CompTIA.XK0-006.v2026-06-18.q108

試験コード：	XK0-006
試験名称：	CompTIA Linux+ Certification Exam
認証ベンダー：	CompTIA
無料問題の数：	108
バージョン：	v2026-06-18
ページの閲覧量：	105
問題集の閲覧量：	1093

https://www.jpnshiken.com/shiken/CompTIA.XK0-006.v2026-06-18.q108.html

質問: **1**
以下の記述のうち、Ansibleを最もよく表しているのはどれですか？
A. クラウドインフラストラクチャを監視するために使用されるツール
B. 独自の宣言型Rubyベース言語を備えたソフトウェア構成ツール
C. パイプラインを用いた自動化を可能にするCI/CDツール
D. YAMLで記述されたプレイブックを使用して自動化を提供するツール。
正解: **D** (コメントを発表する)
正解はDです。Ansibleは、YAMLで記述されたプレイブックを使用して自動化を提供するツールです。なぜなら、Ansibleは広く使用されている自動化および構成管理ツールであり、システム構成、デプロイ、およびオーケストレーションタスクを定義するためにYAMLベースのプレイブックに依存しているからです。
Ansibleはエージェントレス方式で動作するため、管理対象ノードに追加のソフトウェアをインストールする必要はありません。代わりに、SSHなどの標準プロトコルを使用してリモートシステムと通信します。自動化ロジックはプレイブックに記述されます。プレイブックは、タスク、役割、および望ましいシステム状態を記述した、人間が読みやすいYAMLファイルです。このシンプルさと読みやすさにより、AnsibleはDevOpsやLinux管理環境で特に人気があります。
選択肢Aは誤りです。Ansibleは主に監視ツールではなく、インフラストラクチャの監視にはNagios、Prometheus、Zabbixなどのツールが使用されます。
選択肢Bは、宣言型言語を使用し、Rubyをベースとするpuppetについて説明しているため、誤りです。
選択肢Cは、JenkinsやGitLab CIのようなCI/CDツールについて説明しているため、誤りです。これらのツールは、構成管理よりもパイプラインの自動化に重点を置いています。
Linux+の観点から見ると、Ansibleは自動化およびオーケストレーションツールに分類されます。ソフトウェアのインストール、構成管理、システムアップデート、デプロイプロセスといった反復的なタスクを自動化できるため、管理者にとって非常に有用です。YAMLベースのアプローチを採用することで複雑さを軽減し、保守性を向上させるため、現代のインフラストラクチャ管理および自動化ワークフローにおいて欠かせないツールとなっています。

質問: **2**
以下のユーティリティのうち、Linuxディレクトリをファイルシステムから安全に削除し、復元できないようにできるものはどれですか？
A. 追加
B. 細断
C. リンク解除
D. rm
正解: (正解を表示します)
このユーティリティは、ディスク上のデータを安全に上書きすることで復元を防止し、セキュリティのベストプラクティスに従ってファイルシステムからデータを安全に削除するのに適しています。

質問: **3**

Linuxユーザーは以下のコマンドを実行します。
nohup ping comptia.com &
プロセスを現在の端末にアタッチするために、ユーザーが実行すべきコマンドは次のうちどれですか？
A. レニス
B. 仕事
C. 実行
D. fg
正解: **(**正解を表示します**)**
Linuxシステム管理において、プロセスとジョブの実行を制御することは、CompTIA Linux+ V8の目標で広く扱われている基本的なスキルです。ここに示されているコマンドは、2つの重要な概念を組み合わせたものです。
nohupと&を使用したバックグラウンド実行。
nohup コマンドは、ハングアップシグナルの影響を受けないプロセスを実行するために使用されます。つまり、ユーザーがログアウトしたり、端末セッションが終了したりした後でも、プロセスは実行され続けます。デフォルトでは、nohup はプロセスを制御端末から切り離し、標準出力と標準エラーを nohup.out というファイルにリダイレクトします。アンパサンド (&) を末尾に追加すると、プロセスはすぐにバックグラウンドに移行し、コマンドの完了を待たずにシェルプロンプトが戻ることができます。
Linuxには、シェルセッション内でバックグラウンドプロセスとフォアグラウンドプロセスを管理できるジョブ制御メカニズムが備わっています。fgコマンドは、バックグラウンドジョブをフォアグラウンドに切り替えて現在の端末に再接続するために特別に設計されています。ジョブがフォアグラウンドになると、端末からの入力を受け取り、出力を直接表示できるようになり、Ctrl+Cなどのシグナルを使用して中断することもできます。
他の選択肢は、この要件を満たしていません。renice コマンドは、実行中のプロセスのスケジューリング優先度を変更するために使用されますが、端末への接続には影響しません。jobs コマンドは、現在のシェルに関連付けられているバックグラウンド ジョブと停止中のジョブのみを一覧表示し、それらの実行状態は変更しません。exec コマンドは、現在のシェル プロセスを新しいプロセスに置き換えますが、これはバックグラウンド ジョブの再開や接続とは無関係です。
Linux+ V8のドキュメントとジョブ制御のベストプラクティスによると、バックグラウンドプロセスを現在の端末にアタッチする正しいコマンドはfgです。したがって、選択肢Dが正解です。

質問: **4**
Linux管理者は、app-01-imagecontainerを作成し、それに接続する必要があります。以下のコマンドのうち、このタスクを実行するのはどれですか？
A. docker run -it app-01-image
B. docker start -td app-01-image
C. docker build -ic app-01-image
D. docker exec -dc app-01-image
正解: **A (**コメントを発表する**)**
docker run -it コマンドは、指定されたイメージから新しいコンテナを作成すると同時に、そのコンテナに対話的に接続します。これはまさに管理者が必要としている機能です。

質問: **5**
管理者がストレージ容量を拡張するために新しいディスクを追加しました。新しいディスクをLVMに追加するために、管理者は最初に以下のどのコマンドを実行する必要がありますか？
A. vgextend
B. lvextend
C. pvcreate
D. pvresize
正解: **C (**コメントを発表する**)**
正確な抜粋に基づく包括的かつ詳細な説明：

LVMに新しい物理ディスクを追加するには、まずpvcreateコマンドを使用してディスクを物理ボリュームとして初期化する必要があります。これにより、新しいディスクがLVMサブシステムで使用できるようになります。pvcreateで初期化した後、vgextendコマンドを使用して新しい物理ボリュームを既存のボリュームグループに追加します。
その他の選択肢：
* A. vgextend はボリューム グループに物理ボリュームを追加しますが、最初に pvcreate を使用する必要があります。
* B. lvextend は論理ボリュームのサイズを増やすために使用され、新しいディスクを追加するために使用されるものではありません。
* D. pvresize は、既存の物理ボリュームのサイズを変更するために使用され、新しい物理ボリュームを作成するために使用されません。
参照：
CompTIA Linux+ 学習ガイド：試験XK0-006、Sybex、第 7 章：ストレージの管理」、セクション：論理ボリュームの管理」 CompTIA Linux+ XK0-006 目標、ドメイン 4.0 :ストレージとファイルシステム

質問: **6**
Linux システム管理者が、新しいファイル /var/tmp/myfile を作成しています。このファイルは /usr/local/myfile を指すように設定する必要があります。両方のファイルは異なるファイルシステム上に存在します。管理者はこのタスクを実行するために、以下のどのコマンドを使用すべきでしょうか？
A. リンク /usr/local/myfile /var/tmp/myfile
B. ln -s /usr/local/myfile /var/tmp/myfile
C. touch /usr/local/myfile | file /var/tmp/myfile
D. cat /usr/local/myfile > /var/tmp/myfile
正解: **(**正解を表示します**)**
シンボリックリンクは、異なるファイルシステム上のターゲットを参照できるため、ファイルが別々のファイルシステム上に存在する場合に、/var/tmp/myfile から /usr/local/myfile へのポインタを作成するのに適した方法です。

質問: **7**
ユーザーがSSH経由で仮想サーバーへのアクセス要求を送信します。SSH標準ポートを開くには、次のうちどのコマンドを使用しますか？
A. firewalld-cmd --permanent --add-port=22/tcp
B. iptables-save | grep dport-22/tcp
C. iptables -A INPUT -p tcp --dport sshd -j ACCEPT
D. firewalld-cmd --remove-service=ssh --permanent
正解: **A (**コメントを発表する**)**
firewalld-cmd --permanent --add-port=22/tcpcommand (一般的には
firewall-cmd は、永続的な firewalld ルールセットで TCP ポート 22 を開き、SSH トラフィックを許可します。実行後、firewall-cmd --reload を実行して変更を適用します。

質問: **8**
システム管理者は、共有ディレクトリ内で新しく作成されたファイルを変更しようとした際に問題が発生しているというユーザーからの報告を受け取ります。管理者は次のような出力結果を確認します。

```
[student3@hostname share]$ ls -ld /share
drwxrwxr-x. 5 userdata users 56 Jul 9 16:31 /share
[student3@hostname share]$ ls -l
total 4
drwxrwxr-x. 2 student users 6 Jul 9 16:28 originaldata
drwxrwxr-x. 2 student users 6 Jul 9 16:28 originalfile
-rw-rw-r--. 1 student2 student2 0 Jul 9 16:31 newfile2
drwxrwxr-x. 2 student2 student2 6 Jul 9 16:31 mynewdir
-rw-rw-r--. 1 student3 student3 0 Jul 9 16:33 newfile

[student3@hostname share]$ echo "content" >> newfile2
bash: newfile2: Permission denied

[student3@hostname share]$ touch mynewdir/file
touch: cannot touch 'mynewdir/file': Permission denied
```


以下のうち、この問題に対する最適な解決策はどれですか？

A. 共有フォルダ内のユーザーにsetuidビットを追加する

B. 新しく作成されたファイルのグループを手動で変更する

C. ディレクトリの内容をすべて、誰でも書き込みおよび読み取りできるように変更します。

D. 共有フォルダ内のグループにsetgidビットを追加する

正解: **(**正解を表示します**)**

このシナリオは、共有ディレクトリでのコラボレーションに関するもので、CompTIA Linux+ V8の学習目標に含まれる一般的なシステム管理タスクです。重要な点は、ユーザーは共有ディレクトリにファイルを作成できますが、同じグループの他のユーザーはそれらのファイルを変更できないことです。この動作は、グループ所有権の継承に直接関係しています。

デフォルトでは、ユーザーがファイルまたはディレクトリを作成すると、その所有者はユーザー自身となり、親ディレクトリのグループではなく、ユーザーのプライマリグループが割り当てられます。出力に示されているように、/share 内のファイルは異なるグループ (student、student2、student3) によって所有されているため、親ディレクトリがグループ書き込み可能であっても、他のグループメンバーがファイルを変更することはできません。

正しい解決策は、共有ディレクトリにsetgid（グループID設定）ビットを設定することであり、したがってオプションDが正解となります。

setgidビットがディレクトリに適用されている場合、新しく作成されたすべてのファイルとサブディレクトリは、作成者のプライマリグループではなく、親ディレクトリのグループ所有権を継承します。これにより、グループ所有権の一貫性が確保され、共有グループのすべてのメンバーが効果的に共同作業を行うことができます。

他の選択肢は不適切、あるいは好ましくない方法です。選択肢A（setuid）は実行ファイル向けであり、ディレクトリ向けではありません。

オプションBは継続的な手動介入が必要であり、拡張性に欠ける。オプションCはすべてのユーザーに書き込みアクセス権を与えるため、最小権限の原則に違反し、セキュリティを弱める。

Linux+ V8のドキュメントでは、共有ディレクトリでsetgidビットを使用して、共同アクセスを安全かつ効率的に管理することを明示的に推奨しています。

質問: **9**

Linuxユーザーは、/home/user/scriptsディレクトリにあるシェルスクリプトを頻繁にテストします。以下のコマンドのうち、スクリプト名のみを指定してプログラムを実行できるのはどれですか？

A. export SHELL=$SHELL=/home/user/scripts

B. export TERM=$TERM=/home/user/scripts

C. export PATH=$PATH:/home/user/scripts

D. export alias /home/user/scripts='/bin'

正解: **(**正解を表示します**)**

Linuxでは、プログラム名を入力するだけでプログラムを実行できるかどうかは、実行可能ファイルを含むディレクトリがユーザーのPATH環境変数に含まれているかどうかに依存します。PATH変数は、コマンドが入力されたときにシェルが検索するディレクトリをコロンで区切ったリストを定義します。
オプションCの`export PATH=$PATH:/home/user/scripts`は、既存のPATH環境変数に`/home/user/scripts`ディレクトリを正しく追加します。このコマンドを実行すると、そのディレクトリにある実行可能スクリプトは、実行権限があればファイル名を入力するだけで実行できます。この動作は、環境変数とシェル構成に関するLinux+ V8の目標で明示的に説明されています。
他の選択肢は誤りです。選択肢AはSHELL変数を再定義しようとして誤った構文を使用しています。選択肢Bは端末の種類を制御するTERM変数を変更していますが、コマンドの実行とは関係ありません。選択肢Dはエイリアスを作成しようとして誤った構文を使用しており、コマンド検索の動作には影響しません。
Linux+ V8のドキュメントでは、スクリプトの実行を簡素化するための標準的かつ推奨される方法として、PATH環境変数の変更が強調されています。この方法は、カスタムスクリプトを頻繁に実行する開発者や管理者によって一般的に使用されています。
したがって、正解はCです。

質問: **10**
次のうち、ウェブフックを最も正確に説明しているのはどれですか？
A. ウェブサーバー通信のための認証方法
B. ネットワーク機器監視のためのSNMPベースのAPI
C. システム間で機密情報を伝送する手段
D. HTTPベースのコールバック関数
正解: **D** (コメントを発表する)
ウェブフックとは、HTTPベースのコールバックであり、あるシステムがイベント発生時にリアルタイムのデータや通知を別のシステムに送信できるようにするものです。

質問: **11**
システム管理者がLinuxシステムへのパッケージのインストールで問題が発生しています。管理者には以下の出力が表示されます。

```
# yum install packagename
...
The downloaded packages were saved in cache until the next successful transaction.
You can remove cached packages by executing 'yum clean packages'.
Error: Error downloading packages:
packagename-2023.2.60_v7.0.306-80.0.el8_8.noarch: Download failed: Curl error (77): Problem with the SSL CA cert (path? access rights?) for
https://repos.com/pulp/repos/content/dist/rhel8/8/x86_64/baseos/os/Packages/p/packagename-2023.2.60_v7.0.306-80.0.el8_8.noarch.rpm [error setting certificate verify
locations:
CAfile: /etc/pki/tls/certs/ca-bundle.crt
CApath: none]

# update-ca-trust
p11-kit: could not create file: /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem: Unknown error 2

# ls -l /etc/pki/tls/certs/ca-bundle.crt
lrwxrwxrwx 1 root root 49 Aug 3 2023 /etc/pki/tls/certs/ca-bundle.crt -> /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem

# ls -lZ /etc/pki/ca-trust/extracted/
total 4
drwxr-xr-x. 2 root root system_u:object_r:cert_t:s0 39 Jul 8 17:20 edk2
drwxr-xr-x. 2 root root system_u:object_r:cert_t:s0 35 Jul 8 17:20 java
drwxr-xr-x. 2 root root system_u:object_r:cert_t:s0 47 Jul 8 17:20 openssl
drwxr-xr-x. 2 root root system_u:object_r:etc_t:s0 101 Jul 8 17:20 pem
-rw-r--r--. 1 root root ? 560 Aug 3 2023 README

# getenforce
Enforcing
```

この問題を解決するのに最適なコマンドは次のうちどれですか？

A. dnf reinstall ca-certificates

B. touch /etc/pki/tls/certs/ca-bundle.crt

C. restorecon -R /etc/pki/ca-trust/extracted/pem

D. setenforce 0

正解: **C** (コメントを発表する)

CAバンドルパスは/etc/pki/ca-trust/extracted/pem以下のファイルへのシンボリックリンクであり、SELinuxが強制的に有効になっている間はupdate-ca-trustで生成されたバンドルを作成できません。このディレクトリのデフォルトのSELinuxコンテキストを復元することでバンドルファイルを作成できるようになり、パッケージインストール時の証明書検証エラーが解消されます。

質問: **12**

シミュレーション4

ユーザーであるジョーが、以前アンが担当していたポジションに就任しました。システム管理者として、アンのホームディレクトリにあるすべてのファイルをアーカイブし、ジョーのホームディレクトリに展開する必要があります。

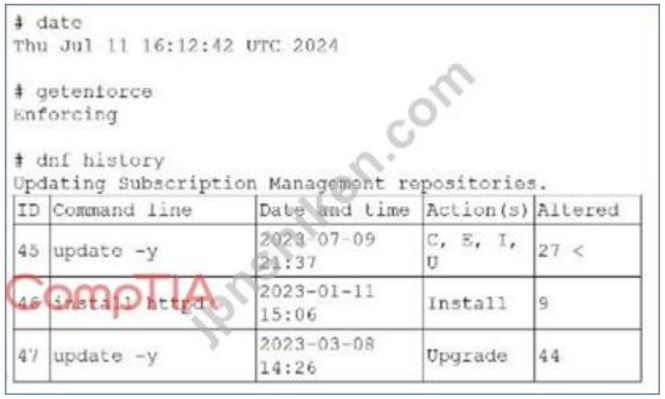
説明書

各タブ内で、オブジェクトをクリックして適切なコマンドを作成します。コマンドオブジェクトは一度しか使用できませんが、スペースバーオブジェクトは複数回使用できます。すべてのオブジェクトが使用されるわけではありません。

シミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。

正解:
アーカイブタブ：
tar -cvf /tmp/ann.tar -C /home ann
タブを抽出する：
tar -xvf /tmp/ann.tar -C /home/joe

質問: **13**
企業のセキュリティマネージャーが、Linuxシステム上の脆弱性についてシステム管理者に通知します。管理者はサーバーにログインした状態で、以下の情報を受け取ります。



```
# date
Thu Jul 11 16:12:42 UTC 2024

# getenforce
Enforcing

# dnf history
Updating Subscription Management repositories.
```

ID	Command line	Date and time	Action(s)	Altered
45	update -y	2023-07-09 21:37	C, E, I, U	27 <
46	install httpd	2023-01-11 15:06	Install	9
47	update -y	2023-03-08 14:26	Upgrade	44

次のうち、最も可能性の高いセキュリティ上の懸念事項はどれですか？
A. サーバーは1年間更新されておらず、パッチを適用する必要があります。
B. システムには httpd がインストールされているため、削除する必要があります。
C. システムはUTC時間を使用するように設定されているため、EDTに設定する必要があります。
D. システムでは SELinux が強制モードに設定されているため、無効にする必要があります。
正解: (正解を表示します)
パッケージ管理履歴を見ると、最後のシステム更新は1年以上前に行われており、セキュリティパッチや脆弱性修正が適用されていないことを強く示唆している。そのため、システムは既知の脆弱性にさらされた状態になっている。

質問: **14**
PEP 8 を説明しているのは次のうちどれですか？
A. Pythonコードのスタイルガイド
B. Python仮想環境
C. Python のパッケージインストーラ
D. 8進数値を保持するPython変数
正解: (正解を表示します)
PythonスクリプトはLinuxの自動化の一部であり、Linux+ V8にはPython開発標準に関する知識が含まれています。PEP 8はPython Enhancement Proposal 8の略で、Pythonコードの公式スタイルガイドを定義しています。
PEP 8は、コードのレイアウト、インデント、命名規則、行長、空白の使い方、コメントの付け方に関する規約を定めています。その目的は、特に共同作業環境において、コードの可読性と保守性を向上させることです。Linux+ V8は、自動化やDevOpsワークフローにおいて、標準化されたコーディング手法が極めて重要であることを強調しています。
他の選択肢は誤りです。Pythonの仮想環境はvenvなどのツールを使用して管理されます。パッケージのインストールはpipによって行われます。8進数値は特定の構文で表現され、PEP 8とは無関係です。
したがって、正解はAです。

質問: **15**
Linuxシステムにおけるプレイブックのユースケースとして、次のうちどれが最も適切でしょうか？
A. アプリケーションをデプロイするためのタスクと構成のセットを提供する
B. リポジトリにバージョン管理を実装するための手順を提供する
C. コンテナに必要なセキュリティ情報を提供する
D. ポッドに必要なストレージ容量情報を提供する
正解: (正解を表示します)

Linuxの自動化およびオーケストレーションの分野では、プレイブックはAnsibleなどの構成管理ツールと最も密接に関連しており、CompTIA Linux+ V8の目標にも明示的に記載されています。プレイブックはYAML形式で記述され、1つまたは複数のLinuxシステムに繰り返し自動的に適用されるべき一連のタスク、構成、および望ましいシステム状態を定義するように設計されています。
プレイブックの主な用途は、アプリケーションのデプロイとシステム構成の自動化です。
プレイブックを使用すると、管理者はパッケージのインストール、サービスの構成、ユーザーの管理、権限の設定、アプリケーションファイルのデプロイ、サービスの起動または有効化といったタスクを指定できます。これは、アプリケーションを複数の環境に一貫してデプロイするために必要な一連のタスクと構成を提供する方法としてプレイブックを正確に説明するオプションAと完全に一致します。
残りのオプションは、プレイブックの機能を正確に表していません。オプションBはバージョン管理の実装に関するもので、これはGitなどのツールによって処理されるものであり、プレイブック自体の目的ではありません（ただし、プレイブックはバージョン管理システムに保存される場合があります）。オプションCはコンテナのセキュリティ情報について説明していますが、これは通常、プレイブックではなく、コンテナのランタイム構成、シークレット、またはセキュリティポリシーによって管理されます。オプションDはPodのストレージボリューム情報に関するもので、Kubernetesマニフェストに特有のものであり、一般的なLinuxプレイブックの使用例ではありません。
Linux+ V8のドキュメントによると、自動化ツールとプレイブックは、人的ミスを減らし、一貫性を向上させ、Infrastructure as Code（IaC）の実践をサポートするのに役立ちます。プレイブックは、複数のシステムにわたる複数ステップの操作をオーケストレーションするための重要なメカニズムであり、現代のLinuxシステム管理に不可欠です。
したがって、正解はAです。Aは、Linuxシステムにおけるプレイブックの実際的かつ文書化された使用例を最もよく表しているからです。

質問: **16**
管理者は、Linuxコマンドの出力を既存のファイルに追加して後で分析する必要があります。管理者は次のコマンドライン文字列のうちどれを使用すべきでしょうか？
A. cat ls > file.txt
B. tee ls > awk file.txt
C. echo ls | sed -i file.txt
D. ls > > file.txt
正解: **D** (コメントを発表する)
正解はDです。`ls > > file.txt` は、Linuxにおいて`> >`（二重大なり演算子）が既存のファイルの内容を上書きせずに出力を追加するために使用されるためです。これはシェルリダイレクトの基本的な概念であり、スクリプト作成や自動化タスクで広く使用されています。
このコマンドでは、ls コマンドがディレクトリの内容一覧を生成し、> > file.txt によってこの出力がファイルの末尾に追加されます。ファイルが存在しない場合は自動的に作成され、既に存在する場合は既存の内容はそのまま保持され、新しい出力はその下に追加されます。
オプションA（cat ls > file.txt）は誤りです。なぜなら、cat lsはlsコマンドを実行するのではなく、「ls」という名前のファイルを読み込もうとするからです。さらに、>は追記ではなく上書きしてしまいます。
オプションB（tee ls > awk file.txt）は構文が無効であり、teeコマンドやリダイレクトが正しく使用されていません。teeコマンドは標準出力とファイルの両方に出力を書き込むために使用されますが、この例は形式が間違っています。
オプションC（echo ls | sed -i file.txt）は、lsコマンドを実行せず、単に文字列「ls」をエコーするだけで、sedを使用してファイルを不適切に変更しようとするため、誤りです。
Linux+の観点から言えば、リダイレクト演算子（>、>>、|）を理解することは、自動化やスクリプト作成において不可欠です。特に、出力ログの記録、コマンド結果の収集、過去のデータを失うことなく時系列でレポートを作成する際には、>>演算子が重要になります。

質問: **17**

Linux 管理者は、マルウェアの痕跡がないか、侵害されたディスクを分析する必要があります。分析を完了するために、管理者はディスクの正確なブロックレベルのコピーを作成したいと考えています。このタスクを実行するコマンドは次のうちどれですか？
A. cp -rp /dev/sdc/* /tmp/image
B. cpio -i /dev/sdc -ov /tmp/image
C. tar cvzf /tmp/image /dev/sdc
D. dd if=/dev/sdc of=/tmp/image bs=8192
正解: **(**正解を表示します**)**
ddコマンドは、デバイスの低レベルなブロック単位のコピーを実行します。if=/dev/sdc（入力ファイル）とof=/tmp/image（出力ファイル）にブロックサイズ（bs）を指定することで、フォレンジック分析に適したディスクの正確な複製を作成できます。

質問: **18**
管理者がファイルシステムのアンマウントを試みた際に、以下の出力が表示されます。
umount /data1: ターゲットがビジー状態です。
ファイルシステムがビジー状態になっている理由を特定するために、管理者は次にどのコマンドを実行すべきでしょうか？
A. ps -f /data1
B. you -sh /data1
C. top -d /data1
D. lsof | grep /data1
正解: **D (**コメントを発表する**)**
ファイルシステムのアンマウント失敗は、Linux+ V8 で取り上げられている一般的なトラブルシューティングシナリオです。
「ターゲットがビジー状態です」というメッセージが表示される場合、1つ以上のプロセスがマウントポイント内のファイルまたはディレクトリをアクティブに使用していることを意味します。
正しい診断コマンドは lsof | grep /data1 です。lsof（開いているファイルの一覧表示）ユーティリティは、開いているすべてのファイルと、それらを使用しているプロセスを表示します。grep /data1 で出力をフィルタリングすることで、ファイルシステム上のファイルディスクリプタを保持し、アンマウントを妨げているプロセスを正確に特定できます。
他のオプションは正しくありません。ps -f はプロセス情報を表示しますが、開いているファイルの使用状況は表示しません。du -sh はディスク使用量を計算しますが、アクティブなプロセスを識別しません。top はシステムのパフォーマンスを監視しますが、ファイルシステムのロックを特定することはできません。
Linux+ V8のドキュメントでは、ファイルシステムをアンマウントする前に、lsofまたはfuserを使用してリソースロックを特定することが推奨されています。したがって、正解はDです。

