CompTIA.220-1102J.v2025-05-05.q379

試験コード:	220-1102J
試験名称:	CompTIA A+ Certification Exam: Core 2 (220-1102日本語版)
認定資格:	CompTIA
無料問題数:	379
バージョン:	v2025-05-05
アクセス数:	1282
ページビュー数:	3790
https://www.jpnpdf.com/CompTIA.220-1102J.v2025-05-05.q379-mondaishu.html	

最新問題: **1**
紛失または盗難にあったモバイル デバイスでデータが回復不可能であることを保証するのは次のどれですか。
A. デバイスの暗号化
B. リモートワイプ
C. データのバックアップ
D. 指紋リーダー
Answer: B (メーッセージを残す**)**
To ensure data is unrecoverable on a lost or stolen mobile device, the best solution is:
* Remote wipe: This feature allows the device owner or IT administrator to remotely erase all data on the device, ensuring that it cannot be recovered by unauthorized users.
* Device encryption: While important for protecting data, encryption alone does not remove data from the device.
* Data backup: Ensures data is saved elsewhere but does not make it unrecoverable on the lost or stolen device.
* Fingerprint reader: Provides security for accessing the device but does not affect data recovery if the device is compromised.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.7: Explain common methods for securing mobile and embedded devices.
Mobile device security practices documentation.

最新問題: **2**
会社が新しい SOHO ルーターを設置した後、顧客は会社がホストする公開 Web サイトにアクセスできなくなりました。顧客が Web サイトにアクセスできる可能性が最も高いのは、次のうちどれですか?
A. ポートフォワーディング
B. ファームウェアのアップデート
C. IP フィルタリング
D. コンテンツ フィルタリング
Answer: B (メーッセージを残す**)**
If customers are unable to access the company-hosted public website after installing a new SOHO router, the company should check for firmware updates1. Firmware updates can fix bugs and compatibility issues that may be preventing customers from accessing the website1. The company should also ensure that the router is properly configured to allow traffic to the website1. If the router is blocking traffic to the website, the company should configure the router to allow traffic to the website1.

最新問題: **3**
管理者は、単一のワークステーションの次のコンポーネントをバックアップする必要があります。
※オペレーティングシステムのインストール
*アプリケーション
*ユーザープロファイル
*システム設定
ワークステーションが適切にバックアップされていることを確認するために、管理者は次のバックアップ方法のうちどれを使用できますか?
A. 差動
B. 画像
C. 合成
D. アーカイブ
Answer: B (メーッセージを残す**)**
An image backup captures a complete snapshot of the entire system at a specific point in time, including the operating system, installed applications, user profiles, and system settings. This method is most suitable for backing up the components listed in the question because it ensures that every aspect of the workstation, from the core OS to individual user settings, is preserved and can be restored in its entirety. This is crucial for quickly recovering a system to a fully operational state after a failure or when migrating to new hardware.
Other methods like differential, synthetic, and archive backups do not provide the comprehensive one-step restoration capability that an image backup offers for the complete system recovery.

最新問題: **4**
ある企業は最近、悪意のあるソフトウェアを含む USB ドライブがワークステーションにマルウェアを密かにインストールできるというセキュリティ インシデントを経験しました。このインシデントの再発を防ぐために、次のアクションのうちどれを実行する必要がありますか? (2 つ選択してください)。
A. ホストベースの IDS をインストールします。
B. ログイン回数を制限します。
C. BIOS パスワードを有効にします。
D. パスワードの複雑さを更新します。
E. 自動実行を無効にします。
F. ウイルス対策定義を更新します。
G. ユーザーの権限を制限します。
Answer: E,G (メーッセージを残す**)**
AutoRun is a feature of Windows that automatically executes a program or file when a removable media such as a USB drive is inserted into the computer. Disabling AutoRun can prevent a USB drive containing malicious software from covertly installing malware on a workstation, as it would require the user to manually open the drive and run the file. Restricting user permissions can also prevent a USB drive containing malicious software from covertly installing malware on a workstation, as it would limit the user's ability to execute or install unauthorized programs or files. Installing a host-based IDS, restricting log-in times, enabling a BIOS password, updating the password complexity, and updating the antivirus definitions are not actions that can directly prevent this incident from happening again.

最新問題: **5**
次のシナリオのうち、リモート ワイプ機能が使用される可能性が最も高いのはどれですか? (2 つ選択してください)。
A. 新しい IT ポリシーでは、ユーザーにロック画面の PIN を設定することが求められています。
B. ユーザーは海外におり、対応する海外 SIM カードを使用したいと考えています。
C. ユーザーが電話機を家に置き忘れたため、子供が電話機にアクセスできないようにしたいと考えています。
D. ユーザーが誤って携帯電話会社のアップグレードのために会社の電話を下取りに出しました。
E. ユーザーが劇場で観劇した後、電話機を見つけることができません。

F. ユーザーがタクシーの中に携帯電話を忘れたため、運転手が会社に電話してデバイスを返してもらいました。
Answer: (解答を表示する**)**
Remote wipe capabilities are used to erase all data on a mobile device remotely. This can be useful in situations where a device is lost or stolen, or when sensitive data needs to be removed from a device. Remote wipe capabilities are most likely to be used in the following scenarios:
E:A user cannot locate the phone after attending a play at a theater. F. A user forgot the phone in a taxi, and the driver called the company to return the device1 In scenario E, remote wipe capabilities would be used to prevent unauthorized access to the device and to protect sensitive data. In scenario F, remote wipe capabilities would be used to erase all data on the device before it is returned to the user.

最新問題**: 6**
ユーザーがメール内のリンクをクリックすると、カーソルが勝手に動き始めます。技術者は、ファイル エクスプローラーが開いており、データがローカル ドライブから不明なクラウド ストレージの場所にコピーされていることに気づきました。
技術者が最初に行うべきことは次のうちどれですか?
A. 報告された症状を調査します。
B. マルウェア対策ソフトウェアを実行します。
C. 危険なリンクについてユーザーを教育します。
D. ワークステーションを隔離します。
Answer: D (メーッセージを残す**)**
When a user's cursor is moving on its own and unauthorized data transfer is occurring, the first step a technician should take is to Quarantine the workstation. This involves isolating the affected system from the network to prevent the spread of malware or unauthorized access to other parts of the network. Quarantining helps in containing the threat and provides a safe environment to investigate and remediate the issue without risking further contamination or data loss.

最新問題**: 7**
ユーザーのラップトップは、カバーを閉じるたびにシャットダウンするため、作業が頻繁に中断されます。ヘルプデスクのスペシャリストは、この問題を解決するために次のどれを実行する必要がありますか?
A. スリープ設定を構成します。
B. 休止状態を無効にします。
C. 電源プランを編集します。
D. 高速スタートアップをオンにします。
Answer: C (メーッセージを残す**)**
When a user's laptop shuts down every time the lid is closed, it typically means that the power settings are configured to put the laptop into a shutdown state when the lid is closed. To remediate this issue:
* Edit the power plan: This involves changing the settings for what happens when the laptop lid is closed.
* Go to Control Panel > Hardware and Sound > Power Options.
* Click on "Choose what closing the lid does."
* Change the settings for "When I close the lid" to either "Sleep" or "Do nothing" instead of "Shut down."
* Configure the sleep settings: While similar to editing the power plan, this option specifically adjusts the sleep settings rather than the overall power plan settings.
* Disable hibernation: This is a less direct solution but could be considered if the laptop was set to hibernate and then experiencing issues.
* Turn on fast startup: This setting affects how quickly the computer starts up from a shutdown, but it does not directly address the issue of what happens when the lid is closed.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 1.5: Given a scenario, use the appropriate Microsoft Windows settings.
Windows power management documentation.

最新問題: **8**
Android モバイル デバイスの起動に時間がかかり、起動時にすべてのアプリケーションがクラッシュするとユーザーが報告しました。ユーザーはサードパーティの Web サイトからアプリケーションをインストールしました。問題を診断するには、技術者が次のどの手順を実行する必要がありますか?
A. システムでマルウェアをスキャンします。
B. Web ブラウザのキャッシュをクリアします。
C. デバイスを MDM システムに登録します。
D. アプリケーションと OS の互換性を確認します。
Answer: A (メーッセージを残す**)**
When an Android device experiences slow boot times and application crashes after installing apps from a third-party website, scanning the system for malware is a critical first step. Third-party sources can often host malicious software that can compromise device performance and security. A malware scan can identify and remove such threats, potentially resolving the performance issues and application instability. Clearing the web browser cache, enrolling the device in an MDM system, and confirming app compatibility are useful steps but do not address the immediate concern of potential malware introduced by third-party app installations.

最新問題: **9**
悪意のあるユーザーが、会社の Web サイト上のフィールドに特定のコマンドを入力することにより、Web サイトのユーザー データベース全体をエクスポートすることができました。悪意のあるユーザーがデータを抽出するために悪用した可能性が最も高いのは次のうちどれですか?
A. クロスサイト スクリプティング
B. SQL インジェクション
C. ブルートフォース攻撃
D. DDoS 攻撃
Answer: B (メーッセージを残す**)**
SQL injection is a type of attack that takes advantage of vulnerabilities in a web application's database query software, allowing an attacker to send malicious SQL commands through the application to the database.
These commands can manipulate the database and can lead to unauthorized data access or manipulation.
SQL injection:In the scenario described, the malicious user was able to export an entire website's user database by entering specific commands into a field on the company's website, which is a classic example of an SQL injection attack. This type of attack exploits vulnerabilities in the database layer of an application to execute unauthorized SQL commands.
Cross-site scripting (A) involves injecting malicious scripts into content from otherwise trusted websites. A brute-force attack (C) is an attempt to gain access to a system by systematically checking all possible keys or passwords until the correct one is found. A DDoS attack (D) is an attempt to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of internet traffic.

最新問題: **10**
ヘルプ デスクの技術者は、マザーボードが故障していると判断します。修復プロセスにおける最も論理的な次のステップは次のうちどれですか?
A. 問題を Tier 2 にエスカレーションする
B. ベンダーに保証状況を確認する
C. マザーボードの交換
D. 別の PC を購入する
Answer: (解答を表示する**)**
Verifying warranty status with the vendor is the most logical next step in the remediation process after determining that a motherboard has failed. A warranty is a guarantee from the vendor that covers the repair or replacement of defective or faulty products within a specified period of time. Verifying warranty status with the vendor can help the technician determine if the motherboard is eligible for warranty service and what steps to take to obtain it. Escalating the issue to Tier 2, replacing the motherboard, and purchasing another PC are not the most logical next steps in the remediation process.

最新問題: **11**
システム管理者は定期チェック中に、ユーザーの PC の動作が遅く、CPU 使用率が 100% になっていることを発見しました。さらに調査すると、大量のリソースが使用されていることがわかりました。リソース使用率が高い原因として最も可能性が高いのは次のどれですか。
A. ファイアウォールアクティビティ
B. ボットネット攻撃
C. DDoS攻撃
D. キーロガー攻撃
Answer: (解答を表示する**)**
When a system administrator discovers a user's PC running slowly with 100% CPU utilization, it often indicates that the system is being used for unauthorized purposes, such as being part of a botnet attack. Here's why:
* Botnet attack: Botnets are networks of computers infected with malware and controlled by an attacker.
These infected computers (bots) are often used to carry out tasks like sending spam or participating in Distributed Denial of Service (DDoS) attacks. The high CPU utilization and resource usage indicate that the computer might be performing tasks dictated by the botnet controller.
* Firewall activities: While firewall activities can use some resources, they generally do not cause sustained high CPU utilization.
* DDoS attack: DDoS attacks target external systems by overwhelming them with traffic. A system participating in a DDoS might have high network usage, but the primary symptom on the user's PC would be high network activity, not necessarily CPU usage.
* Keylogger attack: Keyloggers record keystrokes and generally do not cause high CPU utilization. They are more stealthy and have minimal resource footprints.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.4: Explain common social-engineering attacks, threats, and vulnerabilities.
Security and malware documentation.

最新問題: **12**
技術者は、コンピュータがマルウェアに感染していることを確認しました。技術者はシステムを隔離し、マルウェア対策ソフトウェアを更新します。技術者が次に行うべきことは次のうちどれですか?
A. 1 つのスキャンを実行し、今後のスキャンをスケジュールします。
B. 感染していないファイルをバックアップし、コンピュータを再イメージ化します。
C. 感染したファイルのクリーンなバックアップ コピーを復元します。
D. マルウェアが削除されるまで修復スキャンを繰り返し実行します。
Answer: D (メーッセージを残す**)**
Malware is malicious software that can cause damage or harm to a computer system or network4. A technician has verified a computer is infected with malware by observing unusual behavior, such as slow performance, pop-ups, or unwanted ads. The technician isolates the system and updates the anti-malware software to prevent further infection or spread of the malware. The next step is to run repeated remediation scans until the malware is removed. A remediation scan is a scan that detects and removes malware from the system. Running one scan may not be enough to remove all traces of malware, as some malware may hide or regenerate itself.

最新問題: **13**
企業は、リモートで作業する従業員が企業のイントラネットに安全にアクセスできるようにする必要があります。会社は次のうちどれを実装する必要がありますか?
A. パスワードで保護された Wi-Fi
B. ポートフォワーディング
C. バーチャル プライベート ネットワーク
D. 境界ネットワーク

Answer: (解答を表示する)
A virtual private network (VPN) is a technology that creates a secure and encrypted connection over a public network, such as the internet. A VPN allows remote employees to access the corporate intranet as if they were physically connected to the local network3. Password-protected Wi-Fi is a security measure for wireless networks that does not provide access to the corporate intranet. Port forwarding is a technique that allows external devices to access services on a private network through a router, but does not provide access to the corporate intranet. A perimeter network is a network segment that lies between an internal network and an external network, such as the internet, and provides an additional layer of security, but does not provide access to the corporate intranet.

最新問題**: 14**
従業員がスマートフォンを紛失し、ヘルプデスクにその旨を報告しました。従業員は、個人情報が漏洩する可能性を懸念しています。技術者がスマートフォンのデータを保護するための最善の方法は次のうちどれですか。
A. リモートロックBRリモートワイプ
B. リモートアクセス
C. リモート暗号化
Answer: B (メーッセージを残す)
When a smartphone is lost, especially one that might contain sensitive or private data, the primary concern is to ensure that any data on the device cannot be accessed by unauthorized persons. Among the options provided:
* Remote lock: This option will lock the device remotely, preventing access. However, it does not remove the data and might not be effective if the device is powered off or reset.
* Remote wipe: This is the best option as it allows the technician to erase all data from the device remotely, ensuring that sensitive information is not accessible to anyone who finds or steals the device.
* Remote access: This option would allow a technician to access the device remotely, but it would not directly prevent unauthorized access or data breaches.
* Remote encrypt: Encrypting the device remotely might not be possible if the device is not accessible or turned on, and it does not remove existing data which could be at risk.
Reference: CompTIA A+ Exam Objectives [220-1102] - 3.4: Given a scenario, use best practices to secure a mobile device.

最新問題**: 15**
ユーザーから、USB ドライブからファイルを転送した後、エアギャップのあるコンピュータがウイルスに感染した可能性があると報告されました。技術者は Windows Defender を使用してコンピューターのスキャンを実行しましたが、感染は見つかりませんでした。技術者が次に取るべきアクションは次のうちどれですか? (2 つ選択してください)。
A. イベント ログを調べます。
B. ネットワークに接続します。
C. 調査結果を文書化します。
D. 定義を更新します。
E. コンピューターを再イメージ化します。
F. ファイアウォールを有効にします。
Answer: A,D (メーッセージを残す)
When dealing with a suspected virus infection on an air-gapped computer, after an initial scan with Windows Defender shows no infection, the next steps should include examining the event logs to look for suspicious activity and updating the virus definitions for a more thorough scan. Event logs can provide insights into system changes and potential malicious activities, while updated definitions ensure the antivirus software can detect the latest threats. Connecting to the network or enabling the firewall might not be appropriate due to the risk of spreading the infection, and re-imaging the computer or documenting the findings would be subsequent steps if the initial actions don't resolve the issue.References: Official CompTIA A+ Core 1 and Core 2 Student Guide.

最新問題**: 16**
バークの最高経営責任者は最近、銀行がサポートに使用しているリモート アクセス ツールがこの犯罪にも使用された注目のサイバー犯罪に関するニュース レポートを見ました。レポートは、攻撃者がシステムにアクセスするためにパスワードをブルート フォースすることができたと述べています。次のうち、樹皮のリスクを最も抑えるのはどれですか? (2 つ選択)
A. サポート アカウントごとに多要素認証を有効にする

B. リモート アクセスを企業ネットワーク内の宛先に制限する
C. すべてのサポート アカウントに外国からのログインをブロックする
D. サポート ケース用の代替リモート アクセス ツールを構成します。
E. リモート アクセス ツール ユーザー用のパスワード マネージャーを購入する
F. パスワードを 5 回間違えるとアカウントがロックアウトされます
Answer: (解答を表示する**)**
The best ways to limit the bank's risk are to enable multifactor authentication for each support account and enforce account lockouts after five bad password attempts. Multifactor authentication adds an extra layer of security to the login process, making it more difficult for attackers to gain access to systems. Account lockouts after five bad password attempts can help to prevent brute force attacks by locking out accounts after a certain number of failed login attempts.

最新問題**: 17**
インシデント ハンドラーは、起こり得る訴訟の証拠を保持する必要があります。インシデントハンドラーが証拠を保持するために最も行う可能性が高いのは次のうちどれですか?
A. ファイルを暗号化する
B. 影響を受けるハード ドライブのクローンを作成します。
C. サイバー保険会社に連絡する
D. 法執行機関に通報する
Answer: B (メーッセージを残す**)**
The incident handler should clone any impacted hard drives to preserve evidence for possible litigation1

最新問題**: 18**
次のセキュリティ方式のうち、セキュリティを犠牲にすることなく現在の Wi-Fi 対応デバイスの大部分をサポートしているのはどれですか?
A. WPA3
B. MAC フィレット
C. 半径
D. TACACS+
Answer: A (メーッセージを残す**)**
WPA3 (Wi-Fi Protected Access 3) is a wireless security method that supports the majority of current Wi-Fi- capable devices without sacrificing security. It is backward compatible with WPA2 devices and offers enhanced encryption and authentication features. MAC filtering is another wireless security method, but it can be easily bypassed by spoofing MAC addresses. RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus) are network authentication protocols, but they are not wireless security methods by themselves. Verified References: https://www.comptia.org/blog
/wireless-security-standards https://www.comptia.org/certifications/a

最新問題**: 19**

ユーザーは、電話を使用して店舗で購入しようとしています。ユーザーは電話を支払いパッドに置きますが、デバイスは電話を認識しません。ユーザーは電話機を再起動しようとしますが、結果は同じです。問題を解決するためにユーザーが行うべきことは次のうちどれですか?

A. レジで機内モードをオフにします。
B. NFC が有効になっていることを確認します。
C. 店舗の Wi-Fi ネットワークに接続します。
D. 電話で Bluetooth を有効にします。

Answer: B (メーッセージを残す**)**

The user should verify that NFC is enabled on their phone. NFC is a technology that allows two devices to communicate with each other when they are in close proximity2.
NFC (Near Field Communication) technology allows a phone to wirelessly communicate with a payment terminal or other compatible device. In order to use NFC to make a payment or transfer information, the feature must be enabled on the phone. Therefore, the user should verify that NFC is enabled on their phone before attempting to make a payment with it. The other options, such as turning off airplane mode, connecting to Wi-Fi, or enabling Bluetooth, do not pertain to the NFC feature and are unlikely to resolve the issue. This information is covered in the Comptia A+ Core2 documents/guide under the Mobile Devices section.

最新問題**: 20**
システム管理者は最新の Windows セキュリティ パッチをインストールしましたが、翌日にはパフォーマンスの低下を報告する多数のチケットを受け取りました。この問題を解決するには、管理者が行うべきことは次のうちどれですか?

A. ユーザー プロファイルを再構築します。
B. 更新をロールバックします。
C. サービスを再起動します。
D. システムファイルチェックを実行します。

Answer: (解答を表示する**)**

Rolling back the updates is the best way to resolve the issue of slow performance caused by installing the latest Windows security patch. This can be done by using the System Restore feature or by uninstalling the specific update from the Control Panel. Rebuilding user profiles, restarting the services and performing a system file check are not likely to fix the issue, since they do not undo the changes made by the update.
Verified References: https://www.comptia.org/blog/how-to-roll-back-windows-updates https://www.comptia.
org/certifications/a

最新問題**: 21**
次のうち、MFA の例はどれですか?

A. 指紋スキャンと網膜スキャン
B. パスワードと暗証番号
C. ユーザー名とパスワード
D. スマートカードとパスワード

Answer: A (メーッセージを残す**)**

Smart card and password is an example of two-factor authentication (2FA), not multi-factor authentication (MFA). MFA requires two or more authentication factors. Smart card and password is an example of two-factor authentication (2FA)2

最新問題**: 22**
ユーザーの会社の電話が盗まれました。技術者が次に行うべきことは次のうちどれですか?

A. ローレベルフォーマットを行います。

B. デバイスをリモートでワイプします。
C. デバイスを消磁します。
D. デバイスの GPS 位置を提供します。
Answer: B (メーッセージを残す)
Remotely wiping the device is the best option to prevent unauthorized access to the company data stored on the phone. A low-level format, degaussing, or providing the GPS location of the device are not feasible or effective actions to take in this scenario.
References: The Official CompTIA A+ Core 2 Study Guide1, page 315.

最新問題**: 23**
住宅所有者が最近引っ越したので、新しい ISP が正しく機能するために新しいルーターが必要です。インターネット サービスがインストールされ、機能することが確認されています。関連するすべてのケーブルとハードウェアを設置した後、住宅所有者が最初に行うべき手順は次のうちどれですか?
A. PC を DHCP 割り当てから静的 IP アドレスに変換します。
B. 速度テストを実行して、アドバタイズされた速度が満たされていることを確認します。
C. お客様が使用するすべてのネットワーク共有および印刷機能をテストします。
D. 新しいネットワーク デバイスのデフォルト パスワードを変更します。
Answer: D (メーッセージを残す)
When a homeowner moves and sets up a new router for the new ISP it is important to take appropriate security measures to protect their network from potential security threats. The FIRST step that the homeowner should take after installation of all relevant cabling and hardware is to change the default passwords on new network devices.
Most modern routers come with default usernames and passwords that are widely known to potential attackers. If these defaults are not changed, it could make it easier for external attackers to gain unauthorized access to the network. Changing the passwords on new network devices is a simple but effective way to improve the security posture of the network.

最新問題**: 24**
ユーザーがヘルプ デスクに電話して、Windows が更新プログラムをラップトップにインストールし、夜間に再起動したことを報告しました。ラップトップが再起動すると、タッチパッドが機能しなくなりました。技術者は、タッチパッドを制御するソフトウェアに問題がある可能性があると考えています。技術者が調整を行うために使用する必要があるツールは次のうちどれですか?
A. eventvwr.msc
B. perfmon.msc
C. gpedic.msc
D. devmgmt.msc
Answer: D (メーッセージを残す)
The technician should use devmgmt.msc tool to make adjustments for the touchpad issue after Windows installed updates on a laptop. Devmgmt.msc is a command that opens the Device Manager, which is a utility that allows users to view and manage the hardware devices and drivers installed on a computer. The technician can use the Device Manager to check the status, properties and compatibility of the touchpad device and its driver, and perform actions such as updating, uninstalling or reinstalling the driver, enabling or disabling the device, or scanning for hardware changes. Eventvwr.msc is a command that opens the Event Viewer, which is a utility that allows users to view and monitor the system logs and events. The Event Viewer may provide some information or clues about the touchpad issue, but it does not allow users to manage or troubleshoot the device or its driver directly. Perfmon.msc is a command that opens the Performance Monitor, which is a utility that allows users to measure and analyze the performance of the system

最新問題**: 25**
ある技術者が SOHO に新しいネットワーク機器を設置しており、インターネット上の外部の脅威から機器を確実に保護したいと考えています。技術者が最初に行うべきアクションは次のうちどれですか?
A. クローゼット内のすべてのデバイスをロックします。
B. すべてのデバイスが同じメーカーのものであることを確認してください。

C. デフォルトの管理パスワードを変更します。
D. 最新のオペレーティング システムとパッチをインストールします。
Answer: C (メーッセージを残す)
The technician should change the default administrative password FIRST to ensure the network equipment is secured against external threats on the Internet. Changing the default administrative password is a basic security measure that can help prevent unauthorized access to the network equipment. Locking all devices in a closet is a physical security measure that can help prevent theft or damage to the devices, but it does not address external threats on the Internet. Ensuring all devices are from the same manufacturer is not a security measure and does not address external threats on the Internet. Installing the latest operating system and patches is important for maintaining the security of the network equipment, but it is not the first action the technician should take1

最新問題**: 26**
技術者は、最新のポリシー変更を受け取っていないワークステーションを調査しています。技術者は、最新のドメイン ポリシー変更を適用するために、次のコマンドのどれを使用する必要がありますか?
A. sfc /scannow
B. gpupdare /force
C. chkdsk /y
D. xcopy Zp
Answer: B (メーッセージを残す)
When a workstation has not received the latest policy changes, the gpupdate command is used to manually apply the latest group policies from the domain controller.
* Option A: sfc /scannowThis command is used to scan and repair corrupted system files, not to update group policies.
* Option B: gpupdate /forceThis command forces the workstation to reapply all group policies, ensuring that the latest policies are applied immediately.
* Option C: chkdsk /yThis command checks the integrity of the file system and fixes logical file system errors, not to update group policies.
* Option D: xcopy /ZpThis command is used for copying files and directories, not for updating group policies.
References:
* CompTIA A+ 220-1102 Objective 1.6 (Configure Microsoft Windows networking features on a client /desktop), particularly managing and applying group policies.

最新問題**: 27**
中小企業のシステム管理者は、ユーザーに気付かれずにユーザーのマシンに個別にアクセスし、パッチ レベルを確認したいと考えています。管理者は次のどのリモート アクセス テクノロジを使用する必要がありますか。
A. RDP
B. MSRA
C. SSH
D. VNC
Answer: (解答を表示する)
Detailed Explanation with Core 2 References:SSH allows for remote access to systems securely and discretely, suitable for verifying patch levels and other administrative tasks. This meets Core 2 objectives on using secure remote access tools (Core 2 Objective 4.9).

最新問題**: 28**
技術者は、ユーザーが自宅で作業できるようにコンピューターを構成し、ユーザーがユーザーの共有ファイルや会社の電子メールに安全にアクセスできるようにする必要があります。次のツールのうち、このタスクを最もよく実行できるのはどれですか*?
A. MSRA
B. FTP

C. RMM
D. VPN
Answer: D (メーッセージを残す)
To securely access shared files and corporate email from home, the best tool to use is a Virtual Private Network (VPN). Here's why:
* VPN (Virtual Private Network): A VPN creates a secure connection over the internet, allowing the user to access the corporate network as if they were on-site. It encrypts the data transmitted between the user's home and the corporate network, ensuring privacy and security.
* MSRA (Microsoft Remote Assistance): Used for remote support but not for accessing shared files and emails securely.
* FTP (File Transfer Protocol): Used for transferring files but does not provide secure access to a corporate network or email.
* RMM (Remote Monitoring and Management): Used by IT professionals to manage client systems remotely but not for user access to shared files and emails.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.9: Given a scenario configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.
VPN configuration and security documentation.

最新問題**: 29**
ネットワーク管理者は、組織内のすべてのデバイスの Wi-Fi アクセスに使用するクライアント証明書を展開しています。証明書は、ユーザーの既存のユーザー名とパスワードと共に使用されます。この導入後に実現したセキュリティ上の利点を最もよく表しているのは、次のうちどれですか?
A. Wi-Fi に対して多要素認証が強制されます。
B. すべての Wi-Fi トラフィックは転送中に暗号化されます。
C. 盗聴を防止します。
D. 不正なアクセス ポイントは接続しません。
Answer: B (メーッセージを残す)
The security benefits realized after deploying a client certificate to be used for Wi-Fi access for all devices in an organization are that all Wi-Fi traffic will be encrypted in transit. This means that any data transmitted over the Wi-Fi network will be protected from eavesdropping attempts. Rogue access points will not connect to the network because they will not have the client certificate. However, multifactor authentication will not be forced for Wi-Fi because the client certificate is being used in conjunction with the user's existing username and password12

最新問題**: 30**
ユーザーが問題を報告するために電話をかけると、技術者がユーザーに代わってチケットを送信します。チケットが正しいユーザーに関連付けられていることを確認するために技術者が使用する必要があるのは、次のうちどれですか?
A. チケットに追加するコールバック電話番号をユーザーに提供してもらいます。
B. 部門のパワー ユーザーにチケットを割り当てる
C. 一意のユーザー識別子でチケットを登録します
D. 後続の通話で参照できる一意のチケット番号をユーザーに提供します。
Answer: (解答を表示する)
The technician should provide the user with a unique ticket number that can be referenced on subsequent calls to make sure the ticket is associated with the correct user. This is because registering the ticket with a unique user identifier, having the user provide a callback phone number to be added to the ticket, or assigning the ticket to the department's power user will not ensure that the ticket is associated with the correct user2.

最新問題**: 31**

ある企業は、従業員のコラボレーション プロセスの一部として共有ドライブを使用しています。正しいアクセス権限を確保するために、最上位フォルダーの継承は各部門に割り当てられます。マネージャーのチームは機密資料に取り組んでおり、直属のチームのみが特定のフォルダーとその後続のファイルおよびサブフォルダーを表示できるようにしたいと考えています。次のアクションのうち、技術者が実行する可能性が最も高いのはどれですか?

A. 要求されたフォルダーのみの継承をオフにし、要求されたアクセス許可を各ファイルに手動で設定します。

B. 最上位フォルダーでの継承をオフにし、継承されたすべてのアクセス許可を削除します。

C. 最上位フォルダーでの継承をオフにし、各ファイルとサブフォルダーへのアクセス許可を手動で設定します。

D. 要求されたフォルダーのみで継承をオフにし、要求されたアクセス許可を設定してから、子フォルダーでの継承をオンにします。

Answer: D (メーッセージを残す)

Turning off inheritance on the specific folder requested by the manager and setting the requested permissions, followed by turning on inheritance under the child folders, ensures that only the immediate team has access to the confidential material while maintaining the broader permissions structure for other folders and files. This action isolates the folder's permissions from the top-level inheritance, providing a focused security measure for sensitive content.

最新問題: 32

技術者は、将来のリスクを軽減するためにアップデートとスケジュールされたスキャンを実行した後、感染したコンピュータから悪意のあるソフトウェアを削除することに成功しました。技術者が次に行うべきことは次のうちどれですか?

A. セキュリティのベスト プラクティスについてエンド ユーザーを教育します。

B. ウイルス対策システムでホストを隔離します。

C. システムがどのようにしてマルウェアに感染したかを調査します。

D. システムの復元ポイントを作成します。

Answer: (解答を表示する)

Educating the end user on best practices for security is the next step that the technician should take after successfully removing malicious software from an infected computer. Educating the end user on best practices for security is an important part of preventing future infections and mitigating risks. The technician should explain to the end user how to avoid common sources of malware, such as phishing emails, malicious websites, or removable media. The technician should also advise the end user to use strong passwords, update software regularly, enable antivirus and firewall protection, and backup data frequently. Educating the end user on best practices for security can help the end user become more aware and responsible for their own security and reduce the likelihood of recurrence of malware infections. Quarantining the host in the antivirus system, investigating how the system was infected with malware, and creating a system restore point are not the next steps that the technician should take after successfully removing malicious software from an infected computer. Quarantining the host in the antivirus system is a step that the technician should take before removing malicious software from an infected computer. Quarantining the host in the antivirus system means isolating the infected computer from the network or other devices to prevent the spread of malware.

Investigating how the system was infected with malware is a step that the technician should take during or after removing malicious software from an infected computer. Investigating how the system was infected with malware means identifying the source, type, and impact of malware on the system and documenting the findings and actions taken. Creating a system restore point is a step that the technician should take before removing malicious software from an infected computer. Creating a system restore point means saving a snapshot of the system's configuration and settings at a certain point in time, which can be used to restore the system in case of failure or corruption. References:

* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
* CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

最新問題: **33**
技術者は、32 ビット OS で実行されているレガシー システムを、32 ビット システムと 64 ビット システムの両方で動作する新しいアプリケーションを使用してアップグレードする必要があります。レガシー システムは組織にとって非常に重要です。IT マネージャーは、新しいアプリケーションが会社の財務に悪影響を及ぼしてはいけないと警告しています。IT マネージャーが最も懸念している影響は次のうちどれですか?
A. デバイス
B. ビジネス
C. ネットワーク
D. 操作
Answer: B (メーッセージを残す**)**
The IT manager's caution regarding the new applications not having a detrimental effect on company finances points directly to concerns about the business impact. This encompasses potential costs associated with upgrading legacy systems, compatibility issues that might arise from running new applications on old infrastructure, and the risks of system downtime or reduced performance affecting business operations. The focus here is on ensuring that the integration of new applications into the legacy system does not incur unexpected expenses or disrupt critical business processes.

最新問題: **34**
ユーザーが複数バージョンのファイルに確実にアクセスできるようにするために使用できる機能は次のどれですか?
A. 複数のデスクトップ
B. リモート ディスク
C. タイムマシン
D. FileVault
Answer: (解答を表示する**)**
Time Machine is a backup feature available in macOS that automatically makes hourly backups for the past
24 hours, daily backups for the past month, and weekly backups for all previous months to an external drive or NAS. It allows users to recover the entire system or specific files from any point in time, ensuring access to multiple versions of files. This feature is particularly useful for reverting to earlier versions of a document or recovering a file that has been accidentally deleted or altered. The other options, such as Multiple Desktops, Remote Disc, and FileVault, do not provide versioning capabilities for file access.

最新問題: **35**
お客様の携帯電話の Web ブラウジング速度は数週間ごとに遅くなり、3 ～ 4 日後には通常に戻ります。通常、デバイスを再起動してもパフォーマンスは回復しません。この問題をトラブルシューティングするために、技術者が最初に確認する必要があるのは次のうちどれですか?
A. データ使用制限
B. Wi-Fi接続速度
C. 機内モードの状態
D. システム稼働時間
Answer: (解答を表示する**)**
The technician should check the Wi-Fi connection speed first to troubleshoot this issue. Slow web browsing speed on a mobile phone can be caused by a slow Wi-Fi connection. The technician should check the Wi-Fi connection speed to ensure that it is fast enough to support web browsing. If the Wi-Fi connection speed is slow, the technician should troubleshoot the Wi-Fi network to identify and resolve the issue.

最新問題: **36**
企業ネットワーク上のコンピューターがマルウェアに感染しています。次のうち、コンピュータをサービスに戻すための最良の方法はどれですか?
A. Linux ライブ ディスクを使用してシステムをスキャンし、BIOS をフラッシュしてから、コンピュータをサービスに戻します。

B. BIOS のフラッシュ、ドライブの再フォーマット、OS の再インストール
C. ハード ドライブの消磁、BIOS のフラッシュ、OS の再インストール
D. OS の再インストール。BIOS をフラッシュし、オンプレミスのアンチウイルスでスキャンする
Answer: B (メーッセージを残す)
Flashing the BIOS, reformatting the drive, and then reinstalling the OS is the best method for returning a computer with a malware infection to service. Flashing the BIOS updates the firmware of the motherboard and can remove any malware that may have infected it. Reformatting the drive erases all data on it and can remove any malware that may have infected it. Reinstalling the OS restores the system files and settings to their original state and can remove any malware that may have modified them. Scanning the system with a Linux live disc may not detect or remove all malware infections. Degaussing the hard drive is an extreme method of destroying data that may damage the drive beyond repair. Reinstalling the OS before flashing the BIOS or scanning with antivirus may not remove malware infections that persist in the BIOS or other files.

最新問題**: 37**
Active Directory を使用している企業は、すべてのユーザーの 「ドキュメント」の場所をネットワーク上のファイル サーバーに変更したいと考えています。このタスクを達成するために会社が設定すべきものは次のうちどれですか?
A. セキュリティ グループ
B. フォルダーのリダイレクト
C. 組織単位の構造
D. アクセス制御リスト
Answer: B (メーッセージを残す)
Folder redirection is a feature in Windows that allows administrators to change the default location of certain special folders within the user profile, such as the "Documents" folder, to a different location, typically on a network server. This is commonly used in organizational environments to centralize file storage, simplify backups, and ensure data is stored on network drives with potentially more robust security measures and redundancy.
Folder redirection:By implementing folder redirection through Group Policy in Active Directory, a company can ensure that all users' "Documents" folders are stored on a specified file server on the network, allowing for centralized management and backup of important user files.
Security groups (A) are used to manage user and computer access to shared resources, but they don't directly enable the relocation of user folders. Organizational unit structure (C) helps in managing and applying policies within Active Directory but is not directly related to the physical location of files. Access control lists (D) are used to define permissions for files and directories, but they do not govern where those files and directories should be located.

最新問題**: 38**
お客様は、Windows ラップトップのハード ドライブ上のデータが保護され、安全であることを確認したいと考えています。最良の解決策は次のうちどれですか?
A. Windows バックアップ
B. BitLocker
C. シャドウ コピー
D. 信頼できるプラットフォームモジュール
Answer: B (メーッセージを残す)
BitLocker is a full-disk encryption feature included with Windows Vista and later. It is designed to protect data by providing encryption for entire volumes. By encrypting the hard drive, BitLocker prevents unauthorized access to the data stored on the drive, securing it in case the laptop is lost or stolen. BitLocker is preferable over options like Windows Backup (which is for data recovery, not encryption), Shadow Copy (used for backup and does not encrypt data), and Trusted Platform Module (TPM, which is a hardware component used alongside BitLocker for securing encryption keys).

最新問題**: 39**
小規模オフィスの顧客は、サーバーのないネットワーク内に 3 台の PC を構成する必要があります。この環境に対してお客様が選択するのに最適なのは、次のネットワーク タイプのうちどれですか?

A. ワークグループネットワーク
B. パブリックネットワーク
C. 広域ネットワーク
D. ドメインネットワーク
Answer: A (メーッセージを残す**)**
A workgroup network is a peer-to-peer network where each PC can share files and resources with other PCs without a central server. A public network is a network that is accessible to anyone on the internet. A wide area network is a network that spans a large geographic area, such as a country or a continent. A domain network is a network where a server controls the access and security of the PCs.
Verified References:
https://www.comptia.org/blog/network-typeshttps://www.comptia.org/certifications/a

最新問題**: 40**
開発者のタイプ 2 ハイパーバイザーは、新しいソース コードをコンパイルする際に適切なパフォーマンスを発揮しません。開発者がハイパーバイザーのパフォーマンスを向上させるためにアップグレードする必要があるコンポーネントは次のうちどれですか?
A. システムRAMの容量
B. NIC のパフォーマンス
C. ストレージ IOPS
D. 専用GPU
Answer: (解答を表示する**)**
The correct answer is A. Amount of system RAM. A Type 2 hypervisor is a virtualization software that runs on top of a host operating system, which means it shares the system resources with the host OS and other applications. Therefore, increasing the amount of system RAM can improve the performance of the hypervisor and the virtual machines running on it. RAM is used to store data and instructions that are frequently accessed by the CPU, and having more RAM can reduce the need for swapping data to and from the storage device, which is slower than RAM.
NIC performance, storage IOPS, and dedicated GPU are not as relevant for improving the hypervisor's performance in this scenario. NIC performance refers to the speed and quality of the network interface card, which is used to connect the computer to a network. Storage IOPS refers to the number of input/output operations per second that can be performed by the storage device, which is a measure of its speed and efficiency. Dedicated GPU refers to a separate graphics processing unit that can handle complex graphics tasks, such as gaming or video editing. These components may affect other aspects of the computer's performance, but they are not directly related to the hypervisor's ability to compile new source code.

最新問題**: 41**
BitLocker を含む Windows の最も基本的なバージョンは次のうちどれですか?
A. ホーム
B. プロ
C. エンタープライズ
D. ワークステーションのプロ
Answer: D (メーッセージを残す**)**
The most basic version of Windows that includes BitLocker is Windows Pro. BitLocker is a feature of Windows Pro that provides full disk encryption for all data on a storage drive [1]. It helps protect data from unauthorized access or theft and can help secure data from malicious attacks. Pro for Workstations includes this feature, as well as other features such as support for up to 6 TB of RAM and ReFS.

最新問題**: 42**
開発者がワークステーションに仮想化ソフトウェアをインストールしようとすると、次のエラーが発生します。
VTx はシステムでサポートされていません
次のアップグレードのうち、問題を解決できる可能性が最も高いのはどれですか?

A. プロセッサー
B. ハードディスク
C. メモリ
D. ビデオカード
Answer: A (メーッセージを残す)
The processor is the component that determines if the system supports virtualization technology (VTx), which is required for running virtualization software. The hard drive, memory and video card are not directly related to VTx support, although they may affect the performance of the virtual machines. Verified References:
https://www.comptia.org/blog/what-is-virtualizationhttps://www.comptia.org/certifications/a

最新問題**: 43**
次のオペレーティング システムのうち、ext4 ファイルシステム タイプを使用するものはどれですか?
A. macOS
B. iOS
C. Linux
D. Windows
Answer: C (メーッセージを残す)
The ext4 (fourth extended filesystem) is a journaling file system for Linux. It is widely used in many Linux distributions due to its performance, robustness, and advanced features like large file and volume support.
* macOS: Uses filesystems like HFS+ or APFS.
* iOS: Uses APFS (Apple File System).
* Linux: Uses ext4 among other filesystems like ext3, XFS, Btrfs, etc.
* Windows: Uses NTFS, FAT32, and exFAT, not ext4.
Reference: CompTIA A+ Exam Objectives [220-1102] - 1.1: Compare and contrast common operating system types and their purposes.

最新問題**: 44**
会社がローカル オフィスを取得し、技術者がオフィスのマシンをローカル ドメインに参加させようとしています。技術者は、ドメイン参加オプションが欠落しているように見えることに気付きました。Windows の次のエディションのうち、マシンにインストールされている可能性が最も高いのはどれですか?
A. Windows プロフェッショナル
B. Windows 教育
C. Windows エンタープライズ
D. Windows ホーム
Answer: (解答を表示する)
Windows Home is the most likely edition of Windows installed on the machines that do not have the domain join option. Windows Home is a consumer-oriented edition that does not support joining a domain or using Group Policy. Only Windows Professional, Education, and Enterprise editions can join a domain

最新問題**: 45**
ユーザーは最近、Android デバイスに無料のゲーム アプリケーションをダウンロードしました。その後、デバイスが頻繁にクラッシュし、すぐにバッテリーの充電が失われるようになりました。これらの問題を修復するには、技術者が最初に実行することを推奨するのは次のうちどれですか? (2 つ選択してください)。
A. ゲームアプリケーションをアンインストールします。
B. デバイスを工場出荷時設定にリセットします。

C. デバイスを外部充電器に接続します。
D. 最新のセキュリティ パッチをインストールします。
E. アプリケーションのキャッシュをクリアします。
F. デバイスの組み込みのマルウェア対策保護を有効にします。
Answer: (解答を表示する**)**
When an Android device starts exhibiting issues like frequent crashes and rapid battery drain after downloading an application, the first step should be to address the immediate cause:
Uninstall the game application:Since the issues started after the game application was installed, removing it is a logical first step. Unwanted or malicious applications can cause such symptoms by running harmful processes in the background or exploiting system resources.
Install the latest security patches:Keeping the device updated with the latest security patches is crucial for protecting against vulnerabilities that could be exploited by malicious software. Updating can resolve existing security flaws and improve device stability.

最新問題**: 46**
技術者は、集合住宅の隣にある診療所で Wi-Fi ネットワークの問題を解決するために働いています。技術者は、従業員と患者だけがネットワーク上にいるわけではないことを発見します。この問題を最小限に抑えるために、技術者が行うべきことは次のうちどれですか?
A. 未使用ポートを無効にします。
B. ゲスト ネットワークを削除します
C. ゲスト ネットワークにパスワードを追加する
D. ネットワークチャンネルを変更します。
Answer: (解答を表示する**)**
Changing the network channel is the best solution to minimize the issue of employees and patients not being the only people on the Wi-Fi network5 References: 3. Sample CompTIA Security+ exam questions and answers. Retrieved from https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-Security-exam-questions-and-answers

最新問題**: 47**
次のうち、Web ブラウザ インターフェイスしかないのはどれ?
A. Linux
B. Microsoft Windows
C. iOS
D. Chromium
Answer: (解答を表示する**)**
Chromium is an operating system that only has a web browser interface. Chromium is an open-source project that provides the source code and framework for Chrome OS, which is a Linux-based operating system developed by Google. Chromium and Chrome OS are designed to run web applications and cloud services through the Chrome web browser, which is the only user interface available on the system. Chromium and Chrome OS are mainly used on devices such as Chromebooks, Chromeboxes and Chromebits. Linux is an operating system that does not only have a web browser interface but also a graphical user interface and a command-line interface. Linux is an open-source and customizable operating system that can run various applications and services on different devices and platforms. Linux can

also support different web browsers, such as Firefox, Opera and Chromium. Microsoft Windows is an operating system that does not only have a web browser interface but also a graphical user interface and a command-lineinterface. Microsoft Windows is a proprietary and popular operating system that can run various applications and services on different devices and platforms. Microsoft Windows can also support different web browsers, such as Edge, Internet Explorer and Chrome. iOS is an operating system that does not only have a web browser interface but also a graphical user interface and a voice-based interface. iOS is a proprietary and mobile operating system developed by Apple that can run various applications and services on devices such as iPhone, iPad and iPod Touch. iOS can also support different web browsers, such as Safari, Firefox and Chrome. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

最新問題: **48**
学生は次の学期に向けて新しい Windows 10 ラップトップをセットアップしています。学生は壁紙のカスタマイズに興味があります。学生が壁紙を変更するには次のどれを使用する必要がありますか?
A. アプリと機能
B. パーソナライゼーション
C. ファイルエクスプローラー
D. タスクマネージャー
Answer: B (メーッセージを残す**)**
To change the wallpaper on a Windows 10 laptop, the "Personalization" settings should be used. These settings allow users to customize themes, which include various aspects of the desktop environment such as the desktop wallpaper, screen saver, color scheme, and more. This makes "Personalization" the correct option for customizing the wallpaper.References: Official CompTIA A+ Core 1 and Core 2 Student Guide.

最新問題: **49**
サポート エージェントのチームは、ワークステーションを使用してクレジット カード データを保存します。一般的な規制管理への準拠を維持するために、IT 部門がワークステーションで有効にする必要があるのは次のうちどれですか? (2 つ選択)。
A. 暗号化
B. ウイルス対策
C. オートラン
D. ゲスト アカウント
E. デフォルトのパスワード
F. バックアップ
Answer: (解答を表示する**)**
Encryption is a way of protecting cardholder data by transforming it into an unreadable format that can only be decrypted with a secret key1. Backups are a way of ensuring that cardholder data is not lost or corrupted in case of a disaster or system failure2. Both encryption and backups are part of the PCI DSS requirements that apply to any entity that stores, processes, or transmits cardholder data1. The other options are not directly related to credit card data security or compliance.

最新問題: **50**
開発者は、Linux で基本的なタスクを自動化するシェル スクリプトを作成しています。デフォルトでサポートされているファイルの種類は次のうちどれですか?
A. .py
B. .js
C. .vbs
D. .sh
Answer: D (メーッセージを残す**)**
https://www.educba.com/shell-scripting-in-linux/

最新問題: **51**
技術者が現場で怒っている顧客に対応しています。顧客は問題が解決されていないと考えていますが、技術者は問題が正しく解決されたと考えています。技術者はこの状況に対処するために、次のどれを行うべきでしょうか。
A. 顧客の意見が正しいと主張し、懸念事項を文書化します。
B. 顧客の話を聞き、何も話さない。
C. 問題を次の層にエスカレートします。
D. 謝罪し、問題の解決に役立つ方法を尋ねます。
Answer: D (メーッセージを残す)
When dealing with an angry customer, active listening and empathy are crucial. Even if the technician believes the issue has been resolved, the customer's concerns must be acknowledged professionally.
* Option A (Incorrect): Insisting that the customer is correct and simply documenting the concern does not resolve the issue. The technician should aim to engage with the customer constructively.
* Option B (Incorrect): While listening is important, completely staying silent without engaging in a discussion does not help in resolving the issue.
* Option C (Incorrect): Escalating the issue immediately without attempting to resolve it first is not the best approach unless all other options fail.
* Option D (Correct): Apologizing and asking what would help resolve the issue demonstrates empathy and professionalism. It helps defuse the situation and allows for an opportunity to find a mutually acceptable solution.
CompTIA A+ Core 2 Reference:
* 220-1102 Exam Objective 4.3 - Explain the importance of professionalism, including empathy, active listening, and proper documentation.

