Résolution de problèmes courants NagVis

Sommaire

Impossible 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, il n'est pas possible de se connecter dans NagVis.

L'interface de Visualisation utilisée pour l'authentification est par défaut le backend Livestatus configuré dans NagVis, initialement défini comme le Broker présent sur la machine de l'Arbiter (*127.0.0.1*). Le port utilisé ainsi que le protocole sont également ceux par défaut (*respectivement 7767 et http*).

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:

/opt/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 (*/opt/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'agit 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*":

/opt/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'authentification unique est utilisée dans Shinken (*voir la page* Synchronizer - Authentification unique (SSO)), 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:

  /opt/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.

```
# Pour les cartes générées par l'architecture export :
$ rm -fr /etc/shinken/external/nagvis/var/tmpl/compile/*
# Pour vos cartes personnelles
$ rm -fr /opt/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 utilisateurs ne peuvent pas gérer les cartes

Par défaut, seuls les utilisateurs appartenant au groupe "**admins**" de shinken possède les droits de modifications sur les cartes.

Ce comportement est défini dans le fichier : **/opt/nagvis/etc/perms.db**

```
{
  "admins": {
    "admin": 1
  },
  "it_admins": {
    "view": [ "*" ],
    "edit": [ "*" ]
  },
  "users": {
    "view": [ "*" ]
  },
  "users_site1": {
    "view": [ "site1" ],
```

```
    "edit": [ "site1" ]
  }
}
```

les groupes sont répartis comme suivant:

- Les utilisateurs du groupe "*admins*" ont les droits administrateur dans NagVis
- Les utilisateurs du groupe "*it_admins*" ont accès en lecture et écriture sur toutes les cartes
- Les utilisateurs du groupe "*users*" ont accès en lecture seule à toutes les cartes
- Les utilisateurs du groupe "*users_site1*" ont accès en lecture et écriture seulement sur les cartes "*site1*" et "*site1_bis*"

Il est possible de modifier le fichier pour ajouter un nouveau groupe de droits, si vous ne souhaitez pas utiliser le groupe admins sur des utilisateurs standards.