

LinuC-2 Objectives V5

※出題範囲は変更の可能性がございます。

目次

- LinuCレベル2 概要
 - 名称
 - 認定条件
 - 望まれるスキルレベル
- バージョン情報
- 201試験 出題範囲
 - 2.01: システムの起動とLinuxカーネル (出題比率: 23%)
 - 2.01.1 ブートプロセスとGRUB (4)
 - 2.01.2 システム起動のカスタマイズ (3)
 - 2.01.3 Linux カーネルの構成要素 (2)
 - 2.01.4 Linuxカーネルのコンパイル (2)
 - 2.01.5 カーネル実行時における管理とトラブルシューティング (3)
 - 2.02: ファイルシステムとストレージ管理 (出題比率: 17%)
 - 2.02.1 ファイルシステムの設定とマウント (3)
 - 2.02.2 ファイルシステムの管理 (4)
 - 2.02.3 論理ボリュームマネージャの設定と管理 (3)
 - 2.03: ネットワーク構成 (出題比率: 15%)
 - 2.03.1 基本的なネットワーク構成 (3)
 - 2.03.2 高度なネットワーク構成 (3)
 - 2.03.3 ネットワークの問題解決 (3)
 - 2.04: システムの保守と運用管理 (出題比率: 27%)
 - 2.04.1 makeによるソースコードからのビルドとインストール (3)
 - 2.04.2 バックアップとリストア (3)
 - 2.04.3 ユーザへの通知 (1)
 - 2.04.4 リソース使用状況の把握 (3)
 - 2.04.5 死活監視、リソース監視、運用監視ツール (2)
 - 2.04.6 システム構成ツール (4)
 - 2.05: 仮想化サーバー (出題比率: 10%)
 - 2.05.1 仮想マシンの仕組みとKVM (3)
 - 2.05.2 仮想マシンの作成と管理 (3)
 - 2.06: コンテナ (出題比率: 8%)
 - 2.06.1 コンテナの仕組み (2)
 - 2.06.2 Dockerコンテナとコンテナイメージの管理 (3)
- 202試験 出題範囲
 - 2.07: ネットワーククライアントの管理 (出題比率: 15%)
 - 2.07.1 DHCPサーバーの設定と管理 (2)

- 2.07.2 PAM認証 (3)
- 2.07.3 LDAPクライアントの利用方法 (2)
- 2.07.4 OpenLDAPサーバーの設定 (2)
- 2.08: ドメインネームサーバー (出題比率: 12%)
 - 2.08.1 BINDの設定と管理 (3)
 - 2.08.2 ゾーン情報の管理 (2)
 - 2.08.3 セキュアなDNSサーバーの実現 (2)
- 2.09: HTTPサーバーとプロキシサーバー (出題比率: 18%)
 - 2.09.1 Apache HTTPサーバーの設定と管理 (3)
 - 2.09.2 OpenSSLとHTTPSの設定 (3)
 - 2.09.3 nginxの設定と管理 (3)
 - 2.09.4 Squidの設定と管理 (2)
- 2.10: 電子メールサービス (出題比率: 8%)
 - 2.10.1 Postfixの設定と管理 (3)
 - 2.10.2 Dovecotの設定と管理 (2)
- 2.11: ファイル共有サービス (出題比率: 12%)
 - 2.11.1 Sambaの設定と管理 (4)
 - 2.11.2 NFSサーバーの設定と管理 (3)
- 2.12: システムのセキュリティ (出題比率: 20%)
 - 2.12.1 iptables や firewalld によるパケットフィルタリング (3)
 - 2.12.2 OpenSSH サーバーの設定と管理 (4)
 - 2.12.3 OpenVPNの設定と管理 (2)
 - 2.12.4 セキュリティ業務 (3)
- 2.13: システムアーキテクチャ (出題比率: 15%)
 - 2.13.1 高可用システムの実現方式 (2)
 - 2.13.2 キャパシティプランニングとスケーラビリティの確保 (2)
 - 2.13.3 クラウドサービス上のシステム構成 (2)
 - 2.13.4 典型的なシステムアーキテクチャ (3)

LinuCLレベル2 概要

名称

認定名

LinuCLレベル2

試験の正式名称

- 201試験 : LinuC Level2 Exam 201
- 202試験 : LinuC Level2 Exam 202

認定条件

LinuC-2に認定されるには、201 と 202 の両試験に合格し、かつ有意な LinuC-1 認定を保有している必要があります。

望まれるスキルレベル

LinuCレベル2は、クラウド環境やオンプレミス環境における Linuxによるシステム構築、ネットワーク構築を行ったりLinuxの応用的なシステム管理やサーバー構築ができるために必要な知識を幅広く問います。

