Examen de certification CompTIA A+ Objectifs Core 2

NUMÉRO D'EXAMEN : CORE 2 (220-1102)

CompTIA

À propos de l'examen

Les candidats sont encouragés à utiliser ce document pour se préparer à l'examen de certification CompTIA A+ 220-1102. Pour recevoir la certification CompTIA A+, vous devez réussir deux examens : Core 1 (220-1101) et Core 2 (220-1102). Les examens de certification CompTIA A+ Core 1 (220-1101) et Core 2 (220-1102) vérifieront que le candidat retenu possède les connaissances et les compétences requises pour :

- Installer, configurer et entretenir l'équipement informatique, les appareils mobiles et les logiciels pour les utilisateurs finaux
- Assurer l'entretien des composants en fonction des besoins du client
- Comprendre les bases de la mise en réseau et appliquer les méthodes de cybersécurité de base pour atténuer les menaces
- Diagnostiquer, résoudre et documenter de façon appropriée et en toute sécurité les problèmes matériels et logiciels courants
- Appliquer les compétences en matière de dépannage et fournir un support client en utilisant les compétences de communication appropriées
- Comprendre les bases des scripts, des technologies nuage, de la virtualisation et des déploiements multi-OS dans les environnements d'entreprise

Cela équivaut à 12 mois d'expérience pratique dans un rôle de technicien de support technique, de support de bureau ou de technicien de service sur le terrain. Ces exemples de contenu sont destinés à clarifier les objectifs du test et ne doivent pas être interprétés comme une liste exhaustive de tout le contenu de cet examen.

ACCRÉDITATION DE L'EXAMEN

L'examen CompTIA A+ Core 2 (220-1102) est accréditée par ANSI, attestant la conformité avec la norme ISO 17024 et, à cet effet, le soumettant à des révisions et à des mises à jour régulières des objectifs de l'examen.

DÉVELOPPEMENT DE L'EXAMEN

Les examens CompTIA résultent d'ateliers réunissant des spécialistes du domaine et de résultats d'enquêtes effectuées à l'échelle du secteur axées sur les compétences et les connaissances requises d'un professionnel des TI débutant.

RÈGLEMENT DE CompTIA RELATIF À L'UTILISATION DES SUPPORTS AUTORISÉS

CompTIA Certifications, LLC n'est pas affilié et n'autorise pas, ni ne sanctionne, ni ne tolère l'utilisation de tout contenu fourni par des centres de formation tiers non autorisés, également connus sous le nom de « corbeilles à réflexion ». Les individus qui utilisent de tels supports pour préparer tout examen CompTIA verront leur certification révoquée et seront suspendus en vue de futurs tests, conformément au Contrat de participation CompTIA. Pour communiquer plus clairement le règlement des examens CompTIA relatif aux supports d'apprentissage non autorisés, CompTIA dirige tous les candidats à la certification vers Règlement du programme de certification CompTIA. Veuillez consulter tous les règlements CompTIA avant de commencer le processus d'apprentissage en vue d'un examen CompTIA. Les candidats seront tenus de respecter le Contrat de participation entre CompTIA et le candidat. Si un candidat souhaite savoir si les supports d'apprentissage sont considérés comme non autorisés (aussi appelés, « corbeilles à réflexion »), il ou elle doit contacter CompTIA à l'adresse examsecurity@comptia.org pour confirmer.

REMARQUE

Les listes d'exemples fournies sous forme de puces ne sont pas des listes exhaustives. D'autres exemples de technologies, de processus ou de tâches appartenant à chaque objectif peuvent être inclus dans l'examen, alors qu'ils n'étaient pas énumérés ou mentionnés par ce document sur les objectifs. CompTIA révise constamment le contenu de nos examens et met à jour les questions du test pour s'assurer que les examens sont actualisés et que la sécurité des questions est protégée. Le cas échéant, nous publierons des examens mis à jour basés sur des objectifs d'examen existants. Soyez assuré que tous les supports de préparation à l'examen associés seront toujours valides.

DÉTAILS DU TEST

Examen requis	A+ Core 2 (220-1102)
Nombre de questions	Maximum de 90
Types de questions	Choix multiples et basés sur la performance
Durée du test	90 minutes
Expérience recommandée	12 mois d'expérience pratique dans un rôle de technicien de support technique, de technicien de support de bureau ou de technicien de service sur le terrain
Note de passage	700 (sur une échelle de 100 à 900)

OBJECTIFS DE L'EXAMEN (DOMAINES)

Le tableau ci-dessous dresse la liste des domaines évalués dans le cadre de l'examen ainsi que la pondération qu'ils représentent.

DOMAINE		POURCENTAGE D'EXAMEN
1.0	Systèmes d'exploitation	31 %
2.0	Sécurité	25 %
3.0	Dépannage de logiciels	22 %
4.0	Procédures opérationnelles	22 %
Total		**100 %**

NOTE SUR WINDOWS 11

Les versions de Microsoft® Windows® qui ne sont pas à la fin du support général (tel que déterminé par Microsoft), jusqu'à et y compris Windows 11, sont des matières de contenu prévues pour la certification. Ainsi, les objectifs dans lesquels une version spécifique de Microsoft Windows n'est pas indiquée dans le titre de l'objectif principal peuvent inclure du contenu relatif à Windows 10 et Windows 11, dans la mesure où il est lié au rôle de travail.

