Forcepoint Data Security Posture Management

Powered by Getvisibility

FDV Server Installation Guide

Forcepoint

Report

Forcepoint April 23, 2024

PREREQUISITES	2
K3S INSTALLATION	2
RANCHER	3
KEYCLOAK	5
Logging into Keycloak Admin Panel	5
COMPLETING THE REALM CONFIGURATION	6
COMPLETING THE DASHBOARD CLIENT CONFIGURATION	8

Prerequisites

A VM or server with the following specifications:

- 16 x CPU cores (x86_64 processor with speed of 2.2 GHz or more). The CPU must support the instructions SSE4.1 SSE4.2 AVX AVX2 FMA
- 64GB RAM
- 700GB Free SSD disk. K3s will be installed in /var/lib/rancher so space should be allocated there. We also need 10-20 GB free space at / and /var.
- Ubuntu 20.04 LTS Server OS is recommended. RHEL 8.6, 8.7, 8.8, & 9.2, and Suse Linux 15.3 are also supported but may need extra configuration.
- Port 443/TCP open
- Outbound internet access to download application artefacts. 100 Mbps download speed recommended
- Domain Name Service (DNS) with public name resolution enabled
- Network Time Protocol (NTP)
- Software Update Service access to a network-based repository for software update packages.
- Fixed private IPv4 address
- Unique static hostname

K3s Installation

From the command line of your chosen server, apply the following commands as root.

• This command instals K3s as well as checks the prerequisites:

```
curl -sfL https://assets.master.k3s.getvisibility.com/k3s/k3s.sh |
INSTALL_K3S_VERSION="v1.26.10+k3s1" K3S_KUBECONFIG_MODE="644" sh -s - server --node-
name=local-01
```

 Once complete, copy the cURL command you received when registering the deal. It will look something like this:

read -p "Please type your email address: " user_email && kubectl apply -f
https://rancher.forcepointemea.k3s.getvisibility.com/v3/import/8wc8b6dnb9xvlh7grcrjpdwh55nc
st2s9fqm96kt8zhc2k2stm7vck_c-m-6skspsgh.yaml && curl -k --location

```
"https://customer-management.master.k3s.getvisibility.com/v1/updateClusterState/40093321-
a4e2-4fe2-9493-36dc4b2ba7ab?email=$user email"
```

Make sure to enter your email address to correctly install the platform and register with our customer service.

For security reasons the registration command can be used only a single time, the command becomes invalid after the first use. In case you need to run it again you must contact support.forcepoint.com for a new registration command.

• To monitor the progress of the installation, enter the following command:

```
watch -c "kubectl get deployments -A"
```

The K3s deployment is complete when elements of all the deployments (coredns, local-path-provisioner, metrics-server, traefik and cattle-cluster-agent) show at least "1" as "AVAILABLE"

• In case of errors, you can inspect the logs of a pod using kubectl logs , e.g.

kubectl logs cattle-cluster-agent-d96d648d8-wjvl9 -n cattle-system

When installation is complete go to the rancher site associated with your region.

Rancher

The region and cluster name can be found in the registration email that was sent to you when you registered the deal.

1. Go to your regional Rancher dashboard and wait for the new cluster to become Active.

Forcepoint						:	
Learn more about the improvements and new capabilities in this ve	ersion.						
Clusters 293		Ma	anage Import Ex	isting Create		Links	
State 🗘 Name 🗘	Provider 🗘	Kubernetes Version	CPU 🗘	Memory	Pods 🗘		
Pending	Imported Imported						
Pending	Imported Imported						
Pending	Imported Imported						
Pending	Imported Imported						
Pending	Imported Imported						
Pending	Imported Imported						
Pending	Imported Imported						
Pending	Imported Imported						
Pending	Imported Imported						
Pending	Imported Imported						
Active EXAMPLE_CLUSTER	Imported K3s	v1.24.9+k3s2	20 cores	78 GiB	65/110		

Figure 1.

