

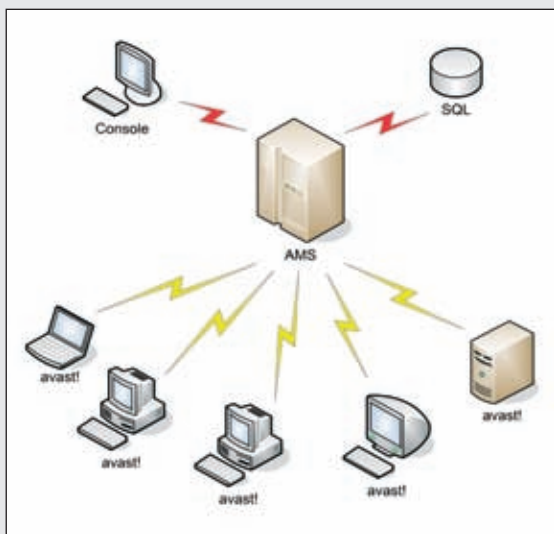
avast! Distributed Network Manager (ADNM) est une suite d'outils performants conçus pour aider les administrateurs de réseaux dans la gestion la gamme de produit avast! antivirus à travers toute l'entreprise. Sa flexibilité et son extensibilité inégalées font d'elle une solution idéale pour les réseaux de toute taille, à partir des réseaux de petites entreprises jusqu'aux grands réseaux hétérogènes à échelle intercontinentale. L'ADNM comprend les composants suivants:

- avast! Management Server (AMS)(Serveur de gestion)
- Base de données SQL
- Console d'administration

Ces trois composants travaillent ensemble avec les produits d'avast! antivirus déployés sur les Postes de travail individuelles et sur les serveurs du réseau, afin de fournir la meilleure protection possible contre les infections et de minimiser les efforts requis pour les observer et gérer leur activité.

Comment travaille-t-il

Le cerveau de tout le système est l'AMS (avast! Management Server). C'est là que l'essentiel du travail s'effectue. Les machines gérées ne se connectent au serveur (AMS) que pour télécharger les dernières règles, et pour rapporter leur statut et les résultats de scan. Aussi, la console d'administration se connecte directement sur le serveur de gestion avast!(AMS). Ce dernier est d'ailleurs basé sur la base de données SQL, soit sur MS SQL Serveur 2000 si disponible, ou alors pour les réseaux de taille petite ou moyenne, sur sa version allégée, MSDE 2000, qui fait partie du package d'installation de l'ADNM. Pour des réseaux plus grands, l'AMS nécessite d'être installé sur un ordinateur qui lui est dédié. On suppose également que le serveur de gestion (AMS) peut se connecter à Internet via protocole de HTTP.



Pour des réseaux plus grands, il est possible de déployer plusieurs serveurs de gestion (AMS), chacun d'entre eux ayant sa propre base de données. Ces serveurs peuvent ensuite être programmés pour dupliquer leurs bases de données régulièrement, et également charger tous les résultats des scans sur un AMS spécifique grâce auquel tous les rapports de l'entreprise pourront être ressortis par la suite. Les administrateurs peuvent choisir entre deux modèles de communication utilisés par l'AMS et les clients: PUSH ou POP. Le modèle POP est approprié surtout pour les grands réseaux et pour ceux contenant des utilisateurs itinérants. Chaque AMS peut contenir jusqu'à 10'000 ordinateurs clients, à condition qu'ils soient tous connectés par LAN (Réseau local).

Les sections suivantes résument les fonctionnalités et les avantages principaux d'avast! Distributed Network Management (ADNM).

