Faire une liaison entre un Shinken Central et un Shinken Deporté

Contexte

Il peut arriver qu'un réseau sécurisé soit complètement isolé du réseau central et que vous ayez besoin de distribuer les alertes des équipements et services supervisés de ce réseau isolé, vers le réseau central.

Nous vous conseillons alors de mettre en place une installation Shinken Entreprise sur ce réseau isolé (dont la politique de supervision est définie par les administrateurs de ce réseau) et de la faire dialoguer avec votre installation Shinken Entreprise Central.

Le concept est que l'installation déportée va pousser ses résultats vers l'installation centrale.

- Le flux réseau ne sera donc ouvert que dans le sens Déporté vers Central.
- Les installations dans des zones sécurisées n'auront donc pas de connexion entrante.

La solution proposée permettra de remonter n'importe quel résultat de checks ou d'hôtes vers l'installation centrale.

- Il s'agit cependant d'un contournement et une utilisation généralisée sur tous les éléments supervisés sera fastidieux.
- Nous vous conseillons de faire des clusters et de remonter seulement les informations des clusters pour avoir une vue agrégée en central.

Prenons par exemple la surveillance de l'hôte H1 dans l'infrastructure Shinken du réseau isolé:

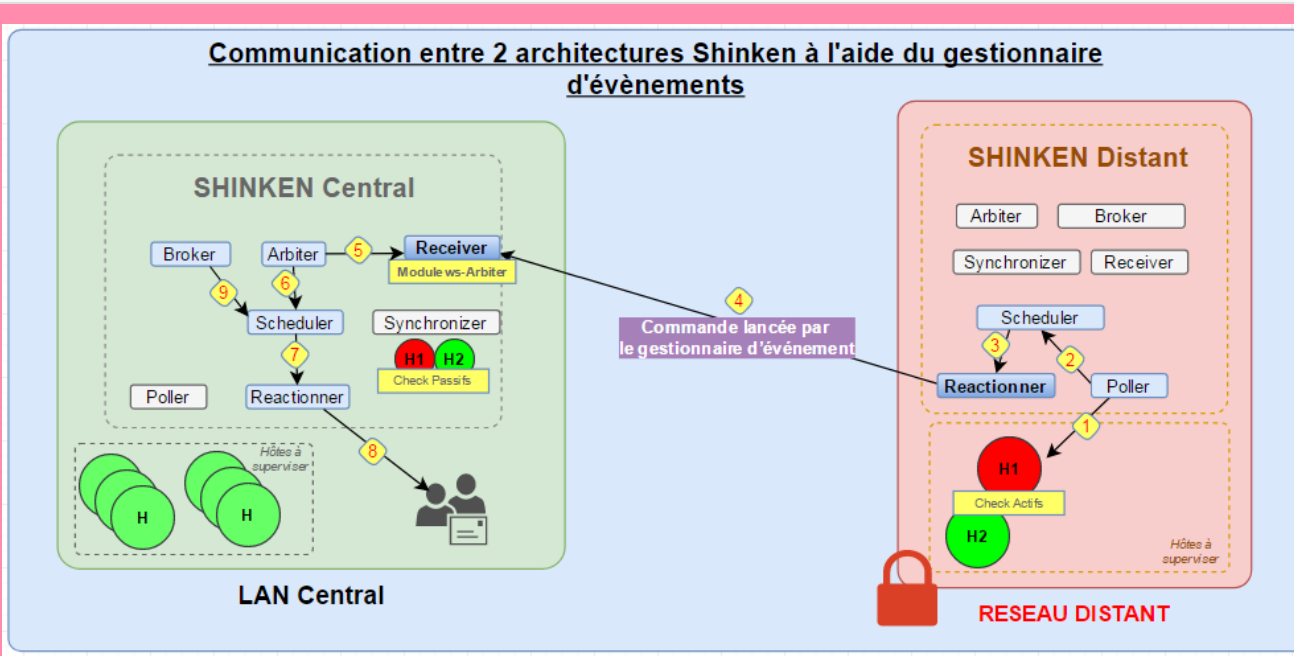
L'objectif est d'obtenir sur l'architecture centrale Shinken la réplique de H1 (avec un objet qui a exactement le même nom, et qui est en mode passif), et que son état en central soit un miroir des états réels déterminés depuis les Pollers/Scheduler du réseau isolé.

- Le dialogue se fera via le mécanisme du **Gestionnaire d'événements** qui, si paramétré sur l'hôte ou le check, enverra une commande définie sur cet hôte ou ce check.
- Ces commandes seront alors récupérées par le module ws-arbiter du daemon Receiver en central, et permettront le changement de l'état de l'hôte ou du check concerné.
- Il faudra définir de chaque coté un élément avec le même nom (hôtes ou couple hôte/check) pour que la remontée d'information ait bien lieu.

Sommaire

Architecture

Architecture Shinken Central / Distant



1. Le Poller de l'infra Shinken du Bunker supervise les Hôtes H1 et H2. Le Roller récupère l'état CRITIQUE pour l'hôte H1.
2. Le Poller envoie le résultat (Statut CRITIQUE) au Scheduler.
3. Le Reactionner récupère l'information auprès du Scheduler afin de procéder à l'envoi des notifications et de la commande déclenchée par le gestionnaire d'évènements
4. Le Reactionner envoie la commande en question. La ligne de commande fait passer, en direction de l'IP du Receiver de l'infrastructure Shinken Centrale (en HTTP ou HTTPS), l'état de l'hôte H1, Hôte qui est aussi définie dans cette infra centrale.
5. Via le module WS-Arbiter du Receiver, l'Arbiter récupère l'information.
6. Le Scheduler récupère la nouvelle information
7. La récupération de la notification est faite par le Reactionner
8. Envoi de la notification aux utilisateurs
9. Le nouvel état est récupéré par le Broker (pour l'UI de visualisation)

Installation - Les étapes de mise en place

Pour cet exemple, basé sur le schéma ci dessus, la supervision de l'hôte H1 du réseau isolé doit envoyer l'information en central, sur le même nom de d'hôte H1 (miroir).

