Configuration du Windows supervisé dans un Domaine (Active Directory) pour le pack windows-by-WinRM__shinken

Sommaire

Contexte

Ce guide vous permettra d'installer Shinken Entreprise sur un serveur Linux.

- Une fois le guide de mise à jour, vous aurez rapidement accès aux interfaces de Configuration et de Visualisation de Shinken dans une architecture par défaut, c'est-à-dire un seul serveur sur lequel tous les démons seront activés.
- La configuration de votre installation Shinken ne sera pas modifiée sur une mise à jour (*vos données dans les fichiers de configuration ne sont pas modifiées*).

Important

L'installation de Shinken Entreprise met en place deux bases de donnée :

- **MongoDB** (*version* ***v3.0.15*** **).** Cette base de données est utilisée par les interfaces de Configuration et de Visualisation et la sauvegarde de la rétention s'il y a plusieurs Scheduler dans un royaume.
  - Voir la page En base de données (MongoDB)
- **Graphite** (*version* ***1.1.8***). Cette base permet de stocker les métriques de vos sondes.
  - Voir la page Base de métrologie (Graphite)

Pour ne pas créer de dysfonctionnement, **nous vous demandons de ne pas mettre à jour MongoDB / Graphite.** Veuillez simplement laisser en place les versions fournies par nos services.

⚠️ Afin de prévenir tout risque, les démons Shinken Entreprise refuseront de démarrer si la version installée de **MongoDB** n'est pas celle préconisée.

⚠️ Si une version différente de **MongoDB** est déjà présente sur le serveur, l'installation sera interrompue

⚠️ Si vous faites une mise à jour de Shinken Entreprise depuis une version antérieure à la 2.6.1 et que la version de **MongoDB** installée n'est pas la 2.6.9, la mise à jour sera interrompue

Historique de l'installeur

Concernant l'installeur à utiliser, il faut prendre le dernier en date.

02.08.02

Voici l'historique des installeurs de cette version:

Nom de la version	Date de parution	Nom de l'installeur	Modification par rapport à la version précédente
RC018	**prochainement**		*Modification de l'installateur :* 1 - Le script de mise à jour de Shinken permet de renseigner les identifiants de connexion à MongoDB lorsque l'authentification par mot de passe est activée dans la base. *Liste des autres modifications :* *Voir la release note*
RC017.02 **...** **RC017**	**19 juin 2025** **...** **20 mai 2025**	shinken-enterprise_V02.08.02-RC017.02_FR_Linux_FULL_2025-06-16.tar.gz	*Modification de l'installateur :* 1 - Mise à jour du Python 3.11 (version 3.11.11) utilisé par Shinken avec les correctifs de sécurité de Python. *Liste des autres modifications :* *Voir la release note*
RC016.06 **...** **RC016**	**19 mai 2025** **...** **27 février 2025**	shinken-enterprise_V02.08.02-RC016.06_FR_Linux_FULL_2025-05-15.tar.gz	*Liste des autres modifications :* *Voir la release note*
RC015.19 **...** **RC015**	**23 juin 2025** **...** **12 Aout 2024**	shinken-enterprise_V02.08.02-RC015.12_FR_Linux_FULL_2025-01-16.tar.gz	*Modification de l'installateur :* 1 - Tous les démons fonctionnent avec Python 3.11.8. 2 - Désormais, l'installation de Shinken est compatible avec les versions RedHat/Alma 8.10. 3 - L'installation de Shinken est désormais possible sur les distributions RockyLinux 8.9 et 8.10. *Liste des autres modifications :* *Voir la release note*

RC014.05 **RC014.04** **RC014.03** **RC014.02** **RC014.01** **RC014**	**11 avril 2024**	shinken-enterprise_V02.08.02-RC014.05_FR_Linux_FULL_2024-04-05.tar.gz	*Modification de l'installateur :* 1 - Désormais, l'installation de Shinken est compatible avec les versions RedHat/Alma 8.9. 2 - Les démons Poller et Reactionner fonctionnent avec Python 3.11.8. 3 - Mise à jour du Python 2.7 (*version 2.7.18-15*) utilisé par les autres démons de Shinken avec les correctifs de sécurité de RedHat. 4 - Ajout de l'option --skip-nagvis. 5 - Suppression du support de RedHat / CentOS 6. *Liste des autres modifications :* *Voir la release note*
RC013	**04 octobre 2023**	shinken-enterprise_V02.08.02-RC013_US/FR_Linux_FULL_2023-10-03.tar.gz	*Voir la release note*
RC012.01 **RC012.02** **RC012.03**	**13 septembre 2023**	shinken-enterprise_V02.08.02-RC012.01_US/FR_Linux_FULL_2023-07-13.tar.gz	*Modification de l'installateur :* 1 - L'exclusion des "nagios-checks" et de leurs dépendances par les paramètres --packs-to-install / --packs-to-exclude est désormais fonctionnelle en RedHat7 / Centos7 (*elle était réservée à la RedHat8 / Alma8 auparavant*) *Liste des autres modifications :* *Voir la release note*
RC012	**06 juillet 2023**	shinken-enterprise_V02.08.02-RC012_US/FR_Linux_FULL_2023-07-05.tar.gz	*Modification de l'installateur :* 1 - Les dossiers /var/lib/shinken-nagvis et /opt/nagvis/ dans lesquels NagVis va s'installer, peuvent maintenant être des points de montage. 2 - Depuis la mise à jour de RedHat/Alma en 8.8 (fait le 18/05/2023), l'installation des versions précédentes de Shinken échouait. Désormais l'installation est compatible sur les RedHat/Alma 8.5 à 8.8 incluses. *Liste des autres modifications :* *Voir la release note*
RC011	**07 Avril 2023**	shinken-enterprise_V02.08.02-RC011_US/FR_Linux_FULL_2023-04-04.tar.gz	*Modification de l'installateur :* 1 - Désormais l'installation est possible sur les systèmes AlmaLinux 8 *Liste des autres modifications :* *Voir la release note*
RC010	**07 Mars 2023**	shinken-enterprise_V02.08.02-RC010_US/FR_Linux_FULL_2023-03-07.tar.gz	*Voir la release note*
RC009	**01 décembre 2022**	shinken-enterprise_V02.08.02-RC009_US/FR_Linux_FULL_2022-11-17.tar.gz	*Modification de l'installateur :* 1 - Désormais l'installation est possible sur les systèmes RedHat 8.5 & 8.6 2 - Rajout de l'option "--packs-to-install" *: permet de ne sélectionner que les dépendances listées* 3 - Rajout de l'option "--packs-to-exclude" : permet de ne pas installer les dépendances listées *Liste des autres modifications :* *Voir la release note*
RC008	**15 novembre 2022**	shinken-enterprise_V02.08.02-RC008_US/FR_Linux_FULL_2022-11-07.tar.gz	*Voir la release note*
RC007.03	**23 septembre 2022**	shinken-enterprise_V02.08.02-RC007.03_US/FR_Linux_FULL_2022-09-23.tar.gz	*Voir la release note*

