

shinken-protected-fields-encryption-disable

Sommaire

- Concept
- Options
 - Option générale
 - Options de désactivation du chiffrement
 - Options de connexion à la base MongoDB
 - Options génériques
 - Options de connexion SSH
 - Options d'authentification
 - Options SSL/TLS
- Exemples

Concept

Cette commande permet de **désactiver** le chiffrement.

- Elle migre la base de données du Synchronizer : toutes les données chiffrées sont converties en clair.
- L'interface de configuration affiche les données en clair en respectant les principes de la protection des données sensibles (voir la page [Protection des données sensibles de l'UI de Configuration](#)).



Attention : La clé de chiffrement actuelle est nécessaire pour désactiver le chiffrement. Sans elle, Shinken Entreprise sera incapable de déchiffrer la base.

Options

Option générale

Option	Valeur par défaut	Description
-h	---	Affiche l'aide de la commande.

Options de désactivation du chiffrement

Option	Valeur par défaut	Description
-q	---	Mode silencieux : n'affiche que le minimum d'informations nécessaires.
-y	---	Force l'activation du chiffrement sans demander la confirmation (utile lors de l'automatisation d'une installation).

Options de connexion à la base MongoDB



Cette commande récupère les paramètres de connexion à la base MongoDB depuis la configuration.

- Il est nécessaire d'utiliser les options de la ligne de commande que si les fichiers de configuration ne correspondent pas à la base MongoDB sur laquelle, la commande doit être exécutée (

migration de base, test sur une préprod ...).

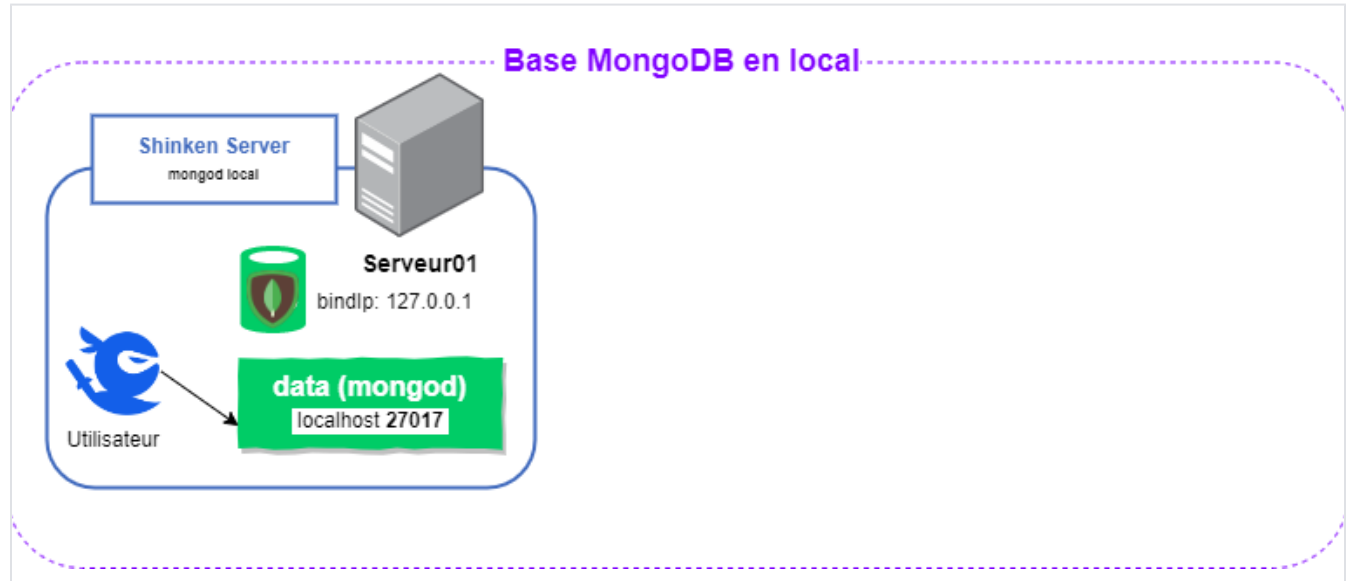
La commande dispose d'options de connexion à la base MongoDB qui peuvent être utilisés dans les cas suivants :

- 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.

