CompTIA.220-1102J.v2025-07-01.q388

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:	388
バージョン:	v2025-07-01
アクセス数:	174
ページビュー数:	3880
https://www.jpnpdf.com/CompTIA.220-1102J.v2025-07-01.q388-mondaishu.html	

最新問題: **1**
ある企業は、ネットワークへの影響を最小限に抑えながら、システム上のすべてのデータのバックアップを提供するソリューションを探しています。次のバックアップ タイプのうち、企業が選択する可能性が最も高いのはどれですか?
A. オフサイト
B. 合成
C. フル
D. 差動
Answer: B (メーッセージを残す**)**
A synthetic backup is a backup type that provides a backup for all data on the system while providing the lowest impact to the network. It combines a full backup with one or more incremental backups to create a single backup set, without requiring access to the original data source. Off-site is a backup location, not a backup type. Full and differential are backup types, but they have a higher impact on the network than synthetic. Verified References: https://www.comptia.org/blog/what-is-a-synthetic-backup https://www.comptia.org/certifications/a

最新問題: **2**
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: 3
Fictional Company. LLC ヘルプデスク従業員としての初日へようこそ。ヘルプデスクのチケットキューにあるチケットを処理してください。
チケットの詳細を表示するには、個々のティッカーをクリックします。問題を特定するには添付ファイルを表示します。
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、解決策」ドロップダウン メニューから最も効率的な解決策を選択します。最後に、解決の確認」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、問題の修正または修正を確認します。

Answer:

Explanation:

最新問題: **4**

Windows の更新中に、技術者は 「プロセスは現在無効になっています」というエラー メッセージを受け取ります。イベントが悪意のあるものではないと仮定すると、技術者が Windows の更新を再度有効にするために使用する最適なコマンドは次のどれですか。

A. wf.msc

B. services.msc

C. msconfig.exe

D. certmgr.msc

E. psr.exe

Answer: (解答を表示する**)**

Comprehensive and Detailed In-Depth Explanation:

The services.msc command opens the Services management console in Windows, which allows users to start, stop, and configure the settings of system services. Windows Update operates as a service named "Windows Update" or "wuauserv." If this service is disabled, Windows updates cannot proceed. By accessing services.

msc, a technician can locate the Windows Update service and set its startup type to "Automatic" or manually start the service, thereby resolving the issue.

* Option A: wf.mscThis command opens the Windows Firewall with Advanced Security console, used for configuring firewall rules. It doesn't manage services.

* Option C: msconfig.exeThis System Configuration utility allows users to configure startup options and services but is not specifically designed for managing individual services like Windows Update.
* Option D: certmgr.mscThis command opens the Certificate Manager, which manages digital certificates. It doesn't control system services.
* Option E: psr.exeThe Problem Steps Recorder is a tool that records user actions to help with troubleshooting but doesn't manage services.
Reference: CompTIA A+ Core 2 (220-1102) Exam Objectives, Domain 1.5: "Given a scenario, use Microsoft operating system tools."

最新問題**: 5**
技術者が新しく組み立てたコンピューターを売りに出しています。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**)**
An unattended installation is the fastest way to install Windows 10 on a newly built computer. It uses an answer file that contains all the configuration settings and preferences for the installation, such as language, product key, partition size, etc. It does not require any user interaction or input during the installation process.
Factory reset, System Restore and in-place upgrade are not methods of installing Windows 10 on a new computer, but ways of restoring or updating an existing Windows installation. Verified References:
https://www.comptia.org/blog/what-is-an-unattended-installation
https://www.comptia.org/certifications/a

最新問題**: 6**
技術者がコマンドを実行すると、次の出力が得られます。
イーサネットアダプタ イーサネット 3:
Connection-specific DNS Suffix . :reddog.microsoft.com
Link-local IPv6 Address ..... :fe80::de3d:9283:4f00:856a%5
IPv4 Address.....:10.203.10.16
Subnet Mask ..... :255.255.255.0
Default Gateway ..... :10.203.10.1
技術者は次のコマンドのどれを使用しましたか?
A. ipconfig
B. トレース
C. だれだ
D. ネット使用

Answer: A (メーッセージを残す)
Detailed Explanation with Core 2 References:The ipconfig command displays the IP address, subnet mask, and default gateway for all network adapters in a Windows computer. This output specifically shows details about an Ethernet adapter, which is directly tied to ipconfig. According to Core 2, understanding command- line tools like ipconfig is essential for network troubleshooting (Core 2 Objective 1.2).

最新問題**: 7**
顧客は、Web サイトからダウンロードした実行可能ファイルを検証する必要があります。顧客がファイルを検証するには、次のどれを使用する必要がありますか?
A. パスワードマネージャー
B. ビットロッカー
C. ファイルボールト
D. チェックサム
E. 安全なサイト
Answer: D (メーッセージを残す)
A checksum is a cryptographic hash function (like MD5 or SHA-256) used to verify the integrity of files.
When downloading files from the internet, websites often provide the checksum value of the file so that users can ensure the file was not altered during download or corrupted. The user can generate the checksum on their local system and compare it to the one provided by the site. If they match, the file is intact and safe to use.
Other options like BitLocker or FileVault are encryption tools, and a password manager is irrelevant to file verification.
References:
CompTIA A+ 220-1102 Domain 3.5: File Integrity Checking (CompTIA) (ProfMesser)

最新問題**: 8**
承認されたシステム パッチで最近更新された Windows ワークステーションが、再起動せずにシャットダウンしました。再起動すると、技術者は、ワークステーションのルート OS フォルダーにマルウェアがあることを示すアラートに気付きます。技術者はすぐにシステムの復元を実行し、ワークステーションを再起動しますが、マルウェアは引き続き検出されます。システムに依然としてマルウェアが存在する理由を最もよく表しているのは、次のうちどれですか?
A. システム パッチにより、ウイルス対策保護とホスト ファイアウォールが無効になりました。
B. システム アップデートには、最新のマルウェア対策定義が含まれていませんでした。
C. システムの復元プロセスがマルウェアによって侵害されました。
D. システムの復元ポイントが作成される前にマルウェアがインストールされました。
Answer: (解答を表示する)
The best explanation for why the system still has malware after performing a System Restore is that the malware was installed before the system restore point was created. A system restore

point is a snapshot of the system settings and configuration at a certain point in time. A System Restore is a feature that allows users to restore their system to a previous state in case of problems or errors. However, a System Restore does not affect personal files or folders, and it may not remove malware that was already present on the system before the restore point was created. A system patch disabling the antivirus protection and host firewall may increase the risk of malware infection, but it does not explain why the malware persists after a System Restore. The system updates not including the latest anti-malware definitions may reduce the effectiveness of malware detection and removal, but it does not explain why the malware persists after a System Restore. The system restore process being compromised by the malware may prevent a successful System Restore, but it does not explain why the malware persists after a System Restore. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

最新問題**: 9**
ユーザーがプログラムやファイルを開こうとすると、Windows コンピュータのパフォーマンスが低下します。ユーザーは最近、外部 Web サイトから新しいソフトウェア プログラムをインストールしました。
さまざまな Web サイトが不正なサイトにリダイレクトされており、タスク マネージャーでは CPU 使用率が一貫して 100% であることが示されています。技術者が最初に行うべきことは次のうちどれですか?
A. 新しいプログラムをアンインストールします。
B. HOSTS ファイルを確認してください。
C. 以前のバックアップから復元します。
D. Web ブラウザ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 symptoms that the user's Windows computer is experiencing suggest that the new software program that the user installed from an external website may be malicious or incompatible with the system. The program may be consuming a lot of CPU resources, slowing down the performance of other programs and files. The program may also be altering the browser settings or the HOSTS file, causing the web redirection to an unauthorized site. The first step that the technician should do is to uninstall the new program from the Control Panel or the Settings app, and then restart the computer. This may resolve the issue and restore the normal functionality of the computer. If the problem persists, the technician may need to perform additional steps, such as scanning for malware, checking the HOSTS file, clearing the web browser cache, or restoring from a previous backup

最新問題**: 10**
技術者がオフィスに新しい Wi-Fi ソリューションを導入し、ユーザーが既存のネットワーク ログインとパスワードを使用して Wi-Fi にログインできることを確認したいと考えています。技術者は次のどの方法を使用する必要がありますか?

A. AES
B. 半径
C. TKIP
D. WPA3
Answer: B (メーッセージを残す)
RADIUS (Remote Authentication Dial-In User Service) (Option B) is a network protocol that allows users to authenticate using their network credentials, such as usernames and passwords, typically stored in a central directory like Active Directory. It ensures that users can log in to the Wi-Fi using their existing network credentials.
* AES (Option A) is an encryption standard but does not handle authentication.
* TKIP (Option C) is a deprecated encryption protocol and not related to network login management.
* WPA3 (Option D) is the latest Wi-Fi security standard but does not specifically handle centralized login management like RADIUS does.
CompTIA A+ Core 2 References:
* 2.2 - Compare and contrast wireless security protocols and authentication methods, including RADIUS.

最新問題**: 11**
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: C (メーッセージを残す)
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-protected devices 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**: 12**
技術者は、USB ポートを使用して追加のモニターを PC に接続します。元の HDMI モニターは、新しいモニターの左側に取り付けられています。元のモニターから新しいモニターにマウスを右

に移動すると、元のモニターの画面の端でマウスが停止します。マウスが新しいモニターに正しく移動できるようにするのは、次のうちどれですか?
A. ディスプレイ設定でモニターの位置を再配置する
B. モニターのケーブルを交換する
C. Ctrl+Alt+> を使用してディスプレイの向きを修正する
D. ビデオ カードのディスプレイ ドライバの更新
Answer: B (メーッセージを残す**)**
The correct answer is B. Swapping the cables for the monitors. When the second monitor is connected with the HDMI port, it is necessary to swap the cables for the monitors so that the mouse can move from the original monitor to the new monitor. This is because the HDMI port is designed to only support one monitor, and the mouse will not be able to move from one to the other without the cables being swapped.
According to CompTIA A+ Core 2 documents, "When connecting multiple displays to a system, the cables used to connect the displays must be swapped between the displays. For example, if a monitor is connected to a system using a VGA cable, the VGA cable must be moved to the next display to allow the mouse to move between the two displays."

最新問題**: 13**
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: A,D (メーッセージを残す**)**
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**: 14**

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: C (メーッセージを残す**)**
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**: 15**
管理者は、従業員が財務データをポータブル ハード ドライブにコピーし、そのデータを持って会社を退職したというインシデントに対応しました。管理者は証拠の移動を文書化しました。管理者が実証した概念は次のうちどれですか?
A. 加工過程の維持
B. データ保護ポリシーの実装
C. 法執行機関に通報する
D. インシデントの概要の作成
Answer: (解答を表示する**)**
Preserving chain of custody is a concept that refers to the documentation and tracking of who handled, accessed, modified, or transferred a piece of evidence, when, where, why, and how. Preserving chain of custody can help establish the authenticity, integrity, and reliability of the evidence, as well as prevent tampering, alteration, or loss of the evidence. An administrator who documented the movement of the evidence demonstrated the concept of preserving chain of custody. Implementing data protection policies, informing law enforcement, and creating a summary of the incident are not concepts that describe the action of documenting the movement of the evidence.

最新問題**: 16**
マネージャーは、スタッフ メンバーがモバイル デバイスやアプリケーションのパスワードをよく忘れてしまうと報告しています。送信されるヘルプ デスク チケットの数を減らすために、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. 多要素認証を有効にします。
B. ログイン失敗のしきい値を大きくします。
C. 複雑なパスワード要件を削除します。

D. 生体認証によるシングル サインオンを実装します。
Answer: A (メーッセージを残す**)**
Multifactor authentication (MFA) is a security measure that requires users to provide multiple pieces of evidence when logging in to an account or system. This can include a combination of something the user knows (e.g. a password or PIN), something the user has (e.g. a security token or smartphone) and something the user is (e.g. biometrics such as a fingerprint or face scan). By enabling MFA, the systems administrator can ensure that users are required to provide multiple pieces of evidence when logging in, making it more difficult for unauthorized users to gain access to the system. This can help reduce the number of help desk tickets submitted due to forgotten passwords.

最新問題**: 17**
次のうち、技術者が使用済みのプリンタ消耗品を廃棄する適切な方法はどれですか?
A. カスタムメーカの手順に進みます。
B. 消耗品は標準のゴミ箱に捨ててください。
C. 消耗品に残っているインクやトナーを空にしてから、標準のごみ箱に廃棄してください。
D. 消耗品は標準のリサイクル容器に廃棄してください。
Answer: A (メーッセージを残す**)**
When it comes to disposing of used printer consumables , it is important to follow the manufacturer's instructions or guidelines for proper disposal, as different types of consumables may require different disposal procedures. Some manufacturers provide specific instructions for proper disposal, such as sending the used consumables back to the manufacturer or using special recycling programs.
Therefore, the proper way for a technician to dispose of used printer consumables is to proceed with the custom manufacturer's procedure , if provided. This option ensures that the disposal is handled in an environmentally friendly and safe manner.

最新問題**: 18**
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: B (メーッセージを残す**)**
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**: 19**
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**: 20**
技術者は、更新プログラムを安全にインストールするために、ユーザーのラップトップに接続しようとしています。ラップトップに関する次の情報が与えられています。
RDP 経由で接続するには、技術者は次のどれを実行する必要がありますか?
A. ユーザーがデフォルトゲートウェイに ping できることを確認します。
B. ユーザーのラップトップの IP アドレスを変更します。
C. ユーザーのラップトップのサブネット マスクを変更します。
D. Windows ファイアウォールでポート 3389 を開きます。
Answer: D (メーッセージを残す**)**

In order to connect to a user's laptop via RDP, the technician should open port 3389 on the Windows firewall. This is because RDP uses port 3389 for communication12. The other options are not necessary or relevant for establishing an RDP connection.
* Confirming the user can ping the default gateway is not required for RDP, as it only tests the network connectivity between the user's laptop and the router. RDP works over the internet, so the technician should be able to ping the user's laptop directly using its IP address3.
* Changing the IP address on the user's laptop is not needed for RDP, as long as the IP address is valid and not conflicting with another device on the network. The user's laptop has a valid IP address of
192.168.0.45, which belongs to the same subnet as the gateway (192.168.0.1) and the subnet mask (255.255.255.0)4.
* Changing the subnet mask on the user's laptop is not required for RDP, as long as the subnet mask matches the network configuration. The user's laptop has a correct subnet mask of 255.255.255.0, which defines a network with 254 possible hosts4.
References:
1: [What is RDP and How Does It Work? - CompTIA] 2: CompTIA A+ Certification Exam Core 2 Objectives
- CompTIA 3: [Ping (networking utility) - Wikipedia] 4: [IP address - Wikipedia] : What is RDP and How Does It Work? - CompTIA : CompTIA A+ Certification Exam Core 2 Objectives - CompTIA : Ping (networking utility) - Wikipedia) : IP address - Wikipedia

最新問題**: 21**
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: A (メーッセージを残す**)**
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**: 22**

BitLocker でハード ドライブを暗号化したい 1 人のユーザーに最も適しているのは、次の Windows 10 エディションのうちどれですか?
A. プロフェッショナル
B. ホーム
C. エンタープライズ
D. 埋め込み
Answer: A (メーッセージを残す**)**
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 is available on supported devices running Windows 10 or 11 Pro, Enterprise, or Education2. Windows 10 Home does not support BitLocker3, and Windows 10 Embedded is designed for specialized devices and does not offer BitLocker as a feature4. Therefore, the most appropriate Windows 10 edition for a single user who wants to encrypt a hard drive with BitLocker is Professional.
References1: BitLocker overview - Windows Security | Microsoft Learn2: Device encryption in Windows - Microsoft Support3: Can You Turn on BitLocker on Windows 10 Home?4: How to enable device encryption on Windows 10 Home

最新問題**: 23**
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**)**
Jailbreaking a device exposes it to various security risks, such as malware, data theft, network attacks, and service disruption1234. Running an antivirus and enabling encryption may not be enough to remove the threats and restore the device's functionality. Undoing the jailbreak may not be possible or effective, depending on the method used. Backing up the files and doing a system restore may preserve the jailbreak and the associated problems. The best option is to erase the device and reinstall the original operating system that is compatible with the corporate policies and standards. This will ensure that the device is clean, secure, and compliant25.
References: 1 What is Jailbreaking & Is it safe? - Kaspersky(https://www.kaspersky.com/resource-center /definitions/what-is-jailbreaking). 2 Jailbreak Detection: Why is jailbreaking a potential security risk? - Cybersecurity ASEE(https://cybersecurity.asee.co/blog/what-is-jailbreaking/). 3 Jailbreaking Information for iOS Devices | University

IT(https://uit.stanford.edu/service/mydevices/jailbreak)4 What does it mean to jailbreak your phone-and is it legal? - Microsoft(https://www.microsoft.com/en-us/microsoft-365-life-hacks /privacy-and-safety/what-is-jailbreaking-a-phone). 5 Resetting a corporate laptop back to a personal laptop...
Enterprise vs Pro - Windows 10(https://community.spiceworks.com/topic/2196812-resetting-a-corporate- laptop-back-to-a-personal-laptop-enterprise-vs-pro).

最新問題**: 24**
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**: 25**
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, the lp command is used to manage print jobs, including setting the default printer. The lp command 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 the lp command, 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: **26**
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: A (メーッセージを残す**)**
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: **27**
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: **28**
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: A (メーッセージを残す)
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**: 29**
Windows ユーザーが最近コンピューターを交換した ユーザーはコンピューターでパブリック インターネットにアクセスできます。ただし、https7/companyintranet.com:8888 の内部サイトは読み込まれなくなりました。問題を解決するために技術者が調整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の設定
B. DHCP 設定
C. IPアドレス設定
D. ファイアウォールの設定
E. ウイルス対策設定
Answer: D (メーッセージを残す)
The technician should adjust the firewall settings to resolve the issue of not being able to access an internal site at https://companyintranet.com:8888. The firewall settings control how the firewall filters and allows network traffic based on rules and policies. The firewall settings may be blocking or preventing the access to the internal site by mistake or by default, especially if the site uses a non-standard port number such as 8888.
The technician should check and modify the firewall settings to allow the access to the internal site or its port number. Default gateway settings determine how a computer connects to other networks or the internet.
Default gateway settings are not likely to cause the issue of not being able to access an internal site if the user can access the public internet. DHCP settings determine how a computer obtains its IP address and other network configuration parameters automatically from a DHCP server. DHCP settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. IP address settings determine how a computer identifies itself and communicates with other devices on a network. IP address settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. Antivirus settings control how the antivirus software scans and protects the computer from malware and threats. Antivirus settings are less likely to cause the issue of not

being able to access an internal site than firewall settings, unless the antivirus software has its own firewall feature that may interfere with the network traffic. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

最新問題: **30**
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: **31**
ユーザーは、Windows ワークステーションで頻繁にマルウェアの兆候を経験しています。ユーザーは状態をロールバックしようと何度か試みましたが、マルウェアは存続します。次のうち、問題を解決する可能性が最も高いのはどれですか?
A. システムファイルを隔離中
B. ワークステーションの再イメージ化
C. ハード ドライブの暗号化
D. TLS 1.0 サポートの無効化
Answer: C (メーッセージを残す**)**
Encrypting the hard drive would most likely resolve the issue1

最新問題: **32**
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**: 33**
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**: 34**
コンピューター技術者が、起動していないコンピューターを調査しています。ユーザーは、昨夜シャットダウンするまでコンピュータは動作していたと報告しました。技術者は、取り外し可能な USB デバイスが挿入されていることに気づき、ユーザーは、そのデバイスが昨日メールで受け取った賞品であると説明しました。これは次のタイプの攻撃のうちどれを表しますか?

A. フィッシング
B. ゴミ箱ダイビング
C. 共連れ
D. 邪悪な双子
Answer: (解答を表示する**)**
Phishing is the correct answer for this question. Phishing is a type of attack that uses fraudulent emails or other messages to trick users into revealing sensitive information or installing malicious software. Phishing emails often impersonate legitimate entities or individuals and offer incentives or threats to lure users into clicking on malicious links or attachments. In this scenario, the user received a removable USB device in the mail as a prize, which could be a phishing attempt to infect the user's computer with malware or gain access to the user's data. Dumpster diving, tailgating, and evil twin are not correct answers for this question.
Dumpster diving is a type of attack that involves searching through trash bins or recycling containers to find discarded documents or devices that contain valuable information. Tailgating is a type of attack that involves following an authorized person into a restricted area without proper identification or authorization. Evil twin is a type of attack that involves setting up a rogue wireless access point that mimics a legitimate one to intercept or manipulate network traffic. References:
* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25
* [CompTIA Security+ SY0-601 Certification Study Guide], page 1004

最新問題**: 35**
ユーザーはデバイスの OS とデータをバックアップしたいと考えています。このタスクを達成するための最良の方法は次のうちどれですか?
A. 増分バックアップ
B. システムイメージ
C. システムの復元ポイント
D. 差分バックアップ
Answer: B (メーッセージを残す**)**
A system image is a complete snapshot of everything on a device's storage at a given point in time, including the operating system, installed programs, system settings, and all user files. This method is the best way to back up the OS and data comprehensively because it allows for the restoration of a system to its exact state at the time the image was taken. This is particularly useful in disaster recovery scenarios where it's crucial to restore a system quickly and efficiently to minimize downtime.

最新問題**: 36**
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: C,F (メーッセージを残す)
To locate a missing file with only a partial name known, the best tools to use in a Linux environment would be grep and find.
* grep: This command is used to search the contents of files for a specific pattern. While grep itself might not be the first choice for finding file names, it can be combined with other commands (like ls or find) 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. find can 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**: 37**
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: A,B (メーッセージを残す)
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: **38**
技術者は、従業員が職場のデスクトップで暗号通貨をマイニングしていることを発見しました。当社は、この行為がガイドラインに違反していると判断しました。この新しい要件を反映するために更新する必要があるのは、次のうちどれですか?
A. MDM
B. EULA
C. IRP
D. AUP
Answer: D (メーッセージを残す**)**
AUP (Acceptable Use Policy) should be updated to reflect this new requirement. The AUP is a document that outlines the acceptable use of technology within an organization. It is a set of rules that employees must follow when using company resources. The AUP should be updated to include a policy on cryptocurrency mining on work desktops

最新問題: **39**
ある組織の最高財務責任者 (CFO) は、ランサムウェアのアウトブレークが発生した場合に、ワークステーションで管理されていない非常に機密性の高い従来の PII にアクセスできなくなることを懸念しています。CFO には、このデータを何年も保持するという規制要件があります。次のバックアップ方法のうち、要件を最もよく満たすのはどれですか?
A. 会社のファイル サーバーに保存される毎日の増分バックアップ
B. ミラー化された RAID 構成の追加のセカンダリ ハード ドライブ
C. サイトのコールド ストレージに保存されているデータの完全バックアップ
D. クラウド ホスティング プロバイダーに保存される週次の差分バックアップ
Answer: (解答を表示する**)**
According to CompTIA A+ Core 2 objectives, a full backup stored off-site provides the greatest protection against data loss in the event of a ransomware attack or other data disaster. By storing the backup in a separate physical location, it is less likely to be affected by the same event that could cause data loss on the original system. Cold storage is a term used for data archiving, which typically refers to a long-term storage solution that is used for retaining data that is infrequently accessed, but still needs to be kept for regulatory or compliance reasons.

最新問題: **40**

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: B (メーッセージを残す)
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**: 41**
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: **42**
給与計算ワークステーションには、すぐに利用できる必要があり、誤って何かが削除された場合でもすぐに回復できるデータが格納されています。このような状況で高速なデータ回復を行うには、次のどのバックアップ方法を使用する必要がありますか?
A. フル
B. 差分
C. 合成
D. 増分
Answer: A (メーッセージを残す**)**
A full backup does not depend on any previous backups, unlike differential or incremental backups, which only save the changes made since the last backup. A synthetic backup is a type of full backup that combines an existing full backup with incremental backups to create a new full backup, but it still requires multiple backup sets to recover data. Therefore, a full backup is the most suitable for the payroll workstation that needs to have its data readily available and recoverable. You can learn more about the differences between full, differential, incremental, and synthetic backups from this article.

最新問題: **43**
ユーザーがヘルプデスクの技術者にシングル サインオン エラーを報告しました。現在、ユーザーは会社のアプリケーション ポータルにサインインできますが、特定の SaaS ベースのツールにアクセスできません。技術者が次のステップとして提案する可能性が高いのは次のうちどれですか。
A. ユーザーのモバイル デバイスを MFA トークンとして使用するために再登録します。
B. ローカル セッションの競合を回避するには、プライベート ブラウジング ウィンドウを使用します。
C. アプリケーションに直接認証することでシングル サインオンをバイパスします。
D. 使用中のデバイスを工場出荷時の設定にリセットします。
Answer: (解答を表示する**)**
Detailed Explanation with Core 2 References:Using a private browsing window can help resolve session conflicts by not relying on cached credentials, which might interfere with single sign-on processes. Core 2 objectives include troubleshooting authentication issues and resolving potential conflicts with single sign-on systems (Core 2 Objective 4.7).

最新問題: **44**

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: D (メーッセージを残す)
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**: 45**
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 used to 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**: 46**
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: (解答を表示する**)**
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**: 47**
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**: 48**
Linux サーバーとデスクトップを Windows Active Directory 環境に統合するために使用されるのは、次のうちどれですか?
A. apt-get
B. CIFS
C. サンバ
D. grP
Answer: C (メーッセージを残す**)**
Samba is a software suite that allows Linux servers and desktops to integrate with Windows Active Directory environments. Samba can act as a domain controller, a file server, a print server, or a client for Windows networks. Samba can also provide authentication and authorization services for Linux users and devices using Active Directory.

最新問題: **49**
アプリケーション ファイル バンドルとして実行されるように設計されたアプリ ファイル タイプは、次のオペレーティング システムのうちどれですか?
A. macOS
B. Chrome
C. Windows
D. Linux
Answer: (解答を表示する**)**
The app file type is designed to run under macOS as an application file bundle. macOS uses application bundles to store executable files and related resources, such as libraries, image files, and localized content, in a single directory hierarchy. This approach simplifies application management and execution within the macOS environment.

