

Température des SI au CNS

«TOPASE»

JSR - 31 mai 2017

Température Opérationnelle de Plate-forme Supervisée

(Alertomètre)

Quoi ?

Tableau de bord synthétique de l'état courant des SI en production sur la PHM

Pour qui ?

- Pilotage opérationnel CNS
- DNE
- Exploitants

Objectifs

- Évaluation de l'état de santé des SI
- Vision synthétique
- Évaluation de l'impact des incidents transverses
- Facile à calculer pour tous les SI
- Intégration avec un calendrier d'évènement
- Point d'entrée vers les consoles de supervision

Difficultés

- Évaluation de la **disponibilité**
 - calcul propre à chaque SI
 - indicateurs pas toujours disponibles
 - fiabilité ?
- Synthétique
 - un indicateur par SI



Température d'un SI

- Basée sur les alertes de supervision en cours
- Tient compte des :
 - maintenances périodiques (timeperiod)
 - maintenances planifiées (downtime)
 - acquittements (acknowledge)
- Pondérée en fonction du type de test
 - NTP, Load, ... => poids faible
 - Page Racvision sur VIP => poids fort

Température d'un SI

- Basée sur les alertes de supervision en cours
- Tient compte des :
 - maintenances périodiques (timeperiod)
 - maintenances planifiées (downtime)
 - acquittements (acknowledge)
- Pondérée en fonction du type de test
 - NTP, Load, ... => poids faible
 - Page Racvision sur VIP => poids fort

Vue globale



Investigations

Tableau de bord - AMIA / AMIA
Zoom Out Last 2 hours Refresh every 1m

Alertes Nagios courantes

	avg	current
CRITICAL	0	0
MAJOR	0.02	0
MINOR	0	0
WARNING	2.20	2.00

APPLICATION AMIA

Activité des logs

	avg	current
EMERGENCY		
SEVERE		
ALERT		
ERROR	1	2
WARNING	1	2
NOTICE	285	139

AMIA

0°

Accès aux ressources et états Nagios par Check_mk

- LISTE DE RESSOURCES** Toutes : serveurs_VIP.....
- ÉTATS KO EN COURS** États : tous

- de 1 jour	de 1 à 7 jours	- de 7 jours	+ de 7 jours
- de 1 jour	de 1 à 7 jours	- de 7 jours	+ de 7 jours
- ÉTATS OK EN COURS** États : tous

- de 1 heure	de 1 à 24 heures	- de 1 jour	de 1 à 7 jours	- de 7 jours	+ de 7 jours
- de 1 heure	de 1 à 24 heures	- de 1 jour	de 1 à 7 jours	- de 7 jours	+ de 7 jours

Accès aux vues cartographiques Nagios par Nagvis

- PHM-AMIA

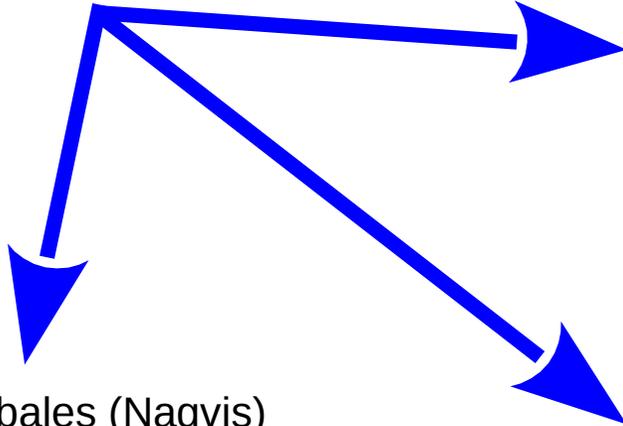
Accès aux logs (dont web et applis) par Kibana

