A Journey of Discovery
ENRISE

~$ 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**

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

Wizard	Name	Triggers	Key	Interval	History	Trends	Type
•••	SSL certificate validity - {$SSL_SITE_1}	Triggers 5	zext_ssl_cert.sh[-d,{$SSL_SITE_1},443]	4h	1w	30d	External check
•••	SSL certificate validity - {$SSL_SITE_2}	Triggers 5	zext_ssl_cert.sh[-d,{$SSL_SITE_2},443]	4h	1w	30d	External check
•••	SSL certificate validity - {$SSL_SITE_8}	Triggers 5	zext_ssl_cert.sh[-d,{$SSL_SITE_8},443]	4h	1w	30d	External check
•••	SSL certificate validity - {$SSL_SITE_7}	Triggers 5	zext_ssl_cert.sh[-d,{$SSL_SITE_7},443]	4h	1w	30d	External check
•••	SSL certificate validity - {$SSL_SITE_6}	Triggers 5	zext_ssl_cert.sh[-d,{$SSL_SITE_6},443]	4h	1w	30d	External check
•••	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!

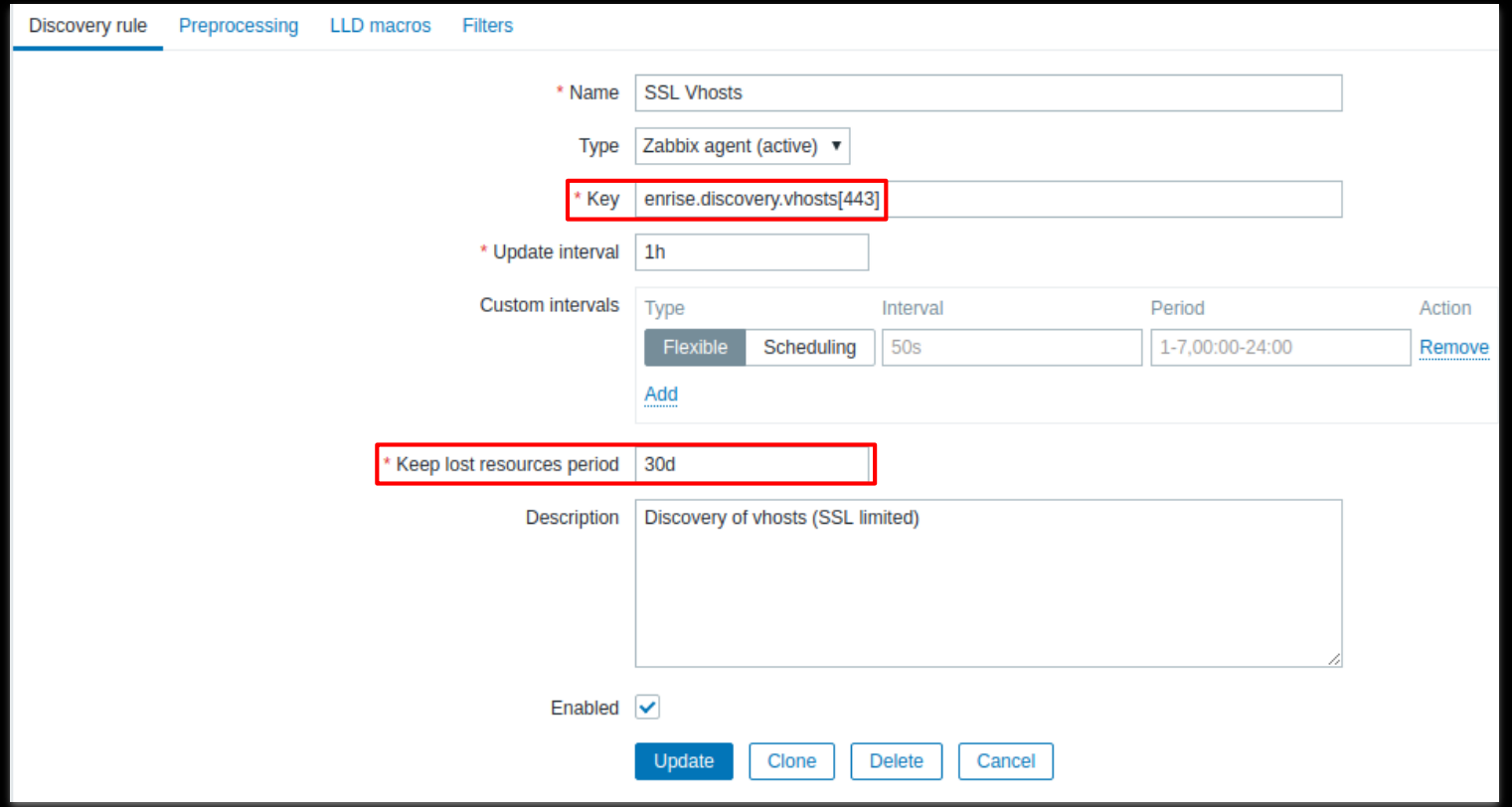
Solving the SSL monitoring issue
Without creating items by hand

