Résolution de problèmes courants (Architecture)

Sommaire

Introduction

La visualisation de l'architecture fait interagir plusieurs composants: Arbiter, Synchronizer et NagVis (installation externe).

Selon la complexité de l'architecture Shinken, il est possible que la configuration automatique effectuée par l'installation/mise à jour de Shinken Entreprise ne puisse pas configurer complètement l'addon, et donc que la visualisation des cartes fonctionne correctement.

Les sections suivantes présentent les problèmes courants pouvant être rencontrés et leur résolution.

Les hôtes générés ne sont pas visibles dans l'interface de Configuration

Lorsque l'addon "nagvis-shinken-architecture" génère la visualisation de l'architecture, des hôtes sont également créés ou modifiés dans l'interface de Configuration.

Ces hôtes sont donc visibles en tant que Nouveaux ou en tant que Différences sur des hôtes Shinken existants. Les données de ces hôtes sont importées par la source listener-shinken.

Si dans cette source, les données des hôtes sont effacées (*grâce au balai*), les éléments en Nouveau et Différence ne sont plus présents dans l'interface de Configuration. On peut obtenir le même problème si les hôtes n'ont pas pu être envoyés à l'interface de Configuration à cause d'une erreur réseau par exemple.

Il faut alors déclencher un nouvel export de l'architecture pour que les informations des hôtes utilisés soient à nouveau disponibles dans l'interface de Configuration. Pour cela, il faut s'assurer que l'addon "nagvis-shinken-architecture" soit activé (*Voir la page* Activation - désactivation des outils supplémentaires (addons)), puis redémarrer l'Arbiter ou envoyer la commande de génération de la carte.

```
# redémarrage de l'arbiter
$ /etc/init.d/shinken arbiter restart
# commande de génération de la carte
$ curl -v -X POST http://localhost:7780/v1/architecture/send
```

Restrictions sur le nom de l'architecture

Lors de la configuration du module 'architecture-export', il est possible de modifier le nom de l'architecture.

Puisque le nom de l'architecture est également présent dans le nom des hôtes générés dans l'interface de Configuration, tous les caractères ne sont pas autorisés dans le nom de l'architecture.

Les restrictions de caractères sont les mêmes que pour les noms d'hôtes, à savoir:

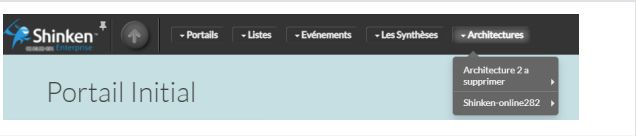
- Les caractères suivants sont interdits dans un nom d'architecture :

```
~!$%^&"'|<>?,()=/+
```

Si ces caractères sont présents dans le nom de l'architecture, l'addon "nagvis-shinken-architecture" ne sera pas capable de générer les hôtes nécessaires et le statut des démons ne pourra jamais être affiché dans les cartes représentatives de l'architecture.

Supprimer des architectures générées

Il peut arriver que certaines architectures générées par l'addon doivent être supprimées. C'est par exemple le cas lorsqu'une architecture de test a été générée, ou alors l'architecture d'une installation Shinken qui n'existe plus.



Il faut alors supprimer ces entrées pour qu'elles n'apparaissent plus dans NagVis, dans la liste des architectures visibles dans l'interface de Visualisation, ainsi que dans la liste des hôtes générés dans l'écouteur "*listener-shinken*" de l'interface de Configuration.

La commande **shinken-architecture-export-delete** permet de supprimer une architecture en effectuant les opérations décrites précédemment de manière automatisée.

Paramètres de la commande

Les paramètres de cette commande sont les suivants:

```
$ shinken-architecture-export-delete -h
Usage: shinken-architecture-export-delete

Removes the specified generated architecture (maps and links in the Visualisation UI)

Options:
  -h, --help            show this help message and exit
  -n NAME, --name=NAME  Name of the architecture to delete
  --id=ID               Architecture ID to delete
  -l, --list            List generated architectures
  -f, --force           Do not ask confirmation before shutting down the
                        Arbiter
```

⚠ Cette commande doit être obligatoirement exécutée sur une machine sur laquelle un Arbiter est actif.

