

*VMware Assured Computer Environment biedt veiligheid via sandbox-methode*

## Virtuele omgeving voor netwerkbezoekers

Het aantal zogenaamde *unmanaged pc's* of laptops die toegang hebben tot enterprise-applicaties en -data neemt voortdurend toe. Deze machines brengen een verhoogd veiligheidsrisico voor elke bedrijfsomgeving met zich mee. De Assured Computer Environment (ACE) van VMware maakt het mogelijk om gebruikers in een afgeschermd, virtuele omgeving te laten werken. Een bespreking van het product.

**Bram Dons**

Met name de zogenaamde *guest workers*, die via een remote verbinding toegang hebben tot een enterprise-omgeving, vormen een belangrijke risicobron. De *unmanaged pc's* waar zij op werken (zogenaamde *pc endpoints*), zijn vaak niet het eigendom van de onderneming zelf of worden niet onderhouden door het IT-beheer van de onderneming waarvan ze op het netwerk worden aangesloten. In de afgelopen jaren zijn er verschillende typen *guest workers* ontstaan. Er zijn gebruikers die regelmatig op kantoor en thuis werken, en daarvoor van dezelfde laptop gebruikmaken (vaak ook nog voor privédoeleinden), maar er zijn er ook die onder contract werken bij een onderneming en die daarvoor hun eigen laptop gebruiken voor verbinding met het enterprisenetwerk. Dan zijn er nog gebruikers die meestal op kantoor werken maar soms hun laptop 's avonds, in het weekend of wanneer ze op reis gaan (privé of zakelijk) mee naar huis nemen.

### **Het gevaar van unmanaged pc's**

*Guest workers* zijn met hun pc of laptop niet altijd rechtstreeks op het beveiligde bedrijfsnetwerk aangesloten maar – zowel binnen als buiten werktijden – vaak vanaf een remote locatie. Deze manier van werken houdt bepaalde

beveiligingsrisico's in. Voor beveiliging van het netwerk maken ondernemingen in het algemeen gebruik van een Virtual Private Network (VPN), of de een of andere terminal service die een veilige remote toegang tot het bedrijfsnetwerk moet garanderen. Maar, alhoewel VPN en terminal services een redelijk veilige verbinding bieden, brengt dit type verbinding (net zoals trouwens iedere andere remote verbinding) toch bepaalde beveiligingsrisico's met zich mee. We schetsen een paar veel voorkomende beveiligingsproblemen die *guest workers* met zich meebrengen.

Wanneer het *guest system* zich buiten de bedrijfsfirewall bevindt en via breedband, modem of draadloos is verbonden met het bedrijfsnetwerk (al of niet via VPN), dan is het mogelijk dat hackers zich toegang kunnen verschaffen tot bedrijfskritische informatie. De op een laptop aanwezige vertrouwelijke gegevens zijn ook kwetsbaar wanneer de laptop zich buiten de firewall bevindt en als deze wordt gestolen. Binnen het bedrijfsnetwerk kunnen voorgeschreven IT-policy's worden afgedwongen, bijvoorbeeld het gebruik van webbrowsers en/of wel of niet toestaan om software van internet te downloaden. Wanneer pc's of laptops

(in het bijzonder die van externe medewerkers) echter buiten het bedrijfsnetwerk worden aangesloten, is het moeilijk om bepaalde policy's af te dwingen en controleren. Kortom, unmanaged pc's en laptops leveren (nog afgezien van de hogere onderhoudskosten) een sterk verhoogd veiligheidsrisico op voor elke bedrijfsomgeving. Altijd is het gevaar aanwezig dat een remote gebruiker zich ongeoorloofde toegang kan verschaffen tot vertrouwelijke gegevens die binnen ondernemingen en organisaties zijn opgeslagen of een hacker ongemerkt inbreekt op een online remote verbinding.

We moeten dus op zoek naar een oplossing om dergelijke gevaren te minimaliseren, met andere woorden om de remote gebruikers te dwingen vanaf een voorgeschreven, afgeschermd, virtuele pc-omgeving gebruik te maken van de eigen pc of laptop. Een dergelijke virtuele omgeving wordt geboden door het product Assured Computer Environment van VMware (ACE; zie figuur 1).

