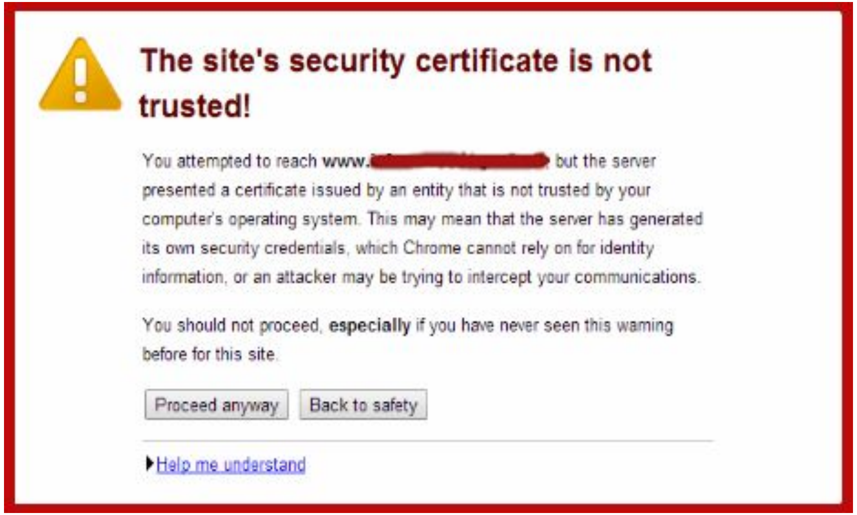
How to prevent the human errors with Zabbix platform

Egor Andreev, AdminDivision, CEO

Abstract

Main idea: SSL certificate can expire and shut the multi-million users web-service platform. Sounds silly? But it does happen in reality.



The site's security certificate is not trusted!

You attempted to reach **www.**[redacted] but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

The few simple issues that may cause the service outage:

- Expiring the date of **domain registration**

- Expiring the **SSL certificate**

- Running out of **balance** in the hosting account

While all of them should be going smoothly:

- The **expiration date is well known** in advance

- There is always a **person** or a team **responsible for payment**

- **Providers never shut down without a notice**, they send reminders prior the event.

What does go wrong then:

- Email **reminder has been missed** in the mailboxes

- **Invoice’s been lost** inside the accounting department

- **New SSL certificate** was purchased but **has not been rolled out** to the servers

Solution

We make Zabbix **check** all these little things and **notify** us if the issue is possible.

And what really matters, we will know when the issue is resolved.

Solution

Just use custom bash scripts with **UserParameter** or **ExternalCheck**:

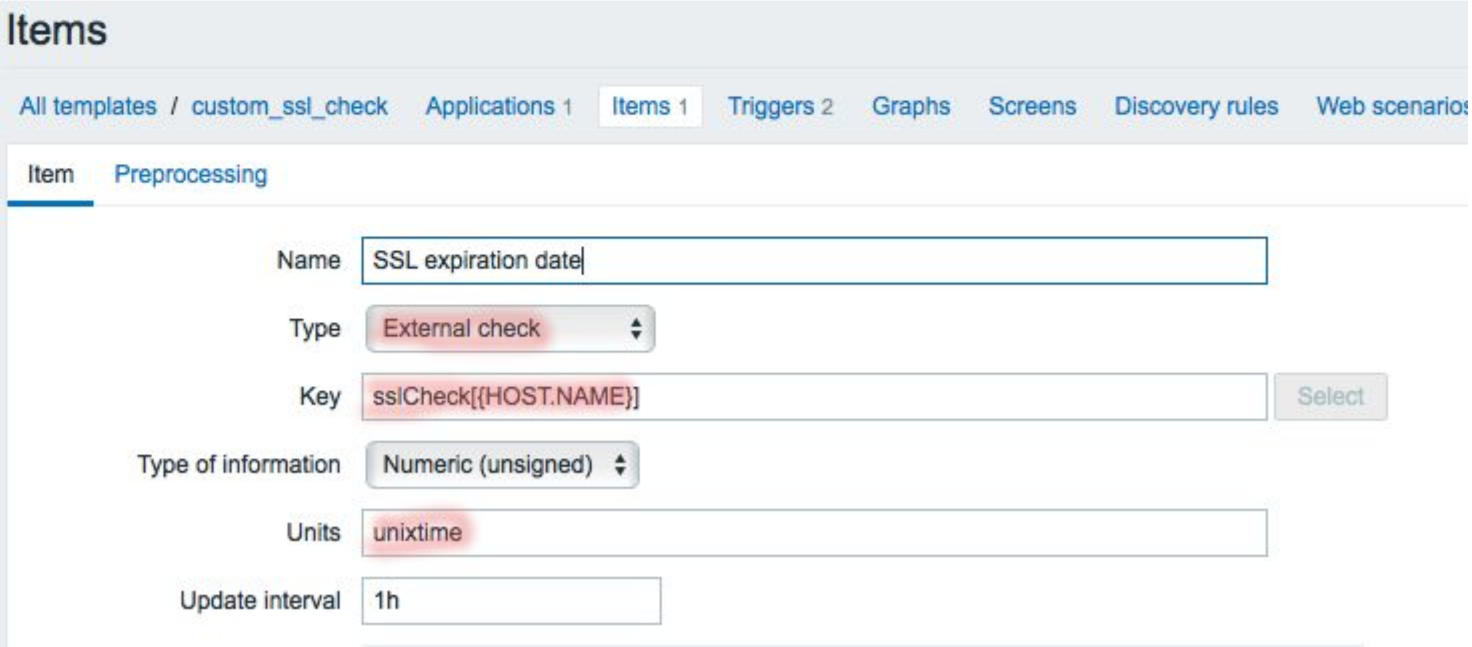
- check domain registration expire date with "**whois**"

