

VMware ACE

Безопасная вычислительная среда для предприятий



Что такое VMware ACE

Доступ к конфиденциальным данным и прикладным программам предприятия все чаще осуществляется через персональные компьютеры, пользователями которых являются контрактные работники, внешние поставщики, сотрудники, работающие из домашних офисов, и партнеры. Такие персональные компьютеры (ПК) не принадлежат отделу информационных технологий (ИТ) предприятия и не обслуживаются его сотрудниками. Это делает невозможным их администрирование в соответствии со стандартами предприятия, поэтому мы будем называть их неадминистрируемыми ПК. Использование неадминистрируемых ПК приводит к увеличению риска для безопасности предприятия и росту затрат на обслуживание парка ПК.

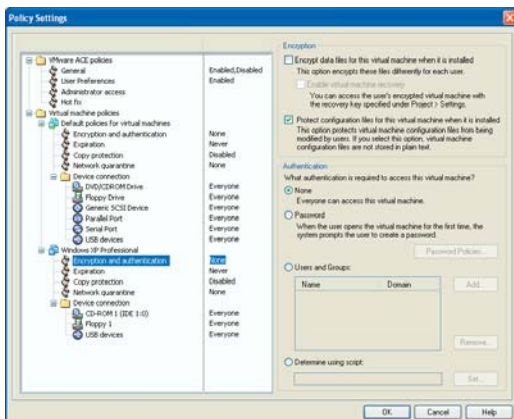
VMware® ACE позволяет администраторам по безопасности закрывать доступ с терминальных устройств и программ к критическим ресурсам компании и таким образом избежать риска, связанного с использованием неадминистрируемых ПК. Кроме этого, VMware ACE предоставит им возможность создать на базе безопасной виртуальной машины администрируемый ПК и развернуть его на физических машинах, находящихся вне зоны их воздействия. Будучи установленной на персональном компьютере, VMware ACE создает устройство доступа (терминал) к ресурсам предприятия. Созданный терминал полностью соответствует требованиям ИТ предприятия к безопасности такого доступа.

VMware ACE обеспечивает полный контроль над аппаратной конфигурацией и сетевыми функциями ПК, преобразуя его в терминальное устройство, соответствующее требованиям ИТ. Эта уникальная возможность улучшения безопасности может быть использована для локальных и удаленных терминальных устройств, для устройств, подключенных к доверительной сети предприятия или отключенных от нее. VMware ACE снижает риск безопасности и сокращает эксплуатационные затраты, возникающие из-за предоставления неадминистрируемым ПК доступа к ИТ-ресурсам предприятия.

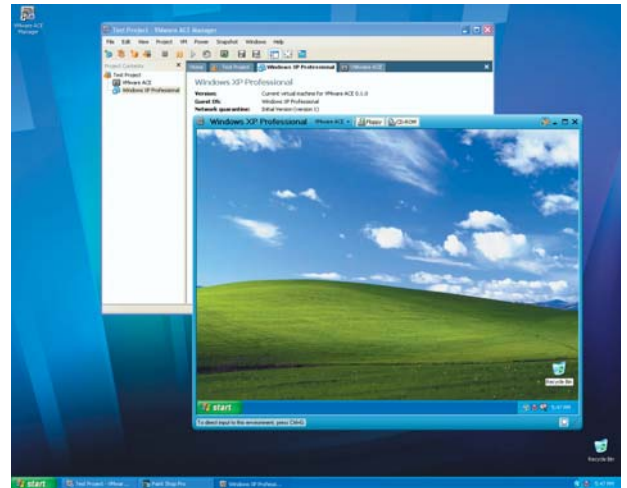
Использование VMware ACE на предприятии

VMware ACE позволит администраторам по безопасности:

- создавать контролируемые ими безопасные терминальные устройства на неадминистрируемых ПК;



Технология управления виртуальными правами, встроенная в VMware ACE Manager, обеспечивает централизованный контроль на основе правил информационной безопасности (ИБ) над сроками действия, идентификацией пользователя, шифрованием данных, доступом в сеть, доступом к периферийным устройствам, а также защиту от несанкционированного копирования для ПО VMware ACE, развернутого на ПК конечного пользователя.