最新問題: **52**
ユーザーは、Windows 10 ラップトップで指紋リーダーをセットアップするためのヘルプを要求しました。ラップトップには指紋リーダーが装備されており、ドメインに参加しています グループ ポリシーは、環境内のすべてのコンピューターで Windows Hello を有効にします。ユーザーの Windows Hello 指紋を設定する方法を説明しているオプションは次のうちどれですか?
A. コントロール パネル ユーティリティに移動し、[セキュリティとメンテナンス] サブメニューを選択し、[セキュリティとメンテナンスの設定の変更] を選択し、[Windows Hello 指紋] を選択します。Windows がセットアップの完了を示すまで、ユーザーに繰り返し指紋リーダーに指紋を入力してもらいます。
B. Windows 10 の [設定] メニューに移動し、[アカウント] サブメニューを選択し、[サインイン オプション] を選択し、[Windows Hello 指紋] を選択します。Windows がセットアップの完了を示すまで、ユーザーに繰り返し指紋リーダーに指紋を入力してもらいます。
C. Windows 10 の [設定] メニューに移動し、[更新とセキュリティ] サブメニューを選択します。[Windows セキュリティ] を選択し、[Windows Hello 指紋] を選択します。Windows がセットアップの完了を示すまで、ユーザーに指紋リーダーに指紋を繰り返し入力してもらいます。
D. コントロール パネル ユーティリティに移動し、[管理ツール] サブメニューを選択し、リストからユーザー アカウントを選択し、[Windows Hello 指紋] を選択します。Windows がセットアップの完了を示すまで、ユーザーに繰り返し指紋リーダーに指紋を入力してもらいます。
Answer: B (メーッセージを残す)
Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete. Windows Hello Fingerprint can be set up by navigating to the Windows
10 Settings menu, selecting the Accounts submenu, selecting Sign in options, and then selecting Windows Hello Fingerprint. The user will then be asked to place a fingerprint on the fingerprint reader repeatedly until Windows indicates that setup is complete. Windows Hello Fingerprint allows the user to log into the laptop using just their fingerprint, providing an additional layer of security.

最新問題: **53**
立ち入り禁止区域へのアクセスを検出して記録するために使用されるのは次のどれですか?
A. ボラード
B. ビデオ監視
C. バッジリーダー
D. フェンス

Answer: C (メーッセージを残す)
Badge readers are devices that scan employee or visitor credentials, logging entries and exits from restricted areas. Video surveillance (B) provides a visual record but does not directly control access. Bollards (A) and fences (D) provide physical security but cannot detect or record access events.
Reference: Core 2, Domain 2.1 - Physical security measures.

最新問題**: 54**
Apple MacBook を使用している従業員は、他の Apple デバイスから写真やビデオを共有したいというランダムなポップアップ要求を頻繁に受け取り、その要求を受け入れるかどうかを尋ねます 技術者は次のどの構成を最初に変更するようユーザーにアドバイスすべきですか ?
A. Wi-Fi
B. iCloud
C. ウイルス対策
D. エアドロップ
Answer: D (メーッセージを残す)
AirDrop is a feature on Apple devices that allows users to wirelessly share files, photos, and videos with nearby Apple devices. If the MacBook is receiving unsolicited AirDrop requests, adjusting the AirDrop settings to allow sharing with contacts only or turning it off completely can help prevent these random pop-up requests.

最新問題**: 55**
従業員は過去数年間、複数のアプリケーションや Web サイトで同じパスワードを使用しています。セキュリティ問題を防ぐのに最適なのは次のうちどれですか?
A. ファイアウォール設定の構成
B. 有効期限ポリシーの実装
C. 複雑さの要件の定義
D. ウイルス対策定義を更新しています
Answer: B (メーッセージを残す)
To prevent security issues related to an employee using the same password for multiple applications and websites, implementing expiration policies (B) is best. Password expiration policies require users to change their passwords at regular intervals, which helps to mitigate the risks associated with password reuse.
Regularly changing passwords reduces the chances of unauthorized access from compromised credentials.

最新問題**: 56**
セキュリティ管理者は、組織のスタッフ全員に BitLocker To Go の使用方法を教えます。このトレーニングの理由として最も適切なのは次のどれですか。
A. 紛失や盗難に備えて、すべてのリムーバブルメディアがパスワードで保護されていることを確認する
B. セキュアブートとBIOSレベルのパスワードを有効にして構成の変更を防ぐ
C. VPN接続をハードウェアモジュールで暗号化するように強制する
D. すべてのラップトップでハードドライブの暗号化要素として TPM を使用するように構成する
Answer: A (メーッセージを残す)
Detailed Explanation with Core 2 References:BitLocker To Go is a feature in Windows that allows for encryption of removable drives to protect sensitive information. Training staff on BitLocker To Go ensures that if a removable drive is lost or stolen, it will be password-protected and encrypted, making the data inaccessible to unauthorized individuals. This aligns with Core 2 objectives related to security measures for data-at-rest encryption and best practices for safeguarding information (CompTIA A+ Core 2 Objective 2.6).

最新問題**: 57**
技術者は、IP アドレスを隠し、すべてのネットワーク トラフィックを保護するトンネルを作成しています。次のプロトコルのうち、強化されたセキュリティに耐えることができるのはどれですか?

A. DNS
B. IPS
C. VPN
D. SSH
Answer: C (メーッセージを残す)
A VPN (virtual private network) is a protocol that creates a secure tunnel between two devices over the internet, hiding their IP addresses and encrypting their traffic. DNS (domain name system) is a protocol that translates domain names to IP addresses. IPS (intrusion prevention system) is a device that monitors and blocks malicious network traffic. SSH (secure shell) is a protocol that allows remote access and command execution on another device. Verified References: https://www.comptia.org/blog/what-is-a-vpn https://www.
comptia.org/certifications/a

最新問題**: 58**
ユーザーから、アプリケーションをアップグレードするための最近のソフトウェア展開後、テスト プログラムが使用できなくなったという報告がありました。
ただし、他の従業員はテスト プログラムを正常に使用できます。
説明書
各タブの情報を確認して展開の結果を確認し、検出された問題を解決するには、以下を選択します。
* イベント ビューアーの問題のインデックス番号
* 問題を解決するための最初のコマンド
* 問題を解決するための2番目のコマンド
ブルースクリーン

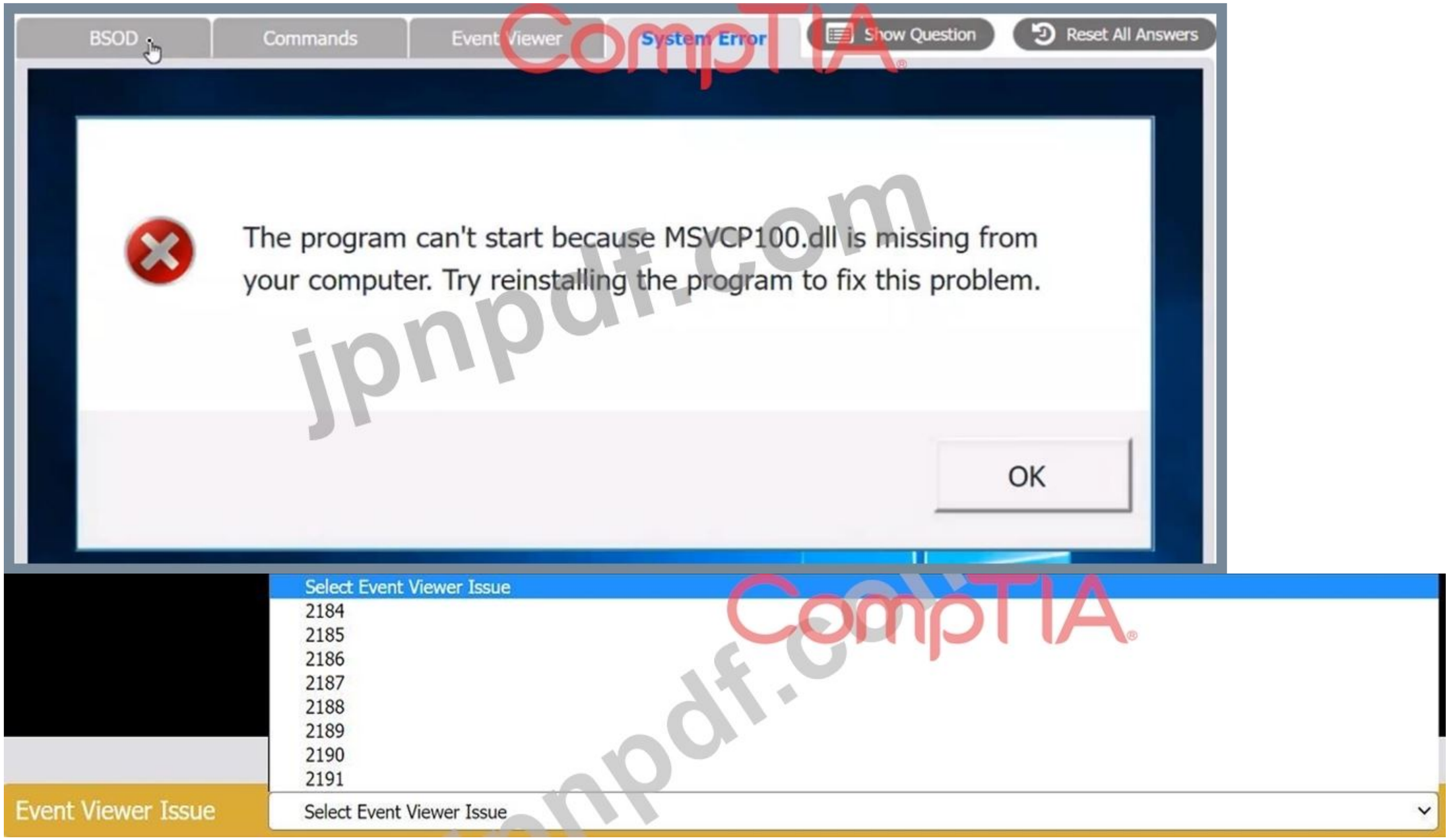

A problem has been detected and system has been shutdown to prevent damage to your computer.
DRIVER_IRQL_NOT_LES_OR_EQUAL
If this is the first time you've seen this stop error screen, restart your computer, if this screen appears again, follow these steps:
Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any system updates you might need.
If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.
Technical information:
*** STOP: 0x000000D1 (0x0000000R, 0x00000007, 0x00000000, 0xG74H2S74)
*** strt1.sys - Address G74H2S74 base at G74H0000, DateStamp 4eh2534df
Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further assistance.

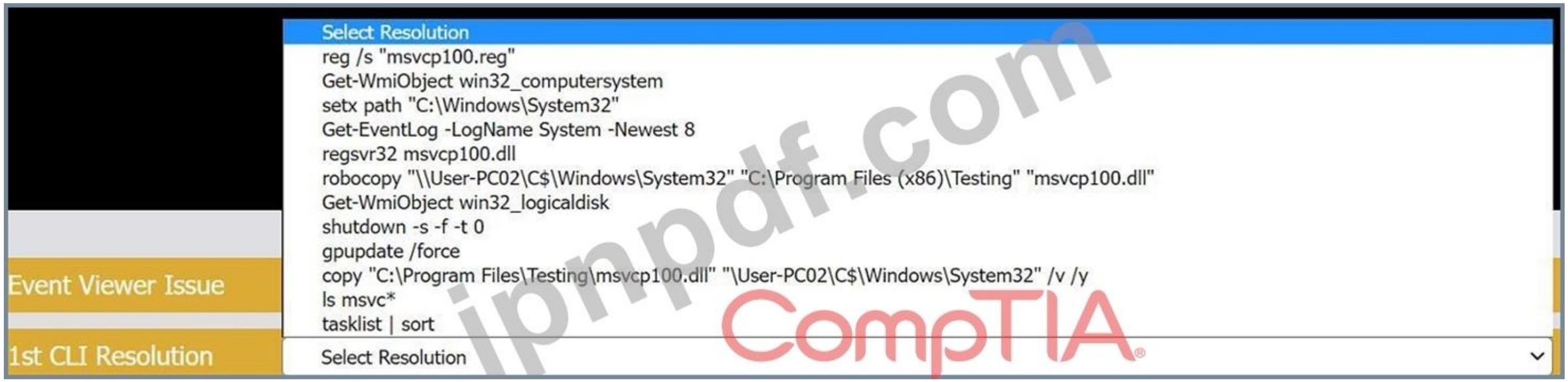
コマンド:

イベント ビューアー:


BSOD
Commands
Event Viewer
System Error
Show Question
Reset All Answers
Index Time EntryType Source InstanceID Message
2191 Mar 03 10:35 Information Service Control M... 1073748860 The Multimedia Class Scheduler service entered ...
2190 Mar 03 10:35 Error Application Error 100 Application has encountered an internal error a...
2189 Mar 03 10:29 Information Service Control M... 1073748860 The TCP/IP NetBIOS Helper service entered the r...
2188 Mar 03 10:29 Information Service Control M... 1073748860 The Multimedia Class Scheduler service entered ...
2187 Mar 03 10:29 Information MsiInstaller 1033 Error Code 0: Windows Installer has successfull...
2186 Mar 03 10:29 Warning DistributedCOM 10016 The application-specific permission settings do...
2185 Mar 03 10:29 Information MEIx64 1074200578 Intel(R) Management Engine Interface driver has...
2184 Mar 03 10:29 Information MEIx64 1074200578 Intel(R) Management Engine Interface driver has...
CompTIA

システムエラー:





Answer:

see the answer below in explanation.

Explanation:

The user is experiencing a system error that prevents them from using the Testing program. The error message indicates that the file MSVCP100.dll is missing from the computer. This file is part of the Microsoft Visual C++ 2010 Redistributable Package, which is required by some applications to run properly. The error may have occurred due to a corrupted or incomplete software deployment.

To resolve this issue, the user needs to restore the missing file and register it in the system. One possible way to do this is to copy the file from another computer that has the Testing program installed and working, and then use the regsvr32 command to register it. The steps are as follows:

* On another computer (User-PC02) that has the Testing program installed and working, locate the file MSVCP100.dll in the folder C:\Program Files\Testing.
* Share the folder C:\Windows\System32 on User-PC02 by right-clicking on it, selecting Properties, then Sharing, then Advanced Sharing, then checking Share this folder, then clicking OK.
* On the user's computer (User-PC01), open a command prompt as an administrator by clicking Start, typing cmd, right-clicking on Command Prompt, and selecting Run as administrator.
* In the command prompt, type the following command to copy the file MSVCP100.dll from User-PC02 to User-PC01: copy "C:\Program Files\Testing\msvcp100.dll" "\\User-PC02\C$\Windows\System32"
* After the file is copied, type the following command to register it in the system: regsvr32 msvcp100.dll
* Restart the user's computer and try to run the Testing program again.

Therefore, based on the instructions given by the user, the correct answers are:

Select Event Viewer Issue: 2187

Select First Command: copy "C:\Program Files\Testing\msvcp100.dll" "\\User-PC02\C$\Windows\System32" Select Second Command: regsvr32 msvcp100.dll

最新問題**: 59**

技術者は、ワークステーションで見つかったトロイの木馬ウイルスを修正する準備をしています。技術者がウイルスを除去する前に完了する必要がある手順は次のうちどれですか?

A. システムの復元を無効にします。

B. マルウェア スキャンをスケジュールします。
C. エンド ユーザーを教育します。
D. Windows Update を実行します。
Answer: A (メーッセージを残す)
Before removing a Trojan virus from a workstation, a technician should disable System Restore. System Restore is a feature that allows users to restore their system to a previous state in case of problems or errors.
However, System Restore can also restore infected files or registry entries that were removed by antivirus software or manual actions. By disabling System Restore, a technician can ensure that the Trojan virus is completely removed and does not reappear after a system restore operation. Scheduling a malware scan may help detect and remove some malware but may not be effective against all types of Trojan viruses. Educating the end user may help prevent future infections but does not address the current issue of removing the Trojan virus. Running Windows Update may help patch some security vulnerabilities but does not guarantee that the Trojan virus will be removed. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

最新問題**: 60**
ユーザーは Web サイトで取引の詳細を確認できず、詳細ボタンをクリックしても何も起こりません。この問題を解決するには、ユーザーが行うべきことは次のうちどれですか?
A. ブラウザのキャッシュをクリアします。
B. ポップアップ ブロッカーを無効にします。
C. プライベート ブラウジングを構成します。
D. 有効な証明書を確認します。
Answer: B (メーッセージを残す)
Pop-up blockers can sometimes prevent essential pop-up windows required by websites to display transaction details.
* Clear the browser cache: Helps with loading issues but not specific to pop-ups.
* Disable the pop-up blocker: The correct solution, as it allows the blocked pop-up to be displayed.
* Configure private browsing: Prevents storing browsing data but does not affect pop-ups.
* Verify valid certificates: Ensures secure connections but does not resolve pop-up issues.
Reference: CompTIA A+ Exam Objectives [220-1102] - 2.10: Given a scenario, install and configure browsers and relevant security settings.

最新問題**: 61**
ユーザーはよく使用される Web ページにアクセスしようとしましたが、予期しない Web サイトにリダイレクトされました。Web ブラウザのキャッシュをクリアしても問題は解決しません。問題を解決するために技術者が NEXT を調査する必要があるのは、次のうちどれですか?
A. ファイアウォール ACL を有効にします。
B. localhost ファイルのエントリを調べます。
C. ルーティング テーブルを確認します。
D. ウイルス対策定義を更新します。
Answer: (解答を表示する)
A possible cause of the user being redirected to unexpected websites is that the localhost file entries have been modified by malware or hackers to point to malicious or unwanted websites. The localhost file is a text file that maps hostnames to IP addresses and can override DNS settings. By examining the localhost file entries, a technician can identify and remove any suspicious or unauthorized entries that may cause the redirection issue. Enabling firewall ACLs may not resolve the issue if the firewall rules do not block the malicious or unwanted websites. Verifying the routing tables may not resolve the issue if the routing configuration is correct and does not affect the web traffic. Updating the antivirus definitions may help prevent future infections but may not remove the existing malware or changes to the localhost file. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.

最新問題: **62**
デスクトップ スペシャリストは、新しく採用された従業員のために Windows 10 を実行するラップトップを準備する必要があります。技術者がラップトップを更新するために使用する必要がある方法は次のうちどれですか?
A. インターネットベースのアップグレード
B. 修復インストール
C. クリーン インストール
D. USB リペア
E. インプレース アップグレード
Answer: C (メーッセージを残す)
The desktop specialist should use a clean install to refresh the laptop. A clean install will remove all data and applications from the laptop and install a fresh copy of Windows 10, ensuring that the laptop is ready for the newly hired employee.

最新問題: **63**
技術者が、電源装置のショートが疑われるコンピューターのトラブルシューティングを行っています。技術者が最初に行うべきステップは次のうちどれですか?
A. 静電気防止用ストラップを装着する
B. PC を修理する前に、電源を切ってください。
C. PC を接地された作業台に置きます。
D. コンポーネントを ESD マットの上に置きます。
Answer: B (メーッセージを残す)
The first step a technician should take when troubleshooting a computer with a suspected short in the power supply is B. Disconnect the power before servicing the PC. This is to prevent any electrical shock or damage to the components. A power supply can be dangerous even when unplugged, as capacitors can maintain a line voltage charge for a long time1. Therefore, it is important to disconnect the power cord and press the power button to discharge any residual power before opening the case2. The other steps are also important for safety and proper diagnosis, but they should be done after disconnecting the power.

最新問題: **64**
技術者は Windows クライアントをドメインに参加させる必要があります。次のどれが必要ですか?
A. ローカルアクセス
B. インターネット接続
C. エンタープライズ管理権限
D. コンピュータのMACアドレス
Answer: C (メーッセージを残す)
Comprehensive and Detailed In-Depth Explanation:Joining a Windows client to a domain requires Enterprise administrative permissions because only domain administrators or authorized users can add computers to an Active Directory (AD) domain.
* A. Local access - Incorrect. A user does not need to be physically near the computer; the action can be performed remotely.
* B. Internet connection - Incorrect. A domain join occurs over a local network, not the internet.

* D. Computer MAC address - Incorrect. MAC addresses are used for network identification but are not required to join a domain.
Steps to Join a Domain:
* Open Settings > System > About > Domain or Workgroup Settings
* Click Change settings > Change
* Enter the domain name and provide admin credentials
* Restart the computer
Reference:
CompTIA A+ 220-1102, Objective 1.6 - Windows Installation and Configuration

最新問題**: 65**
変更管理レビュー委員会は、管理者の変更要求を拒否しました。管理者は、リスク分析とともに、変更の目的と範囲、日時、影響を受けるシステムを提供していました。
Which of the following should be included to approve this change?
A. エンドユーザーの承認
B. コスト分析
C. ロールバック計画
D. 標準メンテナンスウィンドウ
Answer: (解答を表示する**)**
A rollback plan is essential for a change to be approved by a change management review board. It outlines the steps to reverse a change in case something goes wrong, minimizing downtime and mitigating risk. Other items like end-user acceptance and cost analysis are important but not typically the deciding factor for approval.
Reference: CompTIA A+ 220-1102 Exam Objectives, Domain 4.2 Operational Procedures - Change Management

最新問題**: 66**
技術者が複数の Windows ワークステーションの OS を更新しています。複数のワークステーションを正常に更新した後、技術者は、アップグレードに PC の 1 台で使用可能な容量を超えるスペースが必要であることを示すエラーを受け取りました。アップグレードを続行するには、技術者は次のどれを実行する必要がありますか? (2 つ選択してください)。
A. 余分なハードウェアを取り外します。
B. 不要なファイルを削除します。
C. ドライバーソフトウェアを更新します。
D. システム ファイルを復元します。
E. 使用されていないデスクトップ アプリケーションをアンインストールします。
F. メモリを追加します。
Answer: (解答を表示する**)**
To free up space for the upgrade, the technician should delete unnecessary files and uninstall unused desktop applications. These actions will clear storage, making room for the update. Additional memory would not solve a storage issue, and driver updates are not relevant to the storage space problem.
Reference: CompTIA A+ 220-1102 Exam Objectives, Domain 1.9 Operating Systems - Installation

最新問題**: 67**
ユーザーは Web ベースのアプリケーションにアクセスできません。技術者は、コンピュータがどの Web ページにもまったくアクセスできないことを確認します。コンピュータは DHCP サーバーから IP アドレスを取得します。次に、技術者はユーザーが localhost に ping できることを確認します。ゲートウェイ、およびインターネット上の既知の IP アドレス! そして応答を受け取ります。問題の原因として最も考えられるのは次のうちどれですか?
A. ファイアウォールがアプリケーションをブロックしています。

B. 間違った VLAN が割り当てられました。
C. 不正なDNSアドレスが割り当てられました。
D. ブラウザのキャッシュをクリアする必要があります
Answer: (解答を表示する**)**
DNS (domain name system) is a protocol that translates domain names to IP addresses. If the computer has an incorrect DNS address assigned, it will not be able to resolve the domain names of web-based applications and access them. A firewall, a VLAN (virtual local area network) and a browser cache are not the most likely reasons for the issue, since the computer can ping known IP addresses on the internet and receive a response.
Verified References: https://www.comptia.org/blog/what-is-dns https://www.comptia.org/certifications/a

最新問題**: 68**
イメージング ラボでコンピューターをアップグレードした後、アップグレードしたコンピューターは IP アドレスを取得できません。
最も問題になりそうなのは次のどれですか?
A. スイッチは IPv6 アドレスのみを提供します。
B. イメージング ソフトウェアと互換性を持たせるには、OS を更新する必要があります。
C. スイッチのポート セキュリティが有効になっています。
D. スイッチはマルチキャスト トラフィックをサポートしていません。
Answer: C (メーッセージを残す**)**
When upgraded computers are not able to obtain an IP address, the issue often lies in the network configuration. Here's a
* Option A: The switch is only providing IPv6 addresses.This is unlikely because if the switch were providing IPv6 addresses, the devices would still receive an IP address, albeit an IPv6 one. The issue described indicates no IP address is being obtained at all.
* Option B: The OS must be updated to be compatible with the imaging software.This option is unrelated to obtaining an IP address. Compatibility with imaging software would not prevent the devices from getting an IP address.
* Option C: The switch has port security enabled.Correct Answer. Port security on a switch restricts access based on MAC addresses. If the MAC addresses of the upgraded computers are not recognized or have not been added to the allowed list, the switch will not provide network access, resulting in the computers not obtaining an IP address.
Reference: CompTIA A+ Core 1 (220-1101) Exam Objectives, Section 2.6
Option D: The switch does not support multicast traffic.This is unrelated to obtaining an IP address. Multicast traffic deals with specific types of network communication and would not affect the basic DHCP IP address assignment process.

最新問題**: 69**
技術者が Windows ワークステーションを手動で更新しています。現在、各ワークステーションはワークグループ環境で Windows Pro を実行しています。技術者は、より管理しやすい環境を作成するために、次のどの変更を加えることができますか?
A. すべてのワークステーションを OS の Pro バージョンから Home バージョンにダウングレードします。
B. すべてのワークステーションを Pro バージョンから Pro for Workstations にアップグレードします。
C. ドメインを作成し、管理目的でワークステーションをドメインに参加させます。
D. すべてのワークステーションが同じワークグループ名で動作していることを確認します。
Answer: C (メーッセージを残す**)**
Creating a domain and joining the workstations to it provides centralized management and control over the computers, making the environment much more manageable.
Here's why a domain is beneficial:
* Centralized administration: Manage user accounts, security policies, software installations, and updates from a single location (the domain controller).
* Group Policy: Implement and enforce security policies, configure system settings, and control user access to resources.

* Simplified updates: Deploy software updates and patches to multiple computers simultaneously.
* Improved security: Enforce stronger password policies, control access to sensitive data, and enhance overall network security.
Here's why the other options are less suitable:
* A. Downgrade all workstations from the Pro version to the Home version of the OS: The Home version has fewer features and management capabilities than the Pro version, making it less suitable for a business environment.
* B. Upgrade all workstations from the Pro version to Pro for Workstations: While Pro for Workstations has advanced features, it's designed for high-performance tasks and might not be necessary for all users.
* D. Make sure all workstations are operating under the same workgroup name: While being in the same workgroup allows for basic network sharing, it doesn't provide the centralized management capabilities of a domain.

最新問題**: 70**
ユーザーは、ユーザーの銀行を名乗る人物から電話を受け、ユーザーのアカウントが安全であることを確認するための情報を要求します。次のソーシャル エンジニアリング攻撃のうち、ユーザーが経験しているのはどれですか?
A. フィッシング
B. スミッシング
C. 捕鯨
D. ビッシング
Answer: D (メーッセージを残す**)**
The user is experiencing a vishing attack. Vishing stands for voice phishing and is a type of social-engineering attack that uses phone calls or voice messages to trick users into revealing personal or financial information. Vishing attackers often pretend to be from legitimate organizations, such as banks, government agencies or service providers, and use various tactics, such as urgency, fear or reward, to persuade users to comply with their requests. Phishing is a type of social-engineering attack that uses fraudulent emails or websites to trick users into revealing personal or financial information. Phishing does not involve phone calls or voice messages. Smishing is a type of social-engineering attack that uses text messages or SMS to trick users into revealing personal or financial information. Smishing does not involve phone calls or voice messages. Whaling is a type of social-engineering attack that targets high-profile individuals, such as executives, celebrities or politicians, to trick them into revealing personal or financial information. Whaling does not necessarily involve phone calls or voice messages. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.1

最新問題**: 71**
Windows OS を実行しているコンピューターでディスク暗号化を提供するのは次のどれですか?
A. ファイルボールト
B. ビットロッカー
C. 秘密鍵
D. PowerShell
Answer: B (メーッセージを残す**)**
BitLocker is a full-disk encryption feature included with certain editions of Windows, designed to protect data by providing encryption for entire volumes.
* Option A: FileVaultFileVault is a disk encryption program in macOS, not Windows.
* Option B: BitLockerBitLocker is the correct tool for disk encryption on Windows operating systems, providing full disk encryption.
* Option C: Private KeyA private key is part of public key infrastructure (PKI) used in encryption, but it is not a tool for disk encryption by itself.
* Option D: PowerShellPowerShell is a task automation and configuration management framework from Microsoft, not a tool for disk encryption.
References:
* CompTIA A+ 220-1102 Objective 2.5 (Manage and configure basic security settings in the Windows OS), particularly BitLocker for disk encryption.

最新問題**: 72**

技術者がデスクトップ PC のイメージを再作成しています。技術者は PC をネットワークに接続し、電源を入れます。技術者は、NIC を介してコンピューターを起動してコンピューターのイメージを作成しようとしますが、この方法は機能しません。
コンピュータがネットワーク経由でイメージング システムを起動できない理由として最も可能性が高いのは次のうちどれですか?
A. コンピュータの CMOS バッテリーが故障しました。
B. コンピューターの NIC が故障しています。
C. PXE ブート オプションが有効になっていません
D. 技術者がデスクトップをネットワークに接続するために使用しているイーサネット ケーブルに障害があります。
Answer: C (メーッセージを残す)
The most likely reason the computer is unable to boot into the imaging system via the network is that the PXE boot option has not been enabled. PXE (Preboot Execution Environment) is an environment that allows computers to boot up over the network, instead of from a local disk. In order for this to work, the PXE boot option must be enabled in the computer's BIOS settings. As stated in the CompTIA A+ Core 2 exam objectives, technicians should know how to enable PXE in BIOS to enable network booting on a computer.

最新問題**: 73**
ユーザーがワークステーションにログインできません。ユーザーから、日付が正しくないというエラー メッセージが報告されました。技術者が日付を確認し、正しいことを確認しましたが、システム クロックは 1 時間遅れています。技術者は、影響を受けているのはこのワークステーションのみであると判断しました。次のどれが最も可能性の高い問題ですか。
A. 時間のずれ
B. NTP 障害
C. Windows アップデート
D. CMOSバッテリー
Answer: A (メーッセージを残す)
Time drift occurs when the internal clock of a computer is not properly synchronized, often leading to discrepancies like being an hour behind. In this case, the workstation is the only device affected, indicating that it's likely a local issue. Time drift can happen if the system clock isn't syncing properly with an NTP (Network Time Protocol) server or if automatic daylight savings adjustments aren't enabled. It's less likely to be a CMOS battery issue since the technician has already verified the correct date and the system clock isn't completely reset (which is what happens when the CMOS battery fails).
References:
Troubleshooting Time Synchronization Issues in Windows (Help Desk Geek) (Zendesk)

最新問題**: 74**
ユーザーは Windows コンピュータからストレージ容量が少ないことを示す警告を受け取りました。この問題を最もよく解決するのは次のうちどれですか?
A. システム情報の確認
B. ディスク クリーンアップの実行中
C. レジストリの編集
D. パフォーマンス モニターの確認
E. メモリを増やす
Answer: B (メーッセージを残す)
To resolve an issue of low storage space on a Windows computer, the best approach is to Run Disk Cleanup (B). Disk Cleanup is a built-in utility that helps users free up space on their hard drives by deleting temporary files, system files, and other unnecessary files that are no longer needed, thereby resolving low storage space issues

最新問題**: 75**
ネットワーク管理者は、ユーザーのワークステーションでの USB ドライブを禁止する会社のセキュリティ ポリシーを強制したいと考えています。管理者がユーザーのワークステーションで実行する必要があるコマンドは次のうちどれですか?

A. ディスクパート
B. チャウン
C. gpupdate
D. netstat
Answer: C (メーッセージを残す**)**
To enforce a security policy that prohibits USB drives on user workstations, the network administrator should run the gpupdate (C) command. This command forces a Group Policy update, which can include policies to disable USB drives. Group Policy is a feature in Microsoft Windows that allows for centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment.

最新問題**: 76**
ユーザーがラップトップの問題について技術者に問い合わせます。ユーザーは、アプリケーションが起動せずに開いていると述べ、特定の Web サイトにアクセスしようとするとブラウザーがリダイレクトされます。ユーザーの問題の原因として最も可能性が高いのは次のうちどれですか?
A. キーロガー
B. クリプトマイナー
C. ウイルス
D. マルウェア
Answer: D (メーッセージを残す**)**
The most likely cause of the user's issue of applications opening without being launched and browser redirects when trying to go to certain websites is malware. Malware is a general term that refers to any software or code that is malicious or harmful to a computer or system. Malware can perform various unwanted or unauthorized actions on a computer or system, such as opening applications, redirecting browsers, displaying ads, stealing data, encrypting files or damaging hardware. Malware can infect a computer or system through various means, such as email attachments, web downloads, removable media or network connections. Keylogger is a type of malware that records and transmits the keystrokes made by a user on a keyboard. Keylogger can be used to steal personal or sensitive information, such as passwords, credit card numbers or chat messages. Keylogger does not typically open applications or redirect browsers but only captures user inputs. Cryptominers are a type of malware that use the computing resources of a computer or system to mine cryptocurrency, such as Bitcoin or Ethereum. Cryptominers can degrade the performance and increase the power consumption of a computer or system. Cryptominers do not typically open applications or redirect browsers but only consume CPU or GPU cycles. Virus is a type of malware that infects and replicates itself on other files or programs on a computer or system.

最新問題**: 77**
エンド オブ ライト オペレーティング システムの結果として生じるのは、次のうちどれですか?
A. オペレーティング システムは、ハードウェアの保証を無効にします。
B. オペレーティング システムが機能しなくなります。
C. オペレーティング システムは更新プログラムを受信しなくなりました。
D. オペレーティング システムは、新しいオペレーティング システムにデータを移行できません。
Answer: (解答を表示する**)**

End-of-life operating systems are those which have reached the end of their life cycle and are no longer supported by the software developer. This means that the operating system will no longer receive updates, security patches, or other new features. This can leave users vulnerable to security threats, as the system will no longer be protected against the latest threats. Additionally, this can make it difficult to migrate data to a newer operating system, as the old system is no longer supported.

最新問題: **78**
技術者は、ユーザーがシステムに接続しているときに、ユーザーのコンピュータのトラブルシューティングを行う必要があります。技術者は、Windows に組み込まれているリモート アクセス ツールを使用してユーザーのシステムに接続する必要もあります。ユーザーのコンピュータのトラブルシューティングに最適なオプションは次のうちどれですか?
A. 画面共有
B. MSRA
C. 仮想ネットワーク コンピュータ
D. RDP
Answer: (解答を表示する**)**
To troubleshoot a user's computer remotely while the user is connected, the best option is Microsoft Remote Assistance (MSRA). MSRA allows the technician to view and control the user's screen with their permission, facilitating an effective troubleshooting session without disconnecting the user.

最新問題: **79**
技術者が新しいアプリケーションをワークステーションにインストールしました。プログラムが正しく機能するには、パス環境変数にリストされている必要があります。次のコントロール パネル ユーティリティのうち、技術者が使用する必要があるのはどれですか?
A. システム
B. インデックス作成オプション
C. デバイス マネージャー
D. プログラムと機能
Answer: (解答を表示する**)**
System is the Control Panel utility that should be used to change the Path Environment Variable. The Path Environment Variable is a system variable that specifies the directories where executable files are located. To edit the Path Environment Variable, the technician should go to System > Advanced system settings > Environment Variables and then select Path from the list of system variables and click Edit.

最新問題: **80**
ある技術者は、最近のセキュリティ監査でブルート フォース攻撃に対して脆弱であることが判明したため、Windows ワークステーションの強化を希望しています。このような攻撃を軽減するには、技術者が次の機能のうちどれを実装する必要がありますか?
A. システム画面ロック
B. ログインのロックアウトに失敗しました
C. 制限されたユーザー権限
D. 保存データの暗号化
Answer: B (メーッセージを残す**)**
To mitigate brute-force attacks, implementing a failed log-in lockout feature is effective. This security measure temporarily disables user accounts after a specified number of unsuccessful login attempts, preventing attackers from continuously trying different password combinations to gain unauthorized access.

最新問題: **81**
ユーザーは、ワークステーションにインストールされているプログラムでオプション機能が有効になっていないことを確認済みです。技術者がオプション機能をインストールするには、次のどれを実行する必要がありますか?

A. [プログラムと機能] に移動し、プログラムをアンインストールして再インストールします。
B. 管理ツールに移動して、システム構成を編集します。
C. 管理ツールに移動してディスク クリーンアップを実行します。
D. [プログラムと機能] に移動し、プログラムを選択して [変更] をクリックします。
Answer: (解答を表示する**)**
When a user needs to install optional features for a program that is already installed, the technician should:
* Go to Programs and Features: Access this via the Control Panel.
* Select the program: Find the installed program in the list.
* Click on Change: The "Change" option allows modifications to the installed program, such as adding or removing features, without completely uninstalling and reinstalling the program.
This method is the most efficient and avoids unnecessary reinstallation of the software, which could lead to data loss or require reconfiguration.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 1.4: Given a scenario use the appropriate Microsoft Windows 10 Control Panel utility.
Windows application management documentation.

最新問題**: 82**
仮想化の使用によって生じる可能性のある環境への影響は次のどれですか?
A. エネルギー消費量の増加
B. 騒音公害
C. 必要なスペースの削減
D. メンテナンスの必要性が少ない
Answer: C (メーッセージを残す**)**
One of the key environmental benefits of using virtualization is the reduction in physical space requirements.
Virtualization allows multiple virtual machines to run on a single physical server, reducing the need for multiple physical servers. This consolidation leads to fewer physical machines, saving space in data centers and reducing the overall physical footprint.
* A. Greater energy consumption is incorrect as virtualization typically leads to reduced energy consumption due to the consolidation of hardware.
* B. Noise pollution can be reduced because fewer physical machines often mean less overall noise.
* D. Fewer maintenance needs is a possible benefit but not directly related to environmental effects like reduced space requirements.
References:
* CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 4.5: Summarizing environmental impacts and local environmental controls, including the benefits of virtualization.

最新問題**: 83**
ユーザーが銀行の Web サイトにアクセスすると、次のエラーが表示されました。
Web サイトによって提示されたセキュリティは、別の Web サイトのアドレスで発行されました。
技術者はユーザーに次のことを指示する必要があります。
A. ブラウザのキャッシュをクリアし、銀行に連絡してください。
B. サイトを閉鎖し、銀行に連絡してください。
C. サイトに進み、銀行に連絡します。
D. ブラウザを更新し、銀行に連絡してください。
Answer: (解答を表示する**)**

The technician should instruct the user to clear the browser cache and contact the bank (option A). This error indicates that the website the user is visiting is not the correct website and is likely due to a cached version of the website being stored in the user's browser. Clearing the browser cache should remove any stored versions of the website and allow the user to access the correct website. The user should also contact the bank to confirm that they are visiting the correct website and to report the error.

最新問題: **84**
コントロール パネルでネットワーク設定を変更した後、ネットワーク上に存在するデバイスが表示されません。ユーザーは、Windows 10 コンピューターで次の設定のどれを変更しましたか?
A. ネットワークの種類をプライベートからパブリックへ
B. Windows ファイアウォールをオンからオフにする
C. UAC レベルを最高レベルにする
D. ファイル共有権限
Answer: (解答を表示する**)**
Comprehensive and Detailed In-Depth Explanation:In Windows, when a user changes the network type from private to public, network discovery and file sharing are disabled for security reasons. Public networks are treated as untrusted, and devices on the network are hidden from the user.
* B. The Windows Firewall from on to off - Incorrect. Disabling the firewall does not block network visibility.
* C. The UAC level to its highest level - Incorrect. User Account Control (UAC) settings control administrative privileges, not network visibility.
* D. The file-sharing permissions - Incorrect. File-sharing permissions only affect access to shared folders, not network visibility.
Reference:
CompTIA A+ 220-1102, Objective 1.8 - Windows Networking and Configuration

最新問題: **85**
技術者は接続の問題をトラブルシューティングしており、トラフィックが正しいアップストリームの場所に流れていることを確認したいと考えています。技術者は次のコマンドのどれを使用する必要がありますか?
A. net use
B. nslookup
C. traceroute
D. netstat
Answer: C (メーッセージを残す**)**
To verify network traffic flow and identify where packets are being delayed or lost, the traceroute (tracert in Windows) command is the best tool. It maps out the path a packet takes to reach a destination, showing each hop along the way.
* Option A (Incorrect): net use is used for managing shared network resources, such as mapping network drives, and is not related to network traffic flow.
* Option B (Incorrect): nslookup is used to query DNS servers and resolve domain names to IP addresses but does not trace network traffic.
* Option C (Correct): traceroute (tracert in Windows) is the best tool to track the path of network packets and determine where delays or failures occur.
* Option D (Incorrect): netstat displays active network connections and listening ports but does not trace packet routes.
CompTIA A+ Core 2 Reference:
* 220-1102 Exam Objective 2.5 - Given a scenario, troubleshoot common network connectivity issues using appropriate tools and best practices.

最新問題: **86**
次のうち、変化の範囲を定義するものはどれですか?
A. スコープ
B. 目的

C. 分析
D. 衝撃
Answer: A (メーッセージを残す**)**
The term that defines the extent of a change is scope. Scope is a measure of the size, scale and boundaries of a project or an activity. Scope defines what is included and excluded in the project or activity, such as goals, requirements, deliverables, tasks and resources. Scope helps determine the feasibility, duration and cost of the project or activity. Scope also helps manage the expectations and needs of the stakeholders involved in the project or activity. Purpose is the reason or objective for doing a project or an activity. Purpose defines why the project or activity is important or necessary, such as solving a problem, meeting a need or achieving a goal. Purpose helps provide direction, motivation and justification for the project or activity. Analysis is the process of examining, evaluating and interpreting data or information related to a project or an activity.
Analysis helps identify, understand and prioritize issues, risks, opportunities and solutions for the project or activity. Impact is the effect or outcome of a project or an activity on something or someone else. Impact defines how the project or activity affects or influences other factors, such as performance, quality, satisfaction or value. Impact helps measure the success and effectiveness of the project or activity.
References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.2

最新問題**: 87**
次のマルウェアのうち、コンピューターへの管理アクセスを可能にするように設計されているのはどれですか?
A. ルートキット
B. トロイの木馬
C. ワーム
D. ランサムウェア
Answer: (解答を表示する**)**
A rootkit (Option A) is a type of malware designed to gain administrative (root) access to a system while hiding its presence. Rootkits can manipulate system processes and files to remain undetected, making them particularly dangerous.
* Trojan (Option B) is malware disguised as legitimate software but doesn't necessarily provide administrative access.
* Worm (Option C) spreads across networks but doesn't grant administrative access.
* Ransomware (Option D) encrypts data and demands a ransom but doesn't typically provide ongoing administrative access.
CompTIA A+ Core 2 References:
* 2.3 - Explain malware types, including rootkits and their purpose .

最新問題**: 88**
ユーザーがオフィスにいる場合、ユーザーの携帯電話での Web ページの読み込みが遅くなります。この問題を最もよく説明するのは次のどれですか。
A. データ使用量の制限を超えました
B. 応答時間が遅い
C. ネットワークサービスが低下しました
D. ネットワークトラフィックが高い
Answer: (解答を表示する**)**
When a user experiences slow web page loading on their phone while in the office, the most likely cause is:
* High network traffic: In an office environment, many devices are often connected to the network simultaneously, which can lead to congestion and slow internet speeds. High network traffic means more devices are competing for the same bandwidth, causing delays.
* Exceeded the data usage limit: This typically applies to cellular data plans, not Wi-Fi in an office setting.
* Sluggish response time: This is a symptom rather than a cause and can result from high network traffic.
* Degraded network service: While this could be a factor, it is broader and less specific than high network traffic, which is more directly related to the user's experience.
Reference:

CompTIA A+ 220-1102 Exam Objectives, Section 2.7: Given a scenario troubleshoot problems with wired and wireless networks.
Network performance troubleshooting documentation.

最新問題: **89**
次の機能のうち、技術者が Windows 10 Professional デスクトップでポリシーを構成できるのはどれですか?
A. gpedit
B. gpmc
C. gpresult
D. gpupdate
Answer: A (メーッセージを残す**)**
The feature that allows a technician to configure policies in a Windows 10 Professional desktop is gpedit.
Gpedit is a command that opens the Local Group Policy Editor, which is a utility that allows users to view and modify local group policies on their Windows PC. Local group policies are a set of rules and settings that control the behavior and configuration of the system and its users. Local group policies can be usedto configure policies such as security, network, software installation and user rights. Gpmc is a command that opens the Group Policy Management Console, which is a utility that allows users to view and modify domain-based group policies on a Windows Server. Domain-based group policies are a set of rules and settings that control the behavior and configuration of the computers and users in a domain. Domain-based group policies are not available on a Windows 10 Professional desktop. Gpresult is a command that displays the result of applying group policies on a Windows PC. Gpresult can be used to troubleshoot or verify group policy settings but not to configure them. Gpupdate is a command that updates or refreshes the group policy settings on a Windows PC. Gpupdate can be used to apply new or changed group policy settings but not to configure them. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

最新問題: **90**
技術者が新しい Windows 10 ワークステーションを保護しており、スクリーンセーバー ロックを有効にしたいと考えています。技術者が使用すべき Windows 設定のオプションは次のうちどれですか?
A. アクセスのしやすさ
B. プライバシー
C. パーソナライゼーション
D. アップデートとセキュリティ
Answer: C (メーッセージを残す**)**
The technician should use the Personalization option in the Windows settings to enable a Screensaver lock.
The Personalization option allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver. The technician can enable a Screensaver lock by choosing a screensaver from the drop-down menu, setting a wait time in minutes and checking the box that says "On resume, display logon screen". This will lock the computer and require a password or PIN to log back in after the screensaver is activated. Ease of Access is an option in the Windows settings that allows users to adjust accessibility features and settings, such as narrator, magnifier, high contrast and keyboard shortcuts. Ease of Access is not related to enabling a Screensaver lock. Privacy is an option in the Windows settings that allows users to manage privacy and security settings, such as location, camera, microphone and app permissions. Privacy is not related to enabling a Screensaver lock. Update and Security is an option in the Windows settings that allows users to check and install updates, troubleshoot problems, backup files and restore system. Update and Security is not related to enabling a Screensaver lock. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.7

最新問題: **91**
ユーザーが誤って間違ったワープロ アプリケーションを iMac にインストールしてしまいました。ユーザーが間違ったアプリケーションをアンインストールできるのは次のうちどれですか?
A. アプリケーションをデスクトップに移動し、削除を押します。
B. Finder でアプリケーションを特定し、ゴミ箱にドラッグします。
C. Spotlight を使用してアプリケーションを検索し、アプリケーションを実行します。

D. Time Machine を使用して、インストール前の日付に戻ります。
Answer: B (メーッセージを残す)
On macOS, uninstalling an application typically involves locating the app in Finder and dragging it to the Trash. This method is straightforward and commonly used for removing unwanted applications. The other options do not directly relate to the standard process of uninstalling applications on a Mac.

最新問題: **92**
システム管理者は、ユーザーがアクセスできる Web サイトのリストを含む新しいドキュメントを作成しています。管理者が作成する可能性が最も高いドキュメントの種類は次のうちどれですか?
A. アクセス制御リスト
B. 利用規定
C. インシデント レポート
D. 標準操作手順
Answer: A (メーッセージを残す)
An access control list (ACL) is a list of permissions associated with a system resource (object), such as a website. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects1. A systems administrator can create an ACL to define the list of websites that users are allowed to access.
References: 1: Access-control list - Wikipedia (https://en.wikipedia.org/wiki/Access-control_list)

最新問題: **93**
ユーザーが Android タブレット上で組織独自のアプリケーションを開こうとするたびに、アプリケーションはすぐに終了します。他のアプリケーションは正常に動作しています。次のトラブルシューティング アクションのうち、問題を解決する可能性が最も高いのはどれですか? (2 つ選択してください)。
A. アプリケーションをアンインストールする
B. タブレットへの root アクセスの取得
C. Webブラウザのキャッシュをリセットする
D. アプリケーションキャッシュの削除
E. アプリケーションストレージのクリア
F. モバイルデバイス管理を無効にする
Answer: A,E (メーッセージを残す)
Uninstalling and reinstalling the application can resolve the issue of it crashing immediately on an Android tablet, as it can fix any corrupted or missing files or settings. Clearing the application storage can also resolve the issue, as it can free up space and remove any conflicting data. Gaining root access to the tablet, resetting the web browser cache, deleting the application cache and disabling mobile device management are not likely to resolve the issue, as they do not affect how the application runs. Verified References: https://www.comptia.
org/blog/how-to-fix-android-apps-crashing https://www.comptia.org/certifications/a

最新問題: **94**
次の Windows 10 エディションのうち、コンピューターにリモートでアクセスする必要がある単一のユーザーにとって最もコスト効率が高く適切なのはどれですか?
A. 教育

B. プロ
C. エンタープライズ
D. ホーム
Answer: B (メーッセージを残す)
For a single user who needs to access their computer remotely, the Windows 10 Pro edition is the most cost-effective and appropriate choice. It includes features such as Remote Desktop, which are essential for remote access.
* Option A: EducationThis edition is designed for academic institutions and includes educational features. It is not the most cost-effective for a single user.
* Option B: ProWindows 10 Pro includes Remote Desktop and other business features. It is suitable and cost-effective for single users needing remote access.
* Option C: EnterpriseThis edition includes advanced features for large organizations and is more expensive, making it less cost-effective for a single user.
* Option D: HomeWhile cost-effective, Windows 10 Home does not include the Remote Desktop feature, making it unsuitable for this requirement.
References:
* CompTIA A+ 220-1102 Objective 1.1 (Identify basic features of Microsoft Windows editions), particularly comparing editions based on features and cost.

