Creating a vRealize Log Insight Content Pack

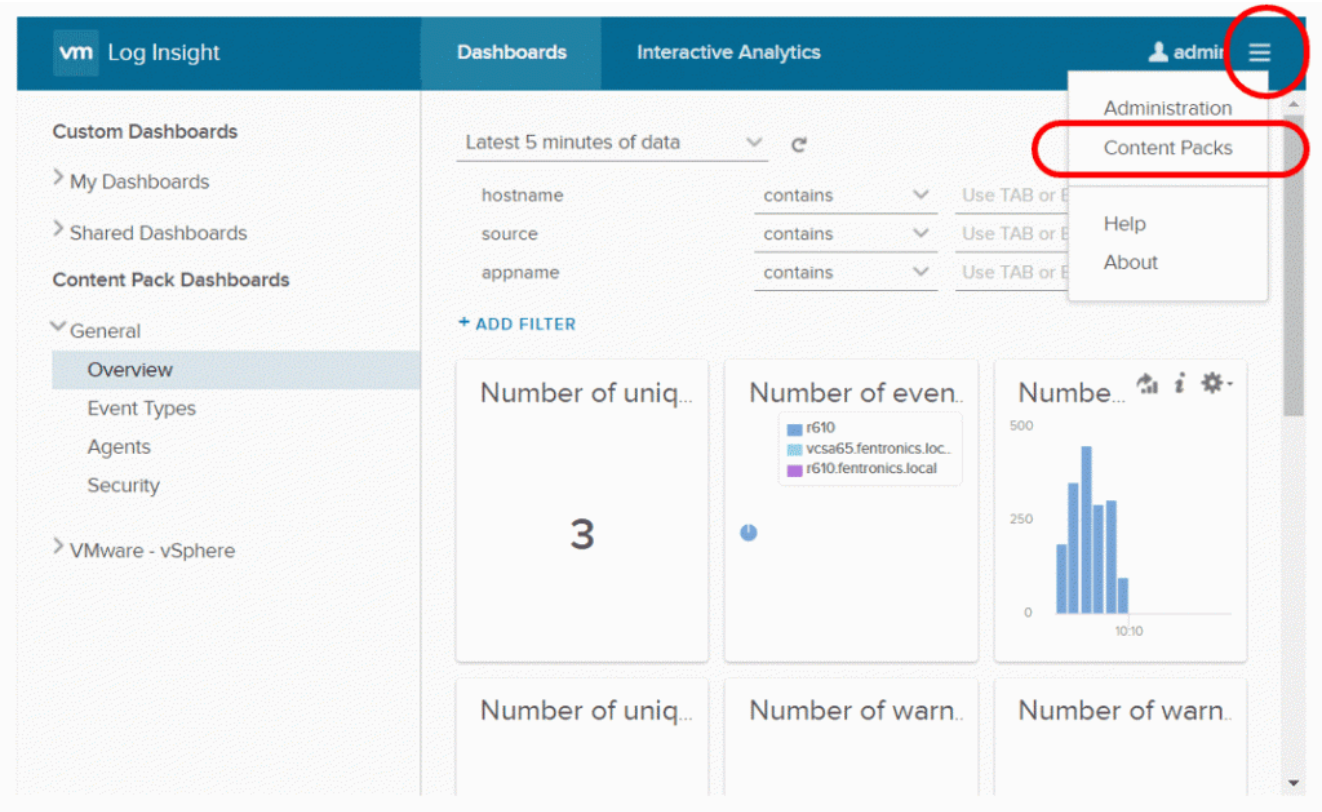
vRealize Log Insight delivers automated log management through aggregation, analytics and search, enabling operational intelligence and enterprise-wide visibility in dynamic hybrid cloud environments. Content Packs are plugins that provide pre-defined knowledge about specific types of events such as log messages. A content pack is made up of information that can be saved from either the Dashboards or Interactive Analytics pages.

Creating a vRLI content pack is relatively easy, but it may not be obvious to the casual vRLI user. Here's how to create a content pack from vRLI objects that you have created so you can use them in a different vRLI environment.

Content packs provide an effortless way to transfer or share vRLI objects from one system to another, allowing you to reuse vRLI objects on multiple vRLI systems.