- 小規模から中規模までのサイトを管理する。
- 仮想マシンやコンテナを含む複数システムを統合管理する。
- 次のような異種OS(Linux, Windows)混在環境ネットワークの計画、実装、保守、一貫性の維持、セキュリティ設定、トラブルシューティングを行う。
 - LANサーバー (Samba, NFS, DNS, DHCP, クライアントの設定)
 - インターネットゲートウェイ(firewall, VPN, SSH, web cache/proxy, mail)
 - インターネットサーバー (HTTP サーバーとリバースプロキシ)
- プロジェクトメンバーを指導する。
- システム導入、案件の発注内容、予算等についてプロジェクトマネージャーに助言やサポートをする。
- 代表的な非機能要件である可用性とスケーラビリティを考慮したシステムアーキテクチャの基本パターンを理解し、実際のシステム構成に応用できる。

バージョン情報

この出題範囲は開発バージョン5.0です（正式名称は未定）。

Objectives V4.5 から V5.0 の変更点の要約と詳細が利用できます。

LinuC-2 Objectives V4.5 も利用できます。

201試験 出題範囲

2.01: システムの起動とLinuxカーネル (出題比率: 23%)

2.01.1 ブートプロセスとGRUB (4)

概要

- ブートプロセス中およびリカバリモードのLinuxシステムを適切に操作する。関連するブートローダはGRUB バージョン2 である。BIOS と UEFI のシステム両方をカバーする。

詳細

- BIOS と UEFI

- Master Boot Record (MBR)
- EFI System Partition (ESP), efibootmgr, UEFI shell
- ブートローダの標準的なオプションの変更とブートローダのシェル(コマンドライン)の使用
- ブートローダの開始とカーネルへの引継ぎ
- GRUB の起動メニューを生成する。
 - grub-mkconfig, grub2-mkconfig
- カーネルローダブルモジュールのロード
 - initrd, initramfs
- ハードウェアの初期化と設定
 - デバイス、モジュール
- ファイルシステムのチェックとマウント
- デモン / サービスの初期化と設定
 - systemctl, systemd.unit
- ハードディスクまたはリムーバブルデバイスにおけるブートローダのインストール場所を知っている。
 - grub-install, grub2-install
 - /boot/, /boot/grub/, /boot/grub2/ および /boot/efi/ の内容

2.01.2 システム起動のカスタマイズ (3)

概要

- さまざまなターゲットのシステムサービスの動作を照会および変更する。systemd と Linux のブートプロセスについての十分な理解が必要である。これには、systemd ターゲットの操作も含まれる。

詳細

- systemd
 - /usr/lib/systemd/, /etc/systemd/, /run/systemd/, systemctl, systemd-delta
 - systemctl status, systemctl list-units, systemctl start/stop, systemctl enable/disable, systemctl mask/unmask
- systemd のrescue モードと emergency モード

2.01.3 Linux カーネルの構成要素 (2)

概要

- 特定のハードウェア、ハードウェアドライバ、システムリソース、およびさまざまな要求に必要なとなるカーネルの構成要素を利用する。これには、異なる種類のカーネルイメージを実装すること、安定版および開発版のカーネルとパッチを区別すること、カーネルモジュールを利用することなども含まれる。

詳細

- Kernel の配布形式
 - bzImage , xz データ圧縮
- Kernelのモジュールとドキュメント
 - /usr/src/linux/
 - /usr/src/linux/Documentation/

2.01.4 Linuxカーネルのコンパイル (2)

概要

- Linuxカーネルの特定の機能を必要に応じて取り込んだり無効化するために、カーネルを適切に構成できる。また、必要に応じてLinuxカーネルをコンパイルし、新しいカーネルに変更点を書き込み、initrdイメージを作成し、新しいカーネルをインストールできる。

詳細

- /usr/src/linux/
 - /usr/src/linux/.config
- カーネルの Makefile
- Kernel 2.6.x、3.x、4.x、5.x のmakeのターゲット
 - all, config, xconfig, menuconfig, gconfig, oldconfig, mrproper, bzImage, modules, modules_install, rpm-pkg, binrpm-pkg, deb-pkg
- カーネル構成をカスタマイズする。
- 新しいカーネルおよび適切なカーネルモジュールを構築する。
 - /lib/modules/kernel-version/, gzip, bzip2
- 新しいカーネルおよび必要なモジュールをインストールする。
 - module tools, depmod
- ブートマネージャが新しいカーネルおよび関連付けられたファイルを探せるようにする。
- モジュールの構成ファイル
- DKMS を使用してカーネルのモジュールをコンパイルする。
 - dkms
- initrd を構成する。
 - Dracut,mkinitrd, mkinitramfs