質問: **19**
システム管理者が新しいWebアプリケーションのセキュリティ対策を支援しています。テスト中に、管理者はアプリケーションを検証するために以下の出力を取得しました。

```
* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-CCM-SHA384
* ALPN, server accepted to use http/1.1
* Server certificate:
*   subject: CN=*.newapp.comptia.org
*   start date: Jan 17 00:00:00 2024 GMT
*   expire date: Feb 16 23:59:59 2034 GMT
*   issuer: C=US; O=CompTIA; OU=IT Security; CN=ssl.comptia.org
*   SSL certificate verify result: unable to get local issuer certificate (20), continuing anyway.
> HEAD /artifactory HTTP1.1
> Host: api.newapp.comptia.org
> User-Agent: curl/7.61.1
> Accept: */*
```

次のうち、検証結果を説明しているのはどれですか？

A. 証明書は信頼できる機関によって署名されておらず、テスト中に強制的に無視されました。

B. 証明書は発行から1ヶ月しか経っておらず、既に期限切れとなっているため、交換が必要です。

C. この証明書は、非常に安全性の低いワイルドカード証明書であり、決して使用すべきではありません。

D. この証明書は古いアルゴリズムを使用しているため、より安全なものに交換する必要があります。

正解: (正解を表示します)

検証出力によると、ローカルシステムが発行元の認証局を信頼していないため、証明書チェーンを検証できませんでしたが、テスト中は検証の失敗を無視して接続が続行されました。

質問: **20**

ユーザー1は、アプリを実行しようとした際に 「アクセス拒否」エラーを報告しました。以下の出力が与えられています。

```
[devops@training data]$ id user1
uid=1011(user1) gid=1011(user1) groups=1011(user1)

$ ls -la app
-rwxrwx---. 1 devops devops 5423 Jan 3 2022 app

$ getfacl app
# file: app
# owner: devops
# group: devops
user::rwx
user:user1:rw
group::rwx
other::---
```

以下の選択肢のうち、この問題を解決するものはどれですか？

A. ACLでuser1に実行権限を付与する

B. 他者に読み取り、書き込み、実行の権限を付与する権限の変更

C. ユーザー1をホイールグループに追加します

D. アプリを別のフォルダに移動する

正解: (正解を表示します)

getfacl app の出力によると、user1 には「rw」（読み書き）権限しかなく、「x」（実行）権限がありません。実行権限がないため、user1 はファイルを実行できません。user1 が app を実行できるようにするには、ACL を更新して実行権限を追加する必要があります（例setfacl -mu:user1:rwx app）。「others」権限を変更する（オプション B）のは安全ではなく、必要でもありません。user1 を wheel グループに追加する（オプション C）のは無関係であり、ファイルを移動する（オプション D）ことでも権限の問題は解決しません。
参照：
CompTIA Linux+ 学習ガイド：試験XK0-006、Sybex、第 7 章：「Linux システムのセキュリティ保護」、セクション：「ファイルとディレクトリのアクセス許可と ACL の管理」、CompTIA Linux+ XK0-006 目標、ドメイン 3.0 :セキュリティ

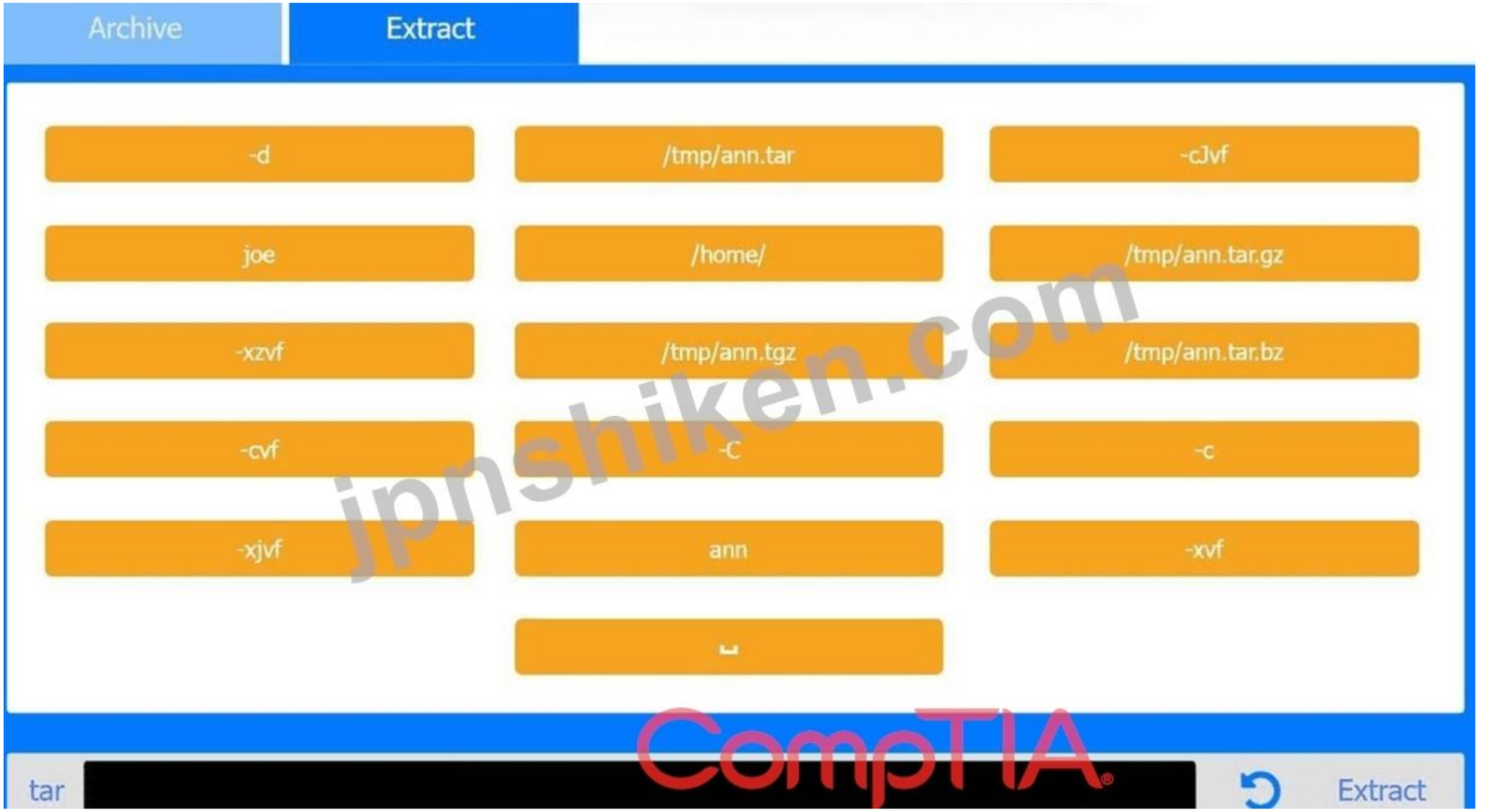
質問: **21**
ユーザーであるジョーが、以前アンが担当していたポジションに就任しました。システム管理者として、アンのホームディレクトリにあるすべてのファイルをアーカイブし、ジョーのホームディレクトリに展開する必要があります。
説明書
各タブ内で、オブジェクトをクリックして適切なコマンドを作成します。コマンドオブジェクトは一度しか使用できませんが、スペースバーとアンダースコア（_）のオブジェクトは複数回使用できます。すべてのオブジェクトが使用されるわけではありません。
シミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。

Archive | Extract

-d	/tmp/ann.tar	-cJvf
joe	/home/	/tmp/ann.tar.gz
-xzvf	/tmp/ann.tgz	/tmp/ann.tar.bz
-cvf	-C	-c
-xjvf	ann	-xvf
␣		

tar /home/-C

Archive



正解:

解決策については、下記の解説をご覧ください。

Explanation:

アーカイブタブ - アンのホームディレクトリからアーカイブを作成します

正しいコマンド:

tar -cvf /tmp/ann.tar -C /home/ann

抽出タブ - アーカイブをジョーのホームディレクトリに展開します

正しいコマンド:

tar -xvf /tmp/ann.tar -C /home/ joe

この実技問題は、CompTIA Linux+ V8の目標に含まれるシステム管理の中核スキルである、tarを使用したファイルアーカイブと復元をテストするものです。課題は、Annのファイルを保存し、Joeのホームディレクトリに正しく配置することです。

アーカイブフェーズの説明

最初のステップの目標は、フルパス（/home）を埋め込まずに、Annのホームディレクトリ全体をアーカイブすることです。
/ann) をアーカイブ内に挿入します。これは -C オプションを使用して行います。
コマンドの詳細：
* tar # アーカイブユーティリティ
* -c # アーカイブを作成する
* -v # 詳細出力（オプションですが使用可能）
* -f /tmp/ann.tar # アーカイブファイルを指定します
* -C /home/ # アーカイブ前にディレクトリを変更します
* ann # ann ディレクトリのみをアーカイブします
これにより、絶対パスを含まないAnnのファイルを含むクリーンなアーカイブが作成されます。これはベストプラクティスであり、Linux+ V8のドキュメントにも明記されています。
抽出フェーズの説明
2番目の手順では、アーカイブされたファイルをジョーのホームディレクトリに展開します。
コマンドの詳細：
* -x # 抽出
* -v # 詳細表示
* -f /tmp/ann.tar # アーカイブを指定します
* -C /home/joe # ファイルをジョーのホームディレクトリに直接展開します
これにより、抽出後の処理に応じて、Joe は Ann のファイルを /home/joe/ann または /home/joe 直下に正しく受け取ることができ、これは Linux+ の管理ユーザー移行に関する期待と一致します。

質問: **22**
Linux 管理者が Linux マシン上で CUPS 印刷サービスを設定しており、ローカル ネットワークからの接続のみを許可する必要があります。管理者は、次のうちどのコマンドを使用すべきでしょうか？
A. iptables -A OUTPUT -d 192.168.100.0/24 --sport 631 -p tcp -j ACCEPT
B. iptables -A OUTPUT -s 192.168.100.0/24 --dport 631 -p tcp -j ACCEPT
C. iptables -A INPUT -s 192.168.100.0/24 --dport 631 -p tcp -j ACCEPT
D. iptables -D INPUT -d 192.168.100.0/24 --dport 631 -p tcp -j ACCEPT
正解: (正解を表示します)
CUPSサービスへのアクセスを許可するには、ローカルネットワークからポート631へのTCP接続を許可する必要があります。送信元ネットワークと宛先ポート631を指定したINPUTルールを追加することで、そのサブネット上のホストのみが印刷サービスに接続できるようになります。

質問: **23**
ユーザーから、Linuxシステムが応答せず、簡単なコマンドの実行に時間がかかりすぎるとの報告がありました。Linux管理者がシステムにログインすると、次の出力が表示されます。出力1:
10:06:29 稼働時間 235日、19:23、ユーザー数 2、ロードアベレージ: 8.71、8.24、7.71

Output 2:

Linux 6.8.0-31-generic (host) 05/10/2024 _x86_64_ (4 CPU)

10:07:42	AM	CPU	%usr	%nice	%sys	%iowait	%irq	%soft	%steal	%guest	%gnice	%idle
10:07:42	AM	all	65.88	0	20.54	5.65	0	7.93	0	0	0	0

システムは以下のうちどれを経験していますか？
A. 高遅延
B. 高い稼働率

C. CPU負荷が高い
D. 高いI/O待ち時間
正解: **(**正解を表示します**)**
このシナリオは、CompTIA Linux+ V8の目標におけるトラブルシューティング領域で扱われる、典型的なパフォーマンス問題のトラブルシューティング事例です。分析すべき主要な指標は、ロードアベレージ値とCPU使用率の統計情報です。
uptimeコマンドの結果によると、1分、5分、15分間隔での負荷平均はそれぞれ8.71、8.24、7.71でした。
ロードアベレージとは、CPU上で実行中または実行待ち状態のプロセスの平均数を表します。4つのCPUコアを搭載したシステムでは、正常なロードアベレージは通常4以下です。ロードアベレージが常に8前後または8を超える場合は、実行可能なプロセス数が利用可能なCPUリソースを大幅に上回っていることを示し、プロセスが待機状態となり、システムの応答性が低下します。
CPU出力もこの状況を裏付けています。%idleの値は0であり、CPUにアイドル時間が全くないことを意味します。CPU時間の大部分はユーザー空間（65.88%）とシステム/カーネル空間（20.54%）で消費されており、計算処理とカーネル処理が活発に行われていることを示しています。%iowaitは5.65%ですが、ディスクI/Oが主なボトルネックであると示唆するほど高い値ではありません。
オプションCの「CPU負荷が高い」が、症状を最もよく説明しています。CPU負荷が高いと、限られたCPU時間をめぐってプロセスが競合するため、コマンドの実行速度が低下します。これは、システムが応答しなくなるという観測された動作と直接的に一致します。
他の選択肢は誤りです。高い稼働時間は、システムが稼働している時間の長さを示すだけであり、それ自体がパフォーマンスの問題を引き起こすわけではありません。高いレイテンシは一般的な用語であり、提供されたメトリックによって示される具体的な診断ではありません。高いI/O待機時間には、%iowaitの値が著しく高くなる必要があります。
Linux+ V8のドキュメントによると、負荷平均とCPUコア数および使用率を関連付けることは、正確なパフォーマンス診断に不可欠です。したがって、正解はC. CPU負荷が高い、です。

質問: **24**
システム管理者は複数のLinuxサーバーを管理しており、OSレベルおよびアプリケーションレベルでのイベントレコード管理の複雑さに対処するための、信頼性が高く安全な方法を確立する必要があります。管理者は次のうちどれを行うべきでしょうか？
A. 必要に応じてサーバーからログを取得する自動化プロセスを作成します。
B. 集中型ログ集約ソリューションを実装する。
C. ログの自動バックアップをリモートストレージに毎日設定します。
D. ログローテーション手順を展開して記録を管理します。
正解: **B (**コメントを発表する**)**
ログ管理は、CompTIA Linux+ V8で特に強調されている重要なシステム管理機能であり、特にマルチサーバー環境においてはその重要性が高まります。システムやアプリケーションの数が増えるにつれて、各サーバー上でローカルにログを管理することは非効率的になり、エラーが発生しやすくなります。
最適な解決策は、集中型ログ集約ソリューションを導入することであり、選択肢Bが正解です。集中型ログ管理では、複数のシステムやアプリケーションからのログを単一の安全な場所に収集します。これにより、監視、検索、相関分析、監査、インシデント対応が簡素化されます。一般的なソリューションとしては、syslogサーバー、ELK/EFKスタック、SIEMプラットフォームなどがあります。
Linux+ V8のドキュメントでは、可用性、トラブルシューティング、セキュリティ分析のためのベストプラクティスとして、集中ログ管理が強調されています。これにより、管理者は個別のログファイルよりも効果的にパターンを検出し、インシデントを調査し、コンプライアンスを維持することができます。
他の選択肢は単独では不十分です。オンデマンド取得は拡張性に乏しく、ログバックアップはデータを保護しますが分析を簡素化しません。ログローテーションはディスク使用量を管理しますが、分散ログの複雑さには対応できません。
したがって、正解はBです。集中型ログ集約ソリューションを実装してください。

質問: **25**
journaldを最もよく表しているのは次のうちどれですか？
A. ログデータを収集・保存するシステムサービス
B. カーネル障害発生時にクラッシュダンプを作成する機能
C. ファイルシステムジャーナルを保持するサービス

D. 監査記録をディスクに書き込む役割を担うサービス
正解: **A (**コメントを発表する**)**
systemdの一部であるjournaldは、最新のLinuxシステムにおけるコアログサービスであり、Linux+ V8のログ記録および監視目標の対象となっています。
正しい説明はAです。systemd-journaldは、カーネル、システムサービス、およびアプリケーションからのログデータを収集、保存、およびインデックス化します。ログは構造化されたバイナリ形式で保存され、journalctlを使用してクエリを実行できます。Journaldは、メタデータタグ付け、ログフィルタリング、および集中ログ統合をサポートしています。
オプションBは、kdumpなどのカーネルクラッシュダンプ機構を指します。オプションCは、ファイルシステムジャーナリング（ext4ジャーナリングなど）について説明します。オプションDは、セキュリティ監査ログを管理するauditdを指します。
Linux+ V8のドキュメントでは、journaldが他のログ記録および監査サービスと明確に区別されています。したがって、正解はAです。

質問: **26**
以下の記述のうち、Ansibleを最もよく表しているのはどれですか？
A. クラウドインフラストラクチャを監視するために使用されるツール
B. 独自の宣言型Rubyベース言語を備えたソフトウェア構成ツール
C. パイプラインを用いた自動化を可能にするCI/CDツール
D. YAMLで記述されたプレイブックを使用して自動化を提供するツール。
正解: **(**正解を表示します**)**
Ansibleは、人間が読みやすいYAMLプレイブックを使用してタスクを定義する自動化および構成管理ツールであり、システム全体で一貫性のあるエージェントレスの自動化を実現します。

質問: **27**
システム管理者は、Linux システム上でネットワーク 10.0.0.0/24 から DNS TCP ポートを開放する必要があります。
管理者はこのタスクに以下のどのコマンドを使用すべきですか？
A. ufw は 10.0.0.0/24 への DNS/TCP を許可します
B. ufw enable 53/tcp from 10.0.0.0/24
C. ufw allow 53/tcp from 10.0.0.0/24
D. ufwを10.0.0.0/24から無効化します
正解: **C (**コメントを発表する**)**
ファイアウォールの設定は、CompTIA Linux+ V8 のセキュリティ分野における重要なトピックです。DNS は主に UDP ポート 53 を使用しますが、ゾーン転送、大規模な応答、および特定の信頼性シナリオでは TCP ポート 53 も必要になります。この場合、管理者は特定のネットワークからの TCP 経由の DNS を明示的に許可する必要があります。
正しいコマンドは `ufw allow 53/tcp from 10.0.0.0/24` です。このルールは、最小権限の原則に従い、指定されたサブネットからのポート 53 への受信 TCP トラフィックのみを許可します。Linux+ V8 のドキュメントでは、攻撃対象領域を最小限に抑えるため、可能な限り送信元ネットワークに基づいてファイアウォールルールを制限することが推奨されています。
オプションAは、dnsなどのUFWサービスエイリアスが必ずしもTCPに明示的にマッピングされるとは限らず、構文も不完全であるため誤りです。オプションBは、ufw enableコマンドはファイアウォールをグローバルに有効にするために使用され、ルールを定義するものではないため無効です。オプションDはファイアウォール保護を無効にし、重大なセキュリティリスクをもたらします。
Linux+V8のベストプラクティスでは、広範囲にわたる対策や無効化措置ではなく、正確で最小限のファイアウォールルールを重視する。
したがって、Cが正しく安全な選択肢である。

質問: **28**
管理者は、ディレクトリ /home/user1/data とそのすべてのコンテンツを削除する必要があります。管理者は、以下のどのコマンドを使用すべきでしょうか？
A. rmdir -p /home/user1/data
B. ln -d /home/user1/data
C. rm -r /home/user1/data

D. cut -d /home/user1/data
正解: (正解を表示します)
ファイルとディレクトリの管理は、Linux+ V8で取り上げられているシステム管理の中核的なスキルです。管理者がファイルやサブディレクトリを含むディレクトリを削除する必要がある場合、再帰的な削除が必要になります。
正しいコマンドは `rm -r /home/user1/data` です。`rm` コマンドはファイルを削除しますが、`-r` (再帰) オプションを使用すると、ディレクトリとその中のすべてのコンテンツ（ネストされたファイルやサブディレクトリを含む）を削除できます。これは、空でないディレクトリを削除するための標準的かつ正しい方法です。
他のオプションは誤りです。rmdir -p は空のディレクトリのみを削除するため、ディレクトリにファイルが含まれている場合は失敗します。ln -d はディレクトリのハードリンクを作成するためのコマンドであり、ディレクトリを削除するためのものではありません。cut -d はファイルシステム操作とは無関係のテキスト処理コマンドです。
Linux+ V8のドキュメントでは、rm -rコマンドの使用には注意が必要だと強調されています。バックアップが存在しない限り、データは完全に削除され、復元することはできません。したがって、正解はCです。

質問: **29**
Linux管理者は、システム上でホストされているアプリケーションが割り当てられた時間内にタスクを完了していないという報告を受け取ります。管理者はシステムに接続し、以下の詳細情報を取得します。

```
# uptime
12:47:43 up 22:17, 2 users, load average: 7.75, 5.72, 5.17

# nproc
4

# vmstat -w 1 3
[...]
r b swpd free    buffcache si so bi bo in   cs  us sy id wa st gu
8 0 671563760348103671476 0  0  0  0 40901 386100 0  0  0  0  0
8 0 671563760348103671476 0  0  0  0 40076 1389100 0  0  0  0  0
8 0 671563760348103671476 0  0  0  0 40076 1389100 0  0  0  0  0

# free -h
       total  used  free shared buff/cache available
Mem:   3.8Gi 334Mi 3.6Gi   20Mi       70Mi     3.5Gi
Swap:  7.8Gi  65Mi 7.8Gi
```

管理者は、ジョブの処理速度を向上させるために、次のうちどの行動をとることができますか？
A. システムが使用できる空きメモリの量を増やします。
B. システムに利用可能なCPUリソースの量を増やします。
C. システムに使用可能なスワップ領域の量を増やします。
D. システムが使用できるディスクの容量を増やします。
正解: (正解を表示します)
このシナリオは、典型的なCPUバウンドのパフォーマンス問題であり、CompTIA Linux+ V8のトラブルシューティング領域で扱われています。最も重要な指標は、利用可能なCPUコア数に対する負荷平均です。システムはnprocで示されるように4つのCPUコアを備えていますが、ロードアベレージは常に5を超え、ピーク時には7.75に達します。ロードアベレージは、CPU上でアクティブに実行されているプロセス、またはCPU時間を待機しているプロセスの数を表します。ロードアベレージが長期間にわたってCPUコア数を超えると、CPU競合が発生していることを示します。プロセスはスケジューリングされるまでより長く待機する必要があり、結果としてタスクの完了が遅延します。
メモリ統計情報から、メモリがボトルネックではないことが確認できます。free -h コマンドでは 3.5 GiB 以上のメモリが利用可能であることが示され、スワップ使用量も最小限です。さらに、vmstat ではスワップインやスワップアウトのアクティビティはほとんどなく、I/O 待機時間も低いため、メモリ負荷やディスクのボトルネックも除外されます。

スワップ領域を増やしても効果はありません。なぜなら、システムはメモリ不足ではないからです。ディスクを追加しても、CPUスケジューリングの遅延は解消されません。十分なメモリが既に確保されているため、空きメモリを増やす必要はありません。
Linux+ V8のドキュメントでは、CPU飽和状態を診断するために、負荷平均とCPUコア数を関連付けることが強調されています。この場合、ジョブの実行速度を向上させる最も効果的な方法は、vCPUの追加、ワークロードをより高性能なシステムへの移行、またはワークロードを複数のシステムに分散するなど、CPUリソースを増やすことです。
したがって、正解はBです。システムに利用可能なCPUリソースの量を増やします。

質問: **30**
システム管理者は、ntpdサービスが起動時に自動的に開始するように設定されているかどうかを確認したいと考えています。以下のコマンドのうち、どれを実行するとその情報が表示されますか？
A. systemctl is-enabled ntpd.service
B. systemctl start ntpd.service
C. systemctl is-active ntpd.service
D. systemctl stop ntpd.service
正解: (正解を表示します)

質問: **31**
Linuxに組み込まれている実行可能ファイルとユーティリティの場所は、次のうちどれですか？
A. /bin
B. /var
C. /etc
D. /sys
正解: (正解を表示します)
/bin には、基本的なシステム操作とユーザー作業に必要な、Linux に組み込まれた必須の実行可能ファイルとコアとなるコマンドラインユーティリティが含まれています。

質問: **32**
Linuxシステムで非対話型アカウントを作成する最良の方法はどれですか？
A. 特別な特権なし
B. パスワードなしでadduserを使用する
C. ホームディレクトリがない場合
D. シェルを /sbin/nologin に設定
正解: (正解を表示します)
ユーザーのシェルを /sbin/nologin に設定すると、対話型ログインは防止されますが、サービスやバックグラウンドプロセス用のアカウントは引き続き存在できます。これは、非対話型アカウントを作成する標準的な方法です。

質問: **33**

以下のうち、JSONを最もよく表しているのはどれですか？
A. 開発者が動的なウェブサイトを構築するために使用するプログラミング言語
B. 隔離された環境の作成と管理を容易にするオープンソースプラットフォーム
C. システム間で情報やデータを交換するためのファイル形式
D. コンピュータが1つまたは複数の機械をシミュレートして、それらが実在するかのように見せるソフトウェアベースの技術。
正解: **C** (コメントを発表する)
JSON（JavaScript Object Notation）は、人間が読み書きしやすく、機械が解析・生成しやすい軽量なデータ交換フォーマットです。JSONは言語に依存せず、様々な環境で使用できるため、サーバーとクライアント間のデータ送信によく用いられます。