最新問題**: 95**
技術者が Linux ディストリビューションの MAC アドレスを取得するために使用できるコマンドはどれですか?
* ネット使用
A. ifconfig
B. ネットスタット
C. ピン
Answer: B (メーッセージを残す)
The ifconfig command is a tool for configuring network interfaces that any Linux system administrator should know. It is used to bring interfaces up or down, assign and remove addresses and routes, manage ARP cache, and much more1. One of the information that ifconfig can display is the MAC address of each network interface, which is a unique identifier of the physical layer of the network device. The MAC address is usually shown as a hexadecimal string separated by colons, such as 00:0c:29:3f:5c:1f. To get the MAC address of a Linux distribution, a technician can use the ifconfig command without any arguments, which will show the details of all the active network interfaces, or specify the name of a particular interface, such as eth0 or wlan0, to show only the details of that interface.
References1: Linux Commands - CompTIA A+ 220-1102 - 1.11 - Professor Messer IT Certification Training Courses1

最新問題**: 96**
ユーザーの会社の電話には保留中のソフトウェア アップデートがいくつかあります。技術者は次の手順を実行します。
*携帯電話を再起動しました
※Wi-Fiに接続しています
※従量制データの無効化
技術者が次に行うべきことは次のうちどれですか?
A. 工場出荷時の設定に戻します。
B. ブラウザ履歴を消去します。
C. アプリケーションをアンインストールして再インストールします。
D. キャッシュをクリアします。
Answer: D (メーッセージを残す)
After rebooting the phone, connecting to Wi-Fi, and disabling metered data, the next step the technician should take is to Clear the cache (D). Clearing the cache can resolve issues with the phone's performance and is often necessary before updating software to ensure that the updates can be downloaded and installed without issues. It removes temporary files that may be interfering with the update process.

最新問題: **97**
ユーザーの携帯電話の動作が遅くなった システム管理者が、デバイス上でいくつかの悪意のあるアプリケーションを発見し、電話をリセットしました。管理者が MDM ソフトウェアをインストールしました。今後この脅威からデバイスを保護するために、管理者が行うべきことは次のうちどれですか? (2 つ選択)。
A. デバイスのルートを防ぐ
B. 生体認証を無効にする
C. ロック解除画面で PIN を要求する
D. 開発者モードを有効にする
E. サードパーティ アプリケーションのインストールをブロックする
F. GPS スプーフィングを防止する
Answer: (解答を表示する**)**
To help secure the device against this threat in the future, the administrator should require a PIN on the unlock screen and block a third-party application installation. Requiring a PIN on the unlock screen can help to prevent unauthorized access to the device, while blocking third-party application installation can help to prevent malicious applications from being installed on the device.

最新問題: **98**
技術者が複数のシステム上のさまざまなサービスのセットアップを自動化するために使用する可能性が高い言語は次のどれですか。
A. SQL
B. HTML
C. PowerShell
D. C#
Answer: C (メーッセージを残す**)**
PowerShell (Option C) is a powerful scripting language used in Windows environments for automating tasks, including the configuration of services across multiple systems. It is widely used by system administrators for scripting and automating administrative tasks.
* SQL (Option A) is used for managing databases, not for scripting system configurations.
* HTML (Option B) is a markup language for web development, not for automating services.
* C# (Option D) is a general-purpose programming language but is not primarily used for administrative automation tasks.
CompTIA A+ Core 2 References:
* 4.8 - Basics of scripting, including PowerShell for automation

最新問題: **99**
ユーザーが疑わしい電子メールの添付ファイルをクリックした後、ユーザーの PC のパフォーマンスが低下しています。技術者は、1 つのプロセスが RAM、CPU、およびネットワーク リソースを 100% 使用していることに気付きました。技術者が最初に行うべきことは何ですか。
A. コンピュータをネットワークから切断する
B. ウイルススキャンを実行する
C. コンピュータを再起動します
D. サイバーセキュリティのベストプラクティスについてユーザーに教育する
Answer: A (メーッセージを残す**)**
The technician should disconnect the computer from the network (Option A) first to prevent any further spread of the infection or data loss. Once the machine is isolated from the network, the technician can safely investigate the malware without risking infection to other systems.
* Running an antivirus scan (Option B) comes after isolating the system.

* Rebooting the computer (Option C) could lead to the loss of critical information or make it harder to diagnose the issue.
* Educating the user (Option D) is important but should happen after resolving the immediate issue.
CompTIA A+ Core 2 References:
* 3.3 - Best practices for malware removal, including isolating the system first.

最新問題**: 100**
次のオペレーティング システムのうち、工場で在庫管理システムを実行するために使用される可能性が最も高いのはどれですか?
A. Windows
B. Chrome OS
C. アンドロイド
D. iOS
Answer: A (メーッセージを残す**)**
Windows is widely used in industrial and business environments due to its major market presence, extensive support from the industry, and a broad selection of operating system options. It supports a wide variety of software, making it suitable for running complex systems like an inventory management system in a factory.
Other options such as Chrome OS, Android, and iOS are either more consumer-oriented or designed for specific types of devices, making them less likely choices for an industrial application like inventory management.References:Professor Messer's CompTIA 220-1102 A+ Course Notes.

最新問題**: 101**
技術者は、権限を昇格させずにシステム変更を容易にするには、Windows ワークステーション上で管理者アクセスが必要です。このタスクを最もよく達成できるのは次のうちどれですか?
A. グループ ポリシー エディター
B. ローカル ユーザーとグループ
C. デバイスマネージャー
D. システム構成
Answer: (解答を表示する**)**
Local Users and Groups is the best option to accomplish this task. Local Users and Groups is a tool that allows managing the local user accounts and groups on a Windows workstation. The technician can use this tool to create a new user account with administrator privileges or add an existing user account to the Administrators group. This way, the technician can log in with the administrator account and make system changes without elevating permissions. Group Policy Editor, Device Manager, and System Configuration are not correct answers for this question. Group Policy Editor is a tool that allows configuring policies and settings for users and computers in a domain environment. Device Manager is a tool that allows managing the hardware devices and drivers on a Windows workstation. System Configuration is a tool that allows modifying the startup options and services on a Windows workstation. None of these tools can directly grant administrator access to a user account. References:
* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 13
* CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 103

最新問題**: 102**
技術者は、ネットワーク上のコンピュータがマルウェアに感染していると考えています。技術者はマルウェア除去ツールの使用を何度か試みましたが、問題は解決しません。技術者は次に何をすべきでしょうか。
A. 前回の正常なバックアップからコンピュータを復元する
B. コンピュータをセーフモードで再起動します
C. 新しいエンドポイント保護ツールを購入する
D. さらなる感染を防ぐためにシステムリカバリを使用してください
Answer: (解答を表示する**)**

Rebooting the computer into safe mode (Option B) limits the processes and services that run, which can help in isolating and removing persistent malware that might be hiding in normal mode. Safe mode provides a cleaner environment to troubleshoot and remove malware.
* Restoring from a backup (Option A) may work but should be considered after attempts to clean the infection.
* Purchasing a new endpoint protection tool (Option C) is unnecessary at this stage since existing tools can be run in safe mode.
* Using system recovery (Option D) could potentially remove the infection, but it's a more drastic step that may not be necessary yet.
CompTIA A+ Core 2 References:
* 3.3 - Best practices for malware removal, including booting into safe mode

最新問題**: 103**
ある会社では、毎日インターネット経由で大量のファイルをダウンロードしています。ダウンロード中にファイルが変更または破損していないことを確認する方法が必要です。ファイルを検証するために、会社が行うべきことは次のどれですか。
A. 閲覧データを消去する
B. SSL証明書をインストールする
C. ハッシュ値を確認する
D. 信頼できるソースを使用する
Answer: C (メーッセージを残す**)**
Comprehensive and Detailed In-Depth Explanation:Checking the hash value (such as MD5, SHA-1, or SHA-256) is the best way to verify file integrity after downloading. A hash function generates a unique string for a file. If even a single bit in the file is changed, the hash value will be different. Many software vendors provide hash values (checksums) on their websites to help users confirm that the files were downloaded without corruption or tampering.
* A. Clear browsing data - Incorrect. Clearing browsing data does not affect downloaded files or their integrity.
* B. Install SSL certificates - Incorrect. SSL certificates encrypt data transmission but do not verify the integrity of downloaded files.
* D. Use trusted sources - While downloading files from trusted sources reduces the risk of corruption, it does not verify file integrity.
Reference:
CompTIA A+ 220-1102, Objective 2.5 - Basic Security Concepts
CompTIA A+ 220-1102, Objective 4.3 - Best Practices for Data Integrity

最新問題**: 104**
技術者が顧客のオフィスで作業しているときに、技術者の家族から緊急ではない状況について繰り返し電話やテキスト メッセージが届きます。技術者は次のうちどれを行う必要がありますか。
A. 脇に寄って答えてください。
B. 電話をサイレントモードにします。
C. テキストで返信します。
D. 電話を無視して作業を続けます。
Answer: (解答を表示する**)**
The correct answer is B. Put the phone on silent.
* IT professionals must maintain professionalism and minimize distractions while on the job.
* Putting the phone on silent ensures that the technician stays focused without causing disruptions to their work environment.
* If necessary, the technician can check and respond during an appropriate break.
Why Other Options Are Incorrect:
* A. Step aside and answer - This is unprofessional unless it is an emergency. Taking personal calls in front of a client can give a bad impression.
* C. Text a reply - While this may seem reasonable, texting in front of a client still creates an unprofessional image.

* D. Ignore the phone and continue working - While ignoring calls prevents distractions, a silent mode ensures that notifications do not cause disturbances (e.g., vibrations or sounds).
CompTIA A+ 220-1102 Exam Reference:
* Objective 5.1 - Given a scenario, use the best practice procedures for documentation, privacy, and professionalism.

最新問題**: 105**
ユーザーがモバイル デバイスの OS を更新します。頻繁に使用されるアプリケーションは、デバイスの起動直後に一貫して応答しなくなります。次のトラブルシューティング手順のうち、ユーザーが最初に実行する必要があるのはどれですか?
A. アプリケーションのキャッシュを削除します。
B. アプリケーションの更新を確認します。
C. OS アップデートをロールバックします。
D. アプリケーションをアンインストールして再インストールします。
Answer: B (メーッセージを残す**)**
Checking for application updates is the first troubleshooting step that the user should perform, because the application may not be compatible with the new OS version and may need an update to fix the issue. Deleting the application's cache, rolling back the OS update, or uninstalling and reinstalling the application are possible solutions, but they are more time-consuming and disruptive than checking for updates. References: :
https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam-objectives : https://www.
lifewire.com/how-to-update-apps-on-android-4173855

最新問題**: 106**
リモート ユーザーのスマートフォンのパフォーマンスが非常に遅いです。ユーザーは、再起動後にパフォーマンスがわずかに向上しますが、その後は再びパフォーマンスが低下することに気づきます。また、ユーザーは、会社の企業ゲスト ネットワークに接続した後も電話の速度が上がらないことにも気づきました。技術者は、電話機に多数のアプリケーションがインストールされていることに気付きました。問題の原因として最も考えられるのは次のうちどれですか?
A. ユーザーは電波状態の悪いエリアにいます。
B. ユーザーが実行しているプロセスが多すぎます。
C. スマートフォンにマルウェアがインストールされています。
D. スマートフォンはジェイルブレイクされました。
Answer: (解答を表示する**)**
One of the common reasons for a slow smartphone performance is having too many apps installed and running in the background. These apps consume the device's memory (RAM) and CPU resources, which can affect the speed and responsiveness of the phone. Rebooting the phone can temporarily clear the RAM and stop some background processes, but they may resume after a while. Connecting to a different network does not affect the performance of the phone, unless the network is congested or has a poor signal. The user can improve the phone's performance by uninstalling unused apps, clearing app caches, and restricting background activities12. Malware can also slow down a phone, but it is not the most likely cause in this scenario, as the user does not report any other symptoms of infection, such as pop-ups, battery drain, or data usage spikes3. Jailbreaking a phone can also affect its performance, but it is not a cause, rather a consequence, of the user's actions. Jailbreaking is the process of removing the manufacturer's restrictions on a phone, which allows the user to install unauthorized apps, customize the system, and access root privileges4. However, jailbreaking also exposes the phone to security risks, voids the warranty, and may cause instability or compatibility issues5.
References1: Speed up a slow Android device - Android Help - Google Help2: Why your phone slows down over time and what you can do to stop it | TechRadar3: How to tell if your phone has a virus | Norton4: What is Jailbreaking? - Definition from Techopedia5: What is Jailbreaking an iPhone? - Lifewire

最新問題: **107**
管理者は、今後のサーバー展開の変更要求に対する承認を受け取りました。次のステップのうち、次に完了する必要があるのはどれですか?
A. リスク分析を実行します。
B. デプロイを実装します。
C. エンド ユーザーの同意を確認する
D. 得られた教訓を文書化します。
Answer: (解答を表示する**)**
Before making any changes to the system, it is important to assess the risks associated with the change and determine whether it is worth implementing. Risk analysis involves identifying potential risks, assessing their likelihood and impact, and determining what steps can be taken to mitigate them. It is important to perform this step before making any changes, as this allows the administrator to make an informed decision about whether or not the change should be implemented. Once the risks have been assessed and the administrator has decided to go ahead with the change, the next step is to implement the deployment.

最新問題: **108**
次のうち最も安全な画面ロックはどれですか?
A. 顔
B. スワイプ
C. パスワード
D. 指紋
Answer: (解答を表示する**)**
Comprehensive and Detailed In-Depth Explanation:Passwords provide the highest level of security because they cannot be bypassed using biometric spoofing techniques.
* A. Face - Can be fooled with 2D images (on some devices).
* B. Swipe - Very weak security.
* D. Fingerprint - More secure than face/swipe but can still be faked.
Reference:
CompTIA A+ 220-1102, Objective 2.3 - Authentication and Security Methods

最新問題: **109**
変更管理計画が確実に遵守されるようにするには、次のうちどれを文書化する必要がありますか?
A. 変更の範囲
B. 変更の目的
C. ロールバック計画の変更
D. 変更リスク分析
Answer: (解答を表示する**)**
The scope of the change is one of the elements that should be documented to ensure that the change management plan is followed. The scope of the change defines the boundaries and limitations of the change, such as what is included and excluded, what are the deliverables and outcomes, what are the assumptions and constraints, and what are the dependencies and risks. The scope of the change helps

to clarify the expectations and objectives of the change, as well as to prevent scope creep or deviation from the original plan. The scope of the change also helps to measure the progress and success of the change, as well as to communicate the change to the stakeholders and the team

最新問題**: 110**
ユーザーのコンピュータ画面に次のエラーが表示されます。
オペレーティング システムが見つかりません
技術者が最初に実行する必要があるトラブルシューティング手順は次のどれですか?
A. 外部ストレージを切断する
B. BIOSをフラッシュする
C. SATAケーブルを交換する
D. デバイスをセーフモードでオンにする
Answer: A (メーッセージを残す**)**
The first step is to disconnect external storage (Option A). Sometimes, the system may be attempting to boot from an external drive or USB device instead of the internal hard drive. By removing the external storage, the system will attempt to boot from the correct drive.
* Flashing the BIOS (Option B) is more complex and typically unnecessary for this issue.
* Replacing the SATA cable (Option C) may help if there's a hardware issue, but it's not the first troubleshooting step.
* Turning on the device in safe mode (Option D) would not work if no operating system is detected.
CompTIA A+ Core 2 References:
* 5.1 - Apply troubleshooting methodologies, including steps for resolving boot issues.

最新問題**: 111**
ウイルス対策ソフトウェアは、ワークステーションが隔離できないランサムウェアに感染していることを示しています。
ホストや他のシステムへのさらなる損傷を防ぐために、最初に実行する必要があるのは次のうちどれですか?
* 機械の電源を切ります。
A. 完全なウイルス対策スキャンを実行します。
B. LANカードを取り外します。
C. 別のエンドポイント ソリューションをインストールします。
Answer: A (メーッセージを残す**)**
Turning off the machine is the first and most urgent step to prevent further damage to the host and other systems. Ransomware can encrypt files, steal data, and spread to other devices on the network if the infected machine remains online. Turning off the machine will stop the ransomware process and isolate the machine from the network12. The other options are either ineffective or risky. Running a full antivirus scan may not detect or remove the ransomware, especially if it is a new or unknown variant. Removing the LAN card may disconnect the machine from the network, but it will not stop the ransomware from encrypting or deleting files on the local drive. Installing a different endpoint solution may not be possible or helpful if the ransomware has already compromised the system or blocked the installation.
References: 1 3 steps to prevent and recover from ransomware(https://www.microsoft.com/en-us/security/blog
/2021/09/07/3-steps-to-prevent-and-recover-from-ransomware/)2 #StopRansomware Guide | CISA (https://www.cisa.gov/stopransomware/ransomware-guide).

最新問題**: 112**
ワイヤレス セキュリティに WEP プロトコルを使用する場合の最も重大な欠点は次のどれですか。
A. 複雑な構成プロセス
B. データ転送速度が遅い

C. キークラッキング攻撃に対する脆弱性
D. 古いデバイスとの非互換性
Answer: C (メーッセージを残す**)**
Comprehensive and Detailed In-Depth Explanation:WEP (Wired Equivalent Privacy) is highly vulnerable to key-cracking attacks, as its encryption key can be easily broken with freely available tools.
* A. Complex configuration process - Incorrect. WEP is actually easy to configure.
* B. Slow data transfer speed - Incorrect. WEP does not significantly impact speed.
* D. Incompatibility with older devices - Incorrect. WEP is compatible with older devices but is insecure.
Reference:
CompTIA A+ 220-1102, Objective 2.6 - Wireless Security Protocols

最新問題**: 113**
ユーザーが企業管理のモバイル デバイスに関するチケットをオープンしました。割り当てられた技術者は、OS のいくつかのバージョンが古いことに気づきました。自動更新がオンになっているため、ユーザーは OS のバージョンが最新ではないことに気づきません。問題の原因として最も考えられるのは次のうちどれですか?
A. デバイスには、OS アップデートをダウンロードするための十分な空き容量がありません。
B. デバイスをメジャー リリースに更新するには、ドメイン管理者の確認が必要です。
C. 最新バージョンのOSに対応していません。
D. 企業のセキュリティ ポリシーにより、デバイスのアップデートが制限されています。
Answer: (解答を表示する**)**
A corporate security policy can restrict a corporate-managed mobile device from updating its OS automatically, even if the auto-update feature is turned on. This can be done to prevent compatibility issues, security risks or performance problems caused by untested or unwanted updates. The device administrator can control when and how the updates are applied to the device. The device not having enough free space, needing domain administrator confirmation or being incompatible with the newest version of the OS are not likely causes of the issue, since the user would receive an error message or a notification in those cases.
Verified References: https://www.comptia.org/blog/mobile-device-management https://www.comptia.org
/certifications/a

最新問題**: 114**
最近、ある中小企業に新しいスパム ゲートウェイが導入されました。ユーザーはまだスパムを受信することがあります。管理チームは、ユーザーがメッセージを開いてネットワーク システムに感染する可能性があることを懸念しています。この問題に対処するための最も効果的な方法は次のうちどれですか?
A. 迷惑メールゲートウェイの調整
B. スパム アプライアンスのファームウェアを更新しています
C. AV設定の調整
D. ユーザートレーニングの提供
Answer: D (メーッセージを残す**)**
The most effective method for dealing with spam messages in a small business is to provide user training1. Users should be trained to recognize spam messages and avoid opening them1. They should also be trained to report spam messages to the IT department so that appropriate action can be taken1. In addition, users should be trained to avoid clicking on links or downloading attachments from unknown sources1. By providing user training, the management team can reduce the risk of users opening spam messages and potentially infecting the network systems1.

最新問題**: 115**

ユーザーが新しいラップトップの電源を入れ、専用のソフトウェアにログインしようとすると、アドレスが既に使用されているというメッセージが表示されます。ユーザーが古いデスクトップにログオンすると、同じメッセージが表示されます。技術者がアカウントを確認すると、ユーザーがソフトウェアに接続する前に特別に割り当てられたアドレスが必要であるというコメントが表示されます。技術者が問題を解決する可能性が最も高いのは、次のうちどれですか?
A. ラップトップとデスクトップの間の LAN 接続をブリッジします。
B. ラップトップ構成を DHCP に設定して、競合を防ぎます。
C. デスクトップから静的 IP 構成を削除します。
D. ラップトップのネットワーク カードに欠陥がある可能性があるため、ネットワーク カードを交換します。
Answer: C (メーッセージを残す**)**
The new laptop was set up with the static IP it needs to connect to the software. The old desktop is still configured with that IP, hence the conflict.

最新問題**: 116**
技術者が macOS コンピューターに新しいソフトウェアをインストールしています。技術者が最も使用する可能性が高いファイルの種類は次のうちどれですか?
A. .deb
B. .vbs
C. .exe
D. .app
Answer: D (メーッセージを残す**)**
The file type that the technician will MOST likely use when installing new software on a macOS computer is
.app. This is because .app is the file extension for applications on macOS1.

最新問題**: 117**
Python 言語で既定で使用されるスクリプトの種類は次のうちどれですか?
A. .ps1
B. .vbs
C. .bat
D. .py
Answer: D (メーッセージを残す**)**
The script type that is used with the Python language by default is .py. .py is a file extension that indicates a Python script file that contains Python code that can be executed by a Python interpreter or compiler. Python is a high-level, general-purpose and interpreted programming language that can be used for various applications, such as web development, data analysis, machine learning and automation. .ps1 is a file extension that indicates a PowerShell script file that contains PowerShell code that can be executed by a PowerShell interpreter or compiler. PowerShell is a task-based, command-line and scripting language that can be used for system administration and automation on Windows systems. .vbs is a file extension that indicates a VBScript file that contains VBScript code that can be executed by a VBScript interpreter or compiler.
VBScript is an Active Scripting language that can be used for web development and automation on Windows systems. .bat is a file extension that indicates a batch file that contains a series of commands that can be executed by a command-line interpreter or shell on Windows systems. Batch files can be used for system administration and automation on Windows systems. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 4.3

最新問題**: 118**
技術者は、コンピューターを開く前にデスクトップ コンピューターのプロセッサを交換しています。技術者は、内部コンポーネントが保護されていることを確認したいと考えています。次の安全手順のうち、PC のコンポーネントを保護するのに最も適しているのはどれですか? (2 つ選択)。
A. ESD ストラップの使用

B. コンピュータを電源から切り離す
C. PSU を帯電防止バッグに入れる
D. 適切な換気の確保
E. 換気扇のホコリ取り
F. 機器の接地の確認
Answer: A,C (メーッセージを残す)
The two safety procedures that would best protect the components in the PC are:
* Utilizing an ESD strap
* Placing the PSU in an antistatic bag
https://www.professormesser.com/free-a-plus-training/220-902/computer-safety-procedures-2/
https://www.skillsoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f4a-a659-dc98f1f00158

最新問題**: 119**
技術者は、復元するのに 2 セットのテープしか必要としないワークステーションでバックアップ方法をセットアップしています。このタスクを達成するのに最も適しているのは次のうちどれですか?
A. 差分バックアップ
B. オフサイトバックアップ
C. 増分バックアップ
D. フルバックアップ
Answer: (解答を表示する)
To accomplish this task, the technician should use a Full backup method1 A full backup only requires two sets of tapes to restore because it backs up all the data from the workstation. With a differential backup, the backups need to be taken multiple times over a period of time, so more tapes would be needed to restore the data1

最新問題**: 120**
顧客がヘルプ デスクに電話して、デスクトップの壁紙を変更する方法についての指示を求めました。技術者が推奨する Windows 10 設定は次のうちどれですか?
A. パーソナライゼーション
B. アプリ
C. アップデート
D. 表示
Answer: (解答を表示する)
Personalization is a Windows 10 setting that allows a user to modify the desktop wallpaper, as well as other aspects of the appearance and behavior of the desktop, such as colors, themes, sounds, etc. Apps is a Windows 10 setting that allows a user to manage the installed applications and their features. Updates is a Windows 10 setting that allows a user to check for and install the latest updates for the OS and other components. Display is a Windows 10 setting that allows a user to adjust the screen resolution, brightness, orientation, etc. Verified References: https://www.comptia.org/blog/windows-10-settings https://www.
comptia.org/certifications/a

最新問題**: 121**
従業員は、職場のコンピューターにマルウェアが感染していることについて技術者に繰り返し連絡しました。技術者はマルウェアを数回削除しましたが、ユーザーの PC は感染し続けます。将来の感染リスクを軽減するために技術者が行うべきことは次のうちどれですか?
A. ファイアウォールを構成します。

B. バックアップからシステムを復元します。
C. エンド ユーザーを教育します。
D. ウイルス対策プログラムを更新します。
Answer: C (メーッセージを残す)
Malware is software that infects computer systems to damage, disable or exploit the computer or network for various malicious purposes5. Malware is typically distributed via email attachments, fake internet ads, infected applications or websites, and often relies on user interaction to execute6. Therefore, one of the most effective ways to prevent malware infections is to educate the end user about the common signs and sources of malware, and how to avoid them7. Configuring the firewall, restoring the system from backups, and updating the antivirus program are also important security measures, but they do not address the root cause of the user's repeated infections, which is likely due to a lack of awareness or caution.
References5: Malware: what it is, how it works, and how to stop it - Norton6: How to Prevent Malware: 15 Best Practices for Malware Prevention7: 10 Security Tips for How to Prevent Malware Infections - Netwrix

最新問題**: 122**
あるユーザーから、週の初めに疑わしい電子メールがワークステーションで開かれた後、ワークステーションのパフォーマンスがおかしいと報告されました。技術者が最初に実行する必要があるのは、次のうちどれですか?
A. チケットを Tier 2 にエスカレートします。
B. ウイルス スキャンを実行します。
C. Windows の復元ポイントを利用します。
D. コンピュータを再イメージ化します。
Answer: B (メーッセージを残す)
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0) When a user reports that their workstation is behaving strangely after opening a suspicious email, the first step a technician should take is to run a virus scan on the computer. This is because opening a suspicious email is a common way for viruses and malware to infect a computer. Running a virus scan can help identify and remove any infections that may be causing the computer to behave strangely.

最新問題**: 123**
企業ネットワークからインターネットにアクセスするには、プロキシ サーバーが必要です。技術者が Windows 10 デバイスを手動で構成してインターネットにアクセスできるようにするには、次のどれを実行する必要がありますか?
A. プロキシ サーバーの URL と IP アドレスを、C: の下にあるコンピューターの hosts ファイルに追加します。
\windows\System32\drivers\etc.
B. プロキシ サーバーの使用を有効にし、[コントロール パネル] > [インターネット オプション] > [接続] > [LAN 設定] でプロキシ サーバーのアドレスを入力します。
C. コマンド プロンプトを開き、ipconfig /release を実行してから、ipconfig /renew を実行します。
D. コンピュータのネットワーク接続 IP 設定で [手動] を選択し、[ゲートウェイ] の下にプロキシ サーバーの IP アドレスを入力して、プロキシ サーバーをデフォルト ゲートウェイとして設定します。
Answer: (解答を表示する)
Detailed Explanation with Core 2 References:Configuring a proxy server in Windows 10 can be done through the Internet Options under LAN settings, where the user can enable and enter a proxy server's address. This aligns with Core 2's objectives of configuring network settings in a Windows environment (Core 2 Objective

1.4).

最新問題**: 124**
Linux で YUM コマンドをいつ使用するべきかを最もよく説明しているのは次のうちどれですか?
A. 機能を追加する場合
B. フォルダーの権限を変更する場合
C. ドキュメントを表示する
D. ファイルの内容を一覧表示する
Answer: A (メーッセージを残す**)**
YUM stands for Yellowdog Updater Modified and it is a command-line tool that allows users to install, update, remove, and manage software packages in Linux. YUM can be used to add functionality to a Linux system by installing new software packages or updating existing ones. To change folder permissions, show documentation, or list file contents, other commands such as chmod, man, or ls can be used in Linux.

最新問題**: 125**
Linux オペレーティング システムを実行している PC 用のパッケージ管理ユーティリティは次のうちどれですか?
A. chmod
B. yum
C. man
D. grep
Answer: B (メーッセージを残す**)**
yum (Yellowdog Updater Modified) is a package management utility for PCs that are running the Linux operating system. It can be used to install, update and remove software packages from repositories. chmod (change mode) is a command that changes the permissions of files and directories in Linux. man (manual) is a command that displays the documentation of other commands in Linux. grep (global regular expression print) is a command that searches for patterns in text files in Linux. Verified References: https://www.comptia.org /blog/linux-package-management https://www.comptia.org/certifications/a

最新問題**: 126**
技術者は SOHO ルーターを構成しており、ネットワーク上で特定のコンピューターのみを許可したいと考えています。技術者が行うべきことは次のうちどれですか?
A. MAC フィルタリングを設定します。
B. DHCP を無効にします。
C. ポート転送を構成します。
D. ゲスト アクセスを無効にします。
Answer: A (メーッセージを残す**)**
For a SOHO (Small Office/Home Office) router setup where the goal is to only allow specific computers on the network, MAC filtering is the appropriate solution:
Configure MAC filtering: This security measure involves creating a list of allowed device MAC (Media Access Control) addresses in the router's settings. Only devices with MAC addresses on this list will be able to connect to the network, effectively restricting access to authorized computers only.

最新問題**: 127**
ネットワーク管理者が SOHO ワイヤレス ネットワークのセキュリティを設定しています。ネットワークを保護するために、管理者は次のオプションのどれを有効にする必要がありますか?
A. NATBWPA3
B. 802.1X

C. 静的IP
Answer: (解答を表示する**)**
To secure a SOHO wireless network, enabling WPA3 is the recommended option. WPA3 (Wi-Fi Protected Access 3) is the latest security certification program developed by the Wi-Fi Alliance to secure wireless computer networks. It provides cutting-edge security protocols and cryptographic methods to enhance and replace its predecessors, WPA2 and WPA, offering improved protection against brute-force attacks and ensuring better privacy on public networks.

最新問題**: 128**
ヘルプ デスク チャット アプリケーションを通じて連絡を受けました。ユーザーが交換用の SOHO ルーターをセットアップしています。ユーザーがルーターをセットアップできるように支援します。
説明書
各回答に最も適切な文を選択してください。各回答の後に送信ボタンをクリックしてチャットを続行します。
いつでも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。
Answer:
See the solution below in Explanation.
Explanation:

To: Customer

I just received a new router for the office, and I need help setting it up.

I am happy to assist you today.

I need to set up my basic security settings.

Is this the first router in your office?

No, it is a replacement. The last router broke.
I am currently logged in and connected to the router's web page.

The first thing you need to do is change the default password.

Create a new password with an uppercase, a lowercase, and a special character.

最新問題: **129**
小規模オフィス環境で使用される可能性が最も高いのは次のうちどれですか?
A. プリントサーバー
B. 仮想化
C. ドメインアクセス
D. ワークグループ

Answer: D (メーッセージを残す)
A workgroup is a network configuration that allows computers to communicate and share resources with each other without requiring a centralized server or domain controller. A workgroup is suitable for small office environments where there are only a few computers and users who need simple file and printer sharing. A workgroup does not have centralized management or security policies, which may be desirable for larger or more complex networks. Print server, virtualization, and domain access are not network configurations that are most likely used in a small office environment.

最新問題**: 130**
アプリケーションのパフォーマンスが低下し、エラーが表示されずにシャットダウンすることがあります。アプリケーションがアクティブなときにトラブルシューティングを行うには、次のタスク マネージャーのどのタブを使用する必要がありますか?
A. ユーザー
B. サービス
C. パフォーマンス
D. 起動
Answer: C (メーッセージを残す)
When troubleshooting an application that is not performing well and occasionally shuts down with no error, the "Performance" tab in Task Manager is the most appropriate tool to use. This tab provides real-time data on CPU, memory, disk, and network usage, which can help identify resource bottlenecks or spikes that could be causing the application to malfunction. Monitoring these metrics while the application is running can offer insights into whether the issue is related to system resources.
* A. Users tab shows which users are currently logged into the system and their resource usage but does not provide detailed performance metrics for troubleshooting application issues.
* B. Services tab shows the status of background services but does not provide direct information about the application's performance.
* D. Startup tab manages which applications start with Windows and their impact on startup time but is not useful for monitoring active application performance.
References:
* CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 1.3: Using features and tools of the Microsoft Windows OS, including Task Manager's Performance tab.

最新問題**: 131**
技術者が、会社の Web サイトにアクセスできない顧客をサポートしています。技術者が最初に行うべきことは何ですか。
A. 顧客にログイン資格情報を尋ねます。
B. 解決策については、会社の内部ナレッジベースを確認してください。
C. より経験豊富な技術者に顧客を紹介します。
D. 問題の詳細を会社のチケット システムに記録します。
Answer: D (メーッセージを残す)
When a customer is having difficulty accessing the company's website, the technician should first document the issue in the company's ticketing system. This step ensures that the problem is officially logged, which allows for proper tracking, prioritization, and assignment to the appropriate personnel if needed. Recording the details helps in maintaining a record of the issue and the troubleshooting steps taken, which is useful for future reference and analysis.
* A. Ask the customer for their log-in credentials. This is not appropriate as it breaches security protocols and is not the first step in troubleshooting.
* B. Check the company's internal knowledge base for solutions. While useful, this step comes after the issue has been documented.
* C. Refer the customer to a more experienced technician. This might be necessary later, but initially, the issue should be documented.
References:
* CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 4.1: Documentation and support systems, including the use of ticketing systems for tracking incidents.

最新問題**: 132**
従業員が個人のスマートフォンを使用してリモートで作業しています。従業員は、会社が提供する VPN サービスを使用してポータルにアクセスできません。問題の原因は次のどれに当てはまりますか?

A. アプリケーションは会社が購入する必要があります。
B. スマートフォンのOSが最新バージョンではありません。
C. スマートフォンはMDMサービスに登録されていません。
D. アプリケーションのインストールと起動に失敗しました。
Answer: C (メーッセージを残す)
When an employee is unable to access the company portal using a VPN on their personal smartphone, the most likely cause is:
* The smartphone is not enrolled in MDM service:Mobile Device Management (MDM) services often control access to company resources. If the smartphone is not enrolled, it may be blocked from accessing the VPN and, consequently, the company portal.
* The application must be purchased by the company:Unlikely, as most VPN applications are free to download or included in the company's software package.
* The smartphone is not on the latest OS version:While this could cause compatibility issues, it is less likely than the MDM enrollment issue.
* The application fails to install and launch:This would be a different problem and would usually present specific error messages.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.7: Explain common methods for securing mobile and embedded devices.
MDM configuration and access control documentation.

最新問題**: 133**
ユーザーから、PC の動作が遅いと報告されました。技術者は、ハード ドライブがひどく断片化されているのではないかと疑っています。技術者は次のどのツールを使用する必要がありますか?
A. resmon exe
B. msconfig.extf
C. dfrgui exe
D. msmfo32.exe
Answer: (解答を表示する)
The technician should use dfrgui.exe to defragment the hard drive1

最新問題**: 134**
大企業がパスワードの長さの要件を変更しています。最高情報責任者は、パスワードの長さを 10 文字ではなく 12 文字以上にすることを義務付けています。この設定を調整するには、次のどれを使用する必要がありますか。
* グループポリシー
A. ユーザーアカウント
B. アクセス制御リスト
C. 認証アプリケーション
Answer: A (メーッセージを残す)
Group Policy is a feature of Windows that allows administrators to manage and configure settings for computers and users on a network12. One of the settings that can be controlled by Group Policy is the password policy, which defines the rules for creating and changing passwords, such as minimum length, complexity, expiration, and history34. By using Group Policy, the Chief Information Officer can enforce the new password length requirement for all users and computers in the company's domain, without having to manually adjust each user account or device.
References1: The Official CompTIA A+ Core 2 Student Guide (Exam 220-1102), page 10-11 2: CompTIA A+ Certification Exam Core 2 Objectives, page 13 3: The Official CompTIA A+ Core 2 Instructor Guide (Exam 220-1102), page 10-12 4: CompTIA A+ Certification Exam: Core 2 (220-1102) Exam Objectives

最新問題**: 135**
技術者にヘルプデスク チケットが割り当てられ、問題が解決されました。他の技術者が同様の問題を解決できるようにするために、技術者は次のどれを更新する必要がありますか?

* エンドユーザートレーニング
A. 進捗メモ
B. ナレッジベース
C. 利用規定文書
Answer: C (メーッセージを残す**)**
A knowledge base is a centralized repository of information that can be used by technicians to find solutions to common problems, best practices, troubleshooting guides, and other useful resources12. Updating the knowledge base with the details of the issue and the resolution can help other technicians who encounter similar issues in the future. It can also reduce the number of tickets and improve customer satisfaction3.
References1: The Official CompTIA A+ Core 2 Student Guide (Exam 220-1102), page 10-11 2: CompTIA A+ Certification Exam Core 2 Objectives, page 13 3: CompTIA A+ Core 2 (220-1102) Certification Study Guide, page 10-12

最新問題**: 136**
問題について顧客を支援しているときに、サポート担当者は、予約が予想よりも長くかかっていることに気付き、次の顧客とのミーティングが 5 分遅れる原因となります。サポート担当者が次に行うべきことは次のうちどれですか?
A. 次の顧客に遅延に関する簡単なメッセージを送信します。
B. 現在の顧客のライムを短く切り、次の顧客に急いで行きます。
C. 遅刻したら次の客に謝る。
D. ライムを認めずに次の会議に遅れる.
Answer: A (メーッセージを残す**)**
The support representative should send a quick message regarding the delay to the next customer. This will help the next customer understand the situation and adjust their schedule accordingly.

最新問題**: 137**
macOS ユーザーは、別の仮想デスクトップ スペースを作成する必要があります。次のアプリケーションのうち、ユーザーがこのタスクを実行できるのはどれですか?
A. ドック
B. スポットライト
C. ミッション コントロール
D. ランチパッド
Answer: C (メーッセージを残す**)**
application that will allow a macOS user to create another virtual desktop space is Mission Control Mission Control lets you create additional desktops, called spaces, to organize the windows of your apps. You can create a space by entering Mission Control and clicking the Add button in the Spaces bar1. You can also assign apps to specific spaces and move between them easily1.

最新問題**: 138**
技術者は PC のマザーボードを交換する必要があります。技術者は PC をシャットダウンします。技術者が次に実行すべき手順は次のうちどれですか?
A. モニターの電源を切ります。

B. 電源コードを抜きます。
C. PSU を取り外します。
D. RAM モジュールを取り外します。
Answer: (解答を表示する**)**
Removing the power cord is the first step to ensure the safety of the technician and the PC components. This will prevent any electrical shock or damage that may occur if the PC is still connected to a power source. The technician should also press the power button to drain any residual power from the capacitors.

最新問題**: 139**
ユーザーがヘルプ デスクに電話して、マップされたドライブにアクセスできなくなったことを報告します。技術者は、ユーザーのマシンのいずれかのドライブをクリックするとエラー メッセージが表示されることを確認します。オフィス内の他のユーザーには問題はありません。最初のステップとして、技術者はドライブを取り外して再接続しようと考えています。
技術者が使用すべきコマンドライン ツールは次のうちどれですか?
A. 正味使用
B. セット
C. mkdir
D. 名前を変更
Answer: A (メーッセージを残す**)**
The technician should use net use command-line tool to remove and reconnect mapped drives. Net use is a command that allows users to manage network connections and resources, such as shared folders or printers.
Net use can be used to map or unmap network drives by specifying their drive letters and network paths. For example, net use Z: \server\share maps drive Z: to \server\share folder, and net use Z: /delete unmaps drive Z:.
Set is a command that displays or modifies environment variables for the current user or process. Set is not related to managing mapped drives. Mkdir is a command that creates a new directory or folder in the current or specified location. Mkdir is not related to managing mapped drives. Rename is a command that renames a file or folder in the current or specified location. Rename is not related to managing mapped drives.
References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

最新問題**: 140**
警察署の証拠室にあったラップトップが行方不明です。保管過程の文書を参照する最も適切な理由は次のうちどれですか?
A. どの当事者がいつマシンを所有したかを判断します。
B. マシンから機密データをリモートで消去します。
C. マシンの交換に必要な情報を収集します。
D. パスワードを変更する必要があることを所有者に警告します。
Answer: A (メーッセージを残す**)**
Chain of custody documentation is a record of the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. It is important to maintain a chain of custody to ensure the integrity and authenticity of the evidence, and to prevent tampering or contamination. If a laptop that was in the evidence room of a police station is missing, the best reason to refer to chain of custody documentation is to determine which party had the machine and when. This can help to identify the possible suspects, locate the missing laptop, and verify if the evidence on the laptop was compromised or not

最新問題**: 141**
パフォーマンスを最適化すると主張する新しいアプリケーションをインストールした後、ユーザーは電話の問題を抱えています。ユーザーはベンダーの Web サイトからアプリケーションを直接ダウンロードしましたが、ネットワークの使用率が高くなり、セキュリティ警告が繰り返し表示されます。問題を軽減するために技術者が最初に実行する必要があるのは、次のうちどれですか?

A. 電話を工場出荷時の設定にリセットします
B. 不正なアプリケーションをアンインストールする
C. データプランの上限を引き上げる
D. モバイル ホットスポットを無効にします。
Answer: B (メーッセージを残す**)**
Installing applications directly from a vendor's website can be risky, as the application may be malicious or fraudulent. Uninstalling the application can help mitigate the issue by removing the source of the problem.

最新問題**: 142**
技術者は、USB デバイスがオペレーティング システムによって一時停止されていないことを確認する必要があります。技術者は、次のコントロール パネル ユーティリティのどれを使用して設定を構成する必要がありますか?
A. システム
B. 電源オプション
C. デバイスとプリンター
D. アクセスのしやすさ
Answer: B (メーッセージを残す**)**
The correct answer is B. Power Options. The Power Options utility in the Control Panel allows you to configure various settings related to how your computer uses and saves power, such as the power plan, the sleep mode, the screen brightness, and the battery status. To access the Power Options utility, you can follow these steps:
Go to Control Panel > Hardware and Sound > Power Options.
Click on Change plan settings for the power plan you are using.
Click on Change advanced power settings.
Expand the USB settings category and then the USB selective suspend setting subcategory.
Set the option to Disabled for both On battery and Plugged in.
Click on OK and then on Save changes.
This will prevent the operating system from suspending the USB devices to save power .
System, Devices and Printers, and Ease of Access are not the utilities that should be used to configure the setting. System is a utility that provides information about your computer's hardware and software, such as the processor, memory, operating system, device manager, and system protection. Devices and Printers is a utility that allows you to view and manage the devices and printers connected to your computer, such as adding or removing devices, changing device settings, or troubleshooting problems. Ease of Access is a utility that allows you to customize your computer's accessibility options, such as the narrator, magnifier, high contrast, keyboard, mouse, and speech recognition. None of these utilities have any option to configure the USB selective suspend setting.

最新問題**: 143**
ユーザーは、オフィスのコンピューターからスポーツ チームの Web サイトにアクセスできないと報告しています。管理者は、このアクセスのブロックは意図的であり、会社のガイドラインに基づいていることをユーザーに伝えます。管理者が言及しているのは次のうちどれですか?
A. NDA
B. AUP
C. VPN
D. SOP
Answer: B (メーッセージを残す**)**

An AUP, or Acceptable Use Policy, is a set of rules applied by the owner, creator, or administrator of a network, website, or service that restricts the ways in which the network, website, or system may be used. In this scenario, the administrator is likely referring to the company's AUP, which outlines what employees can and cannot do on the company's network, including restrictions on accessing certain types of websites, such as sports teams' sites, for non-work-related purposes.
AUP (Acceptable Use Policy): This policy typically includes rules designed to maintain the security of the network, ensure the productivity of employees, and comply with legal regulations. Blocking access to specific websites is a common practice enforced through an AUP to align with these goals.
An NDA (Non-Disclosure Agreement) (A) is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes but wish to restrict access to or by third parties. A VPN (Virtual Private Network) (C) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. SOP (Standard Operating Procedures) (D) are a set of step-by-step instructions compiled by an organization to help workers carry out complex routine operations, which wouldn't typically include website access guidelines.

最新問題**: 144**
ユーザーは Windows デスクトップから会議を主催することが多く、会議参加者は、ユーザーがコンピューターの画面を共有するときにテキストを大きくするようにユーザーに依頼します。会議中でないときは、ユーザーは仕事のタスクのためにテキストを小さくしたいと考えています。テキストのフォント サイズを変更する最も効率的な方法はどれですか。
A. 会議専用にフォントサイズを大きくしたラップトップをユーザーに配布する
B. 会議中にディスプレイ設定を使用してテキストサイズを調整する
C. 会議中にユーザーがログインできるように、フォントサイズを大きく設定したローカルユーザーアカウントを追加します。
D. ユーザーのデスクトップに2台目のモニターを追加し、そのディスプレイのフォントサイズのみを大きくする
Answer: B (メーッセージを残す**)**
Changing the text size efficiently for different scenarios, such as meetings and regular work tasks, can be managed directly through the Windows display settings. This method is both quick and easily reversible, making it the most efficient solution compared to the other options provided.
* Option A: Issuing a laptop to the user with increased font size to be used only for meetingsThis option is not efficient as it requires additional hardware and setup time, which is impractical for simply adjusting text size.
* Option B: Using display settings to adjust the text size during meetingsCorrect Answer. Windows provides built-in functionality to adjust the text size on the display. This can be accessed via:
* Windows Settings > System > Display.
* Under "Scale and layout," you can change the size of text, apps, and other items. This method allows for quick changes and can be reverted just as quickly after meetings.
Reference: CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 1.5
Option C: Adding a local user account, which has a larger font size set, for the user to log in to during meetingsThis approach involves additional steps of logging out and logging back in, which is less efficient than simply adjusting the display settings.
Option D: Adding a second monitor to the user's desktop and increase the font size for only that display While this can be a solution, it is not the most efficient way as it involves additional hardware and configuration. It's more suited for scenarios requiring constant dual-display use rather than just changing text size occasionally.

最新問題**: 145**
技術者は、現場スタッフと在宅スタッフのために会社のデバイスを最新の状態に保つ方法を推奨する必要があります。
ユーザーは全国のさまざまな場所に住んでおり、同社にはスタッフが技術サポートを求めて行ける国内オフィスがいくつかあります。ユーザーにとって最も適切な方法は次のどれですか?
A. アップデートをインストールできるように、週に 1 日は出社を義務付けます。
B. 定期的にデバイスでアップデートを実行し、コンピュータを再起動するようにユーザーに依頼します。
C. ネットワークに影響を与えないように、VPN 経由で更新を週単位で時間差でプッシュ配信します。
D. コンピューターの更新を自動的に管理するようにクラウドベースのエンドポイント管理ソフトウェアを構成します。
Answer: (解答を表示する**)**

For a company with geographically dispersed staff and the need to keep devices updated, using cloud-based endpoint management software is the most efficient method. This type of software allows IT administrators to remotely manage and push updates to company devices, regardless of their location. It ensures that all devices remain up to date with the latest security patches and software updates without requiring physical access or user intervention. This approach is scalable, reduces the risk of unpatched vulnerabilities, and is convenient for both the IT department and the end-users.

最新問題**: 146**
コール センターの技術者が、ユーザーから Windows の更新方法を尋ねる電話を受けました。技術者が何をすべきかを説明しているのは、次のうちどれですか?
A. ユーザーが更新を完了できない場合は、iPad の使用をユーザーに検討してもらいます。
B. ユーザーに、ユーザーのパスワードを技術者にテキストで送信してもらいます。
C. [検索] フィールドをクリックし、「Check for Updates」と入力して Enter キーを押すようにユーザーに依頼します。
D. 今後の自動パッチを待つようにユーザーにアドバイスします。
Answer: C (メーッセージを残す**)**
The technician should guide the user to update Windows through the built-in "Check for Updates" feature.
This can be done by having the user click in the Search field, type "Check for Updates", and then press the Enter key. This will bring up the Windows Update function, which will search for any available updates and give the user the option to install them.

最新問題**: 147**
顧客サイトの技術者がラップトップのトラブルシューティングを行っています ソフトウェアの更新をダウンロードする必要がありますが、会社のプロキシが更新サイトへのトラフィックをブロックしています。技術者は次のうちどれを実行する必要がありますか?
A. DNS アドレスを 1.1.1.1 に変更します。
B. グループ ポリシーの更新
C. サイトをクライアントの例外リストに追加します
D. ソフトウェア ライセンスが最新であることを確認します。
Answer: C (メーッセージを残す**)**
The technician should add the update site to the client's exceptions list to bypass the proxy. This can be done through the client's web browser settings, where the proxy settings can be configured. By adding the update site to the exceptions list, the client will be able to access the site and download the software update.

最新問題**: 148**
macOS コンピュータにソフトウェアをインストールするには、次のどのファイル タイプを使用する必要がありますか? (2 つ選択してください)。
A. .yum
B. .pkg
C. .msi
D. .ps1
E. .exe
F. .dmg
Answer: B,F (メーッセージを残す**)**
The correct answers are B. .pkg and F. .dmg.
pkg (Package Installer) - This is the standard macOS package format for software installations. It often includes installation scripts and can be used for software distribution.
dmg (Disk Image File) - A macOS disk image file that contains software installers. Users typically mount the file and drag the application into the Applications folder to install it.
Why Other Options Are Incorrect:
A: .yum - This is used for Linux package management and is not compatible with macOS.

