VMware vRealize Automation SaltStack SecOps: Deploy and Manage

Table of Content

- Create and manage jobs
- Use the Activities dashboard

Module 6: Configuration Control Through States, Pillars, Requisites, and Declarations

- Define the SaltStack states
- Describe file management in SaltStack Config
- Create the SaltStack state files
- Identify the components of a SaltStack state
- Describe pillar data and the uses of pillar data
- Configure pillar data on the SaltStack Config master server
- Use pillar data in variables in the state files
- Describe the difference between IDs and names in the state files
- Use the correct execution order
- Use requisites in the state files

Module 7: Using Jinja and YAML

- Describe the SaltStack Config renderer system
- Use YAML in the state files
- Use Jinja in the state files
- Use Jinja conditionals, lists, and loops

Module 8: Using SaltStack SecOps Comply

- Describe the SaltStack SecOps Comply architecture
- Describe CIS and DISA STIG benchmarks
- Describe the SaltStack SecOps Comply security library
- Describe the remediation differences between SaltStack SecOps and VMware Carbon Black®
- Create and manage the policies
- Create and manage the custom checks
- Run assessments on the minion systems
- Use SaltStack SecOps to remediate the non-compliant systems
- Manage the SaltStack SecOps Comply configuration options

- Manage the benchmark content ingestion

Module 9: Using SaltStack SecOps Protect

- Describe Common Vulnerabilities and Exposures (CVEs)
- Use the Protect dashboard
- Create and manage the policies
- Update the vulnerability library
- Run the vulnerability scans
- Remediate the vulnerabilities
- Manage the vulnerability exemptions