ネットワーク関連の設定

この章は、次の項で構成されています。

- サーバ NIC の設定 （1 ページ）
- 共通プロパティの設定 （2 ページ）
- ネットワーク セキュリティの設定 （4 ページ）
- ネットワーク タイム プロトコルの設定 （5 ページ）

サーバ NIC の設定

サーバの NIC

NIC モード

NIC モード設定は、Cisco IMC に到達できるポートを決定します。プラットフォームに応じて、次のネットワーク モード オプションを使用できます。

- [Dedicated]：Cisco IMC へのアクセスに使用される管理ポート。

サーバ NIC の設定

NIC モードと NIC 冗長化を設定する場合は、サーバの NIC を設定します。

始める前に

NIC 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] メニューで、[Networking] をクリックします。

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

名前	説明Cisco IMC
[NIC Mode] ドロップダウン リスト	Cisco IMC へのアクセスに使用可能なポート。次のいずれかになります。 • [専用（Dedicated）]：Cisco IMC へのアクセスに使用される管理ポート。 • [Shared LOM]：CIMC へのアクセスにマザーボードのオンボード LAN（LOM）ポートを使用します。
[NIC Interface] フィールド	[NIC Mode] フィールドで選択されているネットワーク インターフェイス。

ステップ 4 [Save Changes] をクリックします。

共通プロパティの設定

共通プロパティの設定の概要

ホスト名

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）拡張機能は、ホスト名を DHCP パケットに追加することによって利用でき、DHCP サーバ側でこれを解釈または表示できます。ホスト名は DHCP パケットのオプション フィールドに追加され、最初に DHCP サーバに送信される DHCP DISCOVER パケットで送信されます。

サーバのデフォルトのホスト名は EXXXX-YYYYYYYYYYY です（XXXX はサーバのモデル番号で、YYYYYYYYYYY はシリアル番号です）。この一意のストリングはクライアント ID として機能し、DHCP サーバから Cisco IMC にリースされる IP アドレスを追跡してマッピングするのに役立ちます。サーバのステッカーまたはラベルとしてデフォルト シリアル番号が製造者から提供され、サーバを識別するのに役立ちます。

ダイナミック DNS

ダイナミック DNS（DDNS）は、Cisco IMC から DNS サーバのリソース レコードを追加または更新するために使用されます。Web UI または CLI を使用してダイナミック DNS をイネーブルにできます。[DDNS] オプションを有効にすると、DDNS サービスは現在のホスト名、ドメイン名、および管理 IP アドレスを記録し、Cisco IMC から DNS サーバのリソース レコードを更新します。

（注） DDNS サーバは、次の DNS 設定のいずれかが変更された場合に、DNS サーバの以前のリソース レコード（もしあれば）を削除し、新しいリソース レコードを追加します。

- ホスト名
- LDAP 設定のドメイン名
- DDNS と DHCP がイネーブルの場合に、ネットワークまたはサブネットの変更による新しい IP アドレスまたは DNS IP またはドメイン名を DHCP が取得する場合。
- DHCP がディセーブルの場合に、CLI または Web UI を使用してスタティック IP アドレスを設定する場合。
- **dns-use-dhcp** コマンドを入力する場合。

[**Dynamic DNS Update Domain**]：ドメインを指定できます。ドメインは、メイン ドメインまたはサブ ドメインのどちらでも可です。このドメイン名は、DDNS 更新のため Cisco IMC のホスト名に付加されます。

共通プロパティの設定

サーバを説明するには、共通プロパティを使用します。

始める前に

共通プロパティを設定するには、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] メニューで、[Networking] をクリックします。

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

a) [Management Hostname] フィールドに、ホストの名前を入力します。

デフォルトでは、ホスト名は EXXXX-YYYYYYYYYYY 形式で表示されます（XXXX はサーバのモデル番号、YYYYYYYYYYY はシリアル番号です）。

（注） また、DHCP が有効である場合、発信される DHCP DISCOVER パケットにも Cisco IMC ホスト名が含まれます。

b) [Dynamic DNS] チェックボックスをオンにします。

c) [**Dynamic DNS Update Domain**] フィールドに、ドメイン名を入力します。

ステップ 4 [Save Changes] をクリックします。

ネットワーク セキュリティの設定

ネットワーク セキュリティ

Cisco IMC は、IP ブロッキングをネットワーク セキュリティとして使用します。IP ブロッキングは、サーバまたは Web サイトと、特定の IP アドレスまたはアドレス範囲との間の接続を防ぎます。IP ブロッキングは、これらのコンピュータから Web サイト、メール サーバ、またはその他のインターネット サーバへの不要な接続を効果的に禁止します。