質問: **34**
システム管理者は、共有ディレクトリ内で新しく作成されたファイルを変更しようとした際に問題が発生しているというユーザーからの報告を受け取ります。管理者は次のような出力結果を確認します。

```
[student3@hostname share]$ ls -ld /share
drwxrwxr-x. 5 userdata users 56 Jul 9 16:31 /share
[student3@hostname share]$ ls -l
total 4
drwxrwxr-x. 2 student users 6 Jul 9 16:28 originaldata
drwxrwxr-x. 2 student users 6 Jul 9 16:28 originalfile
-rw-rw-r--. 1 student2 student2 0 Jul 9 16:31 newfile2
drwxrwxr-x. 2 student2 student2 6 Jul 9 16:31 mynewdir
-rw-rw-r--. 1 student3 student3 0 Jul 9 16:33 newfile

[student3@hostname share]$ echo "content" >> newfile2
bash: newfile2: Permission denied

[student3@hostname share]$ touch mynewdir/file
touch: cannot touch 'mynewdir/file': Permission denied
```

以下のうち、この問題に対する最適な解決策はどれですか？
A. 共有フォルダ内のユーザーにsetuidビットを追加する
B. 新しく作成されたファイルのグループを手動で変更する
C. ディレクトリの内容をすべて、誰でも書き込みおよび読み取りできるように変更します。
D. 共有フォルダ内のグループにsetgidビットを追加する
正解: (正解を表示します)
このシナリオは、共有ディレクトリでのコラボレーションに関するもので、CompTIA Linux+ V8の学習目標に含まれる一般的なシステム管理タスクです。重要な点は、ユーザーは共有ディレクトリにファイルを作成できますが、同じグループの他のユーザーはそれらのファイルを変更できないことです。この動作は、グループ所有権の継承に直接関係しています。
デフォルトでは、ユーザーがファイルまたはディレクトリを作成すると、その所有者はユーザー自身となり、親ディレクトリのグループではなく、ユーザーのプライマリグループが割り当てられます。出力に示されているように、/share 内のファイルは異なるグループ (student、student2、student3) によって所有されているため、親ディレクトリがグループ書き込み可能であっても、他のグループメンバーがファイルを変更することはできません。
正しい解決策は、共有ディレクトリにsetgid（グループID設定）ビットを設定することであり、したがってオプションDが正解となります。
setgidビットがディレクトリに適用されている場合、新しく作成されたすべてのファイルとサブディレクトリは、作成者のプライマリグループではなく、親ディレクトリのグループ所有権を継承します。これにより、グループ所有権の一貫性が確保され、共有グループのすべてのメンバーが効果的に共同作業を行うことができます。

他の選択肢は不適切、あるいは好ましくない方法です。選択肢A（setuid）は実行ファイル向けであり、ディレクトリ向けではありません。
オプションBは継続的な手動介入が必要であり、拡張性に欠ける。オプションCはすべてのユーザーに書き込みアクセス権を与えるため、最小権限の原則に違反し、セキュリティを弱める。
Linux+ V8のドキュメントでは、共有ディレクトリでsetgidビットを使用して、共同アクセスを安全かつ効率的に管理することを明示的に推奨しています。

質問: **35**
LinuxユーザーがWindows Active Directoryドメインに対して認証を行う必要があります。ドメイン構成の詳細が含まれている構成ファイルは、次のうちどれですか？
A. sssd.conf
B. auditd.conf
C. pam.conf
D. smb.conf
正解: **(正解を表示します)**
sssd.conf ファイルには、システムセキュリティサービスデーモンの設定が含まれており、これには Windows Active Directory ドメインに対して Linux ユーザーを認証するために使用される Active Directory ドメインの詳細が含まれています。

質問: **36**
シミュレーション3
あなたはシステム管理者であり、アプリケーションディレクトリの非圧縮バックアップを作成しました。数時間後、バックアップからアプリケーションを復元する必要があります。
説明書
各タブ内で、オブジェクトをクリックすると、アプリケーションのバックアップと復元に使用する適切なコマンドが生成されます。
コマンドオブジェクトは一度しか使用できませんが、スペースバーオブジェクトは複数回使用できます。
すべてのオブジェクトが使用されるわけではありません。矢印をクリックして、コマンドから不要なオブジェクトを削除してください。
シミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。

Backup | Restore

-cvf	-xvf	/opt/
d	-xzvf	/
application	-tvf	/home/
-cJvf	-c	-xjvf
/backups/application.tar.gz	/backups/application.tar	/backups/application.tgz
-j	/backups/application.tar.bz2	-C

tar [redacted] Backup


Restore
Backup
-cvf
-xvf
/opt/
-d
-xzvf
/
application
-tvf
/home/
-cJvf
-xjvf
/backups/application.tar.gz
/backups/application.tar
/backups/application.tgz
/backups/application.tar.bz2
-C
tar
Restore

正解:

Backup | Restore

-cvf	-xvf	/opt/
-d	-xzvf	/
application	-tvf	/home/
-cJvf	-c	-xjvf
/backups/application.tar.gz	/backups/application.tar	/backups/application.tgz
␣	/backups/application.tar.bz2	-C

tar tar -cvf /backups/application.tar -C /opt/ application Backup

-cvf は、/backups/application.tar という名前の詳細な (-v) アーカイブ ファイル (-f) を作成します (-c)。
-C /opt/ はアプリケーションを /opt/ に変更するため、相対的なアプリケーションディレクトリのみが保存され、絶対パスは回避されます。
-xvf は同じアーカイブを展開し (-x)、-C /opt/ は内容を元の場所に復元します。

質問: **37**

Linux管理者は、以下のコマンドを実行してグループメンバーシップを更新しています。

```
$ whoami
admin

$ sudo usermod -aG wheel admin

$ sudo groups
root
```


しかし、グループのメンバー構成は変わっていません。この問題を説明するのに最も適切なのは次のうちどれですか？

A. sudo を使用して usermod を実行することは許可されていません。

B. usermodcommand を使用して、ユーザーをホイールグループに追加することはできません。

C. コマンドグループはsudo権限で実行されました。

D. オプションの wheel と admin が入れ替わっています。

正解: **C** (コメントを発表する)

sudo を付けて groups コマンドを実行すると、root ユーザーのグループが表示され、admin ユーザーのグループは表示されません。そのため、出力には root しか表示されません。sudo を使用しない場合は、groups admin コマンド または再ログイン）を実行すると、wheel を含む更新されたグループメンバーシップが正しく表示されます。

質問: **38**

PAMを使用して辞書攻撃を検出およびブロックするために実装できるものは、次のうちどれですか？

A. pam_tally2

B. pam_limits

C. pam_unix

D. pam_idap

正解: **A** (コメントを発表する)

このPAMモジュールは認証失敗の試行を追跡し、定義されたしきい値を超えた後にアカウントを自動的にロックすることで、辞書攻撃やブルートフォース攻撃を効果的に検知して阻止します。

質問: **39**

Linux管理者は、システム上でホストされているアプリケーションが割り当てられた時間内にタスクを完了していないという報告を受け取ります。管理者はシステムに接続し、以下の詳細情報を取得します。

```
# uptime
12:47:43 up 22:17, 2 users, load average: 7.75, 5.72, 5.17

# nproc
4

# vmstat -w 1 3
[...]
r b swpd free    buffcachesisobibo in   cs   us syidwa stgu
8 0671563760348103671476 0  0  0  040901386100 0 0  0 0  0
8 0671563760348103671476 0  0  0  040761389100 0 0  0 0  0
8 0671563760348103671476 0  0  0  040761389100 0 0  0 0  0

# free -h
       total  used  free shared buff/cache available
Mem:   3.8Gi 334Mi 3.6Gi   20Mi       70Mi     3.5Gi
Swap:  7.8Gi  65Mi 7.8Gi
```

管理者は、ジョブの処理速度を向上させるために、次のうちどの行動をとることができますか？

A. システムが使用できる空きメモリの量を増やします。

B. システムに利用可能なCPUリソースの量を増やします。

C. システムに使用可能なスワップ領域の量を増やします。

D. システムが使用できるディスクの容量を増やします。

正解: **(**正解を表示します**)**

アップタイムの出力を見ると、プロセッサが4つしかないシステム（nproc = 4）で、ロードアベレージが7.75、5.72、5.17となっています。ロードアベレージが利用可能なCPU数よりも大幅に高いため、CPUが飽和状態にあることを示しています。メモリとスワップの使用量は最小限で、vmstatにはI/O待機が表示されていないため、ボトルネックはCPUです。CPUリソースを増やすことで、ジョブの処理速度を向上させることができます。

質問: **40**

Linux管理者は、app-01-imageコンテナを作成し、それに接続する必要があります。以下のコマンドのうち、このタスクを実行するのはどれですか？

A. docker run -it app-01-image

B. docker start -td app-01-image

C. docker build -ic app-01-image

D. docker exec -dc app-01-image

正解: **A (**コメントを発表する**)**

Linux+ V8ドキュメントからの包括的かつ詳細な説明（250〜350語）：

コンテナのライフサイクル管理は、CompTIA Linux+ V8 の自動化、オーケストレーション、スクリプト作成の分野における重要なトピックです。管理者は、コンテナの作成、コンテナの起動、実行中のコンテナ内でのコマンド実行の違いを理解しておく必要があります。
正しいコマンドは `docker run -it app-01-image` です。`docker run` コマンドは、指定されたイメージから新しいコンテナを作成し、コンテナを起動し、オプションで管理者の端末をコンテナに接続するという 3 つのアクションを同時に実行します。`-i` オプションは標準入力を開いたままにし、`-t` オプションは擬似端末 (TTY) を割り当てます。これらのオプションを組み合わせることで、管理者はコンテナ作成直後に対話的に接続できるようになります。
他のオプションは、以下の理由により不適切です。`docker start` は、停止中の既存のコンテナを起動するためにのみ使用され、イメージから新しいコンテナを作成するものではありません。また、`-t` と `-d` は、コンテナの起動中に対話型ターミナルを接続するための有効なオプションではありません。`docker build` は、Dockerfile から Docker イメージをビルドするために使用され、コンテナの作成や接続には使用できません。`docker exec` は、既に実行中のコンテナ内でコマンドを実行するために使用されるため、コンテナの作成には使用できません。
Linux+ V8のドキュメントでは、docker runコマンドは、管理者がイメージからコンテナをインスタンス化して操作する際に使用する主要なコマンドであると強調されています。このコマンドは、テスト、開発、トラブルシューティングのワークフローでよく使用されます。

質問: **41**
Linux管理者は、サーバーに新しいHTTPサービスを追加する必要があります。システム再起動後、他のシステムがそのサービスと通信できるようにするコマンドはどれですか？
A. firewall-cmd --add-service=http --reload
B. firewall-cmd --add-port=http --complete-reload
C. firewall-cmd --add-service=http --permanent
D. firewall-cmd --add-service=http
正解: **(**正解を表示します**)**
このコマンドは、HTTPサービスをファイアウォールの永続的な設定に追加し、システム再起動後もルールが維持されるようにするとともに、再起動後も他のシステムがサービスと通信できるようにします。

質問: **42**
システムのセキュリティ強化中に、管理者がNmapを使用してポートスキャンを実行したところ、以下の出力が得られました。

```
# nmap 104.21.75.76
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-09 18:09 UTC
Nmap scan report for 104.21.75.76
Host is up (0.00087s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
443/tcp open https
8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.93 seconds
```


このセキュリティ問題に対処する最善の方法は、次のうちどれですか？
A. サーバーのポート23のトラフィックをブロックするようにファイアウォールを設定する
B. システム管理者のパスワードを変更して不正アクセスを防止する
C. ネットワークスイッチのポート80を閉じてトラフィックをブロックします
D. サーバー上のTelnetサービスを無効化および削除する

正解: **D** (コメントを発表する)
ポート23/tcpはTelnetを示しますが、これはデータを平文で送信するため安全ではありません。最も効果的な対策は、ファイアウォールでブロックするだけでなく、Telnetサービスを完全に無効化して削除し、脆弱性を排除することです。代わりに、SSHなどの安全な代替手段を使用する必要があります。

質問: **43**
あなたはシステム管理者であり、アプリケーションディレクトリの非圧縮バックアップを作成しました。数時間後、バックアップからアプリケーションを復元する必要があります。
説明書
各タブ内で、オブジェクトをクリックすると、アプリケーションのバックアップと復元に使用する適切なコマンドが生成されます。
コマンドオブジェクトは一度しか使用できず、すべてが使用されるとは限りません。矢印をクリックすると、コマンドから不要なオブジェクトを削除できます。
シミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。

正解:

解決策については、下記の解説をご覧ください。

Explanation:

Suggested Answer:

この実技問題は、CompTIA Linux+ V8 のシステム管理に含まれる、バックアップおよび復元操作における tar ユーティリティの正しい使用方法をテストするものです。重要な点は、バックアップが非圧縮であると明示的に指定されているため、正しいアーカイブファイルは .tar.gz、.tgz、または .tar.bz2 ではなく、通常の .tar ファイルでなければならないということです。

バックアップコマンドの正しい構文は次のとおりです。

tar -cvf /backups/application.tar -C /opt/ application

ここで、-c はアーカイブを作成し、-v は詳細な出力を有効にし、-f はアーカイブファイル名を指定します。-C /opt/ オプションは、アーカイブ前に /opt/ ディレクトリに移動し、アプリケーションはその場所を基準としてアーカイブされます。これは、不要な先頭パス要素をアーカイブに保存しないため、Linux+ の正しい方法です。

復元コマンドの正しい構文は次のとおりです。

tar -xvf /backups/application.tar -C /opt/

ここで、-x はアーカイブを展開し、-v は復元されるファイルを表示し、-f はアーカイブファイルを識別します。-C /opt/ オプションは、アーカイブされたアプリケーションディレクトリが /opt/ に復元され、/opt/application が正しく再作成されるようにします。

その他のファイルオプションとしては、/backups/application.tar.gz、/backups/application.tgz、および/backups/applicationなどがあります。

tar.bz2 は圧縮バックアップを示すため不適切です。質問では圧縮バックアップは明確に除外されています。

同様に、-xzvf や -xjvf などのオプションは gzip または bzip2 で圧縮されたアーカイブに使用されるものであり、ここでは適用されません。

したがって、検証済みの正しいPBQ解答は以下のとおりです。

バックアップ: tar -cvf /backups/application.tar -C /opt/ application

復元: tar -xvf /backups/application.tar -C /opt/

質問: **44**
管理者がKVMディスクファイルを別の形式に変換するには、以下のどのコマンドを使用すべきですか？
A. qemu-kvm
B. qemu-nq
C. qemu-io
D. qemu-img
正解: **(正解を表示します)**
正解はDです。qemu-imgは、KVM（カーネルベース仮想マシン）などの仮想化プラットフォームで使用されるディスクイメージファイルの作成、変換、管理に使用される標準ユーティリティです。主な機能の1つは、qcow2、raw、vmdk、vdiなどの異なる形式間でディスクイメージを変換することです。
例えば、管理者は次のようなコマンドを使用してディスクイメージを変換できます。
qemu-img convert -f qcow2 -O raw disk.qcow2 disk.raw
この機能は、異なるハイパーバイザー間で仮想マシンを移行する場合や、ストレージ形式を最適化する場合に不可欠です。
オプションA（qemu-kvm）は、ディスクイメージの管理や変換ではなく、KVMアクセラレーションを使用して仮想マシンを実行するために使用されるため、誤りです。
オプションB（qemu-nq）は、有効なQEMUコマンドでも一般的なコマンドでもないため、誤りです。
オプションC（qemu-io）は、主にディスクI/O操作のデバッグとテストに使用されるものであり、フォーマット変換に使用されるものではないため、誤りです。
Linux+システム管理の観点から見ると、仮想化は重要なトピックであり、qemu-imgのようなツールは仮想ディスクストレージの管理に不可欠です。管理者は、クラウド、コンテナ化、または仮想化環境で作業する際に、イメージのサイズ変更、整合性のチェック、フォーマット変換などにqemu-imgを頻繁に使用します。このコマンドを理解することで、仮想マシンのストレージを効率的に処理し、仮想化プラットフォーム間の相互運用性を確保できます。

質問: **45**
ユーザーであるジョーが、以前アンが担当していたポジションに就任しました。システム管理者として、アンのホームディレクトリにあるすべてのファイルをアーカイブし、ジョーのホームディレクトリに展開する必要があります。
説明書
各タブ内で、オブジェクトをクリックして適切なコマンドを作成します。コマンドオブジェクトは一度しか使用できませんが、スペースバーとアンダースコア（_）のオブジェクトは複数回使用できます。すべてのオブジェクトが使用されるわけではありません。
シミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。

Archive | Extract

-d | /tmp/ann.tar | -cJvf

joe | /home/ | /tmp/ann.tar.gz

-xzvf | /tmp/ann.tgz | /tmp/ann.tar.bz

-cvf | -C | -c

-xjvf | ann | -xvf

␣

tar /home/-C Archive

正解:

解決策については、下記の解説をご覧ください。

Explanation:

アーカイブタブ - アンのホームディレクトリからアーカイブを作成します

正しいコマンド:

tar -cvf /tmp/ann.tar -C /home/ann

抽出タブ - アーカイブをジョーのホームディレクトリに展開します

正しいコマンド:
tar -xvf /tmp/ann.tar -C /home/ joe
この実技問題は、CompTIA Linux+ V8の目標に含まれるシステム管理の中核スキルである、tarを使用したファイルアーカイブと復元をテストするものです。課題は、Annのファイルを保存し、Joeのホームディレクトリに正しく配置することです。
アーカイブフェーズの説明
最初のステップの目標は、フルパス（/home）を埋め込まずに、Annのホームディレクトリ全体をアーカイブすることです。
/ann) をアーカイブ内に挿入します。これは -C オプションを使用して行います。
コマンドの詳細：
tar # アーカイブユーティリティ
-c # アーカイブを作成する
-v # 詳細出力（オプションですが使用可能）
-f /tmp/ann.tar # アーカイブファイルを指定します
-C /home/ # アーカイブ前にディレクトリを変更します
ann # ann ディレクトリのみをアーカイブします
これにより、絶対パスを含まないAnnのファイルを含むクリーンなアーカイブが作成されます。これはベストプラクティスであり、Linux+ V8のドキュメントにも明記されています。
抽出フェーズの説明
2番目の手順では、アーカイブされたファイルをジョーのホームディレクトリに展開します。
コマンドの詳細：
-x # 抽出
-v # 詳細表示
-f /tmp/ann.tar # アーカイブを指定します
-C /home/joe # ファイルをジョーのホームディレクトリに直接展開します
これにより、抽出後の処理に応じて、Joe は Ann のファイルを /home/joe/ann または /home/joe 直下に正しく受け取ることができ、これは Linux+ の管理ユーザー移行に関する期待と一致します。

質問: **46**
Linux管理者が、新しいボリュームをマウントするためにローカルファイルシステム /data をアンマウントしようとします。しかし、管理者は次のエラーメッセージを受け取ります。
umount: /data: ターゲットがビジー状態です
管理者はこの問題を解決するために、以下のどのコマンドを実行すべきですか？
A. tree -g /data
B. ls -ld /data
C. stat -f /data
D. fuser -mk /data
正解: **(正解を表示します)**
fuserコマンドは、/dataファイルシステムをアクティブに使用しているプロセスを識別して終了させ、それらのプロセスが停止した後に安全にアンマウントできるようにします。

質問: **47**
システム管理者は、NetworkManager サービスの起動にかかった時間を確認したいと考えています。以下のコマンドのうち、この目的を達成できるのはどれですか？
A. resolvectl
B. journalctl
C. systemctl daemon-reload
D. systemd-analyze blame
正解: **(**正解を表示します**)**
システム起動パフォーマンス分析は、Linux+ V8に含まれる重要なシステム管理タスクです。管理者が起動時にサービスが起動するまでにかかる時間を把握する必要がある場合、systemd分析ツールが必要となります。
正しいコマンドは systemd-analyze blame です。このコマンドは、すべての systemd サービスを一覧表示し、起動プロセス中に各サービスが初期化にかかった時間を表示します。NetworkManager など、システム起動パフォーマンスに影響を与える可能性のある起動の遅いサービスを特定するためによく使用されます。
他の選択肢は誤りです。resolvectlはDNS解決管理に使用され、サービスタイミング情報は提供しません。journalctlはログを表示できますが、明確で要約されたサービス起動タイミングレポートは提供しません。systemctl daemon-reloadはsystemdユニットファイルを再読み込みするだけで、分析は行いません。
Linux+ V8のドキュメントでは、サービス起動の遅延を診断するための適切なツールとしてsystemd-analyze blameが明示的に記載されています。したがって、正解はDです。

質問: **48**
ユーザーはコンテナ内で実行されているアプリケーションにアクセスできません。管理者はコンテナが実行されているかどうかを確認したいと考えています。管理者はどのコマンドを使用すべきでしょうか？
A. docker start
B. docker ps
C. docker run
D. Dockerイメージ
正解: **B (**コメントを発表する**)**
コンテナのトラブルシューティングは、CompTIA Linux+ V8 の自動化、オーケストレーション、スクリプト作成の分野における重要な能力です。ユーザーからコンテナ内で実行されているアプリケーションにアクセスできないという報告があった場合、最初に行う検証手順の 1 つは、コンテナが現在実行中かどうかを確認することです。
docker ps コマンドは、システム上で実行中のコンテナを一覧表示するために特別に設計されています。デフォルトでは、コンテナ ID、イメージ名、実行されたコマンド、稼働時間、ポートマッピング、およびコンテナ名が表示されます。これにより、管理者はアプリケーションコンテナがアクティブかどうか、また期待されるポートを公開しているかどうかを迅速に判断できます。これは、コンテナのライフサイクル管理と運用検証に関する Linux+ V8 のガイダンスに直接準拠しています。
他のオプションはこの目的には適していません。docker start は停止中のコンテナを 1 つ以上起動するために使用されますが、コンテナの状態は表示されません。docker run は新しいコンテナを作成して起動しますが、既存のコンテナの状態を確認することだけが目的の場合は適切ではありません。docker images はローカルで使用可能なコンテナイメージを一覧表示しますが、実行中または停止中のコンテナに関する情報は提供しません。
Linux+ V8 のドキュメントでは、コンテナ化されたアプリケーションの診断時に適切な Docker サブコマンドを使用することの重要性が強調されています。docker ps コマンドを使用してコンテナの実行時状態を確認することは、ネットワーク、ファイアウォールルール、またはアプリケーションレベルのエラーを調査する前に行うべき基本的なトラブルシューティング手順です。
したがって、コンテナが実行されているかどうかを確認するための正しいコマンドは docker ps であり、回答 B が正解です。

質問: **49**

システム管理者は、新しいストレージアレイを会社の既存のストレージプールに統合する必要があります。管理者は、サーバーが新しいストレージアレイを検出できることを確認したいと考えています。新しいストレージアレイがシステムに認識されるようにするには、管理者はどのコマンドを使用すべきでしょうか？
A. lsscsi
B. lsusb
C. lsipc
D. lshw
正解: **(**正解を表示します**)**
正確な抜粋に基づく包括的かつ詳細な説明：
lsscsi コマンドは、システムに接続されている SCSI デバイス (ストレージ アレイを含む) に関する情報を一覧表示するために使用されます。これは、新しいストレージ アレイを統合する際に非常に重要です。なぜなら、管理者は、オペレーティングシステムが SCSI レイヤー (ほとんどのエンタープライズ ストレージ ソリューションの基盤となるインターフェイス) で新しいデバイスを検出していることを確認できるからです。lsscsi コマンドは、認識された SCSI デバイス、そのデバイス ノード、および関連情報の一覧を出力します。
その他の選択肢：
* B. lsusb: USB デバイスを一覧表示しますが、SCSI/SATA/SAS 上のストレージ アレイは一覧表示しません。
* C. lsipc: ハードウェア検出とは関係なく、IPC (プロセス間通信) 機能に関する情報を表示します。
* D. lshw: ハードウェアの詳細を表示し、ストレージを表示することもできますが、lsscsi は SCSI デバイスの検出専用に設計されており、このタスクを実行する最も直接的な方法です。
参照：
CompTIA Linux+ 学習ガイド: 試験 XK0-006、Sybex、第 7 章: 「ストレージの管理」、セクション:
「ストレージデバイスの識別とアクセス」
CompTIA Linux+ XK0-006 目標: ドメイン 4.0 - ストレージとファイルシステム

質問: **50**
管理者は、ユーザーがrunreportsユーティリティを実行できないという報告を受け取ります。管理者はそのユーザーとしてログインし、以下のコマンドを実行すると、次の出力が得られます。
$ runreports
runreports: コマンドが見つかりません
$ ls -l /usr/local/bin
-rwxr-xr-x 1 root root 29 5月 10 11:31 runreports
$ echo $PATH
/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
以下のうち、この問題とその解決策を最もよく表しているのはどれですか？
A. runreportsユーティリティがユーザーのパスに含まれていません。管理者は.bash_profileファイルを変更する必要があります。
B. runreportsユーティリティはシェルスクリプトですが、ユーザーが所有していません。管理者はchownコマンドを使用する必要があります。
C. ユーザーに適切なSELinuxコンテキストがありません。管理者はSELinuxテンプレートを変更する必要があります。
D. runreportsユーティリティには実行権限がありません。管理者が実行権限を追加する必要があります。
正解: **A (**コメントを発表する**)**
Linuxでは、コマンドをその名前だけで（絶対パスや相対パスを指定せずに）実行するには、実行可能ファイルを含むディレクトリがユーザーのPATH環境変数に登録されている必要があります。CompTIA Linux+ V8の目標によると、「コマンドが見つかりません」エラーのトラブルシューティングには、バイナリの場所と現在のPATH構成との照合が必要です。
このシナリオでは、ユーティリティ runreports は /usr/local/bin にあります。しかし、echo $PATH の出力では、/usr/local/bin が検索ディレクトリに存在しないことがわかります。現在の PATH には、/usr/sbin、/usr/bin、/sbin、

