
corosync-keygen

Génère une clé d'authentification pour corosync

Description

Pour configurer corosync avec des techniques cryptographiques pour s'assurer de l'authenticité de la protection des données des messages, il faut générer une clé privée. **corosync-keygen** crée cette clé et l'écrit dans **/etc/corosync/authkey**.

La clé privée doit être copiée dans tous les processeurs dans le cluster. Si la clé privée n'est pas la même pour tous les nœuds, ces nœuds ne seront pas capables de se joindre à la même configuration.

Copier la clé dans un stockage sécurisé ou utiliser ssh. Puis l'installer avec la commande suivante :

install -D -group=0 -owner=0 -mode=0400 /path_to_authkey/authkey /etc/corosync/authkey

Si un message "Invalid digest" apparaît dans corosync, les clés ne sont pas consistantes entre les processeursS.

OPTIONS

- k <filename>** Spécifie le chemin où créer la clé. défaut : `/etc/corosync/authkey`
- l** Utilise une source de données aléatoires moins sûre, qui ne nécessite pas l'aide de l'utilisateur pour générer de l'entropie.