RC007.02	**19 septembre 2022**	shinken-enterprise_V02.08.02-RC007.02_US /FR_Linux_FULL_2022-09-19.tar.gz	*Voir la release note*
RC007.01	**30 Août 2022**	shinken-enterprise_V02.08.02-RC007.01_US /FR_Linux_FULL_2022-08-30.tar.gz	*Voir la release note*
RC007	**29 Mai 2022**	shinken-enterprise_V02.08.02-RC007_US /FR_Linux_FULL_2022-06-22.tar.gz	*Modification de l'installateur :* 1 - Ajout du paramètre "--ignore-pre-setup-non-blocking-errors" dans l'installation de patchs et de mise à jour pour passer outre les erreurs non importantes pour le bon fonctionnement de Shinken. Pour l' instant, seul le backup pré-installation est impacté. *Liste des autres modifications :* *Voir la release note*
RC006.02	**23 Mai 2022**	shinken-enterprise_V02.08.02-RC006.02_US /FR_Linux_FULL_2022-04-14.tar.gz	Version d'origine (*non finale pour l'instant*).

Mise à jour de Shinken Entreprise

Prérequis

Concernant l'OS

Environnement requis :

- **Centos : 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9**
- **RHEL : 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10**
- **AlmaLinux : 8.5, 8.6, 8.7, 8.8, 8.9, 8.10**
- **RockyLinux : 8.9, 8.10**

Shinken Entreprise a choisi les distributions suivantes :

- **RHEL (** *Red Hat Enterprise Linux* **)** est la distribution référente dans l'écosystème professionnel Linux
- **CentOS** *(Community* ***ent****erprise* ***O****perating* ***S*** *ystem)* est une distribution dont tous ses paquets, à l'exception du logo, sont des paquets compilés à partir des sources de la distribution ***RHEL (*** *Red Hat Enterprise Linux* ***)***
  - Elle est donc quasiment identique à celle-ci et se veut 100 % compatible d'un point de vue binaire
- **AlmaLinux et RockyLinux** sont deux successeurs de CentOS, la version CentOS 8 ayant été arrêtée.

Ces distributions Linux, principalement destinées aux serveurs, sont stables, performantes et compatibles avec une très grande majorité des environnements professionnels.

Concernant le support de ces distributions :

Distribution	Version distribution	Date support éditeur distribution	Gérée actuellement par Shinken	Sera gérée dans les prochaines versions de Shinken	Recommandations Shinken
RedHat	6.10	*plus supportée*	Non	Non	Cette version de la distribution n'est plus supportée depuis la version **02.08.02-RC014** de Shinken
	7.2 7.9	juin 2024	Oui	Oui	Mettez à jour en RedHat 7.9 si possible.
	8	mai 2029	Oui	Oui	Gérée depuis la **V02.08.02-RC009**
AlmaLinux	8	mai 2029	Oui	Oui	Successeur de CentOS, similaire à la RedHat 8. Gérée depuis la **V02.08.02-RC012**
RockyLinux	8	mai 2029	Oui	Oui	Successeur de CentOS, similaire à la RedHat 8. Gérée depuis la **V02.08.02-RC015**
CentOS	6.10	*plus supportée*	Non	Non	Cette version de la distribution n'est plus supportée depuis la version **02.08.02-RC014** de Shinken
	7.2 7.9	juin 2024	Oui	Oui	Mettez à jour en Centos 7.9 si possible. Nous vous conseillons de déplacer votre installation vers une Alma 8.

	8	*plus supportée*	Non	Non	

Information sur le cycle de vie des versions RedHat / Alma / Rocky

Pour RedHat

Les sous-versions impaires (*Exemple : 8.3, 8.5, 8.7, 8.9*) ont un support que de 6 mois.

- Nous conseillons donc d'utilisé que les sous-versions paires (*Exemple : 8.4, 8.6, 8.8, 8.10*),
  (*voir la page https://access.redhat.com/support/policy/updates/errata*).

Support des versions 8.X de RedHat
? Unknown Attachment

Pour AlmaLinux / RockyLinux

La sortie d'une nouvelle sous-version met fin au support de la sous-version précédente (*voir pour AlmaLinux https://wiki.almalinux.org/release-notes/ et pour RockyLinux https://wiki.rockylinux.org/rocky/version/)*

Concernant la transformation de la CentOS en CentOS Stream (Beta de la Redhat)

Redhat a changé sa politique concernant la Centos, qui devient maintenant une version Béta à la RHEL.
Là où précédemment, elle était une recompilation à l'identique d'une RHEL, elle est désormais une distribution sans version fixe (*dite "rolling release"*) en amont de RHEL :

- qui sert à RedHat afin de tester des nouvelles versions de paquets, avant leur sélection si les tests sont fonctionnels dans la RHEL.
- Elle récupère ainsi le rôle qu'avait la Fedora avant elle.
- Elle ne nous semble donc pas viable pour une utilisation professionnelle en production.

