



A Journey of Discovery

~\$ whois fklaassen

Name: Frank Klaassen
Company: Enrise
Team: InfinIT
Job Title: Senior DevOps Engineer



~\$ whois fklaassen

- Using Zabbix since 2008
- Introduced or improved existing Zabbix environments
- Long time open source user & contributor
- First time conference speaker

~\$ whois enrise

- Enrise develops **high quality software** for the internet
- Founded in 2000
- 50+ people
- **Self-steering** company

~# whois infinit

- Managing internal IT
- Managing various environments on AWS & GCP
- Internal apps/dashboards
- DevOps consultancy

We use Zabbix for monitoring...

- Servers & Services
- Connectivity
- Provisioning
- SSL Certificates
- AWS services
- Application Components

Some facts

- AWS EC2 for Zabbix-server
- AWS RDS for database
(MariaDB with partitioning)
- Zabbix-Proxies for external locations
- Zabbix: 4.4.x
- Hosts: 345
- Items: 19123
- Triggers: 5552

A person is shown in silhouette, standing with their back to the camera and covering their face with both hands. They are wearing a dark long-sleeved shirt. The background is a soft, out-of-focus bokeh of warm, golden-yellow light, likely from a sunset or sunrise, with dark tree branches visible in the upper portion of the frame. The overall mood is one of despair or frustration.

How not to create many items

How not to create many items

- Project with a whitelabel domain per customer
- All domains have 3 subdomains each
- SSL monitoring desired for 5 customer environments

That would mean:

5 domains x 3 subdomains = 15 items

How not to create many items

- Quick & dirty...
You *could* create a template with the required 15 items
- With macros to at least make it **reusable** for the future

<input type="checkbox"/>	Wizard	Name	Triggers	Key	Interval	History	Trends	Type
<input type="checkbox"/>	...	SSL certificate validity - {\$SSL_SITE_1}	Triggers 5	zext_ssl_cert.sh[-d,{\$SSL_SITE_1},443]	4h	1w	30d	External check
<input type="checkbox"/>	...	SSL certificate validity - {\$SSL_SITE_2}	Triggers 5	zext_ssl_cert.sh[-d,{\$SSL_SITE_2},443]	4h	1w	30d	External check
<input type="checkbox"/>	...	SSL certificate validity - {\$SSL_SITE_8}	Triggers 5	zext_ssl_cert.sh[-d,{\$SSL_SITE_8},443]	4h	1w	30d	External check
<input type="checkbox"/>	...	SSL certificate validity - {\$SSL_SITE_7}	Triggers 5	zext_ssl_cert.sh[-d,{\$SSL_SITE_7},443]	4h	1w	30d	External check
<input type="checkbox"/>	...	SSL certificate validity - {\$SSL_SITE_6}	Triggers 5	zext_ssl_cert.sh[-d,{\$SSL_SITE_6},443]	4h	1w	30d	External check
<input type="checkbox"/>	...	SSL certificate validity - {\$SSL_SITE_5}	Triggers 5	zext_ssl_cert.sh[-d,{\$SSL_SITE_5},443]	4h	1w	30d	External check

All was fine!



Until...

- The team wanted to **disable monitoring** for one customer.
No problem! Let's just empty out a few macros.

Until...

- Oh yeah.. and please **add 3 new customers** as well while you're at it!

So that would mean the number of items would go from 15 to 12 items and... back to 18.

It's time for a better solution!

Low Level Discovery



Low Level Discovery

- Built-in functionality of Zabbix since 2.0
- Automatically creates items, triggers & graphs based on JSON input from Agent or Server
- Getting more advanced each release
 - *Hopefully one day also includes discovering web scenarios (ZBXNEXT-2621)*

What we use Low Level Discovery for

- PHP-FPM pools
- OpenVPN clients
- Gitlab health checks
- Docker containers
- Backup tasks
- Dnsmasq metrics
- SSL Certificates
- PM2 applications
- FreeSWITCH trunks
- Cronjobs
- Application Component Monitoring

But it can actually be used for anything that you can generate JSON for!

A close-up photograph of a yellow padlock attached to a dark, weathered metal door handle. The padlock is the central focus, with its yellow body and silver metal shackle. The background is dark and out of focus, showing the texture of the door and handle.