### Wat biedt ACE?

Ondernemingen zijn vaak niet in staat om alle instellingen en policy's van remote computers te beheren die toegang hebben tot het bedrijfsnetwerk. Met ACE kan het IT-beheer worden verlengd tot remote systemen waarmee een standaard, op policy's gebaseerde pc-omgeving voor remote gebruikers kan worden gecreëerd. Het ACE-softwarepak-

ket van VMware biedt IT-beheerders de mogelijkheid om een door hen beheerde en gedefinieerde virtuele pc-omgeving te creëren. Deze veilige omgeving, verpakt in een virtual machine (VM), maakt het mogelijk om een tot dusver unmanaged fysieke pc op een veilige manier binnen de beheeromgeving van de enterprise op te nemen.

In de praktijk kunnen gebruikers standaard-pc-applicaties zonder aanpassing op hun remote laptop of pc draaien en via standaardnetwerkprotocollen verbinding maken met het bedrijfsnetwerk. Belangrijk is dat, of de gebruikers nu wel of niet met het bedrijfsnetwerk zijn verbonden, toch de geldende IT-bedrijfspolicy's kunnen worden afgedwongen (zoals authenticatie en toegang tot devices en netwerken). Bovendien hebben IT-beheerders de mogelijkheid om pc endpoints te vergrendelen en daardoor bedrijfskritische (data)bronnen te beschermen tegen de risico's van unmanaged pc's en laptops.

Kortom, toepassing van ACE geeft de IT-beheerder de complete controle over de aanwezige hardware en netwerkinterfaces van een unmanaged pc en transformeert deze naar een pc endpoint dat voldoet aan de door de onderneming gestelde beveiligingspolicy's voor zowel interne als guest enterprisegebruikers. ACE biedt de mogelijkheid om verschillende soorten beveiligde virtuele pc-omgevingen, al of niet gelijktijdig, op

een enkele fysieke pc of laptop te laten draaien.

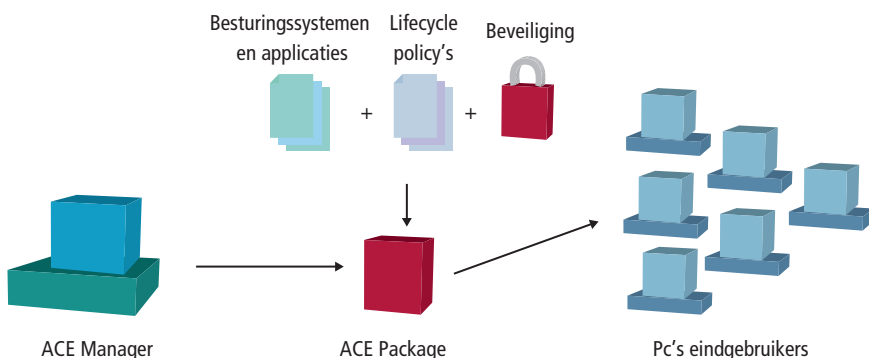
### Beveiliging van bedrijfsgegevens

Met ACE wordt een VM gecreëerd die de gegevens op de remote pc of laptop beschermt door middel van encryptie en die gecontroleerde toegang via wachtwoorden en directory serviceauthenticatie biedt. Op een door de beheerder in te stellen einddatum is een VM weer uit te schakelen, zodat men bijvoorbeeld de toegang van guest workers tot een bedrijfsnetwerk kan beperken tot de lengte van het contract. Bepaalde restricties zijn aan te brengen voor de toegang van VM's of hosts tot netwerken. Zo kan men bijvoorbeeld afdwingen dat alleen een VM via een VPN-server toegang heeft tot het bedrijfsnetwerk en alle andere hosts geblokkeerd worden. Ook is de toegang die een VM heeft tot lokale devices op de pc of laptop (cd-rom/dvd, floppy of usb-apparaten) te blokkeren, zodat remote guests geen kopieën kunnen maken van bedrijfsgegevens naar de eigen opslagapparatuur.

### Implementatie

Voor de installatie van de ACE Manager van VMware is een standaard-pc nodig (500 MHz of sneller) en genoeg geheugen om elk hostbesturingssysteem en bijbehorende applicaties daarop te kunnen laten draaien. De basisinstallatie vraagt 150 Mb diskruimte en voor elk guestbesturingssysteem nog eens 1Gb extra. Als hostbesturingssysteem kan een Windows Server 2003/XP/2000-systeem dienen (zie figuur 2). Met behulp van de ACE Manager zijn een of meer VM's voor een laptop of pc te creëren en installeren. Dit gebeurt in drie stappen: de creatie van een 'project', de toevoeging van een of meer virtual machines en het definiëren van de bijbehorende policy's.

