Forcepoint Data Security Posture Management

Powered by Getvisibility

GV Installation Training



Report

Forcepoint April 23, 2024

Table of Contents

AGENDA	2
QUICK LOOK AT THE INSTALLATION STEPS	2
REQUIREMENTS	2
REQUIREMENTS	2
Hardware specifications (General)	
Additional & Networking	
K3s & Important Notes:	
RANCHER CONFIGURATION	4
Generating a Registration command	4
KEYCLOAK (CONFIGURE DASHBOARD ACCESS)	
BASIC POLICY CONFIGURATION (AGENT V4)	6
System Plugins	7
Plugins	8
Macros (old overrides)	8
Agent Deployment	11
DOCUMENTATION	

Agenda

- 1. Requirements
 - What are the requirements, and how to check them
 - K3s installation
- 2. Rancher configuration
 - Import Cluster & generate registration command
 - Backend configuration & installation
- 3. Keycloak Configuration
 - Configure access to dashboard
- 4. Basic Policy Configuration
 - Configure policy with labels and basic rules
 - Enable/create regex patterns
 - Some Expert mode tips
- 5. Agent Deployment
 - Deploy agent on endpoint
 - Office & OS requirement
- 6. Documentation

Quick Look at the Installation Steps

- 1. Prepare Linux Server with all requirements in place (Customer/partner)
- 2. Install K3s using command provided in GV documentation (Customer/partner)
- 3. Run Registration command to connect your server to Rancher (Customer/partner)
- 4. GV team completes back end installation from Rancher (GV team or FP support)
- 5. Configure dashboard access via Keycloak (Partner)
- 6. Configure basic policy in dashboard (Partner)
- 7. Install agent on endpoints (Partner)

Requirements

Supported OS

- Preferred & simplest setup Ubuntu 20.04.4 LTS Focal fossa (.5/.6 also fine)
- RHEL 8.6 (.7/.8 and 9.2 also fine) requires additional steps to be followed as outlined in K3s installation guide (not followed, will cause complications)
- CentOS 7.9 requires additional steps to be followed as outlined in K3s installation guide not followed, will

cause complications)

• Suse Linux 15.3

Pay close attention to version numbers, incorrect OS leads to failed installations Command to check Linux version: cat /etc/os-release

Hardware Specifications (General)

- 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.
- Storage needs to be mounted to /var
- Synergy (FDC) minimum requirement 8 CPU cores, 32GB RAM, 500GB Free Disk Space
- Focus (FDV) minimum requirement 16 CPU cores, 64GB RAM, 600GB Free Disk Space
- Enterprise (FDV + FDC) minimum requirement 20 CPU cores, 80GB RAM, 700GB Free Disk Space

Commands to check: CPU cores - Iscpu

Storage - df --h

RAM - cat /proc/meminfo

* Under spec hardware will lead to failed installations

Additional & Networking

- **Firewall**: The K3s server needs port 443/TCP to be open to allow the clients to access Synergy/Focus dashboard and API.
- Outbound internet access: To download the application artifacts (Docker images and binaries), updates and configuration files, the cluster needs a public internet connection with download speed of 40 Mbps or more and upload speed of 8 Mbps or more. To speed up the initial setup process it is recommended to have a download speed of 100 Mbps or more.

Ensure the Following Items are in Place and Configured

- 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

Commands: Check connectivity to our servers - curl -vL

https://rancher.forcepointapac.k3s.getvisibility.com/ping

* If no connection to the above URL, DO NOT RUN REGISTRATION COMMAND

K3s & Important Notes:

- Use the command we provide to install K3s, to ensure correct version:
- 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
- Do not run K3s install command or Registration command until you are sure ALL requirements are met
- Check and stop firewall if enabled: sudo ufw status and sudo ufw disable (Ubuntu commands)
- If customer intends to run behind proxy, inform the GV team before running registration command (requires some additional setup in terminal and Rancher), and follow the guidance here: https://getvisibility.atlassian.net/wiki/spaces/KBTES/pages/108167174/K3s+Installation#Proxy-settings
- Registration command can only be run once, if it fails you need to request a new one from FP/GV support
- Ensure DNS is configured K3s requires this to successfully install! Command to check DNS: cat /etc/resolv.conf