/bin など、他のパスも対象となりますが、ユーティリティの場所は明示的に除外されます。シェルは定義済みの検索パスのいずれにもファイルを見つけることができないため、「コマンドが見つかりません」というエラーを返します。この問題をユーザーに対して恒久的に解決するには、管理者は ~/.bash_profile や ~/.bashrc などのシェル初期化ファイルを変更して、/usr/local/bin をユーザーの PATH に追加する必要があります。export PATH=$PATH:/usr/local/bin という行を追加すると、以降のセッションでディレクトリが確実に含まれるようになります。
提供された証拠に基づくと、他の選択肢は誤りです。選択肢Bは、ls -lの出力でファイルに「others」に対するrx権限が付与されていることが示されているため誤りです。つまり、所有者ではないにもかかわらず、ユーザーは既にファイルを実行できるということです。選択肢Cは、SELinuxでは通常「Permission Denied」となり、「Command Not Found」とはならないため、可能性は低いです。選択肢Dも、ls -lの出力で実行（x）ビットが全てのユーザーに対して既に設定されている（755）ことが明確に示されているため誤りです。
したがって、PATHエントリの欠落が根本原因であることが確認されました。

質問: **51**
システム管理者が /home/ ディレクトリのバックアップコピーを作成しています。以下のコマンドのうち、ディレクトリのアーカイブと圧縮を同時に実行できるのはどれですか？
A. cpio -o /backups/home.tar.xz /home/
B. rsync -z /backups/home.tar.xz /home/
C. tar -cJf /backups/home.tar.xz /home/
D. dd of=/backups/home.tar.xz if=/home/
正解: **C** (コメントを発表する)
tar -cJf コマンドは、アーカイブを作成し (-c)、XZ で圧縮し (-J)、ファイルに書き込みます (-f)。これにより、/home/ ディレクトリのアーカイブと圧縮を一度に行うことができます。

質問: **52**
監視呼び出しを受けた後、管理者はLinuxサーバー上で、実行が完了したがプロセス一覧からまだ削除されていないプロセスを確認します。
管理者が検索すべきプロセス状態を表しているのは、次のうちどれですか？
A. A
B. S
CD
C. T
正解: (正解を表示します)
このプロセス状態は、実行は完了しているものの、親プロセスが終了ステータスをまだ読み取っていないため、プロセス一覧に残っているゾンビプロセスを表します。

質問: **53**
DevOpsエンジニアがローカルのGitリポジトリを作成する必要があります。エンジニアは、以下のどのコマンドを使用すべきでしょうか？
A. git init
B. git clone
C. git config
D. git add
正解: **A** (コメントを発表する)
正解はAのgit initです。git initは、ディレクトリ内に新しいローカルGitリポジトリを初期化するために使用されるコマンドです。git initを実行すると、バージョン管理に必要なすべてのメタデータと設定ファイルを含む隠しディレクトリ.gitが作成されます。この操作により、現在のディレクトリがGitリポジトリとなり、ユーザーは変更の追跡を開始できます。
DevOpsと自動化のコンテキストにおいて、リポジトリの初期化は基礎となるタスクです。これにより、スクリプト、設定ファイル、インフラストラクチャ・アズ・コードのバージョン管理が可能になり、これらは現代のLinux環境において重要なコンポーネントとなります。リポジトリが初期化されると、エンジニアはファイルの追加（git add）と変更のコミット（git commit）に進むことができます。

オプションB（git clone）は、既存のリモートリポジトリをローカルシステムにコピーするために使用されるため、誤りです。これは、新しいリポジトリをゼロから作成するのではなく、既に初期化されているリポジトリを複製するものです。
オプションC（git config）は、ユーザー名、メールアドレス、設定などのGit設定を構成するために使用されるものであり、リポジトリを初期化するものではないため、誤りです。
オプションD（git add）は、既に初期化済みのリポジトリ内でコミットのための変更をステージングするため、誤りです。リポジトリが作成される前には使用できません。
Linux+の観点から見ると、自動化とオーケストレーションのトピックにおいて、Gitの操作を理解することは不可欠です。Gitのようなツールは、コラボレーション、変更追跡、およびデプロイメントワークフローをサポートします。git initコマンドは、コードと構成を制御されたバージョン管理方式で管理するための出発点であり、システム管理者やDevOpsエンジニアにとって重要なスキルです。

質問: **54**
ユーザーからの報告によると、システム上でホストされているアプリケーションが約1週間後に応答しなくなり、復旧にはシステムの再起動が必要になるとのことです。システム管理者がシステムに接続し、以下の出力を取得しました。

```
        total    used    free  shared buff/cache   available
Mem:     15Gi    15Gi   286Ki     5.0Mi       309Mi       263Mi
Swap:   8.0Gi   8.0Gi    80Ki

$ dmesg
[...]
28845.746885] OOM: Killed process 10601 (application) total-vm:23228292kB, anon-rss:15181952kB, file-rss:1408kB, shmem-rss:0kB, UID:1000
pgtables:45076kB oom_score_adj:0
```

アプリケーションが応答しなくなる理由として、次のうちどれが適切ですか？
A. アプリケーションの設定が間違っているため、メモリとスワップ領域が不足しています。
B. アプリケーションに誤ったディスククォータが設定されているため、ファイルシステムがいっぱいになっています。
C. アプリケーションにメモリリークがあり、システム上の利用可能なメモリをすべて消費します。
D. アプリケーションはメモリを割り当てることが許可されていないため、システムが遅くなります。
正解: **C** (コメントを発表する)
出力結果から、メモリとスワップ領域が完全に消費され、カーネルが常駐メモリの過剰な使用によりアプリケーションに対してOOMキラーを呼び出したことが分かります。これは、メモリリークによって利用可能なRAMとスワップ領域が徐々に枯渇し、最終的にアプリケーションが応答しなくなるという状況と一致しています。

質問: **55**
新しく採用されたLinux管理者は、4096バイトのパスワードで保護されたRSAキーを生成することで、Linuxサーバーへのアクセス権を付与する必要があります。以下のコマンドのうち、このタスクを実行できるのはどれですか？
A. ssh-keygen -RPb 4096
B. ssh-keygen -t rsa -b 4096
C. ssh-keygen -k rsa -l 4096 -p
D. ssh-keygen -t dsa -B 4096
正解: **B** (コメントを発表する)
ssh-keygenコマンドはSSHキーペアを生成するために使用されます。長さ4096ビットのRSAキーを生成するための正しい構文は次のとおりです。
1.-t rsa: 生成する鍵のタイプを指定します。ここでは RSA を指定します。
2.-b 4096: キーのビット数を指定します。この場合は4096です。
このコマンドを実行すると、ユーザーはキーをパスワードで保護するためのパスフレーズを入力するように求められます。これにより、4096ビットのパスワード保護されたRSAキーを生成するという要件が満たされます。

質問: **56**

システム管理者がサードパーティのAPIエンドポイントで問題が発生しています。管理者には以下の出力が表示されます。

```
# curl https://comptia.com/endpoint
curl: (6) Could not resolve host: comptia.com


# dig comptia.com
; <<>> <<>> comptia.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 14031
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;comptia.com. IN A
;; AUTHORITY SECTION:
com. 900 IN SOA a.gtld-servers.net. nstld.verisign-grs.com. 1720473015 1800 900 604800 86400
;; Query time: 159 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Mon Jul 08 15:10:45 CST 2024
;; MSG SIZE rcvd: 117
```

管理者はこの問題を解決するために、次のうちどの行動を取るべきでしょうか？

A. サーバーのファイアウォールでセキュアポートを開放します。

B. 第三者から新しいAPIエンドポイントを要求する。

C. DNSクライアント設定ファイルをレビューして修正します。

D. ホスト上でインターネット接続を有効にします。

正解: **(正解を表示します)**

このシナリオは名前解決の失敗を表しており、CompTIA Linux+ V8で取り上げられている一般的なトラブルシューティング事例です。重要な手がかりは、curlとdigの両方から返されるエラーメッセージです。curlのエラー「Could not resolve host」は、システムがホスト名をIPアドレスに変換できないことを示しています。これは、digコマンドの出力結果（NXDOMAIN）によって確認でき、DNSリゾルバが要求されたドメイン名を解決できないことを意味します。重要なのは、digコマンドの出力結果から、クエリがDNSサーバー（10.255.255.254）に到達しているにもかかわらず、名前解決に失敗していることです。これは、DNSクライアントの設定に問題があることを強く示唆しています。

オプションC、つまりDNSクライアント設定ファイル（/etc/resolv.confやsystemd-resolvedの設定など）を確認して修正することが正しい対処法です。Linux+ V8のドキュメントでは、DNSの設定ミスがアプリケーション接続問題の主な原因であると指摘されています。ネームサーバーのエントリが間違っていたり、DNSサーバーに到達できなかったり、リゾルバの設定が間違っていたりすると、NXDOMAIN応答が発生することがよくあります。

他の選択肢は誤りです。ファイアウォールの問題は接続タイムアウトの原因となり、DNS解決の失敗にはつながりません。ローカルDNSの機能を確認せずに新しいAPIエンドポイントを要求するのは不要です。インターネット接続の問題は通常、DNS通信を妨げるはずだが、ここでは明らかにDNSサーバーに接続できている。

Linux+ V8では、階層的なトラブルシューティング手法が重視されています。ネットワークポートやアプリケーションロジックを調査する前に、DNS解決を検証する必要があります。したがって、正解はCです。DNSクライアントの設定ファイルを確認して修正してください。

質問: **57**

ユーザーから、NFS共有でランダムな切断が発生しているとの報告がありました。システム管理者は以下の情報を入手しました。

```
#df -h
Filesystem              Size  Used Avail Use% Mounted on
/dev/mapper/fedora-
root                    15G   15G  204K  100% /
devtmpfs                4.0M  0    4.0M  0%   /dev
tmpfs                   2.0G  0    2.0G  0%   /dev/shm
tmpfs                   783M  816K 782M  1%   /run
tmpfs                   2.0G  0    2.0G  0%   /tmp
/dev/vda2               960M  481M 480M  51%  /boot
10.0.0.1:/nfsdata       4T    3.8T 200G  95%  /share

$ ip -s link show
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
link/ether 52:5a:00:f7:27:23 brd ff:ff:ff:ff:ff:ff
RX:  bytes      packets   errors   dropped   missed   mcast
     108487310  149198    9584     40721     0        0
TX:  bytes      packets   errors   dropped   carrier  collsns
     3015941    33656     12780    7854      0        0
```

報告されている症状を最もよく説明しているのは、次のうちどれですか？

A. NFS共有のマウントポイントが間違っています。
B. NFS共有のIPアドレスが間違っています。
C. ファイルシステムがほぼ満杯で、エラーを報告しています。
D. インターフェースで多数のエラーとパケット損失が発生しています。

正解: **D** (コメントを発表する)

この問題は、CompTIA Linux+ V8 のトラブルシューティング領域で推奨されているように、階層的なトラブルシューティング手法を用いて分析するのが最適です。報告されている症状は、NFS 共有からの断続的またはランダムな切断であり、これは通常、構成やファイルシステムの問題ではなく、ネットワークの信頼性の問題を示しています。

最も重要な証拠は、ip -s link show コマンドの出力から得られます。ネットワークインターフェイス enp1s0 では、受信 (RX) パスと送信 (TX) パスの両方で、多数のエラーとパケット損失が発生していることが報告されています。ネットワークインターフェイスレベルでのパケット損失率が高いと、安定した継続的な TCP/IP 通信に依存する NFS などのプロトコルに直接影響します。パケットがドロップまたは破損すると、NFS クライアントはタイムアウト、再送信、および切断状態が発生する可能性があります。

df -h の出力では NFS ファイルシステムが 95% 使用されていると表示されますが、これだけでランダムな切断が発生することは通常ありません。ファイルシステムがほぼ満杯になると書き込みエラーやパフォーマンス低下につながる可能性はありますが、断続的な接続喪失の原因にはなりません。Linux+ V8 のドキュメントには、ファイルシステムの容量の問題は通常、トランスポート層の切断ではなく、I/O エラーとして現れると記載されています。

オプションAとBも除外できます。マウントポイントまたはIPアドレスが間違っていれば、NFS共有は断続的にではなく、常に失敗するはずです。共有がマウントされ、アクセス可能であるという事実は、マウント構成とIPアドレスが正しいことを裏付けています。

Linux+ V8では、NFSのパフォーマンスと信頼性はネットワーク品質に大きく左右されることが強調されています。パケットエラー、パケット損失、NICの故障、ケーブル接続の問題、デュプレックスモードの不一致、ドライバの問題などは、NFSの動作不安定化の一般的な原因となります。

したがって、報告されているランダムな切断に対する最良の説明はDである。インターフェースは、多数のエラーとパケット損失を報告している。

質問: **58**

パスワード有効期限ポリシーを設定する主な理由は次のうちどれですか？
A. 同じパスワードを繰り返し使用しないようにするため
B. パスワード漏洩のリスクを軽減する
C. パスワードなし認証の使用を強制する
D. パスワードの強度と複雑さを高める
正解: (正解を表示します)
パスワード有効期限ポリシーは、たとえパスワードが漏洩した場合でも、その有効期間を制限することで、長期にわたる不正アクセスのリスクを軽減します。

質問: **59**
経験の浅いシステム管理者が誤ってLVMボリュームを削除してしまった。
説明書
パート1
出力結果を確認し、適切なコマンドを選択して復旧プロセスを開始してください。
パート2
出力結果を確認し、適切なコマンドを選択して復旧プロセスを続行してください。
パート3
出力結果を確認し、適切なコマンドを選択して復旧プロセスを完了し、基となるデータにアクセスしてください。

Part 1 | Part 2 | Part 3

>_ Commands

```
[root@comptiasim ~]# df -h
[root@comptiasim ~]# ls -l /dev | grep -v tty
[root@comptiasim ~]# ls -l /etc/lvm/archive
[root@comptiasim ~]# pvdisplay
[root@comptiasim ~]# pvs
[root@comptiasim ~]# vgcfgrestore --list vg01
[root@comptiasim ~]# vgdisplay
[root@comptiasim ~]# vgs
```

```
[root@comptiasim ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        1.9G     0  1.9G   0% /dev
tmpfs           1.9G     0  1.9G   0% /dev/shm
tmpfs           1.9G   17M  1.9G   1% /run
tmpfs           1.9G     0  1.9G   0% /sys/fs/cgroup
/dev/xvda1      8.0G  1.1G  7.0G  13% /
tmpfs           379M     0  379M   0% /run/user/1000
```

Select the appropriate command to begin the recovery process.

```
[root@comptiasim ~]#
```

Select command

- lvchange -a y /dev/vg01/lv01
- lvconvert --type mirror lv01
- pvscan
- vgcfgrestore vg01 -f /etc/lvm/archive/vg01_00002-966141411.vg
- vgcfgrestore vg01 -f /etc/lvm/backup/vg01
- lvchange -a n /dev/vg01/lv01
- vgcfgrestore vg01 -t -M /etc/lvm/archive/vg01_00001-810050352.vg

Select command

Part 1 | Part 2 | Part 3

>_ Commands

```
[root@comptiasim ~]# blkid
[root@comptiasim ~]# dmesg | tail -20
[root@comptiasim ~]# lsblk
[root@comptiasim ~]# ls /
[root@comptiasim ~]# lvdisplay
[root@comptiasim ~]# lvs
[root@comptiasim ~]# lvscan
[root@comptiasim ~]# pvs
[root@comptiasim ~]# vgs
```

```
[root@comptiasim ~]# blkid
/dev/xvda1: UUID="388a99ed-9486-4a46-aeb6-06eaf6c47675" TYPE="xfs"
/dev/xvdf: UUID="1uyvyk-Ffd0-RrYF-cYba-l5zC-EHRZ-UW3UHm" TYPE="LVM2_member"
```

Select the appropriate command to continue the recovery process.

```
[root@comptiasim ~]#
```

Select command

- pvchange -x y /dev/xvdf
- lvextend -L +54 vg01/lv01 /dev/xvdf
- lvchange -a y /dev/vg01/lv01
- mount /dev/vg01/lv01/ /important_data
- lvchange -a n /dev/vg01/lv01

Select command

Part 1 Part 2 **Part 3**

>_ Commands

```
[root@comptiasim ~]# blkid
[root@comptiasim ~]# cat /etc/fstab
[root@comptiasim ~]# ls -l /dev/mapper/
[root@comptiasim ~]# ls -l /
[root@comptiasim ~]# lsblk
[root@comptiasim ~]# lvdisplay
[root@comptiasim ~]# lvscan
[root@comptiasim ~]# tail -f /var/log/messages
[root@comptiasim ~]# xfs_repair -n /dev/vg01/lv01
```

```
[root@comptiasim ~]# blkid
/dev/xvda1:              UUID="388a99ed-9486-4a46-aeb6-06eaf6c47675"
TYPE="xfs"
/dev/mapper/vg01-lv01:   UUID="c63883e9-ceca-45f4-9ad9-f8d8c1814e7e"
TYPE="xfs"
/dev/xvdf:               UUID="1uyvyk-Ffd0-RrYF-cYba-l5zC-EHRZ-UW3UHm"
TYPE="LVM2_member"
```

```
Select command
xfs_repair /dev/vg01/lv01
lvscan -a
mount -a
mount /important_data /dev/vg01/lv01
xfs_mdrestore /dev/vg01 /important_data
```

[root@comptiasim ~]# Select command

Part 1 Part 2 Part 3

Commands

```
[root@comptiasim ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        1.9G     0  1.9G   0% /dev
tmpfs           1.9G     0  1.9G   0% /dev/shm
tmpfs           1.9G   17M  1.9G   1% /run
tmpfs           1.9G     0  1.9G   0% /sys/fs/cgroup
/dev/xvda1      8.0G  1.1G  7.0G  13% /
tmpfs           379M     0  379M   0% /run/user/1000
```

Select the appropriate command to begin the recovery process.

[root@comptiasim ~]# Select command

Part 1 Part 2 Part 3

Commands

```
[root@comptiasim ~]# blkid
/dev/xvda1: UUID="388a99ed-9486-4a46-aeb6-06eaf6c47675" TYPE="xfs"
/dev/xvdf: UUID="1uyvyk-Ffd0-RrYf-cYba-l5zC-EHRZ-UW3U8m" TYPE="LVM2_member"
```

Select the appropriate command to continue the recovery process.

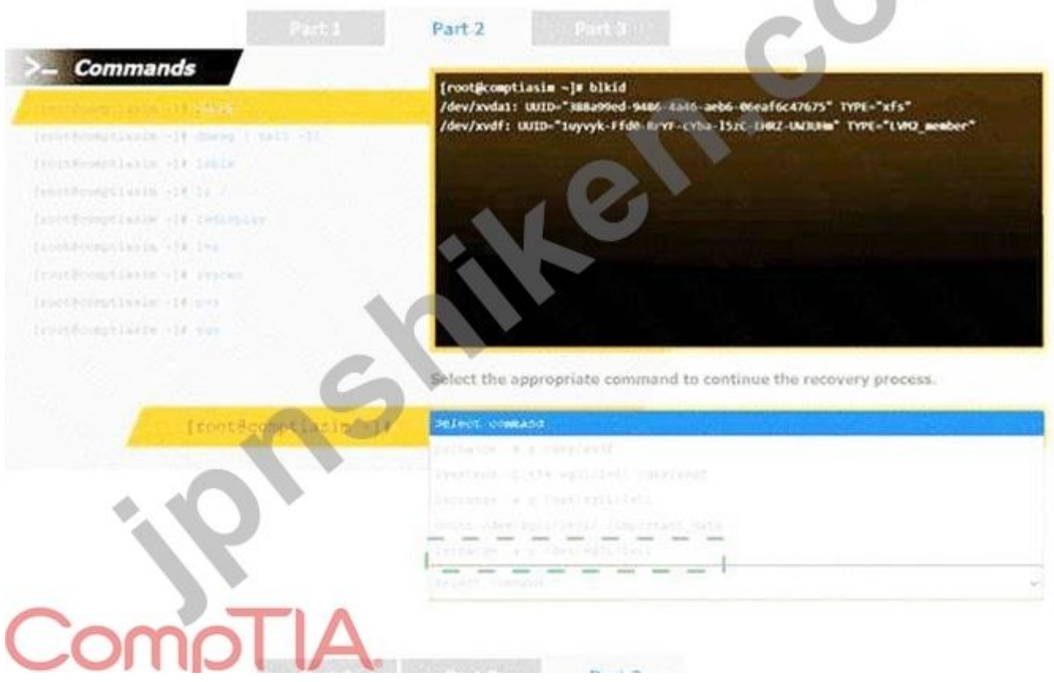
[root@comptiasim ~]# Select command

Part 1 Part 2 Part 3

Commands

```
[root@comptiasim ~]# blkid
/dev/xvda1:                UUID="388a99ed-9486-4a46-aeb6-06eaf6c47675"
TYPE="xfs"
/dev/mapper/vg01-lv01:  UUID="c63883e9-ceca-45f4-9ad9-f8d8c1814e7e"
TYPE="xfs"
/dev/xvdf:                 UUID="1uyvyk-Ffd0-RrYf-cYba-l5zC-EHRZ-UW3U8m"
TYPE="LVM2_member"
```

正解:



Explanation:
パート1 - 復旧プロセスを開始する
The answer:
vgcfgrestore vg01 -f /etc/lvm/archive/vg01_00001-810050352.vg
パート2 - 回復プロセスを継続する
The answer:
lvchange -ay /dev/vg01/lv01
パート3 - 完全な復旧とデータへのアクセス
The answer:
mount /dev/vg01/lv01 /important_data
この実技問題は、CompTIA Linux+ V8 の重要なシステム管理スキルである LVM リカバリをテストするものです。シナリオでは、論理ボリュームが削除されたものの、基となる物理ボリュームとボリュームグループのメタデータは残っている状態を想定しています。
パート 1: ボリューム グループのメタデータの復元
最初のスクリーンショットには、以下の内容が示されています。
物理ボリューム（pvdisplay、pvs）は依然として存在する
論理ボリュームが見つかりません
/etc/lvm/archive/ にはアーカイブされた VG メタデータが含まれています
Linux は、変更が行われるたびに LVM メタデータのバックアップを /etc/lvm/archive に自動的に保存します。正しい最初のステップは、以下のコマンドを使用してボリューム グループのメタデータを復元することです。
vgcfgrestore vg01 -f /etc/lvm/archive/vg01_00001-810050352.vg
これにより論理ボリュームの定義は復元されますが、まだアクティブ化はされません。
これは、Linux+V8の復旧ワークフローにおける唯一正しい出発点です。
パート2：論理ボリュームのアクティブ化
メタデータ復元後：
LVは存在するが、非アクティブである
blkidはLVをTYPE= "LVM2_member"と表示します
論理ボリュームをマウントする前に、そのボリュームをアクティブ化する必要があります。
lvchange -ay /dev/vg01/lv01

これにより、LVは/dev/vg01/lv01で使用可能になります。
Linux+では、復旧後に論理ボリューム（LV）のアクティベーションが明示的に必要となる。
パート3：データへのアクセス
最終出力は以下のとおりです。
ファイルシステムの種類はxfsです
論理ボリュームが表示されました
ファイルシステムの破損を示す兆候がないため、修復は不要です。
正しい最終手順は、ファイルシステムをマウントすることです。
mount /dev/vg01/lv01 /important_data
これにより、基となるデータへの完全なアクセスが回復します。

質問: **60**
システム管理者は、ログファイル内で「FAIL」が何回出現するかをカウントするスクリプトを作成する必要があります。「FAIL」が0回出現した場合、管理者はメッセージを表示したいと考えています。「成功」。以下の条件が満たされた場合：

```
if [ $(grep -c FAIL /var/file.log) ___ 0 ]
then
   echo SUCCESS
else
   echo FAIL
fi
```


スクリプトを完成させるために、ゼロの前に使用すべきなのは次のうちどれですか？
A. -いいえ
B. -gt
C. -lt
D. -eq
正解: **(**正解を表示します**)**
このテストでは、「FAIL」のカウントがゼロに等しいかどうかを確認します。シェル条件式では、演算子 -eq が数値の等価性に使用されるため、[$(grep -c FAIL /var/file.log) -eq 0] はカウントがゼロかどうかを正しく評価します。

質問: **61**
管理者がLinuxサーバーにログインしたところ、時計が37分進んでいることに気づきました。以下のコマンドのうち、この問題を解決するにはどれを使用すればよいでしょうか？
A. timedatectl
B. ntpd -q
C. ntpdate
D. hwclock
正解: **C (**コメントを発表する**)**

