SED セキュリティ ポリシー

自己暗号化ドライブのセキュリティ ポリシー

自己暗号化ドライブ（SED）には、リアルタイムで着信データを暗号化し、送信データを復号化する特殊なハードウェアが搭載されています。ディスク上のデータは常にディスクで暗号化され、暗号化された形式で格納されます。暗号化されたデータはディスクから読み出す際に常に復号化されます。メディア暗号化キーがこの暗号化と復号化を制御します。このキーはプロセッサやメモリには保存されません。 Cisco UCS Manager は、Cisco UCS C シリーズと B-シリーズ M5 サーバ、および S シリーズのサーバの SED セキュリティ ポリシーをサポートしています。

SED は、セキュリティ キーを指定してロックしなければなりません。このセキュリティ キーはキー暗号化キーまたは認証パスフレーズとも呼ばれ、メディア暗号化キーの暗号化に使用されます。ディスクがロックされていない場合は、データの取得にキーは必要ありません。

Cisco UCS Manager では、セキュリティ キーをローカルででも、リモートからでも設定できます。ローカルでキーを設定した場合、そのキーを覚えておく必要があります。キーを忘れた場合、それを取得することはできず、データが失われます。キー管理サーバ (KMIP サーバとも呼ばれる) を使用すると、リモートでキーを設定できます。この方法により、ローカル管理でのキーの保管と取得に伴なう問題に対処することができます。

SEDの暗号化と復号化はハードウェアを介して行われます。したがって、システムの全体的なパフォーマンスには影響がありません。SEDは、瞬間的な暗号化消去によってディスクの廃止コストや再配置コストを削減します。暗号化消去は、メディア暗号キーを変更することによって実行されます。ディスクのメディア暗号キーが変更されると、そのディスク上のデータは復号不能になるので、ただちにデータが使用不可になります。Cisco UCS Manager リリース 3.1(3) では、SED は C シリーズ サーバと S シリーズ サーバにディスク盗難防止機能を提供します。HX サーバについては、SEDはノード盗難防止機能を提供します。Cisco UCS Managerリリース 4.0(2) では、UCS B シリーズ M5 サーバに SED セキュリティ ポリシーを拡張します。

コントローラとディスクのセキュリティ フラグ

セキュリティ フラグは、ストレージ コントローラとディスクの現在のセキュリティ ステータスを示します。

ストレージ コントローラとディスクには、次のセキュリティ フラグがあります。

- Security Capable：コントローラまたはディスクがSED管理をサポートできることを示します。
- Security Enable：コントローラまたはディスクにセキュリティ キーがプログラムされており、セキュリティがデバイス上で有効であることを示します。このフラグは、セキュリティポリシーを設定してサーバに関連付け、コントローラとディスクを保護しているときに設定されます。HX デバイスでは、このフラグは設定されません。
- Secured：コントローラまたはディスクにセキュリティ キーがプログラムされており、セキュリティが HX デバイス上で有効であることを示します。

次のセキュリティ フラグは、ストレージ ディスクにのみ適用されます。

- Locked：ディスク キーがコントローラ上のキーと一致していないことを示します。これは、異なるキーでプログラムされたサーバ間でディスクを移動すると発生します。ロックされたディスク上のデータにはアクセスできないため、オペレーティング システムがディスクを使用できません。このディスクを使用するには、ディスクのロックを解除するか、または外部設定を安全に消去します。
- Foreign Secured：セキュア ディスクは外部設定になっていることを示します。正しいキーでロックされたディスクのロックを解除しても、ディスクが外部設定状態になっており、そのディスク上のデータが暗号化されているとこのようになります。このディスクを使用するには、外部設定をインポートするか、または外部設定をクリアします。

ローカル セキュリティ ポリシーの管理

ローカル セキュリティ ポリシーの作成

始める前に

新しいストレージ プロファイルまたは既存のストレージ プロファイルにローカル ポリシーを作成できます。

手順

ステップ 1 [Navigation] ペインで、**[Storage]** > **[Storage Profiles]** の順に展開します。

ステップ 2 ポリシーを作成するストレージ プロファイルを選択します。

ステップ 3 **[Security Policy]** タブをクリックし、次に **[Create Security Policy]** をクリックするかまたは **[storage profile]** を右クリックして [Create Security Policy] を選択します。