Depuis la version v02.08.02-RC012 Shinken prend en charge l'installation sur les distributions AlmaLinux et d epuis la version V02.08.02-RC015 Shinken prend en charge l'installation sur les distributions RockyLinux. Ce sont deux remplaçants possibles de CentOS.

Transformer une CentOS en Redhat

Nous ne recommandons pas de convertir une CentOS en RedHat, mais de procéder à l'installation d'un nouveau serveur et migrer les données entre les deux serveurs Shinken.

Si vous désirez quand même réaliser cette opération, vous pouvez consulter la page (PROCEDURE) Passer de Centos 7.9 à RedHat 7.9 .

Concernant la Redhat

Attention - Enregistrement Redhat

Lors d'une installation de distribution Redhat Enterprise Linux (commerciale), il faut rattacher votre souscription Redhat à votre système.

Voici les commandes à utiliser depuis le serveur :

1/ subscription-manager register
(-> Nom d'utilisateur / mot de passe)

et il faut également l'attacher à l'OS en cours :

2/ subscription-manager attach

Yum pourra alors être utilisé correctement, car l'abonnement sera valide (et donc Shinken pourra être installé)

Concernant les versions de Shinken Entreprise

IMPORTANT

Pour mettre à jour Shinken d'une version majeur Patché (*exemple: V02.08.01, avec le cumulativePatch-15*) vers une nouvelle version majeure (*exemple: V02.08.02 RC015*) :

- Il faut **directement** installer la nouvelle version majeure sans appliquer avec le dernier patch disponible de la version en installé.
  - Exemple : **inutile** appliquer le CumulativePatch-25 pour passer en V02.08.02
- Ensuite, s'il existe un patch pour cette nouvelle version, vous appliquez **immédiatement** le dernier patch disponible de la version Majeur.

N'hésitez pas à vérifier ce point avec votre revendeur ou Shinken Solutions.

IMPORTANT : Il n'est pas possible de rétrograder de version de Shinken.

- Exemple : Il n'est pas possible de mettre à jour Shinken V02.08.01 vers une autre version Shinken V02.08.00

Extraction du package et mise à jour

Mise à jour :

Il faut être loggué en tant que root,

```
$id
uid=0(root) gid=0(root)
```

Et que le umask du compte root soit à 0022

```
$umask 0022
```

« D écompresser » le package qui vous a été transmis :

- tar zxvf shinken-enterprise_V02.08.XX- **LANGUAGE** .tar.gz
- Cela vous créera un répertoire **shinken-entreprise** contenant le script de mise à jour et les dépendances nécessaires à la mise à jour.

Déplacez-vous dans le répertoire **shinken-entreprise (*cd shinken-enterprise_V02.08.XX- LANGUAGE*)** et exécutez le script :

```
./update.sh
```

Ainsi, la mise à jour :

- Mettra à jour **Shinken Entreprise mais n'aura aucune incidence sur le dossier de configuration de /etc/shinken,** évitant tout risque d' écrasement d'une configuration que vous auriez définie.
- Au lieu d'écraser votre paramétrage, des fichiers "*.cfg.rpmnew" seront ajoutés.
  De nouvelles propriétés pourront figurer dans ces fichiers, il est donc conseillé de parcourir ces fichiers et si besoin, récupérer ces nouvelles propriétés pour les intégrer dans votre architecture.
- Avant la mise à jour, une sauvegarde est effectuée et placée dans **/root/shinken/versions_and_patch_installations/DATE-HEURE-update-NUMERO_VERSION/backup-pre-update/** .
  Elle est nommée de la manière suivante : " **DATE__HEURE__NUMERO_VERSION___backup-preupdate-version-NUMERO_VERSION** ".
  Elle est différente en fonction des démons activés sur la machine :
  - La configuration est sauvegardée si le Synchronizer est activé.
  - Les données utilisateurs sont sauvegardées si le Broker est activé.

Documentation dans le package

La documentation (*en français*) est maintenant intégré au package d'installation.

- Vous pouvez le retrouver à l'intérieur de shinken-enterprise_V02.08.XX- **LANGUAGE** .tar.gz dans le répertoire /tools/documentation/
- La première page de la documentation est index.html qui peut être ouvert avec un navigateur internet.

Mise à jour (Mode avancé)

Options disponibles

Option	Valeur par défaut	Description
--activate-encryption *ARG*	---	Permet d'activer le chiffrement. • Le nom de la clé est optionnel, toutefois il sera demandé lors de l'exécution du programme de la mise à jour s'il n'est pas précisé (*voir le chapitre* Mise en place du chiffrement).
--disable-important-notices-user-input	---	Permet de désactiver les prompts vous demandant confirmation avant de continuer le processus. • ⚠️ Il est cependant fortement conseillé de lire les informations fournies lors de la mise à jour (*voir le chapitre* Passer les demandes de saisies lors de la mise à jour).
--disable-daemons-restart-after-update	---	Permets de désactiver le redémarrage des démons à la fin de la mise à jour (*voir le chapitre* Désactiver le redémarrage des démons à la fin de la mise à jour).
--package-update-only-on-conflict	---	Permet de ne pas chercher à mettre à jour les paquets déjà installés, • cela permet ainsi de tenter d'éviter d'installer des paquets trop à jour par rapport au "repository" interne qui n'est pas à jour (*voir le chapitre* Faire la mise à jour sur un serveur avec des repository internes (non publics) fixés sur une version précise).
--skip-redhat-subscription-check	---	Permet de ne pas lancer la vérification de la souscription du serveur auprès de RedHat • Il doit avoir tout de même accès à des repository locaux. (*voir le chapitre* Faire la mise à jour sur un serveur RedHat non enregistré sur les repository RedHat)
--packs-to-install *ARG*	---	Permet de ne sélectionner que les dépendances listées (*voir le chapitre* Permettre d'exclure l'installation ou la mise à jour de certaines dépendances de sondes)
--packs-to-exclude *ARG*	---	Permet de ne pas installer les dépendances listées (*voir le chapitre* Permettre d'exclure l'installation ou la mise à jour de certaines dépendances de sondes)
--ignore-pre-setup-non-blocking-errors	---	Permets d'ignorer certaines erreurs "mineures" qui pourraient arriver pendant les étapes non essentielles pour le bon fonctionnement de Shinken. Cette option ignore les problèmes suivants : • Les erreurs lors de la sauvegarde du backup avant la mise à jour. **Utiliser cette option qu'en présence de votre support dédié**

--skip-nagvis	---	Permet de ne pas installer Nagvis sur le serveur lors d'une mise à jour de Shinken (*voir la chapitre* Exclure l'installation ou la mise à jour de Nagvis).