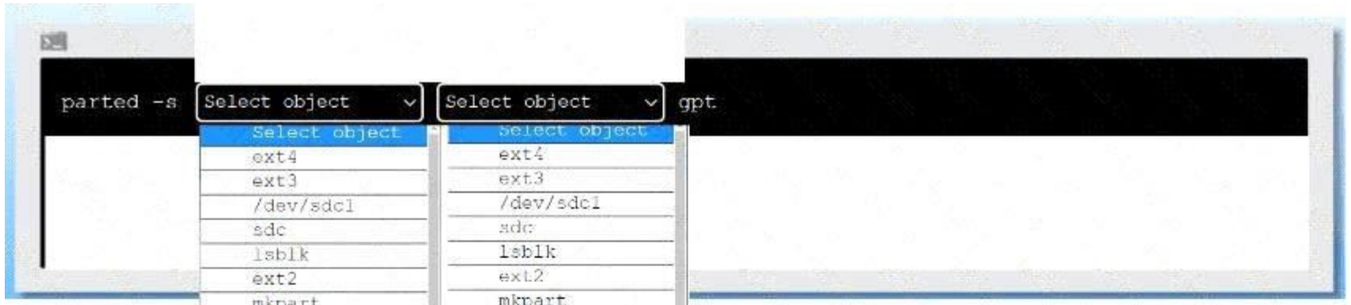
質問: **62**
企業のセキュリティマネージャーが、Linuxシステム上の脆弱性についてシステム管理者に通知します。管理者はサーバーにログインした状態で、以下の情報を受け取ります。
$日付
2024 年 7 月 11 日木 16:12:42 UTC
$ getenforce
執行
$ dnf history
ID | コマンドライン | 日時 | 操作 | 変更内容
45 | 更新 -y | 2023-07-09 | 更新 | 27
46 | httpd のインストール | 2023-01-11 | インストール | 9
47 | 更新 -y | 2023-08-08 | アップグレード | 44
次のうち、最も可能性の高いセキュリティ上の懸念事項はどれですか？
A. サーバーは1年間更新されておらず、パッチを適用する必要があります。
B. システムには httpd がインストールされているため、削除する必要があります。
C. システムはUTC時間を使用するように設定されているため、EDTに設定する必要があります。
D. システムでは SELinux が強制モードに設定されているため、無効にする必要があります。
正解: (正解を表示します)
システムセキュリティを維持するには、脆弱性を軽減するために定期的なパッチ適用とアップデートが必要です。このシナリオでは、管理者には現在のシステム日付（2024年7月11日）と、dnf historyコマンドによるパッケージ管理トランザクションの履歴が表示されます。最後に記録されたアップデートトランザクション（ID 47）は2023年8月8日に発生しました。これは、システムがセキュリティパッチやソフトウェアアップデートをほぼ1年間受け取っていないことを示しています。
CompTIA Linux+ V8のセキュリティベストプラクティスによると、「パッチ未適用システム」は組織のインフラストラクチャにとって最も重大なリスクの一つです。新たな脆弱性（CVE）は常に発見され、ベンダーはこれらの欠陥に対処するためのパッチをリリースしています。1年間アップデートされていないシステムは、より新しいソフトウェアバージョンで修正された多数の脆弱性に対して脆弱である可能性が高いです。したがって、最大のセキュリティ上の懸念は、最新のアップデートが行われていないことです。
その他の選択肢は、この文脈では有効なセキュリティ上の懸念事項ではありません。httpd（Apache）はパッチが適用されていない場合に脆弱性がある可能性がありますが、サービスが業務運営に必要であれば、その存在自体（選択肢B）は本質的にセキュリティ上の懸念事項ではありません。選択肢Cはタイムゾーンの設定（UTCとEDT）に関するもので、システムセキュリティには影響しません。選択肢DはSELinuxを無効にすることを提案していますが、SELinuxを「強制」モードで使用することは、実際にはシステムを保護するための強制アクセス制御（MAC）を提供するセキュリティのベストプラクティスです。
それを無効にすると、システムのセキュリティ体制は強化されるどころか弱体化するだろう。
検証済みの回答は、サーバーの最終更新から時間が経過しているため、直ちにパッチを適用する必要があるということです。

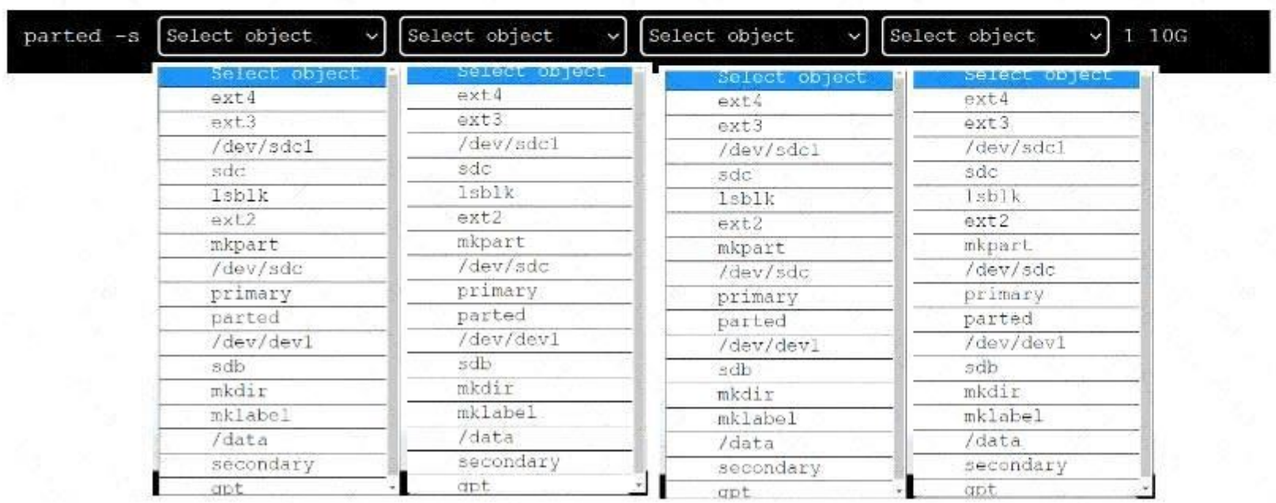
質問: **63**
Linux システム管理者は、/home/dev/web.bkp という名前のファイルの内容を /var に抽出する必要があります。
/www/html/ ディレクトリ。管理者は、以下のどのコマンドを使用すべきでしょうか？
A. cd /var/www/html/ & & gzip -c /home/dev/web.bkp | tar xf -
B. pushd /var/www/html/ & & cpio -idv < /home/dev/web.bkp & & popd
C. tar -c -f /home/dev/web.bkp /var/www/html/

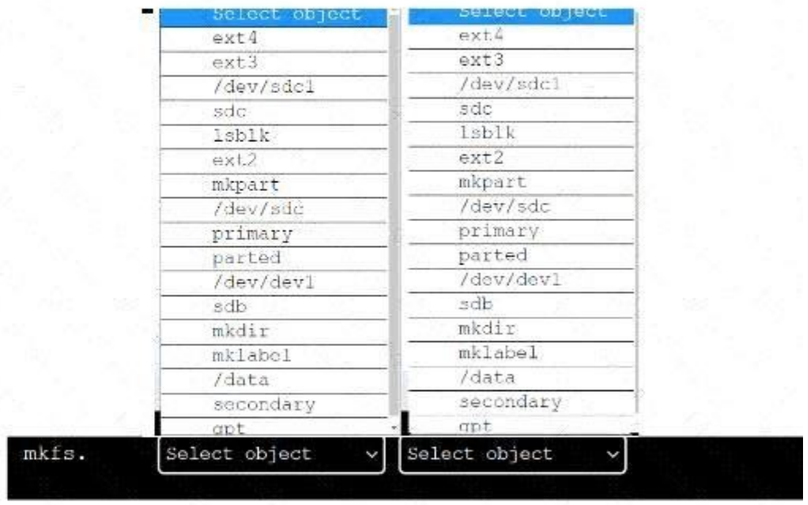
D. unzip -c /home/dev/web.bkp /var/www/html/
正解: (正解を表示します)
ファイル抽出とバックアップ復元は、CompTIA Linux+ V8で扱われる基本的なシステム管理タスクです。このシナリオでは、管理者は既存のバックアップファイルの内容をターゲットディレクトリに抽出する必要があります。
正しいコマンドはオプションBで、抽出モードでcpioを使用します。このコマンドは、pushdを使用して宛先ディレクトリ（/var/www/html/）に移動し、cpio -idvでアーカイブの内容を展開した後、popdで元のディレクトリに戻ります。これにより、アーカイブ内のパスを変更することなく、ファイルが正しい場所に復元されることが保証されます。
cpioユーティリティは、cpio -oで作成されたバックアップによく使用され、標準入力からのアーカイブデータの読み取りをサポートしています。Linux+ V8のドキュメントでは、cpioはバックアップおよびリストア操作で有効なサポート対象のアーカイブ形式として記載されています。
他の選択肢は誤りです。選択肢Aは、バックアップがgzip圧縮されたtarアーカイブであると誤って想定しています。
オプションCは、既存のアーカイブを解凍するのではなく、新しいアーカイブを作成します。オプションDは、ファイルがZIPアーカイブであると想定していますが、拡張子「bkp」はZIPアーカイブであることを示すものではありません。
Linux+ V8では、アーカイブ形式に基づいて適切なツールを使用し、ファイルを目的のディレクトリに復元することが重視されています。したがって、正解はBです。

質問: **64**
システム管理者が、リモートの Git リポジトリにある既存のファイルを更新して変更を適用したいと考えています。このプロセスを完了するために、管理者が最後に実行すべき Git コマンドは次のうちどれですか？
A. git commit -m "新しい情報で更新しました"
B. git checkout -b update-feature
C. git pull origin main
D. git push origin update-feature
正解: (正解を表示します)
git pushコマンドは、ローカルブランチからリモートリポジトリにコミットされた変更を送信し、リモートで更新を利用可能にして更新プロセスを完了します。

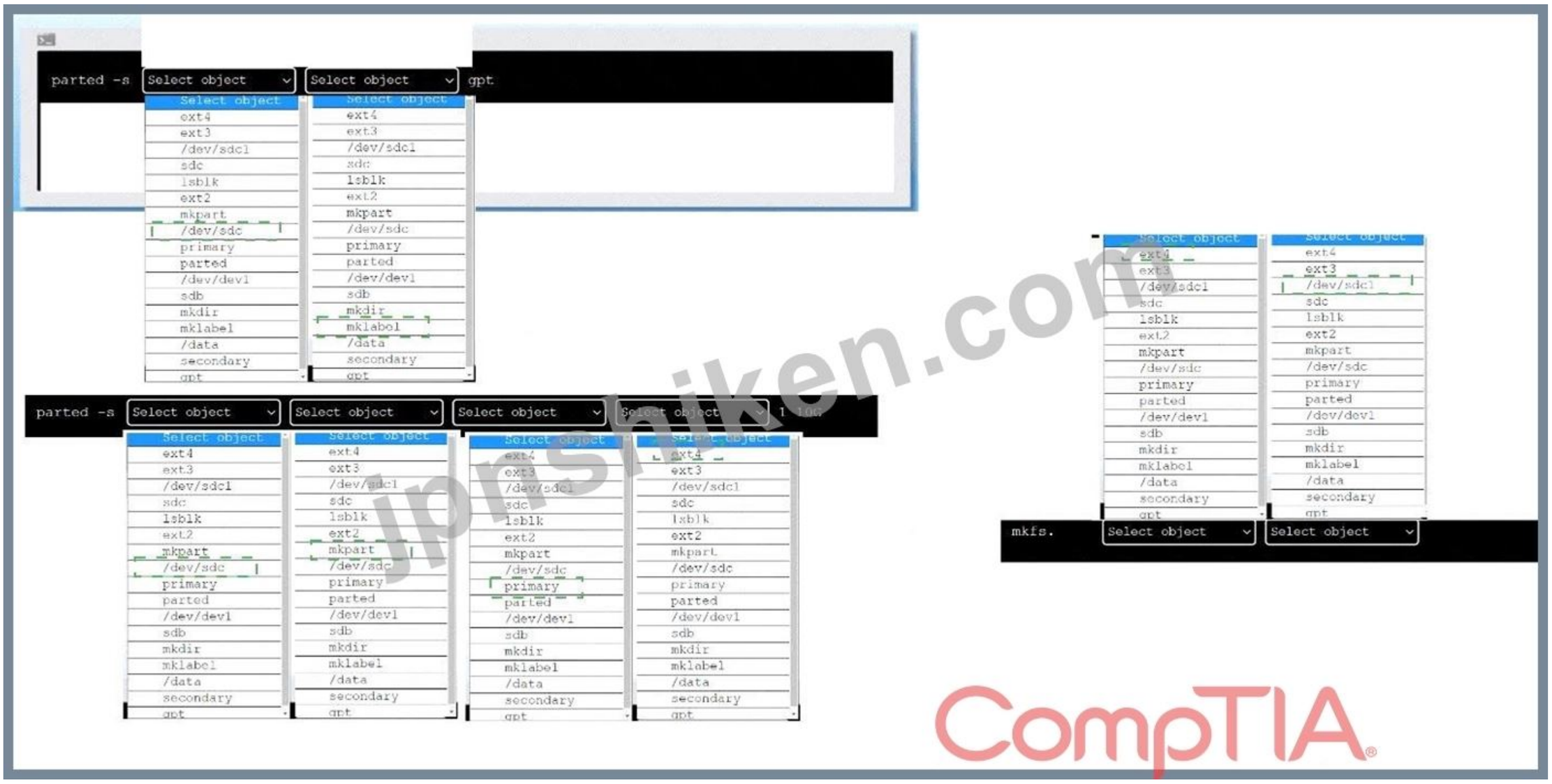
質問: **65**
Linuxシステムに新しいドライブが追加されました。提供された環境とトークンを使用して、以下のタスクを完了してください。
* 適切なデバイスラベルを作成する。
* 新しいパーティションにext4ファイルシステムをフォーマットして作成します。
現在の作業ディレクトリは / です。


parted -s
Select object
Select object
gpt
Select object
ext4
ext3
/dev/sdc1
sdc
lsblk
ext2
mkpart
/dev/sdc
primary
parted
/dev/dev1
sdb
mkdir
mklabel
/data
secondary
gpt

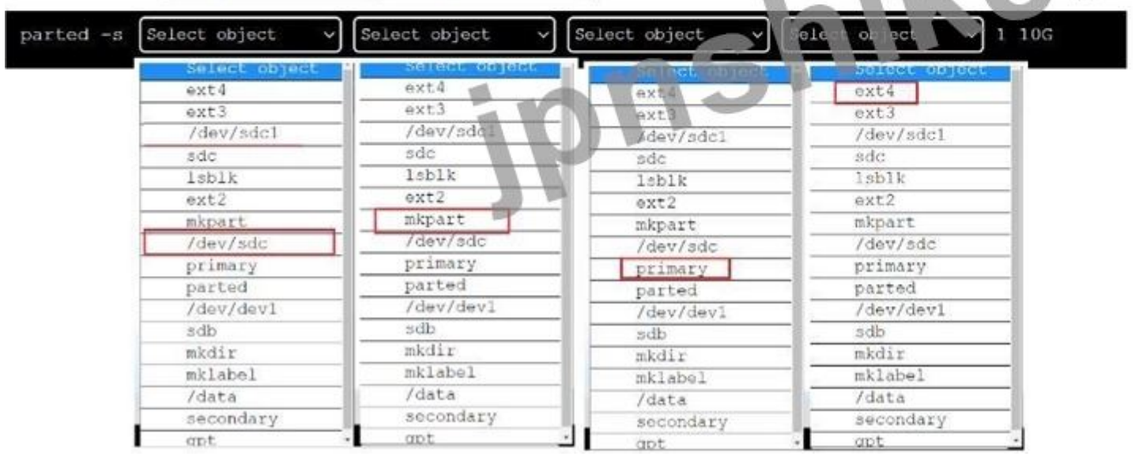

parted -s
Select object
Select object
Select object
Select object
1 10G
Select object
ext4
ext3
/dev/sdc1
sdc
lsblk
ext2
mkpart
/dev/sdc
primary
parted
/dev/dev1
sdb
mkdir
mklabel
/data
secondary
gpt

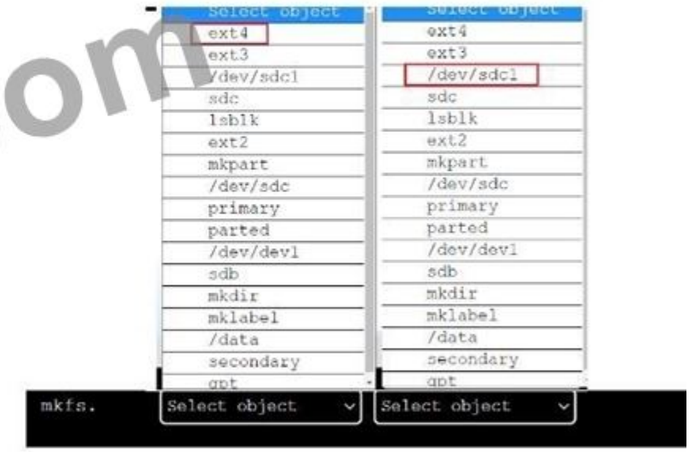

mkfs.
Select object
Select object
Select object
ext4
ext3
/dev/sdc1
sdc
lsblk
ext2
mkpart
/dev/sdc
primary
parted
/dev/dev1
sdb
mkdir
mklabel
/data
secondary
gpt

正解:



Explanation:





適切なデバイスラベルを作成し、新しいパーティションにext4ファイルシステムをフォーマットして作成するには、以下のコマンドを使用できます。
新しいドライブ /dev/sdc に GPT (GUID パーティション テーブル) ラベルを作成するには、parted コマンドに -s オプション (スクリプト モード用)、デバイス名 (/dev/sdc)、mklabel コマンド、およびラベル タイプ (gpt) を指定します。コマンドは次のとおりです。
parted -s /dev/sdc mklabel gpt
新しいドライブ /dev/sdc に 10 GB のプライマリパーティションを作成するには、parted コマンドに -s オプション、デバイス名 (/dev/sdc)、mkpart コマンド、パーティションタイプ (プライマリ)、ファイルシステムタイプ (ext4)、およびパーティションの開始点と終了点 (1G と 10G) を指定します。コマンドは次のとおりです。
parted -s /dev/sdc mkpart primary ext4 1 10G
新しいパーティション /dev/sdc1 に ext4 ファイルシステムをフォーマットして作成するには、mkfs コマンドにファイルシステムの種類 (ext4) とデバイス名 (/dev/sdc1) を指定します。コマンドは次のとおりです。
mkfs.ext4 /dev/sdc1
lsblkコマンドを使用すると、すべてのブロックデバイスとそのプロパティが一覧表示されるため、新しいパーティションとファイルシステムが作成されたことを確認できます。

質問: **66**
ITインフラストラクチャの文脈において、Ansibleが何のために使用されるかを説明しているのは次のうちどれですか？
A. データベース管理
B. 構成管理

C. プロセス管理
D. 資産運用
正解: (正解を表示します)
正解はBです。Ansibleは主にITインフラストラクチャを効率的に管理するための自動化および構成管理ツールとして設計されているため、構成管理が正解となります。Linux環境では、Ansibleを使用することで、システム管理者は人間が読みやすいYAMLベースのプレイブックを使用して、システムの望ましい状態を定義できます。これらのプレイブックは、ソフトウェアのインストール、システムアップデート、サービス構成、複数のマシンへのデプロイプロセスなどのタスクを自動化します。
Ansibleはエージェントレスアーキテクチャを採用しているため、管理対象ノードに追加のソフトウェアをインストールする必要はありません。代わりに、SSHなどの標準プロトコルを使用してリモートシステムと通信します。そのため、他の構成管理ツールに比べて軽量で導入が容易です。Linux+環境においては、Ansibleのような自動化ツールを理解することは、システム間の一貫性を維持し、手動による構成エラーを減らし、運用効率を向上させるために不可欠です。
選択肢A（データベース管理）は、Ansibleがデータベース関連のタスクを自動化することはできるものの、データベースの管理や運用を目的として設計されているわけではないため、誤りです。選択肢C（プロセス管理）は、実行中のプロセスを制御すること（ps、kill、topなどのコマンドを使用すること）を指し、Ansibleの主要機能ではないため、誤りです。選択肢D（資産管理）も、ハードウェアとソフトウェアの在庫を追跡することを指し、Ansibleのコア機能の範囲外であるため、誤りです。
現代のLinuxシステム管理では、Ansibleのようなツールがオーケストレーションや構成管理に広く利用されており、管理者は反復的なタスクを自動化し、システムの一貫性を確保し、インフラストラクチャ管理を効果的に拡張することができる。

質問: **67**
Ansibleプレイブックを作成する際に使用される形式は次のうちどれですか？
A. YAML
B. CSV
C. JSON
D. XML
正解: (正解を表示します)
AnsibleのプレイブックはYAML形式で記述されます。YAMLは、自動化のためのプレイ、タスク、変数、ロールを定義するために使用される、人間が読みやすい構造化されたフォーマットです。

質問: **68**
管理者はサーバーのメンテナンスを完了したが、論理ボリュームを再マウントできない。
以下の出力が与えられた場合：

```
# mount /dev/data/files /opt/data/
mount: /opt/data: special device /dev/data/files does not exist.

# lvs
LV VG Attr LSize Pool Origin Data% Meta% Move Log Cpy%Sync Convert
files data -wi-a----- 600.00m

# vgs
VG #PV #LV #SN Attr VSize VFree
data 1 1 0 wz--n- 1020.00m 420.00m
```

管理者はこの問題を解決するために、以下のどのコマンドを実行すべきですか？
A. vgchange -ay data
B. lvscan --all
C. vgimport data
D. lvchange -ay /dev/data/files
正解: (正解を表示します)
エラーメッセージ「特殊デバイス /dev/data/files が存在しません」は、ボリュームグループ data がアクティブ化されていないことを示しています。lvsand vgsoutput から:

論理ボリュームファイルはデータボリュームグループ内に存在します。
ボリュームグループ（VG）と論理ボリューム（LV）は正しく一覧表示されていますが、メンテナンスのため非アクティブ状態になっている可能性があります。

質問: **69**
Linux管理者は、ハードディスクの内容を安全に消去する必要があります。この作業に最適なコマンドは次のうちどれですか？
A. sudo rm -rf /dev/sda1
B. sudo shred /dev/sda1
C. sudo parted rm /dev/sda1
D. sudo dd if=/dev/null of=/dev/sda1
正解: **(正解を表示します)**
安全なデータ消去は、Linux+ V8の目標で取り上げられている重要なセキュリティ要件です。データを完全に消去する必要がある場合、標準的なファイル削除コマンドではディスク上のデータを上書きできないため、不十分です。
shredコマンドは、ランダムなデータで複数回上書きすることで、ファイルやデバイスを安全に消去またはブロックするように設計されています。sudo shred /dev/sda1を実行すると、パーティション全体が上書きされるため、データの復旧は極めて困難、あるいは不可能になります。これは、安全なデータ消去に関するLinux+ V8のベストプラクティスに完全に合致しています。
他のオプションは正しくありません。`rm -rf` はディレクトリのエントリを削除しますが、ディスクデータは上書きしません。`parted rm` はパーティションのエントリを削除しますが、基となるデータはそのまま残ります。`dd if=/dev/null` はゼロバイトを書き込み、既存のデータブロックを上書きしません。
Linux+ V8のドキュメントでは、コンプライアンスや機密性が求められる場合の安全なデータ消去に最も適したツールとしてshredが挙げられています。したがって、正解はBです。

質問: **70**
管理者は、Webサービスが応答していないという報告を受け取ります。管理者は以下の出力を確認します。

```
$ echo $PWD
/etc/pki/nginx

$ ls -lRt
.:
total 8
drwxr-xr-x. 2 root root 6 Jul 10 10:57 private
-rw-r--r--. 1 root root 895 Jul 10 10:56 server.crt
-rw-------. 1 root root 227 Jul 10 10:56 server.key
./private:
total 0

$ sudo systemctl status nginx
  nginx.service - The nginx HTTP and reverse proxy server
       Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; preset: disabled)
       Active: failed (Result: exit-code) since Wed 2023-11-01 06:56:51 EDT; 6s ago
    Process: 110551 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 110552 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=1/FAILURE)
       CPU: 144ms

Nov 01 06:56:51 webserver systemd[1]: Starting nginx.service - The nginx HTTP and reverse proxy server...
Nov 01 06:56:51 webserver nginx[110552]: nginx: [emerg] cannot load certificate key "/etc/pki/nginx/private/server.key": BIO_new_file()
failed (SSL: error:80000002:system library::No such file or directory:calli>
Nov 01 06:56:51 webserver nginx[110552]: nginx: configuration file /etc/nginx/nginx.conf test failed
Nov 01 06:56:51 webserver systemd[1]: nginx.service: Control process exited, code=exited, status=1/FAILURE
Nov 01 06:56:51 webserver systemd[1]: nginx.service: Failed with result 'exit-code'.
Nov 01 06:56:51 webserver systemd[1]: Failed to start nginx.service - The nginx HTTP and reverse proxy server.
```

ウェブサービスが応答しない理由は次のうちどれですか？

A. サービスがそれを見つけられるように、秘密鍵の名前を server.crt から server, key に変更する必要があります。

B. 秘密鍵と公開鍵が一致しません。両方の鍵を交換する必要があります。

C. 秘密鍵が正しい場所にありません。正しいディレクトリに移動する必要があります。

D. 秘密鍵の権限が正しくないため、サービス用に0755に変更する必要があります。

正解: **(**正解を表示します**)**

この問題は、CompTIA Linux+ V8 の学習目標におけるトラブルシューティング領域、具体的にはサービス起動の失敗と証明書関連のエラーに該当します。提供された出力から、NGINX サービスが起動時に秘密鍵ファイルを見つけられないために失敗していることが明確に分かります。

重大なエラーメッセージは次のとおりです。

証明書キー 「/etc/pki/nginx/private/server.key」を読み込めません: そのようなファイルまたはディレクトリはありません。このメッセージは、NGINXが/etc/pkiディレクトリで秘密鍵を探すように明示的に設定されていることを示しています。