 Once Active elect the cluster name and go to Apps > Charts and install the GetVisibility Essentials and GetVisibility Monitoring Helm charts:

Cluster	*			
Workloads	↓ Charts			
Apps	^ All	 All Categories 	✓ getvis	
Charts Installed Apps	3			
Repositories	3 GetVisibility Docker Image cache	GetVisibility Docker Image Puller	GetVisibility Essentials	GetVisibility Gatekeeper
Recent Operations	0 A Heim chart for GetVisibility Kube auto fledged	A Helm chart for GetVisibility Kube auto puller	A Helm chart for GetVisibility Essential Services (Consul, Postgresql, Kafka, ElasticSearch and MinIO)	A Helm chart for GetVisibility to enforce K8s policies
Service Discovery	Ŭinuxoni	i Unux only	Linux only	Unucony
Storage				
Policy Monitoring	GetVisibility Kafka Console	GetVisibility Kafka UI	GetVisibility Monitoring	GetVisibility Private Registry
More Resources	A Heim chart for Kafka-Console (only accessible in dev environment)	A Helm chart for Kafka-UI (only accessible in dev environment)	Collects several related Helm charts, Grafana dashboards, and Prometheus rules combined with documentation and scripts to provide easy to operat	A Helm chart for GetVisibility Private Registry
	Unacon	Linux only	Linux only	Linux only
	gv-model-deployer GetVisibility Models	gv-models-csi GetVisibility Models CSI mounter	gv-platform GetVisibility Platform	
	GetVisibility Models		GetVisibility Platform	
	Unucon	Linux only	Unuconly	
Cluster Tools				
v2.7.6				

Figure 2.

Use default values for both installations

3. Go to the global (burger) menu **Continuous Delivery > Clusters** and click on **Edit config** (three dots) for the cluster you are using:

Continuous Delivery											fleet-de	rfault ~		л.
board Ippos 4	Clusters													
er Groups 3 ed v	11 Pause	O Force Update	Change workspace	▶ Unpause		l								
ມ *	🔲 State 🗘	Name 0					Nodes Read	dy⊜	Repos R	leady 0	Resources	Last Seen 🌣 Age 🗘		
	Active	EXAMPLE_CLUSTER	2				1		2	1	-	2.9 mins ago 198 day	s i	
						Figure 3								
					Paus	e								
				C	Force	e Upd	ate							
				Ö	Char	nge wo	orkspa	ace						
				- 💊	Edit	Confi	g							
					Edit `	YAML								
				$\overline{\mathbf{T}}$	Dow	nload	YAMI							



4. Add 2 labels product=focus environment=prod and press Save.

Labels		
Key/value pairs that are attached to objects which specify identifying attributes.		
Key	Value	
cluster_name	EXAMPLE_CLUSTER	Remove
cluster_reseller	forcepoint	Remove
environment	prod	Remove
objectset rio.cattle.io/hash	174fe418a2c0c3c0725159260640e351473289432	Remove
product	focus	Remove
	k3s	Remove
provider.cattle.io		

Figure 5.

The cluster is now set up and you can move onto user configuration.

Keycloak

Keycloak is an open-source product that allows Single Sign-On (SSO) and enables Identity and Access Management integration to allow for a quick, safe, and secure integration of authentication within modern applications.

When a cluster is generated via the Getvisibility reseller dashboard, it creates a Keycloak instance within the cluster for managing authentication.

When this cluster is created, a default Keycloak Realm configuration is loaded, and only a few installation steps are required.

This document describes the remaining installation steps required to complete the Keycloak installation setup.

Below are the steps involved in configuring Keycloak, and you may choose to skip the Optional steps based on your preferences:

Logging into Keycloak Admin Panel

The Keycloak admin URL will consist of the following components:

- The domain that has been configured for your reseller to access the application (E.g. **my-dashboard.com or 10.10.121.127**)
- The service path (E.g. auth for Keycloak)
- The keycloak admin path /admin/master/console

An example of the above might look something like this:

https://my-dashboard.com/auth/admin/master/console

Once you have entered the correct address for your cluster Keycloak instance following the above guidelines, you should be able to log in to the Keycloak admin dashboard using the following details:

Username: admin

Password: admin

The access protocol should always be https.

The domain in the example above (e.g. my-dashboard.com) might not be applicable if a domain is not configured, in which case you would need to use the server IP address (e.g. 10.10.121.127).

Once logged into the portal, there are a few steps to complete to configure Keycloak.

Completing the Realm Configuration

In Keycloak, a **Realm** is a top-level authentication domain that contains an isolated authentication configuration.

A good way to imagine this is that each Keycloak Realm might represent a different environment.

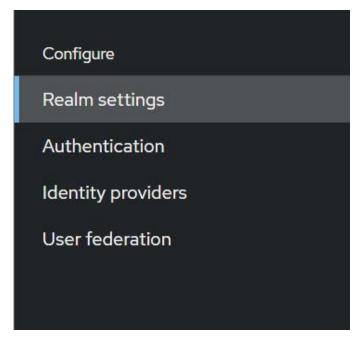
We need to have a Realm for managing our cluster authentication, please follow the steps below to do this:

1. Make sure that the gv realm is selected in the top left, not master.

gv		•
gv		~
master		
	Create Realm	

Figure 6. Dashboard

2. Click on the left-side menu item **Realm settings**.





3. This will load the Gv Realm **Settings** → **General** tab, enter your desired user-friendly **reseller** name into both the **Display name** and **HTML Display name** fields.

