Mise en place d’un serveur Kaspersky

FOUR Lucas
Conseil départemental de la Drôme

Table des matières

Cahier des charges – Expression des besoins

| Descriptif de l'existant |

L'infrastructure de départ étant inexistante, je ne dispose d'aucun service réseau préconfiguré. Mon environnement se limite à un accès à Internet via le réseau local (LAN) du GRETA, qui me permet de télécharger les ressources nécessaires à la mise en place du projet.

| Besoin(s) |

Ce travail pratique a pour objectif de déployer une solution de sécurité centralisée permettant de protéger les postes et le réseau contre les menaces informatiques (virus, malwares, intrusions). L'infrastructure doit offrir une gestion centralisée de la sécurité afin de faciliter l'administration, le déploiement des politiques de protection et la détection des menaces à distance sur l'ensemble des postes clients.

| Contrainte(s) |

La réalisation de ce travail pratique est soumise aux contraintes suivantes :

- **Contrainte de temps** : l'ensemble de l'infrastructure doit être déployé en huit heures.
- **Contrainte logicielle** : la solution de sécurité retenue est Kaspersky, avec un serveur d'administration et un agent client.
- **Contrainte système** : l'architecture repose sur deux machines virtuelles — un serveur sous Windows Server assurant le rôle de serveur de sécurité, et un poste client sous Windows 11 sur lequel l'agent Kaspersky sera déployé.
- **Contrainte réseau** : la communication entre le serveur et le poste client doit être fonctionnelle pour permettre la gestion à distance.
- **Contrainte de validation** : le TP sera validé sur la bonne communication serveur/client, l'application correcte des politiques de sécurité et la détection effective des menaces.

Ressources

| Ressources mises à disposition |

Pour la réalisation de ce travail pratique, je dispose d'une machine hôte équipée de l'hyperviseur Hyper-V, utilisé comme solution de virtualisation pour déployer les différentes machines nécessaires à l'infrastructure de sécurité.
De plus, cette machine est connectée au réseau local (LAN) du GRETA, ce qui me permet de bénéficier d'un accès à Internet indispensable au téléchargement des solutions Kaspersky, des mises à jour de sécurité, ainsi qu'à la communication avec les serveurs de mise à jour et d'activation.

| Ressources nécessaires à la mise en place |

Pour la mise en œuvre de ce travail pratique, plusieurs éléments matériels et logiciels sont nécessaires :

- Une machine hôte équipée d'un logiciel de virtualisation (dans ce cas, Hyper-V) afin de créer et gérer les différentes machines virtuelles ;
- Un accès à Internet, indispensable pour le téléchargement des ressources et la mise à jour des paquets ;
- Les images ISO des systèmes d'exploitation Windows Server et Windows 11
- Les fichiers d'installation de la solution Kaspersky (serveur d'administration et agent de sécurité) nécessaires au déploiement et à la protection des machines.

| Gestion des ressources |

Le temps imparti pour ce travail pratique étant limité à huit heures, et celui-ci incluant l'installation complète du serveur Windows Server ainsi que du poste client Windows 11, j'ai préalablement téléchargé les images ISO correspondantes ainsi que les fichiers nécessaires à l'installation de la solution Kaspersky.
Cette préparation en amont permet de gagner du temps lors de la mise en place des machines virtuelles et d'optimiser le déroulement du TP, notamment pour l'installation, la configuration et le déploiement de la solution de sécurité Kaspersky sur le serveur et le poste client.

