shinken-protected-fields-keyfile-export

Sommaire

Concept

Cette commande permet de récupérer la clé courante utilisée pour le chiffrement des données de Shinken Entreprise.

- Il est important d'utiliser cette commande pour sauvegarder cette clef dans un endroit sécurisé.
- Si la clé sur le serveur venait à être corrompue, ou perdue, il est possible de la restaurer.

Options

Options générales

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

Options concernant l'export de clé

Option	Valeur par défaut	Description
-f *ARG*	---	Spécifier manuellement le chemin vers le fichier de la clé (si non spécifié, la commande exportera celle utilisée par le Synchronizer).

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 correspond pas à la base MongoDB sur laquelle, la commande doit être exécutée (

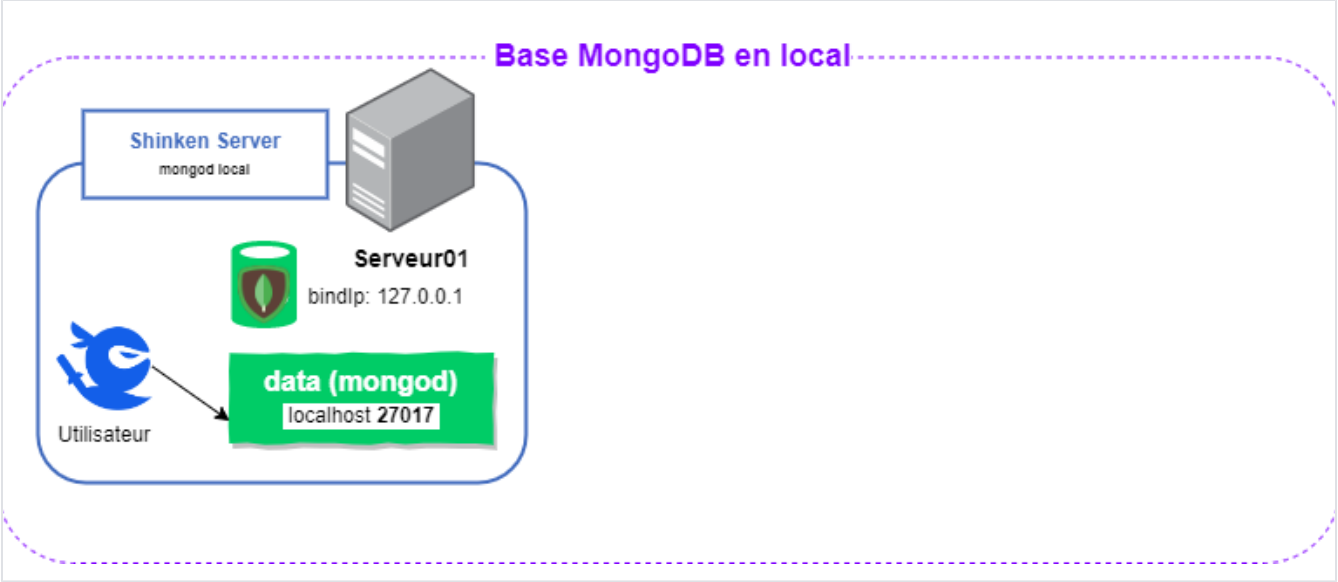
migration de base, test sur une préprod ...).

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.

