Classe BTS SIO SISR 1A

Dossier n°3 : La mise à disposition des nouveaux équipements aux utilisateurs

Sommaire

Les Outils de déploiement

SCCM

System Center Configuration Manager, est un produit de la famille System Center, proposée par Microsoft.

Fonctionnalité de SCCM :

- Mise en place d'un portail self-service pour la distribution d'applications auprès de vos utilisateurs
- Distribution d'applications avec rapport sur l'utilisation des applications
- Distribution de configurations (Wi-Fi, VPN, profils messagerie, etc.)
- Gestion centralisée des appareils, que ce soit des postes de travail (Windows, Mac ou Linux), des serveurs ainsi que des appareils mobiles (Windows, iOS, Android)
- Protection antivirus « System Center Endpoint Protection »
- Gestion et déploiement des mises à jour et correctifs (principe de WSUS)
- Déploiement d'image par le réseau
- Inventaire du parc informatique (ainsi que l'activité des clients et un rapport de santé)
- Intégration à Windows Intune et le Cloud Azure
- Contrôle à distance (via la fonctionnalité « Assistance à distance » native de Windows)

Tarif :

System Center 2022 Editions		
	Datacenter	**Standard**
OSEs / Hyper-V Containers	**Unlimited**	**2**
Windows Server Containers	**Unlimited**	**Unlimited**
Configuration Manager	•	•
Data Protection Manager	•	•
Endpoint Manager	•	•
Operations Manager	•	•
Orchestrator	•	•
Service Manager	•	•
Virtual Machine Manager	•	•
Price*	$3,607	$1,323

WDS et MDT

WDS :

WDS est un rôle disponible sur Windows Serveur. Il remplace RIS depuis Windows Server 2008 SP2 et permet le déploiement de Windows Vista à Windows 10 et des versions serveurs depuis 2008.

MDT :

MDT est un logiciel distribué gratuitement par Microsoft qui permet déployer Windows de façon personnalisé à l'aide de séquences de tâche.

Il doit être utilisé en complément avec WDS car le logiciel n'inclus pas de service TFTP pour pouvoir démarrer en PXE .

Fonctionnalité de MDT :

- Nom de l'ordinateur.
- Jonction au domaine.
- Installation d'applications sélectionnées ou en mode transparent configuré dans une séquence.
- Exécution de scripts (Vbs, CMS, PowerShell)
- Sauvegarde / Restauration des profils
- Activation de BitLocker
- Installation des pilotes

Tarif : Gratuit

Comparaison et choix de l'outil

MDT est un outil léger, flexible et gratuit. Il est parfaitement capable de déployer des systèmes d'exploitation sur 200 PC.
D'un autre côté, SCCM offre plus de fonctionnalités et est plus robuste. Il est conçu pour gérer des déploiements à grande échelle et offre des capacités de reporting avancées. Cependant, il est plus complexe et coûteux que MDT.
Finalement pour répondre à notre besoin de déployer l'os sur 230 machines **MDT** suffit, il est gratuit et simple à mettre en place.

Pratique à respecter pour assurer la sécurité de votre équipement

Bonjour ,

Avant de vous remettre l'équipement, vous devez prendre connaissances de quelques pratiques à respecter pour assurer une sécurité de ce nouveau matériel :

1. **Protégez vos accès avec des mots de passe solides**

(minimum 12 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux)

2. **Sauvegardez vos données régulièrement**

3. **Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones…), et ce, dès qu'elles vous sont proposées**

4. **Utilisez un antivirus**

5. **Téléchargez vos applications uniquement sur les sites officiels**

6. **Méfiez-vous des messages inattendus**

(En cas de réception d'un message inattendu ou alarmiste par messagerie (email), SMS ou chat, demandez toujours confirmation à l'émetteur par un autre moyen s'il vous semble connu et légitime. Il peut en effet s'agir d'une attaque par hameçonnage (phishing) visant à vous piéger pour vous dérober des informations confidentielles (mots de passe, informations d'identité ou bancaires), de l'envoi d'un virus contenu dans une pièce-jointe qu'on vous incite à ouvrir, ou d'un lien qui vous attirerait sur un site malveillant.)

7. **Séparez vos usages personnels et professionnels**

8. **Évitez les réseaux WiFi publics ou inconnus**

(En mobilité, privilégiez la connexion de votre abonnement téléphonique (3G ou 4G) aux réseaux WiFi publics. Ces réseaux WiFi sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer vos informations personnelles ou confidentielles)