1.0 Systèmes d'exploitation

1.1 Identifier les fonctionnalités de base des éditions de Microsoft Windows.

- **Éditions Windows 10**
  - Home
  - Pro
  - Pro pour des Postes de travail
  - Enterprise
- **Difficultés de caractéristiques**
  - Accès au domaine vs groupe de travail
  - Styles de bureau/interface utilisateur
  - Disponibilité du protocole de bureau distant (RDP)
  - Limitations de la prise en charge de la mémoire vive (RAM)
  - BitLocker
  - gpedit.msc
- **Chemins de mise à niveau**
  - Mise à niveau sur place

1.2 Dans une situation donnée, utiliser l'outil de ligne de commande Microsoft approprié.

- **Navigation**
  - cd
  - dir
  - md
  - rmdir
  - Entrées de navigation sur disque :
    - C: ou D: ou x:
- **Outils de ligne de commande**
  - ipconfig
  - ping
  - hostname
  - netstat
  - nslookup
  - chkdsk
  - net user
  - net use
  - tracert
  - format
  - xcopy
  - copy
  - robocopy
  - gpupdate
  - gpresult
  - shutdown
  - sfc
  - [command name] /?
  - diskpart
  - pathping
  - winver

1.3 Dans une situation donnée, utiliser les fonctionnalités et les outils du système d'exploitation Microsoft Windows 10 (OS).

- **Gestionnaire des tâches**
  - Services
  - Démarrage
  - Performance
  - Processus
  - Utilisateurs
- **Composant logiciel enfichable sur la Console d'administration Microsoft (MMC)**
  - Event Viewer (eventvwr.msc)
  - Gestion des disques (diskmgmt.msc)
  - Planificateur de tâches (taskschd.msc)
  - Gestionnaire de périphériques (devmgmt.msc)
  - Gestionnaire de certificats (certmgr.msc)
  - Utilisateurs et groupes locaux (lusrmgr.msc)
  - Moniteur de performances (perfmon.msc)
  - Éditeur de stratégie de groupe (gpedit.msc)
- **Outils supplémentaires**
  - Informations système (msinfo32.exe)
  - Moniteur de ressources (resmon.exe)
  - Configuration du système (msconfig.exe)
  - Nettoyage de disque (cleanmgr.exe)
  - Défragmentation de disque (dfrgui.exe)
  - Éditeur du Registre (regedit.exe)

1.4 Dans une situation donnée, utiliser l'utilitaire approprié du Panneau de configuration de Microsoft Windows 10.

- **Options Internet**
- **Périphériques et imprimantes**
- **Programmes et Fonctionnalités**
- **Centre réseau et partage**
- **Système**
- **Pare-feu Windows Defender**
- **Courrier**
- **Audio**
- **Comptes d'utilisateurs**
- **Gestionnaire de périphériques**
- **Options d'indexation**
- **Outils administrateur**
- **Options Explorateur de fichiers**
  - Afficher les fichiers cachés
  - Masquer les extensions
  - Options générales
  - Afficher les options
- **Options d'alimentation**
  - Mise en veille prolongée
  - Modes de gestion de l'alimentation
  - Mettre en veille/éteindre
  - En attente
  - Choisir ce que fait la fermeture du couvercle
  - Activer le démarrage rapide
  - Suspension sélective Bus série universel (USB)
- **Facilité d'accès**

1.5 Dans une situation donnée, utiliser les paramètres Windows appropriés.

- **Heure et langue**
- **Mise à jour et sécurité**
- **Personnalisation**
- **Applications**
- **Confidentialité**
- **Système**
- **Périphériques**
- **Réseau et Internet**
- **Jeux**
- **Comptes**

1.6 Dans une situation donnée, configurer les fonctionnalités réseau de Microsoft Windows sur un client/bureau.

- **Configuration du groupe de travail vs domaine**
  - Ressources partagées
  - Imprimantes
  - Serveurs de fichiers
  - Unités mappées
- **Paramètres de pare-feu du système d'exploitation local**
  - Restrictions d'application et exceptions
  - Configuration
- **Configuration du réseau client**
  - Schéma d'adressage du protocole Internet (IP)
  - Paramètres du système de noms de domaines (DNS)
  - Masque de sous-réseau
  - Passerelle
  - Fixe vs dynamique
- **Installer des connexions réseau**
  - Réseau privé virtuel (VPN)
  - Sans fil
  - Filaire
  - Réseau étendu sans fil (WWAN)
- **Paramètres proxy**
- **Réseau public vs réseau privé**
- **Navigation dans l'explorateur de fichiers – chemins réseau**
- **Connexions mesurées et limites**

1.7 Dans une situation donnée, appliquer les concepts d'installation et de configuration d'application.

- **Configuration système requise pour les applications**
  - Exigences d'application dépendantes de 32 bits par rapport à 64 bits
  - Carte graphique dédiée vs intégrée
  - Exigences en matière de mémoire vidéo à accès aléatoire (VRAM)
  - Exigences en matière de mémoire vive
  - Exigences de l'unité centrale de traitement (CPU)
  - Jetons matériel externe
  - Exigences de stockage
- **Configuration système d'exploitation requise pour les applications**
  - Application à la compatibilité du système d'exploitation
  - Système d'exploitation 32 bits vs 64 bits
- **Procédés de distribution**
  - Support physique vs téléchargeable
  - Montage ISO
- **Autres considérations pour les nouvelles applications**
  - Impact sur l'appareil
  - Impact sur le réseau
  - Impact sur le fonctionnement
  - Impact sur l'entreprise

1.8 Expliquer les types de systèmes d'exploitation courants et leurs objectifs.

- **Systèmes d'exploitation Workstation**
  - Windows
  - Linux
  - macOS
  - Chrome OS
- **Systèmes d'exploitation pour téléphone portable/tablette**
  - iPadOS
  - iOS
  - Android
- **Différents types de systèmes de fichiers**
  - Système de fichiers nouvelle technologie (NTFS)
  - Tableau d'allocation de fichiers 32 (FAT32)
  - Troisième système de fichiers étendu (ext3)
  - Quatrième système de fichiers étendu (ext4)
  - Système de fichiers Apple (APFS)
  - Tableau de distribution de fichiers étendu (exFAT)
- **Limitations du cycle de vie du fournisseur**
  - Fin de vie (EOL)
  - Limites de mise à jour
- **Problèmes de compatibilité entre les systèmes d'exploitation**

1.9 Dans une situation donnée, effectuer des installations et des mises à niveau du système d'exploitation dans un environnement diversifié de système d'exploitation.

