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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	
ステップ 2	Server# **scope tls-config**	TLS 構成モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	Server/tls-config # **set tlsv2Enabled** *yes*|*no*	確認のために **y** を入力します。 TLS v1.2 を有効または無効にします。
ステップ 4	Server/tls-config* # **Commit**	変更を保存します。
ステップ 5	Server/tls-config # **set tlsv2CipherMode** *Custom*|*High*|*Low*|*Medium*	**[高（High）]**、**[低（Low）]**、または **[中（Medium）]** を選択すると、プリセットの暗号値が自動的に提供されます。
ステップ 6	（任意） Server/tls-config # **set tlsv2CipherMode Custom** *Cipher_Value*	**[カスタム（Custom）]** 暗号モードの有効な暗号値を入力します。 （注） カスタム暗号で提供される特定の暗号用の OpenSSL 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。 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、構成の保存中に、Cisco IMC は自動的に **[TLS v1.2 暗号モード（TLS v1.2 Cipher Mode）]** の値を **[高（High）]** に変更し、構成を保存します。次のステータスが表示される場合があります。 `TLS v1.2 Custom Cipher Status: Error: Configuring an invalid or unsupported TLS v1.2 Cipher List-'Cipher_Name'. Setting TLS v1.2 Cipher Mode to High.`
ステップ 7	Server/tls-config* # **Commit**	変更を保存します。

例

次の例は、TLS v1.2 を有効にし、暗号モードを高に設定する方法を示しています。

```
Server# scope cimc
Server /cimc # scope tls-config
Server /cimc/tls-config # set tlsv2Enabled yes
Server /cimc/tls-config* # commit
Server /cimc/tls-config # set tlsv2CipherMode high
Server /cimc/tls-config* # commit
```

次の例は、TLS v1.2 を有効にし、暗号モードをカスタムに設定する方法を示しています。

```
server# scope cimc
server /cimc # scope tls-config
server /cimc/tls-config # set tlsv2CipherMode Custom
server /cimc/tls-config *# set tlsv2CipherList ECDHE-RSA-AES256-GCM-SHA384
server /cimc/tls-config *# commit
```

TLS 静的キー暗号の有効化

この手順を実行して、Cisco UCS サーバーの TLS 静的キー暗号を有効にします。TLS 静的キー暗号は、デフォルトでは無効です。

（注） この機能は、Cisco IMC CLI インターフェイスを介してのみ有効にできます。

[TLS v1.2 暗号モード（TLS v1.2 Cipher Mode）] が **[高（High）]** または **[カスタム（Custom）]** に設定されている場合、静的キー暗号オプションは適用されません。

静的キー暗号が有効になっている場合、**[TLS v1.2 暗号モード（TLS v1.2 Cipher Mode）]** が **[中（Medium）] / [低（Low）]** から **[高（High）] / [カスタム（Custom）]** に変更されると、自動的に NA に切り替わります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /chassis # **scope tls-config**	TLS 構成モードを開始します。
ステップ 3	Server /chassis/tls-config # **show detail**	**[TLS 静的暗号の有効化（TLS Static Cipher Enabled）]** ステータスを表示します。 `TLS 構成：TLS 静的暗号の有効化：いいえ`
ステップ 4	Server /chassis/tls-config # **set static-cipher-enabled yes**	TLS 暗号を有効にします。
ステップ 5	Server /chassis/tls-config # **commit**	次の警告メッセージが表示されます。 `警告：これにより、TLS で静的暗号が有効になります。KVM、Web サーバー、XMLAPI、および Redfish セッションは切断されます。続行しますか? [[Y]es/[N]o]`

	コマンドまたはアクション	目的
ステップ 6	**[y]** を入力して、**[Enter]** を押します。	トランザクションをシステムの設定にコミットします。

例

次の例は、TLS 静的キー暗号を有効にする方法を示しています。

```
Server# scope cimc
Server /cimc # scope tls-config
Server /cimc/tls-config # show detail
TLS Configuration :
    TLS Static Cipher Enabled: no
Server /cimc/tls-config #
Server /cimc/tls-config # set static-cipher-enabled yes
Server /cimc/tls-config *# commit
Warning: This will enable static ciphers in TLS.
         KVM, Webserver, XMLAPI and Redfish sessions will be disconnected.
Do you wish to continue? [[Y]es/[N]o] y
Server /cimc/tls-config # show detail
TLS Configuration :
    TLS Static Cipher Enabled: yes
```