Analyse

Solutions	Kaspersky Security Center	Microsoft Defender for Endpoint
Coûts	Payant (licence Kaspersky)	Inclus dans certaines licences Microsoft (Microsoft 365 / Azure)
OS d'installation	Windows Server / Linux	Cloud (Azure) + Windows / Linux / macOS
Points forts	Gestion centralisée, déploiement automatique, inventaire réseau, très complet	Intégré à l'écosystème Microsoft, protection avancée (EDR), analyse en temps réel
Interface / utilisation	Interface centralisée (console + web), assez intuitive	Interface web moderne (Microsoft 365 Defender), plus complexe
Mise en place	Installation locale (on-premise), nécessite serveur	Déploiement plus rapide via le cloud
Communauté / Support	Support éditeur + documentation riche	Très grande communauté Microsoft + documentation massive
Idéal pour	PME, entreprises avec infrastructure locale, labs pédagogiques	Entreprises utilisant Microsoft 365 / cloud / grandes infrastructures
Limites	Solution payante, nécessite gestion serveur	Complexité, dépendance au cloud Microsoft

| Choix d'une solution – Argumentation |

J'ai choisi d'utiliser la solution Kaspersky Security Center, car elle offre une solution fiable et centralisée pour la gestion de la sécurité des postes informatiques. En permettant le déploiement des agents de protection, la gestion des politiques de sécurité et la supervision des menaces (virus, malwares, intrusions), Kaspersky simplifie l'administration du parc informatique et réduit les risques liés aux cyberattaques. Cette approche est particulièrement adaptée à un environnement professionnel, où la sécurité, la supervision centralisée et la réactivité face aux menaces sont essentielles pour garantir l'intégrité des systèmes et des données.

| Plan d'adressage réseau |

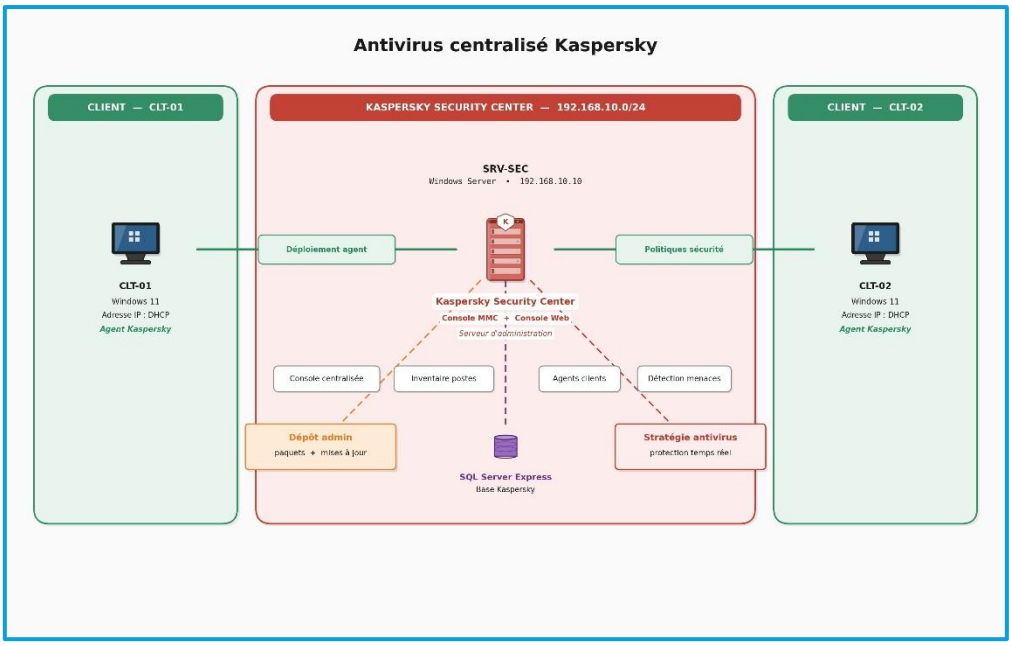
Tableau d'adressage :

Nom du réseau	Adresse réseau	Masque de sous réseau	Première adresse	Dernière adresse	Adresse de broadcast
LAN	192.168.10.10	255.255.555.0	X	X	X
WAN	DHCP	DHCP	DHCP	DHCP	DHCP

Tableau des adresses IP :

Machines	Adresses IP	Masque de sous réseau	Passerelle par défaut	DNS
SRV-SEC	192.168.10.10	255.255.255.0	X	192.168.10.10
CLT-01	DHCP	DHCP	DHCP	DHCP
CLT-02	DHCP	DHCP	DHCP	DHCP

