سرفصل آموزشی

پک پیشرفته متخصص امنیت

فهرست سرفصل‌های دوره‌های آموزشی

سرفصل‌های دوره آموزشی

Bash Scripting

Note: In this course, you will learn each topic with code samples, practical use cases, and exercises.

Getting started with Bash Scripting

- The what and why of scripting with Bash
- What is Bash Scripting?
- Basic script building
- The Shebang!
- Bash Script name format
- Setting up permission on shell scripts
- Execute a script
- Variables and Scopes
- Special parameters
- Importance of quoting, spaces and escaping in bash scripts
- Double quote vs Single quote
- Exit codes
- Exiting an script
- Bash configuration files
- Shells and Subshells
- Random variable usage and control
- Debugging the bash script
- Creating interactive bash scripts

- Bash script controls
- Shell comments
- Documentation
- Command source and period (.)
- Scripts on system startup
- Getting and setting dates and delays

Functional Framework

- Alias and functions
- Functions with arguments
- Writing and calling functions
- Function return values
- Local variables
- Make aliases and functions permanent

Navigating to directories and Listing

- Wildcards
- Pattern matching and regular expression
- Copy, rename, delete and sorting operations
- Log control and IO redirections
- Special characters

Text Processing and Filters in your Scripts

- Head and tail
- The cut command
- The paste command
- The diff command
- The comm command

- The od Command
- The join command
- The uniq command
- The tr command
- The awk command
- The nawk command
- The sed command
- The xargs command
- The tee command

Expressions and Arithmetic

- Assignment operators
- Logical operators
- Logical NOT (!)
- Logical AND (&&)
- Logical OR (||)
- Math with the shell
- Arithmetic operators
- Math using bc
- Using bc in bash scripts
- Scale variable in bc
- Math using bash capabilities like $[ ] and (( ))
- Expr

Using Structured Commands

- Conditional execution of command lists
- Test commands (strings, integers and file types …)
- If statement
- If ... else statement
- Iterations

- Nesting ifs
- The for loop
- Advanced for loops
- Nesting loops
- While loop
- Until loop
- Loop over a range, List and the content of a file
- Internal Field Separator (IFS)
- More than one …
- Testing the loops
- Redirecting loop output
- Exiting the loop with break and Continue
- Using variables and files in loops
- True, False and:
- The Case statement

Files Operation & Navigating Directories

- Reading files and directories
- Basename and dirname
- Execution
- File Pat
- Listing and sorting
- Splitting
- Transfer

Using Sort

- Sort command and output
- Sort & Uniq
- Numeric sort
- Sort by keys

Strings

- Use regex on a string
- Uppercase & Lowercase
- Manage strings Delimiter
- Tips on string handling

Handling Script Inputs

- Positional variables
- Variables referrals
- Controlling null variables
- Reading input from files
- Special cases
- $*, $@ and $#
- Controlling the visibility of entered text
- Passing parameters to functions
- Returning values from functions

Work with files containing information records

- Fixed-length records
- Variable-length records
- Record processing
- Record-related operations
- Operations related to fixed-length records
- Operations related to variable-length records
- Merging operations

Finding files based on properties

- Concepts of file access levels
- Dealing with file sizes
- Filtering searches
- Other notable considerations

Jobs, processes and parallel processing in bash

- Pipes
- Redirections
- Background processes
- Signals and job controls
- Advanced IO redirection
- Substitutions
- Wait and parallel processing

Arrays

- Arrays assignments
- Accessing the array elements
- Array Iteration
- Array modification
- All array operations
- Sorted arrays

Monitoring processes and applications

- Monitor for starting a process
- Monitor for ending a process
- Monitor start and end of processes and log events
- Recording execution times of processes
- Common applications of monitoring
- Waiting for a program to terminate
- System load monitoring using uptime, sar, iostat, vmstat and …

Menus

- Using functions in menus
- Creating operator menus
- Give back our client a menu

