Configurez la gestion externe des clés

ONTAP 9

NetApp
September 12, 2024

Sommaire

Configurez la gestion externe des clés

Configurer la gestion externe des clés en vue d'ensemble

Vous pouvez utiliser un ou plusieurs serveurs externes de gestion des clés pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Un serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol).

Pour ONTAP 9.1 et les versions antérieures, les LIFs de node-management doivent être attribuées à des ports configurés avec le rôle de node-management avant de pouvoir utiliser le gestionnaire de clés externe.

NetApp Volume Encryption (NVE) peut être implémenté avec le gestionnaire de clés intégré dans ONTAP 9.1 et les versions ultérieures. Dans ONTAP 9.3 et versions ultérieures, NVE peut être implémenté avec une gestion des clés externe (KMIP) et un gestionnaire de clés intégré. À partir de ONTAP 9.11.1, vous pouvez configurer plusieurs gestionnaires de clés externes dans un cluster. Voir Configurez les serveurs de clés en cluster.

Collectez des informations réseau dans ONTAP 9.2 et versions antérieures

Si vous utilisez ONTAP 9.2 ou une version antérieure, vous devez remplir la fiche de configuration du réseau avant d'activer la gestion externe des clés.

> Depuis ONTAP 9.3, le système détecte automatiquement toutes les informations réseau nécessaires.

Élément	Remarques	Valeur
Nom de l'interface réseau de gestion des clés		
Adresse IP de l'interface réseau de gestion des clés	Adresse IP de la LIF de node management, au format IPv4 ou IPv6	
Longueur du préfixe réseau IPv6 de gestion des clés	Si vous utilisez IPv6, la longueur du préfixe réseau IPv6	
Masque de sous-réseau de l'interface réseau de gestion des clés		
Adresse IP de la passerelle d'interface réseau de gestion des clés		

Adresse IPv6 pour l'interface réseau du cluster	Requis uniquement si vous utilisez IPv6 pour l'interface réseau de gestion des clés	
Numéro de port pour chaque serveur KMIP	Facultatif. Le numéro de port doit être le même pour tous les serveurs KMIP. Si vous ne fournissez pas de numéro de port, il prend par défaut le port 5696, qui est le port attribué par Internet Numbers Authority (IANA) pour KMIP.	
Nom de la balise clé	Facultatif. Le nom de la balise clé est utilisé pour identifier toutes les clés appartenant à un nœud. Le nom de la balise par défaut est le nom du nœud.	

Informations associées

"Rapport technique NetApp 3954 : exigences et procédures de préinstallation pour IBM Tivoli Lifetime Key Manager pour NetApp Storage Encryption"

"Rapport technique NetApp 4074 : exigences et procédures de préinstallation pour NetApp Storage Encryption pour SafeNet KeySecure"

Installez les certificats SSL sur le cluster

Le cluster et le serveur KMIP utilisent des certificats SSL KMIP pour vérifier l'identité de l'autre et établir une connexion SSL. Avant de configurer la connexion SSL avec le serveur KMIP, vous devez installer les certificats SSL du client KMIP pour le cluster et le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP.

Description de la tâche

Dans une paire haute disponibilité, les deux nœuds doivent utiliser les mêmes certificats SSL publics et privés KMIP. Si vous connectez plusieurs paires haute disponibilité au même serveur KMIP, tous les nœuds des paires haute disponibilité doivent utiliser les mêmes certificats SSL publics et privés.

Avant de commencer

- L'heure doit être synchronisée sur le serveur qui crée les certificats, le serveur KMIP et le cluster.
- Vous devez avoir obtenu le certificat public du client SSL KMIP pour le cluster.
- Vous devez avoir obtenu la clé privée associée au certificat client SSL KMIP pour le cluster.
- Le certificat client SSL KMIP ne doit pas être protégé par un mot de passe.
- Vous devez avoir obtenu le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP.
- Dans un environnement MetroCluster, vous devez installer les mêmes certificats SSL KMIP sur les deux clusters.

Vous pouvez installer les certificats client et serveur sur le serveur KMIP avant ou après l'installation des certificats sur le cluster.

Étapes

1. Installez les certificats client SSL KMIP pour le cluster :

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   Vous êtes invité à entrer les certificats SSL KMIP publics et privés.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Installez le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP :

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Activation de la gestion externe des clés dans ONTAP 9.6 et versions ultérieures (basée sur le matériel)

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous pouvez connecter jusqu'à quatre serveurs KMIP à un nœud. Un minimum de deux serveurs est recommandé pour la redondance et la reprise après sinistre.

