

Configuration des disques à chiffrement automatique (SED)

Publié: 2024-08-09


Ce guide explique comment configurer les disques à chiffrement automatique (SED) dans l'EDA 9300 ou 10300 sonde.

Les SSD chiffrent en permanence les données écrites sur le disque. Les données de ces lecteurs sont protégées en nécessitant une clé pour déverrouiller les lecteurs chiffrés avant de récupérer les données. Les lecteurs ne sont protégés contre le vol que lorsqu'ils sont sécurisés.


Vous pouvez configurer la sécurité des disques virtuels sur les SSD au moment de leur création ou après leur création. Les disques virtuels sécurisés ne peuvent pas être désécurisés sans effacer toutes les données qu'ils contiennent.

Deux options sont disponibles pour activer la sécurité et le chiffrement sur les lecteurs installés :

Gestion des clés locales (LKM)

Activez la sécurité à partir du contrôleur RAID PowerEdge (PERC) et configurez une clé de sécurité et une phrase secrète stockées localement sur le contrôleur. Cette méthode protège les données en cas d'événement de vol de disque physique, mais pas en cas de vol de l'intégralité du système. Pour plus d'informations sur la configuration de LKM, consultez [Gestion des clés de sécurité et des RAID](#) .

Gestion sécurisée des clés d'entreprise (SEKM)

Gérez les clés à partir d'un service de gestion des clés et activez la sécurité sur les lecteurs installés à partir de l'iDRAC9. Les clés étant stockées en externe sur un service de gestion des clés, les données de ces lecteurs sont protégées en cas d'événement de vol du système. Pour plus d'informations sur la configuration du SEKM, consultez la section « Contrôleur RAID PowerEdge (PERC) » du [Guide de configuration et de déploiement du SEKM](#) .

Après avoir activé le LKM ou le SEKM, vous devez chiffrer vos disques virtuels existants.

Configurez LKM sur le contrôleur RAID à partir de l'interface Web iDRAC

Si vous préférez sécuriser le système à l'aide de la gestion des clés locales (LKM), vous pouvez activer la sécurité à partir du contrôleur RAID.

1. Démarrez iDRAC à partir de n'importe quel navigateur compatible.
2. Dans l'interface Web iDRAC, cliquez sur **Rangement**, puis cliquez sur **Vue d'ensemble**.
3. Cliquez **Contrôleurs**.
4. Dans le Contrôleurs section, cliquez **Modifier** dans la liste des actions à côté du contrôleur que vous souhaitez configurer.



Note: Il existe deux contrôleurs : l'un pour les disques internes, qui stockent le microprogramme et la configuration, et l'autre pour les unités de stockage étendues (ESU), qui stockent les paquets.

5. Dans le Propriétés du contrôleur section, cliquez **Sécurité**.
6. À partir du **Sécurité (chiffrement)** liste, cliquez **Créer une clé de sécurité**.
7. Cliquez **Suivant**.
8. Pour le **Identifiant de clé de sécurité**, saisissez l'ID de clé qui sera nécessaire pour sécuriser les disques virtuels.
9. Pour le **Phrase secrète de la clé de sécurité**, saisissez le mot de passe qui sera nécessaire pour sécuriser les disques virtuels.



Note: La phrase secrète fait la distinction entre majuscules et minuscules. La longueur minimale est de 8 caractères et la longueur maximale est de 32 caractères. Assurez-vous que les caractères contiennent au moins un chiffre, une lettre minuscule, une lettre majuscule et un caractère non alphanumérique.

10. Pour le **Confirmer la phrase de passe de la clé de sécurité**, saisissez à nouveau le mot de passe.
11. Cliquez **Ajouter à En attente**.

Prochaines étapes

Ensuite, [chiffrer un disque virtuel existant](#).

Configurer SEKM pour le chiffrement des disques à partir de l'interface Web iDRAC

Avant de commencer

Avant de configurer la gestion sécurisée des clés d'entreprise (SEKM), assurez-vous de configurer votre serveur de gestion de clés externe (KMS), qui gère les clés qui peuvent verrouiller et déverrouiller les unités de stockage via iDRAC. Pour plus d'informations, consultez la section spécifique à votre KMS dans le [Guide de configuration et de déploiement du SEKM](#).

Si vous préférez sécuriser le système avec SEKM, vous pouvez configurer la sécurité à partir du contrôleur RAID.

1. Démarrez iDRAC depuis n'importe quel navigateur compatible.
2. Depuis l'interface Web d'iDRAC, cliquez sur **Rangement**, puis cliquez sur **Vue d'ensemble**.
3. Cliquez **Contrôleurs**.
4. Dans le Contrôleurs section, cliquez sur **Modifier** dans la liste des actions située à côté du contrôleur que vous souhaitez configurer.



Note: Il existe deux contrôleurs : un pour les disques internes, qui stockent le microprogramme et la configuration, et un pour les unités de stockage étendues (ESU), qui stockent les paquets.

5. Dans le Propriétés du contrôleur section, cliquez sur **Sûreté**.
6. À partir du **Sécurité (chiffrement)** liste, cliquez **Gestionnaire de clés d'entreprise sécurisé**.
7. Cliquez **Ajouter à En attente**.
8. Cliquez **Au prochain redémarrage**.
Un message s'affiche pour indiquer que l'ID de tâche a été créé.
9. Accédez au **File d'attente des tâches** page et assurez-vous que cet ID de tâche est marqué comme **Planifié**.
10. Redémarrez le serveur pour exécuter la tâche de configuration.
11. Accédez au **File d'attente des tâches** page pour afficher la tâche planifiée.

Après le redémarrage du serveur, la tâche de configuration s'exécute dans l'application de tâches automatisées pour activer SEKM sur le PERC. Le serveur redémarre automatiquement.

Prochaines étapes

Ensuite, [crypter un disque virtuel existant](#).

Chiffrer un disque virtuel

Vous pouvez configurer la sécurité des disques virtuels sur les SED existants. Les disques virtuels sécurisés ne peuvent pas être désécurisés sans effacer toutes les données du lecteur.

1. Démarrez iDRAC à partir de n'importe quel navigateur compatible.

2. Dans l'interface Web iDRAC, cliquez sur **Rangement**, puis cliquez sur **Vue d'ensemble**.
3. Cliquez **Disques virtuels**.
4. Cliquez **Chiffrer le disque virtuel** à partir de la liste des actions pour le disque virtuel à chiffrer.
5. Cliquez **Ajouter à En attente**.
6. Cliquez **Postulez maintenant**.