コミュニケーション サービスの設定

この章は、次の内容で構成されています。

TLS v1.2 の有効化または無効化

リリース 4.2 (2a) 以降、Cisco IMC は TLS v1.2 の無効化と、v1.2 と v1.3 の両方の暗号値のカスタマイズをサポートしています。

始める前に

[セキュリティの設定（Security Configuration）] の **[CC]**（コモンクライテリア）が有効になっている場合、TLS v1.2 を無効にすることはできません。TLS v1.2 を無効にする前に、**[CC]** が無効になっていることを確認してください。

TLS v1.2 を有効または無効にすると、vKVM、Web サーバー、XML API、および Redfish API セッションが再起動します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（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 **[TLS 構成（TLS Configuration）]** エリアで、次のプロパティを更新します。

名前	説明
TLS v1.2 を有効にするチェックボックス	Cisco IMC で TLS v1.2 が有効になっているかどうか。 （注） TLS v1.2 を有効または無効にすると、vKVM、Web サーバー、XML API、および Redfish API セッションが再起動します。 （注） **[セキュリティの設定（Security Configuration）]** の **[CC]**（コモンクライテリア）が有効になっている場合、TLS v1.2 を無効にすることはできません。
[TLSバージョンの構成（Configured TLS Version）] フィールド	Cisco IMC でサポートされる TLS バージョン。 このフィールドはユーザーが構成できません。ここに表示される値は、**[TLS v1.2 を有効にする]** チェック ボックスで選択した値によって異なります。
TLS v1.2 暗号モードドロップダウン リスト	TLS v1.2 が有効になっている場合、希望の暗号モードを選択できます。次のいずれかになります。 • **高** • **中** • **低** （注） **セキュリティ構成**で **FIPS** が有効になっている場合、**低**モードを選択することはできません。 • **カスタム** — カスタム暗号値を入力できます。 カスタム暗号フィールドで提供される特定の暗号の OpenSSL の同等の暗号名については、https://www.openssl.org/docs/man1.0.2/man1/ciphers.html を参照してください。 例： **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** を設定するには、暗号リストの **ECDHE-RSA-AES256-GCM-SHA384** 入力を入力として提供します。

名前	説明
[TLS v1.2暗号リスト] フィールド	**[TLS v1.2 暗号モード]** ドロップダウン リストで選択した値に基づいて、暗号のリストを表示します。**TLS v1.2 暗号モード**を**カスタム**として選択した場合、暗号値を編集できます。 （注） FIPS が有効になっている場合、FIPS でサポートされていない暗号を設定することはできません。 （注） 入力された暗号値が無効またはサポートされていない場合、設定の保存中に、Cisco IMC は自動的に**TLS v1.2 暗号モード**の値を**高**に変更し、設定を保存します。次に例を示します。 **DH-RSA-AES256-GCM-SHA384** が設定されている場合、**TLS v1.2 暗号化モード**は自動的に**高**に設定されます 設定を保存した後、Cisco IMC は **TLS v1.2 暗号リスト** フィールドを無効にし、マウスを **TLS v1.2 カスタム暗号ステータス** アイコンの上に置くと、次のようなエラー メッセージが表示されます。 `TLS v1.2 カスタム暗号ステータス: エラー: 無効またはサポートされていない TLS v1.2 暗号リストを構成しています-' Cipher_Name '。TLS v1.2 暗号モードを高に設定します。`
TLS v1.3暗号スイート フィールド	TLS v1.3 の暗号値を編集できます。 （注） FIPS が有効になっている場合、FIPS でサポートされていない暗号を設定することはできません。

HTTP の設定

リリース 4.1(2b) 以降、Cisco IMC は個別の HTTPS および HTTP 通信サービスをサポートします。この機能を使用して無効にできるのは HTTP サービスのみです。

この機能は、次のサーバーでのみサポートされています。

- Cisco UCS C220 M5
- Cisco UCS C240 M5
- Cisco UCS C480 M5
- Cisco UCS C480 ML M5

- Cisco UCS C240 SD M5
- Cisco UCS C125 M5

（注） 4.1(2b) より以前のリリースで **[HTTP を HTTPS にリダイレクトすることを有効化する（Redirect HTTP to HTTPS Enabled）]** が無効になっている場合、4.1(2b) 以降のリリースにアップグレードすると、システムによって **[HTTP 有効化（HTTP Enabled）]** の値が **[無効（Disabled）]** に設定されます。

