

# /recheck - ws-arbiter

Le module écoute des requêtes HTTP pour ensuite effectuer des actions sur les hôtes/clusters ou checks concernés.

Un simple curl ou appel HTTP dans votre programme suffit pour envoyer des actions à Shinken.

## Forcer la vérification d'un résultat sur un hôte ou un check

Paramètres de l'appel

Nom	Description
Méthode HTTP utilisé	POST
time_stamp	(optionnel) Date à laquelle a eu lieu la mesure afin que Shinken puisse déterminer la date de la "Dernière Vérification". Par défaut, la date d'appel de l'API sera utilisée.
host_name	Nom de l'hôte cible
service_description	Nom du check cible ( si résultat est celui d'un check )

Exemple:

```
curl -u user:password -X POST -d "time_stamp=$(date +%s)&host_name=host-checked&service_description=service-checked" http://shinken-srv:7760/recheck
```

## Exemples

L'exemple suivant permet de forcer la vérification d'un résultat d'un hôte :

```
curl -u user:password -X POST -d '$host_name=host-checked' http://shinken-srv:7760/recheck
```

L'exemple suivant permet de forcer la vérification d'un résultat de check :

```
curl -u user:password -X POST -d '$host_name=host-checked&service_description=service-checked' http://shinken-srv:7760/recheck
```



On note dans l'exemple précédent que la chaîne de caractères passée dans le curl pour les données POST est passée avec :

```
'$chaîne'
```

et non

```
"chaîne"
```

pour ordonner au check d'interpréter les caractères d'échappement ANSI et passer un véritable '\n' au lieu de '\ suivi de 'n'.

Cette astuce fonctionne si le shell utilisé est bash et peut ne pas être utilisable dans d'autres shells, ou si la requête est envoyée via un autre outil ou via un script dans un autre langage.