vSphere and vSAN Encryption with Entrust KeyControl

ENTRUST

SECURING A WORLD IN MOTION

Why VM encryption?

To fully unlock all of the advantages of virtualization, it's important to have a security posture in place that is uniquely designed to protect your virtualized environment. Encrypting VMs provides a high level of security you can count on to keep critical data safe.

Reduce Risk

In a virtualized environment – with the appropriate access to the hypervisor – it becomes quite easy to copy its full contents or send it through the wire. By using encryption technology, this still may be possible, but the resulting image le is unreadable without the encryption keys.

Guarantee Availability

Adequately protecting your virtual machines by encrypting them results in a more robust solution, especially if the key management solution is designed with a high-availability (HA) architecture.

Accelerate Savings

Cost savings are one of the main reasons to explore virtualization options, but poorly organized VM encryption can quickly cause any IT savings to disappear. Implementing VM encryption at the hypervisor eliminates the need for additional, specialized hardware to perform encryption – which shrinks encryption overhead costs.

Simplify Compliance

Implementing some form of VM encryption is a requirement to comply with many standards and regulations, including Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs), and Health Insurance Portability and Accountability Act (HIPAA). Virtualized environments face new vulnerabilities that can be e ortlessly addressed with workload encryption.

Things to watch out for

Before implementing virtual machine encryption, there are several things to keep in mind.
The following checklist can help you get started:

Entrust KeyControl

Entrust KeyControl includes a fully functional KMIP (Key Management Interoperability Protocol) server that can serve as a vSphere KMS.

Once a trusted connection between KeyControl and vSphere is established, KeyControl manages the encryption keys for virtual machines in the cluster that have been encrypted with vCenter Server for vSphere Virtual Machine Encryption or VMware vSAN Encryption. The procedure is nearly identical no matter which VMware encryption method you use.
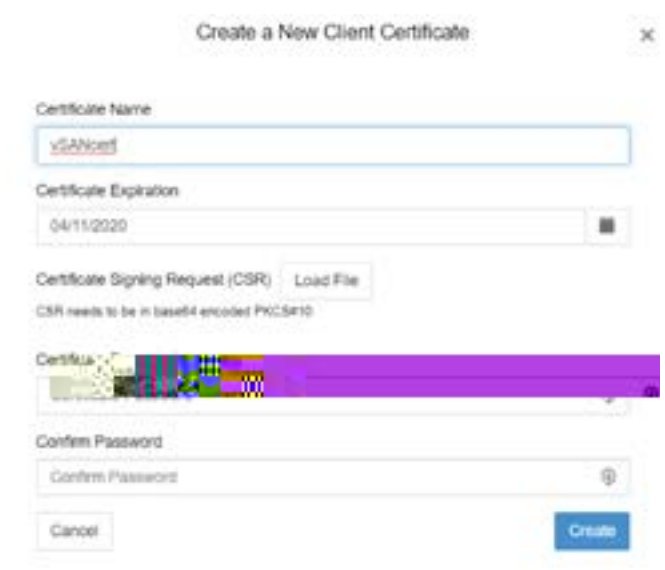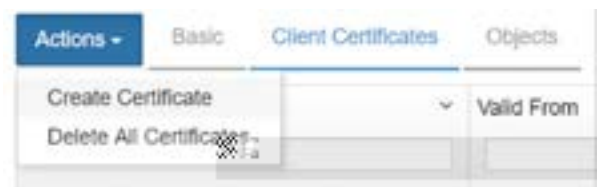
Enabling the KMIP Service

1. Log in to the KeyControl WebGUI using an account with Security Admin privileges

2. In the top menu bar, click KMIP and click the Basic tab

3. Click the State dropdown box and change it to Enable

4. Make sure the Protocol is set to version 1.1

5. Click Apply and con rm the changes when prompted

Create a KeyControl-Signed Certi cate for KMS Trust Establishment

1. In the top menu bar, click KMIP and click the Client Certi cates tab

2. Select Actions > Create Certi cate

3. In the Create a New Client Certi cate dialog box:

   a. Enter a name in the Certi cate Name eld

   b. Set the date on which you want the certi cate to expire in the Certi cate Expiration eld. If the certi cate expires, communication between vCenter and KeyControl will be disrupted until a new certi cate is uploaded

   c. Important: Do not enter a password for the certi cate. Due to a vCenter limitation, you cannot upload encrypted certi cates

   d. Click Create

Option	Description
KMS cluster	Select <Create new cluster>
New cluster name	Enter a name for the cluster. This name is local to vCenter and is not used by KeyControl.
Server address	The IP address for the Entrust KMIP server. This IP address must match the KeyControl KMIP server Host Name shown in the KeyControl WebGUI. Important: Make sure that the KMIP server resides on a device that is not encrypted.