2.01.5 カーネル実行時における管理とトラブルシューティング (3)

概要

- 2.6.x、3.x、4.x、5.x カーネルとそのロード可能なモジュールについての管理や照会ができる。ブートおよび実行時の一般的な問題を特定および修正することができる。udevを使用し

たデバイスの検知と管理について理解する。これには、udevルールのトラブルシューティングが含まれる。

詳細

- コマンドラインユーティリティを使用して、現在実行中のカーネルおよびカーネルモジュールに関する情報を取得する。
 - depmod, modinfo
- 手作業でカーネルモジュールをロードおよびアンロードする。
 - modprobe, insmod, lsmod, rmmod
- モジュールをアンロードできるタイミングを判断する。
- モジュールが受け取るパラメータを判断する。
 - /etc/modprobe.d/
- カーネルのバージョンを確認する。
 - uname
 - /lib/modules/kernel-version/modules.dep
- モジュールをファイル名ではなく別の名前でロードできるようにシステムを設定する。
- /proc ファイルシステム
 - /proc/sys/kernel/
 - /etc/sysctl.conf, /etc/sysctl.d/, /sbin/sysctl
- /sys ファイルシステム (sysfs)
- /bootおよび /lib/modules の内容
- 利用可能なハードウェアに関する情報を分析するツール
 - dmesg, lspci, lsdev, lsusb, journalctl
- udevルール
 - udevmonitor, udevadm monitor, /etc/udev/
 - /etc内のモジュール設定ファイル
- カーネルダンプを取得する。設定は含まない。
 - kdump, kexec

2.02: ファイルシステムとストレージ管理 (出題比率: 17%)

2.02.1 ファイルシステムの設定とマウント (3)

概要

- 標準的なLinuxファイルシステムの適切な設定と操作ができる。これには、各種ファイルシステムの設定およびマウントも含まれる。

詳細

- fstab設定の概念
 - /etc/fstab
- ファイルシステムのマウントとアンマウント

- mount, umount, /etc/mtab, /proc/mounts, systemd
- マウントの順番
- スワップパーティションおよびファイル进行操作するツール
 - swapon, swapoff, mkswap
- ファイルシステムを特定しマウントするための UUID の使用
 - blkid, lsblk

2.02.2 ファイルシステムの管理 (4)

概要

- システムユーティリティを使用して、Linuxファイルシステムを適切に保守できる。これには、標準的なファイルシステムの操作およびSMARTデバイスの監視が含まれる。

詳細

- ファイルシステム进行操作するツール
 - mkfs (mkfs.*), fsck (fsck.*)
- ext4进行操作するツール
 - tune2fs, dumpe2fs, dump, restore
- XFS を操作するツール
 - xfs_info, xfs_check, xfs_repair, xfsdump, xfsrestore
- subvolumes と snapshots を含む、基本的な Btrfs を操作するツール
- ext4 ファイルシステムをBtrfsに変換したり操作する。
 - btrfs, btrfs-convert
- HDD, SSD の健康状態を監視できる。
 - smartd, smartctl

2.02.3 論理ボリュームマネージャの設定と管理 (3)

概要

- 論理ボリューム、ボリュームグループ、および物理ボリュームの作成および削除ができる。これには、スナップショットと論理ボリュームのサイズ変更が含まれる。

詳細

- LVM のツールと設定ファイル
 - lvm, lvm.conf
- 物理ボリュームの作成および削除方法
 - pv* コマンド
- ボリュームグループの作成/削除、物理ボリュームの追加/削除、名前変更、有効化/無効化方法

- vg* コマンド
- 論理ボリュームの作成／削除、サイズ変更、名前変更、有効化／無効化方法
 - lv* コマンド

2.03: ネットワーク構成 (出題比率: 15%)

2.03.1 基本的なネットワーク構成 (3)

概要

- ネットワークデバイスを設定し、有線または無線のローカルネットワークと広域ネットワークに接続できる。

詳細

- Ethernetネットワークインターフェイスを設定および操作する。デフォルトルートの設定を含む。
 - ip, ifconfig, route, arp, nmcli
- 無線ネットワークを構成する。
 - iw, iwconfig, iwlist

2.03.2 高度なネットワーク構成 (3)

概要

- 複数のサブネットへの経路設定ができる。これにはルータ機能の設定も含まれる。
- ネットワークの状態を監視できる。
- ネットワークのデバイス、通信状態などを分析できる。

詳細

- ルーティングテーブルを操作するユーティリティ
 - ip, route
- IPフォワードを設定してルータ機能を実装する。
 - /etc/sysctl.conf, sysctl
- ネットワークデバイスの状態を分析するユーティリティ
 - ip, ifconfig
- TCP/IPの通信状態やトラフィックを監視および分析するユーティリティ
 - ping, ping6, netcat(nc, ncat), tcpdump, nmap, ss, netstat

