Red Hat
Ansible Automation
Platform

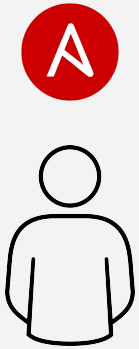
ANSIBLE AUTOMATION SECURITY COMPLIANCE

Overview of Ansible for Security Compliance

Red Hat

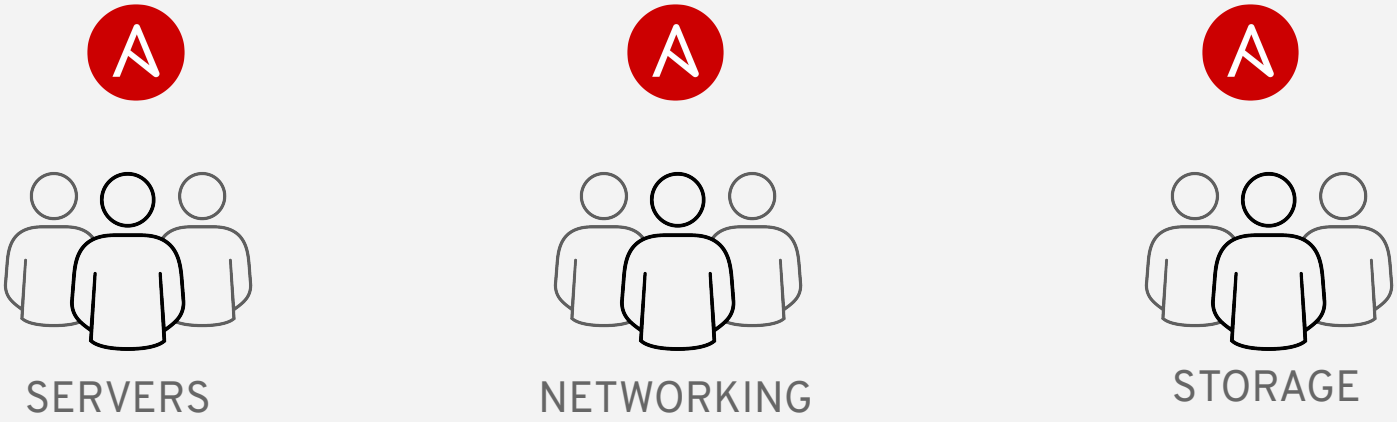
WHAT YOU WILL LEARN

- Intro: What is Ansible Automation
- How Ansible works for Security Compliance
- Playbook Basics
- Reuse and Redistribute of Ansible Content with Roles
- Surveys
- Auditing
- Ansible Tower API
- Red Hat Insights



Automation happens when one person meets a problem they never want to solve again

ANSIBLE ORCHESTRATES TECHNOLOGY



WHY ANSIBLE?

SIMPLE

Human readable automation

No special coding skills needed

Tasks executed in order

Usable by every team

More people can use automation

POWERFUL

App deployment

Configuration management

Workflow orchestration

Network automation

More use cases

AGENTLESS

Agentless architecture

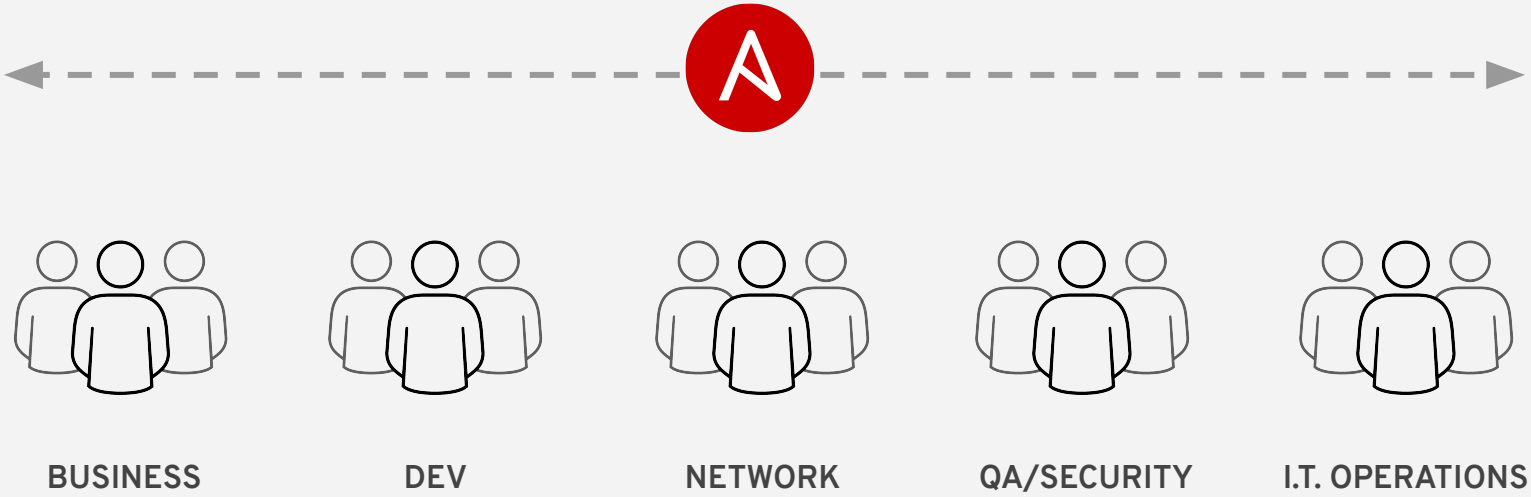
Uses OpenSSH & WinRM

No agents to exploit or update

Get started immediately

More devices and technology

ANSIBLE TOWER ORCHESTRATES YOUR TEAMS



Red Hat Ansible Automation Platform

Network | Lines of business | Security |  | Operations | Infrastructure | Developers

Engage	**Ansible Hosted Services:** Engage users with an automation focused experience
Scale	**Ansible Tower:** Operate & control at scale
Create	**Ansible Engine:** Universal language of automation

Fueled by an open source community

Red Hat

Red Hat Ansible Automation Platform

Network | Lines of business | Security | Operations | Infrastructure | Developers

Engage — **Ansible SaaS:** Engage users with an automation focused experience

Scale — **Ansible Tower:** Operate & control at scale

Create

- **Simple** — Human readable automation
- **Powerful** — Thousands of integrations
- **Agentless** — No agents to exploit or update

Fueled by an open source community

Red Hat

Red Hat Ansible Automation Platform

Network | Lines of business | Security | Operations | Infrastructure | Developers

Engage

Ansible SaaS: Engage users with an automation focused experience

Scale

Control	Delegation	Scale
Web UI and API	Role Based Access Controls	Scalable Execution Capacity

Create

Ansible Engine: Universal language of automation

Fueled by an open source community

Red Hat

Red Hat Ansible Automation Platform

Network | Lines of business | Security | Operations | Infrastructure | Developers

Engage	**Knowledge** Automation Analytics	**Collaborate** Automation Hub	**Trusted** Certified content	**Accelerate** Collections
Scale	**Ansible Tower:** Operate & control at scale			
Create	**Ansible Engine:** Universal language of automation			

Fueled by an open source community

Red Hat

What can I do using Ansible?

Automate the deployment and management of your entire IT footprint.

Do this...

Orchestration	Configuration Management	Application Deployment	Provisioning	Continuous Delivery	Security and Compliance

On these...

Firewalls	Load Balancers	Applications	Containers	Clouds
Servers	Infrastructure	Storage	Network Devices	**And more...**

Ansible automates technologies you use

Time to automate is measured in minutes

Cloud

AWS
Azure
Digital Ocean
Google
OpenStack
Rackspace
+more

Operating Systems

Rhel And Linux
Unix
Windows
+more

Virt & Container

Docker
VMware
RHV
OpenStack
OpenShift
+more

Storage

Netapp
Red Hat Storage
Infinidat
+more

Windows

ACLs
Files
Packages
IIS
Regedits
Shares
Services
Configs
Users
Domains
+more

Network

Arista
A10
Cumulus
Bigswitch
Cisco
Cumulus
Dell
F5
Juniper
Palo Alto
OpenSwitch
+more

Devops

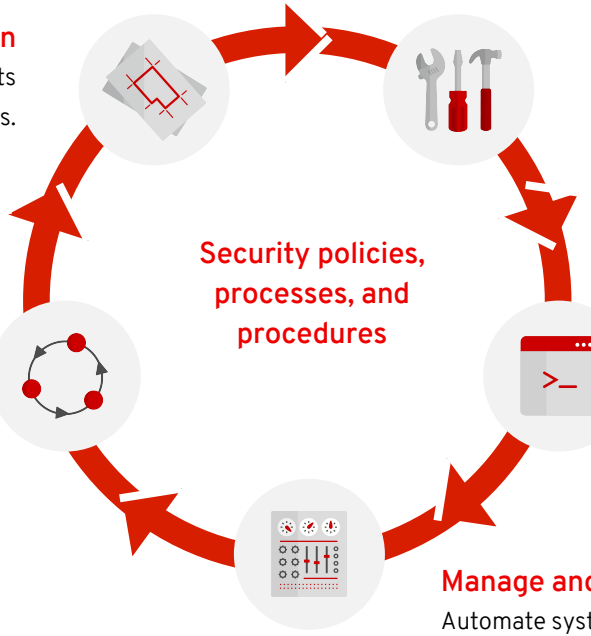
Jira
GitHub
Vagrant
Jenkins
Bamboo
Atlassian
Subversion
Slack
Hipchat
+more

Monitoring

Dynatrace
Airbrake
BigPanda
Datadog
LogicMonitor
Nagios
New Relic
PagerDuty
Sensu
StackDriver
Zabbix
+more

Security must be continuous and holistic

And integrated throughout the I.T. life cycle



Design
Identify security requirements and governance models.

Build
Build security in from the start, not as an afterthought.

Run
Deploy to trusted platforms with enhanced security capabilities.

Manage and Automate
Automate systems to meet security and compliance needs.

Adapt
Revise, updated, and remediate as landscape and needs change.

Red Hat

Red Hat management and automation

Life-cycle management, automated remediation, and prescriptive analytics

Red Hat Satellite

Unified life-cycle management

- Content and patch management
- Small- and large-scale operations
- Standardized operating environment (SOE)

Red Hat Ansible Automation

Centralized automation governance

- Centralized control
- Team and user delegation
- Audit trail

Red Hat Insights

Proactive, automated resolution

- Continuous insight
- Verified knowledge
- Proactive resolution

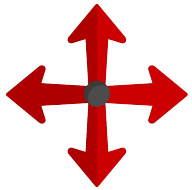
Red Hat Enterprise Linux

Red Hat

How Red Hat delivers automated security and compliance

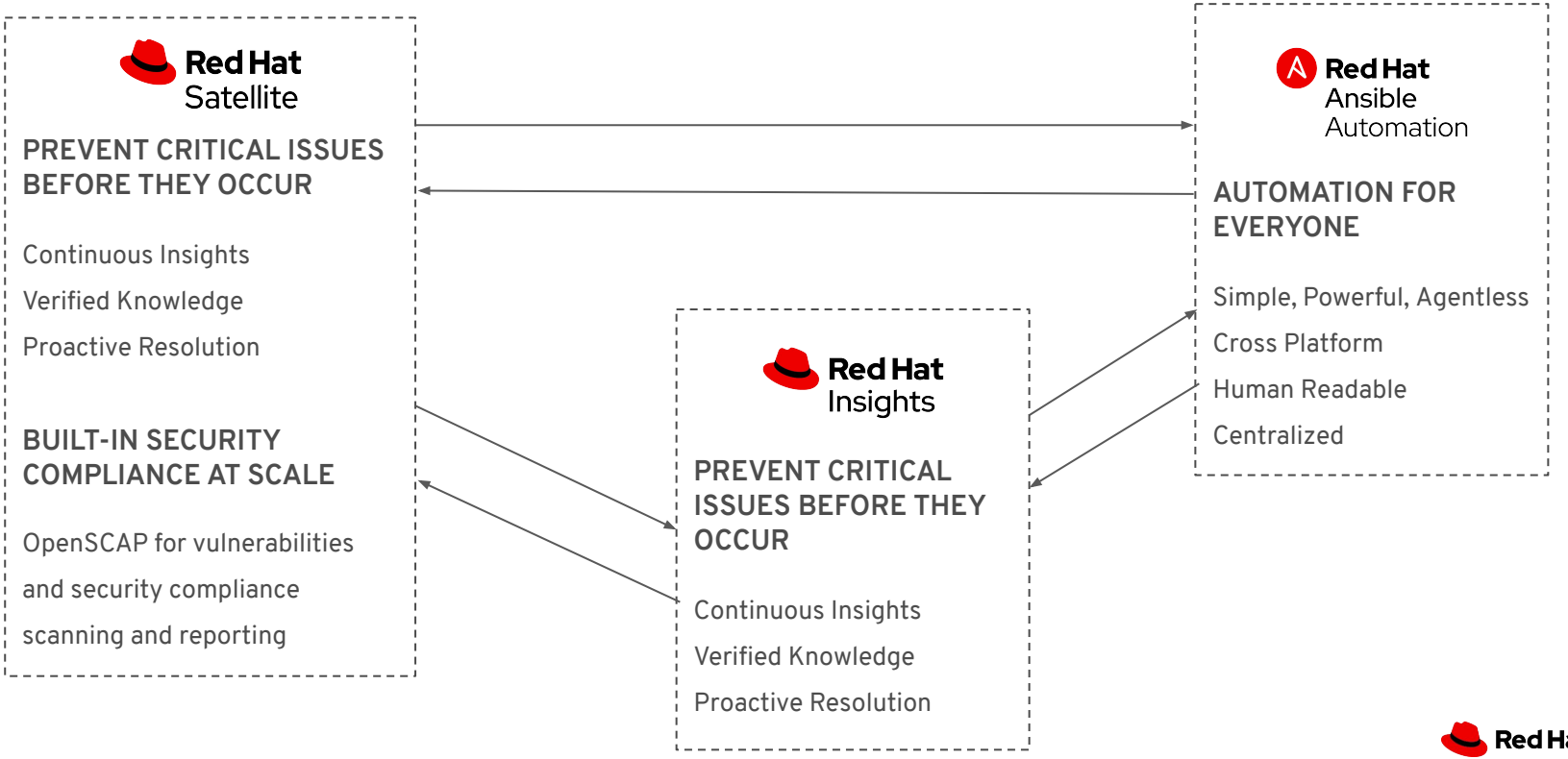
Security and Compliance automation at scale

Security and Compliance as code



Configuration Management

Red Hat Management Portfolio for Automated Security and Compliance



Red Hat

Security at scale with Red Hat Ansible Tower

Centralized

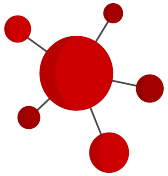
Share one common view

- Overview of present and past
- Dynamic inventory management
- Automation workflows
- Job scheduling
- Ongoing compliance checking
- Centralized job logging

