سرفصل آموزشی

پک حرفه ای متخصص Automation

فهرست سرفصل‌های دوره‌های آموزشی

سرفصل‌های دوره آموزشی

Docker

- Introduction of DevOps
- Understanding DevOps Concepts
- DevOps Culture
- DevOps Automation
- Continuous Integration (CI)
- Continuous Integration Benefits
- Continues Delivery (CD)
- Continuous Deployment (CD)
- Continuous Integration vs Continuous Delivery vs Continuous Deployment
- The Benefits of CI/CD
- The Roles of Docker in CI/CD
- Monolithic Architecture (Benefits and Drawbacks)
- Microservice Architecture (Benefits and Drawbacks)
- Monolithic vs Microservice Architecture
- Applications on bare metals
- Hypervisor-based Virtualization
- Traditional vs Virtualized Architecture
- What is Docker?
- Docker Image
- Docker Image Architecture
- Docker Container
- Docker Registry
- Install Docker on CentOS
- Install Docker on Ubuntu

- Understanding the Docker Setup (Docker version and Docker info)
- Downloading the first Docker image
- Running the first Docker Container
- Manage Docker as a non-root user
- Containers vs Virtual machines
- Run containers on bare metals or VMs?
- Benefits of Docker containers
- What problems does Docker solve?
- Docker History
- LXC vs Docker
- Docker family tree
- Docker Engine Architecture
- Cgroups and Namespaces
- Getting rid of LXC and the monolithic Docker daemon
- Runc and containerd and shim
- Understand what happens when running a container
- Daemonless containers
- Live Restore
- The point of Docker daemon
- Docker Storage Drivers
- Storage driver types
- How to change the storage driver
- choose which storage driver to use
- Docker sock
- Run and manage containers
- List containers
- Runtime constraints on resources (Ram, Swap, CPU and Disk)
- Containers resource usage statistics (stats)
- Image naming and tagging
- Dangling images
- Search images from the CLI
- Multi Architecture images
- Show details of image or containers (inspect)

- Delete image/containers
- Docker attach vs exec
- Copy file(s) between containers and docker host
- Run script inside a container
- Manage container lifecycle (stop, wait, start, restart, kill, pause, unpause, commit, save, load, export and import)
- Container Environment Variables
- Docker Logs
- Docker Events
- Docker Flow
- Docker logging and log drivers
- Blocking and non-blocking log delivery
- Customize log driver output
- Docker Volume
- Volume management (Create, List, Display detailed information, remove, prune)
- Create an NFS Docker volume
- Bind mounts
- Tmpfs
- Sharing volumes
- Volume advantages over bind mounts
- Docker Networking
- Container network model (CNM)
- Sandbox
- Endpoints
- Network
- libnetwork
- Network Drivers (bridge, host, none, overlay, macvlan)
- Bridge network
- Docker network commands
- User-defined bridge vs default bridge
- Port mapping
- Assign dynamic or static IP to containers

- Macvlan drivers
- Service discovery
- Docker network troubleshoot (tcpdump, iperf, nestat, nmap, iftop, ctop, termshark, netcat)
- Build custom Docker image
- Dockerfile instructions (from, label, copy, add, run, env, user, workdir, volume, expose, cmd, entrypoint, shell, healthcheck)
- Dockerfile best practices
- Order matters for caching
- More specific copy to limit cache busts
- Line buddies
- Remove unnecessary dependencies
- Remove package manager cache
- Use official image
- Use more specific tags
- Look for minimal flavors
- Dockerize two sample application
- Distroless images
- Sample distroless images (Java, Python, Nodejs)
- Multistage dockerfile
- History of an image
- Container restart policy
- Docker containers exit codes
- Setup a private registry server
- Docker compose
- Docker compose file
- Deploying applications with docker compose
- Build and run applications with compose
- Docker commands to manage the compose
- Docker-compose syntax and instructions
- Docker compose network
- Docker compose volume
- Docker compose logs