C: .msi - This is the Windows Installer package format, not used on macOS.
D: .ps1 - This is a PowerShell script file used in Windows, not for installing macOS applications.
E: .exe - This is an executable file format for Windows applications and does not run on macOS without third- party emulation (e.g., Wine).
CompTIA A+ 220-1102 Exam Reference:
Objective 1.7 - Identify common features and tools of the macOS/Linux client operating systems.

最新問題**: 149**
ネットワークが停止しているときに、技術者がサポート ドキュメントに記載されていない新しいネットワーク スイッチを発見しました。このスイッチは、新しいオフィスが環境に追加された最近の変更期間中にインストールされました。次のどれが、来月の変更期間後にこの種の不一致を防ぐ可能性が最も高いでしょうか。
A. 年次ネットワークトポロジレビューの実施
B. すべてのネットワーク変更にはネットワーク図の更新が含まれる
C. 年に1回ネットワークの変更を許可する
D. スイッチ設定ファイルの定期的なバックアップ
Answer: B (メーッセージを残す**)**
This would ensure that the support documentation reflects the current state of the network and prevents any confusion or mismatch during a network outage. Updating the network diagrams is also one of the best practices for network documentation, as stated in the Official CompTIA A+ Core 2 Study Guide1. The other options are not as effective or feasible as option B. Performing annual network topology reviews is too infrequent and may not capture recent changes. Allowing network changes once per year is too restrictive and may not meet the business needs. Routinely backing up switch configuration files is important, but it does not help with identifying new switches or devices on the network.

最新問題**: 150**
管理者はモバイル デバイスの新しい発送物を受け取りました。企業ポリシーにより、企業発行のすべてのデバイスには 2 つの認証方法が必要であり、組織はすでに 1 つの方法として PIN コードの使用を強制しています。管理者は次のデバイス機能のうちどれを有効にする必要がありますか?
A. スマートカード
B. 生体認証
C. ハードトークン
D. ワンタイムパスワード
Answer: (解答を表示する**)**
For securing mobile devices with two authentication methods, combining something the user knows (a PIN) with something the user is (biometrics) enhances security by implementing multi-factor authentication.
* Smart card: Generally requires additional hardware and is not commonly used in mobile devices.
* Biometrics: Uses unique biological traits such as fingerprints or facial recognition, providing a convenient and secure second method of authentication.
* Hard token: Involves additional physical devices which might not be practical for mobile devices.
* One-time password: Usually used for specific applications rather than as a general device authentication method.
Reference: CompTIA A+ Exam Objectives [220-1102] - 2.1: Summarize various security measures and their purposes.

最新問題**: 151**
技術者は、ユーザーのワークステーション上の持続的なマルウェア感染を修復できませんでした。技術者が OS を再インストールした後。その日遅くにマルウェア感染が再発しました。最も可能性の高い情報源は次のうちどれですか?
A. トロイの木馬
B. ブート セクター ウイルス

C. スパイウェア
D. ルートキット
Answer: B (メーッセージを残す)
A boot sector virus infects the master boot record (MBR) of a hard drive, the sector that contains information required to start the operating system after the computer is turned on. This type of virus is particularly insidious because it loads into memory immediately upon booting and before most antivirus programs start.
This makes it possible for the virus to evade detection and removal, and can easily reinfect a system even after the operating system is reinstalled if the boot sector is not cleaned.
* Boot sector virus: Given that the malware infection returned after the OS reinstallation, it's likely that the virus was not removed from the boot sector during the reinstallation process. Reinstalling the OS without cleaning the boot sector won't remove the infection, allowing the virus to continue to affect the system.
Other options:
* Trojan: A Trojan is a type of malware that disguises itself as legitimate software. While Trojans can be persistent, the reinstallation of the OS should remove any Trojans unless they are reintroduced after installation.
* Spyware: Spyware is designed to gather information about a person or organization without their knowledge. Like Trojans, spyware should be removed with an OS reinstallation unless it is reintroduced in some way.
* Rootkit: Rootkits are designed to enable continued privileged access to a computer while actively hiding their presence. While a rootkit could potentially survive an OS reinstall if it infects the firmware or certain areas outside the OS, the scenario described points more specifically to a boot sector virus, especially considering the immediate return of the infection after OS reinstallation.

最新問題: **152**
技術者は、ユーザー プロファイルの再構築が必要な問題のトラブルシューティングを行っています。技術者は、Mtv1C コンソールでローカル ユーザーとグループを見つけることができません。問題を解決するために技術者が取るべき次のステップは次のうちどれですか?
A. ウイルス対策スキャンを実行します。
B. 必要なスナップインを追加します。
C. システム バックアップを復元します。
D. 管理コンソールを使用します。
Answer: (解答を表示する)
Local Users and Groups is a Microsoft Management Console (MMC) snap-in that allows you to manage user accounts or groups on your computer1. If you cannot find it in the MMC console, you can add it manually by following these steps2:
Press Windows key + R to open the Run dialog box, or open the Command Prompt.
Type mmc and hit Enter. This will open a blank MMC console.
Click File and then Add/Remove Snap-in.
In the Add or Remove Snap-ins window, select Local Users and Groups from the Available snap-ins list, and click Add.
In the Select Computer window, choose Local computer or Another computer, depending on which computer you want to manage, and click Finish.
Click OK to close the Add or Remove Snap-ins window. You should now see Local Users and Groups in the MMC console.

最新問題: **153**

標準化された一連のソフトウェアがインストールされている組織では、開発者が新しいソフトウェアをインストールするリクエストを送信します。同社は現在このソフトウェアのライセンスを持っていませんが、開発者はすでにインストール ファイルをダウンロードしており、技術者にインストールするよう要求しています。開発者は、経営陣がこのソフトウェアのビジネス利用を承認したと述べています。技術者がとるべき最善の行動は次のうちどれですか?

A. ソフトウェア ベンダーに連絡してユーザーのライセンスを取得し、ライセンスの購入後にユーザーのインストールを支援します。

B. ダウンロードしたインストール ファイルのスキャンを実行して、悪意のあるソフトウェアが含まれていないことを確認し、ソフトウェアをインストールして、ソフトウェアのインストール プロセスを文書化します。

C. 正式な承認が必要であることを開発者に示します。次に、IT チームは、ソフトウェアをインストールする前に、ソフトウェアとそれが組織に与える影響を調査する必要があります。

D. ソフトウェアをインストールし、ウイルス対策ソフトウェアを使用してシステム全体のスキャンを実行し、オペレーティング システムに悪意のあるソフトウェアが存在しないことを確認します。

Answer: C (メーッセージを残す)

Installing new software on an organization's system or device can have various implications, such as compatibility, security, performance, licensing, and compliance issues. Therefore, it is important to follow the best practices for software installation, such as doing research on the software, checking the system requirements, scanning the installation file for malware, and obtaining the proper license345. The technician should not install the software without formal approval from the management team, as this could violate the organization's policies or regulations. The technician should also not install the software without investigating the software and its impact on the organization, as this could introduce potential risks or problems to the system or device. The technician should indicate to the developer that formal approval is needed, and then work with the IT team to evaluate the software and its suitability for the organization before installing it

最新問題**: 154**

技術者は、顧客が会議議事録を保存するための場所を Windows ワークステーション上に作成しています。技術者は次のコマンドのうちどれを使用する必要がありますか?

A. c: \minutes

B. dir

C. rmdir

D. md

Answer: (解答を表示する)

The command md stands for make directory and is used to create a new directory or folder in the current location. In this case, the technician can use md minutes to create a folder named minutes in the C: drive. The other commands are not relevant for this task. c: \minutes is not a command but a path to a folder. dir is used to display a list of files and folders in the current directory. rmdir is used to remove or delete an existing directory or folder.

最新問題**: 155**

リモート ユーザーがオンライン共有にアクセスする際に問題が発生しています。問題のトラブルシューティングに使用される可能性が最も高いツールは次のうちどれですか?

A. 画面共有ソフトウェア

B. セキュアシェル

C. 仮想プライベートネットワーク

D. ファイル転送ソフト

Answer: A (メーッセージを残す)

Screen-sharing software is a tool that allows a technician to remotely view and control a user's screen over the internet. It can be used to troubleshoot issues with accessing an online share, as well as other problems that require visual inspection or guidance. Secure shell (SSH) is a protocol that allows remote access and command execution on another device, but it does not allow screen-sharing. Virtual private network (VPN) is a protocol that creates a secure tunnel between two devices over the internet, but it does not allow remote troubleshooting. File transfer software is a tool that allows transferring files between two devices over the internet, but it does not allow screen-sharing. Verified References: https://www.comptia.org/blog/what-is- screen-sharing-software https://www.comptia.org/certifications/a

最新問題**: 156**

システムにアクセスするための 2 番目の方法として、SMS またはサードパーティのアプリケーションをよく使用するのは次のうちどれですか?

A. MFA
B. WPA2
C. AES
D. 半径
Answer: A (メーッセージを残す)
MFA (Multi-Factor Authentication) is a security measure that often uses an SMS or third-party application as a secondary method to access a system. MFA requires the user to provide two or more pieces of evidence to prove their identity, such as something they know (e.g., password), something they have (e.g., phone), or something they are (e.g., fingerprint)2. WPA2 (Wi-Fi Protected Access 2) is a security protocol for wireless networks that does not use SMS or third-party applications. AES (Advanced Encryption Standard) is a symmetric encryption algorithm that does not use SMS or third-party applications. RADIUS (Remote Authentication Dial-In User Service) is a network protocol that provides centralized authentication and authorization for remote access clients, but does not use SMS or third-party applications.

最新問題**: 157**
次のオペレーティング システムのうち、組み込みシステムで最も一般的に使用されているのはどれですか?
A. Chrome OS
B. macOS
C. Windows
D. Linux
Answer: D (メーッセージを残す)
Linux is the most commonly used operating system in embedded systems because it is open source, free, customizable, and supports a wide range of architectures and devices. Linux also offers many advantages for embedded development, such as real-time capabilities, modularity, security, scalability, and reliability. Linux can run on embedded systems with limited resources, such as memory, storage, or power, and can be tailored to the specific needs of the application. Linux also has a large and active community of developers and users who contribute to its improvement and innovation. Some examples of embedded systems that use Linux are smart TVs, routers, drones, robots, smart watches, and IoT devices

最新問題**: 158**
技術者は、機密情報を含むコンピューターの問題をトラブルシューティングしています。技術者は、コンピューターを修理のために現場から持ち出す必要があると判断しました。次に技術者が行うべきことは次のどれですか。
A. HDD を取り外して、コンピューターを修理に出します。
B. ガイダンスについては企業ポリシーを確認してください。
C. コンピュータが建物から出る前に機密情報を削除します。
D. マネージャーから承認を取得します。
Answer: (解答を表示する)
When dealing with sensitive information, it's crucial to adhere to company policies and procedures. These policies will outline the proper protocols for handling and transporting devices containing sensitive data.
Here's why the other options might not be the best course of action:
* A. Remove the HDD and then send the computer for repair: While this might seem like a good way to protect the data, it might not be compliant with company policy. Some policies might require the entire device to be sent for security reasons or to ensure proper diagnosis and repair.
* C. Delete the sensitive information before the computer leaves the building: Deleting the data might not be sufficient, as it could potentially be recovered. Also, it might violate data retention policies or hinder the repair process.
* D. Get authorization from the manager: While getting manager approval is important, it's essential to first consult the company policies to understand the required procedures.
Recommended Steps:

* Check corporate policies: Review the company's policies on data security, device handling, and off- site repairs.
* Consult with IT security or management: If the policies are unclear or if you have any questions, seek guidance from the appropriate personnel.
* Follow the prescribed procedures: This might involve data encryption, secure data wiping, obtaining necessary approvals, and using approved vendors for off-site repairs.

最新問題**: 159**
技術者は、ラップトップにログインするための最速かつ最も安全な方法を使用することを任されています。次のログイン オプションのうち、これらの要件を満たすものはどれですか?
A. PIN
B. ユーザー名とパスワード
C. SSO
D. 指紋
Answer: A (メーッセージを残す**)**
This is because a PIN is a fast and secure method of logging in to laptops, and it is more secure than a password because it is not susceptible to keyloggers.

最新問題**: 160**
ドライバーは現在使用されているため、技術者はシステム ドライバーをアンインストールできません。技術者がドライバーをアンインストールするために使用する必要があるツールは次のうちどれですか?
A. msinfo32.exe
B. dxdiag.exe
C. msconfig.exe
D. regedit.exe
Answer: C (メーッセージを残す**)**
The msconfig.exe tool, also known as the System Configuration utility, is a tool that allows users to modify various system settings, such as startup options, services, boot options, and more. One of the features of msconfig.exe is the ability to disable or enable device drivers that are loaded during the system startup. By using msconfig.exe, a technician can prevent a driver from being loaded and used by the system, which will allow them to uninstall it without any errors. To use msconfig.exe to disable a driver, the technician can follow these steps:
* Open the Run dialog box by pressing the Windows key + R.
* Type msconfig.exe and press Enter.
* Click on the Boot tab and then click on Advanced options.
* Check the box next to No GUI boot and click OK. This will prevent the graphical user interface from loading during the boot process, which will also prevent some drivers from loading.
* Click on the Services tab and check the box next to Hide all Microsoft services. This will show only the third-party services and drivers that are running on the system.
* Find the service or driver that corresponds to the device that the technician wants to uninstall and uncheck the box next to it. This will disable the service or driver from starting during the system startup.
* Click Apply and OK and then restart the computer.
* After the computer restarts, the technician can use the Device Manager or the Control Panel to uninstall the driver that was previously in use.
References:
* How to Completely Remove/Uninstall a Driver in Windows, section 31
* The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2212

最新問題**: 161**
comptia.org の従業員は、同僚から通常の量の電子メールを受信していると報告しています。技術者は、電子メールが次のアドレスから送信されたことを発見しました。
john@cOmptia.org
これは次のソーシャル エンジニアリング攻撃の例のうちどれですか?
A. Whaling
B. 内部関係者の脅威

C. フィッシング
D. ビッシング
E. Evil twin
Answer: C (メーッセージを残す)
Phishing involves tricking individuals into disclosing sensitive information or installing malware through deceptive emails.
* Whaling: A specific type of phishing targeting high-profile individuals.
* Insider threat: Malicious activities by someone within the organization.
* Phishing: General deceptive emails to trick users into compromising information or installing malware.
* Vishing: Voice phishing, conducted over the phone.
* Evil twin: A rogue Wi-Fi access point mimicking a legitimate one to intercept data.
Reference: CompTIA A+ Exam Objectives [220-1102] - 2.4: Explain common social engineering attacks, threats, and vulnerabilities.

最新問題**: 162**
ログイン時に個人用ストレージ テーブル (.pst ファイル) をネットワーク ドライブにコピーすることを自動化するために、Windows スタートアップ フォルダーで使用されるファイルの種類は次のうちどれですか?
A. .bat
B. .dll
C. .ps1
D. .txt
Answer: A (メーッセージを残す)
The .bat file type would be used in the Windows Startup folder to automate copying a personal storage table (.
pst) file to a network drive at log-in. A .bat file is a batch file that contains a series of commands that can be executed by the command interpreter. A .bat file can be used to perform various tasks, such as copying, moving, deleting, or renaming files or directories. A .bat file can be placed in the Windows Startup folder to run automatically when a user logs in to the system. A .bat file can use the copy command to copy a .pst file from a local drive to a network drive. A .pst file is a personal storage table file that contains email messages, contacts, calendars, and other data from Microsoft Outlook. A .pst file can be backed up to a network drive for security or recovery purposes. The .dll, .ps1, and .txt file types are not used in the Windows Startup folder to automate copying a .pst file to a network drive at log-in. A .dll file is a dynamic link library file that contains code or data that can be shared by multiple programs. A .dll file cannot be executed directly by the user or the system. A .ps1 file is a PowerShell script file that contains commands or expressions that can be executed by the PowerShell interpreter. A .ps1 file can also perform various tasks, such as copying files or directories, but it requires PowerShell to be installed and configured on the system. A .txt file is a plain text file that contains unformatted text that can be read by any text editor or word processor. A .txt file cannot contain commands or expressions that can be executed by the system. References:
* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 18
* CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 459

最新問題**: 163**
技術者は、さまざまな部門が混在するプライベートな作業グループのメッセージング アプリケーションの管理者です。
技術者の同僚の一人が、雇用主が最近重大なセキュリティ侵害を受けたことをグループに開示し、その侵害の詳細をグループに共有しました。技術者が最初に行うべきことは何ですか?
A. グループメンバー全員が同じ雇用主に勤務しているため、メッセージは無視してください。
B. 同僚をグループから削除し、メンバーにメッセージを削除するように依頼します。
C. 同僚に個人的にメッセージを送信し、メッセージをすぐに削除するように依頼します。
D. 上司に連絡し、メッセージのスクリーンショットを添えて同僚に報告する
Answer: D (メーッセージを残す)

In the case of a security breach disclosure, it's crucial to follow proper protocol to handle sensitive information responsibly:
* Ignore the messages: Not appropriate as it disregards the potential impact and severity of the breach.
* Remove the colleague and ask members to delete the messages: While it might limit the spread of the information, it doesn't address the breach reporting requirement.
* Message the colleague privately: Might help in immediate removal of messages but does not follow the proper chain of command and reporting protocols.
* Contact the supervisor: The correct action, as it ensures that the incident is handled by higher authorities who can take appropriate measures. Reporting with screenshots ensures that there is evidence of the disclosure.
Reference: CompTIA A+ Exam Objectives [220-1102] - 2.7: Given a scenario, use proper communication techniques and professionalism.

最新問題**: 164**
Android ユーザーは、同社独自のモバイル アプリケーションを開こうとすると、すぐに処理が開始されると報告しています。ユーザーは、電話を再起動しても問題が解決しないと述べています。アプリケーションには、失うことのない重要な情報が含まれています。システム管理者が最初に試みる必要がある手順は次のうちどれですか?
A. アプリケーションをアンインストールして再インストールする
B. 電話を工場出荷時の設定にリセットします
C. 同様の機能を持つ別のアプリケーションをインストールする
D. アプリケーションのキャッシュをクリアします。
Answer: A (メーッセージを残す**)**
The systems administrator should clear the application cache12
If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application12 Resetting the phone to factory settings is not necessary at this point12 Installing an alternative application with similar functionality is not necessary at this point12

最新問題**: 165**
ある組織が、生成 AI ソリューションを組み込むためのガイドラインを作成しています。これらのガイドラインは次のどれで公開されますか?
* 標準操作手順
A. 利用規定
B. セキュリティプロトコル
C. データフロー図
Answer: B (メーッセージを残す**)**
An acceptable use policy (AUP) is a document that defines the rules and expectations for the users of a system, network, or service. It typically covers topics such as the purpose, scope, responsibilities, and restrictions of using the system, network, or service1. An AUP is a suitable place to publish the guidelines for the incorporation of generative AI solutions, as it can inform the users of the benefits, risks, and ethical implications of using such tools. It can also specify the conditions and limitations for using generative AI solutions, such as the types of data, content, and applications that are allowed or prohibited, the security and privacy requirements, the legal and regulatory compliance, and the accountability and reporting mechanisms23.
References: 1 What is an Acceptable Use Policy (AUP)? - Definition from Techopedia(https://security.
stackexchange.com/questions/84168/the-difference-of-security-policy-and-acceptable-use-policy). 2 Guide on the use of Generative AI - Canada.ca(https://www.canada.ca/en/government/system/digital-government
/digital-government-innovations/responsible-use-ai/guide-use-generative-ai.html)3 Key Considerations for Developing Organizational Generative AI Policies - ISACA(https://www.isaca.org/resources/news-and-trends
/newsletters/atisaca/2023/volume-44/key-considerations-for-developing-organizational-generative-ai-policies).

最新問題**: 166**

技術者がユーザーのために Bluetooth ヘッドセットをインストールします。テスト中、コンピューターのスピーカーからはまだ音が出ています。技術者は、ヘッドセットがデバイス マネージャーに表示されることを確認します。技術者がこの問題を解決するために行う可能性が高いのは次のうちどれですか。
A. ワイヤレス ヘッドセットのドライバーを更新します。
B. ヘッドセットの電池を交換して、しばらくしてからもう一度お試しください。
C. コントロール パネルでサウンドがミュートされていないことを確認します。
D. サウンド設定でヘッドセットをデフォルトのデバイスに変更します。
Answer: (解答を表示する**)**
Reference: CompTIA A+ Certification Core 2 220-1102, Objective 1.7 (Bluetooth and Audio Device Configuration).

最新問題**: 167**
IT セキュリティ チームは、3 分後にコンピュータをログイン状態に戻す新しいグループ ポリシーを実装しています。ポリシーの変更を最もよく説明しているものは次のうちどれですか?
A. ログイン時間
B. 画面ロック
C. ユーザー権限
D. ログインロックアウトの試行
Answer: B (メーッセージを残す**)**
Screen lock is a feature that returns a computer to the login screen after a period of inactivity, requiring the user to enter their credentials to resume their session. Screen lock can be configured using Group Policy settings, such as Screen saver timeout and Interactive logon: Machine inactivity limit. Screen lock can help prevent unauthorized access to a computer when the user is away from their desk. Login times are not a feature that returns a computer to the login screen, but a measure of how long it takes for a user to log in to a system. User permission is not a feature that returns a computer to the login screen, but a set of rights and privileges that determine what a user can do on a system. Login lockout attempts are not a feature that returns a computer to the login screen, but a security policy that locks out a user account after a number of failed login attempts. https://woshub.com/windows-lock-screen-after-idle-via-gpo/

最新問題**: 168**
ユーザーがワイヤレス ヘッドフォンを使用して動き回ると、ユーザーのモバイル デバイスの音声に一貫性がなくなります。
問題をトラブルシューティングするために技術者が実行する必要があるのは、次のうちどれですか?
A. Wi-Fi 接続状態を確認します。
B. デバイスの NFC 設定を有効にします。
C. デバイスを Bluetooth 範囲内に移動します。
D. デバイスのテザリングをオンにします。
Answer: C (メーッセージを残す**)**
Bringing the device within Bluetooth range is the best way to troubleshoot the issue of inconsistent audio when using wireless headphones and moving around. Bluetooth is a wireless technology that allows devices to communicate over short distances, typically up to 10 meters or 33 feet. If the device is too far from the headphones, the Bluetooth signal may be weak or interrupted, resulting in poor audio quality or loss of connection.

最新問題: **169**
ユーザーは、テクニカル サポート エージェントを名乗る人物から電話を受けます。発信者はユーザーにコンピュータにログインするよう求めます。
セキュリティとプライバシーを確保するためにユーザーが講じるべきセキュリティ対策は次のうちどれですか?
A. 既知の人からの電話のみを受けます。
B. 不審なメールは無視してください。
C. ウイルス対策ソフトを更新します。
D. 2 要素認証を有効にします。
E. マルウェア スキャナーをインストールします。
Answer: A (メーッセージを残す)
This is a scenario of a potential tech support scam, where a fraudster pretends to be a technical support agent and tries to trick the user into giving them access to the computer, personal information, or money. The user should not trust any unsolicited calls from unknown people claiming to be from tech support, as they might be trying to install malware, steal data, or charge for fake services. The user should only accept calls from known people, such as their IT department, their service provider, or their software vendor, and verify their identity before logging in to the computer. The user should also report any suspicious calls to the appropriate authorities or organizations.
References:
* How to protect against tech support scams1
* Avoid and report Microsoft technical support scams2
* How to Protect Against Technical Support Scams3
* How To Recognize and Avoid Tech Support Scams4

最新問題: **170**
デスクトップ技術者は、ユーザーの PC のプログラムや保存されたファイルのロードが遅いという報告を受けました。技術者は調査し、十分な空き容量のある古い HDD を発見しました。問題を軽減するために技術者が最初に使用する必要があるのは次のうちどれですか?
A. ディスク管理
B. ディスクのデフラグ
C. ディスクのクリーンアップ
D. デバイスマネージャー
Answer: B (メーッセージを残す)
Disk Defragment is a tool that can be used to improve the performance of a hard disk drive (HDD). HDDs store data in sectors and clusters on spinning platters. Over time, as data is written, deleted, and moved, the data may become fragmented, meaning that it is spread across different locations on the disk. This causes the HDD to take longer to access and load data, resulting in slower performance. Disk Defragment consolidates the fragmented data and rearranges it in a contiguous manner, which reduces the seek time and increases the speed of the HDD. Disk Management, Disk Cleanup, and Device Manager are not tools that can alleviate the issue of slow HDD performance.

最新問題: **171**
技術者は、暗号通貨アドレスへの支払いを要求するファイルを確認しました。技術者が最初に行うべきことは次のうちどれですか?
A. コンピュータを隔離します。
B. システムの復元を無効にします。
C. ウイルス対策ソフトウェアの定義を更新します。
D. セーフモードで起動します。
Answer: (解答を表示する)

Quarantining the computer means isolating it from the network and other devices to prevent the spread of malware or ransomware. Ransomware is a type of malware that encrypts the files on a computer and demands payment (usually in cryptocurrency) to restore them. If a technician sees a file that is requesting payment to a cryptocurrency address, it is likely that the computer has been infected by ransomware. Quarantining the computer should be the first step to contain the infection and prevent further damage. Disabling System Restore, updating the antivirus software definitions, and booting to safe mode are not steps that should be done before quarantining the computer.

最新問題**: 172**
ユーザーの Windows デスクトップのディスク容量が不足しています。技術者は、一部のアップグレード ファイルが削除されなかったと考えています。
問題を修正するために技術者が使用すべきツールは次のうちどれですか?
A. devmgmt.msc
B. cleanmgr.exe
C. dfrgui.exe
D. diskmgmt.mac
Answer: B (メーッセージを残す**)**
The correct tool to use for removing upgrade files and freeing up disk space on a Windows desktop is cleanmgr.exe, which stands for Disk Cleanup. Disk Cleanup is a maintenance utility included in Microsoft Windows designed to free up disk space on a computer's hard drive. The utility scans and analyzes the hard drive for files that are no longer of any use, and then removes the unnecessary files. It can delete temporary files, system files, empty the Recycle Bin, and remove a variety of system files and other items that you might no longer need.

最新問題**: 173**
障害を持つユーザーは、Ctrl + Alt + Del キーボード シーケンスを 1 つずつ押すことができる必要があります。
次のどれがこの簡単操作機能をオンにしますか?
A. Shift キーを 5 回続けて押します。
B. Ctrl+Alt+Esc を同時に押します。
C. Ctrl+Alt+Tab を同時に押します。
D. Windows キー + Tab キーを押します。
Answer: A (メーッセージを残す**)**
The Ease of Access feature in Windows that allows a user to press keyboard shortcuts one key at a time is called "Sticky Keys." Sticky Keys is designed to assist users with disabilities who have difficulty pressing multiple keys simultaneously. To enable Sticky Keys:
* Press the Shift key five times in a row:This is the quickest method to activate Sticky Keys. When you press the Shift key five times, a dialog box appears, asking if you want to turn on Sticky Keys. This method is widely documented as the default shortcut for enabling this feature.
* Confirmation dialog:A confirmation dialog will appear asking if you want to turn on Sticky Keys.
Click "Yes" to enable it.
* Control Panel or Settings:Alternatively, you can enable Sticky Keys through the Control Panel or the Settings app. Go to "Ease of Access" settings, find the "Keyboard" section, and turn on Sticky Keys from there.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 1.4: Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
Windows Ease of Access documentation.

最新問題**: 174**
コンピューターでプライバシー スクリーンを使用すると、次の脅威のどれを防ぐことができますか?
A. なりすまし

B. ショルダーサーフィン
C. Whaling
D. 共連れ
Answer: (解答を表示する**)**
Shoulder surfing is a threat that involves someone looking over another person's shoulder to observe their screen, keyboard, or other sensitive information. Shoulder surfing can be used to steal passwords, personal identification numbers (PINs), credit card numbers, or other confidential data. The use of a privacy screen on a computer can help prevent shoulder surfing by limiting the viewing angle of the screen and making it harder for someone to see the screen from the side or behind. Impersonation, whaling, and tailgating are not threats that can be prevented by using a privacy screen on a computer.

最新問題**: 175**
新しいサービス デスクは、リクエストの量を管理するのに苦労しています。次のうち、部門にとって最適なソリューションはどれですか?
A. サポートポータルの実装
B. 発券システムの作成
C. 自動コールバック システムの試運転
D. メールでチケットを送信する
Answer: A (メーッセージを残す**)**
A support portal is an online system that allows customers to access customer service tools, submit requests and view status updates, as well as access information such as how-to guides, FAQs, and other self-service resources. This would be the best solution for the service desk, as it would allow them to easily manage the volume of requests by allowing customers to submit their own requests and view the status of their requests.
Additionally, the portal would provide customers with self-service resources that can help them resolve their own issues, reducing the amount of tickets that need to be handled by the service desk.

最新問題**: 176**
ある組織は、Wi-Fi に接続するために、ユーザーとユーザーのコンピューターの両方がサーバー上の特定の管理グループに属している必要があるワイヤレス セキュリティの方法を実装しました。次の無線セキュリティ方法のうち、この組織が実装したものを最もよく表しているのはどれですか?
A. TKIP
B. 半径
C. WPA2
D. AES
Answer: B (メーッセージを残す**)**
RADIUS stands for Remote Authentication Dial-In User Service and it is a protocol that provides centralized authentication, authorization, and accounting for network access. RADIUS can be used to implement a method of wireless security that requires both a user and the user's computer to be in specific managed groups on the server in order to connect to Wi-Fi. This is also known as 802.1X authentication or EAP-TLS authentication

最新問題**: 177**
ユーザーがワークステーション上でバックアップをセットアップしています。ユーザーは、復元プロセスをできるだけ簡単にしたいと考えています。ユーザーは次のバックアップ タイプのうちどれを選択する必要がありますか?
A. フル
B. インクリメンタル
C. 差動
D. 合成
Answer: A (メーッセージを残す**)**

Full backup is the best option to ensure that the restore process is as simple as possible. A full backup is a backup type that copies all the data from the source to the destination, regardless of whether the data has changed or not. A full backup provides the most complete and consistent backup of the data, and it allows the user to restore the data from a single backup set without relying on any previous or subsequent backups.
Incremental, differential, and synthetic backups are not as simple as full backups for restoring data. An incremental backup is a backup type that copies only the data that has changed since the last backup, whether it was full or incremental. An incremental backup requires less time and space than a full backup, but it also requires multiple backup sets to restore the data completely. A differential backup is a backup type that copies only the data that has changed since the last full backup. A differential backup requires more time and space than an incremental backup, but it also requires fewer backup sets to restore the data than an incremental backup. A synthetic backup is a backup type that combines a full backup with one or more incremental or differential backups to create a consolidated backup set. A synthetic backup requires less time and bandwidth than a full backup, but it also requires more processing power and storage space than an incremental or differential backup. References:
* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
* CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

最新問題**: 178**
大企業は新しい Windows オペレーティング システムを選択しており、暗号化とエンドポイント保護が組み込まれていることを確認する必要があります。次の Windows バージョンのうち、最も選択される可能性が高いのはどれですか?
A. ホーム
B. プロ
C. ワークステーションのプロ
D. エンタープライズ
Answer: D (メーッセージを残す**)**
When selecting a new Windows operating system for a large company that needs built-in encryption and endpoint protection, the Enterprise edition is the most likely choice. This edition provides advanced security features such as Windows Defender Advanced Threat Protection (ATP), AppLocker, and BitLocker Drive Encryption. These features can help to protect the company's data and endpoints against malware attacks, unauthorized access, and data theft.
The Home and Pro editions of Windows do not include some of the advanced security features provided by the Enterprise edition, such as Windows Defender ATP and AppLocker. The Pro for Workstations edition is designed for high-performance and high-end hardware configurations, but it does not provide additional security features beyond those provided by the Pro edition.

最新問題**: 179**
企業所有の iOS デバイスでアクティベーション ロックの問題が発生する原因は次のうちどれですか?
A. キーチェーンのパスワードを忘れた場合
B. デバイスで使用されている従業員の Apple ID
C. ジェイルブレイクされたオペレーティング システム
D. 有効期限が切れた画面ロック解除コード
Answer: B (メーッセージを残す**)**
Activation Lock is a feature that prevents anyone from erasing or activating an iOS device without the owner's Apple ID and password. If a corporate-owned iOS device is linked to an employee's Apple ID, it will have an Activation Lock issue when the employee leaves the company or forgets their Apple ID credentials.
Reference: CompTIA A+ Core 2 Exam Objectives, Section 4.1

最新問題**: 180**
技術者が、ユーザーのデスクトップ コンピュータに新しいビジネス アプリケーションをインストールしています。マシンは Windows 10 Enterprise 32 ビット オペレーティング システムを実行しています。インストールを完了するために技術者が実行する必要があるファイルは次のうちどれですか?
A. Installer_x64.exe
B. Installer_Files.zip

C. Installer_32.msi
D. Installer_x86.exe
E. Installer_Win10Enterprise.dmg
Answer: D (メーッセージを残す)
The 32-bit operating system can only run 32-bit applications, so the technician should execute the 32-bit installer. The "x86" in the file name refers to the 32-bit architecture.
https://www.digitaltrends.com/computing/32-bit-vs-64-bit-operating-systems/

最新問題**: 181**
ユーザーがネットワークにログインできません。ネットワークは 802.1X と EAP-TLS を使用して有線ネットワークで認証します。ユーザーは長期休暇中で、数か月間コンピュータにログインしていません。
ログインの問題を引き起こしているのは次のうちどれですか?
A. 期限切れの証明書
B. OS アップデート失敗
C. サービスが開始されていません
D. アプリケーションのクラッシュ
E. プロファイルの再構築が必要
Answer: A (メーッセージを残す)
EAP-TLS is a method of authentication that uses certificates to establish a secure tunnel between the client and the server3. The certificates have a validity period and must be renewed before they expire1. If the user has been on an extended leave and has not logged in to the computer in several months, it is possible that the certificate on the client or the server has expired and needs to be renewed2. The other options are not directly related to EAP-TLS authentication or 802.1X network access.

最新問題**: 182**
ユーザーが新しいコンピュータ ゲームをインストールしました。ゲームを開始すると、ユーザーはフレーム レートが低いことに気づきます。
問題を解決するには、ユーザーがアップグレードする必要があるのは次のうちどれですか?
A. ハードドライブ
B. グラフィックカード
C. ランダムアクセスメモリ
D. モニター
Answer: B (メーッセージを残す)
A graphics card, also known as a video card or a GPU (graphics processing unit), is a component that can affect the performance of a computer game. A graphics card is responsible for rendering and displaying graphics on the screen, such as images, animations, and effects. A computer game may require a high level of graphics processing power to run smoothly and achieve high frame rates, which are the number of frames per second (FPS) that the game can display. Upgrading to a better graphics card can improve the performance of a computer game by increasing its graphics quality and frame rates. Hard drive, random-access memory, and monitor are not components that can directly improve the performance of a computer game.

最新問題**: 183**

次のデータのうち、規制される可能性が最も高いのはどれですか?
A. 電話帳の名前
B. 診断名
C. 求職者名義
D. 雇用主のウェブサイト上の名前
Answer: B (メーッセージを残す**)**
A name on a medical diagnosis (B) is most likely to be regulated. This is because it falls under the category of protected health information (PHI), which is subject to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. These regulations aim to protect the privacy and security of individuals' health information.

最新問題**: 184**
ユーザーがパスワードを忘れたため、システム管理者はユーザーのパスワードをリセットする必要があります。システム管理者は新しいパスワードを作成し、ユーザーのアカウントをさらに保護したいと考えています。システム管理者が行うべきことは次のうちどれですか?
A. 次回ログイン時にパスワードの変更を要求します。
B. ユーザーがパスワードを変更できないようにします。
C. アカウントを無効にする
D. 無期限のパスワードを選択します。
Answer: (解答を表示する**)**
This will ensure that the user is the only one who knows their password, and that the new password is secure.
The CompTIA A+ Core 2 220-1002 exam covers this topic in the domain 1.4 Given a scenario, use appropriate data destruction and disposal methods.

最新問題**: 185**
技術者は、大量の法律事務所でドキュメントのバックアップ システムをアップグレードしています。現在のバックアップ システムが保持できるフル バックアップのバージョンは、失敗するまでに 3 つまでです。法律事務所は復元時間については考慮していませんが、可能であればより多くのバージョンを保持するよう技術者に依頼しています。次のバックアップ方法のうち、技術者が実装する可能性が最も高いのはどれですか?
A. フル
B. ミラー
C. インクリメンタル
D. 差動
Answer: (解答を表示する**)**
Incremental backup is a backup method that only backs up the files that have changed since the last backup, whether it was a full or an incremental backup. Incremental backup can save storage space and bandwidth, as it does not copy the same files over and over again. Incremental backup can also retain more versions of backups, as it only stores the changes made to the files. However, incremental backup can have longer restore times, as it requires restoring the last full backup and all the subsequent incremental backups in order to recover the data. The law firm is not concerned about restore times but asks the technician to retain more versions when possible, so incremental backup would be a suitable choice for them.

最新問題**: 186**
技術者がハードディスクのパーティションを分割しています。5 つのプライマリ パーティションには 4TB の空き領域が含まれている必要があります。技術者がデバイスを分割するために使用する必要があるパーティション スタイルは次のうちどれですか?
A. EFS
B. GPT
C. MBR

D. FAT32
Answer: B (メーッセージを残す)
GPT is the correct answer for this question. GPT stands for GUID Partition Table, and it is a partition style that supports up to 128 primary partitions and up to 18 exabytes of disk size per partition. GPT also uses a unique identifier for each partition and provides better data protection and recovery. GPT is suitable for partitioning a hard disk that has five primary partitions with 4TB of free space each. EFS, MBR, and FAT32 are not correct answers for this question. EFS stands for Encrypting File System, and it is a feature that allows encrypting files and folders on NTFS volumes. EFS is not a partition style, but rather a file system attribute.
MBR stands for Master Boot Record, and it is an older partition style that supports up to four primary partitions and up to 2TB of disk size per partition. MBR cannot handle five primary partitions with 4TB of free space each. FAT32 stands for File Allocation Table 32, and it is a file system that supports up to 32GB of disk size per partition and up to 4GB of file size. FAT32 is not a partition style, but rather a file system type. References:
* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 14
* CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 105

最新問題**: 187**
Linux OS を使用している顧客が、ヘルプ デスクに電話して、見つからないファイルを見つけるための支援を求めました。顧客はファイルの正確な名前を知りませんが、ファイル名の一部を提供できます。技術者は次のツールのうちどれを使用する必要がありますか? (2 つ選択してください)。
A. cat
B. df
C. grep
D. ps
E. dig
F. find
G. top
Answer: (解答を表示する)
To locate a missing file with only a partial name known, the best tools to use in a Linux environment would be grepandfind.
grep:This command is used to search the contents of files for a specific pattern. Whilegrepitself might not be the first choice for finding file names, it can be combined with other commands (likelsorfind) to search within file lists or contents.
find:This command is used to search for files in a directory hierarchy based on various criteria like name, size, modification date, etc.findcan be used to search for files by partial name by using wildcards in the search pattern.
cat(A) is used to concatenate and display the content of files.df(B) displays the amount of disk space used and available on filesystems.ps(D) shows information about active processes.dig(E) is used for querying DNS name servers.top(G) displays Linux tasks and system performance information. None of these tools are directly suited for finding files by partial names.

最新問題**: 188**
あるユーザーが、診療所で顧客の受付に使用されていた会社のタブレットを紛失しました。次のアクションのうち、データの不正アクセスから最もよく保護するのはどれですか?
A. オフィスのWi-Fi SSIDとパスワードを変更する
B. デバイスでリモート ワイプを実行中
C. ユーザーのパスワードを変更する
D. リモートドライブの暗号化を有効にする
Answer: B (メーッセージを残す)
The best action to protect against unauthorized access of the data on the lost company tablet is to perform a remote wipe on the device. A remote wipe is a feature that allows an administrator or a user to erase all the data and settings on a device remotely, usually through a web portal or an email command. A remote wipe can help prevent the data from being accessed or compromised by anyone who finds or steals the device.

Changing the office's Wi-Fi SSID and password may prevent the device from connecting to the office network but may not prevent the data from being accessed locally or through other networks. Changing the user's password may prevent the device from logging in to the user's account but may not prevent the data from being accessed by other means or accounts. Enabling remote drive encryption may protect the data from being read by unauthorized parties but may not be possible if the device is already lost or turned off.
References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.1

最新問題**: 189**
ある会社が新しいファイアウォールに移行しているときに、サーバーの 1 つがまだ古いファイアウォールにトラフィックを送信していることを発見しました。この問題を解決するために技術者が変更する必要がある IP アドレス設定は次のどれですか。
A. ダイナミック
B. ゲートウェイ
C. NAT
D. DNS サーバー
Answer: (解答を表示する**)**
Detailed Explanation with Core 2 References:The default gateway directs network traffic to external networks. If the traffic is still going to the old firewall, updating the gateway setting will redirect it to the new firewall. This task is part of network configuration management covered in Core 2 (Core 2 Objective 2.5).

最新問題**: 190**
ユーザーは、ホーム ネットワーク上の PC で個人ファイルを開くことができません。画面上のメッセージには、ファイルが暗号化されており、ファイルにアクセスするには料金を支払う必要があることが示されています。技術者は、まずユーザーに次のどれを実行するよう勧めるべきでしょうか。
A. OS を再インストールします。
B. システムの復元機能を実行します。
C. PCをネットワークから切断します。
D. 要求された金額を支払います。
E. マルウェア対策プログラムを使用して PC をスキャンします。
Answer: C (メーッセージを残す**)**
Detailed Explanation with Core 2 References:The PC is likely infected with ransomware. The immediate step should be to disconnect from the network to prevent the malware from spreading to other devices. Core 2 highlights steps to respond to malware incidents, such as disconnecting from the network as part of containment measures (Core 2 Objective 2.3).

最新問題**: 191**
ユーザーが感染した電子メールを開いた。セキュリティ管理者は悪意のあるイベントに対応し、状況を軽減し、マシンをサービスに戻しました。このイベントが終了したとみなされる前に、次のどれを完了する必要がありますか?
A. 利用規約
B. インシデントレポート
C. エンドユーザー使用許諾契約
D. 標準操作手順
Answer: (解答を表示する**)**
After successfully mitigating a malicious event caused by an infected email, the final step before considering the event closed is to complete an incident report. This document should detail the nature of the incident, the steps taken to resolve it, and any lessons learned to improve future responses to similar threats.

最新問題**: 192**

組織は、カスタマイズ可能なオペレーティング システムを導入したいと考えています。組織は次のうちどれを選択する必要がありますか?
A. Windows 10
B. macOS
C. Linux
D. Chrome OS
E. iOS
Answer: C (メーッセージを残す)
Linux is known for its high degree of customizability and flexibility, making it an ideal choice for organizations looking to deploy a customizable operating system. Unlike proprietary operating systems, Linux allows users to modify or replace almost any part of the system, from the kernel to the desktop environment and applications, to suit their specific needs.
Linux:This open-source operating system provides access to the source code, enabling extensive customization. Organizations can tailor Linux distributions to fit specific requirements, making it a popular choice for servers, specialized workstation environments, and embedded systems.
Windows 10 (A) and macOS (B) offer some level of customization but are more restricted due to their proprietary nature. Chrome OS (D) is designed for simplicity and security, focusing on web applications, which limits deep system-level customizations. iOS(E) is designed for Apple's mobile devices and is not applicable for organizational deployment beyond mobile and tablet devices; it also offers limited customization compared to Linux.

最新問題**: 193**
営業担当者のコンピュータが、コンピュータに接続されているローカル プリンタで注文を印刷できません 営業担当者は、次のどのツールを使用して印刷スプーラを再起動する必要がありますか?
A. コントロールパネル
B. プロセス
C. 起動
D. サービス
Answer: D (メーッセージを残す)
The correct answer is D. Services. The print spooler is a service that manages the print queue and sends print jobs to the printer. To restart the print spooler, the salesperson can use the Services app, which allows them to stop and start the service. Alternatively, they can also use the Task Manager or the Command Prompt to restart the print spooler.
References and Explanation:
The Services app is a tool that displays all the services that are running on the computer. It can be accessed by typing services.msc in the Run window or by searching for Services in the Start menu. The Services app allows users to start, stop, restart, or configure any service, including the print spooler123.
The Task Manager is a tool that shows information about the processes, applications, and services that are running on the computer. It can be accessed by pressing Ctrl + Shift + Esc or by right-clicking on the taskbar and selecting Task Manager. The Task Manager allows users to start, stop, or restart any service by going to the Services tab and right-clicking on the service name12.
The Command Prompt is a tool that allows users to execute commands and perform tasks using text input. It can be accessed by typing cmd in the Run window or by searching for Command Prompt in the Start menu.
The Command Prompt allows users to start, stop, or restart any service by using the net command with the service name. For example, to restart the print spooler, users can type net stop spooler and then net start spooler1.
The Control Panel is a tool that provides access to various settings and options for the computer. It can be accessed by typing control panel in the Run window or by searching for Control Panel in the Start menu. The Control Panel does not allow users to restart the print spooler directly, but it can be used to access other tools such as Devices and Printers, Troubleshooting, or Administrative Tools2.
The Processes tab is a part of the Task Manager that shows information about the processes that are running on the computer. It can be accessed by opening the Task Manager and selecting the Processes tab. The Processes tab does not allow users to restart the print spooler directly, but it can be used to end any process that is related to printing or causing problems with the print spooler2.
The Startup tab is a part of the Task Manager that shows information about the programs that run automatically when the computer starts. It can be accessed by opening the Task Manager and selecting the Startup tab. The Startup tab does not allow users to restart the print spooler directly, but it can be used to disable or enable any program that affects printing or interferes with the print spooler2.

最新問題**: 194**

ヘルプ デスクの技術者がスクリプト Inventory.py を実行します。技術者は、次のエラー メッセージを受け取ります。
このファイルをどのように開きますか?
このスクリプトを実行できない理由として最も可能性が高いのは次のうちどれですか?
A. スクリプトの実行は許可されていません。
B. スクリプトは Windows 用に作成されていません。
C. スクリプトには管理者権限が必要です。
D. 実行環境がインストールされていません。
Answer: D (メーッセージを残す**)**
The error message is indicating that the script is not associated with any program on the computer that can open and run it. This means that the script requires a runtime environment, such as Python, to be installed in order for it to execute properly. Without the appropriate runtime environment, the script will not be able to run.

最新問題**: 195**
技術者は、動作が遅く、ポップアップが頻繁に表示されるユーザーの PC のトラブルシューティングを行っています。技術者は、マルウェアが問題の原因である可能性があると考えていますが、問題が発生する前に、ユーザーはポップアップ ウィンドウに応じてマルウェア対策ソフトウェアをインストールしました。これらの問題の原因として最も可能性が高いのは次のうちどれですか?
A. 証明書の有効期限が切れています
B. 誤った警告
C. システム ファイルがありません
D. OS アップデート失敗
Answer: B (メーッセージを残す**)**
The scenario described is characteristic of a malware tactic known as scareware, where users are tricked into installing malware through false alerts claiming that their system is infected. The anti-malware software installed in response to a pop-up is likely malicious, causing the system to run slowly and display frequent pop-ups.