Integrated

Connect with everything

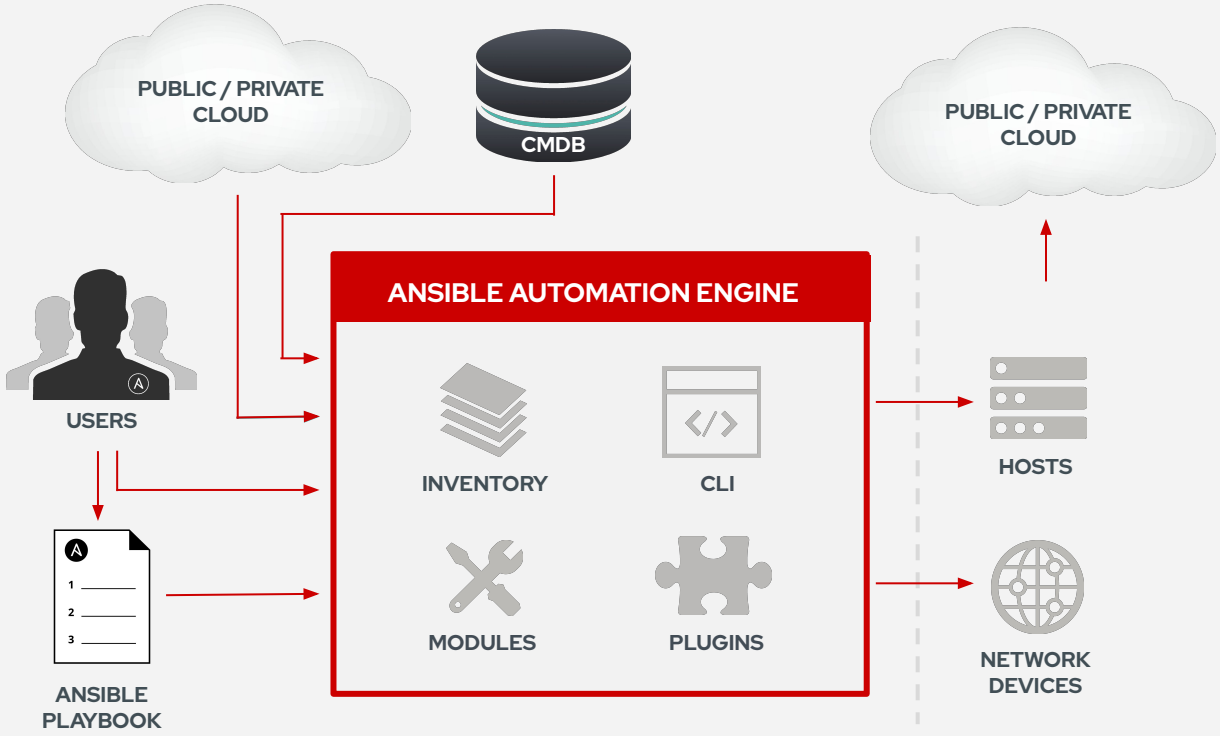
- Simple, powerful application programming interface (API)
- Representational state transfer (REST) architecture for fast adoption
- Easy, agentless integration



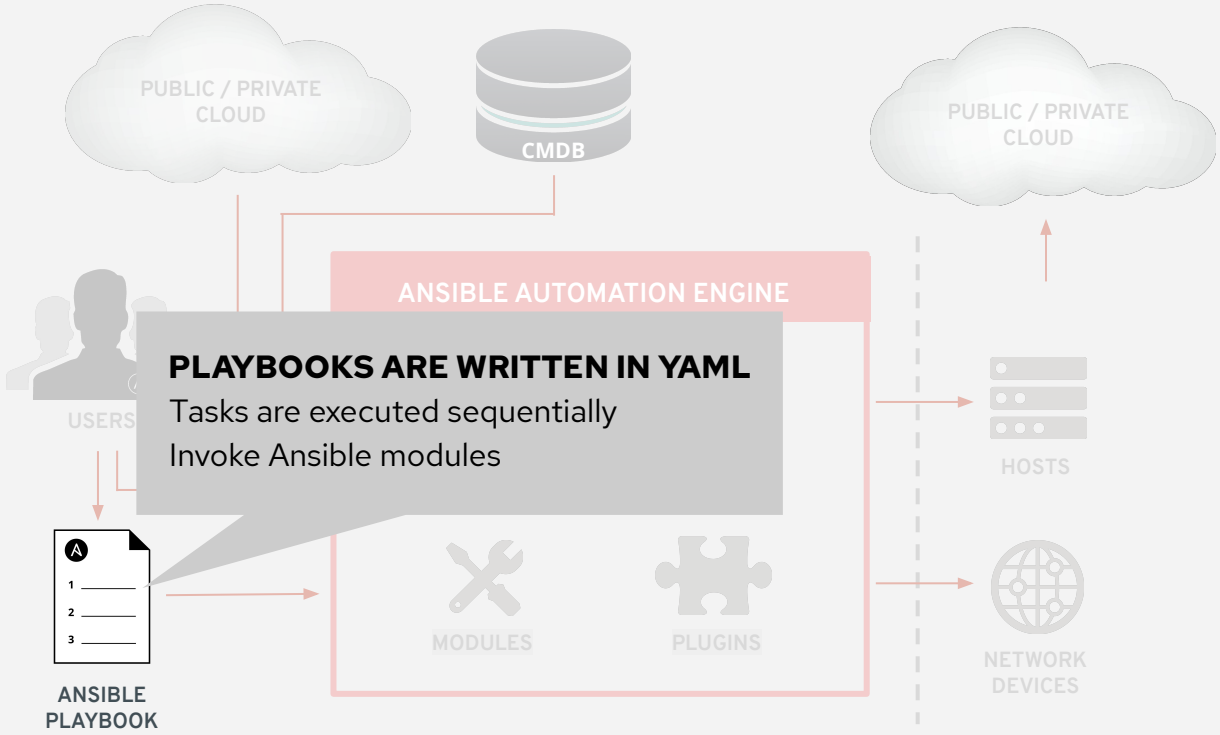
Accessible

Separate access and execution

- Role-based access controls (RBAC)
- Protected credential deposits
- Unprivileged access assignments

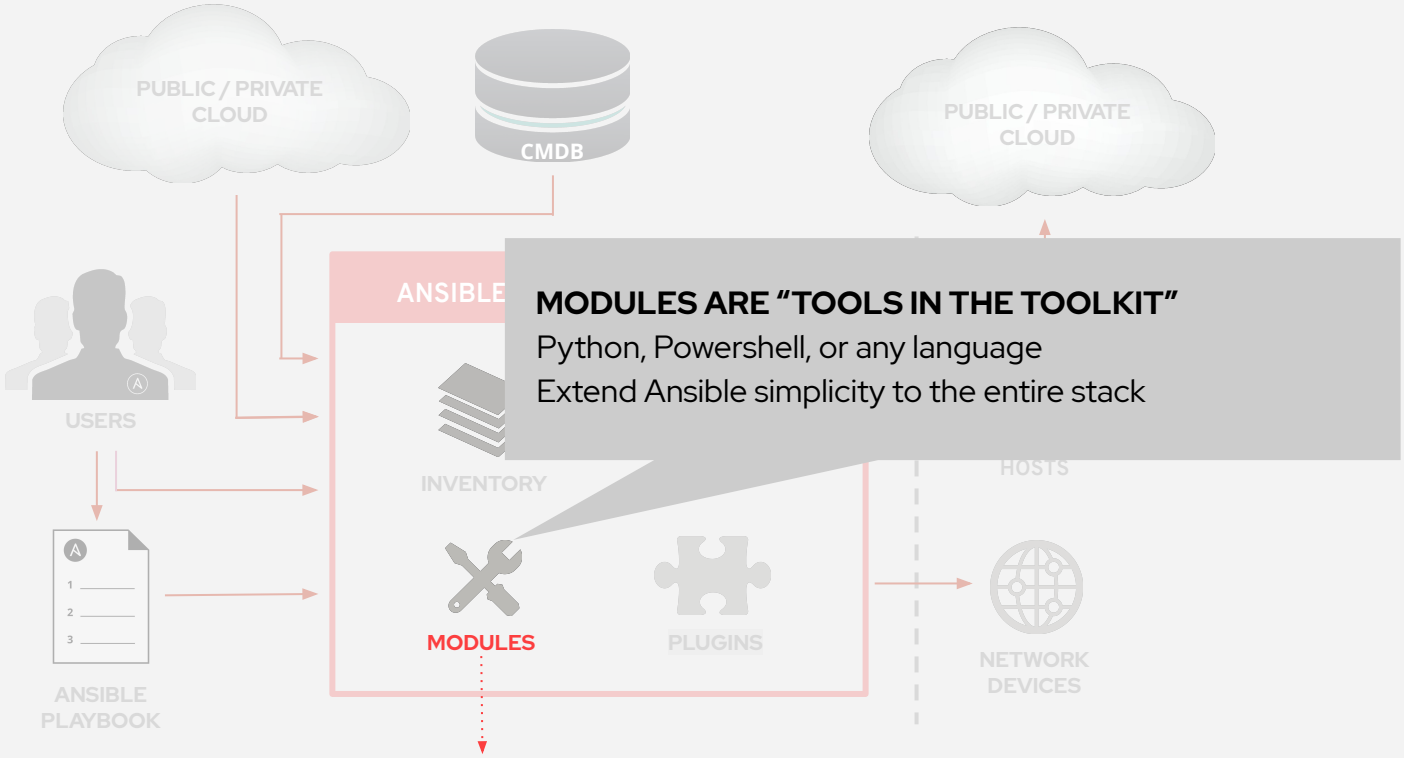

PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
ANSIBLE AUTOMATION ENGINE
USERS
INVENTORY
CLI
HOSTS
MODULES
PLUGINS
ANSIBLE PLAYBOOK
NETWORK DEVICES

Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
ANSIBLE AUTOMATION ENGINE
USERS
PLAYBOOKS ARE WRITTEN IN YAML
Tasks are executed sequentially
Invoke Ansible modules
HOSTS
MODULES
PLUGINS
NETWORK DEVICES
ANSIBLE PLAYBOOK

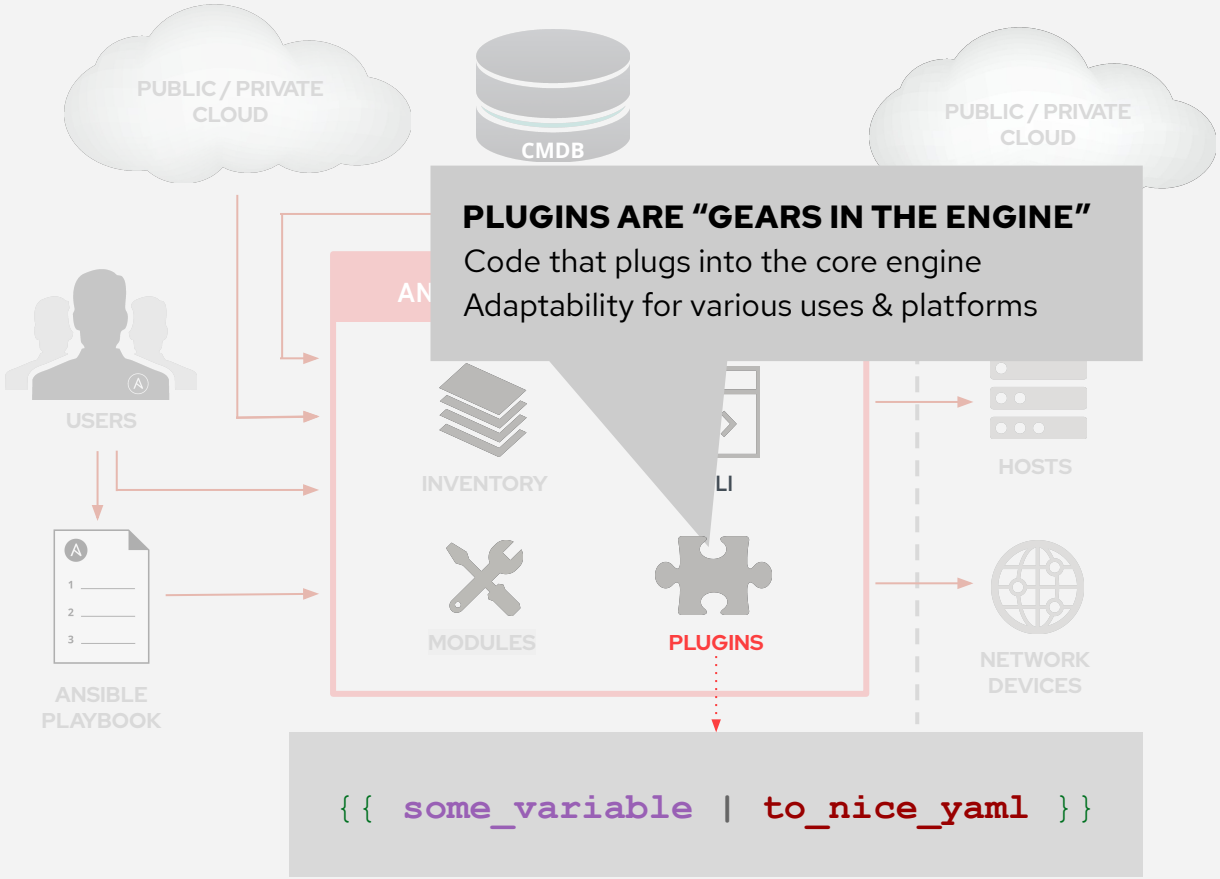
Red Hat

```yaml
---
- name: Ensure Firewall is running
  hosts: web
  become: yes
  tasks:
    - name: Firewall package is installed
      yum:
        name: firewalld
        state: latest

    - name: Firewall is running
      service:
        name: firewalld
        state: started
        enabled: true

    - name: https traffic is allowed
      firewalld:
        service: https
        permanent: yes
        state: enabled
        immediate: yes
```

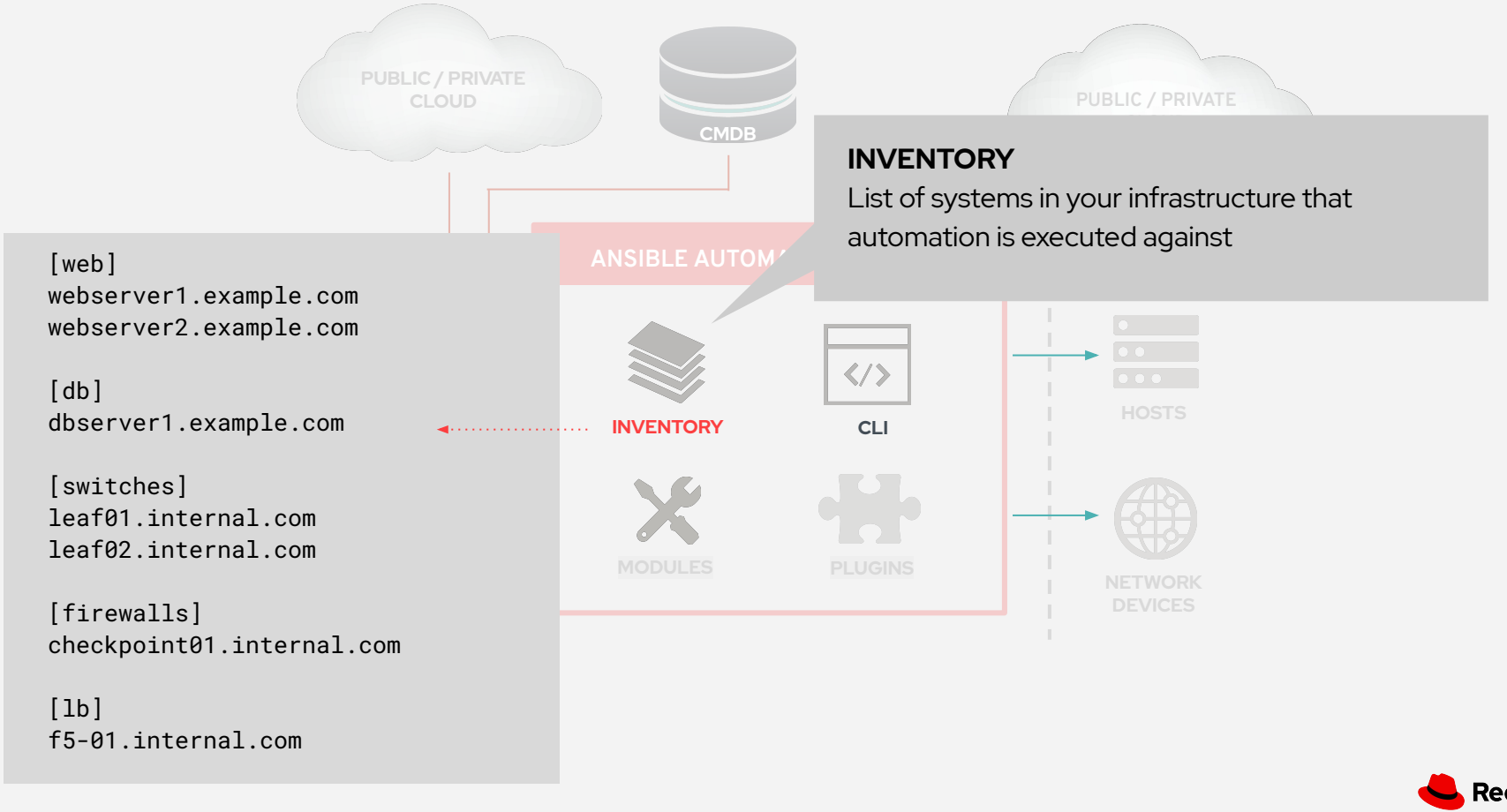



```
- name: Firewall package is installed
  yum:
    name: firewalld
    state: latest
```