- check ssl expire date with "**openssl**". On all servers!

- check your hoster balance via API or just "**curl**"

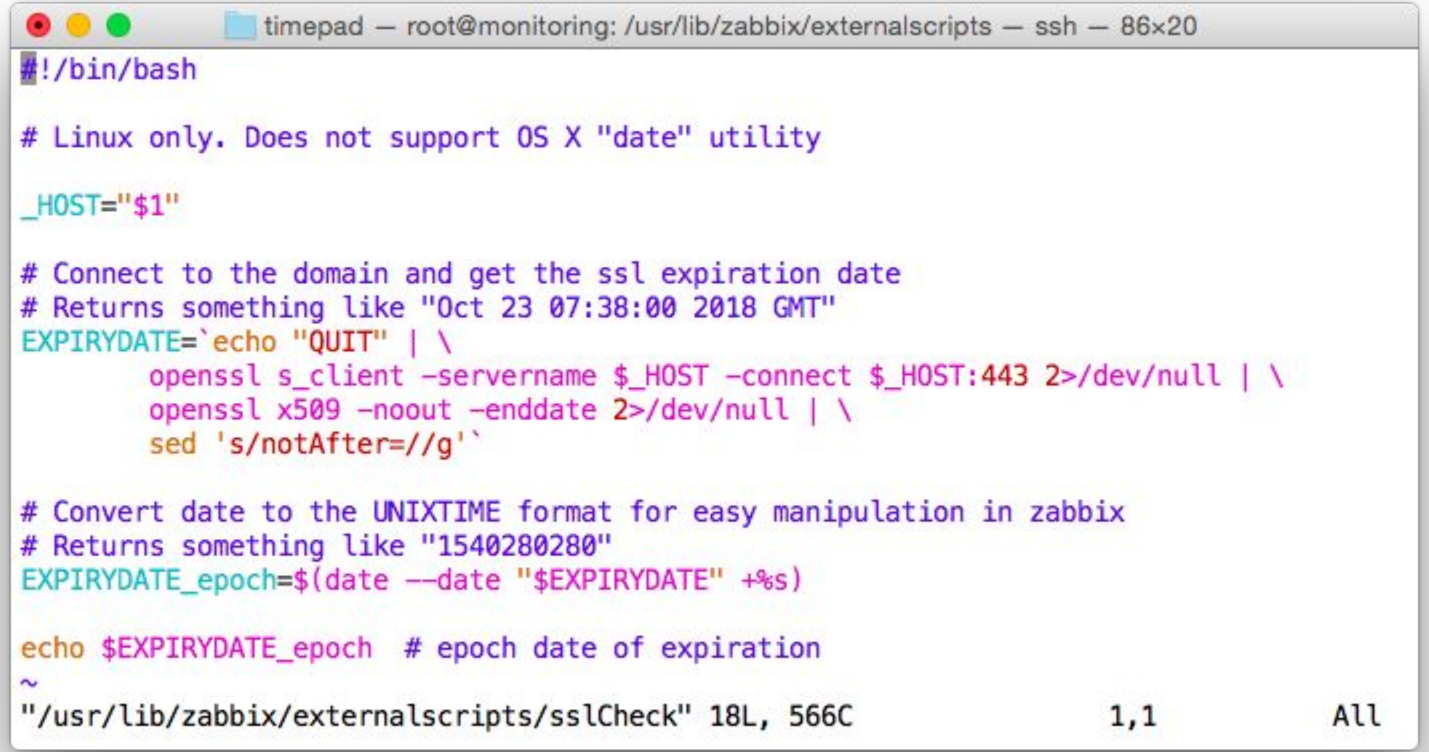
- be calm and happy

Example: ssl check



