Changing IP addresses on Exadata Database Machine (Doc ID 1317159.1)

In this Document

APPLIES TO:

Oracle Exadata Hardware - Version 11.2.0.1 and later
Information in this document applies to any platform.

GOAL

The procedure in this document supports the changing of IP addresses on an Oracle Exadata Database Machine system. The most common use case for this procedure is when a system is moved, so this document was written with that case in mind. Importantly, system hostnames and domain name changes are not handled by this procedure.

SOLUTION

This document is divided into the tasks of changing the IP address in each individual network. These sections can be combined into changing all the IP addresses as in the most common use case for readdressing is when an Exadata system is moved.

Importantly, keep in mind that changing the system hostnames, domain name, or Cluster name are not covered in this document. Those changes can be quite extensive and some will require a complete reinstall.

The procedures in this document primarily describe how to change the IP addresses for the management and client access networks. In the spirit of not duplicating procedures, the primary source for changing the IP addresses of the Private InfiniBand network, can be found in:

Oracle Database Machine Owner's Guide
Chapter 7 - Maintaining Oracle Exadata Database Machine
Section "Changing InfiniBand IP Addresses and Host Names."

Assumptions

The following assumptions apply to the procedures outlined here. These steps are tested with Oracle Grid Infrastructure 11.2.0.2 to 12.1.0.2. Using version 11.2.0.1 should not require any modifications, but should be tested with care.

- The grid infrastructure is installed in ORACLE_HOME=/u01/app/12.1.0.2/grid
- The eth0 interface on all systems is used for the management network.
- The Client Access network on the database nodes uses a bonded interface named bondeth0 (older systems may call this bond1).
- The grid infrastructure owner and the database owner are the same users, oracle.
- The following documentation IP addresses are used (see RFC 5737). For the Management network (192.0.2.0/23) and the Client network (198.51.100.0/23).
- That user equivalence is properly configured for both the root and oracle users.

Pre-Move procedures

In most cases, address changes occur because the Exadata system is being physically moved. This covers the initial shutdown of the system as all reconfiguration will be completed at the destination site.

1. As oracle, stop all databases on the cluster by running the following command once for each database.
   (oracle)$ srvctl stop database -d <dbname>
2. If DBFS is in use, as oracle, stop the DBFS clusterware resource(s):
   (oracle)$ crsctl stop resource dbfs_mount
3. As root, stop clusterware on all nodes:
4. (root)# crsctl stop cluster -all
5. As root, check to see if clusterware startup is set for auto-start:
   (root)# dcli -g dbs_ib_group -l root /u01/app/12.1.0.2/grid/bin/crsctl config crs
   dm01db01-priv: CRS-4622: Oracle High Availability Services autostart is enabled.
   dm01db02-priv: CRS-4622: Oracle High Availability Services autostart is enabled.
6. As root, disable clusterware startup if it is set for auto start:
   (root)# dcli -g dbs_ib_group -l root /u01/app/12.1.0.2/grid/bin/crsctl disable crs
7. Power can be shut down on all nodes in preparation of the rack being moved. See the manual:
   Oracle Exadata Database Machine Maintenance Guide
   Chapter 1 General Maintenance Information
   Powering On and Off Oracle Exadata Rack
8. Once these nodes are shut down, the DNS entries should be updated to reflect the new IP addresses. This should be done as soon as possible in the process so that DNS caches will be allowed time to be refreshed.

Post-Move Startup Procedures

1. Verify the DNS entries have been updated. Ensure that all management network IPs, Client Access network IPs, Virtual IPs (VIPs), and SCAN IPs have been updated in DNS and are resolving properly in both forward (query by name) and reverse (query by IP address) DNS queries.
2. Connect the new network connections on the system.

3. All systems should be powered up. Cluster should not start automatically at boot since it was disabled before shutdown. Ensure that the clusterware is not running on any of the database nodes.
4. If the system has been physically moved, verification of the hardware may be required and is not covered in this document.

If the default gateway is to be changed:

This is a fairly simple procedure that can be performed independently of the change in either the Public or Management network.

