Common System Maintenance Tasks

Bond Ethernet Interfaces for High Availability

Cisco ISE supports bonding of two Ethernet interfaces into a single virtual interface to provide high availability for the physical interfaces. This feature is called Network Interface Card (NIC) bonding or NIC teaming. When two interfaces are bonded, the two NICs appear to be a single device with a single MAC address.

The NIC bonding feature in Cisco ISE does not support load balancing or link aggregation features. Cisco ISE supports only the high availability feature of NIC bonding.

The bonding of interfaces ensures that Cisco ISE services are not affected when there is:

- Physical interface failure

- Loss of switch port connectivity (shut or failure)

- Switch line card failure

When two interfaces are bonded, one of the interfaces becomes the primary interface and the other becomes the backup interface. When two interfaces are bonded, all traffic normally flows through the primary interface. If the primary interface fails for some reason, the backup interface takes over and handles all the traffic. The bond takes the IP address and MAC address of the primary interface.

When you configure the NIC bonding feature, Cisco ISE pairs fixed physical NICs to form bonded NICs. The following table outlines which NICs can be bonded together to form a bonded interface.

Table 1: Physical NICs Bonded Together to Form an Interface

Cisco ISE Physical NIC Name	Linux Physical NIC Name	Role in Bonded NIC	Bonded NIC Name
Gigabit Ethernet 0	Eth0	Primary	Bond 0
Gigabit Ethernet 1	Eth1	Backup	
Gigabit Ethernet 2	Eth2	Primary	Bond 1
Gigabit Ethernet 3	Eth3	Backup	
Gigabit Ethernet 4	Eth4	Primary	Bond 2
Gigabit Ethernet 5	Eth5	Backup	

Supported Platforms

The NIC bonding feature is supported on all supported platforms and node personas. The supported platforms include:

- SNS hardware appliances - Bond 0, 1, and 2

- VMware virtual machines - Bond 0, 1, and 2 (if six NICs are available to the virtual machine)

- Linux KVM nodes - Bond 0, 1, and 2 (if six NICs are available to the virtual machine)

Guidelines for Bonding Ethernet Interfaces

- As Cisco ISE supports up to six Ethernet interfaces, it can have only three bonds, bond 0, bond 1, and bond 2.

- You cannot change the interfaces that are part of a bond or change the role of the interface in a bond. See the above table for information on which NICs can be bonded together and their role in the bond.

- The Eth0 interface acts as both the management interface as well as the runtime interface. The other interfaces act as runtime interfaces.

- Before you create a bond, the primary interface (primary NIC) must be assigned an IP address. The Eth0 interface must be assigned an IPv4 address before you create bond 0. Similarly, before you create bond 1 and 2, Eth2 and Eth4 interfaces must be assigned an IPv4 or IPv6 address, respectively.

- Before you create a bond, if the backup interface (Eth1, Eth3, and Eth5) has an IP address assigned, remove the IP address from the backup interface. The backup interface should not be assigned an IP address.

- You can choose to create only one bond (bond 0) and allow the rest of the interfaces to remain as is. In this case, bond 0 acts as the management interface and runtime interface, and the rest of the interfaces act as runtime interfaces.

- You can change the IP address of the primary interface in a bond. The new IP address is assigned to the bonded interface because it assumes the IP address of the primary interface.

- When you remove the bond between two interfaces, the IP address assigned to the bonded interface is assigned back to the primary interface.

- If you want to configure the NIC bonding feature on a Cisco ISE node that is part of a deployment, you must deregister the node from the deployment, configure NIC bonding, and then register the node back to the deployment.

- If a physical interface that acts as a primary interface in a bond (Eth0, Eth2, or Eth4 interface) has static route configured, the static routes are automatically updated to operate on the bonded interface instead of the physical interface.

Configure NIC Bonding

You can configure NIC bonding from the Cisco ISE CLI. The following procedure explains how you can configure bond 0 between Eth0 and Eth1 interfaces.

Before you begin

If a physical interface that acts as a backup interface (for example, Eth1, Eth3, Eth5 interfaces), is configured with an IP address, you must remove the IP address from the backup interface. The backup interface should not be assigned an IP address.

Step 1 Log in to Cisco ISE CLI with your administrator account.

Step 2 Enter **configure terminal** to enter the configuration mode.

Step 3 Enter the **interface GigabitEthernet 0** command.

Step 4 Enter the **backup interface GigabitEthernet 1** command.
The console displays:

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

Step 5 Enter **Y** and press **Enter**.

Bond 0 is now configured. Cisco ISE restarts automatically. Wait for some time to ensure that all the services are up and running successfully. Enter the **show application status ise** command from the CLI to check if all the services are running.

```
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)#
```

Verify NIC Bonding Configuration

To verify if NIC bonding feature is configured, run the **show running-config** command from the Cisco ISE CLI. You will see an output similar to the following:

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

In the output above, "backup interface GigabitEthernet 1" indicates that NIC bonding is configured on Gigabit Ethernet 0, with Gigabit Ethernet 0 being the primary interface and Gigabit Ethernet 1 being the backup interface. Also, the ADE-OS configuration does not display an IP address on the backup interface in the running config, even though the primary and backup interfaces effectively have the same IP address.

You can also run the **show interface** command to see the bonded interfaces.

```
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
```

Remove NIC Bonding

Use the **no** form of the **backup interface** command to remove a NIC bond.

Before you begin

Step 1   Log in to Cisco ISE CLI with your administrator account.

Step 2   Enter **configure terminal** to enter the configuration mode.