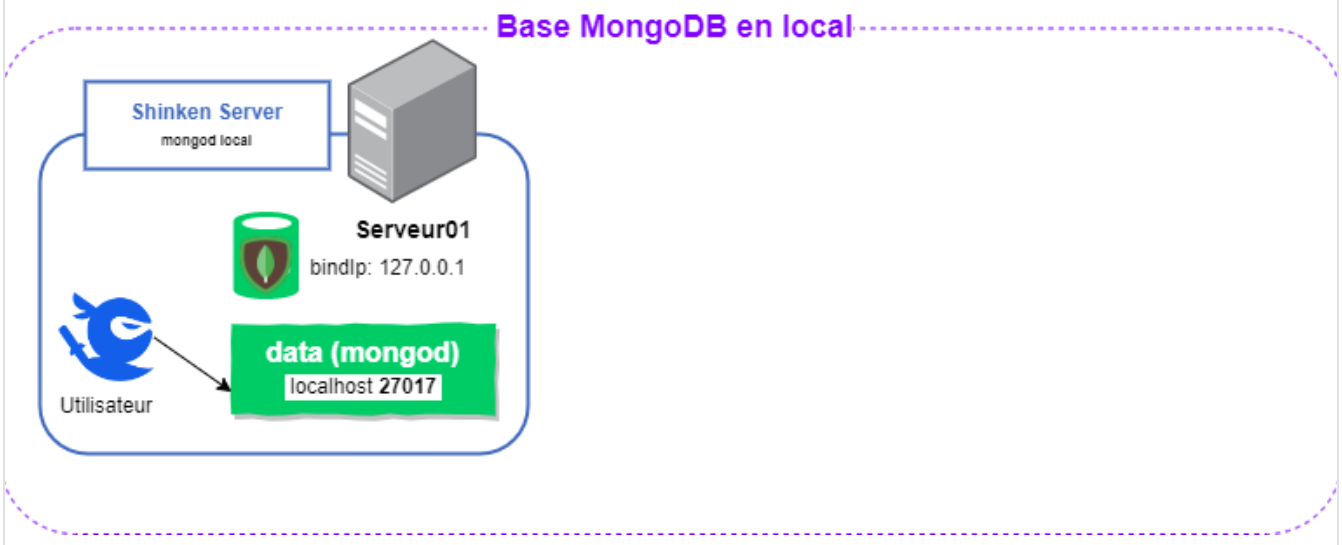
Options de connexion à la base MongoDB

La commande dispose d'options de connexion à la base MongoDB qui peuvent être utilisés dans les cas suivants :

- La base de données MongoDB ne se trouve pas sur la machine qui exécute la commande.
- L'authentification par mot de passe à la base MongoDB est activée.
- Le port de MongoDB n'est pas celui par défaut (*défaut : 27017*).

La combinaison des options de connexion à MongoDB peut rapidement devenir complexe ; voici des paramètres adaptés aux cas les plus courants.

Options génériques

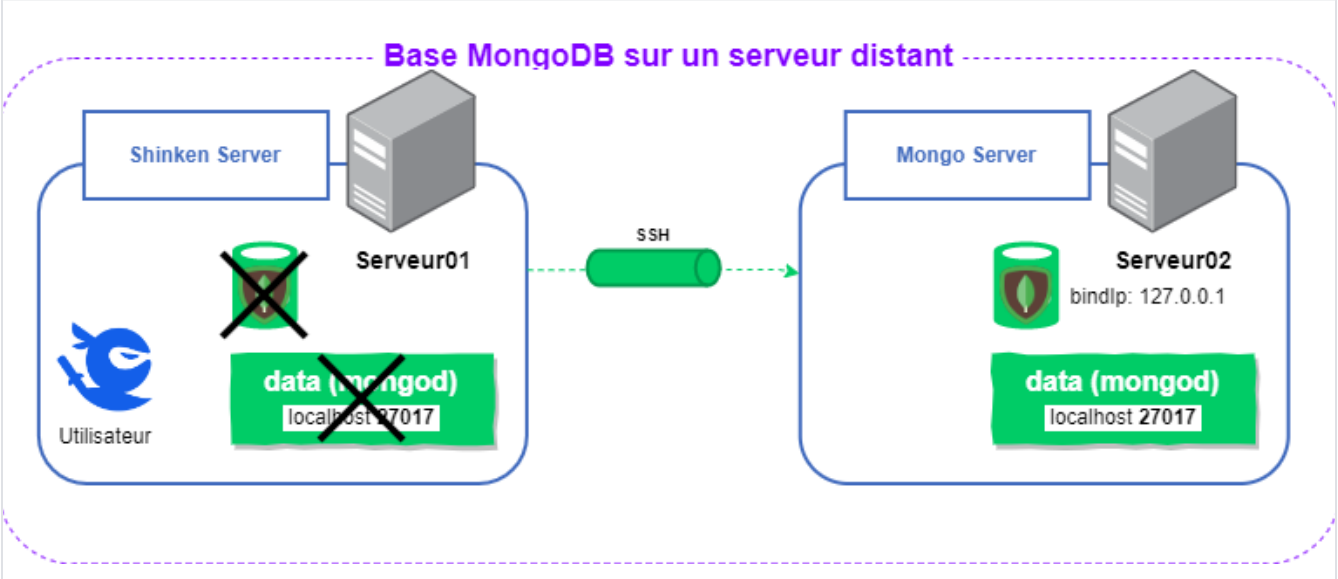



```
[root@serveur01 ~] shinken-commande --mongo-host 127.0.0.1 --mongo-port 27017 --mongo-database shinken
```

Option	Valeur par défaut	Description
--mongo-host *ARG*	**localhost**	Nom ou IP du serveur MongoDB.
--mongo-port *ARG*	**27017**	Port de la base MongoDB.

