

Transformation of monitoring to 21st century in Livesport

Jakub Štollmann
Network & Systems Engineer

@pershinghar

WhoAml?

- Slovak living in Prague
- Livesport s.r.o
- CTU FIT (Bc.)
- Python & Icinga enthusiast (recently)

Agenda

- Introduction
- Motivation
- New conception
- Deployment
- Future

Livesport ?

Livesport

- Livescore provider
- We operate 500+ hosts
 - physical servers
 - virtual servers
 - network hosts
- 3 locations
- Still growing!

Monitoring ?

Perfect monitoring ?

Perfect monitoring

- Automated
 - Flexible
 - Simple
-
- (We didn't match any of these)

Motivation ?


```
define host{
    use          generic-host      ; Name of host template to use
    host_name    lsproxy34
    alias        lsproxy34.edhost.eu
    address      188.92.40.163
}

define host{
    use          generic-host      ; Name of host template to use
    host_name    lsproxy35
    alias        lsproxy35.edhost.eu
    address      188.92.40.164
}

define host{
    use          generic-host      ; Name of host template to use
    host_name    lsproxy36
    alias        lsproxy36.edhost.eu
    address      188.92.40.165
}
```

```

### SERVER
define hostgroup{
    hostgroup_name server
    alias Servers
    hostgroup_members server_mysql,server_mysql_slave,server_http,server_memcached
    members ns1,lspush1,lspush2,lspush3,lspush4,lspush5,lspush6,lspush7,lspush8,lsrlbs1,lsrlbs2,lsrlbw1,lsrlbw2,lscache1,lscache2,lscache3,dcpush,dckvido,dckvido2,lsdns1,lsdns2,lsdns3,lsmongo1,lsmongo2,wata,lssphinx1,lssphinx2,puppet,lsxen01,lsxen02,lsxen03,lsxen04,lsxen05,lsxen06,lsxen07,lsxen08,lsxen09,lsxen10,lsxen11,lsxen12,lsxen13,lsxen14,lsxen15,lsxen16,lsxen17,lsxen18,lsxen19,lsxen20,lsxen21,lsxen22,lsxen23,lsxen24,lsxen25,lsxen26,lsxen27,management,opadmin,oppush,lsweb3,mongoarbiter1,monitor,lsid1,lsid2,dbbs,deploy,cartman,ns3,nagios1,fsp2,dccache1,dccache2,fsstat,jenkins,dccml1,dccml2,dccml3,dccml4,dccron2,inventory,dcapi1,dcapi2,opcache1,opcache2,opproxy01,opproxy02,mrpaja,dcproxy1,dcproxy2,mail1,mail2,lswiki,dcapiadmin,session1,session2,videoplayer,mailz,lsc1,infoport,lkm1,lks1,lks2,lks3,lks4,lks5,lsnp1,lsnp2,lsnp3,lsnp4,lsdocker1,node2,node3,node4,node5,node6,node7,node8,node9,node10,node11,node12,node13,node14,node15,node16,node17,node18,node19,node20,node21,lsbackup1,bs-kernel,lssearch1,dcarchive,lspush9,lspush10,buildsystem,exapi1,exapi2,exw1,exw2,lstrac2,dcredis1,dcredis2,sso1,sso2,ssodb1,lstrac1,lsopenx1,lsopenx2,lsopenx3,lsopenx4,lsnpm2,lsnpm1,lsidm1,lsidm2,dcapi3,dcapi4,dcapi5,opparser1,opparser2,opparser3,opparser4,opparser5,opparser6,oppstor1,oppstor2,adadmin1,adadmin2,oppfp1,oppfp2,gwmedia,cactip1,cactip2,cactip3,sql1,lswatch,dbb1,dcfix,mtprom1,mtweb1,mtifdb1,mtifdb2,mtesdb1,esdbm1,esdb1,esdb2,esdb3,esdb4,dcesc1,dcesc2,dcesc3,lsgitlab1,esdbc1,esdbc2,chat1,lsnpredis1,lsnpredis2,dcapi6,dcapi7,dcapi8,pml1,puppet1,opapiredis1,opmc1,opmc2,opmc3,opmc4,opmc5,opmc6,opmc7,opmc8,opmcbackup1,opmctest1,opmctest2,opmctest3,opapiw1,opapiw2,opapiw3,opapiw4,opapir1,opapir2,opapir3,opapir4,certbot1,lsnpproxy1,lsnpproxy2,dccron1,mailx,dcfix2,dcfix1,lsnp5,lsnp6,kvidomqm1,kvidomqm2,dcapiproxy1,dcapiproxy2,kvidomq1,kvidomq2,esga1,kvxdba1
}

```

Motivation

- still no that bad, we can do some audit and fix that?
- but for 5000 services?
- and what if we will double our hosts count?