- Docker compose and service dependency
- Container health check
- Setup a Python/Java application with Docker compose
- Install Wordpress via Docker compose
- Install NextCloud via Docker compose
- Install Mattermost server via Docker compose
- Install Jitsi server via Docker compose
- Install Minio server via Docker compose
- Docker swarm
- Clustering and Orchestration
- Concepts relating to Docker swarm services (node, manager, worker, service, task, ingress load balancing)
- Initializing a swarm cluster
- Join nodes to a swarm cluster
- Promote and demote a node
- Swarm manager high availability (HA)
- Raft consensus algorithm in swarm mode
- Split brain and quorum
- Swarm services
- Sync desired state with current/actual state
- Scaling a service
- Replicated vs global services
- Rolling updates in swarm mode
- Overlay network
- Ingress vs host mode
- Drain a node on the swarm
- Run a sample application on swarm, scale and update
- Run a sample application behind a HAProxy on swarm
- Docker Stack
- Deploying a sample application with Docker stack on swar
- Docker security
- Linux security technology
- Docker platform security technology

- Docker daemon attack surface
- Docker security - capabilities
- Docker security - seccomp
- Docker security - AppArmor
- Privileged container
- Container Escape
- Trivy
- Swarm tokens
- Swarm TLS and mutual authentication
- Swarm cluster store
- Docker secrets
- Swarm lock

سرفصل‌های دوره آموزشی

LPIC3-303

Topic 325: Cryptography

325.1 X.509 Certificates and Public Key Infrastructures

Weight: 5

Description: Candidates should understand X.509 certificates and public key infrastructures. They should know how to configure and use OpenSSL to implement certification authorities and issue SSL certificates for various purposes.

Key Knowledge Areas:

- Understand X.509 certificates, X.509 certificate lifecycle, X.509 certificate fields and X.509v3 certificate extensions
- Understand trust chains and public key infrastructures
- Generate and manage public and private keys
- Create, operate and secure a certification authority
- Request, sign and manage server and client certificates
- Revoke certificates and certification authorities

The following is a partial list of the used files, terms and utilities:

- openssl, including relevant subcommands
- OpenSSL configuration
- PEM, DER, PKCS
- CSR
- CRL
- OCSP

325.2 X.509 Certificates for Encryption, Signing and Authentication

Weight: 4

Description: Candidates should know how to use X.509 certificates for both server and client authentication. Candidates should be able to implement user and server authentication for Apache HTTPD. The version of Apache HTTPD covered is 2.4 or higher.

Key Knowledge Areas:

- Understand SSL, TLS and protocol versions
- Understand common transport layer security threats, for example Man-in-the-Middle
- Configure Apache HTTPD with mod_ssl to provide HTTPS service, including SNI and HSTS
- Configure Apache HTTPD with mod_ssl to authenticate users using certificates
- Configure Apache HTTPD with mod_ssl to provide OCSP stapling
- Use OpenSSL for SSL/TLS client and server tests

Terms and Utilities:

- Intermediate certification authorities
- Cipher configuration (no cipher-specific knowledge)
- httpd.conf
- mod_ssl
- openssl

325.3 Encrypted File Systems

Weight: 3

Description: Candidates should be able to setup and configure encrypted file systems.

Key Knowledge Areas:

- Understand block device and file system encryption
- Use dm-crypt with LUKS to encrypt block devices
- Use eCryptfs to encrypt file systems, including home directories and
- PAM integration
- Be aware of plain dm-crypt and EncFS

Terms and Utilities:

- cryptsetup
- cryptmount
- /etc/crypttab
- ecryptfsd

- ecryptfs-* commands
- mount.ecryptfs, umount.ecryptfs
- pam_ecryptfs

325.4 DNS and Cryptography

Weight: 5

Description: Candidates should have experience and knowledge of cryptography in the context of DNS and its implementation using BIND. The version of BIND covered is 9.7 or higher.

Key Knowledge Areas:

- Understanding of DNSSEC and DANE
- Configure and troubleshoot BIND as an authoritative name server serving DNSSEC secured zones
- Configure BIND as an recursive name server that performs DNSSEC validation on behalf of its clients
- Key Signing Key, Zone Signing Key, Key Tag
- Key generation, key storage, key management and key rollover
- Maintenance and re-signing of zones
- Use DANE to publish X.509 certificate information in DNS
- Use TSIG for secure communication with BIND

Terms and Utilities:

- DNS, EDNS, Zones, Resource Records
- DNS resource records: DS, DNSKEY, RRSIG, NSEC, NSEC3, NSEC3PARAM, TLSA

- DO-Bit, AD-Bit
- TSIG
- named.conf
- dnssec-keygen
- dnssec-signzone
- dnssec-settime
- dnssec-dsfromkey
- rndc
- dig
- delv
- openssl

Topic 326: Host Security

326.1 Host Hardening

Weight: 3

Description: Candidates should be able to secure computers running Linux against common threats. This includes kernel and software configuration.