--mongo-database *ARG*	**shinken** (*ou* **synchronizer** *si la commande concerne la base du Synchronizer*)	Nom de la base de données à utiliser dans MongoDB. À n'utiliser que si la configuration du module ou du démon a changé la base utilisée par défaut.

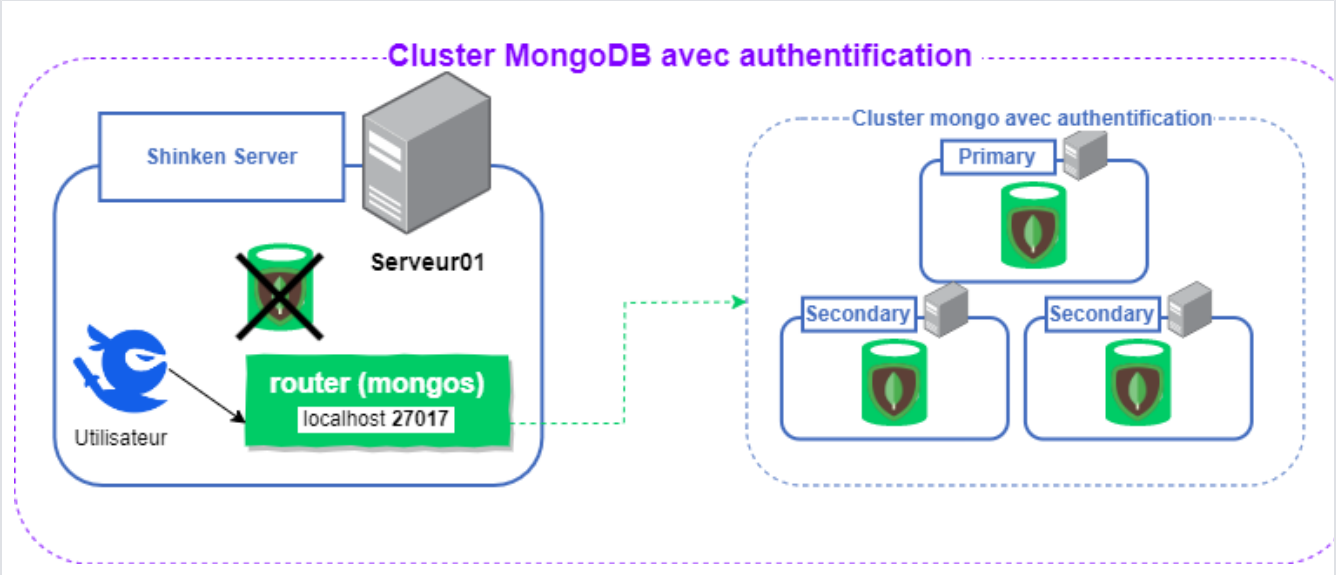
Options de connexion SSH




```
 [root@serveur01 ~] shinken-command --mongo-host serveur02 --mongo-port 27017 --mongo-use-ssh --mongo-ssh-key /var/lib/shinken/.ssh/id_rsa --mongo-ssh-user shinken
```

Option	Valeur par défaut	Description
--mongo-use-ssh	---	Active la connexion SSH au serveur MongoDB.
--mongo-ssh-key *ARG*	**/var/lib/shinken/.ssh/id_rsa**	Clé privée SSH pour la connexion au serveur MongoDB. À utiliser en complément de l'option --mongo-use-ssh.
--mongo-ssh-user *ARG*	**shinken**	Utilisateur à utiliser pour la connexion SSH. À utiliser en complément de l'option --mongo-use-ssh.

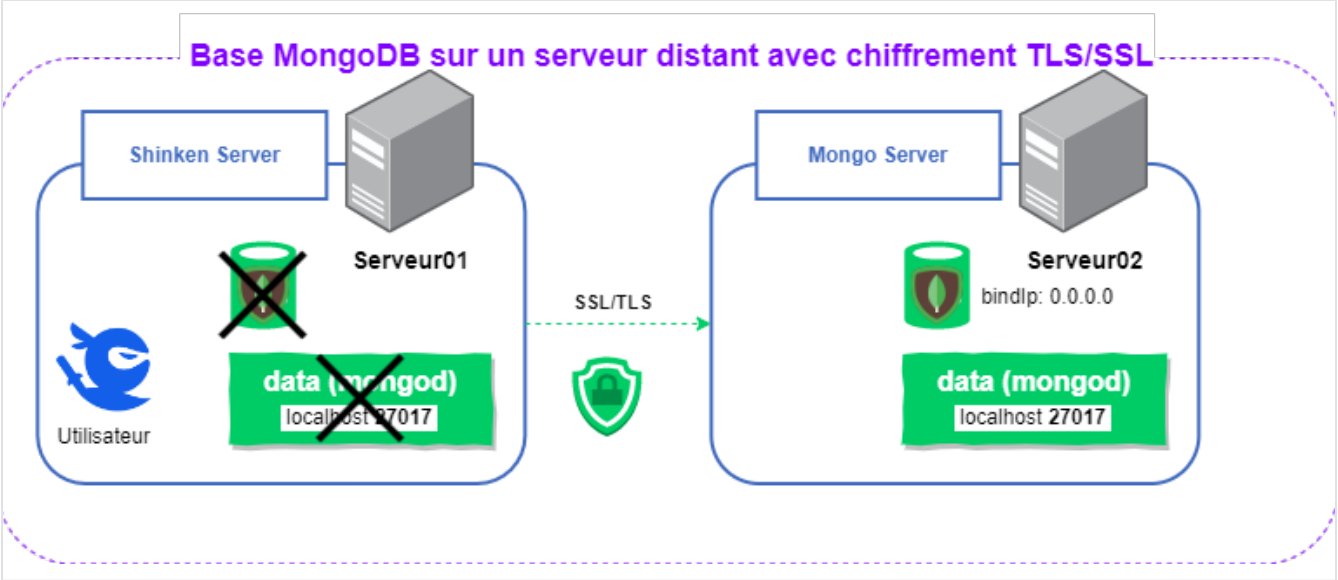
Options d'authentification




```
 [root@serveur01 ~] shinken-command  --mongo-host 127.0.0.1  --mongo-port 27017  --mongo-username shinken --mongo-password shinken
```

