Sécurité des infrastructures

Monitoring

Présentation

- Monitoring

- Monitoring vs. Logging

- Protocoles

- Centreon

Monitoring

- Surveillance IT
- Assure la disponibilité et la performance
- Suivi en temps réel et historique des métriques
- Sécurité de l'infrastructure
  - Pics d'activité
  - Trafic réseau
  - Charges de travail élevées

Monitoring

- Quelques types de métriques
  - CPU
  - Mémoire vive
  - Espace disque
  - Processus et services
  - Accessibilité applications
  - Détection de malwares
  - Température
  - Cartes RAID
  - …

Monitoring
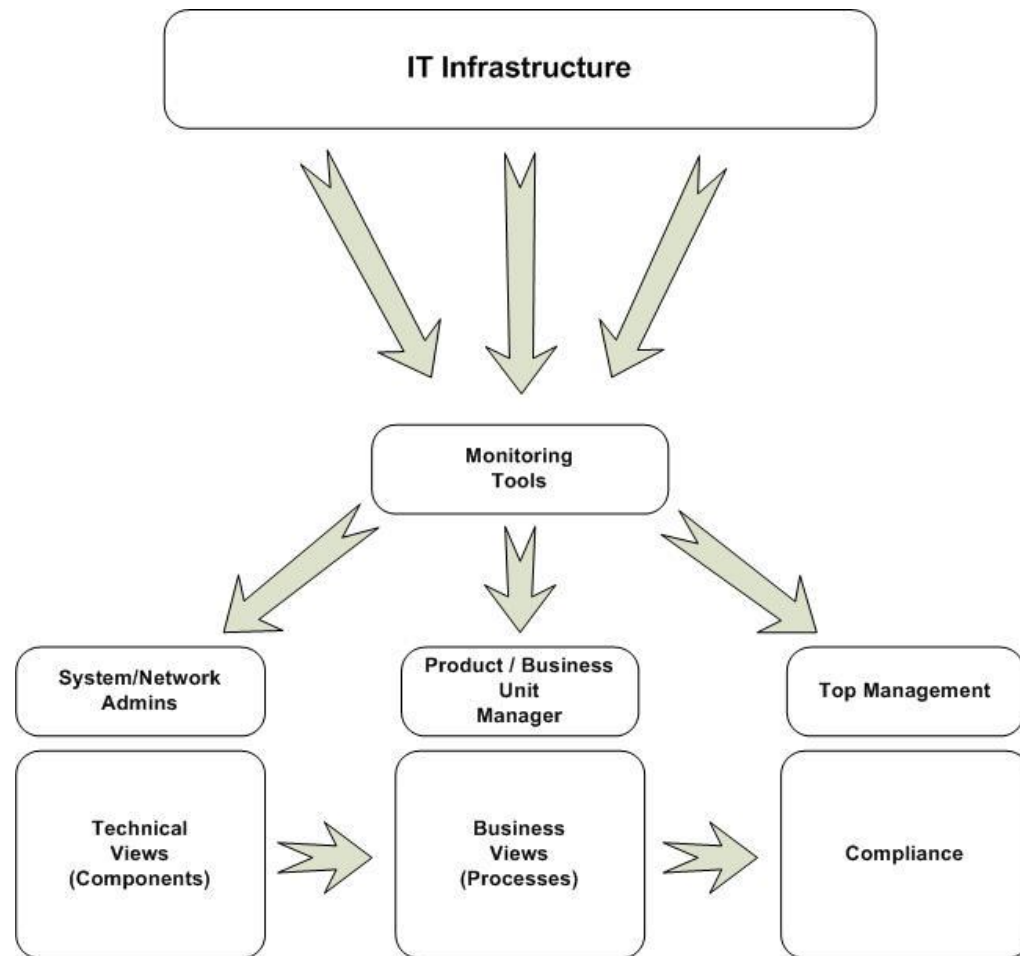
Monitoring

- Challenges :
  - Pertinences des métriques
  - Mixité de technologies
  - Réseaux complexes
  - Alerting ?
  - Sécurité des communications

Monitoring

- Monitoring actif
  - Le serveur de monitoring va chercher l'information sur la machine

- Monitoring passif
  - Les équipements envoient les informations au serveur de monitoring