À partir de ONTAP 9.11.1, vous pouvez ajouter jusqu'à 3 serveurs de clés secondaires par serveur de clés principal pour créer un serveur de clés en cluster. Pour plus d'informations, voir Configurez les serveurs de clés externes en cluster.

Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer un gestionnaire de clés externe.
- Dans un environnement MetroCluster, vous devez installer le certificat SSL KMIP sur les deux clusters.

Étapes

1. Configurer la connectivité du gestionnaire de clés pour le cluster :

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

- Le `security key-manager external enable` la commande remplace le `security key-manager setup` commande. Vous pouvez exécuter le `security key-manager external modify` commande pour modifier la configuration de la gestion externe des clés. Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.
- Dans un environnement MetroCluster, si vous configurez une gestion externe des clés pour le SVM admin, vous devez répéter l'opération `security key-manager external enable` commande sur le cluster partenaire.

La commande suivante active la gestion externe des clés pour `cluster1` avec trois serveurs de clés externes. Le premier serveur de clés est spécifié à l'aide de son nom d'hôte et de son port, le second est spécifié à l'aide d'une adresse IP et du port par défaut, et le troisième est spécifié à l'aide d'une adresse et d'un port IPv6 :

```
clusterl::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Vérifiez que tous les serveurs KMIP configurés sont connectés :

```
security key-manager external show-status -node node_name -vserver SVM -key
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```

Le `security key-manager external show-status` la commande remplace le `security key-manager show -status` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ----------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

Activez la gestion externe des clés dans ONTAP 9.5 et versions antérieures

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous pouvez connecter jusqu'à quatre serveurs KMIP à un nœud. Un minimum de deux serveurs est recommandé pour la redondance et la reprise après sinistre.

Description de la tâche

ONTAP configure la connectivité du serveur KMIP pour tous les nœuds du cluster.

Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer un gestionnaire de clés externe.
- Dans un environnement MetroCluster, vous devez installer le certificat SSL KMIP sur les deux clusters.

Étapes

1. Configurer la connectivité du gestionnaire de clés pour les nœuds du cluster :

   ```
   security key-manager setup
   ```

   La configuration du gestionnaire de clés démarre.

   > Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

2. Entrez la réponse appropriée à chaque invite.
3. Ajoutez un serveur KMIP :

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.1
   ```

   > Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

4. Ajoutez un serveur KMIP supplémentaire pour la redondance :

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.2
   ```

   > Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

5. Vérifiez que tous les serveurs KMIP configurés sont connectés :

   `security key-manager show -status`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   cluster1::> security key-manager show -status

