

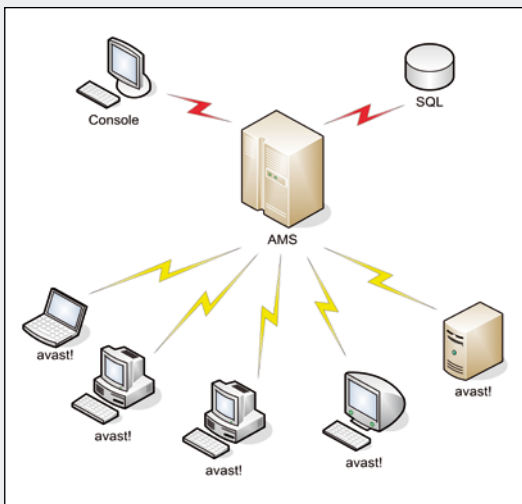
**avast! Distributed Network Manager (ADNM) representa um pacote de poderosas ferramentas destinadas a ajudar administradores de rede a gerir a linha de produtos avast! dentro de toda a empresa. A sua flexibilidade e escalabilidade sem rivais torna-a a solução ideal para redes de quaisquer dimensões, desde redes de pequenos negócios a grandes e heterogéneas redes com distribuição em múltiplos continentes. A ADNM consiste nos seguintes componentes:**

- Avast! management Server (AMS)
- Base de dados SQL
- Consola de Administração

**Estes 3 componentes trabalham em conjunto com os produtos avast! instalados em workstations individuais e em servidores para fornecer a melhor protecção possível contra malware e para minimizar o esforço necessário para gerir e monitorizar o seu estado.**

## How it works Como funciona

O cérebro de todo o sistema é o AMS (avast! Management Server). Aqui é onde todo o trabalho difícil é feito. As máquinas a serem geridas estão ligadas apenas ao AMS para fazer o download das últimas políticas e para reportar o seu estado e os resultados de escaneamento. A Consola de Administração também está directamente ligada ao AMS. O AMS é baseado na base de dados SQL – um MS SQL Server 2000, se disponível, ou, para pequenas e médias redes, a sua versão mais leve.



Para redes maiores é possível desdobrar múltiplos AMS' (cada um com a sua base de dados). Estes podem ser instruídos para replicarem as suas bases de dados regularmente e também fazer o upload de todos os resultados de escaneamento para uma AMS específica na qual pode ser levado a cabo um relatório geral de toda a empresa. É possível escolher de dois modelos de comunicação entre a AMS e os clientes: PUSH ou POP. O modelo POP é destinado a grandes redes e redes com utilizadores em roaming. Cada AMS pode abranger até dezenas de milhares de computadores de clientes, desde que estejam todos ligados por uma rede local.

As seguintes secções resumizam as características e benefícios principais da ADNM.

## Estrutura hierárquica da política

A ADNM mantém a lista de computadores geridos numa estrutura em árvore. A chave para uma gestão efectiva é elaborar e organizar

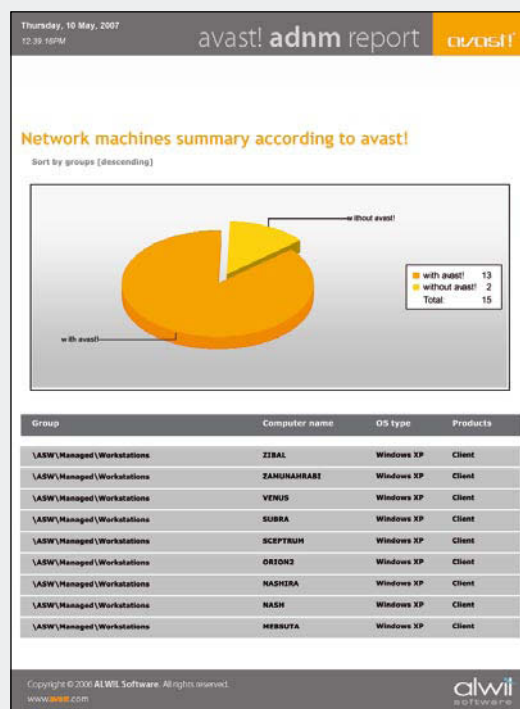
esta estrutura de modo a servir as necessidades da administração. Às vezes o ideal é construir esta árvore de modo a reflectir a actual estrutura geográfica e organizacional da rede. Deste modo também é possível atribuir vários direitos e políticas de acesso de um modo natural visto que a maioria da estrutura das organizações podem ser caracterizadas por uma árvore com as sedes nas raízes e os escritórios afiliados abaixo. A árvore pode ser construída automaticamente ou ser importada de uma fonte externa (sob a forma de ficheiro de texto). Todas as políticas de segurança na árvore são herdadas por defeito de pais para filhos mas podem ser redefinidas de acordo com requisitos específicos.

## Descoberta e distribuição remota

A ADNM suporta distribuição desacompanhada e remota dos pacotes de instalação avast! em toda a rede, mesmo domínios múltiplos. Isto é especialmente útil para o lançamento inicial do produto. ADNM também suporta descobertas periódicas de novas máquinas na rede. Estas duas tecnologias (descoberta e distribuição remota) podem ser combinadas em conjunto, resultando numa busca constante por novas máquinas e distribuição automática e controlável de software de protecção de vírus para estas máquinas.