Option	Valeur par défaut	Description
--mongo-username *ARG*	---	Utilisateur pour l'authentification avec mot de passe.
--mongo-password *ARG*	---	Mot de passe de l'utilisateur pour l'authentification avec mot de passe. À utiliser en complément de l'option --mongo-username. Si l'option **--mongo-password** est utilisée, le mot de passe risque d'être visible dans l'historique des commandes (*via la commande* ***history***). Pour éviter d'exposer le mot de passe, il est possible d'utiliser cette commande uniquement avec l'option **--mongo-username**. Un prompt interactif apparaîtra alors pour demander le mot de passe. Pour automatiser les commandes dans un script, il est possible de rediriger le contenu d'un fichier contenant le mot de passe (*par exemple : --mongo-password $(cat my_file_with_password)*).

Options SSL/TLS




```
[root@serveur01 ~] shinken-command  --mongo-host serveur02  --mongo-port 27017  --mongo-ssl-ca-file /etc
/shinken/certs/mongo/ca.pem --mongo-ssl-pem-key-file  /etc/shinken/certs/mongo/client.pem
```

Option	Valeur par défaut	Description
--mongo-ssl	---	Active SSL/TLS pour les communications avec la base MongoDB.
--mongo-ssl-ca-file *ARG*	---	Chemin vers le fichier de l'autorité de certification (*CA*) utilisé pour vérifier le certificat SSL de MongoDB. À utiliser en complément de l'option --mongo-ssl.
--mongo-ssl-pem-key-file *ARG*	---	Chemin vers le fichier contenant le certificat SSL du client. À utiliser en complément de l'option --mongo-ssl.
--mongo-ssl-pem-key-password *ARG*	---	Mot de passe du certificat SSL du client. À utiliser en complément de l'option --mongo-ssl.
--mongo-ssl-crl-file *ARG*	---	Chemin vers le fichier CRL (*liste de révocation*) des certificats SSL à rejeter. À utiliser en complément de l'option --mongo-ssl.
--mongo-ssl-allow-invalid-hostnames	---	Accepter le certificat SSL de MongoDB même si le nom d'hôte du certificat ne correspond pas à celui du serveur. À utiliser en complément de l'option --mongo-ssl.
--mongo-ssl-allow-invalid-certificates	---	Accepter le certificat SSL de MongoDB même s'il est invalide, par exemple expiré. À utiliser en complément de l'option --mongo-ssl.

Mise en place du chiffrement

Vous pouvez mettre en place le chiffrement (*voir la page* Protection des données sensibles de l'UI de Configuration) de façon automatique au moment de la mise à jour.

Si vous n'avez jamais activé le chiffrement des données sensibles, nous vous conseillons de procéder à la mise à jour sans activer le chiffrement et de découvrir la fonctionnalité par la lecture de la page Protection des données sensibles de l'UI de Configuration)

Une clé de chiffrement sera alors générée lors du processus de mise à jour et la base de données du Synchronizer sera chiffrée.

Pour cela, lancez la commande suivante :

```
./update.sh --activate-encryption <nom de clé>
```

- **--activate-encryption** permet d'activer le chiffrement. Le nom de la clé est optionnel toutefois il vous sera demandé lors de l'exécution du programme d'installation si vous ne le précisez pas.

La mise en place automatique du chiffrement nécessite dans tous les cas d'effectuer l'export et la sauvegarde de la clé générée lors du processus.

Veuillez consulter la page shinken-protected-fields-keyfile-export pour plus d'informations.

Shinken-healthcheck vous permettra de vérifier la bonne configuration des démons et du chiffrement.

Passer les demandes de saisies lors de la mise à jour

Si vous voulez automatiser la mise à jour de Shinken, via un script Ansible par exemple, vous allez avoir besoin de désactiver les demandes de saisies lors de la mise à jour de Shinken.

Nous vous conseillons fortement de faire au moins une installation manuelle afin de lire les informations fournies lors de la mise à jour avant d'automatiser l'installation.

- **--disable-important-notices-user-input** permet de désactiver les prompts vous demandant confirmation avant de continuer le processus.

⚠️ **Il vous est cependant fortement conseillé de lire les informations fournies lors de la mise à jour.**

Désactiver le redémarrage des démons à la fin de la mise à jour

Dans le cas où vous voulez automatiser la mise à jour sur plusieurs machines, vous pouvez avoir envie de redémarrer tous les démons de toutes les machines en même temps (*afin d'éviter par exemple qu'un Arbiter mis à jour tente de parler avec des démons qui ne le sont pas*).

- **--disable-daemons-restart-after-update** permet de désactiver le redémarrage des démons à la fin de la mise à jour.

