Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

VMware vRealize Automation SaltStack SecOps: Deploy and Manage [V8.6]

CODE:	LENGTH:	PRICE:
VMW_VRASSSODM86	16 Hours (2 days)	kr19,250.00

Description

This two-day, hands-on training course provides you with the advanced knowledge, skills, and tools to achieve competency in using VMware vRealize® Automation SaltStack® SecOps. SaltStack SecOps allows you to scan your system for compliance against security benchmarks, detect system vulnerabilities, and remediate your results. This course enables you to create the SaltStack SecOps custom compliance libraries and use SaltStack SecOps. In addition, this course provides you with the fundamentals of how to use VMware vRealize® Automation SaltStack® Config to install software and manage system configurations.

Objectives

By the end of the course, you should be able to meet the following objectives:

• Describe the architecture of SaltStack Config and SaltStack SecOps
• Integrate SaltStack Config with directory services.
• Configure roles and permissions for users and groups to manage and use SaltStack SecOps
• Use targeting to ensure that the jobs run on the correct minion systems
• Use remote execution modules to install the packages, transfer files, manage services, and manage users on minion systems
• Manage configuration control on the minion systems with states
• Use Jinja and YAML code to manage the minion systems with the state files
• Use SaltStack SecOps to update the compliance and vulnerability content libraries
• Use SaltStack SecOps to enforce compliance and remediation on the infrastructure with industry standard benchmarks
• Use SaltStack SecOps to provide automated vulnerability scanning and remediation on your infrastructure

Audience

Security administrators who are responsible for using SaltStack SecOps to manage the security operations in their enterprise.

Prerequisites

You should have the following understanding or knowledge:
• Basic Linux administration skills
• Basic Windows administration skills
• Knowledge and working experience of VMware vSphere® environments

Programme

1 Course Introduction • Introductions and course logistics • Course objectives 2 SaltStack Config Overview and Architecture
• Identify the SaltStack Config deployment types • Identify the components of SaltStack Config
• Describe the role of each SaltStack Config component 3 SaltStack Config Security • Describe local user authentication
• Describe LDAP and Active Directory authentication
• Describe the roles and permissions in vRealize Automation for SaltStack Config
• Describe the roles and permissions in SaltStack Config • Describe the SecOps permissions in SaltStack Config
• Describe the advanced permissions available in SaltStack Config 4 Targeting Minions • Describe targeting and its importance
• Target minions by lists • Target minions by glob • Target minions by minion ID • Target minions by regular expressions
• Target minions by compound matching • Target minions by complex logical matching 5 Remote Execution and Job Management
• Describe remote execution and its importance • Describe functions and arguments • Create and manage jobs
• Use the Activities dashboard 6 SaltStack Config State • Define the SaltStack states
• Describe file management in SaltStack Config • Create the SaltStack state files • Identify the components of a SaltStack state

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 8 Using SaltStack SecOps Compliance • Describe the SaltStack SecOps architecture • Describe CIS and DISA STIG benchmarks • Describe the SaltStack SecOps Compliance security library • Create and manage the policies • Create and manage the custom checks • Run assessments on the minion systems • Use SaltStack SecOps to remediate the noncompliant systems • Manage the SaltStack SecOps Compliance configuration options • Manage the benchmark content ingestion 9 Using SaltStack SecOps Vulnerability • Describe Common Vulnerabilities and Exposures (CVEs) • Use the vulnerability dashboard • Create and manage the policies • Update the vulnerability library • Run the vulnerability scans • Remediate the vulnerabilities • Manage the vulnerability exemptions

Session Dates

På begäran, kontakta oss

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.