DoD Public Key Enablement (PKE) Reference Guide

Configuring VMware Horizon View Versions 5.2 and 5.3 for Use with DoD PKI

Contact: dodpke@mail.mil
URL: http://iase.disa.mil/pki-pke

Enabling PKI Technology
for DoD users

Configuring VMware Horizon View Versions 5.2 and 5.3 for Use with DoD PKI

5 November 2014

Version 1.0

DOD PKE Team

Revision History

Issue Date	Revision	Change Description
11/5/14	1.0	Initial Release

Contents

INTRODUCTION **1**

Purpose 1
Scope 1

GETTING STARTED **2**

Baseline 2
Prerequisites 2

CREATING A MASTER VIRTUAL MACHINE **4**

CONFIGURING VMWARE HORIZON VIEW 5.2/3 .... **5**

Management of the View Virtual Desktop Agent 5
Configure and Deploy View Virtual Desktops 5

CONFIGURING SMART CARDS FOR VMWARE HORIZON VIEW 5.2/3 .... **6**

Configuring Secure Socket Layer (SSL) on VMware Horizon View 5.2/3 Connection Broker 6
Setting Up Smart Card Use 7
Configuring DoD Server Certificate Friendly Name for Upgrade Installs 7
Configuring DoD Server Certificate Friendly Name for New Installs or Certificate Replacement 7
Configuring Smart Card Authentication for View 8
Configuring CRL and OCSP checking 9

APPENDIX A: SUPPLEMENTAL INFORMATION **10**

Web Site 10
Technical Support 10

APPENDIX B: ACRONYMS **11**

APPENDIX C: REFERENCES **12**

Introduction

The DoD Public Key Enablement (PKE) reference guides are developed to help an organization augment their security posture through the use of the DoD Public Key Infrastructure (PKI). The PKE reference guides contain procedures for enabling products and associated technologies to leverage the security services offered by the DoD PKI.

Purpose

This guide is written for DoD system or network administrators and provides instructions for configuring the VMware Horizon View product suite to utilize DoD PKI in accordance with DoD best practices. The VMware Horizon View product suite delivers virtualized desktop services to your enterprise, leveraging your existing cloud computing environment to provide a centrally managed desktop service capability. This desktop service can deploy user centric customization that can satisfy a mix of operating and software application requirements supporting a range of end users, helpdesk staff, and IT administrators.

The VMware Horizon View product suite implements a secure interface, the VMware View Connection Broker, that facilitates access to the Virtual Desktop Infrastructure and Virtual Desktop environment. The View Connection Broker component provides the user interface to the Virtual Desktop Infrastructure and is responsible for authenticating and encrypting the user session.