Rancher Configuration

Generating a Registration Command

- For Forcepoint the registration command is auto generated by registering customer in the reseller portal
- For new command, we log in to the relevant Rancher, go to Import Cluster > New > Generic
- We enter cluster name (all lower case) and set Labels cluster_name, and cluster_reseller with relevant names
- Saving this generates a registration command, which is run in the terminal of the provisioned server by partner/customer which connects your server to Rancher.
- Install the relevant Helm Charts, GV Essentials and Monitoring, then set the final labels indicating environment (production) and product (Synergy/Focus/Enterprise) > this triggers the creation & installation of the relevant pods, and can take up to 1 hour (depending on internet connection speed between Rancher and server)

*The above steps must be 100% complete before you can move on to the next step to configure dashboard access

Keycloak (configure dashboard access)

- 1. Log into Keycloak using https://your-server-ip/auth/admin (initial login credentials is admin & admin)
- Go to Clients > dashboard > Access Settings and enter your server's relevant info(IP address) under the entries valid redirect url and web origins and save:

Access settings

Root URL ③	\${authBaseUrl}	
Home URL ③		
Valid redirect URIs ⑦	https://my-dashboard.com/*	٥
	/*	•
		•
	• Add valid redirect URIs	
	Figure 1.	
Web origins ③	\${authBaseUrl}	•
	https://my-dashboard.com/	•
	• Add web origins	

Figure	2.
--------	----

3. Next go to **Users > Add User >** and enter "agent" as username and "agent@gv.com" as email (nothing else) and "save" (this is required for Synergy/FDC).

Users > User details								
agent							En:	abled A
Details Attrib	utes Credentials	Role mapping	Groups	Consents	Identity provider links	Sessions		
ID *	b943035c-8b6c-4e	00-9646-748457	628265					
	09430330-8000-40	900-9000-748037	020805					
Created at *	2/7/2024, 1:34:40 PM							
Required user actions	Select action						•	
0								
Username *	agent							
Email	agent@gv.com							
			Fig	ure 3.				

4. Finally, we go to Users > Add User same as previous step (to configure your dashboard access). Enter your desired "username" and "Create" > go to "credentials" (in the top menu) type your desired password > confirm password > turn temporary button off > Set Password to save.

Users > Crea	ate user						
Create u	ser						
Required user ⑦	actions Sele	ect action					
Username *	user	1					©
Email							
Email verified	•	No					
First name							
Last name							
Groups ③	Joi	n Groups					
	Cre	eate Cancel					
		Current					
			F	igure 4.			
Jsers > User de	tails						
user1							
Details	Attributes	Credentials	Role mapping	Groups	Consents	Identity provider links	Sessions
No credentials							
This user does not have any credentials. You can set password for this user.							
Set password							



5. Now you can navigate to the dashboard at <u>https://your-server-ip/ui</u> and enter the recently created username and password to log in.

Basic Policy Configuration (Agent v4)

1. Navigate to the "Agent" tab in the dashboard and you will find 4 main areas: Overview, System, Plugins and Macros.

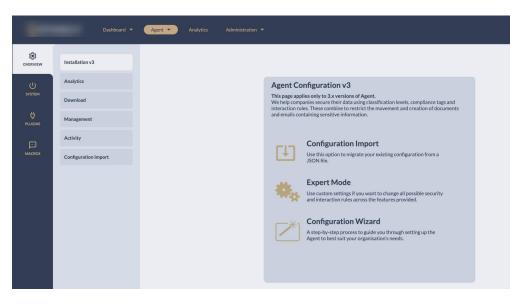


Figure 6.