最新問題**: 196**
ある企業は、ネットワーク上で新しいコンピュータを起動するときに、ベースライン イメージをそれらのコンピュータに展開したいと考えています。
企業はこのタスクに次のどのブート プロセスを使用する必要がありますか?
A. ISO
B. 安全
C. USB
D. PXE
Answer: (解答を表示する**)**
Comprehensive and Detailed In-Depth Explanation:PXE (Preboot Execution Environment) allows a computer to boot from a network server and install a system image remotely. It is commonly used for large-scale deployments because it eliminates the need for physical installation media.
* A. ISO - Incorrect. ISO files are used for manual installations, but they do not automate network deployments.
* B. Secure - Incorrect. There is no "secure boot process" option for automated deployments. Secure Boot is a security feature.
* C. USB - Incorrect. USB boot requires manual installation on each device, making it inefficient for mass deployment.
Reference:
CompTIA A+ 220-1102, Objective 3.3 - Deployment Methods and Imaging

最新問題**: 197**
インターネット カフェには、公共で使用できるコンピューターが数台あります。最近、ユーザーからコンピューターの速度が前週よりも大幅に遅くなったとの報告がありました。技術者は、CPU の使用率が 100% であることを発見しましたが、ウイルス対策スキャンでは現在の感染は報告されていません。問題の原因として最も考えられるのは次のうちどれですか?
A. スパイウェアがブラウザ検索をリダイレクトしています。
B. クリプトマイナーがトランザクションを検証しています。
C. 駆除されたウイルス感染によりファイルが破損しました。
D. キーロガーがユーザーのパスワードをキャプチャしています。
Answer: B (メーッセージを残す**)**
A cryptominer is a malicious program that uses the CPU resources of a computer to generate cryptocurrency, such as Bitcoin or Ethereum. This can cause the CPU to run at 100% utilization and slow down the system.
Spyware, virus and keylogger are other types of malware, but they do not necessarily cause high CPU usage.
Verified References: https://www.comptia.org/blog/what-is-cryptomining https://www.comptia.org
/certifications/a

最新問題**: 198**
システム管理者は、大規模な企業オフィスでネットワーク パフォーマンスの問題のトラブルシューティングを行っています。エンド ユーザーは、特定の内部環境へのトラフィックが安定しておらず、頻繁に低下すると報告しています。次のコマンドライン ツールのうち、問題をさらに調査するための最も詳細な情報を提供できるものはどれですか?
A. ipconfig
B. アルプ
C. nslookup
D. パス指定
Answer: D (メーッセージを残す**)**
Pathping is the best command-line tool to provide the most detailed information for investigating the network performance issue further. Pathping is a utility that combines the functions of ping and tracert, which are two other command-line tools that test network connectivity and latency. Pathping sends packets to each router on the path to a destination and then computes results based on the packets returned from each hop. Pathping can show the route taken by the packets, the number of hops, the latency of each hop, and the packet loss percentage. This information can help the systems administrator identify where the network problem occurs and how severe it is. Ipconfig, arp, and nslookup are not as useful as pathping for this task. Ipconfig shows the configuration of the network interface card, such as IP address, subnet mask, and default gateway. Arp shows the mapping of IP addresses to MAC addresses in the local network. Nslookup queries DNS servers for domain name resolution. References:
* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 21
* CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 457

最新問題**: 199**
最も弱いワイヤレス セキュリティ プロトコルは次のうちどれですか?
A. WEP
B. WPA2
C. TKIP

D. AES
Answer: A (メーッセージを残す)
WEP (Wired Equivalent Privacy) is known to be the weakest wireless security protocol due to its vulnerabilities and ease of being compromised.
* WEP: The oldest and weakest protocol, susceptible to various attacks and easily cracked.
* WPA2: Much stronger security with AES encryption, currently one of the most secure standards.
* TKIP: Used with WPA, stronger than WEP but weaker than WPA2 with AES.
* AES: Advanced Encryption Standard, used in WPA2 and known for strong security.
Reference: CompTIA A+ Exam Objectives [220-1102] - 2.2: Compare and contrast wireless security protocols and authentication methods.

最新問題**: 200**
ユーザーは新しいソフトウェア プログラムの 64 ビット バージョンをダウンロードしましたが、エラーのためインストールに失敗しました。
エラーの原因として最も可能性が高いのは次のどれですか?
A. OS バージョンに互換性がありません。
B. ユーザーは ActiveX を有効にする必要があります。
C. .NET Framework を更新する必要があります。
D. ユーザーに管理者権限が必要です。
Answer: A (メーッセージを残す)
The most likely reason for the installation failure of a 64-bit software is that the operating system is incompatible, specifically if the system is running a 32-bit version of the OS. A 64-bit program requires a 64-bit operating system to run, and if the user's OS is a 32-bit version, the software will fail to install. Other reasons, like needing administrator privileges or updating .NET, are valid but less likely since the error message would be different.
References:
Microsoft Support: 32-bit and 64-bit Windows: Frequently Asked Questions CompTIA A+ 220-1102 Study Guide (CompTIA) (ProfMesser)

最新問題**: 201**
ある macOS ユーザーが、フリーズしているように見えるプログラム上で回転する丸いカーソルが表示されると報告しています。技術者が macOS でプログラムを強制的に終了させるために使用する方法は次のうちどれですか?
A. 技術者は Ctrl+Alt+Del キーを押して [強制終了] メニューを開き、リストでフリーズしたアプリケーションを選択して、[強制終了] をクリックします。
B. 技術者がフリーズしたアプリケーションをクリックし、キーボードの Esc キーを 10 秒間押し続けます。これにより、アプリケーションが強制終了されます。
C. 技術者は Finder を開き、[アプリケーション] フォルダーに移動し、リストでフリーズしているアプリケーションを見つけ、アプリケーションを右クリックして、[強制終了] オプションを選択します。
D. 技術者は Apple アイコン メニューを開き、[強制終了] を選択し、リストでフリーズしたアプリケーションを選択して、[強制終了] をクリックします。
Answer: D (メーッセージを残す)
The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit. This is the most common method of force quitting a program in macOS. This can be done by clicking on the Apple icon in the top left of the screen, selecting Force Quit, selecting the frozen application in the list, and then clicking Force Quit. This will force the application to quit and the spinning round cursor will disappear.

最新問題**: 202**
ユーザーは、子供がインターネットに費やす時間を制限しようとしています。この目的を達成するには、次の Windows 10 設定のうちどれを有効にする必要がありますか?
A. ファミリー オプション
B. アップデートとセキュリティ
C. アクセスのしやすさ

D. ネットワークとインターネット
E. プライバシー
Answer: (解答を表示する**)**
Windows 10 includes a set of parental controls within the "Family Options" section of the Windows settings.
This feature allows parents to manage their children's computing activities, including setting time limits on device use, filtering web content, managing privacy and online safety settings, and viewing activity reports.
Family Options: By enabling and configuring Family Options, the user can set specific times when their children can use the device and access the internet, effectively limiting their overall screen time and internet usage.
Update & Security (B) mainly deals with Windows updates and security features but does not directly provide settings for time management. Ease of Access (C) is focused on accessibility settings and does not include time management options. Network & Internet (D) settings control network connectivity and do not offer parental controls or time limits. Privacy (E) settings manage which applications can access device features and user data but do not include time management options.

最新問題**: 203**
技術者は企業と協力して、ビジネスを行う際に機密性の高い個人情報をオフィス間で転送する最善の方法を決定しています。同社は現在 USB ドライブを使用しており、変化に抵抗しています。同社のコンプライアンス オフィサーは、保管中のすべてのメディアを暗号化する必要があると述べています。現在のワークフローを保護するための最良の方法は次のうちどれですか?
A. 暗号化されたセカンダリ ハード ドライブを適切なワークステーションに展開します。
B. ファイル サーバー間のファイル転送用に強化された SFTP ポータルを構成する
C. ファイルを一意のパスワードで個別にパスワード保護する必要があります
D. 企業の要件を満たすパスワードで BitLocker To Go を有効にします
Answer: D (メーッセージを残す**)**
The BEST way to secure the current workflow of transferring sensitive personal information between offices when conducting business is to enable BitLocker To Go with a password that meets corporate requirements.
This is because BitLocker To Go is a full-disk encryption feature that encrypts all data on a USB drive, which is what the company currently uses, and requires a password to access the data.

最新問題**: 204**
技術者がユーザーの起動時間をトラブルシューティングしています。技術者は、MSConfig を使用して OS で起動しているプログラムを確認しようとしましたが、スタートアップ項目を表示するために使用できなくなったというメッセージが表示されます。技術者がスタートアップ項目を表示するために使用できるプログラムは次のうちどれですか?
A. msinfo32
B. パフォーマンスモン
C. レジストリ編集
D. タスクマネージャー
Answer: D (メーッセージを残す**)**
When troubleshooting boot times for a user, a technician may want to check which programs are starting with the operating system to identify any that may be slowing down the boot process. MSConfig is a tool that can be used to view startup items on a Windows system, but it may not always be available or functional.
In this scenario, the technician receives a message that MSConfig cannot be used to view startup items. As an alternative, the technician can use Task Manager (taskmgr), which can also display the programs that run at startup. To access the list of startup items in Task Manager, the technician can follow these steps:
Open Task Manager by pressing Ctrl+Shift+Esc.
Click the "Startup" tab.
The list of programs that run at startup will be displayed.

最新問題: **205**
セキュリティ ソフトウェアが、環境内のすべてのサーバーから誤ってアンインストールされました。同じバージョンのソフトウェアの再インストールを要求した後、セキュリティ アナリストは、変更要求に記入する必要があることを知りました。このシナリオで変更管理プロセスに従う最も適切な理由は次のうちどれですか?
A. 所有者は、変更が行われていることを通知され、パフォーマンスへの影響を監視できます。最も投票された
B. ソフトウェアが必要かどうかを判断するために、リスク評価を実行できます。
C. エンド ユーザーは、変更の範囲を認識することができます。
D. ソフトウェアがアプリケーションを壊した場合に備えて、ロールバック計画を実装できます。
Answer: (解答を表示する)
change management process can help ensure that owners are notified of changes being made and can monitor them for performance impact (A). This can help prevent unexpected issues from arising.

最新問題: **206**
Windows ユーザーは、ポップアップがセキュリティの問題を示していると報告しました。検査中、ウイルス対策システムは最近のダウンロードからマルウェアを特定しましたが、マルウェアを削除できませんでした。ユーザーのファイルを保持しながらマルウェアを削除するには、次のどのアクションが最適ですか?
A. ウイルス スキャナを管理モードで実行します。
B. オペレーティング システムを再インストールします。
C. システムをセーフ モードで再起動し、再スキャンします。
D. 感染ファイルを手動で削除します。
Answer: C (メーッセージを残す)
Rebooting the system in safe mode will limit the number of programs and processes running, allowing the antivirus system to more effectively identify and remove the malware. Rescanning the system will allow the antivirus system to identify and remove the malware while preserving the user's files.

最新問題: **207**
MFA が提供するものは次のうちどれですか?
A. セキュリティ強化
B. 暗号化
C. デジタル署名
D. 公開鍵インフラストラクチャ
Answer: A (メーッセージを残す)
MFA stands for multi-factor authentication, which is an electronic authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN1. MFA provides security enhancement by making it harder for attackers to compromise the user's identity or credentials, as they would need to obtain more than just the username and password. MFA can also prevent unauthorized access to sensitive data or resources, as well as reduce the risk of identity theft or fraud2.

最新問題: **208**
次のオペレーティング システムのうち、クローズド ソースとみなされているのはどれですか?
A. 無料
B. アンドロイド
C. CentOS
D. OSX
Answer: (解答を表示する)

OSX (now macOS) is an operating system that is considered closed source, meaning that its source code is not publicly available or modifiable by anyone except its developers. It is owned and maintained by Apple Inc. Ubuntu, Android and CentOS are operating systems that are considered open source, meaning that their source code is publicly available and modifiable by anyone who wants to contribute or customize them.
Verified References: https://www.comptia.org/blog/open-source-vs-closed-source-software https://www.
comptia.org/certifications/a

最新問題**: 209**
システム管理者は、新しいユーザー用に Windows コンピュータをセットアップしています。企業ポリシーでは、最小限の特権環境が必要です。ユーザーは、いくつかのアプリケーションの高度な機能と構成設定にアクセスする必要があります。ユーザーが必要とするアカウント アクセス レベルを最もよく表しているのは、次のうちどれですか?
A. パワー ユーザー アカウント
B. スタンダード口座
C. ゲスト アカウント
D. 管理者アカウント
Answer: B (メーッセージを残す**)**
The account access level the user will need to access advanced features and configuration settings for several applications while adhering to corporate policy requiring a least privilege environment is a standard account. This is because a standard account allows the user to access advanced features and configuration settings for several applications while adhering to corporate policy requiring a least privilege environment1.

最新問題**: 210**
変更の実装中に問題が発生した場合に実行する手順を示しているものは次のうちどれですか?
A. テスト中
B. ロールバック
C. リスク
D. 承諾
Answer: B (メーッセージを残す**)**
Rollback refers to the steps to be taken if an issue occurs during a change implementation. It means restoring the system to its previous state before the change was applied, using backup data or configuration files. It can minimize the impact and downtime caused by a failed change. Testing refers to the steps to be taken before a change implementation, to verify that the change works as expected and does not cause any errors or conflicts. Risk refers to the potential negative consequences of a change implementation, such as data loss, security breach, performance degradation, etc. Acceptance refers to the steps to be taken after a change implementation, to confirm that the change meets the requirements and expectations of the stakeholders.
Verified References: https://www.comptia.org/blog/change-management-process https://www.comptia.org
/certifications/a

最新問題**: 211**
技術者は、会議室での視聴覚の問題のトラブルシューティングを任されています。会議の発表者は音声付きのビデオを再生できません。次のエラーが表示されます。
オーディオドライバーが実行されていません。
問題を解決する可能性が最も高いのは次のうちどれですか?
A. compmgmt.msc
B. regedit.exe
C. エクスプローラー.exe
D. taskmgt.exe

E. gpmc.msc
F. services.msc
Answer: F (メーッセージを残す)
services.msc is a tool that can be used to resolve the issue of "The Audio Driver is not running" on a Windows machine. It allows a technician to view, start, stop and configure the services that run on the system, such as the Windows Audio service. compmgmt.msc, regedit.exe, explorer.exe, taskmgt.exe and gpmc.msc are other tools that can be used for different purposes on a Windows machine, but they are not related to audio drivers or services. Verified References: https://www.comptia.org/blog/what-is-services-msc https://www.
comptia.org/certifications/a

最新問題: **212**
技術者は、ユーザーが自宅で作業できるようにコンピューターを構成し、ユーザーがユーザーの共有ファイルや会社の電子メールに安全にアクセスできるようにする必要があります。次のツールのうち、このタスクを最もよく実行できるのはどれですか*?
A. MSRA
B. FTP
C. RMM
D. VPN
Answer: D (メーッセージを残す)
A Virtual Private Network (VPN) creates a secure connection over the internet to a network, allowing a user to access shared files and corporate email as if they were directly connected to the network. This makes VPN the best tool for secure remote work access, compared to the other options which do not offer the same level of secure, remote network access.

最新問題: **213**
技術者は数百台の Mac ラップトップのソフトウェアを更新する必要があります。タスクを完了するための最良の方法は次のうちどれですか?
A. SSH
B. MDM
C. RDP
D. SFTP
Answer: B (メーッセージを残す)
For updating software on several hundred Mac laptops, the best method is Mobile Device Management (MDM). MDM solutions allow administrators to remotely manage and update software across multiple devices efficiently, making it an ideal choice for handling software updates on a large scale.

最新問題: **214**
ある技術者は、業界内で起きている捕鯨攻撃の件数が大幅に増加していることを懸念している。
技術者は、問題を回避するために会社のリスクを制限したいと考えています。技術者が実装する必要がある項目は次のうちどれですか?
A. スクリーンされたサブネット
B. ファイアウォール

C. フィッシング対策トレーニング
D. ウイルス対策
Answer: C (メーッセージを残す**)**
Anti-phishing training is a method of educating users on how to identify and avoid phishing attacks, which are attempts to trick users into revealing sensitive information or performing malicious actions by impersonating legitimate entities or persons. Whaling attacks are a specific type of phishing attack that target high-level executives or influential individuals within an organization. Anti-phishing training can help users recognize the signs of whaling attacks and prevent them from falling victim to them. Screened subnet, firewall, and antivirus are not items that can directly address the issue of whaling attacks.

最新問題**: 215**
技術者は、狭くて混雑したオフィスにワイヤレス ネットワークをセットアップしており、Wi-Fi アクセスを最小限に抑えたいと考えています。技術者は次のどのセキュリティ設定を有効にする必要がありますか?
A. ポート転送
B. 未使用のポート
C. SSIDブロードキャスト
D. 許可リスト
Answer: (解答を表示する**)**
Enabling an allow list (Option D) will limit access to the wireless network by only allowing devices with specified MAC addresses to connect. This is an effective method for minimizing Wi-Fi access in a crowded environment.
* Port forwarding (Option A) controls traffic through specific ports but doesn't minimize wireless access.
* Unused ports (Option B) could refer to physical network ports or firewall settings, unrelated to controlling Wi-Fi access.
* Disabling SSID broadcast (Option C) might hide the network name but doesn't secure access.
CompTIA A+ Core 2 References:
* 2.9 - Configure security settings for SOHO networks, including MAC filtering .

最新問題**: 216**
技術者は、視覚障害のあるユーザー用にコンピューターを構成する任務を負っています。技術者が使用する必要があるユーティリティは次のうちどれですか?
A. デバイス マネージャー
B. システム
C. 簡単操作センター
D. プログラムと機能
Answer: C (メーッセージを残す**)**
The Ease of Access Center is a built-in utility in Windows that provides tools and options for making a computer easier to use for individuals with disabilities, including the visually impaired. In the Ease of Access Center, the technician can turn on options like high contrast display, screen magnification, and screen reader software to help the user better interact with the computer.

最新問題**: 217**
次の言語タイプのうち、タスクの自動化が可能になるのはどれですか?
A. コンパイル済み
B. スクリプト
C. ウェブ
D. データベース
Answer: (解答を表示する**)**

Scripting languages are designed for automating tasks by writing scripts that can execute a series of commands. They are typically easier to write and understand compared to compiled languages and are widely used for automating repetitive tasks, making them the best option for task automation.

最新問題: **218**
Web ページリクエストで任意の文字を送信する必要があるのは次のうちどれですか?
A. SMS
B. SSL
C. XSS
D. VPN
Answer: C (メーッセージを残す)
XSS stands for cross-site scripting, which is a web security vulnerability that allows an attacker to inject malicious code into a web page that is viewed by other users1. XSS involves sending arbitrary characters in a web page request, such as a query string, a form field, a cookie, or a header, that contain a malicious script.
The web server does not validate or encode the input, and returns it as part of the web page response. The browser then executes the script, which can perform various actions on behalf of the attacker, such as stealing cookies, session tokens, or other sensitive information, redirecting the user to a malicious site, or displaying fake content

最新問題: **219**
会社でハードウェアのアップグレードを行っている技術者に、コンピュータのアップグレード要求を送信したユーザーが連絡してきました。技術者はアップグレードするオフィスのリストを確認した後、ユーザーのオフィスがアップグレードのリストに含まれていないことを知りました。技術者は次にどのアクションを実行する必要がありますか?
A. 会社の人事部に問題の解決を依頼してください。
B. ユーザーの懸念事項をプロジェクト マネージャーに通知します。
C. このリクエストはアップグレード対象のリストに含まれていないことをユーザーに伝えます。
D. 技術者がコンピューターをアップグレードする必要があるかどうかをユーザーの上司に問い合わせます。
Answer: (解答を表示する)
When a technician finds that a user's office is not listed for an upgrade but the user has submitted a request, the appropriate action is to:
* Notify the project manager about the user's concern: The project manager oversees the upgrade process and can address any discrepancies or omissions in the upgrade list.
* Ask the company's human resources department to address the issue: HR typically handles personnel matters, not hardware upgrades.
* Tell the user that this request is not on the list to be upgraded: This does not resolve the user's concern and could cause frustration.
* Ask the user's supervisor if the technician should upgrade the computer: The supervisor may not have the authority or information to make decisions about the upgrade list.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 4.1: Given a scenario implement best practices associated with documentation and support systems information management.
Best practices for handling user requests and project management documentation.

最新問題: **220**
技術者は、必要に応じて管理者だけが仮想化テクノロジを有効にできるようにラップトップを構成する必要があります。技術者は次のどれを構成する必要がありますか?
A. BIOSパスワード
B. ゲストアカウント
C. 画面ロック
D. 自動実行設定
Answer: (解答を表示する)
Reference: CompTIA A+ Certification Core 2 220-1102, Objective 2.6 (System Security Controls).

最新問題: **221**
技術者は、ドメインに参加しているすべてのコンピューターに適用されるパスワード要件を実装する必要があります。技術者が実行する必要がある可能性が高いコマンドはどれですか。
A. gpugdate
B. 開発マネージャ
C. レジストリエディター
D. レスモン
Answer: (解答を表示する**)**
The correct command is gpupdate (Option A), which refreshes Group Policy settings. To implement password requirements across domain-joined computers, the policy would be set via Group Policy, and then running the gpupdate command ensures that the new settings are applied to all systems.
* devmgmt (Option B) opens Device Manager, which is unrelated to Group Policy.
* regedit (Option C) opens the Windows Registry Editor, which is not used for group-wide password policy settings.
* resmon (Option D) opens Resource Monitor, which helps monitor system resources, not Group Policy.
CompTIA A+ Core 2 References:
* 1.5 - Using appropriate Windows settings, including password policies via Group Policy.

最新問題: **222**
技術者がファイルから Windows OS のインプレース アップグレードを実行しようとしています。技術者がファイルをダブルクリックすると、ドライブをマウントするように求めるプロンプトが表示されます。技術者がダウンロードしたファイルの種類は次のうちどれですか。
A. 郵便番号
B. exe
C. 等価
D. msi
Answer: C (メーッセージを残す**)**

最新問題: **223**
企業は、光ディスクに保存されたデータを安全に廃棄する必要があります。このタスクを達成するための最も効果的な方法は次のうちどれですか?
A. 消磁
B. ローレベルフォーマット
C. リサイクル
D. シュレッダー
Answer: D (メーッセージを残す**)**
Shredding is the most effective method to securely dispose of data stored on optical discs12 References: 4. How Can I Safely Destroy Sensitive Data CDs/DVDs? - How-To Geek. Retrieved from https://www.howtogeek.com/174307/how-can-i-safely-destroy-sensitive-data-cdsdvds/ 5. Disposal - UK Data Service. Retrieved from https://ukdataservice.ac.uk/learning-hub/research-data-management/store-your- data/disposal/

最新問題: **224**
セキュリティ監査の調査結果は、ラップトップの紛失または盗難によるデータ損失のリスクが高いことを示しています。同社は、ネットワークに接続していないときにラップトップを使用したいユーザーへの影響を最小限に抑えて、このリスクを軽減したいと考えています。Windows ラップトップ ユーザーのこのリスクを軽減するのに最適なのは、次のうちどれですか?
A. 強力なパスワードの要求

B. キャッシュされた資格情報の無効化
C. サインオンに MFA を要求する
D. すべてのハード ドライブで BitLocker を有効にする
Answer: D (メーッセージを残す)
BitLocker is a disk encryption tool that can be used to encrypt the hard drive of a Windows laptop. This will protect the data stored on the drive in the event that the laptop is lost or stolen, and will help to reduce the risk of data loss. Additionally, BitLocker can be configured to require a PIN or other authentication in order to unlock the drive, providing an additional layer of security.

最新問題**: 225**
データセンターの安全性を維持するために最も重要な環境制御は次のうちどれですか?
A. 温度制御
B. 湿度制御
C. 消火制御
D. 電源管理制御
Answer: A (メーッセージを残す)
The most important environmental control to maintain the safety of a data center is Temperature control (A).
Proper temperature control is crucial to prevent overheating, which can lead to hardware failure, reduced performance, and shortened equipment lifespan. Data centers house high-density computing equipment that generates significant amounts of heat, making effective temperature management essential for maintaining operational stability and reliability.

最新問題**: 226**
技術者は、Windows コンピューター上でフォレンジック調査の証拠を追跡する必要があります。このプロセスを説明しているのは次のうちどれですか?
A. 有効なライセンス
B. データ保持要件
C. 製品安全データシート
D. 加工過程の管理
Answer: D (メーッセージを残す)
Chain of custody is a legal term that refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence1. It is important in forensic investigations to establish that the evidence is in fact related to the case, and that it has not been tampered with or contaminated. A technician needs to track evidence for a forensic investigation on a Windows computer by following the proper procedures for collecting, handling, storing, and analyzing the evidence, and documenting every step of the process on a chain of custody form23

最新問題**: 227**
ユーザーは、Windows 10 コンピューターのデスクトップの壁紙を変更する際にサポートが必要です。ユーザーが Windows 10 設定ツールを使用して壁紙を変更できるようにする方法は、次のうちどれですか?
A. [設定] を開き、[アカウント] を選択し、[あなたの情報] を選択して [参照] をクリックし、ユーザーが壁紙として使用する画像を見つけて開きます

B. [設定] を開き、[個人用設定] を選択し、[参照] をクリックして、ユーザーが壁紙として使用したい画像を見つけて開きます
C. [設定] を開き、[システム] を選択し、[ディスプレイ] を選択して、[参照] をクリックし、ユーザーが壁紙として使用する画像を見つけて開きます。
D. [設定] を開き、[アプリ] を選択し、[アプリと機能] を選択して [参照] をクリックし、ユーザーが壁紙として使用する画像を見つけて開きます。
Answer: B (メーッセージを残す**)**
The user can change the wallpaper using a Windows 10 Settings tool by following these steps12:
* Open Settings by pressing the Windows key and typing Settings, or by clicking the gear icon in the Start menu.
* Select Personalization from the left navigation menu.
* On the right side of the window, click Background.
* In the Background settings, click the drop-down menu and select Picture as the background type.
* Click Browse and then locate and open the image the user wants to use as the wallpaper.
The other options are incorrect because they do not lead to the Background settings or they do not allow the user to browse for an image. Accounts, System, and Apps are not related to personalization settings. Your info, Display, and Apps & features are not related to wallpaper settings.
References: 1: https://support.microsoft.com/en-us/windows/change-your-desktop-background-image-175618be-4cf1-c159-2785-ec2238b433a8 2: https://www.computerhope.com/issues/ch000592.htm

最新問題**: 228**
技術者は、ワークステーションに特殊なソフトウェアをインストールします。次に、技術者はソフトウェアを実行しようとします。
ワークステーションには、ソフトウェアの実行が許可されていないことを示すメッセージが表示されます。問題を解決する可能性が最も高いために、技術者が行うべきことは次のうちどれですか?
A. セーフモードでソフトウェアをインストールします。
B. 外部ハードウェアトークンを接続します。
C. OS アップデートをインストールします。
D. インストール後にワークステーションを再起動します。
Answer: B (メーッセージを残す**)**
A hardware token is a physical device that provides an additional layer of security for software authorization.
Some specialized software may require a hardware token to be attached to the workstation in order to run. A hardware token may contain a cryptographic key, a password, or a one-time code that verifies the user's identity or permission. Installing the software in safe mode, installing OS updates, and restarting the workstation after installation are not likely to resolve the issue of software authorization.

最新問題**: 229**
独自の作業が行われたユーザーの会社のラップトップの情報がコーヒー ショップから盗まれました。ユーザーは簡単なパスワードを使用してラップトップにログインしました。そして他のセキュリティメカニズムは導入されていませんでした。保存されたデータの回復を妨げる可能性が最も高いのは次のうちどれですか?
A. 生体認証
B. フルディスク暗号化
C. 強力なシステムパスワードを強制
D. 2要素認証
Answer: (解答を表示する**)**
Full disk encryption is a security mechanism that encrypts the entire data on a hard drive, making it unreadable without the correct decryption key or password. It can prevent the stored data from being recovered by unauthorized persons who steal or access the laptop. Biometrics, enforced strong system password and two-factor authentication are other security mechanisms, but they only protect the login access to the laptop, not the data on the hard drive. Verified References: https://www.comptia.org/blog/what-is-full- disk-encryption https://www.comptia.org/certifications/a

最新問題**: 230**

クライアントのデバイスは最近、他の複数のユーザーによって使用されました。クライアントは、デバイスの動作が通常よりも遅くなっていると報告しています。技術者が最初に実行する必要がある手順はどれですか? (2 つ選択してください。)
A. ウイルススキャンを実行する
B. スタートアッププログラムを確認する
C. データをバックアップする
D. ゲストアカウントを無効にする
E. ファームウェアを更新する
F. オペレーティングシステムを再インストールする
Answer: (解答を表示する**)**
Comprehensive and Detailed In-Depth Explanation:The two best first steps are:
* Perform a virus scan - Multiple users on a device increase the risk of malware, which can cause performance issues.
* Check the startup programs - Unnecessary programs running at startup can slow down the system.
* C. Back up the data - Important but not the first step for performance troubleshooting.
* D. Disable the guest account - May prevent future unauthorized use but does not immediately fix the current issue.
* E. Update the firmware - Firmware updates improve hardware stability but are unlikely to fix a sudden performance drop.
* F. Reinstall the operating system - A last resort, as it erases data and takes significant time.
Reference:
CompTIA A+ 220-1102, Objective 2.4 - Malware and Security Threat Removal

最新問題**: 231**
お客様からヘルプ デスクに電話があり、最近更新されたマシンが動作しなくなったと報告されました。サポート技術者は最新のログをチェックして、どのような更新が展開されたかを確認しますが、3 週間以上経過しても何も展開されませんでした。状況を最善に解決するには、サポート技術者が行うべきことは次のうちどれですか?
A. お客様にデバイスのワイプとリセットを提案します。
B. ヘルプ デスクが調査し、後日フォローアップすることを伝えます。
C. 顧客を保留にして、通話をマネージャーにエスカレーションします。
D. 自由回答形式の質問を使用して、問題をさらに診断します。
Answer: D (メーッセージを残す**)**
Open-ended questions are questions that require more than a yes or no answer and encourage the customer to provide more details and information. Using open-ended questions can help the support technician to understand the problem better, identify the root cause, and find a suitable solution. Some examples of open-ended questions are:
* What exactly is not working on your machine?
* When did you notice the problem?
* How often does the problem occur?
* What were you doing when the problem happened?
* What have you tried to fix the problem?
Offering to wipe and reset the device for the customer is not a good option, as it may result in data loss and inconvenience for the customer. It should be used as a last resort only if other troubleshooting steps fail.
Advising that the help desk will investigate and follow up at a later date is not a good option, as it may leave the customer unsatisfied and frustrated. It should be used only if the problem requires further research or escalation and cannot be resolved on the first call. Putting the customer on hold and escalating the call to a manager is not a good option, as it may waste time and resources. It should be used only if the problem is beyond the support technician's scope or authority and requires managerial intervention.

最新問題: **232**
ユーザーはデスクトップ PC でドメインにログインできませんが、ラップトップ PC は同じネットワーク上で正常に動作しています。技術者はデスクトップ PC にローカル アカウントでログインしますが、安全なイントラネット サイトを参照してトラブルシューティング ツールを入手することはできません。問題の原因として最も可能性が高いのは次のうちどれですか?
A. 時間のずれ
B. デュアル インライン メモリ モジュールの障害
C. アプリケーションのクラッシュ
D. ファイル システム エラー
Answer: A (メッセージを残す**)**
The most likely cause of the issue is a "time drift". Time drift occurs when the clock on a computer is not synchronized with the clock on the domain controller. This can cause authentication problems when a user tries to log in to the domain. The fact that the technician is unable to browse to the secure intranet site to get troubleshooting tools suggests that there may be a problem with the network connection or the firewall settings on the desktop PC12

最新問題: **233**
技術者がいくつかの Windows 10 ワークステーションを企業ドメインに追加しています。スクリプトは大部分のワークステーションを追加できましたが、いくつかのワークステーションでは失敗しました。タスクを手動で完了するには、技術者が次のメニューのうちどれを確認する必要がありますか?
A. ユーザー アカウント
B. システムプロパティ
C. Windows ファイアウォール
D. ネットワークと共有
Answer: B (メッセージを残す**)**
To manually add a workstation to a domain, the technician needs to access the System Properties menu where domain settings are configured.
* User Accounts: Manages user accounts but does not handle domain membership.
* System Properties: The correct place to add or change domain membership settings.
* Windows Firewall: Manages firewall settings but not domain membership.
* Network and Sharing: Manages network connections and sharing but not domain settings.
Reference: CompTIA A+ Exam Objectives [220-1102] - 1.6: Given a scenario, configure Microsoft Windows networking features on a client/desktop.

最新問題: **234**
ユーザーが、モバイル デバイスの画面ロック機能をパターン ロック解除で有効にしました。ユーザーは、デバイスのロックを解除するためにランダムなパターンを繰り返し試行することで、誰かがモバイル デバイスにアクセスする可能性があることを懸念しています。次の機能のうち、ユーザーの懸念に最もよく対処するのはどれですか?
A. リモートワイプ
B. マルウェア対策
C. デバイスの暗号化
D. ログイン制限失敗
Answer: (解答を表示する**)**
The feature that BEST addresses the user's concern is remote wipe. This is because remote wipe allows the user to erase all data on the mobile device if it is lost or stolen, which will prevent unauthorized access to the device1.

最新問題: **235**
ある大規模な組織は、マルチユーザー環境向けにベンダーのサポートを受けて独自のソフトウェアを研究しています。次の EULA タイプのうちどれを選択する必要がありますか?

A. 法人
B. 永久
C. オープンソース
D. 個人的なもの
Answer: A (メーッセージを残す)
A corporate EULA is a type of end-user license agreement that is designed for a large organization that needs to use proprietary software with vendor support for a multiuser environment. A corporate EULA typically grants the organization a volume license that allows it to install and use the software on multiple devices or servers, and to distribute the software to its employees or affiliates. A corporate EULA also usually provides the organization with technical support, maintenance, updates, and warranty from the software vendor, as well as some customization options and discounts. A corporate EULA may also include terms and conditions that specify the rights and obligations of both parties, such as confidentiality, liability, indemnification, termination, and dispute resolution12.
A corporate EULA is a better option than the other choices because:
A perpetual EULA (B) is a type of end-user license agreement that grants the user a permanent and irrevocable license to use the software, without any time limit or expiration date. However, a perpetual EULA does not necessarily include vendor support, updates, or warranty, and it may not allow the user to install the software on multiple devices or servers, or to distribute the software to other users. A perpetual EULA may also be more expensive than a corporate EULA, as it requires a one-time payment upfront, rather than a recurring subscription fee34.
An open-source EULA is a type of end-user license agreement that grants the user a license to use, modify, and redistribute the software, which is publicly available and free of charge. However, an open-source EULA does not provide any vendor support, maintenance, updates, or warranty, and it may impose some restrictions or obligations on the user, such as disclosing the source code, attributing the original author, or using a compatible license for derivative works. An open-source EULA may not be suitable for a large organization that needs proprietary software with vendor support for a multiuser environment56.
A personal EULA (D) is a type of end-user license agreement that grants the user a license to use the software for personal, non-commercial purposes only. A personal EULA may limit the number of devices or servers that the user can install the software on, and prohibit the user from distributing, copying, or reselling the software to other users. A personal EULA may also provide limited or no vendor support, maintenance, updates, or warranty, and it may have a fixed or renewable term. A personal EULA may not meet the needs of a large organization that needs proprietary software with vendor support for a multiuser environment7 .
References:
1: What is a Corporate License Agreement? - Definition from Techopedia1 2: Corporate License Agreement - Template - Word & PDF2 3: What is a Perpetual License? - Definition from Techopedia3 4: Perpetual vs. Subscription Software Licensing: Which Is Best for You?4 5: What is an Open Source License? - Definition from Techopedia5 6: Open Source Licenses: Which One Should You Use?6 7: What is a Personal License Agreement? - Definition from Techopedia7 : Personal License Agreement - Template - Word & PDF

最新問題**: 236**
ユーザーのスマートフォンの画面が回転しません。技術者は回転ロックが無効になっていることを確認します。技術者は次にどの手順を実行する必要がありますか?
A. スクリーンプロテクターを取り外します。
B. スマートフォンのソフトウェアを更新します。
C. スマートフォンを再起動します。
D. スマートフォンを交換してください。
Answer: C (メーッセージを残す)
Restarting a smartphone is a basic troubleshooting step that often resolves temporary software glitches or minor errors that might be preventing the screen rotation from working correctly. It's a quick and easy step to try before moving on to more complex solutions.
Here's why the other options are not the best first step:
* A. Remove the screen protector: While a thick or improperly installed screen protector could potentially interfere with the sensors responsible for screen rotation, it's less likely to be the cause.
* B. Update the smartphone's software: While software updates can fix bugs and improve functionality, they are not always necessary for resolving a screen rotation issue.
* D. Replace the smartphone: Replacing the smartphone is a drastic measure and should only be considered if other troubleshooting steps fail.
Troubleshooting Steps:

* Restart the smartphone: This often clears temporary software issues.
* Check for software updates: If a restart doesn't work, updating the operating system or any relevant apps might resolve the issue.
* Calibrate the accelerometer: Some smartphones have a calibration tool for the accelerometer, the sensor that detects orientation. Check the device settings for this option.
* Check for hardware issues: If the problem persists, there might be a hardware issue with the accelerometer or other components. In this case, contacting the manufacturer or a repair center might be necessary.

最新問題: **237**
技術者がユーザーのデバイスからウイルスを除去しました。ユーザーは 1 週間後に同じウイルスが付着したデバイスを返品しました。将来の感染を防ぐために技術者が行うべきことは次のうちどれですか?
A. システムの復元を無効にします。
B. エンドユーザーを教育します。
C. 最新のOSパッチをインストールします。
D. 環境をクリーンアップして再インストールします。
Answer: B (メーッセージを残す**)**
Educating the end user is the best way to prevent future infections by viruses or other malware. The technician should teach the user how to avoid risky behaviors, such as opening suspicious attachments, clicking on unknown links, downloading untrusted software, etc. Disabling System Restore, installing the latest OS patches and performing a clean installation are possible ways to remove existing infections, but they do not prevent future ones. Verified References: https://www.comptia.org/blog/how-to-prevent-malware
https://www.comptia.org/certifications/a

最新問題: **238**
インストール前にマウントが必要な macOS ファイル タイプは次のうちどれですか?
A. .pkg
B. .zip
C. .app
D. .dmg
Answer: D (メーッセージを残す**)**
The .dmg file type in macOS requires mounting before installation. .dmg files are disk image files used to distribute software on macOS. When opened, they mount a virtual disk on the desktop, from which the application can be installed. Other file types like .pkg, .zip, and .app have different processes for installation and do not require mounting in the same way.

最新問題: **239**
ユーザーがヘルプ デスクに電話し、ワークステーションが悪意のあるソフトウェアに感染していると報告します。ヘルプ デスクの技術者が悪意のあるソフトウェアを削除するために使用する必要があるツールは次のうちどれですか? (2 つ選択)。
A. ファイル エクスプローラー
B. ユーザー アカウント制御
C. Windows のバックアップと復元
D. Windows ファイアウォール
E. Windows ディフェンダー
F. ネットワーク パケット アナライザー
Answer: A,E (メーッセージを残す**)**
The correct answers are E. Windows Defender and A. File Explorer. Windows Defender is a built-in antivirus program that can detect and remove malicious software from a workstation. File Explorer can be used to locate and delete files associated with the malicious software1

最新問題: **240**
大規模な政府契約をサポートする IT サービス会社は、規制要件に準拠するために、数百台のデスクトップ マシンのイーサネット カードを交換しました。非準拠カードの次の廃棄方法のうち、最も環境に優しいのはどれですか?
A. 焼却
B. 転売
C. 物理破壊
D. プラスチックをリサイクルするためのゴミ箱
Answer: (解答を表示する**)**
When disposing of non-compliant Ethernet cards, the most environmentally friendly option is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the production of new materials.
Additionally, recycling plastics helps to reduce the amount of toxic chemicals that can be released into the environment.
According to CompTIA A+ Core 2 documents, "The most environmentally friendly disposal method for non-compliant Ethernet cards is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the production of new materials."
https://sustainability.yale.edu/blog/how-sustainably-dispose-your-technological-waste

最新問題: **241**
裁判所は、政府機関の証拠の取り扱いにより、サイバー犯罪事件はもはや訴追できないとの判断を下した。調査中に違反した可能性が最も高いのは次のうちどれですか?
A. オープンソースソフトウェア
B. EULA
C. 保管過程の管理
D. AUP
Answer: (解答を表示する**)**
Chain of custody is a process that documents how evidence is collected, handled, stored and transferred during a cybercrime investigation. It ensures that the evidence is authentic, reliable and admissible in court. If the chain of custody is violated during an investigation, it can compromise the integrity of the evidence and lead to the case being dismissed. Open-source software, EULA (end-user license agreement) and AUP (acceptable use policy) are not related to cybercrime investigations or evidence handling. Verified References:
https://www.comptia.org/blog/what-is-chain-of-custody https://www.comptia.org/certifications/a

最新問題: **242**
技術者は、顧客が共有ドライブに接続するのを手伝っています。技術者は、すでにマップされている未使用のドライブがいくつかあることに気づき、まずそれらのドライブを切断したいと考えています。技術者は、次のコマンドのどれを使用すればよいでしょうか。
A. フォーマット
B. ネットスタット
C. ディスクパート

D. ネット使用
E. ディレクトリ削除
Answer: D (メーッセージを残す)
The net use (Option D) command is used to manage network drives in Windows. It can be used to display and disconnect mapped network drives, making it the correct choice for removing unused network drives.
* format (Option A) is used to format disks, not for managing network drives.
* netstat (Option B) displays network connections but doesn't manage network drives.
* diskpart (Option C) is used for disk partitioning, not network drive management.
* rmdir (Option E) is used to remove directories, not network drives.
CompTIA A+ Core 2 References:
* 1.2 - Use the appropriate Microsoft command-line tool, including net use for managing network drives .

最新問題**: 243**
ユーザーは部門共有内のファイルにアクセスします。ユーザーが新しいサブフォルダーを作成すると、そのユーザーだけがフォルダーとそのファイルにアクセスできます。すべてのユーザーが新しいフォルダーにアクセスできる可能性が最も高いのは次のうちどれですか?
A. 共有権限の割り当て
B. 継承を有効にする
C. 多要素認証を必要とする
D. アーカイブ属性の削除
Answer: B (メーッセージを残す)
Enabling inheritance is a method that allows new subfolders to inherit the permissions and settings from their parent folder. If users can access files in the department share, but not in the new subfolders created by other users, it may indicate that inheritance is disabled and that each new subfolder has its own permissions and settings that restrict access to only the creator. Enabling inheritance can help resolve this issue by allowing all users to access the new subfolders with the same permissions and settings as the department share. Assigning share permissions, requiring multifactor authentication, and removing archive attribute are not methods that can most likely allow all users to access the new folders.

最新問題**: 244**
ユーザーはスマートフォンの Bluetooth で次の問題を経験しています。
※スマートフォンとペアリングしたスピーカーからは音が出ません。
*ユーザーは、同じく Bluetooth 経由で接続されているスマート ウォッチからのデータの同期に問題を抱えています。
技術者は Bluetooth 設定をチェックし、スピーカーと正常にペアリングされていることを確認し、音量レベルを調整しましたが、それでも何も聞こえませんでした。Bluetooth の問題のトラブルシューティングを行うために、技術者が次に実行すべき手順はどれですか?
A. スマートフォンを再起動します。
B. ネットワーク設定をリセットします。
C. Bluetooth スピーカーのペアリングを解除します。
D. システムのアップデートを確認します。
Answer: A (メーッセージを残す)
Restarting the smartphone can resolve a wide range of technical issues, including those related to Bluetooth connectivity. This simple step can refresh the system and eliminate temporary software glitches that might be interfering with Bluetooth functions like audio output and data synchronization.
Restart the smartphone:This action clears the system's RAM and can resolve conflicts between the Bluetooth service and other processes running on the smartphone, potentially fixing both the audio and synchronization issues.

Resetting network settings (B) could also potentially fix the issue but is a more drastic step that also clears Wi-Fi networks and passwords, cellular settings, and VPN configurations, which might not be necessary.
Unpairing the Bluetooth speaker (C) could help if the issue is specific to the speaker, but since there are also synchronization issues with the smartwatch, the problem seems broader. Checking for system updates (D) is a good general maintenance step, but it's more likely to help with ongoing or known issues rather than immediate connectivity problems.

最新問題**: 245**
サーバールームの環境を維持する際に考慮すべき事項は次のどれですか?
A. 回路ブレーカー容量
B. 配電ユニットの配置
C. RAID構成
D. 仮想化
Answer: (解答を表示する**)**
Comprehensive and Detailed In-Depth Explanation:A server room's environment must account for power capacity and circuit breakers to prevent electrical failures.
* B. Power distribution unit placement - Important, but circuit breaker capacity is more critical.
* C. RAID configurations - Related to data redundancy, not the physical environment.
* D. Virtualization - Does not affect server room conditions.
Reference:
CompTIA A+ 220-1102, Objective 4.2 - Best Practices for Server Room Maintenance

最新問題**: 246**
ユーザーは、適切な端末エミュレーション プログラムを使用して、企業のデスクトップ コンピュータからリモート サーバーにアクセスできません。ユーザーはヘルプ デスクに連絡して問題を報告します。ヘルプ デスクの技術者が問題を理解するためにユーザーに尋ねる質問として、次のどれが最も効果的でしょうか。
A. エラーメッセージは何ですか?
B. プログラムは別のコンピュータでも動作しますか?
C. プログラムは動作しましたか?
D. 他にもこの問題を抱えている人はいますか?
Answer: A (メーッセージを残す**)**
The most effective clarifying question for the help desk technician to ask the user in order to understand the issue is A. What is the error message? This question will help the technician to identify the possible cause and solution of the problem, as the error message will provide specific information about the nature and location of the error, such as the server name, the port number, the protocol, the authentication method, or the network status. The error message will also help the technician to troubleshoot the issue by following the suggested steps or searching for the error code online.
This question is more effective than the other choices because:
B). Does the program work on another computer? is not a very helpful question, as it will not reveal the source of the error or how to fix it. The program may work on another computer for various reasons, such as different network settings, firewall rules, permissions, or software versions. However, this question will not tell the technician what is wrong with the user's computer or the remote server, or what needs to be changed or updated to make the program work.
C). Did the program ever work? is not a very relevant question, as it will not address the current issue or how to resolve it. The program may have worked in the past, but it may have stopped working due to changes in the network configuration, the server status, the software updates, or the user credentials. However, this question will not tell the technician what has changed or how to restore the program functionality.
D). Is anyone else having this issue? is not a very useful question, as it will not explain the reason or the solution for the error. The issue may affect only the user, or multiple users, depending on the scope and the impact of the error. However, this question will not tell the technician what is causing the error or how to fix it for the user or the others.
References:

How to Troubleshoot Terminal Emulation Problems - Techwalla : How to Read and Understand Windows Error Messages - Lifewire : How to Troubleshoot Network Connectivity Problems - How-To Geek : How to Troubleshoot Software Problems - dummies : How to Troubleshoot Common PC Issues For Users - MakeUseOf

最新問題: **247**
従業員がラップトップ PC の問題についてヘルプ デスクに電話します。Windows の更新後、ユーザーはローカルに接続された特定のデバイスを使用できなくなり、再起動しても問題は解決されませんでした。問題を解決するために技術者が実行する必要があるのは、次のうちどれですか?
A. Windows Update サービスを無効にします。
B. アップデートを確認します。
C. 非表示の更新を復元します。
D. 更新をロールバックします。
Answer: D (メーッセージを残す)
The technician should perform a rollback of the Windows update that caused the issue with the locally attached devices. A rollback is a process of uninstalling an update and restoring the previous version of the system. This can help to fix any compatibility or performance issues caused by the update1. To rollback an update, the technician can use the Settings app, the Control Panel, or the System Restore feature. The technician should also check for any device driver updates that might be needed after rolling back the update.
Disabling the Windows Update service is not a good practice, as it can prevent the system from receiving important security and feature updates. Checking for updates might not fix the issue, as the update that caused the issue might still be installed. Restoring hidden updates is not relevant, as it only applies to updates that have been hidden by the user to prevent them from being installed2.
References: 1: https://www.windowscentral.com/how-uninstall-and-reinstall-updates-windows-10 2: https://support.microsoft.com/en-us/windows/show-or-hide-updates-in-windows-10-9c9f0a4f-9a6e-4c8e-8b44-afbc6b33f3cf

最新問題: **248**
リモートの従業員は、会社のローカル サーバーにホストされている情報にアクセスする必要があります。IT 部門は、従業員がオンプレミスにいるかのように会社のリソースに安全にアクセスできるソリューションを見つける必要があります。IT チームが実装すべきリモート接続サービスは次のうちどれですか?
A. SSH
B. VNC
C. VPN
D. RDP
Answer: C (メーッセージを残す)
A VPN (Virtual Private Network) is a service that allows remote employees to access the company's network resources securely over the internet as if they were on premises. A VPN encrypts the data traffic between the employee's device and the VPN server, and assigns the employee a virtual IP address that belongs to the company's network. This way, the employee can access the local servers, files, printers, and other resources without exposing them to the public internet. A VPN also protects the employee's privacy and identity by masking their real IP address and location.

最新問題: **249**
技術者は、Windows ホーム PC のローカル管理者として個人を追加する必要があります。次のユーティリティのうち、技術者が使用する可能性が最も高いのはどれですか?
A. 設定 > 個人設定
B. コントロール パネル > 資格情報マネージャー
C. 設定 > アカウント > 家族とその他のユーザー
D. コントロール パネル > ネットワークと共有センター
Answer: C (メーッセージを残す)

The technician would most likely use Settings > Accounts > Family and Other Users to add an individual as a local administrator on a Windows home PC. Settings > Accounts > Family and Other Users allows users to add and manage other user accounts on their Windows PC. The technician can add an individual as a local administrator by selecting Add someone else to this PC under Other users and following the steps to create a new user account with administrator privileges. Settings > Personalization allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver.
Settings > Personalization is not related to adding an individual as a local administrator on a Windows home PC but to configuring desktop settings and preferences. Control Panel > Credential Manager allows users to view and manage their web credentials and Windows credentials stored on their Windows PC. Control Panel
> Credential Manager is not related to adding

最新問題: **250**
ユーザーのワークステーションは、AV システムが検出した新たに発見されたウイルスに感染しました。完全なウイルス スキャンとワークステーションの再起動後も、ウイルスは OS 内にまだ存在します。ウイルスを削除するには、ユーザーが実行する必要があるアクションは次のうちどれですか?
A. システム ファイアウォールを有効にします。
B. ブータブルウイルス対策メディアを使用してシステムをスキャンします。
C. ウイルスを特にターゲットにするように設計されたソフトウェアをダウンロードします。
D. オペレーティング システムの更新プロセスを実行します。
Answer: B (メーッセージを残す)
Using bootable antivirus media to scan the system is an effective method for removing a persistent virus.
Booting from external antivirus media allows the system to scan for and remove malware without the infected operating system running, which can prevent the virus from hiding or resisting removal efforts that might occur within the active OS environment.