Solving the SSL monitoring issue

Without creating items by hand

Solving the SSL monitoring issue

Created a script reading the webserver (Apache, NGINX) configuration returning an array of all vhosts with a certificate

```
[
  {
    "{#SERVERPORT}" : 443,
    "{#SERVERNAME}" : "enrise.com"
  },
  {
    "{#SERVERPORT}" : 443,
    "{#SERVERNAME}" : "enrise.nl"
  }
]
```

Solving the SSL monitoring issue

Discovery rule Preprocessing LLD macros Filters

* Name

Type

* Key

* Update interval

Custom intervals

Type	Interval	Period	Action
<input checked="" type="checkbox"/> Flexible <input type="checkbox"/> Scheduling	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>	Remove
Add			

* Keep lost resources period

Description

Enabled ☒

Solving the SSL monitoring issue

[Discovery rule](#) [Preprocessing](#) [LLD macros](#) [Filters](#)

Preprocessing steps

Add

Update

Clone

Delete

Cancel

Solving the SSL monitoring issue

[Discovery rule](#) [Preprocessing](#) [LLD macros](#) [Filters](#)

LLD macros

LLD macro	JSONPath	
<input data-bbox="765 521 1219 563" type="text" value="{#MACRO}"/>	<input data-bbox="1232 521 1773 563" type="text" value="\$..path.to.node"/>	Remove
Add		

[Update](#) [Clone](#) [Delete](#) [Cancel](#)

Solving the SSL monitoring issue

Discovery rule Preprocessing LLD macros **Filters**

	Label	Macro		Regular expression	Action
	A	<div><code>{#SERVERPORT}</code></div>	matches ▼	<div>443</div>	Remove
Add					

[Update](#) [Clone](#) [Delete](#) [Cancel](#)

Solving the SSL monitoring issue

<input type="checkbox"/>	Wizard	Name	Key	Interval	History	Trends	Type	Applications	Create enabled ▲
<input type="checkbox"/>	...	SSL certificate validity - {#SERVERNAME} (Local)	check_certificate[-d {#SERVERNAME},{#SSL_PORT}]	4h	1w	30d	Zabbix agent (active)	SSL Certificates	Yes

Displaying 1 of 1 found

<input type="checkbox"/>	Severity	Name ▲	Operational data	Expression	Create enabled	Tags
<input type="checkbox"/>	Disaster	SSL certificate on {#SERVERNAME} expired		{Template SSL Certificate Auto - Agent:check_certificate[-d,{#SERVERNAME},{#SSL_PORT}].last()}<1	Yes	ssl-certificate: {#SERV... ssl-expiry: {ITEM.LAS...
<input type="checkbox"/>	High	SSL certificate on {#SERVERNAME} expires in less than 7 days ({ITEM.LASTVALUE1} remaining) Depends on: Template SSL Certificate Auto - Agent: SSL certificate on {#SERVERNAME} expired		{Template SSL Certificate Auto - Agent:check_certificate[-d,{#SERVERNAME},{#SSL_PORT}].last()}<=7	Yes	ssl-certificate: {#SERV... ssl-expiry: {ITEM.LAS...
<input type="checkbox"/>	Average	SSL certificate on {#SERVERNAME} expires in less than 15 days ({ITEM.LASTVALUE1} remaining) Depends on: Template SSL Certificate Auto - Agent: SSL certificate on {#SERVERNAME} expires in less than 7 days ({ITEM.LASTVALUE1} remaining)		{Template SSL Certificate Auto - Agent:check_certificate[-d,{#SERVERNAME},{#SSL_PORT}].last()}<=15	Yes	ssl-certificate: {#SERV... ssl-expiry: {ITEM.LAS...
<input type="checkbox"/>	Warning	SSL certificate on {#SERVERNAME} expires in less than 30 days ({ITEM.LASTVALUE1} remaining) Depends on: Template SSL Certificate Auto - Agent: SSL certificate on {#SERVERNAME} expires in less than 15 days ({ITEM.LASTVALUE1} remaining)		{Template SSL Certificate Auto - Agent:check_certificate[-d,{#SERVERNAME},{#SSL_PORT}].last()}<=30	Yes	ssl-certificate: {#SERV... ssl-expiry: {ITEM.LAS...