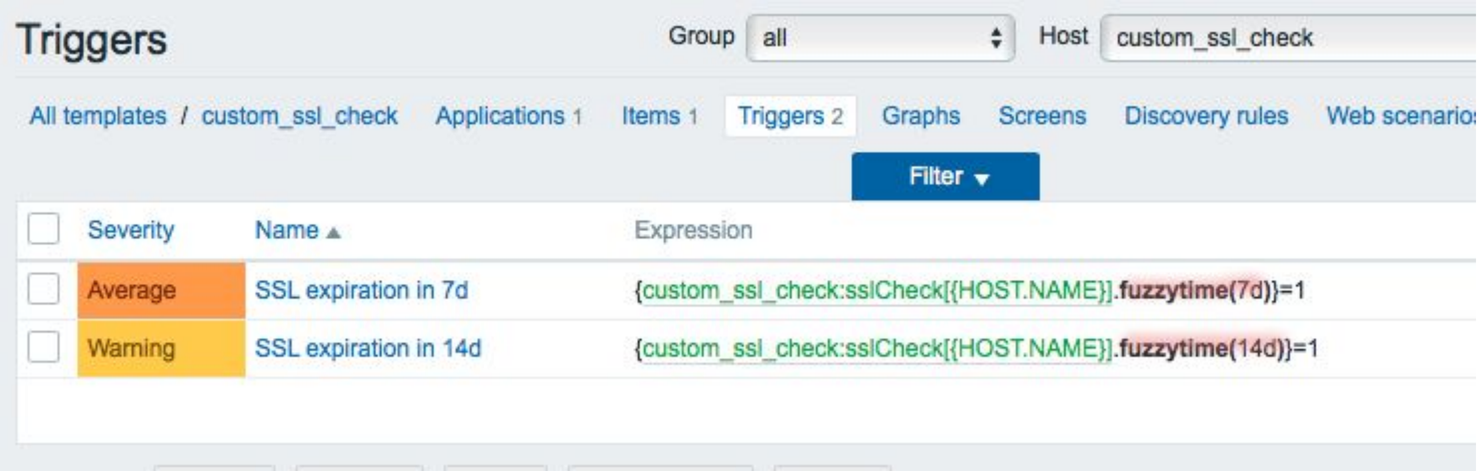
Name	SSL expiration date
Type	External check
Key	sslCheck[{HOST.NAME}]
Type of information	Numeric (unsigned)
Units	unixtime
Update interval	1h