最新問題: **251**
技術者がファイルから Windows OS のインプレース アップグレードを実行しようとしています。技術者がファイルをダブルクリックすると、ドライブをマウントするように求めるプロンプトが表示されます。技術者がダウンロードしたファイルの種類は次のうちどれですか。
A. .msi
B. .iso
C. .zip
D. .exe
Answer: B (メーッセージを残す)
The file type ISO is a disk image format that contains everything from a CD, DVD, or Blu-ray disc in a single file. When an ISO file is accessed, the system prompts the user to mount it as a virtual drive, which is why the technician received a "mount a drive" prompt. MSI (A) is for installing software, ZIP (C) is a compressed file, and EXE (D) is an executable file.
Reference: Core 2, Domain 1.9 - Installation methods and upgrade paths.

最新問題: **252**
技術者が新しい SOHO ワイヤレス ルーターをインストールし、それが安全で最新のネットワーク機能を使用していることを確認したいと考えています。技術者が最初に行うべきことは何ですか。
A. 未使用のポートを無効にします。
B. DHCP 予約を有効にします。
C. ファームウェアを更新します。
D. ゲスト アカウントを無効にします。
Answer: C (メーッセージを残す)

The first step in securing a newly installed SOHO (Small Office/Home Office) wireless router is to ensure it has the latest firmware installed. Firmware updates often include important security patches and new features that protect the router from known vulnerabilities. Other actions, like disabling unused ports or guest accounts, can be useful for hardening the security, but they should come after the router is running the most recent and secure version of its firmware.
References:
CompTIA A+ Core 2 Objectives, Domain 2.1: Best Practices for Securing a SOHO Network (ProfMesser) (Whizlabs)

最新問題**: 253**
ユーザーがパスワードの長さの要件に従っていることを確認するために技術者が使用できる機能は次のうちどれですか?
A. グループ ポリシー
B. ログオン スクリプト
C. アクセス制御リスト
D. セキュリティグループ
Answer: A (メーッセージを残す**)**
Group Policy is a feature in Windows that allows network administrators to manage and configure operating system, application settings, and user settings in an Active Directoryenvironment. It can enforce password policies across the network, including password length requirements, making it the best tool for ensuring compliance with security policies.

最新問題**: 254**
ネットワーク技術者は、ホーム オフィス ユーザーのために SOHO ルーターを設置しました。ユーザーは、ホーム ルーターが悪意のある攻撃者の標的となり、DDoS 攻撃に使用されるというレポートを読みました。この脅威に対して防御するために技術者が実行できる可能性が最も高いのは次のうちどれですか?
A. ネットワーク コンテンツ フィルタリングを追加します。
B. SSID ブロードキャストを無効にします。
C. ポート転送を構成します。
D. デフォルトの資格情報を変更します。
Answer: D (メーッセージを残す**)**
One of the most effective ways to defend against malicious actors targeting home routers for DDoS attacks is to change the default credentials of the router. The default credentials are often well-known or easily guessed by attackers, who can then access and compromise the router settings and firmware. By changing the default credentials to strong and unique ones, a technician can prevent unauthorized access and configuration changes to the router. Adding network content filtering may help block some malicious or unwanted websites but may not prevent attackers from exploiting router vulnerabilities or backdoors. Disabling the SSID broadcast may help reduce the visibility of the wireless network but may not prevent attackers from scanning or detecting it.
Configuring port forwarding may help direct incoming traffic to specific devices or services but may not prevent attackers from sending malicious packets or requests to the router. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

最新問題**: 255**
中小企業の経営者は、新しく購入したソフトウェアをネットワークに接続されたすべての PC にインストールしたいと考えています。ネットワークはドメインとして構成されておらず、所有者は可能な限り簡単な方法を使用したいと考えています。次のうち、所有者がアプリケーションをインストールする最も不十分な方法はどれですか?
A. ネットワーク共有を使用して、インストール ファイルを共有します。
B. ソフトウェアを外付けハード ドライブに保存してインストールします。
C. PC ごとにイメージング USB を作成します。
D. ベンダーの Web サイトからソフトウェアをインストールします。
Answer: B (メーッセージを残す**)**

Saving software to an external hard drive and installing it on each individual PC is the most inefficient method for the small business owner. This method requires manual intervention on each PC, and there is a higher risk of error or inconsistencies between PCs. Additionally, if the software needs to be updated or reinstalled in the future, this process would need to be repeated on each PC.

最新問題: **256**
ある会社は、新しいバックアップおよびリカバリ システムをインストールしました。次のタイプのバックアップのうち、最初に完了する必要があるのはどれですか?
A. フル
B. ノンパリティ
C. 差動
D. インクリメンタル
Answer: (解答を表示する**)**
The type of backup that should be completed FIRST after installing a new backup and recovery system is a full backup. This is because a full backup is a complete backup of all data and is the foundation for all other backups. After a full backup is completed, other types of backups, such as differential and incremental backups, can be performed.

最新問題: **257**
顧客から、スマートフォンでのデータ使用量が多く、各請求サイクルの最初の週に月間データ制限に達するという報告がありました。顧客は主に通話と SMS メッセージに電話を使用し、コンテンツのストリーミングは最小限に抑えています。技術者が電話のトラブルシューティングを行ったところ、開発者モードと不明なソースからのインストールの両方が有効になっていることがわかりました。技術者が次に確認すべきは次のうちどれですか。
A. ストレージキャッシュ
B. 悪意のあるアプリケーション
C. プライバシー設定
D. 権限
Answer: B (メーッセージを残す**)**
Since both developer mode and the ability to install apps from unknown sources are enabled, the technician should check for Malicious applications (Option B). Unknown sources can allow unverified apps that may include malware or apps that use excessive background data without the user's knowledge. Checking for malicious apps is essential in this scenario.
* Storage cache (Option A) would not typically cause high data usage.
* Privacy settings (Option C) control data sharing and permissions but don't directly impact data usage.
* Permissions (Option D) might help identify apps using data, but the focus should be on apps that could be malicious.
CompTIA A+ Core 2 References:
* 2.7 - Explain common methods for securing mobile devices, including detecting and preventing malware.

最新問題: **258**
システム管理者は、PKI を使用してラップトップから企業ネットワークに接続するときに問題が発生しています。システム管理者が問題を解決するために使用できるツールは次のうちどれですか?
A. certmgr.msc
B. msconfig.exe

C. lusrmgr.msc
D. perfmon.msc
Answer: (解答を表示する**)**
certmgr.msc is a tool that can be used to troubleshoot issues with PKI (public key infrastructure) on a Windows machine. It allows a system administrator to view, manage and import certificates, as well as check their validity, expiration and revocation status. msconfig.exe, lusrmgr.msc and perfmon.msc are other tools that can be used for different purposes on a Windows machine, but they are not related to PKI. Verified References: https://www.comptia.org/blog/what-is-certmgr-msc https://www.comptia.org/certifications/a

最新問題**: 259**
ホーム オフィス ユーザーは、PC を確実にバックアップし、地域の自然災害やハードウェア障害から保護したいと考えています。ユーザーの要件を満たすのは次のうちどれですか?
A. エージェントベースのクラウド バックアップ ソリューションの使用
B. 祖父、父、子のバックアップ ローテーションの実装
C. ローカル ネットワーク共有へのバックアップの自動化
D. ファイルを外部ドライブに手動で保存します
Answer: A (メーッセージを残す**)**
For ensuring data protection against local natural disasters and hardware failures, the best approach is to use an off-site solution that provides redundancy and is resilient to local disruptions.
* Using an agent-based cloud backup solution: This method involves backing up data to a remote cloud server, providing protection against local disasters like floods, fires, or hardware failures since the data is stored off-site and can be accessed from anywhere.
* Implementing a grandfather-father-son backup rotation: While effective for managing local backups, this method typically involves physical media which could still be vulnerable to local disasters.
* Automating backups to a local network share: This keeps the backups within the same physical location, making them susceptible to local disasters.
* Saving files manually to an external drive: This method is prone to human error and doesn't provide automated or off-site protection.
Reference: CompTIA A+ Exam Objectives [220-1102] - 4.3: Given a scenario, implement workstation backup and recovery methods.

最新問題**: 260**
コマンド cac cor.pti
を。txt は Linux 端末で発行されました。予想される結果は次のうちどれですか?
A. テキスト comptia.txt の内容は、新しい空白のドキュメントに置き換えられます。
B. テキスト コンプティアの内容。txt が表示されます。
C. テキスト comptia.txt の内容は、アルファベット順に分類されます。
D. テキスト コンプティアの内容。txt は別のコンプティアにコピーされます。txtファイル
Answer: (解答を表示する**)**
The command cac cor.ptia. txt was issued on a Linux terminal. This command would display the contents of the text comptia.txt.

最新問題**: 261**
ある会社が最近、夜勤の清掃サービスを外注しました。技術者は、建物内に監督されていない請負業者がいることを懸念しています。コンピューターへのアクセスを防ぐために使用できるセキュリティ対策は次のどれですか (2 つ選択してください)。
A. 保存データの暗号化の実装
B. 自動実行を無効にする
C. ユーザー権限の制限
D. ログイン時間の制限
E. 画面ロックを有効にする

F. ローカル管理者アカウントを無効にする
Answer: B,E (メーッセージを残す)
The correct answers are D. Restricting log-in times and E. Enabling a screen lock. These are the security measures that can be used to prevent the computers from being accessed by unsupervised contractors in the building.
* Restricting log-in times means setting a policy that allows users to log in only during certain hours, such as the regular working hours of the company. This will prevent unauthorized access by contractors who work at night1.
* Enabling a screen lock means setting a policy that requires users to enter a password or a PIN to unlock their screens after a period of inactivity. This will prevent unauthorized access by contractors who might try to use the computers when the users are away2.
1: CompTIA A+ Certification Exam: Core 2 Objectives, page 19, section 2.3. 2: CompTIA A+ Certification Exam: Core 2 Objectives, page 20, section 2.4.

最新問題**: 262**
技術者は、社内 LAN 上のさまざまな Windows、Linux、macOS デスクトップへのグラフィカル リモート アクセスを必要としています。セキュリティ管理者は、外部インターネット接続を必要としない単一のソフトウェア ソリューションを利用するように技術者に依頼します。次のリモート アクセス ツールのうち、技術者がインストールする可能性が最も高いのはどれですか?
A. VNC
B. RMM
C. RDP
D. SSH
Answer: A (メーッセージを残す)
VNC (Virtual Network Computing) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a graphical user interface. VNC does not require an external internet connection, as it works over a local network or a VPN. VNC uses a client-server model, where the server runs on the remote desktop and the client connects to it from another device. VNC can transmit the keyboard and mouse events from the client to the server, and the screen updates from the server to the client, enabling the technician to interact with the remote desktop as if it were local12.
VNC is a better option than the other choices because:
* RMM (Remote Monitoring and Management) (B) is not a single software solution, but a category of software solutions that enable IT professionals to remotely monitor, manage, and troubleshoot multiple devices and networks. RMM software may include remote access tools, but also other features such as patch management, backup and recovery, security, reporting, and automation. RMM software may require an external internet connection, as it often relies on cloud-based services or web-based consoles34.
* RDP (Remote Desktop Protocol) is a remote access tool that allows the technician to access and control Windows desktops on the company LAN using a graphical user interface. However, RDP is not compatible with Linux or macOS desktops, unless they have third-party software installed that can emulate or translate the RDP protocol. RDP also has some security and performance issues, such as encryption vulnerabilities, bandwidth consumption, and latency problems56.
* SSH (Secure Shell) (D) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a command-line interface. SSH does not require an external internet connection, as it works over a local network or a VPN. SSH uses encryption and authentication to secure the communication between the client and the server. However, SSH does not provide a graphical user interface, which may limit the functionality and usability of the remote desktop7 .
References:
1: What is VNC? - Definition from Techopedia1 2: How VNC Works - RealVNC2 3: What is Remote Monitoring and Management (RMM)? - Definition from Techopedia3 4: What is RMM Software? - NinjaRMM4 5: What is Remote Desktop Protocol (RDP)? - Definition from Techopedia5 6: Remote Desktop Protocol: What it is and how to secure it - CSO Online6 7: What is Secure Shell (SSH)? - Definition from Techopedia7 : How to Use SSH to Access a Remote Server in Linux or Windows - Hostinger Tutorials

最新問題**: 263**

スマートフォンが Wi-Fi に接続されていない場合、ユーザーはスマートフォンでインターネット関連の機能を使用できません スマートフォンが Wi-Fi に接続されている場合、ユーザーはインターネットを閲覧したり、電子メールを送受信したりできます。ユーザーは、スマートフォンが Wi-Fi に接続されていない場合でも、テキスト メッセージや電話の送受信を行うことができます。Wi-Fi に接続していないスマートフォンでインターネットを使用できない理由として最も可能性が高いのは次のうちどれですか?

A. スマートフォンの回線にデータ プランが設定されていない
B. スマートフォンのSIMカードが故障している
C. スマートフォンの Bluetooth 無線が無効になっています。
D. スマートフォンで開いているアプリケーションが多すぎます
Answer: A (メーッセージを残す**)**
The smartphone's line was not provisioned with a data plan. The user is unable to use any internet-related functions on the smartphone when it is not connected to Wi-Fi because the smartphone's line was not provisioned with a data plan. The user can send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi because these functions do not require an internet connection1

最新問題: **264**
ユーザーは、Windows 10 デスクトップ コンピューターのハード ドライブ アクティビティ ライトが 1 時間以上点灯し続け、パフォーマンスが著しく低下していると報告しています。タスク マネージャーの次のタブのうち、技術者がこの問題の原因を特定するために使用する情報が含まれているのはどれですか?

A. サービス
B. プロセス
C. パフォーマンス
D. 起動
Answer: B (メーッセージを残す**)**
Processes tab in Task Manager would contain the information a technician would use to identify the cause of this issue. The Processes tab in Task Manager displays all the processes running on the computer, including the CPU and memory usage of each process. The technician can use this tab to identify the process that is causing the hard drive activity light to remain lit and the performance degradation1

最新問題: **265**
保管過程の維持は、インシデント対応プロセスの重要な部分です。これがなぜ重要であるかを説明する理由は次のどれですか?

A. 情報セキュリティポリシーを維持するため
B. 問題を適切に特定するため
C. 証拠を管理し、完全性を維持するため
D. できるだけ多くの情報を収集する
Answer: C (メーッセージを残す**)**
Maintaining the chain of custody is important to control evidence and maintain integrity. The chain of custody is a process that documents who handled, accessed, or modified a piece of evidence, when, where, how, and why. The chain of custody ensures that the evidence is preserved, protected, and authenticated throughout the incident response process. Maintaining the chain of custody can help prevent tampering, alteration, or loss of evidence, as well as establish its reliability and validity in legal proceedings. Maintaining an information security policy, properly identifying the issue, and gathering as much information as possible are not reasons why maintaining the chain of custody is important. Maintaining an information security policy is a general practice that defines the rules and guidelines for securing an organization's information assets and resources.
Properly identifying the issue is a step in the incident response process that involves analyzing and classifying the incident based on its severity, impact, and scope. Gathering as much information as possible is a step in the incident response process that involves collecting and documenting relevant data and evidence from various sources, such as logs, alerts, or witnesses. References:
* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 26

最新問題: **266**
ネットワーク管理者は、組織内のすべてのデバイスの Wi-Fi アクセスに使用されるクライアント証明書を展開しています 証明書は、ユーザーの既存のユーザー名とパスワードと組み合わせて使用されます この展開後に実現されるセキュリティ上の利点を最もよく表しているのは、次のうちどれですか?
A. Wi-Fi に対して多要素認証が強制されます。
B. すべての Wi-Fi トラフィックは転送中に暗号化されます
C. 盗聴の試みが防止されます
D. 不正なアクセス ポイントは接続されません
Answer: A (メーッセージを残す**)**
Multifactor authentication will be forced for Wi-Fi after deploying a client certificate to be used for Wi-Fi access for all devices in an organization3 References:
* CompTIA Security+ (Plus) Practice Test Questions | CompTIA. Retrieved from https://www.comptia.
org/training/resources/comptia-security-practice-tests

最新問題: **267**
技術者は、ルートキットがインストールされており、削除する必要があるのではないかと疑っています。問題を最もよく解決するのは次のうちどれですか?
A. アプリケーションの更新
B. マルウェア対策ソフトウェア
C. OS の再インストール
D. ファイル復元
Answer: C (メーッセージを残す**)**
If a rootkit has caused a deep infection, then the only way to remove the rootkit is to reinstall the operating system. This is because rootkits are designed to be difficult to detect and remove, and they can hide in the operating system's kernel, making it difficult to remove them without reinstalling the operating system
https://www.minitool.com/backup-tips/how-to-get-rid-of-rootkit-windows-10.html

最新問題: **268**
次のワイヤレス セキュリティ機能のうち、ユーザーがログイン資格情報を使用して利用可能な企業 SSID を接続できるようにするために有効にできるのはどれですか?
A. TACACS+
B. ケルベロス
C. 事前共有キー
D. WPA2/AES
Answer: (解答を表示する**)**
WPA2/AES (Wi-Fi Protected Access 2/Advanced Encryption Standard) is a wireless security standard that supports enterprise mode, which allows a user to use login credentials (username and password) to authenticate to available corporate SSIDs (service set identifiers). TACACS+ (Terminal Access Controller Access-Control System Plus) and Kerberos are network authentication protocols, but they are not wireless security features. Preshared key is another wireless security feature, but it does not use login credentials.
Verified References: https://www.comptia.org/blog/wireless-security-standards https://www.comptia.org
/certifications/a

最新問題: **269**
週末にネットワークが侵害されました システム ログは、辞書攻撃を 500 回試みた後、1 人のユーザーのアカウントが侵害されたことを示しています。この脅威を最も緩和するのは次のうちどれですか?
A. 保存時の暗号化
B. アカウントのロックアウト

C. 自動画面ロック
D. ウイルス対策
Answer: B (メーッセージを残す**)**
Account lockout would best mitigate the threat of a dictionary attack1

最新問題**: 270**
技術者が新しく組み立てたコンピューターをセットアップしています。技術者が Windows 10 をインストールする最も早い方法は次のうちどれですか?
A. 工場出荷時設定にリセット
B. システムの復元
C. インプレースアップグレード
D. 無人インストール
Answer: D (メーッセージを残す**)**
The correct answer is D. Unattended installation. An unattended installation is a way of installing Windows 10 without requiring any user input or interaction. It uses a configuration file called answer file that contains the settings and preferences for the installation, such as the product key, language, partition, and network settings. An unattended installation can be performed by using a bootable USB flash drive or DVD that contains the Windows 10 installation files and the answer file1. This is the fastest way for the technician to install Windows 10 on a newly built computer, as it automates the whole process and saves time.
A factory reset is a way of restoring a computer to its original state by deleting all the data and applications and reinstalling the operating system. A factory reset can be performed by using the recovery partition or media that came with the computer, or by using the Reset this PC option in Windows 10 settings2. A factory reset is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.
A system restore is a way of undoing changes to a computer's system files and settings by using a restore point that was created earlier. A system restore can be performed by using the System Restore option in Windows 10 settings or by using the Advanced Startup Options menu3. A system restore is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system and restore points to be present.
An in-place upgrade is a way of upgrading an existing operating system to a newer version without losing any data or applications. An in-place upgrade can be performed by using the Windows 10 Media Creation Tool or by running the Setup.exe file from the Windows 10 installation media. An in-place upgrade is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.

最新問題**: 271**
技術者は外部 SSD を持っています。技術者は、Mac と Windows PC の両方で外部 SSD の読み取りと書き込みを行う必要があります。次のファイルシステムのうち、両方の OS タイプでサポートされているのはどれですか?
A. NTFS
B. APFS
C. ext4
D. exFAT
Answer: D (メーッセージを残す**)**
The filesystem that is supported by both Macs and Windows PCs is D. exFAT. exFAT is a file system that is designed to be used on flash drives like USB sticks and SD cards. It is supported by both Macs and Windows PCs, and it can handle large files and volumes
https://www.diskpart.com/articles/file-system-for-mac-and-windows-0310.html

最新問題**: 272**
ネットワーク技術者が、DHCP サーバーがない小規模な支社に新しいマシンを導入しています。
新しいマシンは自動的に IP アドレス 169.254.0.2 を受け取り、ネットワークの残りの部分と通信できなくなります。次のどれが通信を回復しますか?
* 静的エントリ
A. ARPテーブル
B. APIPA アドレス
C. NTP仕様
Answer: (解答を表示する**)**
A static entry is the best option to restore communication for the new machine in a small branch office that does not have a DHCP server. A static entry means manually configuring the IP address, subnet mask, default gateway, and DNS server for the network adapter of the machine. A static entry ensures that the machine has a valid and unique IP address that matches the network configuration and can communicate with the rest of the network.
The new machine automatically receives the IP address of 169.254.0.2 because it uses APIPA (Automatic Private IP Addressing), which is a feature that enables computers to self-assign an IP address when a DHCP server is not available. However, APIPA only works for local communication within the same subnet, and does not provide a default gateway or a DNS server. Therefore, the new machine is unable to communicate with the rest of the network, which may be on a different subnet or require a gateway or a DNS server to access.
The other options are not related to restoring communication for the new machine. ARP table is a cache that stores the mapping between IP addresses and MAC addresses for the devices on the network. NTP specification is a protocol that synchronizes the clocks of the devices on the network.
References:
* CompTIA A+ Certification Exam Core 2 Objectives1
* CompTIA A+ Core 2 (220-1102) Certification Study Guide2
* What is APIPA (Automatic Private IP Addressing)? - Study-CCNA3
* How to Configure a Static IP Address in Windows and OS X4

最新問題**: 273**
ある技術者がサーバーに新しいハード ドライブを取り付けようとしていますが、別のタスクに呼び出されました。ドライブは開梱され、机の上に放置されています。技術者が退社する前に実行する必要があるのは、次のうちどれですか?
A. 同僚に、誰もハード ドライブに触れないように依頼してください。
B. ハード ドライブをテーブルに置いたままにします。他のタスクが完了している間は問題ありません。
C. ハード ドライブを帯電防止バッグに入れ、ハード ドライブを含む領域を固定します。
D. 静電放電ストラップをドライブに接続します。
Answer: C (メーッセージを残す**)**
The technician should place the hard drive in an antistatic bag and secure the area containing the hard drive before leaving. This will protect the hard drive from electrostatic discharge (ESD), dust, moisture, and physical damage. Asking coworkers to make sure no one touches the hard drive is not a reliable or secure way to prevent damage. Leaving the hard drive on the table exposes it to ESD and other environmental hazards.
Connecting an electrostatic discharge strap to the drive is not enough to protect it from dust, moisture, and physical damage.

最新問題: **274**
技術者は、macOS を実行しているコンピューターで IP アドレスを手動で設定する必要があります。技術者が使用すべきコマンドは次のうちどれですか?
A. ipconfig
B. ifconfig
C. arpa
D. ping
Answer: B (メーッセージを残す)
ifconfig is a command-line utility that allows you to configure network interfaces on macOS and other Unix-like systems1. To set an IP address using ifconfig, you need to know the name of the network interface you want to configure (such as en0 or en1), and the IP address you want to assign (such as 192.168.0.150). You also need to use sudo to run the command with administrative privileges2. The syntax of the command is:
sudo ifconfig interface address
For example, to set the IP address of en1 to 192.168.0.150, you would type:
sudo ifconfig en1 192.168.0.150
You may also need to specify other parameters such as subnet mask, gateway, or DNS servers, depending on your network configuration3. The other commands are not directly related to setting an IP address on macOS. ipconfig is a similar command for Windows systems4, arpa is a domain name used for reverse DNS lookup, and ping is a command for testing network connectivity.

最新問題: **275**
技術者が Linux ワークステーションにプリンタをセットアップしています。技術者がデフォルトのプリンターを設定するために使用する必要があるコマンドは次のうちどれですか?
A. ipr
B. lspool
C. lpstat
D. lpoptions
Answer: (解答を表示する)
In Linux, thelpcommand is used to manage print jobs, including setting the default printer. Thelpcommand allows users to send print jobs to a printer queue, check the status of print jobs, and cancel print jobs, among other functionalities. By using options and parameters with thelpcommand, a technician can specify a particular printer as the default for future print jobs, ensuring that documents are routed to the correct printer without needing to specify it each time.

最新問題: **276**
あるユーザーが、ワークステーションの動作が遅いと報告している 他の何人かのユーザーが同じワークステーションで作業しており、ワークステーションが正常に動作していると報告しています。システム管理者は、ワークステーションが正常に機能することを確認しました。システム管理者が次に試みる可能性が最も高いのは、次のどの手順ですか?
A. ページング ファイルのサイズを大きくします
B. chkdsk コマンドを実行します。
C. ユーザーのプロファイルを再構築します
D. システム メモリを追加します。
E. ハード ドライブを最適化します。
Answer: C (メーッセージを残す)
Since the systems administrator has validated that the workstation functions normally and other users operate on the same workstation without any issues, the next step should be to rebuild the user's profile. This will ensure that any corrupted files or settings are removed and the user's profile is restored to its default state.

最新問題: **277**

次のどれがグループ ポリシー構成に基づいてネットワーク ドライブを自動的にマップしますか?
A. ログインスクリプト
B. アクセス制御リスト
C. 組織単位
D. フォルダリダイレクト
Answer: (解答を表示する**)**
Network drives can be automatically mapped for users based on Group Policy configuration using log-in scripts. Here's how it works:
* Log-in scripts: These are scripts executed when a user logs in to a domain. They can be configured through Group Policy in Active Directory to map network drives automatically. The scripts can use commands like net use to map drives.
* Access control lists (ACLs): While ACLs control permissions for files and folders, they do not automatically map network drives.
* Organizational units (OUs): OUs are used to organize users and computers in a directory structure but do not map drives.
* Folder redirection: This redirects the path of a folder to a new location, typically on a network share, but it does not automatically map drives.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 1.6: Given a scenario configure Microsoft Windows networking features on a client/desktop.
Group Policy and login script documentation from Microsoft.

最新問題**: 278**
技術者は、信頼性の低い接続を介して多数のファイルを転送する必要があります。接続が中断された場合、技術者はプロセスを再開できるはずです。次のどのツールを使用できますか?
A. afc
B. ええと
C. git クローン
D. ゾボコピー
Answer: (解答を表示する**)**
The technician should use afc to transfer a large number of files over an unreliable connection and be able to resume the process if the connection is interrupted1

最新問題**: 279**
技術者が Web サイトにアクセスすると、無効な証明書エラーが表示されます。同じローカル ネットワーク上の他のワークステーションでは、この問題を再現できません。問題の原因となっている可能性が最も高いのは次のうちどれですか?
A. 日付と時刻
B. ユーザーアクセス制御
C. UEFIブートモード
D. ログオン時間
Answer: (解答を表示する**)**
Date and time is the most likely cause of the issue. The date and time settings on a workstation affect the validity of the certificates used by websites to establish secure connections. If the date and time are incorrect, the workstation may not recognize the certificate as valid and display an invalid certificate error. Other workstations on the same local network may not have this issue if their date and time are correct. User access control, UEFI boot mode, and log-on times are not likely causes of the issue. User access control is a feature that prevents unauthorized changes to the system by prompting for confirmation or credentials. UEFI boot mode is a firmware interface that controls the boot process of the workstation. Log-on times are settings that restrict when a user can log in to the workstation. None of these factors affect the validity of the certificates used by websites. References:
* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 14
* CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 456

最新問題: **280**
ロールバック計画を最もよく説明しているものは次のうちどれですか?
A. 開発者は、完了時に開始状態に戻るようにプロセスを構成します。
B. ユーザーが不要なファイル共有の削除を要求しました。
C. 管理者は、以前の設定が失敗した後、新しい設定をコンピュータに適用します。
D. アップグレードが失敗した後、技術者がシステムを以前の状態に戻します。
Answer: (解答を表示する**)**
A rollback plan describes the process of reverting a system to its previous state after a failed upgrade or change. This ensures system stability and functionality by restoring known good configurations and is a crucial part of change management to minimize disruptions in case of unsuccessful updates.

最新問題: **281**
最近のフライトで、役員が iPhone で機内 Wi-Fi 経由で映画を見ようとしているときに、予期せず犬と猫の写真を何枚か受信しました。幹部は、連絡先がこのような写真を送信したという記録を持っておらず、以前にこれらの写真を見たこともありません. この問題を最善の方法で解決するには、エグゼクティブは次のことを行う必要があります。
A. 転送が既知の連絡先からのみ受け入れられるように AirDrop を設定します。
B. 飛行中はすべての無線システムを完全に無効にします
C. iMessage の使用を中止し、安全な通信アプリケーションのみを使用する
D. 保存された連絡先からのメッセージと通話のみを許可する
Answer: (解答を表示する**)**
To best resolve this issue, the executive should set AirDrop so that transfers are only accepted from known contacts (option A). AirDrop is a feature on iOS devices that allows users to share files, photos, and other data between Apple devices. By setting AirDrop so that it only accepts transfers from known contacts, the executive can ensure that unwanted files and photos are not sent to their device. Additionally, the executive should ensure that the AirDrop setting is only enabled when it is necessary, as this will protect their device from any unwanted files and photos.

最新問題: **282**
次のシステム環境設定項目のうち、macOS 11 でサードパーティ製アプリケーションのインストールを有効にできるのはどれですか?
A. キーチェーン
B. プライバシー
C. アクセシビリティ
D. スポットライト
Answer: (解答を表示する**)**
In macOS, the "Privacy" settings under "Security & Privacy" are where users can control which applications are allowed to run, including third-party apps. By default, macOS may restrict apps that are not downloaded from the App Store, but in the Privacy settings, users can enable installations from identified developers or even from any source. The other options like "Keychain" manage passwords and certificates, "Accessibility" deals with assistive technologies, and "Spotlight" is the search feature.
References:
Apple Support: Safely open apps on your Mac
CompTIA A+ 220-1102 Study Guide (Whizlabs)

最新問題: **283**
次の macOS の機能のうち、開いているすべてのウィンドウの概要をユーザーに提供するのはどれですか?
A. ミッション コントロール

B. ファインダー
C. 複数のデスクトップ
D. スポットライト
Answer: A (メーッセージを残す**)**
Mission Control is the macOS feature that provides the user with a high-level view of all open windows.
Mission Control allows the user to see and switch between multiple desktops, full-screen apps, and windows in a single screen. Mission Control can be accessed by swiping up with three or four fingers on the trackpad, pressing F3 on the keyboard, or moving the cursor to a hot corner

最新問題**: 284**
システム管理者は、企業ネットワーク上のサーバーの CPU 使用率が非常に高いことに気づきました。さらに詳しく調べたところ、管理者は、サーバーが、ハッシュ アルゴリズムを解決するためにデジタル通貨を授与する会社に遡る IP アドレスと一貫して通信していることを確認しました。サーバーを侵害するために使用された可能性が最も高いのは次のうちどれですか?
A. キーロガー
B. ランサムウェア
C. ブートセクターウイルス
D. クリプトマイニング マルウェア
Answer: D (メーッセージを残す**)**
Cryptomining malware is a type of malicious program that uses the CPU resources of a compromised server to generate cryptocurrency, such as Bitcoin or Ethereum. It can cause extremely high CPU utilization and network traffic to the IP address of the cryptocurrency service. Keylogger, ransomware and boot sector virus are other types of malware, but they do not cause the same symptoms as cryptomining malware. Verified References: https://www.comptia.org/blog/what-is-cryptomining https://www.comptia.org/certifications/a

最新問題**: 285**
組織の重要なデータベース ファイルがランサムウェアの攻撃を受けました。会社は復号キーの身代金の支払いを拒否しました。感染の痕跡はすべて基盤サーバーから削除されました。
企業が次に行うべきことはどれでしょうか?
A. 最新のマルウェア対策クリーニング ソフトウェアを使用して、感染したファイルをすべてスキャンします。
B. ファイル共有をホストしているサーバーのオペレーティング システムに完全なパッチを適用します。
C. ファイルを読み取り専用に変更します。
D. バックアップから重要なデータを復元します。
Answer: D (メーッセージを残す**)**
When an organization refuses to pay the ransom for a decryption key after a ransomware attack, and all traces of the infection have been removed, the next critical step is:
* Restore critical data from backup: This is the most effective way to recover from a ransomware attack without paying the ransom. Assuming the organization has good backup practices, the backups should be free from infection and can be restored to get the systems operational again.
* Scan all of the infected files with up-to-date, anti-malware cleaning software: This step is important during the infection removal process but does not address restoring the encrypted files.
* Fully patch the server operating systems hosting the fileshares: While this is necessary to prevent future attacks, it does not recover the encrypted files.
* Change the files to be read-only: This will not help recover the encrypted data.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.8: Given a scenario use common data destruction and disposal methods.
Best practices for ransomware recovery.

最新問題**: 286**

ユーザーから、PC の動作が通常よりも遅いように見えるとの報告がありました。技術者がシステム リソースをチェックしますが、ディスク、CPU、およびメモリの使用率は問題ないようです。技術者は、GPU の温度が非常に高いことを確認します。次のタイプのマルウェアのうち、原因となる可能性が最も高いのはどれですか?

A. スパイウェア
B. クリプトマイナー
C. ランサムウェア
D. ブート セクタ ウイルス

Answer: B (メーッセージを残す)

The type of malware that is most likely to blame for a PC running more slowly than usual and having an extremely high GPU temperature is a "cryptominer". Cryptominers are a type of malware that use the resources of a computer to mine cryptocurrency. This can cause the computer to run more slowly than usual and can cause the GPU temperature to rise. Spyware is a type of malware that is used to spy on a user's activities, but it does not typically cause high GPU temperatures. Ransomware is a type of malware that encrypts a user's files and demands payment to unlock them, but it does not typically cause high GPU temperatures. Boot sector viruses are a type of malware that infects the boot sector of a hard drive, but they do not typically cause high GPU temperatures12

最新問題**: 287**
組織はサポート機能を一元化しており、リモート ユーザーのデスクトップをサポートする機能を必要としています。次のテクノロジのうち、技術者がユーザーと共に問題を確認できるのはどれですか?

A. RDP
B. VNC
C. SSH
D. VPN

Answer: B (メーッセージを残す)

VNC will allow a technician to see the issue along with the user when an organization is centralizing support functions and requires the ability to support a remote user's desktop1

最新問題**: 288**
ユーザーは、PC がマルウェアに感染したというメッセージを受け取ります。技術者がユーザーのマシンをフルスキャンしましたが、マルウェアは検出されませんでした。その日のうちに、同じメッセージが再び表示されました。技術者は、システムを通常の機能に戻すために、次の手順のどれを実行する必要がありますか?

A. Windows の更新プログラムを確認します。
B. コンピューターのイメージを再作成します。
C. Windows ファイアウォールを有効にします。
D. システム ファイル チェッカーを実行します。

Answer: B (メーッセージを残す)

In change management, the scope of a project lists all the changes that are taking place. The scope ensures that all team members understand the boundaries and extent of the project, helping to prevent unexpected changes. Here's a

* Scope: Defines the project's boundaries and deliverables, including all the planned changes. It ensures that everyone involved understands what is included and excluded in the project, minimizing unexpected changes.
* Risk analysis: Identifies potential risks and their impact but does not list the changes.

* Rollback plan: Provides a strategy for reverting changes if something goes wrong but does not list changes.
* Review: Involves evaluating changes but does not compile the list of changes.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 4.2: Explain basic change-management best practices.
Change management documentation.

最新問題**: 289**
ユーザーは、特定のユーザー グループにのみアクセスを許可するように Linux デバイス上のファイル アクセス許可を変更するように要求しました。ユーザーのリクエストを完了するには、次のコマンドのうちどれを使用する必要がありますか?
A. cat
B. chmod
C. pwd
D. cacls
Answer: B (メーッセージを残す**)**
The chmod command is used to change the permissions of files and directories in Linux. It can grant or revoke read, write, and execute permissions for the owner, the group, and others. To change the file permissions to only allow access to a certain group of users, the chmod command can use either the symbolic or the numeric mode. For example, to give read and write permissions to the group and no permissions to others, the command can be:
chmod g+rw,o-rwx filename
or
chmod 660 filename
References: 1 Chmod Command in Linux (File Permissions) | Linuxize(https://linuxize.com/post/chmod- command-in-linux/)2 How To Change File or Directory Permissions in Linux | Tom's Hardware(https://www.
tomshardware.com/how-to/change-file-directory-permissions-linux).

最新問題**: 290**
ある組織がキオスク マシンのモニターを更新しています。アップグレードの実行中に、組織は物理的な入力デバイスを削除したいと考えています。コントロール パネルの次のユーティリティのどれを使用して、オンスクリーン キーボードをオンにし、物理的な入力デバイスを置き換えることができますか。
* デバイスとプリンター
A. アクセスのしやすさ
B. プログラムと機能
C. デバイス マネージャー
Answer: B (メーッセージを残す**)**
Ease of Access is a utility in the Control Panel that allows users to adjust various accessibility settings on Windows, such as the on-screen keyboard, magnifier, narrator, high contrast, etc. The on-screen keyboard can be turned on by going to Ease of Access > Keyboard and toggling the switch to On12. Alternatively, the on- screen keyboard can be opened by pressing Windows + Ctrl + O keys or by typing osk.exe in the Run dialog box3.
References: 1 Use the On-Screen Keyboard (OSK) to type(https://support.microsoft.com/en-us/windows/use- the-on-screen-keyboard-osk-to-type-ecbb5e08-5b4e-d8c8-f794-81dbf896267a)2 How to Enable or Disable the On-Screen Keyboard in Windows 10 - Lifewire(https://www.lifewire.com/enable-or-disable-on-screen- keyboard-in-windows-10-5180667)3 On-Screen Keyboard Settings, Tips and Tricks in Windows 11/10 (https://www.thewindowsclub.com/windows-onscreen-keyboard).

最新問題**: 291**

会社は、ハードドライブを再利用するために、過去のユーザーのハードドライブから情報を削除したいと考えています.次の魔女は、最も安全な方法です.
A. Windows の再インストール
B. クイックフォーマットを行う
C. ディスク消去ソフトの使用
D. コマンドライン インターフェイスからすべてのファイルを削除する
Answer: C (メーッセージを残す)
Using disk-wiping software is the most secure method for removing information from past users' hard drives in order to reuse the hard drives. Disk-wiping software can help to ensure that all data on the hard drive is completely erased and cannot be recovered.

最新問題**: 292**
顧客は、写真やビデオを共有するために古いデスクトップに安価なファイル サーバーを構成しており、複雑なライセンスを回避したいと考えています。技術者は、次のオペレーティング システムのうちどれを推奨する可能性が高いでしょうか。
A. Chrome OS
B. Linux
C. macOS
D. ウィンドウ
Answer: B (メーッセージを残す)
For an inexpensive file server to share photos and videos while avoiding complicated licensing, the technician should recommend:
* Linux: Linux is a free and open-source operating system that is ideal for setting up a file server. It offers robust file-sharing capabilities with minimal licensing complications.
* Chrome OS: Designed primarily for lightweight, web-based tasks and not ideal for a file server.
* macOS: Requires Apple hardware and involves more complex licensing compared to Linux.
* Windows: While capable of being a file server, Windows may involve licensing fees, particularly for server editions.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 1.8: Explain common OS types and their purposes.
Linux documentation and its use in setting up file servers.

最新問題**: 293**
技術者は、サード パーティ製の Windows 10 VoIP アプリケーションで発信音声が聞こえない問題をトラブルシューティングしています。PC は、電源付きハブに接続された USB マイクを使用しています。技術者は、ボイス レコーダーを使用して PC でマイクが動作することを確認します。問題を解決するために技術者が行うべきことは次のうちどれですか?
A. USB ハブからマイクを取り外し、PC の USB ポートに直接接続します。
B. Windows のプライバシー設定でマイクを有効にして、デスクトップ アプリケーションがマイクにアクセスできるようにします。
C. デバイス マネージャーからマイクを削除し、新しいハードウェアをスキャンします。
D. USB マイクを従来の 3.5 mm プラグを使用するものに交換します。
Answer: B (メーッセージを残す)
In Windows 10, there are privacy settings that control access to certain devices, such as microphones, cameras, and other input devices. If the microphone is not enabled under these privacy settings, the VoIP application may not have access to it, causing a lack of outgoing audio.
The technician can go to the Windows 10 Settings menu, select the Privacy submenu, and under App permissions, select Microphone. The technician should then turn on the toggle switch for the VoIP application to allow it to access the microphone.

Removing the microphone from the USB hub and plugging it directly into a USB port on the PC may or may not solve the issue, as the issue could be related to the privacy settings. Deleting the microphone from Device Manager and scanning for new hardware may also not solve the issue, as the issue could be related to the privacy settings. Replacing the USB microphone with one that uses a traditional 3.5mm plug is not recommended, as it would require purchasing a new microphone and may not solve the issue.

最新問題: **294**
ゲーム対応と宣伝されていたユーザーの新しいラップトップは、最新のゲームをプレイしているときにパフォーマンスが低下します。ただし、リソースをあまり必要としないゲームをプレイしているときは、遅延は発生しません。技術者がこの問題を解決するには、次のうちどれを実行する必要がありますか?
A. RAMをオーバークロックする
B. NICチーミングを有効にする
C. 専用グラフィックスを選択
D. CPUハイパースレッディングを有効にする
Answer: (解答を表示する**)**
Comprehensive and Detailed In-Depth Explanation:Many modern laptops have both an integrated GPU (built into the CPU) and a dedicated GPU (such as NVIDIA or AMD). The system may default to the integrated GPU to save power, which results in poor gaming performance. The technician should manually set the game to use the dedicated graphics card to resolve the issue.
* A. Overclock the RAM - Incorrect. While overclocking RAM can improve performance slightly, it does not resolve GPU-related gaming lag.
* B. Enable NIC teaming - Incorrect. NIC teaming improves network bandwidth and has no effect on gaming graphics.
* D. Activate CPU hyperthreading - Incorrect. Hyperthreading improves multitasking but does not directly impact gaming graphics performance.
Reference:
CompTIA A+ 220-1102, Objective 1.8 - Performance Optimization and Troubleshooting

最新問題: **295**
技術者は、会社の最高経営責任者 (CEO) のコンピュータの問題を解決するために何時間も費やしました。CEO は、できるだけ早くデバイスを返却する必要があります。技術者が次に取るべきステップはどれですか?
A. 問題の調査を続行します
B. 反復プロセスを繰り返します
C. CEO に修理に数週間かかることを伝えます
D. チケットをエスカレートする
Answer: D (メーッセージを残す**)**
The technician should escalate the ticket to ensure that the CEO's device is returned as soon as possible1

最新問題: **296**
Windows アップデートは部門のサーバーで実行する必要があります。サーバーへの接続には次のどの方法を使用する必要がありますか?
A. FIP
B. MSRA
C. RDP
D. VPN
Answer: C (メーッセージを残す**)**
RDP (Remote Desktop Protocol) is a protocol that allows a user to connect to and control a remote computer over a network. RDP can be used to perform Windows updates on a department's servers without physically accessing them.
Reference: CompTIA A+ Core 2 Exam Objectives, Section 5.6

最新問題**: 297**
隠しファイルとディレクトリを表示するために使用されるコマンド オプションは次のうちどれですか?
A. -a
B. -s
C. -lh
D. -t
Answer: A (メーッセージを残す**)**
The -a option is used to display hidden files and directories in a command-line interface. Hidden files and directories are those that start with a dot (.) and are normally not shown by default. The -a option stands for
"all" and shows all files and directories, including the hidden ones. The -a option can be used with commands such as ls, dir, or find to list or search for hidden files and directories. The -s, -lh, and -t options are not used to display hidden files and directories. The -s option stands for "size" and shows the size of files or directories in bytes. The -lh option stands for "long human-readable" and shows the size of files or directories in a more readable format, such as KB, MB, or GB. The -t option stands for "time" and sorts the files or directories by modification time. References:
* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 17
* CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 107

最新問題**: 298**
技術者がソフトウェア プログラムをネットワーク共有にダウンロードしました。技術者がインストールのためにプログラムを Windows タブレットにコピーしようとすると、エラーが発生します。技術者が課題を完了するために使用する最適な手順は次のうちどれですか。
* プログラムファイルをUSBドライブにコピーしてインストールします。
A. プログラム ファイルを CD に書き込んでインストールします。
B. HDDをフォーマットしてからインストールを行ってください。
C. HDDを交換してからインストールを行ってください。
Answer: A (メーッセージを残す**)**
Copying the program file to a USB drive and installing it from there is the simplest and most reliable way to transfer the software from the network share to the Windows tablet. The other options are either unnecessary, risky, or impractical. Burning the program file to a CD requires a CD burner and a CD reader, which may not be available on the tablet. Formatting or replacing the HDD will erase all the data and settings on the tablet, which is not advisable unless there is a backup or a serious problem. Moreover, formatting or replacing the HDD will not solve the issue of copying the program file from the network share.
References: 1 How To Copy A Program From One Computer To Another: 5 Ways(https://www.minitool.com
/news/transfer-copy-programs-from-one-computer-to-another.html)2 Transfer files between your Android tablet and PC using Wi-Fi(https://www.techrepublic.com/article/transfer-files-between-your-android-tablet- and-pc-using-wi-fi/)3 Share Files Between Your Tablet and Computer with Huawei Share(https://consumer.
huawei.com/en/support/content/en-us15819174/)4 How to Transfer Installed Programs to Another PC on Windows 10(https://www.diskpart.com/articles/transfer-installed-program-to-another-pc-windows-10-0825.
html).

最新問題**: 299**
ユーザーは、ラップトップの画面が数分間シルトした後すぐにオフになり、コンセントに接続されていないときも非常に暗いと報告しました。その他はすべて正常に機能しているようです。次の Windows 設定のうちどれを構成する必要がありますか?
A. 電源プラン
B. 休止状態

C. スリープ/サスペンド
D. スクリーンセーバー
Answer: A (メーッセージを残す)
Power Plans are Windows settings that allow a user to configure how a laptop's screen behaves when plugged in or running on battery power. They can adjust the screen brightness and the time before the screen turns off due to inactivity. Hibernate, Sleep/Suspend and Screensaver are other Windows settings that affect how a laptop's screen behaves, but they do not allow changing the screen brightness or turning off time. Verified References: https://www.comptia.org/blog/windows-power-planshttps://www.comptia.org/certifications/a

最新問題**: 300**
技術者は、Outlook を開くことができないユーザーから電話を受けました。ユーザーは、昨日は Outlook が正常に動作していたが、コンピュータが夜間に再起動した可能性があると述べています。Outlook が機能しなくなった理由として最も可能性が高いのは次のうちどれですか?
A. 迷惑メールフィルタのインストール
B. 無効なレジストリ設定
C. マルウェア感染
D. オペレーティング システムの更新
Answer: D (メーッセージを残す)
Operating system updates can sometimes cause compatibility issues with some applications, such as Outlook, that may prevent them from opening or working properly. This can happen if the update changes some system files or settings that Outlook relies on, or if the update conflicts with some Outlook add-ins or extensions. To fix this, the technician can try some of these troubleshooting steps:
* Start Outlook in safe mode and disable add-ins. Safe mode is a way of starting Outlook without any add- ins or extensions that may interfere with its functionality. To start Outlook in safe mode, press and hold the Ctrl key while clicking on the Outlook icon. You should see a message asking if you want to start Outlook in safe mode. Click Yes. If Outlook works fine in safe mode, it means one of the add-ins is causing the problem. To disable add-ins, go to File > Options > Add-ins. In the Manage drop-down list, select COM Add-ins and click Go. Uncheck any add-ins that you don't need and click OK. Restart Outlook normally and check if the issue is resolved4.
* Create a new Outlook profile. A profile is a set of settings and information that Outlook uses to manage your email accounts and data. Sometimes, a profile can get corrupted or damaged and cause Outlook to malfunction. To create a new profile, go to Control Panel > Mail > Show Profiles. Click Add and follow the instructions to set up a new profile with your email account. Make sure to select the option to use the new profile as the default one. Restart Outlook and check if the issue is resolved5.
* Repair your Outlook data files. Data files are files that store your email messages, contacts, calendar events, and other items on your computer. Sometimes, data files can get corrupted or damaged and cause Outlook to malfunction. To repair your data files, you can use a tool called scanpst.exe, which is located in the same folder where Outlook is installed (usually C:\Program Files\Microsoft Office\root \Office16). To use scanpst.exe, close Outlook and locate the tool in the folder. Double-click on it and browse to the location of your data file (usually C: \Users\username\AppData\Local\Microsoft\Outlook). Select the file and click Start to begin the scanning and repairing process. When it's done, restart Outlook and check if the issue is resolved.
* Run the /resetnavpane command. The navigation pane is the panel on the left side of Outlook that shows your folders and accounts. Sometimes, the navigation pane can get corrupted or damaged and cause Outlook to malfunction. To reset the navigation pane, press Windows key + R to open the Run dialog box, or open the Command Prompt. Type outlook.exe /resetnavpane and hit Enter. This will clear and regenerate the navigation pane settings for Outlook. Restart Outlook and check if the issue is resolved.