Monitoring

Monitoring

Monitoring vs. Logging

- Monitoring
  - Processus continu de collecte d'informations
  - Analyse des données en temps réel
  - Proactif
  - Prise de décision immédiate | Réactions
  - Processus actif

Monitoring vs. Logging

- Logging
  - Enregistrement des évènements liés aux activités d'un SI
  - Historique des évènements
  - Processus passif | Examination en cas de problème

Monitoring vs. Logging

- Quelques outils de monitoring

Monitoring vs. Logging

- Quelques outils de logging

Protocoles

- Protocoles
  - ICMP (OSI couche 3)
  - SNMP (*Simple Network Management Protocol*)
  - WMI
  - NRPE
  - SSH
  - HTTP
  - SMTP
  - …

Protocoles

- Protocoles
  - **ICMP (OSI couche 3)**
  - **SNMP (*Simple Network Management Protocol*)**
  - **WMI**
  - **NRPE**
  - SSH
  - HTTP
  - SMTP
  - …

Protocoles (ICMP)

- ICMP (*Internet Control Message Protocol*)
- Protocole de couche 3
- *Default host check*
- Ping check

```
pierremichaux@
$ ping google.be
PING google.be (142.250.201.163): 56 data bytes
64 bytes from 142.250.201.163: icmp_seq=0 ttl=59 time=23.028 ms
64 bytes from 142.250.201.163: icmp_seq=1 ttl=59 time=21.299 ms
64 bytes from 142.250.201.163: icmp_seq=2 ttl=59 time=22.351 ms
64 bytes from 142.250.201.163: icmp_seq=3 ttl=59 time=23.781 ms
64 bytes from 142.250.201.163: icmp_seq=4 ttl=59 time=16.436 ms
64 bytes from 142.250.201.163: icmp_seq=5 ttl=59 time=17.105 ms
^C
--- google.be ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 16.436/20.667/23.781/2.861 ms
```

Protocoles (SNMP)

- SNMP (*Simple Network Management Protocol*)
- RFC1157
- UDP 161 ou UDP 162 (TRAP)
- Versions v1 – v2 – v3
- SNMP vs SNMP TRAP
- MIB
- OID

Protocoles (SNMP)

- ## SNMPv1 – SNMPv2
  - Versions similaires
  - v2 corrige quelques imperfections de la v1
  - String partagé agent gestionnaire → communauté
  - v2 intègre les TRAP SNMP

Cadre d'administration SNMPv1

Figure 1
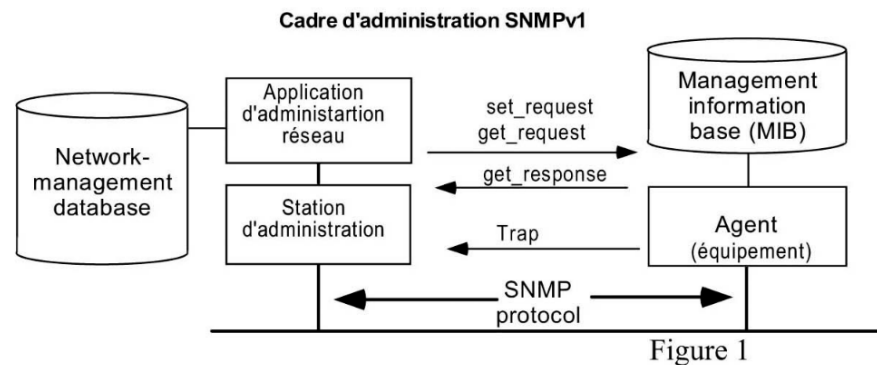
Protocoles (SNMP)

