

VMware ACE

Assured Computing Environment für den unternehmensweiten Einsatz

Was ist VMware ACE?

Auf Unternehmensanwendungen und vertrauliche Daten wird von einer immer größeren Anzahl von nicht verwalteten PCs zugegriffen, die von Auftragnehmern, Telearbeitern und Partnern verwendet werden. Nicht verwaltete PCs sind nicht Eigentum der IT-Abteilung und werden von den IT-Mitarbeitern nicht verwaltet, sodass diese PCs erhöhte Kosten und Sicherheitsrisiken darstellen.

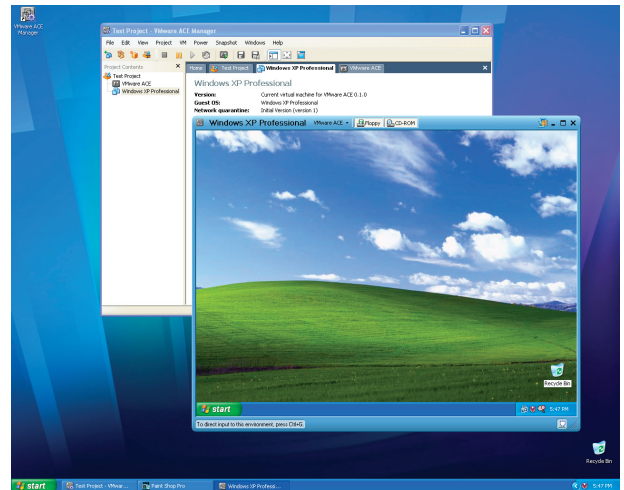
Sicherheitsadministratoren können dank VMware® ACE PC-Endpunkte sperren und wichtige Unternehmensressourcen vor den durch nicht verwaltete PCs vorhandenen Risiken schützen. Mit VMware ACE können Sicherheitsadministratoren einen von der IT-Abteilung verwalteten PC in einen sicheren virtuellen Computer integrieren und diesen PC für einen nicht verwalteten, physischen PC bereitstellen. VMware ACE bietet ab dem Installationszeitpunkt einen geschützten und mit IT-Bestimmungen kompatiblen PC-Endpunkt, der den sicheren Zugriff auf IT-Ressourcen ermöglicht.

Mit VMware ACE ist aufgrund der Transformation eines nicht verwalteten PCs in einen IT-kompatiblen PC-Endpunkt die vollständige Kontrolle der Hardwarekonfiguration und der Netzwerkfunktionen eines nicht verwalteten PCs möglich. Diese einzigartige Möglichkeit zur Verbesserung der Endpunkt-Sicherheit kann intern, remote, mit und ohne Verbindung mit dem vertrauenswürdigen Netzwerk verwendet werden. Mit VMware ACE wird die Sicherheit erhöht und die Kosten zum Einführen nicht verwalteter PCs zum Zugriff auf IT-Ressourcen gesenkt.

Wie wird VMware ACE im Unternehmen eingesetzt?

VMware ACE wird von Sicherheitsadministratoren für folgende Aufgaben eingesetzt:

- Bereitstellen geschützter, von der IT-Abteilung verwalteter Endpunkte auf nicht verwalteten PCs.
- Schützen vertraulicher Daten auf Endpunkt-PCs.
- Ausführen mehrerer sicherer PC-Umgebungen auf einem einzelnen PC.



Wie funktioniert VMware ACE?

Sicherheitsadministratoren erstellen mit VMware ACE Manager MSI-kompatible Bereitstellungspakete mit folgenden Inhalten:

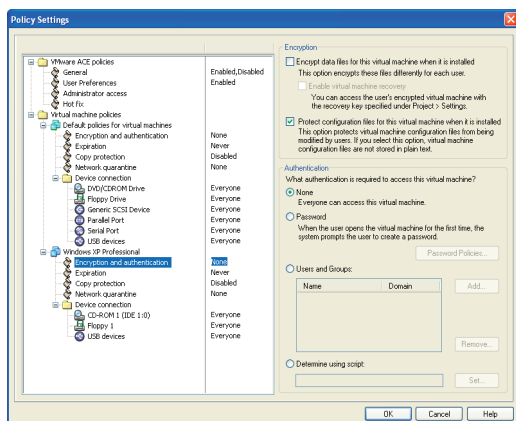
- Mindestens ein eigenständiger virtueller Computer mit einem Betriebssystem, Unternehmens- und Sicherheitsanwendungen sowie Daten
- Sicherheitsrichtlinien zur Kontrolle von Verschlüsselung, Authentifizierung, Ablauf, Kopierschutz, Netzwerkzugriff und Gerätezugriff für den/die virtuellen Computer