Vanuit de ACE Manager creëert men een 'New Project' en geeft men aan waar de diverse bestanden (project-, virtual machine- en packagebestanden) worden opgeslagen. Daarbij wordt automatisch



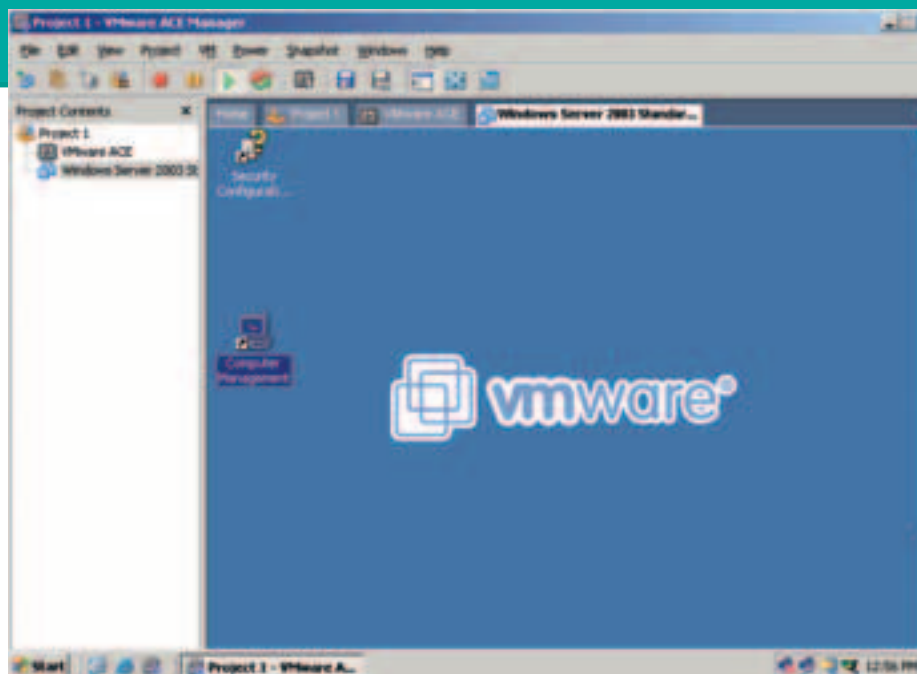
Figuur 1 ACE-omgeving

# security

de ACE-applicatie toegevoegd, die eindgebruikers nodig hebben om de VM op de remote laptop of pc te kunnen draaien. Daarna voegt men een VM toe, waarbij men in de meeste gevallen de defaultwaarden accepteert. Als netwerktype kiest men 'bridging networking', waarbij de 'host quarantine'-regels van toepassing zijn. Kiest men voor 'NAT', dan gelden alle netwerkbeperkingen van de remote pc ook voor de VM. Als laatste moeten de 'Policies' voor de zojuist aangemaakte VM worden gedefinieerd.

## VM policy rules

Policy rules vormen een belangrijke component binnen ACE, omdat ze nauwkeurig aangeven tot welke bronnen de remote gebruiker toegang heeft in het bedrijfsnetwerk. Het aanbrengen van VM-policy's biedt de systeembeheerder de mogelijkheid om restricties aan te brengen die de gebruikersbevoegdheden specificeren, op basis waarvan de remote gebruiker toegang heeft tot bepaalde data op het bedrijfsnetwerk. Met behulp van encryptie-en-authenticatie-



