DOCUMENTATION TECHNIQUE SONDES NAGIOS

CLIENT

- Sonde numéro 1
  Nom de la sonde : CPU_w70_c90_1min
  Objectif de la sonde : Vérifier la charge toutes les minutes. Déclencher un avertissement si l'utilisation a été supérieure à 70 % de la capacité totale au cours de la dernière minute et déclencher un état critique si l'utilisation a été supérieure à 90 %.
  Paramétrage de la sonde : warning à 70 %, critical à 90 %. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : lancer le gestionnaire des tâches, regardez le(s) processus, évaluer leur nécessité, terminer la tâche le cas échéant.

- Sonde numéro 2
  Nom de la sonde : C : Disk Usage 70_85 1min
  Objectif de la sonde : Vérifier le taux d'utilisation du support de stockage. Déclencher un avertissement si l'utilisation dépasse les 70 % et déclencher un état critique si l'utilisation dépasse les 80 %.
  Paramétrage de la sonde : warning à 70 %, critical à 80 %. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : faire une recherche de fichiers par taille sur le poste, demander à l'utilisateur s'il ne peut archiver ou supprimer des documents inutiles.

- Sonde numéro 3
  Nom de la sonde : RAM 70_80 1min
  Objectif de la sonde : Vérifier le taux d'utilisation de la mémoire vive. Déclencher un avertissement si l'utilisation a été supérieure à 70 % de la capacité totale au cours de la dernière minute et déclencher un état critique si l'utilisation a été supérieure à 90 %.
  Paramétrage de la sonde : warning à 70 %, critical à 90 %. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : lancer le gestionnaire des tâches, regardez le(s) processus, évaluer leur nécessité, terminer la tâche le cas échéant.

Serveur : RSYSLOG

- Sonde numéro 1
  Nom de la sonde : CPU Usage 50_70 15min
  Objectif de la sonde : Vérifier la charge toutes les 15 minutes. Déclencher un avertissement si l'utilisation a été supérieure à 50 % de la capacité totale au cours des 15 dernières minutes et déclencher un état critique si l'utilisation a été supérieure à 70 %.
  Paramétrage de la sonde : warning à 50 %, critical à 70 %. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : utiliser un outil de monitoring local comme « top », « htop », « btop » (etc..), regarder le(s) processus, évaluer leur nécessité, récupérer leur PID (« prgrep PROCESSUS ») ou le nom du processus (« ps -ef »), terminer le processus (« kill PID » ou (« pkill PROCESSUS »).

- Sonde numéro 2
  Nom de la sonde : CPU Usage 60_80 5min
  Objectif de la sonde : Vérifier la charge toutes les 5 minutes. Déclencher un avertissement si l'utilisation a été supérieure à 60 % de la capacité totale au cours des 5 dernières minutes et déclencher un état critique si l'utilisation a été supérieure à 80 %.
  Paramétrage de la sonde : warning à 60 %, critical à 80 %. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : utiliser un outil de monitoring local comme « top », « htop », « btop » (etc..), regarder le(s) processus, évaluer leur nécessité, récupérer leur PID (« prgrep PROCESSUS ») ou le nom du processus (« ps -ef »), terminer le processus (« kill PID » ou (« pkill PROCESSUS »).

- Sonde numéro 3
  Nom de la sonde : CPU Usage 70_90 1min
  Objectif de la sonde : Vérifier la charge toutes les 1 minutes. Déclencher un avertissement si l'utilisation a été supérieure à 70 % de la capacité totale au cours de la dernière minute et déclencher un état critique si l'utilisation a été supérieure à 90 %.
  Paramétrage de la sonde : warning à 70 %, critical à 90 %. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : utiliser un outil de monitoring local comme « top », « htop », « btop » (etc..), regarder le(s) processus, évaluer leur nécessité, récupérer leur PID (« prgrep PROCESSUS ») ou le nom du processus (« ps -ef »), terminer le processus (« kill PID » ou (« pkill PROCESSUS »).