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
- Cisco UCS S3260 M4/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

HTTP 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope http**	HTTP コマンド モードを開始します。
ステップ 2	Server /http # **set https-enabled** {**yes** | **no**}	Cisco IMC で HTTPS サービスを有効にするか、または HTTPS と HTTP サービスの両方を無効にします。
ステップ 3	Server /http # **set http-enabled** {**yes** | **no**}	Cisco IMC で HTTP サービスを有効または無効にします。
ステップ 4	Server /http # **set http-port** *number*	HTTP 通信に使用するポートを設定します。デフォルトは 80 です。
ステップ 5	Server /http # **set https-port** *number*	HTTPS 通信に使用するポートを設定します。デフォルトは 443 です。
ステップ 6	Server /http # **set http-redirect** {**yes** | **no**}	（注） このオプションは、HTTP が有効になっている場合にのみ適用されます。 HTTPS への HTTP 要求のリダイレクトをイネーブルまたはディセーブルにします。
ステップ 7	Server /http # **set timeout** *seconds*	HTTP 要求の間に 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を設定します。 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。
ステップ 8	Server /http # **commit**	トランザクションをシステムの設定にコミットします。

例

この例では、Cisco IMC の HTTP を構成します。

```
Server# scope http
Server /http # set https-enabled yes
Server /http # set http-enabled yes
Server /http *# set http-port 80
Server /http *# set https-port 443
Server /http *# set http-redirect yes
```

```
Server /http *# set timeout 1800
Server /http *# commit
Server /http # show
HTTP Port  HTTPS Port Timeout  Active Sessions HTTPS Enabled HTTP Redirected  HT
                                          TP Enabled
---------- ---------- -------- --------------- ------- ---------------- --------
                                             --------
80         443        1800     0               yes     yes              yes
Server /http #
```

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ssh**	SSH コマンド モードを開始します。
ステップ 2	Server /ssh # **set enabled** {**yes** | **no**}	Cisco IMC で SSH をイネーブルまたはディセーブルにします。
ステップ 3	Server /ssh # **set ssh-port** *number*	セキュア シェル アクセスに使用するポートを設定します。デフォルトは 22 です。
ステップ 4	Server /ssh # **set timeout** *seconds*	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を設定します。 60 ～ 10,800 の範囲の整数を入力します。デフォルトは 300 秒です。
ステップ 5	Server /ssh # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 6	Server /ssh # **show** [**detail**]	（任意）SSH の設定を表示します。

例

次に、Cisco IMC に SSH を設定する例を示します。

```
Server# scope ssh
Server /ssh # set enabled yes
Server /ssh *# set ssh-port 22
Server /ssh *# set timeout 600
Server /ssh *# commit
```

```
Server /ssh # show
SSH Port   Timeout  Active Sessions Enabled
---------- -------- --------------- -------
22         600      1               yes

Server /ssh #
```

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope xmlapi**	XML API コマンド モードを開始します。
ステップ 2	Server /xmlapi # **set enabled** {**yes** | **no**}	Cisco IMC の XML API 制御をイネーブルまたはディセーブルにします。
ステップ 3	Server /xmlapi # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、Cisco IMC の XML API 制御をイネーブルにし、トランザクションをコミットする例を示します。

```
Server# scope xmlapi
Server /xmlapi # set enabled yes
Server /xmlapi *# commit
Server /xmlapi #  show detail
XMLAPI Settings:
```

```
    Enabled: yes
    Active Sessions: 0
    Max Sessions: 4

Server /xmlapi #
```

Redfish 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope redfish**	redfish コマンド モード を開始します。
ステップ 2	Server /redfish # **set enabled** {**yes** |**no**}	Cisco IMC の redfish 制御をイネーブルまたはディセーブルにします。
ステップ 3	Server /redfish* # **commit**	トランザクションをシステムの設定にコミットします。

例

この例では、Cisco IMC の redfish 制御をイネーブルにします。

```
Server# scope redfish
Server /redfish # set enabled yes
Server /redfish *# commit
Server /redfish #  show detail
REDFISH Settings:
    Enabled: yes
    Active Sessions: 0
    Max Sessions: 4

Server /redfish #
```