2.03.3 ネットワークの問題解決 (3)

概要

- 一般的なネットワーク設定に関する問題を特定して解決できる。これには、基本的な設定ファイルの位置とコマンドに関する知識も含まれる。

詳細

- ネットワークの設定に関する情報を取得する。
 - hostname, /etc/hostname, /etc/hosts, /etc/resolv.conf, nmcli, ip
- ネットワークの通信経路の問題を特定して解決する。
 - traceroute, traceroute6, ip, route, mtr
- ハードウェアの認識と利用に関する情報を取得する。
 - dmesg, /var/log/syslogおよび/var/log/messagesなどのシステムのログファイルおよび systemd のジャーナル
- システムの初期化ファイルとその内容 (systemd)
- NetworkManagerおよびそれがネットワーク設定に及ぼす影響について知っている。
 - /etc/network/, /etc/sysconfig/network-scripts/

2.04: システムの保守と運用管理 (出題比率: 27%)

2.04.1 makeによるソースコードからのビルドとインストール (3)

概要

- ソースコードから実行プログラムをビルドしてインストールできる。これには、ソースファイルの展開も含まれる。

詳細

- gitを使ってソースコードを入手する。
 - git clone, git tag -l, git checkout
- 一般的な圧縮およびアーカイブユーティリティを使用して、ソースコードを展開する。
 - gzip, gunzip, bzip2, xz, tar, unzip
- ソースコードにパッチを適用する。
 - patch
- configureスクリプトにパラメータを適用する。
 - configure
- プログラムをビルドするmakeの実行について基本を理解する。
 - make, make install

2.04.2 バックアップとリストア (3)

概要

- 重要なシステムデータをバックアップするシステムツールを使用できる。
- Linuxシステムのバックアップ計画を立てられる。

詳細

- バックアップに含める必要があるディレクトリについて決定できる。
- Amanda、Bacula、Bareos、BackupPCなどのネットワークバックアップソリューションについて知っている。
- バックアップ対象として、ファイル、ブロック、イメージを使い分けられる。
- テープ、ハードディスク、光メディアまたはその他のバックアップメディアを選択できる。
 - 容量、保存期間、ライトワンス、シーケンシャル/ランダムアクセス
- 完全バックアップ、差分バックアップ、増分バックアップを使い分けられる。
- バックアップファイルの整合性を確認する。
- バックアップを部分的または完全に復元する。
 - dd, tar, /dev/st*, /dev/nst*, mt, rsync

2.04.3 ユーザへの通知 (1)

概要

- 現在発生しているシステム関連の問題についてユーザに通知できる。

詳細

- ログオンメッセージを使用してユーザへの通知を自動的に行う。
 - /etc/issue, /etc/issue.net, /etc/motd
- アクティブなユーザにシステムの保守を通知する。
 - wall, shutdown, systemctl

2.04.4 リソース使用状況の把握 (3)

概要

- ハードウェアリソースとネットワーク帯域幅の使用率を測定でき、リソースの問題を解決できる。

詳細

- CPU使用率を測定する。
 - top, htop, ps, sar
- メモリ使用量を測定する。
 - vmstat, free, sar
- ディスクI/Oを測定する。
 - iostat, iotop, sar

- I/O 待ちのプロセス, blocks in, blocks out
- ネットワークI/Oを測定する。
 - netstat, iftop, ss, sar
- システムがオープンしているファイルやポートを表示する。
 - lsof
- ファイアウォール機能とルーティングスループットを測定する。
- クライアントの帯域幅使用率をマップする。
- ネットワーキングを含むシステムにおいてスループットを推定し、ボトルネックを見つけ出す。
 - iptraf

2.04.5 死活監視、リソース監視、運用監視ツール (2)

概要

- システム監視の重要性を理解している。
- 監視対象に応じて適切な監視手法を選択できる。
- 運用監視ツールの導入メリットと種類を理解し、適切にシステムを監視できる。

詳細

- システムの障害と予兆についての関連性を知っている。
 - リソースの枯渇、過負荷、異常停止、結果異常、OOMKiller
 - システムの死活、サービスの死活
- 死活監視の対象と手法
 - レスポンス、ログ監視 (サーバー、サービス、プロセス、ネットワーク)
- リソース監視の対象と手法
 - ログ監視、使用率監視 (CPU、メモリ、ストレージ、通信量)、SNMP
- 運用監視ツールによる監視作業の標準化と自動化
 - 標準管理項目、標準のしきい値、標準のアラート方式
 - 監視方式のパッケージ化、複数台の監視
- 主要な監視ツールを知っている。
 - Icinga2、Nagios、collectd、MRTG、Cacti、Zabbix