最新問題: **50**
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: **51**
追加のセキュリティ層を必要とするアプリケーションまたはシステムにアクセスするために必要なパスコードを生成するために使用されるものは次のうちどれですか?
A. 認証アプリケーション
B. アクセス制御リスト
C. 生体認証
D. スマート カード リーダー
Answer: (解答を表示する**)**
Authenticator applications are designed to enhance security by generating temporary, time-sensitive passcodes used in two-factor authentication (2FA) processes. These passcodes are

used in conjunction with traditional credentials (like usernames and passwords) to grant access to systems or applications. This extra layer of security ensures that even if primary login credentials are compromised, unauthorized access is still prevented without the dynamically generated code from the authenticator app.

最新問題: **52**
次の変更管理ドキュメントのうち、パッチをアンインストールする方法が含まれているのはどれですか?
A. 変更の目的
B. ロールバック計画
C. 変更の範囲
D. リスク分析
Answer: B (メーッセージを残す**)**
The change management document that includes how to uninstall a patch is called the "rollback plan". The rollback plan is a document that outlines the steps that should be taken to undo a change that has been made to a system. In the case of a patch, the rollback plan would include instructions on how to uninstall the patch if it causes problems or conflicts with other software12

最新問題: **53**
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: (解答を表示する**)**
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: **54**
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: D (メーッセージを残す**)**
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: **55**
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: (解答を表示する**)**
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: **56**
変更諮問委員会が設定変更を承認したため、技術者が変更を実装することが許可されています。技術者は変更を正常に実装しました。次に行うべきことは次のうちどれですか?
A. 変更の日時を文書化します。

B. 変更の目的を文書化します。
C. リスクレベルを文書化します。
D. サンドボックス テストの結果を文書化します。
Answer: A (メーッセージを残す)
The correct answer is A. Document the date and time of change. After implementing a change, the technician should document the date and time of change in the change log or record. This helps to track the change history, monitor the change performance, and identify any issues or incidents related to the change.
Documenting the date and time of change is also a good practice for auditing and compliance purposes.
Documenting the purpose of the change (B) and the risk level are steps that should be done before implementing the change, not after. These are important information that help to justify, prioritize, and plan the change. The purpose of the change should explain why the change is needed and what benefits it will bring to the organization. The risk level should assess the potential impact and probability of the change causing any problems or disruptions to the business.
Documenting the findings of the sandbox test (D) is also a step that should be done before implementing the change, not after. A sandbox test is a way of testing the change in an isolated environment that mimics the production environment. This helps to verify that the change works as expected and does not cause any errors or conflicts with other systems or processes. The findings of the sandbox test should be documented and reviewed by the change advisory board (CAB) before approving the change for implementation.
References:
What is a Change Advisory Board? (Overview, Roles, and Responsibilities) Best Practices in Change Management
10 Top change management best practices

最新問題**: 57**
技術者は、Linux コンピューターから Windows コンピューターに 20 GB のデータを転送するために USB ドライブを正式に作成する必要があります。次のファイルシステムのうち、技術者が最も使用する可能性が高いのはどれですか?
A. FAT32
B. ext4
C. NTFS
D. exFAT
Answer: C (メーッセージを残す)
Since Windows systems support FAT32 and NTFS "out of the box" and Linux supports a whole range of them including FAT32 and NTFS, it is highly recommended to format the partition or disk you want to share in either FAT32 or NTFS, but since FAT32 has a file size limit of 4.2 GB, if you happen to work with huge files, then it is better you use NTFS

最新問題: **58**
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: **59**
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**: 60**
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**: 61**
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: **62**
Windows 管理者は、数人の新規ユーザーのホーム ディレクトリとネットワーク プリンターを含むユーザー プロファイルを作成しています。技術者がこのタスクを完了するのに最も効率的な方法は次のうちどれですか?
A. アクセス制御
B. 認証アプリ
C. グループポリシー
D. フォルダーのリダイレクト
Answer: C (メーッセージを残す**)**
Group Policy is a feature of Windows that allows administrators to centrally manage and apply policies and settings to computers and users on a domain. Group Policy can be used to create user profiles that include home directories and network printers for several new users, as well as other configurations such as security settings, desktop preferences, and software installation. Group Policy can save time and effort for the administrator by applying the same settings to multiple users at once. Access control, authentication application, and folder redirection are not the most efficient ways to create user profiles that include home directories and network printers for several new users.

最新問題: **63**
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: A (メーッセージを残す**)**
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: **64**
技術者が Windows 10 ラップトップをドメインに参加させることができない 最も可能性の高い理由は次のうちどれですか?
A. ドメインのプロセッサの互換性が満たされていません
B. ラップトップには Windows 10 Home がインストールされています
C. ラップトップにはオンボードのイーサネット アダプタがありません

D. ラップトップには最新の Windows アップデートがすべてインストールされているわけではありません
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**: 65**
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**: 66**
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**: 67**
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: D (メーッセージを残す)
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**: 68**
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: **69**
ユーザーの Windows 10 デバイスのインターネット速度は遅いですが、同じネットワーク上の他のデバイスは通常の速度で動作しています。技術者は、この問題はプロキシ設定に関連している可能性があると考えています。技術者は、プロキシ構成を確認するために次のどれを確認する必要がありますか?
A. ネットワークと共有センター
B. インターネット オプション
C. ファイアウォール設定
D. システム設定
Answer: B (メーッセージを残す)
The correct place to check proxy settings in Windows 10 is under Internet Options (Option B), specifically in the "Connections" tab. Proxy configurations can affect internet speeds if misconfigured or if a proxy is being used unnecessarily.
* Network and Sharing Center (Option A) provides information on network connections but doesn't handle proxy settings.
* Firewall settings (Option C) manage network traffic rules but don't directly affect proxy settings.
* System settings (Option D) contain general system configurations, not specific to proxy settings.
CompTIA A+ Core 2 References:
* 1.6 - Configure networking features in Windows, including proxy settings

最新問題: **70**
ユーザーが新しい SOHO Wi-Fi ルーターを初めて構成しています。ユーザーが最初に変更する必要がある設定は次のうちどれですか?
A. 暗号化
B. Wi-Fi チャンネル
C. デフォルトのパスワード
D. サービスセット識別子
Answer: (解答を表示する)
the user should change the default passwords first when configuring a new SOHO Wi-Fi router1

最新問題: **71**
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: (解答を表示する**)**
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**: 72**
複数のユーザーが簡単にアクセスできる領域にログイン情報を定期的に記録します。この問題を軽減する最善の方法は次のうちどれですか?
A. 信頼できる情報源
B. 有効な証明書
C. ユーザートレーニング
D. パスワードマネージャー
Answer: D (メーッセージを残す**)**
Using a password manager is the best way to mitigate the issue of users recording their login information in accessible areas. Password managers securely store and encrypt passwords and login details, reducing the need for users to write down or remember multiple complex passwords. This approach enhances security by encouraging the use of strong, unique passwords for different accounts without the risk of forgetting them or the unsafe practice of writing them down. Trusted sources, valid certificates, and user training are important security measures but do not directly address the problem of managing multiple secure passwords as effectively as a password manager does.

最新問題**: 73**
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: **74**
技術者が休暇中のユーザーから電話を受けました。ユーザーは必要な資格情報を提供し、技術者にユーザー アカウントにログインして、ユーザーが予期していた重要な電子メールを読むように依頼します。これは次の違反であるため、技術者は拒否します。
A. 利用ポリシー。
B. 規制順守要件。
C. 機密保持契約
D. インシデント対応手順
Answer: A (メーッセージを残す**)**
Logging into a user's account without their explicit permission is a violation of the acceptable use policy, which outlines the rules and regulations by which a user must abide while using a computer system. By logging into the user's account without their permission, the technician would be violating this policy.
Additionally, this action could be seen as a breach of confidentiality, as the technician would have access to information that should remain confidential.

最新問題: **75**
ユーザーのスマートフォンのデータ使用量は平均をはるかに上回っています。ユーザーは、インストールされたアプリケーションがバックグラウンドでデータを送信していると疑っています。ユーザーは、アプリケーションがインターネットとの通信を試みたときにアラートを受け取りたいと考えています。次のうち、ユーザーの懸念に最もよく対処するのはどれですか?
A. オペレーティング システムの更新
B. リモートワイプ
C. ウイルス対策
D. ファイアウォール
Answer: D (メーッセージを残す**)**
A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. In this scenario, the user is concerned about an installed application transmitting data in the background, so a firewall would be the best solution to address their concern. By installing and configuring a firewall, the user can block unauthorized connections to and from the device, and receive alerts whenever an application tries to access the internet.

最新問題: **76**

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**: 77**

macOS で自動バックアップを構成するには、次のどれを使用する必要がありますか?

A. ミッションコントロール

B. タイムマシン

C. 災害復旧

D. システムの復元

Answer: B (メーッセージを残す**)**

Time Machine is the built-in backup feature for macOS that allows users to back up their system automatically. It continuously backs up everything on the Mac, including files, applications, system files, and settings, allowing users to restore their system to a previous state if needed. Time Machine operates by creating hourly backups for the past 24 hours, daily backups for the past month, and weekly backups for all previous months. Other options like "Mission Control" help in organizing windows, while "System Restore" is a feature more common in Windows operating systems, not macOS.
References:
Apple Support: Use Time Machine to back up or restore your Mac
CompTIA A+ Study Guide - Backup and Recovery Concepts in macOS (Whizlabs)

最新問題: **78**
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: **79**
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 (メーッセージを残す**)**
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: **80**

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**: 81**

会社のヘルプデスクには、現在のセキュリティ侵害に関連する問題を報告する従業員からの多数の電話がかかってきます。ヘルプデスク チームは、侵害を記録するために、次の手順のどれを実行する必要がありますか?

A. チケットシステムに詳細を記録します。

B. スクリーンショットを撮り、根本原因分析に添付します。

C. 会社の法務チームと事件について話し合います。

D. 会社のナレッジベースに詳細をリストします。

Answer: (解答を表示する**)**

In the event of a security breach, documenting the incident is crucial for tracking, analysis, and resolution.

The appropriate steps should ensure thorough documentation and communication:

* Option A: Record the details in the ticketing system.Correct Answer. The ticketing system is the primary tool for IT support to track incidents. Recording the details in the ticketing system ensures that all relevant information is documented systematically, can be easily accessed, and tracked through the resolution process.

* This aligns with best practices in incident documentation and support systems information management as outlined in the CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 4.1.

* Option B: Take screenshots and attach them to the root cause analysis.While screenshots can be useful, the first step should be to record the details in the ticketing system. Screenshots may be added later as supplementary information.

* Option C: Discuss the incident with the company's legal team.Involving the legal team is important for certain aspects of a security breach, but the initial step should still be to document the incident in the ticketing system.

最新問題**: 82**

技術者は、タスクを実行するために、ユーザーにルート レベルの権限と同等の権限を割り当てます。技術者は、Windows OS 内の次のユーザー ロールのどれを選択する必要がありますか。
A. パワー
B. デフォルト
C. 管理者
D. スーパーユーザー
Answer: (解答を表示する**)**
In the Windows OS, to grant a user permissions equivalent to root-level permissions (which means full control over the system), the user needs to be given:
* Administrator: The Administrator role provides full control over the system, including the ability to install and uninstall software, change system settings, and access all files and directories.
* Power: The Power User role provides some administrative capabilities but not full control. It is a legacy role with fewer permissions than Administrator.
* Default: This refers to a standard user account with limited permissions.
* Superuser: This term is more commonly associated with Unix/Linux systems and is not a specific role in Windows.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.5: Given a scenario manage and configure basic security settings in the Microsoft Windows OS.
Windows user roles and permissions documentation.

最新問題**: 83**
顧客は、メールで受け取った一方的な USB ドライブから新しい Web ブラウザをインストールしました。
ブラウザが期待どおりに動作せず、インターネット検索が別のサイトにリダイレクトされます。
ブラウザをアンインストールした後、ユーザーが次に行うべきことは次のうちどれですか?
A. ブラウザの Cookie と履歴を削除します。
B. すべてのブラウザ設定をリセットします。
C. ブラウザのデフォルトの検索エンジンを変更します。
D. 信頼できるブラウザをインストールします。
Answer: D (メーッセージを残す**)**
The customer's web browser is likely infected by a browser hijacker, which is a type of malware that changes the browser's settings and redirects the user to malicious websites. A browser hijacker can also steal the user's personal data, display unwanted ads, and install more malware on the device. To remove a browser hijacker, the user should first uninstall the browser from the Control Panel, then scan the device with an antivirus or anti-malware program, and finally install a trusted browser from a legitimate source. Deleting the browser cookies and history, resetting the browser settings, or changing the browser default search engine may not be enough to get rid of the browser hijacker, as it may have embedded itself into the system or other browser components.

最新問題: **84**
技術者は、POS 取引に使用されるワークステーションのインストールを任されています。POS システムは、クレジットカードとポイント カードを処理します。盗難の際にワークステーションを保護するために、次のどの暗号化テクノロジを使用する必要がありますか。
A. 転送中のデータの暗号化
B. ファイルの暗号化
C. USBドライブの暗号化
D. ディスク暗号化
Answer: D (メーッセージを残す**)**
Disk encryption is the best method for securing a workstation used in financial transactions, such as point-of- sale systems. It ensures that if the workstation is stolen, all data on the disk is encrypted and cannot be accessed without proper credentials. File encryption (B) only encrypts individual files, and USB drive encryption (C) only applies to removable storage. Data-in-transit encryption (A) is not relevant for physical security.
Reference: Core 2, Domain 2.6 - Security configurations.

最新問題: **85**
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: **86**
ある企業は古いワークステーションを廃止する予定で、すべてのハードドライブの破壊証明書が必要です。データを確実に復元できないようにするには、次のどれをハードドライブ上で実行するのが最適ですか? (2 つ選択してください)。
A. 標準フォーマット
B. Drilling
C. .消去
D. リサイクル

E. Recycling
F. 低レベルフォーマット
Answer: (解答を表示する**)**
Drilling and incinerating are physical destruction methods that make the data on hard drives unrecoverable.
Standard formatting, erasing and low-level formatting are logical methods that can be reversed with data recovery tools. Recycling is not a destruction method at all. Verified References: https://www.comptia.org
/blog/what-is-a-certificate-of-destruction https://www.comptia.org/certifications/a

最新問題**: 87**
最新の Windows アップデートに続いて、PDF ファイルが Adobe Reader ではなく Microsoft Edge で開かれます。すべての PDF ファイルを Adobe Reader で確実に開くには、次のどのユーティリティを使用する必要がありますか?
A. ネットワークと共有センター
B. プログラムと機能
C. デフォルトのアプリ
D. プログラムの追加または削除
Answer: C (メーッセージを残す**)**
Default Apps should be used to ensure all PDF files open in Adobe Reader1

最新問題**: 88**
技術者はシステムを完全に起動することができません。デスクトップの背景が表示されると OS がフリーズし、システムを再起動しても問題が解決しません。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行うべきことは次のうちどれですか?
A. 該当する BIOS オプションを無効にします。
B. システムをセーフ モードでロードします。
C. フラッシュ ドライブ OS を使用して起動し、システム修復を実行します。
D. セキュアブートを有効にしてシステムを再インストールします。
Answer: B (メーッセージを残す**)**
Loading the system in safe mode is a common troubleshooting step that allows the technician to isolate the problem by disabling unnecessary drivers and services. This can help determine if the issue is caused by a faulty device, a corrupted system file, or a malware infection.

最新問題**: 89**
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: D (メーッセージを残す)
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**: 90**
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**: 91**
機密情報を含む SSD を破棄するには、データ センターが必要です。SSD の物理的破壊に使用する最良の方法は次のうちどれですか?
A. 拭き取り
B. ローレベルフォーマット
C. シュレッダー
D. 消去
Answer: C (メーッセージを残す)

Shredding is the best method to use for the physical destruction of SSDs because it reduces them to small pieces that cannot be recovered or accessed. Wiping, low-level formatting, and erasing are not effective methods for destroying SSDs because they do not physically damage the flash memory chips that store data1.

最新問題: **92**
技術者は、起動時の OS の読み込みに問題がある Windows システムのトラブルシューティングを行っています。問題を診断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. システムでブート ログを有効にします。
B. 最新の正常な構成を起動します。
C. タスク マネージャーでシステム リソースの使用状況を確認します。
D. sfc /scannow コマンドを実行します。
E. イベント ビューアを使用してアプリケーション ログを開きます
Answer: A (メーッセージを残す)
When troubleshooting a Windows system that is experiencing issues during the OS loading phase at startup, enabling boot logging is a practical step. Boot logging creates a record of all drivers and services that are loaded (or attempted to be loaded) during the startup process. This record, typically named ntbtlog.txt, can be reviewed to identify any drivers or services that failed to load, which could be contributing to the startup issues. This diagnostic step helps pinpoint the problematic component(s) and facilitates targeted troubleshooting to resolve the OS loading issues.

最新問題: **93**
技術者は、企業内のすべてのコンピューターに Windows の新しいコピーをインストールしています。以下の要件を考慮します。
* インストール フェーズはネットワーク上で実行するようにスクリプト化する必要があります。
* 各コンピュータにはシステム ドライブとして新しい SSD が必要です。* 既存の HDD はバックアップ ドライブとして残しておく必要があります。
技術者がドライブをインストールし、ネットワーク共有からインストール ファイルを転送するには、次のコマンド ライン ツールのうちどれを使用する必要がありますか? (3 つ選択してください)。

A. 純使用量
B. ロボコピー
C. ウィンバー
D. ディスクパート
E. sfc
F. r.etstat
G. ping
H. chkdsk
Answer: A,B,D (メーッセージを残す)
For scripted network installations requiring new SSDs and keeping HDDs as backup, the necessary tools are:
'net use' to connect to network shares, 'robocopy' to copy files efficiently from the network share to the local drive, and 'diskpart' to manage disk partitions, including initializing and formatting the new SSD. The other options are not relevant to the installation process as described.

最新問題**: 94**
モバイル デバイスを放置したときに、望ましくないアクセスから保護できるのは次のうちどれですか?
A. PINコード
B. OSアップデート
C. ウイルス対策ソフト
D. BYOD ポリシー
Answer: A (メーッセージを残す)
A PIN code is a numeric password that protects a mobile device against unwanted access when it is left unattended. It requires the user to enter the correct code before unlocking the device. OS updates, antivirus software and BYOD policy are other security measures for mobile devices, but they do not prevent unauthorized access when the device is left unattended. Verified References: https://www.comptia.org/blog
/mobile-device-security https://www.comptia.org/certifications/a

最新問題**: 95**
ユーザーは、会社を出る前に、帰宅時の交通状況を確認したいと考えています。午後 4 時 45 分にトラフィック Web サイトを自動的に起動するようにブラウザーをスケジュールするために、ユーザーが使用できるツールは次のうちどれですか?
A. taskschd.msc
B. perfmon.msc
C. lusrmgr.msc
D. Eventvwr.msc
Answer: A (メーッセージを残す)

The user can use the Task Scheduler (taskschd.msc) to schedule the browser to automatically launch a traffic website at 4:45 p.m. The Task Scheduler is a tool in Windows that allows users to schedule tasks to run automatically at specified times or in response to certain events.

最新問題**: 96**
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: A (メーッセージを残す**)**
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**: 97**
ユーザーはコンピューターで OS を起動できなくなり、OS が見つからないことを示すエラーメッセージが表示されます。技術者が監査ログを確認し、ユーザーのシステムがこの問題の数日前に SMART エラーを投稿したことを指摘します。こ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. 起動順序
B. マルウェア
C. ドライブの故障
D. Windows アップデート
Answer: (解答を表示する**)**

A S.M.A.R.T. error is a warning that a hard drive is about to fail or has failed. This means that the OS cannot be loaded from the drive and the user will see an error message indicating there is no OS found. The most likely cause of this issue is drive failure.

最新問題**: 98**
ユーザーが選択した Web 検索プロバイダーにアクセスしようとするたびに、別の Web サイトが開きます。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. システム時刻
B. IPアドレス
C. DNS サーバー
D. Windows アップデート
Answer: C (メーッセージを残す**)**
When a user experiences unexpected or erratic behavior while browsing the internet, it could be caused by the DNS servers. DNS translates human-readable domain names (like google.com) into IP addresses, which computers can use to communicate with web servers. If the DNS servers are not functioning correctly or have been compromised, it can result in the browser being redirected to unintended websites.

最新問題**: 99**
企業は、最小限のコストで全従業員に多要素認証を実装したいと考えています。会社の要件を最もよく満たすものは次のうちどれですか?
A. 生体認証
B. ソフトトークン
C. アクセス制御リスト
D. スマートカード
Answer: (解答を表示する**)**
A soft token, also known as a software token or an OTP (one-time password) app, is a type of multifactor authentication that generates a temporary code or password on a user's device, such as a smartphone or a tablet. The user must enter this code or password along with their username and password to access their account or service. A soft token can help improve security by adding an extra layer of verification and preventing unauthorized access even if the user's credentials are compromised. A soft token can also be implemented at a minimal cost, as it does not require any additional hardware or infrastructure. Biometrics, access control lists, and smart card are not types of multifactor authentication that can be implemented at a minimal cost.

最新問題**: 100**
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**: 101**
旅行先でスマートフォンからメールの受信やインターネットの閲覧ができなくなった。ただし、テキスト メッセージと電話は問題なく機能しています。サポート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. ユーザーアカウントの状態
B. モバイル OS バージョン
C. データプランの補償範囲
D. ネットワーク トラフィックの停止
Answer: C (メーッセージを残す**)**
The first thing that a support technician should check to resolve the issue of not being able to receive emails or browse the internet from a smartphone while traveling is the data plan coverage. The data plan coverage determines how much data and where the user can use on the smartphone's cellular network. The data plan coverage may vary depending on the user's location, carrier and subscription. The data plan coverage may not include or support certain areas or countries that the user is traveling to, or may charge extra fees or limit the speed or amount of data that the user can use. The data plan coverage does not affect text messages and phone calls, which use different network services and protocols. User account status is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the user account has been suspended or terminated by the carrier or the email provider. Mobile OS version is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the mobile OS has a major bug or compatibility problem with the network or the email app.
Network traffic outages may cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, but they are less likely and less common than data plan coverage issues, and they should also affect text messages and phone calls. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.5

最新問題**: 102**
技術者がワークステーションに Windows 10 をインストールしました。技術者が 8GB をインストールしたにもかかわらず、ワークステーションには 3.5GB の使用可能な RAM しかありませ

ん。このシステムが使用可能な RAM をすべて使用してい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. システムにアップデートがありません。
B. システムは 32 ビット OS を使用しています。
C. システムのメモリが故障しています。
D. システムには BIOS の更新が必要です
Answer: B (メーッセージを残す**)**
The most likely reason that the system is not utilizing all the available RAM is that the system is utilizing a
32-bit OS. A 32-bit OS is an operating system that uses 32 bits to address memory locations and perform calculations. A 32-bit OS can only support up to 4GB of RAM, and some of that RAM may be reserved for hardware devices or system functions, leaving less than 4GB of usable RAM for applications and processes.
A 32-bit OS cannot recognize or utilize more than 4GB of RAM, even if more RAM is installed on the system. To utilize all the available RAM, the system needs to use a 64-bit OS, which can support much more RAM than a 32-bit OS. The system missing updates may cause some performance or compatibility issues, but it does not affect the amount of usable RAM on the system. The system's memory failing may cause some errors or crashes, but it does not affect the amount of usable RAM on the system. The system requiring BIOS updates may cause some configuration or compatibility issues, but it does not affect the amount of usable RAM on the system. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

最新問題**: 103**
Web 開発者は、新しい外部 Web サーバーをインストールして起動します。起動直後、ファイアウォールを通過するすべてのトラフィックのパフォーマンスが大幅に低下します。次の考慮事項のうち、見落とされていたものはどれですか?
A. OS の互換性
B. サービスの品質
C. 32 ビット アーキテクチャと 64 ビット アーキテクチャ
D. ストレージ要件
Answer: B (メーッセージを残す**)**
The performance degradation following the launch of a new external web server suggests that Quality of Service (QoS) considerations were overlooked. QoS settings help prioritize traffic to ensure that critical services like web servers receive the bandwidth they need without negatively impacting the overall network performance. Without proper QoS configuration, the new server's traffic could overwhelm the firewall, leading to widespread performance issues.

最新問題**: 104**

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: (解答を表示する**)**
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**: 105**
データセンター内で最も重要な環境問題は次のうちどれですか?
A. 電池の廃棄
B. 静電気対策マット
C. トナー廃棄
D. 湿度レベル
Answer: D (メーッセージを残す**)**
One of the most important environmental concerns inside a data center is the level of humidity. High levels of humidity can cause condensation, which can result in corrosion of components and other equipment. Low levels of humidity can cause static electricity to build up, potentially leading to electrostatic discharge (ESD) and damage to components. Therefore, it is crucial to maintain a relative humidity range of 40-60% in a data center to protect the equipment and ensure proper operation.

最新問題**: 106**
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: (解答を表示する**)**
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**: 107**
ユーザーがスマートフォンでウェブサイトを閲覧しているときに、ポップアップが表示されます。ポップアップには、システムが侵害されたことが示され、侵害を解決するためのアプリケーションにユーザーが誘導されます。ユーザーは次のどれを実行する必要がありますか?