- Sonde numéro 4
  Nom de la sonde : Disk Usage 70_80 1min
  Objectif de la sonde : Vérifier le taux d'utilisation du support de stockage. Déclencher un avertissement si l'utilisation dépasse les 70 % et déclencher un état critique si l'utilisation dépasse les 80 %.
  Paramétrage de la sonde : warning à 70 %, critical à 80 %. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : vérifier les logs de Rsyslog en premier, avant de progresser vers d'autres dossiers, archiver/supprimer en cas besoin.

- Sonde numéro 5

  Nom de la sonde : RAM 70_80 1min

  Objectif de la sonde : Vérifier le taux d'utilisation de la mémoire vive. Déclencher un avertissement si l'utilisation a été supérieure à 70 % de la capacité totale au cours de la dernière minute et déclencher un état critique si l'utilisation a été supérieure à 90%.

  Paramétrage de la sonde : warning à 70 %, critical à 80 %. Voir règle de la sonde sur le tableau récapitulatif.

  Action à entreprendre en cas d'anomalie : utiliser un outil de monitoring local comme « top », « htop », « btop » (etc..), regarder le(s) processus, évaluer leur nécessité, récupérer leur PID (« prgrep PROCESSUS ») ou le nom du processus (« ps -ef »), terminer le processus (« kill PID » ou (« pkill PROCESSUS »).

- Sonde numéro 6

  Nom de la sonde : USERS 1min

  Objectif de la sonde : Comptabiliser le nombre de sessions utilisateurs ouvertes sur le serveur au cours de la dernière minute. Déclencher un avertissement lorsqu'une session utilisateur est ouverte et déclencher un état critique si 2 sessions sont ouvertes.

  Paramétrage de la sonde : warning à 1 utilisateur, critical à 2. Voir règle de la sonde sur le tableau récapitulatif.

  Action à entreprendre en cas d'anomalie : regarder les logs afin de déterminer si l'origine de la connexion est légitime, couper le flux depuis le pare-feu, restreindre le nombre de connexions ou bloquer la connexion de l'utilisateur via SSH, changer le mot de passe, privilégier les connexions par clef…

Serveur : APACHE2 (http)

- Sonde numéro 1
  Nom de la sonde : CPU Usage 50_70 15min
  Objectif de la sonde : Vérifier la charge toutes les 15 minutes. Déclencher un avertissement si l'utilisation a été supérieure à 50 % de la capacité totale au cours des 15 dernières minutes et déclencher un état critique si l'utilisation a été supérieure à 70 %.
  Paramétrage de la sonde : warning à 50 %, critical à 70 %. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : utiliser un outil de monitoring local comme « top », « htop », « btop » (etc..), regarder le(s) processus, évaluer leur nécessité, récupérer leur PID (« prgrep PROCESSUS ») ou le nom du processus (« ps -ef »), terminer le processus (« kill PID » ou (« pkill PROCESSUS »)

- Sonde numéro 2
  Nom de la sonde : CPU Usage 60_80 5min
  Objectif de la sonde : Vérifier la charge toutes les 5 minutes. Déclencher un avertissement si l'utilisation a été supérieure à 60 % de la capacité totale au cours des 5 dernières minutes et déclencher un état critique si l'utilisation a été supérieure à 80 %.
  Paramétrage de la sonde : warning à 60 %, critical à 80 %. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : utiliser un outil de monitoring local comme « top », « htop », « btop » (etc..), regarder le(s) processus, évaluer leur nécessité, récupérer leur PID (« prgrep PROCESSUS ») ou le nom du processus (« ps -ef »), terminer le processus (« kill PID » ou (« pkill PROCESSUS »)

- Sonde numéro 3
  Nom de la sonde : CPU Usage 70_90 1min
  Objectif de la sonde : Vérifier la charge toutes les 1 minute. Déclencher un avertissement si l'utilisation a été supérieure à 70 % de la capacité totale au cours de la dernière minute et déclencher un état critique si l'utilisation a été supérieure à 90 %.
  Paramétrage de la sonde : warning à 70 %, critical à 90 %. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : utiliser un outil de monitoring local comme « top », « htop », « btop » (etc..), regarder le(s) processus, évaluer leur nécessité, récupérer leur PID (« prgrep PROCESSUS ») ou le nom du processus (« ps -ef »), terminer le processus (« kill PID » ou (« pkill PROCESSUS »)

- Sonde numéro 4
  Nom de la sonde : DISK_/_w70_c80_1min
  Objectif de la sonde : Vérifier le taux d'utilisation du support de stockage. Déclencher un avertissement si l'utilisation dépasse les 70 % et déclencher un état critique si l'utilisation dépasse les 80 %
  Paramétrage de la sonde : warning à 70 %, critical à 80 %. Voir règle de la sonde sur le tableau récapitulatif.

