コミュニケーション サービスの設定

この章の内容は、次のとおりです。

- HTTP の設定，1 ページ
- SSH の設定，2 ページ
- XML API の設定，3 ページ
- IPMI の設定，4 ページ
- SNMP の設定，6 ページ

HTTP の設定

はじめる前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。

ステップ 4 [HTTP Properties] 領域で、次のプロパティを更新します。

名前	説明
[HTTP/S Enabled] チェックボックス	HTTP および HTTPS が CIMC でイネーブルかディセーブルか。

名前	説明
[Redirect HTTP to HTTPS Enabled] チェックボックス	イネーブルにすると、HTTP 経由のすべての通信試行は、同等の HTTPS アドレスにリダイレクトされます。 HTTP をイネーブルにする場合は、このオプションをイネーブルにすることを強く推奨します。
[HTTP Port] フィールド	HTTP 通信に使用するポート。 デフォルトは 80 です。
[HTTPS Port] フィールド	HTTPS 通信に使用するポート。 デフォルトは 443 です。
[Session Timeout] フィールド	HTTP 要求の間、CIMC がタイム アウトしてセッションを終了するまで待機する秒数。 60 ～ 10,800 の範囲の整数を入力します。 デフォルトは 1,800 秒です。
[Max Sessions] フィールド	CIMC で許可されている HTTP および HTTPS の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	CIMC で現在実行されている HTTP および HTTPS セッションの数。

ステップ 5 [Save Changes] をクリックします。

SSH の設定

はじめる前に

SSH を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。

ステップ 4 [SSH Properties] 領域で、次のプロパティを更新します。

名前	説明
[SSH Enabled] チェックボックス	SSH が CIMC でイネーブルかディセーブルか。
[SSH Port] フィールド	セキュア シェル アクセスに使用するポート。 デフォルトは 22 です。
[SSH Timeout] フィールド	SSH 要求がタイムアウトしたものとシステムが判断するまで待機する秒数。 60 ～ 10,800 の範囲の整数を入力します。 デフォルトは 1,800 秒です。
[Max Sessions] フィールド	CIMC で許可されている SSH の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	CIMC で現在実行されている SSH セッションの数。

ステップ 5 [Save Changes] をクリックします。

XML API の設定

CIMC の XML API

Cisco CIMC XML アプリケーション プログラミング インターフェイス（API）は、C シリーズ ラックマウント サーバの CIMC に対するプログラミング インターフェイスです。 この API は、HTTP または HTTPS を使用して XML ドキュメントを受け取ります。

XML API の詳細については、『*Cisco UCS Rack-Mount Servers CIMC XML API Programmer's Guide*』を参照してください。

XML API のイネーブル化

はじめる前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。

ステップ 4 [XML API Properties] 領域で、次のプロパティを更新します。

名前	説明
[XML API Enabled] チェックボックス	このサーバで API アクセスが許可されているか、許可されていないか。
[Max Sessions] フィールド	CIMC で許可されている API の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	CIMC で現在実行されている API セッションの数。

ステップ 5 [Save Changes] をクリックします。

IPMI の設定

IPMI Over LAN

インテリジェント プラットフォーム管理インターフェイス（IPMI）では、サーバ プラットフォームに組み込まれているサービス プロセッサとのインターフェイスのためのプロトコルを定義しています。 このサービス プロセッサはベースボード管理コントローラ（BMC）と呼ばれ、サーバのマザーボードに存在します。 BMC は、メイン プロセッサおよびボード上の他の要素に、簡単なシリアル バスを使用してリンクします。

通常動作の間、IPMI は、サーバのオペレーティング システムがシステム ヘルスについての情報を取得し、システムのハードウェアを制御できるようにします。 たとえば、IPMI を使用すると、温度、ファンの速度、および電圧などのセンサーをモニタして、問題を事前に検出できます。 サーバの温度が指定されているレベルより高くなった場合、サーバのオペレーティング システムは BMC に対して、ファンの速度を上げたり、プロセッサの速度を下げたりして問題に対処するよう指示できます。

IPMI over LAN の設定

IPMI over LAN は、CIMC を IPMI メッセージで管理する場合に設定します。

はじめる前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。

ステップ 4 [IPMI over LAN Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enabled] チェックボックス	このサーバで IPMI アクセスが許可されているか、許可されていないか。
[Privilege Level Limit] ドロップダウン リスト	このサーバで IPMI セッションに割り当てることができる最も高い特権レベル。 次のいずれかになります。 • [read-only]：IPMI ユーザは情報を表示できますが、変更することはできません。 このオプションを選択すると、「Administrator」、「Operator」、または「User」ユーザ ロールを持つ IPMI ユーザは、その他の IPMI 特権に関係なく、読み取り専用 IPMI セッションのみを作成できます。 • [user]：IPMI ユーザは、一部の機能を実行できますが、管理タスクは実行できません。 このオプションを選択すると、「Administrator」または「Operator」ユーザ ロールを持つ IPMI ユーザは、このサーバでユーザおよび読み取り専用セッションを作成できます。 • [admin]：IPMI ユーザは、実行可能なすべてのアクションを実行できます。 このオプションを選択すると、「Administrator」ユーザ ロールを持つ IPMI ユーザは、このサーバで管理、ユーザ、および読み取り専用セッションを作成できます。
[Encryption Key] フィールド	IPMI 通信に使用する IPMI 暗号キー。

ステップ 5 [Save Changes] をクリックします。

SNMP の設定

SNMP

Cisco UCS C シリーズ ラックマウント サーバでは、サーバの設定とステータスの表示および SNMP トラップによる障害およびアラート情報の送信のために、簡易ネットワーク管理プロトコル（SNMP）がサポートされています。 CIMC でサポートされている管理情報ベース（MIB）ファイルの詳細については、次の URL にある『*MIB Quick Reference for Cisco UCS*』を参照してください。http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/reference/UCS_MIBRef.html