A. ウェブサイトを閉じてポップアップを無視します
B. スマートフォンを交換する
C. 問題を解決するには、アプリケーションをダウンロードしてインストールしてください
D. スマートフォンを分析して侵入元を見つける
Answer: A (メーッセージを残す**)**
Comprehensive and Detailed In-Depth Explanation:
This is a scareware scam that attempts to trick users into installing malicious applications. The best action is to close the website and ignore the pop-up.
* B. Replace the smartphone - Incorrect. The phone is likely not compromised; it is just displaying a fake warning.
* C. Download and install the application to resolve the issue - Incorrect. Doing so could infect the device with malware.
* D. Analyze the smartphone to find the source of the breach - Unnecessary, as there is no real breach.
Reference:
CompTIA A+ 220-1102, Objective 2.5 - Common Security Threats

最新問題**: 108**
ユーザーの会社の電話が盗まれ、デバイスには会社の企業秘密が含まれています。このリスクを軽減するために実装する必要があるテクノロジは、次のうちどれですか? (2 つ選択)。
A. リモートワイプ
B. ファイアウォール
C. デバイスの暗号化
D. リモートバックアップ
E. ウイルス対策
F. 全地球測位システム
Answer: A,C (メーッセージを残す**)**
Remote wipe is a feature that allows data to be deleted from a device or system remotely by an administrator or owner1. It is used to protect data from being compromised if the device is lost, stolen, or changed hands1. Device encryption is a feature that helps protect the data on a device by making it unreadable to unauthorized users2. It requires a key or a password to access the data2. Both features can help mitigate the risk of losing company trade secrets if a corporate phone is stolen.
References: 1: How to remote wipe Windows laptop (https://www.thewindowsclub.com/remote-wipe- windows-10) 2: Device encryption in Windows (https://support.microsoft.com/en-us/windows/device- encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d)

最新問題**: 109**

新しいベンダーがオフィスを訪れた後、ユーザーは小さな USB ドライブがユーザーのコンピューターに接続されていることに気付きました。技術者は、grabber.exe と output.txt という名前の 2 つのファイルに気付きます。次の攻撃のうち、発生する可能性が最も高いのはどれですか?
A. トロイの木馬
B. ルートキット
C. クリプトマイナー
D. キーロガー
Answer: D (メーッセージを残す)
A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote attacker1.
The attacker can use the captured information to steal passwords, credit card numbers, or other sensitive data. A keylogger can be installed on a computer by attaching a small USB drive that contains a malicious executable file, such as grabber.exe2. The output.txt file may contain the recorded keystrokes. The user should remove the USB drive and scan the computer for malware.
References: 2: What is grabber.exe? (https://www.freefixer.com/library/file/grabber.exe-55857/) 1: What is a keylogger? (https://www.kaspersky.com/resource-center/definitions/keylogger)

最新問題**: 110**
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**: 111**
ユーザーは、会社の電話のデータ プランが上限に達したことを示す通知を受け取ります。ユーザーは、電話のパフォーマンスが異常に遅いことにも気付きました。技術者は、サードパーティの GPS アプリケーションが電話にインストールされていることを発見しました。最も可能性の高い原因は次のうちどれですか?
A. GPS アプリケーションがソフトウェア更新プログラムをインストールしています。
B. GPS アプリケーションにマルウェアが含まれています。

C. GPS アプリケーションが地理空間地図データを更新しています。
D. GPS アプリケーションが内蔵 GPS と競合しています。
Answer: B (メーッセージを残す**)**
The GPS application contains malware. The third-party GPS application is likely the cause of the slow performance of the phone. The application may contain malware that is using up system resources and slowing down the phone. The user should uninstall the application and run a malware scan on the phone1

最新問題**: 112**
ユーザーが PC にウイルスが存在すると報告しました。ユーザーが追加の Real-Lime Protection ウイルス対策ソフトウェアをインストールすると、PC のパフォーマンスが非常に遅くなり始めます。問題を解決するには、技術者が次のどの手順を実行する必要がありますか?
A. 1 つのウイルス対策ソフトウェア プログラムをアンインストールし、別のウイルス対策ソフトウェア プログラムをインストールします。
B. Windows Update を起動し、OS アップデートをダウンロードしてインストールします。
C. 両方のウイルス対策ソフトウェア プログラムでリアルタイム保護を有効にします。
D. 両方のウイルス対策ソフトウェア プログラムで隔離機能を有効にします。
E. ユーザーがインストールしたウイルス対策ソフトウェアを削除します。
Answer: E (メーッセージを残す**)**
Removing the user-installed antivirus software program is the best way to resolve the issue of extremely slow performance caused by installing additional real-time protection antivirus software on a PC. Having more than one antivirus software program running at the same time can cause conflicts, resource consumption and performance degradation. Uninstalling one antivirus software program and installing a different one, activating real-time protection on both antivirus software programs, enabling the quarantine feature on both antivirus software programs and launching Windows Update are not effective ways to resolve the issue.
Verified References: https://www.comptia.org/blog/why-you-shouldnt-run-multiple-antivirus-programs-at-the- same-time https://www.comptia.org/certifications/a

最新問題**: 113**
ユーザーのシステムがマルウェアに感染しています。技術者がマルウェア対策ソフトウェアを更新し、マルウェアを削除するスキャンを実行します。ユーザーがシステムを再起動すると、再びマルウェアに感染します。次のうち、マルウェアを完全に削除するのに最も役立つ可能性が高いのはどれですか?
A. システムの復元を有効にする
B. ユーザーの教育
C. セーフ モードでの起動
D. スキャンのスケジュール
Answer: B (メーッセージを残す**)**

Although updating the anti-malware software and running scans are important steps in removing malware, they may not be sufficient to permanently remove the malware if the user keeps engaging in behaviors that leave the system vulnerable, such as downloading unknown files or visiting malicious websites. Therefore, educating the user on safe computing practices is the best way to prevent future infections and permanently remove the malware.
Enabling System Restore, Booting into safe mode, and scheduling a scan are not the most efficient ways to permanently remove the malware. Enabling System Restore and Booting into safe mode may help in some cases, but they may not be sufficient to permanently remove the malware. Scheduling a scan is also important for detecting and removing malware, but it may not be sufficient to prevent future infections.
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

最新問題**: 114**
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: (解答を表示する**)**
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**: 115**
変更諮問委員会は、実装が失敗した場合の代替アクションがないため、要求された変更を承認しませんでした。再度承認をリクエストする前に更新する必要があるのは、次のうちどれですか?
A. 変更の範囲
B. リスクレベル
C. ロールバック計画
D. エンド ユーザーの承認
Answer: C (メーッセージを残す**)**

The rollback plan should be updated before requesting approval again. A rollback plan is a plan for undoing a change if it causes problems, and it is an important part of any change management process. If the change advisory board did not approve the requested change due to the lack of alternative actions if implementation failed, then updating the rollback plan would be the best way to address this concern.

最新問題**: 116**
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: (解答を表示する**)**
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**: 117**
技術者は、ユーザー入力が悪意のある攻撃者によってキャプチャされたことを発見しました。次のマルウェア タイプのうち、最も使用されている可能性が高いのはどれですか?
A. クリプトマイナー
B. ルートキット
C. スピアフィッシング
D. キーロガー
Answer: D (メーッセージを残す**)**
A keylogger is a type of malware that captures user input, such as keystrokes, mouse clicks, and clipboard data, and sends it to a malicious actor. Keyloggers can be used to steal passwords, credit card numbers, personal information, and other sensitive data.
Reference: CompTIA A+ Core 2 Exam Objectives, Section 5.1

最新問題**: 118**
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**: 119**
ユーザーが、コンピューターの実行速度が遅いと報告しています。次のツールのうち、技術者が発行された
A. ディスクのクリーンアップ
B. グループ ポリシー エディター
C. ディスクの管理
D. リソースモニター
Answer: (解答を表示する**)**
Resource Monitor will help a technician identify the issue when a user reports a computer is running slow1

最新問題**: 120**
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**: 121**
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**: 122**
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**: 123**
技術者が、会社支給のすべてのラップトップに対して特定の NTP サーバーを構成しています。これらの Windows 10 マシンは、Active Directory ドメインに参加していません。この調整には、次のどの設定領域が使用されますか?
A. システム
B. 更新とセキュリティ
C. ネットワークとインターネット
D. 時間と言語
Answer: (解答を表示する**)**
Comprehensive and Detailed In-Depth Explanation:

To configure an NTP (Network Time Protocol) server, navigate to Time and Language > Date & Time settings in Windows 10.
* A. System - Incorrect. This manages system settings but not time synchronization.
* B. Update and Security - Incorrect. This controls Windows updates and security settings.
* C. Network and Internet - Incorrect. This is for networking settings, not time sync.
Reference:
CompTIA A+ 220-1102, Objective 1.8 - Windows Settings Configuration

最新問題**: 124**
システム管理者は、Microsoft Windows マシン上のフォルダーの定期的なバックアップを作成しています。ソース データは非常に動的であり、ファイルは定期的に追加または削除されます。バックアップのソース データをミラーリングするために使用できるユーティリティは次のうちどれですか?
A. コピー
B. xcopy
C. ロボコピー
D. コピー項目
Answer: C (メーッセージを残す**)**
Robocopy is a command-line utility that can be used to mirror the source data for the backup. It can copy files and folders with various options, such as copying only changed files, preserving attributes and permissions, and retrying failed copies. Robocopy is more powerful and flexible than copy or xcopy, which are simpler commands that can only copy files and folders without mirroring or other advanced features. Copy-Item is a PowerShell cmdlet that can also copy files and folders, but it is not a native Windows utility and it requires PowerShell to run1.
References: 1: https://windowsreport.com/mirror-backup-software/

最新問題**: 125**
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: A (メーッセージを残す**)**
* 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**: 126**

ユーザーのアプリケーションが応答しません。次のタスク マネージャーのタブのうち、ユーザーが状況に対処できるのはどれですか?
A. 起動
B. パフォーマンス
C. 申請履歴
D. プロセス
Answer: D (メーッセージを残す)
The Processes tab in the Task Manager shows all the running processes on the computer, including applications and background services. The user can use this tab to identify the unresponsive application and end its process by right-clicking on it and selecting End task. This will free up the system resources and close the application. The other tabs in the Task Manager do not allow the user to address the situation. The Startup tab shows the programs that run when the computer starts, the Performance tab shows the system resource usage and statistics, and the Application history tab shows the resource usage of the applications over time

最新問題**: 127**
技術者は、必要に応じて幹部のラップトップを復元できるバックアップおよびリカバリ ソリューションを実装する必要があります。計画には、きめ細かなリカバリとディスク全体のリカバリを実行する機能を含める必要があります。
技術者が計画を成功裏に実行するための最適なオプションは次のどれですか? (2 つ選択してください。)
A. RAID
B. ボリュームシャドウコピー
C. 増分バックアップ
D. システムの復元
E. 祖父 -父 -息子のバックアップ
F. ディスクイメージング
Answer: (解答を表示する)
To ensure executives' laptops can be restored with both granular and whole-disk recovery, the technician should implement:
* Incremental Backup - This method allows for granular recovery by backing up only the data that has changed since the last backup. This means that users can restore specific files or data from a particular point in time without needing to restore the entire system.
* Disk Imaging - This method captures an exact copy (image) of the entire disk, including the operating system, installed applications, settings, and files. This allows for whole-disk recovery, meaning the entire system can be restored in case of catastrophic failure.
Why Not the Other Options?
* A. RAID - RAID is a redundancy and performance solution for storage, not a backup solution. While it can provide fault tolerance, it does not allow for restoring lost files or recovering previous versions.

* B. Volume Shadow Copy - This feature in Windows allows users to restore previous versions of files, but it is not a full backup solution.
* D. System Restore - While System Restore can revert system files and settings, it does not back up user data or provide full system recovery.
* E. Grandfather-Father-Son Backup - This is a backup rotation strategy, not a specific type of backup method. It organizes how backups are stored but does not specify whether granular or full recovery is possible.
Thus, Incremental Backup and Disk Imaging are the best choices to ensure both granular and full-disk recovery for executives' laptops.

最新問題**: 128**
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: (解答を表示する**)**
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**: 129**
ユーザーは、ヘルプ デスクがリモート管理ツールを使用してユーザーを支援できるように、Windows PC のネットワーク名を検索するように指示されています。次のコマンドのうち、ユーザーが技術者に正しい情報を提供できるのはどれですか? (2 つ選択)。
A. ipconfig /all
B. hostname
C. netstat /?
D. nslookup localhost
E. arp -a
F. ping :: 1
Answer: (解答を表示する**)**
The user can use the following commands to give the technician the correct information: ipconfig /all and hostname 1. The ipconfig /all command displays the IP address, subnet mask, and default gateway for all adapters on the computer 1. The hostname command displays the name of the computer 1.

最新問題: **130**
ユーザーのコンピュータの動作が通常より遅くなり、起動に時間がかかります。問題を調査するために技術者が最初に使用すべきツールは次のうちどれですか?
A. アクション センター
B. タスクマネージャー
C. リソース モニター
D. セキュリティ構成ウィザード
E. イベント ビューア
Answer: (解答を表示する**)**
When a computer is running slower than usual and experiences long startup times, the first tool to use is:
* Task Manager: This utility provides real-time data on the processes and applications consuming system resources like CPU, memory, and disk usage. By identifying resource-heavy processes, a technician can take steps to optimize performance or identify malicious software.

最新問題: **131**
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: C (メーッセージを残す**)**
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: **132**
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: A,F (メーッセージを残す)
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**: 133**
複数の世代の Microsoft オペレーティング システム間で USB フラッシュ ドライブの読み取りと書き込みの互換性を確保するために最適なファイル システム フォーマットは、次のうちどれですか?
A. APFS
B. ext4
C. CDFS
D. FAT32
Answer: D (メーッセージを残す)
The best filesystem format to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems is FAT32. FAT32 stands for File Allocation Table 32-bit and is a filesystem format that organizes and manages files and folders on storage devices using 32-bit clusters.
FAT32 is compatible with most Microsoft operating systems since Windows 95 OSR2, as well as other operating systems such as Linux and Mac OS X. FAT32 can support storage devices up to 2TB in size and files up to 4GB in size. APFS stands for Apple File System and is a filesystem format that organizes and manages files and folders on storage devices using encryption, snapshots and cloning features. APFS is compatible with Mac OS X 10.13 High Sierra and later versions but not with Microsoft operating systems natively. Ext4 stands for Fourth Extended File System and is a filesystem format that organizes and manages files and folders on storage devices using journaling, extents and delayed allocation features. Ext4 is compatible with Linux operating systems but not with Microsoft operating systems natively.

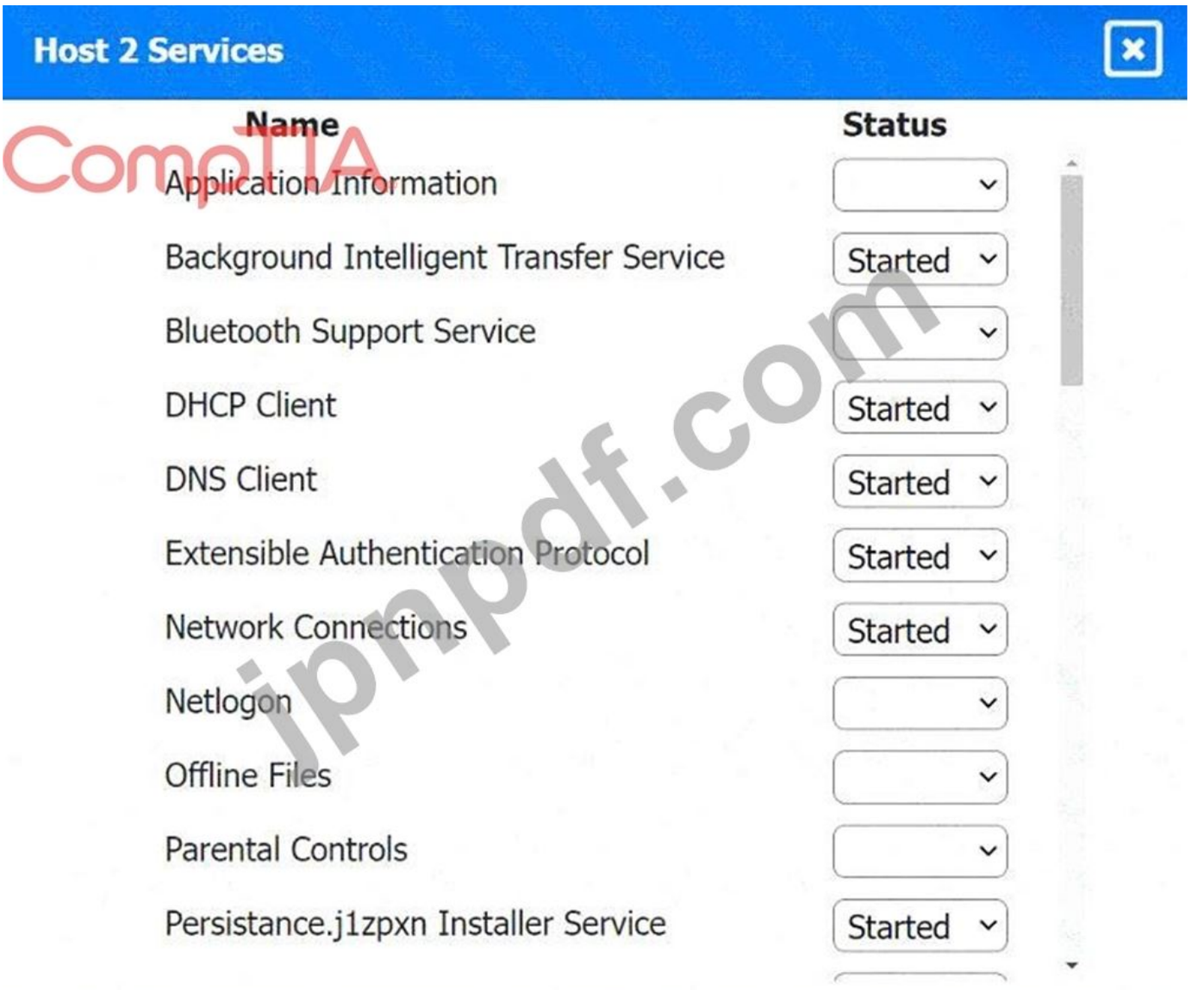
最新問題**: 134**
ユーザーは SOHO PC 用のウイルス対策ソフトウェアを入手したいと考えています。技術者はライセンス付きソフトウェア製品を推奨しますが、ユーザーはライセンス料を支払いたくありません。技術者が推奨するライセンスの種類は次のうちどれですか?
A. 法人
B. オープンソース
C. 個人的なもの
D. エンタープライズ

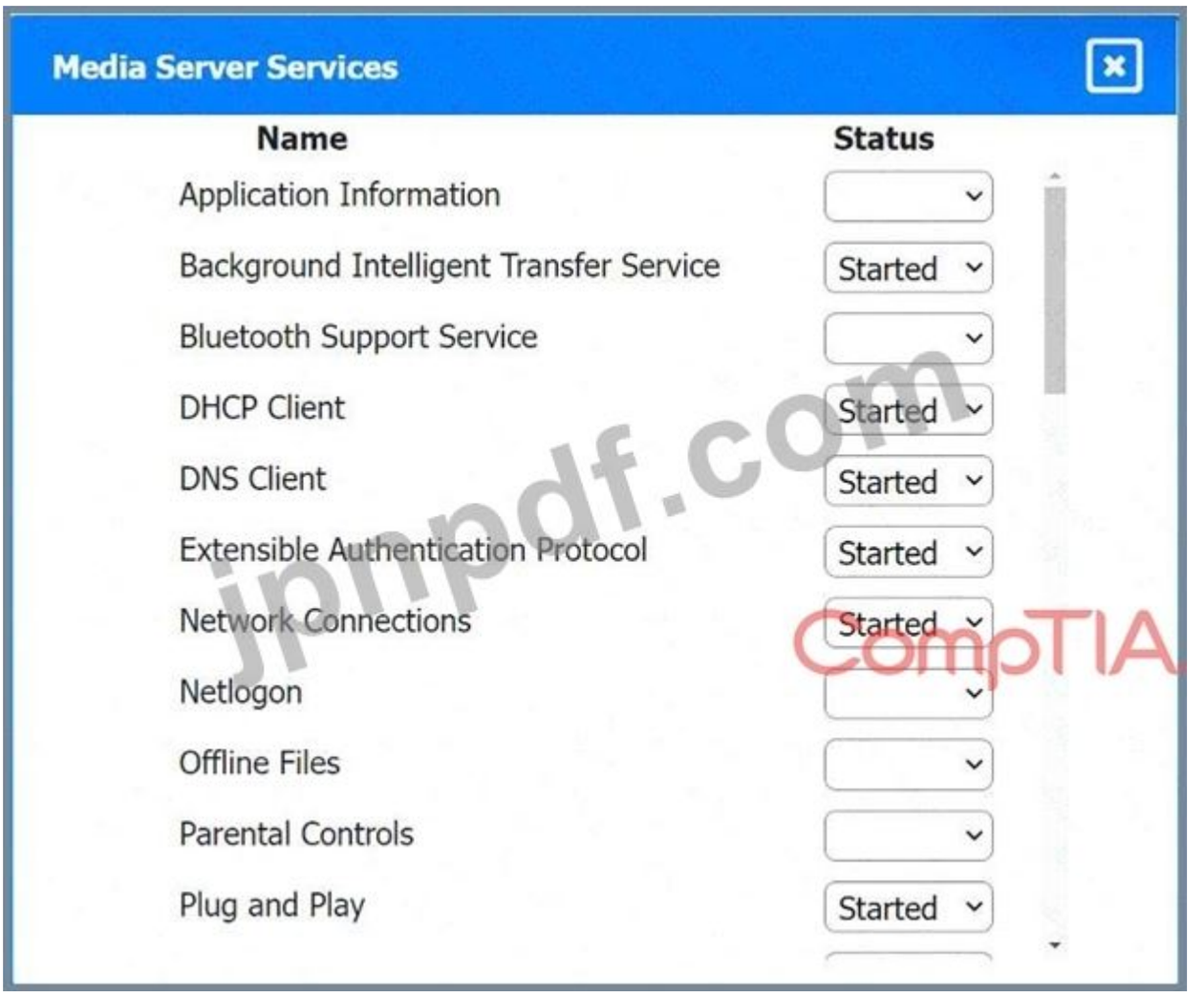
Answer: B (メーッセージを残す)
Open-source software is software that has its source code available for anyone to inspect, modify, and distribute. Open-source software is usually free of charge and does not require a license to use. Some examples of open-source antivirus software are ClamAV, Comodo, and Immunet12. The other license types are either not free or not suitable for a SOHO PC. Corporate and enterprise licenses are designed for large- scale organizations and networks, and they usually require a subscription fee. Personal licenses are for individual users and may have limited features or support.
References: 1 What is Open Source Software? - Definition from Techopedia(https://www.tomsguide.com/us /best-antivirus,review-2588.html). 2 7 Best Lifetime License Antivirus Tools [2023 Guide] - Windows Report (https://windowsreport.com/antivirus-with-unlimited-validity/).

最新問題**: 135**
技術者は、特定のドメインをブロックするために、いくつかの PC でホスト ファイルを編集しています。hostsファイルを編集した後、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. 無差別モードを有効にします。
B. ブラウザのキャッシュをクリアします。
C. 新しいネットワーク アダプターを追加します。
D. ネットワーク アダプタをリセットします。
Answer: D (メーッセージを残す)
Resetting the network adapter is the best way to apply the changes made to the hosts file on a few PCs. The hosts file is a text file that maps hostnames to IP addresses and can be used to block certain domains by redirecting them to invalid or local addresses. Resetting the network adapter will clear the DNS cache and force the PC to use the new entries in the hosts file.

最新問題**: 136**
ある企業は従業員にスマートフォンを支給しており、デバイスが紛失または盗難にあった場合にデータを保護する必要があります。次のうち、最適なソリューションを提供するのはどれですか?
A. マルウェア対策
B. リモートワイプ
C. ロケータ アプリケーション
D. 画面ロック
Answer: B (メーッセージを残す)
This is because remote wipe allows the data on the smartphone to be erased remotely, which helps to ensure that sensitive data does not fall into the wrong hands.

最新問題**: 137**
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。





Answer:

See the Explanation for the solution.

Explanation:

Host 2 and Media Server put them to Quarantine.

最新問題**: 138**

ワークステーションには、ユーザーが暗号通貨を復号キーと交換する必要があることを示すメッセージが表示されます。技術者がデバイスを安全にサービスに戻すための最善の方法は次のうちどれですか?

A. AV スキャンを実行します。

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. ソフトウェアファイアウォールをインストールします。

D. システムの復元を実行します。

E. 画面の指示に従ってください。

Answer: (解答を表示する**)**

The best way for a technician to return the device to service safely is to reinstall the operating system. This is because the device is infected by ransomware, which is a form of malware that encrypts files and demands payment for decryption. Reinstalling the operating system will erase the ransomware and restore the device to its original state. However, this will also delete any data that was not backed up before the infection.
Therefore, it is important to have regular backups of critical data and protect them from ransomware attacks1.
The other options are not effective or safe for ransomware recovery. Running an AV scan may not detect or remove the ransomware, especially if it is a new or unknown variant. Installing a software firewall may prevent future attacks, but it will not help with the current infection. Performing a system restore may not work if the ransomware has corrupted or deleted the restore points. Complying with the on-screen instructions is not advisable, as it will encourage the attackers and there is no guarantee that they will provide the decryption key after receiving the payment.
To prevent and recover from ransomware attacks, it is recommended to follow some best practices, such as234:
* Use strong passwords and multifactor authentication for all accounts and devices.
* Keep all software and firmware updated with the latest security patches.
* Avoid opening suspicious or unsolicited emails and attachments.
* Educate users and staff on how to recognize and report phishing and social engineering attempts.
* Use antivirus software and enable real-time protection.
* Enable network segmentation and firewall rules to limit the spread of ransomware.
* Implement a Zero Trust security model to verify all requests and devices before granting access.
* Create and test backups of critical data and store them offline or in a separate network.
* Recover safely by isolating the infected devices, identifying the ransomware variant, and restoring data from backups.
* Report any ransomware incidents to law enforcement agencies and seek help from experts.

最新問題**: 139**
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: (解答を表示する**)**

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: **140**
システム管理者は、ドメイン上のコンピュータの集中デスクトップ管理を構成しています。管理チームは、すべてのユーザーのワークステーションに同じネットワーク ドライブ、プリンタ、構成を持たせる必要があると決定しました。管理者がこのタスクを実行するには次のどれを使用する必要がありますか?
A. ネットワークと共有センター
B. 純使用量
C. ユーザーアカウント
D. レジストリ編集
E. グループポリシー
Answer: E (メーッセージを残す**)**
Group Policy is a feature of Windows that allows administrators to centrally manage and apply policies and settings to computers and users on a domain3. Group Policy can be used to configure network drives, printers, security settings, desktop preferences, and other configurations for all users' workstations3. Network and Sharing Center, net use, User Accounts, and regedit are not tools that can accomplish this task.