Scope

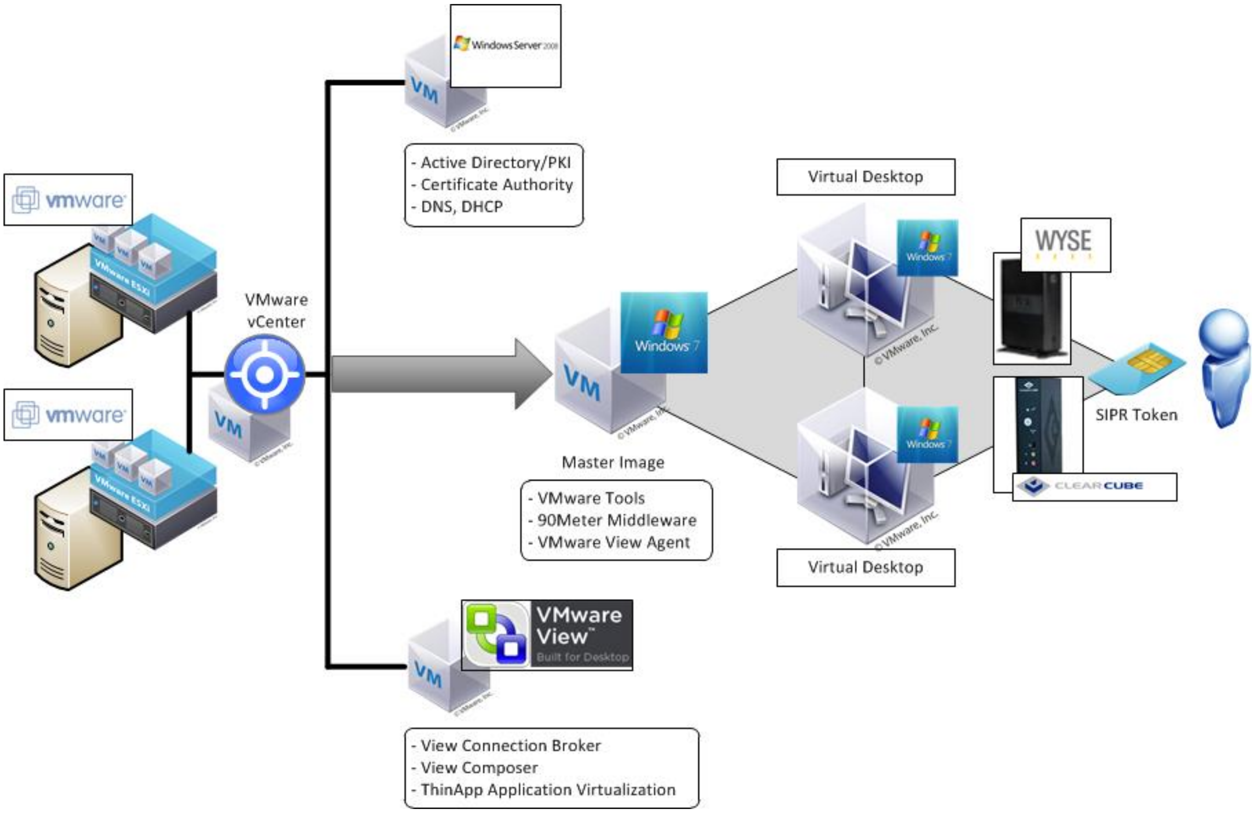
This document is written to guide system and network administrators for the PKE of the VMware Horizon View product using DoD issued certificates. The document assumes the user has basic knowledge of configuration and administration of the VMware Horizon View components and basic knowledge of the DoD PKI. The scope and configuration procedures provided by this PKE guide outline configuration steps that are required to provision a DoD PKI server certificate to the VMware Horizon View service. These steps also include configuration settings that are necessary to enable DoD Common Access Card (CAC) authentication and prerequisite vendor reference guides needed to deploy a VMware Horizon View infrastructure.

Getting Started

Baseline

This guide was developed using VMware Horizon View 5.2/3 on VMware ESXi 5.0 serving Windows 7 desktop clients in a Windows 2008 R2 domain. This is an example architecture. There are other virtualization environments and design implementations that can be used to provide secure access to a Virtual Desktop Infrastructure (VDI) using the DoD PKI.

The following diagram represents the example architecture:



Prerequisites

This guide assumes that VMware Horizon View 5.2/3 has been installed and configured for basic connectivity on a Windows Server 2008 R2 instance. This instance also had a valid DoD server certificate issued to it. Please refer to the *Obtaining a PKI Certificate for DoD Server* guide located on the DoD PKE website at http://iase.disa.mil/pki-pke under *For Administrators, Integrators & Developers* > *Web Servers* for instructions on requesting this server certificate. This server certificate needs to have its friendly name modified for use with Horizon View. Instructions for this modification can be found in the section below. For instructions on installing and configuring a VMware Horizon View 5.2/3 environment, refer to the VMware Horizon

View 5.2/3 Administrator's Guide at http://pubs.vmware.com/view-52/topic/com.vmware.ICbase/PDF/horizon-view-52-administration.pdf

The Windows domain is configured for smart card logon with DoD PKI credentials. Refer to the *Microsoft Windows Server 2008: Enabling Smart Card Logon* guide and the *Microsoft Windows Server 2003: Enabling Smart Card Logon* guide available from the DoD PKE site at http://iase.disa.mil/pki-pke under *For Administrators, Integrators, and Developers* > *Network Configuration* for detailed instructions. The following is a list of configuration(s) used and requirements for this guide.

- The Vmware Horizon View 5.2/3 server is acting as a VDI Connection Broker and the View virtual desktops have the proper middleware installed and patched to the most recent version.
- The latest hotfixes and operating system patches on all View servers are installed.
- The VMware Horizon View 5.2/3 Connection Broker is a part of the Windows Smart Card Enabled domain.
- The reader has the administrative privileges necessary to complete the steps in this guide.

Creating a Master Virtual Machine

This section is intended for administrators who are delivering desktops through virtual machines (VMs). In this example architecture, this section is to be performed on the VMware ESXi platform. It describes how to create a base image that can be used to build your desktop VM environment. These steps also include also provisioning steps to install smartcard middleware software on the base image.

