Enhancing Day 2 Operations with Cisco Compute and the Red Hat Ansible Automation Platform

Cisco CVD Compute Collection

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Published: September 2025



In partnership with:



© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

About the Cisco Validated Design Program

The Cisco Validated Design (CVD) program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information, go to: http://www.cisco.com/go/designzone

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Executive Summary

Organizations in every industry are looking to streamline their infrastructure management through automation. While a consistent initial deployment is critical, the advantages of Day 2 infrastructure automation for data center infrastructure include:

- **Continuous Compliance and Configuration Enforcement:** Automation ensures ongoing compliance by automatically enforcing Cisco UCS configurations, reducing manual errors and drift.
- **Improved Security Posture:** Automated firmware patching and vulnerability remediation help maintain a stronger security stance by promptly addressing risks.
- **Dynamic Resource Scaling:** Automated provisioning of UCS chassis and servers allows for flexible and efficient scaling of resources based on demand.
- **Simplified Operations:** Automation reduces manual efforts in system maintenance, scaling, security enforcement, and performance optimization, leading to more consistent and efficient management.
- **Integration with AI and Application Modernization:** Leveraging platforms like the Red Hat Ansible Automation Platform (AAP) and Cisco Intersight enables seamless operations and modernization of data center infrastructure and networking.
- **Support for DevOps Practices:** Infrastructure as Code (IaC) enables version control, automated testing, and rollback capabilities, facilitating agile and reliable infrastructure management.

These benefits collectively help organizations maintain long-term efficiency, stability, and security in their data center environments while reducing operational complexity and risk.

Cisco's compute products have always benefited from deep integrations with the Ansible Automation Platform through Ansible Certified and Ansible validated content Collections. Cisco Validated Designs (CVDs) play a crucial role in Ansible Automation and Infrastructure as Code (IaC) by providing tested, standardized, and repeatable architectures that accelerate time to value and reduce risk in deployments. The CVDs serve as foundation for implementing Infrastructure as Code with this platform by delivering pre-validated, automated blueprints that simplify and standardize the deployment and management of Cisco compute and network infrastructure, enabling agile and reliable infrastructure automation.

The extended collaboration between Red Hat and Cisco enhances existing solutions by introducing new Ansible validated content that aligns with Cisco Validated Designs for data center infrastructures. These improvements enable comprehensive automation across Day 0, Day 1, and Day 2 operations accessible through the Red Hat Ansible Automation Platform and Ansible Galaxy. The roles included in the new Ansible content deliver a seamless and efficient automation experience for customers, simplifying infrastructure management and operational workflows.

The Red Hat Ansible Automation Platform enables customer to manage and operate their IT infrastructure on a leading technology like Cisco UCS and Cisco Intersight. Our aim is to provide a robust, scalable, and automated foundation for customers who seek automation tools and solutions to modernize their data center infrastructure.

By leveraging automation and Ansible Automation Platform, organizations can simplify Day 2 operations across OpenShift, OpenShift Virtualization, Enterprise storage, and Cisco UCS infrastructure, reducing manual efforts while improving consistency, security, and scalability.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Solution Overview

This chapter contains the following:

- Introduction
- Audience
- Purpose of this document
- Solution Summary

Introduction

The new Ansible validated content offers a robust set of roles designed to automate and manage Cisco Unified Computing System (Cisco UCS) infrastructure efficiently.

Red Hat Ansible Automation Platform delivers a scalable enterprise framework that empowers teams across development, operations, and networking to create, share, and manage automation workflows seamlessly. By integrating Ansible with Cisco UCS, users can simplify complex tasks such as Fabric Interconnect and network configuration management, leveraging the unified computing architecture of Cisco UCS to streamline infrastructure operations and enhance consistency.

Audience

The intended audience for this document includes, but is not limited to, sales engineers, field consultants, DevOps engineers, professional services, IT managers, IT engineers, partners, and customers who are interested in learning about and deploying Cisco Unified Computing System.

Purpose of this document

This document presents the new Cisco UCS Compute Ansible Collection, featuring Ansible validated content that provides an initial set of roles designed to automate Day 2 management and operational tasks for Cisco UCS infrastructure. It aims to enable customers to efficiently manage their compute environments with validated automation aligned to Cisco's best practices, ensuring reliable and consistent infrastructure operations.

Solution Summary

The Cisco UCS Compute Ansible Collection is a Cisco Validated Design (CVD) solution that provides a comprehensive set of Ansible roles to automate Day 2 operations for Cisco UCS infrastructure. This collection is available through Ansible automation hub and GitHub UCS Compute Solutions repositories, enabling users to leverage automation for managing Cisco UCS environments efficiently.

Key Components and Capabilities:

- **Port Configuration Management:** Roles to query Cisco UCS Fabric Interconnects for available ports and their configurations, allowing review, modification, or reassignment of port roles.
- **Firmware Upgrades:** Automation of firmware upgrades for Fabric Interconnects to ensure infrastructure is up to date with minimal manual intervention.
- **Infrastructure Expansion:** Use cases to extend existing Cisco UCS solutions by adding new chassis, UCS C-Series rack servers, or UCS X-Series compute nodes.
- **Network Automation:** Roles to automate the addition of virtual NICs (vNICs) and VLANs within the UCS domain, simplifying network configuration tasks.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

The solution fully supports the Red Hat Ansible Automation Platform, providing flexibility in deployment. Automation workflows are executed via Ansible Playbooks that invoke the collection's roles, consume user-defined variables and defaults, and are aligned with Cisco best practices.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Technology Overview

This chapter contains the following:

- Cisco Unified Computing System
- Cisco Fabric Interconnect
- Red Hat Ansible Automation Platform
- Ansible Content Repositories

Cisco Unified Computing System

Cisco Unified Computing System is an advanced data center platform that integrates compute, networking, storage access, and virtualization into a unified system. Designed to reduce total cost of ownership (TCO) and enhance business agility, Cisco UCS delivers scalable, integrated, and programmable infrastructure that supports modern workloads across bare-metal, virtualized, and cloud environments.

Core Subsystems of Cisco UCS:

- **Compute:** Incorporates servers based on advanced processors, available in rack and modular form factors, managed centrally via Cisco Intersight.
- **Network:** Features a low-latency, lossless Ethernet fabric that consolidates LAN, SAN, and management traffic into a single unified fabric, reducing cables, adapters, and operational expenses.
- **Virtualization:** Enhances scalability and operational control for virtualized environments, extending Cisco security and policy enforcement into virtual workloads.
- **Storage Access:** Provides consolidated access to SAN and NAS storage over the unified fabric, simplifying storage connectivity and management.
- **Management:** Unifies compute, network, and storage management through Cisco Intersight, enabling automation and policy-driven provisioning.

Unique differentiators of Cisco UCS and Cisco Intersight:

- **Embedded Management:** Servers are managed by embedded firmware within Fabric Interconnects, eliminating the need for external management devices.
- **Unified Fabric:** A single Ethernet cable supports LAN, SAN, and management traffic, simplifying infrastructure and reducing costs.
- **Auto Discovery:** Compute nodes are automatically discovered and inventoried upon connection, enabling a wire-once architecture that simplifies expansion without reconfiguring external networks.
- **Cisco Intersight Managed Mode (IMM):** Provides centralized, cloud-powered management, policy enforcement, and operational visibility across all UCS hardware.
- **Model-Based Management:** Cisco Intersight uses model-based configurations and server profiles to automate provisioning and ensure consistent, compliant deployments.
- **Cloud-Enabled Lifecycle Management:** Cisco Intersight offers SaaS and on-premises deployment options, providing a unified dashboard for managing infrastructure across data centers, edge, and remote locations.
- **RESTful API and Automation:** Intersight's cloud-based RESTful API supports full programmability and integration with DevOps tools like Ansible Automation Platform, enabling efficient management of configurations, policies, and remediation steps.
- **Seamless Firmware and Software Upgrades:** Cisco Intersight automates upgrades for UCS domains and components without operational disruptions.

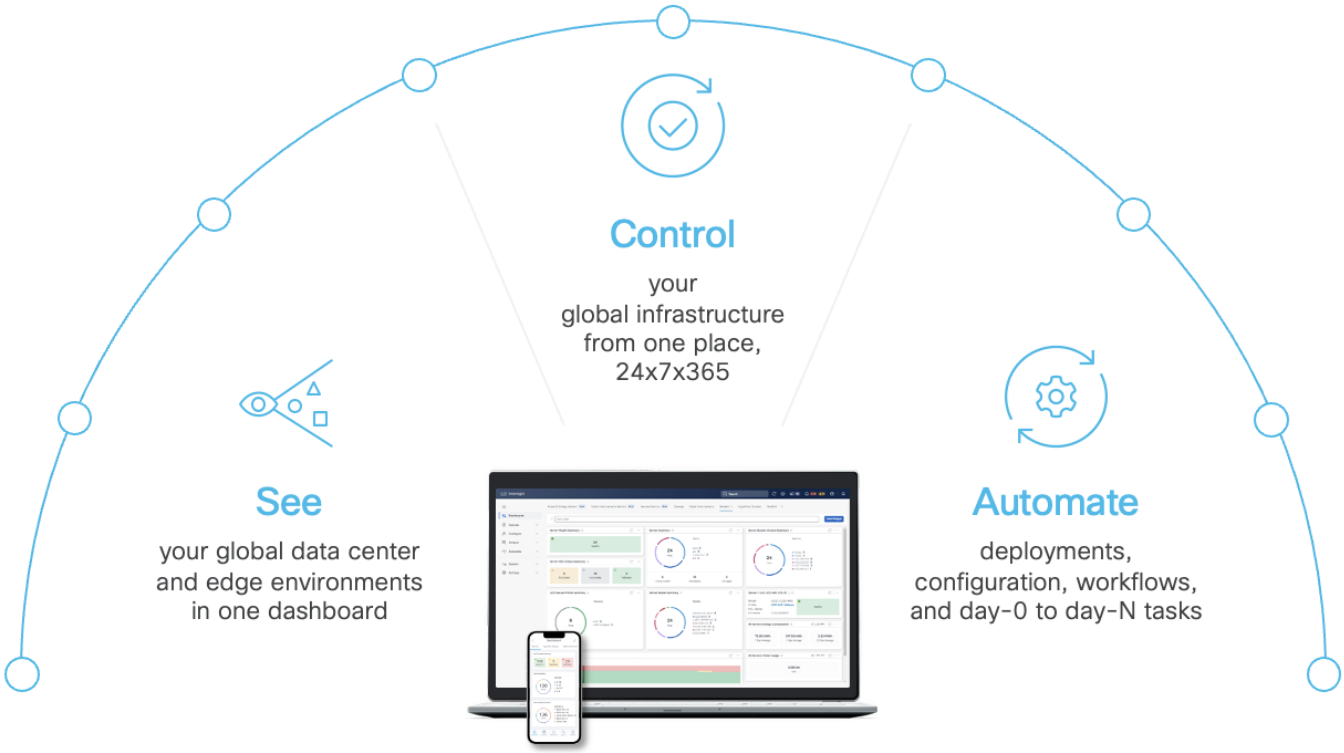
© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

- **Enhanced Operational Efficiency:** Intersight's analytics and integration with Cisco TAC provide proactive support and recommendations to optimize infrastructure performance.

Cisco Intersight

Cisco Intersight is a lifecycle management platform for your infrastructure, regardless of where it resides. In your enterprise data center, at the edge, in remote and branch offices, at retail and industrial sites—all these locations present unique management challenges and have typically required separate tools. Cisco Intersight Software as a Service (SaaS) unifies and simplifies your experience of the Cisco Unified Computing System. It gives you one consolidated dashboard to see your data center and edge infrastructure – including real-time status and interdependencies (Figure 1). Administrators use Cisco Intersight to manage the entire Cisco Unified Computing System as a single logical entity through an intuitive graphical user interface (GUI) and can automate deployments and configurations using a robust application programming interface (API).

Figure 1. Cisco Intersight. IT operations – simplified



Cisco Intersight RESTful API

Cisco Intersight provides a cloud-based RESTful API to manage Intersight connected targets across multiple data centers. Intersight API requests may be read-only queries with no side-effects or produce modifications of managed objects. It accepts and returns messages that are encapsulated through JavaScript Object Notation (JSON) documents and uses HTTP over TLS as the transport protocol.

The integration of Intersight and Red Hat Ansible Automation Platform provides a software-defined approach to manage the entire hardware and software stack including converged infrastructure products. You can automate Intersight policy, resource pool, and resource profile configurations and ongoing management including the ability to detect and remediate unintended changes.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Cisco UCS Fabric Interconnect

The Fabric Interconnect (FI) is the core of the Cisco UCS, combining computing, networking, storage access, and virtualization into a cohesive system. It delivers a low-latency, lossless multi-Gigabit Ethernet fabric that supports unified management and scalable multi-chassis deployments, reducing TCO and increasing agility.

More information on the fabric architecture and the different Fabric Interconnect models is available at: Cisco UCS Fabric Interconnects and Fabric Extenders.

Red Hat Ansible Automation Platform

The Red Hat Ansible Automation Platform is a comprehensive, enterprise-grade IT automation solution designed to simplify and streamline the management of IT infrastructure. It enables organizations to automate tasks like deploying and configuring IT services, whether on-premise or in the cloud. It uses simple, human-readable instructions written in YAML files called “playbooks” to ensure tasks are executed consistently, and efficiently across multiple systems, even at large scale.

One of the key strengths of this automation platform is that its configurations (playbooks) are text-based. This makes them easy to store, version, and collaborate using Source Code Management (SCM) system like GitHub. By following an Infrastructure-as-Code (IaC) approach, teams can treat infrastructure management just like software development. This means teams can adopt best practices like version control, collaboration workflows, and Continuous Integration/Continuous Deployment (CI/CD).

For more advance automation, Ansible Automation Platform integrates seamlessly with REST APIs, allowing teams to automation “as-a-Service” (aaS) solutions and extend infrastructure capabilities, such as managing Cisco UCS domains. Python code and Ansible Playbooks are often used together to implement these automations, making it possible to programmatically define how IT servers are provisioned and consumed.

Other benefits are the automation scalability across multiple data centers and remote locations via centralized control of distributed execution nodes including features like fault tolerance and redundancy. The extensive set of automation content, designed by Red Hat and partners including Cisco, enables teams to jumpstart new automation projects much more quickly. Collections may include Ansible modules, roles, playbooks, and other types of automation content.

By treating infrastructure configurations as code, Ansible enables organizations to apply the same rigorous standards to infrastructure automation as they do to software development. This includes benefits like:

- Quality and consistency: Ensuring repeatable and error-free automation processes.
- CI/CD: Automating deployment pipelines for faster updates and rollouts.
- Traceability: Tracking changes and maintaining a clear history of updates.
- Automated testing: Validating infrastructure changes before they go live.
- Compliance checking: Ensuring infrastructure meets regulatory and organizational standards.

With the Red Hat Ansible Automation Platform, organizations can take full advantage of modern automation techniques to simplify complex IT operations, improve efficiency, and reduce human error.

Learn more here: https://www.redhat.com/en/technologies/management/ansible.

In summary, AAP provides a robust and scalable solution for IT automation, offering a wider range of tools and capabilities than the open-source Ansible engine alone.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

The Red Hat Ansible Automation Platform is an enterprise-grade software solution that enables organizations to automate complex, repetitive IT tasks across their entire IT environment, from infrastructure configuration and software deployment to advanced orchestration and cloud management. In this document, we will focus on two capabilities consisting of two key parts: automation execution and automation content. Both are essential for enabling efficient, consistent, and scalable IT automation.