Lors de l'exécution de la commande, l'Arbiter est éteint automatiquement (*après avoir demandé une confirmation*). L'Arbiter devra être redémarré manuellement une fois la commande exécutée.

Suppression d'une architecture via son nom

Cette commande s'utilise en lui donnant le nom de l'architecture à supprimer:

```
shinken-architecture-export-delete --name "Architecture 2 a supprimer"
```

Suppression d'une architecture via son ID

Lorsque plusieurs architectures ont le même nom, il est possible de cibler l'architecture à supprimer directement via son identifiant.

Cet identifiant peut être récupéré avec la commande et l'option --list:

```
$ shinken-architecture-export-delete --list
* Name    : Shinken-supdesup1
  ID      : sk-44fe74a81bd3269350a20f6a40b3a408-f9c0dab9-fe3f-4c3f-9124-a14bc8f685a4

* Name    : Shinken-master1
  ID      : sk-11c66503cd9405c904812422f781f6cf-1575faa3-863d-477e-9abc-29327e06a7fb
```

L'architecture voulue peut alors être supprimée avec la commande suivante:

```
shinken-architecture-export-delete --id "sk-11c66503cd9405c904812422f781f6cf-1575faa3-863d-477e-9abc-
29327e06a7fb"
```

Impossibilité de se connecter à NagVis

Le Broker et l'interface de Visualisation à utiliser pour l'authentification sont mal configurés

Pour autoriser l'authentification avec un utilisateur Shinken, NagVis communique avec l'interface de Visualisation.

Si la liaison avec l'interface de Visualisation n'est pas correcte ou possible, il sera impossible de se connecter dans NagVis.

Par défaut, l'authentification à NagVis est configurée pour être rattachée à celle de la WebUI du Broker présent sur la même machine que l'Arbiter à l'installation. L'adresse par défaut est alors 127.0.0.1, le port est lui configuré à 7767 (*port par défaut de la WebUI*) et le protocole utilisé est HTTP (*celui paramétré par défaut sur la WebUI*).

Si les paramètres de l'interface de Visualisation ont été modifiés, il faut indiquer à NagVis les paramètres à utiliser pour la contacter.

Les paramètres à modifier sont les suivants :

/etc/shinken/external/nagvis/etc/nagvis.ini.php

```
; Protocol to use when authenticating with Shinken (http or https) when using the CoreAuthModShinken
authentication module
shinken_auth_protocol="https"
; Port of broker webui
shinken_auth_port=1234
; Address of broker webui. If not specified, address of default backend is used instead
shinken_auth_address="10.1.2.3"
; Enable verification of SSL cerificate issued by WebUI
;shinken__authentication__ssl__verify_certificate  = 0
; Enable verification of peer name in SSL certificate issued by WebUI
;shinken__authentication__ssl__verify_certificate_name = 1
; Allow WebUI to issue a self signed certificate
;shinken__authentication__ssl__allow_self_signed_certificate = 1
; Set location of certificate authority on local filesystem ( cf. https://www.php.net/manual/en/context.ssl.
php#context.ssl.cafile )
; - system defaults to "/etc/ssl/certs/ca-bundle.trust.crt"
; - you can use "/etc/shinken/certs/ca.pem" if you generated a self signed certificate four your Shinken
installation
;shinken__authentication__ssl__certificate_authority_file = ""
```

Ces paramètres sont modifiables graphiquement dans l'interface de NagVis ou bien dans le fichier de configuration de NagVis (*/etc/shinken/external /nagvis/etc/nagvis.ini.php*).

Par défaut, NagVis contacte le Broker en HTTP. Si l'interface de Visualisation est configurée en HTTPS, il faudra modifier le paramètre "shinken_auth_protocol".