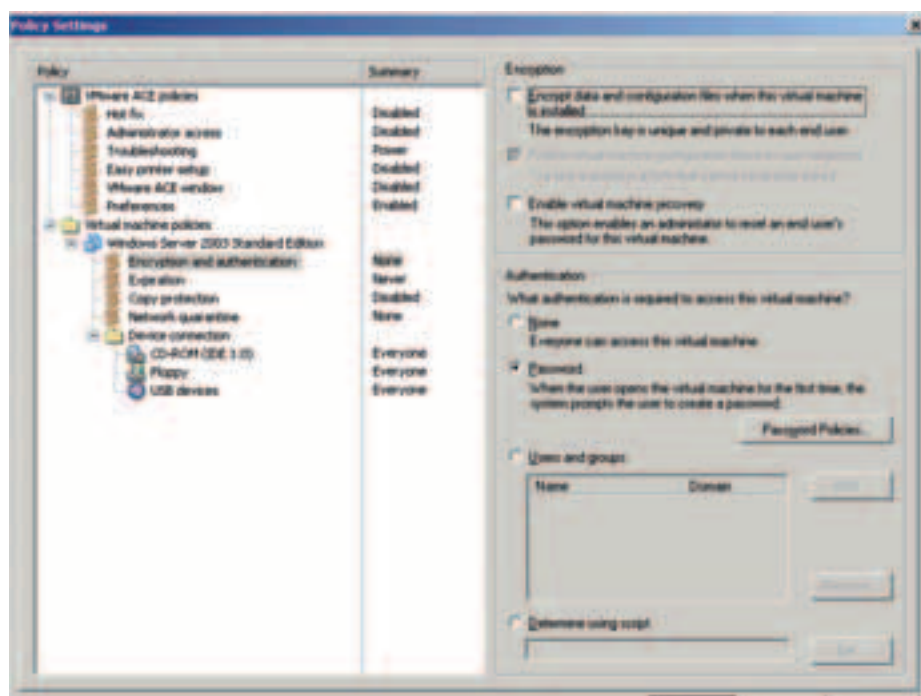
Figuur 2 VMware Windows Server 2003

tiepolicy's kan de beheerder specificeren welke remote gebruiker toegang tot de VM heeft op een guest pc of laptop (zie figuur 3). Bij installatie van de VM kan de beheerder ervoor kiezen om alle VM-bestanden te versleutelen, inclusief de configuratie- en VM-diskbestanden. Hierbij wordt voor elke pc een andere sleutel gebruikt. De versleuteling is transparant voor de eindgebruiker van de VM, de ACE-applicatie handelt zelf alle encryptie- en decryptie binnen de VM af.

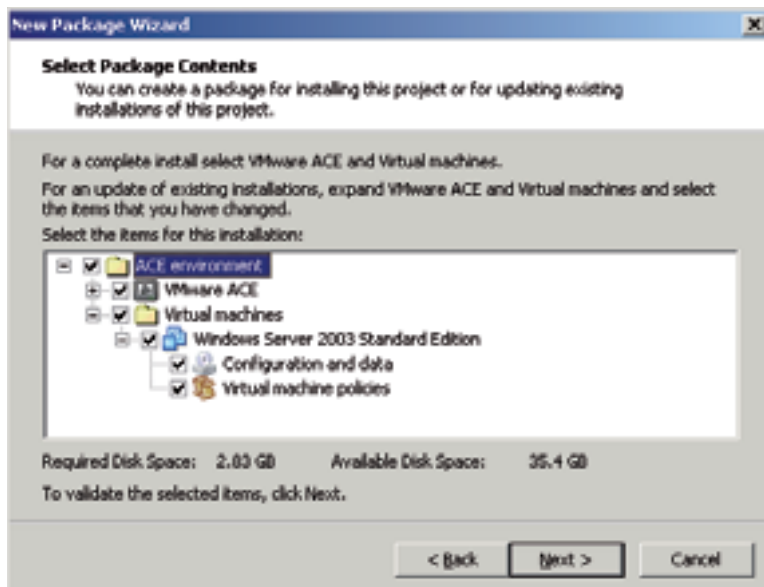
Bij iedere toegang tot de interne harde schijf op de pc of laptop worden de VM-bestanden automatisch versleuteld.

Een VM bestaat uit software die als bestanden op de pc aanwezig is. Het is dan ook eenvoudig om de bestanden in een *package* te verpakken en als een VM-pakket op meerdere fysieke systemen te installeren. Tegelijkertijd biedt het een niet-geautoriseerde persoon de mogelijkheid om de VM naar een andere locatie te kopiëren. Om dit te voorkomen biedt ACE ook een *copy-protection policy*, die de garantie geeft dat de VM alleen kan draaien vanuit de locatie waar de ACE Installer is geïnstalleerd. Het blijft natuurlijk nog steeds mogelijk om VM-bestanden naar een andere locatie te kopiëren, maar vanaf die plaats kunnen ze dan niet gedraaid worden.

