



共通システム メンテナンス タスク

- 高可用性のためのイーサネットインターフェイスのボンディング (1 ページ)
- 紛失、失念、または侵害されたパスワードの DVD を使用したリセット (7 ページ)
- 管理者のロックアウトにより無効化されたパスワードのリセット (8 ページ)
- Return Material Authorization (RMA) (9 ページ)
- Cisco ISE アプライアンスの IP アドレスの変更 (9 ページ)
- インストールおよびアップグレード履歴の表示 (10 ページ)
- システムの消去の実行 (11 ページ)

高可用性のためのイーサネットインターフェイスのボンディング

Cisco ISE は、物理インターフェイスに高可用性を提供するために、1つの仮想インターフェイスへの2つのイーサネットインターフェイスのボンディングをサポートします。この機能は、ネットワーク インターフェイス カード (NIC) のボンディングまたは NIC チーミングと呼ばれます。2つのインターフェイスをボンディングすると、2つの NIC は1つの MAC アドレスを持つ単一のデバイスとして認識されます。

Cisco ISE の NIC ボンディング機能は、ロード バランシングまたはリンク アグリゲーション機能をサポートしていません。Cisco ISE は、NIC ボンディングの高可用性機能だけをサポートします。

インターフェイスのボンディングでは、次の状況でも Cisco ISE サービスが影響を受けないことを保証します。

- 物理インタフェースの障害
- スイッチ ポート接続の喪失 (シャットダウンまたは障害)
- スイッチ ラインカードの障害

2つのインターフェイスをボンディングすると、インターフェイスの一方がプライマリ インターフェイスになり、もう一方はバックアップインターフェイスになります。2つのインターフェイスをボンディングすると、すべてのトラフィックは通常、プライマリインターフェイス

を通過します。プライマリ インターフェイスが何らかの理由で失敗すると、バックアップ インターフェイスがすべてのトラフィックを引き継いで処理します。ボンディングにはプライマリ インターフェイスの IP アドレスと MAC アドレスが必要です。

NIC ボンディング機能を設定する際に、Cisco ISE は固定物理 NIC を組み合わせて NIC のボンディングを形成します。ボンディングインターフェイスを形成するためにボンディングすることができる NIC について、次の表に概要を示します。

表 1: ボンディングしてインターフェイスを形成する物理 NIC

Cisco ISE の物理 NIC の名前	Linux 物理 NIC の名前	ボンディングされた NIC のロール	ボンディングされた NIC の名前
ギガビットイーサネット 0	Eth0	プライマリ	ボンド 0
ギガビットイーサネット 1	Eth1	バックアップ	
ギガビットイーサネット 2	Eth2	プライマリ	ボンド 1
ギガビットイーサネット 3	Eth3	バックアップ	
ギガビットイーサネット 4	Eth4	プライマリ	ボンド 2
ギガビットイーサネット 5	Eth5	バックアップ	

サポートされるプラットフォーム

NIC ボンディング機能は、サポートされているすべてのプラットフォームとノードペルソナでサポートされています。サポートされるプラットフォームは次のとおりです。

- SNS ハードウェアアプライアンス：ボンド 0、1、および 2
- VMware 仮想マシン：ボンド 0、1、および 2（6つの NIC が仮想マシンで使用可能な場合）
- Linux KVM ノード：ボンド 0、1、および 2（6つの NIC が仮想マシンで使用可能な場合）

イーサネットインターフェイスのボンディングに関するガイドライン

- Cisco ISE は最大 6 つのイーサネット インターフェイスをサポートするので、ボンドは 3 つ（ボンド 0、ボンド 1、ボンド 2）のみ設定できます。