Solving the SSL monitoring issue

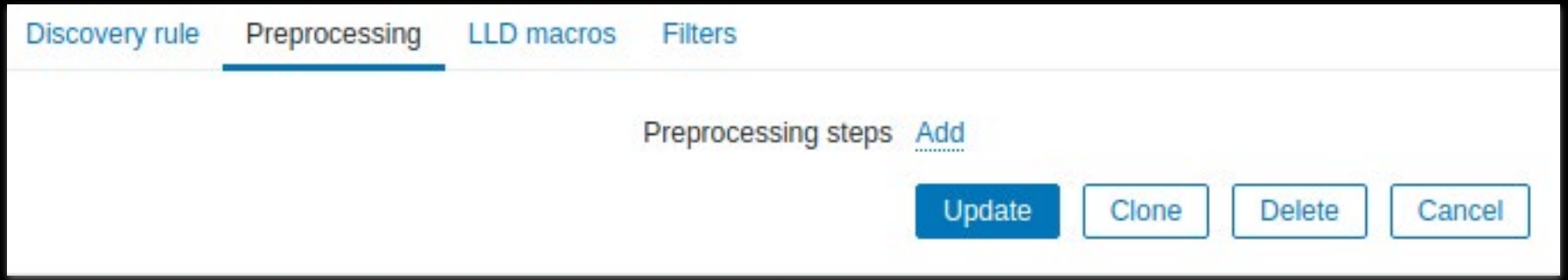
Created a script reading the webserver (Apache, NGINX) configuration returning an array of all vhosts with a certificate

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

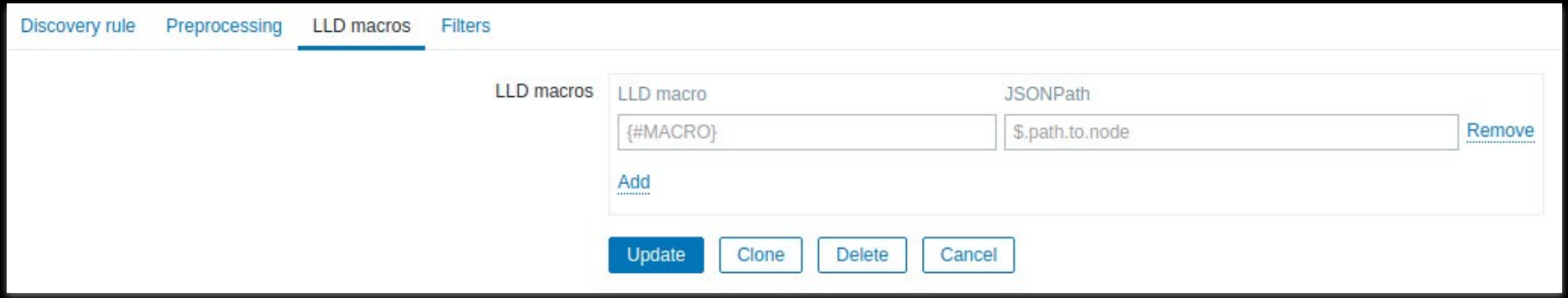
Solving the SSL monitoring issue



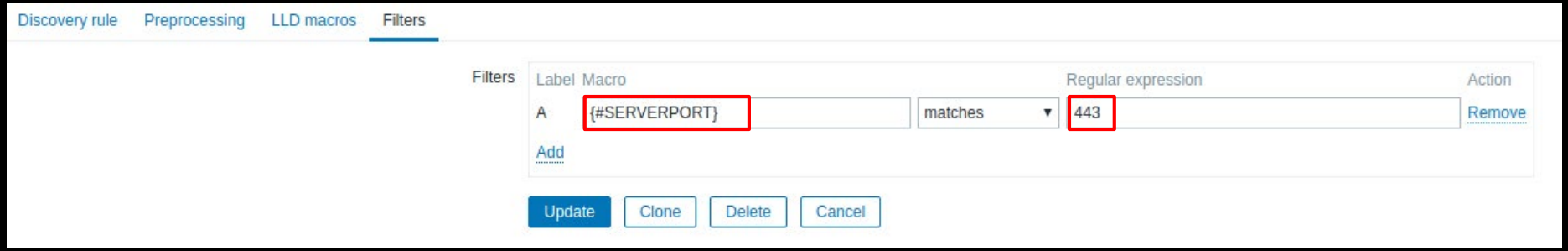
Solving the SSL monitoring issue



Solving the SSL monitoring issue



Solving the SSL monitoring issue



Solving the SSL monitoring issue

Wizard	Name	Key	Interval	History	Trends	Type	Applications	Create enabled ▲
•••	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

