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）
- Configuring SSH （2 ページ）
- XML API の設定 （3 ページ）
- Redfish の有効化 （4 ページ）
- Configuring IPMI （5 ページ）
- Configuring SNMP （6 ページ）
- 電子メール アラートを SMTP で送信するようにサーバを設定 （13 ページ）

HTTP の設定

始める前に

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 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [HTTP プロパティ（HTTP Properties）] 領域で、次のプロパティを更新します。

名前	説明
[HTTP/S 有効（HTTP/S Enabled）] チェックボックス	HTTP および HTTPS が Cisco IMC で有効かどうか。
[HTTP の HTTPS へのリダイレクトを有効（Redirect HTTP to HTTPS Enabled）] チェックボックス	有効の場合、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 を有効にしている場合は、このオプションを有効にすることを強く推奨します。

名前	説明
[HTTP ポート（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 ポート（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。
[セッション タイムアウト（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 の整数を入力します。デフォルトは 1,800 秒です。
[最大セッション数（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。
[アクティブなセッション（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 [変更の保存（Save Changes）] をクリックします。

Configuring SSH

始める前に

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 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [SSH プロパティ（SSH Properties）] 領域で、次のプロパティを更新します。

名前	説明
[SSH 有効（SSH Enabled）] チェックボックス	SSH が Cisco IMC で有効かどうか。
[SSH ポート（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。デフォルト値は 22 です。

名前	説明
[SSH タイムアウト（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 の整数を入力します。デフォルトは 1,800 秒です。
[最大セッション数（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。
[アクティブなセッション（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 [変更の保存（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 の有効化

始める前に

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 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [XML API プロパティ（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 有効（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。
[最大セッション数（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。
[アクティブなセッション（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 [変更の保存（Save Changes）] をクリックします。

Redfish の有効化

始める前に

このアクションを実行するには、admin としてログオンする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [コミュニケーション サービス（Communications Services）] をクリックします。

ステップ 3 [Redfishプロパティ（SSH Properties）] 領域で、次のプロパティを更新します。

名前	説明
[XML API 有効（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。
[最大セッション数（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。
[アクティブなセッション（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 [変更の保存（Save Changes）] をクリックします。

Configuring IPMI

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。

（注） 暗号キーを発行しないで IPMI コマンドを実行する場合は、Cisco IMC で、[暗号キー（Encryption Key）] フィールドを偶数個のゼロに設定し保存します。これにより、暗号キーを含めることなく IPMI コマンドを発行できます。

始める前に

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 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [IPMI over LAN プロパティ（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
[有効（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。

名前	説明
[特権レベルの制限（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。 • [読み取り専用（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。 • [ユーザ（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。 • [管理者（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。
[暗号化キー（Encryption Key）] フィールド	IPMI 通信に使用する IPMI 暗号キー。
[ランダム化（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 [変更の保存（Save Changes）] をクリックします。

Configuring SNMP

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

始める前に

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 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [コミュニケーション サービス（Communications Services）] ウィンドウの [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 有効（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、[変更内容を保存（Save Changes）] をクリックする必要があります。
[SNMP ポート（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。デフォルトのポート番号は 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。
[アクセス コミュニティ ストリング（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 コミュニティ アクセス（SNMP Community Access）] ドロップダウン リスト	次のいずれかになります。 • [無効（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。 • [制限付き（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を部分的に提供します。 • [フル（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。
[トラップ コミュニティ ストリング（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。
[システム連絡先（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。
[システム ロケーション（System Location）] フィールド	SNMP エージェント（サーバ）が動作するホストの場所。 最大 64 文字の文字列を入力します。
[SNMP 入力エンジン ID（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 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 入力エンジン ID（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 [変更の保存（Save Changes）] をクリックします。

次のタスク

SNMP トラップを設定します。

SNMP トラップ設定の指定

始める前に

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 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [コミュニケーション サービス（Communications Services）] ウィンドウの [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 [トラップ宛先（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、[トラップの変更（Modify Trap）] をクリックします。
- 新しいユーザを作成するには、[トラップの追加（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、[有効（Enabled）] を選択します。

