

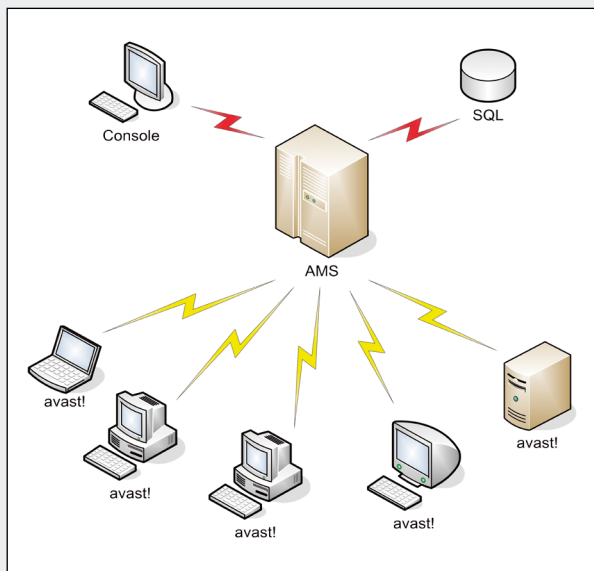
avast! Distributed Network Manager (ADNM) är en serie kraftfulla verktyg för att hjälpa nätverksadministratörer att hantera produktsortimentet avast! viruskydd över hela företaget. Dess flexibilitet och skalbarhet saknar motstycke och gör det till en idealisk lösning för nätverk i alla storlekar, från enkla småföretagsnätverk till stora heterogena nätverk som täcker flera kontinenter. ADNM består av följande delar:

- avast! Management Server (AMS)
- SQL-databas
- Administrationskonsol

De tre delarna samarbetar med avast! viruskyddprodukter som utvecklats på individuella arbetsstationer och servrar för att ge bästa möjliga skydd mot malware och minimera den insats som krävs för att hantera och övervaka deras aktuella status.

## Hur det fungerar

Hjärnan i hela systemet är AMS (avast! Management Server). Det är här det svåra jobbet utförs. De hanterade maskinerna ansluter endast till AMS för att ladda ner de senaste policyerna och rapportera status och resultat av genomsökningen. Administrationskonsolen ansluter också direkt till AMS. AMS:en är baserad på SQL-databasen - antingen en dedicerad MS SQL-server 2000, om det finns tillgängligt, eller för små och medelstora nätverk lättviktsversionen, MSDE 2000, som är en del av ADNM:s installationspaket. För större nätverk bör AMS:en installeras på en dedikerad dator. Det förutsätts också att AMS-maskinen kan ansluta till internet via http-protokoll.



För större nätverk går det att utveckla flera AMS:er (där var och en har en egen databas). De kan sedan få instruktioner om att kopiera sina databaser regelbundet, och även ladda upp alla sökningsresultat till en dedicerad AMS på vilken rapporter från hela företaget kan utföras. Det går att välja två kommunikationsmodeller mellan AMS och klienterna: PUSH eller POP. POP-modellen är särskilt lämplig för större nätverk och för nätverk med rörliga användare. Varje AMS kan ha upp till tiotusentals klientdatorer, förutsatt att alla är anslutna genom ett lokalt nätverk.

Följande avsnitt sammanfattar de viktigaste egenskaperna och fördelarna med ADNM.

## Hierarkisk policystruktur

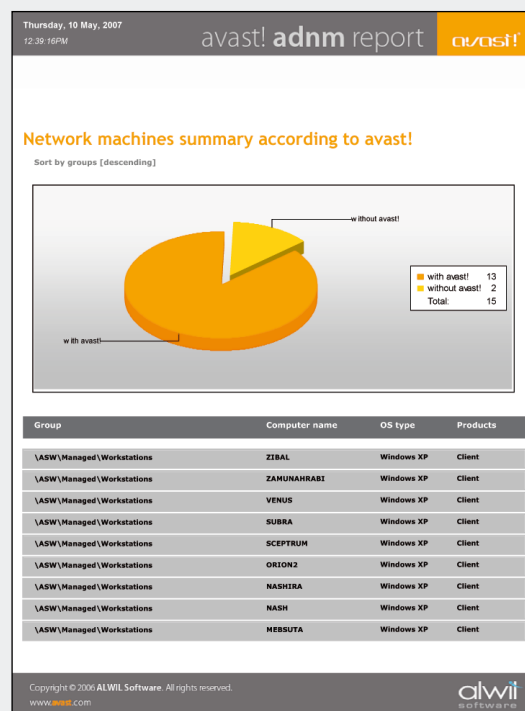
ADNM behåller listan över hanterade datorer i en trädstruktur. Nyckeln till effektiv hantering är att utforma och organisera denna struktur för att passa administratörens behov. Det idealiska är ofta att bygga trädets så att det reflekterar nätverkets faktiska geografiska och organisationella struktur. På det sättet är det också möjligt att tilldela olika administrationsrättigheter och policyer naturligt eftersom de flesta organisationers struktur kan beskrivas som ett träd där huvudkvarteret är vid roten och filialerna undertill. Trädet kan antingen byggas automatiskt eller importeras från en extern källa (i form av en textfil). Alla säkerhetspolicyer i trädet är förvalda som att ärvas från överordnad till underordnad, men kan skrivas över (omdefinieras) enligt särskilda krav.

## Upptäckt och fjärraktivering

ADNM stöder oönskad fjärraktivering av avast! installationspaket över nätverket, och kan till och med spänna över flera domäner. Det är särskilt användbart för en första produktstart. ADNM stöder också periodisk upptäckt av nya maskiner i nätverket. Dessa två teknologier (upptäckt och fjärraktivering) kan kombineras, vilket resulterar i konstant sökande efter nya maskiner och automatisk kontrollerbar aktivering av viruskyddmjukvara till dessa maskiner.

