Server preparation - Server monitoring

Automatic monitoring of production system is crucial for bussiness continuity. Monitoring is recommended also for the testing environment, but it is not mandatory. This page will show you how to set up basic monitoring of server with CzechIdM using Nagios NRPE. It is very useful to store monitored values for trend overview (e.g. with Munin). Some monitoring systems (like Zabbix) can store trends and monitor services at once. It is also practical to install `iostat`, `vmstat` and `sar` utilities on the server.

This article is about real-time monitoring of the server and its services. It does not deal with monitoring of "the insides" of CzechIdM.

Typical CzechIdM server

This is a typical configuration of a production server for a small company. These parameters may need to be adjusted to complexity of particular deployment.

- RHEL7-flavoured system.
- About 80GB HDD.
- At least 8GB RAM.
- At least 2x2GHz CPU.

Monitored parameters

This is a list of monitored server's (and services') parameters. It should be treated as a bare minimum and, if needed, extended according to your company's policy. Parameters and their thresholds mentioned below are based on our best practices for the monitoring of a deployment.

Service/Parameter	Probe binary	Name in NRPE	Warning threshold	Critical threshold	Check frequency	Notification frequency
HOST UP	N/A	this is not implemented on the target machine	N/A or ping RTT threshold	high ping RTT or host is not pingable at all	every 5 minutes	every 6 hours
swap used space	check_swap	check_swap	50% swap free	10% swap free	every 5 minutes	every 24 hours
disk free space	check_disk	check_disk	90% used	95% used	every 5 minutes	every 24 hours
system load	check_load	check_load	4,3.5,3	6,5.5,5	every 5 minutes	every 24 hours
used memory	check_mem	check_mem	90% used	95% used	every 5 minutes	every 24 hours
process count	check_procs	check_procs	300+	500+	every 5 minutes	every 24 hours
zombie process count	check_procs	check_zombies	1+	5+	every 5 minutes	every 24 hours

Service/Parameter	Probe binary	Name in NRPE	Warning threshold	Critical threshold	Check frequency	Notification frequency
system time	check_ntp_time	check_time	skew >1min	skew >5min	every hour	every 24 hours
CzechIdM is running	check_http	check_idm	N/A	CzechIdM not running	every 5 minutes	every 24 hours
HTTPD is running	check_http	check_httpd	response time >1s	HTTPD is not running	every 5 minutes	every 24 hours
HTTPS certificate expiration	check_http	check_httpd_cert	less than 30 days	less than 7 days	once a day	every 24 hours
PostgresSQL is running	check_pgsql	check_postgres	response time >0.5s	response time >1s or not running at all	every 5 minutes	every 24 hours

Implementation

We will use nrpe and probes from the standard system packages. We have epel repository enabled.

- NRPE daemon will listen on 5666\tcp (its default port). Open the port in your iptables by adding the rule: `-A INPUT -m state –state ESTABLISHED,RELATED -p tcp –dport 5666 -j ACCEPT`.
- All probes are located in their default installation location `/usr/lib64/nagios/plugins/`.
- We use one external probe check_mem which can be downloaded here: https://exchange.nagios.org/directory/Plugins/System-Metrics/Memory/check_mem-2Esh/details. This probe, however, returns bad results on RHEL7 because of the different meaning of the `free` command output. You can dowload the fixed version from here.