=										0	admin 🔻	۲
gv • gv		ngs that cor	atrol the o	ptions for us	ers annli	cations role	s and arouns in	the current realm.	arn more 🔽	C Enable	d Action	•
Manage	in settings are setti	ings that cor	ition the o	puons for as	iers, uppir	cutions, role	o, and groups in					
Clients	< General	Login	Email	Themes	Keys	Events	Localization	Security defenses	Sessions	Tokens	Client polici	>
Client scopes												
Realm roles Real	m ID *	gv								¢.		
Users												
Groups	lay name	Getvisibilit	У									
Sessions HTM	1L Display name	Getvisibilit	y									
Events	itend URL ③											
Configure Req	uire SSL ③	External re	quests							•		
Realm settings												
Authentication 3	to LoA Mapping						been defined yet. G tes, key and value a					
Identity providers					button		key pair.	are required for a				
User federation						0	Add an attribute					
Use ⑦	r-managed access	Off										
Endj				nfiguration 🖸								
	J	Save	Revert									
				Figu	re 8.							

4. Click the **Save** button to commit these changes to the Realm Settings.

A Do not change the content of **Realm ID** field, it must be **gv**.

Completing the Dashboard Client Configuration

1. Click on the **Clients** menu item on the left-side menu, this should load a list of authentication clients.

=					③ admin ▾	2
gv 💌	Clients Clients are applications ar	nd services that can request at	uthentication of a	user. Learn more 🔀		
Manage				_		
Clients	Clients list Initia	l access token Client regis	tration			
Client scopes	Q Search for client	→ Create o	lient Impor	client	1-8 * <	>
Realm roles						
Users	Client ID	Name	Туре	Description	Home URL	
Groups	account	\${client_account}	OpenID Connect	=	https://10.30.4.28/auth/realms/gv/account/ 🗹	:
Sessions	account-console	\${client_account-console}	OpenID Connect	-	https://10.30.4.28/auth/realms/getvisibility/account/ 🗹	:
Events	admin-cli	\${client_admin-cli}	OpenID Connect	-	-	÷
Events	agent	-	OpenID Connect	-	-	:
Configure	broker	\${client_broker}	OpenID Connect	Ψ.	-	:
Realm settings	dashboard	Dashboard	OpenID Connect	Dashboard authentication client	Ξ.	÷
	realm-management	\${client_realm-managemen	OpenID Connect		-	:
Authentication	security-admin-console	\${client_security-admin-co	OpenID Connect	-	https://10.30.4.28/auth/admin/gv/console/	÷
Identity providers						
User federation					1-8 - >	

Figure 9.

2. Click on the name link of the item labelled dashboard to navigate to its client configuration page.

dashboard	Dashboard	OpenID Connect Dashboard authentication client	-	:
		Figure 10.		

3. Update the Valid Redirect URIs to include the URL you have configured for the Dashboard UI. This will allow Keycloak to redirect back to your Dashboard UI after authenticating.

Valid redirect URIs 💿	/*	•
	https://my-dashboard.com/*	•
	Add valid redirect URIs	

Figure 11.

4. Update the Web Origins to include the URL you have configured for the Dashboard UI. This will allow CORS endpoint calls to Keycloak from the Dashboard UI.

Web origins ③	\${authBaseUrl}	•
	https://my-dashboard.com	•
	Add web origins	

Figure 12.

5. Open the dropdown for Login Theme and select the theme created for your reseller (E.g. my-reseller-theme).

URL ②

Login theme ③	getvisibility-theme •
	Figure 13.
	nannel logout URL field's content. This way, instead of the "you are getting logged ou straight to the login page upon logout.
Alternatively, you	can enter the Front-channel logout URL in the following format:
https://my-dasl	hboard.com/auth/realms/gv/protocol/openid-connect/logout.

Front-channel logout https://my-dashboard.com/auth/realms/gv/protocol/openid-connect/logout

Figure 14.

6. Click the **Save** button at the bottom of the screen.



forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

© 2024 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners. [Forcepoint Data Security Posture Management Powered by GetVisibility FDV Server Installation Guide] [Status]23 Jul. 24