中潜在的 ReDoS。
    - 软件包已更新： **automation-controller: Django**.
- CVE-2024-28219 - **_imagingcms.c** 中的缓冲区溢出。
    - 软件包已更新： **python3-pillow** 和 **python39-pillow**.
- CVE-2024-28849 - 可能的凭证泄漏。
    - 软件包已更新： **python3-galaxy-ng: follow-redirects**,**python39-galaxy-ng: follow-redirects**, 和 **automation-hub: follow-redirects**.
- CVE-2024-30251 - 当尝试解析不正确的 POST 请求时，DoS。
    - 软件包已更新： **python3-aiohttp**,**python39-aiohttp**, 和 **automation-controller: aiohttp**.
- CVE-2024-32879 - 在 **social-auth-app-django** 中处理大小不当。
    - 软件包已更新： **python3-social-auth-app-django** 和 **python39-social-auth-app-django**。
- CVE-2024-34064 - **xmlattr** 过滤器接受包含非属性字符的密钥。
    - 软件包已更新： **python3-jinja2** 和 **python39-jinja2**。

- CVE-2024-35195 - 对同一主机的额外请求忽略证书验证。
  - 软件包已更新： **python3-requests** 和 **python39-requests**.
- CVE-2024-3651 - 通过特殊精心设计的输入到 **idna.encode （）** 的潜在 DoS，具有资源消耗。
  - 软件包已更新： **python3-idna** 和 **python39-idna**。
- CVE-2024-3772 - ReDoS 带有精心设计的电子邮件字符串。
  - 软件包已更新： **python3-pydantic**,**python39-pydantic**, 和 **automation-controller: python-pydantic**.
- CVE-2024-4340 - 解析大量嵌套列表会导致 DoS。
  - 软件包已更新： **python3-sqlparse** 和 **python39-sqlparse**。
- CVE-2023-5752 - 当使用 **pip** 安装时，在存储库修订中的 Mercurial 配置注入。
  - 软件包已更新： **automation-controller: pip**.

8.1.1.2. 自动化控制器

- 修复了自动化控制器版本 4.5.6 (AAP-24286)的 Redis 连接泄漏。
- 修复了 Python **uwsgitop** 脚本(AAP-22461)）的 **#!** 解释器指令（也称为 shebang）。

8.1.1.3. Automation hub

- 在这个版本中，获取命名空间的用户列表不包括组成员(AAH-3121)。
- 修复了在同步社区存储库(AAH-3111)时导致 "Calculated digest not equal passed in digest" 错误的问题。
- 修复了在将自动化中心更新到最新版本失败(AAH-3218)后同步 **rh-certified** 存储库的问题。

8.1.1.4. Event-Driven Ansible

- 向安装程序(AAP-21620)添加了对 **eda-server** 的 **SAFE_PLUGINS_FOR_PORT_FORWARD** 设置的支持。
- 在这个版本中，**eda-server** 会打开规则手册的端口，它有一个源插件，只有在设置中允许该插件时才需要入站连接(AAP-17416)。
- 修复了在达到 2048 个 pod 限制后无法启动激活的问题，因为卷清理错误(AAP-21065)。
- 修复了由于卷清理错误导致一些激活失败的问题(AAP-22132)。
- 在这个版本中，activation-worker 和 worker 目标可以正确地停止 worker 服务，与其他所需的 Event-Driven Ansible 服务(AAP-23735)独立。

8.1.2. RHSA-2024:1057 - 安全公告 - 2024 年 3 月 1 日

RHSA-2024:1057

8.1.2.1. Automation hub

- 显示自动化中心中每个集合的下载计数(AAP-18298)。

8.1.2.2. Event-Driven Ansible

- 添加了参数来控制每个 Event-Driven Ansible worker 服务(AAP-20672)的运行激活数量。
- 添加了 **EDA_CSRF_TRUSTED_ORIGINS**，它可以由用户输入设置，或者根据安装程序(AAP-20244)决定的允许的主机名定义。
- 现在，当预先存在的自动化控制器版本为 4.4.0 或更早的版本(AAP-20241)时，Event-Driven Ansible 安装会失败。
- 为 containers.conf 添加了 **podman_containers_conf_logs_max_size** 变量，以控制 Podman 安装的最大日志大小。默认值为 10 MiB (AAP-19775)。
- 将 Event-Driven Ansible debug 标志设置为 false 现在可以正确地禁用 Django 调试模式(AAP-19577)。
- 现在，在为 Podman 应用 Event-Driven Ansible linger 设置时，会定义 **XDG_RUNTIME_DIR** (AAP-19265)。
- 修复了在使用自定义 https 端口(AAP-19137)时的 Event-Driven Ansible nginx 配置的问题。
- 这个版本中的一些功能被归类为开发者预览，包括 Event-Driven Ansible 的 LDAP 身份验证功能。有关这些事件驱动 Ansible 开发人员预览功能的更多信息，请参阅 Event-Driven Ansible - Developer Preview。