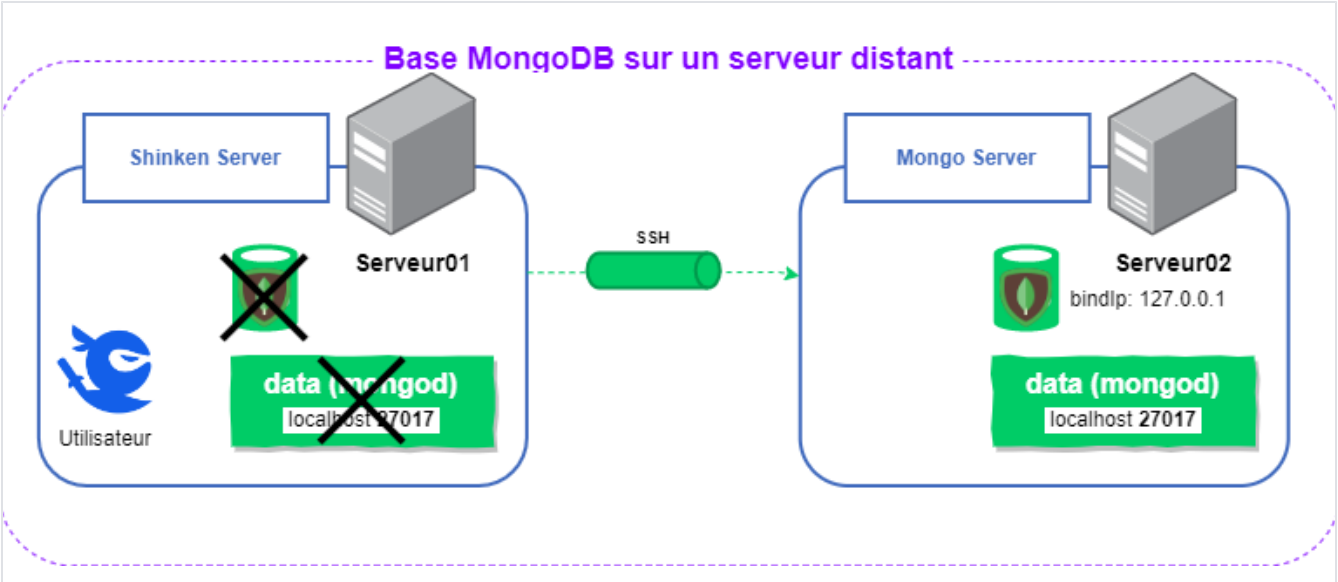
Options génériques




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

Option	Valeur par défaut	Description
--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.