ステップ 6 [トラップの詳細（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。
[有効（Enabled）] チェックボックス 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。
[バージョン（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**
[トラップタイプ（Trap Type）] オプション ボタンドロップダウン 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。 • [トラップ（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。 • [伝達（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
[ユーザ（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。
[トラップ宛先アドレス（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宛先ポート番号を入力します。

ステップ 7 [変更の保存（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、[削除（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

始める前に

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 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [通信サービス（Communication Services）] ウィンドウの [SNMP] をクリックします。

ステップ 4 [トラップ宛先（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 [SNMP テスト トラップの送信（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、有効にされている必要があります。

SNMP ユーザの管理

始める前に

- 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 が有効である必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [コミュニケーション サービス（Communications Services）] ウィンドウの [SNMP] タブをクリックします。

ステップ 4 [ユーザ設定（User Settings）] 領域で、次のプロパティを更新します。

名前	説明
[ユーザの追加（Add User）] 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。
[ユーザの変更（Modify User）] 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。
[ユーザの削除（Delete User）] 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。
[名前（Name）] カラム	SNMP ユーザ名。
[認証タイプ（Auth Type）] カラム	ユーザ認証タイプ。
[プライバシー 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 [変更の保存（Save Changes）] をクリックします。

SNMP ユーザの設定

始める前に

- 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 が有効である必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ウィンドウの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [コミュニケーション サービス（Communications Services）] ウィンドウの [SNMP] タブをクリックします。

ステップ 4 [ユーザ設定（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、[ユーザの変更（Modify User）] をクリックします。
- [ユーザ（Users）] 領域で行を選択し、[ユーザの追加（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 ユーザの詳細（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。
[名前（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。
[セキュリティ レベル（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 フィールドを有効にします。 • [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 フィールドを有効にします。
[認証タイプ（Auth Type）] ドロップダウン	許可タイプ。次のいずれかになります。 • **MD5** • **SHA**

名前	説明
[認証パスワード（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。
[認証パスワードの確認（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。
[プライバシー タイプ（Privacy Type）] ドロップダウン	プライバシー タイプ。次のいずれかになります。 • **[DES]** • **AES**
[プライバシー パスワード（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。
[プライバシーパスワードの確認（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 [変更の保存（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、[ユーザの削除（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。

電子メール アラートを SMTP で送信するようにサーバを設定

Cisco IMC は、SNMP に依存せずに、電子メール ベースのサーバ障害通知を受信者に送信できます。システムは簡易メール転送プロトコル（SMTP）を使用して、設定されている SMTP サーバに電子メール アラートとしてサーバ障害を送信します。

最大 4 人の受信者に対応しています。

電子メール アラートの受信用に SMTP サーバを設定

サーバ障害に関するメール通知を受信できるように、SMTP のプロパティを設定し、[メール アラート（Mail Alert）] タブで電子メール受信者を追加します。

始める前に

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

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [コミュニケーション サービス（Communications Services）] ペインで、[メール アラート（Mail Alert）] タブをクリックします。

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

名前	説明
[SMTP の有効化（SMTP Enabled）] チェックボックス	オンにすると、SMTP サービスが有効になります。
[SMTP サーバ アドレス（SMTP Server Address）] フィールド	SMTP サーバのアドレスを入力できます。
[SMTP ポート（SMTP Port）] フィールド	SMTP ポートの番号を入力できます。デフォルトのポート番号は 25 です。
[報告する最小重大度（Minimum Severity to Report）] ドロップダウン リスト	電子メール アラートを受信する最小重大度レベルを選択できます。次のいずれかになります。 • 条件 • 警告 • [マイナー（Minor）] • [メジャー（Major）] • クリティカル（Critical） 最小重大度レベルを選択すると、そのレベルとそれ以上のレベルに該当する場合にメール アラートが送信されます。たとえば、最小重大度レベルとして [マイナー（Minor）] を選択した場合は、マイナー、メジャー、およびクリティカルな障害イベントが発生したときに電子メール アラートを受信できます。