Mise en place de l'architecture Shinken sur le réseau isolé

- Installez Shinken Entrprise
- Mettez en place la surveillance de l'hôte H1 avec une commande de supervision, par exemple la commande check-host-alive
- Créez la commande qui enverra l'information au Receiver du réseau Shinken central, depuis l'interface de configuration - page des commandes :

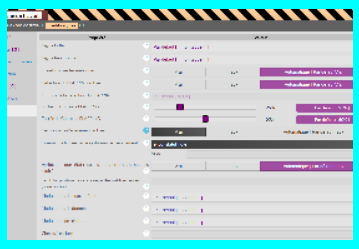
Dans notre exemple, pour un objet hôte, créons par exemple la commande (dans l'interface de configuration) ayant le nom "envoi-statut-hote" et avec la ligne de commande :

```
curl -d "host_name=$HOSTNAME$&return_code=$SERVICESTATEID$" --data-urlencode "output=Statut de l hote recupere" http://IP-RECEIVER-CENTRAL:7760/push_check_result
```

Si on doit effectuer l'envoi du statut d'un check, voici l'exemple de la commande ayant le nom "envoi-statut-check" et avec la ligne de commande :

```
curl -d "host_name=$HOSTNAME$&service_description=$SERVICEDESC$&return_code=$SERVICESTATEID$" --data-urlencode "output=Statut du check recupere" http://IP-RECEIVER-CENTRAL:7760/push_check_result
```

- sur H1: depuis l'interface de configuration, dans l'onglet Expert, activez le Gestionnaire d'événement (ou via un cfg passez la propriété event_handler_enabled à 1)
- et sélectionnez la commande "envoi-statut-hote" pour la Commande lancée par le gestionnaire d'événement (ou via cfg, définie avec la propriété event_handler)

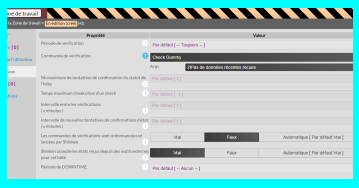


Paramétrage sur le réseau Central

- Configuration
  - Paramétrez votre module ws-arbiter
  - pensez bien à l'appeler depuis la définition de votre Receiver dans la propriété module.
  - Redémarrez Shinken pour la prise en compte du module.

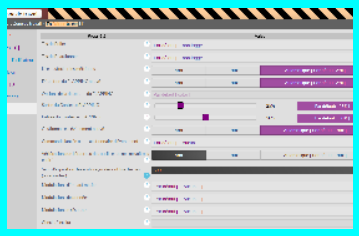
- Créez l'hôte H1 (attention, le nom doit être exactement le même que celui défini dans l'architecture Shinken du réseau isolé)

- Passez H1 en mode Passif :
  - depuis l'interface de configuration, onglet Supervision,
    - via la propriété "Les commandes de vérifications sont ordonnancées et lancées par Shinken" à mettre à **FAUX**
    - et la propriété "Shinken accepte les états reçus depuis des outils externes pour cet hôte" à **VRAI**
  - ou via un fichier de définition CFG (**utilisation d'une source d'import**) :
    - active_checks_enabled 0
    - passive_checks_enabled 1



- Pour génèrer un retour CRITIQUE dans le cas ou l'hôte ne reçoit pas d'information externe, nous vous conseillons de définir la commande de supervision de H1 par la commande "Check Dummy" avec par exemple en argument : 2!Pas de données récentes recues
  Pour un check, vous pouvez renvoyer un état UNKNOWN avec comme arguments : 3!Pas de données récentes recues

- Pour que cette commande soit exécutée, dans l'onglet expert de H1, passez la propriété "Vérification que l'état reçu des outils externes ne soit pas expiré" à **VRAI** et passez la propriété "Seuil d'expiration des états reçus des outils externes (x secondes)" à **300** (ou via CFG : check_freshness 1 et freshness_threshold 300)



Et voila, à chaque changement d'états de l'hôte H1 du réseau isolé, la commande "envoi-statut-hote" sera lancée, et mettra à jour l'hôte de même nom sur le réseau central.

Troubleshoot

Commande manuelle

Pour tester le bon fonctionnement du module ws-arbiter, vous pouvez exécuter simplement cette commande depuis un terminal :

```
curl -d "host_name=mon_hote&return_code=0" --data-urlencode "output=Statut OK" http://IP-DU-RECEIVER:7760/push_check_result
```

Vérifiez alors que l'état de votre hôte depuis l'interface de visualisation de votre réseau Shinken Central a bien été modifié.

Réseau

Au minimum, pour faire communiquer les deux infrastructures, il faut autoriser une communication entre l'IP hébergeant le daemon Reactionner (por 7769) qui enverra les commandes d'Event Handler, et l'IP hébergeant le daemon Receiver (port 7773) à l'écoute des commandes.