System

OVERVIEW	Global	Enable auto-update	
U SYSTEM	Agent	Auto-update: server URL or path	
		Auto-update: regex for agent packages to include	
MACROS		Auto-update: check for updates frequency rate iminutes Timinutes Enable beta version update	
		Machine names for receiving beta version D	
		Heartbeat frequency @	

Figure 7.

Plugins

U Explorer V Outlook Powerpoint Outlook Powerpoint Outlook Vord Outlook Outlook Outlook <tr< th=""><th>OVERVIEW</th><th>Excel</th><th>General settings Classification settings Visual tagging</th></tr<>	OVERVIEW	Excel	General settings Classification settings Visual tagging
Powerpoint Word Suppress ribbon button @ Suppress suggestions dialog @ Lists	_	Explorer	Allow ML suggestions @
Powerpoint Word Suppress ribbon button @ Suppress Share and Export @ Suppress suggestions dialog @ Lists	¢	Outlook	
Word Suppress Share and Export © C Suppress suggestions dialog © Lists		Powerpoint	
Lists		Word	
			Suppress suggestions dialog @
Add New Whitelist			
			Add New Whitelist

Figure 8.

Macros (old overrides)

CVERVIEW OVERVIEW SYSTEM	© <u>Create New Macro</u> New macro	New macro 🖉 🗇 Notes:		
		Trigger Classification Confidential	Compliance Select compliance	Distribution Select distribution
MACROS		Target • Word ~		
		General settings Visual tagging		

Figure 9.

Configure Visual Markings in Office docs

- Choose if you want to display visual marks (checkbox)
- You can set layout, font, size, and style
- You can insert environment variables into markings

Example: Classified as {classification} on {datetime}

Will display Classified as Internal on 2023-06-08

• You can also configure a text watermark to display across the document

_	Times * Tover type *
Word	Enforce page layout option
	All pages V By default, where visual tags should be applied @
	0 Trigger pages number
	ningger Lages number of
	Overwrite V Header/footer overwrite action
	Show header
	<pre>Word D H Classification: {classification}/{distribution}</pre>
	Show footer
	<pre>Word 0 F Classification: {classification}/{distribution}</pre>
	Show watermark
	<pre>Word 0 W Classification: {classification}/(distribution)</pre>

Figure 10.

Configuring Outlook Email Policy

- Warn/block/ignore userssending/printingunclassified emails.
- Warn/block/ignore whether usercan send email with unclassified attachments.
- Will reply and forward inherit the label of original mail (checkbox).
- If a classified file is attached, will the email inherit the attachment label (checkbox).
- Can users change classification to lower label (checkbox).
- Can user select label lower than AI suggestion, and percentage threshold to enforce that (same as in Office apps).

OVERVIEW	Excel	General settings Classification settings Visual tagging
U SYSTEM	Explorer	Default email policy
¢	Outlook	lgnore 🗸
PLUGINS	Powerpoint	Attachment Classification lower than email policy
MACROS	Word	Unclassified attachments policy
		Ignore
		Allow lowering the level of Classification
		S Allow lowering the level of Distrubution
		Auto classify on reply/forward
		Classify emails same as attachments
		Classify attachments same as emails
		Show prefix classification on email subject @
		Show suffix classification on email subject 🛛
		O Default Classification Manual Classification
		Select classification V Ignore V user to classify before sending an email
		Select distribution
	6	Machine learning accuracy classification threshold (%) 🛛



Configure Visual Markings in Emails (Similar to Office Apps)

- Choose if you want to display visual marks (checkbox).
- You can insert environment variables into markings.

Example: Classified as {classification} on {datetime}

Will display Classified as Internal on 2023-06-08.

General settings	Classification settings	Visual tagging		
Show header				
<pre><span <="" pre="" style="color:#00FF00"></pre>	;">Outlook O H Classification:	{classification}/{dis	tribution}	
Show footer				
<pre><span style="color:DarkTur</pre></th><td>rquoise;">Outlook O F Classifica<td>tion: {classification</td><td><pre>//{distribution}<th>an></th></pre></td></pre>	tion: {classification	<pre>//{distribution}<th>an></th></pre>	an>	

Figure 12.