- SNMP vs. SNMP TRAP
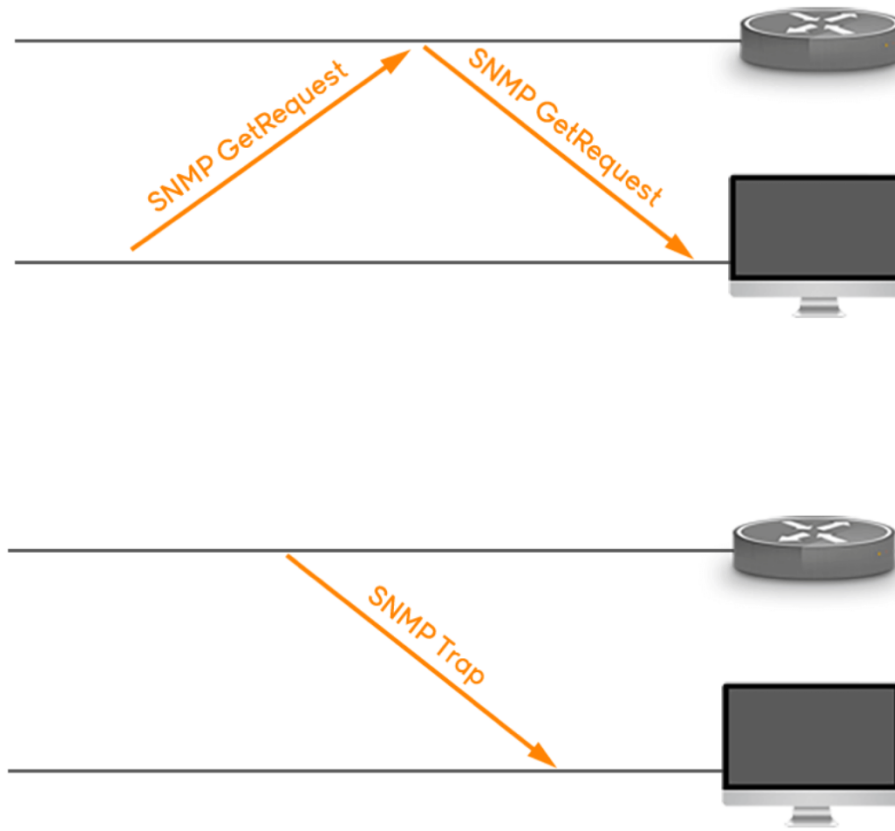
Protocoles (SNMP)

- ## SNMPv3
  - Amélioration du standard SNMPv2
  - Authentification
  - Chiffrement
  - DES

Protocoles (SNMP)

- MIB (Management Information Base)
  - Base de données contenant les objets gérables
  - Objet = donnée spécifique
  - Structuration hiérarchique

- OID (Object IDentifier)
  - Identifiant **unique**
  - Objet contenu dans un MIB
  - Séquence de nombres séparés par des « . »
  - Séquence indique la position de l'objet dans le MIB

Protocoles (SNMP)

- MIB et OID
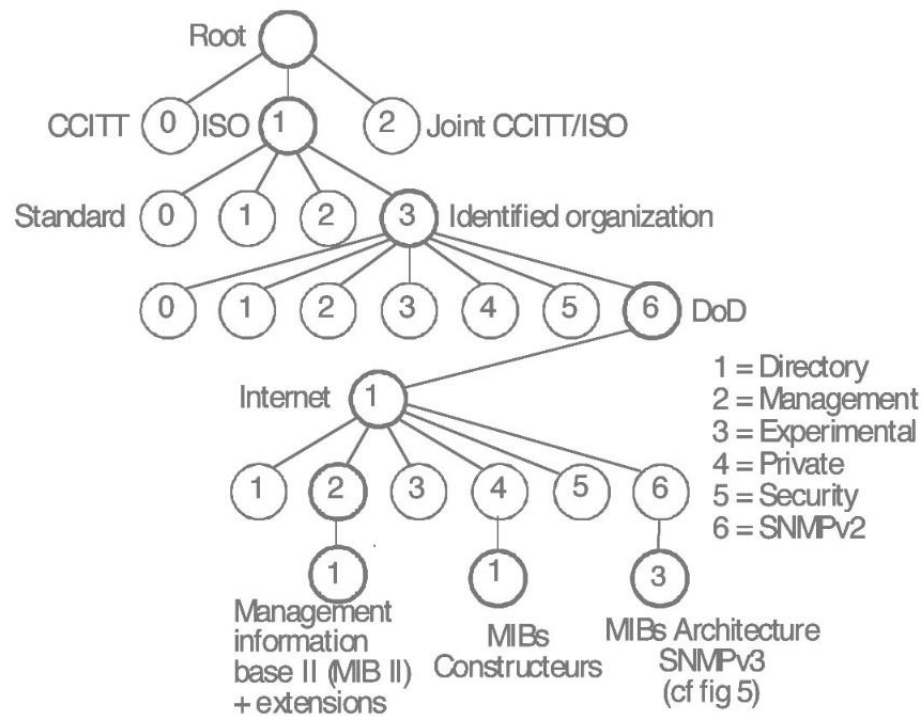
Protocoles (SNMP)