Solving the SSL monitoring issue

- Items are created in Zabbix

Name	Triggers	Key	Interval	History	Trends	Type
SSL Vhosts : SSL certificate validity - enrise.com (Local)	Triggers 4	check_certificate[-d,enrise.com,{\${SSL_PORT}}]	4h	1w	30d	Zabbix agent (active)
SSL Vhosts : SSL certificate validity - enrise.nl (Local)	Triggers 4	check_certificate[-d,enrise.nl,{\${SSL_PORT}}]	4h	1w	30d	Zabbix agent (active)

Solving the SSL monitoring issue

- And a set of triggers to notify us a certificate is about to expire

<input type="checkbox"/>	Severity	Value	Name ▲	Operational data	Expression	Status
<input type="checkbox"/>	Disaster	OK	SSL Vhosts: SSL certificate on enrise.com expired		<code>{web01.enrise.com:check_certificate[-d,enrise.com,{SSL_PORT}].last()}<1</code>	Enabled
<input type="checkbox"/>	High	OK	SSL Vhosts: SSL certificate on enrise.com expires in less than 7 days ({ITEM.LASTVALUE1} remaining) Depends on: web01.enrise.com: SSL certificate on enrise.com expired		<code>{web01.enrise.com:check_certificate[-d,enrise.com,{SSL_PORT}].last()}<=7</code>	Enabled
<input type="checkbox"/>	Average	OK	SSL Vhosts: SSL certificate on enrise.com expires in less than 15 days ({ITEM.LASTVALUE1} remaining) Depends on: web01.enrise.com: SSL certificate on enrise.com expires in less than 7 days ({ITEM.LASTVALUE1} remaining)		<code>{web01.enrise.com:check_certificate[-d,enrise.com,{SSL_PORT}].last()}<=15</code>	Enabled
<input type="checkbox"/>	Warning	OK	SSL Vhosts: SSL certificate on enrise.com expires in less than 30 days ({ITEM.LASTVALUE1} remaining) Depends on: web01.enrise.com: SSL certificate on enrise.com expires in less than 15 days ({ITEM.LASTVALUE1} remaining)		<code>{web01.enrise.com:check_certificate[-d,enrise.com,{SSL_PORT}].last()}<=30</code>	Enabled

A photograph of a road leading out of a tunnel. The road is dark asphalt with double yellow lines, receding into the distance. The tunnel's interior is dark and textured, while the exit reveals a bright, foggy forest scene with green trees. The overall mood is mysterious and atmospheric.

Monitoring OpenVPN Clients

Without creating items by hand

Monitoring OpenVPN Clients

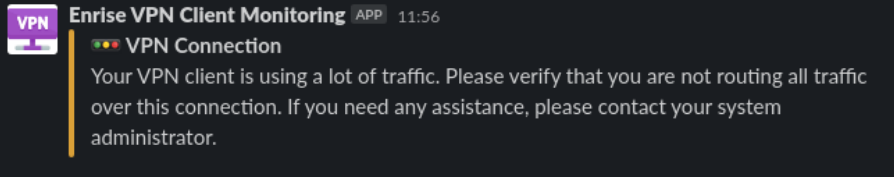
- Users generate their own configuration via our VPN Portal
- UserParameter script on the VPN instance returns a list of users to Zabbix Discovery
- Zabbix creates the desired items (traffic in/out & client IP)

Name ▼	Last check	Last value	Change
VPN Clients (3 Items)			
OpenVPN Client fklaassen - Traffic Outgoing	2020-02-14 10:30:27	1.46 Mbytes	+52.28 Kbytes
OpenVPN Client fklaassen - Traffic Incoming	2020-02-14 10:30:27	17.92 Mbytes	+1.86 Mbytes
OpenVPN Client fklaassen - IP	2020-02-14 10:30:27	256.128.512.64	

Monitoring OpenVPN Clients

Tracking bandwidth usage
per user

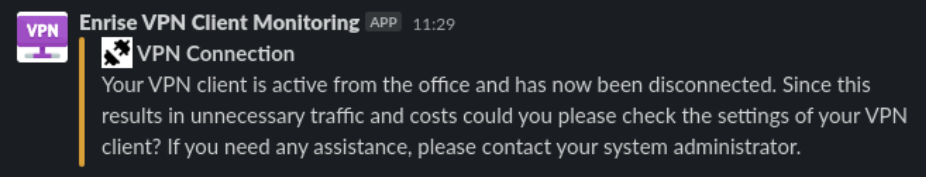
Tracking accidental usage at office



VPN Enrise VPN Client Monitoring APP 11:56

🌈 VPN Connection

Your VPN client is using a lot of traffic. Please verify that you are not routing all traffic over this connection. If you need any assistance, please contact your system administrator.



