

La surcharge des propriétés pour un check

Sommaire

- Principe: Général
- Accéder à la surcharge
 - Activer le mode surcharge
 - Ouvrir le formulaire de surcharge
- Présentation visuelle
- Surcharger une propriété
 - Réaliser une surcharge
 - Revenir à la valeur initiale du check
- Cas spécifiques
 - Les champs non éditables
 - Les champs de type commande
 - Les données
 - Modèles d'hôte hérités
- Les compteurs
 - Les compteurs de surcharge
 - Les compteurs d'avertissement et d'erreur
 - Erreur spécifique
 - Les surcharges dupliquées
- La surcharge dans les modèles d'hôte
 - Affichage dans la surcharge sur l'hôte
- Surcharge et héritage additif
- La surcharge et l'essai des checks
- Surcharge inactive
 - Rattacher une surcharge inactive
 - Compteur de surcharge inactive
 - Supprimer une surcharge inactive
- Surcharges au format Cfg

Contexte

Le modèle `shinken-arbiter` vous permet de superviser un hôte hébergeant le démon [Arbiter](#).

Description du modèle

Modèle d'hôte correspondant: **`shinken-arbiter`** (notez que ce modèle hérite du modèle **`shinken`** et **`shinken-deamon`**)

Afin de superviser le démon Arbiter, le modèle **`shinken-arbiter`** appliqué à votre hôte, attachera deux checks qui vérifieront la santé et la performance de ce démon.

Checks

- Arbiter - \$KEY\$ - Alive

Vérifie que le démon Arbiter peut être correctement contacté sur le réseau ; la version du démon est affichée également (*Résultat court*) et que les modules sont opérationnels (*Résultat long*).

? Unknown Attachment

- Arbiter - \$KEY\$ - Performance

Retourne le temps de connexion au démon Arbiter ainsi que la liste des connexions avec les autres démons de l'architecture avec leurs numéros de version (*si possible*).

Si certains démons ne sont pas à jours, alors un Avertissement sera remonté.

Si jamais le démon Arbiter est en exécution sur une machine virtuelle supervisé par VMware, alors le pourcentage de temps de vol de CPU (*CPU Ready*) sera affiché.

? Unknown Attachment

Données du modèle

Les checks de l'Arbiter peuvent être configurés via des données fournies par le modèle.

Les données suivantes sont disponibles:

Nom de la donnée	Description	Valeur par défaut	Hérité du modèle d'hôte ou locale
SHINKEN_PROTOCOL	Protocole utilisé pour établir la connexion avec l'Arbiter	http	shinken
ARBITER_PORT	Port utilisé pour l'établissement de la connexion avec l'Arbiter	7770	Locale
CHECK_SHINKEN_TIMEOUT	Timeout utilisé pour l'établissement de la connexion avec l'Arbiter	3	shinken
ARBITER_LIST	Liste d'Arbiter (<i>Multi-démon</i>)	arbiter-master\$(\$_HOSTARBITER_PORTS)\$	Locale - Duplicate For Each
THRESHOLD_CPU_STOLEN_WARNING	Seuil de CPU volé (<i>en pourcentage</i>) sur une machine virtuelle supervisée par VMware avant de déclencher un warning	5	shinken-daemon
THRESHOLD_CPU_STOLEN_CRITICAL	Seuil de CPU volé (<i>en pourcentage</i>) sur une machine virtuelle supervisée par VMware avant de déclencher un critique	10	shinken-daemon

Métriques enregistrées

Les checks du modèle enregistrent des données de performance, qui peuvent ensuite être affichées dans l'interface de Visualisation sur l'[Onglet Graphes](#) ou bien le [Widget Graphique](#).