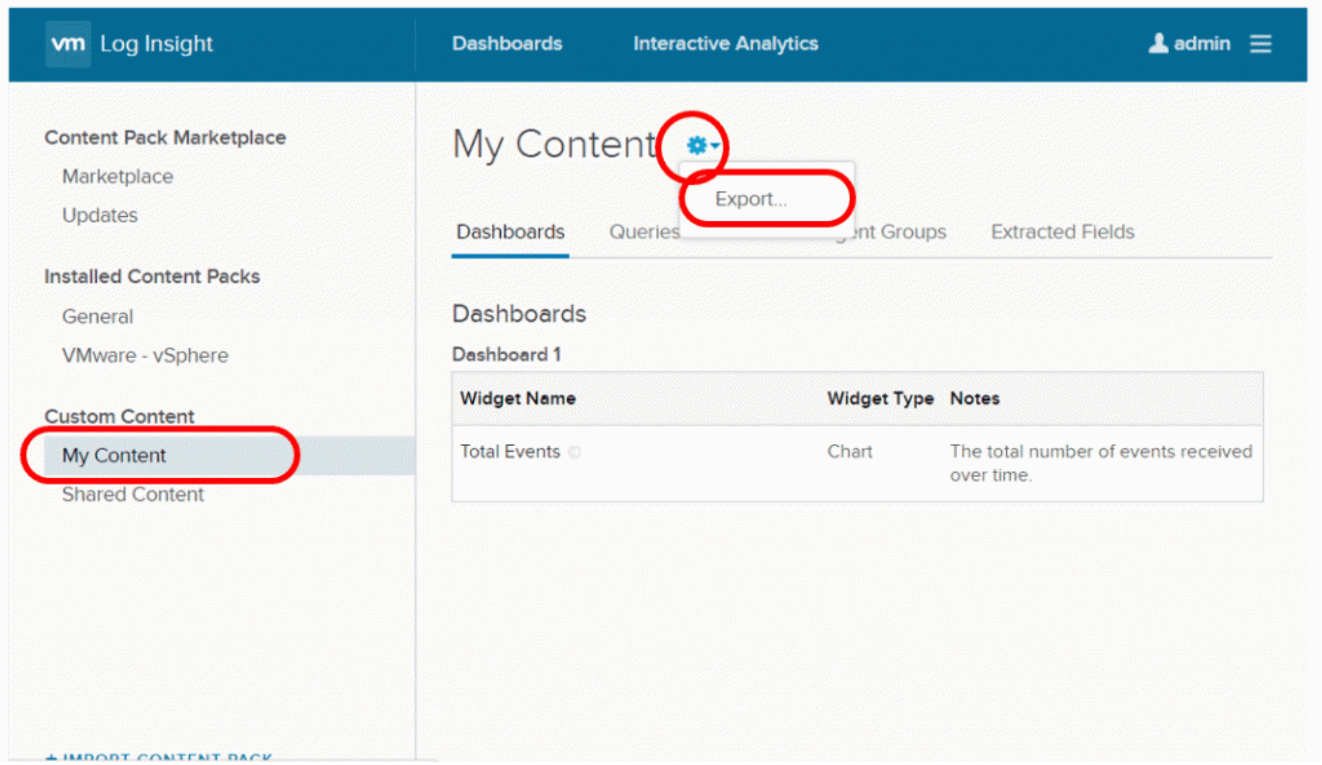
Creating and Exporting Content Packs

After creating your vRLI objects, select **Content Packs**, located on the main vRLI drop-down menu