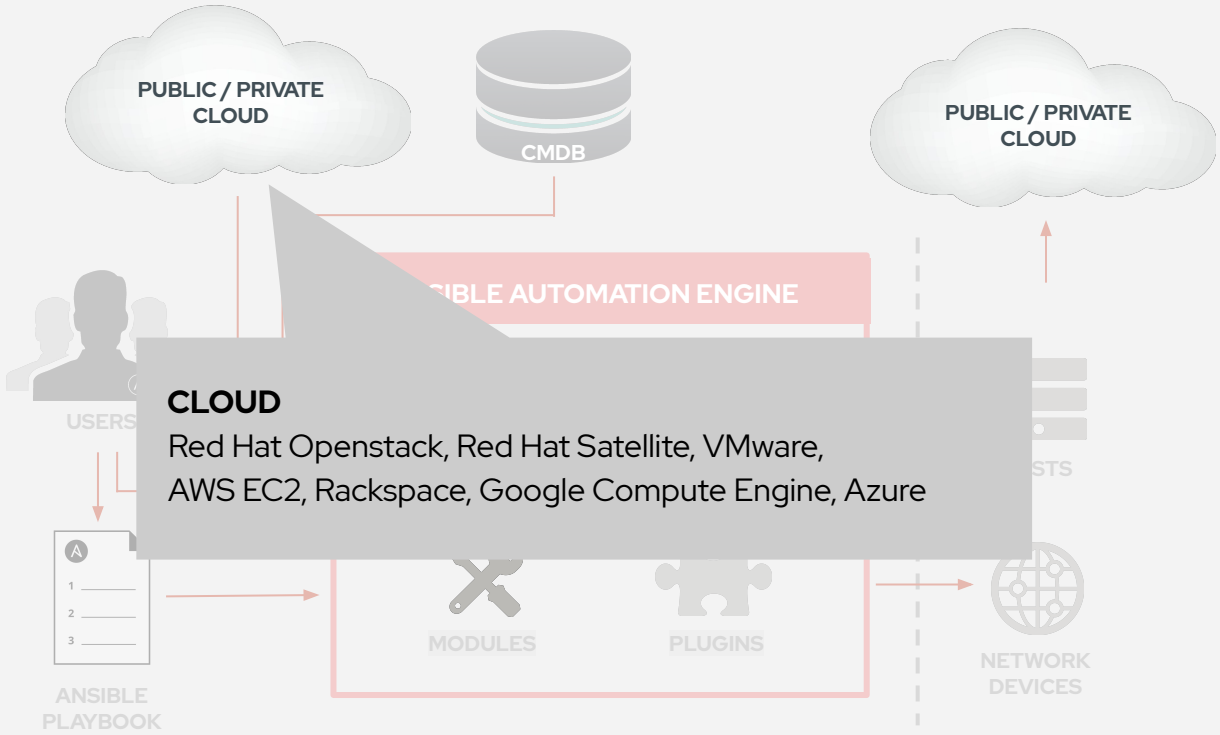
Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
PLUGINS ARE "GEARS IN THE ENGINE"
Code that plugs into the core engine
Adaptability for various uses & platforms
USERS
INVENTORY
HOSTS
MODULES
PLUGINS
NETWORK DEVICES
ANSIBLE PLAYBOOK
{{ some_variable | to_nice_yaml }}

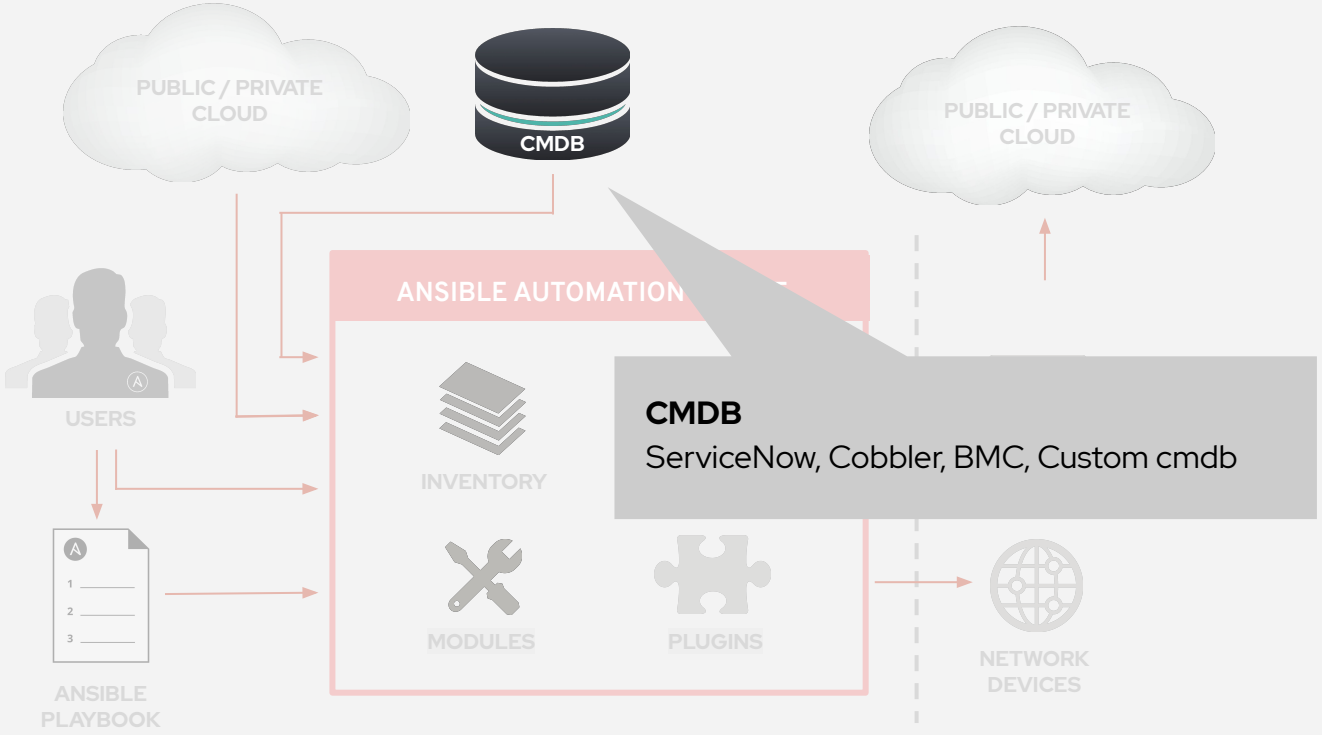
Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE
INVENTORY
List of systems in your infrastructure that automation is executed against
[web]
webserver1.example.com
webserver2.example.com
[db]
dbserver1.example.com
[switches]
leaf01.internal.com
leaf02.internal.com
[firewalls]
checkpoint01.internal.com
[lb]
f5-01.internal.com
ANSIBLE AUTOM
INVENTORY
CLI
MODULES
PLUGINS
HOSTS
NETWORK DEVICES

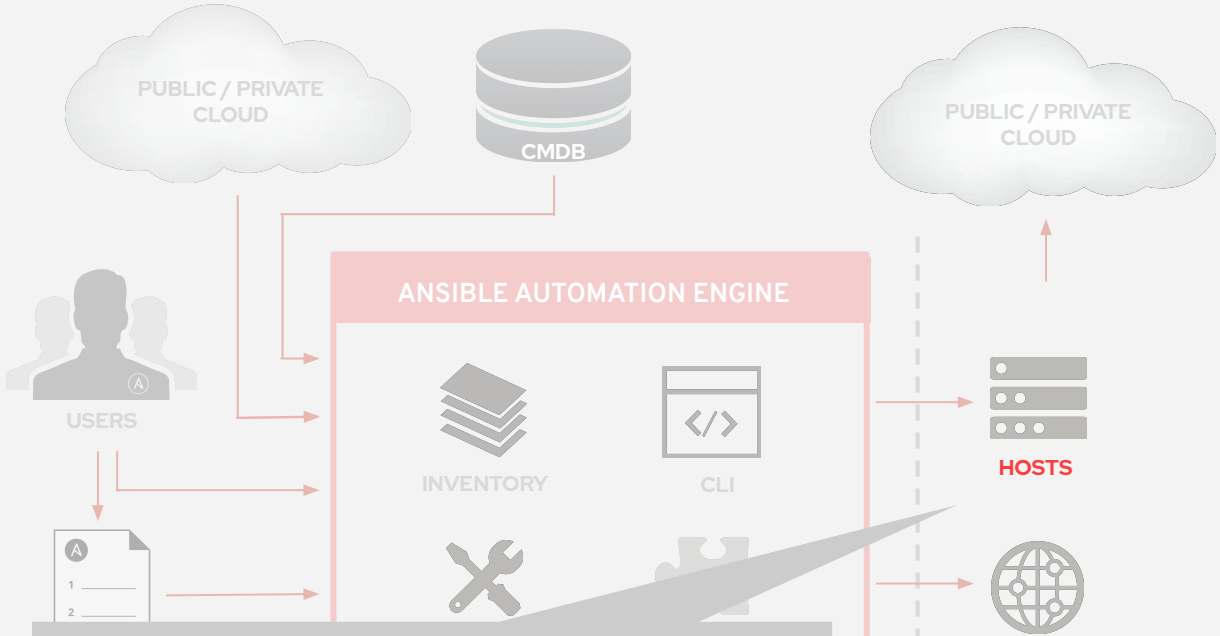
Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
IBLE AUTOMATION ENGINE
USERS
CLOUD
Red Hat Openstack, Red Hat Satellite, VMware,
AWS EC2, Rackspace, Google Compute Engine, Azure
STS
MODULES
PLUGINS
NETWORK DEVICES
ANSIBLE PLAYBOOK

Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
ANSIBLE AUTOMATION
USERS
INVENTORY
CMDB
ServiceNow, Cobbler, BMC, Custom cmdb
MODULES
PLUGINS
NETWORK DEVICES
ANSIBLE PLAYBOOK

Red Hat



AUTOMATE EVERYTHING

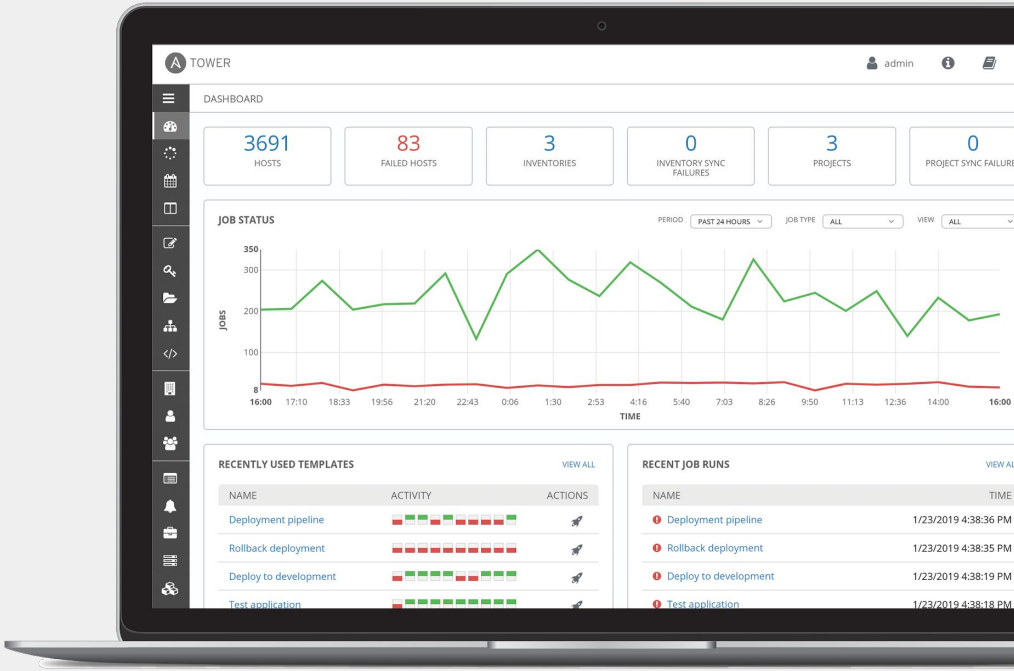
Red Hat Enterprise Linux, Cisco routers, Arista switches, Juniper routers, Windows hosts, Check Point firewalls, NetApp storage, F5 load balancers and more

Red Hat

What is Ansible Tower?

Ansible Tower is a UI and RESTful API allowing you to scale IT automation, manage complex deployments and speed productivity.

- Role-based access control
- Deploy entire applications with push-button deployment access
- All automations are centrally logged
- Powerful workflows match your IT processes



Red Hat

Red Hat Ansible Tower

RBAC

Allow restricting playbook access to authorized users. One team can use playbooks in check mode (read-only) while others have full administrative abilities.

Push button

An intuitive user interface experience makes it easy for novice users to execute playbooks you allow them access to.

RESTful API

With an API first mentality every feature and function of Tower can be API driven. Allow seamless integration with other tools like ServiceNow and Infoblox.

Workflows

Ansible Tower's multi-playbook workflows chain any number of playbooks, regardless of whether they use different inventories, run as different users, run at once or utilize different credentials.

Enterprise integrations

Integrate with enterprise authentication like TACACS+, RADIUS, Azure AD. Setup token authentication with OAuth 2. Setup notifications with PagerDuty, Slack and Twilio.

Centralized logging

All automation activity is securely logged. Who ran it, how they customized it, what it did, where it happened - all securely stored and viewable later, or exported through Ansible Tower's API.