Configure Email Allow/Permission to Send/Warn/Block Lists

You can configure this for individual email addresses or entire domains according to each label.

-	-			
OVERVIEW	Excel	General settings Classification settings Visual tagging		
U SYSTEM	Explorer	Z Allow ML suggestions @		
Ö	Outlook	Specify maximum number of recipients @		
PLUGINS	Powerpoint	10 File acterision to exclude @		
мискоз	Word	Images Select Image file extensions Audio & Video Select autio and video file extensions Other Select other file extensions Select o		
		☐ Suppress suggestions dialog ⊕ Allow	Search	٩
			880	4
		You can use both users (user (bdomain.com) or domains (domain.com) when udding new items to this list.		
		Permission to send	Search	Q
		This page ag	plies only to 4.x versions of Agent.	SUBMIT

Figure 13.

We can enable/create new regex expressions by navigating to **Administration tab > Pattern Matching.**

Pattern Name	Select one or mo	ore languages	Compliance	Distribution		Category	Sul	bcategory		Rattern Name E.g. Credit Card Matcher Enter name
Type to search	Q Select filters	~	Select filters	✓ Select filters	×]	Select friters	~ (s	elect filters	-	Regular Expression
Tags		Enable p	attern		Published					Eg.^f2/7visa>4[0-9]
Select tags		✓ None		~	None		~			Enter keyword or regex
						PUBLISH ADD NOW	PATTERN	X	K SEANCH	
Pattern Name	Select one or more	Compliance	Distribution	Category	Subcategory	Tags	Enabl	Published		Public < Set Associated label,
ABA routing number				Financial Documents	Banking form	Financial		8	0 2	Internal compliance, category, Cardioentel etc.
										n tags based on the regex instead of AL
apple	Confidential	HIPAA/PHI						\oslash	0/	Compliance Distribution
apple test	Confidential	HIPAA/PHI	INT					\oslash	ō /	Citegory Subsitegory Tap
Australia Bank Account						Australia Financial	-	~		NA V NA V NA
Details	Confidential	GDPR/PII		Financial Documents	Banking form	PIL		Ø	0/	CANCL
Australia Disability Insurance Scheme	Confidential	gdpr/pii		Legal Documents	Certificate/Permit	Australia Legal PII PHI		Ø	0/	
Australia Drivers License Number		GDPR/PII		HR Documents	Employee record	Australia) (Legal) (PII)		8	0/	<
Australia Health Insurance	Confidential	GDPR/PII		Financial Documents	Banking form	Australia PI PH		8		Edit existing



Here you can enable and edit existing patterns > save > publish or create new ones > Save > publish.

Agent Deployment

- To install the agent you need 2 files, the .MSI installer as well as a JSON file called "installerConfig".
- Installerconfig JSON file only needs 2 entries to tell the agent where to look for first config.

```
{
"Name": "Mycompanyname",
"ServerAddress": "Myserver IP address",
```

- }
- These 2 files must be kept in the same folder on the PC where you are installing the agent.
- Simply run MSI and follow the prompts to finish installation.
- Agent can also be deployed via GPO or tools like SCCM, you can find complete info on this here: <u>https://getvisibility.atlassian.net/wiki/spaces/KBTES/pages/101318991/Agent+-+Installation</u>

*Please note, we support endpoints with Windows 10 and up, and MS Office 2016 and up.

Documentation

- We have an external Knowledge base where you can access our public documentation: https://getvisibility.atlassian.net/wiki/spaces/KBTES/overview?homepageId=100532593
- We also have a partner portal with brochures, presentations, videos, and more. Please sign up: <u>https://partners.getvisibility.com/</u>
- Synergy (FDC) Admin Guide:

https://getvisibility.atlassian.net/wiki/spaces/KBTES/pages/101384197/Synergy+Administration+Guide



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 GV Installation Training] [Status]23 Apr. 24