4. Click the KMS Certi cate: Upload a File button

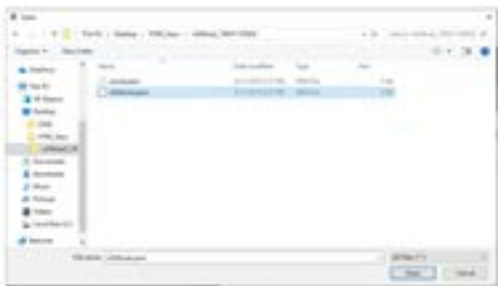

5. Select the <certname>.pem le that was previously created in the Create a KeyControl-Signed Certi cate for KMS Trust Establishment section. Click Open

6. Click the KMS Private Key: Upload a File button

7. Select the <certname>.pem le that was previously created in the Create a KeyControl-Signed Certi cate for KMS Trust Establishment section. Click Open

9. Once the certi cates are uploaded, the connection status of the KMS should change to connected and the KMS Trust Connection is established. Repeat this process again until all other KMS nodes of your HA cluster have been added

If you are required to use a vCenter Server certi cate when establishing a KMS trust connection, please refer to the Entrust KeyControl online documentation section titled, Establishing a Trusted Connection with a vSphere-Generated CSR.

Enabling Encryption on a vSAN Cluster

1. Navigate to the VSAN-enabled cluster

2. Click the Con gure tab

3. Under vSAN, select Services

4. Click the Encryption Edit button

5. On the vSAN Services dialog, enable Encryption, and select a KMS Cluster. Click Next

Optionally, you can also choose to wipe existing data from the disks as they are being encrypted. Just be aware that this can increase the time before a disk can receive data. This option removes any previous data stored on the disks.

In order to use vSphere native encryption, you must be running vCenter/ESXi version 6.5.x or later. If you are running an earlier version of vCenter/ESXi, then you will not be able to follow this procedure. However, you can use Entrust DataControl to enable encryption inside a VM no matter where the VM is running.

There is already a default VM storage policy (VM Encryption Policy) for enabling encryption on a VM. Therefore, this is the procedure to follow to enable encryption on a VM. If you are interested in creating a custom VM storage encryption policy, refer to the VMware online documentation.

1. Right-click the VM you want to encrypt and select VM Policies, Edit VM Storage Policies

3. Optionally, if you prefer to only encrypt a speci c disk attached to your VM, then toggle the Con gure per disk option and select VM Encryption Policy for VM home and/ or each disk you want to encrypt. Click OK

4. If the VM is powered on you will receive the following error. Power o the VM then attempt the operation again

NOTE: Using Entrust DataControl you can encrypt a VM or

5. Once the encryption process has completed, you will see the following icon in the Summary tab for the VM

Summary

This quick start guide describes the procedure on how to install and con gure Entrust KeyControl for enabling encryption key management in a vSphere version 6.5 or later virtual environment. The procedure for enabling vSAN and vSphere VM-based encryption is also described.

Troubleshooting

If vSphere Virtual Machine encryption or VMware vSAN encryption fails with the error "Cannot generate key", check the following:

- The Entrust KeyControl appliance must be powered on and operational. To verify this, log in to the appliance using the KeyControl WebGUI.

- The Entrust KMIP server must be enabled as described in Con guring a KMIP Server.

- The KeyControl nodes must be able to communicate with one another. Make sure the server status is not shown as Degraded in the KeyControl WebGUI.

- The KMIP client certi cate and private key must be valid and current. You can verify the certi cate status in the KeyControl WebGUI on the KMIP Servers Certi cates tab or in the vCenter Web Client on the KMS tab. For details about creating a new certi cate and key, see Creating a Certi cate Bundle for VMware Encryption.

- If the vCenter Web Client reports that the KMIP connection status is Normal (green) but encryption fails, the KMS cluster could have been added with a username and password. To verify this:

  1. Check the Entrust DataControl Audit log for the message "KMIP response rate Operation Failed DENIED".

  2. If you nd that message, edit the properties of the Entrust KMS cluster in the vCenter Web Client and remove any username or password.

- If the KeyControl cluster is functioning properly and the certi cates are valid but the vCenter Web Client reports that the Entrust KMS is not connected, you may need to remove the KMS instance and re-add it to vCenter in order to restore the Trusted connection. Select the Entrust KMS in vSphere Web Client and select All Actions > Remove KMS. Then add the KMS back as described in Creating the KMS Cluster in vSphere section.

- If everything shows as connected but encryption still fails, use the vCenter Web Client to verify that encryption is enabled for the ESXi host using ESXi-server-name > Con gure > Security Pro le > Host Encryption Mode.

	vSphere Encryption	vSphere Encryption	Entrust DataControl
Encryption Boundary	Hypervisor	Storage Driver	VM
Platforms Supported	vSphere	vSAN	vSphere/vSAN/Any Hypervisor Cloud
Granular VM Encryption		X* *Per vSan Cluster	
Dedupe/Compression	X		* *Partial Only
No Downtime	X	* *Can take considerable time to nish	
Public Cloud Support	X	X	
Encryption Travels with VM	* *Can take considerable time to nish	X	
Workload Boot/ Clone Protection	X	X	
Encrypted Backups	X	X	

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

Learn more at
entrust.com

ENTRUST