Nom du check	Nom de la métrique	Explication
Arbiter - \$KEY\$ - Alive	connexion_time	Temps de connexion en secondes pour contacter le démon
Arbiter - \$KEY\$ - Performance	cpu_stolen_vmware_percent_ready	(Seulement si le démon est situé sur une VM VMWare) Valeur de l'indicateur VMWare %ready (temps de blocage de la VM avant d'avoir accès à ses VCpu, donc temps perdu du point de vue de la VM)

Commandes

Nom du check	Commande du check	Ligne de commande
Arbiter - \$KEY\$ - Alive	check_shinken_arbiter! alive! \$ VALUE1 \$	\$PLUGINS_DIR/check_shinken -H "\$HOSTADDRESS\$" -p "\$ARG2\$" --shinkenversion "\$SHINKENVERSION\$" -t arbiter -m \$ARG1\$ --timeout \$_HOSTCHECK_SHINKEN_TIMEOUT\$ -w \$_HOSTTHRESHOLD_CPU_STOLEN_WARNING\$ -c \$_HOSTTHRESHOLD_CPU_STOLEN_CRITICAL\$
Arbiter - \$KEY\$ - Performance	check_shinken_arbiter! stats! \$ VALUE1 \$	\$PLUGINS_DIR/check_shinken -H "\$HOSTADDRESS\$" -p "\$ARG2\$" --shinkenversion "\$SHINKENVERSION\$" -t arbiter -m \$ARG1\$ --timeout \$_HOSTCHECK_SHINKEN_TIMEOUT\$ -w \$_HOSTTHRESHOLD_CPU_STOLEN_WARNING\$ -c \$_HOSTTHRESHOLD_CPU_STOLEN_CRITICAL\$

Description des erreurs de Arbiter - \$KEY\$ - Alive

Erreur de surcharge des disques de logs

- En cas de disques trop lent sur le volume des logs, le check sera mis en **WARNING** avec l'erreur suivante.

? Unknown Attachment

Le démon a bloqué une tentative de chargement d'objet malveillant

Il est possible qu'un démon puisse détecter et bloquer une tentative d'injection d'objet malveillant par le biais de l'une de ses routes.

Un message est remonté :

- le nombre total de ces tentatives que le démon a bloqué ce jour (*le compte commence à minuit*) ;
- pour chacune des tentatives (*maximum 3*) :
 - descriptif de l'objet que l'attaquant essaye de charger,
 - sa provenance de l'attaque, par exemple le nom de la route utilisée, et l'IP à la source de l'attaque,

- sa date.

? Unknown Attachment

Description des erreurs de Arbiter - \$KEY\$ - Performance

Erreur de vol de CPU

Seulement si votre machine virtuelle est hébergé sur un hyperviseur VMWare

- Si la VM se fait voler trop de temps de calcul (CPU Stolen), le check sera mis en **WARNING** ou en **CRITIQUE** (en fonction du taux de vol fixé par défaut ou indiqué par l'utilisateur).
 - Vous pouvez avoir plus d'information sur cet indicateur et comment réduire la part de temps de la VM sur la page [Machine VMWare avec un fort taux de CPU Stolen \(%ready + %costop\)](#)

? Unknown Attachment

? Unknown Attachment

Les serveurs ne sont pas à la même heure

- Si le serveur n'est pas à la même heure que le serveur Arbiter (qui fait office de référence), une erreur **CRITICAL** sera levée, car des temps différents sur les différents serveurs va avoir des effets **désastreux** sur la cohérences des données de supervision.

? Unknown Attachment

Le démon a bloqué une tentative de chargement d'objet malveillant

Il est possible qu'un démon puisse détecter et bloquer une tentative d'injection d'objet malveillant par le biais de l'une de ses routes.

Un message est remonté :

- le nombre total de ces tentatives que le démon a bloqué ce jour (*le compte commence à minuit*) ;
- pour chacune des tentatives (*maximum 3*) :
 - descriptif de l'objet que l'attaquant essaye de charger,
 - sa provenance de l'attaque, par exemple le nom de la route utilisée, et l'IP à la source de l'attaque,
 - sa date.

? Unknown Attachment