Key Knowledge Areas:

- Configure BIOS and boot loader (GRUB 2) security
- Disable useless software and services
- Use sysctl for security related kernel configuration, particularly ASLR, Exec-Shield and IP / ICMP configuration
- Exec-Shield and IP / ICMP configuration
- Limit resource usage
- Work with chroot environments
- Drop unnecessary capabilities
- Be aware of the security advantages of virtualization

Terms and Utilities:

- grub.cfg
- chkconfig, systemctl
- ulimit
- /etc/security/limits.conf
- pam_limits.so
- chroot
- sysctl
- /etc/sysctl.conf

326.2 Host Intrusion Detection

Weight: 4

Description: Candidates should be familiar with the use and configuration of common host intrusion detection software. This includes updates and maintenance as well as automated host scans.

Key Knowledge Areas:

- Use and configure the Linux Audit system
- Use chkrootkit
- Use and configure rkhunter, including updates
- Use Linux Malware Detect
- Automate host scans using cron
- Configure and use AIDE, including rule management
- Be aware of OpenSCAP

Terms and Utilities:

- auditd
- auditctl
- ausearch, aureport
- auditd.conf
- auditd.rules
- pam_tty_audit.so
- chkrootkit
- rkhunter
- /etc/rkhunter.conf
- maldet
- conf.maldet
- aide
- /etc/aide/aide.conf

326.3 User Management and Authentication

Weight: 5

Description: Candidates should be familiar with management and authentication of user accounts. This includes configuration and use of NSS, PAM, SSSD and Kerberos for both local and remote directories and authentication mechanisms as well as enforcing a password policy.

Key Knowledge Areas:

- Understand and configure NSS
- Understand and configure PAM
- Enforce password complexity policies and periodic password changes
- Lock accounts automatically after failed login attempts

- Configure and use SSSD
- Configure NSS and PAM for use with SSSD
- Configure SSSD authentication against Active Directory, IPA, LDAP, Kerberos and local domains
- Kerberos and local domains
- Obtain and manage Kerberos tickets

Terms and Utilities:

- nsswitch.conf
- /etc/login.defs
- pam_cracklib.so
- chage
- pam_tally.so, pam_tally2.so
- faillog
- pam_sss.so
- sssd
- sssd.conf
- sss_* commands
- krb5.conf
- kinit, klist, kdestroy

326.4 FreeIPA Installation and Samba Integration

Weight: 4

Description: Candidates should be familiar with FreeIPA v4.x. This includes installation and maintenance of a server instance with a FreeIPA domain as well as integration of FreeIPA with Active Directory.

Key Knowledge Areas:

- Understand FreeIPA, including its architecture and components
- Understand system and configuration prerequisites for installing FreeIPA
- Install and manage a FreeIPA server and domain
- Understand and configure Active Directory replication and Kerberos cross-realm trusts
- Be aware of sudo, autofs, SSH and SELinux integration in FreeIPA

Terms and Utilities:

- 389 Directory Server, MIT Kerberos, Dogtag Certificate System, NTP, DNS, SSSD, certmonger
- ipa, including relevant subcommands
- ipa-server-install, ipa-client-install, ipa-replica-install
- ipa-replica-prepare, ipa-replica-manage

Topic 327: Access Control

327.1 Discretionary Access Control

Weight: 3

Description: Candidates are required to understand Discretionary Access Control and know how to implement it using Access Control Lists. Additionally, candidates are required to understand and know how to use Extended Attributes.

Key Knowledge Areas:

- Understand and manage file ownership and permissions, including SUID and SGID
- Understand and manage access control lists
- Understand and manage extended attributes and attribute classes

Terms and Utilities:

- getfacl
- setfacl
- getfattr
- setfattr

327.2 Mandatory Access Control

Weight: 4

Description: Candidates should be familiar with Mandatory Access Control systems for Linux. Specifically, candidates should have a thorough knowledge of SELinux. Also, candidates should be aware of other Mandatory Access Control systems for Linux. This includes major features of these systems but not configuration and use.