/nginx/private/ にあります。しかし、ディレクトリー覧を見ると、private ディレクトリは存在しますが空であり、server.key ファイルは /etc/pki/nginx/ にあります。NGINX は設定されたパスに秘密鍵を見つけることができないため、設定テスト (nginx -t) が失敗し、systemd がサービスの起動を阻止します。

オプションCは根本原因を正しく特定しています。秘密鍵が正しい場所に存在しないことが原因です。server.keyを/etc/pki/nginx/private/に移動するか またはNGINXの設定を更新して現在の場所に合わせる）、この問題を解決してください。Linux+ V8のドキュメントでは、サービス障害はファイルの破損ではなく、設定パスの不整合が原因であることが多いと強調されています。

他の選択肢は誤りです。選択肢Aは証明書ファイルの名前変更について誤って言及しており、パスの問題には対処していません。選択肢Bは鍵の不一致を示唆していますが、これはSSLエラーではなく別のSSLエ

ラーを生成します。
「ファイルが見つかりません」というエラーが表示されます。オプションDも誤りです。秘密鍵には0755のような実行権限が付与されるべきではありません。通常、セキュリティ上の理由から、秘密鍵は制限された権限（例えば0600）に設定されます。
したがって、秘密鍵ファイルがNGINXの設定で想定されているディレクトリに存在しないため、Webサービスが応答していません。正解はCです。

質問: **71**
Linux 管理者は、プロセスが
/sbin/app-01 は、新しいコンテナが起動したときに実行されます。次のうち、このタスクを実行するのはどれですか？
A. から
B. エントリーポイント
C. オンビルド
D. 暴露する
正解: (正解を表示します)
この命令は、コンテナの起動時に実行される実行可能ファイルを定義し、指定されたプロセスがイメージから新しいコンテナが作成されるたびに自動的に起動されるようにします。

質問: **72**
ユーザーであるジョーが、以前アンが担当していたポジションに就任しました。システム管理者として、アンのホームディレクトリにあるすべてのファイルをアーカイブし、ジョーのホームディレクトリに展開する必要があります。
説明書
各タブ内で、オブジェクトをクリックして適切なコマンドを作成します。コマンドオブジェクトは一度しか使用できませんが、スペースバーとアンダースコア（_）のオブジェクトは複数回使用できます。すべてのオブジェクトが使用されるわけではありません。
シミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。

Archive | Extract

-d | /tmp/ann.tar | -cJvf

joe | /home/ | /tmp/ann.tar.gz

-xzvf | /tmp/ann.tgz | /tmp/ann.tar.bz

-cvf | -C | -c

-xjvf | ann | -xvf

␣

tar | /home/-C | Archive

正解:

解決策については、下記の解説をご覧ください。

Explanation:

アーカイブタブ - アンのホームディレクトリからアーカイブを作成します

正しいコマンド:

tar -cvf /tmp/ann.tar -C /home/ann

抽出タブ - アーカイブをジョーのホームディレクトリに展開します

正しいコマンド:

tar -xvf /tmp/ann.tar -C /home/ joe
この実技問題は、CompTIA Linux+ V8の目標に含まれるシステム管理の中核スキルである、tarを使用したファイルアーカイブと復元をテストするものです。課題は、Annのファイルを保存し、Joeのホームディレクトリに正しく配置することです。
アーカイブフェーズの説明
最初のステップの目標は、フルパス（/home）を埋め込まずに、Annのホームディレクトリ全体をアーカイブすることです。
/ann) をアーカイブ内に挿入します。これは -C オプションを使用して行います。
コマンドの詳細：
tar # アーカイブユーティリティ
-c # アーカイブを作成する
-v # 詳細出力（オプションですが使用可能）
-f /tmp/ann.tar # アーカイブファイルを指定します
-C /home/ # アーカイブ前にディレクトリを変更します
ann # ann ディレクトリのみをアーカイブします
これにより、絶対パスを含まないAnnのファイルを含むクリーンなアーカイブが作成されます。これはベストプラクティスであり、Linux+ V8のドキュメントにも明記されています。
抽出フェーズの説明
2番目の手順では、アーカイブされたファイルをジョーのホームディレクトリに展開します。
コマンドの詳細：
-x # 抽出
-v # 詳細表示
-f /tmp/ann.tar # アーカイブを指定します
-C /home/joe # ファイルをジョーのホームディレクトリに直接展開します
これにより、抽出後の処理に応じて、Joe は Ann のファイルを /home/joe/ann または /home/joe 直下に正しく受け取ることができ、これは Linux+ の管理ユーザー移行に関する期待と一致します。

質問: **73**
システム管理者は、共有ディレクトリ内で新しく作成されたファイルを変更しようとした際に問題が発生しているというユーザーからの報告を受け取ります。管理者は次のような出力結果を確認します。
以下のうち、この問題に対する最適な解決策はどれですか？
A. 共有フォルダ内のユーザーにsetuidbitを追加する
B. 新しく作成されたファイルのグループを手動で変更する
C. ディレクトリの内容をすべて、誰でも書き込みおよび読み取りできるように変更します。
D. 共有フォルダ内のグループにsetgidbitを追加する
正解: (正解を表示します)
共有ディレクトリにsetgidビットを設定すると、新しく作成されたすべてのファイルとサブディレクトリがディレクトリのグループ所有権を継承し、すべてのグループメンバーが手動操作なしで一貫してファイルを変更できるようになります。

質問: **74**
Kubernetesクラスタにおいて、ポートをインターネット上で公開アクセス可能にするために、次のうちどのリソースを作成する必要がありますか？
A. 展開
B. ネットワーク
C. サービス
D. ポッド

正解: (正解を表示します)
コンテナオーケストレーションの概念は、Linux+ V8 の自動化およびオーケストレーション領域の一部です。Kubernetes では、ワークロードは Pod 内で実行されますが、Pod はクラスタ外部から直接アクセスすることはできません。
アプリケーションを外部に公開するには、サービスリソースを作成する必要があります。サービスは安定したネットワークエンドポイントを提供し、NodePort、LoadBalancer、またはClusterIPとして構成できます。外部への公開は通常、NodePortまたはLoadBalancerタイプを使用して実現されます。
オプションCの 『サービス」が正解です。デプロイメントはPodを管理しますが、ネットワークの公開は処理しません。Podは実行中のコンテナを表しますが、デフォルトでは外部からのアクセスはできません。
『Network」は有効なKubernetesリソースタイプではありません。
Linux+ V8のドキュメントでは、コンテナ化されたアプリケーションを公開するためのメカニズムとしてサービスが強調されています。
したがって、正解はCです。

質問: **75**
システム管理者が新しいLinuxシステムを構成中で、2台のサーバー間でパスワードなし認証を有効にする必要があります。管理者は、以下のどのコマンドを使用すべきでしょうか？
A. ssh-keygen -t rsa && ssh-copy-id -i ~/.ssh/id_rsa.pub john@server2
B. ssh-keyscan -t rsa && ssh-copy-id john@server2 -i ~/.ssh/key
C. ssh-agent -i rsa && ssh-copy-id ~/.ssh/key john@server2
D. ssh-add -t rsa && scp -rp ~/.ssh john@server2
正解: (正解を表示します)
このコマンドはSSHキーペアを生成し、公開鍵をリモートサーバーに安全にコピーすることで、システム間で鍵ベースのSSHログインを可能にし、パスワードなしの認証を実現します。

質問: **76**
毎月のサーバーパッチ適用が完了した後、Linux管理者は重要なアプリケーションが動作していないという報告を受けました。管理者がどのパッケージがインストールされたかを判断するのに役立つコマンドは次のうちどれですか？
A. DNFの歴史
B. dnfリスト
C. dnf情報
D. dnf検索
正解: **A** (コメントを発表する)
パッケージ管理のトラブルシューティングは、CompTIA Linux+ V8で取り上げられる重要なLinux管理者スキルです。システムパッチ適用後、どのパッケージがインストール、更新、または削除されたかを特定することは、アプリケーションの障害を診断する最初のステップとなることがよくあります。
dnf history コマンドは、まさにこの目的のために設計されています。このコマンドは、インストール、アップグレード、ダウングレード、削除など、すべての DNF トランザクションを時系列順に表示します。各トランザクションには ID が割り当てられ、タイムスタンプ、影響を受けたパッケージ、実行されたアクションが含まれます。これにより、管理者はアプリケーションの障害と最近の変更を関連付けることができます。
オプションAが正解です。なぜなら、現在のパッケージの状態だけでなく、履歴情報も提供するからです。Linux+ V8のドキュメントでは、dnf historyが重要な監査およびロールバックツールとして強調されています。
他のオプションでは不十分です。dnf list はインストール済みまたは利用可能なパッケージを表示しますが、インストール日時は表示しません。dnf info は特定のパッケージのメタデータを表示しますが、トランザクション履歴は表示しません。
dnf search は、パッケージを名前または説明で検索するために使用されます。
dnf history を使用した最近のトランザクションを確認することで、管理者は問題のあるアップデートを迅速に特定し、パッケージのロールバックなどの是正措置を講じることができます。
したがって、正解はAです。

質問: **77**
ユーザーから、Linuxシステムが応答せず、簡単なコマンドの実行に時間がかかりすぎるとの報告がありました。Linux管理者がシステムにログインすると、次の出力が表示されます。出力1:
10:06:29 稼働時間 235日、19:23、ユーザー数 2、ロードアベレージ: 8.71、8.24、7.71

Output 2:

```
Linux 6.8.0-31-generic (host) 05/10/2024 _x86_64_ (4 CPU)
```

10:07:42	AM	CPU	%usr	%nice	%sys	%iowait	%irq	%soft	%steal	%guest	%gnice	%idle
10:07:42	AM	all	65.88	0	20.54	5.65	0	7.93	0	0	0	0

システムは以下のうちどれを経験していますか？
A. 高遅延
B. 高い稼働率
C. CPU負荷が高い
D. 高いI/O待ち時間
正解: (正解を表示します)
このシナリオは、CompTIA Linux+ V8の目標におけるトラブルシューティング領域で扱われる、典型的なパフォーマンス問題のトラブルシューティング事例です。分析すべき主要な指標は、ロードアベレージ値とCPU使用率の統計情報です。
uptimeコマンドの結果によると、1分、5分、15分間隔での負荷平均はそれぞれ8.71、8.24、7.71でした。
ロードアベレージとは、CPU上で実行中または実行待ち状態のプロセスの平均数を表します。4つのCPUコアを搭載したシステムでは、正常なロードアベレージは通常4以下です。ロードアベレージが常に8前後または8を超える場合は、実行可能なプロセス数が利用可能なCPUリソースを大幅に上回っていることを示し、プロセスが待機状態となり、システムの応答性が低下します。
CPU出力もこの状況を裏付けています。%idleの値は0であり、CPUにアイドル時間が全くないことを意味します。CPU時間の大部分はユーザー空間（65.88%）とシステム/カーネル空間（20.54%）で消費されており、計算処理とカーネル処理が活発に行われていることを示しています。%iowaitは5.65%ですが、ディスクI/Oが主なボトルネックであると示唆するほど高い値ではありません。
オプションCの「CPU負荷が高い」が、症状を最もよく説明しています。CPU負荷が高いと、限られたCPU時間をめぐってプロセスが競合するため、コマンドの実行速度が低下します。これは、システムが応答しなくなるという観測された動作と直接的に一致します。
他の選択肢は誤りです。高い稼働時間は、システムが稼働している時間の長さを示すだけであり、それ自体がパフォーマンスの問題を引き起こすわけではありません。高いレイテンシは一般的な用語であり、提供されたメトリックによって示される具体的な診断ではありません。高いI/O待機時間には、%iowaitの値が著しく高くなる必要があります。
Linux+ V8のドキュメントによると、負荷平均とCPUコア数および使用率を関連付けることは、正確なパフォーマンス診断に不可欠です。したがって、正解はC. CPU負荷が高い、です。

質問: **78**
管理者は、指定されたユーザーのユーザー ID、ホーム ディレクトリ、および割り当てられたシェルを確認する必要があります。
「会計」。管理者はこの情報を取得するために、以下のどのコマンドを使用すべきでしょうか？
A. getent passwd accounting
B. ID会計
C. grep accounting /etc/shadow
D. 会計担当者
正解: (正解を表示します)
ユーザーアカウント情報はシステムのアカウントデータベースに一元的に保存され、Linux+ V8では、このデータを安全かつ一貫して照会するために標準ツールを使用することが重視されています。

getent passwd accounting コマンドは、ローカルファイルまたは LDAP などのネットワークサービスから取得される passwd データベースからユーザーのエントリを取得します。このエントリには、ユーザー名、ユーザー ID (UID)、グループ ID (GID)、ホームディレクトリ、および割り当てられたログインシェルが含まれます。したがって、オプション A は、要求されたすべての情報を単一のコマンドで提供します。
オプションBのid accountingは、UIDとグループメンバーシップを表示しますが、ホームディレクトリや割り当てられたシェルは表示しません。オプションCは、/etc/shadowにはパスワードハッシュと有効期限データが含まれており、シェルやホームディレクトリの情報が含まれていないため、誤りです。オプションDのwho accountingは、ログインセッションのみを表示し、アカウント構成の詳細を提供しません。
Linux+ V8のドキュメントでは、getent passwdがさまざまな認証バックエンドで動作するため、包括的なユーザーアカウント情報を取得するための推奨方法として強調されています。
したがって、正解はAです。

質問: **79**
次のネットワークタイプのうち、仮想マシンがホストマシンとは独立して物理ネットワーク接続を使用できるのはどれですか？
A. 内部
B. 夜
C. ホスト専用
D. ブリッジド
正解: (正解を表示します)
このネットワークタイプでは、仮想マシンが物理ネットワークに直接接続されるため、ホストによるネットワーク変換に頼ることなく、他の物理デバイスと同じネットワーク接続を使用できます。

質問: **80**
ユーザー、グループ、マシン、組織単位の階層構造を含む分散ディレクトリサービスにアクセスするためのプロトコルは、次のうちどれですか？
A. SMB
B. TLS
C. LDAP
D. KRB-5
正解: (正解を表示します)
LDAP（軽量ディレクトリアクセスプロトコル）は、ユーザー、グループ、コンピュータ、組織単位を階層構造で整理する分散ディレクトリサービスへのアクセスと維持を目的として特別に設計されています。

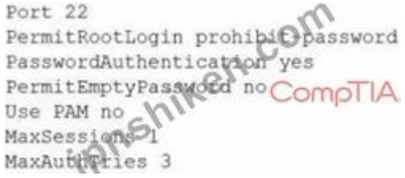
質問: **81**
Linuxシステム上で新しいPythonプロジェクトを開始する際の最初のステップは、次のうちどれですか？
A. python -m venv /path/to/project
B. python -m pip install -r /path/to/project
C. export PYTHON_PATH=/path/to/project
D. python -m source /path/to/project
正解: (正解を表示します)
正解はAです。`python -m venv /path/to/project` は、新しいPythonプロジェクトを開始する際の推奨される最初のステップです。仮想環境は、プロジェクトの依存関係をシステム全体のPythonインストールから分離し、ライブラリやパッケージのバージョンが他のプロジェクトやシステムコンポーネントと競合しないようにします。
コマンド `python -m venv /path/to/project` を実行すると、独自の Python インタープリタ、ライブラリ、スクリプトを含む自己完結型のディレクトリが作成されます。これにより、開発者や管理者はグローバル環境に影響を与えることなく、プロジェクト固有のパッケージをインストールできます。仮想環境を作成した後、通常はそれをアクティブ化し (例: `source /path/to/project/bin/activate`)、その後 pip を使用して依存関係をインストールします。
オプションB（python -m pip install -r /path/to/project）は誤りです。なぜなら、要件ファイルから依存関係をインストールする場合、仮想環境またはプロジェクト構造が既に構築されていることを前提としているからです。これは最初のステップではありません。
オプションC（export PYTHON_PATH=/path/to/project）は誤りです。PYTHONPATHを設定すると、Pythonがモジュールを探す場所が変更されるだけで、隔離された環境が作成されたり、依存関係が管理された

りするわけではありません。
オプション D (python -m source /path/to/project) は、source は環境をアクティブ化するために使用されるシェル組み込みコマンドであり、Python モジュールではないため、正しくありません。また、この構文は無効です。
Linux+の観点から言えば、仮想環境の利用は、自動化とスクリプト作成におけるベストプラクティスに合致する。
これにより、開発環境の一貫性、再現性、および分離性が確保され、Pythonベースのアプリケーションのデプロイ、テスト、および保守にとって非常に重要となります。

質問: **82**
次のうち、しきい値を監視する主な目的を説明しているのはどれですか？
A. 制限を超えた場合にアラートを生成する
B. サービスの可用性を計算する
C. デバイスの健康状態をチェックする
D. サービスを自動的に再起動する
正解: (正解を表示します)
監視しきい値は、指標の許容範囲を定義するものであり、主にこれらの制限を超えた場合にアラートを発動するために使用され、管理者が問題が深刻化する前に対応できるようにします。

質問: **83**
次のうち、ウェブフックを最も正確に説明しているのはどれですか？
A. ウェブサーバー通信のための認証方法
B. ネットワーク機器監視のためのSNMPベースのAPI
C. システム間で機密情報を伝送する手段
D. HTTPベースのコールバック関数
正解: (正解を表示します)
正解はDです。HTTPベースのコールバック関数です。Webhookは、特定のイベントが発生したときに、あるシステムがHTTP経由でリアルタイムデータを別のシステムに自動的に送信できるようにする仕組みです。更新情報を得るためにAPIを継続的にポーリングする代わりに、Webhookはイベント駆動型の通信を可能にし、自動化をより効率的かつ迅速に行えるようにします。
実際のLinuxおよびDevOps環境では、Webhookは自動化、オーケストレーション、および統合ワークフローで広く使用されています。たとえば、GitHubのようなバージョン管理システムは、WebhookをトリガーしてCIに通知することができます。
/CDパイプラインは、新しいコードがプッシュされるたびに実行されます。受信システムはHTTPエンドポイント（URL）を公開し、イベントが発生すると、Webhookは関連データペイロードを含むHTTP POSTリクエストを送信します。この設計は、ポーリング方式と比較してオーバーヘッドを大幅に削減します。
選択肢Aは誤りです。なぜなら、Webhookは認証メカニズムではないからです。認証（トークンや署名など）はWebhook通信のセキュリティ確保に利用できますが、それがWebhookの主な目的ではありません。
選択肢Bは、SNMP（Simple Network Management Protocol）がWebhookとは無関係であるため、誤りです。
SNMPはネットワーク機器の監視と管理に使用される一方、WebhookはHTTP/HTTPSプロトコル上で動作します。
選択肢Cは誤りです。Webhookはデータ（適切に保護されていない場合は機密情報を含む）を送信する可能性がありますが、その目的は機密データを送信することではなく、自動コールバックを通じてシステムにイベントを通知することです。
Linux+の観点から見ると、Webhookの理解は自動化およびオーケストレーションタスクにおいて不可欠です。Webhookは、スクリプト、構成管理ツール、クラウドネイティブワークフローに一般的に統合され、リアクティブでイベント駆動型のシステム動作を実現し、最新のインフラストラクチャ環境における効率性と拡張性を向上させます。

質問: **84**
Linux 管理者が SSH 経由で root としてサーバーにログインしようとすると、次のエラーメッセージが表示されます。「アクセスが拒否されました。もう一度お試しください。」管理者は root でサーバーのコンソールに直接ログインでき、パスワードが正しいことを確認しました。管理者は SSH サービスの設定を確認し、次の出力を得ました。



上記の出力に基づくと、管理者がSSH経由でサーバーにログインできる可能性が最も高いのは次のうちどれですか？

A. 他のユーザーセッションからログアウトしてください。一度に許可されるのは1つだけです。

B. PAMを有効にし、SSHモジュールを設定します。

C. SSHポートを2222に変更します。

D. SSH経由でrootとしてログインするには、キーを使用します。

正解: **(正解を表示します)**

SSH設定オプション「PermitRootLogin prohibit-password」は、rootユーザーがパスワード認証でログインすることを禁止します。この設定により、rootユーザーはSSH経由でパスワードを使用してログインすることはできず、鍵認証のみが許可されます。管理者は引き続きローカルでrootとしてログインできますが、このSSH設定の影響を受けません。rootとしてSSHアクセスを許可するには、管理者はパスワードの代わりにSSH鍵を使用する必要があります。

その他の選択肢：

* A. MaxSessionsは同時SSHセッション数を制御するもので、ここではログイン拒否の原因ではありません。
* B. PAM（Pluggable Authentication Modules）は無効になっていますが、基本的なSSH認証には有効にする必要はありません。
* C. SSHポートの変更は、認証方法の問題とは無関係です。

参照：

CompTIA Linux+ 学習ガイド：試験XK0-006、Sybex、第 11 章：「Linux のセキュリティ保護」、セクション：「SSH アクセスのセキュリティ保護」 CompTIA Linux+ XK0-006 目標、ドメイン 3.0 :セキュリティ

質問: **85**

Linux管理者は、app-01-imageコンテナを作成し、それに接続する必要があります。以下のコマンドのうち、このタスクを実行するのはどれですか？

A. docker run -it app-01-image

B. docker start -td app-01-image

C. docker build -ic app-01-image

D. docker exec -dc app-01-image

正解: **(正解を表示します)**

コンテナのライフサイクル管理は、CompTIA Linux+ V8 の自動化、オーケストレーション、スクリプト作成の分野における重要なトピックです。管理者は、コンテナの作成、コンテナの起動、実行中のコンテナ内でのコマンド実行の違いを理解しておく必要があります。

正しいコマンドは `docker run -it app-01-image` です。`docker run` コマンドは、指定されたイメージから新しいコンテナを作成し、コンテナを起動し、オプションで管理者の端末をコンテナに接続するという 3 つのアクションを同時に実行します。`-i` オプションは標準入力を開いたままにし、`-t` オプションは擬似端末 (TTY) を割り当てます。これらのオプションを組み合わせることで、管理者はコンテナ作成直後に対話的に接続できるようになります。

他のオプションは、以下の理由により不適切です。`docker start` は、停止中の既存のコンテナを起動するためにのみ使用され、イメージから新しいコンテナを作成するものではありません。また、`-t` と `-d` は、コンテナの起動中に対話型ターミナルを接続するための有効なオプションではありません。`docker build` は、Dockerfile から Docker イメージをビルドするために使用され、コンテナの作成や接続には使用できません。`docker exec` は、既に実行中のコンテナ内でコマンドを実行するために使用されるため、コンテナの作成には使用できません。

Linux+ V8のドキュメントでは、docker runコマンドは、管理者がイメージからコンテナをインスタンス化して操作する際に使用する主要なコマンドであると強調されています。このコマンドは、テスト、開発、トラブルシューティングのワークフローでよく使用されます。

質問: **86**

ユーザーはコンテナ内で実行されているアプリケーションにアクセスできません。管理者はコンテナが実行されているかどうかを確認したいと考えています。管理者はどのコマンドを使用すべきでしょうか？
A. docker start
B. docker ps
C. docker run
D. Dockerイメージ
正解: (正解を表示します)
docker psコマンドは、実行中のすべてのコンテナを一覧表示し、管理者がアプリケーションのコンテナがアクティブかどうかを確認できるようにします。

質問: **87**
次のファイルシステムのうち、非永続的または揮発性のデータを含むものはどれですか？
A. /boot
B. /usr
C. /proc
D. /where
正解: (正解を表示します)
Linuxファイルシステムとその目的を理解することは、Linux+ V8の目標に概説されている基本的なシステム管理スキルです。挙げられているオプションの中で、/procは非永続的で揮発性のデータを格納するファイルシステムです。
/proc ファイルシステムは、完全にメモリ上に存在し、Linux カーネルによって動的に生成される仮想ファイルシステムです。ディスク上にデータを保存せず、システムの再起動後も保持されません。その代わりに、/proc は実行中のプロセス、カーネルパラメータ、システムメモリ、CPU 統計、ハードウェアの状態に関するリアルタイム情報を提供します。/proc 内のファイルはカーネルデータ構造を表し、システムの動作に伴って常に変化します。
その他のファイルシステムには、ディスク上に永続的に保存されるデータが含まれています。/boot には、システムの起動に不可欠なブートローダーファイルとカーネルイメージが格納されます。/usr には、ユーザーアプリケーション、ライブラリ、ドキュメントなど、すべて永続的に保存されるデータが格納されます。/var には、ログ、スプールファイル、キャッシュなどの可変データが格納されます。これらのデータは頻繁に変更される可能性がありますが、ディスク上に永続的に保存されます。
Linux+ V8のドキュメントでは、/procは主にシステム監視とチューニングに使用されることが強調されています。
管理者は、sysctlなどのツールを使用してプロセスの詳細を調べたり、カーネルパラメータを変更したりするために、/procにアクセスすることがよくあります。/procの内容は実行時に生成され、再起動時に消去されるため、/procは非永続的または揮発性であると分類されます。
したがって、正解はCです。/proc。

質問: **88**
シミュレーション2
経験の浅いシステム管理者が誤ってLVMボリュームを削除してしまった。
説明書
パート1
出力結果を確認し、適切なコマンドを選択して復旧プロセスを開始してください。
パート2
出力結果を確認し、適切なコマンドを選択して復旧プロセスを続行してください。
パート3
出力結果を確認し、適切なコマンドを選択して復旧プロセスを完了し、基となるデータにアクセスしてください。
シミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。

