THALES

www.thalesesecurity.com

vmware READY
PLATFORM AND COMPUTE

THALES E-SECURITY

VMware Encryption and KMIP: Integration with Vormetric Data Security Manager

Release Date: November 30, 2017

Copyright 2017 Thales e-Security Inc.

Contents

Contents....3
Introduction....4
Tested Configurations....4
Overview....5
Licensing Information....5
Create KMS Cluster in vSphere....7
Establish Trust between vCenter Server and DSM Cluster....8
Verify Trust between vCenter Server and DSM Cluster....9
Enable Encryption for Target Servers....10
Contact Support....11

Introduction

This document outlines the steps required to enable the Vormetric® Data Security Manager (DSM) to be a key management server (KMS) for VMware encryption solutions, vSAN and VM encryption, that use the OASIS KMIP protocol. For instructions on how to install and configure a DSM, refer to the DSM Installation and Configuration Guide

Tested Configurations

The following versions have been tested for vSAN, VM Encryption, with DSM integration:

VMware	DSM Version	KMIP Version	vSphere Version	vSAN Version
VM Encryption	6.0.1.4034	1.1 to 1.4	vSphere 6.5 & vSphere 6.5 U1	N/A
vSAN Data at Rest Encryption	6.0.1.4034	1.1 to 1.4	vSphere 6.5.0d	6.6

If a configuration is not listed above, and you require more information, please contact Thales Support or your local Account Manager.

We recommend that you test your configuration in a safe environment before committing to a production environment.

Overview

The following sections describe how to configure the DSM as a KMS with VM Encryption.

To configure the DSM as a KMS with vSAN, refer to the following VMware guide:

Administering VMware Virtual SAN

To perform specific cryptographic operations using VMware's APIs, refer to:

vSphere Web Services SDK Programming Guide

Configure the DSM as a KMS with VM Encryption

The process consists of the following high-level steps:

1. Create the KMS cluster in vSphere
2. Establish trust between vCenter Server and DSM cluster
3. Verify that trust has been established
4. Enable encryption for VMs via VMware Storage

Licensing Information

The Thales licenses are provided by Thales Customer Support and are uploaded to the DSM. The term of a license begins when you register the KMIP client using that license.

In an HA environment, the license file must be uploaded to the primary DSM only. Once installed on the primary DSM, it automatically replicates to the failover DSM(s).

License requirements are as follows:

For Virtual Machine Encryption:

- 1 KMIP license per vCenter Server

For vSAN encryption:

- 1 KMIP license per vCenter Server
- 1 KMIP license per ESXi vSAN Server

Create KMS Cluster in vSphere

Configure VMware to use a Key Management Server (KMS).

1. In the vSphere Web Client, select the cluster on which to enable encryption and click the **Configure** tab, then click **Key Management Servers**.
2. Click **Add** and enter the following information, relevant to your organization.

Cluster name	Name of the KMS cluster that you want to create
Server alias	Use this alias to connect to the KMS if your vCenter instance becomes unavailable
Server address and port	IP address or FQDN of the DSM, and port via which the vCenter Server connects to the DSM (KMIP port is 5696).

3. Click **Trust** in the Trust Certificates dialog box, to trust the DSM.

Establish Trust between vCenter Server and DSM Cluster

Import the vCenter certificate into the DSM.

1. Select the KMS instance you just created, and click Establish Trust with KMS.
2. In the dialog that displays, select Certificate and click OK.
3. Select Download as File. The file will download in the .pem format.
4. Navigate to the location where you downloaded the .pem file change the file extension to .crt.
5. Display the contents of the downloaded certificate to obtain the common name of the vCenter Server.
6. Use the command: openssl x509 –in certificate.crt –text –noout
7. Or, use an online certificate decoder to view the contents, for example, https://www.sslshopper.com/certificate-decoder.html
8. Copy the vCenter Server certificate common name.
9. Log on to your DSM and switch to the domain used by the KMIP devices.
10. Click Hosts and then click Add to add a new host.
11. Enter the common name copied in step 5, into the Host Name field.
12. Select the Registration Allowed Agents: KMIP check box.
13. Select Communication Enabled check box and click OK.
14. Click the host name of the host you just created.
15. On the Edit Host page, click Import KMIP Certificate on the bottom right-hand corner under the Agent Information table.
16. After importing the certificate, the fingerprint from the vCenter Server certificate is listed in the Certificate Fingerprint field.

Verify Trust between vCenter Server and DSM Cluster

Ensure that the vCenter Server is able to connect securely to the DSM cluster.

- Refresh the vSphere Web Client page and make sure there is a green check mark in the Connection Status column.

Enable Encryption for Target Servers

Enable encryption using VMware Storage Policies.

1. In the vSphere Web Client, right-click the VM for which you would like to enable encryption and select **VM Policies > Edit VM Storage Policies**.
2. Select the storage policy that utilizes the DSM as the Key Management Server and click **Apply to All**, then click **OK**.
3. This will trigger a reconfiguration of the VM.
4. Once the reconfiguration is complete, the disks are encrypted and the keys are managed by the DSM.

Contact Support

To obtain support for your product, visit:

www.thalesesecurity.com/support

Copyright © 2009 - 2017 Thales e-Security, Inc. All rights reserved.
NOTICES AND LICENSE
Vormetric is a registered trademark of Thales e-Security, Inc. in the United States (U.S.) and a registered trademark or trademark in other countries. All other company and/or product names are trademarks and/or registered trademarks of their respective owners. The Software and documentation contains confidential information of Thales e-Security, Inc. The Software and documentation are furnished under Thales' standard Master License Software Agreement (Agreement) and may be used only in accordance with the terms of the Agreement.

THALES HARMLESS FROM AND AGAINST, ANY SHORTFALL IN PERFORMANCE OF THE SOFTWARE, OTHER HARDWARE OR TECHNOLOGY, OR FOR ANY INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AS A RESULT OF THE USE OF THE SOFTWARE IN ANY ENVIRONMENT. LICENSEE SHALL DEFEND, INDEMNIFY, AND HOLD THALES HARMLESS FROM AND AGAINST ANY COSTS, CLAIMS, OR LIABILITIES ARISING OUT OF ANY AGREEMENT BETWEEN LICENSEE AND ANY THIRD PARTY. NO PROVISION OF ANY AGREEMENT BETWEEN LICENSEE AND ANY THIRD PARTY SHALL BE BINDING ON THALES.
Protected by U.S. patents: 6,678,828
6,931,530
7,143,288
7,283,538
7,334,124
Vormetric Data Security includes a restricted license to the embedded IBM DB2 database. That license stipulates that the database may only be used in conjunction with the Vormetric Data Security Manager. The license for the embedded DB2 database may not be transferred and does not authorize the use of IBM or 3rd party tools to access the database directly.

THALES

www.thalesesecurity.com

About Thales e-Security

Thalese-Securityistheleaderinadvanceddatasecuritysolutionsandservicesthatdelivertrustwherever informationis created,sharedorstored.Weensurethatthedatabelongingtocompaniesandgovernment entitiesisbothsecureandtrustedin anyenvironment–on-premise,inthecloud,indatacentersorbigdata environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars andwiththeinternetofthings(IoT)evenhouseholddevices.Thalesprovideseverythingan organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales e-Security is part of Thales Group.

Follow us on:

Americas – 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com

Asia Pacific – Unit 4101-03, 41/F., Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com

Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thalesesecurity.com

© Thales –