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）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [通信サービス（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
[HTTPS 有効（HTTPS Enabled）] チェックボックス	警告 このオプションを無効にすると、終了 Cisco IMC Web GUI セッションが終了します。このオプションを無効にすると、Cisco IMC への HTTP サービスと HTTPS サービスの両方が無効になります。 このオプションは、HTTPS サービスのみが Cisco IMC にアクセスできるようにします。
[HTTP 有効（HTTP Enabled）] チェックボックス	警告 このオプションの変更を正常に保存するには、Cisco IMC Web GUI は自動的に再起動されます。管理コントローラとの通信が一時的に失われ、再起動後に再度ログインする必要があります。 このオプションは、HTTP サービスのみが Cisco IMC にアクセスできるようにします。 （注） HTTPS を無効にすると、Cisco IMC にアクセスするための HTTP サービスも無効になります。

名前	説明
[Redirect HTTP to HTTPS Enabled] チェックボックス	（注） このオプションは、[HTTP 有効（HTTP Enabled）] がオンの場合にのみ適用されます。 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。
[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

始める前に

SSH を設定するには、admin 権限を持つユーザー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）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）] メニューで [通信サービス（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。
[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 サーバー用の 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

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）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）] メニューで [通信サービス（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。

Redfish のイネーブル化

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 [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 [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 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。

（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。
- 最大 4 個の同時 IPMI セッションのみ許可されています。

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）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [通信サービス（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
[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。
[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、管理者（Administrator）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。
[ランダム化（Randomize）] ボタン	IPMI 暗号化キーを乱数値に変更できます。

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 サポートされている Management Information Base（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

リリース 4.1（3b） 以降、Cisco IMC では SNMP v3 バージョンの拡張認証プロトコルが導入されています。

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）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [通信サービス（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 ユーザー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 v2c が有効化されている（SNMP v2c Enabled）] チェックボックス	SNMP v2c バージョンを有効または無効にすることができます。
[SNMP v3 が有効化されている（SNMP v3 Enabled）] チェックボックス	SNMP v3 バージョンを有効または無効にすることができます。
[SNMP Port] フィールド	Cisco IMC SNMP エージェントを実行するポート。 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 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（SNMP Community Access）] 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 ユーザーのみに表示されます。SNMP v3 バージョンは 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 アドレスや名前、電話番号など、最大 254 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（サーバー）が実行するホストの場所。 最大 254 文字の文字列を入力します。
[SNMP Input Engine ID] フィールド	ユーザが定義した静的エンジンの一意の ID。
[SNMP エンジン ID（SNMP Engine ID）] フィールド	管理目的でデバイスを識別する固有の文字列。これは、[SNMP 入力エンジン ID（SNMP Input Engine ID）] がすでに定義されている場合はこの ID から生成され、それ以外の場合は BMC シリアル番号から生成されます。

ステップ 5 [Save Changes] をクリックします。

次のタスク

SNMP トラップ設定を指定します。

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）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [通信サービス（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 [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。
- [トラップの追加（Add Trap）] をクリックして新しいユーザを作成します。

（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 [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 check box	オンにすると、このトラップがサーバー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ても、通知を受信することはありません。 • [通知する（Inform）] : このオプションは、V2 ユーザに対してのみ選択できます。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ーが表示されます。そのリストからユーザーを選択します。 （注） SNMP v3 バージョンの構成時に、暗号化方式が **DES** に設定された SNMP ユーザーは、ドロップダウン リストに表示されません。
[トラップの宛先アドレス（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、[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）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [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）] ペインで [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 **[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、イネーブルにされている必要があります。

Cisco USC C シリーズ M7 および以降のサーバー向け SNMP ユーザーの管理

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 [管理（Admin）] メニューで [通信サービス（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 **[v3 ユーザー設定（v3 User Settings）]**エリアで、**[ここをクリックしてユーザー構成を変更します（CLICK HERE to change the Users configurations）]**