*Network quarantine policy's* stellen de beheerder in staat om de netwerktoegang vanuit een VM tot het bedrijfsnetwerk gedetailleerd in te stellen. De netwerkquarantaine van ACE maakt gebruik van een firewall, om te kunnen afdwingen en specificeren tot welke systemen of subnetten een VM toegang heeft. Standaard heeft een VM onbeperkte netwerktoegang - niet bepaald een veilige default-instelling! Het aanbrengen van restricties (zoals het toestaan van algemene toegang met uitzondering van bepaalde systemen en subnetten) moet via de 'Network Quarantine Wizard'



Figuur 3 Encryptie-en-authenticatiemenu



**Figuur 4** Package aanmaken in de New Package Wizard

worden ingesteld. Daarin valt te kiezen uit 'static', 'dynamic', 'version-based' en 'custom quarantine using script'. Bij de static-instelling wordt de toegangslijst als onderdeel van de package op de VM opgeslagen. Bij de dynamische instelling bevindt zich de lijst op de server die periodiek door de VM wordt opgevraagd. Met de version-based quarantainemethode zijn twee verschillende policy's te creëren, 'normal' of 'restricted', afhankelijk van de versie van de VM die men draait (meest recent of niet). Dezelfde twee mogelijkheden gelden voor de custom quarantine using scriptmethode, waarbij de keuze afhankelijk is van de 'patch state' van de VM. Ten slotte, een gebruiker die om een bepaalde reden (wachtwoord vergeten, geldigheidsduur toegang verstreken, trachten een copy-protected VM vanaf een andere locatie te draaien) geen toegang meer heeft tot de VM, kan een *hot fix* aanvragen.

#### Packaging en installatie

Is men tevreden met alle ingestelde policy's en andere aspecten van het project, dan kan met de ACE Manager een VM package worden aangemaakt (zie figuur 4). Men kan een package lokaal, binnen een netwerk-share opslaan of deze op

een cd of dvd branden. Nadat men een VM package heeft gecreëerd, moet deze op de guest pc of laptop worden geïnstalleerd. Dit gebeurt op dezelfde manier als bij elke andere applicatie: vanaf een locatie binnen het netwerk of via een of meer cd's of dvd's. De VM is daarna als applicatie op te starten. Naar wens is de host zodanig te configureren dat alleen de VM wordt opgestart, waarbij in het Windowsregister de VM als gebruikers-*shell* wordt geconfigureerd, in plaats van standaard de Windows Explorer.

#### Beheer VM

Een belangrijk verschil met andere toepassingen voor remote toegang is dat ACE in de VM de policy's in relatie tot de VPN-server aanbrengt, en niet de op remote pc of laptop zelf. De VPN-server bepaalt nog steeds de policy's waarmee de remote gebruiker toegang heeft. Voor het beheer van de VM definieert men policy's in ACE die betrekking hebben op verschillende aspecten van de VM, waaronder netwerkquarantaine, encryptie en toegang tot devices. De network quarantine policy brengt beperkingen aan in de toegang van de VM tot de VPN-server. Aan de andere kant ken de host-pc waarop de VM draait, deze beperkingen niet.

Naast de toegangspolicy's maakt het beheer van updates en patches een essentieel onderdeel uit van elke IT-omgeving die gebruikmaakt van remote toegang. Deze vorm van beheer heeft betrekking op zaken als antivirus-updates en de verzekering dat gebruikers de recentste versie van applicaties op hun remote pc's gebruiken. Daartoe biedt ACE twee methodes: 'version-based' en 'custom quarantine'. Versiegebaseerde quarantaine werkt samen met een patch managementsysteem. Het maakt gebruik van een sequentiële lijst van versienummers, waarvan elk nummer correspondeert met een lijst in de netwerk policy. Dat wil zeggen: elke keer dat er een update vanuit het patch management beschikbaar komt, wordt een nieuwe versie in de policy list aangemaakt samen met de benodigde stappen om deze te implementeren. ACE ondersteunt dus zelf geen patch managementoplossing, maar is wel eenvoudig te integreren met andere beheertools, waaronder Altiris, Landesk, Microsoft SMS of een eigen beheertool.

#### Conclusie

De toepassingen van Assured Computer Environment bieden een complete en veilig afgeschermd omgeving voor remote gebruikers. Beveiliging en beheer van zo'n omgeving kunnen vanuit een centraal systeem worden geregeld. Het is een ideale oplossing voor gasten op het netwerk, omdat het onafhankelijk van de remote hardware kan worden toegepast. De remote omgeving is volledig naar de wensen van systeembeheerder in te stellen, waarbij zelfs de toegang tot de lokale hardware kan worden afgesloten. In tegenstelling tot de doorgaans toegepaste directe inbel- of internetverbinding met de VPN-server garandeert deze *sandbox*methode een veilige toegang van remote gebruikers tot het bedrijfsnetwerk.

*Bram Dons is onafhankelijk IT-analist.  
b.dons@it-trendwatch.nl.*