Si la vérification du certificat **SSL** de la WebUI a été **activé**, **vérifier** dans un premier temps que **l'erreur n'est pas liée à la négociation SSL** lors de l'établissement de la connexion **https** :

1. Repasser le paramètre **shinken__authentication__ssl__verify_certificate** à 0 pour désactiver la vérification du certificat SSL
    a. Si l'identification ne fonctionne pas, l'erreur n'est pas liée à SSL, régler le problème en explorant les pistes indiquées dans les chapitres suivants.
2. si l'identification fonctionne, il s'agit d'un problème lors de la négociation SSL. Réactiver la vérification du certificat en mettant 1 pour la valeur du paramètre **shinken__authentication__ssl__verify_certificate** :
    a. Si le certificat est auto-signé, activer l'option **shinken__authentication__ssl__allow_self_signed_certificate** en lui affectant la valeur 1.
    b. Si le certificat n'a pas été émis pour le serveur hébergeant la WebUI (*dans le champ **CN***) et que l'on souhaite tout de même l'utiliser, désactiver l'option **shinken__authentication__ssl__verify_certificate_name** en lui affectant la valeur 0.
    c. Pour ajouter le certificat dans la chaine de confiance du protocole SSL, on a deux options :
        i. L'ajouter à la chaine de confiance du système avec les commandes suivantes

```
cp your_certificate.crt /etc/pki/ca-trust/source/anchors/
update-ca-trust
```

        ii. Ou, préciser le certificat définissant la chaine d'autorité de NagVis via le paramètre **shinken__authentication__ssl__certificate_authority_file**, en lui affectant la valeur "/etc/shinken/certs/ca.pem" par exemple

(*Vous trouverez d'autres d'informations dans la page* Les certificats SSL)

Sous CentOS 7 (*ayant une version de PHP < 7*), la vérification du nom du certificat (*paramètre shinken__authentication__ssl__verify_certificate_name*) ne fonctionne pas quand ce certificat est dans la chaine de confiance (*paramètre shinken__authentication__ssl__certificate_authority_file*).

Vous pouvez mettre votre version de PHP à jour en version 7.2 si vous avez besoin de cette fonctionnalité

Le Broker et/ou l'interface de Visualisation ne sont pas joignables

Si les paramètres de connexion à l'interface de Visualisation sont corrects, il est alors possible que cette interface ne soit pas joignable. Il peut s'agir d'un problème réseau (*routage, firewall*), ou bien simplement que le Broker n'est pas opérationnel.

Le statut du Broker et de l'interface de Visualisation peut être vérifié avec le Shinken-healthcheck (*Voir la page Shinken-healthcheck - Vérifier le bon fonctionnement de Shinken Entreprise*).

L'utilisateur qui demande la connexion n'est pas un administrateur Shinken

Par défaut, la connexion des utilisateurs non administrateurs Shinken est refusée. Pour autoriser les utilisateurs autres que les administrateurs Shinken à se connecter à NagVis, il faut modifier le paramètre " *shinken_auth_restrict_to_shinken_admin*":

/etc/shinken/external/nagvis/etc/nagvis.ini.php

```
; Authorize authentication into NagVis to Shinken administrators only
shinken_auth_restrict_to_shinken_admin=0
```

Dans le cas de l'authentification par en-tête HTTP, la configuration de l'authentification SSO ne correspond pas entre NagVis et Shinken.