ステップ 4 [Local Policy] オプションをクリックします。

a) [Key] に入力します。

キーには 32 個の英数字を使用する必要があります。

b) [OK] をクリックします。

次のタスク

こうして作成されたキーは、そのサーバのストレージプロファイルに関連付けられ、ストレージコントローラの下に展開されます。これを確認するには、**[Server ID]** > **Inventory]** > **[Storage]** > **[Controller]** に進み、SAS ストレージ コントローラを選択します。**[General]** タブに移動し、**[Security]** フィールドが **[drive security enable]** として表示されているかどうかを確認します。

ローカル セキュリティ ポリシーの変更

手順

ステップ 1 [Navigation] ペインで、**[Storage]** > **[Storage Profiles]** の順に展開します。

ステップ 2 ポリシーを作成したストレージ プロファイルを選択します。

ステップ 3 [Security Policy] タブをクリックします。

ステップ 4 （任意） ローカル ポリシーのキーを変更するには、[Local Policy] 領域で次の手順を実行します。

a) [Key] フィールドにデータベースの新しいセキュリティ キーを入力します。
b) [Deployed Key] フィールドにデータベースの現在のセキュリティ キーを入力します。

ステップ 5 （任意）セキュリティ ポリシーを **ローカル ポリシー**から**リモート ポリシー**に変更するには、次の手順を実行します。

a) [Remote Policy] オプションをクリックします。
b) [IP Address/Hostname] フィールドにプライマリ サーバの詳細情報を入力します。
c) （任意） [IP Address/Hostname] フィールドにセカンダリ サーバの詳細情報を入力します。
d) （任意） [Deployed Key] フィールドにデータベースの現在のセキュリティ キーを入力します。
e) （任意） [Port] フィールドに、サーバのポート番号を入力します。
f) [KMIP Server Public Certificate] フィールドに KMIP 証明書の内容を入力します。
g) （任意） [Add Login Details] をクリックしてユーザ クレデンシャルを入力します。

ステップ 6 **[Save Changes]**をクリックします。

ローカル セキュリティ ポリシーを使用しているサーバへのセキュアなディスクの挿入

サーバにセキュアなディスクを挿入すると、次のいずれかが行われます。

- ドライブ上のセキュリティキーが、サーバのセキュリティキーと一致し、自動的にロックが解除されます。
- ディスク上のセキュリティキーとサーバ上のセキュリティキーが異なっています。ディスクはロックされたディスクとして表示されます。ロックされたディスク上で次のいずれかを実行できます。
  - セキュアな外部設定を消去してディスク上のすべてのデータを削除します。
  - ディスクの正しいキーを提供してディスクのロックを解除します。ディスクのロックを解除すると、ディスクは Foreign Secured の状態になります。これらのディスクの外部設定は、すぐにインポートするか、またはクリアする必要があります。

（注） 現在の一連のディスクの外部設定をインポートする前に別の一連のディスクのロックを解除すると、現在の一連のディスクは再度ロックされ、Locked の状態になります。

KMIP クライアント証明書ポリシー

KMIPサーバとも呼ばれているキー管理サーバを使用して、キーをリモートから設定できます。リモートポリシーを作成する前に、KMIPクライアント証明書ポリシーを作成する必要があります。証明書の生成に使用するホスト名はKMIP サーバのシリアル番号です。

証明書ポリシーは、2 つの独立した範囲から作成できます。

- グローバルスコープ：最初にこの範囲でグローバル証明書ポリシーを作成できます。この範囲で証明書を変更しても、証明書は再生成されません。
- サーバスコープ：この範囲で証明書ポリシーを作成または変更できます。作成または変更すると、証明書が再生成されます。このような証明書はそのサーバに固有であり、そのサーバについてグローバル証明書がオーバーライドされます。