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。

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ipmi**	IPMI コマンド モードを開始します。
ステップ 2	Server /ipmi # **set enabled** {**yes** | **no**}	このサーバーで IPMI アクセスをイネーブルまたはディセーブルにします。
ステップ 3	Server /ipmi # **set privilege-level** {**readonly** | **user** | **admin**}	このサーバーで IPMI セッションに割り当て可能な最高特権レベルを指定します。ここに表示される値は次のとおりです。 • **readonly** ：IPMI ユーザは情報を表示できますが、変更できません。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

	コマンドまたはアクション	目的
		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」ユーザー ロールを持つ IPMI ユーザーは、管理者、ユーザー、および読み取り専用セッションをこのサーバーで作成できます。
ステップ 4	Server /ipmi # **set encryption-key** *key*	IPMI 通信に使用する IPMI 暗号キーを設定します。キーの値は、40 個の 16 進数であることが必要です。
ステップ 5	Server /ipmi # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 6	Server /ipmi # **randomise-key**	IPMI 暗号化キーをランダムな値に設定します。 （注） ステップ 4 および 5 ではなく、ステップ 6 のアクションを実行できます。
ステップ 7	プロンプトで、**y** を入力し、暗号キーをランダムにします。	IPMI 暗号化キーをランダムな値に設定します。

例

次に、Cisco IMC に IPMI over LAN を設定する例を示します。

```
Server# scope ipmi
Server /ipmi # set enabled yes
Server /ipmi *# set privilege-level admin
Server /ipmi *# set encryption-key abcdef01234567890abcdef01234567890abcdef
Server /ipmi *# commit
Server /ipmi *# show
Enabled Encryption Key                           Privilege Level Limit
------- ---------------------------------------- ---------------------
yes     ABCDEF01234567890ABCDEF01234567890ABCDEF admin

Server /ipmi # randomise-key
This operation will change the IPMI Encryption Key to a random value
Continue?[y|N]y
Setting IPMI Encryption Key to a random value...

Server /ipmi # show
```

```
Enabled Encryption Key                                  Privilege Level Limit
------- ------------------------------------------------ ---------------------
yes     abcdef01234567890abcdef01234567890abcdef admin

Server /ipmi #
```

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

この手順は、Cisco UCS C シリーズ M6 以前のサーバーに適用されます。Cisco UCS C シリーズ M7 以降のサーバーの SNMP ユーザーを構成するには、Cisco USC C シリーズ M7 および以降のサーバー向けローカル ユーザーの構成 を参照してください。

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **set enabled** {**yes** | **no**}	SNMP をイネーブルまたはディセーブルにします。 （注） 追加の SNMP コンフィギュレーション コマンドが受け入れられる前には、SNMP をイネーブルにして保存する必要があります。

	コマンドまたはアクション	目的
ステップ 3	Server /snmp # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /snmp # **set enable-serial-num** {**yes** | **no**}	サーバのリアル番号を使用してトラップにプレフィックスを追加します。
ステップ 5	Server /snmp # **set snmp-port** ポート番号	SNMP エージェントを実行するポート番号を設定します。1 ～ 65535 の範囲内の数字を選択できます。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。
ステップ 6	Server /snmp # **set community-str** コミュニティ	Cisco IMC 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 コミュニティ名を指定します。名前には最大 18 文字を使用できます。
ステップ 7	Server /snmp # **set community-access**	[Disabled]、[Limited]、または [Full] のいずれかになります。
ステップ 8	Server /snmp # **set trap-community-str**	トラップ情報が送信される SNMP コミュニティ グループを指定します。名前には最大 18 文字を使用できます。
ステップ 9	Server /snmp # **set sys-contact** 連絡先	SNMP の実装を担当する、システムの連絡先を指定します。連絡先情報には、電子メール アドレス、名前と電話番号などを最大 254 文字で指定できます。スペースが含まれている値を入力するには、エントリを引用符で囲む必要があります。
ステップ 10	Server /snmp # **set sys-location** 場所	SNMP エージェント（サーバー）が実行されるホストの場所を指定します。ロケーション情報には最大 254 文字を使用できます。スペースが含まれている値を入力するには、エントリを引用符で囲む必要があります。

	コマンドまたはアクション	目的
ステップ 11	Server /snmp # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、SNMP プロパティを設定し、トランザクションをコミットする例を示します。

```
Server# scope snmp
Server /snmp # set enabled yes
Server /snmp *# commit
Server /snmp *# set enable-serial-num yes
Server /snmp *# set snmp-port 20000
Server /snmp *# set community-str cimcpublic
Server /snmp *# set community-access Full
Server /snmp *# set trap-community-str public
Server /snmp *# set sys-contact "User Name <username@example.com> +1-408-555-1212"
Server /snmp *# set sys-location "San Jose, California"
Server /snmp *# commit
Server /snmp #  show detail
SNMP Settings:
    SNMP Port: 20000
    System Contact: User Name <username@example.com> +1-408-555-1212
    System Location: San Jose, California
    SNMP Community: cimcpublic
    SNMP Trap Community: public
    SNMP Community access: Full
    Enabled: yes
    Serial Number Enabled: yes

Server /snmp #
```