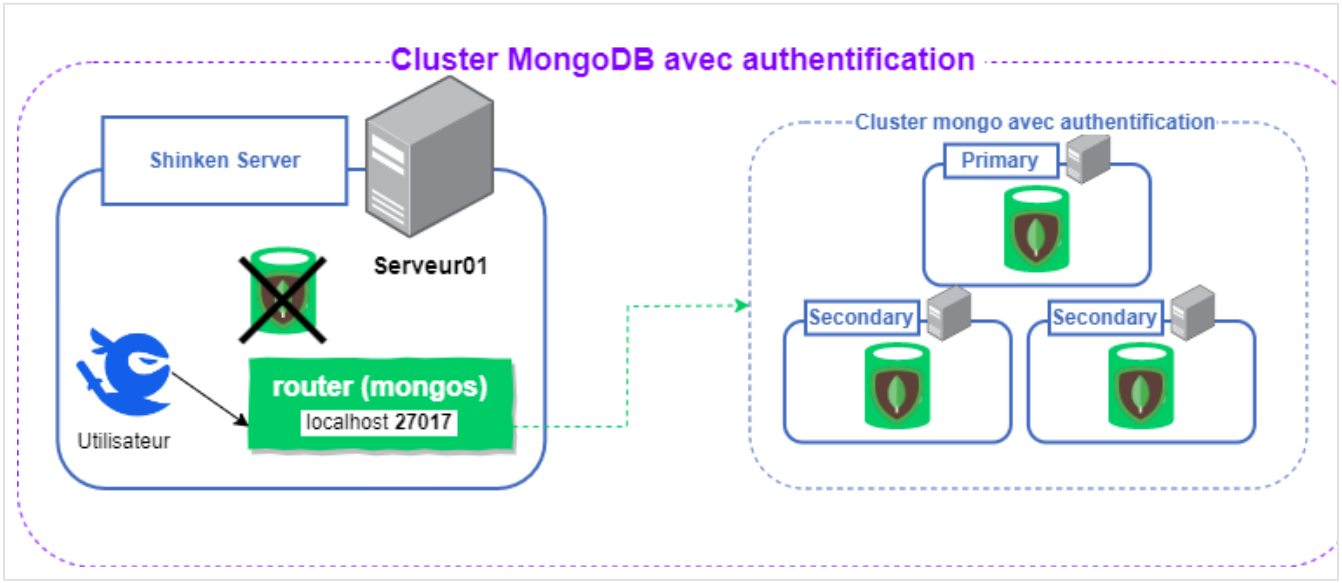
Options de connexion SSH



```
[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

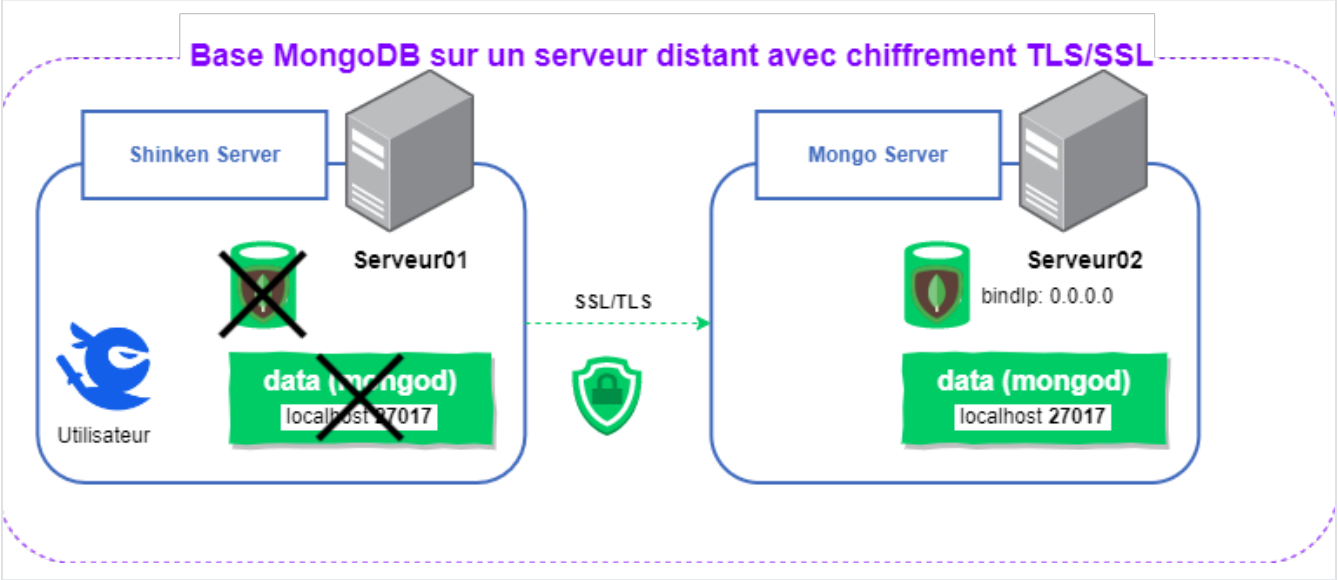



```
[root@serveur01 ~] shinken-command  --mongo-host 127.0.0.1  --mongo-port 27017  --mongo-username shinken --mongo-password shinken
```

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.

Exemples

```
$ shinken-protected-fields-keyfile-export

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

The following line represents the protected fields cipher key named : secret key

c2VjcmV0IGtleXxWeEJnYzQzdkZlR0oraDZGR1hpVm55T1B4M2tRZW8vNWZqN2F5YkdCQ2x3PQo=

You are responsible for saving it securely in a separate place from the Shinken backup.
You can restore this key export by running the following command :

   shinken-protected-fields-keyfile-restore c2VjcmV0IGtleXxWeEJnYzQzdkZlR0oraDZGR1hpVm55T1B4M2tRZW8vNWZqN2F5YkdCQ2x3PQo=
```

La commande affichera :

- le nom de la clé
- un hash de la clé de chiffrement.

Ces valeurs affichées seront nécessaires lors de la restauration de la clé.

Il est important d'utiliser cette commande pour extraire les clés car :

- Des vérifications d'intégrité sont faites.
- Une compatibilité ascendante est assurée par l'utilisation de ces commandes si le principe de chiffrement de Shinken Entreprise venait à évoluer.

Dans le but d'un haut niveau de sécurité, il est conseillé de stocker cette clé dans un emplacement différent que les sauvegardes Shinken.