Automation Execution

This part refers to the framework and tools that run Ansible Playbooks or automation workflows, which are an ordered collection of multiple playbooks and other automation content designed to automate more comprehensive management needs. This framework provides an enterprise-grade environment to build, manage, and execute automation at scale across diverse IT infrastructure. Automation execution handles provisioning, configuration, deployment, and management of resources and applications. It supports agentless operation, uses simple YAML-based playbooks, and integrates with APIs for extensibility. This execution layer ensures repeatable, predictable automation that reduces manual errors and accelerates operational tasks.

Automation Content

Automation content includes reusable, tested, and validated modules, roles, and collections that define specific automation tasks. For example, Cisco provides Ansible Certified Content Collections and validated content tailored for Cisco infrastructure, enabling automation of complex operations like firmware upgrades, port configuration, and server profile deployment. This content encapsulates best practices and simplifies automation development by providing ready-to-use building blocks.

Ansible Content Repositories

The following two options represent central repositories for Ansible content:

- **Ansible automation hub:** A hosted service (cloud.redhat.com) that provides certified and supported Ansible Content Collections from Red Hat and its partners.
- **Private automation hub:** A component of the Red Hat Ansible Automation Platform that is an on-premise and private repository that allows you to manage, share, and curate content, including content synced from Ansible automation hub. This is especially useful for disconnected or air-gapped environments.

Ansible Content Collections

Ansible Content Collections are essential building blocks of automation. The modules, playbooks, plugins, roles, and related documentation help to quickly inject automation into IT systems and solutions.

Red Hat Ansible content contains two types of content:

- Ansible Certified Content
- Ansible Validated Content

The Red Hat Ansible Automation Platform includes Ansible validated content, which complements existing Red Hat Ansible certified content. You can use both, Ansible certified content like the Cisco Intersight Collection and Ansible validated content like the Cisco CVD Compute Collection in parallel to build your automation library.

Ansible validated content contains pre-build YAML content (such as playbooks and roles) to address the most common automation use cases and needs to pass ansible-lint tests without errors or warnings as well as ansible-test sanity if Python code is included. You can use Ansible validated content out-of-the-

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

box or as a learning opportunity to develop your skills. It's a trusted starting point to bootstrap your automation: use it, customize it, and learn from it.

Ansible validated content provides expert-led guidance on how to perform operations and tasks. Validated content is customizable for your organization's specific use cases, so it is not subject to the same support requirements as Red Hat Certified collections. Any issues with the validated collection content should be filed directly at the source repository of the Cisco CVD Compute Collection.

You can see the full set of Red Hat certified or validated content from Cisco in the Red Hat Ecosystem Catalog.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Solution Design

This chapter contains the following:

- Cisco CVD Compute Collection

Cisco CVD Compute Collection

The Cisco CVD Compute Collection offers a robust set of roles that have thoroughly tested by Cisco and validated by Red Hat to ensure seamless integration and high reliability within Cisco environments. These roles focus on reusable Day 2 automation tasks specifically for Cisco compute solutions.

Serving as a foundational element of a broader automation strategy, this collection extends the existing Day 0 automation capabilities found in Cisco Validated Designs by reducing manual configuration errors and accelerating deployment timelines.

This chapter describes the key Ansible roles, and their functions as published in the initial release of the Cisco CVD Compute Collection.

Prerequisites for all roles are:

- Cisco UCS Fabric Interconnects configured with IP management access
- Valid Cisco ID and Cisco Intersight account
- Cisco Intersight Infrastructure Services Essentials license or higher

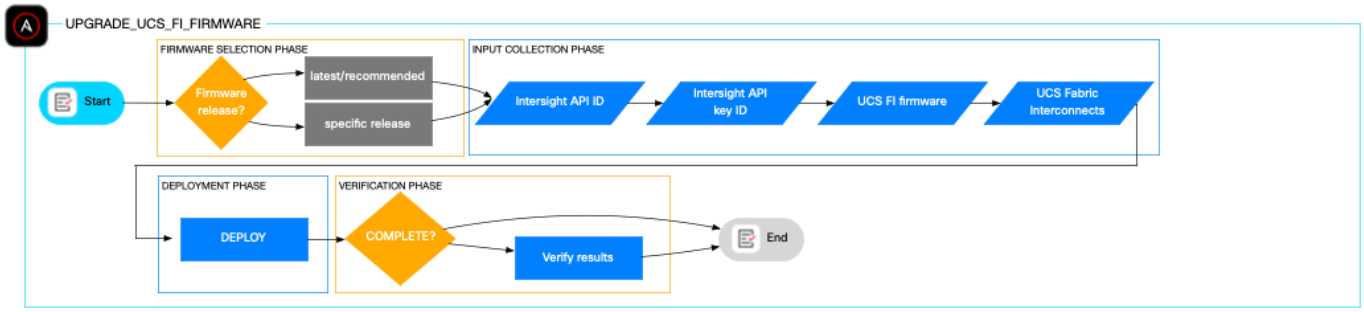
Fabric Interconnect Firmware Update

The role upgrade_ucs_fi_firmware automates the firmware upgrade process for Fabric Interconnects within a Cisco UCS domain. Configure the firmware distributable type (recommended, latest, or specific version) which will default otherwise to the Cisco recommended version. When you configure a specific version as the distributable type you need to provide the firmware release additionally to the Cisco Intersight API ID, Cisco Intersight private key and the list for fabric interconnects to be updated.

Executing the playbook triggers an immediate upgrade (or downgrade), sequentially updating a Fabric Interconnect cluster. The test folder of the repository contains an optional playbook which verifies the fabric interconnect firmware after the deployment.

Note: The Fabric Interconnect firmware upgrade (or downgrade) will be executed immediately.

Figure 2. Ansible role flowchart – upgrade_ucs_fi_firmware



© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

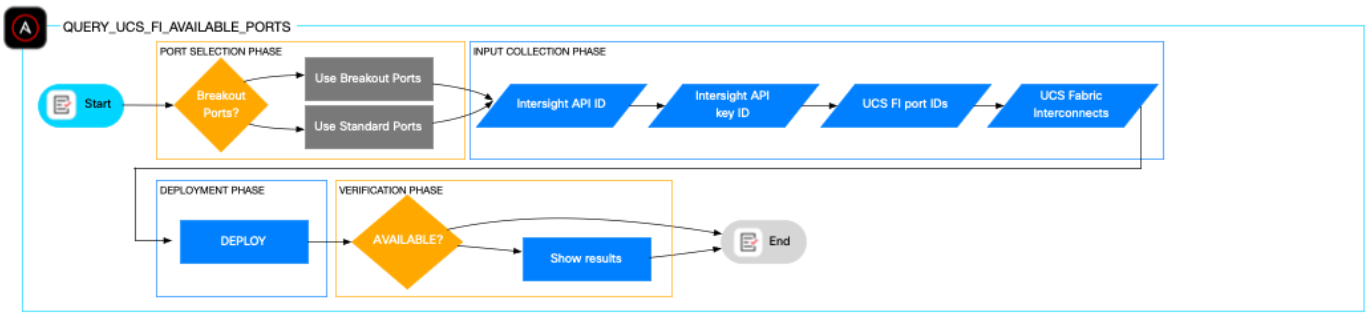
Query available ports on Fabric Interconnects

The query_ucs_fi_available_ports role assesses current Fabric Interconnect port usage and verifies port availability before provisioning. It supports querying breakout, non-breakout, or ranges of ports, defaulting to all available ports if none are specified.

The role relies additionally on input parameters such as which fabric interconnects to be examined, the Cisco Intersight API ID and the Cisco Intersight private key.

The playbook will provide a summarized provisioning report if the requested ports are available,

Figure 3. Ansible role flowchart -query_ucs_fi_available_ports



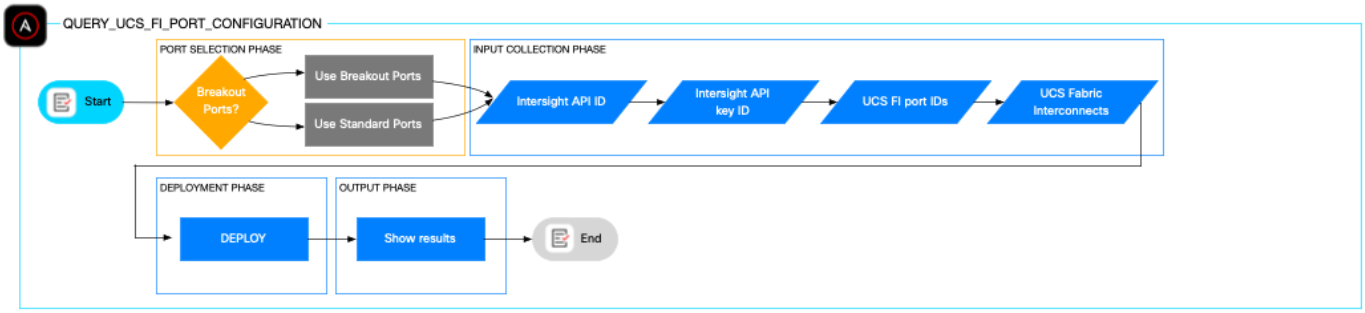
Query the Fabric Interconnect configuration

The role query_ucs_fi_port_configuration retrieves detailed Fabric Interconnect port configuration data, including administrative and operational states, port speeds, port roles, and group assignments. This information aids administrators in evaluating port usage and breakout configurations prior to provisioning or for troubleshooting purposes.

The role relies on input parameters such as which fabric interconnects to be examined, the Cisco Intersight API ID and the Cisco Intersight private key. It supports querying breakout, non-breakout, or ranges of ports, defaulting to all available ports if none are specified.

The playbook output provides a consolidated configuration report, including administrative and operational state, port speed, role, and group data.

Figure 4. Ansible role flowchart - query_ucs_fi_port_configuration



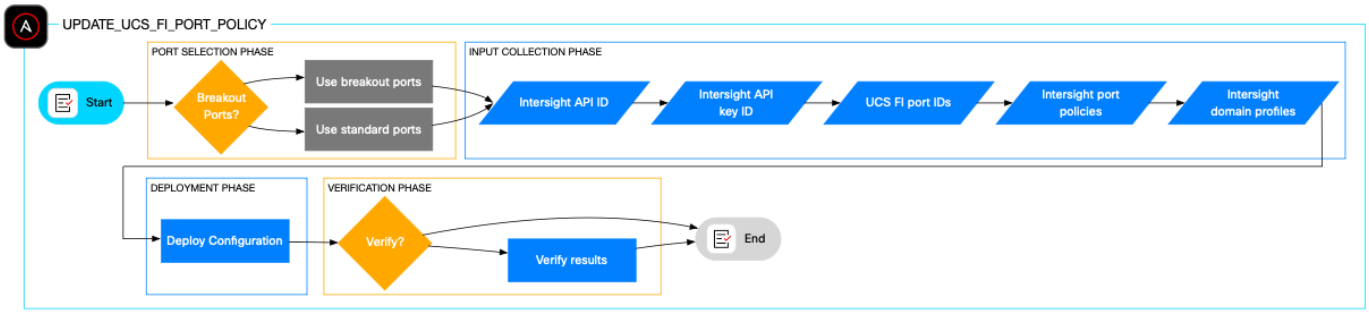
Update Fabric Interconnect Port policy

The update_ucs_fi_port_policy role automates updating unified port configurations, particularly when expanding a Cisco UCS domain with additional Cisco UCS C-Series, Cisco UCS X-Series chassis, or Cisco UCS X-Series compute nodes.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

It accepts input parameters such as domain profile names, port policy names, port IDs, and optionally port slot IDs for breakout configurations. An optional validation playbook is included to verify successful port configuration.

Figure 5. Ansible role flowchart - update_ucs_fi_port_policy

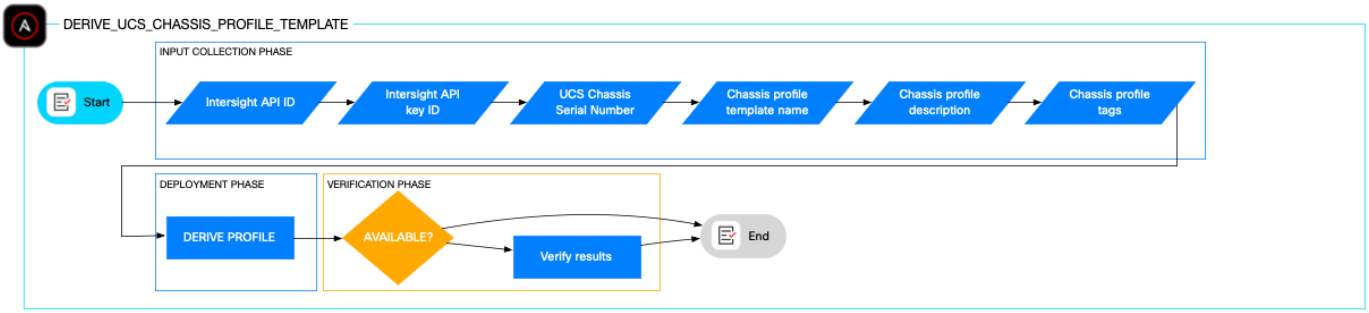


Derive UCS chassis profile from template

The derive_ucs_chassis_profile_template role automates creating UCS chassis profiles derived from template, specifically for Cisco UCS X-Series systems. It standardizes configuration parameters such as IMC access, power, SNMP configuration, and thermal policies, enabling rapid creation of consistent chassis profiles. Input parameters include chassis serial number, Chassis profile template name, description, as well as optional tags to customize the chassis profile according to the deployment environment requirements.

An optional validation playbook is included to verify a successful chassis profile configuration.

Figure 6. Ansible role flowchart - derive_ucs_chassis_profile_template



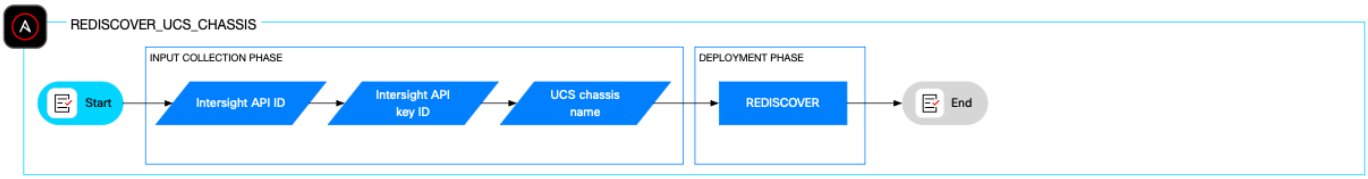
Rediscover UCS chassis

The role rediscover_ucs_chassis initiates the UCS chassis rediscovery process within Cisco Intersight, rebuilding connectivity between Fabric Interconnects and Input/Output Modules (IOMs) or Intelligent Fabric Modules (IFMs), updating inventory, cleaning up disconnected ports, and synchronizing firmware versions if needed. This process is generally non-disruptive, but a maintenance window is recommended as a best practice.

The role relies on input parameters such as the Cisco Intersight API ID, the Cisco Intersight private key, and a chassis name or comma separated chassis list in which to apply the rediscovery process.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Figure 7. Ansible role flowchart – rediscover_ucs_chassis



Add vNIC to a vNIC template

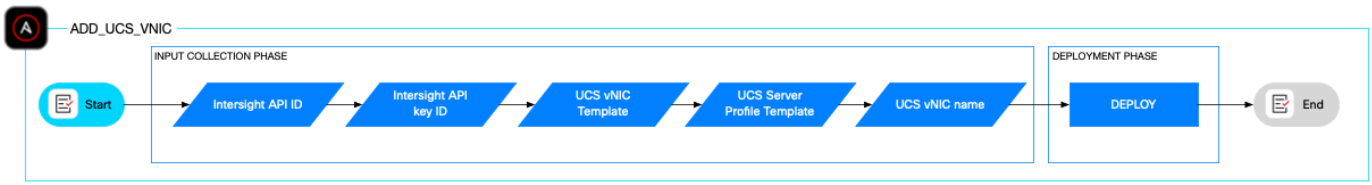
The approach of using a vNIC template which consists of common configuration simplifies the network configuration across multiple servers. The LAN connectivity policy part of the vNIC template determines the connections and the network communication resources between the server and the LAN on the network.

