Installation Checklist – Helm Chart

Virsec Security Platform 2.6

www.virsec.com
support@virsec.com

Contents

About This Document

This document describes all the information related to the **Virsec Security Platform (VSP)** infrastructure. The pre-requisites for Management and Worker Nodes along with VSP components specifications are described in various sections. The information related to Interfaces configuration and Application creation in CMS is also specified.

1. Contact Virsec

In case of any questions please contact Virsec Systems at 1-877-213-3558 OR support@virsec.com.

2. Virsec Security Platform Version

The version is **Virsec Security Platform (VSP) 2.6**

3. Pre-requisites

NOTE:

It is expected that relevant licenses and required operational support are procured for the software mentioned in the pre-requisites

3.1. Management Node

Management Node has the below pre-requisites:

1. Ensure that the below software is installed:
   a. Helm v2 OR v3
2. Ensure access to the docker registry

3.2. Worker Node

VSP CMS is deployed across multiple-pods.

3.2.1. CMS Services Pod

1. Disc space: Min 28 GB in `/var` partition
2. Docker must be installed
3. Internet connectivity is required for the installation of some dependencies if Alpine/Debian installers are utilized
4. Minimum Specification
   a. CMS – 16 GB Node

4. Overview

VSP is composed of various architectural elements. The components include:

1. LFR Pod – Local File Repository Pod
2. CMS Services Pod – CMS component hosting all service containers and Ngnix container
3. Kafka Pod – CMS component hosting Kafka infrastructure
4. Redis Pod – CMS component hosting Redis infrastructure
5. MongoDB Pod – CMS component hosting MongoDB infrastructure
6. VSP Agent – VSP component installed on the Application Container
7. VSP Controller – VSP component that interacts with CMS
8. vRule Engine – VSP's rule engine

5. VSP Components Specifications

Table 1 below lists the specifications for VSP components

Component	Minimum Configuration	Container Operating System
CMS		
LFR Pod	CPU: 1 CPU RAM: 1 GB	Debian 10
Kafka Pod	CPU: 2 CPUs RAM: 4 GB	Alpine Linux
CMS Services Pod with CMS services and Ngnix Container	CPU: 8 CPUs RAM: 16 GB	Alpine Linux
Redis Container	CPU: 1 CPU RAM: 2 GB	Alpine Linux
MongoDB Container	CPU: 2 CPUs RAM: 8 GB	Alpine Linux

Table 1 – VSP Component Specification

Here are the VSP Idle usage specifications:

Component	Operating System	Feature	Minimum Requirements	
			Memory (MB)	Disc (MB)
VSP Probe	RHEL and Ubuntu	VSP-Host, VSP-Memory	100-200	100-200
VSP Sidecar	Alpine Linux	VSP-Host, VSP-Memory	200-300	200-300
VSP Probe	RHEL and Ubuntu	VSP-WEB	200-600	500-600
VSP Sidecar	Alpine Linux	VSP-WEB	200-600	500-600
vRule Engine	RHEL	Remote vRule Engine	500-600	500-600

Table 2 – VSP Idle Usage specification

6. Communication Matrix

Table 3 below lists all the ports utilized by VSP components. If the VSP components are installed in different subnets or zones, the below firewall rules need to be established for seamless communication among them.

Client	Server	Client Port	Server Port	Protocol
VSP Controller	**CMS**	**Any**	**443**	**TCP**
VSP Controller	**Kafka**	**Any**	**9092 (**Secure Kafka ***not*** enabled**) OR** **9093 (**Secure Kafka enabled**)**	**TCP**
VSP Controller	**Remote vRule (Optional)**	**Any**	**55555**	**TCP**

Table 3 – Communication Matrix

All nodes should have high-speed internet access to the below URL list:

Client	Server
LFR	**Artifactory Directory:** https://vartifacts.jfrog.io
CMS **VSP Controller**	**Virus Total:** https://www.virustotal.com/
	Reversing Labs: https://ticloud-aws1-api.reversinglabs.com/ https://ticloud-cdn-api.reversinglabs.com/
	VSP Licenses: https://flex1298.compliance.flexnetoperations.com/

Table 4 – URL Access

Ensure that the nodes have connectivity to the below URLs/repositories during VSP Probe (Controller and vRule Engine) installation:

Operating System	URL/Repository	Dependency Packages Downloaded
Ubuntu, Debian	"apt-get" repo	sudo, libexpat1, libffi6 and libssl-dev
	https://download.java.net/java/ga/jdk11/openjdk-11_linux-x64_bin.tar.gz	openjdk11
Amazon Linux	https://corretto.aws/downloads/latest/amazon-corretto-11-x64-linux-jdk.tar.gz	jdk
Alpine	"apk" repository	sudo, libstdc++, hyperscan and openjdk11

Table 5 – Dependencies URL Access

7.Interfaces Configuration

7.1.Email Service

Specify the following attributes in CMS to configure the email service used to notify the application updates to the users. Configure either CMS Internal Server or an External Email Server on CMS.