KMIP クライアント証明書ポリシーを作成したら、次のいずれかを実行します。

- KMIP サーバに生成された証明書をコピーします。
- 生成された証明書署名要求を使用して CA 署名付き証明書を取得します。この CA 署名付き証明書を CIMC にコピーします。

グローバル KMIP クライアント証明書ポリシーの作成

グローバル KMIP クライアント証明書ポリシーを作成することができます。

このポリシーを使用しているときに証明書の作成に使用するホスト名はサーバのシリアル番号です。

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 [Work] ペインの [Policies] タブをクリックします。

ステップ 3 [Security] サブタブをクリックします。

ステップ 4 [Create KMIP Client Cert Policy] をクリックします。

ステップ 5 表示された [Create KMIP Client Cert Policy] ダイアログボックスで、次の情報を入力します。

名前	説明
Country Code	会社所在国の国コード。 アルファベット2文字を大文字で入力します。

名前	説明
状態	証明書を要求している会社の本社が存在する州または行政区分。 32 文字以下で入力します。
地名	証明書を要求している会社の本社が存在する市または町。 32 文字以下で入力します。
組織名	証明書を要求している組織。 32 文字以下で入力します。
部署名	組織ユニット 最大 64 文字まで入力できます。
Email	要求に関連付けられている電子メール アドレス。
Validity	証明書の有効期間。

ステップ 6 **[OK]** をクリックします。

サーバ用の KMIP クライアント証明書ポリシーの作成

サーバ用のKMIPクライアント証明書ポリシーを作成できます。この証明書は、特定のサーバにのみ適用され、グローバル KMIP クライアント証明書をオーバーライドします。

このポリシーを使用しているときに証明書の作成に使用するホスト名はサーバのシリアル番号です。

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 のC シリーズおよびS シリーズ サーバでは、展開**機器** > **ラック マウント** > **サーバ** > **のサーバの ID**。

ステップ 3 B シリーズ サーバ展開**機器** > **シャーシ** > **シャーシ ID** > **サーバ** > **サーバ ID**

ステップ 4 [Work] ペインで、[Inventory] タブをクリックし、[Storage] サブタブをクリックします。

ステップ 5 [Security] サブタブをクリックします。

ステップ 6 [Create KMIP Client Cert Policy] をクリックします。

ステップ 7 表示された [Create KMIP Client Cert Policy] ダイアログボックスで、次の情報を入力します。

名前	説明
Country Code	会社所在国の国コード。 アルファベット2文字を大文字で入力します。
状態	証明書を要求している会社の本社が存在する州または行政区分。 32 文字以下で入力します。
地名	証明書を要求している会社の本社が存在する市または町。 32 文字以下で入力します。
組織名	証明書を要求している組織。 32 文字以下で入力します。
部署名	組織ユニット 最大 64 文字まで入力できます。
Email	要求に関連付けられている電子メール アドレス。
Validity	証明書の有効期間。

ステップ 8 **[OK]** をクリックします。

リモート セキュリティ ポリシーの管理

リモート セキュリティ ポリシーの作成

新規ストレージ プロファイルまたは既存のストレージ プロファイルにリモート ポリシーを作成できます。

始める前に

KMIP クライアント証明書ポリシーを作成したことを確認します。

手順

ステップ 1 [Navigation] ペインで、**[Storage]** > **[Storage Profiles]** の順に展開します。
ステップ 2 ポリシーを作成するストレージ プロファイルを選択します。

ステップ 3 **[Security Policy]** タブをクリックし、次に **[Create Security Policy]** をクリックするかまたは **[storage profile]** を右クリックして [Create Security Policy] を選択します。

ステップ 4 [Remote Policy] オプションをクリックします。

a) [IP Address/Hostname] フィールドにプライマリ サーバの詳細情報を入力します。
b) （任意） [IP Address/Hostname] フィールドにセカンダリ サーバの詳細情報を入力します。
c) （任意） [Port] フィールドに、サーバのポート番号を入力します。
d) [KMIP Server Public Certificate] フィールドに KMIP 証明書の内容を入力します。
e) （任意） [Add Login Details] をクリックしてユーザ クレデンシャルを入力します。
f) [OK] をクリックします。