Example: ssl check


timepad — root@monitoring: /usr/lib/zabbix/externalscripts — ssh — 86×20

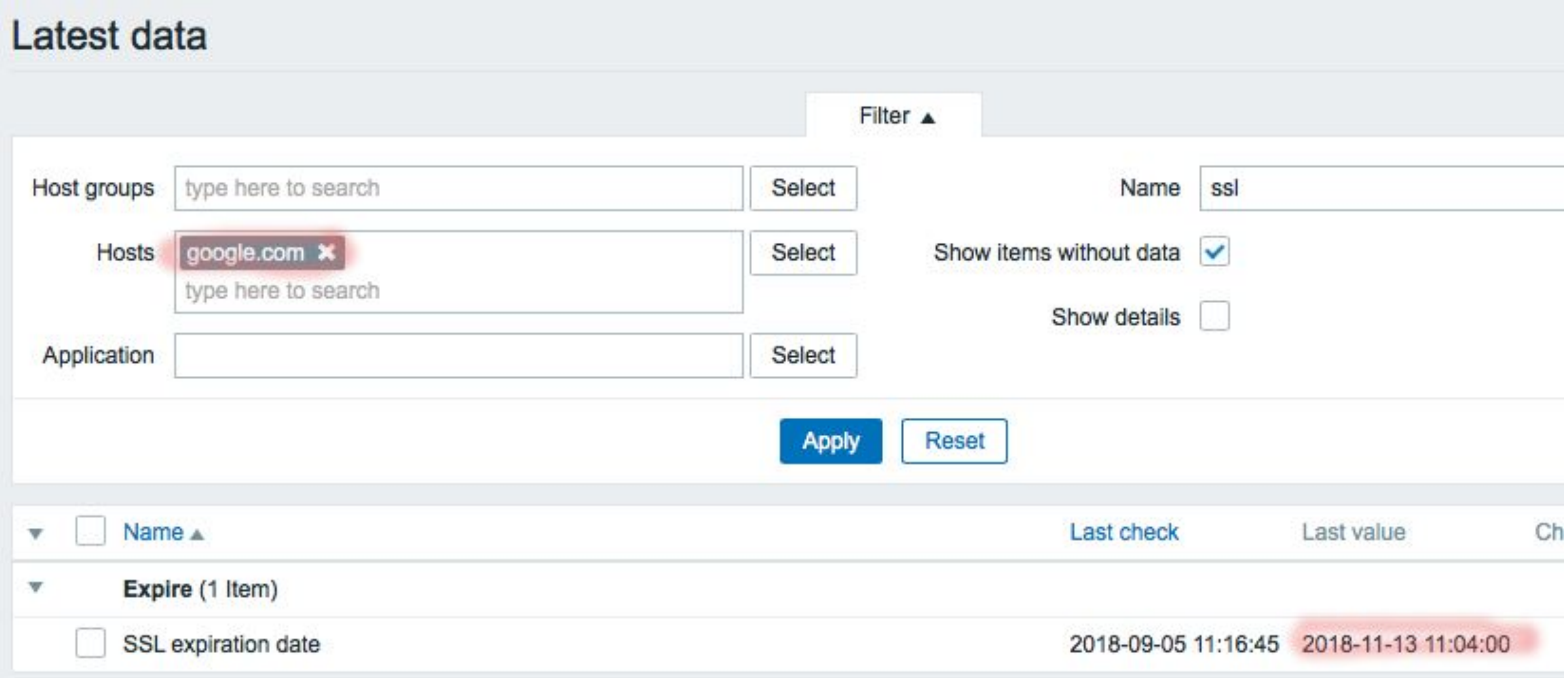
```
#!/bin/bash

# Linux only. Does not support OS X "date" utility

_HOST="$1"

# Connect to the domain and get the ssl expiration date
# Returns something like "Oct 23 07:38:00 2018 GMT"
EXPIRYDATE=`echo "QUIT" | \
        openssl s_client -servername $_HOST -connect $_HOST:443 2>/dev/null | \
        openssl x509 -noout -enddate 2>/dev/null | \
        sed 's/notAfter=//g'`

# Convert date to the UNIXTIME format for easy manipulation in zabbix
# Returns something like "1540280280"
EXPIRYDATE_epoch=$(date --date "$EXPIRYDATE" +%s)

echo $EXPIRYDATE_epoch  # epoch date of expiration
~
"/usr/lib/zabbix/externalscripts/sslCheck" 18L, 566C                    1,1           All
```

Example: ssl check



☐	Severity	Name ▲	Expression
☐	Average	SSL expiration in 7d	{custom_ssl_check:sslCheck[{HOST.NAME}].fuzzytime(7d)}=1
☐	Warning	SSL expiration in 14d	{custom_ssl_check:sslCheck[{HOST.NAME}].fuzzytime(14d)}=1

Example: ssl check



Latest data

Host groups: type here to search

Hosts: google.com ✖ type here to search

Application:

Name: ssl

Show items without data ☑

Show details □

□ Name ▲	Last check	Last value	Ch
Expire (1 Item)			
□ SSL expiration date	2018-09-05 11:16:45	2018-11-13 11:04:00	

Thank you! Questions?

Egor Andreev

AdminDivision.com

egor@admindivision.ru

+7 916 848 3919

http://fb.com/eg.andr