1. Shut down the network stack:
   (root)# service network stop

2. Edit the /etc/sysconfig/network file to update the GATEWAY parameter. Depending on the chosen network design, this could be either a router on the Public Access network, or the Management network.

If the NTP, DNS, or Time Zone is to be changed

If the only changes are to specify updated NTP or DNS servers, please follow the proper sections in the:
Database Machine Maintenance Guide
Chapter 4 Maintaining Other Components of Oracle Exadata Racks

Management Network Change

Gather information for new addresses

Using the new IP address and netmask, compute the IP range's broadcast and network addresses using a utility like ipcalc. The ipcalc utility doesn't make any changes on the system and can be run at any time; it just helps with computing the values for various fields in the subsequent updates. Make note of these values as they will be used later.

```
(root)# ipcalc -bnm 192.0.2.66 255.255.254.0
NETMASK=255.255.254.0
BROADCAST=192.0.3.255
NETWORK=192.0.2.0
```

Alternatively, one can use CIDR notation instead:

```
(root)# ipcalc -bnm 192.0.2.66/23
NETMASK=255.255.254.0
BROADCAST=192.0.3.255
NETWORK=192.0.2.0
```

Validate the choice of the default gateway for the system. Depending on the network design choice, it can either be a router on either the Public Access network or the Management network. If in doubt, use the same choice of network as the original configuration but use the new address for the new subnet.
Set the $ORACLE_ to the grid home:

/u01/app/12.1.0.2/grid

Then prepend $ORACLE_HOME/bin to the PATH.

It might be advantageous to set the environment for root and the oracle software owner in separate terminal sessions. Various commands below have to be run by either root or oracle. They will be differentiated by notation of either "(root)#" or "(oracle)$" as part of the command prompt.

Database node OS Reconfiguration

Note that each database node will need to be modified manually and individually. It may be helpful to utilize the private network to connect from one system to another. For example, if one database node is reconfigured using the console, it may be possible to then leave the server room and connect remotely to the newly reconfigured database node. From that database node, it will be possible to use the private network to connect to the remaining nodes to reconfigure them. This assumes the Private network has not changed.

1. Shut down the management interface, if it is not already down:
   (root)# ifdown eth0

2. On each Database node, modify the file:
   /etc/sysconfig/network-scripts/ifcfg-eth0
   with the new IPADDR, NETMASK, BROADCAST, GATEWAY, and NETWORK parameters.

   If a backup of the original file is made, use a prefix to name the file like "backup-ifcfg-eth0". If a suffix is used, like ".orig" the OS will interpret the ifcfg-eth0.orig file as a configuration file for the eth0.orig device and will cause network configuration problems at boot time.
3. Modify the routing rules if the database node has them. In some recent image versions, the default deployment may include routing rules. If these files exist:
   /etc/sysconfig/network-scripts/route-eth0
   /etc/sysconfig/network-scripts/rule-eth0
   they require modification. The rule-eth0 file contains the management IP address and the route-eth0 file contains the management network number and netmask (in CIDR notation), like these:

   ```
   (root)#cat rule-eth0
   from 192.0.2.8 table 220
   to 192.0.2.8 table 220
   (root)#cat route-eth0
   192.0.2.0/23 dev eth0 table 220
   default via 192.0.2.1 dev eth0 table 220
   ```

   These files, if present, require modification to the new IP address and new network numbers and netmask in CIDR notation - see reference:
   http://en.wikipedia.org/wiki/CIDR#Prefix_aggregation
   for translation between the quad-dotted notation and CIDR notation. Also see Document 1306154.1 for more information regarding routing configurations on Exadata servers.

4. Update the /etc/hosts file for the existing entries with the new management network addresses.
5. If the network service was stopped, check your work now and restart it:
   (root)# service network start
   If just the eth0 interface was changed, restart it
   (root)# ifup eth0
   This will validate the above files were properly modified. Please follow the next steps if applicable. At the step where the Database node is to be rebooted, please follow that step at that time.
6. Review the /etc/ssh/sshd_config to find any uncommented ListenAddress lines. If there are uncommented ListenAddress entries, update the entry corresponding to the old management network IP addresses with the new management network IP address.
7. If the addresses of the name servers are changing, follow the section above for changing DNS.
8. If the addresses of the time servers are changing, follow the section above for changing NTP.
9. If the time zone is changing follow the section above for changing Time Zone.
10. To change the ILOM network settings, run these commands from the command line of the Database node using the proper new values for that node's ILOM. Substitute your proper addresses for NTP servers, DNS (only one DNS entry is allowed), IP address, gateway, and netmask.