- RECHERCHE SUR TOUS** Tous les logs
- RECHERCHE PAR SÉVÉRITÉ** en partant égale à

informational=6	notice=5	warning=4	error=3	critical=2	alert=1	emerg=0	debug=7
-----------------	----------	-----------	---------	------------	---------	---------	---------
- HISTORIQUE NAGIOS** tous sans redondance en partant des notifications en partant des alertes
- LOGS WEB (Apache)** tous sans code retour http code retour sans erreur <400 code retour avec erreur >400
- LOGS APPLI (jBoss ...)** tous

info=1xx	succès=2xx	redirection=3xx	erreur client web =4xx	erreur serveur appli =5xx
jBoss	Weblogic	Tomcat		

Liens vers autres outils



Autres Vues globales (Nagvis)

CNS - CRT SUPERVISION

Services Transverses d'Infrastructure

DNS

- dnss01
- dnss02
- dnsmast01
- dnsslex01
- dnsslex02

NTP

- ntp01
- ntp02

PROXY

- proxyext01
- proxyrac01

SMTP

- smtp01
- smtp02
- smtp-out-01
- smtp-out-02

LDAP TECH

- vipldap01
- ldap01a
- ldap02b

LOGS

- syslog01a
- syslog02b
- vipslog
- analog
- analog01a
- analog02b

SUPERVISION

- supervision
- supervision01a
- supervision02b
- imc01
- imc02
- imcddd01
- imcddd02
- imcddd03
- imcddd04
- imcddd05
- imcddd06
- imcddd07
- imcddd08
- imcddd09
- imcddd10
- imcddd11
- imcddd12
- imcddd13
- imcddd14
- imcddd15
- imcddd16
- imcddd17
- imcddd18
- imcddd19
- imcddd20
- imcddd21
- imcddd22
- imcddd23
- imcddd24
- imcddd25
- imcddd26
- imcddd27
- imcddd28
- imcddd29
- imcddd30
- imcddd31
- imcddd32
- imcddd33
- imcddd34
- imcddd35
- imcddd36
- imcddd37
- imcddd38
- imcddd39
- imcddd40
- imcddd41
- imcddd42
- imcddd43
- imcddd44
- imcddd45
- imcddd46
- imcddd47
- imcddd48
- imcddd49
- imcddd50
- imcddd51
- imcddd52
- imcddd53
- imcddd54
- imcddd55
- imcddd56
- imcddd57
- imcddd58
- imcddd59
- imcddd60
- imcddd61
- imcddd62
- imcddd63
- imcddd64
- imcddd65
- imcddd66
- imcddd67
- imcddd68
- imcddd69
- imcddd70
- imcddd71
- imcddd72
- imcddd73
- imcddd74
- imcddd75
- imcddd76
- imcddd77
- imcddd78
- imcddd79
- imcddd80
- imcddd81
- imcddd82
- imcddd83
- imcddd84
- imcddd85
- imcddd86
- imcddd87
- imcddd88
- imcddd89
- imcddd90
- imcddd91
- imcddd92
- imcddd93
- imcddd94
- imcddd95
- imcddd96
- imcddd97
- imcddd98
- imcddd99
- imcddd100

HYPERVISION

- bbpm-server
- bbpm-agent
- pr-sti-bppmbo01
- pr-sti-bppmbdd01
- pr-sti-bppmgen01

VIRTUALISATION

- adv01
- adv02
- vcenter01
- pr-sti-psc10

SAUVEGARDE

- tsm01a
- tsm01b
- cli-ro001
- cli-vt001
- cli-ro001
- cli-vt001
- clg-ro001
- clg-vt001

BACKBONES

- Backbone FC
- Backbone réseau

Centre national de Services

Liste des alertes (Nagios)