8.1.3. RHSA-2024:0733 - 安全公告 - 2024 年 2 月 7 日

RHSA-2024:0733

8.1.3.1. 自动化控制器

- 修复了导致 **rsyslogd** 停止向 Splunk HTTP Collector (AAP-19069)发送事件的错误。

8.1.3.2. Automation hub

- 自动化中心现在在 nginx 中使用系统加密策略(AAP-18974)。

8.1.3.3. Event-Driven Ansible

- 修复了在将 Event-Driven Ansible 固定到旧版本时导致手动安装失败的错误(AAP-19399)。

8.1.3.4. 捆绑包安装程序的相关 RPM 和容器发行版本

- RHSA-2024:0322
- RHBA-2023:7863

8.1.4. RHBA-2024:0104 - 程序错误修复公告 - 2024 年 1 月 11 日

RHBA-2024:0104

8.1.4.1. General

- 修复了条件代码语句，使其与 ansible-core issue #82295 (AAP-19099)的更改一致。
- 修复了导致为控制器中的执行节点跳过 **update-ca-trust** 处理程序的问题(AAP-18911)。
- 改进了自动化控制器的错误页面(AAP-18840)。
- 实施 **libffi** 修复，以避免在失败的导入时进行 **uWSGI** 核心转储(AAP-18196)。
- 修复了在之前未完成升级导致的升级后检查许可证类型的问题(AAP-17615)。
- 现在，当检查 Postgres 版本的 SSL 模式 **verify-full** (AAP-15374)时，postgres 证书会被临时复制。

8.1.4.2. 捆绑包安装程序的相关 RPM 和容器发行版本

- RHSA-2023:7773
- RHBA-2023:7728
- RHBA-2023:7863

8.1.5. RHBA-2023:7460 - 2023 年 11 月 21 日

RHBA-2023:7460

8.1.5.1. General

- 修复了在从备份中恢复 Event-Driven Ansible 时选择不正确的目标数据库的错误(AAP-18151)。
- 在 FIPS 环境中创建用户的 postgres 任务现在使用 **scram-sha-256** (AAP-17516)。
- 所有 Event-Driven Ansible 服务会在安装完成后启用(AAP-17426)。
- 在运行备份和恢复之前，请确保清理所有备份和恢复暂存的文件和目录。您还必须在备份或恢复后标记要删除的文件(AAP-16101)。
- 将 nginx 更新至 1.22 (AAP-15962)。
- 向虚拟机添加了一个任务，该任务将运行 **awx-manage** 命令，以在执行 **pg_dump** 前预先创建事件表分区，并为预先创建的默认小时数添加一个变量(AAP-15920)。

8.1.5.2. Event-Driven Ansible

- 修复了在在没有控制器的情况下安装 Event-Driven Ansible 时的自动化控制器 URL 检查的问题(AAP-18169)。
- 为 Event-Driven Ansible 激活添加了单独的 worker 队列，以不会影响应用程序任务，如项目更新(AAP-14743)。