Notification of events automatically

- Automate emailing
- Automate emailing with attachment
- Mail vs mailx
- The uuencode package
- Ftp, Rsync and … automation
- Remote Connection
- Passwordless connections

File Transfer automation

- Merging concepts
- Using FTP to retrieve server machine files
- Downloading files from the server

- Updating server files
- nlist
- Configuring SSH
- Reading passwords in scripts

Scheduling jobs to run in the future

- Using cron
- Using anacron
- Using at
- Controlling User access to schedulers

Debugging

- Syntax checking
- Shell tracking
- Log tracking
- Using the set command

Tricks with Shell Scripting

Security with Shell Scripting

Real-World Bash Script Training Course Scenarios:

- Generate Data Integrity Reports
- Compare Data Integrity Reports
- Unique and Duplicates Controller
- Random Digit Generator

- Files Special Filters
- Automated Interactive Input
- Parallel Executions for Time Saving
- Rotate Function
- Get and Sort play
- Get and Sort Play with Arrays
- Backup and Integrity check
- Ftp Client Automation
- User Lock and Unlock from Scratch
- Elapsed Time in Special Format
- Chkconfig Emulator (Report Generator in Fixed Length)
- High-Low Game
- Automated Pinging for Availability Check
- Multi-Platform Ping for Each OS
- Disk Space Check
- Service Control - Web Server as Sample
- Rotating Old Files
- Test Variables
- All Path Executables Files Reporter
- Id (id Command Emulation)
- Custom UserAdd Script
- File Systems and Disk Space Monitoring
- UID and GID Checker
- Data Manipulation with Fixed Offset

سرفصل‌های دوره آموزشی

Ansible

Introduction of DevOps

Understanding DevOps concepts

DevOps Automation

Continuous Integration

Continues Delivery

Continuous Deployment

The roles of Ansible in CI/CD

The benefit of CICD

What is Ansible?

Automation Deployment Pipeline

Need of Ansible

What Ansible can do?

Advantages of using Ansible?

Agent-Based VS Agentless systems

Ansible’s Agentless Architecture

Install Ansible

Validate Ansible Installation

Ansible Vs Puppet Vs Chef Vs SaltStack

Ansible Architecture

Host, Group and Host Inventory

Ansible Ad-Hoc commands

Playbooks, plays, tasks and modules

Ansible configuration

Ansible-playbook Structure

Taks, vars, files, templates, meta, defaults, handlers

Ansible-playbook Syntax

Run ansible playbook

Variables, variable types and priorities

Command, expect, script, shell and raw modules file, copy and fetch modules

Group and user modules

zyper_repository, zypper, yum_repository and you modules

Template, lineinfile, replace and service module

Archive and unarchive module

Async actions and concurrent tasks

wait_for and wait_for_connection modules

Mail module

Subversion and git modules

get_url, timezone and iptables modules

Mariadb modules

Find module and local_action feature

Conditions

Loops

Standard loops

Nested loops

Import playbooks and tasks

Handlers

Ansible Vault

Encrypt files and strings

Vault ID

Implement an Ansible playBook to Setup a webserver

Integrate Jenkins & Ansible

CICD with Git, Jenkins and Ansible (Application Deployment)