SNMP プロパティの設定

はじめる前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

ステップ 4 [SNMP Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enabled] チェックボックス	このサーバから指定されたホストまで SNMP トラップを送信するかどうか。
[SNMP Port] フィールド	サーバで SNMP ホストと通信するために使用するポート。 この値は変更できません。
[Access Community String] フィールド	CIMC が SNMP ホストに送信するトラップ メッセージに含まれるデフォルトの SNMP v1 または v2c コミュニティ名あるいは SNMP v3 ユーザ名。 最大 18 文字の文字列を入力します。
[System Contact] フィールド	SNMP 実装のシステム連絡先担当者。 電子メール アドレスまたは名前と電話番号など、最大 64 文字の文字列を入力します。

名前	説明
[System Location] フィールド	SNMPエージェント（サーバ）が実行されているホストの場所。 最大 64 文字の文字列を入力します。

ステップ 5 [Save Changes] をクリックします。

次の作業

SNMP トラップ設定の指定, （7 ページ）の説明に従って、SNMP トラップ設定を指定します。

SNMP トラップ設定の指定

はじめる前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

ステップ 4 [Common Trap Destination Settings] 領域で、次のフィールドに入力します。

名前	説明
[Trap Community String] フィールド	トラップ情報の送信先となるSNMPコミュニティグループの名前。
[SNMP Version] ドロップダウンリスト	トラップに使用されるSNMPバージョンとモデル。 次のいずれかになります。 • V1 • V2 • V3
[Type] フィールド	バージョンとして[V2]を選択した場合、このタイプのトラップが送信されます。 次のいずれかになります。 • Trap • Inform

ステップ 5 [Trap Destinations] 領域で、次のフィールドに入力します。

名前	説明
[ID] カラム	トラップの宛先 ID。 この値は変更できません。
[Enabled] カラム	使用する SNMP トラップの宛先ごとに、このカラムの対応するチェックボックスをオンにします。
[Trap Destination IP Address] カラム	SNMP トラップ情報の送信先の IP アドレス。

ヒント トラップの設定を変更したり、テスト トラップ メッセージを送信したりする場合、管理者はテーブルのトラップ行をクリックできます。

ステップ 6 [Save Changes] をクリックします。

SNMP テスト トラップ メッセージの送信

はじめる前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Event Management] をクリックします。

ステップ 3 [Event Management] ペインの [Trap Settings] タブをクリックします。

ステップ 4 [Trap Destinations] 領域で、目的の SNMP トラップの宛先の行をクリックします。
[Traps Details] ダイアログボックスが開きます。

ステップ 5 [Send SNMP trap] をクリックします。
SNMPv1 テスト トラップ メッセージがトラップの宛先に送信されます。

（注） テスト メッセージを送信するには、トラップが設定され、イネーブルである必要があります。

SNMPv3 ユーザの管理

はじめる前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- SNMP がイネーブルである必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

ステップ 4 [SNMPV3 Users] 領域で、次のプロパティを更新します。

名前	説明
[Add] ボタン	テーブルで使用可能な行をクリックし、このボタンをクリックして新しい SNMP ユーザを追加します。
[Modify] ボタン	テーブルで変更するユーザを選択し、このボタンをクリックして選択した SNMP ユーザを変更します。
[Delete] ボタン	テーブルで削除するユーザを選択し、このボタンをクリックして選択した SNMP ユーザを削除します。
[ID] カラム	システムによって SNMP ユーザに割り当てられた ID。
[Name] カラム	SNMP ユーザ名。
[Auth Type] カラム	ユーザ認証タイプ。
[Privacy Type] カラム	ユーザ プライバシー タイプ。

ステップ 5 [Save Changes] をクリックします。

SNMPv3 ユーザの設定

はじめる前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

- SNMP がイネーブルである必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

ステップ 4 [SNMPV3 Users] 領域で、次のアクションのいずれかを実行します。

- 既存のユーザをテーブルから選択し、[Modify] をクリックします。
- [Add] をクリックし、新しいユーザを作成します。

（注） ボタンがディセーブルの場合は、SNMP をイネーブルにして [Save Changes] をクリックします。

ステップ 5 [SNMPV3 User Details] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[ID] フィールド	ユーザの固有識別情報。 このフィールドは変更できません。
[Name] フィールド	SNMP ユーザ名。
[Security Level] ドロップダウンリスト	このユーザのセキュリティ レベル。 次のいずれかになります。 • [no auth, no priv]：ユーザには許可パスワードまたはプライバシー パスワードが必要ありません。 • [auth, no priv]：ユーザには許可パスワードが必要ですが、プライバシーパスワードは必要ありません。 このオプションを選択すると、CIMC で後述の許可フィールドがイネーブルになります。 • [auth, priv]：ユーザには許可パスワードとプライバシー パスワードの両方が必要です。 このオプションを選択すると、CIMC で許可フィールドとプライバシー フィールドがイネーブルになります。
[Auth Type] フィールド	許可タイプ。 次のいずれかになります。 • MD5 • SHA
[Auth Password] フィールド	この SNMP ユーザの許可パスワード。

名前	説明
[Confirm Auth Password] フィールド	確認のための許可パスワードの再入力。
[Privacy Type] フィールド	プライバシー タイプ。 次のいずれかになります。 • DES • AES
[Privacy Password] フィールド	この SNMP ユーザのプライバシー パスワード。
[Confirm Privacy Password] フィールド	確認のための許可パスワードの再入力。

ステップ 6 [Save Changes] をクリックします。