## Rapportering

En av ADNM:s bästa egenskaper är rapporteringskapaciteten. ADNM erbjuder ett stort omfång rapporter, grafiska och i tabellform, som passar både vanlig hanteringsrapportering och daglig nätverksadministration. Rapporterna kan antingen skapas direkt till databasen och ses i administrationskonsolen med den inbyggda Viewern, eller exporteras till flera olika format (som PDF, HTML och DOC) och sparas till hårddisken. De kan till och med skickas automatiskt med e-post till en tilldelad mottagare - en särskilt användbar egenskap för periodisk hanteringsrapportering.



Precis som med alla andra typer av ADNM-uppgifter kan rapporteringarna schemaläggas för att köras periodiskt på givna intervall (varje dag, varje vecka osv).

## Varningar

Med hjälp av avast! Notification Manager tillåter ADNM nätverkets administratörer att ställa in mycket kraftfulla varningsmekanismer. Det finns ett antal meddelandeobjekt som stöds, såsom att skicka e-post med SMTP eller MAPI (Outlook), meddelande med Windows popup-mekanism (nätverksmeddelande), att skriva ut meddelandet på en nätverkskrivare, SNMP-fällor, eller till och med att skicka IM-meddelanden med MSN/Windows Messenger.

## Automatiska uppdateringar

Snabba, automatiska uppdateringar är en av de viktigaste delarna i effektivt viruskydd. Med avast är uppdateringarna inkrementella, och endast ny data laddas ner, vilket minskar överföringstiden och bandbreddskraven dramatiskt. En uppdatering av virusdatabasen är typiskt ungefär 20-80 kb, en programuppdatering vanligtvis ungefär 200-500 kb.

ADNM stöder utveckling av en eller fler "spegelservrar" - maskiner i lokala nätverk som agerar förvaring för uppdateringsdata, och som automatiskt synkroniseras med vårt system av internetserverar. De individuella noderna i nätverket laddar sedan ner data från speglarna. Det kan finnas ett valfritt antal speglar och dessa kan också ställas in för att fungera i en hierarkisk (träd-) struktur.

En annan specialfunktion i avast! är PUSH-uppdateringar. I PUSH-scenariot börjar uppdateringarna direkt av våra servrar (utan polling); de gör så att spegelservrarna snabbt svarar och utför den nödvändiga synkroniseringen. Systemet använder SMTP/POP3-protokoll som transportlager (dvs. klassisk e-post). Teknologisystemet skyddas av asymmetriska chiffer och står emot oauktorerad användning.

## Säkerhet

AMS:en behåller ett system av användare och användargrupper, och deras tillgångsrättigheter. Varje objekt (uppgift, dator, schema, händelse, varningsobjekt eller något annat) har en tillgångskontrolllista där det går att ställa in vem som får tillgång och inte. Det gör att huvudadministratörerna kan begränsa de lokala administratörernas granskning till endast de objekt de är ansvariga för, utan att riskera oauktorerade ändringar i policyinställningar utanför deras arbetsområde.

All kommunikation mellan AMS och konsolen är krypterad av industristandarden SSL-protokoll för att garantera maximal säkerhet. AMS:en identifierar sig för konsolen genom ett siffercertifikat (antingen ett certifikat som administratören ordnat eller ett ad hoc-självsignerat) för att visa sin pålitlighet. Först när rätt krypteringskanal är etablerad överförs data över nätverket.

## Stöd för Notebook-användare

Rörliga maskiner är alltid en stor utmaning för hanteringssystem. De tillhör ingen särskild filial, ansluter mer eller mindre slumpmässigt till företagets nätverk, är i allmänhet inte direkt åtkomliga och deras användare försöker ofta kringgå begränsningar som är inställda på maskinerna av systemadministratören. ADNM utformades redan från början med tanke på användare av bärbara datorer. Kommunikation mellan AMS och klienterna startas alltid av klienterna (POP-system), vilket överbygger "not-addressable"-problemet.

Så snart en bärbar dator ansluter till företagets nätverk, oavsett i vilken filial, eller till och med om det är via VPN eller över internet, laddas nya policyer och uppdateringar ner, och appliceras, innan den potentiellt osäkra datorn kan orsaka skada. Om företagets nätverk är otillgänglig men det fortfarande går att komma ut på internet tas uppdateringarna direkt från våra internetserverar.

## Tekniska detaljer

### Systemkrav

#### avast! MANAGEMENT SERVER

- Windows NT 4 Service Pack 4 eller senare eller Windows 2000 SP1 eller senare eller Windows XP eller Windows Server 2003
- 128MB RAM (256-512MB rekommenderas)
- 200MB hårddiskutrymme
- MQ SQL-server 2000 eller inbyggd MSDE

#### ADMINISTRATIONSKONSOL

- Windows NT 4 Service Pack 4 eller senare eller Windows 2000 SP1 eller senare eller Windows XP eller Windows Server 2003
- 64MB RAM (128MB rekommenderas)
- 50MB hårddiskutrymme
- Internet Explorer 4 eller senare

### SPRÅK SOM STÖDS

Engelska, japanska, tjeckiska, tyska, franska, spanska, portugisiska, italienska, nederländska, ungerska, polska, ryska, koreanska, turkiska och slovakiska

### PRODUKTER SOM STÖDS FÖR HANTERING

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

### HANTERINGSMÖJLIGHETER

- fjärrinstallation av avast! viruskydd
- automatisk förstärkning av säkerhetspolicyer (inställningar, scheman, uppdateringar...)
- realtidsövervakning av avast!-funktion och uppdatering
- statusrapportering för avast! viruskydd
- komplex varningshantering