ポリシーが正常に作成されたというメッセージが表示されます。

次のタスク

こうして作成されたキーは、そのサーバのストレージプロファイルに関連付けられ、ストレージコントローラの下に展開されます。これを確認するには、**[Server ID]** > **Inventory]** > **[Storage]** > **[Controller]** に進み、SAS ストレージ コントローラを選択します。**[General]** タブに移動し、**[Security]** フィールドが **[drive security enable]** として表示されているかどうかを確認します。

リモート セキュリティ ポリシーの変更

手順

ステップ 1 [Navigation] ペインで、**[Storage]** > **[Storage Profiles]** の順に展開します。

ステップ 2 ポリシーを作成したストレージ プロファイルを選択します。

ステップ 3 [Security Policy] タブをクリックします。

ステップ 4 リモート ポリシーを変更するには、[Remote Policy] 領域で次の手順を実行します。

a) [IP Address/Hostname] フィールドにプライマリ サーバの詳細情報を入力します。
b) （任意） [IP Address/Hostname] フィールドにセカンダリ サーバの詳細情報を入力します。
c) （任意） [Port] フィールドに、サーバのポート番号を入力します。
d) [KMIP Server Public Certificate] フィールドに KMIP 証明書の内容を入力します。

この証明書をブラウザから Base 64 形式で保存します。

e) （任意） [Add Login Details] をクリックしてユーザ クレデンシャルを入力します。

ステップ 5 セキュリティ ポリシーを **リモート ポリシー**から**ローカル ポリシー**に変更するには、次の手順を実行します。

a) [Local Policy] オプションをクリックします。
b) [Key] フィールドにコントローラの新しいセキュリティ キーを入力します。

ステップ 6 **[Save Changes]**をクリックします。

リモート セキュリティ キーの変更

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 のCシリーズおよびSシリーズ サーバでは、展開**機器** > **ラック マウント** > **サーバ** > **のサーバの ID**。

ステップ 3 B シリーズ サーバ展開**機器** > **シャーシ** > **シャーシ ID** > **サーバ** > **サーバ ID**

ステップ 4 [Work] 領域の [Inventory] タブをクリックします。

ステップ 5 [Storage] サブタブをクリックします。

ステップ 6 [Controllers] タブで、SAS コントローラを選択します。

ステップ 7 [General] タブで、[Modify Remote Key] をクリックします。

リモート セキュリティ ポリシーを使用しているサーバへのセキュアなディスクの挿入

リモート セキュリティ ポリシーを使用しているサーバにセキュアなディスクを挿入すると、ストレージ ディスクはロックされたディスクとして表示されます。次のいずれかを実行します。

- 以前にローカル キーを使用してディスクがロックされていた場合は、そのローカル キーを使用してディスクのロックを手動で解除します。
- リモート KMIP サーバを使用してロックを解除します。

セキュアなディスクをローカル セキュリティ ポリシーを使用しているサーバからリモート セキュリティ ポリシーを使用しているサーバに移動すると、ディスクはロックされた状態として表示されます。ローカル キーを使用してディスクのロックを手動で解除します。

ディスクのセキュリティのイネーブル化とディセーブル化

始める前に

- ディスクのセキュリティを有効にするには、ディスクがJBODであることを確認します。

- ディスクをセキュアに消去するには、そのディスクが未設定で良好な状態になっている必要があります。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 の C シリーズおよび S シリーズ サーバでは、展開**機器** > **ラック マウント** > **サーバ** > **のサーバの ID**。