CheckMK 1.2.6p1

Service search

State	Service	Icons	Status detail	Age	Checked	Perf-O-Meter	Host
WARN	CPU utilization		WARN - 97.7 % used, (warning level at 95.00), 2 CPUs	12 min	3 min	98 %	bbpm-bdd01.tec.phm
CRIT	TSM sauvegarde		TSM backup CRITICAL - No lastbackup for IP 172.29.43.235 CRIT in TSM servers : TSM01A, TSM01B	2016-10-17 10:56:16	2 min		pr-sti-supadmin01.tec.phm
CRIT	Awstatats_analog		CRIT - CRITICAL - analog n'est pas mis à jour (20161202)	38 min	2 min		pr-sti-suptb01.tec.phm
CRIT	Awstatats_foed-centra		CRIT - CRITICAL - foed-centra n'est pas mis à jour (20161202)	38 min	2 min		pr-sti-suptb01.tec.phm
CRIT	Awstatats_foed-edoceo-delta		CRIT - CRITICAL - foed-edoceo-delta n'est pas mis à jour (20161202)	38 min	2 min		pr-sti-suptb01.tec.phm
CRIT	Awstatats_foed-portail		CRIT - CRITICAL - foed-portail n'est pas mis à jour (20161202)	38 min	2 min		pr-sti-suptb01.tec.phm
CRIT	Awstatats_gospel-dadsu		CRIT - CRITICAL - gospel-dadsu n'est pas mis à jour (20161202)	38 min	2 min		pr-sti-suptb01.tec.phm
CRIT	Awstatats_gospel-pale		CRIT - CRITICAL - gospel-pale n'est pas mis à jour (20161202)	38 min	2 min		pr-sti-suptb01.tec.phm
CRIT	Awstatats_sirhen-gestionnaire		CRIT - CRITICAL - sirhen-gestionnaire n'est pas mis à jour (20161202)	38 min	2 min		pr-sti-suptb01.tec.phm
CRIT	Awstatats_sirhen-portail-agent		CRIT - CRITICAL - sirhen-portail-agent n'est pas mis à jour (20161202)	38 min	2 min		pr-sti-suptb01.tec.phm

Recherche dans les logs

Last 60m

groups: amv-stb-supervision-pr

Search

78,889 hits

Load Save

Columns

2000
1500
1000
500
0

doc_count per 30s

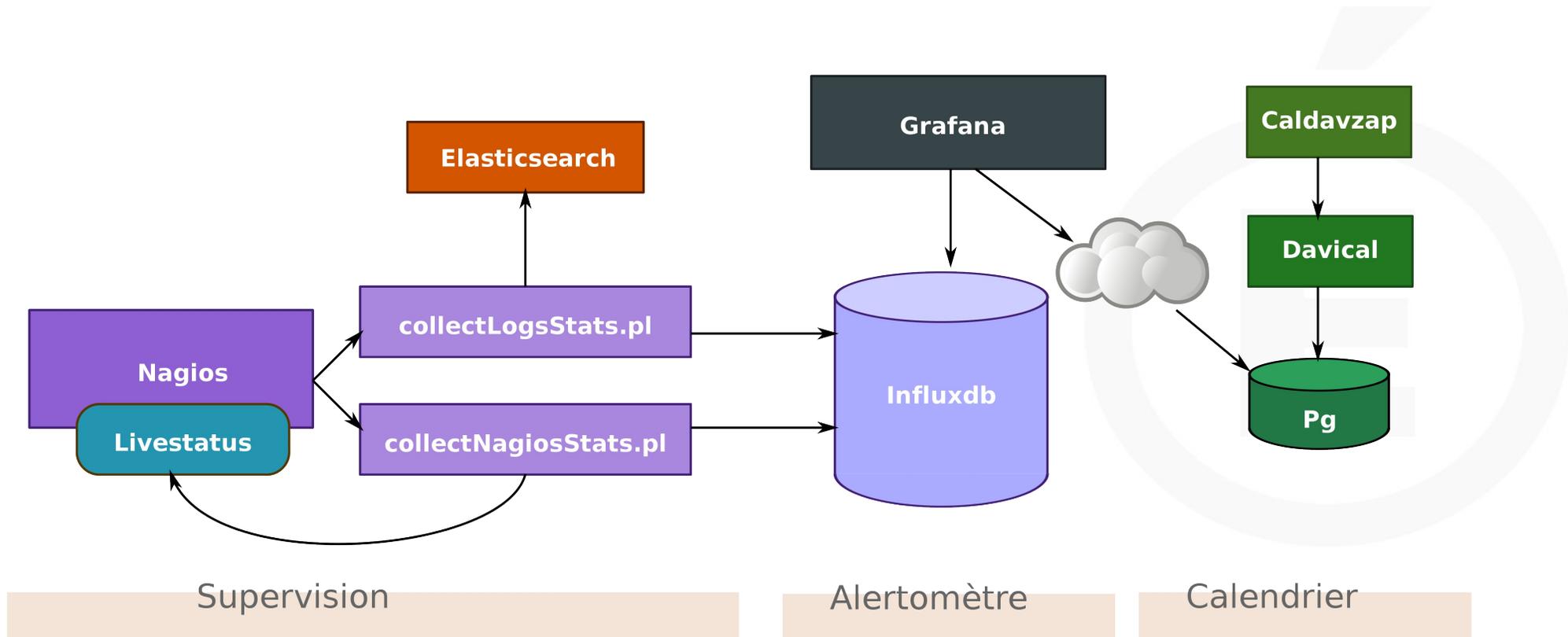
07:50:00 07:55:00 08:00:00 08:05:00 08:10:00 08:15:00 08:20:00 08:25:00 08:30:00 08:35:00 08:40:00 08:45:00

