ESCアクティブ/スタンバイおよびアクティブ/アクティブHAデータレプリケーションのDRBD暗号化

この章は、次の項で構成されています。

ESC HA データレプリケーションの DRBD 暗号化

ESC は DRBD を使用して、HA クラスタ環境のさまざまなノード間でデータレプリケーションを実行します。DRBD は、クラスタノード上の既存のローカルブロックデバイスを介して論理ブロックデバイスを階層化します。

アクティブノードに書き込まれたデータは、下位層のブロックデバイスに転送され、同時にセカンダリノードに伝送されます。現在、ESC は DRBD デバイスを `/opt/cisco/esc/esc_database` に直接マウントします。

例：

```
# df
Filesystem            1K-blocks    Used Available Use% Mounted on
devtmpfs                2961760       0   2961760   0% /dev
tmpfs                   2972164       4   2972160   1% /dev/shm
tmpfs                   2972164    8748   2963416   1% /run
…
tmpfs                    594436       0    594436   0% /run/user/1004
/dev/mapper/esc_crypt   3028620   57212   2797848   3% /opt/cisco/esc/esc_database
```

ブロックデバイスの暗号化では、ブロックデバイスからの書き込み/読み取り時にデータが透過的に暗号化または復号化されます。基盤となるブロックデバイスは、暗号化されたデータのみを認識します。

`dm-crypt/LUKS` レイヤによってセキュリティが強化されて、ファイルシステムと DRBD デバイス間で DRBD パーティション内のデータが暗号化されます。LUKS（Linux Unified Key Setup）は、ブロックデバイスの暗号化向けの仕様です。

DRBD 暗号化を使用した ESC HA

次の bootvm コマンドは、DRBD が暗号化された状態で ESC HA を起動します。

bootvm.py を使用して DRBD LUKS の暗号化を選択します。ESC VM インスタンスに渡された場合、ESC day-0 user-data/esc-config. yaml と同等の結果になるのに 4 つのバリエーションがあります。

```
bootvm.py --fs_encryption_type luks --fs_luks_key_prompt
bootvm.py --fs_encryption_type luks --fs_luks_key 'LuksKeyValue'
=> injects the luks key into default file location /opt/cisco/esc/esc-config/luks_key

bootvm.py --fs_encryption_type luks --file
root:0400:/opt/cisco/esc/esc-config/luks_key:path-to-local-luks-key-file
=> injects a local file containing the luks key
```

次のコマンドは、ESC VM ファイルシステム上の別のパスにある luks キーファイルを管理するための高度な使用法を示しています。

```
bootvm.py --fs_encryption_type luks --fs_luks_key_file path-on-esc-vm-luks-key-file
--fs_luks_key_prompt
bootvm.py --fs_encryption_type luks --fs_luks_key_file path-on-esc-vm-luks-key-file
--fs_luks_key 'LuksKeyValue'
=> injects the luks key into a different file location

bootvm.py --fs_encryption_type luks --fs_luks_key_file path-on-esc-vm-luks-key-file
--file root:0400:path-on-esc-vm-luks-key-file:path-to-local-luks-key-file
=> injects the luks key as read from a local file into a different file location
```

Heatテンプレートを使用してESCアクティブ/アクティブ構成を展開するように、カスタムユーザデータを使用して ESC をインストールする場合は、次のコマンドを使用します。

luks キーは、day-0 ファイルや属性として esc-config. yaml / filesystem の下に指定します。

luks キーを base64 としてエンコードします。

```
base64 <<<'LuksKeyValue'
THVrc0tleVZhbHVlCg==
```

次に、以前の luks キーをユーザデータ/クラウド コンフィギュレーション ファイルに挿入します。

```
write_files:
 - path: /opt/cisco/esc/esc-config/luks_key
   owner: root:root
   permissions: '400'
   encoding: b64
   content: THVrc0tleVZhbHVlCg==

 - path: /opt/cisco/esc/esc-config/esc-config.yaml
   owner: root:esc-user
   permissions: '0640'
   content: |
     resources:
       filesystem:
         depend_on: drbd:active
         encryption_type: luks
         luks_key_file: /opt/cisco/esc/esc-config/luks_key
```