Key Knowledge Areas:

- Understand the concepts of TE, RBAC, MAC and DAC
- Configure, manage and use SELinux
- Be aware of AppArmor and Smack

Terms and Utilities:

- getenforce, setenforce, selinuxenabled
- getsebool, setsebool, togglesebool
- fixfiles, restorecon, setfiles
- newrole, runcon
- semanage
- sestatus, seinfo
- apol
- seaudit, seaudit-report, audit2why, audit2allow
- /etc/selinux/*

327.3 Network File Systems

Weight: 3

Description: Candidates should have experience and knowledge of security issues in use and configuration of NFSv4 clients and servers as well as CIFS client services. Earlier versions of NFS are not required knowledge.

Key Knowledge Areas:

- Understand NFSv4 security issues and improvements
- Configure NFSv4 server and clients
- Understand and configure NFSv4 authentication mechanisms (LIPKEY, SPKM, Kerberos)
- Understand and use NFSv4 pseudo file system
- Understand and use NFSv4 ACLs
- Configure CIFS clients
- Understand and use CIFS Unix Extensions

- Understand and configure CIFS security modes (NTLM, Kerberos)
- Understand and manage mapping and handling of CIFS ACLs and SIDs in a Linux system

Terms and Utilities:

- /etc/exports
- /etc/idmap.conf
- nfs4acl
- mount.cifs parameters related to ownership, permissions and security modes
- winbind
- getcifsacl, setcifsacl

Topic 328: Network Security

328.1 Network Hardening

Weight: 4

Description: Candidates should be able to secure networks against common threats. This includes verification of the effectiveness of security measures.

Key Knowledge Areas:

- Configure FreeRADIUS to authenticate network nodes
- Use nmap to scan networks and hosts, including different scan methods
- Use Wireshark to analyze network traffic, including filters and statistics
- Identify and deal with rogue router advertisements and DHCP messages

Terms and Utilities:

- radiusd
- radmin
- radtest, radclient
- radlast, radwho
- radiusd.conf
- /etc/raddb/*
- nmap
- wireshark
- tshark
- tcpdump
- ndpmon

328.2 Network Intrusion Detection

Weight: 4

Description: Candidates should be familiar with the use and configuration of network security scanning, network monitoring and network intrusion detection software. This includes updating and maintaining the security scanners.

Key Knowledge Areas:

- Implement bandwidth usage monitoring
- Configure and use Snort, including rule management
- Configure and use OpenVAS, including NASL

Terms and Utilities:

- ntop
- Cacti
- snort
- snort-stat
- /etc/snort/*
- openvas-adduser, openvas-rmuser
- openvas-nvt-sync
- openvassd
- openvas-mkcert
- /etc/openvas/*

328.3 Packet Filtering

Weight: 5

Description: Candidates should be familiar with the use and configuration of packet filters. This includes netfilter, iptables and ip6tables as well as basic knowledge of nftables, nft and ebtables.

Key Knowledge Areas:

- Understand common firewall architectures, including DMZ
- Understand and use netfilter, iptables and ip6tables, including standard modules, tests and targets
- Implement packet filtering for both IPv4 and IPv6
- Implement connection tracking and network address translation
- Define IP sets and use them in netfilter rules
- Have basic knowledge of nftables and nft
- Have basic knowledge of ebtables
- Be aware of conntrackd

Terms and Utilities:

- iptables
- ip6tables
- iptables-save, iptables-restore
- ip6tables-save, ip6tables-restore
- ipset
- nft
- ebtables

328.4 Virtual Private Networks

Weight: 4

Description: Candidates should be familiar with the use of OpenVPN and IPsec.

Key Knowledge Areas:

- Configure and operate OpenVPN server and clients for both bridged and routed VPN networks
- Configure and operate IPsec server and clients for routed VPN networks using IPsec-Tools / racoon
- Awareness of L2TP

Terms and Utilities:

- /etc/openvpn/*
- openvpn server and client
- setkey
- /etc/ipsec-tools.conf
- /etc/racoon/racoon.conf

سرفصل‌های دوره آموزشی

Kubernetes

Core Concepts

- Core Concepts Section Introduction
- Cluster Architecture
- Docker vs ContainerD
- ETCD For Beginners
- ETCD in Kubernetes
- Kube API Server
- Kube Controller Manager
- Kube Scheduler
- Kubelet
- Kube Proxy
- Pods
- Practice Test PODs
- ReplicaSets
- Practice Tests ReplicaSet
- Deployments
- Namespaces
- Practice Test Namespaces
- Services
- Services ClusterIP
- Practice Test Services
- Imperative Commands with kubectl
- Practice Test Imperative Commands

