

EPO : EPolicy Orchestrator

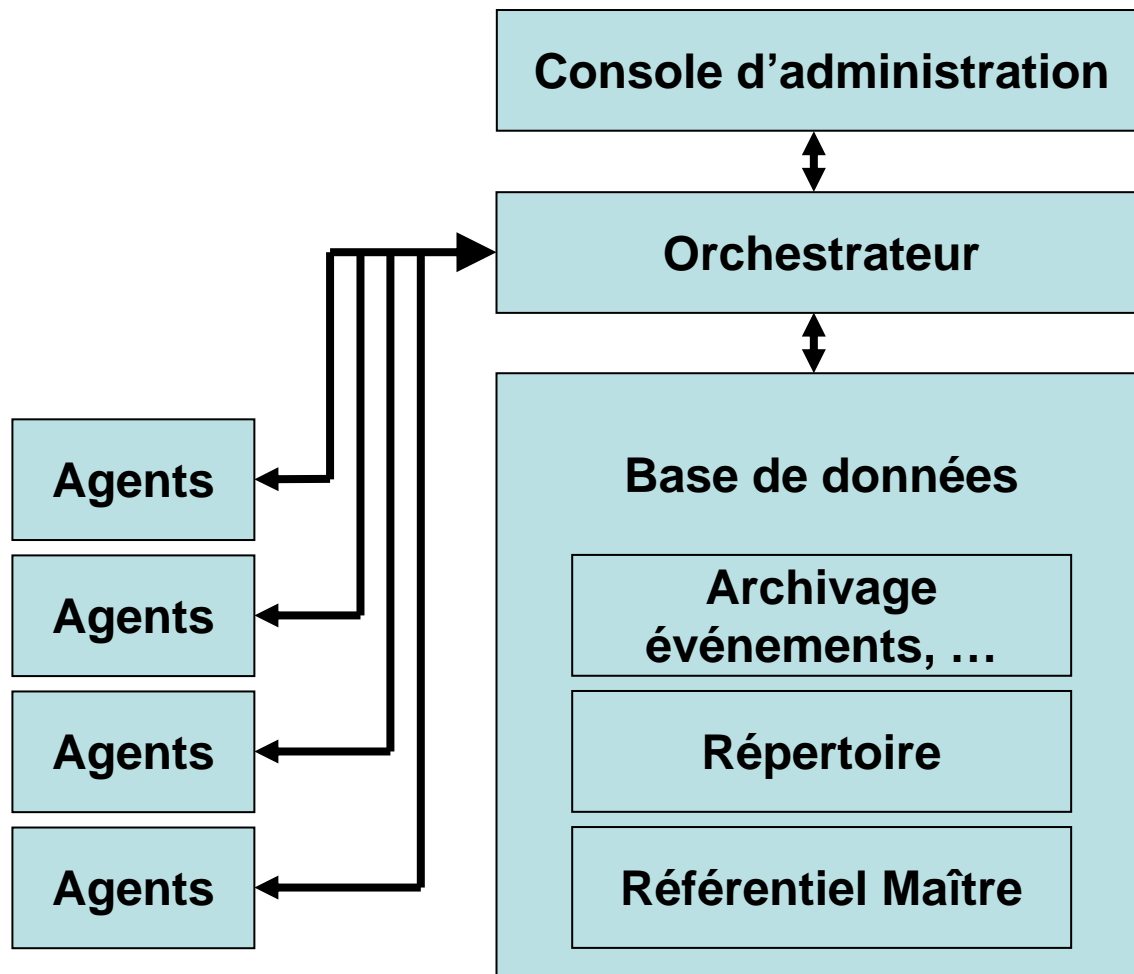
EPO est le premier outil de gestion centralisée des Antivirus des clients.

Il est édité par McAfee, Il permet à un administrateur de déployer sur les clients puis configurer et mettre à jour :

**Les antivirus McAfee
Les pare feu McAfee
Norton AntiVirus
Patches de sécurité SuS**



EPO : Le principe



Administrateur manage l'ensemble du dispositif.

Orchestration des communications entre les différents éléments du dispositif

La base de données Contient l'ensemble Des données

- Logiciels
- Machines
- ...

ePO est un progiciel qui fonctionne sur le mode Client/serveur

L'Agent installé sur un client se réveille :

Toutes les 5' pour appliquer la Stratégie courante

Toutes les 60' pour contacter le serveur afin d'appliquer une éventuelle nouvelle Stratégie.

A tout instant, l'administrateur peut réveiller l'Agent depuis la console pour anticiper la communication ainsi programmée.

L'Administrateur utilise une Console d'administration pour :

Organiser les clients en groupes homogènes

Programmer les Stratégies applicables par les groupes de clients

Gérer les Packages : télécharger, installer, déployer, mettre à jour.