Attribute	Description
Internal Email Server	
Sender Email	**Email Address of the Sender**
Sender Name	**Name of the Sender**

External Email Server	
Server Host	The DNS hostname or IP address of the Email Server
Protocol Type	Mailing protocol to be utilized
Use STARTTLS Encryption	Select appropriate option to turn the Encryption On or Off
TLS Version	Select the version of TLS protocol
Account Username	Account representing VSP on the Email Server
Password	Password associated with the Account Username
Port	Email Server Port
Retry Count	Maximum number of retry attempts to establish connection with the Email server
Sender Email	Email Address of the Sender
Sender Name	Name of the Sender

Table 6 – Email Service Attributes

7.2.LDAP Integration

Attribute	Description
LDAP Connection	
Host	The DNS hostname or IP address of the LDAP or AD server
Port	Port number for LDAP or AD server access
Protocol	Select the appropriate Protocol from the drop-down: LDAP or LDAPS
Validate Server Certificate	If enabled, the server certificate is validated
Authentication Realm	User defined value that defines the authentication directory and associated policies to search for users and groups
Timeout (seconds)	The number of seconds the system waits for a response from the LDAP server before it closes the connection and tries to connect again
Dead Time (minutes)	The time (in minutes) that the system considers an unresponsive authentication server to be “dead” or “out of service”. During this time, the system falls back to using local authentication. After every Dead Time expiry, the system attempts to determine if the server is active again
Retry Count	The number of times that the system attempts to connect to the LDAP server. If the number of timed-out attempts reaches the configured Retry count, it is considered inactive (dead) and the Dead Time timer starts. Further traffic is not sent to the server till it becomes responsive again

LDAP Connection Authentication Parameters	
Authentication Method	Select the appropriate method from the drop-down – Anonymous, Simple or Strong. LDAP supports Simple method ONLY
Bind DN (Username)	Distinguished Name (DN) of a user in the directory that has read access to all information about valid users. Example: `uid=admin,ou=system`
Bind Password	Password for the provided Bind DN
LDAP User Binding Parameters	
Base DN	The base of the search tree for all users. Example: `ou=users,dc=adobe,dc=com`
User Object Class	Filter for directories where the Base DN is a mix of object types (Example: people, groups, printers, etc) and the search scope has to be limited to “people”
Login Attribute	Attribute of the LDAP directory users that will be used to log in. Example: user ID or full email address or both. Value must be `“cn”`
Real Name Attributes	Attributes of the Object class that supplies the real name of the user to be mapped to the real name of the user in CMS
Email Attributes	Attributes of the Object class that supplies the email address of the user
Advanced	
Search within Nested Group	Enable or disable searching within nested groups. This option is disabled by default

Follow Referrals	**In multi-tenant or multi-domain enterprise forests, AD/LDAP queries may be referred to another server. A referral is when an LDAP server forwards an LDAP client request to another LDAP server. This option is disabled by default**
Limit Referrals	**The number of referrals that should be followed when AD replies with a Referral response. Select the appropriate value from the drop-down. The default selected value is "5"**

Table 7 – LDAP Integration Attributes

7.3.Proxy Settings

When direct internet connection is NOT available for CMS, configure a proxy server to enable CMS to Procure the Threat Intelligence and Communicate with Cloud based License Server

Attribute	Description
IP Address	**IP Address of the Proxy Server**
Port	**Port of the Proxy server**
Username	**Authentication username**
Password	**Password associated with the configured Username**
Authentication Method	**None OR NTLM**
Domain	**For NTLM only**

Table 8 – Proxy Server Attributes

7.4. Threat Intelligence

Specify the following attributes to configure Threat Intelligence as VirusTotal OR Virsec Threat Intelligence tool

Tool	Attribute
VirusTotal	**URL**
	API Key
Virsec Threat Intelligence	**Username**
	Password

Table 9 – Threat Intelligence Attributes

-- END OF DOCUMENT --