Step 3   Enter the **interface GigabitEthernet 0** command.

Step 4   Enter the **no backup interface GigabitEthernet 1** command.

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

Step 5   Enter **Y** and press Enter.

Bond 0 is now removed. Cisco ISE restarts automatically. Wait for some time to ensure that all the services are up and running successfully. Enter the **show application status ise** command from the CLI to check if all the services are running.

```
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)#
```

Reset a Lost, Forgotten, or Compromised Password Using a DVD

Before you begin

Make sure you understand the following connection-related conditions that can cause a problem when attempting to use the Cisco ISE Software DVD to start up a Cisco ISE appliance:

- You have a terminal server associated with the serial console connection to the Cisco ISE appliance that is set to exec. Setting it to *no exec* allows you to use a keyboard and video monitor connection and a serial console connection.

- You have a keyboard and video monitor connection to the Cisco ISE appliance (this can be either a remote keyboard and a video monitor connection or a VMware vSphere client console connection).

- You have a serial console connection to the Cisco ISE appliance.

Step 1 Ensure that the Cisco ISE appliance is powered up.

Step 2 Insert the Cisco ISE Software DVD.

Step 3 Use the arrow keys to select **System Utilities (Serial Console)** if you use a local serial console port connection or select **System Utilities (Keyboard/Monitor)** if you use a keyboard and video monitor connection to the appliance, and press **Enter**.

The system displays the ISO utilities menu as shown below.

```
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:
```

Step 4 Enter **1** to recover the administrator password.

The console displays:

```
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]:
```

Step 5   Enter the number corresponding to the admin user whose password you want to reset.

Step 6   Enter the new password and verify it.

Step 7   Enter **Y** to save the changes.

Reset a Disabled Password Due to Administrator Lockout

An administrator can enter an incorrect password enough times to disable the account. The minimum and default number of attempts is five.

Use these instructions to reset the administrator user interface password with the **application reset-passwd ise** command in the Cisco ISE CLI. It does not affect the CLI password of the administrator. After you successfully reset the administrator password, the credentials are immediately active and you can log in without having to reboot the system. .

Cisco ISE adds a log entry in the **Administrator Logins** window. To view this window, click the **Menu** icon (≡) and choose **Operations** > **Reports** > **Reports** > **Audit** > **Administrator Logins**. The credentials for that administrator ID is suspended until you reset the password associated with that administrator ID.

Step 1   Access the direct-console CLI and enter:

application reset-passwd ise administrator_ID

Step 2   Specify and confirm a new password that is different from the previous two passwords that were used for this administrator ID:

```
Enter new password:
Confirm new password:

Password reset successfully
```

Return Material Authorization

In case of a Return Material Authorization (RMA), if you are replacing individual components on an SNS server, be sure to reimage the appliance before you install Cisco ISE. Contact Cisco TAC for assistance.

Change the IP Address of a Cisco ISE Appliance

Before you begin

- Ensure that the Cisco ISE node is in a standalone state before you change the IP address. If the node is part of a distributed deployment, deregister the node from the deployment and make it a standalone node.

• Do not use the **no ip address** command when you change the Cisco ISE appliance IP address.

Step 1   Log in to the Cisco ISE CLI.

Step 2   Enter the following commands:

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

The system prompts you for the IP address change. Enter **Y**. A screen similar to the following one appears.

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

Cisco ISE prompts you to restart the system.

Step 3   Enter **Y** to restart the system.

View Installation and Upgrade History

Cisco ISE provides a Command Line Interface (CLI) command to view the details of installation, upgrade, and uninstallation of Cisco ISE releases and patches. The **show version history** command provides the following details:

• Date—Date and time at which the installation or uninstallation was performed

• Application—Cisco ISE application

• Version—Version that was installed or removed.

• Action—Installation, Uninstallation, Patch Installation, or Patch Uninstallation

- Bundle Filename—Name of the bundle that was installed or removed

- Repository—Repository from which the Cisco ISE application bundle was installed. Not applicable for uninstallation.

Step 1   Log in to the Cisco ISE CLI.

Step 2   Enter the following command: **show version history**.

The following output appears:

```
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#
```

Perform a System Erase

You can perform a system erase to securely erase all information from your Cisco ISE appliance or VM. This option to perform a system erase ensures that Cisco ISE is compliant with the NIST Special Publication 800-88 data destruction standards.

Before you begin

Make sure you understand the following connection-related conditions that can cause a problem when attempting to use the Cisco ISE Software DVD to start up a Cisco ISE appliance:

- You have a terminal server associated with the serial console connection to the Cisco ISE appliance that is set to exec. Setting it to *no exec* allows you to use a KVM connection and a serial console connection.

- You have a keyboard and video monitor (KVM) connection to the Cisco ISE appliance (this can be either a remote KVM or a VMware vSphere client console connection).

- You have a serial console connection to the Cisco ISE appliance.

Step 1   Ensure that the Cisco ISE appliance is powered up.

Step 2   Insert the Cisco ISE Software DVD.

Step 3   Use the arrow keys to select **System Utilities (Serial Console)**, and press Enter.

The system displays the ISO utilities menu as shown below:

```
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:
```

Step 4   Enter **3** to perform a system erase.

The console displays:

```
 **********   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
```

Step 5   Enter **Y**.

The console prompts you with another warning:

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

Step 6   Enter **Y** to perform a system erase.

The console displays:

```
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.
```

After you perform a system erase, if you want to reuse the appliance, you must boot the system using the Cisco ISE DVD and choose the install option from the boot menu.