Programmer des Tâches d'Extraction :

- Déploiement de Packages sur les clients.
- Extraction : récupération des Mise à jour
- Réplication : copie du Référentiel maître sur des Référentiels distribués

EPO : Configuration requise



Configuration requise matériel

Espace disque disponible : 1 Go recommandé

Mémoire : 256 Mo de RAM

Processeur : Intel Pentium II ou supérieur, 400 MHz ou supérieur

Moniteur : VGA, 1024x768, 256 couleurs

Serveur dédié : recommandé par McAfee pour la gestion de plus de 250

Configuration logicielle requise

Windows 2000 Advanced Server avec Service Pack 1, 2, 3 ou 4

Windows 2000 Server avec Service Pack 1, 2, 3 ou 4

Windows Server 2003 Enterprise

Windows Server 2003 Standard

Le serveur s'appuie sur un «AGENT» installé sur les stations.

Il est distribué :

Par «push» dans un domaine NT/2000 ou un Workgroup administré.

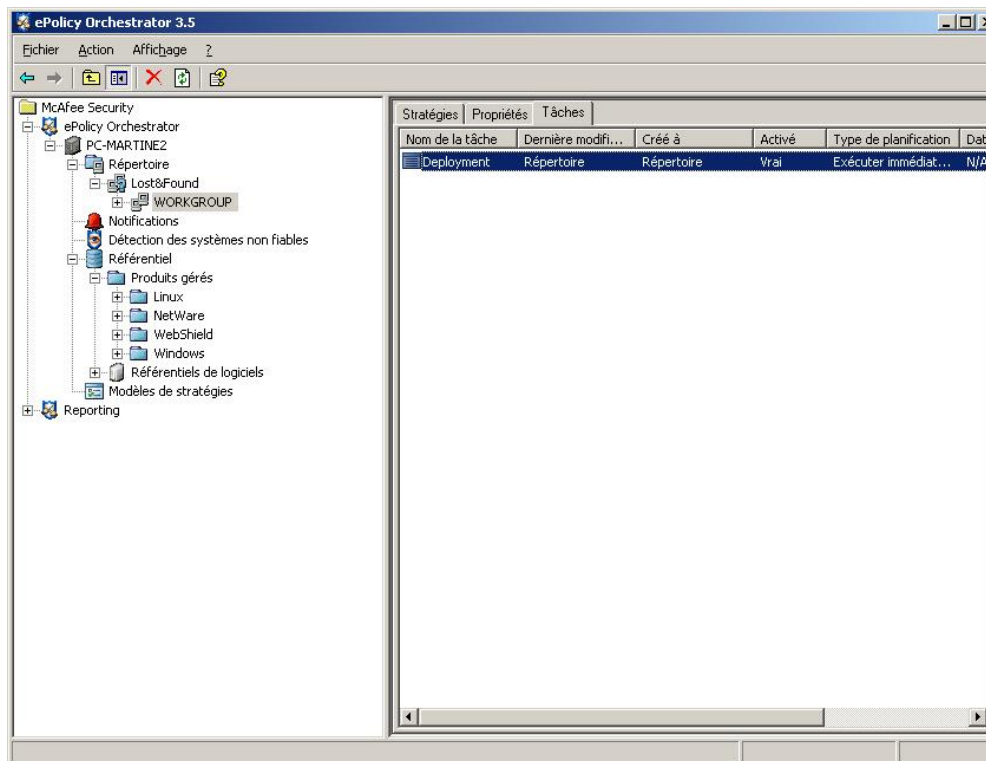
Manuellement (ftp, http, partage réseau etc.) pour les stations ou groupes isolés (taille : 535 Ko).

L'agent envoie au serveur un état de la station à intervalles programmés.

En fonction de cet état le serveur renvoie à l'agent les opérations à effectuer.

L'agent se déconnecte du serveur et applique localement les opérations sur la station