Red Hat


Red Hat
Ansible
Automation
Working With Ansible Inventory
Red Hat

Understanding Inventory - Basic

```
# Static inventory example:
[myservers]
10.42.0.2
10.42.0.6
10.42.0.7
10.42.0.8
10.42.0.100
host.example.com
```

Understanding Inventory - Variables

```
[app1srv]
appserver01 ansible_host=10.42.0.2
appserver02 ansible_host=10.42.0.3

[web]
node-[1:30] ansible_host=10.42.0.[31:60]

[web:vars]
apache_listen_port=8080
apache_root_path=/var/www/mywebdocs/

[all:vars]
ansible_user=kev
ansible_ssh_private_key_file=/home/kev/.ssh/id_rsa
```

Understanding Inventory - Variable Precedence

```
[webservers]
web01 ansible_host=52.14.208.176 tmp_dir=/tempdir
web02 ansible_host=52.14.208.179 tmp_dir=/tmpwsdir

[appservers]
app01 ansible_host=18.221.195.152
app02 ansible_host=18.188.124.127

[loadbalancers]
balancer01 ansible_host=3.15.11.56

[webservers:vars]
ansible_user=ec2-user
ansible_notify_owner=frances
apache_max_clients=288
```

Host variables apply to the host and override group vars

Group variables apply for all devices in that group

Red Hat

Ansible Inventory - Managing Variables In Files

```
[user@ansible ~]$ tree /somedir

/somedir
├── group_vars
│   ├── app1srv
│   ├── db
│   └── web
├── inventory
└── host_vars
    ├── app01
    ├── app02
    └── app03
```

```
[user@ansible ~]$ cat /somedir/inventory

[web]
node-[1:30] ansible_host=10.42.0.[31:60]

[appxsrv]
app01
app02
app03
```

```
[user@ansible ~]$ cat /somedir/group_vars/web

apache_listen_port: 8080
apache_root_path: /var/www/mywebdocs/
```

```
[user@ansible ~]$ cat /somedir/host_vars/app01

owner_name: Chris P. Bacon
owner_contact: 'cbacon@mydomain.tld'
server_purpose: Application X
```

Understanding Inventory - Groups

There is always a group called **"all"** by default

```
[nashville]
bnaapp01
bnaapp02

[atlanta]
atlapp03
atlapp04

[south:children]
atlanta
nashville
hsvapp05
```

Understanding Inventory - Windows

Windows systems use winrm for connectivity

```
[winservers]
windc01             ansible_host=10.10.2.20
winfile[1:3]        ansible_host=10.13.128.[7:9]
winwebsrv01         ansible_host=10.14.27.16

[winservers:vars]
ansible connection=winrm
ansible winrm transport=credssp
ansible port=5986
ansible winrm server cert validation=ignore
```

Red Hat
Ansible Automation
Platform

Section 1

Topics Covered:

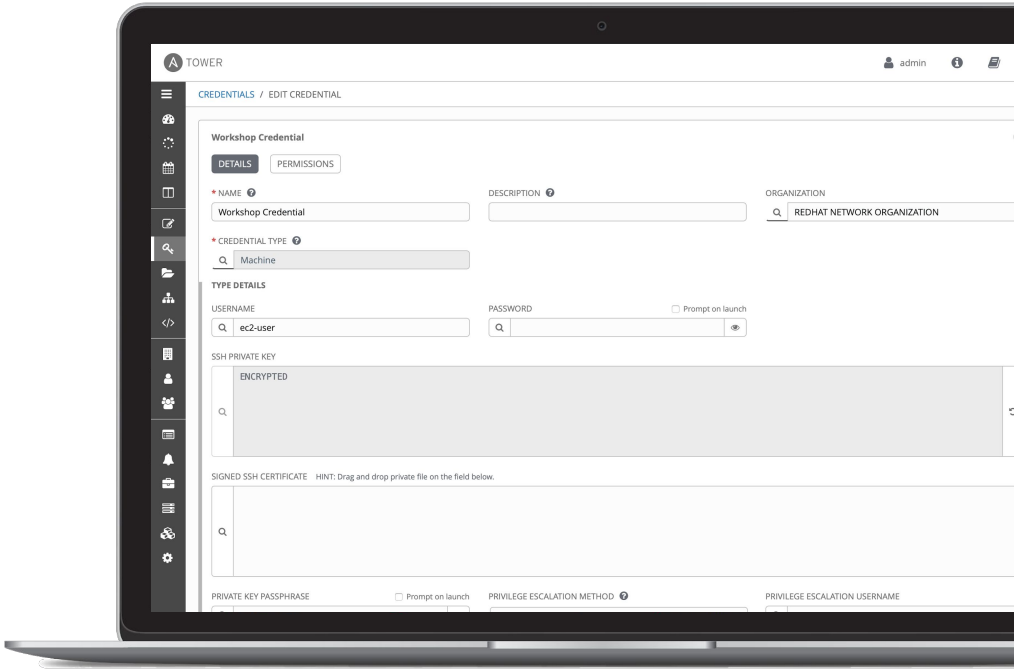
- Tower Basics
- Intro and initial configuration of Ansible Tower

Credentials

Credentials are utilized by Ansible Tower for authentication with various external resources:

- Connecting to remote machines to run jobs
- Syncing with inventory sources
- Importing project content from version control systems
- Connecting to and managing network devices

Centralized management of various credentials allows end users to leverage a secret without ever exposing that secret to them.

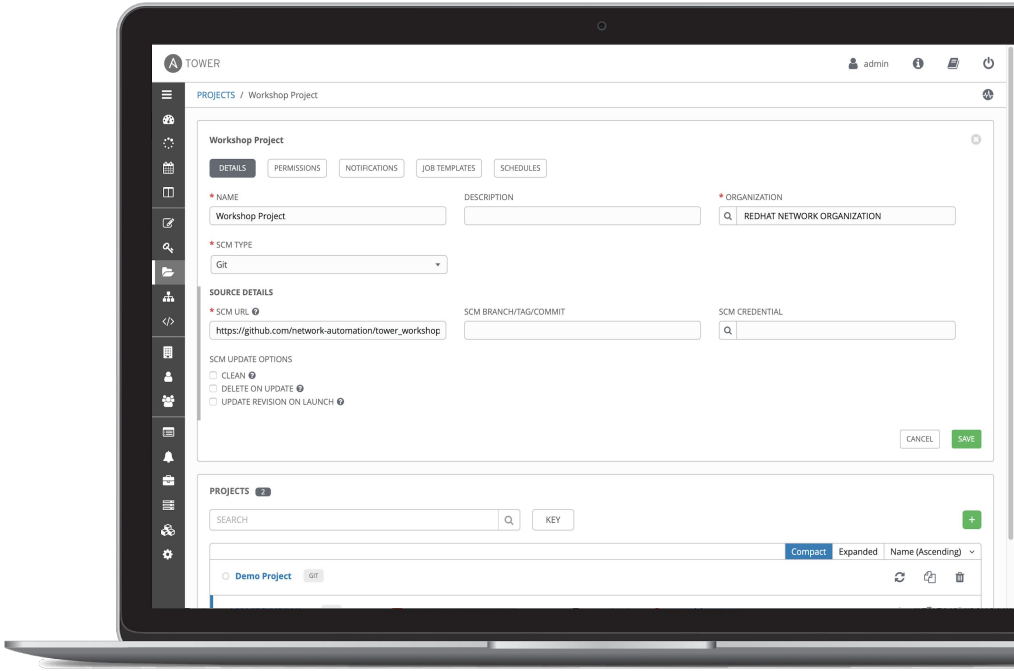


Red Hat

Project

A project is a logical collection of Ansible Playbooks, represented in Ansible Tower.

You can manage Ansible Playbooks and playbook directories by placing them in a source code management system supported by Ansible Tower, including Git, Subversion, and Mercurial.

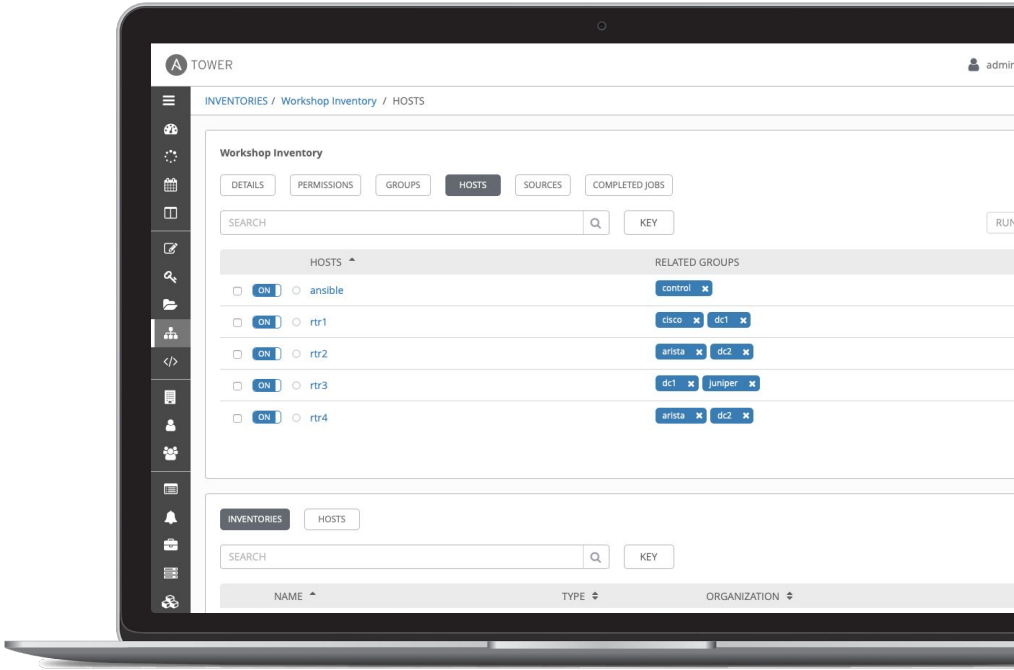


Red Hat

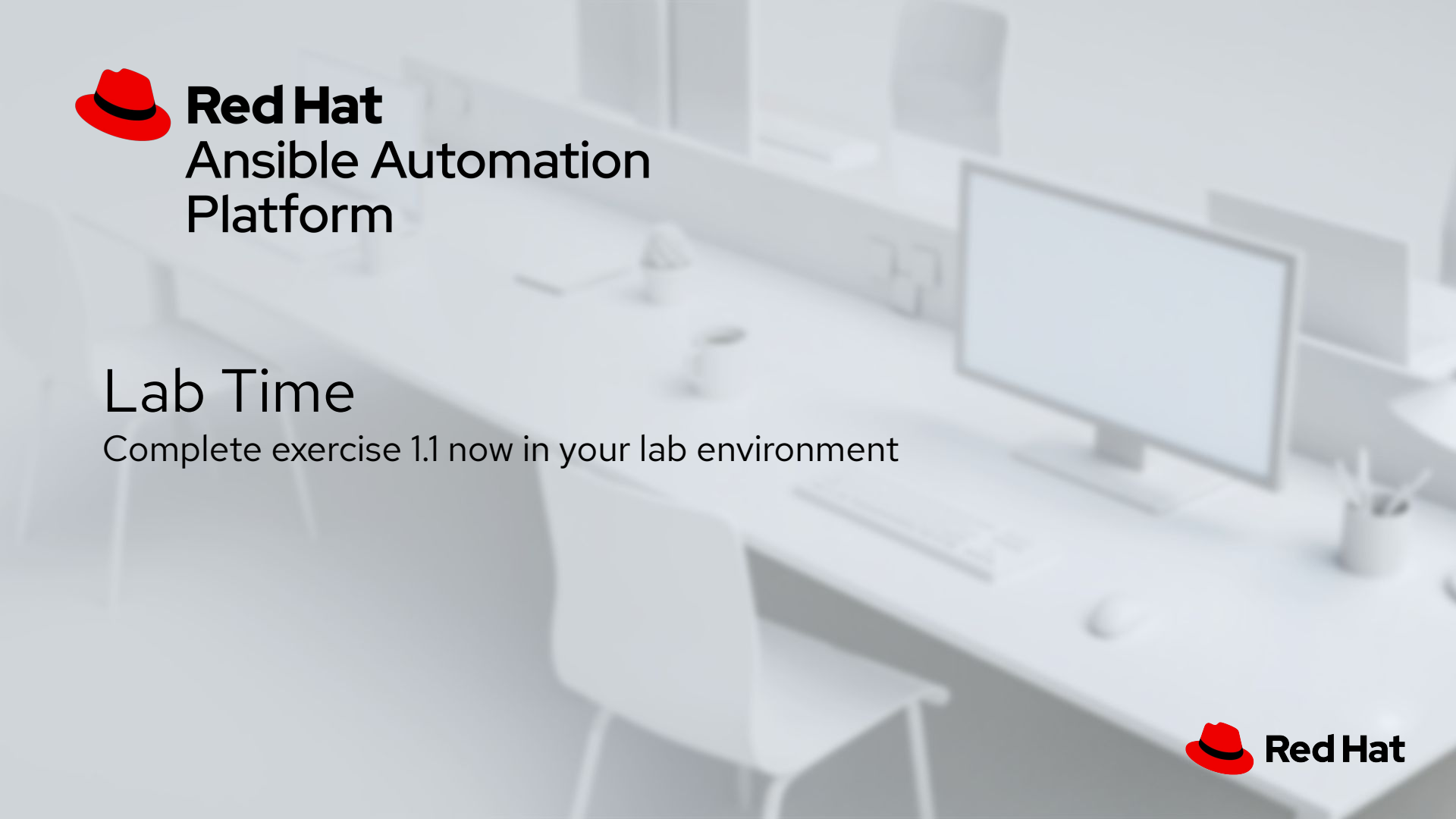
Inventory

Inventory is a collection of hosts (nodes) with associated data and groupings that Ansible Tower can connect to and manage.

- Hosts (nodes)
- Groups
- Inventory-specific data (variables)
- Static or dynamic sources



Red Hat

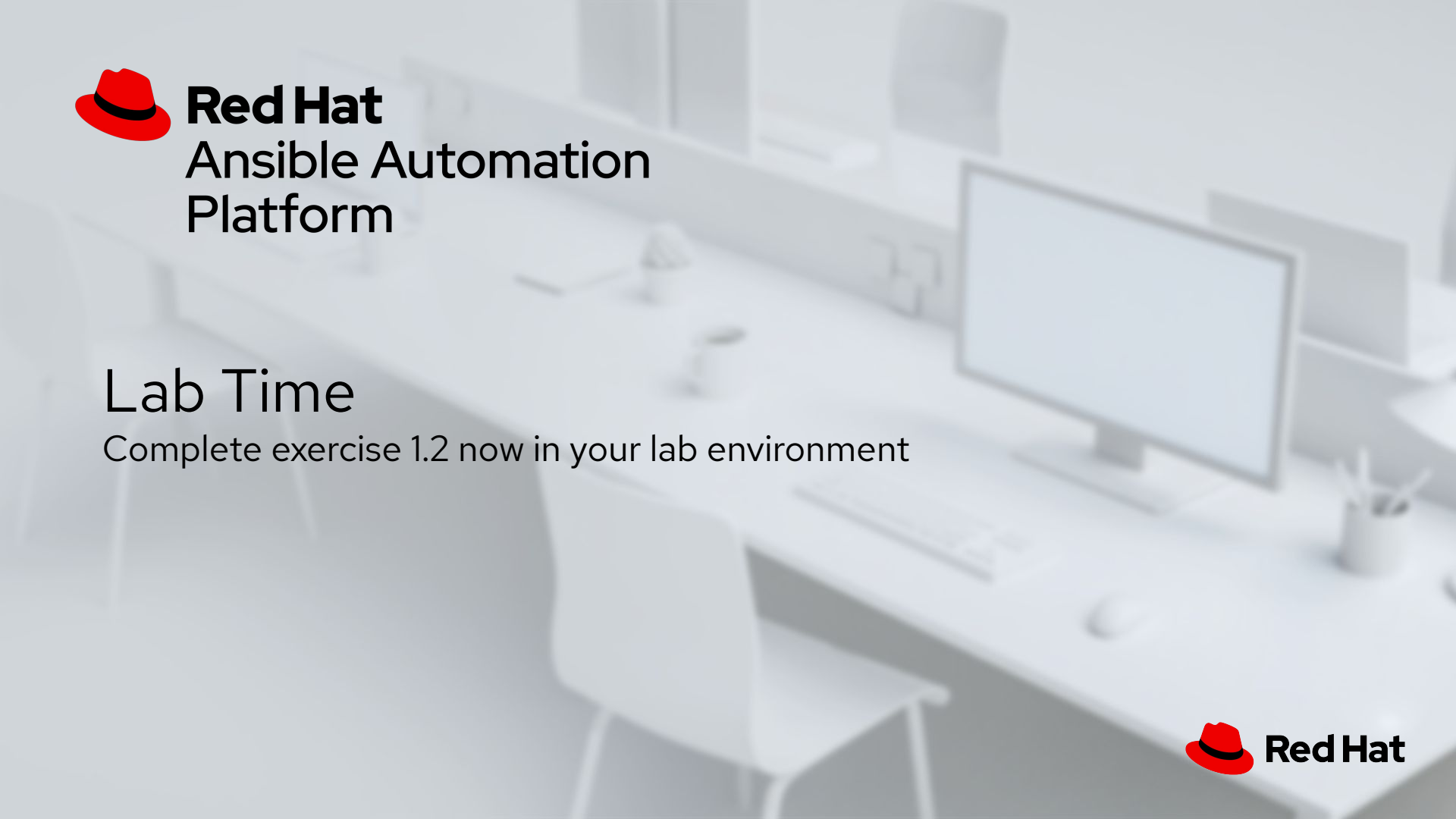

Red Hat
Ansible Automation
Platform
Lab Time
Complete exercise 1.1 now in your lab environment
Red Hat