The add_ucs_vnic role attaches a new vNIC to a vNIC template, specifically by modifying the LAN Connectivity Policy. It uses an incrementing PCI order and includes validation checks to ensure successful updates. This role reduces manual GUI intervention, maintains policy consistency, and minimizes deployment downtime.

The role relies on input parameters such the Server Profile Template name, the vNIC Profile Template name, the vNIC name, the Cisco Intersight API ID, and the Cisco Intersight private key.

An optional validation playbook is included to verify the vNIC was added successfully to the vNIC template.

Figure 8. Ansible role flowchart – add_ucs_vnic



Add a new VLAN to a vNIC configuration

A UCS Domain Profile assigned to a pair of Fabric Interconnects defines the network characteristics like port and port channel configuration as well as the VLAN configuration of the Network Interface Cards (NICs). The add_ucs_vlan_to_vnic role automates the modification of the Ethernet Network Group Policy and ensures the VLAN is defined in the VLAN policy the Ethernet Network Group Policy refers to.

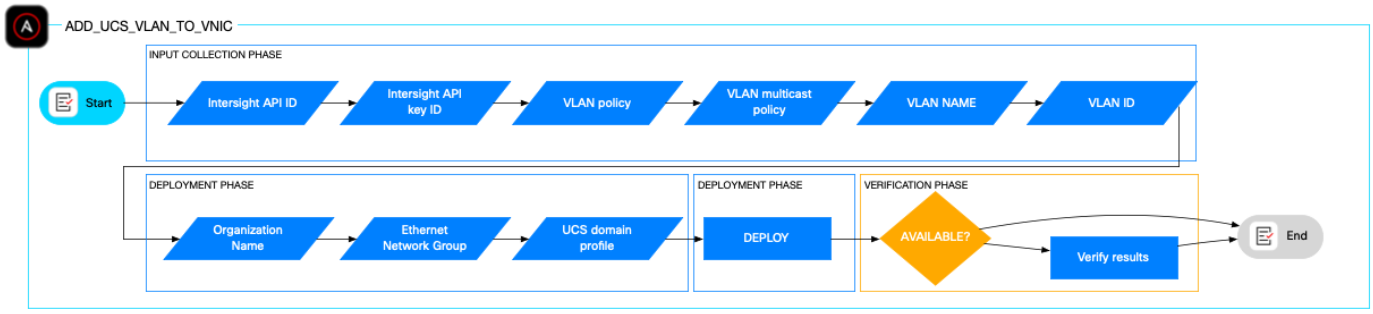
The role relies on several input parameters such the Network Group policy, the VLAN policy, the multicast policy, VLAN name and VLAN ID, the Domain Profile list, the Cisco Intersight API ID, and the Cisco Intersight private key.

An optional validation playbook is included to verify the VLAN was added successfully. This role supports frequent and consistent VLAN configuration changes in large or dynamic data centers, reducing manual errors and downtime.

This role is ideal for automating network configuration changes in Cisco UCS environments, especially in large-scale or dynamic data centers where VLAN configurations need to be updated frequently and consistently.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Figure 9. Ansible role flowchart – add_ucs_vlan_to_vnic

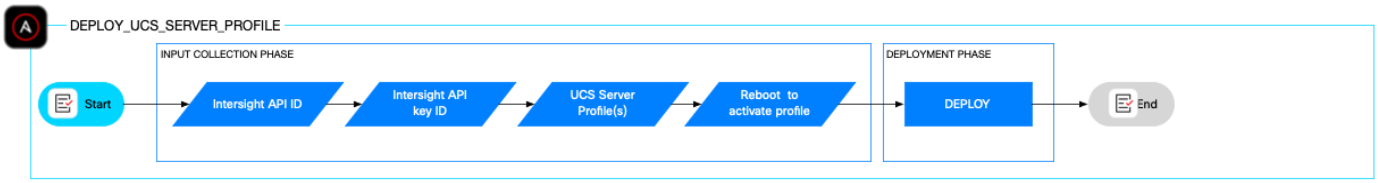


Deploy UCS server profile

A Cisco UCS server profile defines and standardizes the configuration of a Cisco UCS server, including computing, management, storage, and network policies. It enables automated, consistent, and scalable deployment of server settings, ensuring policy compliance and simplifying server provisioning and management across multiple servers. This abstraction allows administrators to manage hardware configurations as software-defined profiles, reducing manual effort and configuration errors.

The deploy_ucs_server_profile role automates deployment and optional activation of Cisco UCS server profiles derived from templates. It enables consistent, scalable server provisioning and management in Day 2 deployments, with an option to reboot servers immediately to apply configuration changes.

Figure 10. Ansible role flowchart – deploy_ucs_server_profile



© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Install and Configure

This chapter contains the following:

- Prerequisites
- Ansible Automation Hub
- Create GitHub Repository
- Configure Ansible Automation Platform
- Ansible Automation Platform Project Setup

Prerequisites

This guide will help you get started with the unified automation solution Red Hat Ansible Automation Platform.

To get started, we assume the following prerequisites are complete:

- Red Hat Ansible Automation Platform 2.5+ is installed and running.
- All new hardware (like Cisco UCS X-Chassis, C-Series servers and/or X-Series compute nodes, and so on) is physically racked, cabled, powered, configured with management IP addresses, and claimed in Cisco Intersight.
- Cisco Intersight API credentials and the Cisco Intersight endpoint information is available.

If you are new to Cisco Intersight, follow the Cisco Intersight REST API Learning Lab which guides you through creating Intersight REST API keys.

After you first login in AAP as administrator you typically must configure authentication for your users. Depending on your organization's needs and resources you can set up role-based access control (RBAC) by creating users, teams, and organizations. For simplification purposes this guide uses the standard admin user and the default organization.

Note: While the Red Hat Ansible Automation Platform is the preferred solution, the roles and playbooks are fully functional in any Ansible Execution Environment with the necessary Python modules and Ansible collections installed as per the repository requirement files.

Ansible Automation Hub

The Ansible automation hub is the central repository for Ansible content. Depending on customer requirements, for example a disconnected or air-gapped environment, it is possible to use the on-premise and private automation hub as alternate repository.

Private Automation Hub

Skip this section if a private automation hub setup is not required and use the Ansible automation hub repository instead.

Procedure 1. Create the API token in automation hub

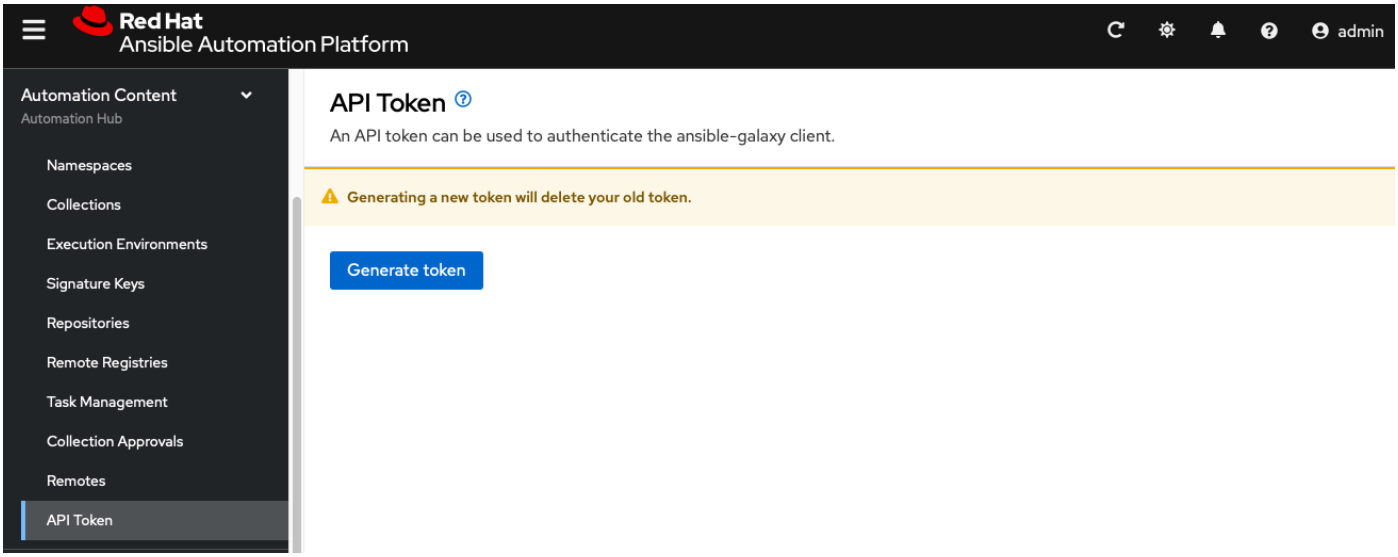
The offline token in the private automation hub is a secret token used to protect your content.

Step 1. Log into Ansible Automation Platform with your user credentials.

Step 2. From the navigation panel, select Automation Content > API token.

Step 3. Click Generate token.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

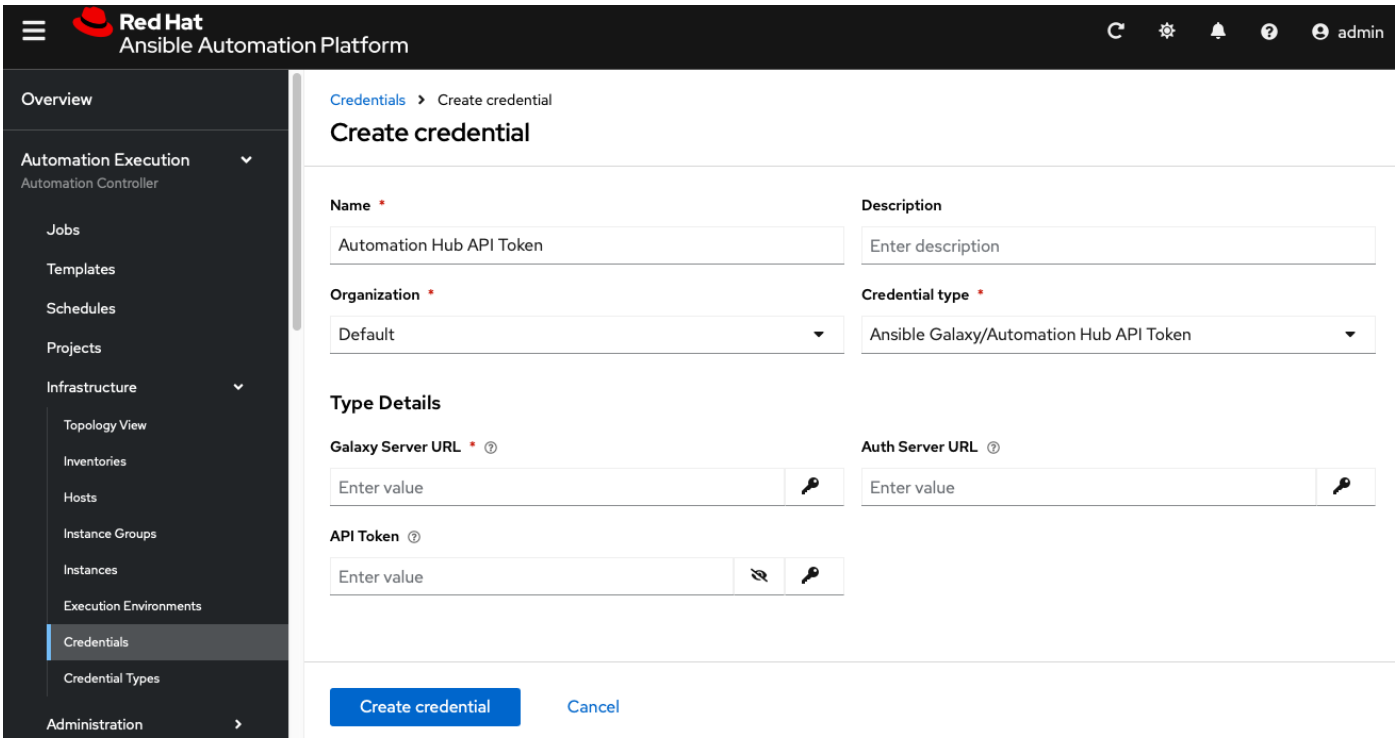


Step 4. Save the API token

Procedure 2. Create an automation hub API Token Credential

Step 1. From the navigation panel, select Automation Execution > Infrastructure > Credentials.

Step 2. Click Create credential.



Step 3. Enter the credential name, for example Automation Hub API Token, in the name field.

Step 4. Select the organization you want to use the credential.

Step 5. Select the credential type Ansible Galaxy/Automation Hub API Token.

Step 6. Under Type Details, enter the Galaxy Server URL, such as https://< AAP instance IP/FQDN >/pulp_ansible/galaxy/published/

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Note: To prevent a 301 redirect, all API URLs must end with a trailing slash /.

Step 7. Enter the API Token saved before.

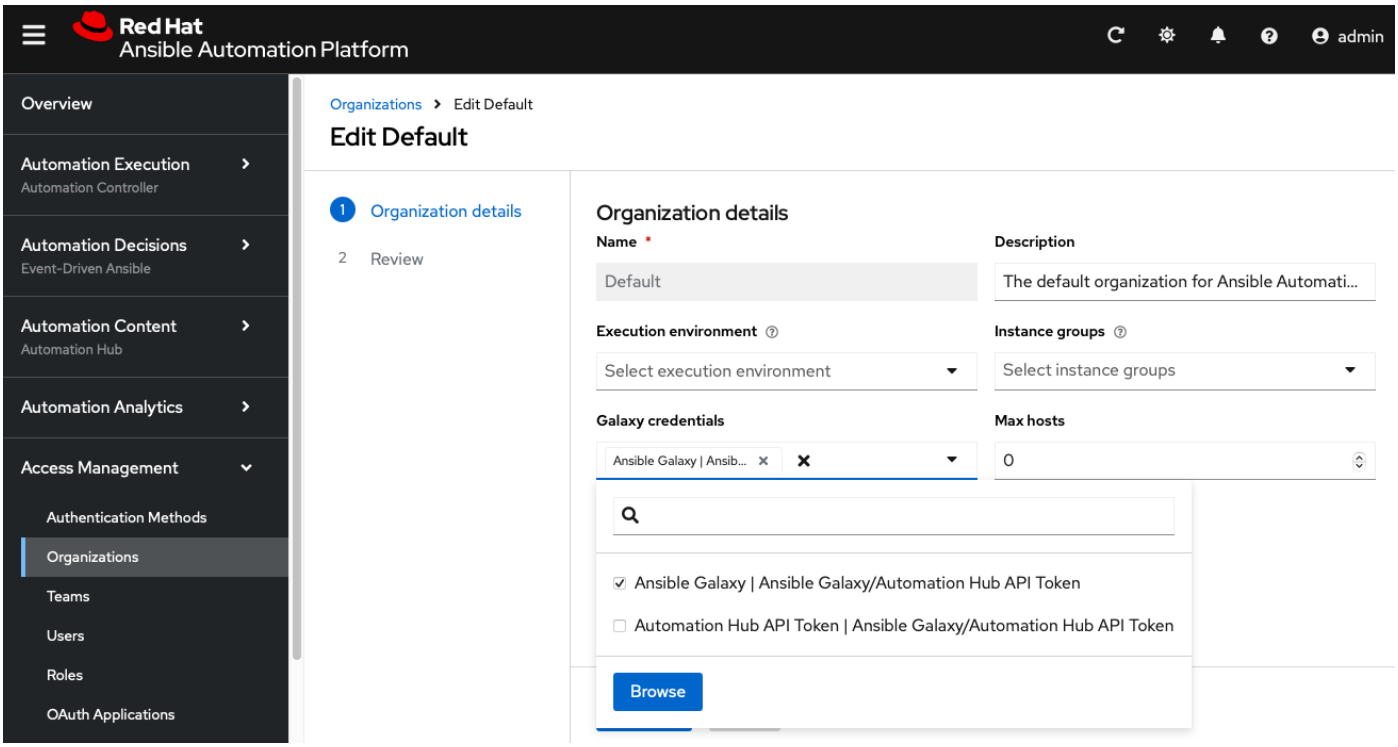
Step 8. Click Create credential.