Action à entreprendre en cas d'anomalie : vérifier les logs de Rsyslog en premier, avant de progresser vers d'autres dossiers, archiver/supprimer en cas besoin.

- Sonde numéro 5

  Nom de la sonde : HTTPD 1min

  Objectif de la sonde : Vérifier le bon fonctionnement du service httpd (apache2) toutes les 1 minute. Déclencher un avertissement en cas de défaillance du service et déclencher un état critique si le service se met en défaut.

  Paramétrage de la sonde : warning lors d'un défaut de configuration, critical en cas d'arrêt du service.

  Action à entreprendre en cas d'anomalie : vérifier l'état du service (systemctl status apache2), si le service est arrêté, tenter de le relancer (systemctl restart apache2), utiliser les commandes de diagnostics (journalctl -xe). Si un outil comme fail2ban est présent, regarder les jail et les bannissements afin de déterminer s'il ne s'agît pas d'une attaque, regarder le nombre de connexions au serveur dans les logs (var/log/apache2) regarder la présence des fichiers index des sites hébergés, vérifier la bonne configuration des vhosts….

- Sonde numéro 6

  Nom de la sonde : INDEX 1min

  Objectif de la sonde : Vérifier la présence du fichier index.php de wordpress toutes les 1 minute. Déclencher un avertissement en cas d'absence du fichier.

  Paramétrage de la sonde : warning lorsque le fichier n'est plus présent.

  Action à entreprendre en cas d'anomalie : mettre en corrélation avec l'état des autres sondes (4 et 6), regarder les logs de connexion, l'historique des commandes tapées, restaurer le fichier depuis une sauvegarde.

- Sonde numéro 7

  Nom de la sonde : RAM 70_85 1min

  Objectif de la sonde : Vérifier le taux d'utilisation de la mémoire vive. Déclencher un avertissement si l'utilisation a été supérieure à 70 % de la capacité totale au cours de la dernière minute et déclencher un état critique si l'utilisation a été supérieure à 90 %

  Paramétrage de la sonde : warning à 70 %, critical à 90 %. Voir règle de la sonde sur le tableau récapitulatif.

  Action à entreprendre en cas d'anomalie : utiliser un outil de monitoring local comme « top », « htop », « btop » (etc..), regarder le(s) processus, évaluer leur nécessité, récupérer leur PID (« prgrep PROCESSUS ») ou le nom du processus (« ps -ef »), terminer le processus (« kill PID » ou (« pkill PROCESSUS »)

- Sonde numéro 8

  Nom de la sonde : USERS 1min

  Objectif de la sonde : Comptabiliser le nombre de sessions de l'utilisateur ouvertes sur le serveur au cours de la dernière minute. Déclencher un avertissement lorsque 2 sessions utilisateur sont ouvertes et déclencher un état critique si 4 sessions sont ouvertes.

  Paramétrage de la sonde : warning à 2 utilisateurs, critical à 4. Voir règle de la sonde sur le tableau récapitulatif.

