

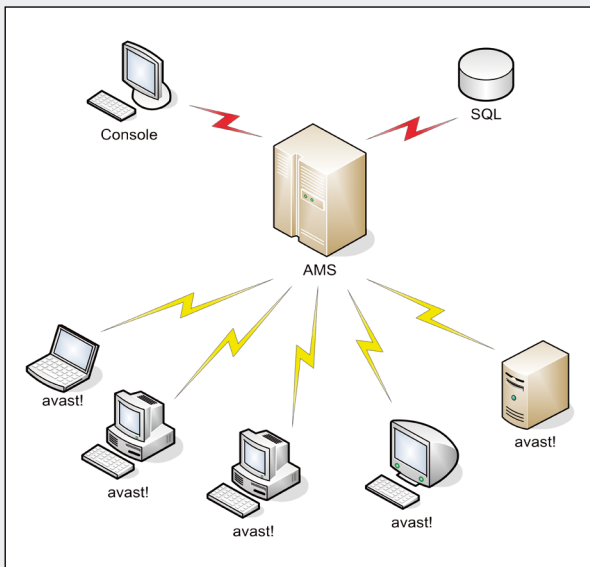
avast! Distributed Network Manager (ADNM) representa una suite de potentes herramientas diseñadas para ayudar a los administradores de red a gestionar los productos de la línea avast! antivirus a través de toda la compañía o corporación. Su flexibilidad y escalabilidad le hacen una solución ideal para redes de cualquier tamaño, desde simples redes de PYMES a grandes y heterogéneas redes corporativas en múltiples continentes. El sistema de ADNM consiste en los componentes siguientes:

- avast! Management Server (AMS)
- Base de datos SQL
- Consola de Administración

Estos tres componentes trabajan junto a los productos antivirus de avast! distribuidos en puestos de trabajo y servidores individuales en la red para proporcionar la mejor protección posible contra malware y para reducir al mínimo el esfuerzo necesario para manejar y supervisar su estado actual.

Como trabaja

El cerebro de todo el sistema es el AMS (avast! Management Server). Aquí es donde se hace todo el trabajo duro. Las máquinas gestionadas se conectan solo al AMS para descargarse las últimas políticas y para informar de su estado y de los resultados de exploraciones en busca de virus. La Consola de Administración también se conecta directamente al AMS. El AMS se cimenta en una base de datos SQL: en una base de datos dedicada MS SQL Server 2000 o superior, si está disponible, o en una versión reducida de MSDE 2000 que es parte del paquete de instalación de ADNM. Para grandes redes, el AMS debe ser instalado en un ordenador dedicado. Se considera que la máquina de AMS puede conectarse a Internet vía protocolo HTTP.



También es posible desplegar múltiples AMS, cada uno conteniendo su propia base de datos. Estos pueden ser configurados para replicar su base de datos en una centralizada y enviar todos los resultados de exploraciones en busca de virus al servidor dedicado de AMS, en el que se pueden obtener informes globalizados sobre todas las instalaciones. Los administradores pueden elegir entre dos modelos de comunicaciones usados por los clientes de AMS: PUSH o POP. El modelo POP está especialmente indicado para redes grandes y redes con usuarios itinerantes (roaming). Cada AMS puede ser escalado hasta decenas de miles de ordenadores clientes, con tal de que todos estén conectados a una red de área local.

Estructura jerárquica de políticas

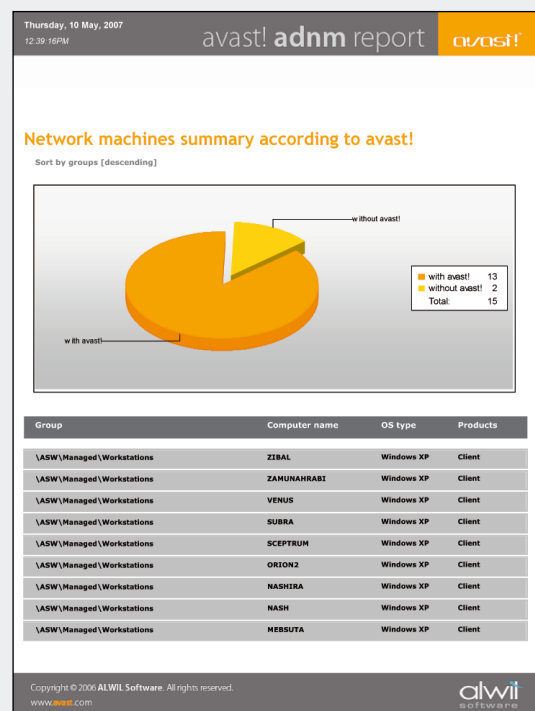
ADNM mantiene la lista de ordenadores gestionados en una estructura de árbol. La clave para una gestión eficaz es diseñar y organizar esta estructura para que satisfaga, lo mejor posible, las necesidades de administración. A menudo es bueno construir el árbol de modo que refleje la estructura geográfica y de organización real de la red. De esta manera, es muy sencillo asignar derechos de acceso administrativos y políticas de una manera natural, puesto que la mayoría de las estructuras de las organizaciones se caracteriza por un árbol con las jefaturas en la raíz y las sucursales debajo. La definición del árbol se puede construir automáticamente, o puede ser importada de una fuente externa (archivo de texto). Todas las políticas de la seguridad en el árbol están por defecto heredadas de padres a hijos pero pueden ser redefinidas según requisitos específicos.

Descubrimiento y despliegue/instalación remota

ADNM soporta el despliegue/instalación remoto desatendido del paquete de instalación de avast! a través de la red, incluso con múltiples dominios. Esto es especialmente útil para la instalación inicial. ADNM también soporta descubrimiento periódico de nuevas máquinas en la red. Estas dos tecnologías, descubrimiento y despliegue remoto, puede ser combinadas de manera que resulta una búsqueda constante de nuevas máquinas y una distribución automática y controlable del software de protección de virus en estas máquinas.

