Quintessence Labs

APPLICATION NOTE

qCrypt Key Management Server

Using qCrypt for VMware VM image and vSAN Encryption

Overview

This document shows how to deploy QuintessenceLabs' qCrypt key manager with VMware for virtual machine image encryption and VSAN encryption.

Intended audience: VMware and cyber security operations personnel.
Assumptions: Familiarity with configuration of VMware vSphere/vSAN.
Versions: The instructions in this document have been tested with qCrypt 1.6.3 and vSphere 6.5U2 and vSphere 6.7.

Although not formally tested, the instructions are expected to work for vSphere versions 6.5 and later. Except where otherwise indicated, instructions are expected to work for all versions of qCrypt from 1.5 and later.

Introduction

VMware added support for vSAN data-at-rest encryption, and VM image encryption in vSphere 6.5. To support encryption, it is necessary to use a third party Key Management Server (KMS) that conforms to the OASIS Key Management Interoperability Protocol (KMIP) version 1.1. The qCrypt Key Manager conforms to the OASIS KMIP standard and supports the key management requirements for VM image, and vSAN data-at-rest encryption.

In order for vSphere to communicate with qCrypt using KMIP, a mutually authenticated TLS session must be established over a TCP connection. During the TLS handshake, both vSphere (the client) and qCrypt (the server) perform a number of public key cryptography (PKC) operations to authenticate each other. Additionally, establishing the secret key used to encrypt the communications between VMware and qCrypt involves PKC operations.

The vSphere instance must be configured with PKI credentials (private key, client certificate, and trusted root, or CA, certificate) in order to successfully establish a TLS session with qCrypt.

This document shows how to configure vSphere and qCrypt to work together to enable VM image, and vSAN data-atrest encryption.

Configure vCenter

Use the following procedure to configure TLS credentials for access to qCrypt.

1. Logon to the vCenter server.
2. Navigate to vCenter >> Configure >> Key Management Servers and click on the (green +) icon to add a new KMS.
3. Fill in the required fields, including the server IP address and server port number. The default port for KMIP is 5696. The username and password fields are for optional KMIP identity information and can be left blank. They are not required for VM and vSAN encryption.
4. If you have only one qCrypt key manager, or a cluster of qCrypt key managers accessible via a load balancer through a VIP (virtual IP address), then make this the default KMS. If you have multiple qCrypt key managers, each directly accessible (i.e. not behind a load balancer), then you can either make this KMS the default, or another one.
5. You will be presented with a pop-up window displaying the TLS certificate presented by the qCrypt server to identify itself. Click "Trust" to accept this certificate. This will make vSphere trust the qCrypt appliance. The remaining steps are to make qCrypt trust vSphere.
6. Click on the link, "Establish trust with KMS...".

7. The pop-up wizard will present a number of options for trust. qCrypt supports two of the presented options. You only need to use one of the methods.

- **The certificate and private key method**
  a) Connect to the qCrypt Administration Console as an administrator with permissions to generate client credentials and register a KMIP client.
  b) Navigate to PKI Management >> Credentials and generate client credentials. Do not enter a password to encrypt the client private key file.
  c) Navigate to KMIP Clients >> Clients and create a KMIP client linked to the client credentials.
     i. In the *Action Policy* drop-down list, select *Default All Allowed*.
     ii. Leave the *Rate Limiting Policy* value set to *None*.
  d) Download the client's connection pack, selecting PEM format (you may choose either zip or tar archive options).
  e) Extract the files from the client connection pack.
  f) Copy the contents of the KMIP client certificate file, and private key file into the appropriate sections of the vCenter wizard.

- **The CSR method**
  This method is a little more complicated but has the advantage that the client's private key is kept private to the client.

  <u>On vSphere</u>
  a) Select the "New Certificate Signing Request" option and click "OK".
     This will cause vSphere to generate a new CSR, which can be copied to a clipboard or downloaded as a file.
  <u>On qCrypt</u>
  b) Connect to the qCrypt Administration Console as an administrator with permissions to modify identity information and register a KMIP client.
  c) Navigate to PKI Management >> Authority. Sign the CSR and register/download the certificate using the following four-step process:
     i. Select the file containing the CSR, or paste its contents into the box provided, and click "Upload request".
     ii. Check the validity period and selected authority, then click "Sign request".
     iii. Click on "Download certificate".
     iv. Import the signed certificate as a credential, ensuring that you select the role *client*.
  d) Navigate to KMIP Clients >> Clients and create a KMIP client linked to the newly imported certificate.
     i. In the *Action Policy* drop-down list, select *Default All Allowed*.
     ii. Leave the *Rate Limiting Policy* value set to *None*.
  <u>On vSphere</u>
  e) Click on the button "Upload file" and select the file downloaded in step c)iii above.
  f) Click on "OK".

- **The Certificate method**
  This method is not officially supported.

- **The Root CA method**
  This method is not officially supported.

vCenter is now ready for configuration of storage policies for VM and/or vSAN encryption.

About QuintessenceLabs

QuintessenceLabs' portfolio of modular products addresses the most difficult security challenges, helping implement robust security strategies to protect data today and in the future. For more information on QuintessenceLabs' data protection solutions, please visit **www.quintessencelabs.com**

Quintessence Labs

AUSTRALIA
Unit 1, Lower Ground
15 Denison St
Deakin, ACT 2600
+61 2 6260 4922

UNITED STATES
175 Bernal Road
Suite 220
San Jose CA 95119
+1 650 870 9920

www.quintessencelabs.com

Document ID: 3509
AN-2018016-001