Action à entreprendre en cas d'anomalie : regarder les logs afin de déterminer si l'origine de la connexion est légitime, couper le flux depuis le pare-feu, restreindre le nombre de connexions via SSH, changer le mot de passe, privilégier les connexions par clef…

Poste : DYNFI

- Sonde numéro 1
  Nom de la sonde : CPU Usage 70_80 1min
  Objectif de la sonde : Vérifier la charge toutes les minutes. Déclencher un avertissement si l'utilisation a été supérieure à 70 % de la capacité totale au cours de la dernière minute et déclencher un état critique si l'utilisation a été supérieure à 80 %.
  Paramétrage de la sonde : warning à 70 %, critical à 80 %. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : Vérifier l'utilisation CPU en temps réel (« top -P », « vmstat 1 », « systat -vmstat 1 »)
  Identifier la cause : Processus gourmands/Surcharge (« ps aux | sort -nrk 3 | head -10 », « top -o cpu »)
  Redémarrer les services (« service nginx restart »), tuer les processus gourmands (« kill -9 PID »).

- Sonde numéro 2
  Nom de la sonde : USER 1min
  Objectif de la sonde : Comptabiliser le nombre de sessions de l'utilisateur ouvertes sur le serveur au cours de la dernière minute. Déclencher un avertissement lorsque 2 sessions utilisateur sont ouvertes et déclencher un état critique si 4 sessions sont ouvertes.
  Paramétrage de la sonde : warning à 2 utilisateurs, critical à 4. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : regarder les logs afin de déterminer si l'origine de la connexion est légitime, couper le flux depuis le pare-feu, restreindre le nombre de connexions via SSH, changer le mot de passe, privilégier les connexions par clef…

- Sonde numéro 3
  Nom de la sonde : RAM Usage 1min
  Objectif de la sonde : Vérifier le taux d'utilisation de la mémoire vive. Déclencher un avertissement si l'utilisation a été supérieure à 70 % de la capacité totale au cours de la dernière minute et déclencher un état critique si l'utilisation a été supérieure à 80 %
  Paramétrage de la sonde: warning à 70 %, critical à 80 %. Voir règle de la sonde sur le tableau récapitulatif.
  Paramétrage de la sonde : Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : Vérifier l'utilisation mémoire en temps réel (« top -o res », « vmstat 1 », « sysctl vfs.zfs.arcstats.size »),
  Identifier la cause : Processus/ Cache ZFS/ Trop de connexions/ SWAP, (« ps aux | sort -nrk 4 | head -10 », « swapinfo -h »)
  Redémarrer les services lourds (« service nginx restart »), limiter ARC (« sysctl vfs.zfs.arc_max=536870912 »),
  Libérer le cache (« sync && sysctl vm.drop_caches=3 »),
  Ajouter de la SWAP (« swapon /dev/ada0p2 »),
  Ajouter de la RAM si nécessaire, optimiser les services (« sysctl kern.maxproc=20000").

- Sonde numéro 4

  Nom de la sonde : Traffic Int LAN_DMZ 1min
  Objectif de la sonde : Récuperer le trafique entrant sur les interfaces vtnet1 et 2 (respectivement LAN et DMZ) du par-feu.
  Paramétrage de la sonde : Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : Vérifier le trafic en temps réel (« netstat -i, iftop -i vtnet1, bmon »)
  Identifier la cause : Trop de connexions/ DDoS/ Interface saturée, (« netstat -an | wc -l, pfctl -si, vmstat 1 »)
  Limiter les connexions suspectes (« pfctl -t blacklist -T add IP »), ajuster les règles (« pfctl -f /etc/pf.conf && pfctl -e »).

  POUR LES SONDES 2, 3, ET 4 IL FAUDRAIT AJOUTER DES SEUILS .

Serveur : NAGIOSXI

- Sonde numéro 1
  Nom de la sonde : CURRENT LOAD 1min
  Objectif de la sonde : Vérifier la charge toutes les minutes. Déclencher un avertissement si la charge est supérieure à 2.0 (sur 1 min), 1.5 (sur 5 min) ou 1.0 (sur 10 min) et déclencher un état critique si la charge est supérieure à 4.0, 3.0 ou 2.0 respectivement.
  Paramétrage de la sonde : Warning à 2.0 (1 min), 1.5 (5 min), 1.0 (10 min). Critical à 4.0 (1 min), 3.0 (5 min), 2.0 (10 min).
  Action à entreprendre en cas d'anomalie : Vérifier la charge système en temps réel avec (« top -d 1 », « uptime », « sysctl vm.loadavg »)
  Causes : Trop de processus/ Charge excessive sur les cœurs, Vérifier les processus avec (« ps aux --sort=-%cpu | head -10 », « top -o cpu) »
  Identifier et tuer les processus gourmands en ressources avec (« kill -9 PID », « pkill PROCESSUS »), redémarrer des services si nécessaire (service nginx restart)
  Voir à ajuster les seuils Nagios en fonction des exigences du serveur.