Procedure 3. Update the organization's Galaxy credentials

Step 1. From the navigation panel, select Access Management > Organizations.

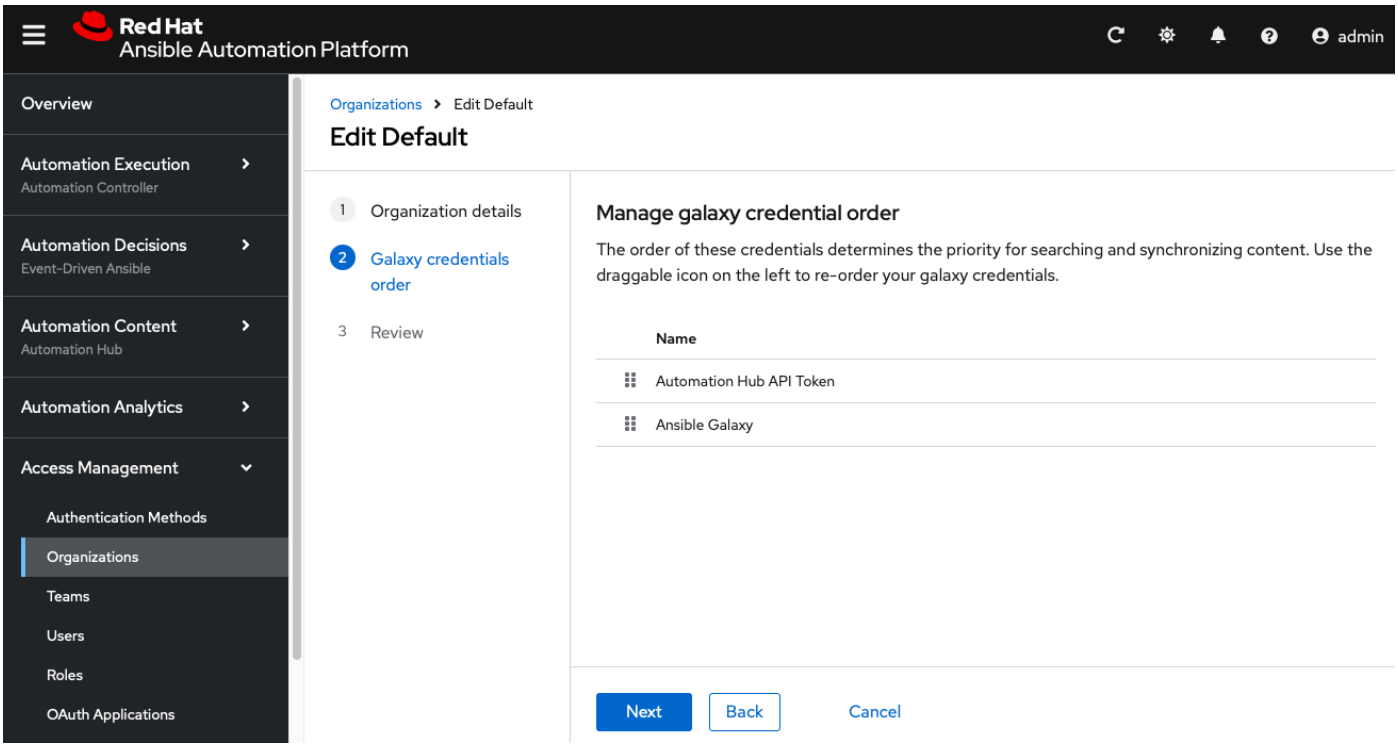
Step 2. Click on the pencil icon next to the organization where you want to add your Galaxy credential.

Step 3. Under Galaxy credentials, add the Automation Hub API Token and click Next.



Step 4. Select the Automation Hub API Token credential and place it at the beginning of the list.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.



Step 5. Click Next to review the changes. Then click Finish to save the changes.

Procedure 4. Import Cisco Collections in private automation hub

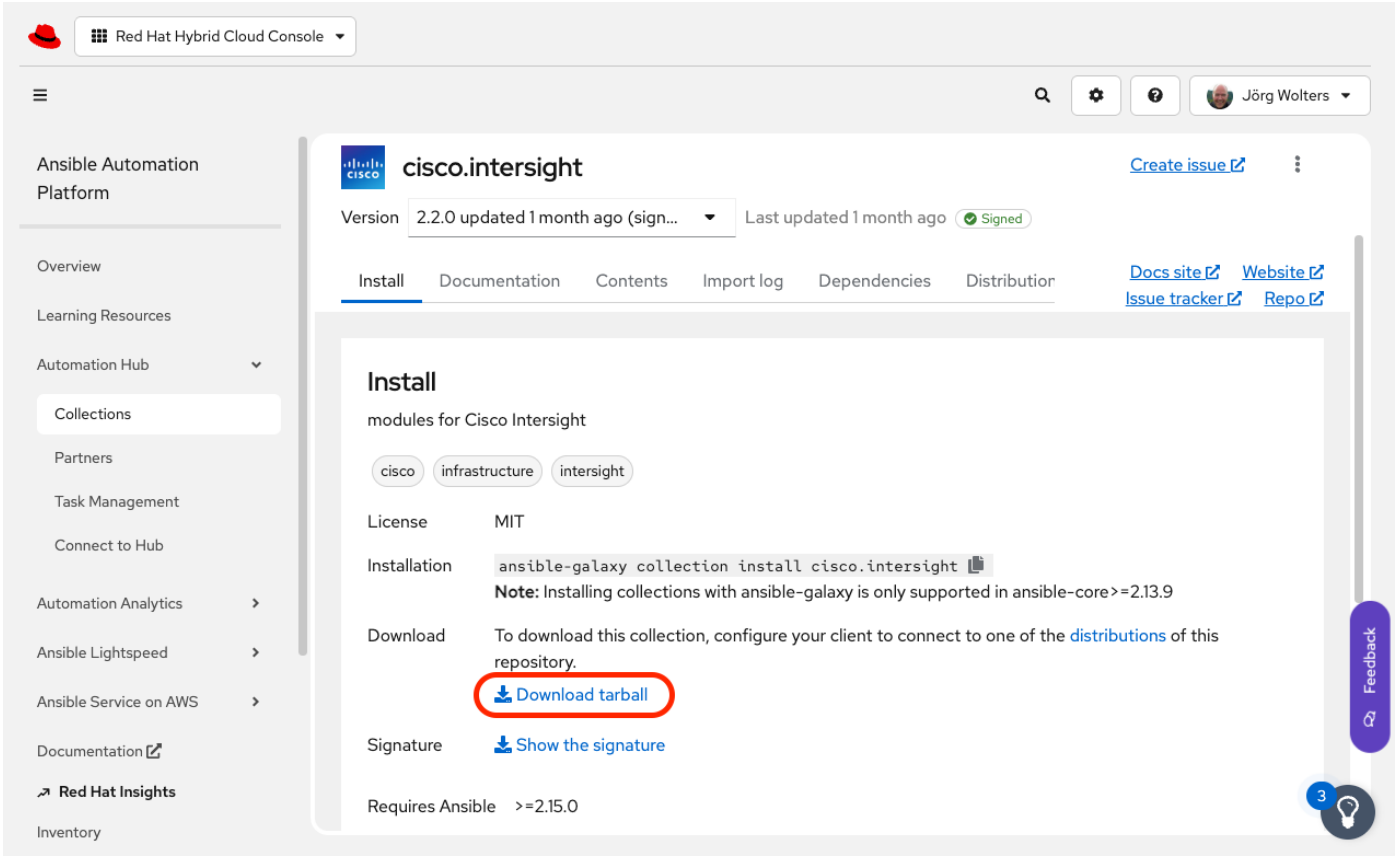
When setting up private automation hub as the central repository to discover and manage Ansible Collections you need to download the collections first and upload them in the private automation hub after.

Step 1. Log into https://console.redhat.com – Ansible Automation Platform

Step 2. Search for the Ansible certified collection of Cisco Intersight.

Step 3. Click the link download tarball to download the Cisco Intersight collection.

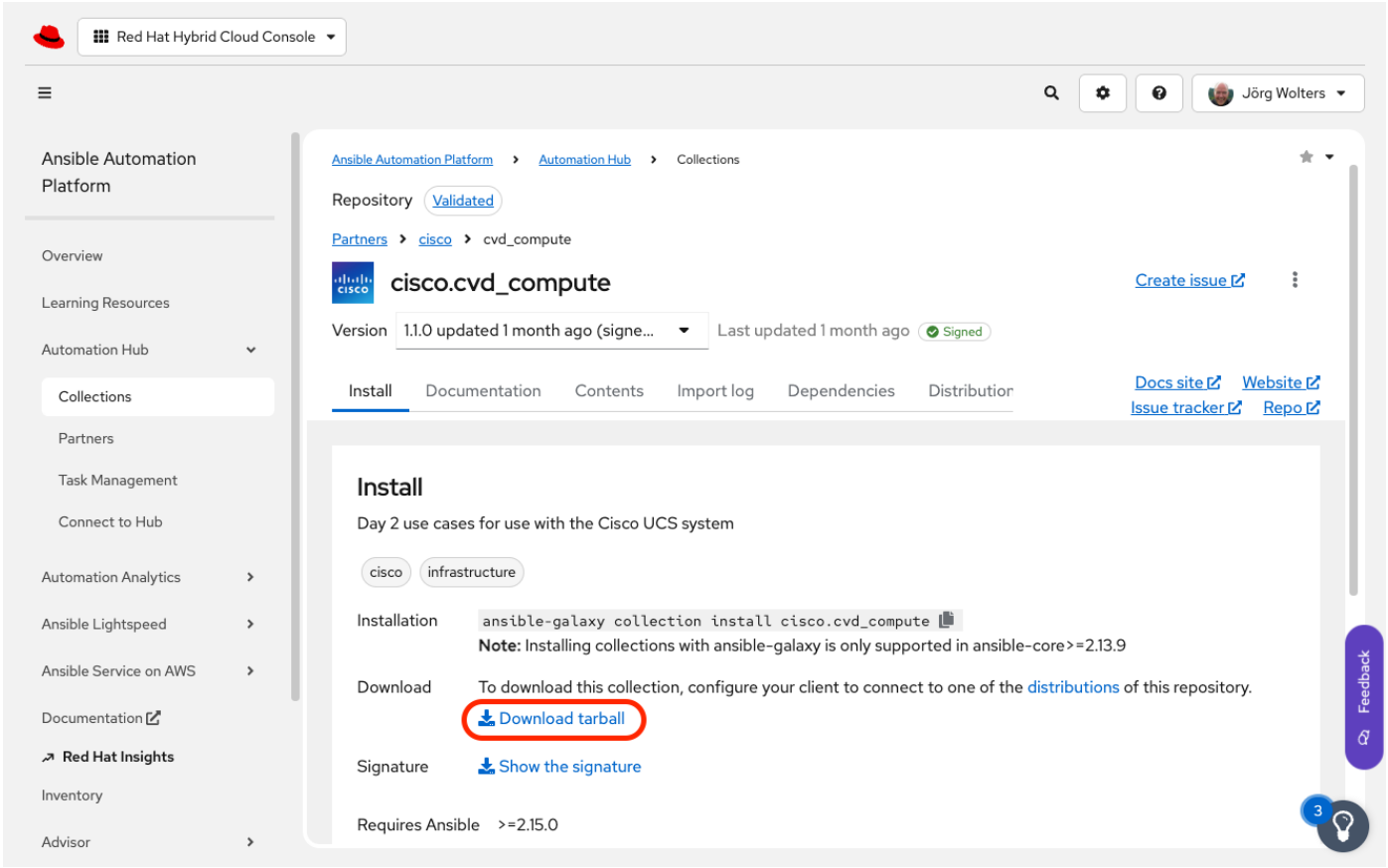
© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.



Step 4. Search for the Ansible validated collection Cisco CVD Compute.

Step 5. Click the link download tarball to download the Cisco CVD Compute Collection.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.



Step 6. Log into Ansible Automation Platform with your user credentials.

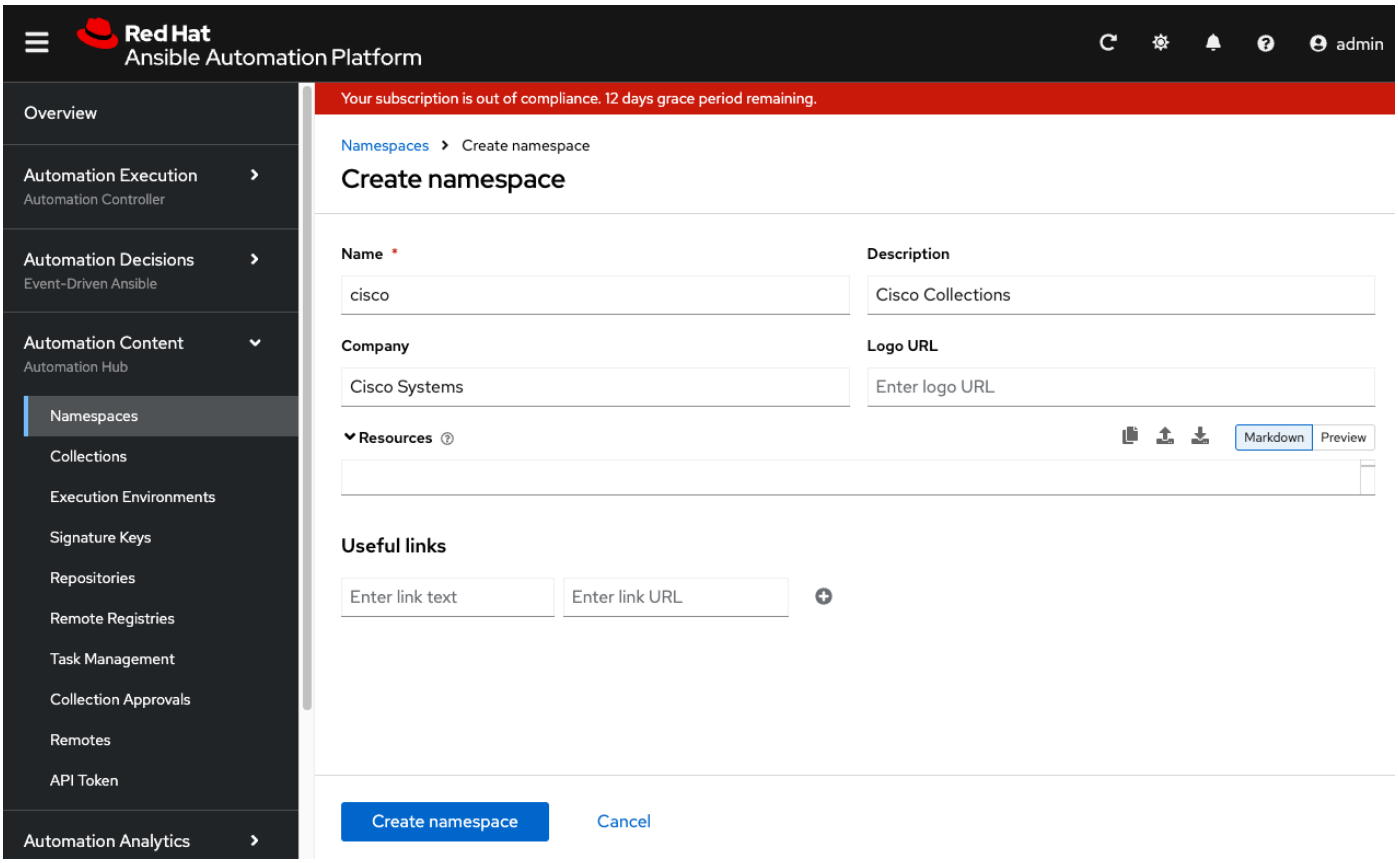
Step 7. From the navigation panel, select Automation Content > Namespaces.