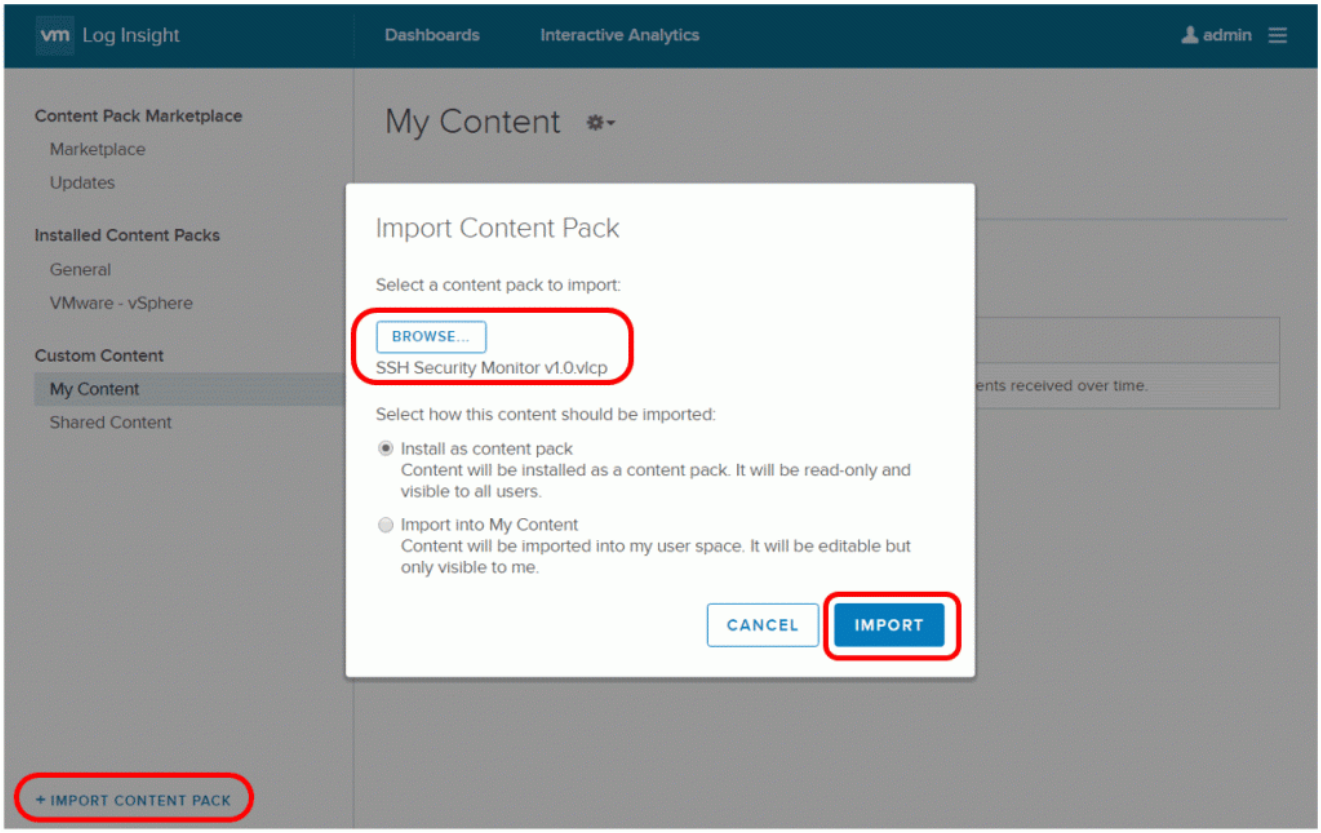
On the Content Pack page, select **My Content** from the menu in the left pane, then select the **Settings (gear)** icon to the right of My Content in the center pane. The settings icon will only appear after pointing to it. From the settings drop-down menu, select Export.

After the Export Content Pack pop-up window appears, select which objects you would like to have in your content pack on the left pane, then create a name for the content pack as well as fill out additional information on the right pane. Finally, select **EXPORT**. This will save a .vlcp file to your local system.



Importing a Content Pack

You can import the .vlcp file you created into another vRLI instance by transferring the vlcp file to the system you will be accessing the vRLI instance from, and then going to the Content Pack page. Selecting **IMPORT CONTENT PACK** at the bottom of the left pane activates up a pop-up window which allows you to import your content pack by selecting the .vlcp file saved to your local system.



[source: https://code.vmware.com/web/loginsight]

Setting up vSphere encryption

Starting from vSphere 6.5, vSphere supports VM encryption. for that a Key Management Server is required. Once a virtual machine is encrypted, vSphere needs somewhere to save the decryption key and for that it uses the KMS.VMware officially supports the use of 12 KMS products with vSphere.

https://www.vmware.com/resources/compatibility/search.php?deviceCategory=kms&details

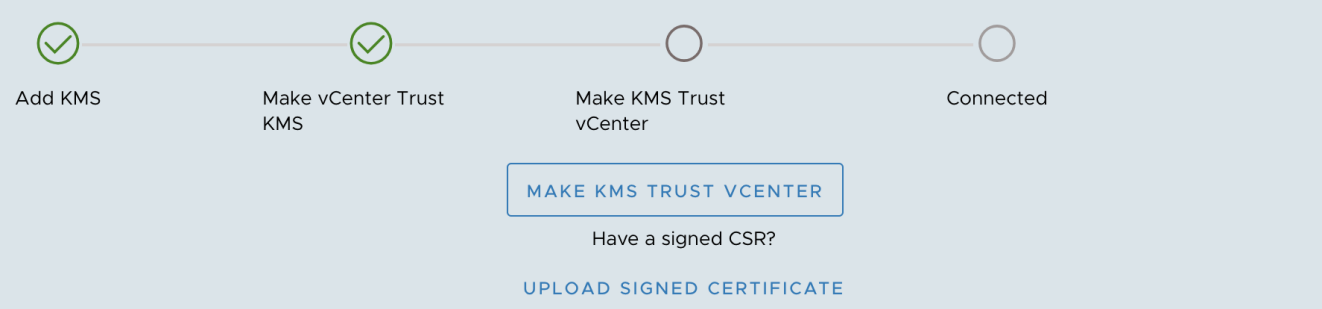
The above list is of products which have been specifically tested and certified by VMware.

After choosing the KMS solution, the appliance can be easily deployed through OVF Template.

Upon the successful deployment, You will now be shown the IP address of the KMS.