Lorsque l'Synchronizer - Authentification unique (SSO) est utilisée dans Shinken, il est possible de tirer avantage de cette fonctionnalité afin de l'appliquer également à NagVis. Si cette authentification par en-tête HTTP ne fonctionne pas dans NagVis pour connecter l'utilisateur automatiquement, il faut d'abord vérifier que ce mécanisme est bien configuré dans NagVis ET dans Shinken. Les points suivants sont à contrôler pour assurer l'authentification par SSO dans NagVis en liaison avec Shinken:

- Lorsque NagVis reçoit une requête avec en-tête HTTP, il vérifie auprès de Shinken si l'utilisateur fourni dans cet en-tête est un utilisateur existant. **Il est donc nécessaire que l'interface de Visualisation à contacter soit joignable et correctement configurée dans NagVis** (voir sections précédentes)
- **Dans Shinken, il faut que l'authentification SSO soit activée dans le Broker** (*Voir la page* Synchronizer - Authentification unique (SSO)).
- **Dans NagVis, il faut que l'en-tête utilisé soit le même que celui défini dans Shinken pour le Broker**.
  Pour utiliser l'authentification par en-tête HTTP dans NagVis, il faut définir le nom de l'en-tête à utiliser:

  /etc/shinken/external/nagvis/etc/nagvis.ini.php

  ```
  ; This value must be the same as the one configured in Shinken. An empty value means authentication
  by http header is disabled.
  shinken_auth_remote_user_variable="X-Forwarded-User"
  ```

Il faut que le paramètre "*shinken_auth_remote_user_variable*" de NagVis soit le même que le paramètre "*remote_user_variable*" du module webui dans Shinken.

L'authentification automatique entre Shinken et NagVis ne fonctionne pas

Avec la configuration effectuée par l'installeur Shinken Entreprise, on est automatiquement connecté dans NagVis lorsqu'on est connecté sur l'interface de Visualisation.

Pour authentifier automatiquement l'utilisateur, NagVis vérifie auprès de l'interface de Visualisation s'il est connecté. Si c'est le cas, l'utilisateur sera automatiquement connecté dans NagVis.

Il se peut que cette authentification automatique ne fonctionne pas si NagVis n'arrive pas à obtenir les informations de connexion à l'interface de Visualisation. C'est le cas lorsque NagVis et l'interface de visualisation ne sont pas sur le même domaine.

Par exemple, l'adresse de l'Arbiter est une adresse IP, alors que l'interface de Visualisation est accédée via le nom DNS de cette adresse (*exemple 127.0.0.1 et localhost*).

Pour que l'authentification à l'interface de Visualisation soit partagée entre NagVis et Shinken, il faut que l'adresse d'accès soit identique entre l'interface de Visualisation et NagVis.

Dates incorrectes sur Nagvis

Si vous avez un décalage de temps entre votre serveur Shinken et les dates affichées dans Nagvis, éditez votre fichier php.ini pour configurer votre Timezone :

```
date.timezone = Europe/Paris
```

Puis redémarrez le serveur Web :

```
systemctl restart httpd
```

La page de NagVis est inaccessible

Il se peut que la page des cartes reste blanche ou seulement le caractère "1" soit affiché. Ce problème peut survenir lorsque le cache de l'application NagVis est dans un état instable (*arrêt de la machine ou du service httpd pendant la régénération du cache*).

Pour corriger ce problème, il suffit de supprimer le cache des fichiers compilé.

```
$ rm -fr /etc/shinken/external/nagvis/var/tmpl/compile/*
```

Retourner ensuite sur la page. L'application régénérera le cache correctement.

Ce bug a été corrigé dans la version 02.08.02

Les statuts des objets Shinken sont tous en N/A

Il se peut que la communication entre Nagvis et Shinken ne soit plus correcte suite à un changement de nom du module Livestatus et de son port, ou à un changement de Broker.

Pour corriger ce problème, veuillez vérifier votre configuration de la communication entre Nagvis et Shinken (*Voir la page* Configuration de la Visualisation de l'architecture).

La redirection vers la WebUI ne fonctionne pas

Il est possible qu'en cliquant sur un objet Shinken sur une carte nagvis, la redirection vous envoie au mauvais endroit, ceci peut arriver suite à un changement de nom du Module WebUI et de son port, ou à un changement de Broker.

Pour corriger ce problème, veuillez vérifier votre configuration de la communication entre Nagvis et Shinken (*Voir la page* Configuration de la Visualisation de l'architecture).