   Node            Port      Registered Key Manager  Status
   --------------  ----      ----------------------  ---------------
   cluster1-01     5696      20.1.1.1                available
   cluster1-01     5696      20.1.1.2                available
   cluster1-02     5696      20.1.1.1                available
   cluster1-02     5696      20.1.1.2                available
   ```

6. Vous pouvez également convertir des volumes en texte brut en volumes chiffrés.

   `volume encryption conversion start`

   Un gestionnaire de clés externe doit être entièrement configuré avant la conversion des volumes. Dans un environnement MetroCluster, un gestionnaire de clés externe doit être configuré sur les deux sites.

Configurez les serveurs de clés externes en cluster

À partir de ONTAP 9.11.1, il est possible de configurer la connectivité aux serveurs de gestion externe des clés en cluster sur un SVM. Avec des serveurs de clés en cluster,

vous pouvez désigner des serveurs de clés principaux et secondaires sur une SVM. Lors de l'enregistrement des clés, ONTAP essaie d'abord d'accéder à un serveur de clés principal avant de tenter d'accéder aux serveurs secondaires de manière séquentielle jusqu'à ce que l'opération s'effectue correctement, ce qui évite la duplication des clés.

Les serveurs de clés externes peuvent être utilisés pour les clés NSE, NVE, NAE et SED. Un SVM peut prendre en charge jusqu'à quatre principaux serveurs KMIP externes. Chaque serveur principal peut prendre en charge jusqu'à trois serveurs de clés secondaires.

Avant de commencer

- "La gestion des clés KMIP doit être activée pour le SVM".
- Ce processus prend uniquement en charge les serveurs de clés qui utilisent KMIP. Pour obtenir la liste des serveurs de clés pris en charge, reportez-vous à la "Matrice d'interopérabilité NetApp".
- Tous les nœuds du cluster doivent exécuter ONTAP 9.11.1 ou une version ultérieure.
- L'ordre des serveurs répertorie les arguments dans `-secondary-key-servers` Paramètre correspond à l'ordre d'accès des serveurs de gestion externe des clés (KMIP).

Créer un serveur de clés mis en cluster

La procédure de configuration varie selon que vous avez configuré ou non un serveur de clés principal.

Ajout de serveurs de clés primaires et secondaires à un SVM

1. Vérifier qu'aucune gestion des clés n'a été activée pour le cluster :
   `security key-manager external show -vserver` *`svm_name`*
   Si le SVM possède déjà le maximum de quatre serveurs de clés principaux activés, vous devez supprimer l'un des serveurs de clés principaux existants avant d'en ajouter un nouveau.
2. Activez le gestionnaire de clés principal :
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. Modifiez le serveur de clés principal pour ajouter des serveurs de clés secondaires. Le `-secondary-key-servers` paramètre accepte une liste séparée par des virgules de trois serveurs de clés au maximum.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

Ajoutez des serveurs de clés secondaires à un serveur de clés principal existant

1. Modifiez le serveur de clés principal pour ajouter des serveurs de clés secondaires. Le `-secondary-key-servers` paramètre accepte une liste séparée par des virgules de trois serveurs de clés au maximum.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   Pour plus d'informations sur les serveurs de clés secondaires, reportez-vous à la section [mod-secondary].

Modifier les serveurs de clés en cluster

Vous pouvez modifier les clusters de serveurs de clés externes en modifiant l'état (principal ou secondaire) de serveurs de clés spécifiques, en ajoutant et en supprimant des serveurs de clés secondaires ou en modifiant l'ordre d'accès des serveurs de clés secondaires.

Conversion des serveurs de clés principaux et secondaires

Pour convertir un serveur de clés principal en serveur de clés secondaire, vous devez d'abord le supprimer de la SVM avec le `security key-manager external remove-servers` commande.

Pour convertir un serveur de clés secondaire en serveur de clés principal, vous devez d'abord supprimer le serveur de clés secondaire de son serveur de clés principal existant. Voir [mod-secondary]. Si vous convertissez un serveur de clés secondaire en serveur principal lors de la suppression d'une clé existante, toute tentative d'ajout d'un nouveau serveur avant la suppression et la conversion peut entraîner la duplication des clés.

Modifier les serveurs de clés secondaires

Les serveurs de clés secondaires sont gérés à l'aide du `-secondary-key-servers` paramètre du `security key-manager external modify-server` commande. Le `-secondary-key-servers` le paramètre accepte une liste séparée par des virgules. L'ordre spécifié des serveurs de clés secondaires dans la liste détermine la séquence d'accès des serveurs de clés secondaires. L'ordre d'accès peut être modifié en exécutant la commande `security key-manager external modify-server` les serveurs de clés secondaires étant entrés dans une séquence différente.

Pour supprimer un serveur de clés secondaire, le `-secondary-key-servers` les arguments doivent inclure les serveurs clés que vous voulez conserver lors de l'omission de celui à supprimer. Pour supprimer tous les serveurs de clés secondaires, utilisez l'argument `-`, indiquant aucun.

Pour plus d'informations, reportez-vous au `security key-manager external` dans le "Référence de commande ONTAP".

Créez des clés d'authentification dans ONTAP 9.6 et versions ultérieures

Vous pouvez utiliser le `security key-manager key create` Commande permettant de créer les clés d'authentification d'un nœud et de les stocker sur les serveurs KMIP configurés.

Description de la tâche

Si votre configuration de sécurité exige que vous utilisiez des clés différentes pour l'authentification des données et l'authentification FIPS 140-2, vous devez créer une clé distincte pour chacune d'elles. Si ce n'est pas le cas, vous pouvez utiliser la même clé d'authentification pour la conformité FIPS que pour l'accès aux données.

ONTAP crée des clés d'authentification pour tous les nœuds du cluster.

- Cette commande n'est pas prise en charge lorsque le gestionnaire de clés intégré est activé. Toutefois, deux clés d'authentification sont créées automatiquement lorsque le gestionnaire de clés intégré est activé. Les clés peuvent être affichées à l'aide de la commande suivante :

