

# Gestion de l'authentification

## 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.
- **Un 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...)

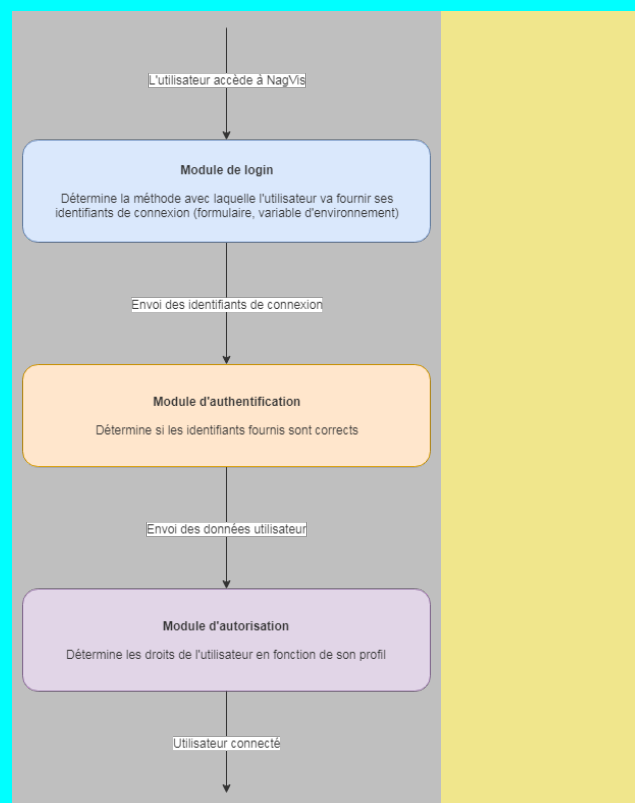
Les modules par défaut dans l'installation NagVis utilisée pour l'export de l'architecture sont les suivants:

- **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](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 de l'interface de Visualisation Shinken à contacter
shinken_auth_address	Vide	Adresse du module webui à contacter (exemple: 192.168.0.3). Lorsque ce champ est vide, l'adresse du backend par défaut configuré dans NagVis est utilisée. Dans la majorité des cas, il ne sera pas nécessaire de spécifier une adresse particulière.
shinken_auth_restrict_to_shinken_admin	Oui	Restreint la connexion aux utilisateurs définis comme Administrateurs Shinken dans Shinken

Ces paramètres peuvent être modifiés de 2 manières différentes:

#### ■ Par le fichier de configuration de NagVis:

`/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="http"
; Port of broker webui
;shinken_auth_port=7767
; Address of broker webui. If not specified, address of default backend is used instead
;shinken_auth_address=""
; Name of the HTTP header to use to perform SSO authentication with Shinken.
; 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=""
; Authorize authentication into NagVis to Shinken administrators only
;shinken_auth_restrict_to_shinken_admin=1
```

#### ■ Par l'interface Web de NagVis (Options > Configuration générale).

Le lien vers l'interface Web de NagVis est présent dans l'interface de visualisation (menu "Architectures"), ou directement à l'adresse suivante:

- <http://IP-ARBITER/shinken-core-map/>

## Configuration Générale

Global Settings	Object Defaults	Paths	Automap	Overview	State Updates	States
audit_log	<input type="checkbox"/>	No				
authmodule	<input checked="" type="checkbox"/>	CoreAuthModShinken				
authorisationmodule	<input checked="" type="checkbox"/>	CoreAuthorisationModShinken				
dateformat	<input type="checkbox"/>	Y-m-d H:i:s				
dialog_ack_sticky	<input type="checkbox"/>	Yes				
dialog_ack_notify	<input type="checkbox"/>	Yes				
dialog_ack_persist	<input type="checkbox"/>	No				
file_group	<input checked="" type="checkbox"/>	apache				
file_mode	<input type="checkbox"/>	660				
geomap_server	<input type="checkbox"/>	http://geomap.nagvis.org/				
http_proxy	<input type="checkbox"/>					
http_proxy_auth	<input type="checkbox"/>					
http_timeout	<input type="checkbox"/>	2				
language_detection	<input type="checkbox"/>	user,session,browser,config				
language_available	<input type="checkbox"/>	de_DE,en_US,es_ES,fr_FR,pt_BR,zh_CN				
language	<input type="checkbox"/>	en_US				
logonmodule	<input checked="" type="checkbox"/>	LogonShinkenMixed				
multisite_snapin_layout	<input type="checkbox"/>	list				
only_permitted_objects	<input type="checkbox"/>	No				
user_filtering	<input type="checkbox"/>	No				
refreshtime	<input type="checkbox"/>	60				
sesscookiedomain	<input type="checkbox"/>					
sesscookiepath	<input checked="" type="checkbox"/>	/shinken-core-map				
sesscookieexpiration	<input type="checkbox"/>	86400				
sesscookiesecure	<input type="checkbox"/>	No				
sesscookiehttponly	<input type="checkbox"/>	No				
shinken_features	<input checked="" type="checkbox"/>	Oui				
staleness_threshold	<input type="checkbox"/>	1.5				
startmodule	<input type="checkbox"/>	Overview				
startaction	<input type="checkbox"/>	view				
startshow	<input type="checkbox"/>					
worldmap_start_pos	<input type="checkbox"/>	51.505,-0.09				
worldmap_start_zoom	<input type="checkbox"/>	13				
shinken_auth_protocol	<input type="checkbox"/>	http				
shinken_auth_port	<input type="checkbox"/>	7767				
shinken_auth_address	<input type="checkbox"/>					
shinken_auth_remote_user_variable	<input type="checkbox"/>					
shinken_auth_restrict_to_shinken_admin	<input checked="" type="checkbox"/>	Oui				

26-a986-c533f841391c#

Sauvegarder

## Modules de login

### Utilisation d'entêtes HTTP

**Nom du module:** CoreLogonShinkenHeader

Lorsque la connexion par SSO est activée dans Shinken (**Authentification unique (SSO)**), il est alors possible d'utiliser cette fonctionnalité pour se connecter dans NagVis en utilisant les mêmes entêtes HTTP que ceux utilisés pour Shinken.

L'entête utilisé dans NagVis doit être le même que celui utilisé dans l'interface de Visualisation de Shinken. Pour utiliser l'authentification par SSO dans NagVis avec le module fourni par Shinken, l'authentification par entête HTTP doit également être activée dans Shinken sur l'UI de Visualisation

Le nom de l'entête contenant le nom d'utilisateur doit être spécifié dans NagVis avec le paramètre "*shinken\_auth\_remote\_user\_variable*".

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