- Commandes
  - SNMPWALK
  - SNMPGET
  - SNMPBULKWALK
  - SNMPTABLE
  - SNMPSET
  - SNMPTRAPD

Protocoles (SNMP)

- Debian
  - Installation SNMP**D**
  - /etc/snmp/snmpd.conf
  - *agentaddress* → possibilité d'indiquer simplement le protocole:port
  - *viewsystemonly* → OID level
  - *rocommunity* → communauté pour v2c
  - SNMPv3
    - Authentification
    - Chiffrement
    - Création utilisateur
    - Création passphrase

Protocoles (SNMP)

- Windows
  - Installation dans rôles et services
  - Configuration *community string*
  - Restart service SNMP

Protocoles (SNMP)

- Commandes
  - **SNMPWALK**
  - **SNMPGET**
  - SNMPBULKWALK
  - SNMPTABLE
  - SNMPSET
  - SNMPTRAPD

Protocoles (WMI)

- WMI (*Windows Management Instrumentation*)
- Propriétaire Microsoft
- WMIC : ligne de commandes WMI (maintenant dépréciée)
- WMIC remplacé par WSMAN (*agentless*)
  - Activer WinRM
  - Configuration firewall (TCP 5986)
  - Création certificat *self-signed*
  - Création utilisateur dédié
  - Configuration WMI (ROOT/CIMv2)

Protocoles (NRPE)

- NRPE (*Nagios Remote PluginExecutor*)
- Monitoring via un agent
- Exécution de plugins sur un serveur (Linux / Windows)
- Commande *check_nrpe* sur le serveur de monitoring
- Agent **daemon nrpe** sous Linux
- Agent **NSClient++** sous Windows

Protocoles (NRPE)

- Paquet NRPE Centreon : **centreon-nrpe3-plugin**
- Paquet NRPE client Linux : **nrpe-ng**
- /etc/nrpe/centreon-nrpe4.cfg
- Configuration de base :
  - IP poller
  - Port
  - SSL
  - ...

```
command[check_users]=/usr/lib/nagios/plugins/check_users -w 5 -c 10
command[check_load]=/usr/lib/nagios/plugins/check_load -r -w .15,.10,.05 -c .30,.25,.20
command[check_hda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/hda1
command[check_zombie_procs]=/usr/lib/nagios/plugins/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 200
command[check_centreon_plugins]=/usr/lib/centreon/plugins/centreon_linux_local.pl --plugin=$ARG1$ --mode=$ARG2$ $ARG3$
```

Protocoles (NRPE)

- Agent Windows : **NSClient++**
- Directive **ssl_version=xxxxx**
- Commandes à ajouter dans le fichier .ini !

Centreon

- Monitoring / supervision
- Fork Nagios
- Licence GPL v2
- Open source
- CentOS
- Centreon Web
- Centreon Engine
- Centreon Broker
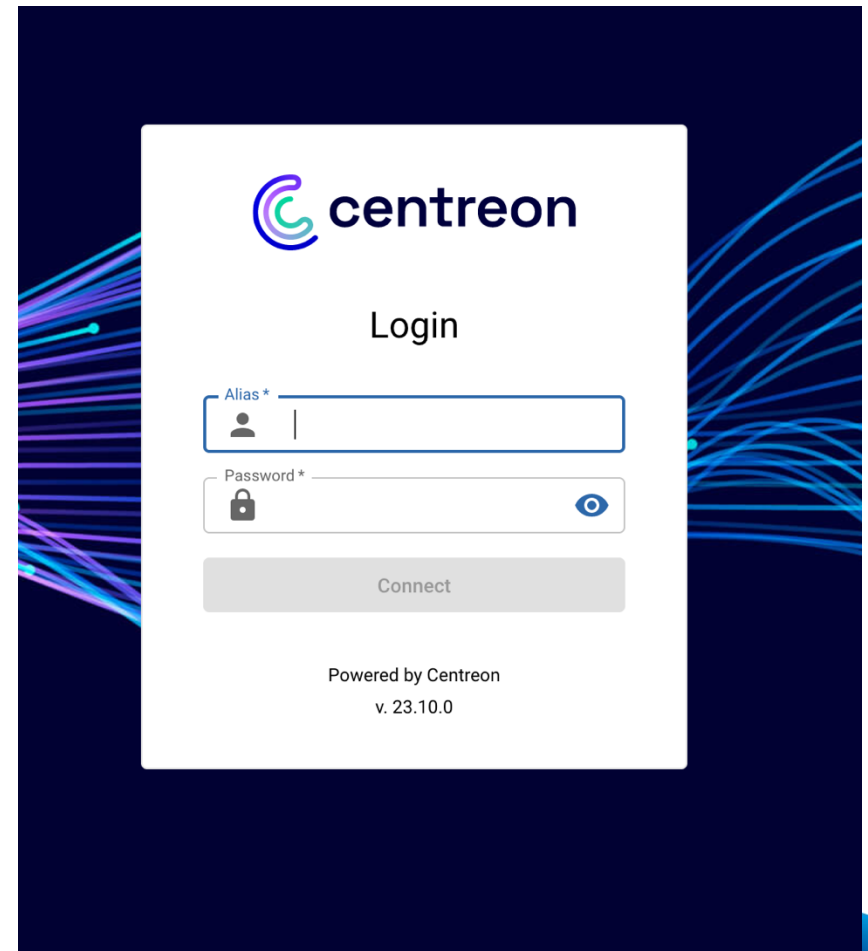
Centreon