- ボンドに含まれるインターフェイスを変更したり、ボンドのインターフェイスのロールを変更したりすることはできません。ボンディングできるNICとボンドでのロールについての情報は、上記の表を参照してください。
- Eth0 インターフェイスは、管理インターフェイスとランタイムインターフェイスの両方として機能します。その他のインターフェイスは、ランタイムインターフェイスとして機能します。
- ボンドを作成する前に、プライマリ インターフェイス（プライマリ NIC）に IP アドレスを割り当てる必要があります。ボンド 0 を作成する前は、Eth0 インターフェイスに IPv4 アドレスを割り当てる必要があります。同様に、ボンド 1 と 2 を作成する前は、Eth2 と Eth4 インターフェイスに IPv4 または IPv6 アドレスをそれぞれ割り当てる必要があります。
- ボンドを作成する前に、バックアップ インターフェイス（Eth1、Eth3、および Eth5）に IP アドレスが割り当てられている場合は、バックアップ インターフェイスからその IP アドレスを削除します。バックアップ インターフェイスには IP アドレスを割り当てないでください。
- ボンドを 1 つのみ（ボンド 0）作成し、残りのインターフェイスをそのままにすることもできます。この場合、ボンド 0 は管理インターフェイスとランタイムインターフェイスとして機能し、残りのインターフェイスはランタイムインターフェイスとして機能します。
- ボンドでは、プライマリ インターフェイスの IP アドレスを変更できます。プライマリ インターフェイスの IP アドレスと想定されるので、新しい IP アドレスがボンディングされたインターフェイスに割り当てられます。
- 2 つのインターフェイス間のボンドを削除すると、ボンディングされたインターフェイスに割り当てられていた IP アドレスは、プライマリ インターフェイスに再び割り当てられます。
- デプロイメントに含まれる Cisco ISE ノードで NIC ボンディング機能を設定するには、そのノードをデプロイメントから登録解除し、NIC ボンディングを設定して、デプロイメントに再度登録する必要があります。
- ボンド（Eth0、Eth2、または Eth4 インターフェイス）のプライマリ インターフェイスとして機能する物理インターフェイスにスタティックルートが設定されている場合は、物理インターフェイスではなくボンディングされたインターフェイスで動作するようにスタティックルートが自動的に更新されます。

NIC ボンディングの設定

NIC ボンディングは Cisco ISE CLI から設定できます。次の手順では、Eth0 と Eth1 インターフェイス間にボンド 0 を設定する方法を説明します。

始める前に

バックアップインターフェイスとして動作する物理インターフェイス（Eth1、Eth3、Eth5 インターフェイスなど）に IP アドレスが設定されている場合は、バックアップインターフェイスからその IP アドレスを削除する必要があります。バックアップインターフェイスには IP アドレスを割り当てないでください。

- ステップ 1** 管理者アカウントを使用して Cisco ISE CLI にログインします。
- ステップ 2** `configure terminal` と入力して、コンフィギュレーション モードを開始します。
- ステップ 3** `interface GigabitEthernet 0` コマンドを入力します。
- ステップ 4** `backup interface GigabitEthernet 1` コマンドを入力します。
コンソールに次のメッセージが表示されます。

```
% Warning: IP address of interface eth1 will be removed once NIC bonding is enabled. Are you sure you want to proceed? Y/N [N]:
```

- ステップ 5** Y を入力して、Enter を押します。

ボンド 0 が設定されました。Cisco ISE が自動的に再起動します。しばらく待ってから、すべてのサービスが正常に稼働していることを確認します。すべてのサービスが実行していることを確認するために、CLI から `show application status ise` コマンドを入力します。

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# backup interface gigabitEthernet 1
Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
```

```
ise/admin(config-GigabitEthernet)#
```

NIC ボンディング設定の確認

NIC ボンディング機能が設定されているかどうかを確認するには、Cisco ISE CLI から **show running-config** コマンドを実行します。次のような出力が表示されます。

```
!  
interface GigabitEthernet 0  
  ipv6 address autoconfig  
  ipv6 enable  
  backup interface GigabitEthernet 1  
  ip address 192.168.118.214 255.255.255.0  
!
```

上記の出力では、「**backup interface GigabitEthernet 1**」は、ギガビットイーサネット 0 に NIC ボンディングが設定されていて、ギガビットイーサネット 0 がプライマリインターフェイス、ギガビットイーサネット 1 がバックアップインターフェイスとされていることを示します。また、ADE-OS 設定では、プライマリおよびバックアップのインターフェイスに効果的に同じ IP アドレスを設定していても、**running config** でバックアップインターフェイスの IP アドレスは表示されません。

また、**show interfaces** コマンドを実行して、ボンディングされたインターフェイスを表示できます。