最新問題: **141**
ユーザーはヘルプデスクに電話して、スマートフォンの問題を報告します。出張から戻った後、スマートフォンで Wi-Fi 接続がないと、電子メールにアクセスしたり、Web サイトにアクセスしたりできなくなります。
問題を解決するためにユーザー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. 携帯データ通信を有効にします。
B. データ制限を増やします。
C. VPN を切断します。
D. SIMカードを再インストールします。
Answer: A (メーッセージを残す**)**
The most likely solution to this issue is to enable cellular data. After a business trip, the user may have disabled cellular data to avoid roaming charges, or the phone may have been set to Wi-Fi only for internet access. Enabling cellular data would restore internet access outside of Wi-Fi networks.
Reference: CompTIA A+ 220-1101 Exam Objectives, Domain 1.4 Mobile Devices - Wireless/Cellular Network

最新問題: **142**
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: **143**
技術者は、Windows 10 ラップトップで BitLocker を有効にしたいと考えていますが、コントロール パネルで BitLocker ドライブ暗号化のメニュー項目を見つけることができません。技術者がこのメニュー項目を見つけられない理由を説明しているのは、次のうちどれですか?
A. ハードウェアが BitLocker の最小システム要件を満たしていません。
B. BitLocker は Windows 10 用に名前が変更されました。
C. BitLocker は Windows 10 Home には含まれていません。
D. ラップトップのレジストリで BitLocker が無効になっています
Answer: C (メーッセージを残す**)**

BitLocker is only available on Windows 10 Pro, Enterprise, and Education editions1. Therefore, the technician is unable to find the BitLocker Drive Encryption menu item in Control Panel because it is not included in the Windows 10 Home edition1.

最新問題: **144**
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: **145**
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: (解答を表示する**)**
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: **146**
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: (解答を表示する**)**
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**: 147**
ユーザーの携帯電話のバッテリーが長持ちせず、ナビゲーションが非常に遅いです。問題を解決するために技術者が最初に行うべきことはどれですか?
A. 使用していないプログラムをアンインストールする
B. 実行中のアプリケーションを確認する
C. モバイルOSを更新する
D. ネットワークサービスを無効にする
Answer: (解答を表示する**)**
Checking running applications (Option B) is the best first step, as background apps consume CPU, RAM, and battery. Identifying and closing resource-heavy apps can immediately improve performance and battery life.
Uninstall unused programs (Option A): Helps free up storage, but it does not address performance and battery drain as directly as managing running apps.
Update the mobile OS (Option C): Important but may not provide immediate relief, and updates sometimes cause additional issues.
Disable network services (Option D): While turning off features like Wi-Fi or Bluetooth can save battery, it does not directly address slow performance.
Reference: CompTIA A+ Core 2 (220-1102) Exam Objectives - 3.4: Given a scenario, troubleshoot and resolve mobile device issues.

最新問題**: 148**
ユーザーは、オンライン バンキング サイトから次のようなエラー メッセージを受け取ります。あなたの接続は非公開ではありません。権限が無効です。
ユーザーが次に取るべきアクションは次のうちどれですか?
A. サイトに進みます。
B. 別のブラウザを使用してください。
C. 銀行にエラーを報告します。
D. ブラウザを再インストールします。
Answer: C (メーッセージを残す**)**

The error message "Your connection is not private. Authority invalid." means that the web browser cannot verify the identity or security of the website's SSL certificate. This could indicate that the website has been compromised, has a configuration error, or has an expired or invalid certificate. The user should not proceed to the site or use a different browser, as this could expose their sensitive information to potential attackers.
The user should also not reinstall the browser, as this is unlikely to fix the error and could cause data loss. The best action for the user to take is to report the error to the bank and wait for them to resolve it.
References: : How to Fix "Your Connection Is Not Private" Errors (https://www.howtogeek.com/874436/how- to-fix-your-connection-is-not-private-errors/) : Fix connection errors (https://support.google.com/chrome /answer/6098869?hl=en)

最新問題**: 149**
技術者が、落としたモバイル デバイスのトラブルシューティングを行っています。技術者は、設定が正しく適用されているにもかかわらず、画面が回転しないことを発見しました。技術者が問題を解決するには、次のどのハードウェアを交換する必要がありますか?
A. 液晶
B. バッテリー
C. 加速度計
D. デジタイザー
Answer: C (メーッセージを残す**)**
The piece of hardware that the technician should replace to resolve the issue of the screen failing to rotate on a mobile device that was dropped is the accelerometer. The accelerometer is a sensor that detects the orientation and movement of the mobile device by measuring the acceleration forces acting on it. The accelerometer allows the screen to rotate automatically according to the position and angle of the device. If the accelerometer is damaged or malfunctioning, the screen may not rotate properly or at all, even if the settings are correctly applied. LCD stands for Liquid Crystal Display and is a type of display that uses liquid crystals and backlight to produce images on the screen. LCD is not related to the screen rotation feature but to the quality and brightness of the display. Battery is a component that provides power to the mobile device by storing and releasing electrical energy. Battery is not related to the screen rotation feature but to the battery life and performance of the device. Digitizer is a component that converts touch inputs into digital signals that can be processed by the mobile device. Digitizer is not related to the screen rotation feature but to the touch sensitivity and accuracy of the display.
References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.5

最新問題**: 150**
クレジット カードを保護するためのデータ セキュリティ基準は次のうちどれですか?
A. ファイ

B. NIST
C. PCI
D. GDPR
Answer: (解答を表示する**)**
The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

最新問題**: 151**
顧客のコンピューターに USB 専用プリンターが接続されています。技術者は、ネットワーク上の他のコンピューターでプリンターを使用できるように設定しています。技術者は、顧客のデスクトップのどの場所でこの設定を行う必要がありますか?
A. 印刷設定/詳細設定タブ
B. プリンターのプロパティ/共有タブ
C. プリンターのプロパティ/セキュリティタブ
D. プリンターのプロパティ/ポートタブ
Answer: B (メーッセージを残す**)**
The correct answer is B. Printer Properties/Sharing tab. This is the location where the technician can enable printer sharing and assign a share name for the USB printer. This will allow other computers on the network to access the printer by using the share name or the IP address of the computer that has the printer attached1.
1: CompTIA A+ Certification Exam: Core 2 Objectives, page 15, section 1.9.

最新問題**: 152**
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**: 153**
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**: 154**
安全な内部ネットワークにアクセスしようとすると、「この Web サイトのセキュリティ証明書には問題があります」というエラー メッセージが表示されます。ユーザーはデスクトップを再起動

し、Web サイトに再度アクセスしようとしますが、問題は解決しません。このエラーの再発を防ぐ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. システムを再イメージ化し、SSL をインストールします。
B. 信頼されたルート証明書をインストールします。
C. [証明書の表示]、[証明書のインストール] の順に選択します。
D. 引き続き Web サイトにアクセスします。
Answer: C (メーッセージを残す**)**
The error message indicates that the website's security certificate is not trusted by the user's device, which may prevent the user from accessing the secure internal network. To resolve this issue, the user can view the certificate details and install it on the device, which will add it to the trusted root certificate store. Reimaging the system and installing SSL, installing Trusted Root Certificate, or continuing to access the website are not recommended solutions, as they may compromise the security of the device or the network.

最新問題**: 155**
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: (解答を表示する**)**
https://www.educba.com/shell-scripting-in-linux/

最新問題**: 156**
技術者は、次の症状がある従業員のスマートフォンを調査しています
※本機は使用していなくても熱くなっています。
* 特に他のアプリケーションを起動するとアプリケーションがクラッシュする
* GPS などの特定のアプリケーションは、ランドスケープ モードである必要があるときにポートレート モードになっています。これらの問題を最小限の影響で解決するために、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? (2 つ選択)。
A. オートローテーションをオンにする
B. 機内モードを有効にします。
C. 不要なアプリケーションを閉じる
D. ファクトリー リセットを実行します。
E. デバイスのオペレーティング システムを更新します。
F. クラッシュしたアプリケーションを再インストールします。
Answer: A,C (メーッセージを残す**)**
The technician can close unnecessary applications and turn on autorotation to resolve these issues with minimal impact. Autorotation can help the device to switch between portrait and

landscape modes automatically. Closing unnecessary applications can help to free up the device's memory and reduce the device's temperature1 Reference:
CompTIA A+ Certification Exam: Core 2 (220-1102) Exam Objectives Version 4.0. Retrieved from https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

最新問題: **157**
ユーザーが追加のソフトウェアをインストールしようとすると、UAC プロンプトが表示されます。この問題を解決する最善の方法は次のうちどれですか?
A. ローカル管理者のグループにユーザー アカウントを追加します。
B. すべてのネットワークへのアクセスを許可するように Windows Defender ファイアウォールを構成します。
C. Microsoft アカウントを作成します。
D. ゲストアカウントを無効にします。
Answer: A (メーッセージを残す**)**
A user account that belongs to the local administrator's group has the permission to install software on a Windows machine. If a user receives a UAC (user account control) prompt when trying to install software, it means the user does not have enough privileges and needs to enter an administrator's password or switch to an administrator's account. Adding the user account to the local administrator's group can resolve this issue.
Configuring Windows Defender Firewall, creating a Microsoft account and disabling the guest account are not related to this issue. Verified References: https://www.comptia.org/blog/user-account-control https://www.
comptia.org/certifications/a

最新問題: **158**
証拠の一部を扱う場合、法医学的証拠のライフサイクル全体で維持する必要があるのは、次のうちどれですか?
A. 使用可
B. 保管の連鎖
C. セキュリティ ポリシー
D. 情報管理
Answer: (解答を表示する**)**
The aspect of forensic evidence life cycle that must be maintained when dealing with a piece of evidence is chain of custody. This is because chain of custody is the documentation of the movement of evidence from the time it is collected to the time it is presented in court, and it is important to maintain the integrity of the evidence

最新問題: **159**

技術者が、Windows Defender を実行できない PC のトラブルシューティングを行っています。Windows Defender は無効になっており、他のウイルス対策ソフトウェアは PC にインストールされていません。この問題の原因は次のどれでしょうか。
A. ランサムウェア
B. ルートキット
C. スパイウェア
D. キーロガー
Answer: B (メーッセージを残す**)**
Rootkits are particularly dangerous because they modify the operating system to hide their presence and can disable antivirus software like Windows Defender. Ransomware (A) encrypts files, but usually does not disable antivirus software. Spyware (C) and Keyloggers (D) typically do not directly disable antivirus programs either.
Reference: Core 2, Domain 2.3 - Malware types and impacts.

最新問題**: 160**
ある企業が DDoS 攻撃を受けています。いくつかの内部ワークステーションがトラフィックの送信元です。次の種類の感染のうち、ワークステーションで発生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. ゾンビ
B. キーロガー
C. アドウェア
D. ボットネット
E. ランサムウェア
F. スパイウェア
Answer: A,D (メーッセージを残す**)**
Zombies and botnets are terms that describe the types of infections that can cause internal workstations to participate in a DDoS (distributed denial-of-service) attack. A DDoS attack is a malicious attempt to disrupt the normal functioning of a website or a network by overwhelming it with a large amount of traffic from multiple sources. Zombies are infected computers that are remotely controlled by hackers without the owners' knowledge or consent. Botnets are networks of zombies that are coordinated by hackers to launch DDoS attacks or other malicious activities. Keylogger, adware, ransomware, and spyware are not types of infections that can cause internal workstations to participate in a DDoS attack.

最新問題**: 161**
顧客から、Android スマートフォンでは非接触型電子決済が利用できないとの報告がありました。この問題を解決するには、次のどれを有効にする必要がありますか?
A. Wi-Fi
B. 近くのシェア
C. NFC

D. ブルートゥース
Answer: C (メーッセージを残す**)**
To enable contactless payment, NFC (Near Field Communication) (Option C) needs to be enabled. NFC is the technology used in most mobile payment systems to enable close-range communication between the phone and a payment terminal.
* Wi-Fi (Option A) and Bluetooth (Option D) are unrelated to contactless payments.
* Nearby share (Option B) is a file-sharing feature, not a payment technology.
CompTIA A+ Core 2 References:
* 2.7 - Explain common mobile device security settings, including enabling NFC for mobile payments.

最新問題**: 162**
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。技術者が次に行うべきことは次のうちどれですか?
A. HDD を取り外し、コンピュータを修理に出してください。
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を離れる前に機密情報を削除します。
D. 管理者から承認を得る。
Answer: D (メーッセージを残す**)**
The next step that the technician should do before taking the computer off site for repair is to get authorization from the manager. Getting authorization from the manager is important because it ensures that the technician has permission and approval to remove the computer from the premises and perform the repair work off site.
Getting authorization from the manager can also help document and communicate the reason and duration of the repair and avoid any misunderstanding or conflict with the user or the organization. Removing the HDD and then sending the computer for repair may not be feasible or necessary if the issue is not related to the HDD or if the HDD contains essential data or software for the repair. Checking corporate policies for guidance may be a good step but it does not replace getting authorization from the manager who is responsible for the computer and its data. Deleting the sensitive information before the computer leaves the building may not be possible or advisable if the issue prevents access to the data or if the data is needed for troubleshooting or recovery purposes. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

最新問題**: 163**
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**: 164**
技術者は、ネットワークにアクセスできない場所でデスクトップのイメージを再作成する必要があります。技術者は次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. USB
B. PXE
C. 光学メディア
D. パーティション
E. ブートレコード
F. SMB
Answer: A,C (メーッセージを残す)
A technician needs to reimage a desktop in an area without network access, which means that the technician cannot use network-based methods such as PXE or SMB to deploy the image. Therefore, the technician should use offline methods that involve removable media such as USB or optical media. USB and optical media are common ways to store and transfer system images, and they can be used to boot the desktop and initiate the reimaging process. The technician will need to create a bootable USB or optical media that contains the system image and the imaging software, and then insert it into the desktop and change the boot order in the BIOS or UEFI settings. The technician can then follow the instructions on the screen to reimage the desktop

最新問題**: 165**

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: (解答を表示する**)**
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**: 166**
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: (解答を表示する**)**
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**: 167**
システム管理者は、キオスク マシンからの異常な量のネットワーク トラフィックを監視しているため、トラフィックの送信元を特定するために調査する必要があります。管理者は、キオスク マシン上のどのプロセスがインターネットに接続しているかを確認するために、次のツールのうちどれを使用できますか?
A. リソースモニター
B. パフォーマンスモニター
C. コマンドプロンプト
D. システム情報
Answer: (解答を表示する**)**
Resource Monitor is a tool that shows the network activity of each process on a Windows machine, including the TCP connections and the sent and received bytes. Performance Monitor is a tool that shows the performance metrics of the system, such as CPU, memory, disk and network usage. Command Prompt is a tool that allows running commands and scripts on a Windows machine. System Information is a tool that shows the hardware and software configuration of a Windows machine. Verified References: https://www.comptia.org/blog/how-to-use-resource-monitor https://www.comptia.org/certifications/a

最新問題**: 168**
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**: 169**
デスクトップ エンジニアがマスター イメージを展開しています。デスクトップ エンジニアがマスター イメージを構築する際に考慮する必要があるのは、次のうちどれですか? (2 つ選択)。
A. デバイスドライバー
B. キーボードのバックライト設定
C. インストールされているアプリケーションのライセンス キー
D. ディスプレイの向き
E. ターゲットデバイスの電源
F. エクスプレス充電を無効にする
Answer: A,C (メーッセージを残す**)**
* A. Device drivers23: Device drivers are software components that enable the operating system to communicate with hardware devices. Different devices may require different drivers, so the desktop engineer should include the appropriate drivers in the master image or configure the deployment process to install them automatically.
* C. Installed application license keys2: Installed application license keys are codes that activate or authenticate software applications. Some applications may require license keys to be entered during installation or after deployment. The desktop engineer should include the license keys in the master image or configure the deployment process to apply them automatically.

最新問題**: 170**
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: (解答を表示する**)**

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**: 171**
フラッシュ ドライブが接続されているときに、悪意のあるファイルが自動的に実行されました。この種のインシデントを防ぐ機能は次のどれですか?
A. UAC を無効にする
B. ローカル管理者を制限する
C. UPnPを有効にする
D. 自動再生をオフにする
Answer: (解答を表示する**)**
AutoPlay is a feature that automatically runs programs or files when a removable media device, such as a flash drive, is plugged in. This can be exploited by malware authors who place malicious files on flash drives that execute automatically when inserted into a computer. Turning off AutoPlay can prevent this type of incident by requiring the user to manually open or run files from removable media devices. Disabling UAC (user account control), restricting local administrators and enabling UPnP (universal plug and play) are not effective ways to prevent this type of incident. Verified References: https://www.comptia.org/blog/autoplay- security-risk https://www.comptia.org/certifications/a

最新問題**: 172**
ユーザーは、Web ベースの独自のオペレーティング システムを搭載したネットブックを購入しました。次のオペレーティング システムのうち、ネットブック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. macOS
B. Linux
C. Chrome OS
D. Windows
Answer: C (メーッセージを残す**)**
4. Chrome OS. Retrieved from https://en.wikipedia.org/wiki/Chrome_OS 5. What is Chrome OS? Retrieved from https://www.google.com/chromebook/chrome-os/ A netbook with a web-based, proprietary operating system is most likely running Chrome OS. Chrome OS is a web-based operating system developed by Google that is designed to work with web applications and cloud storage. It is optimized for netbooks and other low-power devices and is designed to be fast, secure, and easy to use.

最新問題**: 173**

次の物理的なセキュリティ制御のうち、ラップトップの盗難を防ぐことができるものはどれですか?
A. 暗号化
B. ロージャック
C. 多要素認証
D. 機器ロック
E. 車止め
Answer: D (メーッセージを残す)
An equipment lock is a physical security device that attaches a laptop to a fixed object, such as a desk or a table, with a cable and a lock. This can prevent the laptop from being stolen by unauthorized persons.
Encryption, LoJack, multifactor authentication and bollards are other security measures, but they do not physically prevent theft. Verified References: https://www.comptia.org/blog/physical-security https://www.
comptia.org/certifications/a

最新問題**: 174**
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: (解答を表示する)
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: **175**
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: D (メーッセージを残す**)**
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: **176**
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: (解答を表示する**)**
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**: 177**
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 (メーッセージを残す**)**
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**: 178**
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: (解答を表示する**)**
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**: 179**

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**: 180**
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**: 181**

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**: 182**

エンドユーザー情報に関する政府のポリシーによって保護されているのは次のどれですか?

A. DRM

B. EULA

C. PCI

D. PII

Answer: D (メーッセージを残す**)**

Personally Identifiable Information (PII) (Option D) is protected by government regulations. PII includes sensitive data such as names, addresses, social security numbers, and other information that can identify individuals. Various laws, such as GDPR and HIPAA, mandate the protection of PII.

* DRM (Option A) refers to digital rights management, which controls access to digital media.

* EULA (Option B) refers to software licensing agreements.

* PCI (Option C) relates to payment card industry standards for handling cardholder information but is more specific to payment data than general PII.
CompTIA A+ Core 2 References:
* 4.6 - Explain prohibited content and privacy concepts, including the protection of PII.

最新問題: **183**
技術者は、会社の新しいセキュリティ ポリシーによって、支社で使用中のアプリケーションが機能しなくなったことを発見しました。
アプリケーションが修正され、問題が再発しないようにするために、技術者は次のどれを実行する必要がありますか?
A. アプリケーションの要件が満たされるまでの間、ポリシーの例外を適用するよう要求する
B. 各コンピュータのローカル管理者権限を使用して、影響を受けるソフトウェアを再インストールします。
C. 新しいセキュリティ設定を削除し、ブランチオフィスのコンピュータの管理アカウントを変更して、設定が再適用されないようにする
D. 新しいポリシーによって悪影響を受けない代替アプリケーションを調査して入手する
Answer: A (メーッセージを残す**)**
Comprehensive and Detailed In-Depth Explanation:
If a new security policy disrupts an essential application, the best course of action is to request a policy exception while a permanent solution is developed. This allows the application to function while ensuring compliance with company security policies.
* B. Reinstall the affected software using local administrative rights for each computer - Incorrect. If the security policy is blocking the application, reinstalling it will not resolve the issue.
* C. Remove the new security settings and change administrative accounts - Incorrect. Altering security settings without approval could violate company policies and create security risks.
* D. Research and procure a replacement application - Incorrect. While replacing the application may be an option, it is not an immediate solution to restoring functionality.
Reference:
CompTIA A+ 220-1102, Objective 2.2 - Security Best Practices

最新問題: **184**
警察官は、一度に数分間ワークステーションを離れることがよくあります。次のうち、警官が立ち去るときにワークステーションをすばやく保護するための最良の方法はどれですか?
A. キーの組み合わせを使用して、コンピュータを離れるときにロックします。
B. 許可されていない人員がそのエリアにいないことを確認してください。
C. 約 30 分間非アクティブな状態が続くと、コンピューターを自動的にロックするようにスクリーンセーバーを構成します。
D. モニターの電源をオフにして、情報が不正に閲覧されるのを防ぎます。
Answer: A (メーッセージを残す**)**

The BEST way to secure the workstation quickly when walking away is to use a key combination to lock the computer when leaving1

最新問題: **185**
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: **186**
刑事訴訟において、証拠が有効であるとみなされるために、証拠が触れられたり譲渡されたりするたびに更新する必要がある文書は次のどれですか。
A. ライセンス契約
B. 規制遵守
C. インシデントドキュメント
D. 保管の連鎖
Answer: D (メーッセージを残す**)**
In criminal proceedings, maintaining the integrity of evidence is crucial. The document that must be updated every time evidence is handled or transferred is:

* Chain of custody: This document tracks the history of the evidence, detailing every person who has handled it and every transfer that has occurred. It ensures that the evidence has not been tampered with and maintains its validity in court.
* Licensing agreement: Pertains to software usage rights and has no relation to evidence handling.
* Regulatory compliance: Refers to adherence to laws and regulations, not evidence tracking.
* Incident documentation: Details the incident but does not specifically track evidence handling.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 4.6: Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.
Legal documentation and evidence handling procedures.

最新問題**: 187**
ユーザーは Windows 10 デバイスをバックアップしたいと考えています。ユーザーは次のうちどれを選択する必要がありますか?
A. デバイスとプリンター
B. 電子メールとアカウント
C. アップデートとセキュリティ
D. アプリと機能
Answer: C (メーッセージを残す**)**
Update and Security is the section in Windows 10 Settings that allows the user to back up their device.
Backing up a device means creating a copy of the data and settings on the device and storing it in another location, such as an external drive or a cloud service. Backing up a device can help the user restore their data and settings in case of data loss, corruption, or theft. Devices and Printers, Email and Accounts, and Apps and Features are not sections in Windows 10 Settings that allow the user to back up their device.

最新問題**: 188**
組織全体で広く使用されている Web サイトにユーザーがアクセスできず、次のエラー メッセージが表示されます。
この Web サイトで提示されたセキュリティ証明書は、有効期限が切れているか、まだ有効ではありません。
技術者は、ユーザーのコンピューターからではなく、別のコンピューターから Web サイトにアクセスしたときに Web サイトが機能することを確認します。問題をトラブルシューティングするために技術者が次の手順を実行する必要があるのは、次のうちどれですか?
A. コンピュータを再起動します。
B. OS を再インストールします。
C. 静的 12 を構成します。
D. コンピュータの日付と時刻を確認します。

Answer: (解答を表示する**)**
The error message indicates that the security certificate presented by the website has either expired or is not yet valid. This can happen if the computer's clock has the wrong date or time, as SSL/TLS certificates have a specific validity period. If the clock is off by too much, it may cause the certificate to fail to validate.
Therefore, the technician should check the computer's date and time and ensure that they are correct.

最新問題**: 189**
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**: 190**
Active Directory アカウント作成のスクリプト作成に使用される言語は次のどれですか?
A. バッシュ
B. 構造化クエリ言語
C. ハイパーテキスト プリプロセッサ
D. PowerShell
Answer: D (メーッセージを残す**)**
For scripting the creation of Active Directory accounts, PowerShell (D) is used. PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and the associated scripting language. It is built on the .NET framework and is particularly suited for automating and managing Windows-based systems, including Active Directory tasks.

最新問題**: 191**

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: B (メーッセージを残す**)**
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**: 192**
ある企業では WAP を設置し、新しいラップトップとドッキング ステーションを全従業員に配備しました。ドッキング ステーションは LAN ケーブルを介して接続されます。現在、ユーザーからネットワーク サービスの低下が報告されています。IT 部門は、WAP メッシュ ネットワークで予想を超える量のトラフィックが発生していると判断しました。ワイヤレス ネットワークが予想されるワイヤレス ユーザー数を確実にサポートできるようにする最も効率的な方法は次のうちどれですか?
A. モバイル以外のユーザーのラップトップを有線デスクトップ システムに置き換える
B. ワイヤレス ネットワーク アダプターのメトリックを増やす
C. 建物全体にワイヤレス リピータを追加する
D. 802.11 n 仕様をサポートするために現在のメッシュ ネットワークをアップグレードします。
Answer: (解答を表示する**)**
When a WAP (Wireless Access Point) mesh network is experiencing a higher than anticipated amount of traffic, leading to degraded network service, upgrading the network to a more advanced wireless standard can help alleviate the problem. The 802.11n specification, also known as Wireless-N, offers significant improvements over earlier standards like 802.11b/g in terms of speed, range, and reliability. It allows for increased data throughput and better coverage, which can support a higher number of wireless users effectively.

* Upgrading to 802.11n: This involves replacing existing WAPs with those that support the 802.11n standard or higher. The upgrade can result in improved network performance by accommodating more wireless connections with higher data rates, reducing congestion and improving overall network efficiency.
Replacing non-mobile users' laptops with wired desktop systems (A) could reduce wireless traffic but may not be feasible or desirable for all users. Increasing the wireless network adapter metric (B) would affect route priority but not overall network capacity. Adding wireless repeaters (C) can extend the range but might also introduce additional latency and does not necessarily increase the network's capacity to handle more users efficiently.