次のタスク

「SNMP トラップ設定の指定 （13 ページ）」の説明に従って SNMP トラップ設定を設定します。

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。
- トラップの設定を実行する前に、SNMP をイネーブルにして保存する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /snmp # **scope trap-destinations** *number*	指定した宛先に対して SNMP トラップ宛先コマンドモードを開始します。4つのSNMPトラップ宛先を使用できます。宛先の *number* は、1 ～ 15 の範囲の整数です。
ステップ 3	Server /snmp/trap-destinations # **set enabled** {**yes** | **no**}	SNMP トラップ宛先をイネーブルまたはディセーブルにします。
ステップ 4	Server /snmp/trap-destinations # **set version** { | **2** | **3**}	必要なトラップ メッセージの SNMP バージョンを指定します。 （注） SNMPv3 トラップは SNMPv3 ユーザーおよびキー値が正しく設定されている場所だけに配信されます。
ステップ 5	Server /snmp/trap-destinations # **set type** {**trap** | **inform**}	SNMP通知メッセージを単純なトラップとして送信するのか、レシーバによる確認応答が必要なインフォーム要求として送信するかを指定します。 （注） 通知オプションは V2 ユーザーに対してのみ選択できます。
ステップ 6	Server /snmp/trap-destinations # **set user** *user*	（注） SNMP v3 バージョンの構成中、暗号化方式が **[DES]** に設定されている SNMP ユーザーを使用することはできません。
ステップ 7	Server /snmp/trap-destination # **set trap-addr** *trap destination address*	トラップ情報を送信するトラップの宛先アドレスを指定します。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。

	コマンドまたはアクション	目的
		（注） Ipv6 をイネーブルにすると、SNMP トラップの宛先発信元アドレスは、SLAAC Ipv6 アドレス（使用可能な場合）かユーザが割り当てた IPv6 アドレスのいずれかにすることができます。これらは両方とも、サーバを一意に識別する有効な SNMP Ipv6 宛先アドレスです。
ステップ 8	Server /snmp/trap-destinations # **set trap-port** *trap destination port*	サーバがトラップの宛先との通信に使用するポート番号を設定します。1 ～ 65535 の範囲内の数字を選択できます。
ステップ 9	Server /snmp/trap-destination # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、汎用の SNMP トラップとトラップの宛先番号 1 を設定し、トランザクションをコミットする例を示します。

```
Server# scope snmp
Server /snmp # Scope trap-destinations 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *#  set version 2
Server /snmp/trap-destination *# set type inform
Server /snmp/trap-destination *# set user user1
Server /snmp/trap-destination *# set trap-addr www.cisco.com
Server /snmp/trap-destination *# set trap-port 10000
Server /snmp/trap-destination *# commit
Server /snmp/trap-destination # show detail
Trap Destination 1:
    Enabled: yes
    SNMP version: 2
    Trap type: inform
    SNMP user: user1
    Trap Address: www.cisco.com
    Trap Port: 10000
    Delete Trap: no
Server /snmp/trap-destination #
```

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **send-test-trap**	イネーブルにされている設定済みの SNMP トラップ宛先に SNMP テスト トラップを送信します。 （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。

例

次に、イネーブルにされているすべての SNMP トラップ宛先にテスト メッセージを送信する例を示します。

```
Server# scope snmp
Server /snmp #  send-test-trap
SNMP Test Trap sent to the destination.
Server /snmp #
```