禁止 IP の設定は、一般的に、サービス拒否（DoS）攻撃から保護するために使用されます。Cisco IMC は、IP ブロッキングの失敗回数を設定して、IP アドレスを禁止します。

ネットワーク セキュリティの設定

IP ブロッキングの失敗回数を設定する場合は、ネットワーク セキュリティを設定します。

始める前に

ネットワーク セキュリティを設定するには、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 [Networking] ペインで、[Network Security] をクリックします。

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

名前	説明
[Enable IP Blocking] チェックボックス	このチェックボックスをオンにすると、IP ブロッキングがイネーブルになります。
[IP Blocking Fail Count] フィールド	指定された時間ユーザがロックアウトされる前に、ユーザが試行できるログインの失敗回数。 この回数のログイン試行失敗は、[IP Blocking Fail Window] フィールドで指定されている期間内に発生する必要があります。 3 ～ 10 の範囲の整数を入力します。
[IP Blocking Fail Window] フィールド	ユーザをロックアウトするためにログイン試行の失敗が発生する必要のある期間（秒数）。 60 ～ 120 の範囲の整数を入力します。

名前	説明
[IP Blocking Penalty Time] フィールド	ユーザが指定されている期間内にログイン試行の最大回数を超えた場合に、ユーザがロックアウトされている秒数。 300 ～ 900 の範囲の整数を入力します。

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

名前	説明
[Enable IP Filtering] チェックボックス	IP フィルタリングをイネーブルにするには、このボックスをオンにします。
[IP フィルタ（IP Filter）] フィールド	サーバへのセキュアなアクセスを提供するために、選択した IP のセットのみにアクセスを許可するフィルタを設定できるようになりました。このオプションでは、IP アドレスを保存するための 4 つのスロット（IP フィルタ 1、2、3、および 4）が提供されます。IP フィルタの設定時に、単一の IP アドレスまたは IP アドレスの範囲を割り当てることができます。IP フィルタを設定すると、他の IP アドレスを使用してサーバにアクセスできなくなります。

ステップ 5 [Save Changes] をクリックします。

ネットワーク タイム プロトコルの設定

ネットワーク タイム プロトコル サービス設定

デフォルトでは、Cisco IMC がリセットされると、ホストと時刻が同期されます。NTP サービスを導入すると、Cisco IMC を設定して NTP サーバで時刻を同期することができます。デフォルトでは、NTP サーバは Cisco IMC で動作しません。少なくとも 1 台、最大 4 台の、NTP サーバまたは時刻源サーバとして動作するサーバの IP/DNS アドレスを指定し、NTP サービスをイネーブルにして設定する必要があります。NTP サービスをイネーブルにすると、Cisco IMC は設定された NTP サーバと時刻を同期します。NTP サービスは Cisco IMC でのみ変更できます。

（注） NTP サービスをイネーブルにするには、DNS アドレスよりも、サーバの IP アドレスを指定することを推奨します。

ネットワーク タイム プロトコル設定の設定

NTP を設定すると、IPMI の **Set SEL time** コマンドはディセーブルになります。

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 [Navigation] ペインの [Admin] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Networking] をクリックします。

ステップ 3 [Networking] ペインで、[NTP Setting] をクリックします。

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

名前	説明
[Enable NTP]	NTP サービスをイネーブルにするには、このボックスをオンにします。
[Server 1]	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
[Server 2]	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
[Server 3]	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
[Server 4]	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
[Status] メッセージ	サーバがリモートの NTP サーバと時刻を同期できるかどうかを示します。次のいずれかになります。 • [synchronized to NTP server (RefID) at stratum 7]：NTP サービスが有効で、複数または個々の IPv4 または IPv6 ベースの NTP サーバが追加される場合。 • [unsynchronized]：NTP サービスが有効で、不明または到達不能なサーバが追加される場合。 • [NTP service disabled]：NTP サービスが無効な場合。

ステップ 5 [Save Changes] をクリックします。