最新問題: **193**
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: **194**
技術者は、ユーザーのコンピューターがウイルスに感染していることを確認しました。ウイルス対策ソフトウェアは最新ではありません。技術者が次に取るべきステップはどれですか?
A. コンピュータを隔離します。
B. 以前の復元ポイントを使用します。
C. ウイルスについてエンド ユーザーを教育する
D. 最新のウイルス定義をダウンロード
Answer: (解答を表示する**)**
The first step in removing a virus from a computer is to update the antivirus software with the latest virus definitions. Virus definitions are files that contain information about the characteristics and behavior of known viruses and malware. They help the antivirus software to identify and remove the malicious threats from the computer. Without the latest virus definitions, the antivirus software may not be able to detect or remove the virus that infected the user's computer.
Therefore, the technician should download the latest virus definitions from the antivirus vendor's

website or use the update feature in the antivirus program before scanning the computer for viruses.
References:
How to remove malware or viruses from my Windows 10 PC, section 21
How to Remove a Virus From a Computer in 2023, section 32
The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2193

最新問題**: 195**
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: (解答を表示する**)**
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**: 196**
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:\Wlndows\wlndows.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**: 197**
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**: 198**
フォレンジック分析のためにハード ドライブのデータを保存する場合、最も考慮すべきオプションは次のうちどれですか? (2 つ選択)。
A. ライセンス契約
B. 保管の連鎖

C. インシデント管理文書
D. データの完全性
E. 製品安全データシート
F. 保持要件
Answer: B (メーッセージを残す**)**
Chain of custody and data integrity are two options that should most likely be considered when preserving data from a hard drive for forensic analysis. Chain of custody refers to the documentation and tracking of who has access to the data and how it is handled, stored, and transferred. Data integrity refers to the assurance that the data has not been altered, corrupted, or tampered with during the preservation process

最新問題**: 199**
ユーザーのアクセス許可は、NTFS セキュリティ設定を使用した共有ネットワーク フォルダーでの読み取りに制限されます。このタイプのセキュリティ制御について説明しているのは次のうちどれですか?
A. SMS
B. MFA
C. ACL
D. MDM
Answer: C (メーッセージを残す**)**
ACL (access control list) is a security control that describes what permissions a user or group has on a shared network folder using NTFS (New Technology File System) security settings. It can be used to grant or deny read, write, modify, delete or execute access to files and folders. SMS (short message service), MFA (multifactor authentication), MDM (mobile device management) are not security controls that apply to shared network folders. Verified References: https://www.comptia.org/blog/what-is-an-acl https://www.comptia.org /certifications/a

最新問題**: 200**
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: B (メーッセージを残す**)**
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**: 201**
ユーザーが新しい Windows 10 ラップトップをセットアップしています。SSID とパスワードの入力には次の Windows 設定のどれを使用する必要がありますか?
A. ネットワークとインターネット
B. システム
C. パーソナライゼーション
D. アカウント
Answer: A (メーッセージを残す**)**
The Network & Internet settings in Windows 10 allow the user to input the SSID and password of a Wi-Fi network, as well as manage other network-related options, such as airplane mode, mobile hotspot, VPN, proxy, etc1. To access the Network & Internet settings, the user can select the Start button, then select Settings > Network & Internet2. Alternatively, the user can right-click the Wi-Fi icon on the taskbar and click
"Open Network & Internet Settings"3.
The System settings in Windows 10 allow the user to configure the display, sound, notifications, power, storage, and other system-related options1. The Personalization settings in Windows 10 allow the user to customize the background, colors, lock screen, themes, fonts, and other appearance-related options1. The Accounts settings in Windows 10 allow the user to manage the user accounts, sign-in options, sync settings, and other account-related options1. None of these settings can be used to input the SSID and password of a Wi-Fi network.
References:
The Official CompTIA A+ Core 2 Study Guide1, page 221, 222, 223, 224.

最新問題**: 202**
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: **203**
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: (解答を表示する**)**
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: **204**
技術者は、Linux コンピューターから Windows コンピューターに 20 GB のデータを転送するために、USB ドライブをフォーマットする必要があります。次のファイルシステムのうち、技術者が最も使用する可能性が高いのはどれですか?
A. FAT32
B. ext4
C. NTFS
D. exFAT
Answer: (解答を表示する**)**
exFAT is a file system that is supported by both Linux and Windows and can handle large files1.

最新問題: **205**
評判の良い銀行を名乗る詐欺師が会社の従業員に電話をかけます。この事件を説明しているのは次のうちどれですか?

A. 口実
B. なりすまし
C. ビッシング
D. スケアウェア
Answer: C (メーッセージを残す)
Vishing is a type of social engineering attack where a fraudulent caller impersonates a legitimate entity, such as a bank or financial institution, in order to gain access to sensitive information. The caller will typically use a variety of techniques, such as trying to scare the target or providing false information, in order to get the target to provide the information they are after. Vishing is often used to gain access to usernames, passwords, bank account information, and other sensitive data.

最新問題**: 206**
技術者が Windows 10 オペレーティング システムのベアメタル インストールを行っています。技術者がインストール プロセスを開始する前に、次の前提条件を満たしている必要があるのはどれですか?
A. インターネット接続
B. プロダクト キー
C. 十分なストレージ容量
D. UEFI ファームウェア
E. レガシー BIOS
Answer: C (メーッセージを残す)
Before starting a bare-metal installation of Windows 10, ensuring that there is sufficient storage space on the system's hard drive or SSD is crucial. This is because the installation files need enough room to be copied and for the operating system to be installed and function properly. Without adequate storage, the installation process can fail or the operating system might not perform optimally. Other prerequisites like internet connection, product key, and specific firmware types might be necessary at different stages of installation or activation, but the fundamental requirement is enough storage space to accommodate the new OS.

最新問題**: 207**
ユーザーが、コンピューターの実行速度が遅いと報告しています。技術者が問題を特定するのに役立つツールは次のうちどれですか?
A. ディスクのクリーンアップ
B. グループ ポリシー エディター
C. ディスクの管理
D. リソースモニター
Answer: D (メーッセージを残す)
Resource Monitor is a Windows utility that can be used to monitor and analyze the system resources and processes running on a computer. It can be used to identify and troubleshoot any

issues that might be causing the computer to run slowly, such as CPU usage, memory usage, disk I/O, and network usage.

最新問題**: 208**
ユーザーが Windows オペレーティング システムを最新の機能リリースにアップグレードした後、アップグレード前には正常に実行されていたレガシー アプリケーションの 1 つが一部のウィンドウを開かず、部分的にしか機能しないことに気付きました。この問題のトラブルシューティングを行うには、次のどのアクションを実行する必要がありますか。
A. アプリケーションを管理者として実行します。
B. ユーザー アカウント制御レベルを上げます。
C. Windows Defender ファイアウォールをオフにします。
D. アプリケーションの互換モードを無効にします。
Answer: A (メーッセージを残す**)**
When a legacy application is not fully functional after upgrading the Windows operating system, the first step to troubleshoot the issue is to:
* Run the application as Administrator: Legacy applications often require administrative privileges to run correctly. Running the application with these privileges can resolve issues related to permissions and access to certain system resources.
* Raise the User Account Control level: This increases security prompts but does not resolve compatibility issues.
* Turn off Windows Defender Firewall: This can expose the system to security risks and is unlikely to resolve application functionality issues.
* Disable compatibility mode for the application: Compatibility mode should generally be enabled for legacy applications to ensure they run properly on newer OS versions.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 1.3: Given a scenario use features and tools of the Microsoft Windows 10 operating system (OS).
Windows application compatibility troubleshooting documentation.

最新問題**: 209**
技術者が共用エリアにあるコンピュータのセキュリティを設定しています。コンピュータの上にある標識には、許可されたユーザーだけがコンピュータを使用できることが示されています。オフィスを訪れるゲストは、オフィスに出入りする際にコンピュータの前を通らなければなりません。次のどれが物理的な脅威に対して最も効果的な保護を提供しますか?
A. 画面ロックの使用
B. プライバシースクリーンの取り付け
C. パスワードの複雑さの実装
D. コンピュータケースをロックする
E. ドライブ暗号化を有効にする
Answer: D (メーッセージを残す**)**

The best protection against physical threats, especially in a common area where the computer is publicly accessible, involves physically securing the hardware.
* Option A: Using screen lockScreen locks are good for securing access temporarily but do not protect against physical tampering or theft.
* Option B: Installing a privacy screenPrivacy screens prevent visual access but do not secure the hardware.
* Option C: Implementing password complexityPassword complexity helps secure digital access but does not prevent physical threats.
* Option D: Locking the computer casePhysically securing the case prevents unauthorized individuals from tampering with internal components or stealing the computer.
* Option E: Enabling drive encryptionEncryption protects data but does not prevent physical access to the hardware itself.
References:
CompTIA A+ 220-1102 Objective 2.1 (Physical security), particularly physical security measures like locking the computer case.

最新問題**: 210**
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: D (メーッセージを残す**)**
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**: 211**
技術者が、互換性のある正常なマザーボードを新しいラップトップに取り付けました。ただし、マザーボードはラップトップで動作していません。損傷を防ぐために、技術者が最も実行すべきだったのは次のうちどれですか?
A. 宝石をすべて外した
B. 使用前に道具の棚卸しを完了
C. 電気火災安全の実践
D. 適切な ESD ストラップを接続
Answer: (解答を表示する**)**

The technician should have connected a proper ESD strap to prevent damage to the motherboard. ESD (electrostatic discharge) can cause damage to electronic components, and an ESD strap helps to prevent this by grounding the technician and preventing the buildup of static electricity. Removing all jewelry is also a good practice, but it is not the most likely solution to this problem.

最新問題**: 212**
応答を停止したアプリケーションをユーザーが閉じるのに役立つ macOS の機能は次のうちどれですか?
A. ファインダー
B. ミッションコントロール
C. システム環境設定
D. 強制終了
Answer: (解答を表示する**)**
The correct answer is D. Force Quit. Force Quit is a macOS feature that allows users to close an application that has stopped responding. To use Force Quit, users can press and hold Option (or Alt), Command, and Esc (Escape) keys together, or choose Force Quit from the Apple menu in the corner of the screen. A Force Quit window will open, where users can select the application that they want to close and click Force Quit123.
References and Explanation:
The web search results provide information about how to force an app to quit on Mac using different methods, such as keyboard shortcuts, mouse clicks, or menu options. The results also explain what to do if the app cannot be forced to quit or if the Mac does not respond.
The first result1 is from the official Apple Support website and provides detailed instructions and screenshots on how to force an app to quit on Mac using the keyboard shortcut or the Apple menu. It also explains how to force quit the Finder app and how to restart or turn off the Mac if needed.
The second result2 is from the same website but for a different region (UK). It has the same content as the first result but with some minor differences in spelling and wording.
The third result4 is from a website called Lifehacker that provides tips and tricks for various topics, including technology. It compares how to close a program that is not responding on

different operating systems, such as Windows, Mac, and Linux. It briefly mentions how to force quit an app on Mac using the keyboard shortcut or the mouse click.
The fourth result3 is from a website called Parallels that provides software solutions for running Windows on Mac. It focuses on how to force quit an app on Mac using the keyboard shortcut and provides a video tutorial and a screenshot on how to do it. It also suggests some alternative ways to close an app that is not responding, such as using Activity Monitor or Terminal commands.

最新問題**: 213**
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-virtualization https://www.comptia.org/certifications/a

最新問題**: 214**
技術者は、ユーザーのドキュメント フォルダー内のすべてのファイルが変更されているように見え、各ファイルのファイル拡張子が look になっているという電話を受けました。技術者が最初に実行する必要がある次のアクションはどれですか?
A. Runa ライブ ディスク クローン。
B. 完全なウイルス対策スキャンを実行します。
C. バッチ ファイルを使用してファイルの名前を変更します。
D. 本機をネットワークから切断します
Answer: D (メーッセージを残す**)**
The CompTIA A+ Core 2 220-1002 exam covers this topic in the following domains: 1.2 Given a scenario, use appropriate resources to support users and 1.3 Explain the importance of security awareness.

最新問題**: 215**
スマートフォン用に設計されたオペレーティング 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. 無料

B. CentOS
C. macOS
D. Chrome OS
E. iOS
F. アンドロイド
Answer: E,F (メーッセージを残す)
The operating systems designed for smartphones include iOS and Android. iOS is developed by Apple Inc.
for its iPhone range, while Android, developed by Google, is used across a variety of devices from different manufacturers. Both operating systems are specifically tailored to provide a mobile computing experience, with interfaces, applications, and functionalities designed for touchscreen input and mobile hardware.

最新問題**: 216**
ワークステーションがプリンタを認識しません。ただし、前日、プリンタはワークステーションからジョブを正常に受信しました。技術者は、障害が発生する前に何が起こったかを確認するために、次のどのツールを使用する必要がありますか?
A. パフォーマンスモニター
B. デバイスとプリンター
C. タスク スケジューラ
D. イベント ビューアー
Answer: D (メーッセージを残す)
When troubleshooting a printer that was previously working but is no longer recognized by a workstation, Event Viewer is the most appropriate tool to check for historical logs and events related to the printer and the system.
* Option A: Performance MonitorPerformance Monitor is used for monitoring system performance and resources in real-time and does not provide specific historical event logs related to device failures.
* Option B: Devices and PrintersDevices and Printers show the status and properties of connected devices but do not provide a historical log of events or errors.
* Option C: Task SchedulerTask Scheduler manages and monitors scheduled tasks but does not log hardware events or errors.
* Option D: Event ViewerEvent Viewer logs system events, including errors, warnings, and information related to hardware and software. It is ideal for checking what happened prior to the printer failure.
References:
CompTIA A+ 220-1102 Objective 3.1 (Troubleshoot common Windows OS problems), particularly using Event Viewer for diagnosing issues.

最新問題**: 217**

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**: 218**
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: D (メーッセージを残す**)**
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**: 219**
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: (解答を表示する**)**

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**: 220**
ある企業が学校用に新しいコンピューターを購入しました。コンピュータはメーカーもモデルも同じなので、標準イメージをロードする必要があります。デスクトップ管理者が大規模な展開に使用する必要があるオーケストレーション ツールは次のうちどれですか?
A. USB ドライブ
B. DVDインストールメディア
C. PXEブート
D. 回復パーティション
Answer: (解答を表示する**)**
PXE (Preboot eXecution Environment) boot is an orchestration tool that allows a desktop administrator to deploy a standard image to multiple computers over a network. It requires a PXE server that hosts the image and a PXE client that boots from the network interface card (NIC). USB drive and DVD installation media are not orchestration tools, but manual methods of installing an image on each computer individually. Recovery partition is not an orchestration tool, but a hidden partition on the hard drive that contains an image of the factory settings. Verified References: https://www.comptia.org/blog/what-is-pxe-boot https://www.comptia.org/certifications/a

最新問題**: 221**
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: (解答を表示する**)**
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: **222**
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: **223**
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**: 224**
ユーザーは、会社のラップトップのウイルス対策保護が期限切れであることを示す通知を受け取ります。技術者はユーザーのラップトップに ping を送信できます。技術者はウイルス対策の親サーバーをチェックし、最新の署名がインストールされていることを確認します。次に、技術者はユーザーのラップトップをチェックし、ウイルス対策エンジンと定義が最新であることを確認します。次のうち、最も発生する可能性が高いのはどれですか?
A. ランサムウェア
B. OS アップデートの失敗
C. アドウェア
D. システム ファイルがありません
Answer: D (メーッセージを残す**)**
If the antivirus protection notification incorrectly indicates that the antivirus is out of date, despite the technician verifying that the engine and definitions are current, it is likely caused by corrupt or missing system files. These files may be necessary for the operating system to recognize the antivirus status correctly.
Possible causes of missing system files:
* Corrupted Windows Management Instrumentation (WMI), which is responsible for reporting system statuses.
* Issues with Windows Security Center, which tracks antivirus and firewall status.
* Corrupt system files due to improper shutdowns, malware, or disk errors.
Why Not the Other Options?
* A. Ransomware - Ransomware encrypts user files and usually presents a ransom demand. It would not cause a false antivirus update notification.
* B. Failed OS updates - While failed updates can cause issues, they typically do not interfere with antivirus update notifications unless they specifically affect system files.
* C. Adware - Adware generally displays unwanted ads but does not impact antivirus notifications.
Solution:
To resolve the issue, the technician can:
* Run System File Checker (SFC) using sfc /scannow in Command Prompt (Admin).
* Restart Windows Security Center and ensure its services are running.
* Check for WMI corruption using winmgmt /verifyrepository and repair if needed.

* Reinstall the antivirus software to refresh its registration with the OS.
Thus, the most likely cause is missing system files (D).

最新問題: **225**
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: **226**
次の一般的なセキュリティ脆弱性のうち、入力検証を使用することで軽減できるものはどれですか?
A. ブルートフォース攻撃
B. クロスサイトスクリプティング
C. SQL インジェクション
D. クロスサイトリクエストフォージェリ
Answer: B,C (メーッセージを残す**)**
Cross-site scripting (XSS) and SQL injection are common security vulnerabilities that can be mitigated by using input validation. Input validation is a technique that checks the user input for any malicious or unexpected characters or commands before processing it. XSS is an attack that injects malicious scripts into web pages to steal cookies, session tokens or other sensitive information from users or web servers. SQL injection is an attack that injects malicious SQL statements into web applications to manipulate databases, execute commands or access unauthorized data. Verified References: https://www.comptia.org/blog/what-is- input-validation https://www.comptia.org/certifications/a

最新問題: **227**
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: **228**
技術者がワークステーションに Windows 10 をインストールしました。技術者が 8GB をインストールしたにもかかわらず、ワークステーションには 3.5GB の使用可能な RAM しかありません。このシステムが使用可能な RAM をすべて使用してい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. システムにアップデートがありません。
B. 32 ビット OS を使用するシステム。
C. システムのメモリが故障しています。
D. システムには BIOS の更新が必要です。
Answer: B (メーッセージを残す**)**
The most likely reason that the system is not utilizing all the available RAM is that it is running a 32-bit OS. A 32-bit OS can only address up to 4GB of RAM, and some of that is reserved for hardware and system use1. Therefore, even if the technician installed 8GB of RAM, the system can only use around 3.5GB of usable RAM. To use the full 8GB of RAM, the technician would need to install a 64-bit OS, which can address much more memory2. The system missing updates, the system's memory failing, or the system requiring BIOS updates are not likely to cause this issue.

References: 2: https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715 1: https://www.makeuseof.com/tag/unlock-64gb-ram-32-bit-windows-pae- patch/

最新問題**: 229**
最近、クライアントが Windows 10 マシンを Windows 11 にアップグレードしました。クライアントは、コンピューターの電源を入れると 「オペレーティング システムの読み込みエラー」というメッセージが表示されると報告しました。この問題のトラブルシューティングを行うために、技術者が最初に行うべきことは何ですか?
A. セキュア ブート機能を無効にします。
B. 自動起動回復を使用します。
C. ドライブをフォーマットします。
D. ブート パーティションのサイズを変更します。
Answer: (解答を表示する**)**
The "Error loading operating system" message in Windows typically indicates a problem with the boot process. This could be due to corrupted system files, boot configuration data (BCD) errors, or issues with the hard drive.
Windows has a built-in automated startup recovery tool designed to diagnose and fix these types of problems.
It attempts to automatically find and repair issues that are preventing Windows from starting correctly.
Here's why the other options are not the best first step:
* A. Disable the Secure Boot feature: Secure Boot is a security feature that helps prevent malware from loading during startup. While it can sometimes cause issues with incompatible hardware or software, it's unlikely to be the primary cause of this error after a Windows upgrade.
* C. Format the drive: Formatting the drive should be a last resort as it will erase all data on the hard drive.
* D. Resize the boot partition: Resizing the boot partition is a complex task and not usually necessary to fix a boot error.
Troubleshooting Steps:
* Use the automated startup recovery:
* This is usually attempted automatically when Windows fails to boot.
* If it doesn't start automatically, you might need to access the Advanced Startup Options menu (usually by repeatedly pressing F8 or Shift+F8 during startup).
* If automated repair fails, try other options from the Advanced Startup Options menu:
* System Restore: Restore the system to a point before the upgrade.
* Startup Repair: This tool can fix more complex boot errors.
* Command Prompt: Use the command prompt to run commands like bootrec /fixmbr, bootrec /fixboot, and bootrec /rebuildbcd to repair the boot configuration.

最新問題: **230**
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: B (メーッセージを残す**)**
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: **231**
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: **232**
災害後、企業はすべてのデータと機器を失いました。災害のため、企業はシステムのバックアップを維持できなくなりました。将来の損失を防ぐために、企業は次のどれを実施する必要がありますか?
A. テスト環境
B. ローカルバックアップ
C. コールドサイト
D. クラウドストレージ
Answer: D (メーッセージを残す)
Comprehensive and Detailed In-Depth Explanation:
Cloud storage ensures that data is backed up off-site, protecting against physical disasters like fires or floods.
* A. Test environment - Incorrect. This is for software testing, not data recovery.
* B. Local backups - Incorrect. These could also be destroyed in a disaster.
* C. Cold site - Useful for disaster recovery but does not automatically back up data.
Reference:
CompTIA A+ 220-1102, Objective 4.1 - Backup and Recovery Best Practices

最新問題: **233**
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: (解答を表示する)
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: **234**
技術者がインターネットまたは名前付きネットワーク リソースにアクセスできません。技術者は DHCP サーバーから有効な IP アドレスを受信し、デフォルト ゲートウェイに ping を実行できます。問題を解決するために技術者が次に確認する必要があるのは次のうちどれですか。
A. DNS サーバーの設定を確認します。
B. Windows ファイアウォールをオフにします。
C. サブネットマスクが正しいことを確認します。

D. 静的 IP アドレスを設定します。
Answer: A (メーッセージを残す**)**
The correct answer is A. Verify the DNS server settings. This is because the DNS server is responsible for resolving domain names to IP addresses, which is necessary for accessing the internet or named network resources. If the DNS server settings are incorrect or the DNS server is down, the technician will not be able to access these resources even if they have a valid IP address and can ping the default gateway1.
1: CompTIA A+ Certification Exam: Core 2 Objectives, page 16, section 1.10.

最新問題**: 235**
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**: 236**
ある会社では、従業員のコラボレーション プロセスの一環として共有ドライブを使用しています。適切な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が各部門に割り当てられています。マネージャーのチームは機密資料を扱っており、特定のフォルダーとそれに続くファイルおよびサブフォルダーを直属のチームだけが閲覧できるようにしたいと考えています。技術者が取るべきアクションは次のうちどれですか。
A. 要求されたフォルダーのみの継承をオフにし、各ファイルに要求されたアクセス許可を手動で設定します。
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の継承をオフにし、要求されたアクセス許可を設定してから、子フォルダーの下の継承をオンにします。
Answer: D (メーッセージを残す**)**
For managing permissions where a specific folder needs to have different access controls than its parent, turning off inheritance for that specific folder is the correct approach.
* Option A: Turn off inheritance on the requested folder only and set the requested permissions to each file manuallyThis is partially correct, but setting permissions manually for each file is inefficient and error-prone.
* Option B: Turn off inheritance at the top-level folder and remove all inherited permissionsThis action would disrupt permissions for all other folders and files, not just the confidential folder.
* Option C: Turn off inheritance at the top-level folder and set permissions to each file and subfolder manuallyThis approach is overly broad and inefficient, impacting more than just the specific folder that needs restricted access.
* Option D: Turn off inheritance on the requested folder only, set the requested permissions, and then turn on inheritance under the child foldersThis ensures the specific folder has unique permissions while allowing those permissions to propagate to its children, maintaining security and ease of management.
References:
CompTIA A+ 220-1102 Objective 2.5 (Manage and configure basic security settings in the Windows OS), particularly file and folder permissions and inheritance settings.

最新問題**: 237**
技術者はファイルをユーザーのワークステーションに転送する必要があります。ワークステーションの組み込みプロトコルを利用してこのタスクを実行するのに最も適しているのは次のうちどれですか?
A. VPN
B. SMB
C. RMM
D. MSRA
Answer: (解答を表示する**)**
SMB stands for Server Message Block, which is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. SMB is a built-in protocol in Windows operating systems and can be used to transfer files between computers over a network. The technician can use SMB to access a file share on the user's workstation and copy the file to or from it. VPN stands for virtual private network, which is a technology that creates a secure and encrypted connection over a public network. VPN is not a built-in protocol in Windows operating systems and does not directly transfer files between computers. RMM stands for remote monitoring and management, which is a type of software solution that allows remote management and monitoring of devices and networks. RMM is not a built-in protocol in Windows operating systems and does not directly transfer files between computers.

MSRA stands for Microsoft Remote Assistance, which is a feature that allows a user to invite another user to view or control their computer remotely. MSRA is not a protocol, but an application that uses Remote Desktop Protocol (RDP) to establish a connection. MSRA does not directly transfer files between computers.
https://www.pcmag.com/picks/the-best-desktop-workstations

最新問題**: 238**
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**: 239**
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: C (メーッセージを残す**)**
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**: 240**
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: (解答を表示する**)**
When a new SOHO (Small Office/Home Office) router is installed, it often comes with a default firewall setting that blocks unsolicited inbound traffic. If customers are unable to access the company-hosted public website, it is likely because the router is not correctly forwarding incoming requests to the web server inside the network.
Port Forwarding allows external requests on a specific port (such as port 80 for HTTP or port 443 for HTTPS) to be redirected to the internal web server that is hosting the website. Without this configuration, the router will drop incoming traffic by default, making the website inaccessible to external users.
Why Not the Other Options?
* B. Firmware updates - While keeping the router's firmware updated is good practice, it is not directly related to resolving this issue unless there was a known bug preventing port forwarding.
* C. IP filtering - IP filtering is used to allow or block traffic from specific IP addresses. Unless the router is incorrectly blocking all external traffic, this would not be the best solution.
* D. Content filtering - Content filtering is used to restrict access to certain websites or categories of content, typically for internal users. It does not impact inbound traffic to a company-hosted website.
Solution:
The technician should configure port forwarding on the SOHO router, directing HTTP (port 80) and HTTPS (port 443) traffic to the internal web server's private IP address.

最新問題**: 241**
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: (解答を表示する**)**
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: **242**
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: **243**
対象企業のユーザー用に Microsoft Windows PC をセットアップする必要があります。ユーザーが電子メールや共有ドライブにアクセスするには、企業ドメインにアクセスする必要があります。技術者がユーザーに展開する可能性が最も高い Windows のバージョンは次のうちどれですか?
A. Windows Enterprise Edition
B. Windows Professional Edition
C. Windows Server Standard Edition
D. Windows Home Edition
Answer: B (メーッセージを残す)
The Windows Professional Edition is the most likely version that a technician would deploy for a user at a target corporation. This version of Windows is designed for business use and provides the necessary features and capabilities that a user would need to access the corporate domain, such as email and shared drives.