Schéma réseau :



| Etude de l'impact sur le SI existant |

Étant donné que ce travail s'inscrit dans un contexte de formation, il n'existe aucun système d'information (SI) préexistant, mis à part l'accès à Internet. L'ensemble de l'infrastructure nécessaire au déploiement de la solution Kaspersky doit donc être créé et configuré intégralement dans le cadre de ce TP.
La mise en place d'une solution de sécurité comme Kaspersky dans mon entreprise permettrait de centraliser la gestion de la protection des postes, de renforcer la sécurité du système d'information et de réduire les risques liés aux cybermenaces. Elle facilite également le déploiement des agents de sécurité, la supervision des équipements et l'application de politiques de sécurité cohérentes sur l'ensemble du parc informatique.

| Phasage de l'intervention |

Dans un premier temps, je préparerai deux machines : un serveur sous Windows Server et une machine cliente sous Windows 11.
Sur le serveur Windows Server, j'installerai Kaspersky Security Center afin de permettre la gestion centralisée de la sécurité du réseau. Cette installation comprendra la configuration du serveur d'administration ainsi que des différents composants nécessaires au déploiement de la solution.
Après l'installation, je configurerai les paramètres principaux, notamment la création des groupes d'administration, la mise en place des politiques de sécurité et la préparation du déploiement des agents Kaspersky.
Ensuite, sur la machine cliente Windows 11, j'installerai l'agent Kaspersky afin qu'elle puisse être administrée à distance par le serveur.
Une fois ces étapes réalisées, je vérifierai la bonne communication entre le serveur et le poste client, ainsi que l'application des politiques de sécurité.
Pour terminer, je testerai le bon fonctionnement de la solution en simulant des analyses ou des détections afin de m'assurer que la protection est correctement active sur le poste client.

| Prévision des tests et validation |

Lors de l'installation de la solution Kaspersky, je procéderai à plusieurs vérifications afin de m'assurer de son bon fonctionnement. Je vérifierai notamment que le serveur d'administration Kaspersky est bien opérationnel et que les services associés sont correctement démarrés.
Par la suite, après la configuration des politiques de sécurité et des groupes d'administration, je contrôlerai que les paramètres définis (analyse antivirus, mises à jour, protection en temps réel) sont bien appliqués.
Ensuite, après le déploiement de l'agent Kaspersky sur la machine cliente, je vérifierai que celle-ci remonte correctement dans la console d'administration et qu'elle est bien gérée par le serveur.
Enfin, une fois la configuration terminée, je testerai le bon fonctionnement de la solution en lançant une analyse ou en simulant une détection afin de m'assurer que la protection est active.
Je vérifierai également que les remontées d'événements et les alertes fonctionnent correctement entre le client et le serveur. Cela permettra de valider entièrement la mise en place de la solution Kaspersky.

Mise en place

1 - Installation de Kaspersky :

| Etape 1 : Installation de la base de données |

Avant de déployer l'antivirus, l'installation de **Microsoft SQL Server Express** était indispensable. En effet, Kaspersky Security Center s'appuie sur une base SQL pour centraliser la gestion du parc : inventaire des machines, événements de sécurité, rapports d'analyse et stratégies d'administration. L'édition **Express** a été privilégiée car elle offre une solution gratuite et légère, parfaitement adaptée à une infrastructure de petite taille. L'opération a permis de créer l'instance **SQLEXPRESS**, qui hébergera localement toutes les données du serveur de sécurité.

| Etape 2 : Lancement de l'installation |

L'installation du serveur antivirus a été lancée à partir du programme d'installation fourni avec la solution. L'assistant d'installation guide l'utilisateur à travers les différentes étapes nécessaires à la configuration du serveur d'administration. Le choix d'installer Kaspersky Security Center sur le serveur **SRV-SEC** permet de centraliser la gestion de la sécurité informatique dans l'infrastructure mise en place pour ce TP.

