コミュニケーション サービスの設定

この章は、次の項で構成されています。

- 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] メニューをクリックします。

ステップ 2 [Admin] メニューの [Communication Services] をクリックします。

ステップ 3 [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 Cisco IMC でイネーブルかどうか。
[Redirect HTTP to HTTPS Enabled] チェックボックス	イネーブルの場合、HTTP 経由で試行される通信はすべて同等の HTTPS アドレスにリダイレクトされます。 HTTPをイネーブルにしている場合は、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。

名前	説明
[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、Cisco IMC 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	Cisco IMC 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	Cisco IMC 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 4 [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] メニューをクリックします。

ステップ 2 [Admin] メニューの [Communication Services] をクリックします。

ステップ 3 [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 Cisco IMC でイネーブルかどうか。
[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。

名前	説明
[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	Cisco IMC 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	現在 Cisco IMC で実行されている SSH セッションの数。

ステップ 4 [Save Changes] をクリックします。

XML API の設定

Cisco IMC 用の XML API

Cisco Cisco IMC 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 サーバ用の Cisco IMC に対するプログラマチック インターフェイスです。この API は、HTTP または HTTPS 経由で 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 Cisco IMC 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] メニューをクリックします。

ステップ 2 [Admin] メニューの [Communication Services] をクリックします。

ステップ 3 [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どうか。
[Max Sessions] フィールド	Cisco IMC 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	現在 Cisco IMC で実行されている API セッションの数。

ステップ 4 [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、Cisco IMC 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] メニューをクリックします。

ステップ 2 [Admin] メニューの [Communication Services] をクリックします。

ステップ 3 [IPMI over LAN Properties] 領域で、BMC 1、BMC 2、CMC 1、CMC 2 の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どうか。
[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可能な最高特権レベル。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した場合、「Administrator」、「Operator」、または「User」ユーザ ロールを持つ IPMI ユーザが作成できるのは、読み取り専用の IPMI セッションだけです。それ以外に所持している IPMI 特権は関係ありません。 • [user]：IPMI ユーザはいくつか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した場合、「Administrator」または「Operator」ユーザ ロールを持つ IPMI ユーザがこのサーバで作成できるのは、ユーザ セッションと読み取り専用セッションだけです。 • [admin]：IPMI ユーザは使用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した場合、「Administrator」ユーザ ロールを持つ IPMI ユーザは、管理者、ユーザ、および読み取り専用セッションをこのサーバで作成できます。
[Encryption Key] フィールド	IPMI 通信に使用する IPMI 暗号キー。
[Randomize] ボタン	IPMI 暗号化キーをランダムな値に変更できます。

ステップ 4 [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 は、サーバの設定およびステータスを表示したり、SNMP トラップによって障害とアラートを送信したりするために、簡易ネットワーク管理プロトコル（SNMP）をサポートしています。Cisco IMC 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/c/en/us/td/docs/unified_computing/ucs/sw/mib/b-series/b_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] メニューをクリックします。

ステップ 2 [Admin] メニューの [Communication 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
[SNMP Enabled] チェックボックス	このサーバが指定のホストに SNMP トラップを送信するかどうか。 （注） このチェックボックスをオンにしたら、SNMP ユーザまたはトラップを設定する前に、[Save Changes] をクリックする必要があります。
[SNMP Port] フィールド	Cisco IMC SNMP エージェントが動作するポート。 1 ～ 65535 の範囲内の SNMP ポート番号を入力します。デフォルト ポート番号は、161 です。 （注） システム コールに予約済みのポート番号（たとえば 22、23、80、123、443、623、389、636、3268、3269、2068 など）は、SNMP ポートとして使用できません。
[Access Community String] フィールド	Cisco IMC が任意の SNMP に含めるデフォルトの SNMP v1 または v2c コミュニティ名により、動作が実行されます。 最大 18 文字の文字列を入力します。

名前	説明
[SNMP Community Access] ドロップダウン リスト	次のいずれかになります。 • [Disabled]：このオプションは、インベントリ テーブルの情報へのアクセスをブロックします。 • [Limited]：このオプションは、インベントリ テーブルの情報の読み取りアクセスが部分的に提供します。 • [Full]：このオプションは、インベントリ テーブルの情報の読み取りフル アクセスを提供します。 （注） SNMP コミュニティ アクセスは、SNMP v1 および v2c ユーザのみに適用されます。
[Trap Community String] フィールド	他のデバイスに SNMP トラップを送信するために使用される SNMP コミュニティ グループの名前。 最大 18 文字の文字列を入力します。 （注） このフィールドは、SNMP v1 および v2c ユーザのみに表示されます。SNMP v3 ユーザは、SNMP v3 クレデンシャルを使用する必要があります。
[System Contact] フィールド	SNMP の実装を担当するシステムの連絡先。 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。
[System Location] フィールド	SNMP エージェント（サーバ）が実行するホストの場所。 最大 64 文字の文字列を入力します。
[SNMP Input Engine ID] フィールド	ユーザ定義の一意の静的エンジン ID。
[SNMP Engine ID] フィールド	管理用デバイスを識別する一意の文字列。[SNMP Input Engine ID] が定義されている場合は、その値から文字列が生成されます。そうでない場合は、BMC シリアル番号から派生します。