- **Procédés de démarrage**
  - USB
  - Support optique
  - Réseau
  - Disques électroniques/flash
  - Basé sur Internet
  - Disque externe/remplaçable à chaud
  - Disque dur interne (partition)
- **Types d'installations**
  - Mise à niveau
  - Partition de restauration
  - Nouvelle installation
  - Déploiement d'une image
  - Installation de réparation
  - Installation du réseau à distance
  - Autres considérations
    - Pilotes tiers
- **Partitionnement**
  - GUID Table de partition GUID (GPT) [identificateur global unique]
  - Enregistrement d'amorçage maître (MBR)
- **Format de disque**
- **Considérations relatives à la mise à niveau**
  - Fichiers de sauvegarde et préférences de l'utilisateur
  - Prise en charge des applications et des pilotes/rétrocompatibilité
  - Compatibilité matérielle
- **Mises à jour des fonctionnalités**
  - Cycle de vie du produit

1.10 Identifier les fonctionnalités et outils communs du système d'exploitation macOS/desktop.

- **Installation et désinstallation d'applications**
  - Types de fichier
    - .dmg
    - .pkg
    - .app
  - App Store
  - Processus de désinstallation
- **Identifiant Apple et restrictions d'entreprise**
- **Meilleures pratiques**
  - Sauvegardes
  - Antivirus
  - Mises à jour/correctifs
- **Préférences de système**
  - Affiches
  - Réseaux
  - Imprimantes
  - Scanners
  - Confidentialité
  - Accessibilité
  - Time Machine
- **Caractéristiques**
  - Plusieurs bureaux
  - Contrôle de mission
  - Chaîne de clé
  - Projecteur
  - iCloud
  - Gestes
  - Localisateur
  - Disque distant
  - Station d'accueil
- **Utilitaire de disque**
- **FileVault**
- **Terminal**
- **Forcer à quitter**

1.11 Identifier les fonctionnalités et les outils communs du système d'exploitation client/bureau Linux.

- **Commandes communes**
  - ls
  - pwd
  - mv
  - cp
  - rm
  - chmod
  - chown
  - su/sudo
  - apt-get
  - yum
  - ip
  - df
  - grep
  - ps
  - man
  - top
  - find
  - dig
  - cat
  - nano
- **Meilleures pratiques**
  - Sauvegardes
  - Antivirus
  - Mises à jour/correctifs
- **Outils**
  - Shell/terminal
  - Samba

2.0 Sécurité

2.1 Résumer les diverses mesures de sécurité et leurs objectifs.

- **Sécurité physique**
  - Vestibule avec contrôle d'accès
  - Lecteur de badges
  - Vidéosurveillance
  - Systèmes d'alarme
  - Détecteurs de mouvement
  - Verrous de porte
  - Verrous d'équipement
  - Gardes
  - Bornes
  - Clôtures
- **Sécurité physique du personnel**
  - Porte-clés
  - Cartes à puce
  - Clés
  - Biométrie
    - Scanner rétinien
    - Lecteur d'empreintes digitales
    - Scanner d'empreintes palmaires
  - Éclairage
  - Magnétomètres
- **Sécurité logique**
  - Principe du moindre privilège
  - Listes des contrôles d'accès (ACL)
  - Authentification multifacteur (MFA)
  - Courriel
  - Jeton d'authentification
  - Jeton logiciel
  - Messagerie texte (SMS)
  - Appel vocal
  - Application d'authentification
- **Gestion des postes mobiles (MDM)**
- **Service d'annuaire**
  - Script de connexion
  - Domaine
  - Stratégie de groupe/mises à jour
  - Unités organisationnelles
  - Dossier de départ
  - Redirection de dossier
  - Groupes de sécurité

2.2 Comparer et évaluer les protocoles de sécurité sans fil et les procédés d'authentification.

- **Protocoles et cryptage**
  - Accès Wi-Fi protégé 2 (WPA2)
  - WPA3
  - Protocole d'intégrité de clé temporelle (TKIP)
  - Norme de chiffrement avancé (AES)
- **Authentification**
  - Service utilisateur d'appel entrant d'authentification distante (RADIUS)
  - Système de contrôle d'accès du contrôleur d'accès au terminal (TACACS+)
  - Kerberos
  - Multifacteur

2.3 Dans une situation donnée, détecter, supprimer et prévenir les logiciels malveillants à l'aide des outils et des procédés appropriés.

- **Logiciel malveillant**
  - Cheval de Troie
  - Outil de dissimulation d'activité
  - Virus
  - Logiciel espion
  - Rançongiciel
  - Enregistreur de frappe
  - Virus du secteur d'amorçage
  - Cryptomineur
- **Outils et procédés**
  - Mode de récupération
  - Antivirus
  - Anti-logiciel malveillant
  - Pare-feux logiciels
  - Formation anti-hameçonnage
  - Formation des utilisateurs sur les menaces courantes
  - Réinstallation du système d'exploitation

2.4 Expliquer les attaques, les menaces et les vulnérabilités courantes d'ingénierie sociale.

- **Ingénierie sociale**
  - Hameçonnage
  - Hameçonnage vocal
  - Espionnage par-dessus l'épaule
  - Harponnage de cadre
  - Talonnage
  - Usurpation d'identité
  - Glanage urbain
  - Jumeau maléfique
- **Menaces**
  - Déni de service distribué (DDoS)
  - Déni de service (DoS)
  - Attaques du jour zéro
  - Mystification
  - Attaque de l'homme du milieu
  - Attaque de force brute
  - Attaque par dictionnaires
  - Menace interne
  - Injection de langage de requête structuré (SQL)
  - Script intersite (XSS)
- **Vulnérabilités**
  - Systèmes non conformes
  - Systèmes non corrigés
  - Systèmes non protégés (antivirus/pare-feu manquants)
  - Fin de vie de systèmes d'exploitation
  - Apporter votre propre appareil (BYOD)

2.5 Dans une situation donnée, gérer et configurer les paramètres de sécurité de base dans le système d'exploitation Microsoft Windows.