| Etape 3 : Choix du type d'installation |

Lors de l'installation, l'option **installation locale** a été sélectionnée. Cette option permet d'installer tous les composants nécessaires directement sur le serveur. Ce choix est adapté à l'infrastructure de test car il permet de centraliser la gestion de la sécurité sur une seule machine. Dans un environnement professionnel plus important, il serait possible de répartir certains composants sur plusieurs serveurs afin d'améliorer les performances et la disponibilité du service.

| Etape 4 : Choix des interfaces d'administration |

L'installation propose deux interfaces d'administration : la **console MMC** et la **console Web**. La console MMC (Microsoft Management Console) est l'interface d'administration principale dans les environnements Windows. Elle permet de gérer les machines administrées, de configurer les stratégies de sécurité, de déployer les agents antivirus et de consulter les rapports. La console Web permet quant à elle d'accéder à l'administration du serveur à distance via un navigateur Internet. Dans ce TP, les deux interfaces ont été installées afin de disposer de plusieurs méthodes d'administration du serveur antivirus.

| Etape 5 : Configuration de la base de données |

Lors de la configuration de la base de données, l'instance SQL **SQLEXPRESS** installée précédemment a été utilisée. Le serveur de base de données correspond au serveur local, identifié par l'adresse : **.\SQLEXPRESS**. L'authentification Windows a été sélectionnée afin d'utiliser les comptes du système d'exploitation pour accéder à la base de données. Cette méthode permet une meilleure intégration avec l'environnement Windows et simplifie la gestion des comptes. Le nom de la base de données proposé par défaut a été conservé.

| Etape 6 : Création du certificat de sécurité |

Pendant l'installation, un certificat de sécurité a été généré automatiquement. Ce certificat permet d'authentifier le serveur d'administration et de sécuriser les communications entre le serveur Kaspersky et les agents installés sur les machines clientes. Dans le cadre de cette infrastructure de test, un certificat auto-signé est suffisant. Dans un environnement professionnel, il serait possible d'utiliser une autorité de certification interne afin de gérer les certificats de manière centralisée.

| Etape 7 : Configuration du gestionnaire des identités |

Lors de la configuration du gestionnaire des identités, l'authentification Windows a été utilisée. Ce choix permet d'utiliser les comptes existants du système et de s'intégrer avec l'infrastructure Active Directory déjà mise en place. Cette méthode simplifie l'administration et permet de gérer les droits d'accès à la console d'administration à l'aide des comptes du domaine.

| Etape 8 : Création du dépôt d'administration |

L'installation de Kaspersky Security Center crée également un dépôt d'administration sur le serveur. Ce dépôt permet de stocker les packages d'installation des agents antivirus ainsi que les mises à jour de sécurité. Les machines clientes pourront télécharger ces composants directement depuis le serveur, ce qui permet de centraliser la distribution des logiciels et de réduire le trafic Internet.

| Etape 9 : Fin de l'installation |

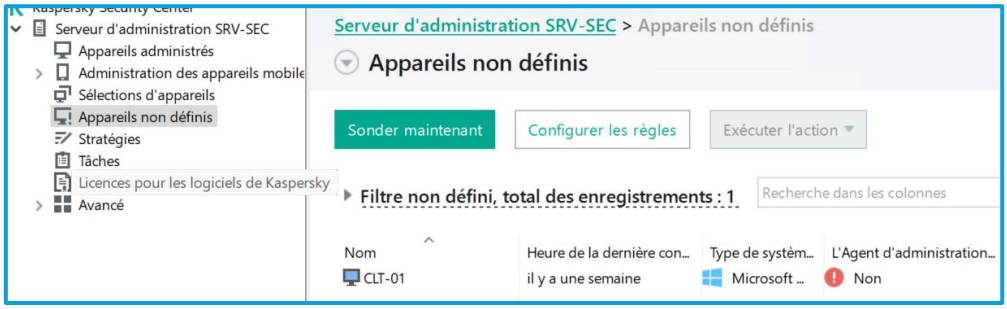
Une fois l'installation terminée, la console d'administration de Kaspersky Security Center s'ouvre automatiquement. Cette console permet à l'administrateur système de gérer les machines du réseau, de déployer les agents antivirus et de surveiller l'état de sécurité du parc informatique. Le serveur est alors prêt à être utilisé pour mettre en place la protection antivirus sur les machines clientes.