Red Hat
Ansible Automation
Platform

Section 2

Topics Covered:

- Execute Ad-Hoc Commands
- Add or remove modules from the list


Red Hat
Ansible Automation
Platform
Lab Time
Complete exercise 1.2 now in your lab environment
Red Hat

Red Hat
Ansible Automation
Platform

Section 3

Topics Covered:

- Playbook basics
- Versioning of playbooks

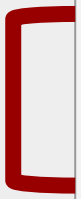
An Ansible Playbook

A play

```
---
- name: Ensure Firewall is running
  hosts: web
  become: yes
  tasks:
    - name: Firewall package is installed
      yum:
        name: firewalld
        state: latest

    - name: Firewall is running
      service:
        name: firewalld
        state: started
        enabled: true

    - name: https traffic is allowed
      firewalld:
        service: https
        permanent: yes
        state: enabled
        immediate: yes
```

An Ansible Playbook

A task



```
---
- name: Ensure Firewall is running
  hosts: web
  become: yes
  tasks:
    - name: Firewall package is installed
      yum:
        name: firewalld
        state: latest

    - name: Firewall is running
      service:
        name: firewalld
        state: started
        enabled: true

    - name: https traffic is allowed
      firewalld:
        service: https
        permanent: yes
        state: enabled
        immediate: yes
```

An Ansible Playbook

module

```
---
- name: Ensure Firewall is running
  hosts: web
  become: yes

  tasks:
    - name: Firewall package is installed
      yum:
        name: firewalld
        state: latest

    - name: Firewall is running
      service:
        name: firewalld
        state: started
        enabled: true

    - name: https traffic is allowed
      firewalld:
        service: https
        permanent: yes
        state: enabled
        immediate: yes
```

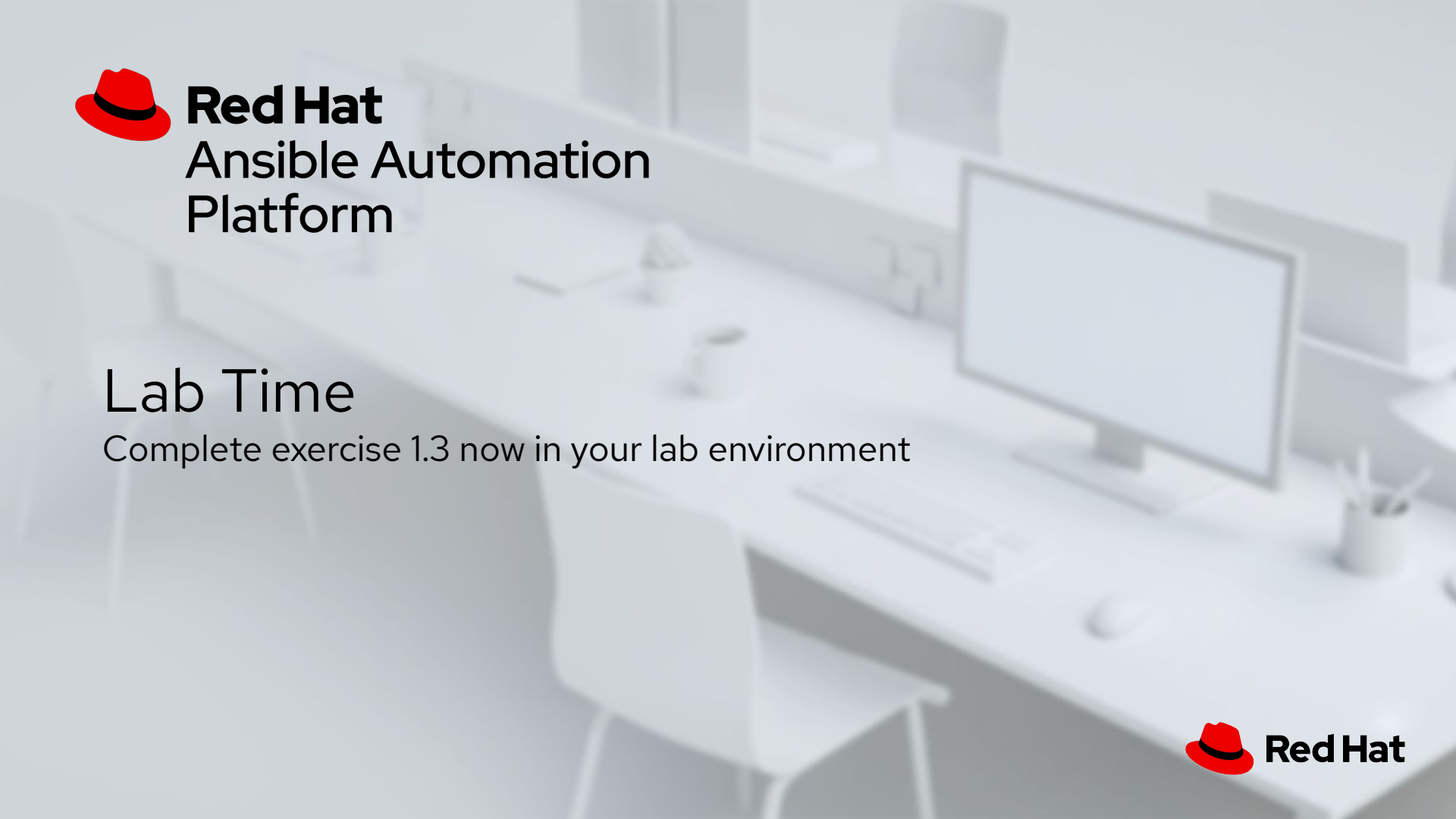
Running an Ansible Playbook:

The most important colors of Ansible

```
A task executed as expected, no change was made.

A task executed as expected, making a change

A task failed to execute successfully
```

Running an Ansible Playbook

```
[user@ansible] $ ansible-playbook firewall.yml

PLAY [web] *********************************************************************

TASK [Gathering Facts] *********************************************************
ok: [web2]
ok: [web1]
ok: [web3]

TASK [Firewall package is installed] *******************************
changed: [web2]
changed: [web1]
changed: [web3]

TASK [Firewall is running] *****************************************
changed: [web2]
changed: [web1]
changed: [web3]

TASK [https traffic is allowed]
*********************************************************************
changed: [web2]
changed: [web1]
changed: [web3]

PLAY RECAP *********************************************************************
web2                       : ok=1 changed=3 unreachable=0 failed=0
web1                       : ok=1 changed=3 unreachable=0 failed=0
web3                       : ok=1 changed=3 unreachable=0 failed=0
```


Red Hat
Ansible Automation
Platform
Lab Time
Complete exercise 1.3 now in your lab environment
Red Hat

Red Hat
Ansible Automation
Platform

Section 4

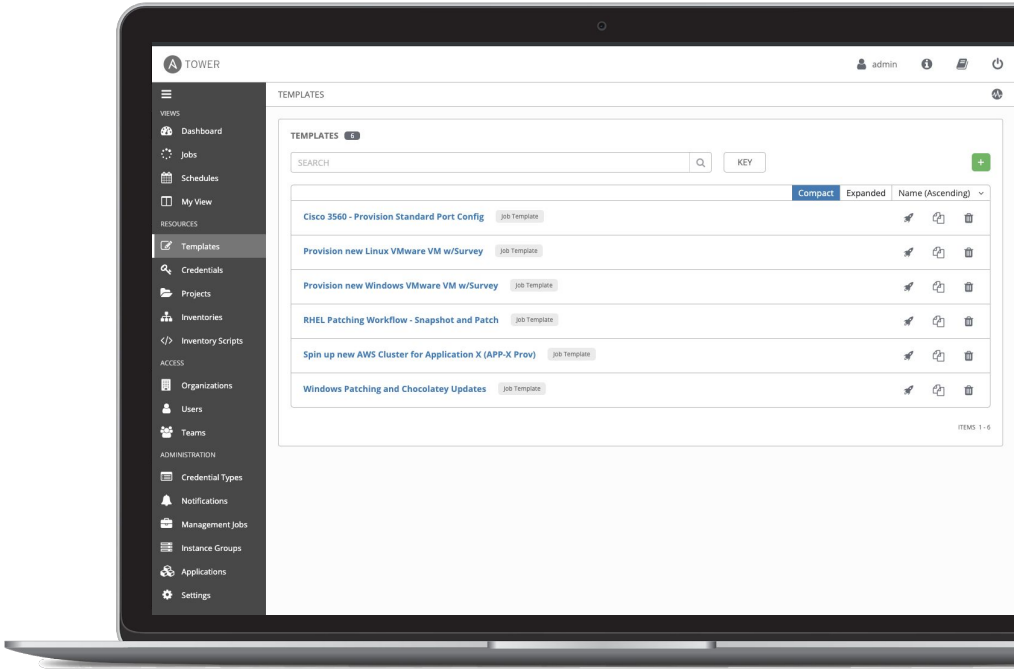
Topics Covered:

- Create a Job Template
- Running our first Playbook

Job Templates

A Job Template is where all the pieces come together, defining how your Ansible job will run. A Job Template is made up of:

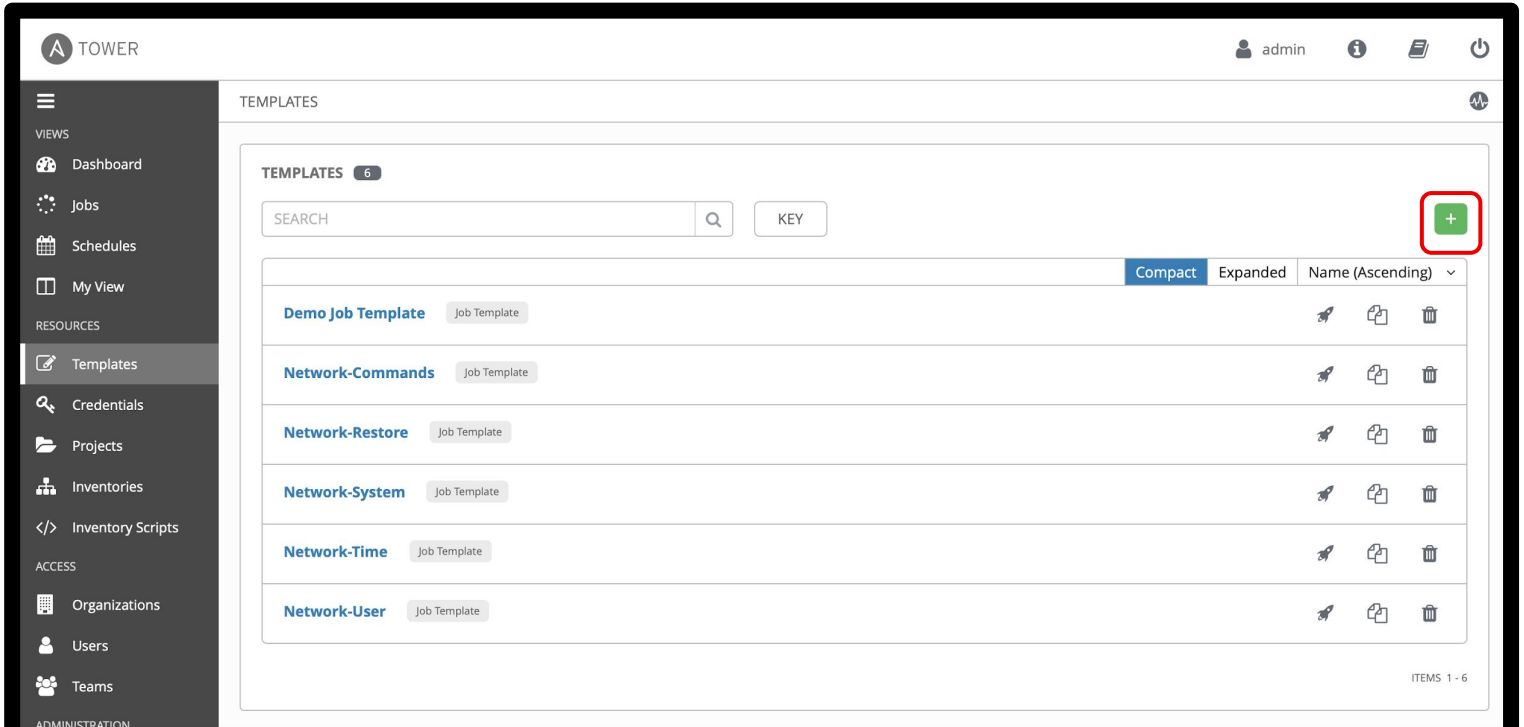
- Inventory
- Project (containing a playbook)
- Credentials
- Survey or optional vars
- Jobs can be launched via UI or API



Red Hat

Creating a new Job Template (1/2)