- **Defender Antivirus**
  - Activer/désactiver
  - Définitions mises à jour
- **Pare-feu**
  - Activer/désactiver
  - Sécurité des ports
  - Sécurité des applications
- **Utilisateurs et groupes**
  - Compte local vs Microsoft
  - Compte standard
  - Administrateur
  - Utilisateur invité
  - Utilisateur principal
- **Options de connexion au système d'exploitation**
  - Nom d'utilisateur et mot de passe
  - Numéro personnel d'identification (PIN)
  - Empreinte digitale
  - Reconnaissance faciale
  - Authentification unique (SSO)
- **NTFS vs partage des autorisations**
  - Attributs de fichiers et de dossiers
  - Héritage
- **Exécuter en tant qu'administrateur vs utilisateur standard**
  - Contrôle du compte de l'utilisateur (UAC)
- **BitLocker**
- **Bitlocker To Go**
- **Système de chiffrement des fichiers (EFS)**

2.6 Dans une situation donnée, configurer un poste de travail pour respecter les meilleures pratiques en matière de sécurité.

- **Chiffrement des données au repos**
- **Bonnes pratiques en matière de mots de passe**
  - Exigences de complexité
    - Longueur
    - Types de caractères
  - Conditions d'expiration
  - Mots de passe de système de base d'entrée/de sortie (BIOS)/Interface micrologicielle extensible unifiée (UEFI)
- **Meilleures pratiques de l'utilisateur final**
  - Utiliser les verrous d'écran de veille
  - Se déconnecter lorsqu'il n'est pas utilisé
  - Sécuriser/protéger le matériel critique (par exemple, les ordinateurs portables)
  - Sécuriser les informations personnelles identifiables (PII) et les mots de passe
- **Gestion du compte**
  - Restreindre les autorisations des utilisateurs
  - Limiter les temps de connexion
  - Désactiver le compte invité
  - Utiliser le verrouillage après des tentatives infructueuses
  - Utiliser le verrouillage après le délai d'attente/de l'écran
- **Modifier le compte utilisateur/mot de passe de l'administrateur par défaut**
- **Désactiver l'exécution automatique**
- **Désactiver la lecture automatique**

2.7 Expliquer les procédés courants pour sécuriser les appareils mobiles et intégrés.

- **Verrouillages de l'écran**
  - Reconnaissance faciale
  - Codes PIN
  - Empreinte digitale
  - Motif
  - Balayage
- **Nettoyage à distance**
- **Applications de localisation**
- **Mises à jour du système d'exploitation**
- **Chiffrement de l'appareil**
- **Applications de sauvegarde à distance**
- **Restrictions après des tentatives de connexion infructueuses**
- **Antivirus/anti-logiciel malveillant**
- **Pare-feux**
- **Politiques et procédures**
  - BYOD vs détenu par une société
  - Exigences de sécurité du profil
- **Internet des objets (IoT)**

2.8 Dans une situation donnée, utiliser les procédés communs de destruction et d'élimination des données.

- **Destruction physique**
  - Forage
  - Destructeur de données
  - Démagnétisation
  - Incinérations
- **Meilleures pratiques de recyclage ou de réorientation**
  - Effacement/nettoyage
  - Formatage de bas niveau
  - Mise en forme standard
- **Concepts d'externalisation**
  - Fournisseur tiers
  - Certification de destruction/ recyclage

2.9 Dans une situation donnée, configurer les paramètres de sécurité appropriés sur les réseaux filaires et sans fil de l'informatique individuelle et des petites entreprises (SOHO).

- **Paramètres du routeur domestique**
  - Changement des mots de passe par défaut
  - Filtrage IP
  - Mises à jour du micrologiciel
  - Filtrage des contenus
  - Placement physique/ emplacements sécurisés
  - Réservations de protocole de configuration dynamique des hôtes (DHCP)
  - IP statique du réseau étendu (WAN)
  - Plug and Play universel (UPnP)
  - Sous-réseau filtré
- **Spécifique au sans fil**
  - Modification du nom de réseau sans fil (SSID)
  - Désactiver la diffusion SSID
  - Paramètres de cryptage
  - Désactiver le compte invité
  - Changer de chaînes
- **Paramètres du pare-feu**
  - Désactiver les ports inutilisés
  - Transfert/mappage de port

2.10 Dans une situation donnée, installer et configurer les navigateurs et les paramètres de sécurité pertinents.

- **Téléchargement/installation du navigateur**
  - Sources fiables
    - Hachage
  - Sources non fiables
- **Extensions et plug-ins**
  - Sources fiables
  - Sources non fiables
- **Gestionnaires de mots de passe**
- **Connexions/sites sécurisés - certificats valides**
- **Paramètres**
  - Bloqueur de fenêtres contextuelles
  - Effacer les données de navigation
  - Effacer le cache
  - Mode de navigation privée
  - Synchronisation des données de connexion/navigateur
  - Bloqueurs de publicités

3.0 Dépannage de logiciels

3.1 Dans une situation donnée, résoudre les problèmes courants du système d'exploitation Windows.

- **Symptômes courants**
  - Écran bleu de la mort (BSOD)
  - Performances lentes
  - Problèmes de démarrage
  - Arrêts fréquents
  - Les services ne démarrent pas
  - Plantage d'applications
  - Avertissements de mémoire faible
  - Avertissements de contrôleur de ressource USB
  - Instabilité du système
  - Aucun logiciel d'exploitation trouvé
  - Charge de profil lente
  - Dérive temporelle
- **Étapes de dépannage courantes**
  - Redémarrer
  - Redémarrer les services
  - Désinstaller/réinstaller/mettre à jour les applications
  - Ajouter des ressources
  - Vérifier les exigences
  - Vérificateur de fichiers système
  - Réparer Windows
  - Restaurer
  - Réimager
  - Annuler les mises à jour
  - Reconstruire les profils Windows