- Home
- Monitoring
- Reporting
- Configuration
- Administration

Centreon – configuration

- Hosts
- Services
- Users
- Commands
- Notifications
- Monitoring collector manager
- Pollers
- Knowledge base (utilise MediaWiki)

Centreon – configuration

- Hosts

Centreon – configuration

Host Configuration   **Notification**   **Relations**   **Data Processing**   **Host Extended Infos**

I Add a Host

Notification

? Notification Enabled   ○ Yes ○ No ● Default

Notification receivers

? Linked Contacts   [   ] ⊗

? Linked Contact Groups   [   ] ⊗

Notification options

? Notification Options   ☐ Down ☐ Unreachable ☐ Recovery ☐ Flapping ☐ Downtime Scheduled ☐ None

? Notification Interval   [   ] * 60 seconds

? Notification Period   [Notification Period   ▼] ⊗

? First notification delay [   ] * 60 seconds

? Recovery notification delay [   ] * 60 seconds

                                    [Save] [Reset]

Centreon – configuration

- Services

Centreon – configuration

- Users

Centreon – configuration

- Commands

Name	Command Line	Type	Host Uses	Services Uses	Status	Options
App-Centreon-MySQL-Partitioning	$CENTREONPLUGINS$/centreon_centreon_database.pl --...	Check	0 (0)	0 (1)	ENABLED	⊘
App-DB-MySQL	$CENTREONPLUGINS$/centreon_mysql.pl --plugin=datab...	Check	0 (0)	0 (6)	ENABLED	⊘
App-DB-MySQL-Database-Size	$CENTREONPLUGINS$/centreon_mysql.pl --plugin=datab...	Check	0 (0)	0 (1)	ENABLED	⊘
App-DB-MySQL-Long-Queries	$CENTREONPLUGINS$/centreon_mysql.pl --plugin=datab...	Check	0 (0)	0 (1)	ENABLED	⊘
App-DB-MySQL-MariaDB-Replication	$CENTREONPLUGINS$/centreon_mysql.pl --plugin=datab...	Check	0 (0)	0 (1)	ENABLED	⊘
App-DB-MySQL-Qcache-Hitrate	$CENTREONPLUGINS$/centreon_mysql.pl --plugin=datab...	Check	0 (0)	0 (1)	ENABLED	⊘
App-DB-MySQL-Queries	$CENTREONPLUGINS$/centreon_mysql.pl --plugin=datab...	Check	0 (0)	0 (1)	ENABLED	⊘
App-DB-MySQL-Sql	$CENTREONPLUGINS$/centreon_mysql.pl --plugin=datab...	Check	0 (0)	0 (1)	ENABLED	⊘
App-DB-MySQL-Sql-String	$CENTREONPLUGINS$/centreon_mysql.pl --plugin=datab...	Check	0 (0)	0 (1)	ENABLED	⊘
App-DB-MySQL-Threads-Connected	$CENTREONPLUGINS$/centreon_mysql.pl --plugin=datab...	Check	0 (0)	0 (1)	ENABLED	⊘
App-Monitoring-Centreon-Central-Broker-Stats	$CENTREONPLUGINS$/centreon_centreon_central.pl --p...	Check	0 (0)	0 (1)	ENABLED	⊘
App-Monitoring-Centreon-Host-Dummy	$CENTREONPLUGINS$/centreon_centreon_poller.pl --pl...	Check	0 (2)	0 (0)	ENABLED	⊘
App-Monitoring-Centreon-Service-Dummy	$CENTREONPLUGINS$/centreon_centreon_poller.pl --pl...	Check	0 (0)	0 (1)	ENABLED	⊘