SNMPv3 ユーザーの設定

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。
- これらのコンフィギュレーション コマンドが受け入れられる前には、SNMP をイネーブルにして保存する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /snmp # **scope v3users** *number*	指定したユーザー番号の SNMPv3 ユーザーのコマンドモードを開始します。
ステップ 3	サーバー/snmp/v3users # **set v3add** {**yes** |**no**}	SNMPv3 ユーザーを追加または削除します。次のいずれかになります。 • **yes**：このユーザーは SNMPv3 ユーザーとしてイネーブルになり、SNMP OID ツリーにアクセスできます。 （注） セキュリティ名とセキュリティ レベルがこの時点で設定されていないと、ユーザーの追加に失敗します。 • **no**：このユーザー設定は削除されます。
ステップ 4	Server /snmp/v3users # **set v3security-name** *security-name*	このユーザーの SNMP ユーザー名を入力します。
ステップ 5	Server /snmp/v3users # **set v3security-level** {**noauthnopriv** |**authnopriv** |**authpriv**}	このユーザーのセキュリティ レベルを選択します。次のいずれかになります。 • **noauthnopriv**：このユーザーには、許可パスワードもプライバシー パスワードも必要ありません。 • **authnopriv**：このユーザー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した場合は、認証キーを設定する必要があります。 • **authpriv**：このユーザーには、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した場合は、認証キーおよび秘密暗号キーを設定する必要があります。

	コマンドまたはアクション	目的
		（注） v3 バージョンでは、authnopriv および authpriv セキュリティ レベルのみが使用可能です。
ステップ 6	Server /snmp/v3users # **set v3proto** {**MD5** | **SHA**}	（注） v3 バージョンでは、SHA 認証方式のみを使用できます。 このユーザーの認証プロトコルを選択します。
ステップ 7	Server /snmp/v3users # **set v3auth-key** *auth-key*	このユーザーの許可パスワードを入力します。
ステップ 8	Server /snmp/v3users # **set v3priv-proto** {**DES** |**AES**}	（注） v3 バージョンでは、AES オプションのみを使用できます。 このユーザーの暗号化プロトコルを選択します。
ステップ 9	Server /snmp/v3users # **set v3priv-auth-key** *priv-auth-key*	このユーザーの秘密暗号キー（プライバシー パスワード）を入力します。
ステップ 10	Server /snmp/v3users # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、SNMPv3 ユーザー番号 2 を設定し、トランザクションをコミットする例を示します。

```
Server# scope snmp
Server /snmp # scope v3users 2
Server /snmp/v3users # set v3add yes
Server /snmp/v3users *# set v3security-name ucsSNMPV3user
Server /snmp/v3users *# set v3security-level authpriv
Server /snmp/v3users *# set v3proto SHA
Server /snmp/v3users *# set v3auth-key
Please enter v3auth-key:ex4mp1ek3y
Please confirm v3auth-key:ex4mp1ek3y
Server /snmp/v3users *# set v3priv-proto AES
Server /snmp/v3users *# set v3priv-auth-key
Please enter v3priv-auth-key:!1@2#3$4%5^6&7*8
Please confirm v3priv-auth-key:!1@2#3$4%5^6&7*8
Server /snmp/v3users *# commit
Settings are being applied ... allow a few minutes for the process to complete
Server /snmp/v3users # show detail
```

```
User 2:
    Add User: yes
    Security Name: ucsSNMPV3user
    Security Level: authpriv
    Auth Type: SHA
    Auth Key: ******
    Encryption: AES
    Private Key: ******

Server /snmp/v3users #
```

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ように SMTP サーバを設定

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope smtp**	SMTP コマンド モードを開始します。
ステップ 2	Server /smtp # **set enabled** {**yes** | **no**}	SMTP 機能をイネーブルまたはディセーブルにします。
ステップ 3	Server /smtp * # **set server-addr** *IP_Address*	SMTP サーバの IP アドレスを割り当てます。
ステップ 4	Server /smtp * # **set port** *port_number*	SMTP サーバに使用するポート番号を指定します。
ステップ 5	Server /smtp # **set-mail-addr** *email_address recipient_minimum_severity informational | warning | minor | major | critical*	受信者の E メール アドレスを最小のシビラティ（重大度）レベルで設定します。
ステップ 6	Server /smtp * # **commit**	トランザクションをシステムの設定にコミットします。

	コマンドまたはアクション	目的
ステップ 7	Server /smtp # **send-test-mail recipient1**	選択した受信者に割り当てられたメール アドレスにテスト メール アラートを送信します。

例

この例では、メール アラートを受信するための SMTP を設定する方法を示します。

```
Server # scope smtp
Server /smtp # set enabled yes
Server /smtp *# set server-addr 10.10.10.10
Server /smtp *# set port 25
Server /smtp *# set-mail-addr recipient4 user@cisco.com critical
This operation will add the recipient4
Continue?[y|N]y
Server /smtp *#
Server /smtp *# commit
Server /smtp #
```

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。