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。

CLI を使用した SPDM セキュリティ証明書ポリシーの作成と構成

セキュリティ プロトコルおよびデータ モデル（SPDM）ポリシーを作成して、認証のためにセキュリティ アラート レベルと証明書の内容を BMC に提示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **create spdm-certificate-policy** *policy-name*	新しい SPDM セキュリティ証明書ポリシーを指定されたポリシー名で作成し、

	コマンドまたはアクション	目的
		組織 SPDM 証明書ポリシー モードを開始します。 （注） サポートされている証明書の種類は **pem** のみです。
ステップ 3	UCS-A /org/spdm-certificate-policy* # **set fault-alert** {**full** | **partial** | **no**}	このポリシーの障害アラート レベルを構成します。
ステップ 4	（任意） UCS-A /org/spdm-certificate-policy* # **set descr** *description*	SPDM セキュリティ証明書ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、 **show** コマンド出力の説明フィールドには表示されません。
ステップ 5	UCS-A /org/spdm-certificate-policy* # **create certificate** *certificate-name*	
ステップ 6	UCS-A /org/spdm-certificate-policy* # **set content**	これにより、外部証明書の内容を求めるプロンプトが表示されます。証明書の内容を 1 行ずつ入力します。証明書の終了後、プロンプトに ENDOFBUF と入力してコマンド ラインに戻ります。 （注） 証明書の内容をコミットせずに終了するには、**c** を入力します。
ステップ 7	UCS-A /org/spdm-certificate-policy # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

次のタスク

必要に応じて、外部のセキュリティ証明書を割り当てます。

セキュリティ ポリシー違反警告レベルの表示

ポリシーを作成したら、SPDM ポリシーのアラート レベルを確認できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /org/spdm-certificate-policy # **show fault-alert** 例： `UCS-A /server/cimc/spdm-certificate #show fault-alert`	返された結果は、この SPDM ポリシーの設定がデフォルトである [部分（Partial）] であることを示しています。 `SPDM Fault Alert Setting: Partial`

外部 SPDM セキュリティ証明書ポリシーのロード

SPDM を使用すると、外部のセキュリティ証明書をダウンロードできます。

始める前に

SPDM セキュリティ証明書ポリシーを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /org # **scope spdm-certificate-policy**	SPDM セキュリティ証明書ポリシーモードを開始します。
ステップ 2	UCS-A org/spdm-certificate-policy# **create spdm-cert** *Certificate name*	指定された外部証明書の SPDM セキュリティ証明書ポリシーを作成します。
ステップ 3	UCS-A /org/spdm-certificate-policy* # **set** {*certificate* }	証明書を指定すると、外部証明書の内容を求めるプロンプトが表示されます。サポートされている証明書の種類は pem のみです。
ステップ 4	UCS-A /org/spdm-certificate-policy # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

次の例は、PEM タイプの Broadcom の証明書をロードする方法を示しています。

例

```
UCS-A-FI-A /org/spdm-certificate-policy# create spdm-cert?
Name - Certificate name

UCS-A-FI-A /org/spdm-certificate-policy# create spdm-cert Broadcom
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert* # set?
certificate - Certificate content
```

```
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert* # set certificate
{enter certificate content}
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert* # commit-buffer
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert# show detail
SPDM Certificate:
Name: Broadcom
Certificate Type: pem
Certificate Content:
```

証明書インベントリの表示

アップロードされたSPDM証明書を表示し、指定された証明書の詳細を要求することもできます。

手順

	コマンドまたはアクション	目的
ステップ1	UCS-A # **scope server** *server*	
ステップ2	UCS-A/server # **scope cimc** *server*	
ステップ3	UCS-A/server/cimc # **scope spdm** *server*	
ステップ4	UCS-A/server/cimc/spdm # **show certificate**	返される結果は、証明書のインベントリを示しています。

ステップ5	UCS-A/server/cimc/spdm # **show certificate** *certificate-id***detail**
	例：
	`UCS-A /server/cimc/spdm-certificate #show certificate 3 detail`
	`Certificate Information`
	`Certificate Id : 3`
	`Subject Country Code (C) : US`
	`Subject State (ST) : Colorado`
	`Subject Organization (O) : Broadcom Inc.`
	`Subject Organization Unit(OU) : NA`
	`Subject Common Name (CN) : NA`
	`Issuer Country Code (C) : US`
	`Issuer State (ST) : Colorado`
	`Issuer City (L) : Colorado Springs`
	`Issuer Organization (O) : Broadcom Inc.`
	`Issuer Organization Unit(OU) : NA`
	`Issuer Common Name (CN) : NA`
	`Valid From : Oct 23 00:25:13 2019 GMT`
	`Valid To : Apr 8 10:36:14 2021 GMT`
	`UserUploaded : Yes`
	`Certificate Content : <Certificate String>`
		返される結果は、証明書ID、識別子、および有効期限を示しています。

	コマンドまたはアクション	目的
	`Certificate Type : PEM`	

ステップ 6	UCS-A /org/spdm-certificate-policy/certificate # **show**
	例：
	`SPDM Certificate:`
	`Name SPDM Certificate Type`
	`---------- ----------`
	`cert1 Pem`
	例：
	`UCS-A /server/cimc/spdm-certificate/certificate #up`
	`UCS-A /server/cimc/spdm-certificate #show`
	`SPDM Certificate Policy:`
	`Name Fault Alert Setting`
	`---------- ----------`
	`Broadcom Full`
		返される結果は、証明書の詳細の種類を示しています。
		返される結果は、障害アラートの設定を示しています。

SPDM ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、org-name に / と入力します。
ステップ 2	UCS-A /org # **delete spdm-certificate-policy** *policy-name*	指定された SPDM 制御ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例は、VendorPolicy2 という名前の電力制御ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete spdm-certificate-policy VendorPolicy2
UCS-A /org* # commit-buffer
UCS-A /org #
```

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。