VMware ACE 2.5 Test Drive

vmware

Contents

Introduction

VMware ACE is a technology and software solution that enables organizations to deploy and manage secure, platform-independent virtual machines that you can use on work PC, personal computer, laptops, or even a portable USB media device. VMware ACE implements **Virtual Rights Management** (VRM) on virtual machines by enabling users to configure their virtual machine with a flexible set of security and management policies. For example, policies like copy-protection controls and automatic encryption can prevent theft, tampering, and unauthorized copying of applications and/or data. On the other hand, policies like expiration can be used to effectively execute a timely expiration of software evaluation or contract.

An ACE is an *assured computing environment*, where each instance comprises of a preconfigured virtual machine (operating system and applications) and policy settings. ACE instances can be deployed to endpoints on and off the network, and can be managed or standalone.

Go ahead and try: In case of enterprise deployments, VMware ACE enables safe access to enterprise resources from assured computing environment.

In this Test Drive Guide, you will learn about how to securely take your desktop with you everywhere you go by deploying a Pocket ACE. The guide will walk through

- Define and apply security rules and access policies with the VRM technology
- Create and deploy a Pocket ACE package - secure virtual desktop environments that can be deployed on portable devices. You will need a USB device for this exercise.

Providing Feedback

Thank you for taking on the VMware ACE 2.5 Test Drive. Please send us your feedback from this experience as well as this Test Drive Guide here

Key Benefits of VMware ACE

VMware ACE implements Virtual Rights Management (VRM) technology that enables security policies to be applied to virtual machines that govern endpoint security, including authentication, secure network connectivity, data leakage prevention with data encryption, device and copy protection control, and time-based expiration of virtual machines. VMware ACE provides the ideal solution to:

- **Secure mobile computing –** Deploy secure, managed virtual desktops that adhere to corporate processes and security policies to remote and mobile users, allowing them to work from anywhere, anytime without compromising corporate security.
- **Compliance in a Sandbox –** Manage and maintain compliance to leading regulation standards, including Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI) by securing access to sensitive data via secure, managed virtual desktop.
- **Legacy OS support –** Minimize application and operating system compatibility issues during system migration by re-hosting legacy applications and operating systems in isolated virtual machines.
- **Desktop business continuity** - Provide organizations with continuous access to secure corporate working environments on USB keys via Pocket ACE in case of unforeseen circumstances that prevent workers from the workplace.

- **Kiosks/Shared PCs -** Safely deliver and control access to applications that run on shared physicals PCs**,** which are typically used in libraries, computer labs, bank offices, shopping
- malls, airports via lock-downed virtual desktops, yet preventing the host operating system on shared PCs from misuse and malicious attacks.

Terminology

The following are frequently used terms in describing VMware ACE:

- **ACE-enabled VM** - A VM template which can be configured with various policies, devices, and deployment settings and then used as the basis for creating any number of packages to be sent to ACE users.
- **ACE instance** – An actual instance of VRM-enforced VM that is deployed and installed
  - **Managed ACE Instance**: An ACE instance that is managed by an ACE Management Server.
  - **Standalone ACE Instance**: An ACE instance that is not managed by an ACE Management Server.
- **ACE Management Server** - The ACE Management Server enables you to manage ACE instances, to publish policy changes to dynamically update those instances, and to test and deploy packages more easily. Adds new integration with Active Directory setups and provides secure Active Directory and LDAP integration, with role based secure SSL communication.
- **ACE Package** – A complete installation package that can be deployed to multiple which includes a VM, its associated VRM-policies, resources, and a virtualization runtime (optional, for either Linux or Windows, or both).
- **Pocket ACE** – ACE instance that can be is deployed on a USB portable media device, including USB flash drives, Apple iPod mobile digital devices, and portable hard drives.

Getting Started

Test driving ACE is easy. Here are the steps that we'll be following through in this exercise:

1. Enable ACE features on a VM (via VM settings). You can create or clone a VM, or convert one from physical machine or 3rd party format.
2. Set VRM policies.
3. Specify deployment settings.
4. Package and deploy an ACE instance.
5. Install and run an ACE Instance.

For the purpose of this exercise, prepare a VM and a USB 2 device[1] for your pocket ACE. Make sure that your USB device will have enough room for your VM. Let us begin!

VRM Policies

VRM policies give you control over many aspects of the ACE instances that you create and distribute. Before you can use the policy editor on a VM, enable the ACE capabilities for the VM:

1. Enable ACE via **VM> Settings > Options > ACE**
2. Choose **VM > ACE > Policies.**
3. In the policy editor, select an item in the **Policy** list.

[1] Pocket ACE packages on the following types of devices:
- Flash memory drives (USB* keys)
- Flash-based Apple iPod mobile digital devices
- Hard drive-based Apple iPod mobile digital devices
- Portable hard drives

4. Complete the settings panel for that policy and either click **OK** or select another policy to edit.

Access Control

Activation and authentication policies enable access-control on both installed ACE packages as well as instances created from those packages. While an *activation* policy specifies who can access an installed ACE package and turn it into an ACE instance, the *authentication* policy specifies who can run an ACE instance. ACE supports several authentication models, find out more from the Workstation 6.5 User's Manual.

Go ahead and try: Since you are taking your personal laptop to go, you would prefer to enforce access control. Configure your ACE to require passwords for both the activation (so that if you lose the media carrying the ACE, no one else but you can install) and authentication (in case you lose the laptop with the ACE, no one else but you can power on the machine).