Part 1 | Part 2 | Part 3

Commands

```
[root@comptiasim ~]# df -h
[root@comptiasim ~]# ls -l /dev | grep -v tty
[root@comptiasim ~]# ls -l /etc/lvm/archive
[root@comptiasim ~]# pvdisplay
[root@comptiasim ~]# pvs
[root@comptiasim ~]# vgcfgrestore --list vg01
[root@comptiasim ~]# vgdisplay
[root@comptiasim ~]# vgs
```

```
[root@comptiasim ~]# vgs
  VG   #PV #LV #SN Attr   VSize   VFree
  vg01   1   0   0 wz--n- <10.00g <10.00g
```

Select the appropriate command to begin the recovery process.

```
[root@comptiasim ~]#
```

Select command
lvchange -a n /dev/vg01/lv01
lvchange -a y /dev/vg01/lv01
vgcfgrestore vg01 -f /etc/lvm/archive/vg01_00002-966141411.vg
pvscan
lvconvert --type mirror lv01
vgcfgrestore vg01 -f /etc/lvm/backup/vg01
vgcfgrestore vg01 -t -M /etc/lvm/archive/vg01_00001-810050352.vg

Part 1 ● | Part 2 ● | Part 3 ●

Commands

```
[root@comptiasim ~]# blkid
[root@comptiasim ~]# dmesg | tail -20
[root@comptiasim ~]# lsblk
[root@comptiasim ~]# ls /
[root@comptiasim ~]# lvdisplay
[root@comptiasim ~]# lvs
[root@comptiasim ~]# lvscan
[root@comptiasim ~]# pvs
[root@comptiasim ~]# vgs
```

```
[root@comptiasim ~]# blkid
/dev/xvda1: UUID="388a99ed-9486-4a46-aeb6-06eaf6c47675" TYPE="xfs"
/dev/xvdf: UUID="1uyvyk-Ffd0-RrYF-cYba-15zC-EHRZ-UW3UHm" TYPE="LVM2_member"
```

Select the appropriate command to continue the recovery process.

```
[root@comptiasim ~]#
```

Select command
mount /dev/vg01/lv01/ /important_data
pvchange -x y /dev/xvdf
lvchange -a n /dev/vg01/lv01
lvchange -a y /dev/vg01/lv01
lvextend -L +54 vg01/lv01 /dev/xvdf

Part 1 ● Part 2 ● Part 3 ✓

Commands

```
[root@comptiasim ~]# blkid
[root@comptiasim ~]# cat /etc/fstab
[root@comptiasim ~]# ls -l /dev/mapper/
[root@comptiasim ~]# ls -l /
[root@comptiasim ~]# lsblk
[root@comptiasim ~]# lvdisplay
[root@comptiasim ~]# lvscan
[root@comptiasim ~]# tail -f /var/log/messages
[root@comptiasim ~]# xfs_repair -n /dev/vg01/lv01
```

```
[root@comptiasim ~]# lsblk
NAME        MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda        202:0    0   8G  0 disk
└─xvda1     202:1    0   8G  0 part /
xvdf        202:80   0  10G  0 disk
└─vg01-lv01 253:0    0   9G  0 lvm
```

Select the appropriate command to complete the recovery process and access the underlying data.

```
[root@comptiasim ~]#
```

Select command
mount /important_data /dev/vg01/lv01
xfs_repair /dev/vg01/lv01
mount -a
xfs_mdrestore /dev/vg01 /important_data
lvscan -a

正解:

Part 1 ✓ | Part 2 ● | Part 3 ●

Commands

```
[root@comptiasim ~]# df -h
[root@comptiasim ~]# ls -l /dev | grep -v tty
[root@comptiasim ~]# ls -l /etc/lvm/archive
[root@comptiasim ~]# pvdisplay
[root@comptiasim ~]# pvs
[root@comptiasim ~]# vgcfgrestore --list vg01
[root@comptiasim ~]# vgdisplay
[root@comptiasim ~]# vgs
```

```
[root@comptiasim ~]# vgs
  VG   #PV #LV #SN Attr   VSize   VFree
  vg01   1   0   0 wz--n- <10.00g <10.00g
```

Select the appropriate command to begin the recovery process.

```
[root@comptiasim ~]#
```

Select command
lvchange -a n /dev/vg01/lv01
lvchange -a y /dev/vg01/lv01
vgcfgrestore vg01 -f /etc/lvm/archive/vg01_00002-966141411.vg
pvscan
lvconvert --type mirror lv01
vgcfgrestore vg01 -f /etc/lvm/backup/vg01
vgcfgrestore vg01 -t -M /etc/lvm/archive/vg01_00001-810050352.vg

LVMアーカイブからボリュームグループ（VG）構成を復元することで、VGメタデータが失われた後の復旧プロセスが開始されます。

Part 1 ● | Part 2 ● | Part 3 ●

Commands

```
[root@comptiasim ~]# blkid
[root@comptiasim ~]# dmesg | tail -20
[root@comptiasim ~]# lsblk
[root@comptiasim ~]# ls /
[root@comptiasim ~]# lvdisplay
[root@comptiasim ~]# lvs
[root@comptiasim ~]# lvscan
[root@comptiasim ~]# pvs
[root@comptiasim ~]# vgs
```

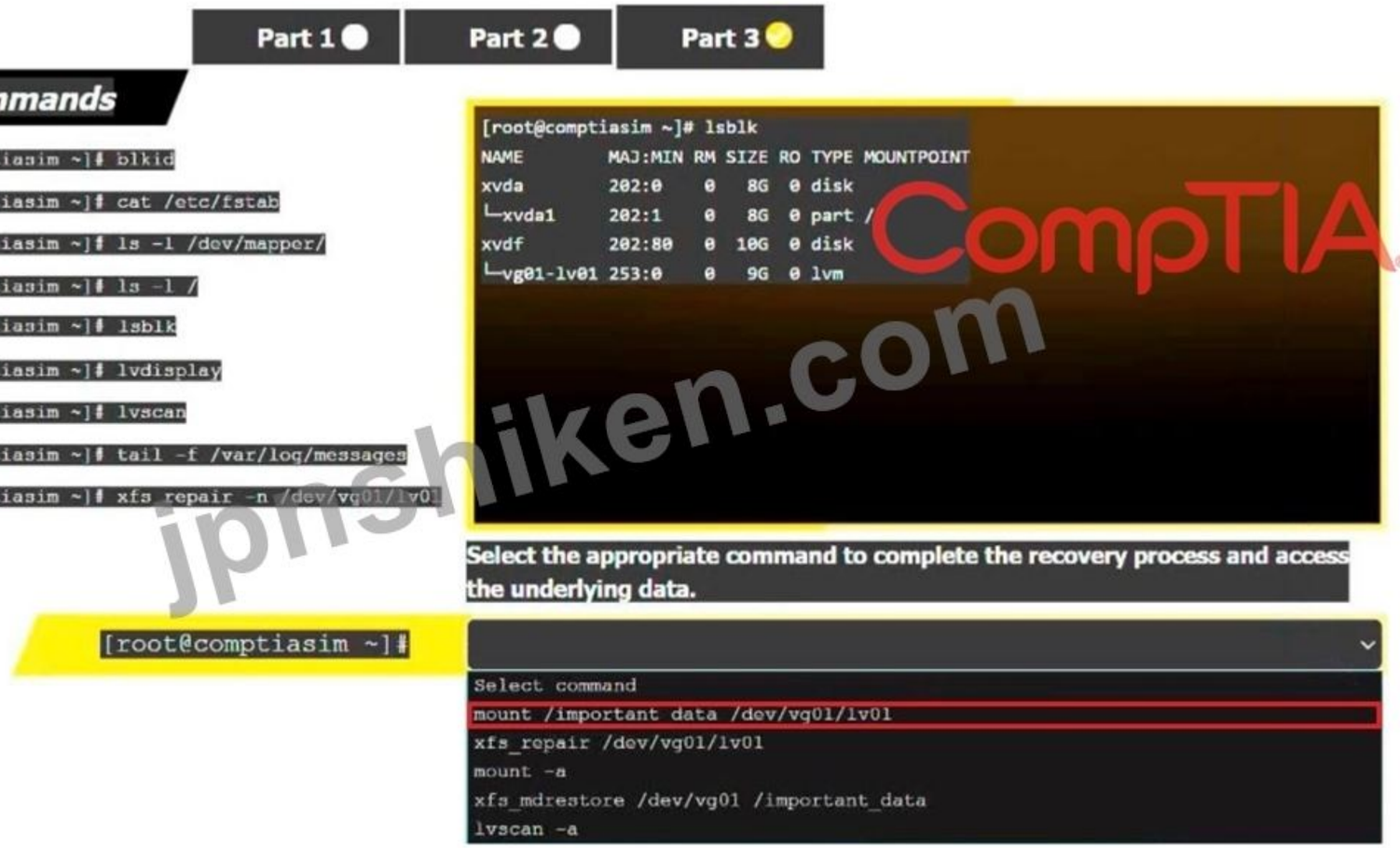
```
[root@comptiasim ~]# blkid
/dev/xvda1: UUID="388a99ed-9486-4a46-aeb6-06eaf6c47675" TYPE="xfs"
/dev/xvdf: UUID="1uyvyk-Ffd0-RrYF-cYba-l5zC-EHRZ-UW3UHm" TYPE="LVM2_member"
```

Select the appropriate command to continue the recovery process.

```
[root@comptiasim ~]#
```

```
Select command
mount /dev/vg01/lv01/ /important_data
pvchange -x y /dev/xvdf
lvchange -a n /dev/vg01/lv01
lvchange -a y /dev/vg01/lv01
lvextend -L +54 vg01/lv01 /dev/xvdf
```


VGメタデータを復元した後、論理ボリュームを再アクティブ化（ayオプション）して、システムからアクセスできるようにする必要があります。



論理ボリュームがアクティブになったら、それを/important_dataディレクトリにマウントすることでファイルシステムにアクセスできるようになり、復旧プロセスが完了します。

質問: **89**
アプリケーションの互換性の問題があるため、Python 3 の OpenSSL ライブラリはアップグレードしないでください。
システム管理者は、パッケージを最新バージョンに維持するために、以下のどのコマンドを使用すべきでしょうか？
A. dpkg --hold python3-openssl
B. apt set-selections python3-openssl
C. apt-mark hold python3-opensal
D. echo "python3-openssl > hold" |apt set-selections
正解: (正解を表示します)
このコマンドは、指定されたパッケージを保留状態にし、システムアップデート中にそのパッケージがアップグレードされるのを防ぎます。一方、他のパッケージは通常どおりアップデートされます。

質問: **90**
dmesg は以下のうちどれを表示しますか？
A. ログイン試行が間違っています

B. セッションが閉じられました」メッセージ
C. ウィンドウマネージャーの警告
D. USB機器の接続
正解: (正解を表示します)
dmesg（診断メッセージ）ユーティリティは、Linux+ V8におけるシステム管理およびハードウェアのトラブルシューティングに不可欠なツールです。これは、Linuxカーネルが起動プロセス中およびシステム実行中に生成するメッセージを含むカーネルリングバッファを表示するために使用されます。
カーネルリングバッファは、主にハードウェアの初期化、デバイスドライバの状態、およびシステムリソースに関連するイベントを記録します。USBドライブ、ネットワークカード、キーボードなどのハードウェアデバイスがシステムに接続されると、カーネルはそのイベントを検出し、詳細をログに記録します。たとえば、USBデバイスが接続されると、dmesgには製造元、デバイスID、および割り当てられたマウントポイントまたはデバイスノード（例/dev/sdb1）が表示されます。
その他のオプションは、通常、異なるサービスによって処理されるログに関するものです。
* 誤ったログイン試行 (オプション A) および セッションが閉じられました」メッセージ (オプション B) は、認証およびセキュリティ イベントです。これらは通常、sshd または pam によってログに記録され、/var/log/auth.log または /var/log に保存されます。
/安全な。
* ウィンドウマネージャの警告 (オプション C) は、グラフィカルユーザーインターフェイス (X11 または Wayland) に関連しており、デスクトップ固有のログファイルまたは systemd ジャーナルに保存されます。
CompTIA Linux+ のドキュメントによると、dmesg はハードウェア検出の確認とドライバの問題診断のための主要なツールです。カーネルとハードウェアのインターフェースに焦点を当てているため、選択肢の中では USB デバイス接続」が正解です。

質問: **91**
Linuxシステム上でリアルタイムに実行中のプロセスを表示するために使用できるコマンドは次のうちどれですか？
A. ps
B. トップ
C. df
D. 無料
正解: (正解を表示します)
正解はBです。topコマンドは、実行中のプロセスとシステムリソースの使用状況を動的かつリアルタイムに表示します。topコマンドは、CPU使用率、メモリ消費量、実行中のプロセス、負荷平均、システム稼働時間に関する情報を継続的に更新する、Linuxシステム監視に不可欠なユーティリティです。システム管理者は、パフォーマンス監視やトラブルシューティングに広く利用しています。
topコマンドを実行すると、アクティブなプロセスがリソース使用量（デフォルトでは通常CPU）順に並べられた全画面インターフェースが表示されます。定期的に更新されるため、管理者はリアルタイムで変化を監視できます。さらに、プロセスの並べ替え、プロセスの強制終了、出力のフィルタリングといった対話型機能も備えており、システム管理機能を強化します。
オプションA（ps）は、実行中のプロセスを一覧表示しますが、特定の時点のスナップショットしか提供しないため、誤りです。繰り返し実行したり、他のツールと組み合わせたりしない限り、動的に更新されることはありません。
選択肢C（df）は、実行中のプロセスではなく、ファイルシステムのディスク使用量を表示するため、誤りです。
選択肢D（空き）は、合計メモリ、使用済みメモリ、空きメモリなどのメモリ使用統計を表示するものの、プロセスレベルのアクティビティを表示しないため、誤りです。
Linux+の観点から見ると、topのようなツールを理解することは、システム管理の目的において非常に重要です。これにより、管理者はシステムの状態を監視し、リソースを大量に消費するプロセスを特定し、必要に応じて是正措置を講じることができます。リアルタイム監視は、パフォーマンスの問題を迅速に診断して解決する必要がある本番環境では特に重要です。

質問: **92**
Linuxシステムのハードウェアインベントリ全体を確認するには、管理者はどのコマンドを使用すべきでしょうか？
A. dmidecode
B. lsmod
C. dmesg
D. lscpu
正解: **A** (コメントを発表する)
ハードウェアインベントリとシステム情報の収集は、Linuxシステム管理における重要な責務であり、CompTIA Linux+ V8の目標にも明確に含まれています。記載されているコマンドの中で、dmidecodeは詳細なハードウェアインベントリ情報を取得するための最も包括的なツールです。
dmidecodeコマンドは、システムファームウェア（BIOSまたはUEFI）によって提供されるシステムのDMI（デスクトップ管理インターフェース）/SMBIOSテーブルからデータを直接読み取ります。マザーボードの詳細、BIOSバージョン、システムメーカー、CPUソケット、メモリスロット、インストール済みRAMモジュール、シリアル番号、資産タグなど、システムハードウェアコンポーネントに関する詳細情報を報告します。そのため、ハードウェアの完全なインベントリが必要な場合に最適なツールです。
他のオプションでは、部分的な情報または特定の情報しか得られません。lsmod は現在ロードされているカーネルモジュールの一覧を表示し、物理的なハードウェアインベントリは提供しません。dmesg はカーネルリングバッファメッセージを表示します。これにはハードウェア検出ログが含まれる場合がありますが、構造化された完全なインベントリデータではありません。lscpu は CPU アーキテクチャとプロセッサの詳細のみを報告し、システム全体のハードウェア情報は報告しません。
Linux+ V8のドキュメントでは、システムハードウェアの検出とインベントリ監査のための権威あるユーティリティとしてdmidecodeが挙げられています。これは、企業環境において、ドキュメント作成、トラブルシューティング、キャパシティプランニング、コンプライアンスレポート作成などに広く利用されています。
システムファームウェアから入手できる最も完全で信頼性の高いハードウェア情報を提供するため、正解はA. dmidecodeです。

質問: **93**
管理者がLinuxサーバーにログインしたところ、時計が37分進んでいることに気づきました。以下のコマンドのうち、この問題を解決するにはどれを使用すればよいでしょうか？
A. hwclock
B. ntpdate
C. timedatectl
D. ntpd -q
正解: **B** (コメントを発表する)
正確な抜粋に基づく包括的かつ詳細な説明：
ntpdateコマンドは、システムクロックをリモートNTPサーバーと即座に同期させ、大きな時刻ずれを修正します。これは、一度限りの時刻修正に最適です。
例えば：
バッシュ
コピー編集
ntpdate pool.ntp.org
その他の選択肢：
* A. hwclock はハードウェアクロックを読み取ったり設定したりしますが、ネットワーク時刻とは同期しません。
* C. timedatectl は時刻を手動で設定したり、時刻設定を管理したりできますが、リモート NTP サーバーとすぐに同期しません。
* D. ntpd -q も一度だけ時計を同期できますが、ntpdate は即時同期のために特別に設計されており、一度限りの修正にはより簡単です。
参照：
CompTIA Linux+ 学習ガイド：試験XK0-006、Sybex、第 5 章：「システム管理」、セクション：「時刻同期」 CompTIA Linux+ XK0-006 目標、ドメイン 1.0 :システム管理

質問: **94**
Linux 管理者が $HOME/.local/bin 内に新しいプログラムをインストールし、絶対パスを使用せずに実行しようとしています。このタスクを実行するには、管理者は次のうちどれを使用すべきでしょうか？

A. export PATH=PATH:$HOME/.local/bin
B. export $PATH=PATH:$HOME/.local/bin
C. export PATH=$PATH:$HOME/.local/bin
D. export $PATH=$PATH:$HOME/.local/bin
正解: **(**正解を表示します**)**
正解はCです。`export PATH=$PATH:$HOME/.local/bin`はディレクトリを正しく追加します。
既存のPATH環境変数に$HOME/.local/binを追加します。PATH変数は、ユーザーがコマンドのフルパスを指定せずに入力した際にシェルが検索するディレクトリのリストを定義します。PATHにディレクトリを追加することで、そのディレクトリ内の実行可能ファイルをコマンドラインから直接実行できるようになります。
この場合、管理者は$HOME/.local/binにプログラムをインストールしましたが、このディレクトリはすべてのシステムやユーザーのデフォルトのPATHに必ずしも含まれているとは限りません。export PATH=$PATH:$HOME/.local/binを使用することで、既存のPATHが維持され、新しいディレクトリが追加されます。$PATHを使用することで、以前に定義されたディレクトリへのアクセスが確保され、コロン :) は複数のディレクトリエントリを区切ります。
オプションAは、現在のPATH変数を参照する代わりに文字列 PATH」をそのまま代入しているため、コマンド検索が事実上機能しなくなるため、誤りです。
選択肢BとDは、$PATHに値を代入しようとしているため、構文的に誤りです。
環境変数は、ドル記号ではなく、その名前 PATHなど）を使用して指定する必要があります。
Linux+の観点から見ると、環境変数の管理はユーザーおよびシステム設定における基本的なスキルです。PATH変数を適切に設定することで、特にカスタムアプリケーションやユーザー固有のアプリケーションをインストールする際に、コマンドの効率的な実行と使いやすさが確保されます。永続性を確保するため、この変更は通常、~/.bashrcや~/.profileなどのシェル設定ファイルに追加されます。

質問: **95**
システム管理者がLinuxシステム内の既存のユーザーアカウントを再構成しています。管理者は myuser」をfinanceグループに追加するために、以下のどのコマンドを使用すべきでしょうか？
A. groupadd finance myuser
B. groupmod Finance myuser
C. useradd -g finance myuser
D. usermod -aG finance myuser
正解: **D (**コメントを発表する**)**
正確な抜粋に基づく包括的かつ詳細な説明：
既存のユーザー myuser）を既存のグループ finance）に追加する際に、他のグループから削除しない場合は、usermod -aG finance myuser というコマンドを使用します。-aG オプションは、指定された補助グループにユーザーを追加します。
その他の選択肢：
A) groupaddは新しいグループを作成するためのものであり、ユーザーをグループに追加するためのものではありません。
B) groupmodはグループのプロパティを変更するためのものであり、ユーザーのメンバーシップを変更するためのものではありません。
C). useraddは新規ユーザーを作成します。既存ユーザーには適用されません。
参照：
CompTIA Linux+ 学習ガイド: 試験 XK0-006、Sybex、第 6 章: ユーザーとグループの管理」、セクション: グループメンバーシップの変更」 CompTIA Linux+ XK0-006 目標、ドメイン 1.0: システム管理

質問: **96**
Linux管理者が2つのノード間でパスワードなしのSSH認証の設定を完了しました。しかし、テスト検証時にリモートホストからパスワードの入力を求められます。以下のログを参照してください。

```
-rw-------. 1 root root 588 Apr 3 2022 authorized_keys

avc: denied { read } for pid=xxxx comm="sshd" name="authorized_keys" dev="dm-5" ino=xxxx scontext=system_u:system_r:sshd_t:s0-s0:c0.c1023
tcontext=unconfined_u:object_r:home_root_t:s0 tclass=file
[...]

SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Max kernel policy version: 31
```


以下のうち、この問題の最も可能性の高い原因はどれですか？

A. SELinux ポリシーが unconf ined_u コンテキストを誤ってターゲットにしています。

B. 管理者が authorizedjceys ファイルを作成した後、SSHD を再起動するのを忘れていました。

C. authorized_keys ファイルに誤ったルート権限が割り当てられています。

D. authorized_keys ファイルに SELinux ポリシーに一致する正しいセキュリティ コンテキストがありません。

正解: **(**正解を表示します**)**

この問題は、CompTIA Linux+ V8 のセキュリティ分野における重要なトピックである SELinux の強制適用に直接関係しています。ログには、従来のファイル権限や SSH 設定の問題ではなく、SELinux のアクセス制御違反が原因で SSH キーベース認証が失敗していることが明確に示されています。

最も重要な手がかりは、sshd プロセスが authorized_keys ファイルへの読み取りアクセスを拒否されていることを示す AVC 拒否メッセージです。ファイルのセキュリティコンテキストは unconfined_u:object_r: と表示されます。

home_root_t:s0。特定のSELinuxポリシーの下では、SSHは、通常ssh_home_tである正しいSELinuxタイプでラベル付けされたauthorized_keysファイルのみを読み取ることが許可されます。

SELinuxは強制モードで動作しているため、標準的なUNIXパーミッションが正しくても、ポリシー規則に違反するアクセスは積極的にブロックします。authorized_keysファイルのファイルパーミッション（600）は許容範囲内ですが、SELinuxは従来のパーミッションのみに依存するわけではありません。想定されるSELinuxコンテキストと実際のコンテキストの不一致により、sshdはファイルにアクセスできず、SSHはパスワード認証にフォールバックします。

オプションDは根本原因を正しく特定しています。authorized_keysファイルに適切なSELinuxセキュリティコンテキストが設定されていないことが原因です。これはLinux+ V8におけるよくあるトラブルシューティングシナリオであり、restoreconなどのコマンドを使用して正しいコンテキストを復元するか、ファイルが適切なラベルの付いたホームディレクトリに存在することを確認することで解決するのが一般的です。

他の選択肢は誤りです。sshdを再起動してもSELinuxのラベル付けの問題は解決しません。ポリシー自体は意図どおりに機能しており、ファイル所有権だけではSELinuxのアクセス制御を上書きすることはできません。

Linux+ V8のドキュメントでは、SELinuxによるアクセス拒否は、セキュリティ制御を弱めるのではなく、ファイルコンテキストを修正することで対処する必要があると強調されています。したがって、正解はDです。

質問: **97**

LinuxユーザーがWindows Active Directoryドメインに対して認証を行う必要があります。ドメイン構成の詳細が含まれている構成ファイルは、次のうちどれですか？

A. sssd.conf

B. krb5.conf

C. pam.conf

D. smb.conf

正解: **(**正解を表示します**)**

現代のLinuxエンタープライズ環境では、Windows Active Directory（AD）との統合は、集中型ID管理のための一般的な要件となっています。CompTIA Linux+ V8によると、ADやLDAPなどのリモートプロバイダに対する認証と認可を処理する推奨方法は、システムセキュリティサービスデーモン（SSSD）です。
sssd.conf ファイル（通常は /etc/sssd/ にあります）は、このサービスの主要な設定ファイルです。このファイルには、以下のような重要な「ドメイン設定の詳細」が含まれています。
* ADドメイン名。
* 認証プロバイダー（例id_provider = ad）。
* ドメインコントローラーのURI。
* オフラインログイン用のキャッシュ設定。
SSSDは、LinuxシステムとADドメイン間の通信を管理する統一インターフェースを提供し、認証スタックを簡素化します。
その他のオプションは関連していますが、主要なドメイン構成ファイルとしては機能しません。krb5.conf（オプションB）は、基盤となるチケットベースの認証に使用されるKerberosを構成しますが、SSSDはこれらの詳細を自動的に管理するか、サブコンポーネントとしてKerberosに依存していることがよくあります。pam.conf（オプションC）は、プラグイン可能な認証モジュールスタックを管理しますが、ドメイン固有の詳細は保存しません。
smb.conf（オプションD）はSambaの設定ファイルです。Sambaはファイル共有に使用され、ドメインへの参加を支援することができますが、sssd.confはLinux+V8環境における最新のID統合の詳細を確認するための検証済みの場所です。