最新問題**: 301**
ユーザーは Windows 10 Home がインストールされたコンピューターを持っており、Windows 10 Pro ライセンスを購入しました。ユーザーは OS をアップグレードする方法がわかりません。このライセンスを適用するために技術者が行うべきことは次のうちどれですか?
A. c:\Windows\windows.lie ファイルをマシンにコピーし、再起動します。
B. 付属のアクティベーション キー カードをプロダクト キーと引き換えます。
C. Windows USB ハードウェア ドングルを挿入し、アクティベーションを開始します。
D. デバイスのハードウェアに含まれるデジタル ライセンスを使用してアクティベートします。
Answer: B (メーッセージを残す)

Redeeming the included activation key card for a product key is the correct way to apply a Windows 10 Pro license to a computer that has Windows 10 Home installed. The activation key card is a physical or digital card that contains a 25-digit code that can be used to activate Windows 10 Pro online or by phone. Copying the windows.lie file, inserting a Windows USB hardware dongle and activating with the digital license are not valid methods of applying a Windows 10 Pro license. Verified References: https://www.comptia.org/blog /how-to-upgrade-windows-10-home-to-pro https://www.comptia.org/certifications/a

最新問題: **302**
ドメイン環境で Android フォンのセキュリティ設定を制御するために使用する必要があるのは、次のうちどれですか?
A. MDM
B. MFA
C. ACL
D. SMS
Answer: (解答を表示する**)**
The best answer to control security settings on an Android phone in a domain environment is to use "Mobile Device Management (MDM)". MDM is a type of software that is used to manage and secure mobile devices such as smartphones and tablets. MDM can be used to enforce security policies, configure settings, and remotely wipe data from devices. In a domain environment, MDM can be used to manage Android phones and enforce security policies such as password requirements, encryption, and remote wipe capabilities12

最新問題: **303**
次のうち、EULA に含まれている可能性が最も高いのはどれですか?
A. 保管の連鎖
B. ソフトウェアコードのバックアップ
C. 個人を特定できる情報
D. 使用制限
Answer: D (メーッセージを残す**)**
An EULA (End-User License Agreement) is a legally binding contract between a software supplier and a customer or end-user, generally made available to the customer via a retailer acting as an intermediary. A EULA specifies in detail the rights and restrictions which apply to the use of the software. Some of the main terms included in an EULA are the terms and scope of the license, any licensing fees, warranties and disclaimers, limitation of liability, revocation or termination of the license, and intellectual property information and restrictions on using the license (e.g. modification and copying)1 https://www.termsfeed.com/blog/eula-vs-terms-conditions/

最新問題: **304**
次の macOS ユーティリティのうち、起動ディスクの暗号化に AES-128 を使用するものはどれですか?
A. fdisk
B. ディスパート
C. ディスクユーティリティ
D. ファイルボルト

Answer: D (メーッセージを残す)
FileVault is a macOS utility that uses AES-128 (Advanced Encryption Standard) to encrypt the startup disk of a Mac computer. It protects the data from unauthorized access if the computer is lost or stolen. fdisk and Diskpart are disk partitioning utilities for Linux and Windows, respectively. Disk Utility is another macOS utility that can perform disk management tasks, such as formatting, resizing, repairing, etc.
Verified References: https://www.comptia.org/blog/what-is-filevault https://www.comptia.org/certifications/a

最新問題**: 305**
技術者は、ユーザーが外部 Web ページを解決できないことを示すチケットを受け取りますが、特定の IP アドレスは機能しています。問題を解決するために技術者がワークステーションで最も変更する必要があるのは、次のうちどれですか?
A. デフォルトゲートウェイ
B. ホストアドレス
C. ネームサーバー
D. サブネットマスク
Answer: (解答を表示する**)**
The technician most likely needs to change the default gateway on the workstation to resolve the issue. The default gateway is the IP address of the router that connects the workstation to the internet, and it is responsible for routing traffic between the workstation and the internet. If the default gateway is incorrect, the workstation will not be able to access external web pages.

最新問題**: 306**
ユーザーが電子メールを読むために携帯電話を水平に回転させますが、設定で自動回転がオンになっているにもかかわらず、ディスプレイは垂直のままです。次の VT1ich で問題が解決する可能性が最も高いですか?
A. 磁力計の再校正
B. コンパスの再校正
C. デジタイザの再調整
D. 加速度計の再校正
Answer: D (メーッセージを残す**)**
When a user rotates a cell phone horizontally to read emails and the display remains vertical, even though the settings indicate autorotate is on, this is typically due to a problem with the phone's accelerometer. The accelerometer is the sensor that detects changes in the phone's orientation and adjusts the display accordingly.
If the accelerometer is not calibrated correctly, the display may not rotate as expected.
Recalibrating the accelerometer is the most likely solution to this issue. The process for recalibrating the accelerometer can vary depending on the specific device and operating system, but it typically involves going to the device's settings and finding the option to calibrate or reset the sensor. Users may need to search their device's documentation or online resources to find specific instructions for their device.

最新問題**: 307**
ユーザーのラップトップのパフォーマンスが低下し、見慣れない Web サイトにリダイレクトされます。ユーザーは、ランダムなポップアップ ウィンドウにも気づきました。問題を解決するために技術者が最初に実行すべきステップは次のうちどれですか?
A. マルウェアとランサムウェアをスキャンします。
B. システムの復元を実行します。
C. ネットワーク使用率を確認します。
D. ウイルス対策ソフトウェアを更新します。
Answer: A (メーッセージを残す**)**

The most likely cause of the user's laptop issues is that it has been infected by some type of malware or ransomware. Malware and ransomware are malicious software that can harm, exploit, or disrupt devices or networks12. They can cause symptoms such as slow performance, browser redirects, pop-up windows, data encryption, or ransom demands12. Therefore, the first step a technician should take to resolve the issue is to scan the laptop for malware and ransomware using a reliable and updated anti-malware tool34. This can help identify and remove any malicious software that may be present on the laptop. Scanning for malware and ransomware is more effective and urgent than the other options because:
* Performing a system restore may not remove the malware or ransomware, as some of them can persist or hide in the system files or backup copies34. Moreover, a system restore may result in data loss or corruption, as it restores the system to a previous state and deletes any changes made after that point5.
* Checking the network utilization may not help diagnose or fix the problem, as the malware or ransomware may not be using the network at all, or may be using it in a stealthy or encrypted manner34. Furthermore, checking the network utilization does not address the root cause of the issue, which is the presence of malicious software on the laptop.
* Updating the antivirus software may not be sufficient to detect or remove the malware or ransomware, as some of them may evade or disable the antivirus software, or may be too new or unknown for the antivirus software to recognize34. Additionally, updating the antivirus software does not guarantee that the laptop will be scanned for malware or ransomware, as the user may need to initiate or schedule the scan manually.

最新問題**: 308**
次に行うべきことは次のうちどれですか?
A. Telecom に電子メールを送信して問題を通知し、再発を防止します。
B. チケットを閉じます。
C. 次回は時間をかけて自分で修正するようユーザーに伝えます。
D. 実行した解決策についてユーザーを教育します。
Answer: D (メーッセージを残す**)**
educating the user on the solution that was performed is a good next step after resolving an issue. This can help prevent similar issues from happening again and empower users to solve problems on their own.

最新問題**: 309**
管理者は、使用するストレージ容量を最小限に抑えるサーバー バックアップ システムを設計および実装しています。合成完全バックアップと組み合わせて使用するのに最適なバックアップ アプローチは次のうちどれですか?
A. 差動
B. ファイルを開く
C. アーカイブ
D. インクリメンタル
Answer: D (メーッセージを残す**)**
Incremental backups are backups that only include the changes made since the last backup, whether it was a full or an incremental backup. Incremental backups minimize the capacity of storage used and are often used in conjunction with synthetic full backups, which are backups that combine a full backup and subsequent incremental backups into a single backup set.
Reference: CompTIA A+ Core 2 Exam Objectives, Section 3.3

最新問題**: 310**
システム ドライブがほぼいっぱいになっているため、技術者はスペースを確保する必要があります。技術者は次のツールのうちどれを使用する必要がありますか?
A. ディスクのクリーンアップ
B. リソースモニター
C. ディスクのデフラグ
D. ディスク管理

Answer: A (メーッセージを残す)
Disk Cleanup is a tool that can free up some space on a system drive that is nearly full. It can delete temporary files, cached files, recycle bin files, old system files and other unnecessary data. Resource Monitor is a tool that shows the network activity of each process on a Windows machine. Disk Defragment is a tool that optimizes the performance of a hard drive by rearranging the data into contiguous blocks. Disk Management is a tool that allows creating, formatting, resizing and deleting partitions on a hard drive.
Verified References: https://www.comptia.org/blog/how-to-use-disk-cleanup https://www.comptia.org
/certifications/a

最新問題**: 311**
Windows 10 OS を修復しようとしているときに、技術者はキーを要求するプロンプトを受け取ります。技術者は管理者パスワードを試行しますが、拒否されます。技術者が OS の修復を続行するために必要なものは次のうちどれですか?
A. SSLキー
B. 事前共有キー
C. WPA2キー
D. 回復キー
Answer: (解答を表示する)
A recovery key is a code that can be used to unlock a BitLocker-encrypted drive when the normal authentication methods (such as password or PIN) are not available or have been forgotten. BitLocker is a feature of Windows that encrypts the entire drive to protect data from unauthorized access. If a technician is trying to repair a Windows 10 OS that has BitLocker enabled, they will need the recovery key to access the drive and continue the OS repair. SSL key, preshared key, and WPA2 key are not keys that are related to BitLocker or OS repair.

最新問題**: 312**
Windows ユーザーは、システムに物理的にアクセスできる攻撃者から機密データを保護するファイルシステムを望んでいます。ユーザーは次のどれを選択する必要がありますか?
A. ext
B. APFS
C. FAT
D. EFS
Answer: D (メーッセージを残す)
EFS (Encrypting File System) is a feature of Windows that provides filesystem-level encryption. It is designed to encrypt files and folders to protect them from unauthorized access, even if an attacker has physical access to the computer.
* ext: A filesystem type used primarily in Linux, without native encryption features for Windows.
* APFS: Apple's filesystem, used in macOS and iOS.
* FAT: A simple filesystem type with no encryption features.
* EFS: The correct choice for a Windows user needing to encrypt data at the filesystem level to protect against unauthorized physical access.
Reference: CompTIA A+ Exam Objectives [220-1102] - 1.6: Given a scenario, use appropriate Microsoft Windows features and tools.

最新問題**: 313**
技術者は新しいワークステーションに RAM を取り付けているため、静電気の放電から保護する必要があります。
この懸念を最もよく解決するのは次のうちどれですか?
A. バッテリーバックアップ
B. サーマルペースト
C. ESDストラップ

D. 安定したパワー
Answer: C (メーッセージを残す**)**
An ESD strap, also known as an antistatic wrist strap, is a device that prevents electrostatic discharge (ESD) from damaging sensitive electronic components such as RAM. ESD is the sudden flow of electricity between two objects with different electrical charges, which can cause permanent damage or malfunction to electronic devices. An ESD strap connects the technician's wrist to a grounded surface, such as a metal case or a mat, and equalizes the electrical potential between the technician and the device. Battery backup, thermal paste, and consistent power are not devices that can protect against ESD.

最新問題**: 314**
技術者は、迅速に復元する必要があるバックアップおよびリカバリ ソリューションを設定しています。ストレージ スペースは考慮されません。技術者は次のどのバックアップ方法を実施する必要がありますか。
A. Differential
B. Synthetic
C. Full
D. Incremental
Answer: C (メーッセージを残す**)**
The correct answer is C. Full Backup.
* A Full Backup creates a complete copy of all selected data every time it runs. This method ensures the fastest possible recovery time because all the necessary data is contained in a single backup file.
* Since storage space is not a concern, full backups are ideal because they avoid the need to restore multiple incremental or differential backups.
* Recovery Time Objective (RTO) is minimized, making full backups the best choice for quick restoration.
Why Other Options Are Incorrect:
* A. Differential Backup - Backs up only the data that has changed since the last full backup. While faster to restore than an incremental backup, it still requires both the last full backup and the most recent differential backup for restoration.
* B. Synthetic Backup - A synthetic full backup is created by combining previous full and incremental backups without needing to back up data again from the source. While efficient in terms of backup creation, restoration can be slower compared to a traditional full backup.
* D. Incremental Backup - Backs up only data that has changed since the last backup (whether full or incremental). While efficient in storage, restoring from incremental backups can be slow because multiple backups must be restored in sequence.
CompTIA A+ 220-1102 Exam Reference:
* Objective 4.3 - Given a scenario, apply best practices to secure a workstation.
* Objective 4.4 - Given a scenario, implement methods for securing mobile devices.

最新問題**: 315**
ユーザーのホーム システムがマルウェアに感染しました。技術者はシステムをネットワークから分離し、システムの復元を無効にしました。技術者は次に次のどれを行う必要がありますか。
A. ウイルス対策スキャンを実行します。
B. Windows の更新プログラムを実行します。
C. システムを再イメージ化します。
D. システムの復元を有効にします。
Answer: (解答を表示する**)**
When dealing with a malware-infected system, isolating the system from the network and disabling System Restore are critical initial steps. The next step in the malware removal process should be:
* Perform an antivirus scan: This helps to identify and remove the malware from the system. Running a thorough scan using updated antivirus software is essential to detect and clean any malicious files.
* Run Windows updates: This is important for system security but should be done after the malware is removed to avoid further issues.
* Reimage the system: This is a more drastic measure and should be considered if the antivirus scan cannot fully clean the system.

* Enable System Restore: This should only be done after the system is confirmed to be clean.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 3.3: Given a scenario use best practice procedures for malware removal.
Malware removal best practices documentation.

最新問題**: 316**
技術者が、最新の OS アップデートをダウンロードしてインストールできないスマートフォンのトラブルシューティングを行っています。技術者は、再起動してすべてのアプリケーションを閉じた後でも、デバイスの動作が予想よりも遅いことに気づきました。技術者が次にチェックすべき点は次のうちどれですか?
A. アプリケーションの権限
B. 利用可能なストレージ容量
C. バッテリー充電レベル
D. Wi-Fi 接続速度
Answer: B (メーッセージを残す**)**
When a smartphone is unable to download and install the latest OS update and is operating slower than expected, one of the first things to check is the available storage space. Operating system updates often require a significant amount of free space for downloading and installing, and insufficient space can prevent the update process from initiating or completing.
* Available Storage Space: Smartphones use their internal storage to hold the OS, apps, user data, and temporary files needed for updates. If the storage is nearly full, the device can slow down due to the lack of space for writing temporary files and may not have enough space to download and install updates. Clearing up space can resolve these issues.
Checking application permissions (A) might be relevant for specific app-related issues but is less likely to affect OS updates. The battery charge level (C) can affect the initiation of an update, as some devices require a minimum charge level to start the update process, but it doesn't typically cause slow operation. While a stable Wi-Fi connection (D) is necessary for downloading updates, it's less likely to be the cause of slowed operation and update issues compared to insufficient storage space.

最新問題**: 317**
CYOD ポリシーの一環として、システム管理者は各ユーザーの Windows デバイスを構成して、スリープ状態または非アクティブ状態から再開するときにパスワードを要求する必要があります。管理者を正しい設定に導くパスは次のうちどれですか?
A. [設定] を使用して、スクリーンセーバーの設定にアクセスします
B. [設定] を使用して、画面のタイムアウト設定にアクセスします
C. 設定を使用して一般にアクセスします
D. 設定を使用してディスプレイにアクセスします。
Answer: A (メーッセージを残す**)**
The systems administrator should use Settings to access Screensaver settings to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity1

最新問題**: 318**
ローカル オフィスで作業している技術者が、コンピュータに複数のホーム エディション ソフトウェアのコピーがインストールされていることを発見しました。これが最も違反している可能性が高いのは次のうちどれですか?

A. EULA
B. ピル
C. DRM
D. オープンソース契約
Answer: A (メーッセージを残す)
The installation of home edition software on computers at a local office most likely violates the EULA.
EULA stands for End User License Agreement and is a legal contract that specifies the terms and conditions for using a software product or service. EULA typically covers topics such as license scope, duration and limitations, rights and obligations of the parties, warranties and disclaimers, liability and indemnity clauses, and termination procedures. EULA may also restrict the use of home edition software to personal or non- commercial purposes only, and prohibit the use of home edition software in business or professional settings.
Violating EULA may result in legal actions or penalties from the software vendor or developer. PII stands for Personally Identifiable Information and is any information that can be used to identify or locate an individual, such as name, address, phone number, email address, social security number or credit card number. PII is not related to software installation or licensing but to data protection and privacy. DRM stands for Digital Rights Management and is a technology that controls or restricts the access and use of digital content, such as music, movies, books or games. DRM is not related to software installation or licensing but to content distribution and piracy prevention. Open-source agreement is a type of license that allows users to access, modify and distribute the source code of a software product or service freely and openly. Open-source agreement does not restrict the use of software to home edition only but encourages collaboration and innovation among developers and users. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version
4.0, Domain 5.1

最新問題: 319
技術者が、GUI を起動できない Windows 10 PC のトラブルシューティングを行っています。最近、新しい SSD と新しい Windows のコピーが PC にインストールされました。この問題を解決するために使用する最も適切なコマンドは次のどれですか。
* msconfig
A. chkdsk
B. sfc
C. diskpart
D. mstsc
Answer: C (メーッセージを残す)
The sfc command is a tool for scanning and repairing system files that are corrupted or missing on Windows operating systems12. System files are essential files that are required for the proper functioning of the operating system, such as the GUI, drivers, services, and applications. If system files are damaged or deleted, the operating system may fail to start or run properly, causing errors, crashes, or blue screens.
The sfc command can be used to fix the issue of the PC that is unable to start the GUI, assuming that the problem is caused by corrupted or missing system files. The sfc command can be run from the command prompt, which can be accessed by booting the PC from the installation media, choosing the repair option, and selecting the command prompt option3. The sfc command can be used with different switches, such as
/scannow, /verifyonly, /scanfile, or /offbootdir, depending on the situation and the desired action4. The most common switch is /scannow, which scans all the system files and repairs any problems that are found5. The syntax of the sfc command with the /scannow switch is:
sfc /scannow
The sfc command will then scan and repair the system files, and display the results on the screen. If the sfc command is able to fix the system files, the PC should be able to start the GUI normally after rebooting. If the sfc command is unable to fix the system files, the PC may need further troubleshooting or a clean installation of Windows.
References1: CompTIA A+ Certification Exam Core 2 Objectives, page 10 2: CompTIA A+ Core 2 (220-
1102) Complete Video Course, Lesson 26 Documentation 3: How to use SFC Scannow to repair Windows system files 4: SFC Command (System File Checker) 5: How to Repair Windows 10 using Command Prompt

最新問題: **320**
ユーザーが最新のパッチ ノートを表示するためにゲーム ベンダーの Web サイトにアクセスしましたが、この情報はページでは入手できません。ユーザーはページをリロードする前に次のどれを実行する必要がありますか?
A. ブラウザのデータを同期します。
B. プライベートブラウズモードを有効にします。
C. サイトを信頼済みとしてマークします。
D. キャッシュされたファイルをクリアします。
Answer: D (メーッセージを残す)
Clearing the cached file is an action that can help resolve the issue of not seeing the latest patch notes on a game vendor's website. A cached file is a copy of a web page or file that is stored locally on the user's browser or device for faster loading and offline access. However, sometimes a cached file may become outdated or corrupted and prevent the user from seeing the most recent or accurate version of a web page or file. Clearing the cached file can force the browser to download and display the latest version from the server instead of using the old copy from the cache. Synchronizing the browser data, enabling private browsing mode, and marking the site as trusted are not actions that can help resolve this issue.

最新問題: **321**
ある企業が ODDS 攻撃に遭遇しています。いくつかの内部ワークステーションがトラフィックの発生源です。ワークステーションで発生する可能性が最も高い感染の種類は次のうちどれですか? (2つ選択してください)
A. ゾンビ
B. キーロガー
C. アドウェア
D. ボットネット
E. 身代金要求
F. スパイウェア
Answer: A,D (メーッセージを残す)
The correct answers are A and D) Zombies and botnets are types of infections that allow malicious actors to remotely control infected computers and use them to launch distributed denial-of-service (DDoS) attacks against a target. A DDoS attack is a type of cyberattack that aims to overwhelm a server or a network with a large volume of traffic from multiple sources, causing it to slow down or crash.
A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote server, often for the purpose of stealing passwords, credit card numbers, or other sensitive information.
Adware is a type of software that displays unwanted advertisements on a user's computer, often in the form of pop-ups, banners, or redirects. Adware can also collect user data and compromise the security and performance of the system.
Ransomware is a type of malware that encrypts the files or locks the screen of a user's computer and demands a ransom for their restoration. Ransomware can also threaten to delete or expose the user's data if the ransom is not paid.
Spyware is a type of software that covertly monitors and collects information about a user's online activities, such as browsing history, search queries, or personal data. Spyware can also alter the settings or functionality of the user's system without their consent.

最新問題: **322**
更新に失敗すると、アプリケーションが起動しなくなり、次のエラー メッセージが生成されます。
アプリケーションを修復する必要があります。技術者がこの問題に対処するために使用する必要がある Windows 10 ユーティリティは次のうちどれですか?
A. デバイス マネージャー
B. 管理者ツール
C. プログラムと機能
D. 回復

Answer: (解答を表示する**)**
Recovery is a Windows 10 utility that can be used to address the concern of a failed update that prevents an application from launching. Recovery allows the user to reset the PC, go back to a previous version of Windows, or use advanced startup options to troubleshoot and repair the system2. Device Manager, Administrator Tools, and Programs and Features are not Windows 10 utilities that can fix a failed update.

最新問題**: 323**
技術者は、コンピュータが紛失または盗難された場合に、不正なデータ アクセスを軽減したいと考えています。技術者は次の機能のうちどれを有効にする必要がありますか?
A. ネットワーク共有
B. グループポリシー
C. BitLocker
D. 静的 IP
Answer: (解答を表示する**)**
BitLocker is a Windows security feature that provides encryption for entire volumes,addressing the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned devices1. BitLocker helps mitigate unauthorized data access by enhancing file and system protections, rendering data inaccessible when BitLocker-protecteddevices are decommissioned or recycled1. Network share, Group Policy, and Static IP are not features that can prevent unauthorized data access if a computer is lost or stolen.
References:
BitLocker overview - Windows Security | Microsoft Learn1
The Official CompTIA A+ Core 2 Study Guide2, page 315.

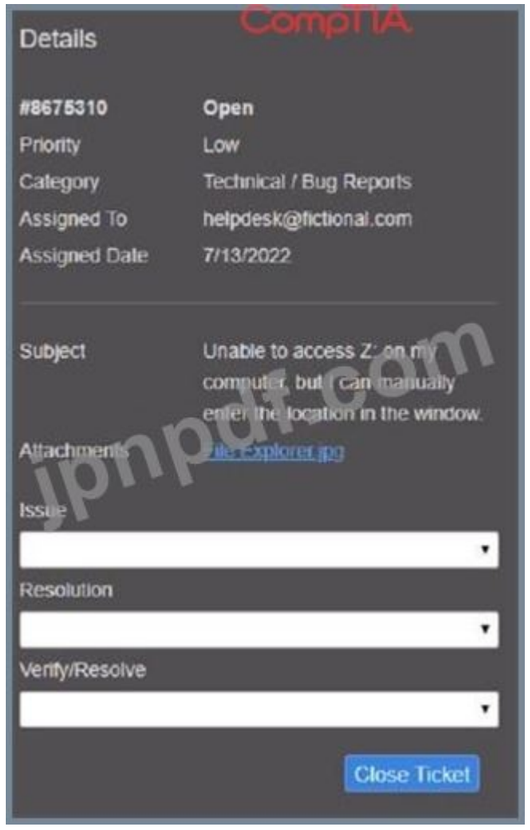
最新問題**: 324**
管理者がヘルプ デスクに電話して、非ドメイン環境にある財務部門のより安全な環境を作成するための支援を求めました。不正使用から保護するための最良の方法は次のうちどれですか?
A. パスワード有効期限の実装
B. ユーザー権限の制限
C. 画面ロックの使用
D. 不要なサービスの無効化
Answer: B (メーッセージを残す**)**
Restricting user permissions is a method of creating a more secure environment for the finance department in a non-domain environment. This means that users will only have access to the files and resources that they need to perform their tasks and will not be able to modify or delete other files or settings that could compromise security or functionality.

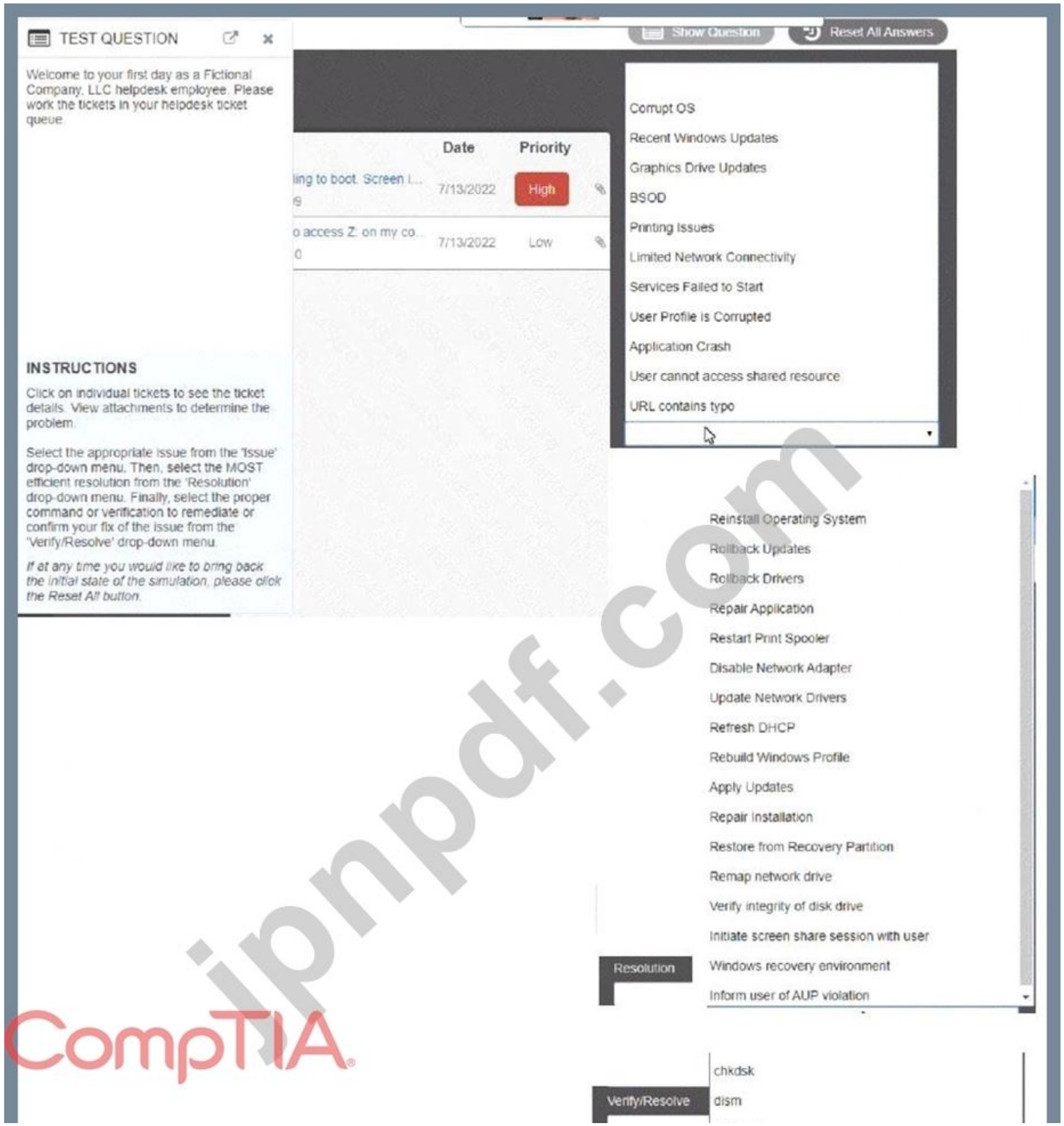
最新問題**: 325**
紛失または盗難にあったモバイル デバイスがオフラインのときに、そのデバイス上の機密情報にアクセスできないようにするには、次のどれが効果的ですか。
A. リモートワイプ
B. 必須の画面ロック
C. 位置情報アプリケーション
D. デバイスデータの暗号化
Answer: D (メーッセージを残す**)**
Device data encryption (Option D) ensures that even if the device is lost or stolen, its data cannot be accessed without proper credentials, even while offline. Encryption protects the data at rest, making it unreadable without the decryption key.
* Remote wipe (Option A) requires the device to be online to receive the wipe command.
* Mandatory screen locks (Option B) provide a layer of security but can be bypassed with physical access in some cases.

* Location applications (Option C) help track the device but don't protect data.
CompTIA A+ Core 2 References:
* 2.7 - Explain methods for securing mobile devices, including encryption

最新問題**: 326**
Linux で実行中のプロセスを一覧表示するコマンドは次のどれですか?
A. top
B. apt-get
C. ls
D. cat
Answer: A (メーッセージを残す**)**
The 'top' command in Linux is used to display the running processes along with information about system resources like CPU and memory usage. It provides a real-time view of the system's resource consumption, making it an essential tool for monitoring and managing system performance.

最新問題**: 327**
架空の会社としての初日へようこそ。LLC ヘルプデスクの従業員。ヘルプデスクのチケット キューでチケットを処理してください。
個々のティッカーをクリックして、チケットの詳細を表示します。添付ファイルを表示して問題を特定します。
[問題] ドロップダウン メニューから適切な問題を選択します。次に、[解像度] ドロップダウン メニューから最も効率的な解像度を選択します。最後に、[Verify Resolve] ドロップダウン メニューから適切なコマンドまたは検証を選択して、問題を修正または確認します。





Answer:

Explanation:

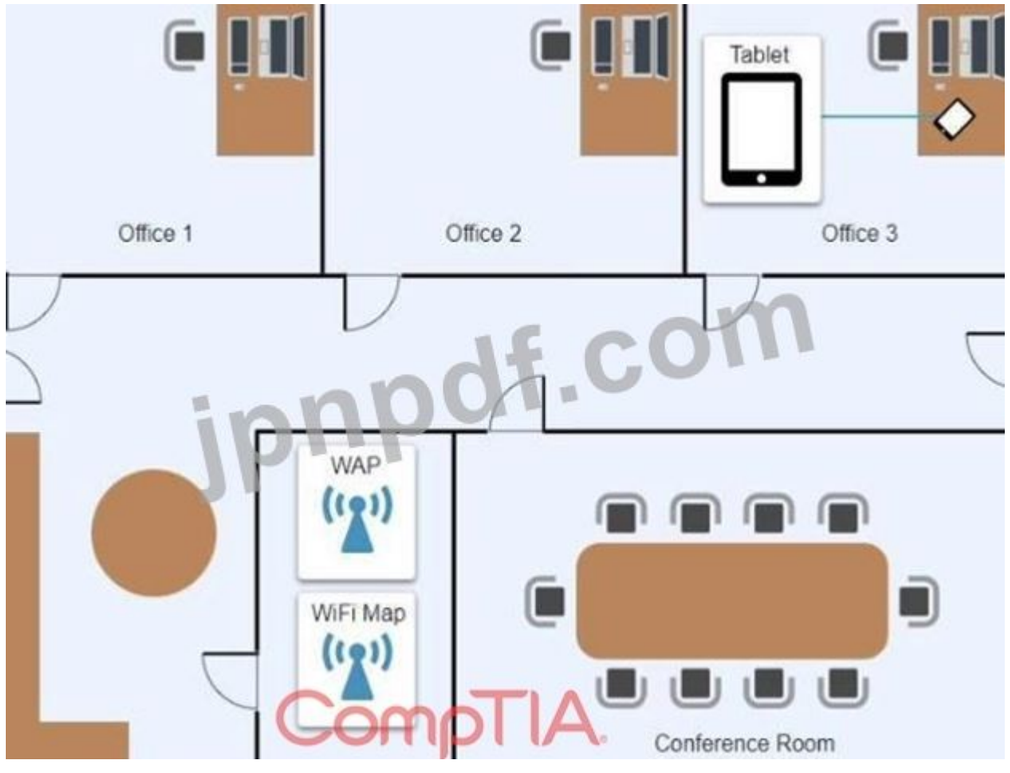
最新問題: **328**

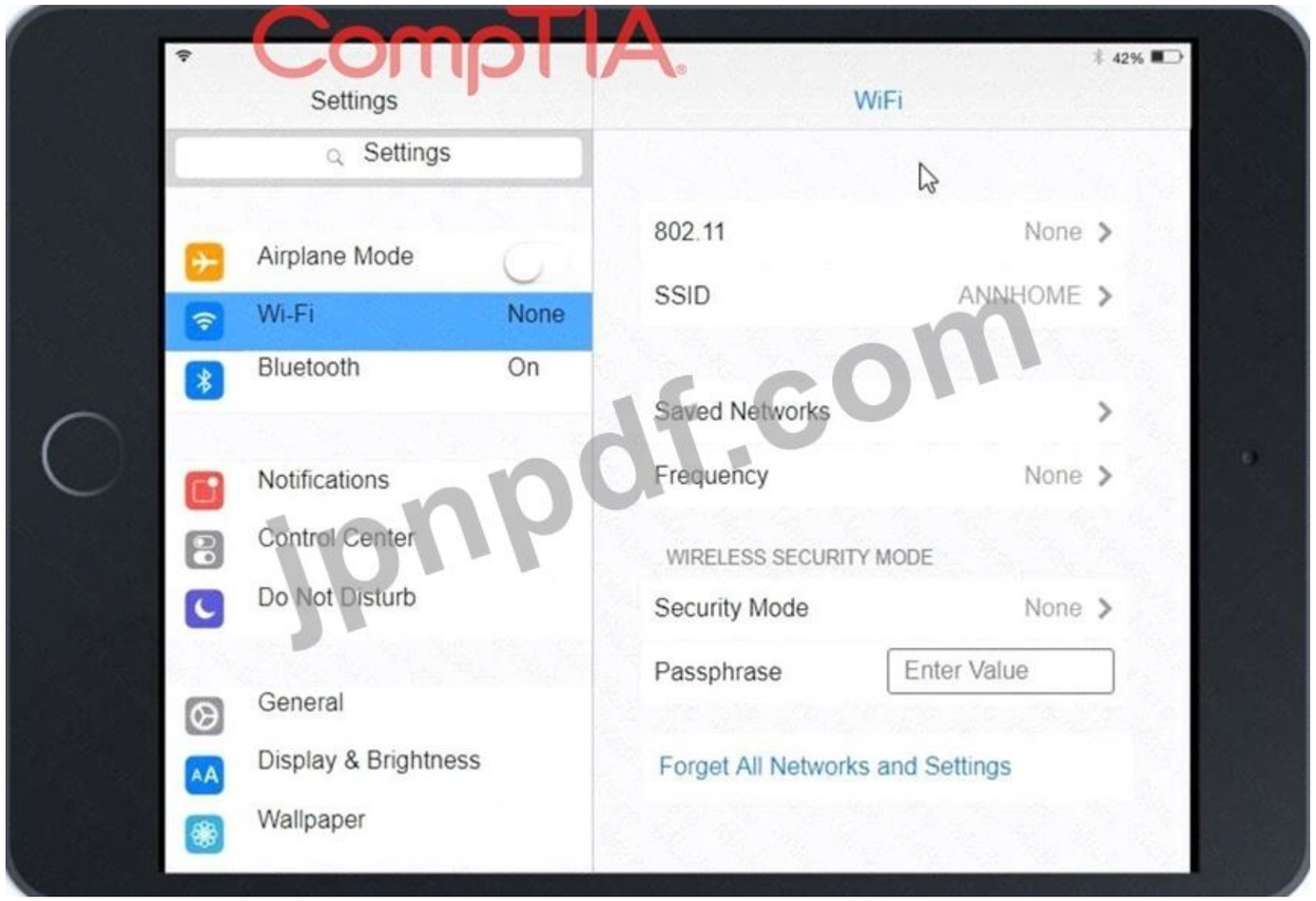
CEO のアンは個人使用のために新しいコンシューマー クラスのタブレットを購入しましたが、会社のワイヤレス ネットワークに接続できません。会社のラップトップはすべて問題なく接続しています。彼女はあなたに、デバイスをオンラインにするための支援を依頼しました。

説明書

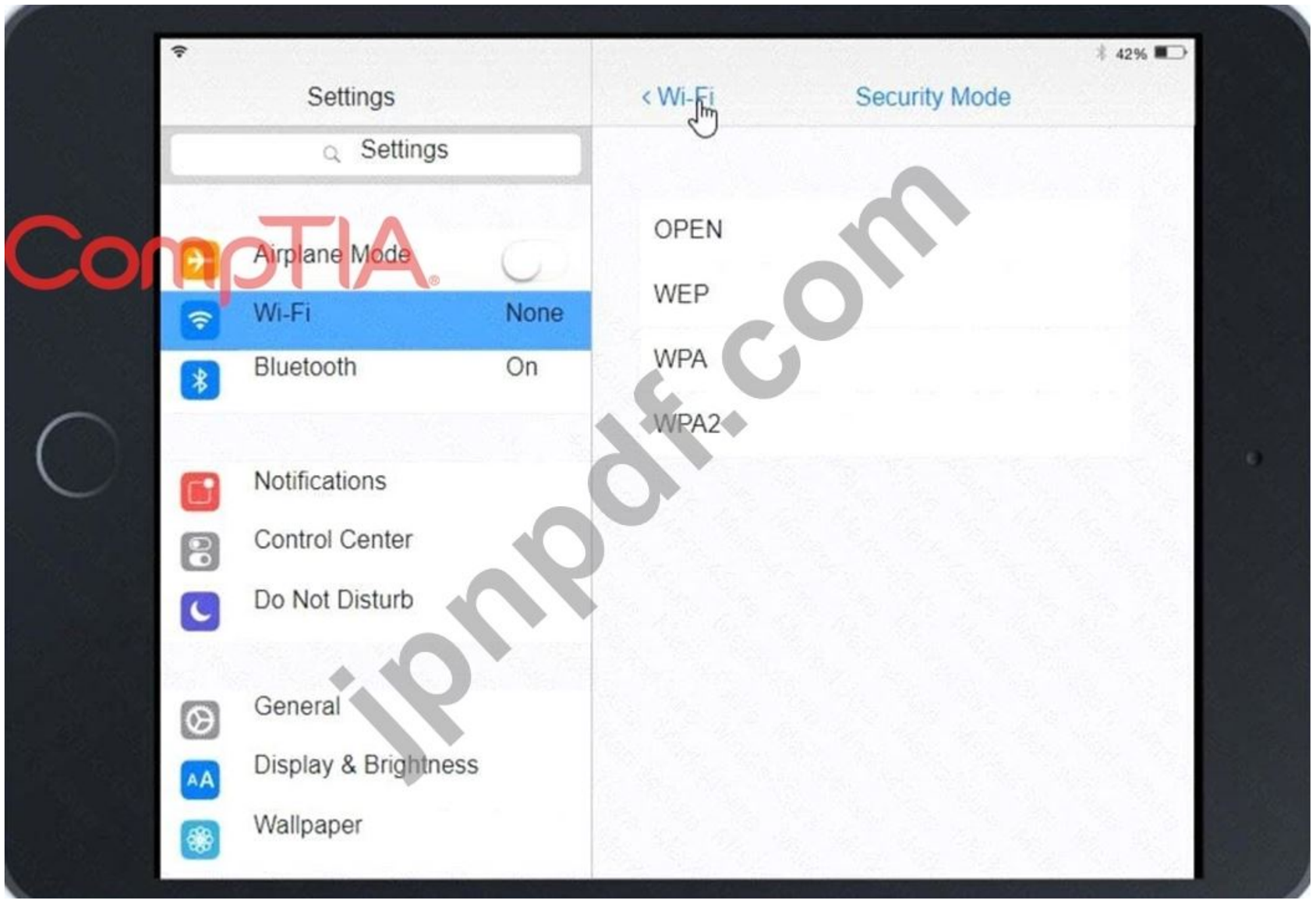
ネットワーク図とデバイス構成を確認して問題の原因を特定し、発見された問題を解決します。

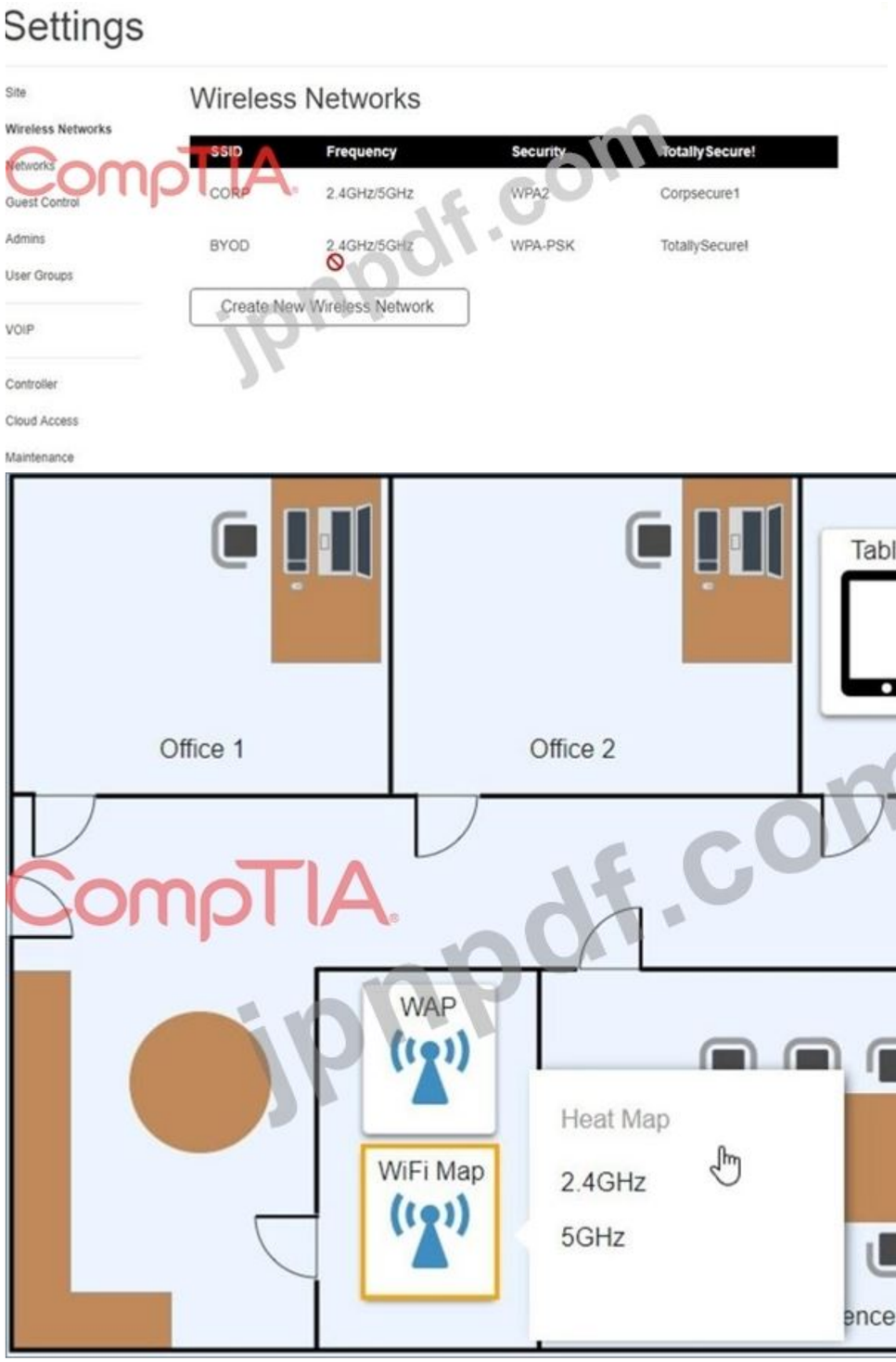
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。






Settings
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
42%
Wi-Fi
802.11
b/g
a
ac





Answer:

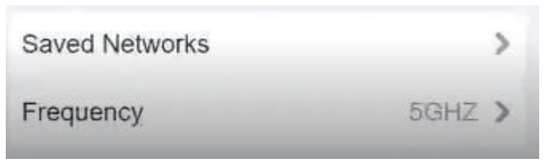
See the Explanation below:

Explanation:

Click on 802.11 and Select ac

Click on SSID and select CORP

Click on Frequency and select 5GHz



At Wireless Security Mode, Click on Security Mode

Select the WPA2

Ann needs to connect to the BYOD SSID, using 2.4GHZ. The selected security method chose should be WPA PSK, and the password should be set to TtotallySecret.

最新問題: **329**
電子メールのリンクをクリックした後、最高財務責任者 (CFO) は次のエラーを受け取りました。

その後、CFO はインシデントを技術者に報告しました。リンクは、組織の銀行にあると言われています。技術者が最初に実行する必要があるのは、次のうちどれですか?
A. ブラウザの CRL を更新する
B. 銀行にトラブル チケットを提出します。
C. ISP に連絡して CFC に関する懸念を報告する
D. CFO にブラウザを終了するように指示します。
Answer: A (メーッセージを残す**)**
The technician should update the browser's CRLs first. The error message indicates that the certificate revocation list (CRL) is not up to date. Updating the CRLs will ensure that the browser can verify the authenticity of the bank's website.

最新問題: **330**
コンピューターが自動的に再起動し、次のエラー メッセージが表示されます。 お使いの PC に問題が発生したため、再起動する必要があります。エラー情報を収集しているところです。その後、自動的に再起動します。(完了率 0%)。」問題を診断するために技術者が最初に行うべきことは次のどれですか。
A. システム イベント ログを確認します。
B. ハードウェア ドライバーのバージョンを確認します。
C. Windows の更新プログラムをインストールします。
D. RAM 診断を実行します。
Answer: A (メーッセージを残す**)**
The first step is to check the system event logs using tools like Event Viewer. This will allow the technician to identify any critical errors or warnings that occurred before the restart. Based on these logs, further troubleshooting can be done. Verifying driver versions and performing diagnostics can follow once the root cause is identified.
Reference: CompTIA A+ 220-1102 Exam Objectives, Domain 3.1 Software Troubleshooting

最新問題: **331**
APFS を最もよく表すのは次のどれですか?
A. Linux OSで使用されるファイルシステム
B. iOSで使用されるファイルシステム

C. Windows OSで使用されるファイルシステム
D. macOSで使用されるファイルシステム
Answer: (解答を表示する**)**
XFS is a high-performance filesystem created by Silicon Graphics in 1994 and is commonly used by Linux operating systems. It supports large files and directories and is known for its robustness and scalability. Other filesystems like NTFS (Windows), APFS (macOS), and HFS (macOS) are used on different platforms.
Reference: Core 2, Domain 1.8 - OS types and filesystem structures.

最新問題**: 332**
週に 1 回、ユーザーは、現在インストールされている Windows プラットフォームでは利用できない特定のオープンソース アプリケーションを実行するために Linux を必要とします。ユーザーは、1 日を通して帯域幅が制限されています。Linux アプリケーションと Windows アプリケーションの並列実行を可能にする最も効率的なソリューションは、次のうちどれですか?
A. Linux と必要なアプリケーションを PaaS クラウド環境にインストールして実行する
B. Linux と必要なアプリケーションを、Windows OS にインストールされた仮想マシンとしてインストールして実行します。
C. ブート ドライブにスワップ可能なドライブ ベイを使用し、アプリケーションを含む各 OS を独自のドライブにインストールする 必要に応じてドライブを交換する
D. Windows と一緒に Linux をインストールするオプションを選択して、デュアル ブート システムをセットアップします。
Answer: (解答を表示する**)**
The user should install and run Linux and the required application as a virtual machine installed under the Windows OS. This solution would allow for parallel execution of the Linux application and Windows applications2.
The MOST efficient solution that allows for parallel execution of the Linux application and Windows applications is to install and run Linux and the required application as a virtual machine installed under the Windows OS. This is because it allows you to run both Linux and Windows together without the need to keep the Linux portion confined to a VM window3.

最新問題**: 333**
Microsoft Windows 10 を実行しているキオスクでは、顧客がチケット番号を入力できるようにするために数字キーパッドのみに依存していますが、その他の情報は入力できません。キオスクが 4 時間アイドル状態になると、ログイン画面がロックされます。
次のサインオン オプションのうち、従業員がキオスクのロックを解除できるのはどれですか?
A. 従業員にユーザー名とパスワードの入力を求める
B. 従業員ごとに顔認証を設定
C. PIN の使用と従業員への提供
D. 従業員に指紋の使用を義務付ける
Answer: C (メーッセージを残す**)**
The best sign-on option that would allow any employee the ability to unlock the kiosk that relies exclusively on a numeric keypad is to use a PIN and provide it to employees. A PIN is a Personal Identification Number that is a numeric code that can be used as part of authentication or access control. A PIN can be entered using only a numeric keypad and can be easily shared with employees who need to unlock the kiosk. Requiring employees to enter their usernames and passwords may not be feasible or convenient if the kiosk only has a numeric keypad and no other input devices. Setting up facial recognition for each employee may not be possible or secure if the kiosk does not have a camera or biometric sensor. Requiring employees to use their fingerprints may not be possible or secure if the kiosk does not have a fingerprint scanner or biometric sensor.
References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

最新問題: **334**
技術者がインターネットからソフトウェアをダウンロードした場合、技術者はテキスト ボックスをスクロールし、テキスト ボックスの最後にある [同意する] というラベルの付いたボタンをクリックする必要があります。
A. DRM
B. 秘密保持契約
C. EULA
D. MOU
Answer: (解答を表示する)
The most likely agreement in use here is a EULA (End User License Agreement). This is a legally binding agreement between the user and the software developer, outlining the terms and conditions that the user must agree to in order to use the software. It is important that the user understands and agrees to the EULA before they can proceed with downloading and installing the software. As stated in the CompTIA A+ Core 2 exam objectives, users should be aware of the EULA before downloading any software.

