**Formation Technique #KL 014.30**

# Kaspersky Security for Virtualization. Agentless

## Agenda

### Jour 1

Présentation des cours et vue d'ensemble

### Chapitre 1. Introduction

Vue d'ensemble de VMware vSphere et vShield Endpoint: Introduction à vCloud Networking and Security. Introduction à Kaspersky Security for Virtualization Agentless, comparaison avec l'approche traditionnelle de la protection anti-virus.

### Chapitre 2. Installation de Kaspersky Security for Virtualization

Déploiement de vShield Endpoint. Description des prérequis pour Kaspersky Security for Virtualization Agentless. Image OVA et contenus de la distribution. Procédure d'installation.

- Lab 1 : Installation de Kaspersky Security for Virtualization Agentless

### Chapitre 3. Gestion de la protection

Gestion des licences de Kaspersky Security for Virtualization Agentless. Tâche de mise à jour. Principes de fonctionnement de la protection en temps réel. Configuration d'une stratégie pour Kaspersky Security for Virtualization Agentless dans Kaspersky Security Center.

- Lab 2 : Mises à jour
- Lab 3 : Test de la protection en temps réel
- Lab 4 : Paramètres de la protection en temps réel

### Chapitre 4. Analyse à la demande

Analyse à la demande, leurs types, les spécificités liées à l'environnement virtuel. Configuration d'une tâche.

- Lab 5 : Analyse à la demande

### Chapitre 5. Maintenance

Surveillance du statut de la machine virtuelle de sécurité depuis le client vSphere. Particularités de l'administration via Kaspersky Security Center.

### Chapitre 6. Blocage des attaques réseaux

Description de la solution vSphere. Prérequis système et infrastructure virtuelle. Procédure d'installation.

- Lab 6 : Installation du blocage des attaques réseaux
- Lab 7 : blocage des attaques réseaux

### Chapitre 7. Dépannage

Collecter les informations sur le fonctionnement de l'application. Problèmes potentiels et méthodes de diagnostic.

**Formation Technique #KL 031.30**

# Kaspersky Security for Virtualization. Light Agent

## Agenda

**Jour 2**

Présentation des cours et vue d'ensemble

### Chapitre 1. Introduction

Virtualisation. Protection des machines virtuelles. Kaspersky Security for Virtualization 3.0|Light Agent: structure et principes de fonctionnement

### Chapitre 2. Déploiement

Planification. Installation du Serveur de Protection. Déploiement des Light Agents.

- Lab 1. Pré-installation du Serveur de Protection
- Lab 2. Installation du Serveur de Protection
- Lab 3. Installation des licences
- Lab 4. Mise à jour
- Lab 5. Localiser le Serveur de Protection depuis plusieurs sous-réseaux
- Lab 6. Pré-Installation du Light Agent
- Lab 7. Installation du Light Agent sur des machines virtuelles persistantes
- Lab 8. Préparation d'un modèle
- Lab 9. Recréation de machines virtuelles dans une VDI
- Lab 10. Mode dynamique pour VDI

### Chapitre 3. Administration

Principes de l'administration de Kaspersky Security for Virtualization 3.0|Light Agent. Configuration des paramètres de protection (comparé à Kaspersky Endpoint Security). Surveillance de la protection.

- Lab 11 : Tolérance aux pannes
- Lab 12 : Déceler les problèmes de connectivité au Serveur de Protection

### Chapitre 4. Dimensionnement et maintenance

Dimensionner les ressources du Serveur de Protection. Particularités de la découverte du Serveur de Protection par les Light Agents. Particularités de la compatibilité des Serveurs de Protection avec la répartition automatique des charges dans un cluster d'hyperviseurs. Particularités de l'exploitation du Contrôle des périphériques sur les machines virtuelles. Reconfigurer les paramètres de connexion du Serveur de Protection et suppression du Serveur de Protection.

- Lab 13 (facultatif): Contrôle des périphériques