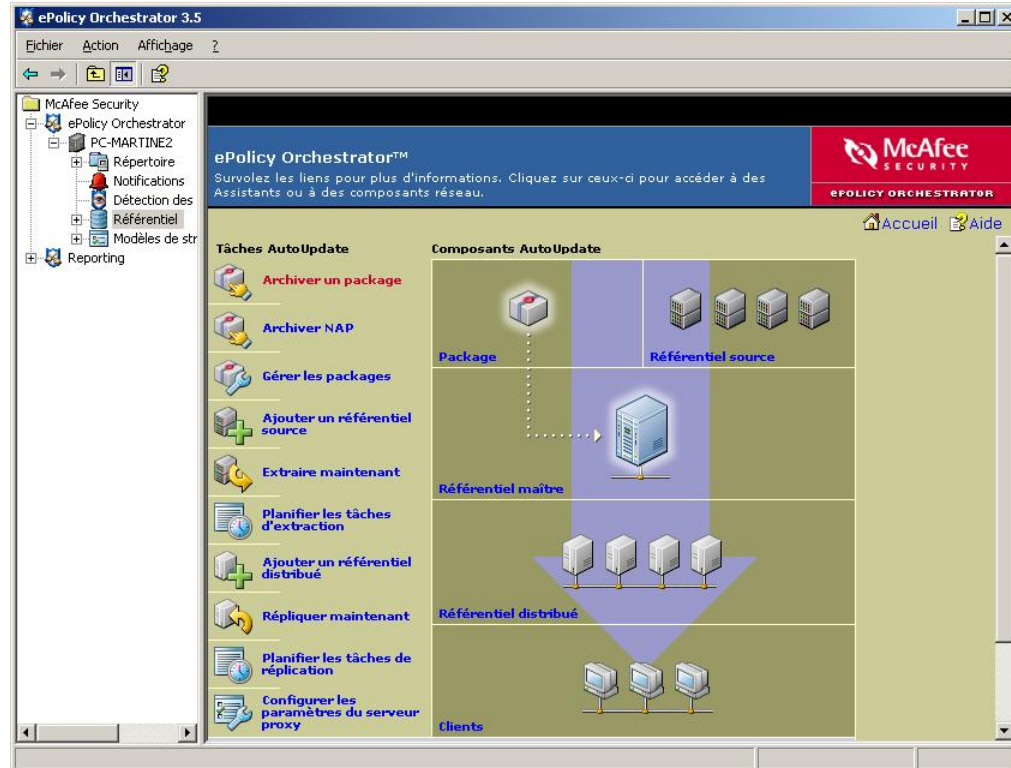
EPO : Le Répertoire



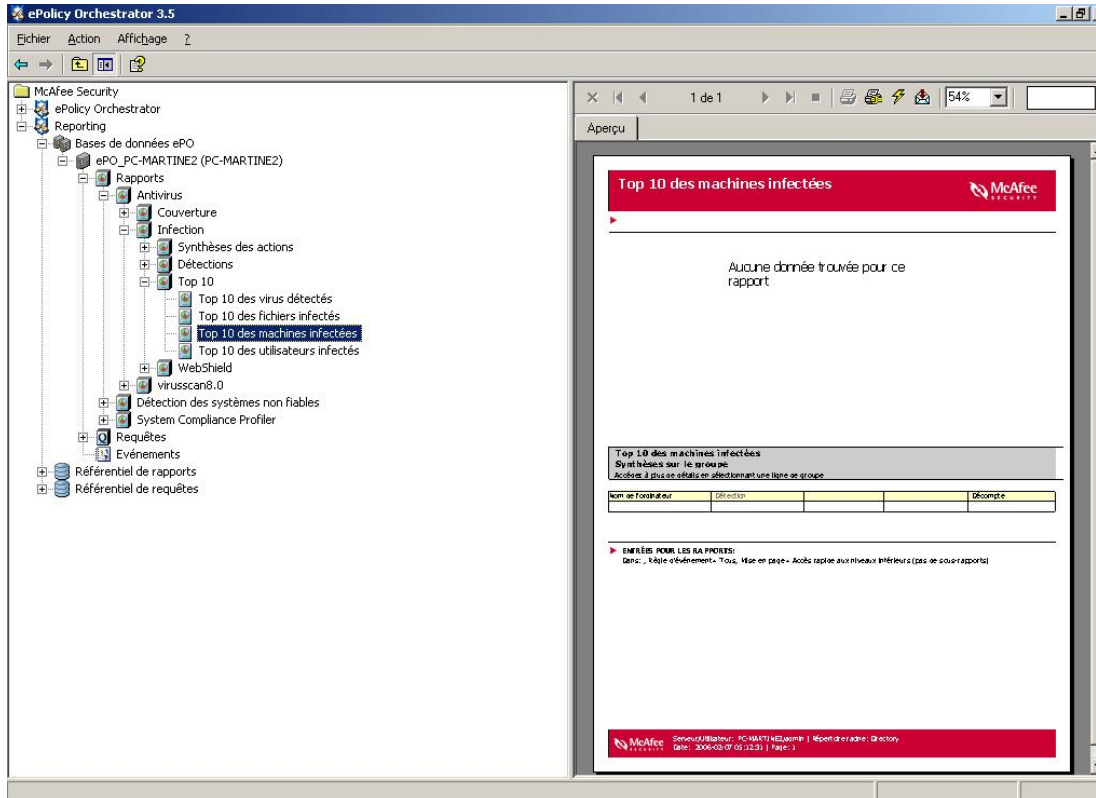
EPO : La Base de données



EPO : Le Référentiel

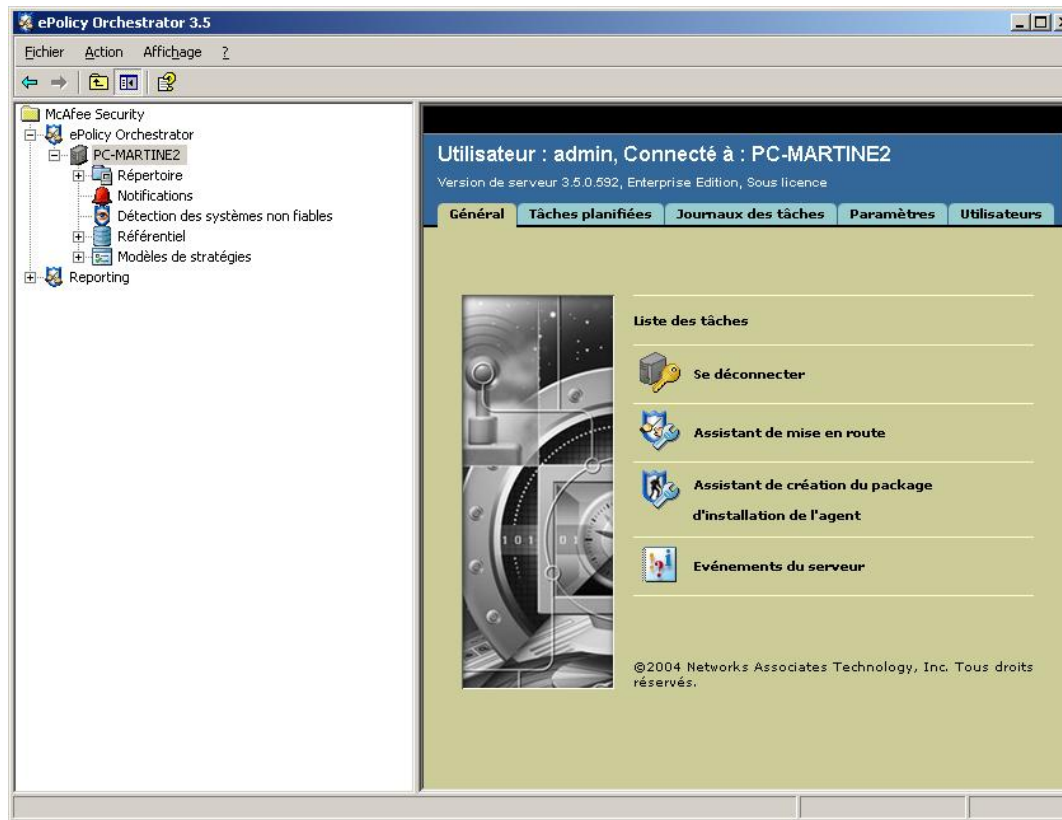


EPO : Les Rapports



The screenshot displays the McAfee ePolicy Orchestrator 3.5 interface. On the left, a tree view shows the navigation structure under 'McAfee Security' > 'ePolicy Orchestrator' > 'Reporting' > 'Bases de données ePO' > 'ePO_PC-MARTINE2 (PC-MARTINE2)' > 'Rapports' > 'Antivirus' > 'Infection' > 'Top 10 des machines infectées'. The main pane on the right shows a report titled 'Top 10 des machines infectées' with the McAfee logo. The report content indicates that no data was found for this report. Below this, there is a section for 'Top 10 des machines infectées' with a table header and a red warning message: 'ENFÉRÉS POUR LES RA PPOR TES: Dans ce tableau d'événement, Tous, Mise en page - Accès rapide aux niveaux inférieurs (pas de sous-rapports)'. At the bottom, the footer shows 'McAfee Security ePolicy Orchestrator - PC-MARTINE2 | Rapport de sécurité - Directory'.

EPO : La Console d'administration



Début de l'installation (options)

- Licence d'enregistrement
- Dossier de l'installation
- Mot de passe pour administrer EPO (chef d'orchestre)
- Identification de la base de données (lieu)
- Mot de passe pour administrer la base de données
- Port d'accès à EPO (port TCPIP http)
- Adresse Internet de l'administrateur EPO

Installation des package

- Mise en place d'une autorité de certification pour les communications
- Archivage de logiciels (package) dans le référentiel
- Déploiement de l'agent
- Stratégies et tâches de l'agent
- Planification de EPolicy Orchestrator
- Gestion des rapports
- Installation des agents