```
ise/admin# show interface  
bond0: flags=5187<UP,BROADCAST,RUNNING,PRIMARY,MULTICAST> mtu 1500  
  inet 10.126.107.60 netmask 255.255.255.0 broadcast 10.126.107.255  
  inet6 fe80::8a5a:92ff:fe88:4aea prefixlen 64 scopeid 0x20<link>  
  ether 88:5a:92:88:4a:ea txqueuelen 0 (Ethernet)  
  RX packets 1726027 bytes 307336369 (293.0 MiB)  
  RX errors 0 dropped 844 overruns 0 frame 0  
  TX packets 1295620 bytes 1073397536 (1023.6 MiB)  
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
GigabitEthernet 0  
  flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST> mtu 1500  
  ether 88:5a:92:88:4a:ea txqueuelen 1000 (Ethernet)  
  RX packets 1726027 bytes 307336369 (293.0 MiB)  
  RX errors 0 dropped 844 overruns 0 frame 0  
  TX packets 1295620 bytes 1073397536 (1023.6 MiB)  
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  device memory 0xfab00000-fabfffff  
  
GigabitEthernet 1  
  flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST> mtu 1500  
  ether 88:5a:92:88:4a:ea txqueuelen 1000 (Ethernet)  
  RX packets 0 bytes 0 (0.0 B)  
  RX errors 0 dropped 0 overruns 0 frame 0  
  TX packets 0 bytes 0 (0.0 B)  
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  device memory 0xfaa00000-faafffff
```

NIC ボンディングの削除

backup interface コマンドの **no** 形式を使用して、NIC ボンドを削除します。

始める前に

ステップ 1 管理者アカウントを使用して Cisco ISE CLI にログインします。

ステップ 2 **configure terminal** と入力して、コンフィギュレーションモードを開始します。

ステップ 3 **interface GigabitEthernet 0** コマンドを入力します。

ステップ 4 **no backup interface GigabitEthernet 1** コマンドを入力します。

```
% Notice: Bonded Interface bond 0 has been removed.
```

ステップ 5 **Y** を入力して Enter キーを押します。

ボンド 0 が削除されました。Cisco ISE が自動的に再起動します。しばらく待ってから、すべてのサービスが正常に稼働していることを確認します。すべてのサービスが実行していることを確認するために、CLI から **show application status ise** コマンドを入力します。

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# no backup interface gigabitEthernet 1

Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config-GigabitEthernet)#
```

紛失、失念、または侵害されたパスワードの DVD を使用したリセット

始める前に

次の接続関連の状態が原因で、Cisco ISE ソフトウェア DVD を使用して Cisco ISE アプライアンスを起動しようとしたときに問題が発生する場合があります。これを理解しておいてください。

- ターミナル サーバーにシリアル コンソールから Cisco ISE アプライアンスへの `exec` に設定された接続が関連付けられている。これを `no exec` に設定すると、キーボードとビデオモニター接続およびシリアル コンソール接続を使用できるようになります。
- Cisco ISE アプライアンスへのキーボードおよびビデオモニター接続がある（これはリモート キーボードおよびビデオ モニター接続または VMware vSphere Client コンソール接続のいずれかになります）。
- Cisco ISE アプライアンスへのシリアル コンソール接続がある。

ステップ 1 Cisco ISE アプライアンスの電源がオンになっていることを確認します。

ステップ 2 Cisco ISE ソフトウェア DVD を挿入します。

ステップ 3 矢印キーを使用して、ローカル シリアル コンソール ポート接続を使用する場合は [システムユーティリティ (シリアル コンソール) (System Utilities (Serial Console))] を選択し、アプライアンスに対してキーボードとビデオモニター接続を使用する場合は [システムユーティリティ (キーボード/モニター) (System Utilities (Keyboard/Monitor))] を選択して、Enter を押します。