    ```
    (root)# ipmitool sunoem cli "set /SP/clients/ntp/server/1 address=203.0.113.140"
    (root)# ipmitool sunoem cli "set /SP/clients/ntp/server/2 address=203.0.113.141"
    (root)# ipmitool sunoem cli "set /SP/clients/dns nameserver=203.0.113.52"
    (root)# ipmitool sunoem cli "set /SP/network \
    ```

```
        pendingipaddress=192.0.2.29 \
        pendingipgateway=192.0.2.1 \
        pendingipnetmask=255.255.252.0 \
        commitpending=true"
```

11. Verify the settings are in place:

```
    (root)# ipmitool sunoem cli "show /SP/clients/ntp/server/1"
    (root)# ipmitool sunoem cli "show /SP/clients/ntp/server/2"
    (root)# ipmitool sunoem cli "show /SP/clients/dns"
    (root)# ipmitool sunoem cli "show /SP/network"
```

12. Reboot the Database node once these changes are made so that the new updates can take effect.
13. Verify that ILOM is accessible. The ILOM network changes should be immediate (once commitpending=true is sent through).

Oracle Grid Infrastructure Reconfiguration

The Oracle Grid Infrastructure does not use the Management Network. No changes need to be made to the Oracle Grid Infrastructure for this section.

Storage Cell Reconfiguration

This change will need to be completed locally on each storage cell.

1. If the SMTP server or SNMP server used at the new location or on the new network configuration have changed, those settings need to be updated on each storage cell. For example, if the storage cell's SMTP server require update, it may be set using a command like this:
   (root)# dcli -g cell_group -l root "cellcli -e alter cell \
   smtpserver=\'new.smtp.server.com\'"
2. From the management node (often the first database node), stop the cell services on all storage nodes by running:
   (root)# dcli -g cell_ib_group -l root cellcli -e alter cell shutdown services all
3. From the management node, backup the configuration file:
   (root)# dcli -g cell_ib_group -l root cp /opt/oracle.cellos/cell.conf /root/new.cell.conf
4. Reconfigure each cell using ipconf. It needs to be run interactively. First shut down all the cell services, and then run ipconf.
   (root)# cellcli -e alter cell shutdown services all
   (root)# /opt/oracle.cellos/ipconf
   (root)# cellcli -e alter cell startup services all

   An alternate method is to change settings using this "bulk" method. It is faster, but it results in a configuration that *adds* the NTP server(s) and DNS server(s) to the existing ones instead of replacing the old ones with the new ones.
   a. On each cell, edit /root/new.cell.conf to make the changes to only the following fields. Other settings in this file should not be modified.

```
        <Interface>
        <Name>eth0</Name>
        <Net_Type>Magement</Net_Type>
        <Gateway>{new gateway}</Gateway>
        <IP_address>{new address}</IP_address>
        <Netmask>{new netmask}</Netmask>
        </Interface>
        <Ntp_servers>{first new time server}</Ntp_servers>
        <Ntp_servers>{second new time server}</Ntp_servers>
```

```
<Nameservers>{first new name server}</Nameservers>
<Nameservers>{second new name server}</Nameservers>
<Timezone>{new timezone}</Timezone>
<ilom>
<ILOM_Gateway>{new gateway}</ILOM_Gateway>
<ILOM_IP_address>{new address}</ILOM_IP_address>
<ILOM_Nameserver>
{new name servers comma delimited}</ILOM_Nameserver>
<ILOM_Netmask>{new netmask}</ILOM_Netmask>
<ILOM_First_NTP_server>{first new time server}</ILOM_First_NTP_server>
<ILOM_Second_NTP_server>{second new time server}</ILOM_Second_NTP_server>
<ILOM_Timezone>{new timezone}</ILOM_Timezone>
</ilom>
```

  b. On each cell, commit the changes to the cell's config (the cell will reboot):
     (root)# /opt/oracle.cellos/ipconf -force -newconf /root/new.cell.conf -reboot
  c. After reboot, on each cell, verify the modified configuration file:
     (root)# /opt/oracle.cellos/ipconf -verify -conf /root/new.cell.conf -verbose

     If the above procedure does not work properly or does not produce the desired results, you should run the ipconf utility interactively instead.