ユーザー設定の変更のためには、Cisco USC C シリーズ M7 および以降のサーバー向けローカル ユーザーの追加を参照してください。

SMTP を使用して電子メール アラートを送信するようにサーバーを設定する

Cisco IMC は、SNMP に依存せずに受信者に対する電子メール ベースのサーバー障害の通知をサポートします。システムは Simple Mail Transfer Protocol（SMTP）を使用して、設定された SMTP サーバーに電子メール アラートとしてサーバー障害を送信します。

最大 4 人の受信者がサポートされます。

電子メール アラートを受信するための SMTP サーバーの設定

サーバー障害に関する電子メール通知を受信するように、[Mail Alert] タブで SMTP プロパティを設定し、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 権限を持つユーザー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 [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 [Mail Alert] タブをクリックします。

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

名前	説明
[SMTP を有効にする（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 アドレスを入力できます。
[SMTP ポート（SMTP Port）] フィールド	SMTP ポート番号を入力できます。デフォルトのポート番号は 25 です。
SMTP送信元アドレス	送信される SMTP メール アラートの送信元アドレスを設定できます。ここで入力するメール アドレスは、受信するすべてのSMTPメール アラートの送信元アドレス（メール送信者のアドレス）として表示されます。 （注） これはオプションのフィールドです。このフィールドに電子メールアドレスを入力しない場合、デフォルトで、サーバーのホスト名 ID が送信元アドレス（メール送信者のアドレス）として表示されます。

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

a) [Add (+)] ボタンをクリックして、通知の送信先としての電子メール受信者を追加します。電子メール ID を入力して、[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、[Delete (X)] ボタンをクリックします。

b) **[最小シビラティ（重大度）レベル（最小シビラティ（重大度）レベル）]**ドロップダウン リスト電子メールアラートを受信するための最小シビラティ（重大度）レベルを選択できます：次のいずれかになります。

- の条件
- 警告
- マイナー
- メジャー
- 重大

最小シビラティ（重大度）レベルを選択した場合、そのレベルと、それよりも高い他のシビラティ（重大度）レベルについてメールアラートが送信されます。たとえば、最小シビラティ（重大度）レベルとして「Minor」を選択すると、マイナー、メジャー、およびクリティカルな障害イベントに関する電子メール アラートが送信されます。

c) [Send Test Mail] をクリックして、追加した電子メール受信者に到達可能であるかどうかを確認します。
電子メール アドレスと SMTP 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とともに確認ポップアップ ウィンドウが表示されます。設定が有効でない場合は、電子メールが送信されていないことを示すメッセージとともに確認ポップアップ ウィンドウが表示されます。[Reachability]カラムは、テストメールが電子メール受信者に正常に送信されたかどうかを示します。[Reachability] カラムの値は次のいずれかになります。

- [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ていない場合）
- [na]（テスト メールが送信されていない場合）

ステップ 6 [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。
サーバーに接続できませんでした	SMTP IP または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、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

サーバー障害に関する電子メール通知を受信するように、[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 権限を持つユーザーとしてログインする必要があります。

- [SMTP Properties] 領域で、SMTP サーバー プロパティを設定します。電子メール アラートを受信するための SMTP サーバーの設定 （14 ページ）を参照してください。

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 [Mail Alert] タブをクリックします。

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

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

b) **[最小シビラティ（重大度）レベル（最小シビラティ（重大度）レベル）]**ドロップダウン リスト電子メール アラートを受信するための最小シビラティ（重大度）レベルを選択できます：次のいずれかになります。

- の条件
- 警告
- マイナー
- メジャー
- 重大

最小シビラティ（重大度）レベルを選択した場合、そのレベルと、それよりも高い他のシビラティ（重大度）レベルについてメール アラートが送信されます。たとえば、最小シビラティ（重大度）レベルとして「Minor」を選択すると、マイナー、メジャー、およびクリティカルな障害イベントに関する電子メール アラートが送信されます。

c) [Send Test Mail] をクリックして、追加した電子メール受信者に到達可能であるかどうかを確認します。
電子メール アドレスと SMTP 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とともに確認ポップアップ ウィンドウが表示されます。設定が有効でない場合は、電子メールが送信されていないことを示すメッセージとともに確認ポップアップ ウィンドウが表示されます。[Reachability] カラムは、テスト メールが電子メール受信者に正常に送信されたかどうかを示します。[Reachability] カラムの値は次のいずれかになります。

- [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ていない場合）
- [該当なし（na）]（テスト メールが送信されていない場合）

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。