## Relatório

Uma das características principais ADNM é a capacidade de relatório. A ADNM providencia uma grande escala de relatórios em gráfico e em tabelas apropriados para relatórios de gestão e para administração diária de redes. Os relatórios podem ser gerados directamente na base de dados e visualizados na Consola de Administração ou Visualizador integrado, ou podem ser exportados para uma grande variedade de formatos (incluindo PDF, HTML e DOC) e guardados no disco. Os relatórios até podem ser enviados automaticamente por email para um recípiante pré-definido, o que é uma característica bastante útil para uma gestão periódica.



Tal como qualquer outro tipo de tarefa do ADN, as tarefas de relatório podem ser agendadas para correr periodicamente em intervalos pré-definidos (diária, semanalmente, etc.).

### Alerting Alertas

Com a ajuda do avast! Notification Manager, a ADN permite aos administradores de rede preparar mecanismos de alerta muito poderosos. É suportado um grande número de objectos de notificação, tais como o envio de emails usando SMTP ou MAPI (Outlook), ou utilizando para notificação o Windows popup mechanism (network message), imprimir uma mensagem numa impressora em rede, armadilhas SNMP, ou até o envio de mensagens IM usando MSN/Windows Messenger.

### Actualizações automáticas

As rápidas actualizações automáticas é uma das chaves para uma protecção de vírus eficaz. Com avast, as actualizações são incrementais, e apenas a nova informação é actualizada, reduzindo drasticamente o tempo de transferência e a necessidade de uso de banda larga. O tamanho típico de uma actualização é aproximadamente 20-80kb, enquanto que a actualização total de um programa é 200-500kb.

O ADN suporta a distribuição de um ou mais "servidores espelho" – máquinas em redes locais que funcionam como armazenamento para a informação de actualização e que são automaticamente sincronizadas com o nosso sistema de servidores de internet. Depois os nós individuais na rede fazem o download da informação a partir dos espelhos. Podem haver vários espelhos e estes podem ser dispostos de modo a funcionar hierarquicamente (em árvore).

Uma das características especiais do avast! são as actualizações PUSH. Num cenário PUSH as actualizações são iniciadas directamente pelos nossos servidores (sem polling); isto resulta da resposta rápida dos espelhos e da execução rápida da sincronização necessária. O sistema usa o protocolo SMTP/POP3 como camada de transporte (i.e. como um email normal). O sistema desta tecnologia é protegido por cifras assimétricas e é resistente a uso não autorizado.

### Segurança

O AMS mantém um sistema de utilizadores e de grupos de utilizadores, e dos seus direitos de acesso. Cada objecto (seja uma tarefa, um computador, uma programação, um evento, um alarme ou que quer que seja) tem uma lista de control de acesso, na qual é possível definir

quem o pode aceder e quem não pode. Isto permite aos principais administradores estreitar o que os administradores locais vêm aos objectos pelos quais eles são responsáveis, sem arriscar alterações não autorizadas nos ajustes das políticas fora das suas áreas.

Todas as comunicações entre AMS e a Consola são encriptadas pelo protocolo de standart industrial SSL para assegurar a segurança máxima. O AMS identifica-se à consola através de um certificado digital (um certificado certificado pelo administrador ou um ad hoc auto fornecido) para provar a sua confiança. Apenas depois de ser estabelecido um canal de encriptação em condições é que a informação é transferida através da rede.

### Apoio para utilizadores de portáteis

Máquinas com roaming sempre representam um grande desafio para sistemas de administração. Elas não pertencem a nenhum ramo de escritório específico, ligam-se à rede da corporação mais ou menos aleatoriamente, são de um modo geral não são endereçáveis e os seus utilizadores estão frequentemente a tentar passar as restrições impostas nas suas máquinas pelos administradores do sistema. A ADN foi desenhada desde o início com os utilizadores de portáteis em mente. A comunicação entre AMS e o cliente é sempre iniciada pelos clientes (sistema POP), superando o problema de ser não-endereçável. Assim que um portátil se liga à rede da corporação, não interessando em que escritório ou em que ramo ou nem mesmo que seja via VPN pela internet, são feitos os downloads das novas políticas e actualizações automaticamente e aplicadas, antes que uma potencial máquina que não seja segura cause algum mal. Se a rede da corporação não está disponível mas é possível o acesso à internet, as actualizações são agarradas directamente dos nossos servidores.

## Detalhes Técnicos

### Requisitos do sistema

#### AVAST! MANAGEMENT SERVER

- Windows NT 4 Service Pack 4 ou superior ou Windows 2000 SP1 ou superior ou Windows XP ou Windows Server 2003
- 128MB RAM (256-512MB recomendado)
- 200MB de espaço no disco rígido
- MQ SQL Server 2000 ou built-in

#### MSDE CONSOLA DE ADMINISTRAÇÃO

- Windows NT 4 Service Pack 4 ou superior ou Windows 2000 SP1 ou superior ou Windows XP ou Windows Server 2003
- 64MB RAM (128MB recomendado)
- 50MB de espaço no disco rígido
- Internet Explorer 4 ou superior

### SUPORTADO NAS SEGUINTE LÍNGUAS

Inglês, Japonês, Checo, Alemão, Francês, Espanhol, Português, Italiano, Holandês, Hungaro, Polaco, Russo e Eslovaco.

### PRODUTOS SUPORTADOS PARA GERÊNCIA

- avast! Professional Edition (managed version)
- avast! Server Edition (managed version)

### CAPACIDADES DE GERÊNCIA

- Instalação remota do antivirus avast!
- Reforço automático das políticas de segurança (ajustes, programações, actualizações...)
- Monitorização a tempo real da funcionalidade e actualização do avast!
- Relatório de estado de antivirus avast!
- Gerência de alarmes complexa