Step 8. Click Create namespace and enter cisco as namespace name.

Step 9. Optionally, provide a description, company, or useful links in the appropriate fields.

Step 10. Click create namespace.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.



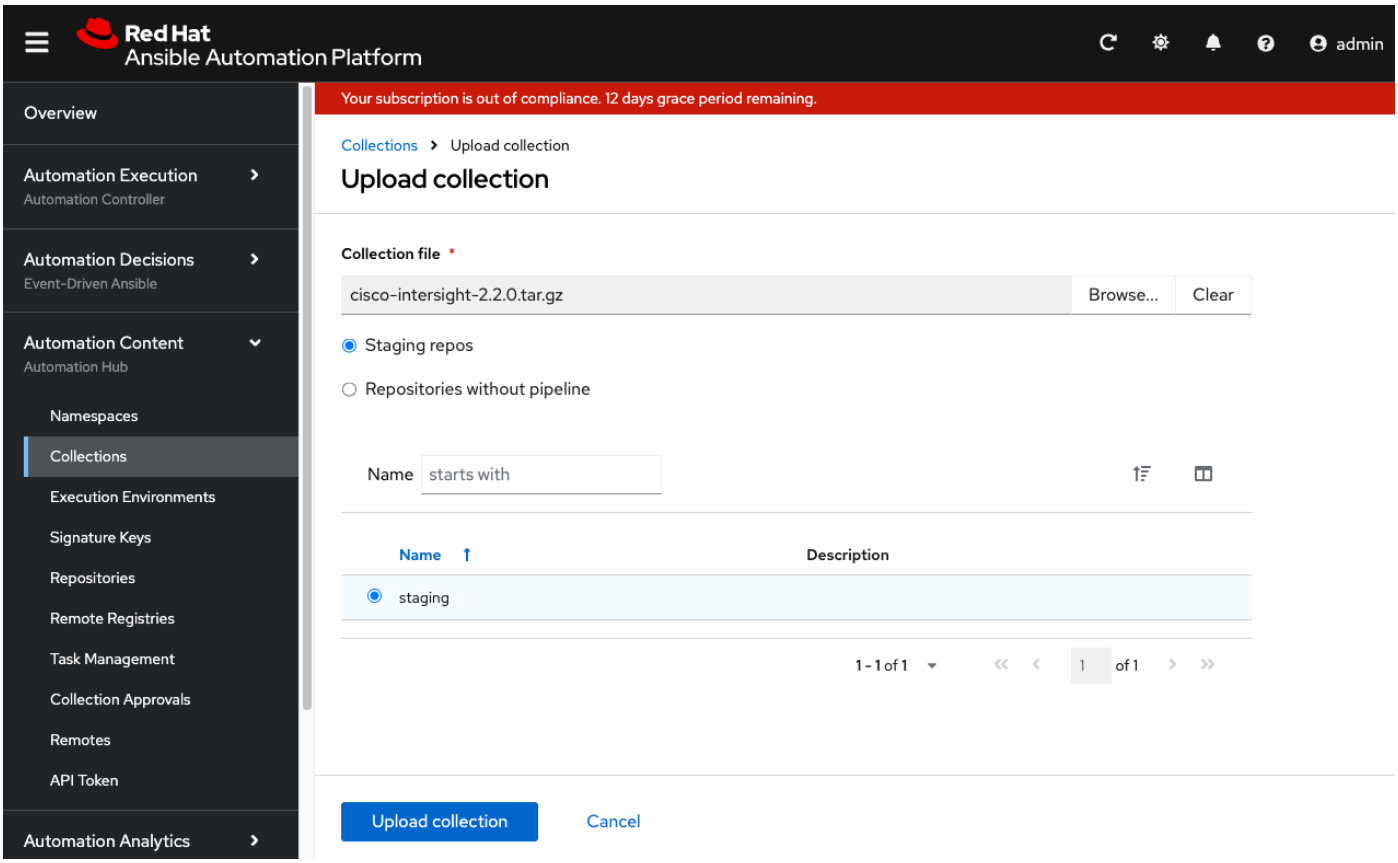
Step 11. From the navigation panel, select Automation Content > Namespaces and select the cisco namespace.

Step 12. Select the Collections tab and click Upload collection.

Step 13. Click Browse next to the Collection file field and select the Cisco Intersight collection for upload.

Step 14. Keep the defaults and click upload collection.

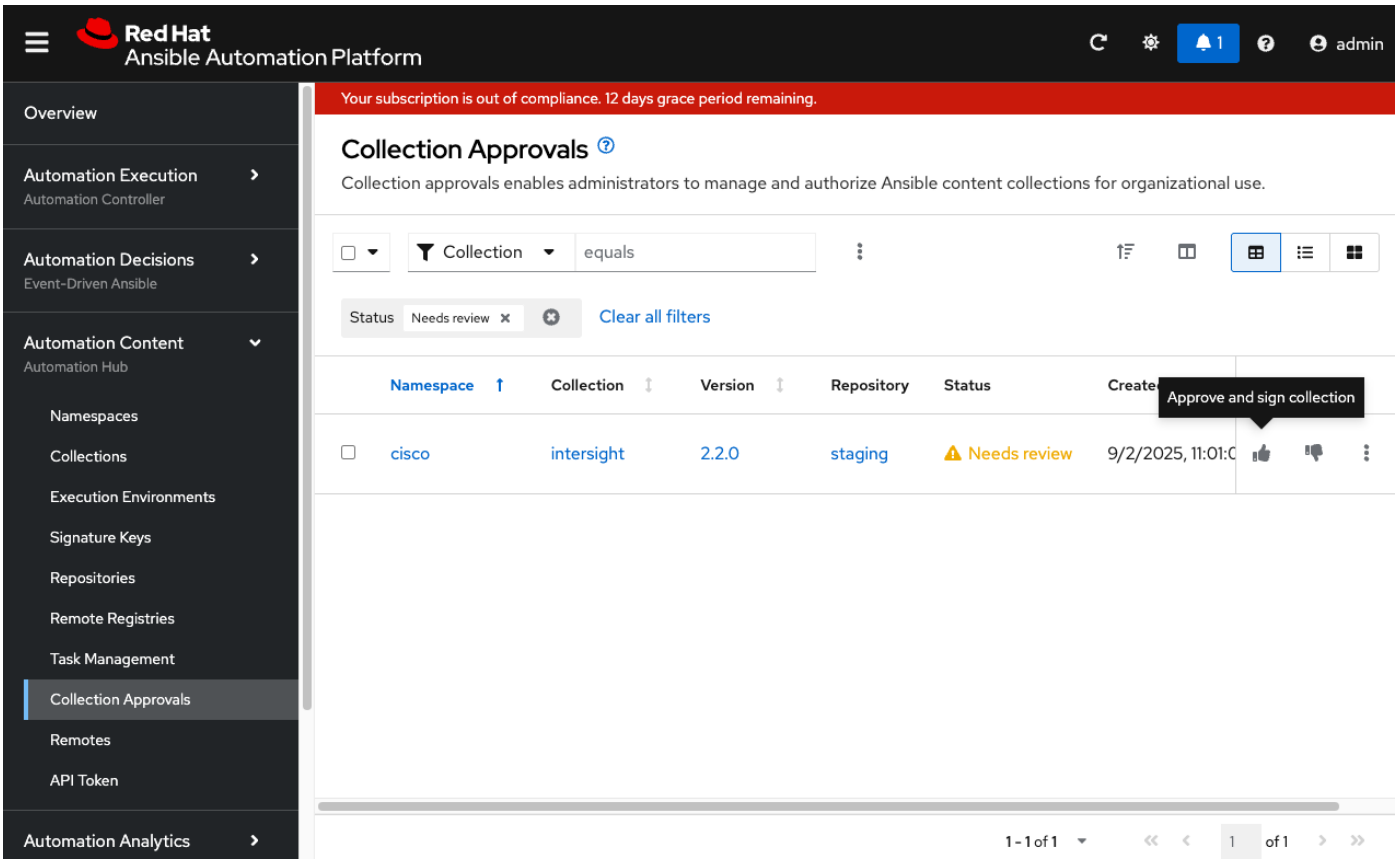
© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.



Step 15. When the upload finishes, the collection requires review and approval.

Step 16. Navigate to Automation Content > Collection Approvals.

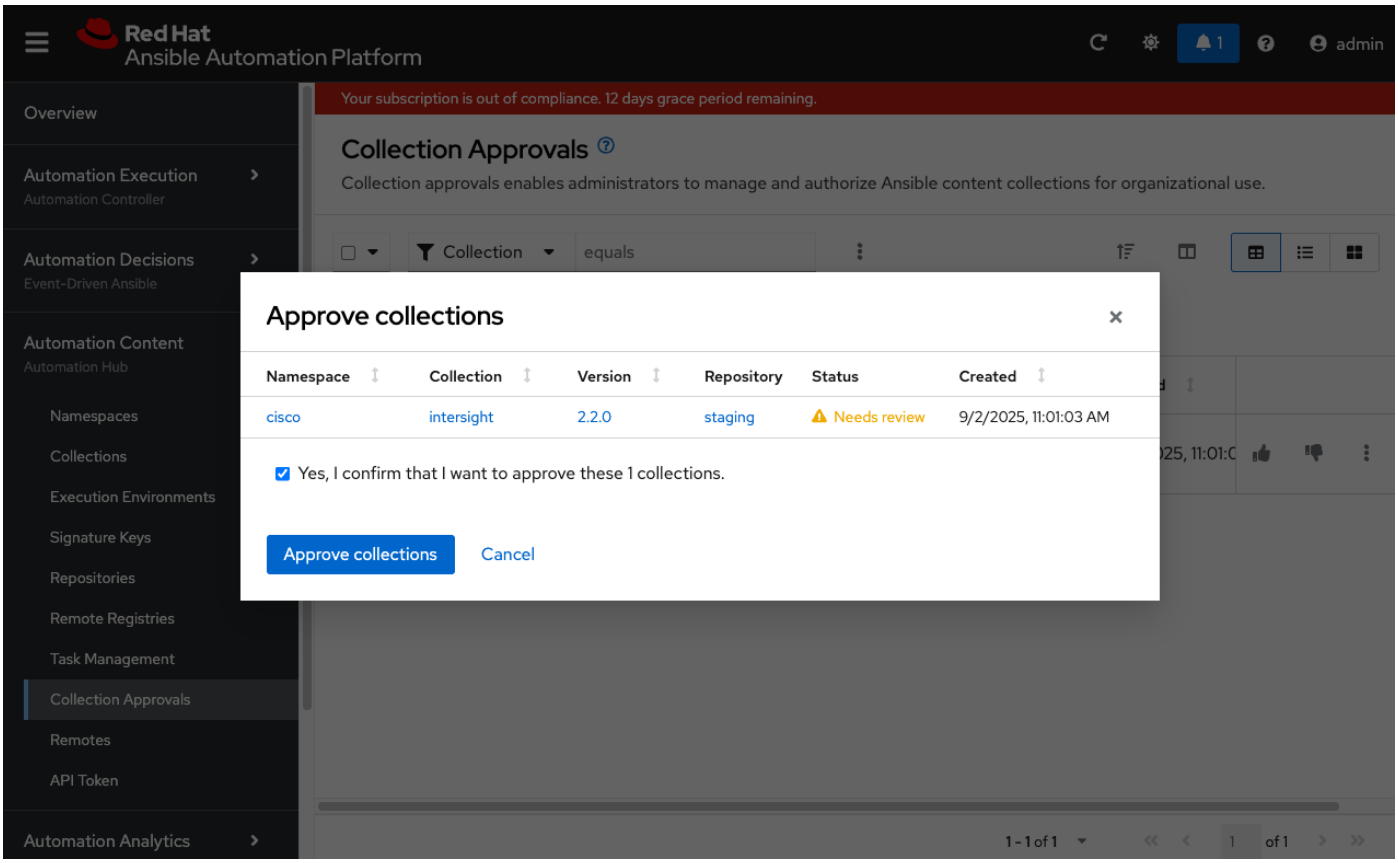
© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.



Step 17. Click the thumbs up icon to approve and sign the collection.

Step 18. Confirm your choice in the modal dialog that appears.

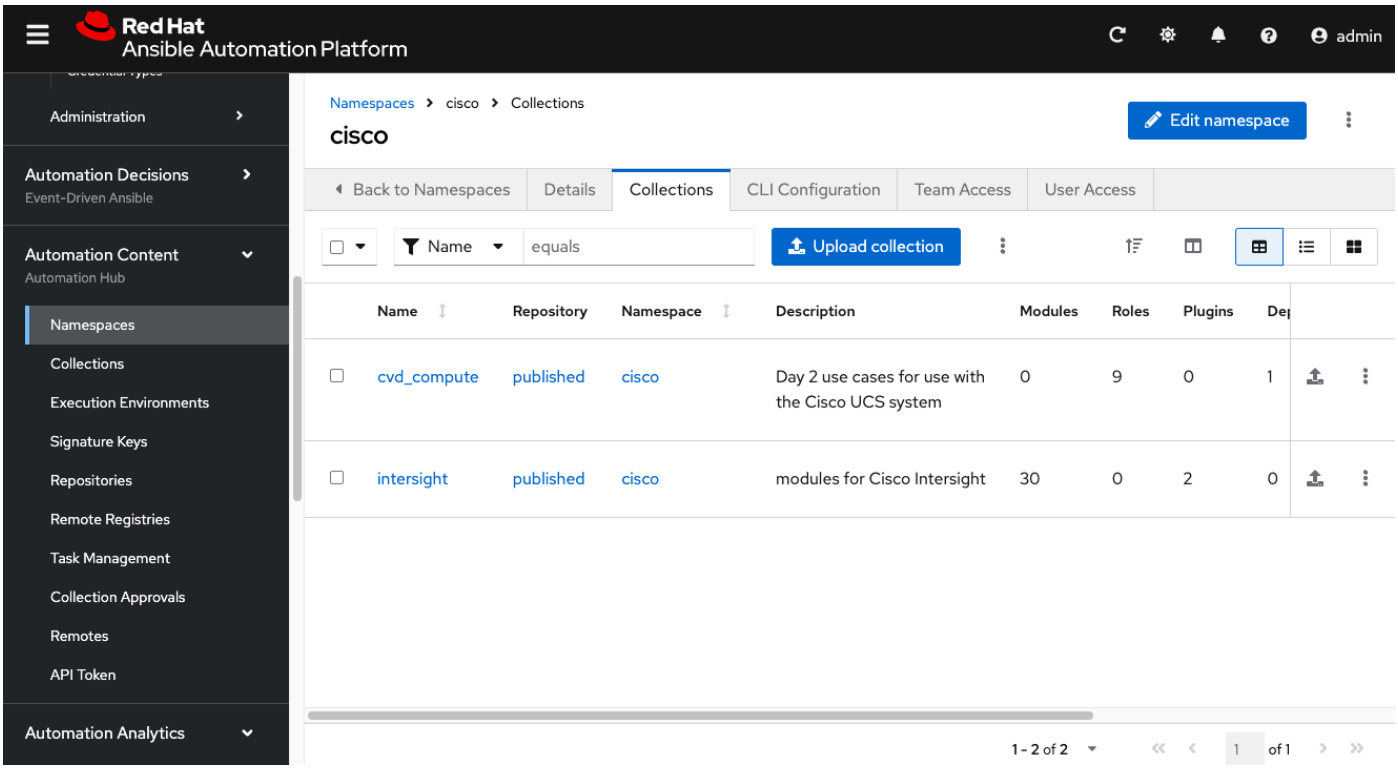
© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.



