SPDM セキュリティ

SPDM セキュリティ

Cisco UCS M6 サーバーには、デバイス自体に対する攻撃のベクトルを提供したり、デバイスを使用してシステム内の別のデバイスを攻撃したりする可能性のある可変コンポーネントが含まれている場合があります。これらの攻撃を防御するために、セキュリティ プロトコルおよびデータ モデル （SPDM）仕様では、デバイスがその ID と変更可能なコンポーネント構成の正確さを証明するように要求する安全なトランスポートの実装が可能になっています。この機能は、Cisco UCS Manager リリース 4.2(1d) 以降の Cisco UCS C220 および C240 M6 サーバーでサポートされています。

（注） SPDM は現在、Cisco UCS C225 M6サーバ および Cisco UCS C245 M6サーバ ではサポートされていません。

SPDMは、さまざまなトランスポートおよび物理メディアを介してデバイス間でメッセージ交換を実行するためのメッセージ、データ オブジェクト、およびシーケンスを定義します。これは、管理コンポーネント トランスポート プロトコル（MCTP）を介したベースボード管理コントローラ（BMC）とエンドポイント デバイス間のメッセージ交換を調整します。メッセージ交換には、BMC にアクセスするハードウェア ID の認証が含まれます。SPDM は、デバイス認証、ファームウェア測定、および証明書管理の管理レベルを指定することにより、低レベルのセキュリティ機能と操作へのアクセスを可能にします。エンドポイント デバイスは、認証を提供するように求められます。 BMC はエンドポイントを認証し、信頼できるエンティティのアクセスのみを許可します。

UCS Manager では、オプションで外部セキュリティ証明書を BMC にアップロードできます。ネイティブの内部証明書を含め、最大 40 の SPDM 証明書が許可されます。制限に達すると、

証明書をアップロードできなくなります。ユーザーがアップロードした証明書は削除できますが、内部/デフォルトの証明書は削除できません。

SPDM セキュリティ ポリシーでは、3 つのセキュリティ レベル設定のいずれかを指定できます。セキュリティは、次の 3 つのレベルのいずれかで設定できます。

- フル セキュリティ：

  これは、最高の MCTP セキュリティ設定です。この設定を選択した場合、エンドポイントの認証またはファームウェアの測定が失敗すると、障害が生成されます。エンドポイントのいずれかでエンドポイント認証またはファームウェア測定がサポートされていない場合にも、障害が生成されます。

- 部分的なセキュリティ (デフォルト):

  この設定を選択した場合、エンドポイントの認証またはファームウェアの測定が失敗すると、障害が生成されます。エンドポイントのいずれかでエンドポイント認証またはファームウェア測定がサポートされていない場合には、障害が生成されません。

- No Security

  この設定を選択した場合（エンドポイント測定やファームウェア測定が失敗しても）障害は発生しません。

1 つ以上の外部/デバイス証明書のコンテンツを BMC にアップロードすることもできます。SPDM ポリシーを使用すると、必要に応じてセキュリティ証明書または設定を変更または削除できます。証明書は、不要になったときに削除または置き換えることができます。

証明書は、システムのすべてのユーザー インターフェイスに一覧表示されます。

SPDM セキュリティ ポリシーの作成

この手順では、SPDM ポリシーを作成します。

（注） 最大 40 の SPDM 証明書 (ネイティブ証明書を含む) をアップロードできます。

手順

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 **[ポリシー（Policies）]** に移動します。[root] ノードを展開します。

ステップ 3 **[SPDM 証明書ポリシー（SPDM Certificate Policies）]** を右クリックして **[SPDM ポリシー（SPDM Policies の作成）]** を選択します。

ステップ 4 このポリシーの名前を入力し、セキュリティ レベルとして **[障害アラート設定（Fault Alert Setting）]** を選択します：これは **[無効（Disabled）]**、**[一部（Partial）]**、または **[完全（Full）]** のいずれかです。

デフォルトは **[一部（Partial）]** です。

ステップ 5 **[追加（Add）]**（**[ポリシーの作成（Create Policy）]** ウィンドウ）をクリックします。**[SPDM 証明書の追加（Add SPDM Certificate)]** ウィンドウが開きます。

ステップ 6 証明書に名前を付けます。

UCS Manager は、**Pem** 証明書のみをサポートします。

ステップ 7 [証明書（Certificate）] フィールドに証明書の内容を貼り付けます。

ステップ 8 **[OK]** をクリックして証明書を追加し、**[SPDM ポリシーの作成（Create SPDM Policy）]** ウィンドウに戻ります。

最大 40 件の証明書を追加できます。

ステップ 9 **[SPDM ポリシーの作成（Create SPDM Policy）]** メニューで、**[OK]** をクリックします。

SPDMポリシーを作成してから、サーバールートポリシーの下で**SPDM証明書ポリシー（SPDM Certificate Policy）]** を選択すると、アラート設定とともにすぐにリストに表示されます。

次のタスク

証明書をサービス プロファイルに割り当てます。サービス プロファイルを有効にするには、サービス プロファイルをサーバーに関連付ける必要があります。

セキュリティ ポリシーとサーバーの関連付け

始める前に

SPDM セキュリティ ポリシーの作成

手順

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 **[サービス プロファイル（Service Profiles）]** に移動します。[root] ノードを展開します。

ステップ 3 作成したポリシーに関連付けるサービス プロファイルを選択します。

a) **[ポリシー（Policies）]** タブで、下にスクロールして **[SPDM 証明書ポリシー（SPDM Certificate Policy）]**を展開します。**[SPDM 証明書ポリシー（SPDM Certificate Policy）]** ドロップダウンで、このサービスプロファイルに関連付ける目的のポリシーを選択します。

ステップ 4 [OK] をクリックします。

SPDM ポリシーがこのサービス プロファイルに関連付けられます。

次のタスク

障害アラート レベルをチェックして、目的の設定に設定されていることを確認します。

障害アラート設定の表示

特定のシャーシに関連付けられている障害アラート設定を表示できます。

始める前に

ポリシーを作成して、それとサービス プロファイルを関連付けることができます。

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインで **[機器（Equipment）]** をクリックします。

ステップ 2 ラックマウント サーバーを選択します。

ステップ 3 **[インベントリ（Inventory）]** タブで **[CIMC]** を選択します。.

ユーザーがアップロードした証明書が一覧表示され、特定の証明書の情報を選択して表示できます。

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。