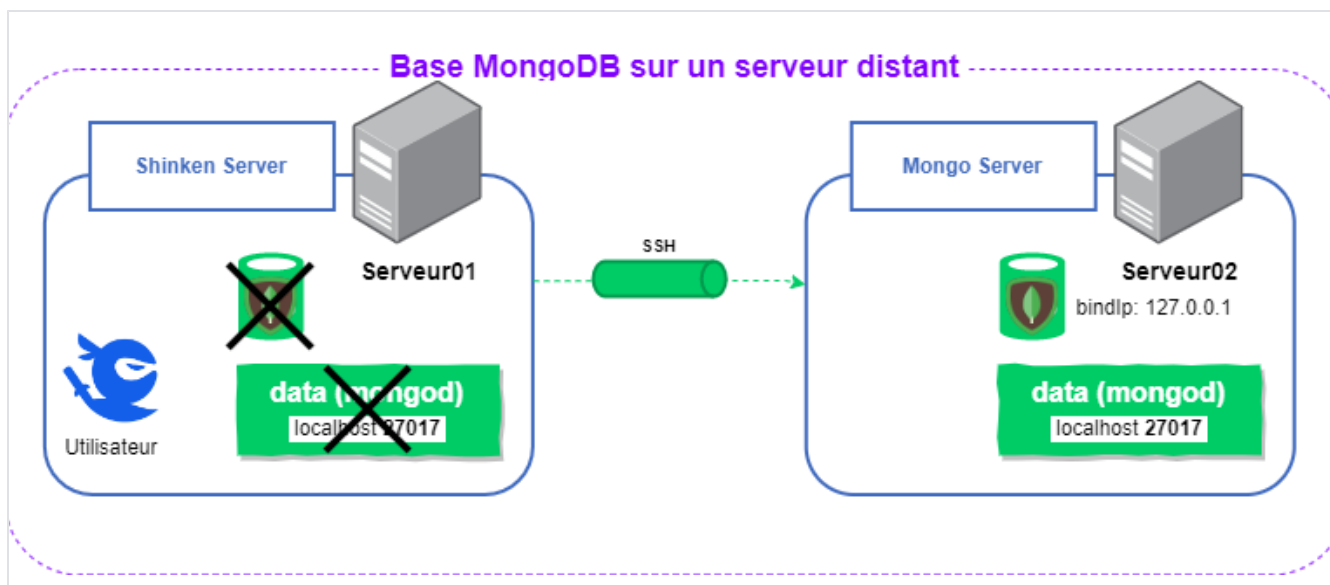
Options génériques



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

Option	Valeur par défaut	Description
<code>--mongo-host</code> <i>ARG</i>	localhost	Nom ou IP du serveur MongoDB.
<code>--mongo-port</code> <i>ARG</i>	27017	Port de la base MongoDB.
<code>--mongo-database</code> <i>ARG</i>	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.