最新問題: **244**
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**: 245**
技術者は、ユーザーのトラブルシューティングを支援するために Linux デスクトップにリモート接続する必要があります。技術者は、Linux 用にネイティブに設計されたツールを使用する必要があります。次のツールのうち、技術者が最も使用する可能性が高いのはどれですか?
A. VNC
B. MFA
C. MSRA
D. RDP
Answer: (解答を表示する**)**
The tool that the technician will most likely use to remotely connect to a Linux desktop is VNC. VNC stands for Virtual Network Computing and is a protocol that allows remote access and control of a graphical desktop environment over a network. VNC is natively designed for Linux and can also support other operating systems, such as Windows and Mac OS. VNC can be used to assist users with troubleshooting by viewing and interacting with their desktops remotely. MFA stands for Multi-Factor Authentication and is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. MFA is not a tool that can be used to remotely connect to a Linux desktop but a technique that can be used to enhance security for systems or services. MSRA stands for Microsoft Remote Assistance and is a feature that allows remote access and control of a Windows desktop environment over a network. MSRA is not natively designed for Linux and may not be compatible or supported by Linux systems. RDP stands for Remote Desktop Protocol and is a protocol that allows remote access and control of a Windows desktop environment over a network. RDP is not natively designed for Linux and may not be compatible or supported by Linux systems. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

最新問題**: 246**
ユーザーが不審なメール内のリンクをクリックすると、デバイスにマルウェアがインストールされます。マルウェアを削除する最善の方法は次のうちどれですか?
A. システムの復元を実行します。
B. リカバリーモードにします。
C. スキャンをスケジュールします。
D. PCを再起動します。
Answer: B (メーッセージを残す**)**

Recovery mode is a special boot option that allows the user to access advanced tools and features to troubleshoot and remove malware from the device. Recovery mode can also restore the system to a previous state or reset the device to factory settings. Running System Restore, scheduling a scan, or restarting the PC may not be effective in removing the malware, as it may still be active or hidden in the system files.

最新問題**: 247**
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: D (メーッセージを残す**)**
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**: 248**
ホテルに滞在中、ユーザーはホテルの Wi-Fi に接続しようとしましたが、複数の SSID が非常によく似た名前であることに気付きました。次のソーシャル エンジニアリング攻撃のうち、試みられているのはどれですか?
A. 悪の双子
B. なりすまし
C. 内部脅威
D. 捕鯨
Answer: A (メーッセージを残す**)**

An evil twin is a type of social-engineering attack that involves setting up a rogue wireless access point that mimics a legitimate one. The attacker can then intercept or modify the traffic of the users who connect to the fake SSID. The attacker may also use phishing or malware to steal credentials or personal information from the users

最新問題: **249**
技術者は、ユーザーのために新しいワークステーションを完成させています。ユーザーの PC はインターネットに接続されますが、毎回同じプライベート アドレスは必要ありません。次のプロトコルのうち、技術者が使用する可能性が最も高いのはどれですか?
A. DHCP
B. SMTP
C. DNS
D. RDP
Answer: A (メーッセージを残す**)**
DHCP stands for Dynamic Host Configuration Protocol and it is used to assign IP addresses and other network configuration parameters to devices on a network automatically. This is useful for devices that do not require the same private address each time they connect to the internet.

最新問題: **250**
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: (解答を表示する**)**
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: **251**
技術者が、DNS ルックアップを実行できない PC のトラブルシューティングを行っています。次のファイアウォール出力を利用します。
プロトコル/ポートアクション方向
1許可アウト
445ブロックアウト
53ブロックアウト

123ブロックアウト
80ブロックアウト
DNS 再帰を可能にするには、次のポートのうちどれを開く必要がありますか?
A. 1
B. 53
C. 80
D. 123
E. 445
Answer: B (メーッセージを残す)
DNS (Domain Name System) lookups are essential for translating human-friendly domain names into IP addresses that computers use to communicate. DNS typically uses port 53 for its communication.
In the provided firewall output, various ports are either allowed or blocked for outgoing traffic. For DNS recursion, which is the process of resolving domain names to IP addresses, port 53 must be open.
* Port 53: This is the standard port used by DNS for queries and responses. The fact that it is currently blocked (as per the firewall output) is the reason why DNS lookups are failing. Opening port 53 will allow the DNS requests to pass through the firewall, enabling the resolution of domain names to IP addresses.
Other ports mentioned in the output are used for different services and protocols:
* Port 1 is generally not used for standard services.
* Port 445 is associated with SMB (Server Message Block) for file sharing in Windows environments.
* Port 123 is used by NTP (Network Time Protocol) for time synchronization.
* Port 80 is used for HTTP traffic, which is web traffic but not related to DNS lookups.

最新問題**: 252**
コール センターは、複数の医療施設の請求に関する問い合わせを処理します。セキュリティ アナリストは、コール センターのエージェントが自分のワークステーションから離れて、患者のデータを誰でも見られるようにしたままにしておくことが多いことに気付きました。コールセンター内でのデータの盗難を最大限に防止するために、ネットワーク管理者が行うべきことは次のうちどれですか?
A. ワークステーションのハード ドライブを暗号化します。
B. 非アクティブ状態が 5 分間続くと、ワークステーションをロックします。
C. プライバシー スクリーンをインストールします。
D. ワークステーションが使用されていないときにユーザーをログオフします。
Answer: (解答を表示する)
The BEST solution for preventing data theft within the call center in this scenario would be to lock the workstations after a period of inactivity. This would prevent unauthorized individuals from

accessing patient data if call center agents were to step away from their workstations without logging out.

最新問題: **253**
ある企業は、最新のテクノロジーを活用して、対面での会議から移行したいと考えています。次の種類のソフトウェアのうち、会社に最も利益をもたらすものはどれですか? (2 つ選択してください)。
A. ビデオ会議
B. ファイル転送
C. 画面共有
D. 財務
E. リモート アクセス
F. 記録保持
Answer: A,C (メーッセージを残す)
For a company looking to transition away from face-to-face meetings, videoconferencing and screen-sharing software would be most beneficial.
* Videoconferencing software allows participants to conduct virtual meetings with audio and video capabilities, effectively simulating a face-to-face interaction without the need for physical presence.
This can greatly reduce travel costs and time while maintaining the personal touch of meetings.
* Screen-sharing enables participants in a virtual meeting to view one another's computer screens in real time. This is particularly useful for presentations, collaborative work, and troubleshooting, as it allows for a more interactive and engaging meeting experience.
Both technologies support the company's goal of leveraging modern technology to enhance communication and collaboration while reducing reliance on physical meetings.

最新問題: **254**
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: **255**
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: B (メーッセージを残す**)**
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: **256**
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: **257**
ユーザーは PC で Web サイトを閲覧できません。技術者が Web サイトの PC の DNS 解決を確認するには、次のコマンドのどれを使用する必要がありますか?
A. nslookup
B. hostname
C. tracert
D. netstat
Answer: A (メーッセージを残す)
The nslookup command is a network administration tool used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record. It's the most direct way to verify if a PC can resolve a website's domain name to its IP address.
Here's why the other options are not the primary tools for this task:
* B. hostname: This command displays the hostname of the computer.
* C. tracert: This command traces the route packets take to reach a specific destination. It can help identify network connectivity issues but doesn't directly test DNS resolution.
* D. netstat: This command displays active network connections and listening ports. It's not used for DNS troubleshooting.
How to use nslookup:
* Open a command prompt.
* Type nslookup <website address> (e.g., nslookup google.com) and press Enter.
* The output will show the DNS server used and the IP address(es) associated with the website.
* If the command returns an error or doesn't show an IP address, it indicates a problem with DNS resolution.

最新問題: **258**
ユーザーから、個人所有の新しいタブレットが会社の Wi-Fi ネットワークに接続できないという報告がありました。ユーザーは他のデバイスで Wi-Fi ネットワークに接続でき、タブレットは最新

のソフトウェアを実行しています。この問題の原因として最も可能性が高いのは次のどれですか。
A. 暗号化設定が正しくありません
B. ブロックされたMACアドレス
C. 古いドライバー
D. 位置情報サービスが無効になっています
Answer: B (メーッセージを残す**)**
When a user reports that a new, personally owned tablet will not connect to the corporate Wi-Fi network, but other devices can connect, and the tablet is running the latest software, the most likely cause of the issue is a blocked MAC address. Here's why:
* MAC Filtering: Many corporate networks implement MAC address filtering as a security measure. This involves only allowing devices with specific MAC addresses to connect to the network. If the MAC address of the new tablet is not on the allowed list, it will be blocked from connecting.
* Check Network Settings: To troubleshoot this, the network administrator can check the network's MAC filtering settings to see if the tablet's MAC address is blocked.
* Add MAC Address: If the MAC address is blocked, adding the tablet's MAC address to the allowed list will resolve the issue.
Other options like incorrect encryption settings or outdated drivers are less likely because the user can connect with other devices and the tablet is running the latest software. Disabled location services do not affect Wi-Fi connectivity.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.6: Given a scenario configure basic mobile device network connectivity and application support.
Corporate network security practices documentation.

最新問題**: 259**
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**: 260**
技術者が検証済みのセキュリティ ツールをダウンロードし、a58e87a2 のベンダー ハッシュを記録します。ダウンロードが完了すると、技術者は再びハッシュを検証しますが、値は 2a876a7d3 として返されます。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. プライベート ブラウジング モード
B. 無効な証明書
C. 変更されたファイル
D. ブラウザのキャッシュ
Answer: C (メーッセージを残す**)**
The most likely cause of the issue of having different hash values for a downloaded security tool is a modified file. A hash value is a unique and fixed-length string that is generated from an algorithm that processes data or files. A hash value can be used to verify the integrity and authenticity of data or files by comparing it with a known or expected value. If the hash values do not match, it means that the data or file has been altered or corrupted in some way. A modified file may result from intentional or unintentional changes, such as editing, encryption, compression or malware infection. Private-browsing mode is a feature that allows users to browse the web without storing any browsing history, cookies or cache on their browser. Private-browsing mode does not affect the hash value of a downloaded file but only how the browser handles user data. Invalid certificate is an error that occurs when a website or a server does not have a valid or trusted digital certificate that proves its identity and secures its communication. Invalid certificate does not affect the hash value of a downloaded file but only how the browser verifies the website or server's credibility. Browser cache is a temporary storage that stores copies of web pages, images and other content that users have visited on their browser.

最新問題**: 261**
海外旅行者は、スマートフォンを紛失したり盗まれたりした場合に、他人がそのスマートフォンの内容にアクセスすることを心配しています。旅行者は生体認証を有効にしています。次のどの追加セキュリティ対策により、不正なデータアクセスのリスクをさらに軽減できますか。
A. リモートバックアップ

B. 位置追跡
C. PINコード画面ロック
D. デバイスの暗号化
Answer: D (メーッセージを残す)
Comprehensive and Detailed In-Depth Explanation:
Device encryption ensures that even if someone gains physical access to the smartphone, they cannot access its contents without the encryption key.
* A. Remote backups - Useful for data recovery but does not prevent unauthorized access.
* B. Location tracking - Helps locate the device but does not protect its data.
* C. PIN code screen lock - Adds security but is less effective than full encryption.
Reference:
CompTIA A+ 220-1102, Objective 2.3 - Security Features of Mobile Devices

最新問題**: 262**
予期しない変更が発生しないようにするために、プロジェクトで行われるすべての変更をリストする変更管理プラクティスは次のどれですか。
A. リスク分析
B. スコープ
C. ロールバックプラン
D. レビュー
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**: 263**
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**: 264**
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: **265**
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: B (メーッセージを残す**)**
In a professional work environment, distractions should be minimized, especially when working onsite for a client. The best approach is to put the phone on silent (Option B) to avoid interruptions while remaining professional.
Step aside and answer (Option A): Not recommended as it disrupts work and appears unprofessional.
Text a reply (Option C): While this may seem reasonable, it still causes a distraction.
Ignore the phone and continue working (Option D): While focusing on work is important, completely ignoring calls may not be the best approach. Silent mode ensures work continuity while allowing the technician to check messages later.
Reference: CompTIA A+ Core 2 (220-1102) Exam Objectives - 4.6: Given a scenario, apply best practices associated with documentation and professionalism.

最新問題: **266**
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: **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**
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: A (メーッセージを残す**)**
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: **269**
SOHO のユーザーが、オフサイトのリモート技術者にユーザーのラップトップに安全に接続するように依頼します。技術者は VPN に接続できますが、ユーザーのラップトップに接続できません。技術者は次のどの設定を確認する必要がありますか?
A. 無線プロトコル
B. DHCPプール
C. コンテンツフィルタリング
D. ファイアウォール
Answer: (解答を表示する**)**
When a technician is unable to connect to a laptop over a VPN, one of the most common reasons is that the firewall settings on either the laptop or the network are blocking the connection.
* Wireless protocol: Unrelated, as the technician is already connected to the VPN.
* DHCP pool: Unlikely to be the issue, as it deals with IP address assignment.
* Content filtering: Typically involves filtering web content, not affecting direct connections.
* Firewall: The correct setting to review, as it may block the necessary ports or services required for remote access.
Reference: CompTIA A+ Exam Objectives [220-1102] - 2.3: Given a scenario, troubleshoot common wired and wireless network problems.

最新問題: **270**
ユーザーが会社のネットワークにアクセスできません。技術者は、ログイン試行が複数回失敗したため、ユーザーのアカウントにアクセスできなくなったことを知りました。また、問題が発生する前にユーザーはパスワードを変更していました。
問題を解決するために技術者が実行する必要がある手順はどれですか?
A. ユーザーの問題をネットワーク チームにエスカレーションします。
B. ユーザーのパスワードをリセットします。
C. ユーザーのアカウントのロックを解除します。
D. ユーザーのログインとパスワードを確認します。
Answer: C (メーッセージを残す**)**
Detailed Explanation with Core 2 References:If multiple unsuccessful attempts led to the account being locked, the technician should unlock the account. Core 2 covers user account management practices, including unlocking accounts and managing failed login attempts (Core 2 Objective 2.5).

最新問題: **271**
技術者は、電話機を更新できないユーザーからヘルプ デスク チケットを受け取ります。技術者が問題を調査すると、次のエラー メッセージが表示されることに気付きます。ストレージ容量が不足しています 電話機の分析中に、技術者はサードパーティのアプリケーションや写真を検出できませんでした。問題を解決する最善の方法は次のうちどれですか?

A. デバイスを新しいものに交換します。
B. オンボードストレージをアップグレードします。
C. 工場出荷時のアプリケーションを削除して、より多くのスペースを割り当てます。
D. ファクトリーアプリケーションを外部メモリに移動します。
Answer: D (メーッセージを残す)
The best way to resolve the issue is to move factory applications to external memory. This will free up some space on the phone's internal storage, which is required for updating the phone. To do this, you can follow these steps1:
Insert a microSD card into your phone if you don't have one already.
Go to Settings > Apps and tap on the app you want to move.
Tap on Storage and then on Change.
Select the SD card option and tap on Move.
You may need to repeat this process for multiple apps until you have enough space to update your phone.
Alternatively, you can also clear the cache and data of some apps, or uninstall the apps that you don't use frequently. You can find more information on how to fix insufficient storage error on your phone in these articles234. I hope this helps.

最新問題: **272**
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**: 273**
次のデバイス タイプのうち、技術者がセキュリティ上の懸念と見なすのはどれですか?
A. NIC
B. IoT
C. PoE
D. LC
Answer: B (メーッセージを残す**)**
IoT (Internet of Things) devices are often considered a security concern due to their typically weak security protocols and the fact that many IoT manufacturers do not prioritize security when designing these devices.
These devices often lack the capability to be regularly patched or updated, which leaves them vulnerable to exploitation by attackers. The multitude of IoT devices, such as smart thermostats, cameras, and even light bulbs, when connected to a network, can serve as entry points for cyberattacks if not secured properly. In contrast, NICs (Network Interface Cards), PoE (Power over Ethernet), and LC (a type of fiber optic connector) do not inherently pose the same level of security risk as IoT devices because they are more established technologies and typically have better security practices in place.
References:
CompTIA A+ Exam Objectives - 220-1102, Domain 2.7: Security (CompTIA) (ProfMesser)

最新問題**: 274**
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: (解答を表示する**)**
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**: 275**
ある会社の幹部が、多数の参加者が集まる大規模な音楽フェスティバルに参加しているのですが、仕事用のメール アカウントにアクセスできないという問題が発生しています。メール アプリケーションがメールをダウンロードできず、接続試行中に停止しているようです。この障害の原因として最も可能性が高いのは次のどれですか。
A. 携帯電話に使用可能なストレージ容量がありません。
B. 会社のファイアウォールは、電子メール リソースへのリモート アクセスをブロックするように構成されています。
C. 同じエリア内でモバイル ネットワークに接続しようとしているデバイスが多すぎます。
D. フェスティバル主催者はイベント中のインターネットの使用を禁止し、インターネット信号をブロックしました。
Answer: C (メーッセージを残す**)**
Reference: CompTIA A+ Certification Core 2 220-1102, Objective 2.2 (Networking Concepts).

最新問題**: 276**
ユーザーが在宅勤務中に、会社支給のラップトップから共有ドライブにアクセスしようとしています。ユーザーはファイルにアクセスできず、各共有ドライブの横に赤い X が表示されています。共有ドライブへのユーザーのアクセスを復元するには、次のどれを設定する必要がありますか?
A. IPv6
B. VPN
C. IPS
D. DNS
Answer: B (メーッセージを残す**)**
When a user is unable to access shared drives from a company-issued laptop while working from home, the likely requirement is:
* VPN (Virtual Private Network): A VPN allows secure access to the company's network from a remote location. Without a VPN connection, the user cannot access network resources such as shared drives.

* IPv6: Involves IP addressing and is not directly related to accessing shared drives.
* IPS (Intrusion Prevention System): Provides network security but does not facilitate access to shared drives.
* DNS: Manages domain name resolution and is not typically the issue when specific shared drives are inaccessible.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.7: Explain common methods for securing mobile and embedded devices.
VPN configuration and remote access documentation.

最新問題**: 277**
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**: 278**
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: (解答を表示する**)**
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**: 279**
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**: 280**
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**: 281**

技術者は、小規模オフィスのワイヤレス ネットワークを保護するためのオプションを調査しています。要件の 1 つは、パスワードの代わりに証明書を使用してネットワークへの自動ログインを許可することです。この機能をサポートするには、ワイヤレス ソリューションに次のどれが必要ですか?

A. 半径

B. AES

C. EAP-EKE

D. MFA

Answer: A (メーッセージを残す**)**

RADIUS is the correct answer for this question. RADIUS stands for Remote Authentication Dial-In User Service, and it is a protocol that provides centralized authentication, authorization, and accounting for wireless networks. RADIUS can support certificate-based authentication, which allows users to log in to the network automatically without entering passwords. RADIUS also provides other benefits, such as enforcing security policies, logging user activities, and managing network access. AES, EAP-EKE, and MFA are not wireless solutions, but rather encryption algorithms, authentication methods, and security factors, respectively. References:

* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 23
* CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 459

最新問題**: 282**

アプリケーション ユーザーは、現在使用しているアプリケーションのバージョンが販売されなくなることを示す電子メールを受け取りました。このバージョンのアプリケーションを使用しているユーザーは、パッチやアップデートも受け取れなくなります。ベンダーが製品をサポートしなくなったことを示しているのは次のうちどれですか?

A. AUP

B. EULA

C. EOL

D. UAC

Answer: C (メーッセージを残す**)**

EOL (end-of-life) is a term that indicates a vendor no longer supports a product. It means that the product will no longer be sold, updated or patched by the vendor, and that the users should migrate to a newer version or alternative product. AUP (acceptable use policy), EULA (end-user license agreement) and UAC (user account control) are not terms that indicate a vendor no longer supports a product. Verified References: https://www.
comptia.org/blog/what-is-end-of-life https://www.comptia.org/certifications/a

最新問題**: 283**

技術者は、企業ネットワーク上のエンドポイントに最新のアプリケーション セキュリティ更新プログラムを実装しています。

業界のベスト プラクティスに準拠しながらネットワーク上のデバイスのセキュリティを確保するために、技術者は次のどのソリューションを使用する必要がありますか。
A. パッチ適用プロセスを自動化します。
B. ファイアウォールの構成を監視します。
C. アクセス制御リストを実装します。
D. すべての変更を文書化します。
Answer: (解答を表示する**)**
To ensure device security on the network while adhering to industry best practices, the technician should:
* Automate the patching process: This ensures that all devices receive the latest security updates in a timely manner without manual intervention, reducing the risk of vulnerabilities.
* Monitor the firewall configuration: Important for network security but does not directly ensure all devices are patched.
* Implement access control lists: Controls access to resources but does not ensure devices are patched.
* Document all changes: Important for change management but does not directly impact the patching process.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.6: Given a scenario configure a workstation to meet best practices for security.
Best practices for application security updates and patch management.

最新問題**: 284**
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**: 285**
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**: 286**
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: B (メーッセージを残す**)**
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.

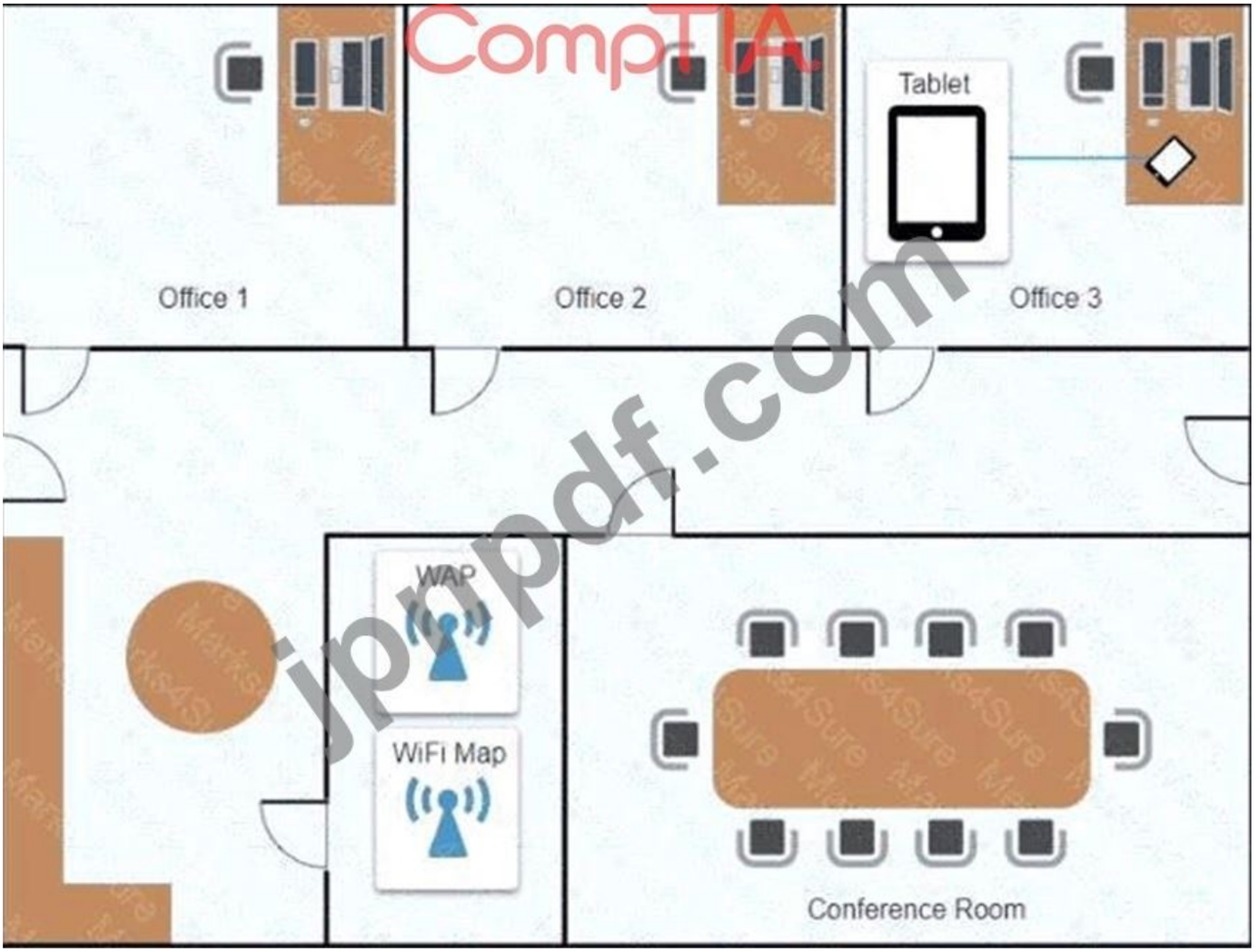
最新問題: **287**
次のうち、MFA の例はどれですか?
A. 指紋スキャンと網膜スキャン
B. パスワードと暗証番号
C. ユーザー名とパスワード
D. スマートカードとパスワード
Answer: (解答を表示する**)**
Smart card and password is an example of two-factor authentication (2FA), not multi-factor authentication (MFA). MFA requires two or more authentication factors. Smart card and password is an example of two- factor authentication (2FA)2

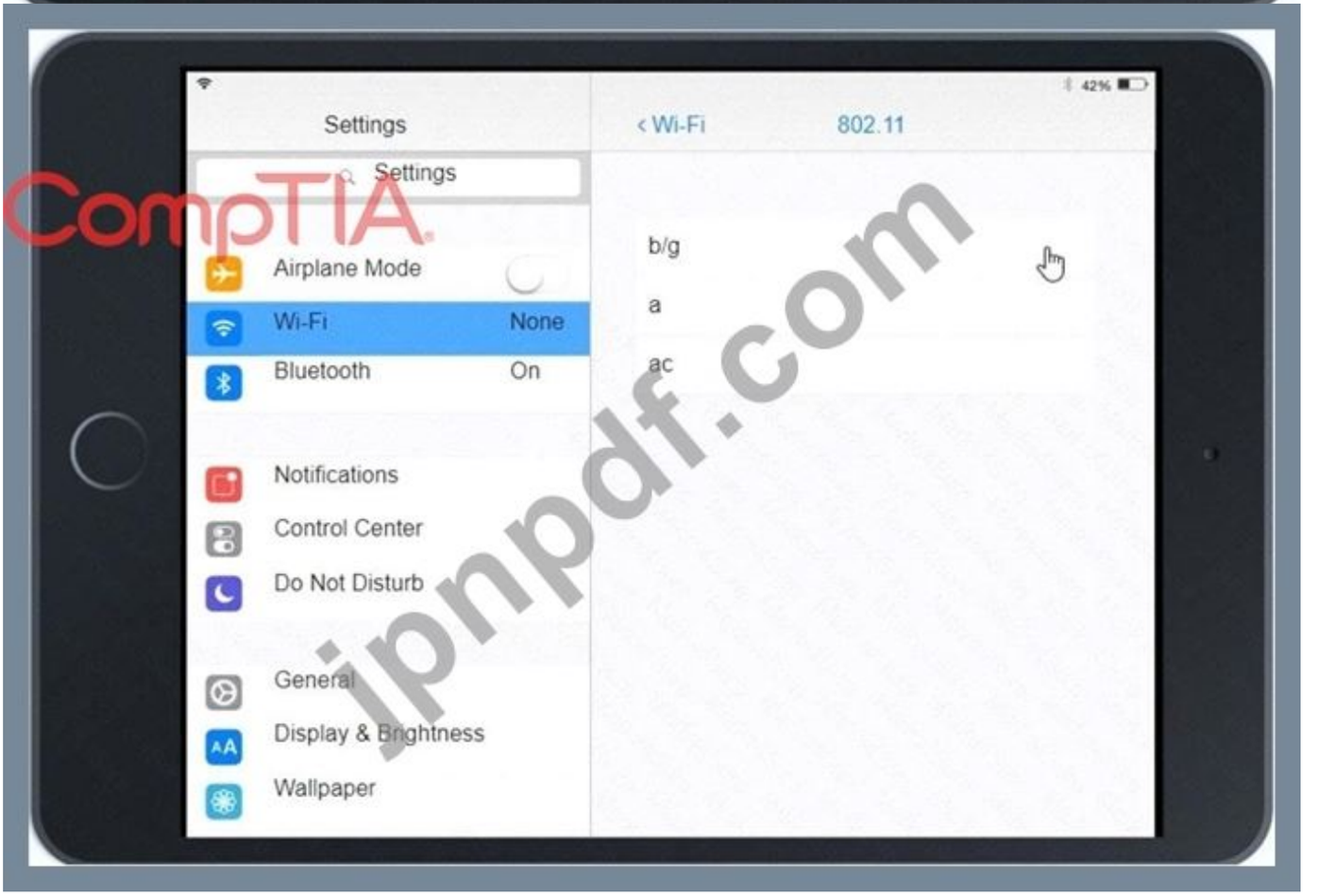
最新問題: **288**
デバイスの寿命を延ばすために最もよく使用されるのは次のどれですか?
A. バッテリーバックアップ
B. 静電気放電マット
C. 適切な換気
D. グリーン廃棄
Answer: C (メーッセージを残す**)**
Proper ventilation is a factor that can extend the life of a device by preventing overheating and thermal damage to the device's components. Proper ventilation means ensuring that there is enough airflow around and inside the device to dissipate heat and maintain a suitable temperature for optimal performance. Proper ventilation can be achieved by using fans, heat sinks, vents, or liquid cooling systems, as well as avoiding placing the device near heat sources or in enclosed spaces. Battery backup, electrostatic discharge mat, and green disposal are not factors that can extend the life of a device.