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

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

Monitoring OpenVPN Clients
Without creating items by hand

Monitoring OpenVPN Clients

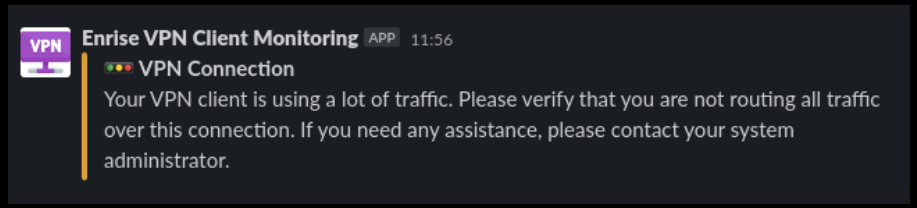
- Users generate their own configuration via our VPN Portal
- UserParameter script on the VPN instance returns a list of users to Zabbix Discovery
- Zabbix creates the desired items (traffic in/out & client IP)

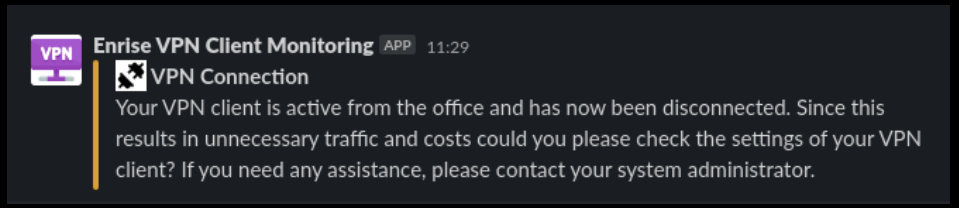
Name ▾	Last check	Last value	Change
VPN Clients (3 Items)			
OpenVPN Client fklaassen - Traffic Outgoing	2020-02-14 10:30:27	1.46 Mbytes	+52.28 Kbytes
OpenVPN Client fklaassen - Traffic Incoming	2020-02-14 10:30:27	17.92 Mbytes	+1.86 Mbytes
OpenVPN Client fklaassen - IP	2020-02-14 10:30:27	256.128.512.64	

Monitoring OpenVPN Clients

Tracking bandwidth usage per user

Tracking accidental usage at office





With automatic Slack notifications

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)

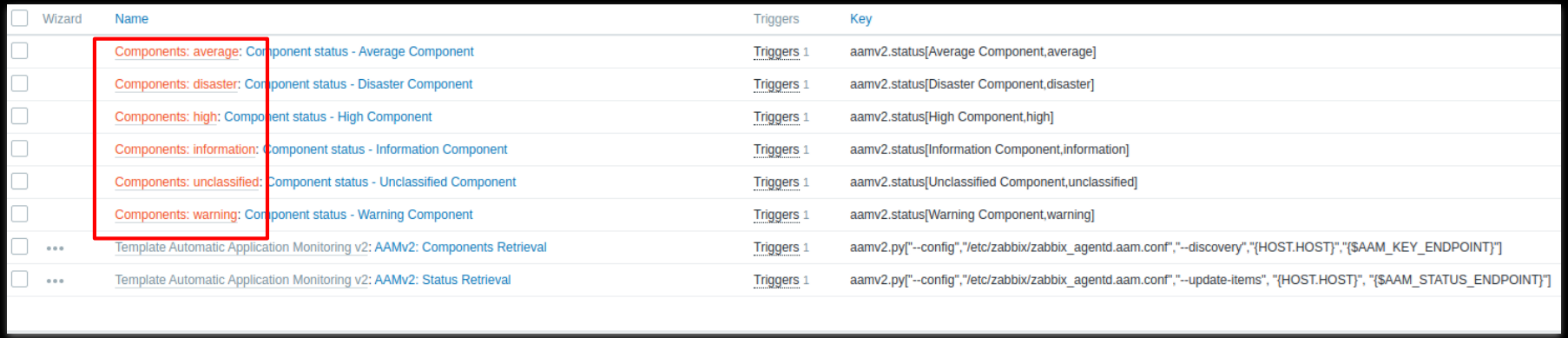
```
{
    "Warning Component": {
        "severity": "warning"
    },
    "Average Component": {
        "severity": "average"
    },
    "High Component": {
        "severity": "high"
    },
    "Disaster Component": {
        "severity": "disaster"
    }
}
```

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



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

Application Component Monitoring

Opensource! Source is available on GitHub:

https://enri.se/zabbix-appmonitor

Questions?