3.2 Dans une situation donnée, résoudre les problèmes de sécurité courants des ordinateurs personnels (PC).

- **Symptômes courants**
  - Impossible d'accéder au réseau
  - Alertes de bureau
  - Fausses alertes concernant la protection antivirus
  - Système modifié ou fichiers personnels
    - Fichiers manquants/renommés
  - Notifications indésirables dans le système d'exploitation
  - Échecs de la mise à jour du système d'exploitation
- **Symptômes liés au navigateur**
  - Pop-ups aléatoires/fréquents
  - Avertissements de certificat
  - Redirection

3.3 Dans une situation donnée, utiliser les procédures de meilleures pratiques pour la suppression des logiciels malveillants.

1. **Enquêter et vérifier les symptômes des logiciels malveillants**
2. **Mettre en quarantaine les systèmes infectés**
3. **Désactiver la restauration du système pour Windows**
4. **Traiter les systèmes infectés**
   a. Mettre à jour l'anti-logiciel malveillant
   b. Techniques d'analyse et de suppression (par exemple, mode sans échec, environnement de préinstallation)
5. **Programmer des analyses et exécuter des mises à jour**
6. **Activer la restauration du système et créer un point de restauration pour Windows**
7. **Former l'utilisateur final**

3.4 Dans une situation donnée, résoudre les problèmes courants liés au système d'exploitation mobile et aux applications.

- **Symptômes courants**
  - L'application ne se lance pas
  - L'application ne se ferme pas/ se bloque
  - L'application ne se met pas à jour
  - Lent à répondre
  - Le système d'exploitation ne parvient pas à se mettre à jour
  - Problèmes de durée de vie de la batterie
  - Redémarre aléatoirement
  - Problèmes de connectivité
    - Bluetooth
    - WiFi
    - Communication en champ proche (NFC)
    - AirDrop
  - L'écran ne tourne pas automatiquement

3.5 Dans une situation donnée, résoudre les problèmes courants de sécurité des applications et des systèmes d'exploitation mobiles.

- **Problèmes de sécurité**
  - Source du package Android (APK)
  - Mode développeur
  - Accès root/débrider
  - Application bootleg/malveillante
    - Mystification des applications
- **Symptômes courants**
  - Trafic réseau élevé
  - Temps de réponse lent
  - Notification de limite d'utilisation des données
  - Connectivité Internet limitée
  - Pas de connexion Internet
  - Nombre élevé d'annonces
  - Faux avertissements de sécurité
  - Comportement inattendu de l'application
  - Fuite de fichiers personnels/ données

4.0 Procédures opérationnelles

4.1 Dans une situation donnée, mettre en œuvre les meilleures pratiques associées à la documentation et à la gestion des informations des systèmes de support.

- **Systèmes de tickets**
  - Informations de l'utilisateur
  - Informations sur l'appareil
  - Description des problèmes
  - Catégories
  - Gravité
  - Niveaux d'escalade
  - Communication écrite claire et concise
    - Description du problème
    - Notes d'évolution
    - Résolution de problèmes
- **Gestion d'actifs**
  - Listes d'inventaire
  - Système de base de données
  - Étiquettes d'actif et identifiants
  - Cycle de vie d'approvisionnement
  - Garantie et licence
  - Utilisateurs assignés
- **Types de documents**
  - Politique d'utilisation acceptable (AUP)
  - Diagramme de la topologie du réseau
  - Exigences de conformité réglementaire
    - Écrans de démarrage
  - Rapports d'incidents
  - Procédures d'exploitation normalisées
    - Procédures d'installation personnalisée du progiciel
  - Liste de contrôle de configuration pour les nouveaux utilisateurs
  - Liste de contrôle de résiliation de l'utilisateur final
- **Base de connaissances/articles**

4.2 Expliquer les meilleures pratiques de base en matière de gestion du changement.

- **Processus commerciaux documentés**
  - Plan de restauration
  - Test du bac à sable
  - Membre du personnel responsable
- **Gestion du changement**
  - Formulaires de demande
  - Objet du changement
  - Portée du changement
  - Date et heure du changement
  - Systèmes affectés/impact
  - Analyse de risque
    - Niveau du risque
  - Modifier les approbations du conseil
  - Acceptation de l'utilisateur final

4.3 Dans une situation donnée, implémenter des méthodes de sauvegarde et de restauration des postes de travail.

- **Sauvegarde et récupération**
  - Complète
  - Incrémentielle
  - Différentielle
  - Synthétique
- **Test de sauvegarde**
  - Fréquence
- **Schémas de rotation de sauvegarde**
  - Sur site vs hors site
  - Grand-père-Père-Fils (GFS)
  - Règle de sauvegarde 3-2-1

4.4 Dans une situation donnée, utiliser les procédures de sécurité courantes.

- **Sangles de décharge électrostatique (ESD)**
- **Tapis antistatiques**
- **Mise à la terre des équipements**
- **Bonne manipulation des équipes électriques**
- **Manipulation et stockage appropriés des composants**
- **Sacs antistatiques**
- **Respect des réglementations gouvernementales et locales**
- **Sécurité personnelle**
  - Déconnecter l'alimentation avant de réparer l'ordinateur
  - Techniques de levage
  - Sécurité contre les incendies électriques
  - Lunettes de sécurité
  - Masque à filtre à air

4.5 Résumer les impacts environnementaux et les contrôles environnementaux locaux.

- **Fiche de données de sécurité (FDS)/documentation pour la manipulation et l'élimination**
  - Élimination appropriée de la batterie
  - Élimination appropriée du toner
  - Élimination appropriée des autres appareils et actifs
- **Sensibilisation à la température, au niveau d'humidité et aération adéquate**
  - Emplacement/placement des équipements
  - Dépoussiérage
  - Air comprimé/vide
- **Surtensions, événements de sous-tension et pannes de courant**
  - Batterie de secours
  - Parasurtenseur

4.6 Expliquer l'importance des contenus/activités interdits et des concepts de confidentialité, de licence et de politique.