Structure hiérarchique de règles

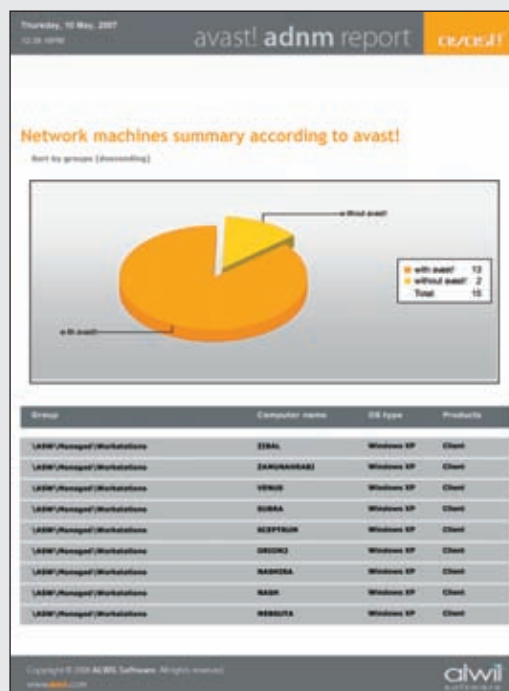
ADNM maintient la liste des ordinateurs pris en charge dans une structure sous forme d'arbre. La clé pour une gestion efficace réside avant tout dans la création et l'organisation d'une arborescence qui répond le mieux possible aux besoins administratifs. Il est souvent pratique de construire un agencement qui reflète la géographie et l'organisation structurelles de votre réseau. Dans cette optique, il semble plutôt facile, et naturel, de définir les différents droits d'accès à l'administration, puisque la majorité des structures organisationnelles d'une entreprise est caractérisée par un arbre comprenant les quartiers généraux à la racine et les succursales sur les branches. Cette arborescence peut être élaborée automatiquement, ou alors importée d'une source externe (dans le format d'un fichier texte). Toutes les règles et stratégies de sécurité sont par défaut reportées des parents aux enfants dans la structure en arbre, mais ceci peut bien sûr être redéfini suivant des besoins spécifiques.

Découverte et Déploiement à Distance

ADNM supporte des installations sur le réseau sans présence physique et à distance, couvrant même plusieurs domaines. Ceci s'avère particulièrement utile lors de la première mise en place. ADNM supporte aussi la détection périodique de nouvelles machines connectées au réseau. Ces deux technologies (découverte et déploiement à distance) peuvent être associées afin de bénéficier d'une recherche constante de nouvelles machines et d'un déploiement automatique et contrôlable du logiciel de protection antivirus sur ces ordinateurs.

Rapport

Une des fonctionnalités d'ADNM les plus appréciée est la performance de ses rapports. ADNM fournit un large éventail de rapports graphiques et tabulaires, adaptés à une gestion régulière et à une administration quotidienne du réseau. Ces rapports peuvent être générés directement dans la base de données et donc visibles sur la console d'administration en utilisant la visionneuse de rapports, ou alors peuvent être exportés vers différents formats (tels que PDF, HTML, DOC), puis sauvés sur le disque. Ils peuvent même être automatiquement envoyés par message électronique vers une boîte de réception définie; fonctionnalité particulièrement utile pour une gestion cyclique des rapports.



Comme tous les autres types de tâches dans ADN, l'exécution des rapports peut être planifiée périodiquement à intervalles donnés (quotidien, hebdomadaire, etc.)

Alertes

Avec l'aide du gestionnaire de notification d'avast!, l'ADNM permet aux administrateurs réseaux de paramétrer des mécanismes d'alertes très puissants. Différentes méthodes d'avertissement sont supportées, tel que l'envoi de messages électroniques en utilisant SMTP ou MAPI (MS Outlook), le procédé Windows pop-up (messages réseaux), l'impression du message sur une imprimante du réseau, les trappes SNMP, ou même l'envoi de messages instantanés (IM) en utilisant MSN/Windows Messenger.

Mises à jour automatiques

Des mises à jour rapides et automatiques sont l'un des points clés d'une protection antivirus efficace. Avec avast!, les mises à jours sont incrémentales, seules les nouvelles données sont téléchargées, ce qui réduit fortement le temps de transfert et les besoins en bande passante. La taille standard d'une mise à jour de la base de données des virus est approximativement de 20 à 80kb, tandis qu'une mise à jour du programme ne dépasse généralement pas 200 à 500kb.

ADNM peut être déployé sur un ou plusieurs „serveurs miroirs“, qui sont des machines connectées au réseau local et servant à stocker les données des mises à jour. Ces machines sont automatiquement synchronisées avec notre système de serveurs Internet en ligne. Les machines individuelles du réseau téléchargent ensuite les données depuis les miroirs. Il peut y avoir un nombre illimité de miroirs et ils peuvent également être paramétrés pour travailler dans une structure hiérarchique sous forme d'arbre.