2.04.6 システム構成ツール (4)

概要

- システム構成ツールの必要性を理解している。
- システム構成ツールを使って、対象ホストの設定が行える。

詳細

- システム構成ツールの機能、メリットを知っている。
 - 自動化の標準化, 効率化, スケール可能, 冪等性
- Ansible の構成要素を理解している。
 - インベントリ、モジュール、Playbook
- システムの構成変更を自動化する。
 - 仮想サーバー・コンテナの払い出し
 - アプリケーションのリリース
 - ネットワーク機器のステータス取得・設定変更
- 自動化のためのファイルとツール
 - Playbook, YAML
 - ansible, ansible-playbook

2.05: 仮想化サーバー (出題比率: 10%)

2.05.1 仮想マシンの仕組みとKVM (3)

概要

- 基本的な仮想マシンの仕組みについて理解し、KVMを導入して仮想マシンの実行環境を構築できる。

詳細

- 仮想マシンの基本について知っている。
 - ホスト型とハイパーバイザー型 (KVM, VirtualBox, Xen)
 - コンピュータリソース (CPU、メモリ、ストレージ、ネットワーク) の仮想化
- KVMを導入し、仮想マシンが稼働するための環境構築および設定ができる。
 - QEMU
 - 仮想化支援技術 (vmxとsvm)
 - /proc/cpuinfo, lscpu
 - KVMモジュール (kvm-intelとkvm-amd)
 - libvirt
 - virt-manager
 - ネットワークの構成 (bridge-utils)

2.05.2 仮想マシンの作成と管理 (3)

概要

- 各種ツールを使って、仮想マシンを作成し、起動や停止ができる。

詳細

- 仮想マシンを作成し、OSをインストールする。
 - virt-manager, virt-install, 完全仮想化と準仮想化 (virtio)
- 仮想マシンを起動、停止する。
 - virt-manager, virsh
- パフォーマンスを監視する。
 - virt-manager

2.06: コンテナ (出題比率: 8%)

2.06.1 コンテナの仕組み (2)

概要

- 基本的なコンテナの仕組みについて理解している。

詳細

- 物理マシン、仮想マシン、コンテナの特徴と違いを理解している。
- コンテナのファイルシステムとイメージの関係を知っている。
- コンテナを実現する技術の概念を知っている。
 - 名前空間, cgroups

2.06.2 Dockerコンテナとコンテナイメージの管理 (3)

概要

- Dockerを導入してコンテナ実行環境を構築できる。
- Dockerコンテナを実行できる。
- コンテナイメージを管理できる。

詳細

- Dockerを導入して、ネットワークを構成する。
 - ポート変換, フラットL2ネットワーク
- Dockerコンテナを実行して、停止する。
 - docker ps/stats, docker run/create/restart, docker pause/unpause, docker stop/kill, docker rm
- Dockerコンテナに接続してプロセスを実行する。
 - docker attach, docker exec
- コンテナイメージを管理する。
 - Dockerレジストリ: docker images, docker pull, docker rmi, docker import
 - Dockerfile: docker build, docker commit

202試験 出題範囲

2.07: ネットワーククライアントの管理 (出題比率: 15%)

2.07.1 DHCPサーバーの設定と管理 (2)

概要

- DHCPサーバーを設定できる。これには、デフォルトおよびクライアントごとのオプションの設定と、静的ホストおよびBOOTPホストの追加も含まれる。また、DHCPリレーエージェントの設定とDHCPサーバーの保守も含まれる。

詳細

- DHCPの設定ファイル、用語、ユーティリティ
 - arp, dhcpd, dhcpd.conf, dhcpd.leases
 - syslog や systemd のジャーナル内の DHCP のログメッセージ
- サブネットと動的割り当て範囲の設定
- DHCPv6 と IPv6 のルータ広告について知っている。
 - radvd, radvd.conf

2.07.2 PAM認証 (3)

概要

- さまざまな方法で認証をサポートするようにPAMを設定できる。これには基本的なSSSD(System Security Services Daemon) の機能を含む。

詳細

- PAMの設定ファイル、用語、ユーティリティ
 - /etc/pam.d/, pam.conf, nsswitch.conf, sssd.conf
 - pam_unix, pam_cracklib, pam_limits, pam_listfile, pam_sss

2.07.3 LDAPクライアントの利用方法 (2)

概要

- LDAPサーバーの照会と更新ができる。また、アイテムの追加およびインポートと、ユーザの追加および管理も含まれる。

詳細

- データ管理のLDAPユーティリティ
 - ldapadd, ldapdelete, ldapmodify
- LDAPディレクトリを照会する。
 - ldapsearch
- ユーザのパスワードを変更する。
 - ldappasswd