8.1.5.3. 用于捆绑安装程序的相关 RPM 和容器发行版本。

- RHSA-2023:7517
- RHBA-2023:7460
- RHBA-2023:6853

- RHBA-2023:6302
- RHBA-2023:7462

8.1.6. RHBA-2023:5347 - 程序错误修复公告 - 2023 年 9 月 25 日

RHBA-2023:5347

8.1.6.1. General

- 现在，当使用 a **-k** 选项(AAP-15565)运行 **setup.sh** 时，安装程序会正确生成新的 **SECRET_KEY**。
- 添加了 Podman 的临时文件清理，以防止在作业执行过程中 **无法重新执行进程** 错误（AAP-1586]。
- 添加了每个组件的额外 nginx 配置的新变量(AAP-15overlayfs)。
- 安装程序现在可以正确地强制每个 Ansible Automation Platform 安装(AAP-15122)只强制有一个 Event-Driven Ansible 主机。
- 现在，您可以在升级时将自动化中心中的执行环境镜像同步到自动化控制器(AAP-15121)。
- **awx** 用户配置现在支持无根 Podman (AAP-15072)。
- 现在，您可以在执行节点上将 **/var/lib/awx** 目录作为单独的文件系统挂载(AAP-15065)。
- 修复了 Event-Driven Ansible 用户的 linger 配置(AAP-14745)。
- 修复了用于为内部 postgres 安装签名安装程序受管证书的值(AAP-14236)。
- 现在，只有在启用了 https 时，才会检查组件主机的主题备用名称(AAP-14235)。
- 修复了 postgres sslmode，用于对内部管理的 postgres (AAP-13962)影响 external postgres 和 postgres signed for 127.0.0.1 的问题。
- **更新了清单文件，使其包含提供的 SSL Web 证书的 SSL 密钥和证书参数(AAP-13854)。**
- **修复了 awx-rsyslogd 进程的问题，它以错误的用户(AAP-13664)开头。**
- **修复了恢复过程无法在 RHEL 9 上停止 pulpcore-worker 服务(AAP-13xdg)的问题。**
- **Podman 配置现在可以正确地与 Event-Driven Ansible 主目录(AAP-13289)保持一致。**

8.1.6.2. 捆绑包安装程序的相关 RPM 和容器发行版本

- RHSA-2023:5208
- RHBA-2023:5271
- RHBA-2023:5316

8.2. 安装程序发行版本

表 8.2. 每个安装捆绑包的组件版本

安装捆绑包	组件版本
2.4-7 ，2424 年 6 月 12 日	• **ansible-automation-platform-setup** 2.4-7 • **ansible-core** 2.15.11 • 自动化控制器 4.5.7 • Automation hub 4.9.2 • event-Driven Ansible 1.0.7

8.2.1. RHBA-2024:3871 - 捆绑包安装程序版本 2.4-7 - 2024 年 6 月 12 日

RHBA-2024:3871

8.2.1.1. 相关的 RPM 发行版本

- RHSA-2024:3781 - 安全公告 - 2024 年 6 月 10 日

8.2.1.2. 相关的容器发行版本

- RHBA-2024:3782 - 程序错误修复公告 - 2024 年 6 月 10 日

8.2.2. RHBA-2024:2074 - 捆绑包安装程序版本 2.4-6.2 - 2024 年 4 月 25 日

RHBA-2024:2074

8.2.2.1. General

- 解决了当同一集合几乎同时上传时发生的竞争条件。(AAH-2699)

8.2.2.2. 自动化控制器

- 修复了在 wsrelay 主 asyncio 循环崩溃时发生的数据库连接泄漏。(AAP-22938)

8.2.3. RHBA-2024:1672 - 捆绑包安装程序版本 2.4-6.1 - 2024 年 4 月 4 日

RHBA-2024:1672

8.2.3.1. General

- 修复了 worker 节点不可用并处于运行状态(AAP-21828)的问题。
- automation-controller: axios：公开存储在 Cookie 中的机密数据(CVE-2023-45857)
- python-django: Potential 正则表达式 denial-of-service in django.utils.text.Truncator.words （） (CVE-2024-27351)
- receptor: golang-fips/openssl: Memory leaks in code decrypting RSA payloads (CVE-2024-1394)
- automation-controller: python-aiohttp: HTTP 请求 smuggling (CVE-2024-23829)
- python-aiohttp: HTTP request smuggling (CVE-2024-23829)
- automation-controller: aiohttp: follow_symlinks 目录遍历漏洞(CVE-2024-23334)
- python3x-aiohttp: aiohttp: follow_symlinks 目录遍历漏洞(CVE-2024-23334)

- python-aiohttp: aiohttp: follow_symlinks 目录遍历漏洞(CVE-2024-23334)
- automation-controller: Django: 拒绝 intcomma 模板过滤器中的服务(CVE-2024-24680)
- Automation-controller：当将用户输入作为密钥传递给 xmlattr 过滤器时，jinja2: HTML 属性注入(CVE-2024-22195)
- automation-controller: python-cryptography: NULL-dereference when load PKCS7 certificate (CVE-2023-49083)
- receptor: golang: net/http/internal: 通过 HTTP 请求进行资源消耗(CVE-2023-39326)
- automation-controller: python-aiohttp: issues in HTTP parser with header parsing (CVE-2023-47627)
- Automationcontroller: GitPython: Blind local file inclusion (CVE-2023-41040)
- automation-controller: python-twisted: Disordered HTTP pipeline in twisted.web (CVE-2023-46137)

