avast! Distributed Network Edition

avast! DataSheet

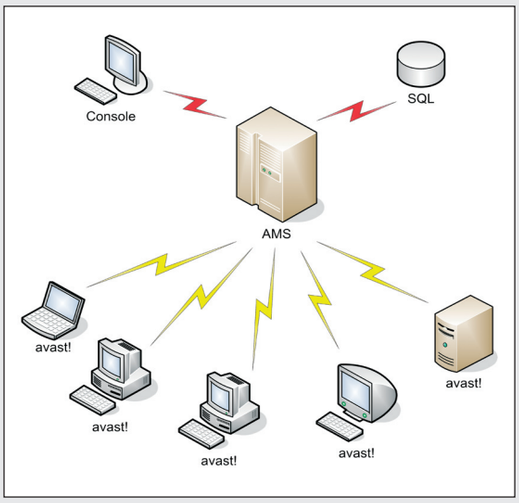
avast! Distributed Network Manager (ADNM) represents a suite of powerful tools designed to help network administrators manage the avast! antivirus product line across the whole enterprise. Its unrivaled flexibility and scalability makes it an ideal solution for networks of any size, from simple small-business networks up to large heterogenous networks spanning multiple continents. ADNM consists of the following components:

- **avast! Management Server (AMS)**
- **SQL Database**
- **Administration Console**

These three components work together with the avast! antivirus products deployed on individual workstations and servers to provide the best possible protection against malware and to minimize the effort needed to manage and monitor their current status.

How it works

The brain of the whole system is the AMS (avast! Management Server). This is where all the hard work work is done. The managed machines connect only to the AMS to download latest policies and to report their status and scan results. The Administration Console also connects directly to the AMS. The AMS is based on the SQL Database – either a dedicated MS SQL Server 2000, if available, or for small and medium-size networks its lightweight version, MSDE 2000, which is part of the ADNM installation package. For larger networks, the AMS should be installed on a dedicated computer. It is also assumed that the AMS machine can connect to the Internet via HTTP protocol.



For larger networks, it is possible to deploy multiple AMS' (each having its own database). These can then be instructed to replicate their databases on regular basis, and also upload all scanning results to a dedicated AMS on which enterprise-wide reporting can then be carried out. It is possible to choose from two communication models between AMS and the clients: PUSH or POP. The POP model is suitable especially for larger networks and for networks with roaming users. Each AMS can scale up to tens of thousands of client computers, provided they are all connected by local area network.

The following sections summarize major ADNM features and benefits.

Hierarchical policy structure

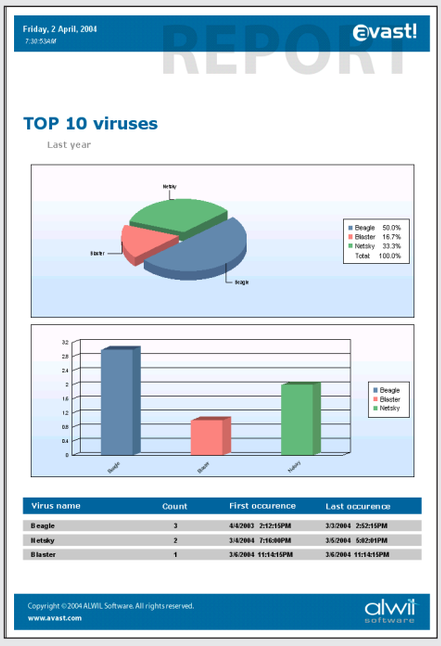
ADNM maintains the list of managed computers in a tree structure. The key to effective management is to design and organize this structure to suit administration needs. It is often ideal to build the tree so that it reflects the actual geographical and organizational structure of the network. In this way, it is also possible to assign various administration access rights and policies in a natural way since most organizations' structure can be characterized by a tree with headquarters in the root and branch offices underneath. The tree can either be built automatically, or can be imported from an external source (in the form of text file). All security policies in the tree are by default inheritied from parents to children but can be overriden (redefined) according to specific requirements.

Discovery and remote deployment

ADNM supports unattended, remote deployment of the avast! installation packages across the network, even spanning multiple domains. This is especially useful for initial product roll out. ADNM also supports periodic discovery of new machines on the network. These two technologies (discovery and remote deployment) can be combined together, resulting in constant search for new machines and automated, controllable deployment of virus protection software to these machines.

Reporting

One of ADNM's top features is its reporting capability. ADNM provides a wide range of graphical and tabular reports suitable for both regular management reporting and daily network administration. Reports can either be generated directly to the database and viewed in the Administration Console using the integrated Viewer, or can be exported to a variety of formats (including PDF, HTML and DOC) and saved to disk. They can even be automatically sent by e-mail to a designated recipient set – an especially useful feature for periodic management reporting.