最新問題: **289**
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: A (メーッセージを残す**)**
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.

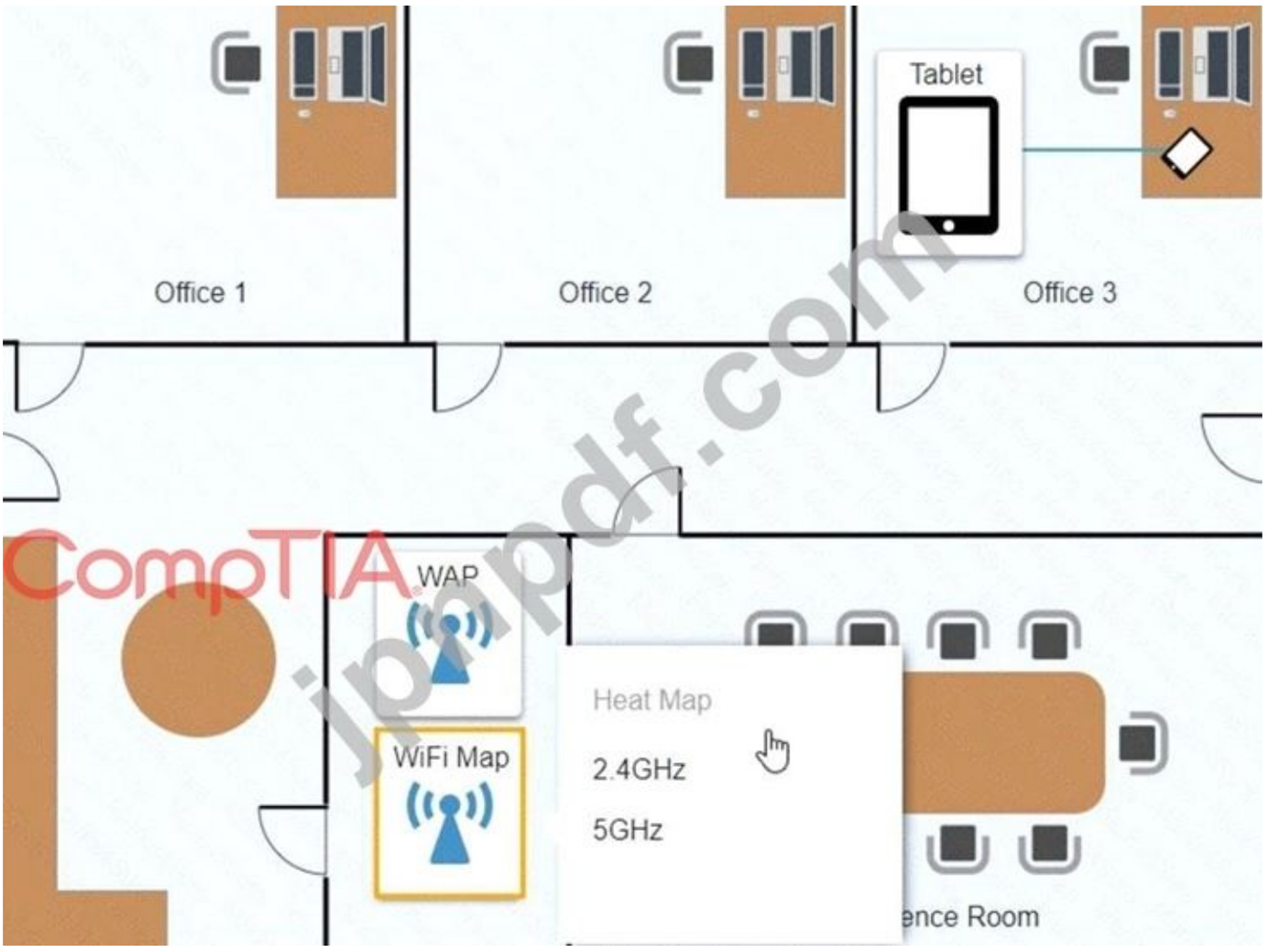
* C. The UAC level to its highest level - Incorrect. User Account Control (UAC) settings control administrative privileges, not network visibility.
* D. The file-sharing permissions - Incorrect. File-sharing permissions only affect access to shared folders, not network visibility.
Reference:
CompTIA A+ 220-1102, Objective 1.8 - Windows Networking and Configuration

最新問題**: 290**
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。






CompTIA
42%
Settings
Wi-Fi
SSID
Settings
Airplane Mode
Wi-Fi
None
Bluetooth
On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
BYOD
DEFAULT
CORP
ANNHOME



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 TotallySecret.

最新問題: **291**
ユーザーの Windows コンピューターは、一日の初めは正常に動作しているように見えます。しかし、一日を通してパフォーマンスが低下し、複数のアプリケーションを開いているとシステムがフリーズします。技術者がこの問題を解決するために行うべきことは、次のうちどれですか (2 つ選択してください)。
* 最新の GPU ドライバーをインストールします。
A. OS を再インストールします。
B. RAM を増やします。
C. ハードドライブの容量を増やします。
D. 不要なソフトウェアをアンインストールします。
E. スケジュールされたタスクを無効にします。
Answer: C,E (メーッセージを残す**)**
The most likely causes of the user's Windows computer performance degradation and freezing are insufficient RAM and excessive software running in the background. Therefore, the technician should do the following to resolve the issue:
* Increase the RAM. RAM is the memory that the computer uses to store and run applications and processes. If the RAM is not enough to handle the workload, the computer will use the hard drive as a virtual memory, which is much slower and can cause performance issues. Increasing the RAM will allow the computer to run more applications and processes smoothly and avoid freezing. The technician should check the system requirements of the applications that the user needs to run, and install additional RAM modules that are compatible with the motherboard and the existing RAM. The technician should also make sure that the system is managing the page file size automatically, or adjust it manually to optimize the virtual memory usage12.
* Uninstall unnecessary software. Software that the user does not need or use can take up valuable disk space and system resources, and can interfere with the performance of other applications. Some software may also run in the background or start automatically when the computer boots up, which can slow down the system and cause freezing. The technician should

help the user to identify and uninstall unnecessary software from the control panel or the settings app, and disable unnecessary startup programs from the task manager or the system configuration tool. The technician should also check for and remove viruses and malware that may affect the system performance134.
References:
1: Tips to improve PC performance in Windows - Microsoft Support1 2: How to Upgrade or Install RAM on Your Windows PC - Lifewire5 3: How to Uninstall Programs on Windows 10 - PCMag6 4: How to Fix a Windows Computer that Hangs or Freezes - wikiHow

最新問題**: 292**
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: B (メーッセージを残す**)**
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**: 293**
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: (解答を表示する**)**
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: **294**
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: B (メーッセージを残す**)**
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: **295**
ユーザーが仕事で支給されたラップトップを初めて家に持ち帰ります。ユーザーが自宅のインターネット上の Web サイトを閲覧しようとすると、次のエラーが表示されます。
「このサイトにアクセスできません。」
職場の技術者は、マシンに設定されていた静的 IP が DHCP に戻されたことを確認しました。
修正する必要があるものは次のうちどれですか?
A. HTTPS
B. VLAN
C. DNS
D. SMTP
Answer: (解答を表示する**)**
The error "This site cannot be reached" often indicates a problem with DNS (Domain Name System) resolution, where the browser is unable to translate a website's domain name into its corresponding IP address. Since the laptop was set to use DHCP (Dynamic Host Configuration Protocol) at home, it's possible that it's not receiving the correct DNS server information from the home network, or the DNS servers it was using at work are not accessible from the home network.
* DNS: Checking and possibly correcting the DNS settings to ensure they are appropriate for the home network might resolve the browsing issue. The user can try using public DNS servers like those provided by Google (8.8.8.8 and 8.8.4.4) or Cloudflare (1.1.1.1) if the default DNS servers provided by the home ISP are not working properly.
HTTPS (A) is a protocol for secure communication over a computer network but is not something that needs to be configured on the user's end to solve this type of issue. VLAN (B) stands for Virtual Local Area Network and is more related to network segmentation and management within

larger networks, not typically applicable to home internet issues. SMTP (D) stands for Simple Mail Transfer Protocol, which is used for sending emails, not for general web browsing issues.

最新問題: **296**
技術者は Windows マシン上のローカル セキュリティ ポリシーを更新したいと考えていますが、期待されたスナップインを起動できません。最も考えられる理由は次のうちどれですか?
A. コンピューターは Windows Home を実行しています。
B. ユーザーはエンド ユーザー使用許諾契約に署名しませんでした。
C. ユーザーがユーザー アカウント制御を無効にしました。
D. ウイルス対策アプリケーションがアクセスをブロックしています。
Answer: A (メーッセージを残す**)**
The inability to launch the expected security policy snap-in is likely because the computer is running Windows Home edition, which does not include the Group Policy Editor or certain other administrative tools available in Professional, Enterprise, and Education editions. The Home edition is designed for general consumer use and lacks some of the advanced security and management features found in higher editions.

最新問題: **297**
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: B (メーッセージを残す**)**
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: **298**
従業員の新しい携帯電話のバッテリー寿命が予想より大幅に短いようで、従業員が電話を置いた後も画面が非常に長い間オンのままです。この問題のトラブルシューティングを行うために、技術者が最初に確認す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. 画面解像度
B. 画面ズーム
C. 画面タイムアウト

D. 画面の明るさ
E. 画面の損傷
F. 画面の動きの滑らかさ
Answer: C,D (メーッセージを残す)
Screen timeout is the setting that determines how long the screen stays on after the user stops interacting with the phone. Screen brightness is the setting that determines how much light the screen emits. Both of these settings affect the battery life of the phone, as keeping the screen on longer and brighter consumes more power than turning it off sooner and dimmer. A technician should check these settings first to troubleshoot the issue of low battery life and adjust them accordingly. Screen resolution, screen zoom, screen damage, and screen motion smoothness are not settings that directly affect the battery life or the screen staying on for a long time.

最新問題**: 299**
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**: 300**

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**: 301**

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: 302
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
コマンド:
イベント ビューアー:

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**: 303**
技術者が SOHO デバイスを構成しています。会社のポリシーでは、静的 IP アドレスは使用できないと規定されています。会社は、サーバーが常に同じ IP アドレスを維持することを望んでいます。技術者は次のうちどれを使用する必要がありますか?
A. DHCP 予約
B. ポートフォワーディング
C. DNS A レコード
D. NAT
Answer: A (メーッセージを残す**)**
The technician should use DHCP reservation to maintain the same IP address for the server at all times.
DHCP reservation allows the server to obtain an IP address dynamically from the DHCP server, while ensuring that the same IP address is assigned to the server each time it requests an IP address.

最新問題**: 304**
会社は携帯電話を 1 対 1 で展開していますが、IT マネージャーは、ユーザーが携帯電話をルート化/ジェイルブレイクすることを懸念しています。この問題を防ぐために実装できるテクノロジは次のうちどれですか?
A. 署名付きシステム イメージ

B. ウイルス対策
C. SSO
D. MDM
Answer: D (メーッセージを残す)
MDM stands for Mobile Device Management, and it is a way of remotely managing and securing mobile devices that are used for work purposes1. MDM can enforce policies and restrictions on the devices, such as preventing users from installing unauthorized apps, modifying system settings, or accessing root privileges2. MDM can also monitor device status, wipe data, lock devices, or locate lost or stolen devices1.

最新問題**: 305**
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**: 306**
技術者は、Web 広告 Now をクリックしたユーザーから電話を受けました。ユーザーがマウスを動かすたびに、モニター上にポップアップが表示されます。技術者が実行すべき手順は次のうちどれですか?
A. セーフモードで起動します。
B. マルウェア スキャンを実行します。
C. マシンを再起動します。
D. ブラウザを再インストールします
Answer: (解答を表示する)
Booting into safe mode and performing a malware scan are the steps that a technician should perform when troubleshooting an issue with pop-up advertising messages on a PC. Safe mode is a diagnostic mode that starts the PC with minimal drivers and services, which can prevent the pop-up malware from running.
Malware scan is a tool that can detect and remove the pop-up malware, as well as prevent further infection or damage. Investigating how the malware was installed, reinstalling the browser and

restarting the machine are possible steps that can be done after booting into safe mode and performing a malware scan, depending on the situation and the results of the scan. Verified References: https://www.comptia.org/blog/how-to-boot-into- safe-mode https://www.comptia.org/certifications/a

最新問題: **307**
ユーザーのスマートフォンから機密データが流出しました。技術者は、承認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を発見し、ユーザーはデバイスのコマンド シェルに完全にアクセスできます。漏洩したデータの原因を突き止め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. デバイスを工場出荷時の設定に戻します。
B. 承認されていないアプリケーションをアンインストールします。
C. 提供元不明のアプリケーションをインストールする機能を無効にします。
D. デバイスが企業の WiFi ネットワークに接続されていることを確認します。
Answer: B (メーッセージを残す**)**
The technician should disable the user's access to the device's command shell. This will prevent the user from accessing sensitive data and will help to prevent further data leaks. The technician should then investigate the unapproved application to determine if it is the cause of the data leak. If the application is found to be the cause of the leak, the technician should uninstall the application and restore the device to factory settings. If the application is not the cause of the leak, the technician should investigate further to determine the cause of the leak. Disabling the ability to install applications from unknown sources can help to prevent future data leaks, but it is not the next step the technician should take in this scenario. Ensuring the device is connected to the corporate WiFi network is not relevant to this scenario1

最新問題: **308**
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: (解答を表示する**)**
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: **309**
Active Directory アカウント作成のスクリプト作成に使用される言語は次のどれですか?
A. Bash
B. SQL
C. PHP
D. PowerShell
Answer: D (メーッセージを残す)
PowerShell is a scripting language that can interact with Active Directory and other Windows components. It has a built-in cmdlet called New-ADUser that can create user accounts in Active Directory. PowerShell can also use the Active Directory module to access other AD-related functions and attributes. Other languages, such as Bash, SQL, and PHP, are not designed for creating Active Directory accounts and would require additional tools or libraries to do so.

最新問題: **310**
次のうち、ネイティブ ファイル システムとして NTFS を使用する可能性が最も高いのはどれですか?
A. macOS
B. Linux
C. Windows
D. アンドロイド
Answer: C (メーッセージを残す)
NTFS stands for New Technology File System, which is a proprietary file system developed by Microsoft4. NTFS is the default file system for the Windows NT family of operating systems, which includes Windows 10, Windows Server 2019, and other versions5. NTFS provides features such as security, encryption, compression, journaling, and large volume support45. NTFS is not the native file system for other operating systems, such as macOS, Linux, or Android, although some of them can read or write to NTFS volumes with third-party drivers or tools

最新問題: **311**
特定の Web サイトにアクセスすると、ユーザーは あなたの接続はプライベートではありません」というメッセージを受け取ります。この問題について説明しているのは次のうちどれですか?
A. 証明書の警告
B. マルウェア
C. JavaScript エラー
D. OS アップデートがありません
Answer: A (メーッセージを残す)
A certificate warning is a message that appears when a web browser cannot verify the identity or security of a website. It usually means that there is a problem with the website's SSL certificate,

such as expiration, invalidity, or mismatch. A certificate warning can indicate that the website is unsafe or compromised, and that the user's connection is not private123.
References: 1 How to Fix "Your Connection Is Not Private" Errors - How-To Geek(https://www.howtogeek.com/874436/how-to-fix-your-connection-is-not-private-errors/)2 How to fix a "Your connection is not private" error - Norton(https://us.norton.com/blog/how-to/your-connection-is-not-private)3 "Your Connection Is Not Private" Error: 8 Ways to Fix It - HubSpot Blog(https://blog.hubspot.com/website/how-to-fix-your- connection-is-not-private).

最新問題**: 312**
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**: 313**
エンジニアは、ベアメタル インストールを必要とする新しいサーバーを構成しています。インストール メディアが現場で入手できない場合、エンジニアは次のインストール方法のうちどれを使用する必要がありますか?
A. イメージの展開
B. 回復パーティションのインストール
C. リモートネットワークインストール
D. 修復インストール
Answer: D (メーッセージを残す**)**
Remote network installation is the best option for configuring a new server that requires a bare-metal installation without installation media on site. A remote network installation is a method of installing an operating system or an application over a network connection, such as LAN, WAN, or Internet. A remote network installation can use various protocols, such as PXE, HTTP, FTP, or SMB, to access the installation files from a server or a cloud service. A remote network installation can also use various tools, such as Windows Deployment Services, Microsoft Deployment Toolkit, or Red Hat Kickstart, to automate and customize the installation process. A remote network installation can save time and resources by eliminating the need for physical

media and allowing centralized management of multiple installations. Image deployment, recovery partition installation, and repair installation are not correct answers for this question. Image deployment is a method of installing an operating system or an application by copying a preconfigured image file to a target device. Image deployment requires an existing image file and a compatible device.
Recovery partition installation is a method of restoring an operating system or an application from a hidden partition on the hard disk that contains the original factory settings. Recovery partition installation requires an existing recovery partition and a functional hard disk. Repair installation is a method of fixing an operating system or an application that is corrupted or damaged by replacing or repairing the system files without affecting the user data or settings. Repair installation requires an existing operating system or application and a working device.
References:
* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 16
* CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 106

最新問題**: 314**
セキュリティ イベントの後、技術者は影響を受けるラップトップからマルウェアを削除し、ラップトップをネットワークから切断します。オペレーティング システムが自動的に感染状態に戻るのを防ぐために、技術者が行うべきことは次のうちどれですか?
A. システムの復元を有効にします。
B. システムの復元を無効にします。
C. ウイルス対策を有効にします。
D. ウイルス対策を無効にします。
E. ユーザーを教育します。
Answer: B (メーッセージを残す**)**
System Restore is a feature that allows the user to revert the system to a previous state. However, this can also restore the malware that was removed by the technician. Disabling System Restore can prevent the operating system from automatically returning to an infected state. Enabling antivirus, educating the user, and enabling System Restore are good preventive measures, but they do not address the question. Disabling antivirus can make the system more vulnerable to malware attacks

最新問題**: 315**
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**: 316**
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**: 317**
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**: 318**
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**: 319**

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**: 320**
技術者は、Windows 10 ワークステーションでセキュリティ設定を構成する必要があります。技術者はパスワードの試行を制限するために次のどれを構成する必要がありますか?
A. アカウント ロックアウト ポリシー
B. ユーザー アクセス制御
C. システム保護
D. ファイアウォール
Answer: (解答を表示する**)**
Configuring the Account Lockout Policy in Windows 10 is the appropriate action to limit password attempts.
This security setting determines the number of failed login attempts that will trigger a lockout, preventing unauthorized access due to repeated password guessing. It is an effective measure to enhance security by deterring brute-force attacks.

最新問題**: 321**
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: D (メーッセージを残す)
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**: 322**
ユーザーの Android スマートフォンがランダムに再起動しています。技術者が調査したところ、標準のマーケットプレイスでは入手できないアプリケーションがいくつかインストールされていることがわかりました。この問題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 の更新に失敗しました。
B. ユーザーがマルウェアをダウンロードしました。
C. デバイスは開発者モードです。
D. 無線キャリアアップデートに失敗しました。
Answer: (解答を表示する)
Random restarting of an Android phone and the presence of applications not from the standard marketplace strongly suggest the possibility of malware.
* Option A: The OS update failedWhile an OS update failure can cause issues, it is less likely to result in random restarts compared to malware.
* Option B: The user downloaded malwareMalware is a common cause of erratic behavior, including random restarts, especially when applications are installed from unofficial sources.
* Option C: The device is in developer modeDeveloper mode alone does not typically cause random restarts. It may make the device more susceptible to issues if improper apps are installed.
* Option D: The over-the-air carrier update failedSimilar to the OS update, this would more likely cause consistent issues rather than random restarts.
References:
CompTIA A+ 220-1102 Objective 2.3 (Detect, remove, and prevent malware) and Objective 3.5 (Mobile OS and application security issues).

最新問題**: 323**
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**: 324**
技術者がワークステーションに Windows 10 をインストールしました。技術者が 8 GB をインストールしたにもかかわらず、ワークステーションには 3.5 GB の使用可能な RAM しかありません。このシステムが使用可能な RAM をすべて使用していない理由として最も可能性が高いのは次のどれですか。
A. システムに BIOS アップデートが必要です。
B. システムのメモリに障害が発生しています。
C. システムに更新がありません。
D. 32 ビット OS を利用するシステム。
Answer: D (メーッセージを残す**)**

最新問題**: 325**
ユーザーが職務を遂行するために適切なレベルのアクセス権を持っていることを確認するために使用されるのは次のうちどれですか?
A. アクセス制御リスト
B. 多要素認証
C. 最低権限
D. モバイルデバイス管理
Answer: (解答を表示する**)**
Least privilege is the principle that is used to ensure users have the appropriate level of access to perform their job functions. Least privilege means granting users only the minimum amount of access rights and permissions they need to perform their tasks, and nothing more. Least privilege reduces the risk of unauthorized access, data leakage, malware infection, or accidental damage by limiting what users can do on the system or network. Access control list, multifactor authentication, and mobile device management are not principles, but rather mechanisms or methods that can implement least privilege. Access control list is a list that specifies the users or groups that are allowed or denied access to a resource, such as a file, folder, or printer. Multifactor authentication is a method that requires users to provide two or more pieces of evidence to prove their identity, such as a password, a token, or a biometric factor. Mobile device management is a tool that allows managing and securing mobile devices, such as smartphones or tablets, that are used by employees to access corporate data or applications. References:
* Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25
* [CompTIA Security+ SY0-601 Certification Study Guide], page 1003

最新問題: **326**
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: **327**
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: **328**
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**: 329**
次のファイルタイプのうち、ゴミ箱に入れるだけで macOS からソフトウェアを簡単にアンインストールできるのはどれですか?
* .exe
A. .dmg
B. . app
C. . rpm
D. .pkg
Answer: C (メーッセージを残す)
app files are application bundles that contain all the necessary files and resources for a Mac app. They can be easily deleted by dragging them to the Trash or using Launchpad12. Other file types, such as .exe, .dmg, .rpm, and .pkg, are either not compatible with macOS or require additional steps to uninstall34.
References: 1 Uninstall apps on your Mac - Apple Support(https://support.apple.com/en-us/102610)2 How to Uninstall Apps on a Mac (and Make Sure Leftover Files Are ... (https://www.pcmag.com/how-to/uninstall- delete-apps-from-mac)3 How to install and uninstall software on a Mac - Laptop Mag(https://www.laptopmag.com/articles/install-unininstall-mac-software)4 How to completely uninstall an app on a Mac and delete all junk files(https://www.xda-developers.com/how-to-uninstall-app-mac/).