8.2.3.2. 自动化控制器

- 更新执行环境镜像不再会失败，并显示使用上一个镜像的作业(AAP-21733)。
- 使用错误代码替换英语文字的字符串验证，以允许通用验证和比较(AAP-21721)。
- 现在，当分配程序终止(AAP-21049)时，分配程序会正确终止子进程。
- 修复了在更改一个基本表单字段(AAP-20967)时，调度提示变量和调查答案以编辑模式重置的错误。
- 从 Ansible Tower 3.8.6 升级到 Ansible Automation Platform 2.4 不再在数据库架构迁移

后失败(AAP-19738)。

- 修复了在 OpenShift Container Platform 部署中导致控制器任务容器重启(AAP-21308)的错误。

8.2.4. RHBA-2024:1158 - 捆绑包安装程序版本 2.4-6 - 2024 年 3 月 6 日

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 decrypt in PyCryptodome and pycryptodomex (CVE-2023-52323)
- python-pygments: pygments: ReDoS in pygments (CVE-2022-40896)
- python3x-jinja2: jinja2: HTML 属性注入，当将用户输入作为密钥传递给 xmlattr 过滤器 (CVE-2024-22195)
- python-jinja2: jinja2: HTML 属性注入，当将用户输入作为密钥传递给 xmlattr 过滤器 (CVE-2024-22195)
- python3x-aiohttp: CRLF 注入，如果用户使用 aiohttp 客户端(CVE-2023-49082)控制 HTTP 方法
- python-aiohttp: aiohttp: CRLF 注入，如果用户使用 aiohttp 客户端(CVE-2023-49082)控制 HTTP 方法
- python3x-aiohttp: aiohttp: HTTP 请求修改(CVE-2023-49081)

- python-aiohttp: aiohttp: HTTP 请求修改(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: 当 ImageDraw 实例中的文本长度在长文本参数上运行时，不会控制资源消耗(CVE-2023-44271)
- python-pillow ：当 ImageDraw 实例中文本长度在长文本参数(CVE-2023-44271)上运行时，不会控制的资源消耗。

8.2.4.2. Event-Driven Ansible

- event_driven: Ansible Automation Platform：在与 Event-Driven Ansible 服务器交互时使用的不安全 WebSocket (CVE-2024-1657)。

8.2.5. RHBA-2023:6831 - 捆绑包安装程序版本 2.4-2.4 - 2023 年 11 月 8 日

RHBA-2023:6831

8.2.5.1. General

- python3-urllib3/python39-urllib3: Cookie 请求标头不会在跨原始重定向期间剥离(CVE-2023-43804)

8.2.5.2. 自动化控制器

- automation-controller: Django: Denial-of-service may in django.utils.text.Truncator (CVE-2023-43665)
- 使用 infra.controller_configuration 集合（使用 ansible.controller 集合）更新其 Ansible Automation Platform 环境的客户不再收到 HTTP 499 响应(AAP-17422)。

8.2.6. RHBA-2023:5886 - 捆绑包安装程序版本 2.4-2.3 - 2023 年 10 月 19 日

RHBA-2023:5886

8.2.6.1. General

- receptor: golang: net/http, x/net/http2: rapid stream resets may cause too work (CVE-2023-44487) (CVE-2023-39325)
- receptor: golang: crypto/tls: 验证包含大型 RSA 密钥的证书链的速度(CVE-2023-29409)

8.2.6.2. 自动化控制器

- receptor: HTTP/2：启用了多个 HTTP/2 的 Web 服务器会受到 DDoS 攻击(Rapid Reset Attack) (CVE-2023-44487)

8.2.7. RHBA-2023:5812 - 捆绑包安装程序版本 2.4-2.2 - 2023 年 10 月 17 日

RHBA-2023:5812

8.2.7.1. General

- ansible-core: malicious role archive 可能会导致 ansible-galaxy 覆盖任意文件(CVE-2023-5115)
- python3-django/python39-django: Denial-of-service may in django.utils.text.Truncator (CVE-2023-43665)