- **Plan de réponse aux incidents**
  - Chaîne de possession
  - Informer la direction/les forces de l'ordre si nécessaire
  - Copie du disque (intégrité et conservation des données)
  - Documentation de l'incident
- **Licence/gestion des droits numériques (DRM)/contrat de licence utilisateur final (CLUF)**
  - Licences valides
  - Licences non expirées
  - Licence d'utilisation personnelle vs licence d'utilisation d'entreprise
  - Licence open source
- **Données réglementées**
  - Transactions par carte de crédit
  - Informations personnelles émises par le gouvernement
  - Informations personnelles identifiables
  - Données de santé
  - Exigences de conservation des données

4.7 Dans une situation donnée, utiliser des techniques de communication appropriées et faire preuve de professionnalisme.

- **Apparence et tenue professionnelles**
  - Accorder la tenue vestimentaire requise à l'environnement donné
    - Formelle
    - Affaires décontractées
- **Utiliser un langage approprié et éviter le jargon, les acronymes et l'argot, le cas échéant**
- **Maintenir une attitude positive/confiance dans le projet**
- **Écouter activement, prendre des notes, et éviter d'interrompre le client**
- **Tenir compte de la dimension culturelle**
  - Utiliser les titres professionnels appropriés, le cas échéant
- **Être ponctuel (en cas de retard, contacter le client)**
- **Éviter toute distraction**
  - Appels personnels
  - Envoyer des messages/se rendre sur des réseaux sociaux
  - Interruptions personnelles
- **Gestion des clients ou situations difficiles**
  - Ne pas se disputer avec les clients et/ou ne pas être sur la défensive
  - Éviter d'ignorer les problèmes du client
  - Éviter de porter un jugement
  - Éclaircir les déclarations du client (poser des questions ouvertes pour réduire l'étendue du problème, reformuler le problème ou poser des questions pour vérifier que vous avez bien compris)
  - Ne pas divulguer les expériences sur les réseaux sociaux
- **Fixer et satisfaire les exigences/échéances et communiquer le statut au client**
  - Proposer des options de réparation/remplacement, au besoin
  - Fournir la documentation appropriée sur les services fournis
  - Assurer le suivi du client/utilisateur ultérieurement pour vérifier qu'il est satisfait
- **Traiter les données confidentielles et privées des clients de façon appropriée**
  - Situées sur un ordinateur, bureau, imprimante, etc.

4.8 Identifier les bases du script.

- **Types de fichiers de script**
  - .bat
  - .ps1
  - .vbs
  - .sh
  - .js
  - .py
- **Cas d'utilisation pour les scripts**
  - Automatisation de base
  - Redémarrage des machines
  - Remappage des lecteurs réseau
  - Installation d'applications
  - Sauvegardes automatisées
  - Collecte d'informations/données
  - Lancement des mises à jour
- **Autres considérations lors de l'utilisation de scripts**
  - Introduire involontairement des logiciels malveillants
  - Modifier par inadvertance des paramètres du système
  - Plantages du navigateur ou du système dus à une mauvaise gestion des ressources

4.9 Dans une situation donnée, utiliser les technologies d'accès à distance.

- **Procédés/outils**
  - RDP
  - VPN
  - Informatique virtuelle en réseau (VNC)
  - Secure Shell (SSH)
  - Surveillance et gestion à distance (RMM)
  - Assistance à distance Microsoft (MSRA)
  - Outils tiers
    - Logiciel de partage d'écran
    - Logiciel de visioconférence
    - Logiciel de transfert de fichiers
    - Logiciel de gestion de bureau
- **Considérations de sécurité de chaque procédé d'accès**

CompTIA A+ Core 2 (220-1102) Liste des acronymes

Voici une liste des acronymes figurant sur l'examen CompTIA A+ Core 2 (220-1102). Les candidats sont encouragés à revoir la liste complète et à apprendre la signification de tous les acronymes énumérés dans le cadre d'un programme complet de préparation à l'examen.

Acronymes	Définition
AAA	Authentification, autorisation et comptabilité
CA	Courant alternatif
ACL	Liste de contrôle d'accès
ADF	Chargeur automatique de documents
AES	Norme de chiffrement avancé
AP	Point d'accès
APFS	Système de fichiers Apple
APIPA	Adressage automatique du protocole IP
APK	Package Android
ARM	Machine avancée RISC [ordinateur à jeu d'instructions réduit]
ARP	Protocole de résolution d'adresse
ATA	Technologie d'attache avancée
ATM	Mode de transfert asynchrone
ATX	Technologie avancée étendue
AUP	Politique d'utilisation acceptable
BIOS	Système de base d'entrée/sortie
BSOD	Écran bleu de la mort
BYOD	Prenez vos appareils personnels
CAPTCHA	Test de Turing public entièrement automatisé pour différencier les ordinateurs des humains
CD	Disque compact
CDFS	Système de fichiers sur disque compact
CDMA	Accès multiple par répartition en code
CERT	Équipe d'intervention d'urgence informatique
CIFS	Système de fichiers Internet commun
CMD	Invite de commande
CMOS	Semi-conducteur à oxyde de métal complémentaire
CPU	Unité centrale de traitement
CRL	Liste de révocation de certificats
CC	Courant continu
DDoS	Déni de service distribué