次に示すような ISO ユーティリティ メニューが表示されます。

```
Available System Utilities:
  [1] Recover Administrator Password
  [2] Virtual Machine Resource Check
  [3] Perform System Erase
  [q] Quit and reload
Enter option [1 - 3] q to Quit:
```

ステップ 4 管理者パスワードを回復するには、**1** を入力します。

コンソールに次のメッセージが表示されます。

```
Admin Password Recovery
This utility will reset the password for the specified ADE-OS administrator.
At most the first five administrators will be listed. To cancel without
saving changes, enter [q] to Quit and return to the utilities menu.
```

```
[1]:admin
[2]:admin2
[3]:admin3
[4]:admin4
```

```
Enter choice between [1 - 4] or q to Quit: 2
```

```
Password:  
Verify password:
```

```
Save change and reboot? [Y/N]:
```

ステップ 5 パスワードをリセットする管理者ユーザーに対応する番号を入力します。

ステップ 6 新しいパスワードを入力して確認します。

ステップ 7 変更を保存するには **y** と入力します。

管理者のロックアウトにより無効化されたパスワードのリセット

管理者が、誤ったパスワードをアカウントが無効になる所定の回数入力する場合があります。デフォルトの最小試行回数は 5 です。

次の手順によって、Cisco ISE CLI で **application reset-passwd ise** コマンドを使用して、管理者ユーザー インターフェイス パスワードをリセットします。このコマンドは、管理者の CLI のパスワードには影響を与えません。正常に管理者パスワードをリセットすると、クレデンシャルはただちにアクティブになり、システムをリブートせずにログインできます。

Cisco ISE により、[管理者ログイン (Administrator Logins)] ウィンドウにログエントリが追加されます。このウィンドウを表示するには、[メニュー (Menu)] アイコン (☰) をクリックして選択します。[運用 (Operations)] > [レポート (Reports)] > [レポート (Reports)] > [監査 (Audit)] > [管理者ログイン (Administrator Logins)] です。その管理者 ID に関連付けられたパスワードがリセットされるまで、管理者 ID のログイン情報は一時的に停止されます。

ステップ 1 ダイレクト コンソール CLI にアクセスして、次を入力します。

```
application reset-passwd ise administrator_ID
```

ステップ 2 この管理者 ID に使用されていた前の 2 つのパスワードと異なる新しいパスワードを指定して、確認します。

```
Enter new password:  
Confirm new password:
```

```
Password reset successfully
```


Return Material Authorization (RMA)

Return Material Authorization (RMA) の場合、SNS サーバー上の個々のコンポーネントを交換する場合は、Cisco ISE をインストールする前に必ずアプライアンスを再イメージ化してください。Cisco TAC に連絡して、サポートを受けてください。

Cisco ISE アプライアンスの IP アドレスの変更

始める前に

- IP アドレスを変更する前に、Cisco ISE ノードがスタンドアロン状態であることを確認します。ノードが分散デプロイメント環境の一部である場合は、その環境からノードを登録解除して、スタンドアロンノードにします。
- Cisco ISE アプライアンスの IP アドレスを変更する場合は、**no ip address** コマンドを使用しないでください。

ステップ 1 Cisco ISE CLI にログインします。

ステップ 2 次のコマンドを入力します。

- a) **configure terminal**
- b) **interface GigabitEthernet 0**
- c) **ip address new_ip_address new_subnet_mask**

システムにより、IP アドレスを変更するように求められます。**Y**を入力します。次のような画面が表示されます。

```
ise-13-infra-2/admin(config-GigabitEthernet)# ip address a.b.c.d 255.255.255.0
```

```
% Changing the IP address might cause ISE services to restart
Continue with IP address change? Y/N [N]: y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Identity Mapping Service...
Stopping ISE pxGrid processes...
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE pxGrid processes...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Identity Mapping Service...
Starting ISE AD Connector...
```

インストールおよびアップグレード履歴の表示

Note: ISE Processes are initializing. Use 'show application status ise' CLI to verify all processes are in running state.

