

Corrigé attaché d'État 2018 : Windows Server

Proposition de corrigé — non officielle. Ministère de la Culture, concours réservé 2018, épreuve du 30 octobre. Les trois modules et leurs dix questions sont traités dans le contexte de la session.

[Sujet officiel](#) · [Annales de ce concours ou examen](#)

Étude de cas — 95 postes sur trois sites

1. Collecter l'état des correctifs

WSUS, Windows Server Update Services, est le rôle serveur adapté à la centralisation des mises à jour Microsoft et au suivi des clients. On installe le rôle et sa base, prévoit l'espace de stockage et le proxy éventuel, choisit les produits effectivement présents — ici Windows 7 et Windows 10 — ainsi que langues et classifications utiles, puis configure la synchronisation depuis Microsoft Update.

Les postes sont orientés vers le serveur par une stratégie de groupe : emplacement du service de mise à jour intranet et paramètres de mise à jour automatique. Les URL et ports doivent correspondre à la configuration effective du serveur ; les installations utilisant les ports par défaut emploient notamment 8530 ou 8531 selon la configuration HTTP/HTTPS. Les groupes d'ordinateurs distinguent au minimum un pilote et le reste du parc ; on teste puis approuve les correctifs avant déploiement élargi.

Les 60, 22 et 13 postes doivent tous être inventoriés et communiquer avec WSUS. Pour les antennes, on vérifie connectivité, bande passante et horaires ; un serveur relais local peut se justifier, mais n'est pas automatiquement nécessaire pour ces petits effectifs. Les politiques de redémarrage et la récupération après échec sont préparées. Les commandes PowerShell d'inventaire des correctifs complètent le diagnostic ponctuel, sans remplacer la remontée centralisée.

2. Tableaux de bord et types de mise à jour

La console et les rapports WSUS permettent de restituer les mises à jour nécessaires, installées, en échec ou dont l'état n'est pas connu, par ordinateur et par groupe. Un tableau par site indique le nombre de clients attendus, remontés récemment, conformes et nécessitant une action. **Un poste silencieux ne compte pas comme corrigé.** On examine aussi date du dernier contact, correctifs critiques manquants et redémarrages en attente.

Les classifications distinguent notamment mises à jour de sécurité, critiques, mises à jour ordinaires, ensembles de mises à jour, Service Packs lorsqu'ils existent pour le produit, définitions de sécurité, pilotes et mises à niveau. Elles n'ont pas toutes le même risque ni le même circuit de validation. Une mise à niveau fonctionnelle de Windows 10 ne se confond pas avec l'application d'un correctif de sécurité. Les résultats doivent distinguer les deux versions de Windows et ne pas prétendre que chaque machine reçoit tous les paquets.

3. Télédistribution par GPO

On place les paquets, généralement **MSI**, sur un partage accessible en lecture aux bénéficiaires, avec un chemin UNC. Une GPO est liée au site, domaine ou à l'unité d'organisation appropriée, avec des filtres et permissions maîtrisés.

Dans une **stratégie utilisateur**, une application peut être attribuée ou publiée. L'attribution prépare sa disponibilité à l'ouverture de session et son installation selon les options et l'usage ; la publication permet à l'utilisateur de choisir l'installation par le mécanisme prévu. Dans une **stratégie ordinateur**, le paquet est attribué à la machine et s'installe au démarrage selon la politique : il est disponible pour les utilisateurs de ce poste. L'ordinateur doit pouvoir accéder au partage avec ses propres droits.

Un exécutable quelconque ne devient pas automatiquement un MSI géré. On vérifie format, paramètres, dépendances, droits, déploiement pilote, mises à jour et désinstallation. La GPO détermine le périmètre ; elle ne dispense pas de tester le logiciel.

4. Alternatives libres

Dans le paysage de 2018, **GLPI associé à FusionInventory** peut réunir inventaire, remontée d'informations et télédistribution ; **OCS Inventory NG** fournit également inventaire et déploiement de paquets. Ces outils donnent un inventaire hétérogène et des fonctions au-delà des seuls correctifs Microsoft. Ils nécessitent toutefois agents, serveurs, maintenance, sécurisation et définition précise des paquets ; leur télédistribution ne reproduit pas automatiquement les classifications et approbations de WSUS.

On peut combiner WSUS pour les correctifs Microsoft et un outil libre pour l'inventaire ou les logiciels tiers. Le choix dépend des systèmes couverts, de l'effort d'exploitation et de la qualité des rapports, plutôt que du seul caractère gratuit. Les modules d'inventaire apparus dans des versions ultérieures ne doivent pas être attribués rétroactivement à GLPI 2018.