Faire la mise à jour sur un serveur avec des repository internes (non publics) fixés sur une version précise

Dans le cas d'un serveur qui n'a accès qu'à des " **repository** " internes qui ne sont pas forcément synchronisés sur les dernières versions des " **repository** " Centos/Redhat officiel, le comportement de base de l'installeur et le script d'update sont de mettre à jour tous les packages si une mise à jour est possible, mais ceci peux entrainer des problèmes si l'installeur a une mise à jour à faire trop récente par rapport à ce qu'il a de disponible dans ses " **repository** ".
Dans ce cas, il faut lancer avec l'option qui demande à ne pas mettre à jour les paquets s'ils sont déjà installés :

- **--package-update-only-on-conflict** : permets de ne pas chercher à mettre à jour les paquets déjà installés et ainsi tente d'éviter d'installer des paquets trop à jour par rapport au " **repository** " interne qui n'est pas à jour.

Accès à un repository yum

Il est a noté que le serveur doit tout de même avoir accès à un " **repository** " valide, et des conflits de paquets peuvent survenir dans le cas de nouveaux paquets installés et que dans ce cas seul yum requêtant les "repository" peut les résoudre (*arrive dans le cas de paquets de l'installeur trop à jour par rapport à ce qui est disponible dans le repository*).

Faire la mise à jour sur un serveur RedHat non enregistré sur les repository RedHat

Si un serveur RedHat a un accès uniquement à des " **repository** " locaux, il ne sera pas enregistré directement chez RedHat.

- La vérification de l'installeur et du script d'update sur les RedHat se base sur la vérification de cette connexion afin de déterminer si le serveur a bien accès aux " **repository** ".
- Ici cette vérification va bloquer la mise à jour alors que le serveur a bien accès à des " **repository** " locaux.
- Il faut alors utiliser l'option suivante :
  - **--skip-redhat-subscription-check** : permets de ne pas lancer la vérification de la souscription du serveur auprès de RedHat (*qui doit avoir tout de même accès à des repository locaux*).

Permettre d'exclure l'installation ou la mise à jour de certaines dépendances de sondes

L'installeur permet de refuser l'installation ou la mise à jour de certaines dépendances de sondes que l'administrateur ne souhaite pas installer, comme par exemple les paquets sqlplus d'Oracle.

Il est important de noter qu'à l'heure actuelle seules les dépendances des sondes ne sont pas installées.

- les modèles, checks et commandes sont toujours présents dans l'interface de configuration suite à l'installation
- Nous allons faire en sorte que modèles, checks, et commande des packs que vous avez exclus ne soient pas présent après une installation.

Les options disponibles sont :

- **--packs-to-install** : permet de ne sélectionner que les dépendances listées
- **--packs-to-exclude** : permet de ne pas installer les dépendances listées

Les "packs" disponibles pour ces options sont :

- oracle: les dépendances des sondes oracle, notamment le paquet sqlplus fournis par Oracle.
- mssql: les dépendances pour les sondes Mssql/Sqlserver.
- nagios-checks: les sondes Nagios et leurs dépendances.
- bacula: le check de vérification de l'outil de backup Bacula, avec ses dépendances systèmes.
  - A exclure si vous utilisez une version de bacula issue du site www.bacula.org , car ce dernier fourni des dépendances incompatibles.

L'administrateur peut choisir d'utiliser une ou l'autre des options :

```
--packs-to-install : nagios-checks,mssql
```

installera uniquement les dépendances ***(fichiers rpm)*** des packs nagios et mssql, donc pas les paquets pour oracle par exemple

```
--packs-to-exclude: oracle,nagios-checks
```

exclura les dépendances des dépendances ***(fichiers rpm)*** des packs oracle et nagios-checks

Exclure l'installation ou la mise à jour de Nagvis

L'installeur vous offre la possibilité de refuser l'installation ou la mise à jour de Nagvis lors de la mise à jour de Shinken.

Nagvis est installé par défaut avec Shinken et est nécessaire au fonctionnement de deux addons :

- nagvis (*voir la page NagVis (Addon)*)
- nagvis-shinken-architecture (*voir la page Configuration de la Visualisation de l'architecture*)

Ces deux addons sont utilisés exclusivement par le Broker et l'Arbiter.

Si vous mettez à jour un autre démon ou si ces addons ne sont pas nécessaires, vous pouvez choisir de ne pas installer ou mettre à jour Nagvis en utilisant l'option **--skip-nagvis**.

Pour les futures mises à jour de Shinken, vous devrez utiliser cette option à chaque fois pour ignorer l'installation de Nagvis.

Après une installation sans Nagvis, si vous souhaitez activer les addons, vous devrez effectuer une mise à jour de votre Shinken sans l'option pour installer Nagvis.

Error rendering macro 'excerpt-include'

No link could be created for 'MERGED - FOR_MERGE - 005.0 - SEF-11995 - MongoDB - options de connexion à la base MongoDB des commandes Shinken'.

Migration de certains fichiers de configuration

Lors d'une mise à jour, il peut arriver que certains fichiers de configuration changent de place.

- Le script de mise à jour va gérer ces déplacements de façon transparente.
- Si un de ces déplacements implique d'écraser des fichiers existants, les fichiers originaux seront préservés et copiés avec l'extension **. patchsave**

Les modules à activer manuellement (car les précédentes versions ne les activées par défaut)

Lors d'une mise à jour depuis une version antérieure, avec une architecture complexe, le script de mise à jour ne peut pas toujours déterminer, avec certitude, quel module peut être installé / activé automatiquement.

- C'est pourquoi, si vous ne les voyez pas, vous pouvez les configurer manuellement.

Activer le Bac à événements

Il est nécessaire d'ajouter les modules :

- Le module **event-manager-writer** sur vos brokers (*cela permettra d'enregistrer les données aux nécessaires événements*).
  (*voir la page* Module event-manager-writer)
- Le module **event-manager-reader** sur vos WebUI (*cela permettra aux WebUI d'accéder aux données enregistrées pour les événements*).
  (*voir la page* Module event-manager-reader)

Activer la Météo des services

Lors d'une mise à jour depuis une version antérieure, avec une architecture complexe, le script de mise à jour ne peut pas toujours déterminer avec certitude sur quelles WebUI la météo des services doit être installé.