Sicherheitsadministratoren verteilen das VMware ACE-Paket dann mittels direkten Download, Bereitstellungs-Tools oder DVD-/CD-Medien an die Endanwender. Endanwender installieren dieses Paket zur Erstellung eines geschützten und von der IT-Abteilung verwalteten Endpunkts.

Mit VMware ACE Virtual Rights Management (VRM) wird die Verwaltung von auf virtuellen VMware-Computern angewendeten Sicherheitsrichtlinien und Zugriffsrechten zentralisiert, sodass Lebenszyklen für PC-Umgebungen kontrolliert und die Kompatibilität von Endpunkten mit IT-Richtlinien gewährleistet werden können.

„Dank VMware ACE können wir einem Mitarbeiter, der zuhause arbeitet, oder einem Auftragnehmer, der vorübergehend bei uns vor Ort arbeitet, einen virtuellen Computer mit einem Betriebssystem und der für die Arbeit erforderlichen Software bereitstellen. Wir können mithilfe der in das Produkt integrierten VRM-Technologie Richtlinien für die Zugriffskontrolle, Bildversionskontrolle, Bildverfall, Kopierschutz und Virenkontrolle festlegen, sodass die Daten von Baptist Healthcare System umfassend geschützt werden.“

Tom Taylor, Senior Client Server Analyst, Baptist Healthcare System



Die in VMware ACE Manager integrierte Virtual Rights Management-Technologie ermöglicht die zentralisierte Kontrolle der Sicherheitsrichtlinien für Verfall, Authentifizierung, Verschlüsselung, Netzwerkzugriff, Gerätezugriff und Kopierschutz für auf Endanwender-PCs bereitgestellte VMware ACE-Software

ZENTRALE MERKMALE

- **Zentralisierte Sicherheits- und Verwaltungsrichtlinien.** Mit Virtual Rights Management (VRM) wird die Verwaltung von Sicherheitsrichtlinien und Zugriffsrechten zentralisiert, die auf einem Endanwender-PC mit VMware ACE angewendet werden.
- **Geschützte Datenverarbeitungsumgebung.** Schutz der gesamten VMware ACE-Umgebung (einschließlich Daten und Systemkonfiguration) mit Authentifizierung und integrierter Verschlüsselung.
- **Auf Regeln basierender Netzwerkzugriff.** Ermöglichung von Endpunktkompatibilität durch Identifizierung und Isolierung abgelaufener, nicht autorisierter oder veralteter VMware ACE-Umgebungen.
- **Gerätekontrolle.** Gewähren oder Verweigern von Zugriff auf Server-PC-Geräten, beispielsweise Drucker, USB-Memory Keys oder DVD-RW/CD-RW-Geräten.
- **Digital Rights Management-(DRM-)Funktion.** Verhindern, dass Endanwender VMware ACE auf ein separates oder Wechselgeräte, auf ein Netzwerkdateisystem oder einen anderen Computer kopieren.
- **Ablaufsteuerung.** Konfigurieren von VMware ACE zum Ablauf an einem vorab definierten Zeitpunkt oder nach einem vorab festgelegten Zeitraum.
- **Einmalige Entwicklung, Bereitstellung an beliebigem Ort.** Erstellen standardisierter, hardware-unabhängiger PC-Umgebungen und Bereitstellen dieser Umgebungen für jeden Standard-PC.
- **Anpassbare Benutzeroberfläche.** Anpassung des Verhaltens und des „Look and Feel“ für Anwender.
- **Flexible Datenverarbeitungsumgebung.** Endanwender können den vorherigen Zustand ihrer Arbeitsumgebung innerhalb von Sekunden wiederherstellen. Endanwender können in der VMware ACE-Umgebung unabhängig davon arbeiten, ob eine Verbindung zum Netzwerk besteht.