Centreon – configuration

- Commands

- Macro [(https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/macrolist.html)](https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/macrolist.html)

Legend:

No	The macro is not available
Yes	The macro is available

Macro Name	Service Checks	Service Notifications	Host Checks	Host Notifications	Service Event Handlers and OCSP	Host Event Handlers and OCHP	Service Perf Data	Host Perf Data
Host Macros: [3]								
$HOSTNAME$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTDISPLAYNAME$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTALIAS$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTADDRESS$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTSTATE$	Yes	Yes	Yes [1]	Yes	Yes	Yes	Yes	Yes
$HOSTSTATEID$	Yes	Yes	Yes [1]	Yes	Yes	Yes	Yes	Yes
$LASTHOSTSTATE$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$LASTHOSTSTATEID$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTSTATETYPE$	Yes	Yes	Yes [1]	Yes	Yes	Yes	Yes	Yes
$HOSTATTEMPT$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$MAXHOSTATTEMPTS$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTEVENTID$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$LASTHOSTEVENTID$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTPROBLEMID$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$LASTHOSTPROBLEMID$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTLATENCY$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTEXECUTIONTIME$	Yes	Yes	Yes [1]	Yes	Yes	Yes	Yes	Yes
$HOSTDURATION$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTDURATIONSEC$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTDOWNTIME$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTPERCENTCHANGE$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTGROUPNAME$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTGROUPNAMES$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$LASTHOSTCHECK$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$LASTHOSTSTATECHANGE$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$LASTHOSTUP$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$LASTHOSTDOWN$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$LASTHOSTUNREACHABLE$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTOUTPUT$	Yes	Yes	Yes [1]	Yes	Yes	Yes	Yes	Yes
$LONGHOSTOUTPUT$	Yes	Yes	Yes [1]	Yes	Yes	Yes	Yes	Yes
$HOSTPERFDATA$	Yes	Yes	Yes [1]	Yes	Yes	Yes	Yes	Yes
$HOSTCHECKCOMMAND$	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
$HOSTACKAUTHOR$ [8]	No	No	No	Yes	No	No	No	No
$HOSTACKAUTHORNAME$ [8]	No	No	No	Yes	No	No	No	No
$HOSTACKAUTHORALIAS$ [8]	No	No	No	Yes	No	No	No	No
$HOSTACKCOMMENT$ [8]	No	No	No	Yes	No	No	No	No

Centreon – configuration

- Custom macro
  - Host : $_HOST****
  - Service : $_SERVICE****

  - Cas spéciaux
    - SNMP communauté → $_HOSTSNMPCOMMUNITY$
    - SNMP version → $_HOSTSNMPVERSION$

Centreon – configuration

- Pollers
  - Serveurs équipés avec un *scheduler* et un *broker module* (serveur de monitoring)

	Name	IP Address	Server type	Is running ?	Conf Changed *	PID	Uptime	Last Update	Version	Default	Status	Actions	Options
☐	Central	127.0.0.1	Central	YES	NO	19303	19 days	April 16, 2024 1:47:37 PM	Centreon Engine 23.10.0	Yes	ENABLED	🖉📄	🚫 1
													30 ⌄

  - Recharge configuration

I Configuration Files Export

Polling instances

⑦ Pollers *   Central ✕   ⊗

Actions

⑦ ☑ Generate Configuration Files

⑦ ☑ Run monitoring engine debug (-v)

⑦ ☑ Move Export Files

⑦ ☑ Restart Monitoring Engine   Method Reload   ⌄

⑦ ☐ Post generation command

Export

Centreon – administration

- Pour aller plus loin…
  - Configuration authentification (// LDAP)
  - Restrictions visions via ACL
  - Backup configuration
  - Images personnalisées
  - Extensions (gratuites et payantes)
  - Logging
  - …