最新問題: **335**
ユーザーから、PC の動作が遅いと報告されました。技術者は、ディスク I/O が高いと考えています。技術者が次に実行する必要があるのは次のうちどれですか?
A. resmon_exe
B. dfrgui_exe
C. msinf032exe
D. msconfig_exe
Answer: A (メーッセージを残す)
If a technician suspects high disk I/O, the technician should use the Resource Monitor (resmon.exe) to identify the process that is causing the high disk I/O1. Resource Monitor provides detailed information about the system's resource usage, including disk I/O1. The technician can use this information to identify the process that is causing the high disk I/O and take appropriate action1.

最新問題: **336**
ユーザーが特定の Web サイトを閲覧するときに OTP を自動的に要求するように設計されたプラグインを含むアプリケーションをダウンロードします。プラグインは警告やエラーなしでインストールされます。ユーザーが初めてサイトにアクセスしたときにはプロンプトが開かず、ユーザーはサイトにアクセスできません。ユーザーは次のどのブラウザ設定を構成する必要がありますか?
A. 拡張機能/アドイン
B. 証明書の有効性
C. プロキシ設定
D. Trusted sources
Answer: A (メーッセージを残す)
The user should configure extensions/add-ins. Since the issue involves a browser plug-in, checking if the extension or add-in is enabled or properly configured can resolve the issue. If the plug-in is disabled, the OTP prompt will not appear as expected.
Reference: CompTIA A+ 220-1102 Exam Objectives, Domain 3.0 Software Troubleshooting

最新問題: **337**
リモート ユーザーがラップトップで企業電子メール アカウントに接続する際に問題が発生しています。ユーザーがインターネット接続アイコンをクリックしても、接続されている Wi-Fi が認識されません。問題のトラブルシューティングを行っているヘルプ デスク技術者は、これが不正なアクセス ポイントであると想定しています。技術者が最初にとるべき行動は次のうちどれですか?
A. ワイヤレスアダプターを再起動します。
B. ブラウザを起動して、不明なサイトにリダイレクトされるかどうかを確認します。
C. ユーザーに Wi-Fi の切断を指示します。

D. インストールされているウイルス対策ソフトウェアを実行するようにユーザーに指示します。
Answer: (解答を表示する**)**
Instructing the user to disconnect the Wi-Fi is the first action the technician should take if they suspect a rogue access point. A rogue access point is an unauthorized wireless network that could be used to intercept or manipulate network traffic, compromise security, or launch attacks. Disconnecting the Wi-Fi would prevent further exposure or damage to the user's device or data. Restarting the wireless adapter, launching the browser, or running the antivirus software are possible actions to take after disconnecting the Wi-Fi, but they are not as urgent or effective as the first step. References:
* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 22
* CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 456

最新問題**: 338**
MDM レポートによると、ユーザーの会社の携帯電話に許可されていないアプリケーションがインストールされていることが示されています。デバイスは最近 MDM サーバーにチェックインされており、会社側はまだデバイスをリモートで消去する権限を持っています。
ユーザーが実行したアクションを説明するものは次のどれですか?
A. ルートアクセスを取得しました
B. OSをアップグレードしました
C. VPNをインストールしました
D. MDMソフトウェアをアンインストールしました
Answer: A (メーッセージを残す**)**
Comprehensive and Detailed In-Depth Explanation:If an MDM (Mobile Device Management) solution detects unauthorized applications, it is likely that the user has rooted (Android) or jailbroken (iOS) the device to bypass security restrictions. Root access allows the user to install unauthorized applications that MDM policies would normally block.
* B. Upgraded the OS - Incorrect. Upgrading the OS does not bypass security policies or allow unauthorized apps.
* C. Installed a VPN - Incorrect. A VPN does not affect the MDM system or allow unauthorized apps.
* D. Uninstalled the MDM software - Incorrect. If the MDM software was removed, the device would not still be reporting to the MDM server.
Reference:
CompTIA A+ 220-1102, Objective 2.7 - Mobile Device Security and MDM

最新問題**: 339**
技術者は Windows ラップトップに開発者モードをインストールしたいと考えていますが、「パッケージのインストールに失敗しました」というメッセージが表示されます。技術者が最初に行うべきことは次のうちどれですか?
A. インターネット接続を確認します。
B. Windows アップデートを確認します。
C. SSHを有効にします。
D. コンピュータを再起動します。
Answer: B (メーッセージを残す**)**
Developer Mode on Windows 10 is a feature that allows developers to test and debug their applications on their devices, as well as sideload apps and access other developer tools12. To enable Developer Mode, the user needs to go to the Settings app, select Update & Security, choose For Developers, and switch to Developer Mode123. However, enabling Developer Mode requires internet connectivity, as Windows will download and install a package of features, such as Windows Device Portal and SSH services, that are necessary for Developer Mode124. If the user does not have internet connectivity, they will receive a "failed to install package" message when trying to enable Developer Mode4. Therefore, the first thing that the technician should do is to ensure that the laptop has internet access, either through Wi-Fi or Ethernet, and then try to enable Developer Mode again4

最新問題**: 340**

次の種類の悪意のあるソフトウェアのうち、暗号通貨での支払いを要求する可能性が最も高いのはどれですか?
A. ランサムウェア
B. キーロガー
C. 暗号通貨マイニング
D. ルートキット
Answer: A (メーッセージを残す)
Comprehensive and Detailed In-Depth Explanation:Ransomware is a type of malware that encrypts files and demands payment (usually in cryptocurrency) to decrypt them.
* B. Keylogger - Tracks keystrokes but does not demand payment.
* C. Cryptomining - Uses system resources to mine cryptocurrency without the user's consent.
* D. Rootkit - Hides malicious software but does not demand payment.
Reference:
CompTIA A+ 220-1102, Objective 2.5 - Common Security Threats

最新問題**: 341**
技術者は、Windows 10 マシン上のプログラムが起動時に読み込まれるが起動時間が長すぎるという問題のトラブルシューティングを行っています。プログラムのロードを選択的に防止するために技術者が行うべきことは、次のうちどれですか?
A. Windows ボタンを右クリックし、[実行] を選択してシェル スタートアップに入り、[OK] をクリックしてから、項目を 1 つずつごみ箱に移動します。
B. HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows>CurrentVersion>Run
C. 現在有効としてリストされているすべてのスタートアップ タスクを手動で無効にし、起動時に問題解決のために再起動チェックを行います。
D. [スタートアップ] タブを開き、現在有効としてリストされている項目を系統的に無効にして再起動し、起動するたびに問題の解決を確認します。
Answer: D (メーッセージを残す)
This is the most effective way to selectively prevent programs from loading on a Windows 10 machine. The Startup tab can be accessed by opening Task Manager and then selecting the Startup tab. From there, the technician can methodically disable items that are currently listed as enabled, reboot the machine, and check for issue resolution at each startup. If the issue persists, the technician can then move on to disabling the next item on the list.

最新問題**: 342**
ユーザーは、Windows OS からデスクトップ データをバックアップするための推奨事項を技術者に尋ねます。技術者は毎日の完全バックアップの実装を推奨しますが、ユーザーは十分なスペースがあるかどうかを懸念しています。技術者は次のどの追加のバックアップ方法を推奨する必要がありますか。
A. トランザクションログ
B. 増分
C. 合成
D. 差分
Answer: (解答を表示する)
Detailed Explanation with Core 2 References:Incremental backups only save changes made since the last backup, significantly reducing storage space requirements compared to full backups. This approach is consistent with the Core 2 objective of understanding various backup methods and their space requirements (Core 2 Objective 4.3).

最新問題**: 343**
次のプロトコルのうち、ネットワーク間の高速ローミングをサポートしているものはどれですか?
A. WEP
B. WPA
C. WPA2

D. LEAP
E. PEAP
Answer: C (メッセージを残す**)**
WPA2 is the only protocol among the options that supports fast roaming between networks. Fast roaming, also known as IEEE 802.11r or Fast BSS Transition (FT), enables a client device to roam quickly in environments implementing WPA2 Enterprise security, by ensuring that the client device does not need to re-authenticate to the RADIUS server every time it roams from one access point to another1. WEP, WPA, LEAP, and PEAP do not support fast roaming and require the client device to perform the full authentication process every time it roams, which can cause delays and interruptions in the network service.
References:
The Official CompTIA A+ Core 2 Study Guide2, page 263.
WiFi Fast Roaming, Simplified3

最新問題**: 344**
技術者が社内のすべてのワークステーションのデフォルトのホームページを変更しています。この変更の実装に役立つのは次のうちどれですか?
A. グループポリシー
B. ブラウザ拡張機能
C. システム構成
D. タスクスケジューラ
Answer: A (メッセージを残す**)**
Group Policy is a feature of Windows that allows administrators to centrally manage and configure the settings of computers and users in a domain network. Group Policy can be used to modify the default home page of all the workstations in a company by creating and applying a policy that specifies the desired URL for the home page. This way, the change will be automatically applied to all the workstations that are joined to the domain and receive the policy.

最新問題**: 345**
ユーザーがヘルプ デスクに電話して、コンピューター上のマルウェアの可能性を報告します。ユーザーが最近の電子メールで無料のギフト カードへのリンクをクリックした後、異常なアクティビティが開始されました。技術者は、パフォーマンスの低下、過剰なポップアップ、ブラウザのリダイレクトなど、異常なアクティビティについて説明するようユーザーに求めます。技術者が次に行うべきことは次のうちどれですか?
A. OS マルウェア対策アプリケーションを使用して完全なシステム スキャンを実行するようユーザーにアドバイスします。
B. マシンをセーフ モードで再起動し、異常なアクティビティがまだ存在するかどうかを確認するようにユーザーをガイドします。
C. ユーザーに最近インストールされたアプリケーションを確認してもらい、電子メールのリンクをクリックしてからインストールされたアプリケーションの概要を説明します。
D. ユーザーに、企業ネットワークへのイーサネット接続を切断するように指示します。
Answer: (解答を表示する**)**
First thing you want to do is quarantine/disconnect the affected system from the network so whatever malicious software doesn't spread.

最新問題**: 346**
技術者が新しい Windows ラップトップを構成しています 企業ポリシーでは、モバイル デバイスは常にフル ディスク暗号化を使用する必要があります。技術者は次の暗号化ソリューションのうちどれを選択する必要がありますか?
A. 暗号化ファイル システム
B. ファイルボルト
C. ビットロッカー
D. 暗号化された LVM
Answer: A (メッセージを残す**)**
The encryption solution that the technician should choose when configuring a new Windows laptop and corporate policy requires that mobile devices make use of full disk encryption at all times is BitLocker.

This is because BitLocker is a full-disk encryption feature that encrypts all data on a hard drive and is included with Window

最新問題**: 347**
Windows 10 コンピューターに更新プログラムがインストールされず、手動による更新プログラムのインストール中もエラーが発生し続けます。問題を解決するために技術者が行うべきことは次のうちどれですか? (2 つ選択してください)。
A. Windows Update ユーティリティが最新バージョンであることを確認します。
B. コンピューター上のローカル WSUS 設定を更新します。
C. Windows Update キャッシュを削除します。
D. システム チェックを実行してシステム ファイルを確認します。
E. ユーザー ファイルを保持したままオペレーティング システムを再イメージ化します。
F. WMI をリセットし、システム .dll を再登録します。
Answer: B,C (メーッセージを残す**)**
Refreshing local Windows Server Update Services (WSUS) settings and deleting the Windows Update cache are effective steps in resolving issues with Windows 10 not installing updates. These actions help in rectifying any corrupt update files and ensuring that the workstation is properly communicating with the update servers, which can resolve errors during manual and automatic update installations.

最新問題**: 348**
システム管理者は、オフラインになったハイパーバイザーにアクセスする必要があります。ポート スキャンを実行した後、管理者は会社のポリシーによって RDP のデフォルト ポートがブロックされていることに気付きました。管理者は、マシンにアクセスするために次のどのポートを使用する必要がありますか。
A. 22
B. 23
C. 80
D. 3090
Answer: A (メーッセージを残す**)**
When a systems administrator needs to access a hypervisor and the default RDP port (3389) is blocked by company policy, the administrator can use an alternative method. One common alternative is using SSH:
* Port 22: This is the default port for SSH (Secure Shell), which is commonly used for secure remote access to servers and hypervisors, especially in Unix/Linux environments.
* Port 23: This is the default port for Telnet, which is an unsecured protocol and generally not recommended for remote access due to security concerns.
* Port 80: This is the default port for HTTP, used for web traffic, not remote access.
* Port 3090: This is not a standard port for remote access protocols.
Using SSH (port 22) is a secure and widely accepted method for remote management of servers and hypervisors.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.6: Compare and contrast network services and protocols.
SSH and remote access documentation.

最新問題**: 349**

技術者は、操作エリア内で頻繁に発生するマイクロ停電を軽減しようとしています。停止は通常短時間で、最長でも 5 分間続きます。この問題を軽減するために、技術者は次のうちどれを使用する必要がありますか?

A. サージキラー
B. バッテリーバックアップ
C. CMOS バッテリー
D. 発電機バックアップ

Answer: B (メーッセージを残す)

A battery backup, also known as an uninterruptible power supply (UPS), is a device that provides backup power during a power outage. When the power goes out, the battery backup provides a short amount of time (usually a few minutes up to an hour, depending on the capacity of the device) to save any work and safely shut down the equipment.

最新問題**: 350**

下級管理者は、組織内の大規模なコンピューター グループにソフトウェアを展開する責任があります。管理者は、人気のあるコーディング Web サイトでこの配布を自動化するスクリプトを見つけましたが、スクリプト言語を理解していません。このスクリプトを実行する際のリスクを最もよく説明しているのは、次のうちどれですか?

A. ソフトウェア会社の指示に従っていない。
B. セキュリティ コントロールは、自動展開をマルウェアとして扱います。
C. 展開スクリプトが不明なアクションを実行しています。
D. インターネットからスクリプトをコピーすることは、剽窃と見なされます。

Answer: (解答を表示する)

The risks in running this script are that the deployment script is performing unknown actions. Running the script blindly could cause unintended actions, such as deploying malware or deleting important files, which could negatively impact the organization's network and data1.

最新問題**: 351**

FAT に代わって Microsoft Windows OS の優先ファイルシステムとなったのは、次のファイルシステムのうちどれですか?

A. APFS
B. FAT32
C. NTFS
D. ext4

Answer: (解答を表示する)

NTFS stands for New Technology File System and it is the preferred filesystem for Microsoft Windows OS since Windows NT 3.1 in 19931. NTFS replaced FAT (File Allocation Table) as the default filesystem for Windows because it offers many advantages over FAT, such as:

* Support for larger volumes and files (up to 16 exabytes)2
* Support for file compression, encryption, and permissions2
* Support for journaling, which records changes to the filesystem and helps recover from errors2
* Support for hard links, symbolic links, and mount points2
* Support for long filenames and Unicode characters2

FAT32 is an improved version of FAT that supports larger volumes and files (up to 32 GB and 4 GB respectively) and is compatible with older versions of Windows and other operating systems3. However, FAT32 still has many limitations and drawbacks compared to NTFS, such as:

* No support for file compression, encryption, and permissions3
* No support for journaling, which makes it vulnerable to corruption and data loss3
* No support for hard links, symbolic links, and mount points3
* No support for long filenames and Unicode characters3

APFS (Apple File System) is the default filesystem for macOS, iOS, iPadOS, watchOS, and tvOS since
20174. APFS replaced HFS+ (Hierarchical File System Plus) as the preferred filesystem for Apple devices because it offers many advantages over HFS+, such as:
* Support for larger volumes and files (up to 8 zettabytes)4
* Support for file cloning, snapshots, and encryption4
* Support for space sharing, which allows multiple volumes to share the same storage pool4
* Support for fast directory sizing, which improves performance and efficiency4 ext4 (Fourth Extended Filesystem) is the default filesystem for most Linux distributions since 20085. ext4 replaced ext3 as the preferred filesystem for Linux because it offers many advantages over ext3, such as:
* Support for larger volumes and files (up to 1 exabyte and 16 terabytes respectively)5
* Support for extents, which reduce fragmentation and improve performance5
* Support for journal checksumming, which improves reliability and reduces recovery time5
* Support for delayed allocation, which improves efficiency and reduces metadata overhead5 References:
1: NTFS - Wikipedia 2: [NTFS vs FAT32 vs exFAT: What's the Difference?] 3: [FAT32 - Wikipedia] 4:
[Apple File System - Wikipedia] 5: [ext4 - Wikipedia] : NTFS vs FAT32 vs exFAT: What's the Difference? :
FAT32 - Wikipedia : Apple File System - Wikipedia : ext4 - Wikipedia

最新問題**: 352**
技術者がラックマウント UPS を交換しています。技術者は次のどれを考慮する必要がありますか?
A. 圧縮空気の可用性の判断
B. ハードウェアを持ち上げる際に支援を受ける
C. 地域の低電圧規制の確認
D. 消火システムのテスト
Answer: B (メーッセージを残す**)**
Detailed Explanation with Core 2 References:Rack-mounted UPS units are often heavy, so technicians should seek assistance to lift them to avoid injury, following safety procedures. Core 2 includes handling hardware safely as part of best practices (Core 2 Objective 4.4).

最新問題**: 353**
新しいアプリケーションを企業に展開する際、技術者は、管理するライセンスの数を減らしながら、アプリケーションの EULA への準拠を検証する必要があります。この目的を達成するのに最も適したライセンスは次のうちどれですか?
A. 個人使用ライセンス
B. 法人利用ライセンス
C. オープンソースライセンス
D. 無期限ライセンス
Answer: (解答を表示する**)**
A corporate use license, also known as a volume license, is a type of software license that allows an organization to purchase and use multiple copies of a software product with a single license key. A corporate use license can help validate compliance with an application's EULA (end-user license agreement), which is a legal contract that defines the terms and conditions of using the software. A corporate use license can also reduce the number of licenses to manage, as it eliminates the need to activate and track individual licenses for each copy of the software. Personal use license, open-source license, and non-expiring license are not types of licenses that can best accomplish this goal.

最新問題**: 354**
ユーザーは、Windows コマンド ラインを介してドライブをマップする必要があります。ドライブのマッピングに使用できるコマンドライン ツールは次のうちどれですか?
A. gpupdate

B. 純使用量
C. ホスト名
D. ディレクトリ
Answer: B (メーッセージを残す**)**
Net use is a command-line tool that can be used to map a drive in Windows. Mapping a drive means assigning a drive letter to a network location or a local folder, which allows the user to access it more easily and quickly. Net use can also be used to disconnect a mapped drive, display information about mapped drives, or connect to shared resources on another computer. Gpupdate, hostname, and dir are not command-line tools that can be used to map a drive.

最新問題**: 355**
複数のコンピュータがマルウェアに感染し、会社のネットワークの速度が低下し、会社の機密情報が失われました。IT 部門はマルウェアを削除するために新しいウイルス対策ソフトウェアをインストールし、将来のマルウェア感染を防ぐための最善の方法を決定する必要があります。次の方法のうち、最も効果的なものはどれですか。
A. 保存データの暗号化
B. ファイアウォールの実装
C. 侵入検知システムの活用
D. 定期的にデータをバックアップする
Answer: C (メーッセージを残す**)**
Detailed Explanation with Core 2 References:Intrusion Detection Systems (IDS) monitor network traffic for malicious activities and alert administrators, helping to prevent malware infections before they can impact the network significantly. CompTIA Core 2 emphasizes the importance of implementing preventive measures like IDS to proactively detect and respond to potential threats (Core 2 Objective 2.3).

最新問題**: 356**
次のうち、macOS のデフォルトの GUI とファイル マネージャーはどれですか?
A. ディスクユーティリティ
B. ファインダー
C. ドック
D. ファイルボルト
Answer: B (メーッセージを残す**)**
Finder is the default GUI and file manager in macOS. Finder is an application that allows users to access and manage files and folders on their Mac computers. Finder also provides features such as Quick Look, Spotlight, AirDrop and iCloud Drive. Finder uses a graphical user interface that consists of icons, menus, toolbars and windows to display and interact with files and folders. Disk Utility is a utility that allows users to view and manage disk drives and partitions on their Mac computers. Disk Utility is not a GUI or a file manager but a disk management tool. Dock is a feature that allows users to access and launch applications on their Mac computers. Dock is not a GUI or a file manager but an application launcher. FileVault is a feature that allows users to encrypt and protect their data on their Mac computers. FileVault is not a GUI or a file manager but an encryption tool. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

最新問題**: 357**
技術者が、ログインの期待事項を詳しく説明する Windows スプラッシュ スクリーンを作成しています。技術者が最も使用すべきは次のうちどれですか。
A. エンドユーザー使用許諾契約
B. 秘密保持契約
C. 規制遵守
D. 利用規定
Answer: D (メーッセージを残す**)**
The appropriate choice is "Acceptable Use Policy" (Option D). This policy defines the rules for how users should use the system, including login expectations and proper behavior when using company resources. It's typically displayed as a splash screen to remind users of their responsibilities.

* End-user license agreement (Option A) pertains to the terms of software usage.
* Non-disclosure agreement (Option B) deals with confidentiality but is unrelated to login behavior.
* Regulatory compliance (Option C) relates to adherence to laws and regulations, but it is not typically displayed on a splash screen for login expectations.
CompTIA A+ Core 2 References:
* 4.6 - Explain the importance of prohibited content/activity and acceptable use policies.

最新問題**: 358**
次の Wi-Fi プロトコルのうち、最も安全なのはどれですか?
A. WPA3
B. WPA-AES
C. WEP
D. WPA-TKIP
Answer: (解答を表示する**)**
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

最新問題**: 359**
次のコマンドライン ツールのうち、ディレクトリを削除するのはどれですか?
A. md
B. デル
C. ディレクトリ
D. rd
E. cd
Answer: D (メーッセージを残す**)**
To delete an empty directory, enter rd Directory or rmdir Directory . If the directory is not empty, you can remove files and subdirectories from it using the /s switch. You can also use the /q switch to suppress confirmation messages (quiet mode).

最新問題**: 360**
ある企業は、事業の環境への悪影響を軽減したいと考えており、機器の廃棄のために電子廃棄物処理会社を雇うことにしました。電子廃棄物処理会社は、次のどれを企業に提供すべきでしょうか。
A. 秘密保持契約
B. 破棄の証明
C. 低レベルのフォーマット
D. 破砕/掘削
Answer: B (メーッセージを残す**)**
When disposing of e-waste, it is important to ensure that the data on the equipment is securely destroyed and that the disposal process complies with environmental regulations.
* Non-disclosure agreement: Relates to confidentiality, not disposal.
* Certification of destruction: The correct document verifying that the equipment has been disposed of in accordance with regulations and standards, ensuring data is irretrievably destroyed.
* Low-level formatting: A method to wipe data but does not guarantee compliance with e-waste disposal regulations.
* Shredding/drilling: Physical destruction methods that might be used, but certification of destruction is the documentation needed.
Reference: CompTIA A+ Exam Objectives [220-1102] - 3.7: Explain the importance of physical security measures.

最新問題**: 361**

会社所有のモバイル デバイスに大量の広告が表示され、データ使用量制限の通知が届き、応答が遅くなっています。技術者がデバイスをチェックしたところ、デバイスがジェイルブレイクされていることに気付きました。技術者は次に次のどれを行うべきでしょうか。
* ウイルス対策を実行し、暗号化を有効にします。
A. デフォルトを復元し、企業の OS を再イメージ化します。
B. ファイルをバックアップし、システムを復元します。
C. ジェイルブレイクを元に戻し、ウイルス対策を有効にします。
Answer: (解答を表示する**)**
The best course of action for the technician is to restore the defaults and reimage the corporate OS on the device. This will remove the jailbreak and any unauthorized or malicious apps that may have been installed on the device, as well as restore the security features and policies that the company has set for its devices. This will also ensure that the device can receive the latest updates and patches from the manufacturer and the company, and prevent any data leakage or compromise from the device.
Jailbreaking is a process of bypassing the built-in security features of a device to install software other than what the manufacturer has made available for that device1. Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features1. However, jailbreaking also exposes the device to various risks, such as:
* The loss of warranty from the device manufacturers2.
* Inability to update software until a jailbroken version becomes available2.
* Increased security vulnerabilities32.
* Decreased battery life2.
* Increased volatility of the device2.
Some of the signs of a jailbroken device are:
* A high number of ads, which may indicate the presence of adware or spyware on the device3.
* Receiving data-usage limit notifications, which may indicate the device is sending or receiving data in the background without the user's knowledge or consent3.
* Experiencing slow response, which may indicate the device is running unauthorized or malicious apps that consume resources or interfere with the normal functioning of the device3.
* Finding apps or icons that the user did not install or recognize, such as Cydia, which is a storefront for jailbroken iOS devices1.
The other options are not sufficient or appropriate for dealing with a jailbroken device. Running an antivirus and enabling encryption may not detect or remove all the threats or vulnerabilities that the jailbreak has introduced, and may not restore the device to its original state or functionality. Backing up the files and doing a system restore may not erase the jailbreak or the unauthorized apps, and may also backup the infected or compromised files. Undoing the jailbreak and enabling an antivirus may not be possible or effective, as the jailbreak may prevent the device from updating or installing security software, and may also leave traces of the jailbreak or the unauthorized apps on the device.
References:
* CompTIA A+ Certification Exam Core 2 Objectives4
* CompTIA A+ Core 2 (220-1102) Certification Study Guide5
* What is Jailbreaking & Is it safe? - Kaspersky1
* Is Jailbreaking Safe? The ethics, risks and rewards involved - Comparitech3
* Jailbreaking : Security risks and moving past them2

最新問題: 362
技術者が、SOHO ルーターをお持ちの顧客のためにネットワーク プリンターをセットアップしています。技術者は、プリンタが今後も接続された状態を維持し、家内のすべてのコンピュータで利用できるよ

うにしたいと考えています。技術者がプリンタで設定すべきものは次のうちどれですか?
A. DNS 設定
B. 静的 IP
C. WWAN
D. 従量制課金接続
Answer: B (メーッセージを残す)
Configuring a static IP address for a network printer in a SOHO (Small Office/Home Office) environment ensures that the printer maintains the same IP address over time. This consistency is crucial for networked devices like printers, as computers and other devices rely on this specific address to connect to the printer. If the printer's IP address were to change (as it might with DHCP), devices would no longer be able to communicate with it without reconfiguration.
* Static IP: Assigning a static IP address to the printer ensures it always uses the same IP, making it reliably accessible to all computers in the house regardless of network changes or router reboots.
DNS settings (A) are generally not necessary to configure directly on most network printers unless you're dealing with advanced network configurations or using the printer for scanning to email functions.
WWAN (C) stands for Wireless Wide Area Network, which is not typically relevant for a standard network printer setup in a home or small office. Metered connection (D) is a Windows feature that helps reduce data usage on a connection, it's not relevant to configuring a printer's network settings.

最新問題**: 363**
Windows 10 アクション センターで、一見悪意がないと思われるランダムな広告通知が表示されるとユーザーが報告しています。通知は、広告が Web ブラウザから送信されていることを示します。技術者が実装するのに最適なソリューションは次のうちどれですか?
A. ブラウザーがアクション センターに通知を送信できないようにします。
B. コンピュータで完全なウイルス対策スキャンを実行します。
C. アクション センターの通知をすべて無効にします。
D. 特定のサイトの通知を 許可」から ブロック」に移動します。
Answer: (解答を表示する)
The best solution for a technician to implement is to disable the browser from sending notifications to the Action Center. This will prevent the random advertisement notifications from appearing in the Windows 10 Action Center, which can be annoying and distracting for the user. The technician can follow these steps to disable the browser notifications1:
Open the browser that is sending the notifications, such as Microsoft Edge, Google Chrome, or Mozilla Firefox.
Go to the browser settings or options menu, and look for the privacy and security section.
Find the option to manage site permissions or notifications, and click on it.
You will see a list of sites that are allowed or blocked from sending notifications to the browser and the Action Center. You can either block all sites from sending notifications, or select specific sites that you want to block or allow.
Save the changes and close the browser settings.
This solution is better than the other options because:
Running a full antivirus scan on the computer (B) is not necessary, as the advertisement notifications are not malicious or harmful, and they are not caused by a virus or malware infection. Running a scan will not stop the notifications from appearing, and it will consume system resources and time.
Disabling all Action Center notifications is not advisable, as the Action Center is a useful feature that shows notifications and alerts from various apps and system events, such as email, calendar, security, updates, etc. Disabling all notifications will make the user miss important information and reminders, and reduce the functionality of the Action Center.
Moving specific site notifications from Allowed to Block (D) is not the best solution, as it will only stop the notifications from some sites, but not from others. The user may still receive advertisement notifications from other sites that are not blocked, or from new sites that are added to the Allowed list. This solution will also require the user to manually manage the list of sites, which can be tedious and time-consuming.
References:
1: How to Disable Annoying Browser Notifications - PCMag

最新問題: **364**
ある会社は、複数の地理的な場所から多数のコンピューターが非常に多数の接続要求を送信していることを発見しました。これにより、会社の Web サーバーが一般に利用できなくなります。発生している攻撃は次のうちどれですか?
A. ゼロデイ
B. SOL 注入
C. クロスサイト スクリプティング
D. 分散型サービス拒否
Answer: (解答を表示する**)**
The company is experiencing a distributed denial of service (DDoS) attack. A DDoS attack is a type of cyber attack in which multiple compromised systems are used to target a single system, causing a denial of service for users of the targeted system.

最新問題: **365**
スマートフォンで使用されているモバイル オペレーティング システムは次のうちどれですか? (2 つ選択してください)。
A. macOS
B. Windows
C. Chrome OS
D. Linux
E. iOS
F. Android
Answer: E,F (メーッセージを残す**)**
iOS and Android are the two most popular and widely used mobile operating systems for smartphones. They are both based on Unix-like kernels and provide a variety of features and applications for users and developers. iOS is developed by Apple and runs exclusively on Apple devices, such as iPhones and iPads.
Android is developed by Google and runs on a range of devices from different manufacturers, such as Samsung, Huawei, and Motorola. The other options are not mobile operating systems for smartphones, but rather for other types of devices or platforms. macOS is a desktop operating system for Apple computers, such as MacBooks and iMacs. Windows is a desktop operating system for Microsoft computers, such as Surface and Dell. Chrome OS is a web-based operating system for Google devices, such as Chromebooks and Chromecast. Linux is a family of open-source operating systems for various devices and platforms, such as Ubuntu, Fedora, and Raspberry Pi.

最新問題: **366**
技術者がマルウェア対策の削除ツールを使用して、企業のラップトップでユーザーのマルウェアの問題を解決しました。次のうち、技術者がラップトップをユーザーに返却する前に行うべきことを最もよく説明しているのはどれですか?
A. マルウェアの削除についてユーザーを教育します。
B. ラップトップ OS を再インストールする方法をユーザーに説明します。
C. リカバリ モードにアクセスする方法をユーザーに説明します。
D. 一般的な脅威とその回避方法についてユーザーを教育します。
Answer: (解答を表示する**)**
educating the user on common threats and how to avoid them (D) would be a good step before returning the laptop to the user. This can help prevent similar issues from happening again.

最新問題: **367**
技術者は、ハリケーンが頻繁に発生し、送電網が不安定な地域のサイトのバックアップ ソリューションをアップグレードする方法について、推奨事項を提供する必要があります。技術者が実装を推奨する必要があるのは、次のうちどれですか?
A. 高可用性

B. 地域ごとに異なるバックアップ
C. オンサイトバックアップ
D. 増分バックアップ
Answer: B (メーッセージを残す**)**
Regionally diverse backups are backups that are stored in different geographic locations, preferably far away from the primary site1. This way, if a disaster such as a hurricane or a power outage affects one location, the backups in another location will still be available and accessible2. Regionally diverse backups can help ensure business continuity and data recovery in case of a disaster3. The other options are not the best backup solutions for a site in an area that has frequent hurricanes and an unstable power grid. High availability is a feature that allows a system to remain operational and accessible even if one or more components fail, but it does not protect against data loss or corruption4. On-site backups are backups that are stored in the same location as the primary site, which means they are vulnerable to the same disasters that can affect the primary site. Incremental backups are backups that only store the changes made since the last backup, which means they require less storage space and bandwidth, but they also depend on previous backups to restore data and may not be sufficient for disaster recovery.

最新問題**: 368**
次のうち、macOS でパスワード マネージャーとして使用されているものはどれですか?
A. ターミナル
B. ファイルボルト
C. プライバシー
D. キーホルダー
Answer: D (メーッセージを残す**)**
Keychain is a feature of macOS that securely stores passwords, account numbers, and other confidential information for your Mac, apps, servers, and websites1. You can use the Keychain Access app on your Mac to view and manage your keychains and the items stored in them1. Keychain can also sync your passwords and other secure information across your devices using iCloud Keychain1. Keychain can be used as a password manager in macOS to help you keep track of and protect your passwords.
References: 1: Manage passwords using keychains on Mac (https://support.apple.com/guide/mac-help/use- keychains-to-store-passwords-mchlf375f392/mac)

最新問題**: 369**
次の方法のうち、ハードドライブ上のファイルを表面的に削除する方法はどれですか?
A. 掘削
B. 消磁
C. ワイプ
D. シュレッディング
E. 低レベルフォーマット
Answer: A (メーッセージを残す**)**
Drilling is a method of physically damaging the hard drive by drilling holes through it, which renders the drive inoperable. However, it is not a secure method for ensuring data cannot be recovered. Methods such as wiping or degaussing are more secure.
Reference: CompTIA A+ 220-1102 Exam Objectives, Domain 2.8 Security - Data Destruction

最新問題**: 370**
部門には、新しいアプリケーションに対して次の技術的要件があります。

```
Quad Core processor
250GB of hard drive space
6GB of RAM
Touch screens
```

同社は、32 ビット Windows OS から 64 ビット OS へのアップグレードを計画しています。アップグレード後に会社が十分に活用できるのは、次のうちどれですか?
A. CPU

B. ハードドライブ
C. ラム
D. タッチスクリーン
Answer: C (メーッセージを残す**)**
https://www.makeuseof.com/tag/difference-32-bit-64-bit-windows/
After upgrading from a 32-bit Windows OS to a 64-bit OS, the company will be able to fully take advantage of the RAM of the computer. This is because a 64-bit operating system is able to use larger amounts of RAM compared to a 32-bit operating system, which may benefit the system's overall performance if it has more than 4GB of RAM installed

最新問題**: 371**
変更諮問委員会が変更要求を承認しました。変更プロセスの次のステップとして最も可能性が高いのは次のうちどれですか?
A. エンド ユーザーの承認
B. リスク分析の実行
C. 利害関係者とのコミュニケーション
D. サンドボックス テスト
Answer: C (メーッセージを残す**)**
The risk analysis should be performed before it's taken to the board. The step after the board approves the change is End User Agreenment Reference: https://www.youtube.com/watch?v=Ru77iZxuElA&list=PLG49S3nxzAnna96gzhJrzkii4hH_mgW4b&index=59

最新問題**: 372**
ユーザーが会社支給のスマートフォンを使用してメールを開こうとすると、メールが暗号化されているため開けないことを示すメッセージが表示されます。ユーザーは電子メールを個人アカウントに転送し、同じメッセージを受け取ります。その後、ユーザーは IT 部門に連絡して支援を求めます。技術者は、メッセージを解読するために送信者に連絡して情報を交換するようにユーザーに指示します。ユーザーは送信者から次のどれを受け取りますか?
A. キー
B. トークン
C. パスワード
D. ルートCA
Answer: A (メーッセージを残す**)**
When an email is encrypted and the recipient cannot open it, the issue typically revolves around the need for encryption keys. Encryption keys are used to encode and decode the email content, ensuring that only authorized recipients with the correct key can access the information. In this scenario, the user would need to receive the appropriate decryption key from the sender to unlock and read the encrypted email. This exchange ensures that sensitive information remains secure during transmission and is only accessible to intended recipients.

最新問題**: 373**
隣人がユーザーの Wi-Fi ネットワークに正常に接続しました。隣人が再び接続できないようにするためにネットワーク構成を変更した後、ユーザーは次のうちどれを実行する必要がありますか?
A. SSID ブロードキャストを無効にします。
B. 暗号化設定を無効にします。
C. DHCP 予約を無効にします。
D. ロギングを無効にします。
Answer: (解答を表示する**)**
A: Disable the SSID broadcast1: The SSID broadcast is a feature that allows a Wi-Fi network to be visible to nearby devices. Disabling the SSID broadcast can make the network harder to find by unauthorized users, but it does not prevent them from accessing it if they know the network name and password.

最新問題: **374**
次のファイルシステムのうち、ジャーナリングをサポートしているのはどれですか?
A. NTFS
B. exFAT
C. HFS
D. 内線2
Answer: (解答を表示する**)**
Journaling is a feature that helps maintain the integrity of the filesystem by keeping a record of changes not yet committed to the main file system. This feature is supported by various filesystems, but not all.
* Option A: NTFSNTFS (New Technology File System) is a filesystem used by Windows that supports journaling. This makes it resilient to corruption from unexpected shutdowns or crashes by keeping a log of file changes.
* Option B: exFATexFAT (Extended File Allocation Table) does not support journaling. It is optimized for flash drives and large files but lacks advanced features like journaling.
* Option C: HFSHFS (Hierarchical File System) is an older filesystem used by Apple. HFS+ (also known as Mac OS Extended) supports journaling, but HFS itself does not.
* Option D: ext2ext2 (Second Extended File System) is a filesystem for Linux that does not support journaling. Its successor, ext3, introduced journaling.
References:
* CompTIA A+ 220-1102 Objective 1.8 (Explain common OS types and their purposes), particularly filesystems and their features.

最新問題: **375**
技術者は、ユーザーの PC に「OS が見つかりません」というエラー メッセージが表示されていることを発見しました。技術者は次にどの手順を実行する必要がありますか?
A. 外部ストレージを取り外し、PC を再起動します。
B. SSD を交換し、ディスク デフラグを実行します。
C. セーフモードで起動し、最新のセキュリティ更新プログラムをロールバックします。
D. 個人データをバックアップし、ユーザー プロファイルを再構築します。
Answer: (解答を表示する**)**
Detailed Explanation with Core 2 References:A "No OS found" message often occurs if the PC is trying to boot from an external storage device that does not contain an OS. Removing any external devices and rebooting can resolve this issue. This approach is part of troubleshooting boot-related problems, as emphasized in Core 2 (Core 2 Objective 3.1).

最新問題: **376**
技術者は、合計 16 GB の RAM を搭載した PC に Windows 10 のインストールを完了しました。技術者は、Windows OS で使用できる RAM が 4GB しかないことに気付きました。OS が 46B の RAM にしかアクセスできない理由を説明しているのは、次のうちどれですか?
A. UEFI 設定を変更する必要があります。
B. RAM には Windows 10 との互換性の問題があります。
C. 一部の RAM に欠陥があります。
D. 新規にインストールする OS は x86 です。
Answer: D (メーッセージを残す**)**
The newly installed OS is x86. The x86 version of Windows 10 can only use up to 4GB of RAM. The x64 version of Windows 10 can use up to 2TB of RAM1.

最新問題: **377**

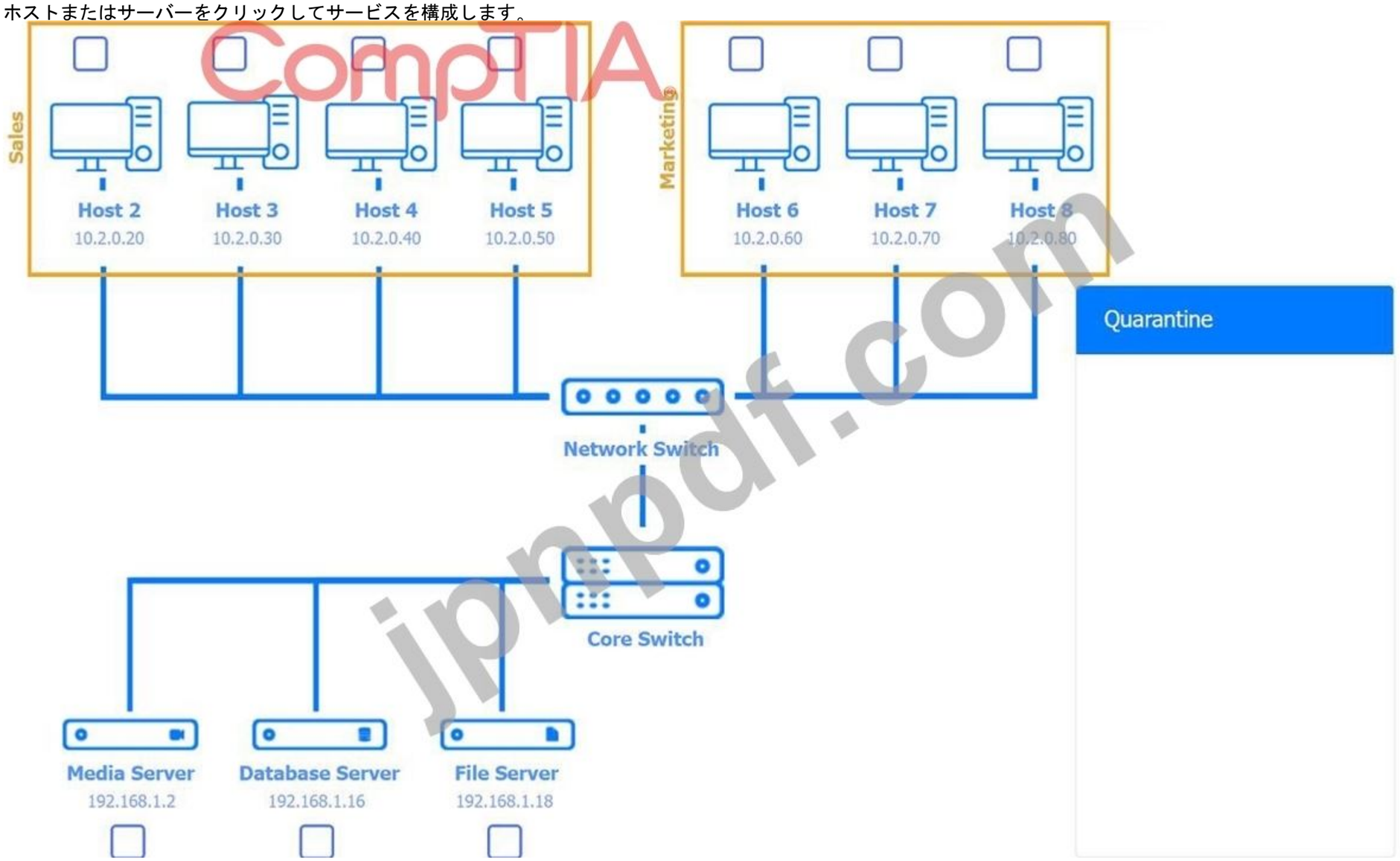
複数のユーザーから、許可されていないソフトウェアをダウンロードした後にオーディオの問題やパフォーマンスの問題が報告されています。ベスト プラクティスの手順を使用してネットワーク上の問題を特定し、解決するために派遣されました。

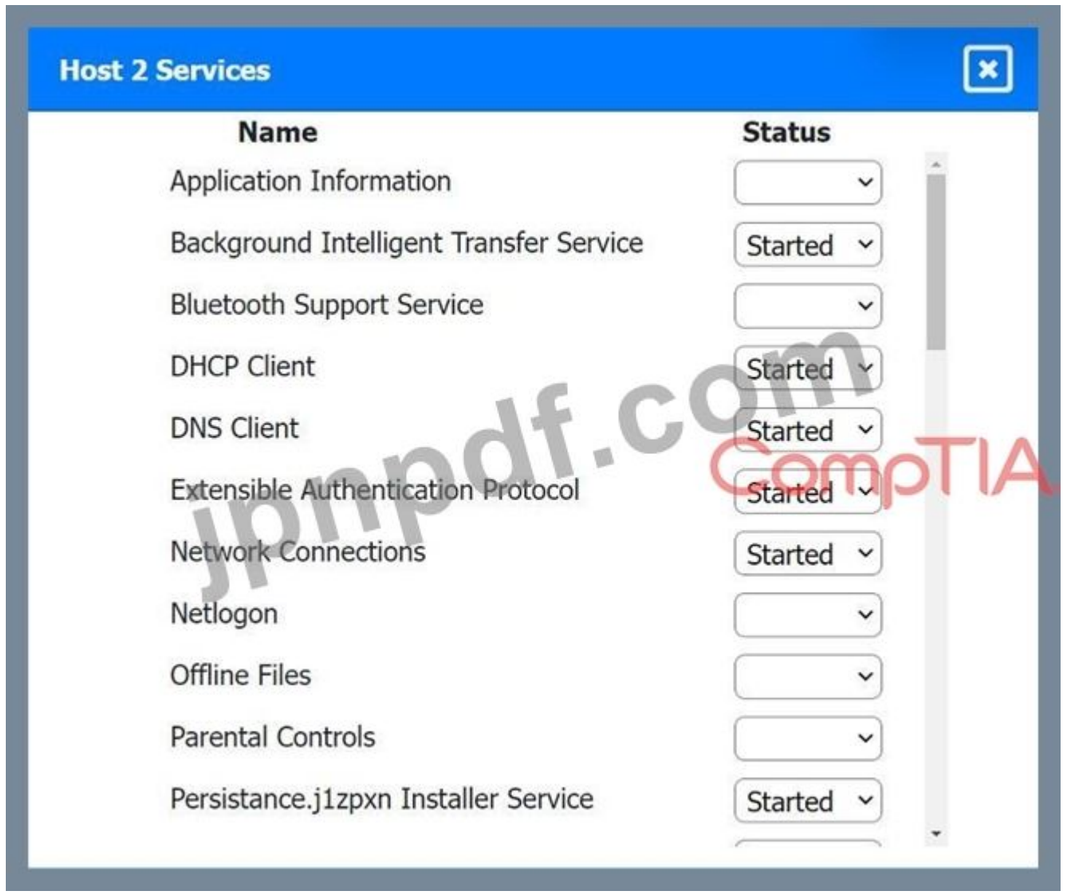
説明書

ベスト プラクティスの手順を使用してユーザーのオーディオの問題が解決されるように、適切なデバイスを隔離して構成します。

隔離対象として複数のデバイスを選択できます。

ホストまたはサーバーをクリックしてサービスを構成します。





Host 2 Services

Name	Status
Volume Shadow Copy	
Windows Audio	
Windows Backup	
Windows CardSpace	
Windows Defender	
Windows Event Log	Started
Windows Firewall	
Windows Installer	
Windows Search	Started
Windows Time	
Windows Update	Started

Answer:
See the Explanation for the solution.
Explanation:
Host 2 and Media Server put them to Quarantine.

最新問題**: 378**
技術者は、ワークステーションを使用して 3D プロモーション ムービーをレンダリングするユーザーのために、新しいデスクトップ マシンを構築しています。最も重要なコンポーネントは次のうちどれですか?
A. Dedicated GPU
B. DDR5 SODIMM
C. NVMe disk

D. 64-bit CPU
Answer: A (メーッセージを残す**)**
A dedicated GPU (graphics processing unit) is the most important component for rendering 3-D promotional movies, as it can handle the complex calculations and graphics operations required for creating realistic and high-quality images. A dedicated GPU has its own memory and processor, which are optimized for graphics tasks. A dedicated GPU can also support multiple monitors, high resolutions, and advanced features such as ray tracing12.
References: 1 What Kind of Computer Do You Need for 3D Rendering in 2021?(https://kitbash3d.com/a/blog
/best-computer-for-3d-rendering-2021)2 How to Choose the Best Hardware for a 3D Artist - GarageFarm (https://garagefarm.net/blog/how-to-choose-the-best-hardware-for-a-3d-artist).

最新問題**: 379**
技術者は、パフォーマンスが低下している PC のトラブルシューティングを行っています。タスク マネージャーを見ると、技術者は CPU とメモリ リソースは問題ないように見えますが、ディスク スループットは 100% です。
システムが感染している可能性が最も高いマルウェアの種類は次のうちどれですか?
A. キーロガー
B. ルートキット
C. ランサムウェア
D. トロイの木馬
Answer: (解答を表示する**)**
Ransomware is a type of malware that encrypts the files on the victim's computer and demands a ransom for their decryption. Ransomware can cause high disk throughput by encrypting large amounts of data in a short time.