Acronymes	Définition
DDR	Double débit de données
DHCP	Protocole de configuration dynamique des hôtes
DIMM	Module de mémoire double en ligne
DKIM	Messagerie identifiée par DomainKeys
DMA	Accès direct à la mémoire
DMARC	Authentification, rapport et conformité des messages basés sur le domaine
DNS	Système de noms de domaines
DoS	Déni de service
DRAM	Mémoire vive dynamique
DRM	Gestion des droits numériques
DSL	Ligne d'abonné numérique
DVI	Interface visuelle numérique
DVI-D	Interface visuelle numérique-numérique
ECC	Code de correction d'erreur
EFS	Système de chiffrement des fichiers
EMI	Interférence électromagnétique
EOL	Fin de vie
eSATA	Connexion en série de technologie avancée externe
ESD	Décharge électrostatique
EULA	Contrat de licence utilisateur final (CLUF)
exFAT	Tableau de distribution de fichier étendu
ext	Système de fichiers étendu
FAT	Tableau d'allocation de fichiers
FAT12	Tableau d'allocation de fichiers 12 bits
FAT16	Tableau d'allocation de fichiers 16 bits
FAT32	Tableau d'allocation de fichiers 32 bits
FSB	Bus frontal
FTP	Protocole de transfert de fichiers
GFS	Grand-père-Père-Fils
GPS	Système de positionnement mondial
GPT	Table de partition GUID [identificateur global unique]

Acronymes	Définition
CPU	Unité de traitement graphique
GSM	Système mondial pour les communications mobiles
GUI	Interface utilisateur graphique
GUID	Identificateur global unique
HAL	Couche d'abstraction matérielle
HAV	Virtualisation assistée par matériel
HCL	Liste de compatibilité matérielle
HDCP	Système de protection des contenus numériques haute définition
HDD	Lecteur de disque dur
HDMI	Interface multimédia haute définition
HSM	Module de sécurité matériel
HTML	Langage de balisage hypertexte
HTTP	Protocole de transfert hypertexte
HTTPS	Protocole de transfert hypertexte sécurisé
I/O	Entrée/sortie (E/S)
IaaS	Infrastructure en tant que service
ICR	Reconnaissance intelligente de caractères
IDE	Électronique pour appareil intégré
IDS	Système de détection d'intrusion
IEEE	Institut des ingénieurs électriciens et électroniciens
IMAP	Protocole de messagerie
IOPS	Opérations d'entrée/sortie par seconde
IoT	Internet des objets
IP	Protocole Internet
IPS	Système de Prévention d'intrusion
IPS	Commutation dans le plan
IPSec	Protocole de sécurité Internet
IR	Infrarouge
IrDA	Association de données par infrarouge
IRP	Plan d'intervention en cas d'incidents
ISO	Organisation internationale de normalisation
ISP	Fournisseur d'accès à Internet (FAI)
ITX	Technologie de l'information étendue
BC	Base de connaissances
KVM	Commutateur écran-clavier-souris
LAN	Réseau local
LC	Connecteur Lucent
LCD	Affichage à cristaux liquides
LDAP	Protocole d'accès aux annuaires légers
LED	Diode électroluminescente (DEL)
MAC	Contrôle d'accès multimédia/ Contrôle d'accès obligatoire
MAM	Gestion des applications mobiles

Acronymes	Définition
MAN	Réseau métropolitain
MBR	Enregistrement d'amorçage maître
MDM	Gestion des postes mobiles
MFA	Authentification multifacteur
MFD	Appareil multifonction
MFP	Imprimante multifonction
MMC	Console d'administration Microsoft
MOU	Protocole d'accord
MSDS	Fiche de données de sécurité (FDS)
MSRA	Assistance à distance Microsoft
MX	Mail eXchange
NAC	Contrôleur d'accès réseau
NAT	Traduction d'adresses de réseau
NDA	Accord de non-divulgation
NetBIOS	Système de base d'entrée/sortie mis en réseau
NetBT	NetBIOS sur TCP/IP [Protocole de contrôle de transmission/ Protocole Internet]
NFC	Communication en champ proche
NFS	Système de gestion de fichiers en réseau
NIC	Carte d'interface réseau
NTFS	Système de fichier nouvelles technologies
NVMe	Mémoire non volatile express
ROC	Reconnaissance optique de caractères
LEDO	Diode électroluminescente organique (DELO)
PTO	Point de Terminaison Optique
OS	Système d'exploitation
PaaS	Infrastructure en tant que service
PAN	Réseau personnel
PC	Ordinateur personnel
PCIe	Interconnexion expresse de composants périphériques
PCL	Langage de commande d'imprimante
PE	Environnement de préinstallation
PII	Informations personnellement identifiables
PIN	Numéro personnel d'identification (NIP)
PKI	Infrastructure à clé publique
PoE	Alimentation par Ethernet
POP3	Protocole de messagerie électronique 3
POST	Auto-test de démarrage
PPP	Protocole point-à-point
PRL	Liste d'itinérance préférée
PSU	Bloc d'alimentation
PXE	Environnement d'exécution prédémarrage