Step 19. Repeat steps 1 – 18 and upload the Cisco CVD Compute Collection as well.

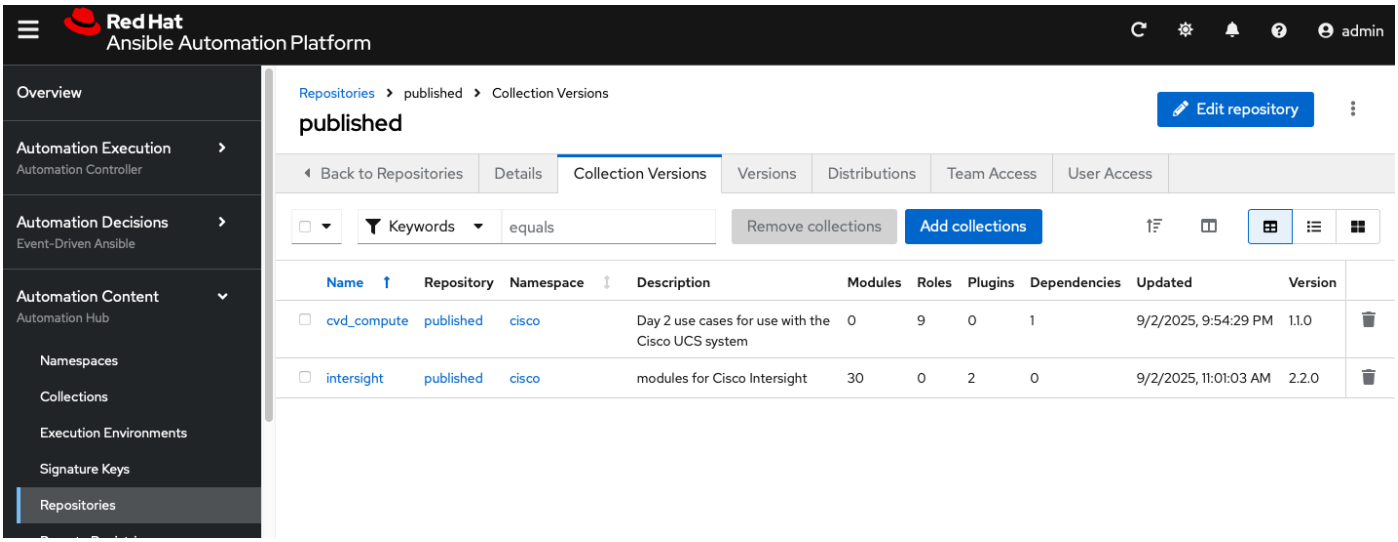
Step 20. In the navigation panel, select Automation Content > Namespaces and open the cisco namespace.

Step 21. Review both collections are listed under the tab Collections.



© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Step 22. The approved collections are moved to the Published repository where you can view and download them for use.



Procedure 5. Change the SSL validation handling

In the default AAP installation self-signed certificates are being used. Galaxy is configured to do SSL validation which will cause failures when running job templates.

Step 1. From the navigation panel, select Access Management > Job.

Step 2. Click Edit to change the job settings.

Step 3. Scroll to the end and check the option Ignore Ansible Galaxy SSL Certificate Verification.

Step 4. Click Save.

Create Github Repository

As best practice, configure a project to synchronize Ansible playbooks from SCM systems such as GitHub, as it provides version control and a centralized repository for your automation code.

To manage your automation code either create a new repository in GitHub or fork the Cisco CVD compute repository and use the fork as a centralized repository for your automation code. Configure an Ansible requirements file which allows the installation of multiple collections at the same time. When working with a fork, the Cisco Intersight collection only needs to be loaded as dependency for the roles part of the Cisco CVD Compute Collection.

Procedure 1. Create a new automation project repository

Step 1. Create the Ansible requirements.yml file in the root folder with following content:

```
---
collections:
  # Cisco Intersight Collection
  - name: cisco.intersight
  # Cisco CVD Compute Collection
  - name: cisco.cvd_compute
```

Step 2. Optionally, specify a version tag to force the usage of a specific version instead of the latest version.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Step 3. Create an initial playbook in the root folder. In this example we use the Cisco UCS chassis rediscovery role of the Cisco CVD Compute Collection.

```
---
- name: Test Cisco UCS chassis rediscovery in Cisco Intersight
  hosts: localhost
  vars:
    rediscover_ucs_chassis_name_list: ['AC05-6454-1']
  roles:
    rediscover_ucs_chassis
```

> **Note:** The playbook variables for the Intersight API ID and private key are managed by the Cisco Intersight API credential within the Ansible Automation Platform.

Step 4. Create a fine-grained personal access token (PAT).

Step 5. Select the appropriate expiration date and limit the access to this single repository or according to your needs.

Step 6. Add the Permission "Deployments"

Step 7. Click Generate token and save the token.

Configure Ansible Automation Platform

Procedure 1. Create GitHub credential

Provide access to the automation project GitHub repository.

Step 1. Log into Ansible Automation Platform with your user credentials.

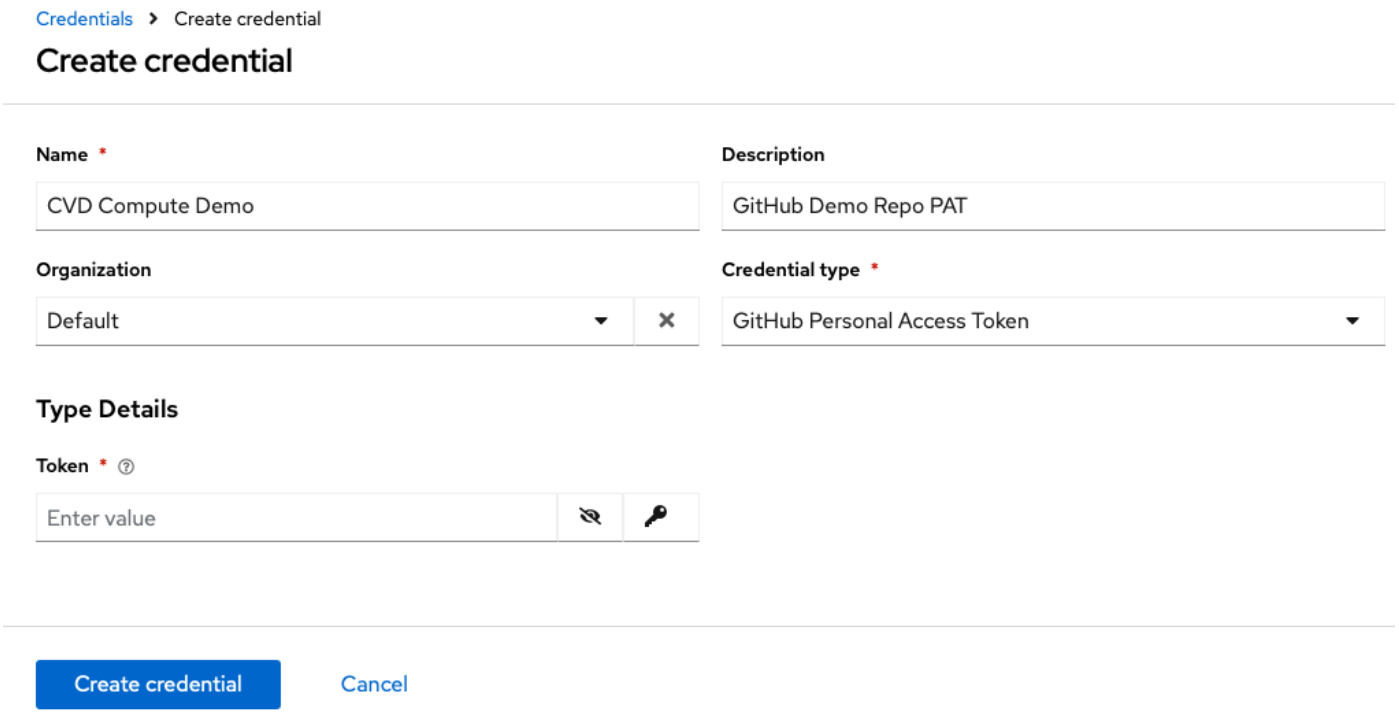
Step 2. From the navigation panel, select Automation Execution > Infrastructure > Credentials.

Step 3. Click Create credential.

Step 4. Provide a credential name and the PAT to access the GitHub repository.

Step 5. Click Create Credential.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.



Procedure 2. Grant GitHub access

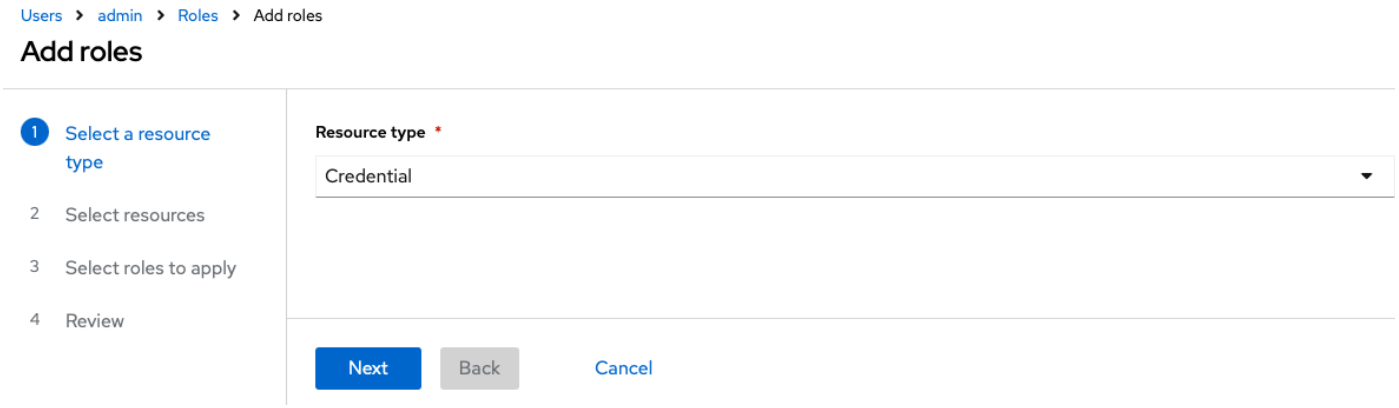
Assign a new role to the user to grant access to use and read the GitHub credential.

Step 1. From the navigation panel, select Access Management > Users.

Step 2. Select the user and change to the roles tab

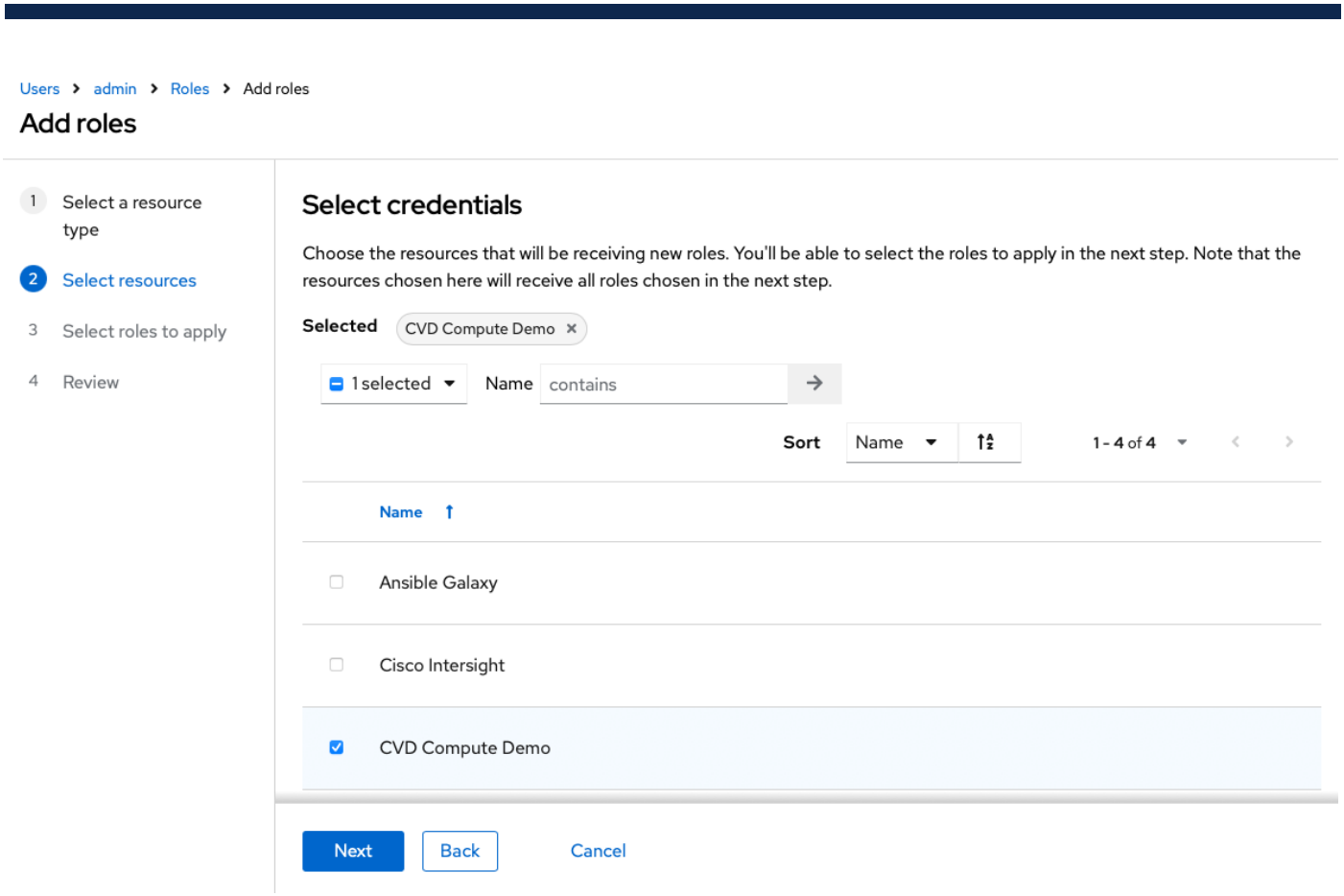
Step 3. Click Add Roles.

Step 4. Select credential as resource type and click Next.