Thruk preferences

Current Network Status
 Last Updated: Mon Sep 10 12:49:38 CEST 2018
 Updated every 90 seconds
 Thruk 2.04 - www.thruk.org
 Logged in as *pershing*

Host Status Totals

Up	Down	Unreachable	Pending
750	0	0	0
All Problems		All Types	
0		750	

Service Status Totals

OK	Warning	Unknown	Critical	Pending
6902	6	1	10	0
All Problems		All Types		
17		6919		

Service Status Details For All Host

Select hosts / services with leftclick to send multiple commands. Select multiple with shift + mouse.
 select all (hosts) - unselect all - all problems - all with downtime

Host	Service	Status	Last Check	Duration	Attempt	Status Information
dbbs	Backup_zrm_12 DC	WARNING	12:49:33	0d 0h 10m 5s	9/30	Making one.
	Backup_zrm_12 OP	WARNING	12:39:37	0d 0h 38m 41s	30/30	Making one.
	Disk Check	WARNING	12:49:27	0d 0h 3m 51s	12/30	(/dev/mapper/sql-data-AD)(/data-AD): WARNING - Space 91%
docache2	Firewall Enabled	UNKNOWN	12:48:00	0d 0h 1m 38s	3/3	NRPE: Unable to read output
	LDAP client	CRITICAL	12:41:59	0d 0h 9m 39s	3/3	Nebezi unsod. Nebezi nsld.
	MemCached Response	CRITICAL	12:48:53	0d 0h 50m 25s	3/3	MEMCACHED CRITICAL - Can't connect to 192.168.248.240
	MemCached Size	CRITICAL	12:49:29	0d 0h 49m 49s	3/3	MEMCACHED CRITICAL - Can't connect to 192.168.248.240
	Root login	WARNING	12:48:45	0d 0h 9m 53s	3/3	Root is logged.
docsc1	Elasticsearch Backup	CRITICAL	12:39:08	17d 21h 41m 10s	3/3	Za posledni 3 dny neni k dispozici uspesna zaloha.
dorm1	Replication check	CRITICAL	12:48:47	12d 2h 26m 48s	3/3 #2	Slave_IO_Running: No Slave_SQL_Running: Yes
lbproxy7	Backup_dirvish_crontabs	CRITICAL	12:43:25	2d 12h 43m 33s	3/3	Nop, there's no backup.
	Backup_dirvish_etc	CRITICAL	12:44:15	2d 12h 42m 43s	3/3	Nop, there's no backup.
	Backup_dirvish_home	CRITICAL	12:45:06	2d 12h 41m 52s	3/3	Nop, there's no backup.
	Backup_dirvish_opt	CRITICAL	12:41:41	2d 12h 45m 17s	3/3	Nop, there's no backup.
	Backup_dirvish_usr-local	CRITICAL	12:49:18	2d 12h 37m 40s	3/3	Nop, there's no backup.
lseq2	General Health	WARNING	12:49:16	41d 2h 46m 24s	3/3	OVERALL HEALTH WARNING
mtesd01	ElasticSearch	WARNING	12:47:52	22d 12h 48m 47s	10/10	One or more indexes are missing replica shards. Use -vv to list them.

select all (hosts) - unselect all - all problems - all with downtime

17 of 17 Matching Service Entries Displayed

Services

10 Critical	6 Warning	1 Unknown	6902 OK	0 Pending
9 Unhandled Problems	6 Unhandled Problems	1 Unhandled Problems		
1 Acknowledged				

Monitoring Features

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Enabled All Services Enabled 1 Services Flapping All Hosts Enabled No Hosts Flapping	Enabled 409 Services Disabled 25 Host Disabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled

Motivation

- same here?

Let's summarize!

Motivation

- The old system: Nagios 3
 - began with a few servers, experienced big growth
 - manual configuration
 - our config - almost no possibility of automation
 - complicated readability
 - approx 10 000+ lines of configuration in few files (biggest around 5000)

Motivation

- Bad Incident handling
 - disabling notifications
 - ignoring critical and warning messages
- Lot's of false alarms
- Unreadable frontend