Acronymes	Définition
RADIUS	Service utilisateur d'appel entrant d'authentification distante
RAID	Réseau redondant de disques indépendants (ou économiques)
RAM	Mémoire vive
RDP	Protocole bureau distant
RF	Radiofréquence
RFI	Interférence électromagnétique
RFID	Identification par radiofréquence
RJ11	Fonction Jack enregistré 11
RJ45	Fonction Jack enregistré 45
RMM	Surveillance et gestion à distance
RTO	Objectif de temps de restauration
SaaS	Logiciel en tant que service
SAN	Réseau de stockage
SAS	Série attachée SCSI [*Small Computer System Interface*, littéralement en français, Interface de système pour petit ordinateur]
SATA	Connexion en série de technologie avancée
SC	Connecteur abonné
SCADA	Contrôle de supervision et acquisition de données
SCP	Protection contre la copie
SCSI	Interface de petit système d'ordinateur
SDN	Mise en réseau logicielle
SFTP	Protocole de transfert de fichiers
SIM	Module d'identification de l'abonné
SIMM	Module de mémoire à simple rangée de connexions
S.M.A.R.T.	Prévision des défaillances des unités de disque
SMB	Bloc de messages du serveur
SMS	Messagerie texte
SMTP	Protocole de transfert de courrier simple
SNMP	Protocole de gestion de réseau simple
SNTP	Protocole de synchronisation de réseau simple
SODIMM	Module de mémoire à double rangée de connexions
SOHO	Informatique individuelle et des petites entreprises
SPF	Cadre de politique de l'expéditeur
SQL	Langage de requête structuré
SRAM	Mémoire vive statique
SSD	Disque électronique
SSH	Secure Shell
SSID	Nom de réseau sans fil
SSL	Couche de sockets sécurisés
SSO	Signature unique
ST	Bout droit
STP	Paire torsadée blindée
TACACS	Système de contrôle d'accès du contrôleur d'accès au terminal
TCP	Protocole de contrôle de transmission
TCP/IP	Protocole de contrôle de transmission/ Protocole Internet
TFTP	Protocole simplifié de transfert de fichiers
TKIP	Protocole d'intégrité de clé temporelle
TLS	Sécurité de la couche de transport
TN	Nématique en hélice
TPM	Module de plateforme sécurisée
UAC	Contrôle du compte de l'utilisateur
UDP	Protocole de datagramme utilisateur
UEFI	Interface micrologicielle extensible unifiée
UNC	Convention universelle des noms
UPnP	Plug-and-Play universel (Protocole réseau)
UPS	Alimentation sans coupure (ASC)
USB	Bus série universel
UTM	Gestion unifiée des menaces
UTP	Paire torsadée non blindée
VA	Alignement vertical
VDI	Infrastructure de bureau virtuel
VGA	Carte vidéographique
VLAN	LAN (Réseau local) virtuel
VM	Machine virtuelle
VNC	Informatique virtuelle en réseau
VoIP	Voix sur protocole internet
VPN	Réseau privé virtuel
VRAM	Mémoire vidéo à lecture-écriture
WAN	Réseau étendu
WEP	Confidentialité équivalente aux transmissions par fil
WISP	Fournisseur d'accès Internet (FAI) sans fil
WLAN	LAN (Réseau local) sans fil
WMN	Réseau sans fil maillé
WPA	Accès protégé WiFi
WWAN	Réseau étendu sans fil
XSS	Script intersite

CompTIA A+ Core 2 (220-1102)
Liste du matériel et des logiciels proposés

**CompTIA a inclus cet exemple de liste de matériel et de logiciels pour aider les candidats à se préparer à l'examen A+ Core 2 (220-1102). Cette liste peut également s'avérer utile pour les sociétés de formation désireuses de créer un élément laboratoire à leur offre de formation. Les listes à puces sous chaque sujet sont des exemples de listes et ne sont pas exhaustives.

Équipement

- Tablette/smartphone Apple
- Tablette/smartphone Android
- Tablette Windows
- Chromebook
- Ordinateur portable Windows/ ordinateur portable Mac/ ordinateur portable Linux
- Bureau Windows/bureau Mac/ bureau Linux
- Serveur Windows avec Service d'annuaire, Active Directory, et Gestionnaire d'impression, Print Management
- Écrans
- Projecteurs
- Routeur/commutateur SOHO
- Point d'accès
- Téléphone sur Voix sur protocole internet (VoIP)
- Imprimante
  - Laser/jet d'encre
  - Sans fil
  - Imprimante 3D
  - Thermique
- Parasurtenseur
- Alimentation sans coupure (ASC)
- Appareils intelligents (appareils Internet des objets [IoT])
- Serveur avec un hyperviseur
- Bloc de frappe
- Panneau de brassage
- Webcams
- Haut-parleurs
- Microphones

Pièces détachées/matériel

- Cartes mères
- Mémoire vive
- Disques durs
- Blocs d'alimentation
- Cartes graphiques
- Cartes son
- Cartes réseau
- Cartes d'interface réseau sans fil (NIC)
- Ventilateurs/dispositifs de refroidissement/dissipateur thermique
- Unités centrales
- Connecteurs et câbles assortis
  - USB
  - Interface multimédia haute définition (HDMI)
  - Port d'affichage
  - Interface visuelle numérique (DVI)
  - Carte vidéographique (VGA)
- Adaptateurs
  - Adaptateur Bluetooth
- Câbles réseau
- Câbles réseau ou connecteurs sans terminaison
- Adaptateurs de courant alternatif (CA)
- Lecteurs optiques
- Vis/douilles-entretoises
- Boîtiers
- Kit de maintenance
- Souris/claviers
- Commutateur écran-clavier-souris (KVM)
- Câble console
- Disque électronique (SSD)

Outils

- Tournevis
- Multimètre
- Coupe-fils
- Pince d'insertion Krone
- Pince à sertir
- Testeur d'alimentation électrique
- Pince à dénuder
- Boîte à outils standard du technicien
- Sangle de décharge électrostatique (ESD)
- Pâte thermique
- Testeur de câble
- Câble de toner
- Analyseur WiFi
- Connexion en série de technologie avancée (SATA) des connecteurs USB

Logiciel

- Systèmes d'exploitation
  - Linux
  - Chrome OS
  - Microsoft Windows
  - macOS
  - Android
  - iOS
- Disque compact (CD) vivant/ autonome de l'environnement de préinstallation (PE)
- Logiciel antivirus
- Logiciel de virtualisation
- Anti-logiciel malveillant
- Logiciels de pilotes

CompTIA