- обеспечить безопасность конфиденциальных данных на конечных ПК;
- иметь несколько безопасных вычислительных сред на одном ПК.

Принцип работы VMware ACE

С помощью ПО VMware ACE Manager администраторы по безопасности создают пакеты для развертывания программного обеспечения, соответствующие стандартам MSI. Они состоят из:

- одной или более автономных виртуальных машин, оснащенных операционной системой, прикладными программами, обеспечивающими информационную безопасность (ИБ), корпоративными прикладными программами и данными;
- правил ИБ, которые контролируют шифрование, идентификацию пользователя, сроки действия, защиту от несанкционированного копирования, доступ в сеть и к периферийным устройствам для одной или нескольких виртуальных машин.

Затем администраторы по ИБ могут распространить созданные пакеты среди конечных пользователей, предоставляя им возможность прямой загрузки, с помощью специального программного обеспечения или на носителях информации (DVD/CD). Установив эти пакеты, конечные пользователи создадут безопасный управляемый терминал.

Управление виртуальными правами VMware ACE (VRM) позволяет централизовать управление правилами информационной безопасности (ИБ) и правами доступа к информации в виртуальных машинах фирмы VMware. Таким образом они могут осуществлять контроль над жизненным циклом ПК и обеспечением его соответствия правилам ИТ.

** VMware ACE позволяет предоставить сотрудникам, работающим с удаленных терминалов, и контрактным работникам виртуальные машины, содержащие операционные системы и ПО, необходимое для их работы. Технология управления виртуальными правами обеспечивает возможность установить контроль над доступом к виртуальной машине, управлять версиями образа VM, сроком их действия, а также обеспечить защиту от вирусов. Все это позволило нам защитить данные Baptist Healthcare System.*

Том Тэйлор, старший аналитик по архитектуре «клиент-сервер», Baptist Healthcare System

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

- **Централизованные правила информационной безопасности (ИБ) и управления.** Управление виртуальными правами (VRM) позволяет централизовать управление правилами ИБ и правами доступа в приложении к виртуальным машинам, работающим на ПК конечных пользователей.
- **Безопасная вычислительная среда.** Обеспечение безопасности всей среды VMware ACE, включая данные и системные конфигурации, с помощью проверки подлинности и шифрования, прозрачного для пользователей и прикладных программ.
- **Доступ в сеть на основе правил.** Обеспечение соответствия терминалов требованиям ИТ благодаря выявлению и изоляции неавторизованных или просроченных виртуальных машин с VMware ACE.
- **Управление устройствами.** Разрешение или запрещение доступа из среды VMware ACE к периферийным устройствам базового ПК, таким как печатающие устройства, USB-устройства для хранения информации и дисководы для записи информации на CD/DVD.
- **Функция управления цифровыми правами (DRM).** Не позволяет пользователям копировать VMware ACE на сменные носители, сетевые файловые системы или другие ПК.
- **Управление сроками действия.** Возможность установить период времени, в течение которого VMware ACE будет работать, или дату и время прекращения работы.
- **Универсальность пакетов.** Возможность создания стандартных сред, независимых от аппаратного обеспечения, и дальнейшего их развертывания на любом стандартном ПК.
- **Настраиваемый интерфейс конечного пользователя.** Возможность настройки режима работы и внешнего вида пользовательского интерфейса.
- **Гибкая вычислительная среда.** Конечные пользователи могут вернуть среду к предыдущему состоянию всего за несколько секунд. Конечные пользователи могут работать в среде VMware ACE как в оперативном (подключение к сети активно), так и в автономном (подключение к сети отсутствует) режимах.