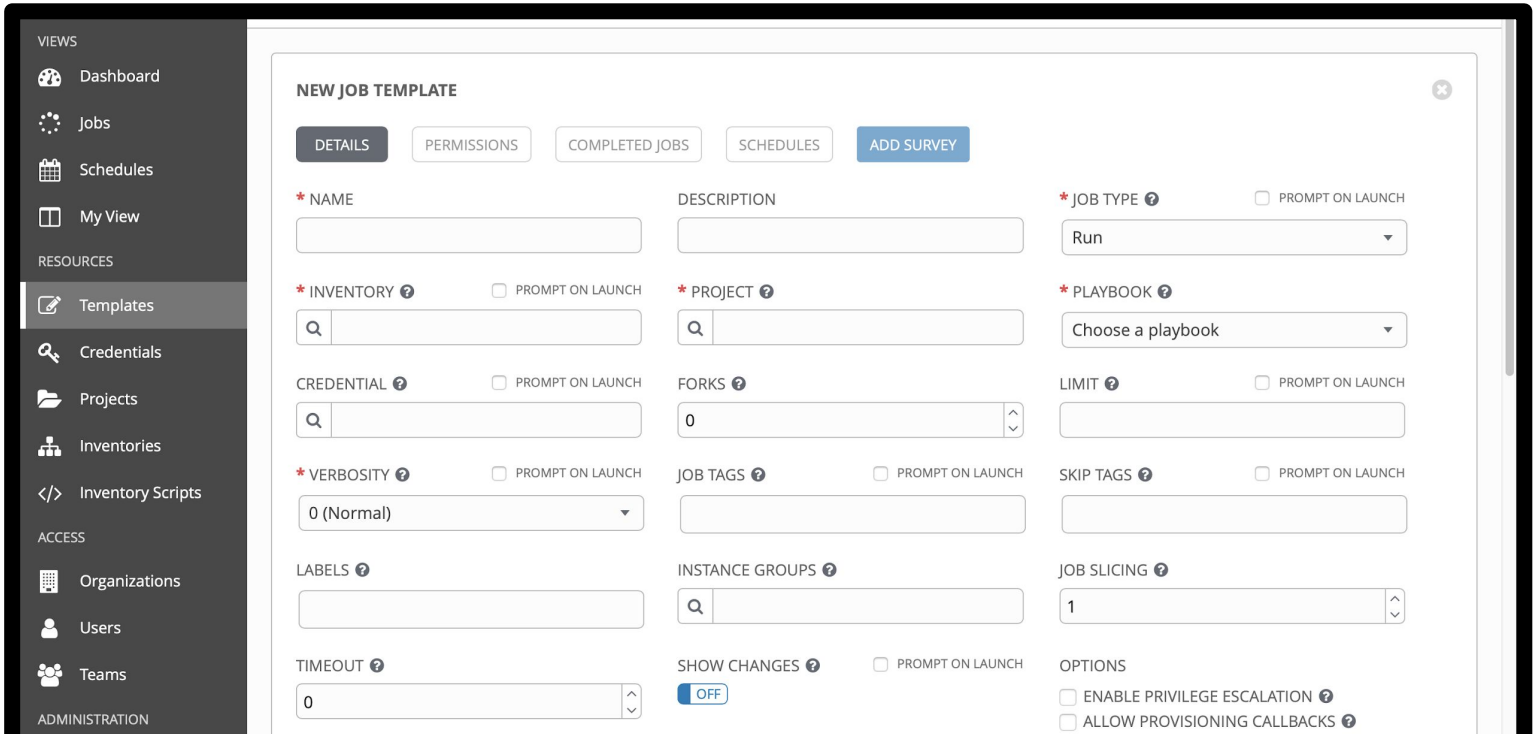
New Job Templates can be created by clicking the **plus butt**



Red Hat

Creating a new Job Template (2/2)

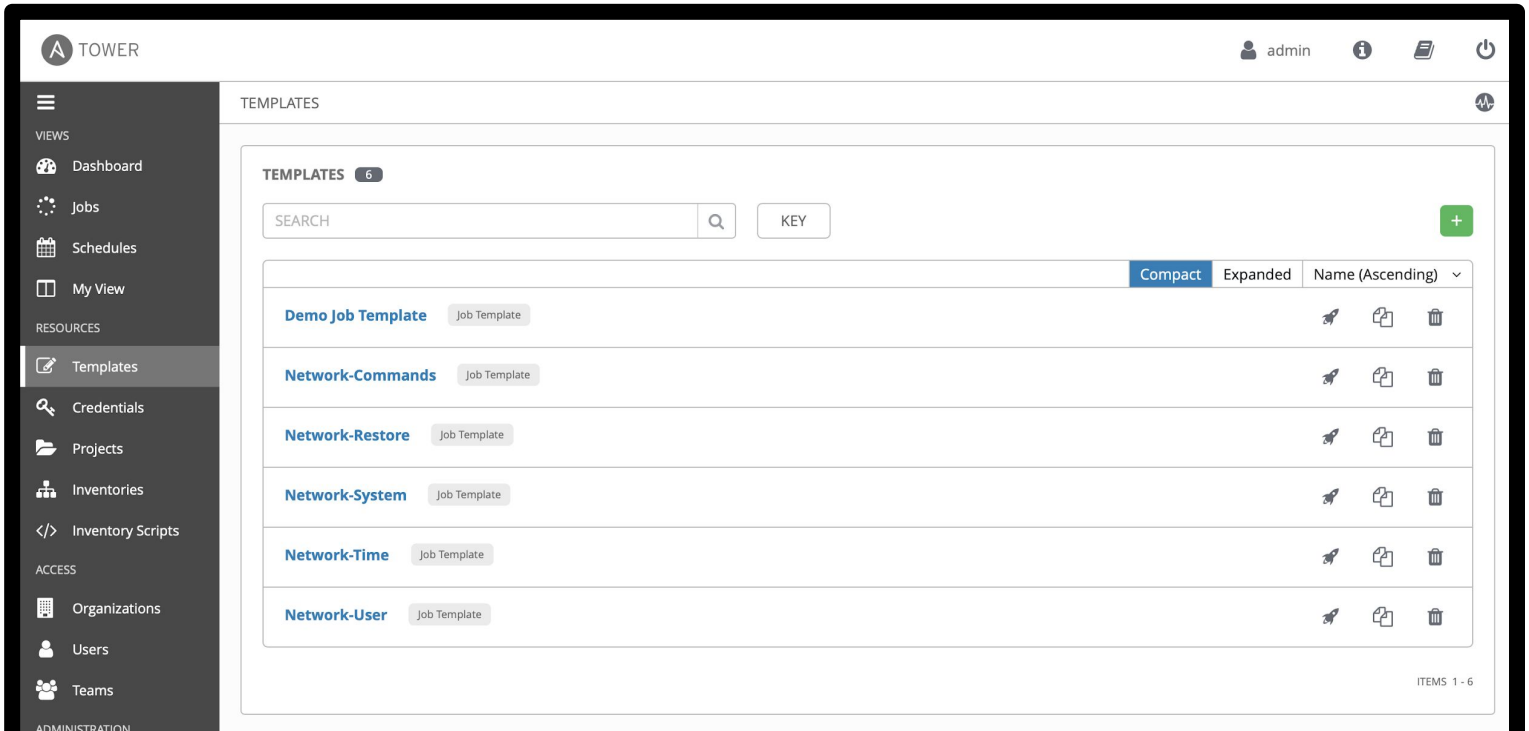
This **New Job Template** window is where the inventory, project and credential are assigned. The red asterisk * means the field is required .



Red Hat

Expanding on Job Templates

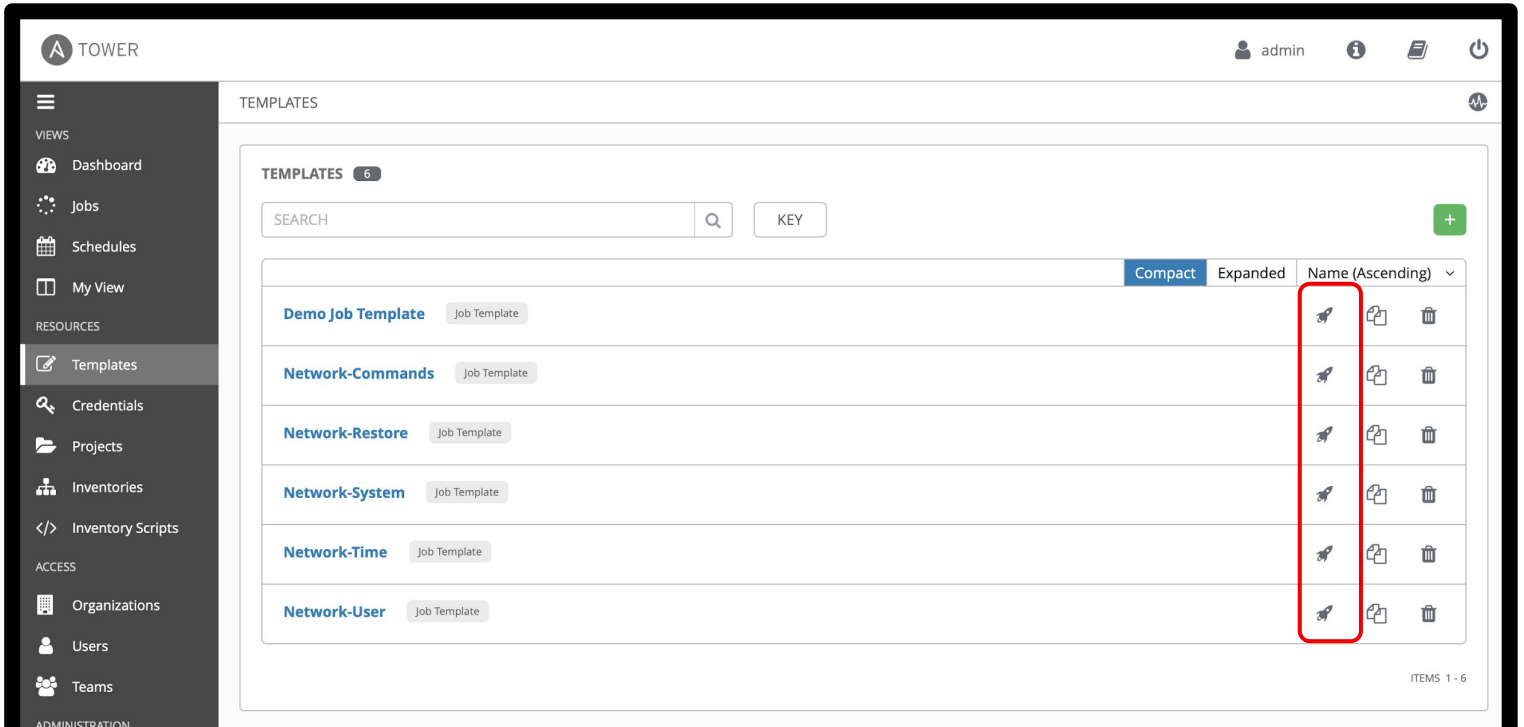
Job Templates can be found and created by clicking the **Template** button under the *RESOURCES* section on the left menu.



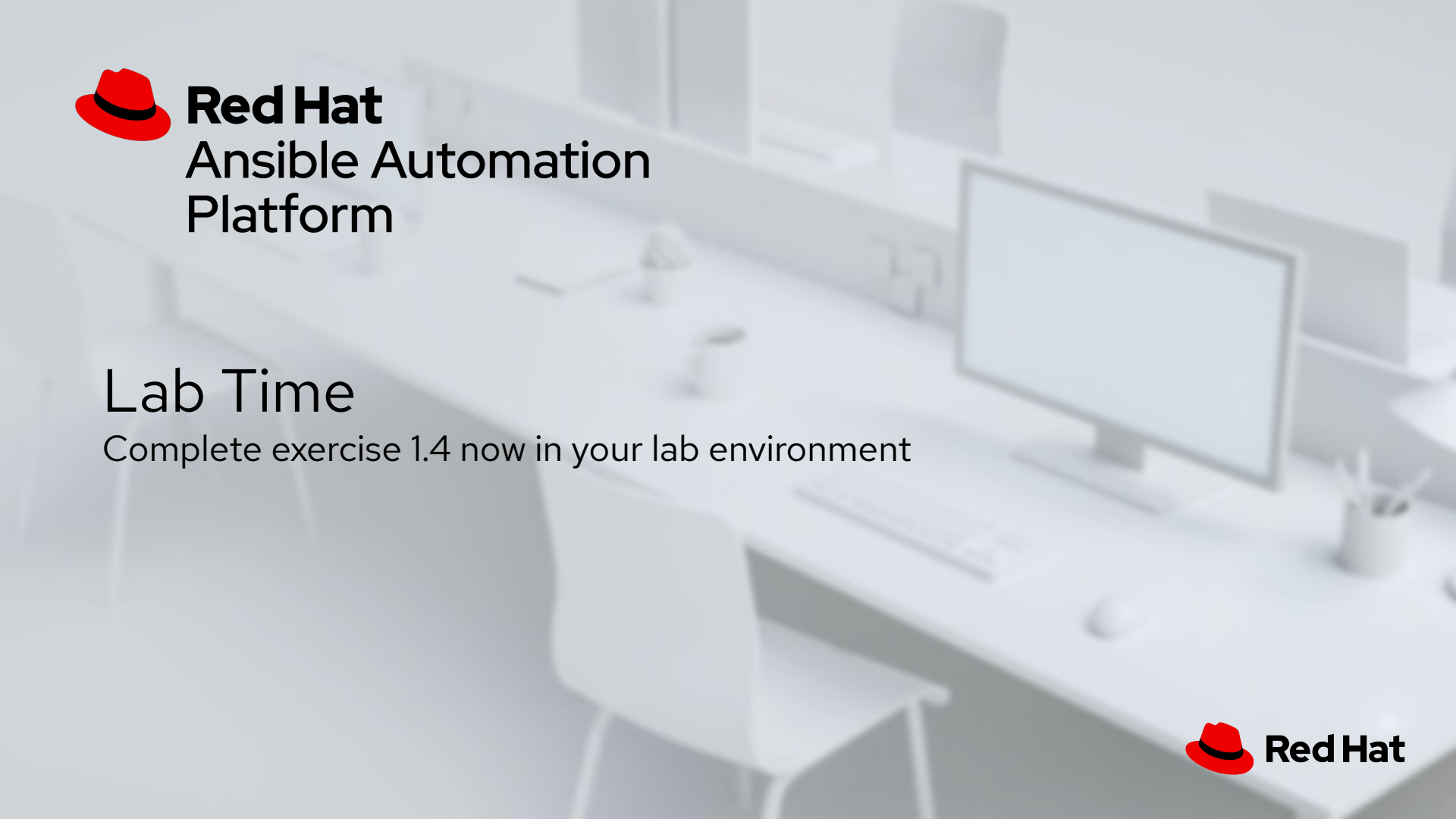
Red Hat

Executing an existing Job Template

Job Templates can be launched by clicking the **rocketship button** for the corresponding Job Template



Red Hat


Red Hat
Ansible Automation
Platform
Lab Time
Complete exercise 1.4 now in your lab environment
Red Hat

Red Hat
Ansible Automation
Platform

Section 5

Topics Covered:

- Role Overview
- An example Ansible Playbook

Role structure

- Defaults: default variables with lowest precedence (e.g. port)
- Handlers: contains all handlers
- Files: static files to deploy
- Meta: role metadata including dependencies to other roles
- Tasks: plays or tasks
  Tip: It's common to include tasks in main.yml with "when" (e.g. OS == xyz)
- Templates: templates to deploy
- Tests: place for playbook tests
- Vars: variables (e.g. override port)

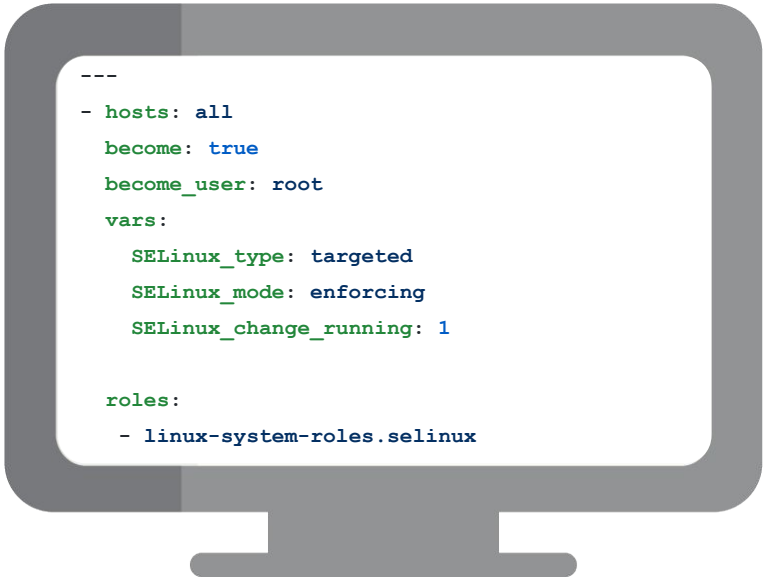
```
example_role/
├── defaults
│   └── main.yml
├── files
├── handlers
│   └── main.yml
├── meta
│   └── main.yml
├── README.md
├── tasks
│   └── main.yml
├── templates
└── vars
    └── main.yml
```