Warum VMware ACE?

EINSATZSZENARIEN	VORTEILE
<p>Bereitstellen geschützter, von der IT-Abteilung verwalteter Endpunkte Schützen nicht verwalteter PCs, die von Außendienstmitarbeitern, Telearbeitern oder Auftragnehmern verwendet werden</p>	<ul style="list-style-type: none"> • Reduzieren der Anfälligkeit für Malware bei nicht verwalteten und ungeschützten Computern • Schutz der vertraulichen Daten des Unternehmens an sicheren, verschlüsselten und kopiergeschützten PC-Arbeitsplätzen • Senken der Kosten bei der Ermöglichung von Zugriff auf nicht verwaltete PCs • Keine Korrektur nicht verwalteter, physischer PCs erforderlich
<p>Schützen vertraulicher Daten auf Endpunkt-PCs Verschlüsseln und Schützen des geistigen Eigentums und persönlicher Informationen des Unternehmens</p>	<ul style="list-style-type: none"> • Zentralisierung von Sicherheits-, Kopierschutz- und Verschlüsselungs-Richtlinien mit VRM-Technologie (Virtual Rights Management) • Verringern des Risikos von Diebstählen und unbefugter Nutzung von geistigem Eigentum, urheberrechtlich geschützten digitalen Medien und persönlichen Informationen des Unternehmens
<p>Ausführen mehrerer sicherer PC-Umgebungen auf einem einzelnen PC Erstellen hardware-unabhängiger, simulierter PC-Umgebungen, die auf beliebigen PCs ausgeführt werden</p>	<ul style="list-style-type: none"> • Keine Notwendigkeit zur Verwendung mehrerer physischer PCs zur Isolation von Arbeitsumgebungen, Informationen und Netzwerkzugriff • Zentralisierung der Kontrolle von Sicherheitsrichtlinien mithilfe der VRM-Technologie

TECHNISCHE DATEN

Server-System-Anforderungen für Anwender

- PC Hardware**
- Standard-PC
 - x86-kompatibler Prozessor mit mind. 500 MHz (empfohlen; mind. 400 MHz erforderlich)
- Kompatible Prozessoren:**
- Intel®: Celeron®, Pentium® II, Pentium III, Pentium 4, Pentium M, Xeon
 - AMD: Athlon, Athlon MP, Athlon XP, Duron, Opteron
- Mehrprozessorsysteme werden unterstützt
 - Zurzeit laufen Tests für die Unterstützung der folgenden Prozessoren: AMD64 Opteron, Athlon 64 und Intel IA-32e
- Hauptspeicher**
- 256 MB empfohlen, mind. 128 MB erforderlich

Anzeige

- 16-Bit-Grafikadapter empfohlen, Grafikadapter mit mehr als 8 Bit erforderlich

Laufwerke

- 80 MB freier Speicherplatz für die Basisinstallation erforderlich
- Mindestens 1 GB freier Speicherplatz empfohlen für Gastbetriebssysteme und Anwendungen
- Unterstützung für IDE- oder SCSI-Festplatten sowie für CD-ROM- und DVD-ROM-Laufwerke

Windows-Host-Betriebssysteme

- Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition mit Service Pack 1
- Windows XP Professional und Windows XP Home Edition mit Service Pack 1 oder 2

- Windows 2000 Professional Service Pack 3 oder 4, Windows 2000 Server Service Pack 3 oder 4, Windows 2000 Advanced Server Service Pack 3 oder 4

Server-System-Anforderungen für ACE Manager

- Windows-Host-Betriebssysteme**
- Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition
 - Windows XP Professional und Windows XP Home Edition mit Service Pack 1 oder 2
 - Windows 2000 Professional Service Pack 3 oder 4, Windows 2000 Server Service Pack 3 oder 4, Windows 2000 Advanced Server Service Pack 3 oder 4

SYSTEMANFORDERUNGEN

Unter http://www.vmware.com/support/ace/doc/intro_sysreqs_ace.html finden Sie eine vollständige Liste der aktuellen Systemanforderungen.