2 - Déploiement de l'agent sur une machine du domaine :

| Etape 1 : Accès et Détection |

Lancez la console Kaspersky Security Center sur le serveur. Pour trouver votre machine, rendez-vous dans Périphériques non-administrés > Appareils détectés.

- *Note :* Si le poste est absent, lancez une recherche via le réseau ou synchronisez avec l'Active Directory.

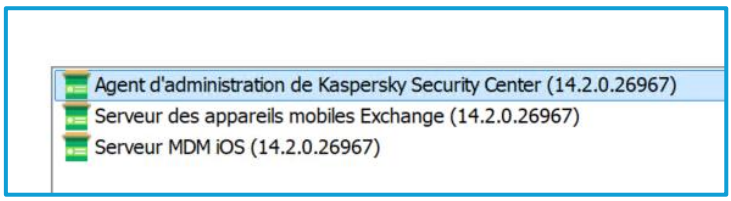


| Etape 2 : Création de la tâche |

Allez dans l'onglet Tâches, créez une Nouvelle tâche et choisissez le type Installation distante d'une application. Suivez l'assistant pour sélectionner votre machine cible précédemment détectée.

| Etape 3 : Sélection du Paquet et identifiants |

Choisissez uniquement le paquet Agent d'administration Kaspersky (Network Agent). Pour l'installation, renseignez les identifiants d'un compte administrateur du domaine (ex: DOMAINE\Administrateur) afin d'autoriser l'accès distant au poste client.



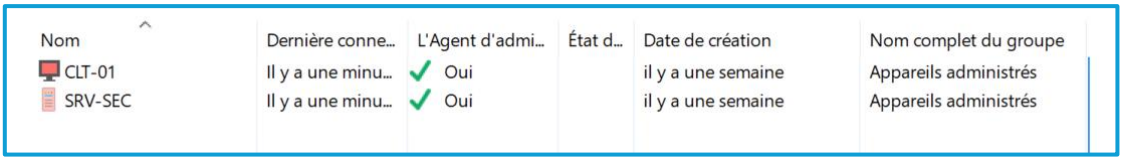
| Etape 4 : Paramétrage et Lancement |

Configurez les options (installation automatique, redémarrage si besoin) et déplacez la machine vers le groupe final (ex: "Postes domaine"). Terminez l'assistant et lancez la tâche immédiatement.

| Etape 4 : Suivi et Vérification |

Surveillez l'état dans l'onglet Statut de la tâche jusqu'à obtenir la mention Succès.

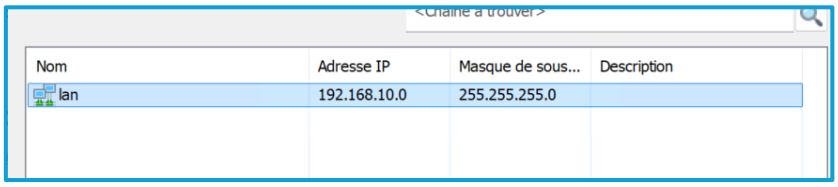
- Validation : Le poste doit apparaître dans les Appareils administrés sur la console et l'agent doit être visible dans les programmes installés sur le PC client