ステップ 5 [Save Changes] をクリックします。

次の作業

SNMP トラップを設定します。

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] メニューをクリックします。

ステップ 2 [Admin] メニューの [Communication 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 [Trap Destinations] タブをクリックします。

ステップ 5 [Trap Destinations] 領域で、次のいずれかを実行できます。

- テーブルから既存のユーザを選択し、[Modify Trap] をクリックします。
- 新しいユーザを作成するには、[Add Trap] をクリックします。

（注） フィールドが強調表示されていない場合は、[Enabled] を選択します。

ステップ 6 [Trap Details] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[ID] フィールド	トラップの宛先 ID。この値は変更できません。
[Enabled] ドロップダウン リスト	オンにすると、このトラップがサーバでアクティブになります。
[Version] ドロップダウン リスト	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 • V2 • V3
[Trap Type] ドロップダウン リスト	送信するトラップのタイプ。次のいずれかになります。 • [Trap]：このオプションを選択すると、トラップが宛先に送信されますが、通知は受信しません。 • [Inform]：V2 ユーザに対してのみこのオプションを選択できます。これを選択すると、宛先でトラップが受信されたときに通知を受け取ります。

名前	説明
[User] ドロップダウン リスト	ドロップダウン リストに使用可能なすべてのユーザが表示されます。そのリストからユーザを選択します。
[Trap Destination Address] フィールド	SNMP トラップ情報の送信先のアドレス。トラップの宛先としてIPv4またはIPv6アドレスまたはドメイン名を設定できます。
[Port]	サーバがトラップの宛先との通信に使用するポート。 1 ～ 65535 の範囲内のトラップの宛先のポート番号を入力します。

ステップ 7 [Save Changes] をクリックします。

ステップ 8 トラップの宛先を削除する場合は、行を選択し、[Delete] をクリックします。
削除の確認プロンプトで、[OK] をクリックします。

テスト SNMP 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] メニューをクリックします。

ステップ 2 [Admin] メニューの [Communication Services] をクリックします。

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

ステップ 4 [Trap Destinations] 領域で、目的の SNMP トラップ宛先の行を選択します。

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

（注） テスト メッセージを送信するために、トラップは設定済みで、イネーブルにされている必要があります。

SNMP 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] メニューをクリックします。

ステップ 2 [Admin] メニューの [Communication 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 [User Settings] 領域で、次のプロパティを更新します。

名前	説明
[AddUser] ボタン	テーブル内で使用できる行をクリックし、このボタンをクリックして新規の SNMP ユーザを追加します。
[ModifyUser] ボタン	テーブル内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。
[DeleteUser] ボタン	テーブル内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	SNMP ユーザに対してシステムが割り当てる識別子。
[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。

SNMP 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] メニューをクリックします。

ステップ 2 [Admin] メニューの [Communication 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 [User Settings] 領域で、次のいずれかの操作を実行します。

- テーブルから既存のユーザを選択し、[Modify User] をクリックします。
- [Users] 領域で行を選択し、[Add User] をクリックして新しいユーザを作成します。

ステップ 5 [SNMP 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。 1 ～ 31 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[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]：このユーザには、許可パスワードもプライバシー パスワードも不要です。 • [auth, no priv]：このユーザには、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不要です。このオプションを選択すると、Cisco IMC は後述の Auth フィールドをイネーブルにします。 • [auth, priv]：このユーザには、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、Cisco IMC は Auth フィールドおよび Privacy フィールドをイネーブルにします。
[Auth Type] オプション ボタン	許可タイプ。次のいずれかになります。 • MD5 • SHA

名前	説明
[Auth Password] フィールド	この SNMP ユーザの許可パスワード。 8 ～ 64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[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] オプション ボタン	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。 8 ～ 64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[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。

ステップ 7 ユーザを削除する場合は、ユーザを選択し、[Delete User] をクリックします。
削除の確認プロンプトで、[OK] をクリックします。