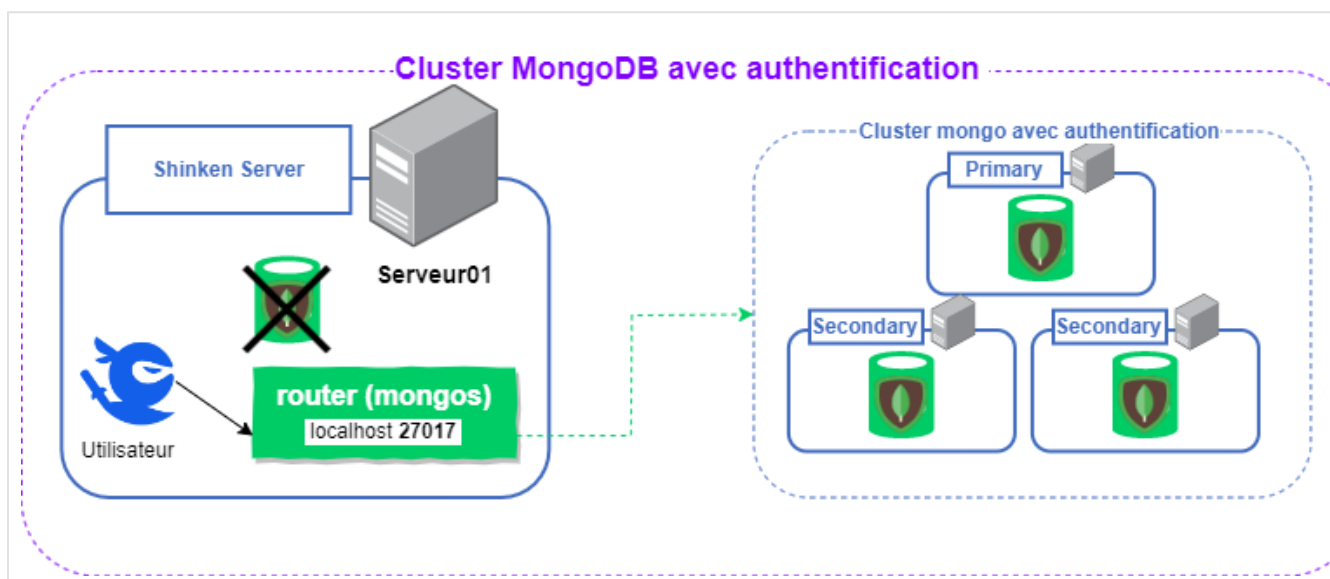
Options de connexion SSH



```
[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
<code>--mongo-use-ssh</code>	---	Active la connexion SSH au serveur MongoDB.
<code>--mongo-ssh-key ARG</code>	<code>/var/lib/shinken/.ssh/id_rsa</code>	Clé privée SSH pour la connexion au serveur MongoDB. À utiliser en complément de l'option <code>--mongo-use-ssh</code> .
<code>--mongo-ssh-user ARG</code>	<code>shinken</code>	Utilisateur à utiliser pour la connexion SSH. À utiliser en complément de l'option <code>--mongo-use-ssh</code> .

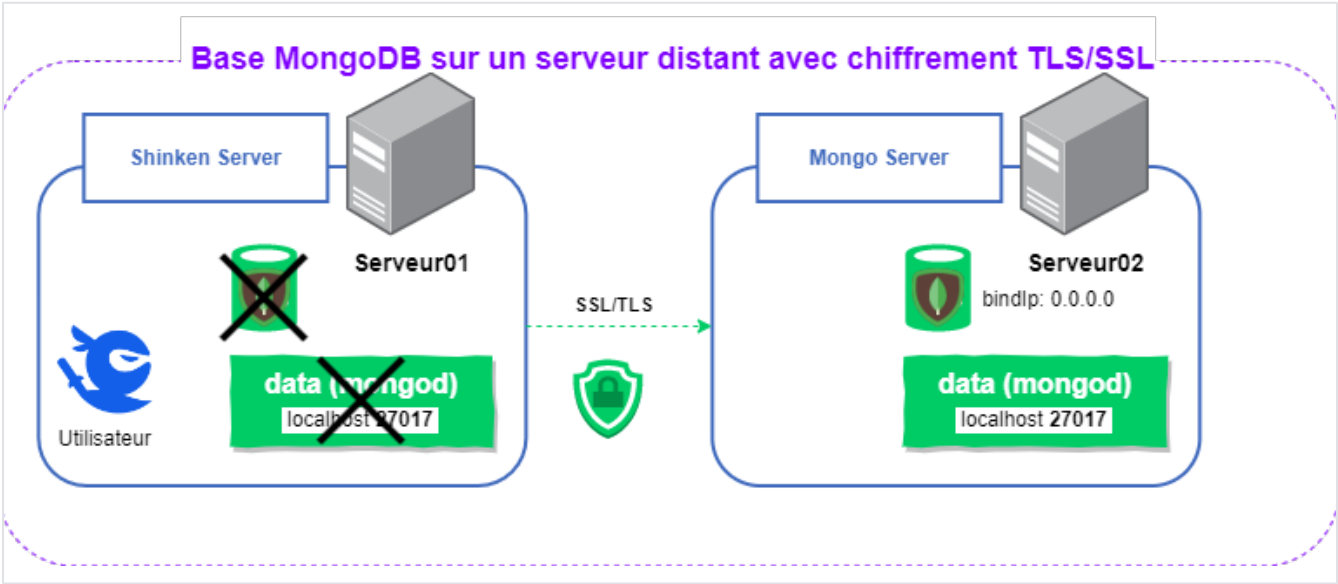
Options d'authentification



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

Option	Valeur par défaut	Description
<code>--mongo-username ARG</code>	---	Utilisateur pour l'authentification avec mot de passe.
<code>--mongo-password ARG</code>	---	Mot de passe de l'utilisateur pour l'authentification avec mot de passe. À utiliser en complément de l'option <code>--mongo-username</code>.  Si l'option <code>--mongo-password</code> est utilisée, le mot de passe risque d'être visible dans l'historique des commandes (<i>via la commande <code>history</code></i>). Pour éviter d'exposer le mot de passe, il est possible d'utiliser cette commande uniquement avec l'option <code>--mongo-username</code>. 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 (<i>par exemple : <code>--mongo-password \$(cat my_file_with_password)</code></i>).

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
<code>--mongo-ssl</code>	---	Active SSL/TLS pour les communications avec la base MongoDB.

<code>--mongo-ssl-ca-file ARG</code>	---	Chemin vers le fichier de l'autorité de certification (<i>CA</i>) utilisé pour vérifier le certificat SSL de MongoDB. À utiliser en complément de l'option <code>--mongo-ssl</code> .
<code>--mongo-ssl-pem-key-file ARG</code>	---	Chemin vers le fichier contenant le certificat SSL du client. À utiliser en complément de l'option <code>--mongo-ssl</code> .
<code>--mongo-ssl-pem-key-password ARG</code>	---	Mot de passe du certificat SSL du client. À utiliser en complément de l'option <code>--mongo-ssl</code> .
<code>--mongo-ssl-crl-file ARG</code>	---	Chemin vers le fichier CRL (<i>liste de révocation</i>) des certificats SSL à rejeter. À utiliser en complément de l'option <code>--mongo-ssl</code> .
<code>--mongo-ssl-allow-invalid-hostnames</code>	---	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 <code>--mongo-ssl</code> .
<code>--mongo-ssl-allow-invalid-certificates</code>	---	Accepter le certificat SSL de MongoDB même s'il est invalide, par exemple expiré. À utiliser en complément de l'option <code>--mongo-ssl</code> .

Exemples

```
$ shinken-protected-fields-encryption-disable

This command will disable encryption and restart the synchronizer to decrypt the protected fields.

Checking consistency between the synchronizer configuration file and the currently running configuration... DONE

    Are you sure you want to proceed and disable encryption ? (y/N) y
Disabling encryption with key named 'secret key'...
Now stopping the Synchronizer... OK
Encryption disabled
Now restarting the Synchronizer... OK
```