Linux System Roles

- Consistent user interface to provide settings to a given subsystem that is abstract from any particular implementation

Examples

Automate security tasks with Red Hat Ansible Automation



```
---
- hosts: all
  become: true
  become_user: root
  vars:
    SELinux_type: targeted
    SELinux_mode: enforcing
    SELinux_change_running: 1

  roles:
   - linux-system-roles.selinux
```

Examples

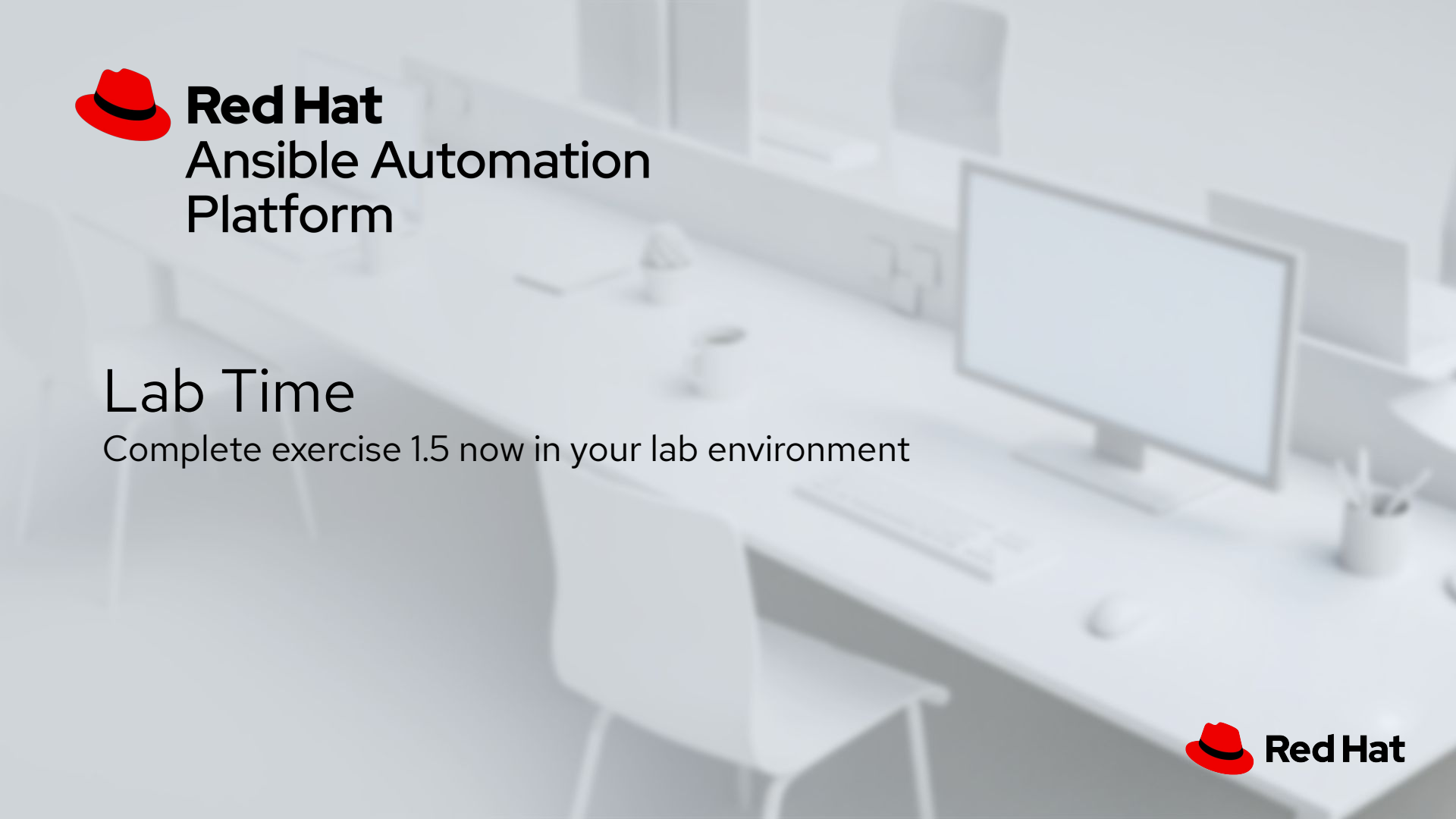
- Prevent ShellShock exploitation with SELinux system roles
- Configure login banner and other system standards
- Harden operating system and application settings

Playbook Example

- Define variables
- Don’t reinvent the wheel,

  use galaxy.ansible.com
- Use modules for idempotent changes
- Define security standards as code

```
---
- hosts: all
  vars:
    ssh_banner: true
    sftp_enabled: true
    ssh_print_motd: true

  roles:
  - motd-splash
  - hardening
  - dev-sec.ssh-hardening

  tasks:
  - name: Configure Sudoers
    lineinfile:
      path: /etc/sudoers
      state: present
      regexp: '^%ADMIN ALL='
      line: '%ADMIN ALL=(ALL) NOPASSWD: ALL'
      validate: /usr/sbin/visudo -cf %s
```


Red Hat
Ansible Automation
Platform
Lab Time
Complete exercise 1.5 now in your lab environment
Red Hat

Red Hat
Ansible Automation
Platform

Section 6

Topics Covered:

- OpenSCAP scan run
- Examine the compliance report
- Running a remediation job and rescan

Security compliance automation with OpenSCAP

Red Hat's security scanner is included with Red Hat Enterprise Linux, Red Hat Satellite, and Red Hat Smart Management

Validated and certified tool
National Institute of Standards and Technology (NIST) certified Security Content Automation Protocol (SCAP) scanner with National Checklist content

System and container scanning
Known vulnerability and security policy compliance scanning

Automation support
Red Hat® Ansible® Automation remediation playbooks provided and supported by Red Hat

Customizable content
Content customization through SCAP Workbench graphical interface

Improve visibility and ease compliance audits with OpenSCAP reports

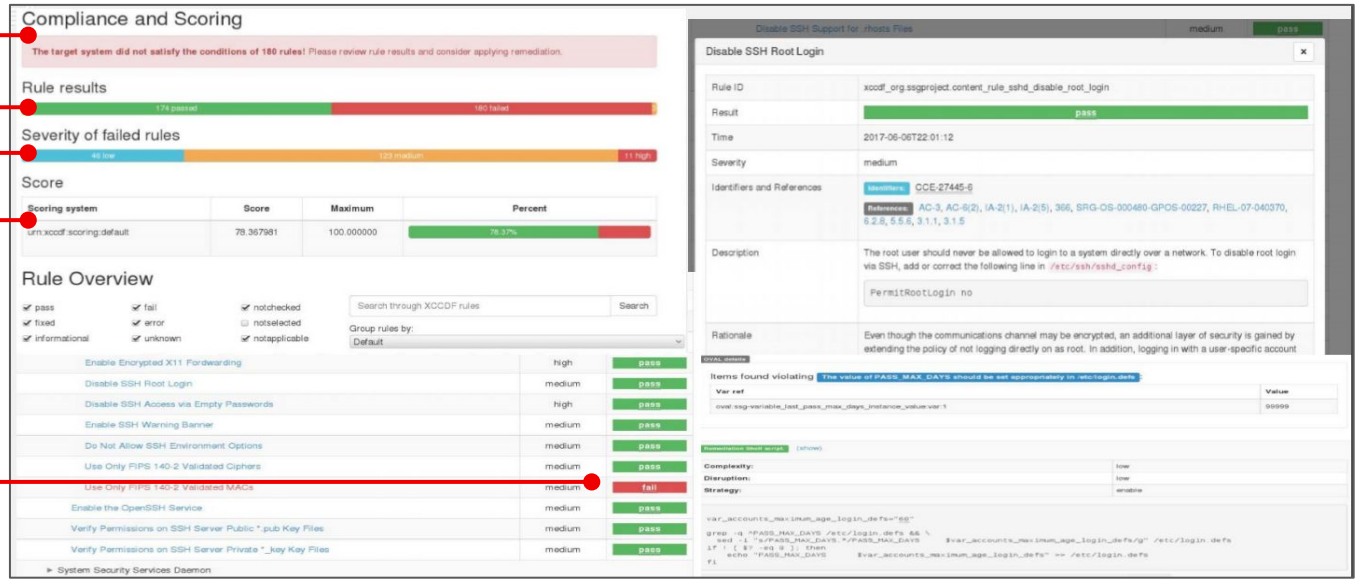
Overall compliance score message

Simple pass-fail visual display

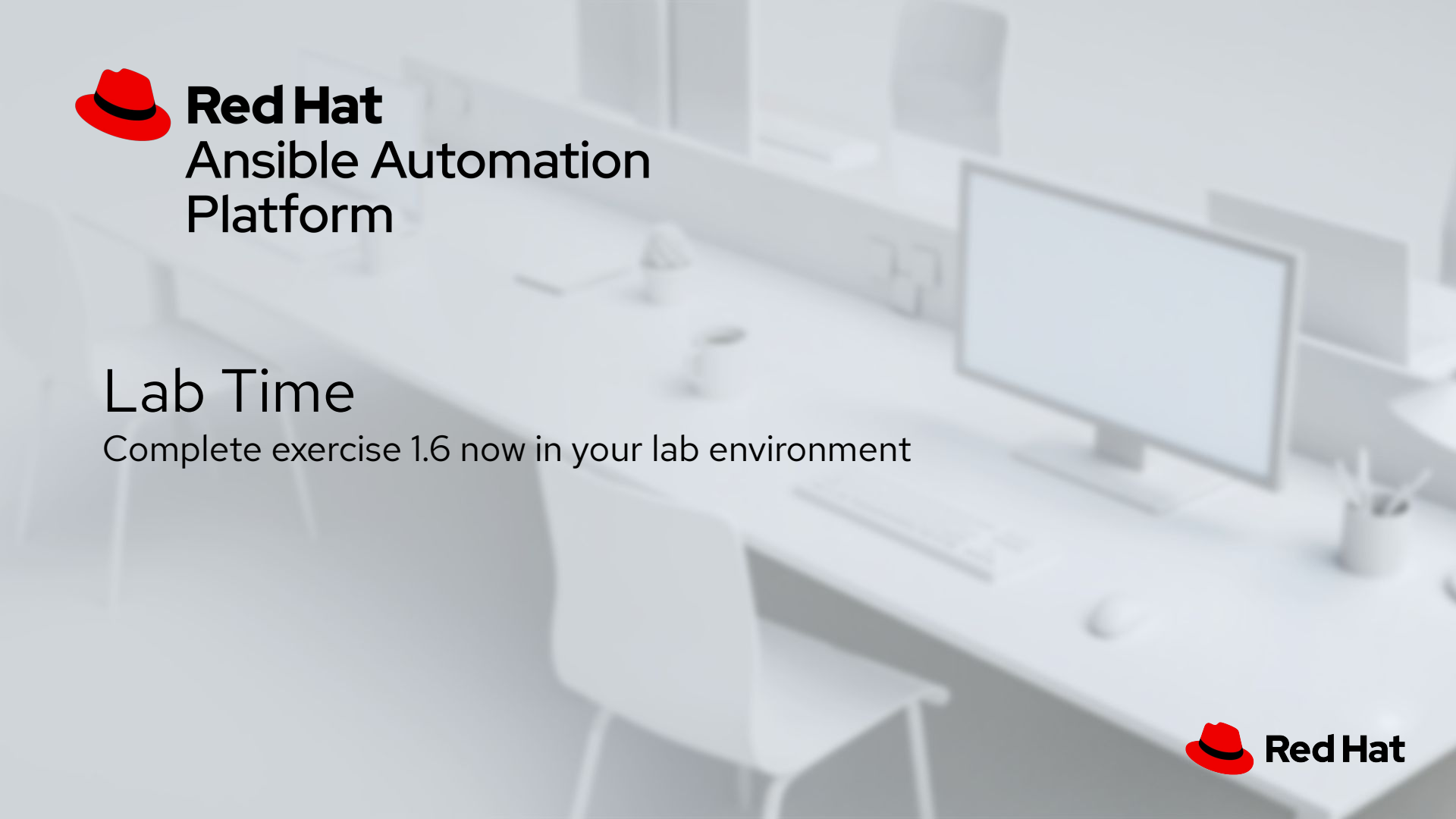
Issue severity highlights

Calculated score

Additional information and remediation action details



Red Hat


Red Hat
Ansible Automation
Platform
Lab Time
Complete exercise 1.6 now in your lab environment
Red Hat

Red Hat
Ansible Automation
Platform

Section 7

Topics Covered:

- Building a Tower Survey
- Self-service IT with Tower Surveys

Surveys

Tower surveys allow you to configure how a job runs via a series of questions, making it simple to customize your jobs in a user-friendly way.

An Ansible Tower survey is a simple question-and-answer form that allows users to customize their job runs. Combine that with Tower's role-based access control, and you can build simple, easy self-service for your users.