Connaissances générales

1. RGPD

Le règlement européen 2016/679 est applicable depuis **le 25 mai 2018**. Il encadre les traitements de données personnelles : finalité, base juridique, minimisation, exactitude, durée de conservation et sécurité. Il renforce les droits des personnes et la responsabilité démontrable des organismes. Le consentement n'est pas la seule base possible ; une mission publique ou une obligation légale peuvent être pertinentes selon le traitement.

Un service doit identifier ses traitements, informer les personnes, organiser les droits, encadrer les sous-traitants et adapter les mesures de sécurité. Une autorité ou un organisme public relève de l'obligation de désignation d'un délégué à la protection des données dans le champ prévu. Inventaire et journaux d'incidents peuvent contenir des données personnelles : l'utilité technique ne dispense pas de contrôler accès et conservation.

2. Suivre les incidents de sécurité

Un **SIEM** centralise et corrèle journaux et alertes. Journaux Windows, collecte d'événements, syslog, IDS et outils de supervision fournissent les observations ; un système de tickets trace qualification, responsable, actions et résolution. Il faut synchroniser les horloges, protéger les traces, limiter les accès et organiser la conservation.

Les règles de détection doivent être ajustées et les alertes traitées : collecter sans analyste ni procédure ne constitue pas une réponse à incident. Un tableau utile indique criticité, périmètre, statut et délai de prise en charge, sans publier les informations sensibles à tous les utilisateurs.

Windows Server et Active Directory

1. Contenu d'une forêt

Une forêt AD comprend un ou plusieurs domaines, éventuellement organisés en arbres, partageant notamment schéma, configuration et catalogue global. Chaque domaine contient des objets — utilisateurs, groupes, ordinateurs — organisés en unités d'organisation ; les contrôleurs de domaine portent l'annuaire et répliquent les données selon les règles prévues. Sites et sous-réseaux décrivent la topologie physique. Des relations d'approbation permettent les échanges entre domaines ; la forêt constitue une limite majeure d'isolation de sécurité.

2. Authentification

Kerberos est le protocole principal d'authentification dans un domaine AD. Le poste localise un contrôleur de domaine, notamment grâce au DNS. Le client demande au service d'authentification du KDC un **TGT** après preuve de son identité ; ce ticket sert ensuite à obtenir un ticket pour un service déterminé auprès du service d'octroi de tickets. Le client présente ce dernier au serveur cible, qui le vérifie avec les éléments cryptographiques appropriés. Le mot de passe n'est pas envoyé à chaque service.

Horloge, DNS, comptes et noms de service doivent être cohérents. NTLM peut subsister comme mécanisme de repli dans certains cas ; LDAP sert aux accès à l'annuaire et ne résume pas à lui seul cette chaîne d'authentification. Une identité authentifiée doit encore être autorisée à utiliser la ressource.

3. Description des ressources

Dans l'annuaire, une ressource est représentée par un **objet d'une classe définie par le schéma**, avec des attributs, un nom distinctif et des identifiants. L'objet ordinateur décrit son rattachement et son compte ; une imprimante peut être publiée avec ses propriétés pour faciliter sa découverte. Ces objets ne constituent pas un inventaire exhaustif de chaque composant matériel.

Pour la configuration physique — processeur, mémoire, disques — Windows fournit aussi des interfaces d'inventaire comme WMI/CIM et les informations des pilotes. On distingue donc description et publication dans AD, inventaire matériel et droit effectif d'usage.

4. Autoriser l'usage

On place les utilisateurs dans des groupes puis attribue à ces groupes les droits nécessaires. Pour une imprimante, les permissions **Imprimer**, gérer l'imprimante et gérer les documents ont des effets distincts. Pour un partage de fichiers, les permissions du partage et celles du système de fichiers se combinent ; on ne donne pas systématiquement le contrôle total.

Pour l'ouverture de session sur un ordinateur, comptes, groupes locaux et droits de connexion applicables — éventuellement distribués par GPO — doivent être vérifiés. Lire l'objet ordinateur dans AD ne donne pas, à lui seul, le droit de s'y connecter. On applique le moindre privilège, teste avec un utilisateur représentatif et conserve une procédure de retrait des accès.

Références

[Configuration de WSUS](#), [installation de logiciels par GPO](#), [authentification Kerberos](#), [CNIL](#), [entrée en application du RGPD](#), [archives des versions FusionInventory](#).