ANS201 - DEFENDING ANSIBLE

Course Learning Objectives

In the four modules of this course, we'll explore how to establish an Ansible workflow that ensures safe, consistent infrastructure configurations, covering topics such as how Ansible implements Infrastructure as Code, how to run a playbook, and how to protect and secure the control node.

In addition we'll see how to automate the initial security setup of servers, how to encrypt secrets using Ansible Vault, how to safely store Vault passwords in a file or a secrets manager, how to rotate Vault passwords, how to use role-based access control in Automation Controller, how to collect logs for analysis and auditing, and how to implement common security practices with Automation Hub.

Description

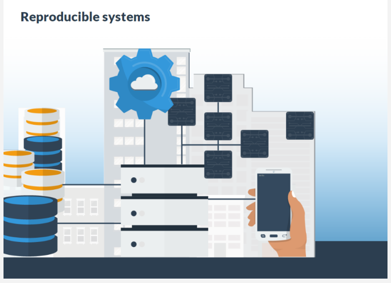
Defending Ansible is for anyone involved in deploying and configuring IT infrastructure, including DevOps and DevSecOps professionals.

Audience

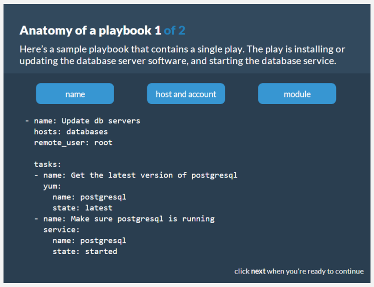
DevOps
DevSecOps

Time Required

Tailored learning - 70 minutes total



Reproducible systems



Anatomy of a playbook 1 of 2

Here's a sample playbook that contains a single play. The play is installing or updating the database server software, and starting the database service.

```
- name: Update db servers
  hosts: databases
  remote_user: root

  tasks:
  - name: Get the latest version of postgresql
    yum:
      name: postgresql
      state: latest
  - name: Make sure postgresql is running
    service:
      name: postgresql
      state: started
```

click **next** when you're ready to continue

The danger of root access in Ansible

Many of Ansible's tasks require elevated privileges. However, you should never log in to a host with the root account.

Security Compass

ANS201 - DEFENDING ANSIBLE

Course Outline

1. Ansible Fundamentals

- Reproducible systems
- Infrastructure as Code (IaC)
- Benefits of Ansible
- The architecture of Ansible
- Ansible playbooks
- Anatomy of a playbook
- Running a playbook
- Performing a dry run
- Linting playbooks
- Establishing a workflow
- Enforcing your workflow
- Automating Ansible
- Advantages of automating Ansible
- Integrating Ansible
- Continuous deployment
- Extending playbooks

2. Hardening the Ansible Nodes

- Vulnerabilities in the architecture
- The danger of root access in Ansible
- Privilege escalation with become
- Run playbooks without human intervention
- Remote authentication
- SSH public key authentication
- Host checking
- SSH best practices
- Protecting the control node
- Automate host configuration

3. Protecting Secrets with Ansible Vault

- The danger of hardcoded secrets
- Encrypt secrets with Ansible Vault
- Encrypted playbooks
- A workflow with Ansible Vault
- Editor integration
- Managing Vault passwords
- Static password files
- Storing a Vault password in a file
- Credentials in a cloud-based key manager
- Rotate passwords with rekey
- Encryptsensitive values separately
- Using multiple passwords
- Other secret store options

4. Ansible Automation Platform

- Ansible Automation Platform
- Automation Controller objects
- Store credentials in Automation Controller
- Creating users
- Enforce separation of duties
- Team permissions
- Use RBAC to implement the principle of least privilege
- Adding team permissions to a job template
- The Activity Stream
- Automation Hub
- Ansible Security Automation

Security Compass