```
; Name of the HTTP header to use to perform SSO authentication with Shinken.  
; 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=""
```

Lorsque cette variable est vide, l'authentification par entête HTTP est désactivée. Par défaut, l'utilisation des entêtes HTTP est donc désactivée dans NagVis.

### Utilisation des cookies des interfaces Web Shinken

**Nom du module:** CoreLogonShinkenCookie

Ce module utilise les cookies des interfaces Web de Shinken Entreprise. Lorsque l'utilisateur est connecté dans une interface (interface de Configuration ou interface de Visualisation), il sera donc automatiquement connecté dans NagVis. La connexion peut être restreinte aux administrateurs Shinken grâce au paramètre "*shinken\_auth\_restrict\_to\_shinken\_admin*".



Cette solution ne sera fonctionnelle que si NagVis est installé sur une machine qui héberge également au moins une interface Shinken (Configuration ou Visualisation). En d'autres mots, cette solution ne sera fonctionnelle que si le Synchronizer ou un Broker avec le module "webui" sont présents sur la même machine que le démon Arbitre.

## Formulaire de connexion

**Nom du module:** CoreLogonDialog

Ce module est le module par défaut de connexion NagVis. Il affiche un formulaire qui demande à l'utilisateur d'entrer son nom d'utilisateur et son mot de passe pour se connecter dans NagVis.

Lorsqu'il est utilisé avec le module d'authentification "*CoreAuthModShinken*", les identifiants entrés dans le formulaire seront vérifiés avec Shinken.

## Agrégation des modules précédents

**Nom du module:** CoreLogonShinkenMixed (*par défaut*)

Ce module rassemble les différents modes de connexion précédents en un seul module. Le fonctionnement du module est le suivant:

- Tentative de connexion en utilisant les entêtes HTTP
- Si l'authentification avec entête HTTP échoue (utilisateur invalide, entête HTTP non défini), le module tente de connecter l'utilisateur en utilisant le cookie des interfaces Web Shinken.
- Si l'authentification par cookie a échoué, le formulaire de connexion est présenté à l'utilisateur.

## Modules d'authentification

### Authentification avec Shinken Entreprise

**Nom du module:** CoreAuthModShinken (*par défaut*)

Ce module utilise les données de connexion fournies par le module de login et vérifie auprès de Shinken (en particulier l'interface de visualisation) si les identifiants correspondent bien à un utilisateur Shinken existant.

Le comportement de ce module est configurable avec les variables définies dans la section précédente sur la configuration générale des modules d'authentification.

## Modules d'autorisation

### Définition des droits selon le profil Shinken

**Nom du module:** CoreAuthorisationModShinken (*par défaut*)

Ce module définit des droits par défaut pour un utilisateur connecté avec Shinken. Ces droits, non configurables, sont les suivants:

- Visualisation en lecture seule de toutes les cartes définies

- Visualisation en lecture seule des rotations définies dans NagVis (plus d'information sur les rotations dans la documentation NagVis: [http://ocs.nagvis.org/1.9/en\\_US/nagvis\\_config\\_format\\_description.html#rotation](http://ocs.nagvis.org/1.9/en_US/nagvis_config_format_description.html#rotation))
- Modification autorisée de la configuration générale de NagVis

## Définition des droits selon les groupes d'utilisateurs

**Nom du module:** CoreAuthorisationModShinken

Ce module est très similaire au module "*CoreAuthorisationModGroups*" présent dans une installation NagVis classique. Il permet de définir des droits utilisateurs en fonction des groupes d'utilisateur Shinken dans lequel l'utilisateur est présent.

La configuration des droits se fait grâce au fichier `perms.db` présent par défaut dans `/etc/shinken/external/nagvis/etc/`.

Le chemin de ce fichier est configurable dans la configuration de NagVis avec le paramètre "`authorisation_group_perms_file`".

Dans l'exemple, les groupes sont répartis comme suivant:

- Les utilisateurs du groupe "`admins`" ont les droits administrateurs 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`"

`/etc/shinken/external/nagvis/etc/perms.db`

```
{
  "admins": {
    "admin": 1
  },
  "it_admins": {
    "view": [ "*" ],
    "edit": [ "*" ]
  },
  "users": {
    "view": [ "*" ]
  },
  "users_site1": {
    "view": [ "site1", "site1_bis" ],
    "edit": [ "site1", "site1_bis" ]
  }
}
```



La différence de ce module avec celui livré par défaut dans NagVis (*CoreAuthorisationModGroups*) se situe sur le paramètre "admin".

Dans ce module, "admin: 1" aura pour effet de donner tous les droits à l'utilisateur, sauf les droits des gestion des utilisateurs, puisque ceux ci sont gérés dans Shinken et non dans NagVis.