



SECRETS MANAGER INTEGRATION

(Agentless Central Credential Provider CCP)

AAM INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company: LogicMonitor

Website: <https://www.logicmonitor.com/>

Name of Product: LogicMonitor Collector

Version: 1.0

Date: 7/21/2021

Partner Solution OVERVIEW

Version: 152

Platform components:

- The LogicMonitor platform consists of our cloud-based application portal and our on-premise Collector software.
- The LogicMonitor Collector can remotely monitor everything in your infrastructure, from power supplies, up to applications.
- We use existing protocols your devices already speak of (WMI, SNMP, JDBC, JMX, SSH, etc.) so you don't have to install an agent on each host.
- Monitoring is fully automated, just give us a network range and credentials, we'll discover everything and monitor it automatically.

KEY BENEFITS

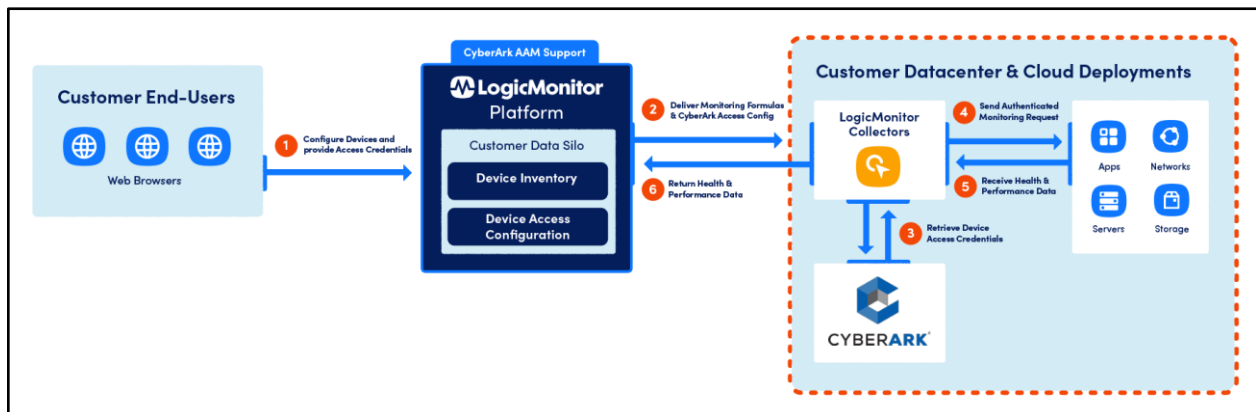
Benefits of LogicMonitor:

- Get full visibility into your hybrid infrastructure with minimal configuration.
- Reduce MTTR and increase business continuity

Benefits of integrating LogicMonitor with Secrets Manager:

- Monitor your entire infrastructure with the peace of mind that all of your secrets reside within your security parameter.
- Easily deploy, rotate, and revoke secrets and credentials used for monitoring.
- Meet compliance requirements and security regulations.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

- The integration lives on the Collector, and all of the heavy liftings takes place between the Collector and CyberArk, right in your security perimeter.
- It can be enabled on existing Collectors installed at remote sites or customer locations
- Typically you'll have two collectors at a site (one for failover), both configured to use CyberArk

CREDENTIAL RETRIEVAL

- The Collector will retrieve only the credentials it needs to monitor the devices it is assigned to. The update interval can be configured by the user.
- The Collector will retrieve credentials and refresh them as needed. Users can configure how long they're cached.
- The Collector gets CyberArk authentication information from the portal. These settings (client certificates, CyberArk AAM URL) are configured as resource properties in the LogicMonitor portal. These are the only credentials that will leave your security perimeter.
- To make queries to CyberArk, you'll need:
 - Linux
 - Client authentication certificates required
 - Windows
 - Client authentication certificates, or
 - OS user authentication

REQUIREMENTS

- One or more LogicMonitor Collectors (EA 29.108 or higher) with access to the Internet, and your CyberArk AAM instance.

AAM INSTALLATION

Refer to [CyberArk Agentless installation and configuration](#).