8.2.7.2. 自动化控制器

- 在控制器 UI 中添加了一个新的 Subscription Usage 页面，以查看许可证的历史使用情况 (AAP-16983)。
- automation-controller: Django: 在 django.utils.encoding.uri_to_iri （）(CVE-2023-41164中拒绝服务漏洞)

8.2.8. RHBA-2023:5653 - 捆绑包安装程序发行版本 2.4-2.1 - 2023 年 10 月 10 日

RHBA-2023:5653

8.2.8.1. General

- 更新了 ansible-lint，使其包含默认启用的离线模式，以防止出站网络调用(AAH-2606)。

8.2.8.2. 自动化控制器

- 修复了设置查找，不再使某些服务处于 supervisord FATAL 无响应状态(AAP-16460)。
- 用 ATTACH PARTITION 创建分区的 SQL 命令替换，以避免在事件表(AAP-16350)上专用表锁定。
- 修复了设置，允许为给定机构同时使用 SOCIAL_AUTH_SAML_ORGANIZATION_ATTR 和 SOCIAL_AUTH_SAML_ORGANIZATION_MAP。
- 修复了内容安全策略(CSP)以启用 Pendo retrieve (AAP-16057)。
- 更新了 Thycotic DevOps Secrets Vault 凭证插件，允许根据 secret_field (AAP-15695)进行过滤。

8.2.9. RHBA-2023:5140 - 捆绑包安装程序版本 2.4-1.4 - 2023 年 9 月 12 日

RHBA-2023:5140

8.2.9.1. 自动化控制器

- 修复了在 Redis 不可用时导致关闭时死锁的错误(AAP-14203)。
- 由于安全问题(AAP-15545)，登录表单不再支持 password 字段上的自动完成。

- Automation-controller：加密：通过不可变对象发生内存损坏(CVE-2023-23931)
- Automation-controller: GitPython: 在 clone 和 clone_from 中不安全非多选项，不会阻断(CVE-2023-40267)
- python3-gitpython/python39-gitpython: Insecure non-multi options in clone_from is not blocked (CVE-2023-40267)

8.2.10. RHBA-2023:4782 - 捆绑包安装程序版本 2.4-1.3 - 2023 年 8 月 28 日

RHBA-2023:4782

8.2.10.1. 自动化控制器

- automation-controller: python-django: 在 EmailValidator/URLValidator (CVE-2023-36053)中拒绝服务漏洞。
- automation-controller: python-django ：文件上传中的拒绝服务漏洞(CVE-2023-24580)
- 使用 Launch prompt 窗口中的下拉列表更改凭证类型不再会导致屏幕消失(AAP-11444)。
- 升级 python 依赖项，其中包括从 Django 3.2 升级到 4.2.3、psycopg2 到 psycopg3，以及其他库。另外，在 UI 中添加了一个新设置，用于公开 CSRF_TRUSTED_ORIGIN 设置(AAP-12345)。
- 修复了作业事件表上的较慢的数据库 UPDATE 语句，这可能会导致任务管理器超时(AAP-12586)。
- 修复了通过 Prompt On Launch 选项向作业添加新标签时，不会将标签添加到作业详情(AAP-14204)。
- 向控制器 UI 中添加了 noopener 和 noreferrer 属性，这些链接缺少这些属性(AAP-14345)。

- 修复了 Edit Subscription Details 页面中的 broken User Guide 链接(AAP-14375)。
- 关闭缺少了该属性的其余控制器 UI 表单的自动完成功能(AAP-14442)。
- 现在，具有正确权限的用户可以访问凭证页面中的 Add 按钮(AAP-14525)。
- 修复了在使用大小为 10 (AAP-14675)的清单时添加新主机时出现的意外错误。
- 在运行凭证查找插件时，从 AWX_TASK_ENV 设置应用环境变量(AAP-14683)。
- 如果作业在执行节点(AAP-14878)上运行，则中断作业（如已取消的作业）不再从主机清除事实。
- 使用缺少 usage 属性的许可证不再返回 400 错误(AAP-14880)。
- 修复了 HashiCorp Vault Secret Lookup 响应下的子键，以检查 secret （如果找到）(AAP-14946)。
- 修复了 Ansible 事实，以便在出现数据库死锁(AAP-15021)时重试保存到主机。

8.2.10.2. Event-Driven Ansible

- automation-eda-controller：在导入项目时公开的令牌(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)
- 贡献者和编辑器角色现在具有访问用户的权限并设置 AWX 令牌(AAP-11573)。