Deployment

First, install necessary packages:

```
yum install nrpe nagios-plugins-nrpe nagios-plugins-swap nagios-plugins-disk
nagios-plugins-load nagios-plugins-procs nagios-plugins-ntp nagios-plugins-
http nagios-plugins-pgsql
```

If you use SELinux, we need to permit the check_disk plugin access to the `/sys/kernel/…`. Easiest way (but not necessarily the most correct) is to set permissive mode for some plugins:

```
yum install policycoreutils-python
semanage permissive -a nagios_checkdisk_plugin_t
```

Edit the `/etc/nagios/nrpe.cfg` file and add your monitoring server address to the allowed_hosts directive:

```
allowed_hosts=127.0.0.1,IPofMonitoringServer
```

Create a configuration of system checks in the file `/etc/nrpe.d/checks.cfg`. Fill in the

YOUR_NTP_SERVER and IDM_SERVICE_DOMAIN_NAME accordingly. The MONITORING_USER and MONITORING_USER_PASSWORD are values filled with credentials of an user which is capable to log into the PostgreSQL database. **Create separate user just for this purpose**.

checks.cfg

```
command[check_swap]=/usr/lib64/nagios/plugins/check_swap -w 50% -c 10%
command[check_disk]=/usr/lib64/nagios/plugins/check_disk -w 90 -c 95
command[check_load]=/usr/lib64/nagios/plugins/check_load -w 4,3.5,3 -c
6,5.5,5
command[check_mem]=/usr/lib64/nagios/plugins/check_mem -w 90 -c 95
command[check_procs]=/usr/lib64/nagios/plugins/check_procs -w 300 -c
500
command[check_zombies]=/usr/lib64/nagios/plugins/check_procs -w 1 -c 5
-s Z
command[check_time]=/usr/lib64/nagios/plugins/check_ntp_time -H
YOUR_NTP_SERVER -w60 -c300
command[check_idm]=/usr/lib64/nagios/plugins/check_http -H 127.0.0.1 -p
8080 -u '/idm/api/v1/status'
command[check_httpd]=/usr/lib64/nagios/plugins/check_http -H
IDM_SERVICE_DOMAIN_NAME -S -p443 -w1
command[check_httpd_cert]=/usr/lib64/nagios/plugins/check_http -H
IDM_SERVICE_DOMAIN_NAME -S -p443 -C30,7
command[check_postgres]=/usr/lib64/nagios/plugins/check_pgsql -H
127.0.0.1 -P 5432 -d template1 -l MONITORING_USER -p
MONITORING_USER_PASSWORD -w0.5 -c1
```

Add the check_mem script to the /usr/lib64/nagios/plugins/ directory, make it executable:

```
cp check_mem /usr/lib64/nagios/plugins/
chmod 755 /usr/lib64/nagios/plugins/check_mem
```

Create the MONITORING_USER in the PostgreSQL. Generate some strong password - you can use pwgen for that.

```
create user monitoring password 'somepassword';
```

Start and enable the NRPE daemon:

```
systemctl start nrpe
systemctl enable nrpe
```

To test the probes, you can use check_nrpe plugin:

```
/usr/lib64/nagios/plugins/check_nrpe -H 127.0.0.1 -b 127.0.0.1 -c check_swap
```

Nagios server configuration

This is a sample configuration for the Nagios server. It is meant more as an inspiration, feel free to

adapt it to your Nagios deployment.

Configure the check_nrpe command (you probably already have this in your Nagios configuration):

```
define command{
        command_name check_nrpe
        command_line /usr/lib64/nagios/plugins/check_nrpe -H $HOSTADDRESS$ -
c $ARG1$
}
```

Define CzechIdM server host:

```
define host {
        use                             linux-server
        host_name                       czechidm_server
        alias                           idmserver.example.com - CzechIdM
server
        address                         1.2.3.4
        check_period                    24x7
        # we expect interval_length=60 as is the default, so 1440*60s = 1
day
        notification_interval           1440
        notification_period             24x7
}
```

Define checks:

```
define service {
        use                             generic-service
        host_name                       czechidm_server
        service_description             SWAP
        check_command                   check_nrpe!check_swap
        # we expect interval_length=60 as is the default, so 5*60s = 5
minutes
        check_interval          5
        # we expect interval_length=60 as is the default, so 1440*60s = 1
day
        notification_interval           1440
        contacts            user1,user2
        contact_groups          admins1,admins2
}

... and similarly the other checks ...
```