12-2 12-2 12-2 12-2 12-2 12-2 12-2 12-2 12-2 12-2 12-2 12-2

0 to 100

Time	< severity >	< program >	< source_host >	< short_message >
2016-12-02T08:49:00	informational	dovecot	supervision02b.tec.in.phm.education.gouv.fr	imap-login: Login: user=racmail-, method=PLAIN, ip=172.29.43.237, ip=172.29.43.237, mpid=9369, TLS
2016-12-02T08:49:00	informational	dovecot	supervision02b.tec.in.phm.education.gouv.fr	imap-login: Login: user=racmail-, method=PLAIN, ip=172.29.43.237, ip=172.29.43.237, mpid=9367, TLS
2016-12-02T08:49:00	informational	dovecot	supervision02b.tec.in.phm.education.gouv.fr	imap-login: Login: user=racmail-, method=PLAIN, ip=172.29.43.237, ip=172.29.43.237, mpid=9366, TLS
2016-12-02T08:49:00	informational	dovecot	supervision02b.tec.in.phm.education.gouv.fr	imap-login: Login: user=racmail-, method=PLAIN, ip=172.29.43.237, ip=172.29.43.237, mpid=9365, TLS
2016-12-02T08:49:00	informational	httpd	analog01a.tec.in.phm.education.gouv.fr	GET /rabbottmg/api/overview
2016-12-02T08:48:58	informational	postfix	supervision02b.tec.in.phm.education.gouv.fr	connect from supervision02b(172.29.43.231)
2016-12-02T08:48:58	informational	sshd	pr-sti-suptb01.tec.in.phm.education.gouv.fr	Connection closed by 172.29.43.231
2016-12-02T08:48:58	informational	httpd	supervision02b.tec.in.phm.education.gouv.fr	GET /index.php
2016-12-02T08:48:58	informational	httpd	supervision02b.tec.in.phm.education.gouv.fr	GET /check_mki/dashboard_dashlet.py
2016-12-02T08:48:58	informational	httpd	supervision02b.tec.in.phm.education.gouv.fr	GET /hagis/serveur/core/ajax_handler.php
2016-12-02T08:48:57	informational	httpd	supervision02b.tec.in.phm.education.gouv.fr	GET /check_mki/mwep.py
2016-12-02T08:48:56	informational	postfix	supervision02b.tec.in.phm.education.gouv.fr	F01EA8005A: removed
2016-12-02T08:48:56	informational	postfix	supervision02b.tec.in.phm.education.gouv.fr	F01EA8005A: message-id=<

Architecture (simplifiée)



Le calendrier des évènements

- Un agenda spécialisé maintenu par le CRT Supervision
- Évènements :
 - incidents importants et/ou transverses
 - maintenances
- Utilisation possible pour le calcul de disponibilité
- Accessible en caldav

Évolutions prévues

- Influxdb → Elasticsearch
- Intégration plus forte du calendrier d'évènements
- Intégration à iTop (référentiel)
- Packaging



Questions ?