質問**: 98**
Linuxシステムの動作中に、以下のエラーが表示されます。
カーネルパニック - 同期していません: 致命的なマシンチェック
Pid: 0、comm: swapper、Tainted: GM
通話追跡：
...
mce_パニック
マシンチェックを実行する
この問題の最も可能性の高い原因は次のうちどれですか？
A. ファイルシステムの破損
B. ハードウェア障害（CPUまたはメモリ）
C. ブートローダーの設定ミス
D. ファイル権限が正しくありません
正解: (正解を表示します)
正解はBです。ハードウェア障害（CPUまたはメモリ）エラーメッセージは明示的に参照しています。
「マシンチェック例外（MCE）」とは、CPUによって検出されたハードウェアレベルのエラーです。「カーネルパニック - 同期していません: 致命的なマシンチェック」という行は、カーネルが回復不能な重大なハードウェア障害に遭遇し、さらなる損傷やデータ破損を防ぐためにシステムを停止したことを示しています。
マシンチェック例外は、CPUがキャッシュ障害、バスエラー、メモリ破損などの内部エラーを検出した際に発生します。これらのエラーは通常、プロセッサ、RAM、マザーボードなどのハードウェアコンポーネントの不具合、あるいは過熱問題に関連しています。コールトレースにmce_panicやdo_machine_checkといった関数が存在することは、カーネルがハードウェアレベルの障害に対応していることをさらに裏付けています。
オプションA（「ファイルシステムの破損」）は誤りです。ファイルシステムの問題は通常、I/Oエラーやマウント失敗を引き起こし、マシンチェック例外は発生させません。
オプションC（「ブートローダーの設定ミス」）は誤りです。ブートローダーの問題は通常、ハードウェア関連のトレースを伴う実行時カーネルパニックを引き起こすのではなく、システムの正常な起動を妨げるからです。
オプションD（「ファイル権限の誤り」）は誤りです。権限の問題は、カーネルレベルの操作ではなく、ユーザーアクセスとアプリケーションの動作に影響します。
Linux+のトラブルシューティングの観点から、マシンチェックに関連するカーネルパニックにはハードウェア診断が必要です。管理者は、システムログ（/var/log/messages、dmesg）を確認し、メモリテスト（memtest86+など）を実行し、CPUの状態をチェックし、システムの冷却状態を確認する必要があります。問題を解決するには、ハードウェアの交換またはファームウェアのアップデートが必要になる場合があ

ります。

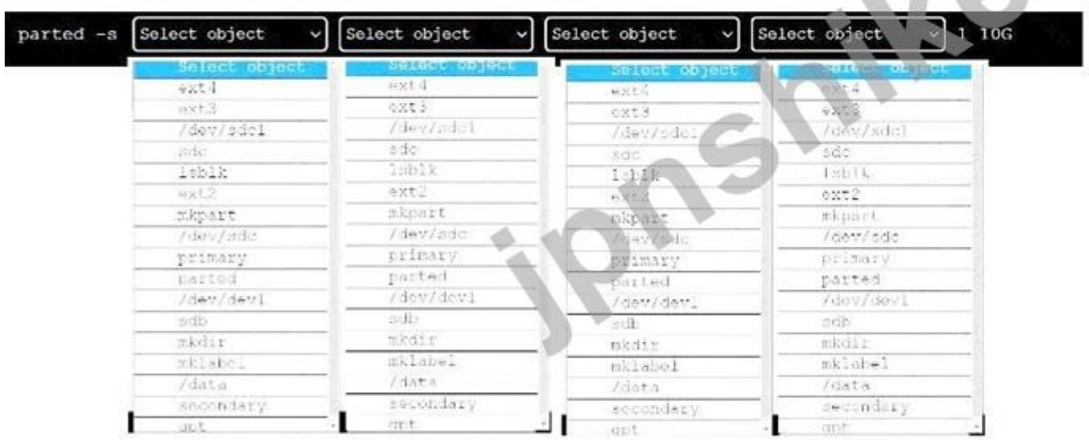
質問: **99**
管理者は、myFile という名前のファイルを検索し、少なくとも 5 文字を含む文字列のすべての出現箇所を探します。ただし、2 番目と 5 番目の文字は i であり、3 番目の文字は b ではないものとします。管理者が目的の結果を得るには、次のうちどのコマンドを実行すればよいでしょうか？
A. grep .a*^b-.a myFile
B. grep .a., [a] myFile
C. grepa^b*a myFile
D. grep .i[^b].i myFile
正解: **D (**コメントを発表する**)**
正規表現を用いたパターンマッチングは、CompTIA Linux+ V8で取り上げられる重要なトラブルシューティングおよびテキスト処理スキルです。grepコマンドと正規表現を組み合わせることで、管理者はファイル内の複雑な文字列パターンを検索できます。
要件には以下が規定されている。
* 文字列は少なくとも5文字以上でなければなりません
* 文字2は
* 文字3はbであってはならない
* 文字5は
これらの条件を満たすための正しい正規表現の構造は次のとおりです。
* . # 任意の文字（位置1）
* i # リテラル i (位置 2)
* [^b] # b以外の任意の文字（位置3）
* . # 任意の文字 4番目の位置）
* i # リテラル i (位置 5)
その結果、次の式が得られます。
i[^b].i
オプションDのgrep .i[^b].i myFileは、このロジックを正しく実装しています。位置一致を保証し、Linux+ V8正規表現の目標で明示的に扱われている否定文字クラス [^b] を使用して不要な文字を除外します。
その他のオプションには、無効な正規表現や形式が正しくない正規表現が含まれており、位置指定や除外の要件を満たしていません。Linux+ V8 では、ログファイルや設定データのトラブルシューティングを行う際に、アンカー、文字クラス、位置ベースのマッチングを理解することを重視しています。
したがって、正解はDです。

質問: **100**
次のうち、ウェブフックを最も正確に説明しているのはどれですか？
A. ウェブサーバー通信のための認証方法
B. ネットワーク機器監視のためのSNMPベースのAPI
C. システム間で機密情報を伝送する手段
D. HTTPベースのコールバック関数
正解: **(**正解を表示します**)**
Webhookは、Linux+ V8の目標で重視されている自動化およびDevOpsワークフローで一般的に使用されています。Webhookは、特定のイベントが発生した際に、あるシステムが別のシステムに通知できるようにするHTTPベースのコールバックメカニズムと説明するのが最適です。
選択肢Dは、Webhookを正しく定義しています。Webhookを使用すると、APIを定期的にポーリングする代わりに、イベントが発生したときに、アプリケーションが事前に定義されたURLにHTTPリクエスト（通

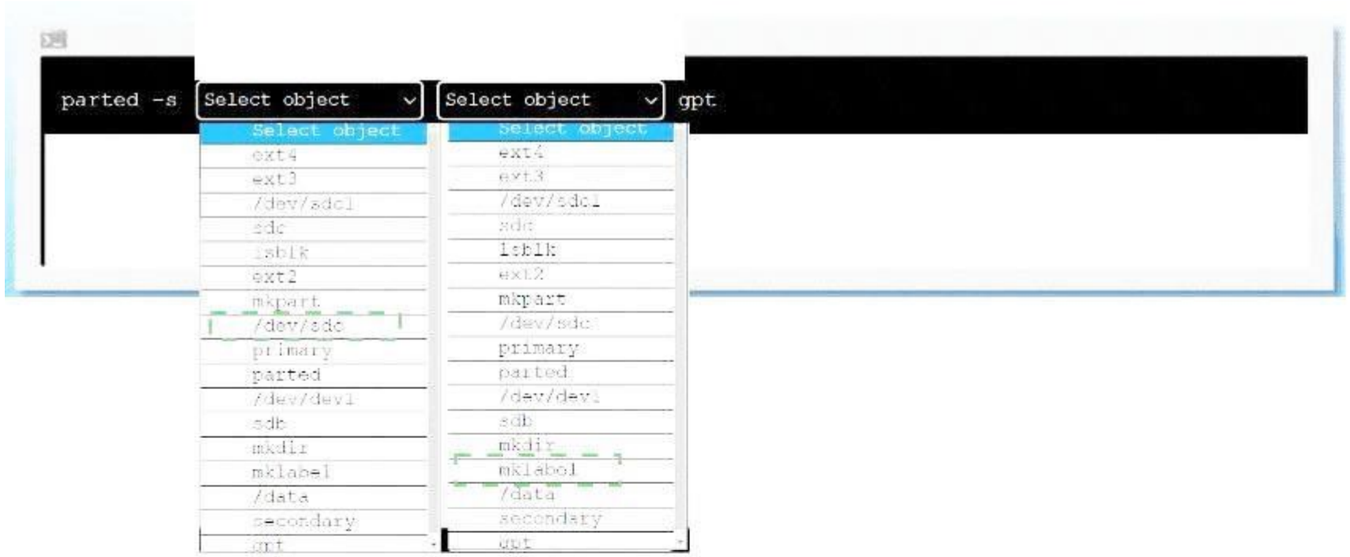
常はPOST）を自動的に送信できます。これにより、Webhookは効率的でイベント駆動型となり、自動化パイプライン、CI/CDシステム、および監視統合に最適です。
他の選択肢は誤りです。選択肢Aは、Webhookと認証メカニズムを混同しています。選択肢Bは、WebhookをSNMPと誤って関連付けていますが、SNMPは別のプロトコルです。選択肢Cは、Webhookは本来機密データの送信を目的として設計されておらず、TLSや認証などの追加のセキュリティ対策が必要となるため、誤解を招きます。
Linux+ V8のドキュメントでは、自動化環境における重要な統合方法としてWebhookが強調されており、これによりシステムは変更やトリガーにリアルタイムで対応できるようになります。
したがって、正解はDです。

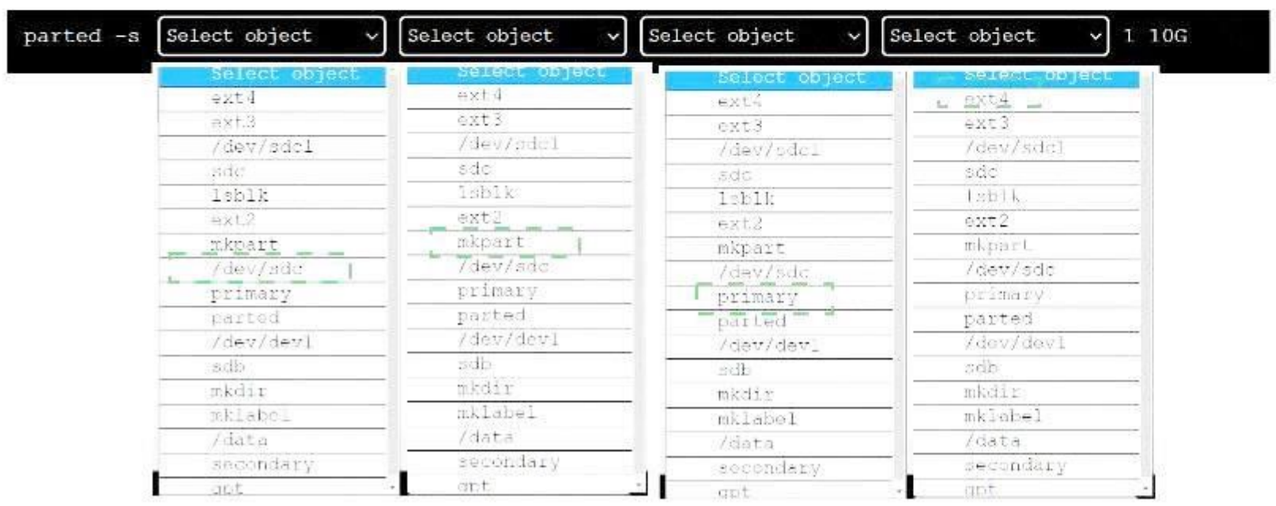
質問: **101**
システム管理者が /home/ ディレクトリのバックアップコピーを作成しています。以下のコマンドのうち、ディレクトリのアーカイブと圧縮を同時に実行できるのはどれですか？
A. cpio -o /backups/home.tar.xz /home/
B. rsync -z /backups/home.tar.xz /home/
C. tar -cJf /backups/home.tar.xz /home/
D. dd of=/backups/home.tar.xz if=/home/
正解: **(**正解を表示します**)**
バックアップの作成はLinuxシステム管理における重要な責務であり、Linux+ V8の目標ではアーカイブおよび圧縮ツールの適切な使用が重視されています。tarユーティリティはアーカイブファイルを作成するための標準的なLinuxツールであり、さまざまなオプションによる圧縮もサポートしています。
コマンド tar -cJf /backups/home.tar.xz /home/ は、アーカイブと圧縮を単一のステップで正しく組み合わせます。-c オプションは新しいアーカイブを作成し、-J オプションは XZ 圧縮を指定し、-f オプションは管理者が出力ファイル名を定義できるようにします。これにより、/home/ ディレクトリ全体が圧縮されたアーカイブが作成され、ストレージと転送に効率的です。
他の選択肢は誤りです。cpioはアーカイブツールですが、追加のコマンドやパイプラインなしでは圧縮は実行しません。rsync -zは転送中にデータを圧縮しますが、アーカイブファイルは作成しません。
ddコマンドは生データの低レベルコピーを実行するため、ディレクトリベースのバックアップには適していません。
Linux+ V8のドキュメントでは、tarは柔軟性、信頼性、および複数の圧縮アルゴリズムのサポートといった利点から、ファイルシステムのバックアップに最適なユーティリティとして挙げられています。したがって、正解はCです。

質問: **102**
Linuxシステムに新しいドライブが追加されました。提供された環境とトークンを使用して、以下のタスクを完了してください。
* 適切なデバイスラベルを作成する。
* 新しいパーティションにext4ファイルシステムをフォーマットして作成します。
現在の作業ディレクトリは / です。

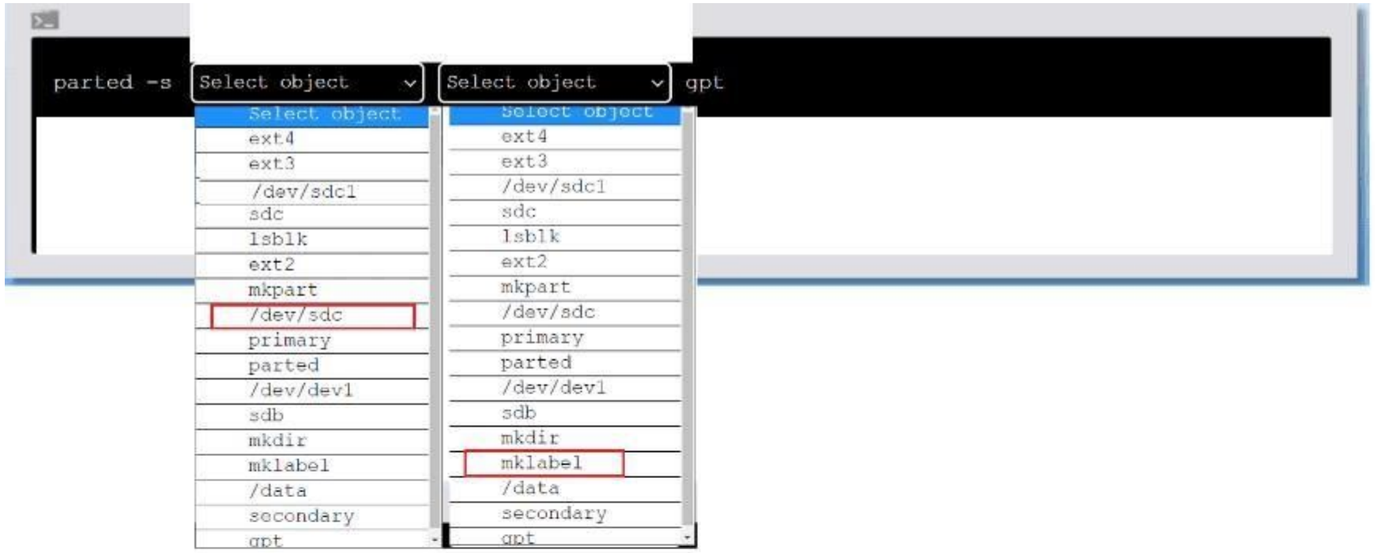


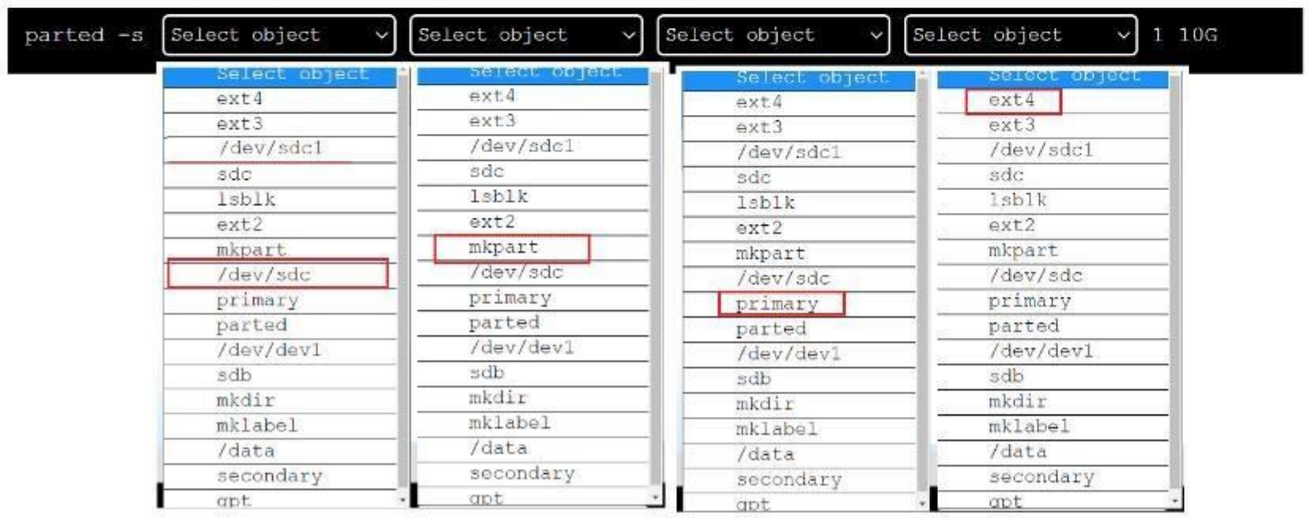
正解:

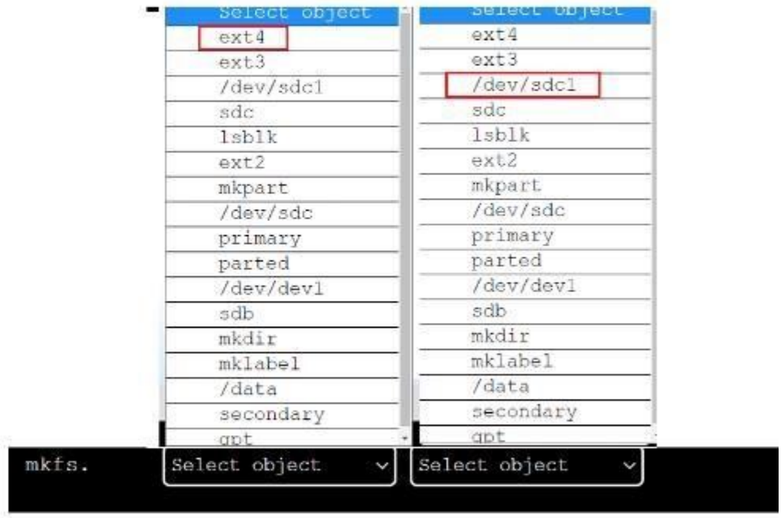




Explanation:







適切なデバイスラベルを作成し、新しいパーティションにext4ファイルシステムをフォーマットして作成するには、以下のコマンドを使用できます。
新しいドライブ /dev/sdc に GPT (GUID パーティション テーブル) ラベルを作成するには、parted コマンドに -s オプション (スクリプト モード用)、デバイス名 (/dev/sdc)、mklabel コマンド、およびラベル タイプ (gpt) を指定します。コマンドは次のとおりです。
parted -s /dev/sdc mklabel gpt
新しいドライブ /dev/sdc に 10 GB のプライマリパーティションを作成するには、parted コマンドに -s オプション、デバイス名 (/dev/sdc)、mkpart コマンド、パーティションタイプ (プライマリ)、ファイルシステムタイプ (ext4)、およびパーティションの開始点と終了点 (1G と 10G) を指定します。コマンドは次のとおりです。
parted -s /dev/sdc mkpart primary ext4 1 10G
新しいパーティション /dev/sdc1 に ext4 ファイルシステムをフォーマットして作成するには、mkfs コマンドにファイルシステムの種類 (ext4) とデバイス名 (/dev/sdc1) を指定します。コマンドは次のとおりです。
mkfs.ext4 /dev/sdc1
lsblkコマンドを使用すると、すべてのブロックデバイスとそのプロパティが一覧表示されるため、新しいパーティションとファイルシステムが作成されたことを確認できます。
質問: **103**

SSH認証中にユーザーの公開鍵がどのように使用されるかを説明しているのは、次のうちどれですか？
A. SSH認証中にパスワードをハッシュ化するためにユーザーの公開鍵が使用されます。
B. ユーザーの公開鍵が認証済み鍵のリストと照合されます。一致した場合、ユーザーはログインを許可されます。
C. サーバーへのアクセスを許可するために、パスワードの代わりにユーザーの公開鍵が使用されます。
D. ユーザーの公開鍵は、クライアントとサーバー間の通信を暗号化するために使用されます。
正解: **(**正解を表示します**)**
正確な抜粋からの包括的かつ詳細な説明：
SSH公開鍵認証中、サーバーはユーザーの公開鍵が~/.sshに存在するかどうかを確認します。
/authorized_keys ファイル。キーが見つかった場合、サーバーはそれを使用して、対応する秘密鍵でのみ応答できるチャレンジを送信することで、ユーザーの身元を確認します。このプロセスでは、パスワードのハッシュ化や、通信ストリームの暗号化に公開鍵を直接使用することはありません。代わりに、公開鍵は認証の参照としてのみ使用されます。
参照：
CompTIA Linux+ 学習ガイド：試験XK0-006、Sybex、第 11 章：「Linux のセキュリティ保護」、セクション：「SSH キーベース認証」CompTIA Linux+ XK0-006 目標、ドメイン 3.0 :セキュリティ

質問: **104**
システム管理者は、NetworkManagerservice の起動にかかった時間を確認したいと考えています。以下のコマンドのうち、この目的を達成できるのはどれですか？
A. resolvectl
B. journalctl
C. systemctl daemon-reload
D. systemd-analyze blame
正解: **D (**コメントを発表する**)**
systemd-analyze blameコマンドは、systemdによって管理されている各サービスの起動時間を表示するため、管理者はNetworkManager またはその他のサービス）の起動にかかった時間を確認できます。

質問: **105**
システム起動後、X Window System GUIのログイン画面が表示されません。システム起動プロセス中にGUIが起動するようにするには、次のうちどのコマンドを使用すればよいでしょうか？
A. systemctl isolate graphical.target
B. systemctl unmask xwindow.service
C. systemctl enable xwindow.service
D. systemctl set-default graphical.target
正解: **(**正解を表示します**)**
デフォルトのターゲットを graphical.target に設定すると、systemd は起動時にグラフィカルインターフェイスを起動します。コマンド systemctl set-default graphical.target を実行すると、起動時に GUI ログイン画面が自動的に表示されます。

質問: **106**
システム管理者は、新しいDNSサーバーのIPアドレスを設定する必要があります。この作業を完了するために、管理者は次のどのファイルを変更する必要がありますか？
A. /etc/whois.conf
B. /etc/resolv.conf
C. /etc/nsswitch.conf
D. /etc/dnsmasq.conf
正解: **(**正解を表示します**)**
/etc/resolv.conf ファイルは、ホスト名の解決にシステムが使用すべき DNS サーバーの IP アドレスなど、DNS リゾルバの設定を定義します。

質問: **107**
次のAnsibleコンポーネントのうち、グループと個々のホストを定義するために使用され、各ホストまたはグループに固有の変数を含めることができるのはどれですか？
A. ハンドラー
B. モジュール
C. プレイブック
D. 在庫
正解: **D** (コメントを発表する)

質問: **108**
システム管理者が新しいセキュアなWebサーバーを導入しようとしているが、起動に問題が発生している。
管理者は以下の出力結果を確認します。

```
# systemctl status -l httpd
httpd.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
Active: failed (Result: exit-code) since Tue 2024-07-09 12:30:05 EDT; 2min 30s ago
Docs: man:httpd.service(8)
Process: 12233 ExecReload=/usr/sbin/httpd $OPTIONS -k graceful (code=exited, status=0/SUCCESS)
[...]
Jul 09 12:30:05 node.comptia.com systemd[1]: httpd.service: Succeeded.
Jul 09 12:30:05 node.comptia.com systemd[1]: Stopped The Apache HTTP Server.
Jul 09 12:30:05 node.comptia.com systemd[1]: Starting The Apache HTTP Server...
Jul 09 12:30:05 node.comptia.com httpd[12233]: (13)Permission denied: AH00072: make_sock: could not bind to address
[::]:1234

# getenforce
Enforcing

# semanage port -l
[...]
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t tcp 5988

# getsebool -a
[...]
httpd_can_network_connect --> on
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> on
```


以下のコマンドのうち、セキュリティのベストプラクティスに従いながらこの問題を解決するものはどれですか？
A. setsebool -P http_port_t 1234

B. setenforce 0
C. semarage -a -t http_port_t -p tcp 1234
D. systemctl unmask httpd
正解: **(**正解を表示します**)**
Web サーバーは SELinux を強制モードで実行しており、そのポートが HTTP サービス用にラベル付けされていないため、Apache は TCP ポート 1234 にバインドする権限を拒否されています。
SELinux の http_port_t タイプを使用すると、セキュリティのベストプラクティスに従い、SELinux の強制設定を維持しながら Apache がポートにバインドできるようになります。