2.07.4 OpenLDAPサーバーの設定 (2)

概要

- LDIF形式および重要なアクセス制御に関する知識も含め、基本的なOpenLDAPサーバーを設定する。

詳細

- OpenLDAP
 - slapadd, slapcat, slapindex, slapd, /var/lib/ldap/
- ディレクトリベースの設定
 - slapd-config
- アクセス管理
 - slapd.access
- 識別名 (DN)
- LDIF
- ディレクトリ
- エントリの操作
- スキーマ
 - オブジェクト ID、属性、クラス
- ホワイトページ

2.08: ドメインネームサーバー (出題比率: 12%)

2.08.1 BINDの設定と管理 (3)

概要

- 権威サーバー、再帰サーバー、キャッシュ専用DNSサーバーとして機能するようにBINDを設定できる。これには、稼働中のサーバーを管理すること、ログの設定も含まれる。

詳細

- BIND の設定ファイル、用語、ユーティリティ
 - named.conf, host, dig, nslookup
- BIND の設定ファイルで、BINDゾーンファイルの位置を定義する。

- named.conf
- 変更した設定ファイルおよびゾーンファイルの再読込
 - rndc, named-checkconf
- 代替ネームサーバーとしての dnsmasq, Unbound, NSD, PowerDNS について知っている。

2.08.2 ゾーン情報の管理 (2)

概要

- 正引き、逆引きのゾーンファイルおよびルートヒントファイルを作成できる。これには、レコードに適切な値を設定すること、ホストをゾーンに追加すること、ゾーンをDNSに追加することも含まれる。また、他のDNSサーバーにゾーンの委任を行うことも含まれる。

詳細

- BINDゾーンファイルのレイアウト、内容、ファイル配置
 - ゾーンファイルの書式, リソースレコードの書式
- 逆引きゾーンを含む、ゾーンファイルに新しいホストを追加する際の確認方法
 - named-compilezone, named-checkzone

2.08.3 セキュアなDNSサーバーの実現 (2)

概要

- DNSサーバーをroot以外のユーザとしてchroot 環境で実行するよう設定できる。これには、DNSサーバー間で安全なデータ交換を行うことも含まれる。

詳細

- chroot 環境で稼働するようBINDを設定する。
- forwarders文を使用してBINDの構成を分割する。
 - named.conf
- DNSSEC および基本的なツールについて知っている。
 - dnssec-keygen, dnssec-signzone, TSIG(Transaction Signature)
- DANE および関連レコードについて知っている。

2.09: HTTPサーバーとプロキシサーバー (出題比率: 18%)

2.09.1 Apache HTTPサーバーの設定と管理 (3)

概要

- Apache HTTP サーバーのインストールと設定ができる。これには、サーバーの負荷と性能の監視、クライアントからのユーザアクセスの制限、モジュールとしてのスクリプト言語をサポートする設定、およびクライアントユーザの認証設定も含まれる。また、サーバーのオプション設定でリソースの使用を制限することも含まれる。仮想ホストを使用するようApache HTTP サーバーを設定し、ファイルへのアクセスをカスタマイズできる。

詳細

- Apache HTTP サーバー の設定ファイル、用語、ユーティリティ
 - httpd, apache2
 - httpd.conf, mod_auth_basic, mod_authz_host
 - apachectl, apache2ctl
- Apache HTTP サーバーのログファイルの設定と内容
 - アクセスログとエラーログ
- アクセス制限の方法とファイル
 - .htaccess, AuthUserFile, AuthGroupFile
- クライアントユーザを認証するファイルとユーティリティ
 - htpasswd
- 最大リクエスト数、最小/最大サーバー数およびクライアント数の設定
- Apache HTTP サーバー における仮想ホストの実装
- ファイルへのアクセスをカスタマイズするために、Apache HTTP サーバーの設定ファイルで Redirect 文を使用する。

2.09.2 OpenSSLとHTTPSの設定 (3)

概要

- HTTPSを提供するために Apache HTTPサーバーを設定できる。

詳細

- SSL設定ファイル、ツール
 - /etc/ssl/, /etc/pki/
 - Apache HTTPサーバーの設定ファイル
 - SSLEngine, SSLCertificateKeyFile, SSLCertificateFile
 - SSLProtocol, SSLCipherSuite
- サーバーの秘密鍵および商用 CA向けのCSR を生成する。
 - openssl
- 自己署名証明書を生成する。
 - openssl
- 中間 CA を含む鍵および証明書をインストールする。
 - SSLCACertificateFile, SSLCACertificatePath
- SSLの使用に関するセキュリティ問題および安全でないプロトコルと cipher を無効にする。