Cisco ISE により、システムを再起動するように求められます。

ステップ3 システムを再起動する場合は **Y** と入力します。

インストールおよびアップグレード履歴の表示

Cisco ISE は Cisco ISE リリースおよびパッチのインストール、アップグレード、およびアンインストールの詳細を表示するコマンドラインインターフェイス (CLI) コマンドを提供します。 **show version history** コマンドでは次の詳細が提供されます。

- 日付: インストールまたはアンインストールが実行された日時
- アプリケーション: Cisco ISE アプリケーション
- バージョン: インストールまたは削除されたバージョン
- 操作: インストール、アンインストール、パッチのインストール、パッチのアンインストール
- バンドル ファイル名: インストールまたは削除されたバンドルの名前
- リポジトリ: Cisco ISE アプリケーション バンドルがインストールされたリポジトリ
インストールには適用されません。

ステップ1 Cisco ISE CLI にログインします。

ステップ2 コマンド **show version history** を入力します。

次の出力が表示されます。

```
ise/admin# show version history
-----
Install Date: Fri Nov 30 21:48:58 UTC 2022
Application: ise
Version: 3.x.0.xxx
Install type: Application Install
Bundle filename: ise.tar.gz
Repository: SystemDefaultPkgRepos

ise/admin#
```

システムの消去の実行

Cisco ISE アプライアンスまたは VM からすべての情報を安全に消去するために、システムの消去を実行できます。システムの消去を実行するこのオプションは、Cisco ISE が NIST Special Publication 800-88 データ破壊に関する標準を確実に準拠するようにします。

始める前に

次の接続関連の状態が原因で、Cisco ISE ソフトウェア DVD を使用して Cisco ISE アプライアンスを起動しようとしたときに問題が発生する可能性があることを理解しておいてください。

- ターミナル サーバーにシリアル コンソールから Cisco ISE アプライアンスへの `exec` に設定された接続が関連付けられている。これを `no exec` に設定すると、KVM 接続およびシリアル コンソール接続を使用できるようになります。
- Cisco ISE アプライアンスへのキーボードおよびビデオ モニタ (KVM) 接続がある (これはリモート KVM または VMware vSphere Client コンソール接続のいずれかの場合があります)。
- Cisco ISE アプライアンスへのシリアル コンソール接続がある。

ステップ 1 Cisco ISE アプライアンスの電源がオンになっていることを確認します。

ステップ 2 Cisco ISE ソフトウェア DVD を挿入します。

ステップ 3 矢印キーを使用して [システムユーティリティ (シリアルコンソール) (System Utilities (Serial Console))] を選択して、Enter キーを押します。

次に示すような ISO ユーティリティ メニューが表示されます。

```
Available System Utilities:

[1] Recover administrator password
[2] Virtual Machine Resource Check
[3] System Erase
[q] Quit and reload

Enter option [1 - 3] q to Quit:
```

ステップ 4 **3** を入力してシステムの消去を実行します。

コンソールに次のメッセージが表示されます。

```
***** W A R N I N G *****
THIS UTILITY WILL PERFORM A SYSTEM ERASE ON THE DISK DEVICE(S). THIS PROCESS CAN TAKE UP TO 5 HOURS
TO COMPLETE. THE RESULT WILL BE COMPLETE
DATA LOSS OF THE HARD DISK. THE SYSTEM WILL NO LONGER BOOT AND WILL REQUIRE A RE-IMAGE FROM INSTALL
MEDIA TO RESTORE TO FACTORY DEFAULT STATE.

ARE YOU SURE YOU WANT TO CONTINUE? [Y/N] Y
```

ステップ 5 **y** と入力します。

コンソールプロンプトで、別の警告が表示されます。

```
THIS IS YOUR LAST CHANGE TO CANCEL. PROCEED WITH SYSTEM ERASE? [Y/N] Y
```

ステップ 6 **Y**を入力してシステムの消去を実行します。

コンソールに次のメッセージが表示されます。

```
Deleting system disk, please wait...
Writing random data to all sectors of disk device (/dev/sda)...
Writing zeros to all sectors of disk device (/dev/sda)...
Completed! System is now erased.
Press <Enter> to reboot.
```

システムの消去を実行した後、アプライアンスを再利用する場合は、Cisco ISE DVD を使用してシステムを起動し、起動メニューからインストール オプションを選択します。

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。