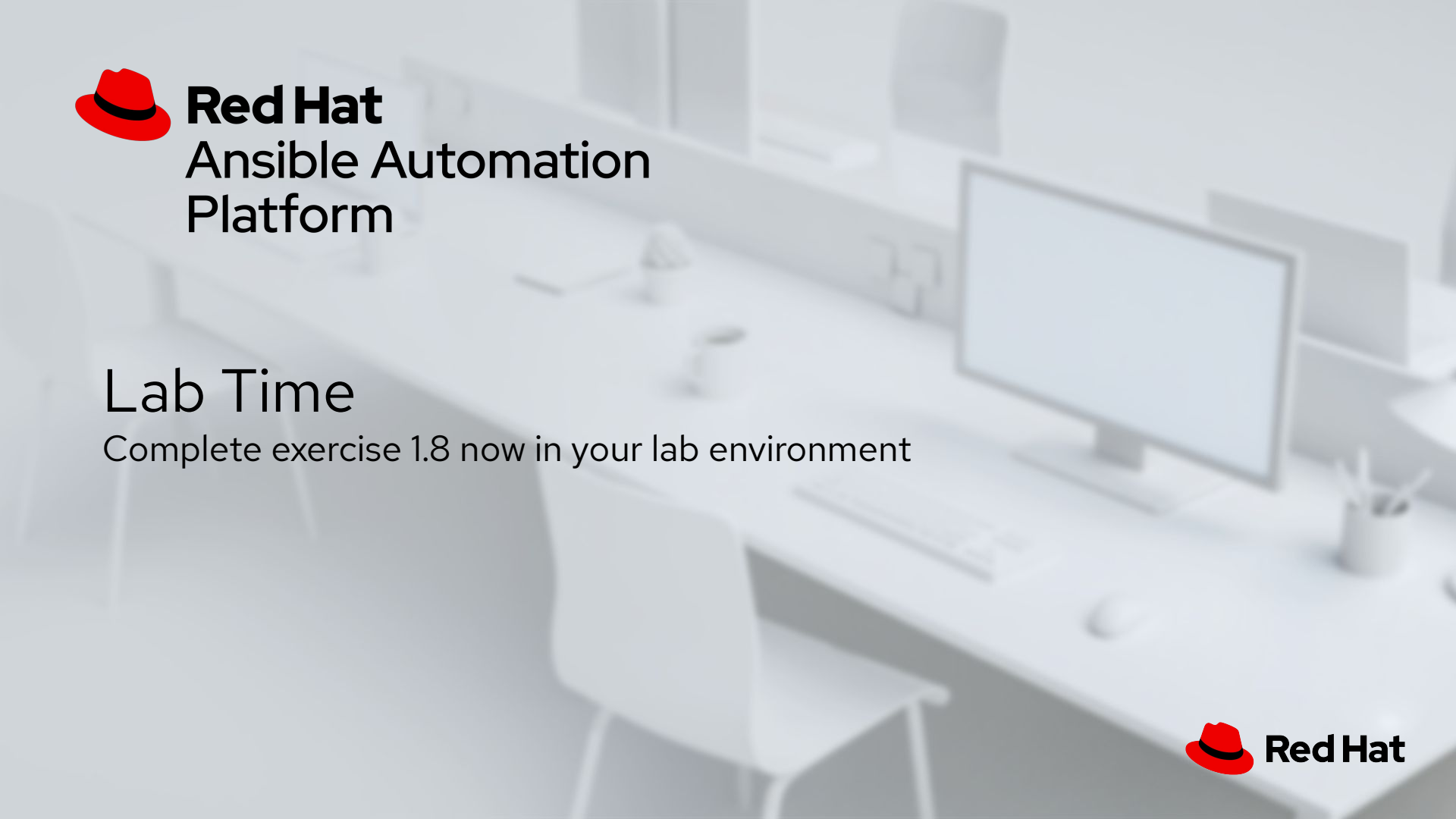

Red Hat
Ansible Automation
Platform
Lab Time
Complete exercise 1.7 now in your lab environment
Red Hat

Red Hat
Ansible Automation
Platform

Section 8

Topics Covered:

- Overview of the Ansible Tower API
- How to execute via the API


Red Hat
Ansible Automation
Platform
Lab Time
Complete exercise 1.8 now in your lab environment
Red Hat

External API call

```
curl -f -k -H 'Content-Type: application/json' -XPOST -d '{"limit":
"web","job_type": "run","extra_vars": "{'ssg_profile':
'xccdf_org.ssgproject.content_profile_pci-dss'}"}' --user admin:Hrdq5xFmdwSjUX
https://student1.7d1e.open.redhat.com/api/v2/job_templates/Openscap_scan/launch/
```

Use Oauth2

```
curl -kH "Authorization: Bearer tvTL9dT6XOxd6IU0OZxTWF5dB0cBPn" -H "Content-Type:
application/json" https://student1.7d1e.open.redhat.com/api/v2/job_templates/16/launch/ -XPOST -d
'{"limit": "web","job_type": "run","extra_vars": "{'ssg_profile':
'xccdf_org.ssgproject.content_profile_pci-dss'}"}'
```

Red Hat
Ansible Automation
Platform

Section 9

Topics Covered:

- Understanding Insights
- How Insights integrates with Ansible Tower

Red Hat Insights

Included with your Red Hat Enterprise Linux subscription

Assesses

customer's Red Hat environments

Remediates

findings with prescriptive remediation steps or an Ansible playbook

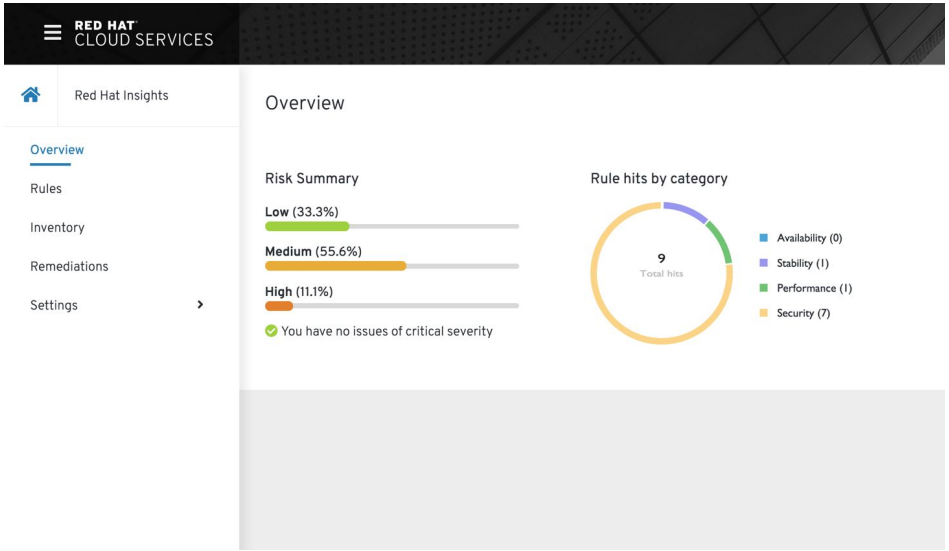
Insights

rule contributions directly from Red Hat subject matter experts

Identifying risks for Availability, performance, stability and security

Red Hat

Detect and fix issues with Red Hat Insights



https://cloud.redhat.com

Proactive advice
Identification of issues before they become problems

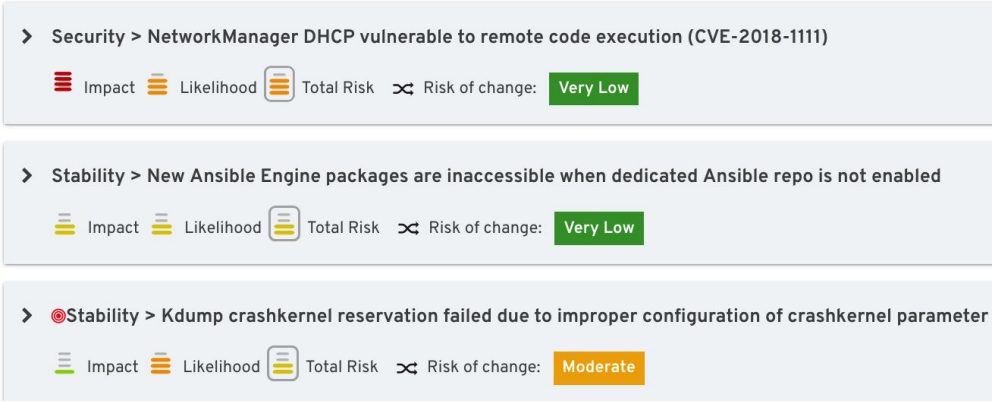
Continuous assessment
Real-world results to help find new risks

Simpler remediations
Tailored results at the host level

Red Hat

Get ahead of key security risks

Don’t wait for your security team to tap you on the shoulder



- Prioritizes security response by analyzing runtime configuration and usage
- Automates security analysis, beyond just CVEs

*“ …when a vulnerability is released, it’s likely to be exploited within **40-60** days. However, it takes security teams between 100-120 days on average to remediate…”*

— KENNA SECURITY GROUP

Red Hat

Data collection

Very small amount of data and only data that is needed for rule analysis

Example files:

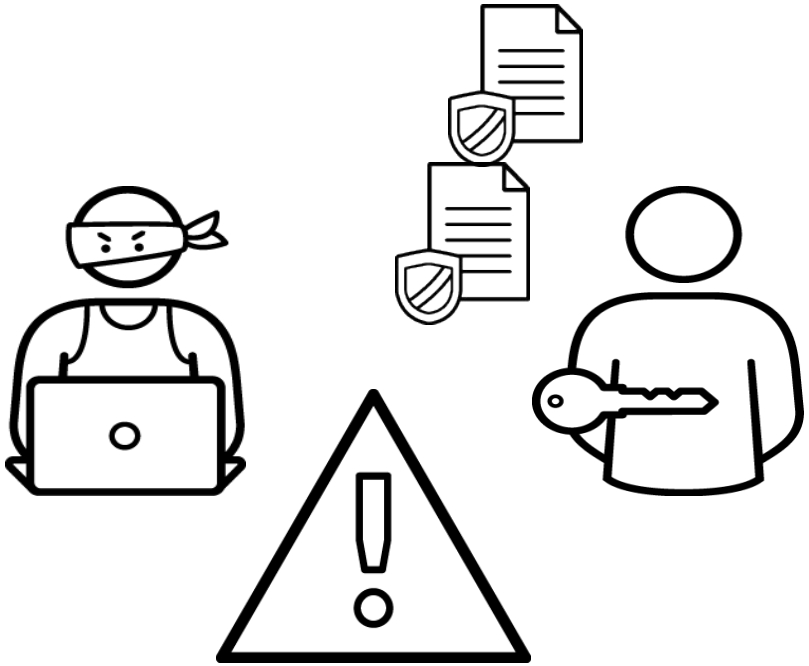
- `/etc/redhat-release`
- `/proc/meminfo`
- `/var/log/messages`
- `/boot/grub/grub.conf`
- `/boot/grub2/grub.cfg`
- `/etc/modprobe.conf`

We do not collect log files, but rather the lines that match a potential rule (i.e. page allocation failure)

Commands:

- `/bin/rpm -qa`
- `/bin/uname -a`
- `/usr/sbin/dmidecode`
- `/bin/netstat -i`
- `/bin/ps auxcww`

Concerned about security?

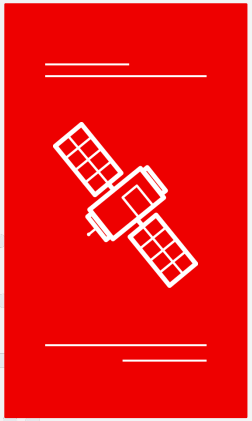


DATA SECURITY ASSURED

- Data encryption using LUKS
- Data sent over TLS
- Truster certificate bundled
- Hostname and IP obfuscation available
- System information to be tailored

Red Hat Smart Management

Red Hat Satellite

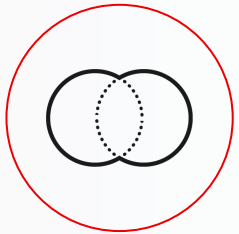


+

Cloud management services for Red Hat Enterprise Linux

Vulnerability

Compliance



System comparison

Red Hat

Red Hat
Ansible Automation
Platform

Insights Demo

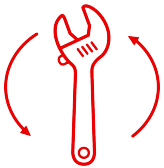
Red Hat

Vulnerability

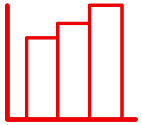
Remediate all Common Vulnerabilities and Exposures (CVEs) with errata

Vulnerability offers

Assess and monitor the risk of vulnerabilities that impact Red Hat products with operational ease



Remediate known Common Vulnerabilities and Exposures (CVEs)



Ability to generate JavaScript Object Notation and CSV view-based **reports** to keep relevant stakeholders informed

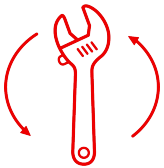
Red Hat

Compliance

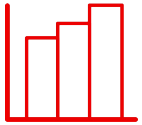
Built on OpenSCAP reporting

Compliance offers

Assess and monitor the degree/level of compliance to a policy for Red Hat products with operational ease



Remediate known issues of non-compliance in the Red Hat environment via Ansible playbooks based on business risk & relevance



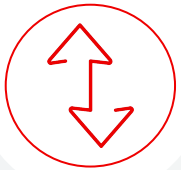
Ability to generate JavaScript Object Notation and CSV view-based **reports** to keep relevant stakeholders informed

Red Hat

System Comparison

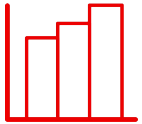
Compare system profiles

System Comparison offers



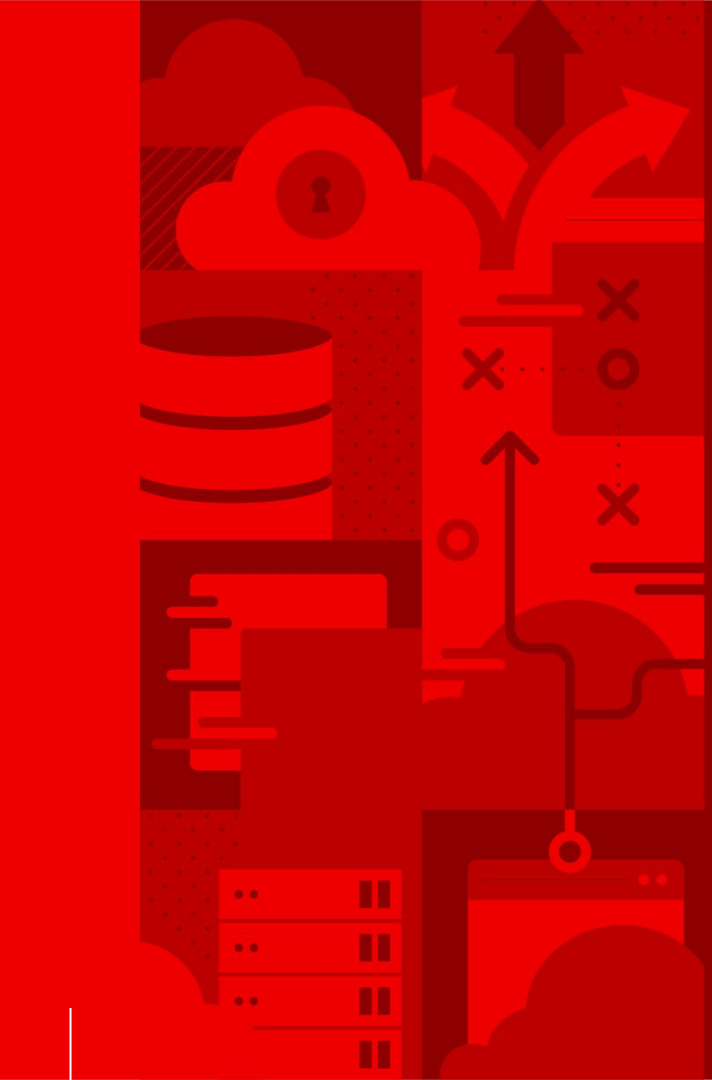
Compare system configuration of one host to other hosts

Filter displayed profile facts, highlighting areas that match, are different, or where information is missing.



Ability to generate CSV view-based output

Red Hat



Next Steps and Resources

Red Hat Training Offerings

1. D0500: DevOps Culture and Practice Enablement
2. D0700: Container Adoption Boot Camp
3. D0426: Securing Containers and OpenShift (with exam)

   <Also free OpenShift hands-on training on : http://learn.openshift.com/>
4. RH415: Red Hat Security: Linux in Physical, Virtual, Cloud (with exam)
5. RH413: Red Hat Security and Server Hardening (with exam)

Red Hat Security Related Links

- Solution Brief: Increase Security and Compliance with Advanced Automation
  - https://www.redhat.com/en/resources/automate-security-compliance-solution-brief
- Whitepaper: Red Hat Automated Security and Compliance
  - https://www.redhat.com/en/resources/red-hat-automated-security-and-compliance
- Video: https://www.redhat.com/en/about/videos/red-hat-automated-security-compliance-for-telecommunications-service-providers
- Red Hat Consulting Services Datasheet: Automate Security and Reliability Workflows
  - https://www.redhat.com/en/resources/services-consulting-automate-security-reliability-datasheet
- Red Hat provided and supported Ansible security hardening Ansible playbooks in Ansible Galaxy
  - https://galaxy.ansible.com/RedHatOfficial
- Red Hat Security Hands-on Labs : https://red.ht/securitylabs

Red Hat Security Related Links (cont..)

- Guide to continuous security
  - https://www.redhat.com/en/technologies/guide/it-security
- Understanding IT Security
  - https://www.redhat.com/en/topics/security
- Container Security
  - https://www.redhat.com/en/topics/security/container-security
- Red Hat Product Security
  - https://access.redhat.com/security/overview