2.09.3 nginxの設定と管理 (3)

概要

- リバースプロキシサーバーであるnginxのインストールおよび設定ができる。これには、HTTPサーバーとしてのnginxの設定が含まれる。

詳細

- nginxの設定と管理
 - /etc/nginx/, nginx
- nginxのSSL設定
 - ssl, ssl_certificate, ssl_certificate_key, ssl_ciphers, ssl_protocols
- リバースプロキシサーバーとしての設定
 - proxy_pass, proxy_http_version, proxy_set_header
- nginxでリダイレクトを行う

2.09.4 Squidの設定と管理 (2)

概要

- プロキシサーバーのインストールと設定ができる。これには、アクセスポリシー、認証、リソースの利用方法も含まれる。

詳細

- Squid 3.xの設定ファイル、用語、ユーティリティ
 - squid.conf, squidclient
- アクセス制限の方法
 - http_access
- クライアントユーザの認証方法
- Squid設定ファイルにおけるACLのレイアウトと内容
 - acl

2.10: 電子メールサービス (出題比率: 8%)

2.10.1 Postfixの設定と管理 (3)

概要

- 電子メールサーバーを管理できる。これには、電子メールのエイリアス、アクセス制限、仮想ドメインの設定も含まれる。また、内部的な電子メールリレーの設定および電子メールサーバーの監視も含まれる。

詳細

- Postfixの設定ファイル、スプール、ログファイル
 - /etc/postfix/, /etc/aliases, /var/spool/postfix/, /var/log/のメール関連のログ
- Postfixの基本的な TLS の設定
- SMTP認証の設定
- SMTPプロトコルに関する基本的な知識
- eximを知っている。

2.10.2 Dovecotの設定と管理 (2)

概要

- POPおよびIMAPのデーモンのインストールと設定ができる。

詳細

- Dovecot の POP と IMAP の設定と管理
 - /etc/dovecot/, dovecot.conf , doveconf, doveadm
- Dovecot 向けの基本的な TLS の設定

2.11: ファイル共有サービス (出題比率: 12%)

2.11.1 Sambaの設定と管理 (4)

概要

- さまざまなクライアント用にSambaサーバーを設定できる。これには、クライアントがログインするSambaの設定やサーバーが参加するワークグループの設定、共有ディレクトリの定義、インストールにおけるトラブルシューティングも含まれる。

詳細

- Samba の設定ファイルとログファイル
 - /etc/samba/, /var/log/samba/
- Samba のユーティリティとデーモン
 - samba, smbd, nmbd, winbindd
 - smbcontrol, smbstatus, testparm, smbpasswd, nmblookup, net, smbclient, samba-tool
- Windowsのユーザ名をLinuxのユーザ名にマッピングする。
- ACL および AD のセキュリティ
 - getfacl, setfacl

2.11.2 NFSサーバーの設定と管理 (3)

概要

- NFSを使用してファイルシステムをエクスポートできる。これには、アクセス制限、クライアントでのNFSファイルシステムのマウント、NFSの保護も含まれる。

詳細

- NFS の設定ファイル
 - /etc/exports
- NFSのユーティリティとデーモン
 - exportfs, showmount, nfsstat, rpcinfo
 - mountd, portmapper
- 特定のホストやサブネットへのアクセス制限
- サーバーとクライアントにおけるマウントオプション
 - /etc/fstab, /proc/mounts

2.12: システムのセキュリティ (出題比率: 20%)

2.12.1 iptables や firewalld によるパケットフィルタリング (3)

概要

- IPパケットを転送したり、ネットワークアドレス変換（NATやIPマスカレード）を実行するようシステムを設定し、ネットワークを保護することができる。これには、ポートリダイレクトの設定、フィルタルールの管理、攻撃の回避も含まれる。

詳細

- iptables および ip6tables のツール
 - iptables, ip6tables
- IPパケットの転送
 - /proc/sys/net/ipv4/, /proc/sys/net/ipv6/
- ルーティングテーブルを管理するためのツール
- ポートリダイレクト
- 発信元や宛先のプロトコルやポート、アドレスに基づいて、IP パケットの受入と拒否を行うフィルタおよびルールの表示と保存
 - /etc/services
- フィルタ設定の保存および再読込
 - iptables-save, iptables-restore
- firewalld で設定の確認と変更ができる。
 - firewalld, firewall-cmd
- ufw で設定の確認と変更ができる。
 - ufw