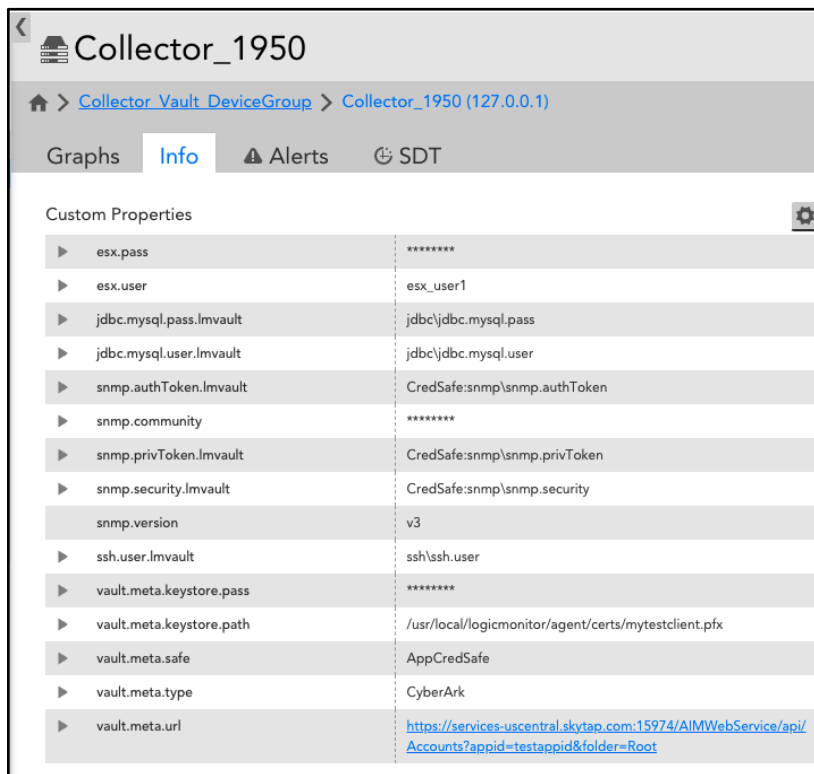
AAM CONFIGURATION

The following sections provide details on LogicMonitor CyberArk Secrets Manager Integration configuration with CyberArk.

INTEGRATING CREDENTIAL VAULT PROPERTIES

To integrate the Credential Vault with LogicMonitor Collector, complete the following steps.

1. Navigate to **Resource> Device> Collector> Info** tab and add vault metadata properties to the Collector. For more information on vault properties, see [Adding Vault Properties](#).



2. Click **Settings** on the left panel and select **Collectors**.
3. Select the required Collector and click the **Settings** icon under the Manage column.
4. On the Manage Collector dialog box, select **Collector Configuration** from the **Support** drop-down list.

Manage Collector Support

Description
ip-172-31-1-131.us-west-2.compute.internal

Collector Group
MRods LMX Collector Group

Collector Down Escalation Chain
Disable notification

Send Collector Down Notifications
☐ One time
☒ Every 15 minutes

Failover Collector
None

Custom Properties

Name	Value
No records. Click here or the "+" button to add a new record.	

[Delete](#) [Save](#)

5. Ensure to set the vault.bypass value to **false** in agent.conf. Additionally, you can add the required agent configuration properties to set the Collector. For more information, see [Collector Configurations](#).

Collector Configuration Support

Agent Config WatchDog Config Wrapper Config Sbproxy Config Website Config

Collector Size
Nano (requires < 2GB)

[Collector Size Info](#)

☒ Edit agent.conf manually

```
# logsource.k8spodlog.filter.6.message.regexnotmatch=
config.source.collect.retry.count=3

lmlogs.encrypt.data.saved.in.queue=false
lmlogs.salt.for.encryption=

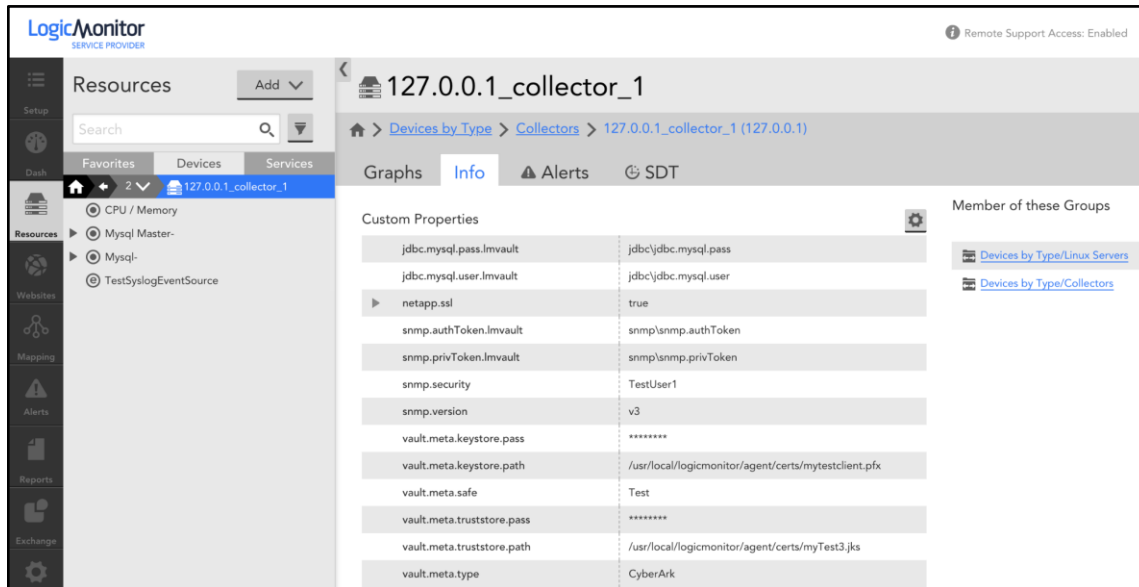
lmlogs.logsource.syslog.unmapped.resource=
# OMI configurations: linux to windows Monitoring
omi.https.enable=true
linux.collector.enable.windows.monitoring=false

EnforceLogicMonitorSSL=false
reduce.logger.enable=true
vault.bypass=false
```