- 加入向导现在请求控制器令牌创建(AAP-11907)。
- 更正了 Rule Audit 屏幕的过滤功能，以便搜索结果以函数 开头 (AAP-11987)。
- 启用或禁用规则手册激活不再增加 1 的重启计数器(AAP-12042)。
- 根据文本字符串过滤现在显示所有 UI 中的适用项目，包括那些在那个时间无法在(AAP-12446)列表中可见的项目。
- 当使用多个作业(AAP-12522)运行激活时，审计记录不再缺失。
- 当作业模板失败时，事件有效负载不再缺少密钥属性(AAP-12529)。
- 修复了导入项目失败时出现的 Git 令牌泄漏(AAP-12767)。
- Kubernetes (k8s)中的重启策略现在会重启一个成功激活，该激活被错误地标记为 failed (AAP-12862)。
- 现在，无论您要禁用还是启用它们，都会正确报告激活状态(AAP-12896)。
- 当 run_job_template 操作失败时，ansible-rulebook 会在激活输出中打印错误日志，并在规则审计中创建条目，以便用户被警告规则失败(AAP-12909)。
- 当用户尝试从列表中批量删除规则手册激活时，请求现在可以成功完成并一致(AAP-13093)。
- Rulebook 激活 链接现在可以在 规则审计详情 UI (AAP-13182)中正常工作。
- 现在，如果处理的规则手册有一个 run_job_template 操作(AAP-13209)，ansible-rulebook 现在才会连接到控制器。

- 修复了一些审计规则记录错误的规则链接(AAP-13844)的错误。
- 修复了只有前 10 个审计规则具有正确的链接(AAP-13845)的错误。
- 在此次更新之前，如果项目中使用的凭证有变化，则无法更新项目凭证。在这个版本中，可以使用新的或不同的凭证(AAP-13983)）在项目中更新凭证。
- 导航面板的 User Access 部分在创建决策环境(AAP-14273)后不再消失。
- 修复了过滤审计规则无法在 OpenShift Container Platform (AAP-14512)上正常工作的错误。

8.2.11. RHBA-2023:4621 - 捆绑包安装程序版本 2.4-1.2 - 2023 年 8 月 10 日

RHBA-2023:4621

8.2.11.1. 自动化控制器

- 自动化控制器：在自定义登录信息中的 Html 注入(CVE-2023-3971)
- 机构管理员用户不再在 Instances 列表中显示错误(AAP-11195)。
- 修复了工作流批准中的工作流作业，以显示正确的详情(AAP-11433)。
- 在临时命令提示中搜索凭证名称不再需要区分大小写的输入(AAP-11442)。
- 控制器 UI 中的 Back to list 按钮现在维护以前的搜索过滤器(AAP-11527)。
- 拓扑视图 和实例仅作为 System Administrators 和 System Auditors (AAP-11585)的边栏菜单选项提供。

- 修复了调度程序的频率，以便每周的某一天由用户(AAP-11776)指定。
- 修复了在使用嵌套任务(include_tasks)导致任务管理器超时时较慢的数据库 UPDATE 语句的问题(AAP-12586)。
- 添加了从 UI 添加执行和跃点节点到基于虚拟机的控制器安装的功能(AAP-12849)。
- 添加了 awx-manage 命令，用于创建将来的事件表分区(AAP-12907)。
- 通过提供正确的 Pendo API 密钥(AAP-13415)来重新启用 Pendo 支持。
- 添加了使用对话框中的部分名称来过滤团队的功能，以授予团队对资源的访问权限(AAP-13557)。
- 修复了一个没有 BYDAY 值的每周 rrule 字符串会导致 UI 抛出 TypeError (AAP-13670)的错误。
- 修复了在事件分区迁移前删除工作流作业时出现的服务器错误(AAP-13806)。
- 添加了新批量 API 端点的 API 参考文档(AAP-13980)。
- 修复了在某些情况下无法看到相关项目的问题。例如，作业模板实例组、机构 galaxy 凭证和机构实例组(AAP-14057)。

8.2.12. RHBA-2023:4288 - 捆绑包安装程序版本 2.4-1.1 - 2023 年 7 月 26 日

RHBA-2023:4288

8.2.12.1. Automation hub

- 使用 gpg 密钥签名服务(AAH-2445)的 gpg 密钥解决了这个问题。