

Migration vers Symantec Endpoint Protection 11.x

DESCRIPTIF DU COURS

Ce cours offre une formation pratique aux clients qui réalisent une mise à niveau de Symantec AntiVirus Corporate Edition 9.x et supérieur et Symantec Client Security (SCS) 2.x et supérieur vers Symantec Endpoint Protection (SEP) 11.x. Les sujets abordés comprennent la planification et l'installation de Symantec Endpoint Protection Manager (SEPM), de la base de données et de l'interface cliente.

Parmi les sujets complémentaires on compte : comment déployer des logiciels sur des clients antivirus, comment ajouter et migrer des paramètres antivirus et des politiques de pare-feu, et comment ces paramètres et politiques sont gérés par Symantec Endpoint Protection Manager (SEPM).

Mode d'administration

Cours dispensé par un formateur

Durée

Deux jours

Objectifs du cours

A la fin de ce cours vous devriez être en mesure de :

- Décrire les produits et composants de Symantec Endpoint Protection (SEP) et Symantec Network Access Control (SNAC).
- Comparer des serveurs et groupes de clients SAV et SCS existants et des paramètres aux groupes et stratégies de SEP.
- Déterminer des tâches de migration.
- Installer Symantec Enterprise Protection Manager (SEPM) et les composants d'administration.
- Migrer les serveurs et clients SAV hérités.
- Installer et configurer la protection contre les menaces réseau.
- Migrer vos politiques de pare-feu SCS vers SEP 11.x.
- Contrôler votre nouvel environnement.

Audience concernée

Ce cours s'adresse aux administrateurs réseau et administrateurs système, aux administrateurs de sécurité client, aux professionnels des systèmes, aux revendeurs et consultants qui effectuent la mise à niveau vers un environnement Symantec Endpoint Protection 11.x et qui se chargent de l'installation, de la configuration et de la gestion quotidienne de Symantec Endpoint Protection 11.x dans divers environnements réseau.

Pré requis

Des connaissances de base de Symantec AntiVirus Corporate Edition ou Symantec Client Security sont requises, ainsi que des connaissances de niveau administrateur réseau (y compris TCP/IP), et des systèmes d'exploitation Microsoft Windows 2000/XP/2003.

Formation pratique

Ce cours comprend des exercices pratiques vous permettant de tester vos nouvelles compétences et de commencer à les utiliser dans un environnement professionnel.

PLAN DU COURS

Leçon 1 : Introduction aux composants de SEP 11.x

- Description des produits SEP et SNAC
- Description des composants SEP
- Définition des versions de SAV et SCS prises en charge pour la migration
- Choix des produits et composants à installer
- Description des concepts de politique, groupe, héritage et emplacement

Leçon 2 : Préparation à la migration vers SEP11.x

- Corrélation entre les groupes de serveurs SAV/SCS, les serveurs, les groupes de clients, et SEP 11.x.
- Corrélation entre les paramètres de SAV/SCS Antivirus, LiveUpdate et les politiques de SEP 11.x.
- Définition des paramètres de SAV/SCS à migrer
- Description des scénarios de migration
- Identification des tâches de pré migration

Leçon 3 : Installation de l'environnement de SEP 11.x

- Réalisation des tâches de pré migration
- Installation de Symantec Endpoint Protection Manager
- Conversion de la hiérarchie du système de SAV/SCS vers la structure du groupe de SEP.
- Protection de Symantec Endpoint Protection Manager
- Planification de LiveUpdate pour le Manager
- Création de domaines, d'administrateurs et de mots de passe

Leçon 4 : Migration de l'environnement de SEP 11.x

- Utilisation de l'assistant de migration
- Identification des clients
- Migration des logiciels et politiques vers les clients
- Déploiement des mises à jour de clients (Patch et Delta)



Jour 2

Leçon 5 : Mise à jour des politiques antivirus et antispyware pour SEP 11.x

- Planification de LiveUpdate pour le client
- Configuration d'exceptions
- Planification d'analyses sur demande
- Configuration d'une politique d'analyse de protection proactive
- Modification des politiques de protection antivirus et antispyware

Leçon 6 : Installation, déploiement et gestion de la protection de menaces réseau

- Description de politiques de protection réseau par défaut
- Création d'une politique de protection réseau personnalisée
- Personnalisation d'une politique IDS / IPS
- Création d'un emplacement
- Déploiement d'une politique de protection réseau
- Migration des politiques de pare-feu SCS

Leçon 7 : Contrôle de l'environnement de SEP 11.x

- Restriction de l'accès aux groupes spécifiques
- Configuration de la page d'accueil et des contrôles pour répondre aux menaces et aux risques
- Analyse des rapports et journaux