[Cancel](#) [Save and Restart](#)

LOGICMONITOR COLLECTOR AND CYBERARK VAULT INTEGRATION

1. Multi-Safe support: Specify the multiple safes under a device to retrieve the credentials from Multiple Safe.



2. Multi-Vault support: You can use multiple vaults for the devices under the collector. Each of the devices can point to a single Vault.
3. You can call Vault API over HTTP or HTTPS. However, if you are calling the Vault APIs over HTTPS, you must configure the RootCA cert. For more information, see [RootCA cert](#).
4. You must complete the CyberArk Authentication. For more information, see [CyberArk Application Authentication Methods](#) section.

Note: Device-specific cache is implemented at the Collector to avoid frequent requests to the Vault API.

CYBERARK COLLECTOR AGENT CONFIGURATION SETTINGS

The following table contains the collector agent configuration related to the vault:

Name	Type	Default	Details
vault.bypass	Boolean	True	If the value is set as true, the vault API will not be called. If the value is set as false, the vault API would be called.
vault.credentials.cache.expirationtime	Integer	60 minutes	Expiration timeout (in minutes) for credentials in vault cache. After this time, the credentials in the vault cache expires and would have to be re-fetched from the Vault.
vault.credentials.refresh.delay	Integer	15 seconds	The amount of time delay (in seconds) after credentials cache expiration time. Refresh the task after the cache expiration time. Note: You may customize the amount of time delay while installing the Collector. For more information, see agent.conf Collector Settings .

CYBERARK VAULT PROPERTIES

Vault properties, such as Vault Metadata and Vault Keys for the Collector, can be configured at the device or device group level.

Note: CyberArk does not allow special characters, such as \ / : * ? " < > <tab>, to be used in Safe names and object names.

VAULT METADATA

The following table lists the Vault Metadata properties.

Vault Metadata	Description
vault.meta.url	URL of the vault. This URL must contain the folder and application id only.
vault.meta.safe	Safe (Applicable only in case of CyberArk). A device can have only a single safe.
vault.meta.type	The type of the Vault. Currently, only the "CyberArk" vault integration is supported in the Collector.
vault.meta.header	The headers required for HTTP Get Request. The value for this custom property would be the header separated with "&" the header key value would be separated with "=" as shown in the below example: vault.meta.header - Content-Type=application/json&Accept-Encoding=gzip, deflate, br
Vault.meta.ca.authentication.method - basic	The basic authentication method is used for integrating the vault.
vault.meta.ca.user.name	The username to authenticate the vault.

vault.meta.ca.user.pass	The password to authenticate the vault.
vault.meta.keystore.type	Type of the key store. If the key store type is not specified, the default type for the key store is JKS.
vault.meta.keystore.path	Path of the Keystore file.
vault.meta.keystore.pass	Password for the Keystore.

VAULT KEYS

Vault keys need to be specified at the device level with suffix **.Imvault**. For example, **ssh.user** information should have the key specified as **ssh.user.Imvault**.

Vault Keys	Description
Property suffixed with .Imvault	The custom property for which value must be retrieved from the Vault and must be specified at the device level by adding suffix .Imvault. The value of such property would be the path of the key in the Vault. For example: <code>ssh.user.Imvault = ssh\ssh.user</code> For <code>ssh.user.Imvault</code>, the property should be retrieved from the Vault. The value of this property "<code>ssh\ssh.user</code>" represents the path in the Vault where the credential is stored.
Property suffixed with .Imvault : Multi-Safe	The multi-Safe approach allows fetching the values for Imvault properties from different safes within the Vault. The LM vault property value should be specified in the format <code>safe:path</code>. For example, the property referring to the safe <code>sshcreds</code> and object path as <code>ssh\ssh.user</code> can be specified as: <code>ssh.user.Imvault = sshcreds:ssh\ssh.user</code>

	The Safe specified at the property level would override the value specified at the device level through the “vault.meta.safe” property.
--	--

PARTNER CONTACT INFO

Business Contact	Name	Catherine Davis
	Email	catherine.davis@logicmonitor.com
	Tel	805-617-3884
Technical Contact	Name	Michael Rodrigues
	Email	michael.rodrigues@logicmonitor.com
	Tel	805-617-3884
Support Contact	Name	Michael Rodrigues
	Email	michael.rodrigues@logicmonitor.com
	Tel	805-617-3884