C'est pourquoi vous devez vous-même effectuer la configuration manuellement.

Il est nécessaire d'ajouter le module :

- Le module **webui-module-service-weather** sur vos WebUI.
  (*voir la page* Module webui-module-service-weather)

Vérification du bon fonctionnement

Pour vérifier que Shinken Entreprise est bien mis à jour, configuré et fonctionnel, lancez dans un shell la commande :

```
$ shinken-healthcheck
```

Elle vous permettra en ligne de commande d'avoir une vision des différents serveurs/éléments qui composent votre architecture Shinken Entreprise.

- Voir la page Shinken-healthcheck - Vérifier le bon fonctionnement de Shinken Entreprise pour plus de détail sur résultat de cette commande.

Mise à jour des checks via la source cfg-file-shinken

Lors de l'installation de Shinken, nous incluons de nombreux checks (*via des modèles du Pack shinken - Pack Linux - Pack windows*).

Ces éléments de ces packs (*checks, modèles, commandes*) sont disponibles au travers de la source "cfg-file-shinken" :

? Unknown Attachment

Lors d'une update, nous vous fournissons également toutes les mises à jour de ces packs, nous vous conseillons donc d'activer la source et de bien regarder les mises à jour possibles, via les éléments qui apparaîtront en "nouveau" et en "différence".

Si vous avez déjà fait des personnalisations sur les éléments de ces packs, soyez vigilant avant d'appliquer les différences.
Cependant, nous vous conseillons au minimum de mettre à jour les éléments relatifs aux Pack shinken (*éléments en "nouveau" et en "différence"*)

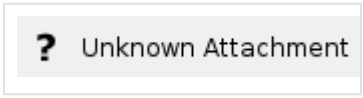
Mise à jour avec un cluster Mongo

Dans la version V02.07.00, la base Mongodb est mise à jour.

- Lorsque Mongodb a été configuré pour fonctionner en tant que cluster, le comportement du script de mise à jour de Shinken Entreprise a été modifié pour prendre en compte cette configuration particulière.
- Des explications détaillées sont présentes dans la page de documentation dédiée : Si Shinken Inférieur à V02.07.00 - Montée de version en Mongodb 3.0 (réalisée automatiquement sous conditions)

Clé de licence Shinken Enterprise

Une fois Shinken Enterprise installé, la commande **shinken-healthcheck** lancée depuis votre serveur Arbiter affichera un message d'erreur au sujet de la licence:



La licence par défaut installée est une licence d'essai. Vous ne pourrez placer en supervision qu'un très faible nombre d'hôtes.

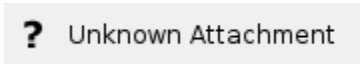
Le service Commercial de Shinken Enterprise a dû vous envoyer une licence nominative vous permettant d'utiliser pleinement le produit.

La licence est un fichier qui a le nom suivant : **user.key** et cette licence est nominative et limitée dans le temps.

Pour l'installer, rien de plus simple, il suffit de :

- Placer ce fichier sur le serveur hébergeant l'Arbiter et sur les serveurs hébergeant le ou les UIs de Visualisation, dans le chemin suivant : **/etc /shinken/user.key**
- Redémarrez alors Shinken Enterprise via la commande : **service shinken restart**

Relancez alors la commande **shinken-healthcheck** le message d'erreur de licence doit avoir disparu et voici un exemple d'information de licence valide :



Si vous n'avez pas de clé de licence ou que celle-ci a expiré, contactez-nous : contact@shinken-solutions.com

Résolution des problèmes liés à la mise à jour

Les logs de la mise à jour

Pour chaque installation/mise à jour, un dossier est créé dans ~/shinken /versions_and_patch_installations/ et nommé de la manière suivante :

- Pour les mises à jour:

```
YYYY-MM-DD-HHhMMmSS-update-VXX.XX.XX
```

Ce dossier contient les données suivantes :

- Affichage du script d'installation (*installation seulement*) : *shinken.enterprise.install.log*
- Détails d'installation des paquets : *shinken.enterprise.install.detail.log*
- Nettoyage de la configuration : *sanatize.update.log*
- Affichage du script de mise à jour (*mise à jour seulement*): *shinken.enterprise.update.log*
- Backup de la configuration et données utilisateur (*mise à jour seulement*)
- Log de l'installation des packages via yum: *rpm_tmp_install.log*

Erreur lors des actions fait automatiquement lors de la mise à jour

Lors de la mise à jour, il y a un certain nombre d'actions (*sanatize*) qui sont automatiquement réalisées.

Si une de ces actions échoue, il vous faudra créer un ticket au prêt du support avec les fichiers de logs de la mise à jour.

Exemple d'erreur

? Unknown Attachment

Erreurs concernant MongoDB

Si script de mise à jour ne parvient pas à se connecter à la base Mongo

Lors du démarrage de la mise à jour de Shinken, une vérification est effectuée pour s'assurer que la base de données est accessible. Si MongoDB n'est pas accessible, la mise à jour de Shinken est interrompue, et le message suivant s'affiche :

? Unknown Attachment

Il est nécessaire de vérifier que la base de données est bien démarrée et que les paramètres d'accès sont correctement configurés (*port, nom du serveur, authentification, tunnel SSH, etc*).

Vérifier que la base de données est opérationnelle

```
systemctl status mongod
```

Vérifier les paramètres d'accessibilité de la base dans le fichier de conficuration de votre base : **/etc/mongod.conf**

La version de MongoDB installée sur votre système n'est pas une version validée par Shinken Solutions.

Le script de mise à jour refuse de s'exécuter avec l'erreur suivante :

```
ERROR: Mongodb is already installed but your Mongodb version XX.YY.ZZ is not supported for install/update"
```

Assurez-vous que la version de MongoDB utilisée est la 2.6.9 pour les installations antérieures à Shinken Entreprise 2.6.1 et la 3.0.15 pour les versions de Shinken Entreprise plus récentes.