Scheduling

- Scheduling Section Introduction
- Manual Scheduling
- Practice Test Manual Scheduling
- Labels and Selectors
- Practice Test Labels and Selectors
- Taints and Tolerations
- Practice Test Taints and Tolerations
- Node Selectors
- Node Affinity
- Practice Test Node Affinity
- Taints and Tolerations vs Node Affinity
- Resource Limits
- Practice Test Resource Limits
- DaemonSets
- Practice Test DaemonSets
- Static Pods
- Practice Test StaticPods
- Multiple Schedulers
- Practice Test Multiple Schedulers
- Configuring Kubernetes Schedulers

Logging and Monitoring

- Logging and Monitoring Section Introduction
- Monitor Cluster Components
- Practice Test Monitor Cluster Components
- Managing Application Logs
- Download Presentation Deck
- Practice Test Managing Application Logs

Application Lifecycle Management

- Application Lifecycle Management Section Introduction
- Rolling Updates and Rollback
- Practice Test Rolling Updates Rollback
- Commands and Arguments in Docker
- Commands and Arguments in Kubernetes
- Practice Test Commands and Arguments
- Configure Environment Variables in Applications
- Configure ConfigMaps in Applications
- Practice Test Env Variables
- Secrets
- Practice Test Secrets
- Multi Containers PODs
- Practice Test Multi Container Pods
- Multi Container Pods Design Patterns
- Init Containers
- Practice Test Init Containers
- Self-Healing Applications

Cluster Maintenance

- Cluster Maintenance Section Introduction
- OS Upgrades
- Practice Test OS Upgrades
- Kubernetes Software Versions
- Cluster Upgrade Introduction
- Practice Test Cluster Upgrade Process
- Backup and Restore Methods
- Working with ETCDCTL
- Practice Test Backup and Restore Methods
- Practice Test Backup and Restore Methods 2

Security

- Security Section Introduction
- Kubernetes Security Primitives
- Authentication
- TLS Certificates
- TLS Basics
- TLS in Kubernetes
- TLS in Kubernetes Certificate Creation
- View Certificate Details
- Certificate Health Check Spreadsheet
- Practice Test View Certificate Details
- Certificate API
- Practice Test Certificates API
- kubeconfig
- Practice Test KubeConfig
- API Groups
- Authorization
- RBAC
- Practice Test RBAC
- Cluster Roles
- Practice Test Cluster Roles
- Image Security
- Practice Test Image Security
- Security Context
- Practice Test Security Context
- Network Policies
- Practice Test Network Policies
- kubectx and kubens commands
- Download Presentation Deck

Storage

- Storage Section Introductio
- Introduction to Docker Storage
- Storage in Docker
- Volume Driver Plugins in Docker
- Container Storage Interface
- Volumes
- Persistent Volumes
- Persistent Volume Claims
- Using PVC in PODs
- Practice Test Persistent Volume Claims
- Download Presentation Deck
- Storage Class
- Practice Test Storage Class

Networking

- Networking Introduction
- Pre requisite Switching Routing Gateways
- Pre requisite DNS
- Pre requisite CoreDNS
- Pre requisite Network Namespace
- Pre requisite Docker Networking
- Pre requisite CNI
- Cluster Networking
- Practice Test Explore Env
- Pod Networking
- CNI in Kubernetes
- CNI weave
- Practice Test CNI weave
- Practice Test Deploy Network Solution

- ipam weave
- Practice Test Networking weave
- Service Networking
- Practice Test Service Networking
- DNS in kubernetes
- CoreDNS in Kubernetes
- Practice Test CoreDNS in Kubernetes
- Ingress
- Ingress Annotations and rewrite target
- Practice Test CKA Ingress Net 1
- Practice Test CKA Ingress Net 2
- Download The Presentation Deck

Design and Install Kubernetes Cluster

- Designing a Kubernetes Cluster
- Choosing Kubernetes Infrastructure
- Configure High Availability
- ETCD in HA
- Important update k8s hard way
- Download Presentation Deck

Install Kubernetes the kubeadm way

- Introduction to Deployment with kubeadm
- Resources
- Provision VMs with Vagrant
- Demo Deployment with Kubeadm
- Practice Test Deploy Kubernetes Cluster using Kubeadm