1) In VMware vCenter, create a New Virtual Machine and install a Windows Vista or Windows 7 operating system for the Master Image for Vmware Horizon View 5.2/3.
2) After the installation of the operating system is complete, run Windows Update and install all applicable updates on the New Master Image for the operating system.
3) Install VMware Tools onto the New Master Image.
4) Install Smartcard middleware onto the New Master Image.
5) Install the Vmware Horizon View 5.2/3 Agent onto the New Master Image.
6) Shut down the New Master Image. The Master Image will be referenced as the template to deploy View virtual desktops.

NOTE: Refer to vendor documentation for individual installation specifics for other vendors and implementation models.

Configuring VMware Horizon View 5.2/3

This section provides references to VMware's documentation that will guide the VMware administrator through the process of creating and provisioning virtual Machines in their Virtual Desktop Infrastructure. The creation and deployment of desktop VMs requires specific configuration procedures that integrate your desktop VMs into the VMware Horizon View product suite. The deployment of desktop VMs requires specific Horizon View provisioning steps that create and provision desktop VMs with Horizon View compatible configurations and invoke pre-deployment settings that install and enable smartcard support to the Virtual Desktop Infrastructure. Additional Horizon View configuration steps must also be implemented to allocate and assign virtual desktop resource pools to the user.

Management of the View Virtual Desktop Agent

Refer to the section entitled *Creating and Preparing Virtual Machines* in the VMware Horizon View 5.2/3 Administration Guide documentation.

Configure and Deploy View Virtual Desktops

Refer to the section entitled *Creating Desktop Pools* in the VMware Horizon View 5.2/3 Administration Guide documentation.

NOTE: This will register the virtual desktop pools with its associated Entitlements.

Configuring Smart Cards for VMware Horizon View 5.2/3

The section provides configuration steps that will enable the VMware administrator to issue a DoD PKI server certificate to the Horizon View Connection Broker and settings necessary to require DoD CAC authentication to the Horizon View application. The steps outlined in this section provide vendor reference material that guides the administrator and details configuration steps to configure and install a third party Certification Authority (CA) issued certificate. The ***VMware Horizon View 5.2/3 Installation Guide***[i] in the ***Configuring SSL Certificates for View Servers*** chapter outlines the steps that the administrator must follow to create the certificate signing request (CSR) and configuration steps taken to install the server certificate. DoD specific references have been provided that can be used to determine what DoD PKI enrollment page is applicable to their organization. Once the CSR has been created using the vendor documentation, the CSR must then be submitted to a DoD PKI enrollment page in order to receive and provision a DoD PKI server certificate.

Additional vendor documentation has been provided as reference material to configure backend authorization with the Horizon View application. Refer to the ***VMware Horizon View 5.2/3 Administration Guide***[ii] in the ***Setting Up User Authentication*** chapter to configure backend authorization. The VMware Horizon View product supports the ability to use Active Directory as the backend directory resource. Configuration steps outlined in this guide provide instructions for authorizing users using the users' certificate attributes stored on the DoD CAC. The VMware Horizon View product leverages the DoD CAC user certificate attributes, specifically the user principal, to identify and map the user to a user account stored in Active Directory.

Configuring Secure Socket Layer (SSL) on VMware Horizon View 5.2/3 Connection Broker

Refer to the ***VMware Horizon View 5.2/3 Installation Guide*** documentation referencing ***Configuring SSL Certificates for View Servers***. Use this documentation to generate an RSA key pair, CSR, and install a DoD PKI server certificate. Submit the CSR to your proper CA using the instructions found in the **Obtaining a DoD PKI Certificate for a Web Server** reference guide available from the DoD PKE site at http://iase.disa.mil/pki-pke/ under *For Administrators, Integrators and Developers* > *Web Servers*. The reference guide is unclassified; however, a DoD PKI certificate is required for access.

Setting Up Smart Card Use

Refer to the ***VMware Horizon View 5.2/3 Administration Guide*** documentation referencing ***Setting Up User Authentication*** for additional information. Use this documentation to configure Horizon View's backend authorization features.

Configuring DoD Server Certificate Friendly Name for Upgrade Installs

These section provides you with configuration steps that will ensure local system certificate settings are compatible with Horizon View software upgrades. If upgrading an existing system to Horizon View version 5.2/3, the friendly name of the current DoD certificate on the system needs to be changed. The DoD server certificate friendly name needs to be changed to **vdm.** Also, the Horizon View application requires that only a single instance of the **vdm** friend name exists or the server may randomly choose which certificate to use on a system restart or reboot.