 5. Reboot the cell and once it comes back on line, as a final check verify that cell services are running:
    (root)# dcli -g cell_ib_group -l root cellcli –e list cell detail

InfiniBand Switch reconfiguration

To reconfigure the manage network in the InfiniBand switches, follow the procedures in the Exadata Database Machine Installation and Configuration Guide, Chapter 5 Configuring Oracle Exadata Database Machine, in the section labeled "Configuring Sun Datacenter InfiniBand Switch 36 Switch."
For procedures to change the DNS, NTP addresses, or Time Zone, see the Oracle Exadata Database Machine Maintenance Guide, Chapter 4 Maintaining Other Components of Oracle Exadata Racks, in the respective sections labeled either "Changing the DNS Servers" or "Changing the NTP Servers".

Cisco Ethernet switch reconfiguration

Note that before making any Cisco Ethernet switch changes, the network administrator should be consulted to verify that the switch's configuration may be modified using the default deployment procedures and assumptions in this section.
To reconfigure the Cisco Ethernet switch, follow the procedures in the Oracle Exadata Database Machine Installation and Configuration Guide, Chapter 5 Configuring Oracle Exadata Database Machine, in the section labeled "Configuring the Cisco Ethernet Switch".

For procedures to change the DNS, NTP addresses, or Time Zone, see the Oracle Exadata Database Machine Maintenance Guide, Chapter 4 Maintaining Other Components of Oracle Exadata Racks, in the respective sections labeled either "Changing the DNS Servers" or "Changing the NTP Servers".

Power Distribution Unit (PDU) reconfiguration

If the PDUs are connected to the network, they require reconfiguration. If not, this section may be skipped.
To reconfigure the PDUs, follow the procedures in the Oracle Exadata Database Machine Installation and Configuration Guide, Chapter 5 Configuring Oracle Exadata Database Machine, in the section labeled "Configuring the Power Distribution Units."

KVM switch reconfiguration

To reconfigure the KVM switch, see the Oracle Exadata Database Machine Maintenance Guide, Chapter 4 Maintaining Other Components of Oracle Exadata Racks, in the section labeled "Configuring the KVM Switch." This section also includes changing the DNS and NTP servers.

Client Access Network Change

The interrelationship of the network stack and the Clusterware requires changes to occur in order. In essence, the applicable components of the Clusterware need to be stopped, the network changed, and then the Cluster reconfigured to accommodate the network changes.

This document assumes the names for the SCAN, VIP and hosts do not change. The only changes made are to the IP addresses. If the various names change, there will be more steps necessary. These steps are not covered in this document.

The Storage Cells do not have a public facing interface. No changes are required for them.

Once all nodes are reconfigured with proper IP addresses and all nodes are running, grid infrastructure may be reconfigured. This procedure cannot be done in a rolling fashion, so a database outage must be taken.

Note that each database node will need to be modified separately and manually. It may be helpful to utilize the private network to connect from one system to another. For example, if one database node is reconfigured using the console, it may be possible to then leave the server room and connect remotely to the newly reconfigured database node. From that database node, it will be possible to use the private network to connect to the remaining nodes to reconfigure them.

Gather information for new addresses

Using the new IP address and netmask, compute that IP range's broadcast and network addresses using ipcalc. The ipcalc utility doesn't make any changes on the system and can be run at any time; it just helps with computing the values for various fields in the subsequent updates. Make note of these values as they will be used later.

```
(root)# ipcalc -bnm 198.51.100.66 255.255.254.0
NETMASK=255.255.254.0
BROADCAST=198.51.101.255
NETWORK=198.51.100.0
```

 Alternatively, one can use CIDR notation instead:

```
(root)# ipcalc -bnm 198.51.100.66/23
NETMASK=255.255.254.0
BROADCAST=198.51.101.255
NETWORK=198.51.100.0
```

Validate the choice of the default gateway for the system. Depending on the network design choice, it can either be a router on either the Public Access network or the Management network. If in doubt, use the same choice of network as the original configuration but use the new address for the new subnet.