Expiration Policies

Expiration policies are useful, for instance if you want to prevent the VM from being accessed beyond a certain date or for more than a certain number of days. This is particularly useful if you would like to share your desktop for someone to temporarily access resources from your desktop or evaluate a software application.

Go ahead and try: For this evaluation, assume configure a 30-day expiration period.

Copy Protection

Copy protection policies ensure that an ACE instance runs only from the location where it was originally installed. If you copy-protect an ACE instance, its files can be moved or copied, but the instance cannot run from the new location.

Go ahead and try: Given this will be your desktop-on-the-go, would you want to enable the instance to be copied and/or moved? Configure your ACE accordingly.

Removable Devices

Removable devices policies allow you to control whether users can connect and disconnect removable devices from their ACE instances. When you select Removable Devices in the policy editor, all removable device types for this ACE-enabled VM are displayed in a list. You can specify which devices to allow end users to access.

Go ahead and try: ACE provides granular control over the access control of USB devices. Setup your policy to disable all "Mass Storage" USB devices. This way, your friend will still be able to use his iPods and Webcams while trying out your application, but won't be able to copy any personal data out of the ACE to a mass storage USB.

Virtual Printer

VMware ACE includes a virtual printer that allows users to print to any printer available to the host computer without installing additional drivers in the VM.

The virtual printer feature is currently available for ACE instances running with these Windows host and guest operating systems:

- Host – Windows 2000, XP, 2003, or Vista, 32-bit only
- Guest – Windows 2000, XP, 2003, Vista (32- and 64-bit), Red Hat Enterprise Linux 4 (32-bit only), Ubuntu, and SUSE

Go ahead and try: If you have a Windows desktop environment and expect that you will run the Pocket ACE on Windows systems, then enable the virtual printer.

Runtime Preference

You can set options on the runtime preferences policy page to specify runtime behaviors and which of those may be user-configurable. For example, you may consider what your ideal runtime behaviors are, for example:

- Do you want this ACE to run in full-screen by default?
- If you plan to run your Pocket ACE on public/shared terminals, do you want to be alerted or have the session stop should a keylogger be detected on the host?
- What would you like to see when you close your Pocket ACE instance - would you want to set a default behavior or be prompted to choose each time?
- Would you consider using the host computer to cache file from the USB during use? For performance reasons files from the USB device are cached as needed on the host. For example, you can disable this caching if you do not have enough disk space on the host.

Go ahead and try: For this exercise, configure the ACE to always run in full-screen. Then, consider how you might like to use your desktop-to-go and configure the exit behavior.

Kiosk Mode

When an ACE instance runs in kiosk mode, the user cannot access the host system at all. For example, the user cannot shut down the host machine. The VM runs in full screen mode and does not display the ACE menu bar or ACE Player online help. When a user exits kiosk mode, the VM is powered off or suspended, according to the runtime preference policy for exit behavior. Pocket ACE instances are powered off and synchronized. When the VM is powered off, the ACE Player prompts the user to exit kiosk mode.

Deployment Settings

Deployment settings enable you to configure package characteristics, such as instance customization and encryption, and then apply those settings to as many packages as you choose.

Encryption

Encryption settings are of two types:

- **Package encryption** – Protects package files from being copied or altered while in transit. If you set package protection to **Encrypted**, the New Package wizard encrypts the VM when a package is created.
- **ACE instance encryption** – Protects ACE instance files from being copied or altered after installation and activation. You must specify an authentication method if you want the installer to encrypt the ACE instance. The Workstation software uses defaults that the activation and authentication policies determine to apply encryption settings to the package and files.

Preview Configuration

Preview mode enables you to run an ACE instance as it runs on an end user's machine. You can see the effects of changed policies without having to package and deploy them. Preview mode also enables you to see the effects of setup choices without having to create, deploy, and install a full package.

Go ahead and try: Using the preview feature, take a sneak peak at your Pocket ACE that you have defined so far. Did your Pocket ACE run in fullscreen mode as you've configured? What menus do you see in the Player runtime?

Package and Deploy

After you create an ACE-enabled VM and configure policies, devices, and deployment settings, use the New Package wizard to create a package to deploy instances to users.

Go ahead and try: Make sure the VM is powered off rather than suspended and use the wizard to create a new Pocket ACE and deploy the package immediately to your USB device.

Install and Run

After you deploy a Pocket ACE package to a removable device, running it usually involves only plugging it in. The Pocket ACE runs primarily from the host cache, although it occasionally reads from the parent disk on the portable device. The ACE instance does not write to the parent disk. When the ACE instance runs, its disk and checkpoint caches are initialized. The checkpoint state and virtual disk are cached on the host during use and synchronized back to the portable device later. The checkpoint state and virtual disk are protected with the same encryption level used for the ACE instance on the portable device.

Go ahead and try: Plug your Pocket ACE into a computer and run! ☺

Additional Resources

VMware ACE 2.5 Beta Documentation

- Workstation 6.5 User's Manual
  http://www.vmware.com/products/beta/ws/ws65_manual_beta.pdf
- ACE 2.5 Release Notes
  http://www.vmware.com/products/beta/ace/releasenotes_ace25_beta.html

VMware ACE Product Information
http://www.vmware.com/products/ace/

ACE Test Drive Program
http://www.vmware.com/communities/content/beta/ws65ace25/ACE25TestDrive.html