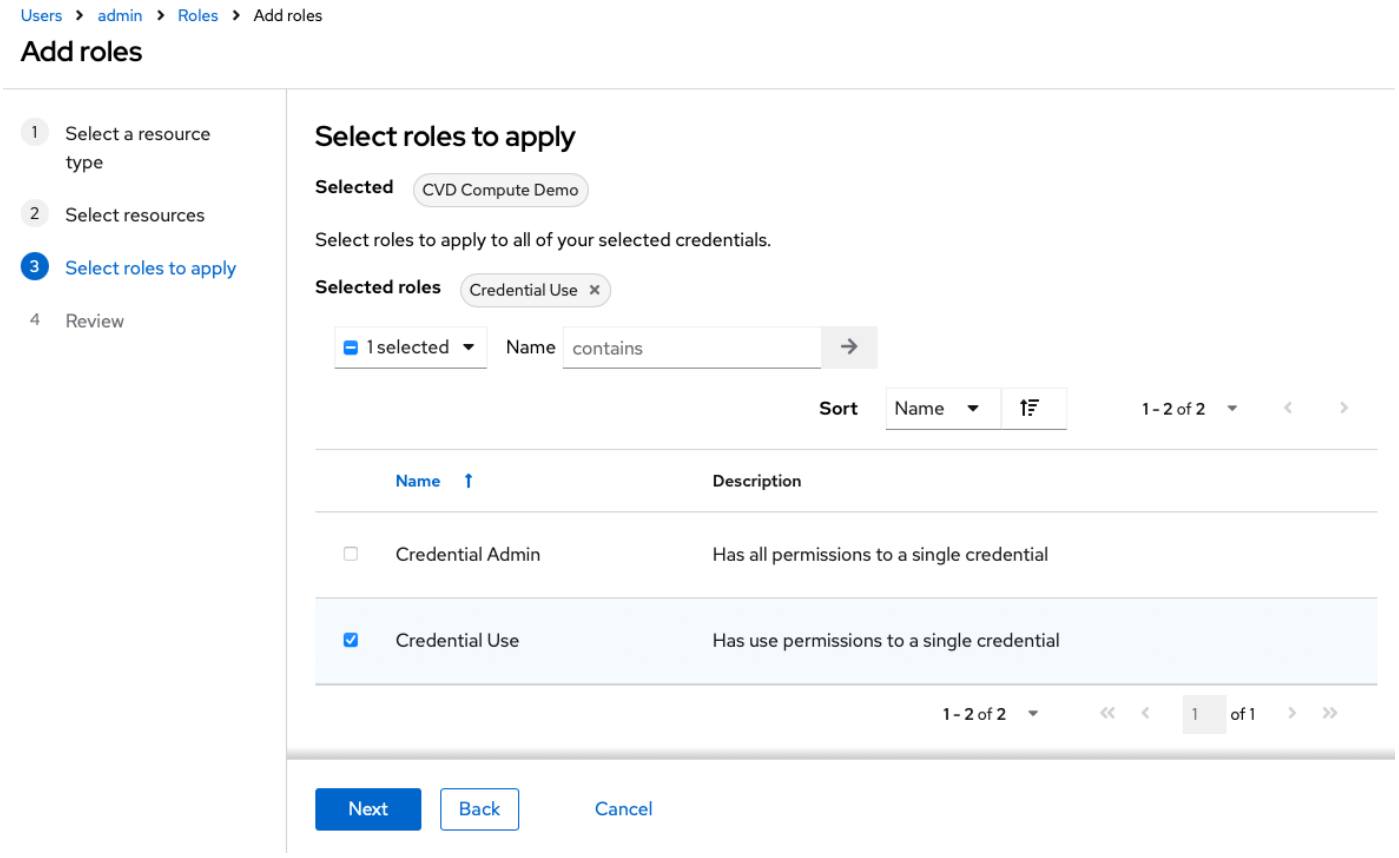


Step 5. Select the credential name, in this example CVD Compute Demo, and click Next.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.



Step 6. Select Credential Use and click Next.



© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Step 7. Review the role configuration and click Finish to add the role.

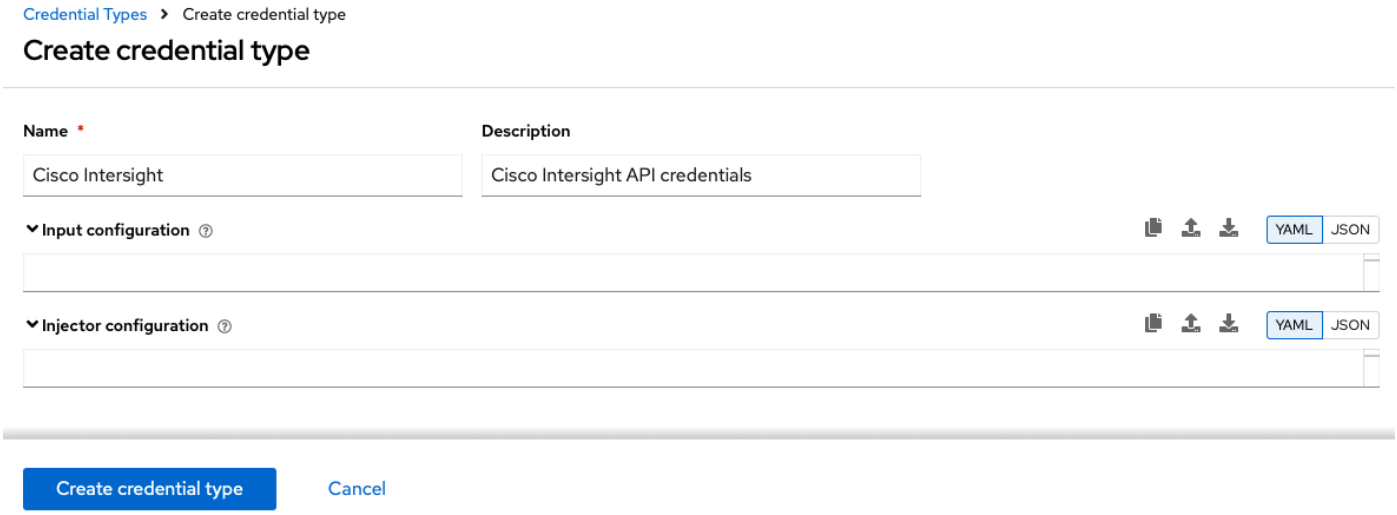
Procedure 3. Create Cisco Intersight API credential type

Create a new credential type to store Cisco Intersight API credentials.

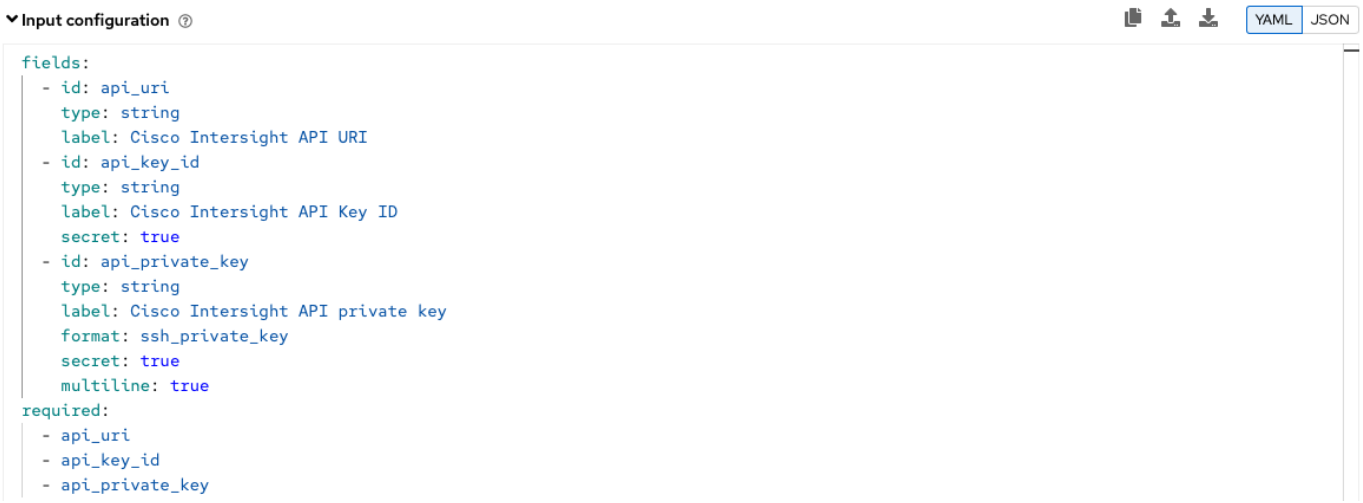
Step 1. From the navigation panel, select Automation Execution > Infrastructure > Credential Types.

Step 2. Click Create credential type.

Step 3. Enter a credential type name and description.



Step 4. Enter the following YAML code as input configuration:



Step 5. Enter the following YAML code as Injector configuration:



Step 6. Click Create Credential Type to save the new credential type.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Procedure 4. Create Cisco Intersight API credential

Create a credential to store the Cisco Intersight API ID and private key.

Step 1. From the navigation panel, select Automation Execution > Infrastructure > Credential.

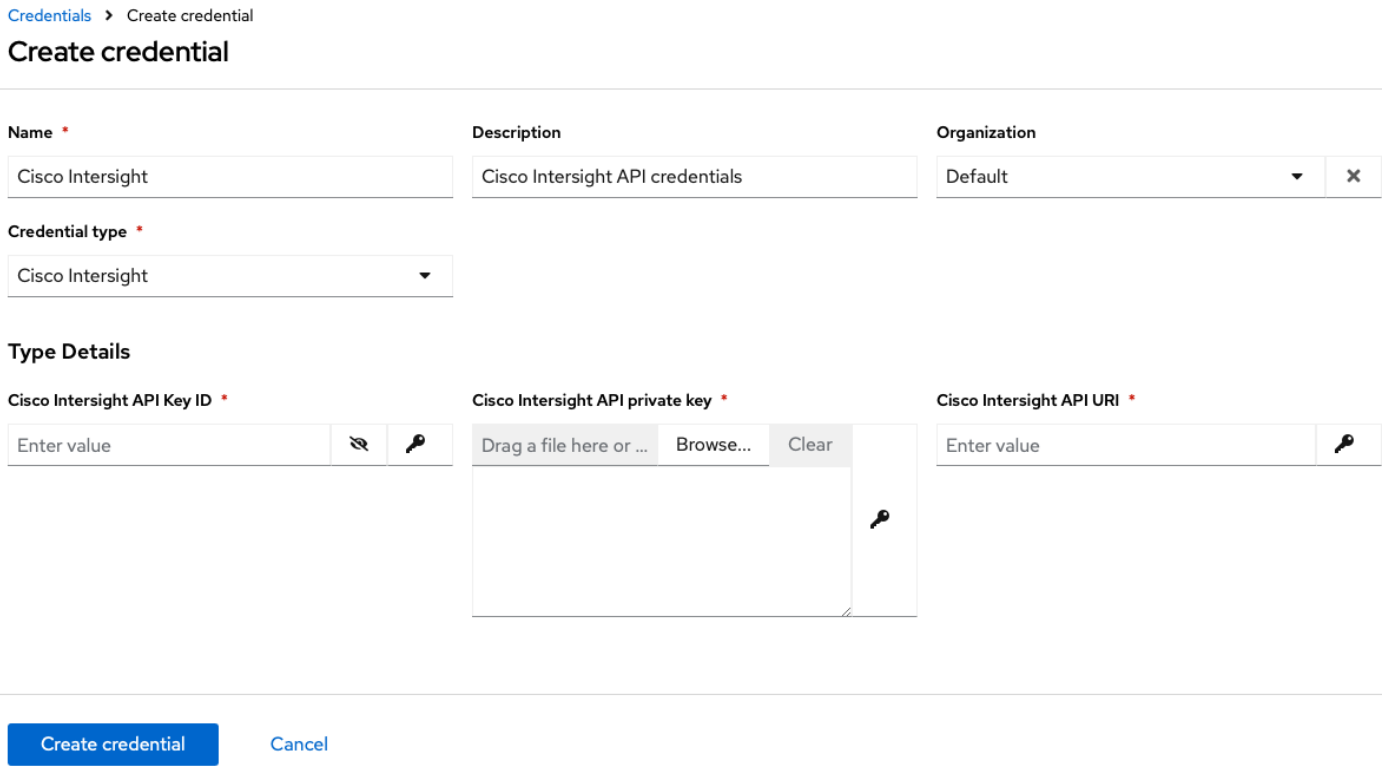
Step 2. Click Create credential.

Step 3. Provide a credential name and description. Select the organization and the credential type created before, in this example Cisco Intersight.

Step 4. Enter the API key ID, the API private key and the endpoint URI https://intersight.com/api/v1.

Step 5. Click Create credential.

> **Note:** The configuration of the endpoint URI is optional. The roles default to https://intersight.com/api/v1.



Ansible Automation Platform Project Setup

A project in Ansible Automation Platform is a logical collection of Ansible playbooks, represented in the controller.

To run your playbook in Ansible Automation Platform, create a project in the automation controller which is linked to the GitHub repository where you store your automation playbooks. Afterwards, create a job template for each playbook required as part of the project.

Procedure 1. Project set up

Now all prerequisites are complete and you are ready to set up a new project.

Step 1. From the navigation panel, select Automation Execution > Projects.

Step 2. Click Create Project.

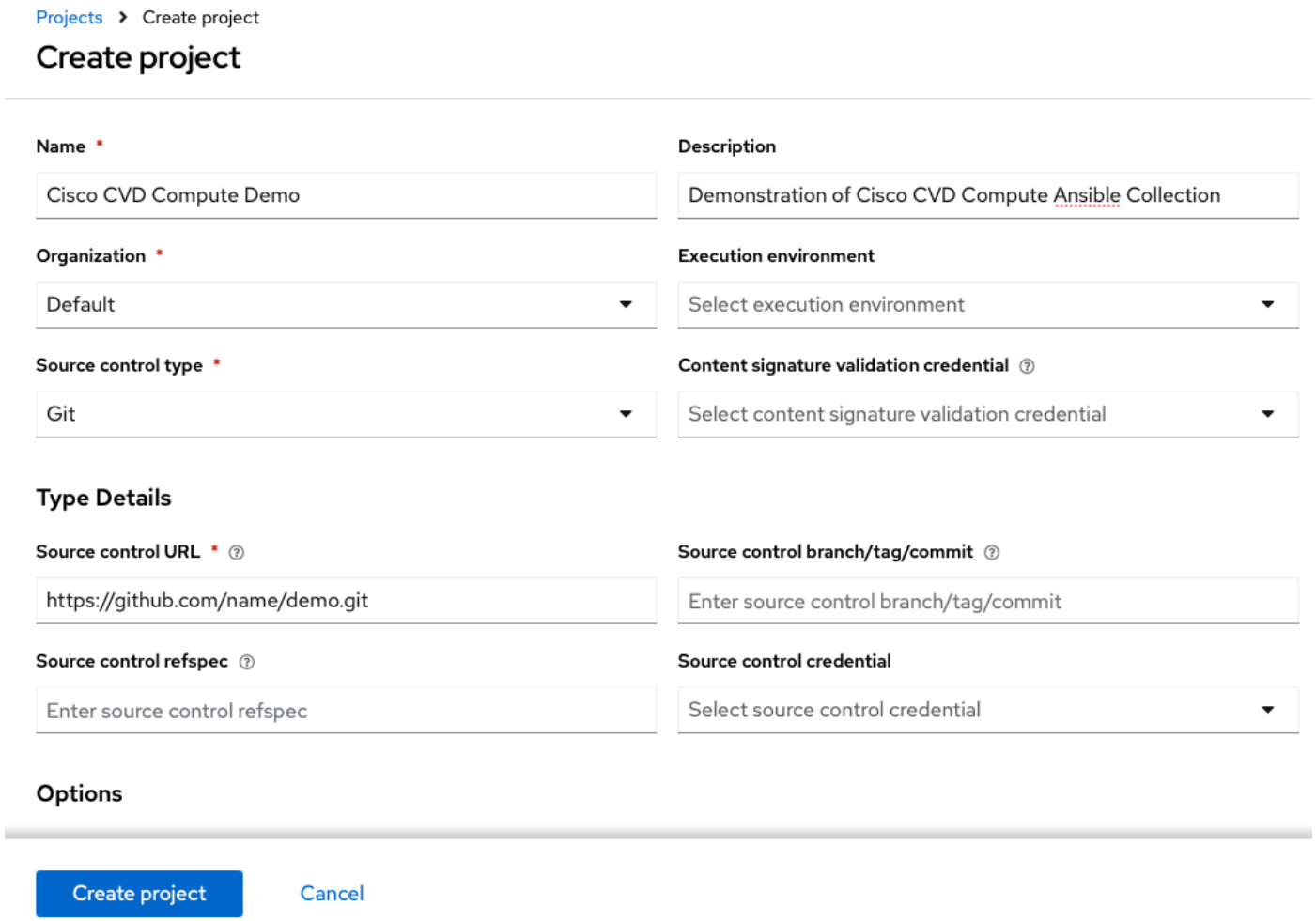
© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Step 3. Enter a project name, a description, and select the organization.