1) The DoD server certificate needs to have its friendly name changed to **vdm**.
2) Open an mmc console and add the certificates snap in. Navigate to **Certificates (Local Computer) > Personal > Certificates**.
3) Open properties on the DoD Server Certificate and open the general tab. Under **Friendly Name** add the text *vdm***.**

Configuring DoD Server Certificate Friendly Name for New Installs or Certificate Replacement

This section provides you with configuration steps that will ensure local system certificate settings are compatible with new Horizon View software installs. In the case of a new install or the replacement of the old DoD Server certificate, several extra steps may be required. Also, the Horizon View application requires that only a single instance of the **vdm** friend name exists or the server may randomly choose which certificate to use on a system restart or reboot.

1) Obtain the root certificate from the CA and add the certificate to the **Server Truststore File**.
2) If a DoD server certificate has not been obtained, obtain one now.
3) The DoD server certificate needs to have its friendly name changed to **vdm**.
4) Open an mmc console and add the certificates snap in. Navigate to **Certificates (Local Computer) > Personal > Certificates**.
5) Remove VDM from the VMware generated self-signed certificate if it exists.
6) Remove VDM from the old DoD server certificate if it exists.

7) Open properties on the DoD Server Certificate and open the general tab. Under **Friendly Name** add the text *vdm*.

Configuring Smart Card Authentication for View

This section provides procedures that will enable DoD CAC authentication to the Horizon View application. These steps configure the Horizon View application to use DOD PKI CA trust anchors to authenticate and validate DoD CAC user certificates. Additional steps also outline configurations that must be implemented to only allow DoD CAC authentication as an allowed authentication factor.

1) To add the certificate, run the following command on the VMware Horizon View 5.2/3 server:

   keytool -import -alias alias -file root_certificate -keystore truststorefile.key

2) Copy the trust store file to the SSL gateway folder on the View Connection server.

   install_directory\VMware\Vmware View\Server\sslgateway\conf\truststorefile.key

3) Next, edit the locked.properties file in the SSL gateway folder on the View Connection Server.

   install_directory\VMware\Vmware View \Server\sslgateway\conf\locked.properties

4) Add the trustKeyfile, trustStoretype, and useCertAuth properties to the locked.properties file.

   a) Set trustKeyfile to the name of your trust store file.

   b) Set trustStoretype to **JKS**.

   c) Set useCertAuth to **true** to enable certificate authentication.

5) Restart the View Connection Server service.

6) Next, login to the View Administrator console and in the left pane, expand View Configuration and select **Servers**.

7) Select the View Connection server and click **Edit**.

8) On the **Authentication** tab, configure smart card authentication to **Required**.

9) Configure the smart card removal policy to disconnect user sessions on smart card removal, if applicable.

10) Click **OK** and restart the View Connection server service.

Configuring CRL and OCSP checking

For configuring CRL checking, OCSP checking, or OCSP checking with CRL fallback, follow the configuration instructions available in the ***VMware Horizon View Administration Guide*** in the section ***Using Smartcard Certificate Revocation Checking***.

Appendix A: Supplemental Information

Web Site

Please visit the URL below for additional information.
http://iase.disa.mil/pki-pke

Technical Support

Contact technical support at the email address below.
dodpke@mail.mil

Appendix B: Acronyms

CAC	Common Access Card
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DoD	Department of Defense
FQDN	Fully Qualified Domain Name
OCSP	Online Certificate Status Protocol
PKE	Public Key Enablement
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, and Adleman
SSL	Secure Socket Layer
URL	Uniform Resource Locator
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine

Appendix C: References

The resources below were used to help develop the content of this document.

[i] "VMware Horizon View 5.2/3 Installation Guide", http://pubs.vmware.com/view-50/topic/com.vmware.ICbase/PDF/view-50-installation.pdf.

[ii] "VMware Horizon View 5.2/3 Administration Guide", http://pubs.vmware.com/view-50/topic/com.vmware.ICbase/PDF/view-50-administration.pdf.

[iii] "Smart Card Certificate Authentication with VMware Horizon View 5.2/3 and Above", www.vmware.com/files/pdf/VMware-View-SmartCardAuthentication-WP-EN.pdf