Почему следует выбрать VMware ACE

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ	ПРЕИМУЩЕСТВА
Создание безопасных управляемых терминалов Обеспечение безопасности неадминистрируемых ПК, используемых дистанционными работниками и контрактными работниками.	<ul style="list-style-type: none"> • Снижение уязвимости к вредоносным программам, источниками которых могут быть неадминистрируемые незащищенные ПК. • Сохранение конфиденциальных данных в безопасных, зашифрованных, защищенных от несанкционированного копирования средах ПК. • Снижение затрат на предоставление доступа с неадминистрируемых ПК в вычислительную сеть предприятия. • Устранение необходимости в восстановлении поврежденных (например, вирусами) неадминистрируемых физических ПК.
Обеспечение безопасности конфиденциальных данных на оконечных ПК (терминалах) Шифрование и защита важной интеллектуальной собственности предприятия и личных данных сотрудников.	<ul style="list-style-type: none"> • Централизация правил информационной безопасности, защиты от несанкционированного копирования и шифрования с помощью технологии управления виртуальными правами (VRM). • Сокращение риска кражи и несанкционированного копирования интеллектуальной собственности предприятия, цифровых носителей, охраняемых авторским правом, и личной информации сотрудников.
Развертывание нескольких безопасных сред на одном ПК Создание изолированных, независимых от аппаратного обеспечения сред, которые можно развернуть на любом ПК.	<ul style="list-style-type: none"> • Устранение необходимости в использовании нескольких физических ПК для изоляции рабочих сред, информации и доступа в сеть. • Централизация управления правилами информационной безопасности с помощью технологии управления виртуальными правами (VRM).

СПЕЦИФИКАЦИИ

Требования к базовой системе конечных пользователей

Аппаратное обеспечение ПК

- Стандартный ПК
- Рекомендуется процессор x86 с частотой 500 МГц или выше (минимальная частота 400 МГц)

Совместимые процессоры

- Intel®: Celeron®, Pentium® II, Pentium III, Pentium 4, Pentium M, Xeon
- AMD: Athlon, Athlon MP, Athlon XP, Duron, Opteron
- Поддерживаются многопроцессорные системы
- Экспериментальная поддержка для процессоров AMD64 Opteron, Athlon 64 и Intel IA-32e

Оперативная память

- Рекомендуемый объем памяти 256 Мбайт, минимальный 128 Мбайт

Экран

- Рекомендуется 16-разрядный видеоадаптер, требуется видеоадаптер не ниже 8-разрядного

Дисковые накопители

- 80 Мбайт свободного места для базовой установки
- Для гостевой операционной системы и приложений рекомендуется не менее 1 Гбайт свободного места
- Поддерживаются жесткие диски IDE и SCSI, приводы CD-ROM и DVD-ROM

Базовые операционные системы Windows

- Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition, включая пакет обновления 1 (SP1)
- Windows XP Professional и Windows XP Home Edition с пакетами обновления 1 или 2 (SP1 или SP2)

- Windows 2000 Professional с пакетами обновления 3 или 4 (SP3 или SP4), Windows 2000 Server с пакетами обновления 3 или 4 (SP3 или SP4), Windows 2000 Advanced Server с пакетами обновления 3 или 4 (SP3 или SP4)

Требования к базовой операционной системе для ACE Manager

- **Базовые операционные системы Windows**
- Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition
- Windows XP Professional и Windows XP Home Edition с пакетами обновления 1 или 2 (SP1 или SP2)
- Windows 2000 Professional с пакетами обновления 3 или 4 (SP3 или SP4), Windows 2000 Server с пакетами обновления 3 или 4 (SP3 или SP4), Windows 2000 Advanced Server с пакетами обновления 3 или 4 (SP3 или SP4)

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Полный список системных требований см. по адресу http://www.vmware.com/support/ace/doc/intro_sysreqs_ace.htm.