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

はじめる前に

HTTP 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

	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 enabled** {**yes** | **no**}	Cisco IMC で HTTP および HTTPS サービ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 /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 4	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。

	コマンドまたはアクション	目的
ステップ 5	Server /http # **set http-redirect** {**yes** | **no**}	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 6	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 の整数を入力します。デフォルトは 1,800 秒です。
ステップ 7	Server /http # **commit**	トランザクションをシステム設定にコミットします。

次に、Cisco IMC に HTTP を設定する例を示します。

```
Server# scope http
Server /http # set 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 Enabled HTTP Redirected
---------- ---------- -------- --------------- ------- ----------------
80         443        1800     0               yes     yes

Server /http #
```

Configuring SSH

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopessh**	SSH コマンド モードを開始します。
ステップ 2	Server /ssh # **setenabled** {**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 # **setssh-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。デフォルト値は 22 です。
ステップ 4	Server /ssh # **settimeout** *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。

	コマンドまたはアクション	目的
		60 ～ 10,800 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。

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopexmlapi**	XML API 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 /xmlapi # **setenabled** {**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設定にコミットします。

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 #
```

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。

はじめる前に

このタスクを実行するには、admin 権限で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# **scopeipmi**	IPMI コマンド モードを開始します。
ステップ 2	Server /ipmi # **setenabled** {**yes** | **no**}	このサーバで 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 # **setprivilege-level** {**readonly** | **user** | **admin**}	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。
ステップ 4	Server /ipmi # **setencryption-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。

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 #
```

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の情報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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopesnmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **setenabled** {**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設定にコミットします。
ステップ 4	Server /snmp # **setenable-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 # **setsnmp-port** *port number*	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。
ステップ 6	Server /snmp # **setcommunity-str** *community*	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。名前は最大で 18 文字にできます。
ステップ 7	Server /snmp # **setcommunity-access**	[無効（Disabled）]、[制限（Limited）]、または [フル（Full）] のいずれかになります。
ステップ 8	Server /snmp # **settrap-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。名前は最大で 18 文字にできます
ステップ 9	Server /snmp # **setsys-contact** *contact*	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 # **setsys-location** *location*	SNMP エージェント（サーバ）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。
ステップ 11	Server /snmp # **commit**	トランザクションをシステム設定にコミットします。

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 #
```

次の作業

SNMP トラップ設定の指定, （8 ページ）の説明に従って 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 権限で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# **scopesnmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **scopetrap-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 # **setenabled** {**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 # **setversion** { | **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 # **settype** {**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。

	コマンドまたはアクション	目的
		（注） 通知オプションはV2ユーザに対してのみ選択できます。
ステップ 6	Server /snmp/trap-destinations # **setuser** *user*	
ステップ 7	Server /snmp/trap-destination # **settrap-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。 （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 # **settrap-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設定にコミットします。

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

はじめる前に

このタスクを実行するには、admin 権限で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# **scopesnmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **send-test-trap**	有効になっている設定済みの 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。

次に、有効になっているすべての 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。
- 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。
ステップ 2	Server /snmp # **scope v3users** *number*	指定したユーザ番号の SNMPv3 ユーザのコマンド モードを開始します。
ステップ 3	Server /snmp/v3users # **set v3add** {**yes** | **no**}	SNMPv3 ユーザを追加または削除します。次のいずれかになります。

	コマンドまたはアクション	目的
		• **yes**：このユーザは SNMPv3 ユーザとしてイネーブルであり、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、ユーザの追加に失敗します。 • **no**：このユーザ コンフィギュレーションは削除されます。
ステップ 4	Server /snmp/v3users # **set v3security-name** *security-name*	このユーザの SNMP ユーザ名を入力します。
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。 • **authnopriv**：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。
ステップ 6	Server /snmp/v3users # **set v3proto** {**MD5** | **SHA**}	このユーザ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**}	このユーザ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設定にコミットします。

次に、SNMPv3 ユーザ番号 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 #
```

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 アラートを受信するように SMTP サーバを設定

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopesmtp**	SMTP コマンド モードを開始します。
ステップ 2	Server /smtp # **setenabled** {**yes** | **no**}	SMTP機能をイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
ステップ 3	Server /smtp * # **setserver-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 * # **setfault-severity** {**critical** | **major** | **minor** | **warning** | **condition**}	メール アラートに障害の重大度を割り当てます。
ステップ 5	Server /smtp * # **setport** *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 6	Server /smtp * # **commit**	トランザクションをシステム設定にコミットします。
ステップ 7	Server /smtp # **set-mail-addr** {**recipient1** | **recipient2** | **recipient3** | **recipient4**} *email_address*	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。
ステップ 8	Server /smtp # **send-test-mailrecipient1**	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。

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 fault-severity major
Server /smtp *# set port 25
There is no change in the configured port number.
Please verify if you wish to choose a different one before commit.
Server /smtp *# commit
Server /smtp # set-mail-addr recipient1 test@cisco.com
Server /smtp # show detail
SMTP Setting:
    Enabled: yes
    Port Number: 25
    Server Address: 10.104.10.10
    Minimum Severity to Report: critical
    Recipient1:
        Name     : seduggir@fpmr2.com
        Reachable: na
    Recipient2:
        Name     :
        Reachable: na
    Recipient3:
        Name     :
        Reachable: na
    Recipient4:
        Name     :
        Reachable: na

Server /smtp # send-test-mail recipient1
Test mail sent Successful.
Server /smtp # show detail
SMTP Setting:
```

```
    Enabled: yes
    Port Number: 25
    Server Address: 10.10.10.10
    Minimum Severity to Report: critical
    Recipient1:
        Name     : test@cisco.com
        Reachable: yes
    Recipient2:
        Name     :
        Reachable: na
    Recipient3:
        Name     :
        Reachable: na
    Recipient4:
        Name     :
        Reachable: na

Server /smtp #
```