Set the $ORACLE_ to the grid home:

/u01/app/12.1.0.2/grid

Then prepend $ORACLE_HOME/bin to the PATH.

It might be advantageous to set the environment for root and the oracle software owner in separate terminal sessions. Various commands below have to be run by either root or oracle. They will be differentiated by notation of either "(root)#" or "(oracle)$" as part of the command prompt.

Procedure on Database nodes

1. If not already started, start the cluster on all nodes:
   (root)# dcli -g dbs_group -l root /u01/app/12.1.0.2/grid/bin/crsctl start crs
   And verify:
   (root)# crsctl stat res -t
2. Verify the current network configuration. This command should be run as oracle on one node in the cluster.
   (oracle)$ oifcfg getif
3. Check the existing cluster and OS configuration
   (oracle)$ srvctl config scan
   (oracle)$ srvctl config nodeapps
   (oracle)$ oifcfg getif
   (root#) ifconfig
4. Stop the Clusterware components
   (oracle)$ srvctl stop listener -node {each node}
   (oracle)$ srvctl stop scan_listener
   In 12.2 and later the Cluster Health Analyzer was introduced. It uses the new Management database and that database listener uses a VIP. Before stopping all the VIP's, this service needs to be stopped.
   (oracle)$ srvctl stop cha
   (oracle)$ srvctl stop mgmtdb
   (oracle)$ srvctl stop mgmtlsnr
   (oracle)$ srvctl stop vip -n {each node}
   (oracle)$ srvctl stop scan
   And validate the state of the various components
   (oracle)$ srvctl status scan
   (oracle)$ srvctl status nodeapps
   (root)# ifconfig
5. Delete the current public network interface from the configuration. This command should be run as oracle on only one node in the cluster.
   (oracle)$ oifcfg delif -global bondeth0
6. On each Database node change the IP address of bondeth0.
   a. Shut down the Public interface, if it is not already down
      (root)# ifdown bondeth0
      If the network stack was shut down in Step 2, this step can be skipped, or the error ignored.
   b. Modify the file:
      /etc/sysconfig/network-scripts/ifcfg-bondeth0
      To this file change IPADDR, NETMASK, BROADCAST, GATEWAY, and NETWORK parameters with the new values.
      If a backup of the original file is made, use a prefix to name the file like "backup-ifcfg-bondeth0". If a suffix is used, like ".orig" the OS will interpret the ifcfg-bondeth0.orig file as a device's configuration file and will cause network configuration problems at boot time.
   c. Modify the routing rules if the database node has them. In some recent image versions, the default deployment may include routing rules. If the files exist, they require modification:
      (root)# ls /etc/sysconfig/network-scripts/route-bondeth0
      (root)# ls /etc/sysconfig/network-scripts/rule-bondeth0
      The rule-bondeth0 file contains the Public IP address and the route-bondeth0 file contains the Public network number and netmask (in CIDR notation), like these:

      ```
      (root)# cat rule-bondeth0
      from 198.51.100.8 table 220
      to 198.51.100.8 table 220
      (root)# cat route-bondeth0
      198.51.100.0/23 dev bondeth0 table 220
      default via 198.51.100.1 dev bondeth0 table 220
      ```

These files, if present, require modification to the new IP address and new network numbers with the netmask in CIDR notation - see reference:
http://en.wikipedia.org/wiki/CIDR#Prefix_aggregation
for translation between the quad-dotted notation and CIDR notation. Also see Document 1306154.1 for more information regarding routing configurations on Exadata servers.

If a backup of the original files are made, use a prefix to name the file like "backup-urle-bondeth0". If a suffix is used, like ".orig" the OS will interpret the rule-bondeth0.orig file as a device's rule file and will cause network configuration problems at boot time.

d. If the default gateway is the bondeth0 interface, modify the /etc/sysconfig/network file to change the GATEWAY parameter.

e. