ネットワーク関連の設定

この章の内容は、次のとおりです。

サーバ NIC の設定

サーバの NIC

CIMC への接続には、2 種類の NIC モードを使用できます。 一方のモードでは、プラットフォームに応じて、active-active または active-standby の冗長化モードを選択することもできます。

NIC モード

CIMC ネットワークの設定により、CIMC に到達できるポートが決定します。 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。

- [Cisco Card]：CIMC への接続は、搭載されたアダプタ カードを経由して使用できます。
- [Dedicated]：CIMC への接続は、管理イーサネット ポートを経由して使用できます。
- [Shared LOM]：CIMC への接続は、LAN On Motherboard（LOM; マザーボードのオンボード LAN）イーサネット ホスト ポートを経由した場合だけ使用できます。 一部のプラットフォームでは、[10 Gigabit Ethernet LOM] オプションを使用できます。

（注） Shared LOM モードでは、すべてのホスト ポートが同じサブネットに属している必要があります。

- Shipping（サポートされている場合）：CIMC への接続は、制限された出荷時デフォルト設定を使用して、管理イーサネット ポートを経由して使用できます。

（注） shipping モードは、CIMC への初期接続の目的だけに用意されています。 運用時には別のモードを設定します。

NIC 冗長化

CIMC ネットワーク冗長化の設定により、NIC 冗長化の処理方法が決定します。

- [None]：冗長化は使用できません。
- [Active-Active]：すべてのイーサネット ポートが同時に動作します。 このモードは、CIMC への複数のパスを提供します。
- [Active-Standby]：1 つのポートから別のポートにフェールオーバーします。

使用できる冗長化モードは、選択されているネットワーク モードとプラットフォームによって異なります。 使用できるモードについては、サーバのサーバ インストレーションおよびサービス ガイドを参照してください。 このガイドは http://www.cisco.com/go/unifiedcomputing/c-series-doc の『*Cisco UCS C-Series Servers Documentation Roadmap*』から入手できます。

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。

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **set mode** {**dedicated** |	NIC モードを次のいずれかに設定します。

	コマンドまたはアクション	目的
	shared_lom | **shared_lom_10g** | **shipping** | **cisco_card**}	• Dedicated：CIMC へのアクセスに管理イーサネット ポートを使用します。 • Shared LOM：CIMC へのアクセスに LAN On Motherboard（LOM; マザーボードのオンボード LAN）イーサネット ホスト ポートを使用します。 （注） Shared LOM を選択した場合は、すべてのホスト ポートが同じサブネットに属することを確認してください。 • Shared LOM 10G：CIMC へのアクセスに 10 G ポートを使用します。 • Shipping：初期接続用の制限付き設定。 通常の操作には、別のモードを選択します。 • Cisco Card：CIMC へのアクセスにアダプタ カードのポートを使用します。
ステップ 4	Server /cimc/network # **set redundancy** {**none** | **active-active** | **active-standby**}	NIC モードが Shared LOM である場合に、NIC 冗長モードを設定します。 冗長モードは、次のいずれかになります。 • none：LOM イーサネット ポートは単独で動作し、問題が生じた場合もフェールオーバーしません。 • active-active：サポートされている場合は、すべての LOM イーサネット ポートが利用されます。 • active-standby：1 つの LOM イーサネット ポートに障害が発生すると、トラフィックは別の LOM ポートにフェールオーバーします。
ステップ 5	Server /cimc/network # **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。 （注） 使用可能な NIC モードおよび NIC 冗長モードのオプションは、お使いのプラットフォームによって異なります。 サーバでサポートされていないモードを選択すると、変更を保存するときにエラー メッセージが表示されます。

次に、CIMC ネットワーク インターフェイスを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set mode dedicated
Server /cimc/network *# commit
```

```
Server /cimc/network #
```

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。

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **set hostname** *host-name*	ホストの名前を指定します。
ステップ 4	Server /cimc/network # **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。

次に、コマンドのプロパティを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set hostname Server
Server /cimc/network *# commit
Server /cimc/network #
```

IPv4 の設定

はじめる前に

IPv4 ネットワークの設定を実行するには、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 cimc**	CIMC 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 /cimc # **scope network**	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **set dhcp-enabled** {**yes** | **no**}	CIMC で DHCP を使用するかどうかを選択します。 （注） DHCP がイネーブルである場合は、CIMC 用に 1 つの IP アドレスを予約するように DHCP サーバを設定することを推奨します。 サーバの複数のポートを通じて CIMC に到達できる場合、それらのポートの全範囲の MAC アドレスに対して 1 つの IP アドレスを予約する必要があります。
ステップ 4	Server /cimc/network # **set v4-addr** *ipv4-address*	CIMC の IP アドレスを指定します。
ステップ 5	Server /cimc/network # **set v4-netmask** *ipv4-netmask*	IP アドレスのサブネット マスクを指定します。
ステップ 6	Server /cimc/network # **set v4-gateway** *gateway-ipv4-address*	IP アドレスのゲートウェイを指定します。
ステップ 7	Server /cimc/network # **set dns-use-dhcp** {**yes** | **no**}	CIMC が DNS サーバ アドレスを DHCP から取得するかどうかを選択します。
ステップ 8	Server /cimc/network # **set preferred-dns-server** *dns1-ipv4-address*	プライマリ DNS サーバの IP アドレスを指定します。
ステップ 9	Server /cimc/network # **set alternate-dns-server** *dns2-ipv4-address*	セカンダリ DNS サーバの IP アドレスを指定します。
ステップ 10	Server /cimc/network # **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 11	Server /cimc/network # **show** [**detail**]	（任意）IPv4 ネットワークの設定を表示します。

次に、IPv4 ネットワークの設定を実行し、表示する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dhcp-enabled yes
Server /cimc/network *# set v4-addr 10.20.30.11
Server /cimc/network *# set v4-netmask 255.255.248.0
Server /cimc/network *# set v4-gateway 10.20.30.1
Server /cimc/network *# set dns-use-dhcp-enabled no
```

```
Server /cimc/network *# set preferred-dns-server 192.168.30.31
Server /cimc/network *# set alternate-dns-server 192.168.30.32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
    IPv4 Address: 10.20.30.11
    IPv4 Netmask: 255.255.248.0
    IPv4 Gateway: 10.20.30.1
    DHCP Enabled: yes
    Obtain DNS Server by DHCP: no
    Preferred DNS: 192.168.30.31
    Alternate DNS: 192.168.30.32
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Hostname: Server
    MAC Address: 01:23:45:67:89:AB
    NIC Mode: dedicated
    NIC Redundancy: none

Server /cimc/network #
```

サーバ VLAN の設定

はじめる前に

サーバ VLAN を設定するには、admin としてログインしている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンドモードを開始します。
ステップ 3	Server /cimc/network # **set vlan-enabled** {**yes** | **no**}	CIMC を VLAN に接続するかどうかを選択します。
ステップ 4	Server /cimc/network # **set vlan-id** *id*	VLAN 番号を指定します。
ステップ 5	Server /cimc/network # **set vlan-priority** *priority*	VLAN でのこのシステムのプライオリティを指定します。
ステップ 6	Server /cimc/network # **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 7	Server /cimc/network # **show** [**detail**]	（任意）ネットワークの設定を表示します。

次に、サーバ VLAN を設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
```

```
Server /cimc/network # set vlan-enabled yes
Server /cimc/network *# set vlan-id 10
Server /cimc/network *# set vlan-priority 32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
    IPv4 Address: 10.20.30.11
    IPv4 Netmask: 255.255.248.0
    IPv4 Gateway: 10.20.30.1
    DHCP Enabled: yes
    Obtain DNS Server by DHCP: no
    Preferred DNS: 192.168.30.31
    Alternate DNS: 192.168.30.32
    VLAN Enabled: yes
    VLAN ID: 10
    VLAN Priority: 32
    Hostname: Server
    MAC Address: 01:23:45:67:89:AB
    NIC Mode: dedicated
    NIC Redundancy: none

Server /cimc/network #
```

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

CIMC 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、Denial of Service（DoS; サービス拒絶）攻撃から保護するために使用されます。 CIMC 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。

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC 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 /cimc # **scope network**	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **scope ipblocking**	IP ブロッキング コマンド モードを開始します。
ステップ 4	Server /cimc/network/ipblocking # **set enabled** {**yes** | **no**}	IP ブロッキングをイネーブルまたはディセーブルにします。
ステップ 5	Server /cimc/network/ipblocking # **set fail-count** *fail-count*	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を設定します。 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。
ステップ 6	Server /cimc/network/ipblocking # **set fail-window** *fail-seconds*	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）を設定します。 60 ～ 120 の範囲の整数を入力します。
ステップ 7	Server /cimc/network/ipblocking # **set penalty-time** *penalty-seconds*	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を設定します。 300 ～ 900 の範囲の整数を入力します。
ステップ 8	Server /cimc/network/ipblocking # **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。

次に、IP ブロッキングを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ipblocking
Server /cimc/network/ipblocking # set enabled yes
Server /cimc/network/ipblocking *# set fail-count 5
Server /cimc/network/ipblocking *# set fail-window 90
Server /cimc/network/ipblocking *# set penalty-time 600
Server /cimc/network/ipblocking *# commit
Server /cimc/network/ipblocking #
```