Then, you can do the rest configurations using the web browser.

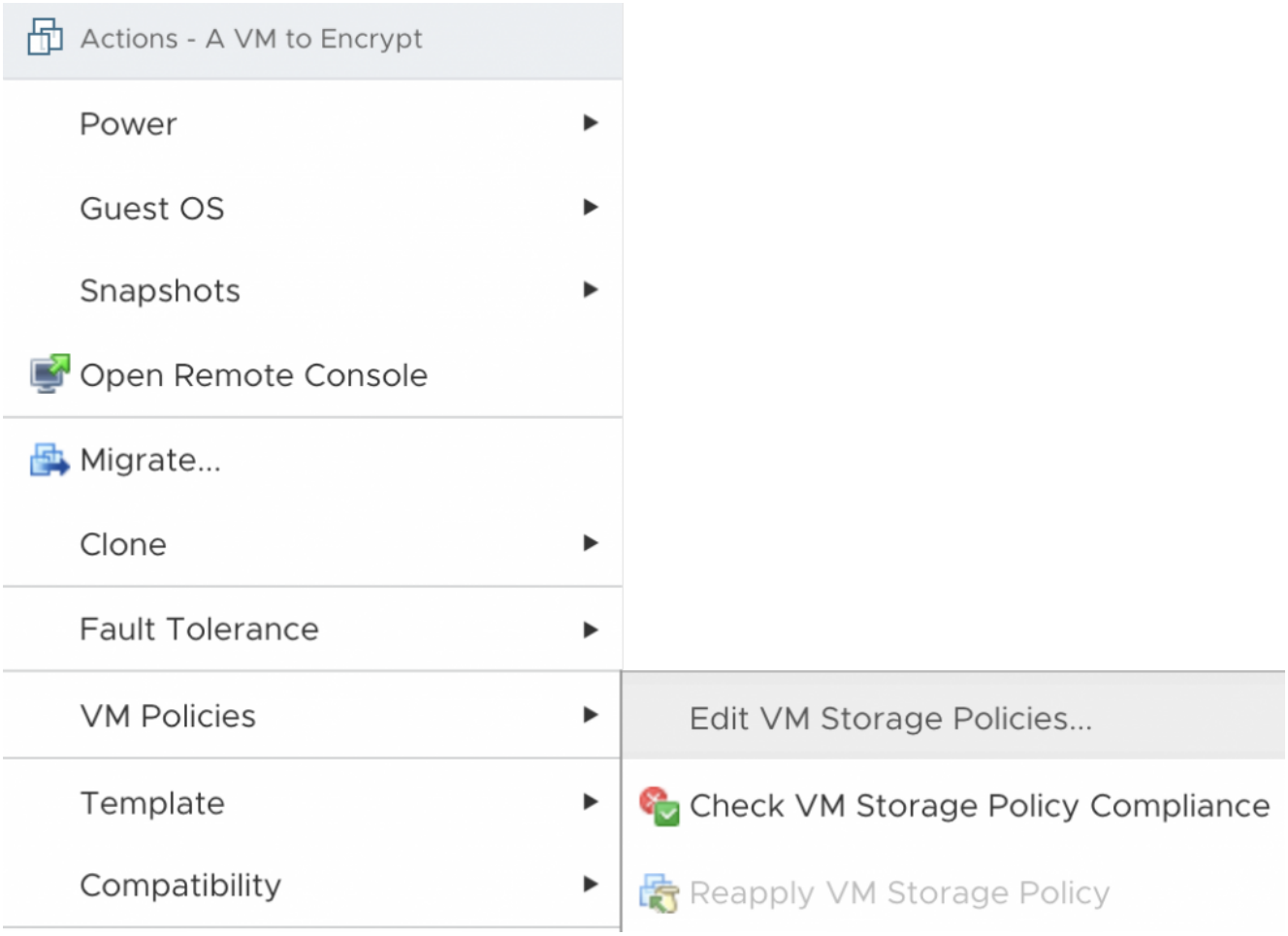
Finally, you need to setup a secure two-way trust (default method is to use Certificates) between vSphere and the KMS. Once this trust has been established the full suite of vSphere encryption features will become available.



You will now be asked to upload a KMS Certificate and a KMS Private Key file. This is the certificate we created. Open the downloaded .ZIP file and you will see two .PEM files. Ignore the ‘cacert.pem’ file, instead use the .PEM file with the name you decided earlier.

Lastly, click establish trust.

Once all the above tasks are completed, you may get the chance to encrypt the desired VMs.



Within vCenter right-click on a virtual machine that you intend to encrypt, **expand VM Policies and then select Edit VM Storage Policies, also make sure to change this to VM Encryption Policy**. Once done select OK.