ALWIL Software, Průběžná 76, 100 00 Praha 10, Czech Republic
sales@avast.com, support@avast.com
http://www.avast.com

As with any other ADNM task type, reporting tasks can be scheduled to run periodically at given intervals (daily, weekly etc.).

Alerting

With the help of the avast! Notification Manager, the ADNM allows the network administrators to set up very powerful alerting mechanisms. Supported are a number of notification objects, such as sending e-mail messages using SMTP or MAPI (Outlook), notification using the Windows popup mechanism (network message), printing the message on a network printer, SNMP traps, or even sending IM messages using MSN/ Windows Messenger.

Automatic Updates

Fast, automatic updates are one of the key points of effective virus protection. With avast, the updates are incremental, and only new data is downloaded, thus dramatically reducing transfer time and bandwidth requirements. Typical size of a virus database update is approximately of 20-80kb, a program update usually has approximately 200-500kb.

ADNM supports deployment of one or more "mirror servers" – local networked machines that act as storage for the update data, and that are automatically synchronized with our system of Internet servers. The individual nodes in the network then download the data from the mirrors. There can be any number of mirrors and these can also be set up to work in a hierarchical (tree) structure.

Another special feature of avast! is the PUSH updates. In the PUSH scenario, the updates are initialized directly by our servers (without polling); they result in the mirror servers quickly responding and performing the necessary synchronization. The system uses the SMTP/ POP3 protocol as transport layer (i.e. classic e-mail). The technology system is protected by asymmetric ciphers and are resistant to unauthorized use.

Security

The AMS maintains a system of users and user groups, and their access rights. Each object (be it a task, computer, schedule, event, alerting object or anything else) has an access control list, in which it is possible to set up who can access it and who can't. This allows the main administrators to narrow down the view of local administrators only to the objects they're responsible for, without risking any unauthorized changes in the policy settings outside their scope.

All communication between AMS and the console is encrypted by the industry-standard SSL protocol to ensure maximum security. The AMS identifies itself to the console by a digital certificate (either an administrator-supplied certificate or an ad hoc self-signed one) to prove its trustworthiness. Only after a proper encryption channel is established will credential data be transferred over the network.

Support for notebook users

Roaming machines always represent a great challenge for management systems. They belong to no specific branch office, they connect to the corporate network more or less randomly, they are general not directly addressable and their users are often trying to bypass restrictions set up on their machines by system administrators. ADNM was designed from the very beginning with notebook users in mind. Communication between AMS and the clients is always initiated by the clients (POP system), overcoming the 'not-addressable issue'. As soon as a notebook connects to the corporate network, no matter in which branch office, or even if it is via VPN over the Internet, new policies and updates are automatically downloaded, and applied, before the potentialy unsafe machine can cause any harm. If the corporate network is unavailable but it's still possible to access the Internet, the updates are grabbed directly from our Internet servers.

Technical Details

System Requirements

AVAST! MANAGEMENT SERVER

- Windows NT 4 Service Pack 4 or higher or Windows 2000 SP1 or higher or Windows XP or Windows Server 2003
- 128MB RAM (256-512MB recommended)
- 200MB hard disk space
- MQ SQL Server 2000 or built-in MSDE

ADMINISTRATION CONSOLE

- Windows NT 4 Service Pack 4 or higher or Windows 2000 SP1 or higher or Windows XP or Windows Server 2003
- 64MB RAM (128MB recommended)
- 50MB hard disk space
- Internet Explorer 4 or higher

LANGUAGES SUPPORTED

English, Japanese, Czech, German, French, Spanish, Portuguese, Italian, Dutch, Hungarian, Polish, Russian, Korean, Turkish and Slovak

SUPPORTED PRODUCTS FOR MANAGEMENT

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

MANAGEMENT CAPABILITIES

- remote installation of avast! antivirus
- automatic enforcement of security policies (settings, schedules, updates...)
- real-time monitoring of avast! functionality and updating
- status reporting of avast! antivirus
- complex alerting management

avast! is registered trademark of ALWIL Software. Microsoft and Windows are registered trademarks of Microsoft Corporation. Sun and Solaris are trademarks of Sun Microsystems, Inc. Red Hat is a registered trademark of Red Hat, Inc. Linux is a registered trademark of Linus Torvalds. All other brands and products are trademarks of their respective holder/s. Copyright © 2005 ALWIL Software. All product information is subject to change without notice.

ALWIL Software, Průběžná 76, 100 00 Praha 10, Czech Republic
sales@avast.com, support@avast.com
http://www.avast.com