Informes

Una de las mejores características de ADNM es su capacidad de generar informes. ADNM proporciona una amplia gama de informes gráficos y tabulares apropiados para la gestión regular y la administración diaria de la red. Los informes se pueden generar directamente en la base de datos y por lo tanto ver en la consola de administración usando el visor de informes integrado, o puede ser exportado a una variedad de formatos (incluyendo PDF, HTML y DOC) y guardados en disco. Incluso pueden ser enviados automáticamente por E-mail a un destinatario fijado, algo muy útil para los informes de gestión periódica.



Como cualquier otro tipo de tarea de ADN, las tareas de informes pueden ser programadas para sean ejecutadas a intervalos de tiempos dados: diario, semanal, mensual, etc.

Alerting

Con la ayuda del Gestor de Notificaciones de avast!, ADN permite a los administradores de la red, configurar sistemas de alerta muy potentes. La nueva versión soporta objetos de notificación como mandar un mensaje de correo electrónico usando SMTP o MAPI (Outlook). También permite SMS, notificaciones usando los mecanismos de Windows popup (mensajes de red), imprimir el mensaje en una impresora de red, tramas SMTP, o incluso enviar un mensaje IM usando MSM/Windows Messenger.

Actualizaciones Automáticas

Las actualizaciones rápidas, automáticas son uno de los puntos clave en la protección contra virus. Con avast!, las actualizaciones son incrementales, y sólo los nuevos datos son descargados, lo que reduce drásticamente el tiempo de transferencia y los requerimientos de ancho de banda. El tamaño típico de una actualización de base de datos de virus es aproximadamente de 20-80 kb, la actualización del programa es de 200-500kb.

ADNM soporta la instalación de uno o más "mirror server", máquinas de red local que actúan como almacén para las actualizaciones y que se sincroniza automáticamente con nuestros sistemas online en Internet. Los nodos individuales de la red se descargan las actualizaciones de los "mirror servers". Puede haber cualquier número de espejos y pueden ser configurados para trabajar en una estructura jerárquica de árbol.

Una característica especial de avast! son las actualizaciones PUSH. En el escenario PUSH, las actualizaciones son iniciadas directamente por nuestro servidor, lo que da lugar a una respuesta inmediata por parte de los "mirror server" y procediendo a la sincronización necesaria. El sistema utiliza protocolos SMTP/POP3 como capa de transporte.

Seguridad

El AMS mantiene un sistema de usuarios y de grupos de usuario, y sus derechos de acceso. Cada objeto (sea una tarea, ordenador, horario, evento, objeto de aleta o cualquier cosa) tiene una lista de control de acceso, en la cual es posible configurar quién pueden tenerle acceso y quién no. Esto permite a los administradores principales delegar a administradores locales sólo los objetos de los que ellos son responsables, sin arriesgarse a cualquier cambio no autorizado de los ajustes de política fuera de su alcance.

Toda la comunicación entre el AMS y la consola es cifrada por el protocolo estándar SSL para ofrecer seguridad máxima. El AMS se identifica a la consola por un certificado digital. Solamente después de que se establece un canal apropiado de cifrado los datos credenciales se transfieren sobre la red.

Soporte para los usuarios de portátiles

Las máquinas itinerantes siempre representan un gran desafío para los sistemas de gestión. No pertenecen a una LAN específica u oficina, se conectan con la red corporativa más o menos aleatoriamente, están en el general, no directamente direccionados y sus usuarios están intentando, a menudo, saltarse las restricciones fijadas por los administradores de sistemas en sus máquinas. ADN fue diseñado desde el principio pensando en los usuarios con portátiles. La comunicación entre el AMS y los clientes es siempre iniciada por los clientes (sistema POP), superando el tema de no direccionamiento. Tan pronto como el portátil se conecta a la red corporativa, no importa en que oficina (o incluso si es vía VPN a través de Internet), las nuevas políticas y actualizaciones son automáticamente descargadas y aplicadas, antes de que la máquina potencialmente insegura pueda causar cualquier daño. Si la red corporativa no está disponible, pero todavía es posible el acceso a Internet, las actualizaciones se realizan directamente desde nuestros servidores de Internet.

Detalles Técnicos

Requerimientos del Sistema

avast! MANAGEMENT SERVER

- Windows NT 4 Service Pack 4 o superior, o Windows 2000 SP1 o superior, o Windows XP, o Windows Server 2003
- 128MB RAM (256-512MB recomendado)
- 200MB de espacio libre en disco
- MQ SQL Server 2000 o built-in MSDE

CONSOLA DE ADMINISTRACIÓN

- Windows NT 4 Service Pack 4 o superior, o Windows 2000 SP1 o superior, o Windows XP, o Windows Server 2003
- 64MB RAM (128MB recomendado)
- 50MB de espacio libre en disco
- Internet Explorer 4 o superior

IDIOMAS SOPORTADOS

Inglés, Japonés, Checo, Alemán, Francés, Español, Portugués, Italiano, Holandés, Húngaro, Polaco, Ruso, Coreano, Turco y Eslovaco.

PRODUCTOS SOPORTADOS PARA LA GESTIÓN

- avast! Professional Edition (versión gestionada)
- avast! Server Edition (versión gestionada)

CAPACIDADES DE GESTIÓN

- instalación remota de avast! antivirus
- aplicación automática de las políticas de la seguridad (ajustes, programaciones, actualizaciones...)
- monitorización de la funcionalidad y las actualizaciones de avast! en tiempo real
- informe de estado de avast! antivirus
- gestión compleja de alertas