2.12.2 OpenSSH サーバーの設定と管理 (4)

概要

- SSHデーモンの設定と保護ができる。これには、鍵の管理とユーザ用にSSHを設定することも含まれる。

詳細

- OpenSSH サーバーの設定ファイルとデーモン
 - sshd, /etc/ssh/sshd_config
 - /etc/ssh/ssh_host_*_key および ssh_host_*_key.pub
- スーパーユーザおよび一般ユーザのログインを制限する。
 - PermitRootLogin, PubKeyAuthentication, AllowUsers, PasswordAuthentication

2.12.3 OpenVPNの設定と管理 (2)

概要

- VPN (仮想プライベートネットワーク) の設定および安全なポイントツーポイントまたはサイトツーサイトの接続ができる。

詳細

- OpenVPN の機能概要を理解している。
- OpenVPN の設定ファイルとツール
 - /etc/openvpn/, openvpn

2.12.4 セキュリティ業務 (3)

概要

- さまざまな情報源からセキュリティ警告を収集できる。侵入検知システムをインストール、設定、および実行できる。セキュリティパッチやバグ修正を適用できる。

詳細

- サーバーのポートをテストおよびスキャンするユーティリティ
 - netcat(nc, ncat), nmap, iptables, firewalld
- Bugtraq、CERT、CIACやその他のセキュリティ警告を報告する組織と、そのアドレスに関する知識
- IDS (Intrusion Detection System : 侵入検知システム) を実装するユーティリティ
 - fail2ban, snort
- OpenVAS や OpenSCAPについて知っている。

2.13: システムアーキテクチャ (出題比率: 15%)

2.13.1 高可用システムの実現方式 (2)

概要

- 求められる可用性のレベルを実現するシステム構成を把握している。

詳細

- 可用性に影響のある事象を理解している。
 - 故障・障害のパターン、メンテナンスによる停止（計画、緊急）など
 - 物理障害と論理障害
 - SPoF、回復性(難易度、時間)
- 可用性の評価方法を知っている。ただし計算式は含まない。
 - MTBF、MTTR、稼働率、SLA
 - RPO、RTO
- 高可用性(HA)を実現するシステム構成を知っている。
 - 冗長化によるHAの実現
 - Pacemaker, Corosync
 - HA構成の種類として クラスタやロードバランシングの概念を知っている。
- 物理的、地理的な分散による可用性レベルの違いについて知っている。

2.13.2 キャパシティプランニングとスケーラビリティの確保 (2)

概要

- 必要なリソース量を事前に予見できるシステムにおいて、近い将来に向けた拡張方法を知っている。
- 将来的に必要なリソース量が容易に予見できないシステムにおいて、現在のリソース使用状況を継続的に把握できる。

詳細

- キャパシティプランを作成するために把握しておくべきシステムリソースの観点と項目
- リソースを増減させる方法と必要な対応を知っている。
 - スケールアップ・ダウン
 - スケールアウト・イン
- スケールアップの方式を知っている。
 - 必要リソース量を搭載したマシンの再構成
- スケールアウトの方式を知っている。
 - スケールアウトに対応できるアプリケーション構成（ステートレスな構成 - DB、セッションなど）
 - 構成管理ツールや仮想マシンイメージを使ったノードの増減
 - アクセスの振り分け - ロードバランサ、DNS ラウンドロビン

2.13.3 クラウドサービス上のシステム構成 (2)

概要

- クラウドサービス上の IaaS を中心としたシステム構成の特徴を理解している。
- 必要に応じて IaaS リソースの増減が可能であることを理解している。

詳細

- クラウドのストレージの種別を理解している。
 - インスタンス動作中にのみ使用可能なストレージ(エフェメラルストレージ)
 - インスタンス停止/起動をまたいで使用可能なストレージ(永続化ストレージ)
- クラウドのネットワークの種別を理解している。
 - 固定IPアドレス、フローティングIPアドレス
- クラウドのネットワークセキュリティを理解している。
 - テナントネットワーク、ファイアウォール(セキュリティグループ)
- クラウドを支える主要な技術やサービスを理解している。
 - オブジェクトストレージ、メッセージングシステム (キュー) 、オートスケーラー

2.13.4 典型的なシステムアーキテクチャ (3)

概要

- 高可用性やスケーラビリティを確保するためのシステム構成のパターンを把握している。

詳細

- 代表的なシステム構成パターンとその特徴を知っている。
 - PHP/Apache HTTP Server+PostgreSQL/MySQLによるLAPP、LAMP構成
 - Webサーバー+APサーバー+DBサーバーによるWeb3層モデル
 - ロードバランサ、HA構成、データベースレプリケーションによる冗長性を担保したWeb3層モデル
 - ロードバランサ/DNSラウンドロビン+Webサーバーの水平スケールによるスケーラブルなWebシステム
 - プロキシサーバーによるキャッシュやCDNを活用したスケーラブルなWebシステム
 - メッセージングキューを活用した非同期データ処理システム