VPN Enrise VPN Client Monitoring APP 11:29

🌐 VPN Connection

Your VPN client is active from the office and has now been disconnected. Since this results in unnecessary traffic and costs could you please check the settings of your VPN client? If you need any assistance, please contact your system administrator.

With automatic Slack notifications

A close-up photograph of a person's hand, wearing a grey sleeve and an orange beaded bracelet, placing a green wooden block on top of a stack of other colorful blocks (red, yellow, green, purple). The background is blurred, showing a green and blue structure, possibly a play area. The text "Application Component Monitoring" is overlaid in white, bold, sans-serif font across the center of the image.

Application Component Monitoring

Application Component Monitoring

- External API's
- Database connectivity

Application Component Monitoring

Dev Team

- **Knows best** how to monitor their application
- **Does not** have or **need** knowledge of Zabbix
- Wants to make changes **without** involving Ops

Ops Team

- Has Zabbix knowledge
- **Does not (need to) know** what components the application has

Application Component Monitoring

Key Endpoint

(/monitoring/keys.json)

```
{
  "Warning Component": {
    "severity": "warning"
  },
  "Average Component": {
    "severity": "average"
  },
  "High Component": {
    "severity": "high"
  },
  "Disaster Component": {
    "severity": "disaster"
  }
}
```

Status Endpoint

(/monitoring/status.json)

```
{
  "Warning Component": {
    "statusCode": 0,
    "severity": "warning"
  },
  "Average Component": {
    "statusCode": 0,
    "severity": "average"
  },
  "High Component": {
    "statusCode": 0,
    "severity": "high"
  },
  "Disaster Component": {
    "statusCode": 0,
    "severity": "disaster"
  }
}
```


Application Component Monitoring

<input type="checkbox"/>	Wizard	Name	Triggers	Key
<input type="checkbox"/>		Components: average: Component status - Average Component	Triggers 1	aamv2.status[Average Component,average]
<input type="checkbox"/>		Components: disaster: Component status - Disaster Component	Triggers 1	aamv2.status[Disaster Component,disaster]
<input type="checkbox"/>		Components: high: Component status - High Component	Triggers 1	aamv2.status[High Component,high]
<input type="checkbox"/>		Components: information: Component status - Information Component	Triggers 1	aamv2.status[Information Component,information]
<input type="checkbox"/>		Components: unclassified: Component status - Unclassified Component	Triggers 1	aamv2.status[Unclassified Component,unclassified]
<input type="checkbox"/>		Components: warning: Component status - Warning Component	Triggers 1	aamv2.status[Warning Component,warning]
<input type="checkbox"/>	...	Template Automatic Application Monitoring v2: AAMv2: Components Retrieval	Triggers 1	aamv2.py["--config","/etc/zabbix/zabbix_agentd.aam.conf","--discovery","{HOST.HOST}","{SAAM_KEY_ENDPOINT}"]
<input type="checkbox"/>	...	Template Automatic Application Monitoring v2: AAMv2: Status Retrieval	Triggers 1	aamv2.py["--config","/etc/zabbix/zabbix_agentd.aam.conf","--update-items","{HOST.HOST}","{SAAM_STATUS_ENDPOINT}"]

Application Component Monitoring

Opensource! Source is available on GitHub:

[**https://enri.se/zabbix-appmonitor**](https://enri.se/zabbix-appmonitor)

A close-up, low-angle shot of a person's hand raised in the air, palm facing forward. The hand is positioned on the right side of the frame. The person is wearing a silver-toned watch with a dark face and a metal link bracelet. The background is dark and out of focus, featuring several warm, glowing string lights hanging from above. In the center, the word "Questions?" is written in a white, sans-serif font. The overall mood is one of an interactive session or a Q&A period at an event.

Questions?