ステップ 5 [SMTP 受信者（SMTP Recipients）] 領域で、次の手順を実行します。

a) [追加 (+)（Add (+)）] ボタンをクリックし、通知の送信先となる電子メール受信者を追加します。メール ID を入力し、[保存（Save）] をクリックします。

電子メール受信者を削除するには、電子メール受信者を選択して [削除 (X)（Delete (X)）] ボタンをクリックします。

b) 追加した電子メール受信者に到達可能かどうかを確認するには、[テスト メールの送信（Send Test Mail）] をクリックします。
電子メールアドレスおよびSMTPの設定が有効な場合は、電子メールが送信されたことを示すメッセージが確認ポップアップ ウィンドウに表示されます。設定が無効な場合は、電子メールが送信されなかったことを示すメッセージが確認ポップアップ ウィンドウに表示されます。[到達可能性（Reachability）] カラムは、電子メール受信者にテスト メールが正常に送信されたかどうかを示します。[到達可能性（Reachability）] カラムには次のいずれかの値が示されます。

- [はい（Yes）]（テスト メールが正常に送信された場合）
- [いいえ（No）]（テスト メールが正常に送信されなかった場合）
- [na]（テスト メールの送信が実行されなかった場合）

ステップ 6 [変更の保存（Save Changes）] をクリックします。

トラブルシューティング

次の表では、（到達可能性ステータスが [なし（No）] の場合に）Cisco IMC ログに表示される可能性のある SMTP メールアラートの設定の問題に対するトラブルシューティング上の推奨事項を説明しています。

問題	推奨されるソリューション
タイムアウトに達しました	設定されている SMTP の IP アドレスに到達できない場合に発生する可能性があります。有効な IP アドレスを入力してください。
ホスト名を解決できませんでした	設定されている SMTP ドメイン名に到達できない場合に発生する可能性があります。有効なドメイン名を入力します。
サーバに接続できませんでした	SMTP の IP、ドメイン名、またはポート番号が正しく設定されていない場合に発生する可能性があります。有効な設定の詳細を入力します。
ピアへのデータ送信に失敗しました	無効な受信者の電子メール ID が設定されている場合に発生する可能性があります。有効な電子メール ID を入力します。

SMTP 電子メール受信者の追加

サーバ障害に関するメール通知を受信できるように、[メール アラート（Mail Alert）] タブで電子メール受信者を追加します。

始める前に

- 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。
- [SMTP プロパティ（SMTP Properties）] 領域で SMTP サーバのプロパティを設定します。電子メール アラートの受信用に SMTP サーバを設定 （14 ページ）を参照してください。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [コミュニケーション サービス（Communications Services）] ペインで、[メール アラート（Mail Alert）] タブをクリックします。

ステップ 4 [SMTP 受信者（SMTP Recipients）] 領域で、次の手順を実行します。

a) [追加 (+)（Add (+)）] ボタンをクリックし、通知の送信先となる電子メール受信者を追加します。メール ID を入力し、[保存（Save）] をクリックします。

b) 追加した電子メール受信者に到達可能かどうかを確認するには、[テスト メールの送信（Send Test Mail）] をクリックします。
電子メールアドレスおよびSMTPの設定が有効な場合は、電子メールが送信されたことを示すメッセージが確認ポップアップ ウィンドウに表示されます。設定が無効な場合は、電子メールが送信されなかったことを示すメッセージが確認ポップアップ ウィンドウに表示されます。[到達可能性（Reachability）] カラムは、電子メール受信者にテスト メールが正常に送信されたかどうかを示します。[到達可能性（Reachability）] カラムには次のいずれかの値が示されます。

- [はい（Yes）]（テスト メールが正常に送信された場合）
- [いいえ（No）]（テスト メールが正常に送信されなかった場合）
- [na]（テスト メールの送信が実行されなかった場合）