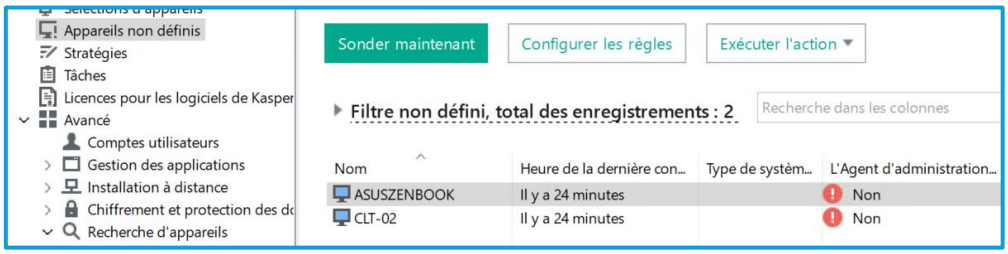


3 – Déploiement de l'agent sur une machine hors du domaine :

| Etape 1 : Configuration |

Pour faire un déploiement de l'agent sur une machine hors domaine il faut créer une plage IP puis sonder pour que l'ordinateur qui n'est pas dans le domaine remonte dans « appareils non définis »





| Etape 2 : Validation du Succès |

Côté Client : Vérifiez que le "Kaspersky Network Agent" apparaît bien dans la liste des programmes installés.

- **Côté Console :** La machine doit maintenant remonter automatiquement dans le groupe **Appareils administrés**. Vérifiez que l'icône est colorée (indiquant qu'elle est connectée et administrée).

4 – Automatisation par GPO :

| Etape 1 : Préparation du Partage Réseau |

Créez un dossier partagé (ex: \\SERVEUR\Deploiement) accessible en **lecture** pour les groupes **"Utilisateurs authentifiés"** et **"Domain Computers"**. **Impératif :** Seul le format **.msi** est compatible avec les GPO. Exportez-le depuis Kaspersky Security Center et copiez-le dans ce dossier.

| Etape 2 : Création et Liaison de la GPO |

Ouvrez la console **GPMC** et créez un nouvel objet GPO nommé *"Déploiement Agent Kaspersky"*.

- Liez cet objet à l'**Unité d'Organisation (OU)** contenant les ordinateurs cibles.
- Vérifiez que vos postes de test sont bien déplacés dans cette OU avant de continuer.

| Etape 3 : Configuration logicielle |

Faites un clic droit sur la GPO > **Modifier**. Naviguez dans : Configuration ordinateur ➔ Politiques ➔ Paramètres logiciels ➔ Installation de logiciel.

- **Nouveau > Paquet :** Sélectionnez votre fichier via son **chemin UNC** (ex: \\SERVEUR\Deploiement\agent.msi).
- **Méthode :** Choisissez impérativement **Attribué (Assigned)** pour une installation automatique.

| Etape 4 : Application sur les postes |

L'installation se déclenche au **redémarrage** de l'ordinateur client, avant l'ouverture de session.

- Pour accélérer le test sur un poste, lancez la commande gpupdate /force puis redémarrez.
- Le message *"Installation du logiciel en cours..."* confirmera le bon fonctionnement de la stratégie.

| Etape 5 : Validation finale |

Côté Client : Vérifiez la présence de "Kaspersky Network Agent" dans les programmes installés.

Côté Console KSC : La machine doit remonter dans les **Appareils administrés** avec un statut **Connecté** (icône verte).

Conclusion

La mise en place de la solution Kaspersky et sa configuration m'ont permis de déployer un système de sécurité centralisé, fiable et efficace pour protéger les machines du réseau. Les tests que j'ai réalisés, comme la vérification de la communication entre le serveur et le poste client, l'application des politiques de sécurité et le bon fonctionnement des analyses antivirus, ont montré que la solution fonctionne correctement.
Grâce à cette infrastructure, les postes du réseau sont protégés automatiquement contre les menaces, tout en étant administrés de manière centralisée, ce qui facilite leur gestion et renforce la sécurité globale du système d'information.

Auto-évaluation

Le temps imparti de huit heures a été respecté, grâce à une bonne préparation en amont, notamment le téléchargement anticipé des ISO et la connaissance préalable de la procédure d'installation.
Cette anticipation m'a permis d'optimiser le déroulement du TP et d'atteindre les objectifs fixés dans les délais.