# Paramétrage de l'interface de Visualisation

## Problématiques rencontrées avec l'authentification NagVis

Lorsqu'un utilisateur utilise une instance de NagVis, il utilise des identifiants propres à cette installation de NagVis. Il est possible de gérer les utilisateurs et leur droits directement dans NagVis.

Lorsque NagVis est installé pour être utilisé de manière transparente avec Shinken Entreprise, cette fonctionnalité devient un problème puisqu'il devient nécessaire de synchroniser les bases d'utilisateurs de Shinken et de NagVis. Dans Shinken, une base d'utilisateurs est déjà présente

Pour simplifier la gestion de l'authentification entre NagVis et Shinken, plusieurs modules ont été ajoutés dans NagVis.

## Fonctionnement de l'authentification de NagVis

Dans une installation NagVis classique, la gestion des utilisateurs est gérée avec 3 types de modules différentes:

- **Un module de login**
  Définit la manière avec laquelle l'utilisateur fournit ses identifiants de connexion. Selon les modules, les identifiants peuvent être passés par un formulaire ou par variable d'environnement.
- **Une module d'authentification**
  Utilise les identifiants de connexion fournis par le module de login et vérifie si ces identifiants sont corrects. Le module d'authentification par défaut vérifie les identifiants de connexion dans la base d'utilisateur propre à NagVis.
- **Un module d'autorisation**
  Utilise les données de l'utilisateur (son profil et ses réglages) pour lui attribuer les droits nécessaires (droits d'administration de NagVis, droits et vue et d'édition des cartes, etc...)

? Unknown Attachment

Les modules par défaut dans l'installation NagVis utilisée pour l'export de l'architecture sont les suivants:

- **Module de login**: LogonShinkenMixed
  Récupère les informations de connexion via des entêtes HTTP. Si aucun entête d'authentification n'est passé, les identifiants de connexion sont récupérés depuis le cookie des interfaces Web Shinken. Sinon, un formulaire de connexion classique est utilisé.
- **Module d'authentification**: CoreAuthModShinken
  Vérifie la validité des identifiants de connexion avec les informations stockées dans la base d'utilisateurs de Shinken.
- **Module d'autorisation**: CoreAuthorisationModShinken
  Définit des droits par défaut (non modifiables).

Le fonctionnement de ces modules est décrit de manière détaillée dans les sections suivantes.

Pour plus d'informations sur les modules disponibles par défaut, la documentation NagVis présente un récapitulatif des fonctionnalités disponibles:

- http://docs.nagvis.org/1.9/en_US/index.html

# Solutions d'authentification mises en place

Pour permettre une gestion de l'authentification transparente entre Shinken et NagVis, plusieurs modules ont été ajoutés.

## Configuration générale

Pour permettre la liaison de l'authentification avec Shinken, les différents modules utilisés pour la connexion ont besoin de savoir quelle est l'adresse de l'installation Shinken avec laquelle il lui faut se connecter.

De manière plus précise, pour se connecter avec Shinken, NagVis utilise le module WebUI (l'interface de visualisation).

Plusieurs paramètres sont ajoutés pour spécifier l'installation Shinken à contacter:

| Paramètre | Valeur par défaut | Description |
|---|---|---|
| shinken_auth_protocol | http | Protocole à utiliser pour la connexion à Shinken (http ou https) |
| shinken_auth_port | 7767 | Port du module webui à contacter |
| shinken_auth_address | *Vide* | Adresse du module webui à contacter |
| shinken_auth_restrict_to_shinken_admin | Oui | Restreint la connexion aux utilisateurs définis comme Administrateurs Shinken dans Shinken |

## Modules de login

### Utilisation d'entêtes HTTP

**Nom du module**: CoreLogonShinkenHeader

### Utilisation des cookies des interfaces Web Shinken

### Formulaire de connexion

### Aggrégation des modules précédents

## Modules d'authentification

### Authentification avec Shinken Entreprise

## Modules d'autorisation

### Définition des droits selon le profil Shinken

### Définition des droits selon les groupes d'utilisateurs