最新問題**: 330**
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: D (メーッセージを残す**)**
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**: 331**
技術者が新しいコンピュータにオペレーティング システムをインストールしています。プロセスの最初のステップは次のどれですか。
A. 起動順序の設定
B. ハードドライブのフォーマット
C. プロダクトキーの入力
D. ファイルシステムの選択
Answer: A (メーッセージを残す**)**
The first step in installing an operating system on a new computer is Setting the boot order (Option A). This ensures that the computer can boot from the installation media (USB, DVD, etc.). Once the boot order is configured, the system can start from the installation source, and the rest of the OS installation process can proceed.
* Formatting the hard drive (Option B) comes later in the process, after the installation media is booted.
* Entering the product key (Option C) and Selecting the filesystem (Option D) are subsequent steps during the installation process.
CompTIA A+ Core 2 References:
* 1.9 - Perform OS installations and upgrades, including setting boot methods and boot order.

最新問題**: 332**
エンド ユーザーは、職務上特別な責任があるため、Windows システム ファイルのプロパティを編集する権限が必要です。ユーザーには、すでにローカル管理者権限が付与されています。ファイル

に簡単にアクセスできるようにするには、次のコントロール パネル ユーティリティのどれを使用する必要がありますか。
A. ファイルエクスプローラーのオプション
B. アクセスのしやすさ
C. インデックスオプション
D. 管理ツール
Answer: D (メーッセージを残す)
The correct answer is Administrative Tools (Option D), which provides access to several system utilities, including those needed for managing system files and settings. Since the user already has local administrator privileges, this would allow them to edit system properties efficiently.
* File Explorer Options (Option A) manage general file display settings but do not provide administrative access.
* Ease of Access (Option B) is related to accessibility settings, not file management.
* Indexing Options (Option C) control how files are indexed for search, but are unrelated to system file editing.
CompTIA A+ Core 2 References:
* 1.3 - Use features and tools of the Windows operating system, including Administrative Tools.

最新問題**: 333**
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: (解答を表示する)
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: **334**
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: **335**
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: **336**
次のデフォルトのシステム ツールのうち、技術者がユーザーと同時に画面を表示できるようにするために macOS で使用できるものはどれですか?
A. リモート アシスタンス

B. リモート デスクトップ プロトコル
C. 画面共有
D. 仮想ネットワーク コンピューティング
Answer: (解答を表示する**)**
Screen Sharing is the default system tool that can be used in macOS to allow the technician to view the screen simultaneously with the user. Screen Sharing is a built-in app that lets users share their Mac screen with another Mac on the network. The user can enable screen sharing in the System Preferences > Sharing pane, and then allow other users to request or enter a password to access their screen1. The technician can launch the Screen Sharing app from the Spotlight search or the Finder sidebar, and then enter the user's name, address, or Apple ID to connect to their screen2. Remote Assistance is a Windows feature that allows users to invite someone to help them with a problem on their PC3. Remote Desktop Protocol (RDP) is a protocol that allows users to connect to a remote computer over a network4. Virtual Network Computing (VNC) is a technology that allows users to share their screen with other devices using a VNC viewer app1. These are not default system tools in macOS, although they can be used with third-party software or settings.
References: 1: https://support.apple.com/guide/mac-help/share-the-screen-of-another-mac-mh14066/mac 2:
https://www.howtogeek.com/449239/how-to-share-your-macs-screen-with-another-mac/ 3:
https://support.
microsoft.com/en-us/windows/solve-pc-problems-over-a-remote-connection-b077e31a-16f4-2529-1a47-
21f6a9040bf3 4: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients
/remote-desktop-protocol

最新問題**: 337**
顧客サービス担当者は、リモートの支社にあるプリンタにジョブを送信できません。ただし、担当者はローカル ネットワーク プリンタに正常に印刷できます。技術者が PC からネットワーク トラフィックのパスを表示するには、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. netstat
B. ping
C. format
D. tracert
Answer: D (メーッセージを残す**)**
The "tracert" command is used to view the path that network traffic takes from a PC to a specified destination.
It is helpful in identifying where along the path the traffic may be failing or experiencing delays. In the scenario where a customer service representative can't send jobs to a remote printer but can print locally,

"tracert" can help diagnose if there's a network routing issue affecting the connection to the remote branch office.

最新問題: **338**
技術者は、ワークステーションのソフトウェアの問題に関するヘルプ デスク チケットを受け取ります。ワークステーションは企業データベースへの唯一のアクセスを提供するため、技術者はワークステーションを迅速に回復する必要があります。技術者は次のどのアクションを実行する必要がありますか。
A. 最後のバックアップからワークステーションを復元します。
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 ファイル チェッカーを実行します。
D. ハードウェア診断ツールを実行します。
Answer: (解答を表示する**)**
Full Comprehensive Explanation: In this situation, the priority is to get the workstation back online and accessing the corporate database as quickly as possible. Restoring from the last backup is the most efficient way to achieve this. It will revert the system to a known working state, likely resolving the software issue without the need for extensive troubleshooting.

最新問題: **339**
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: A (メーッセージを残す**)**
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: **340**
最近、ある顧客が SOHO で停電を経験しました。顧客は、コンポーネントが正しく接続されていないと考えています。停電後も数分間は印刷ジョブが継続していましたが、顧客はコンピューターを操作できませんでした。UPS のビープ音が止まると、機能しているすべてのデバイスもオフになりました。将来停電が発生した場合に備えて、顧客はクラウド ドキュメントを保存し、デー

タを失うことなくコンピューターをシャットダウンするための時間を最大限に確保したいと考えています。
Answer:
UPS > Surge protector = Computer, wifi router, cable modem
Surge protector = wallOutlet , printer and scanner

最新問題**: 341**
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: (解答を表示する**)**
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**: 342**
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: (解答を表示する**)**

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**: 343**
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**: 344**
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**: 345**
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**: 346**
macOS が使用するファイルシステムの種類は次のうちどれですか?
A. ext4
B. exFAT
C. NTFS
D. APFS
Answer: D (メーッセージを残す**)**
APFS stands for Apple File System and it is the default filesystem type for macOS since High Sierra (10.13) version1. APFS is optimized for flash storage and supports features such as encryption, snapshots, cloning, and space sharing1.

最新問題**: 347**
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**: 348**
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**: 349**
ユーザーは、職場の PC に保存されているいくつかのドキュメントにアクセスできません。技術者はファイルが破損していることを発見し、問題を修正するにはレジストリ エディター内でいくつかのシステム設定を変更する必要があります。技術者がレジストリ キーを変更する前に行うべきことは次のうちどれですか?
A. マルウェア対策ソフトウェアを更新します。
B. 復元ポイントを作成します。
C. PC をステート モードで実行します。
D. システムアップデートをロールバックします。
Answer: B (メーッセージを残す**)**
A restore point is a snapshot of the system settings and configuration at a specific point in time2. Creating a restore point before modifying the registry keys allows the technician to revert the system back to a previous state if something goes wrong or causes instability2. Updating the anti-malware software, running the PC in safe mode, and rolling back the system updates are not necessary steps before modifying the registry keys.

最新問題**: 350**
Linux 技術者には、次の要件を満たすファイルシステム タイプが必要です。
すべての変更が追跡されます。
ファイルが破損する可能性が低減されます。
* データの復旧は簡単です。
次のファイルシステムの種類のどれがこれらの要件を最もよく満たしていますか?
* 拡張子3
A. FAT32
B. exFAT
C. NTFS
Answer: A (メーッセージを残す**)**
The ext3 file system is a Linux native file system that meets the requirements of the question. It has the following features:
* All changes are tracked. The ext3 file system uses a journaling mechanism that records all changes to the file system metadata in a special log called the journal before applying them to the

actual file system. This ensures that the file system can be restored to a consistent state in case of a power failure or system crash12.
* The possibility of file corruption is reduced. The journaling feature of ext3 also reduces the possibility of file corruption, as it avoids the need for a full file system check after an unclean shutdown. The file system can be quickly replayed from the journal and any inconsistencies can be fixed12.
* Data recovery is easy. The ext3 file system supports undeletion of files using tools such as ext3grep or extundelete, which can scan the file system for deleted inodes and attempt to recover the data blocks associated with them34.
References:
1: Introduction to Linux File System [Structure and Types] - MiniTool1 2: 7 Ways to Determine the File System Type in Linux (Ext2, Ext3 or Ext4) - Tecmint3 3: How to Recover Deleted Files in Linux with ext3grep 4: How to Recover Deleted Files from ext3 Partitions

最新問題**: 351**
従業員の会社のスマートフォンが紛失または盗難された場合に、機密データの損失を制限する最善の方法は次のうちどれですか?
A. VPN のインストール
B. 位置追跡の実装
C. リモート ワイプの構成
D. バックアップの有効化
Answer: C (メーッセージを残す**)**
Configuring remote wipe allows the device owner or administrator to erase all the data on the device remotely, in case it is lost or stolen. This prevents unauthorized access to confidential data and reduces the risk of data breaches. Installing a VPN, implementing location tracking, and enabling backups are useful features, but they do not directly limit the loss of data if the device is compromised. References: CompTIA A+ Certification Exam Core 2 Objectives, Domain 2.0: Security, Objective 2.5: Given a scenario, use methods to secure mobile devices.

最新問題**: 352**
最近、ある企業がランサムウェアによる攻撃を受けました。IT 部門は脅威を修復し、使用された攻撃方法は電子メールであると判断しました。この問題の再発を防ぐ最も効果的な方法は次のうちどれですか?
A. スパムフィルタリング
B. マルウェア防止ソフトウェア
C. エンドユーザー教育
D. ステートフル ファイアウォール検査
Answer: C (メーッセージを残す**)**
To prevent ransomware attacks via email, the most effective way is End user education (C). Educating users about the dangers of phishing emails, how to recognize suspicious emails, and

the importance of not clicking on unknown links or attachments can significantly reduce the risk of ransomware infections. Awareness and training can empower users to act as the first line of defense against such cyber threats

最新問題: **353**
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: C (メーッセージを残す**)**
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: **354**
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: D (メーッセージを残す**)**
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**: 355**
顧客はビデオをレンダリングできるデスクトップを購入する必要があります。顧客は次のどれを優先すべきでしょうか?
A. NIC
B. USB
C. GPU
D. HDMI
Answer: (解答を表示する**)**
For rendering video, the most critical component a customer should prioritize in a desktop is:
* GPU (Graphics Processing Unit): The GPU is specifically designed to handle complex graphics and video rendering tasks. A powerful GPU will significantly improve performance in video rendering applications.
* NIC (Network Interface Card): Important for network connectivity but irrelevant for video rendering.
* USB: Useful for peripherals but does not impact video rendering capabilities.
* HDMI: An important output interface for connecting monitors but not crucial for the rendering process itself.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 1.8: Explain common OS types and their purposes, including hardware components for specific tasks.
GPU importance in video rendering documentation.

最新問題**: 356**
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: **357**
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: **358**
技術者は、Windows ワークステーションでのアプリケーションのクラッシュのトラブルシューティングを行っています。ワークステーション ユーザーがブラウザで Web サイトを開こうとするたびに、次のメッセージが表示されます。
crypt32.d11 が見つからない
技術者が最初に試みる必要があるのは、次のうちどれですか?
A. Windows プロファイルを再構築します。
B. ワークステーションの再イメージ化
C. 更新をロールバックします
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**)**
If this file is missing or corrupted, it can cause application crashes or errors when trying to open websites in a browser. To fix this, the technician can perform a system file check, which is a utility that scans and repairs corrupted or missing system files1. To perform a system file check, the technician can follow these steps:
* Open the Command Prompt as an administrator. To do this, type cmd in the search box on the taskbar, right-click on Command Prompt, and select Run as administrator.

* In the Command Prompt window, type sfc /scannow and hit Enter. This will start the scanning and repairing process, which may take some time.
* Wait for the process to complete. If any problems are found and fixed, you will see a message saying Windows Resource Protection found corrupt files and successfully repaired them. If no problems are found, you will see a message saying Windows Resource Protection did not find any integrity violations.
* Restart your computer and check if the issue is resolved.

最新問題**: 359**
技術者は、起動時に不要なアプリケーションが起動する Windows 10 PC で作業しています。技術者が起動時にアプリケーションを無効に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. システム構成
B. タスクマネージャー
C. パフォーマンスモニター
D. グループ ポリシー エディター
Answer: B (メーッセージを残す**)**
Task Manager is the best tool to use to disable applications on startup in Windows 10. Task Manager is a built-in utility that shows the current processes, performance, and users on a system. It also has a Startup tab that lists the applications that run on boot and their impact on the system. The technician can use Task Manager to disable or enable any application on startup by right-clicking on it and selecting the appropriate option. System Configuration, Performance Monitor, and Group Policy Editor are other tools that can be used to manage system settings, but they are not as simple or convenient as Task Manager for this task. 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**: 360**
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: (解答を表示する**)**
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: **361**
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: **362**
ユーザーから次の問題が報告されました:
*彼らのコンピュータは常に動作が遅いです。
※Webブラウザのデフォルトのホームページが怪しい検索エンジンに変更されました。
※画面上にポップアップ広告が表示されるようになりました。

これらの問題に対処するために技術者が最初に行うべきことはどれですか?
A. ウイルス対策プログラムを更新し、システム全体のスキャンを実行します。
B. 疑わしい検索エンジンをアンインストールし、ホームページをリセットします。
C. オペレーティング システムの最新の更新プログラムをインストールします。
D. Web ブラウザの設定を使用してポップアップ広告をブロックします。
Answer: (解答を表示する**)**
When a user reports slow performance, a changed home page, and pop-up ads, these are classic signs of malware infection. The first step should be:
* Update the antivirus program and run a full system scan: This helps identify and remove any malware present on the system, addressing the root cause of the issues.
* Uninstall the suspicious search engine and reset the home page: This addresses the symptom but not the underlying cause, which is likely malware.
* Install the latest updates for the operating system: Important for security but secondary to removing malware.
* Block the pop-up ads using the web browser settings: Again, addresses the symptom but not the root cause.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 3.3: Given a scenario use best practice procedures for malware removal.
Malware identification and removal documentation.

最新問題**: 363**
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**: 364**
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: (解答を表示する**)**
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**: 365**
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: **366**
最近の停電の後、複数のコンピューターで起動時にエラーが発生しました。技術者は、ファイルの破損が発生した疑いがあります。問題を解決するために技術者が最初に試すべき手順は次のうちどれですか?
A. Windows プロファイルを再構築します。
B. コンピュータをバックアップから復元します。
C. コンピュータを再イメージ化します。
D. システム ファイル チェッカーを実行します。
Answer: (解答を表示する**)**
The technician should run the System File Checker (SFC) first to correct file corruption errors on computers after a power outage. SFC is a command-line utility that scans for and repairs corrupted system files. It can be run from the command prompt or from the Windows Recovery Environment. Rebuilding the Windows profiles, restoring the computers from backup, and reimaging the computers are more drastic measures that should be taken only if SFC fails to correct the issue1

最新問題: **367**
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: **368**
技術者は午後 10 時から時間外サービスを実行する必要があります。技術者は現在 20 分遅れています。顧客も遅れる予定です。適切なコミュニケーション技術とプロ意識を考慮して、技術者は次のうちどれを行う必要がありますか。
※お客様より先に到着する場合は、お客様に通知しないでください。
A. 顧客を解雇し、営業時間外の作業を進めます。
B. 技術者が遅れて到着する場合は顧客に連絡します。

C. ソーシャルメディアを通じて体験を公開します。
Answer: C (メーッセージを残す**)**
The best option for the technician to demonstrate proper communication techniques and professionalism is to contact the customer if the technician is arriving late. This shows respect for the customer's time and expectations, and allows the customer to adjust their schedule accordingly. It also helps to maintain a positive relationship and trust between the technician and the customer. The technician should apologize for the delay and provide a realistic estimate of their arrival time. The technician should also thank the customer for their patience and understanding.
The other options are not appropriate or professional. Do not notify the customer if arriving before the customer is not a good practice, as it may cause confusion or frustration for the customer. The customer may have made other plans or arrangements based on the technician's original schedule, and may not be available or prepared for the service. Dismiss the customer and proceed with the after-hours work is rude and disrespectful, as it ignores the customer's needs and preferences. The customer may have questions or concerns about the service, or may want to supervise or verify the work. The technician should always communicate with the customer before, during, and after the service. Disclose the experience via social media is unethical and unprofessional, as it may violate the customer's privacy and the company's policies. The technician should not share any confidential or sensitive information about the customer or the service on social media, or make any negative or inappropriate comments about the customer or the situation.
References:
CompTIA A+ Certification Exam Core 2 Objectives1
CompTIA A+ Core 2 (220-1102) Certification Study Guide2
8 Ways You Can Improve Your Communication Skills3
Professionalism in Communication | How To Do It And How It Pays4

最新問題**: 369**
リモート ユーザーが、歪んでいると思われる電子メールについてヘルプ デスクに問い合わせました。技術者はユーザーの意味がわからないため、トラブルシューティングを支援するために電子メールを確認する必要があります。技術者がユーザーを支援するために使用すべきものは次のうちどれですか?
A. VNC
B. SSH
C. VPN
D. RMM
Answer: (解答を表示する**)**
The best tool to use to assist the user with viewing the email is RMM, which stands for remote monitoring and management. This is a software that allows the technician to remotely access, monitor, and manage the user's computer and applications. The technician can use RMM to view the user's screen, control the mouse and keyboard, and troubleshoot the email issue. The other

tools are not suitable for this task. VNC is a software that allows remote desktop sharing, but it requires the user to install and configure it on their computer, which may not be feasible or convenient. SSH is a protocol that allows secure remote access to a command-line interface, but it is not useful for viewing graphical applications such as email. VPN is a technology that creates a secure and encrypted connection over a public network, but it does not provide remote access or control of the user's computer.

最新問題: **370**
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: D (メーッセージを残す)
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: **371**
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: C (メーッセージを残す)
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: **372**

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**: 373**
ユーザーが最近、新しいスキャナーと関連ソフトウェアをコンピューターにインストールしたところ、コンピューターの起動が非常に遅くなっていることに気付きました。この問題のトラブルシューティングに最適なツールは次のどれですか。
A. リソースモニター
B. タスク マネージャー
C. デバイス マネージャー
D. Windows アップデート
E. イベント ビューアー
Answer: B (メーッセージを残す)
Reference: CompTIA A+ Certification Core 2 220-1102, Objective 3.1 (Windows Performance Troubleshooting).

最新問題**: 374**
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: A (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)

最新問題**: 375**
macOS でコマンド ラインへのアクセスを許可するのは次のうちどれですか?

A. PsExec
B. command.com
C. Terminal
D. CMD
Answer: C (メーッセージを残す)
Terminal is an application that allows access to the command line in macOS. The command line is an interface that allows users to interact with the operating system and perform various tasks by typing commands and arguments. Terminal can be used to launch programs, manage files and folders, configure settings, troubleshoot issues, and run scripts in macOS. PsExec, command.com, and CMD are not applications that allow access to the command line in macOS.

最新問題**: 376**
ある銀行は、顧客が簡単にアクセスできるようにしながら、車両が建物に侵入するのを防ぐために、建物のセキュリティを強化したいと考えています。次のうち、このニーズに対応するのに最も適しているのはどれですか?
A. ガード
B. ボラード
C. モーションセンサー
D. アクセス制御前庭
Answer: B (メーッセージを残す)
Bollards are the best solution to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers4 References: 2. Bollards. Retrieved from https://en.wikipedia.org/wiki/Bollard

最新問題**: 377**
ユーザーが Internet Explorer を使用してインターネットを閲覧しようとしています。使い慣れた Web ページを読み込もうとすると、ユーザーは予期せず見慣れない Web サイトにリダイレクトされます。次のうち、問題を解決する可能性が最も高いのはどれですか?
A. OSのアップデート
B. プロキシ設定の変更
C. ブラウザの再インストール

D. ポートフォワーディングを有効にする
Answer: C (メーッセージを残す**)**
Reinstalling the browser would most likely solve the issue. This would remove any malicious software or add- ons that may be causing the issue and restore the browser to its default settings.

最新問題**: 378**
予期せぬ支払い期限切れの請求書のメール添付ファイルを開こうとして失敗した後、スマートフォン ユーザーはモバイル ブラウザーやその他のアプリケーションの使用時に異常なパフォーマンスを経験します。ユーザーはデバイスを再起動しましたが、問題は解決しません。次に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. スマートフォンをシャットダウンしてコールドスタートする
B. 添付ファイルを含むメールを削除する
C. デバイスを消去して工場出荷時の状態にリセットします
D. モバイルブラウザをアンインストールして再インストールする
Answer: C (メーッセージを残す**)**
In this case, abnormal behavior after opening a suspicious email suggests malware might have infected the device. A full factory reset is recommended to remove any persistent malware, especially when a restart does not resolve the issue. Deleting the email or reinstalling the browser will not remove the malware already on the device.
Reference: Core 2, Domain 2.3 - Malware detection and removal.

最新問題**: 379**
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**: 380**

小規模オフィスの管理チームは、不適切な Web サイトへのアクセスをブロックし、これらのアクセス試行のログを作成したいと考えています。これらの要件を満たす方法は次のうちどれですか?
A. コンテンツフィルター
B. スクリーンされたサブネット
C. ポートフォワーディング
D. アクセス制御リスト
Answer: A (メーッセージを残す**)**
A content filter is a device or software that blocks or allows access to web pages based on predefined criteria, such as keywords, categories, or ratings. A content filter can also create a log of the blocked or allowed web requests, which can help the management team monitor and audit the web usage of their employees. A content filter is different from the other options because:
* A screened subnet is a network segment that is protected by two firewalls, one facing the internet and one facing the internal network. A screened subnet can isolate servers or hosts that need to be accessed from both sides, such as a web server or a bastion host. A screened subnet does not filter web content based on predefined criteria, but rather on network addresses, ports, and protocols.
* Port forwarding is a technique that allows a router to forward packets from one port to another port, usually on a different device. Port forwarding can enable remote access to services or applications that are hosted on a private network, such as a web server or a game server. Port forwarding does not filter web content based on predefined criteria, but rather on destination ports and addresses.
* An access control list (ACL) is a set of rules that defines which packets are allowed or denied on a network device, such as a router or a firewall. An ACL can filter packets based on source and destination addresses, ports, protocols, and other criteria. An ACL can also create a log of the matched or unmatched packets, which can help the management team troubleshoot and secure their network. An ACL does not filter web content based on predefined criteria, but rather on packet headers and fields.

最新問題**: 381**
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: C (メーッセージを残す**)**

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: **382**
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: **383**
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: **384**
ユーザーがラップトップをワイヤレス ネットワークに接続し、だまされて Web サイトのログイン資格情報を提供させられました。攻撃の実行に使用された脅威は次のうちどれですか?
A. Zero day
B. Vishing
C. DDoS
D. Evil twin
Answer: (解答を表示する**)**
Vishing, also known as voice phishing, is a type of social engineering attack where the attacker tricks the victim into divulging sensitive information over the phone. In this case, the attacker tricked the user into providing login credentials for a website.

最新問題: **385**
Windows 10 の次のエディションのうち、180 日ごとに再アクティベーションが必要なのはどれですか?
A. Enterprise
B. Pro for Workstation
C. Home
D. Pro
Answer: A (メーッセージを残す**)**
Windows 10 Enterprise is an edition of Windows 10 that is designed for large organizations that need advanced security and management features. Windows 10 Enterprise can be activated using different methods, such as Multiple Activation Key (MAK), Active Directory-based Activation (ADBA), or Key Management Service (KMS)1. KMS is a method of activation that uses a local server to activate multiple devices on a network. KMS activations are valid for 180 days and need to be renewed periodically by connecting to the KMS server2. If a device does not renew its activation within 180 days, it will enter a grace period of 30 days, after which it will display a warning message and lose some functionality until it is reactivated3. The other editions of Windows 10 do not require reactivation every 180 days. Windows 10 Pro for Workstation is an edition of Windows 10 that is designed for high-performance devices that need advanced features such as ReFS file system, persistent memory, and faster file sharing. Windows 10 Pro for Workstation can be activated using a digital license or a product key. Windows 10 Home is an edition of Windows 10 that is designed for personal or home use. Windows 10 Home can be activated using a digital license or a product key. Windows 10 Pro is an edition of Windows 10 that is designed for business or professional use. Windows 10 Pro can be activated using a digital license or a product key. None of these editions require reactivation every 180 days unless there are significant hardware changes or other issues that affect the activation status.

最新問題: **386**

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: C (メーッセージを残す)

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**: 387**

コンピューター上のアプリケーションが更新されていないため、ユーザーは特定のファイルを開けることができません。問題のトラブルシューティングを続けるために、技術者が次に起動する必要がある MMC スナップインは次のうちどれですか?

A. gpedit.msc

B. perfmon.msc

C. devmgmt.msc

Answer: (解答を表示する)

devmgmt.msc is the MMC snap-in that opens the Device Manager, a tool that allows the technician to view and manage the hardware devices and their drivers on the computer1. If the applications are not updating properly, it could be due to outdated, corrupted, or incompatible drivers that prevent the hardware from functioning normally. The technician can use the Device Manager to update, uninstall, rollback, or disable the drivers, as well as scan for hardware changes, troubleshoot problems, and view device properties2.

gpedit.msc is the MMC snap-in that opens the Group Policy Editor, a tool that allows the technician to configure the local or domain group policy settings for the computer or a group of computers3. Group policy settings can affect the security, performance, and functionality of the system, but they are not directly related to the application updates or the hardware drivers.

perfmon.msc is the MMC snap-in that opens the Performance Monitor, a tool that allows the technician to monitor and analyze the performance of the system and its components, such as processor, memory, disk, network, etc4. Performance Monitor can display real-time data or collect log data for later analysis, as well as generate reports and alerts based on the performance counters5. Performance Monitor can help the technician identify and diagnose performance issues, but it does not provide a way to manage the hardware drivers.

References:

The Official CompTIA A+ Core 2 Study Guide6, page 223, 225, 227, 228.

最新問題: **388**
ユーザーはインターネットにアクセスできませんが、ネットワーク プリンターに印刷することはできます。他のユーザーはこの問題を経験していません。技術者が問題を診断するために最初に実行する必要がある手順はどれですか。
A. 物理的な接続を検証します。
B. ルーターを再起動します。
C. IPv6 を無効にします。
D. DNS設定を確認してください。
Answer: D (メーッセージを残す**)**
When a user can access the local network (as evidenced by printing to network printers) but not the internet, the issue is often related to Domain Name System (DNS) resolution. DNS is responsible for translating domain names (like google.com) into IP addresses that computers use to communicate. If the DNS settings are incorrect or the DNS server is unreachable, the computer won't be able to find the IP addresses of websites and other internet resources.