Step 4. Select Git as source control type.

Step 5. Provide the source control URL, https://github.com/<user name>/<repository-name>.git

Step 6. Click Create project.



Confirm the project has been synced successful before creating a job template. You can manually start a synchronization against the SCM system and update the project from the Details tab, Sync button, or from the project list view and click the sync button next to the project name.

During the sync, the controller will automatically detect the Ansible requirements file and download the specified collections from the configured automation hub.

Procedure 2. Create a job template

A job template is a definition and set of parameters for running an Ansible job. Create a job template based on a playbook within the GitHub automation project repository.

Step 1. From the navigation panel, select Automation Execution > Templates. Click Create template.

Step 2. Click Create job template.

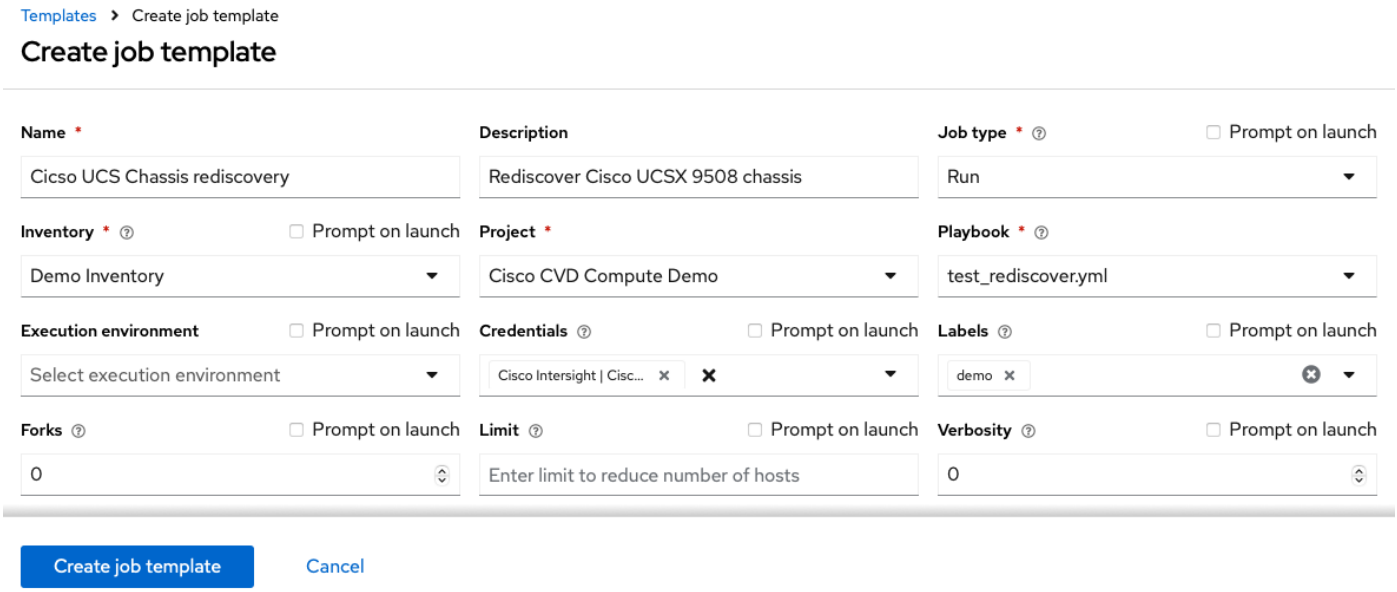
Step 3. Provide a job template name and description.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Step 4. Select the project created before from the drop-down list, in this example Cisco CVD Compute Demo. The demonstration and validation repository contains a single playbook only which is pre-selected automatically.

Step 5. Select the Cisco Intersight credentials.

Step 6. Optionally, create a label that describes the job template and keep the other settings on default.



Step 7. Click Create job template.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Validate

This chapter contains the following:

- Test Plan

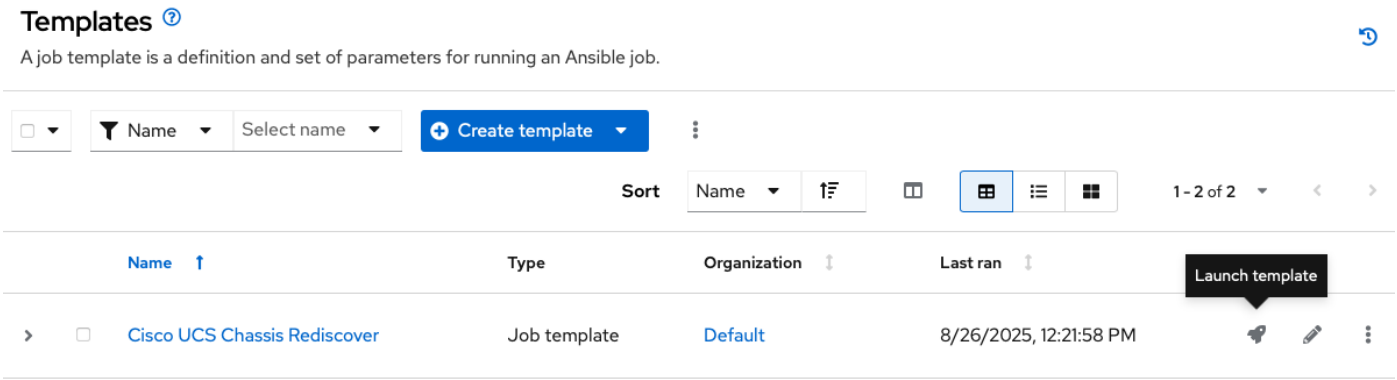
Test Plan

Procedure 1. Implement the Test Plan

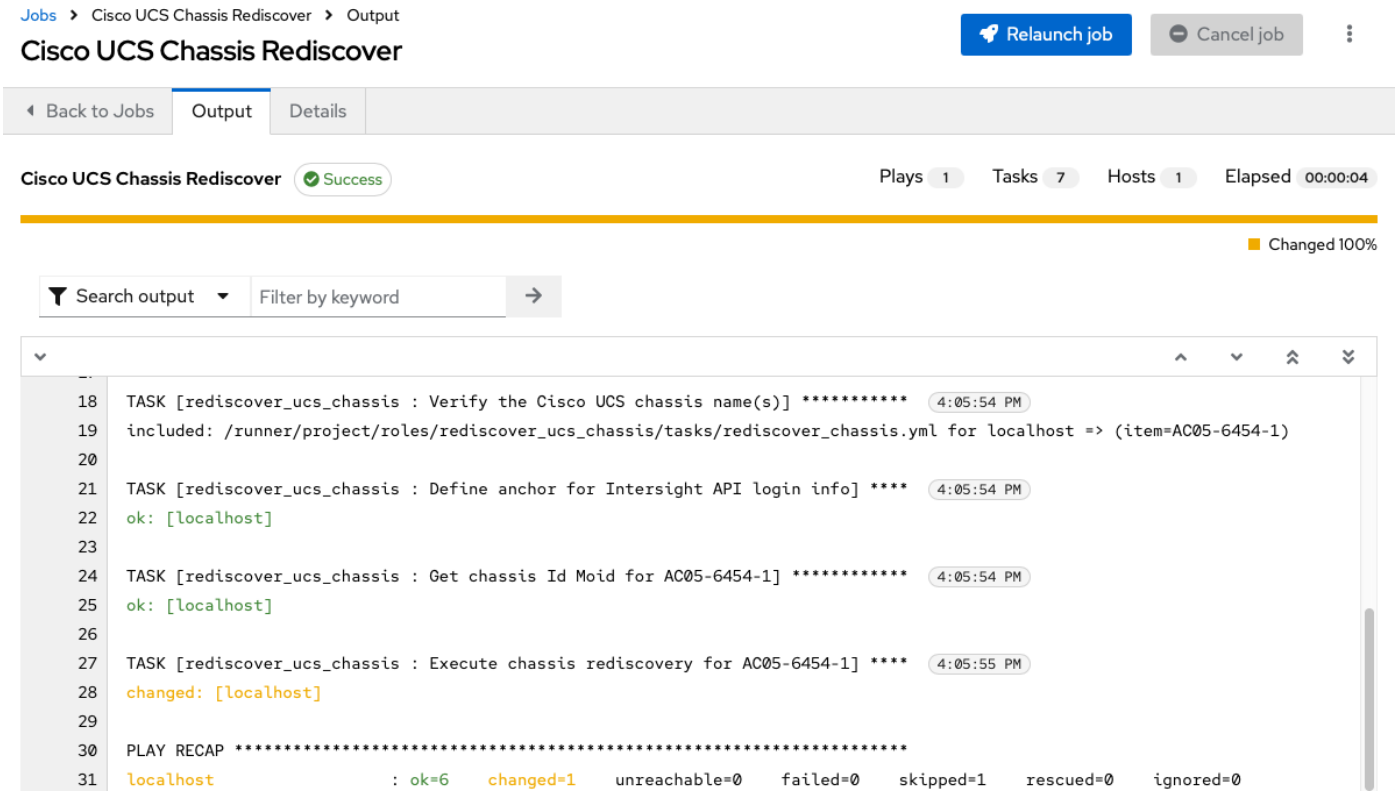
Run the playbook from the automation controller by launching the job template.

Step 1. From the navigation panel, select Automation Execution > Templates.

Step 2. Click the launch template button next to the job template.



Step 3. Verify the successful job execution from the job output screen.



Step 4. Verify the successful job execution from the Requests page in Cisco Intersight.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Name	Status	Target Type	Target Name	Start Time	Duration	ID	Execution Type
Blade Discovery	Success	Blade Server	AC05-6454-1-1	7 minutes ago	4 m 34 s	68adbf4b696f6e...	Execute
Blade Discovery	Success	Blade Server	AC05-6454-1-8	7 minutes ago	4 m 23 s	68adbf4b696f6e...	Execute
Blade Discovery	Success	Blade Server	AC05-6454-1-2	7 minutes ago	4 m 35 s	68adbf4b696f6e...	Execute
Blade Discovery	Success	Blade Server	AC05-6454-1-5	7 minutes ago	4 m 24 s	68adbf4b696f6e...	Execute
Blade Discovery	Success	Blade Server	AC05-6454-1-7	7 minutes ago	3 m 51 s	68adbf4b696f6e...	Execute
Blade Discovery	Success	Blade Server	AC05-6454-1-6	7 minutes ago	4 m 22 s	68adbf4b696f6e...	Execute
Blade Discovery	Success	Blade Server	AC05-6454-1-3	7 minutes ago	4 m 13 s	68adbf4a696f6e...	Execute
Blade Discovery	Success	Blade Server	AC05-6454-1-4	7 minutes ago	3 m 47 s	68adbf4a696f6e...	Execute
Chassis Inventory	Success	Chassis	AC05-6454-1	7 minutes ago	7 s	68adbf47696f6e...	Execute
Chassis Inventory	Success	Chassis	AC05-6454-1	7 minutes ago	8 s	68adbf46696f6e...	Execute
Chassis Discovery	Success	Chassis	AC05-6454-1	7 minutes ago	2 s	68adbf44696f6e...	Execute
Chassis Discovery	Success	Chassis	AC05-6454-1	7 minutes ago	2 s	68adbf44696f6e...	Execute
Chassis Rediscover	Success	Chassis	AC05-6454-1	7 minutes ago	1 s	68adbf43696f6e...	Execute

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Conclusion

This Cisco Validated Design for Cisco UCS Day 2 Operations with the Red Hat Ansible Automation Platform demonstrates a powerful and practical approach to modern infrastructure management. As organizations increasingly seek to optimize their IT environments, the automation of Day 2 tasks—including continuous compliance, security enforcement, resource scaling, and performance optimization—becomes paramount for ensuring long-term efficiency and stability.

By leveraging the robust capabilities of the Red Hat Ansible Automation Platform and the newly introduced Ansible validated content aligned with Cisco Validated Designs, customers can achieve full automation of Day 0, Day 1, and Day 2 operations. This integrated solution simplifies complex tasks such as Fabric Interconnect firmware updates, port configuration, chassis profile management, and vNIC/VLAN adjustments, significantly reducing manual effort and potential human error.

The " Infrastructure as Code" paradigm, central to this solution, empowers IT teams to treat their infrastructure configurations with the same rigor and benefits as software development, leading to improved quality, consistency, traceability, and accelerated deployment cycles. Coupled with Cisco Intersight's unified management and API-driven capabilities, this validated design provides a scalable, secure, and automated foundation for modernizing application infrastructure and data center computing.

In conclusion, the integration of Cisco UCS with Ansible Automation Platform, supported by the certified and validated content, delivers a streamlined and secure experience. It enables organizations to enhance system reliability, improve security posture, and dynamically scale resources, ultimately driving greater operational agility and business value.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

About the author

Joerg Wolters, Technical Marketing Engineer, Cisco Systems GmbH

As a member of the Cisco Cloud + AI infrastructure business unit, Joerg brings over 20 years of expertise in data center applications and technologies. At Cisco, Joerg manages hardware architectures, drives feature and product introductions, and shapes Cisco Validated Design and Deployment guidelines for Cisco UCS Converged Infrastructure and solutions.

Acknowledgements

For their support and contribution to the design, validation, and creation of the Cisco CVD Compute Collection and this Cisco Validated Design, the author would like to thank:

- Archana Sharma, Technical Marketing Engineer, Cisco Systems Inc.
- John George, Technical Marketing Engineer, Cisco Systems Inc.
- Steve Fulmer, Principal Product Manager, Red Hat Inc.
- Martin Jackson, Senior Principal Software Engineer, Red Hat Inc.
- Ron Gershburg, Software Engineer, Red Hat Inc.
- Shahar Golshani, Principal Software Engineer, Red Hat Inc.

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Appendix

This appendix contains the following:

- Appendix A – References
- Appendix B – Acronym Glossary

Appendix A – References

Red Hat Ansible Automation Platform:

https://www.redhat.com/en/technologies/management/ansible

Red Hat Ansible Automation Platform 2.5 documentation:

https://docs.redhat.com/en/documentation/red_hat_ansible_automation_platform/2.5

Ansible Validated Content Collection for Cisco UCS Compute:

https://github.com/ucs-compute-solutions/cisco.cvd_compute

Cisco Intersight Help Center:

https://intersight.com/help/saas

Cisco Intersight Ansible Community Documentation:

https://docs.ansible.com/ansible/latest/collections/cisco/intersight/index.html

Cisco Intersight RESTful API:

https://www.intersight.com/apidocs/introduction/overview

Introduction to the Cisco Intersight REST API:

https://developer.cisco.com/learning/labs/cisco-intersight-rest-api-keys/introduction-to-the-cisco-intersight-rest-api

Appendix B – Acronym Glossary

This glossary addresses some acronyms used in this document, for the purposes of aiding understanding.

API – Application Programming Interface

APP – Ansible Automation Platform

CVD – Cisco Validated Design

DC – Data Center

IaC – Infrastructure as Code

RBAC – Role-based access control

REST – Representational State Transfer

SCM – Source Code Management System

UCS – Cisco Unified Computing System

URL – Uniform Resource Locator

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

VLAN – Virtual Local Area Network

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.

Feedback

For comments and suggestions about this guide and related guides, join the discussion on Cisco Community here: https://cs.co/en-cvds.

CVD Program

" DESIGNS") IN THIS MANUAL ARE PRESENTED " AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS X-Series, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series. Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trade-marks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. (LDW_P2)

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2025 Cisco Systems, Inc., and/or its affiliates. All rights reserved.