- Sonde numéro 2
  Nom de la sonde : Disk Usage 70_80 1min
  Objectif de la sonde : Vérifier le taux d'utilisation du support de stockage. Déclencher un avertissement si l'utilisation dépasse les 70 % et déclencher un état critique si l'utilisation dépasse les 80 %
  Paramétrage de la sonde : warning à 70 %, critical à 80 %. Voir règle de la sonde sur le tableau récapitulatif.
  Action à entreprendre en cas d'anomalie : vérifier les logs de Rsyslog en premier, avant de progresser vers d'autres dossiers, archiver/supprimer en cas besoin.

- Sonde numéro 3
  Nom de la sonde : HTTPD 1min
  Objectif de la sonde : Vérifier le bon fonctionnement du service httpd (apache) toutes les 1 minute. Déclencher un avertissement en cas de défaillance du service et déclencher un état critique si le service se met en défaut.
  Paramétrage de la sonde : warning lors d'un défaut de configuration, critical en cas d'arrêt du service.
  Action à entreprendre en cas d'anomalie : vérifier l'état du service (systemctl status apache2), si le service est arrêté, tenter de le relancer (systemctl restart apache2), utiliser les commandes de diagnostics (journalctl -xe). Si un outil comme fail2ban est présent, regarder les jail et les bannissements afin de déterminer s'il ne s'agît pas d'une attaque, regarder le nombre de connexions au serveur dans les logs (var/log/apache2) regarder la présence des fichiers index des sites hébergés, vérifier la bonne configuration des vhosts….

- Sonde numéro 4
  Nom de la sonde : MYSQL_1min
  Objectif de la sonde : Vérifier que le service mysql tourne. Déclencher un état critique si le service est arrêté.
  Paramétrage de la sonde : critical lorsque le service mysql est coupé.

Action à entreprendre en cas d'anomalie : vérifier l'état du service (systemctl status mysql), si le service est arrêté, tenter de le relancer (systemctl restart mysql), utiliser les commandes de diagnostics (journalctl -xe). Si un outil comme fail2ban est présent, regarder les jail et les bannissements afin de déterminer s'il ne s'agît pas d'une attaque.

- Sonde numéro 5

  Nom de la sonde : RAM 70_85 1min

  Objectif de la sonde : Vérifier le taux d'utilisation de la mémoire vive. Déclencher un avertissement si l'utilisation a été supérieure à 70 % de la capacité totale au cours de la dernière minute et déclencher un état critique si l'utilisation a été supérieure à 85 %

  Paramétrage de la sonde : warning à 70 %, critical à 85 %. Voir règle de la sonde sur le tableau récapitulatif.

  Action à entreprendre en cas d'anomalie : utiliser un outil de monitoring local comme « top », « htop », « btop » (etc..), regarder le(s) processus, évaluer leur nécessité, récupérer leur PID (« prgrep PROCESSUS ») ou le nom du processus (« ps -ef »), terminer le processus (« kill PID » ou (« pkill PROCESSUS »)

- Sonde numéro 6

  Nom de la sonde : USERS 1min

  Objectif de la sonde : Comptabiliser le nombre de sessions utilisateurs ouvertes sur le serveur au cours de la dernière minute. Déclencher un avertissement lorsqu'une session utilisateur est ouverte et déclencher un état critique si 2 sessions sont ouvertes.

  Paramétrage de la sonde : warning à 1 utilisateur, critical à 2.Voir règle de la sonde sur le tableau récapitulatif.

  Action à entreprendre en cas d'anomalie : regarder les logs afin de déterminer si l'origine de la connexion est légitime, couper le flux depuis le pare-feu, restreindre le nombre de connexions ou bloquer la connexion de l'utilisateur via SSH.