Ansible & VMWare

Ansible & Cisco

Ansible & Mikrotik

Develop Custom Module

Module format

Module’s return value and error handling

Setup nginx servers behind haproxy via Ansible playBook

Ansible & Windows Hosts

Manage windows features

Manage windows services

Execute shell module on windows

Windows Package management

Package Silent Installation

Implement an Ansible PlayBook to Setup IIS

Integrate Ansible and Docker

Docker_image and docker_image modules

docker_container and docker_container modules

docker_network and docker_network_info modules

docker_volume and docker_volume_info modules

docker_swarm module

Ansible Galaxy

Ansible Tower

Ansible AWX

AWX prerequisites and Installation

AWX Dashboard

AWX - organizations, teams and users

AWX - hosts, groups and inventory

AWX - credentials

AWX - projects and templates

AWX - Schedule templates, notification and permissions

سرفصل‌های دوره آموزشی

ELK Stack

Introduction to Elastic Stack

- What is the Elastic Stack? Overview and History
- Working with data, structured vs. semi-structured vs. unstructured data
- Overview of the data analysis process
- What is Big Data? Characteristics (3Vs: Volume, Velocity, Variety)
- Elastic Stack vs. ELK Stack, Evolution and Components
- Common Use Cases: Log Management, Business Analysis, Security Analytics, Monitoring
- Installing Elastic Stack Components: Elasticsearch, Logstash, Kibana, Beats

Deep Dive into Elasticsearch

- Elasticsearch Architecture: Nodes, Clusters, and Indexes
- What is API and advanced usage of API in Elasticsearch
- Data Modeling and Indexing
- Understanding Mapping, Documents, and Fields
- CRUD Operations: Create, Read, Update and Delete data
- Search Queries: Term, Match, Range, Aggregations
- Advanced Search and Filtering: Bool Queries, Nested, and Geo Queries
- Performance Tuning with Sharding, Replication, Caching, and Index Management

Data Collection with Logstash

- Introduction to Logstash, architecture and Pipeline Concepts
- Configuring input plugins for various data sources
- Reading data from different sources (logs, metrics, CSVs, Databases, etc.)
- Input Plugins: File, Syslog, Beats, JDBC
- Data Transformation using filters for parsing, enriching, and transforming data
- Output Plugins: Elasticsearch, File, Email, Kafka
- Managing and Debugging Pipelines
- Logstash Configuration Best Practices

Data Visualization with Kibana

- Introduction to Kibana, Interface and Navigation
- Index Patterns and Data Discovery
- Building Visualizations with Pie Charts, Bar Graphs, Line Graphs, and Maps
- Creating Dashboards for Monitoring and Analytics
- Working with Kibana Lens for Simplified Data Exploration
- Advanced Visualizations: Timelion, Vega, Canvas
- Alerts and Reporting in Kibana
- Alarm and triggers in Kibana
- Security and Access Control in Kibana

Data Shipping with Beats

- Overview of Beats: Filebeat, Metricbeat, Packetbeat, Auditbeat, Heartbeat
- Installing and Configuring Beats
- Collecting and Parsing Log Files with FileBeat
- System and Application Metrics with MetricBeat
- Network Traffic Analysis with PacketBeat
- Security Event and File Integrity Monitoring with AuditBeat
- Uptime Monitoring with HeartBeat

- Sending Data from Beats to Elasticsearch/Logstash

Unified Data Collection with Elastic Agent

- Introduction to Elastic Agent
- Replacing Beats with Elastic Agent
- Configuring Elastic Agent for Data Collection (Log and Metric)
- Centralized Management with Fleet

Security and Monitoring in the Elastic Stack

- Securing the Stack: Role-Based Access Control (RBAC) and Encryption
- HTTPS interfaces and Secure communications
- Auditing and Compliance, Monitoring Access and Changes
- Implementing Security Rules and Alerts
- SIEM (Security Information and Event Management) and SOC Use Cases

Advanced Elastic Stack Topics

- Machine Learning in Elastic Stack: Anomaly Detection and Forecasting
- IoT integration with Elastic Stack
- Advanced alarm and triggers deployment (sending email, SMS, Physical action, etc)
- APM (Application Performance Monitoring): Tracing and Performance Metrics
- Scaling Elasticsearch Clusters, High Availability and Load Balancing
- Backup and restore Strategies for Elasticsearch
- Handling Large Datasets, Index Lifecycle Management (ILM) and Rollups

Real-World Use Cases and Projects

- Setting Up a Centralized Logging Solution
- Building a Real-Time Monitoring Dashboard for Infrastructure Metrics
- Security Analytics and Threat Detection with the Elastic Stack
- Implementing Application Performance Monitoring (APM) for services
- IoT Management and monitoring platform with elastic stack