ステップ 3 B シリーズ サーバ展開**機器** > **シャーシ** > **シャーシ ID** > **サーバ** > **サーバ ID**

ステップ 4 [Work] 領域の [Inventory] タブをクリックします。

ステップ 5 [Storage] サブタブをクリックします。

ステップ 6 [Disks] タブで、ディスクを選択します。

ステップ 7 [Details] 領域で、[Enable Encryption] をクリックします。

ステップ 8 セキュア ディスクを無効にするには、[Secure Erase] をクリックします。

コントローラのセキュリティのディセーブル化

始める前に

SAS コントローラ上でのみ、セキュリティを無効にすることができます。コントローラ上のセキュリティを無効にするには、まずすべてのセキュアディスク上のセキュリティを無効にしてから、コントローラのすべてのセキュア仮想ドライブを削除します。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 の C シリーズおよび S シリーズ サーバでは、展開**機器** > **ラック マウント** > **サーバ** > **のサーバの ID**。

ステップ 3 B シリーズ サーバ展開**機器** > **シャーシ** > **シャーシ ID** > **サーバ** > **サーバ ID**

ステップ 4 [Work] 領域の [Inventory] タブをクリックします。

ステップ 5 [Storage] サブタブをクリックします。

ステップ 6 [Controllers] タブで、SAS コントローラを選択します。

ステップ 7 [General] タブで、[Disable Security] をクリックします。

ロックされたディスクのロックの解除

SED のキーがコントローラ上のキーと一致していない場合、そのディスクは [Locked, Foreign Secure] と表示されます。そのディスクのセキュリティキーを提供するか、またはリモート KMIP サーバを使用して、ディスクのロックを解除します。ディスクのロックを解除した後、外部設定をインポートするか、またはクリアします。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 **[Equipment]** > **[Rack-Mounts]** > **[Servers]** > **[Server Number]** の順に展開します。

ステップ 3 [Work] 領域の [Inventory] タブをクリックします。

ステップ 4 [Storage] サブタブをクリックします。

ステップ 5 [Controller] タブで、SAS コントローラを選択します。

ステップ 6 ローカル セキュリティ ポリシーで保護されているディスクのロックを解除するには、次の手順を実行します。

a) [General] タブで、[Unlock Disk] をクリックします。

b) [Key] テキスト ボックスに、そのディスクをロックするのに使用したキーを入力します。

c) [OK] をクリックします。

ステップ 7 リモート KMIP サーバで保護されているディスクのロックを解除するには、[General] タブで [Unlock For Remote] をクリックします。

ロックされたディスクのロックを解除すると、そのディスクのセキュリティ ステータスは [Foreign Secure] と表示されます。

次のタスク

外部設定をインポートするか、またはクリアします。

セキュア外部設定ディスクの消去

ロックされた状態のディスクがあり、そのディスクを既存のデータにアクセスせずに使用する場合は、セキュアな外部設定ディスクを消去できます。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 のCシリーズおよびSシリーズ サーバでは、展開**機器** > **ラック マウント** > **サーバ** > **のサーバの ID**。

ステップ 3 B シリーズ サーバ展開**機器** > **シャーシ** > **シャーシ ID** > **サーバ** > **サーバ ID**

ステップ 4 [Work] 領域の [Inventory] タブをクリックします。

ステップ 5 [Storage] サブタブをクリックします。

ステップ 6 [Disks] タブで、ディスクを選択します。

ステップ 7 [General] タブで、[Secure Erase Foreign Configuration] をクリックします。

データを安全に削除する

委員会規制 (EU) 2019/424 は、データを安全に処分することを要求しています。

データの安全な廃棄は、Cisco UCS サーバのさまざまなドライブ、メモリ、およびストレージからデータを消去し、工場出荷時の設定にリセットするための、一般的なツールを使用することによって可能になります。

委員会規制 (EU) 2019/424 に準拠するためのデータの安全な削除は、次の Cisco UCS サーバでサポートされています。

- Cisco UCS B200
- Cisco UCS B480
- Cisco UCS C125
- Cisco UCS C220
- Cisco UCS C240
- Cisco UCS C480
- Cisco UCS S3260

安全にデータを削除するため、UCSサーバに取り付けられているデバイスについて十分に理解し、適切なツールを実行する必要があります。場合によっては、複数のツールを実行する必要がある場合があります。

データを安全に消去する方法の詳細については、https://www.cisco.com/web/dofc/18794277.pdf を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。