```
security key-manager key query -key-type NSE-AK
```

- Vous recevez un avertissement si les serveurs de gestion des clés configurés stockent déjà plus de 128 clés d'authentification.
- Vous pouvez utiliser le `security key-manager key delete` commande permettant de supprimer les clés inutilisées. Le `security key-manager key delete` La commande échoue si la clé donnée est actuellement utilisée par ONTAP. (Vous devez avoir des privilèges supérieurs à « admin » pour utiliser cette commande.)

> Dans un environnement MetroCluster, avant de supprimer une clé, veillez à ce que cette clé ne soit pas utilisée sur le cluster partenaire. Vous pouvez utiliser les commandes suivantes sur le cluster partenaire pour vérifier que la clé n'est pas utilisée :
>
> - `storage encryption disk show -data-key-id` *`key-id`*
> - `storage encryption disk show -fips-key-id` *`key-id`*

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Créer les clés d'authentification pour les nœuds du cluster :

   ```
   security key-manager key create -key-tag passphrase_label -prompt-for-key
   true|false
   ```

   > Réglage `prompt-for-key=true` provoque l'invite de l'administrateur de cluster à utiliser la phrase secrète lors de l'authentification de disques cryptés. Dans le cas contraire, le système génère automatiquement une phrase de passe de 32 octets. Le `security key-manager key create` la commande remplace le `security key-manager create-key` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant crée les clés d'authentification pour `cluster1`, génération automatique d'une phrase de passe de 32 octets :

   ```
   cluster1::> security key-manager key create
   Key ID:
   00000000000000000200000000000001006268333f870860128fbe17d393e5083b00000000
   00000000
   ```

2. Vérifiez que les clés d'authentification ont été créées :

   ```
   security key-manager key query -node node
   ```

> Le `security key-manager key query` la commande remplace le `security key-manager query key` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man. L'ID de clé affiché dans la sortie est un identificateur utilisé pour faire référence à la clé d'authentification. Ce n'est pas la clé d'authentification ou la clé de chiffrement des données.

L'exemple suivant vérifie que les clés d'authentification ont été créées pour `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Création de clés d'authentification dans ONTAP 9.5 et versions antérieures

Vous pouvez utiliser le `security key-manager create-key` Commande permettant de créer les clés d'authentification d'un nœud et de les stocker sur les serveurs KMIP

configurés.

Description de la tâche

Si votre configuration de sécurité exige que vous utilisiez des clés différentes pour l'authentification des données et l'authentification FIPS 140-2, vous devez créer une clé distincte pour chacune d'elles. Si ce n'est pas le cas, vous pouvez utiliser la même clé d'authentification pour la conformité FIPS que celle utilisée pour l'accès aux données.

ONTAP crée des clés d'authentification pour tous les nœuds du cluster.

- Cette commande n'est pas prise en charge lorsque la gestion intégrée des clés est activée.
- Vous recevez un avertissement si les serveurs de gestion des clés configurés stockent déjà plus de 128 clés d'authentification.

  Vous pouvez utiliser le logiciel du serveur de gestion des clés pour supprimer toutes les clés inutilisées, puis exécuter de nouveau la commande.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Créer les clés d'authentification pour les nœuds du cluster :

   ```
   security key-manager create-key
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > L'ID de clé affiché dans la sortie est un identificateur utilisé pour faire référence à la clé d'authentification. Ce n'est pas la clé d'authentification ou la clé de chiffrement des données.

   L'exemple suivant crée les clés d'authentification pour `cluster1`:

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. Vérifiez que les clés d'authentification ont été créées :

   `security key-manager query`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant vérifie que les clés d'authentification ont été créées pour `cluster1`:

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

Attribution d'une clé d'authentification de données à un lecteur FIPS ou SED (gestion de clés externe)

Vous pouvez utiliser le `storage encryption disk modify` Commande permettant d'attribuer une clé d'authentification de données à un lecteur FIPS ou SED. Les nœuds de cluster utilisent cette clé pour verrouiller ou déverrouiller des données chiffrées sur le disque.

Description de la tâche

Un disque à chiffrement automatique est protégé contre tout accès non autorisé uniquement si son ID de clé d'authentification est défini sur une valeur autre que celle par défaut. L'ID sécurisé du fabricant (MSID), qui possède l'ID de clé 0x0, est la valeur par défaut standard des lecteurs SAS. Pour les disques NVMe, la valeur standard par défaut est une clé nulle, représentée sous forme d'ID de clé vierge. Lorsque vous attribuez l'ID de

clé à un disque auto-crypté, le système remplace son ID de clé d'authentification par une valeur autre que celle par défaut.

Cette procédure n'est pas perturbatrice.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Attribuez une clé d'authentification de données à un lecteur FIPS ou SED :

   `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > Vous pouvez utiliser le `security key-manager query -key-type NSE-AK` Commande permettant d'afficher les ID de clés.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

2. Vérifiez que les clés d'authentification ont été attribuées :

   `storage encryption disk show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   [...]
   ```