Une fonctionnalité spéciale d'avast! est les mises à jour PUSH. Dans un scénario PUSH, les mises à jour sont lancées directement par nos serveurs, ce qui permet aux serveurs miroirs de répondre et d'effectuer les synchronisations nécessaires plus rapidement. Le système utilise le protocole SMTP/POP3 comme couche de transport (par exemple la messagerie électronique classique). Cette technologie est protégée par des codes asymétriques et résiste aux emplois non autorisés.

Sécurité

L'AMS maintient un système d'utilisateurs et de groupes d'utilisateurs avec leurs droits d'accès. Chaque objet (que ce soit une tâche, un ordinateur, une planification, un événement, une méthode d'alerte ou quoi que ce soit d'autre) possède une liste de contrôle d'accès, dans laquelle il est possible de définir qui peut y accéder et qui ne peut pas. Cela permet aux administrateurs principaux de réduire les accès des administrateurs locaux uniquement aux objets pour lesquels ils sont responsables, sans risquer un quelconque changement non autorisé des paramètres de sécurité

en dehors de leur périmètre. Toutes les communications entre l'AMS et la console sont cryptées par le protocole SSL, qui assure une sécurité maximum. L'AMS s'identifie lui-même sur la console par un certificat digital pour prouver sa bonne foi. Les données sensibles ne sont transmises sur le réseau qu'une fois une liaison cryptée valable établie.

Support pour les utilisateurs d'ordinateurs portables

Les machines itinérantes représentent toujours un challenge important pour les systèmes de gestion. Ils n'appartiennent à aucun réseau local (LAN) spécifique, ils se connectent sur le réseau de l'entreprise plus ou moins aléatoirement, ils ne sont en général pas directement adressables et leurs utilisateurs essaient souvent d'outrepasser les restrictions imposées sur leurs machines par les administrateurs systèmes. Par conséquent, ADN a été désigné dès le début en pensant aux utilisateurs d'ordinateurs portables. La communication entre l'AMS et les clients est toujours lancée par les clients eux-mêmes (système POP), résolvant le problème du „non-adressable“. Dès que les ordinateurs portables se connectent au réseau de l'entreprise, aucune importance sur quelle filiale (ou même si c'est par un tunnel VPN à travers l'Internet), les nouvelles règles et stratégies, ainsi que les mises à jours, sont automatiquement téléchargées et installées, avant qu'une machine potentielle non-sécurisée ne puisse causer de dégâts. Si le réseau de l'entreprise n'est pas disponible, mais qu'il est toujours possible d'accéder à Internet, les mises à jour sont acquises directement depuis nos serveurs Internet.

Détails Techniques

Système Requis

avast! MANAGEMENT SERVER

- Windows NT 4 Service Pack 4 ou supérieur / Windows 2000 SP1 ou supérieur / Windows XP ou Windows Server 2003
- 128MB RAM (256-512MB recommandés)
- 200MB d'espace libre sur le disque dur
- MQ SQL Server 2000 ou built-in MSDE

Console d'Administration

- Windows NT 4 Service Pack 4 ou supérieur / Windows 2000 SP1 ou supérieur / Windows XP or Windows Server 2003
- 64MB RAM (128MB recommandés)
- 50MB d'espace libre sur le disque dur
- Internet Explorer 4 ou supérieur

LANGUES SUPPORTEES

Anglais, Japonais, Tchèque, allemand, Français, Espagnole, Portugais, Italien, Hollandais, Hongrois, Polonais, Russe, Coréen, Turque et Slovaque

PRODUITS SUPPORTES POUR LA GESTION

- avast! Edition Professionnelle (version gérée)
- avast! Server Edition (version gérée)

CAPACITES DE GESTION

- installation à distance d'avast! Antivirus
- exécution automatique des règles de sécurité (réglages, planifications, mises à jour...)
- contrôle en temps réel des fonctionnalités et de la mise à jour d'avast!
- rapport de statut d'avast! Antivirus
- gestion d'alerte complexe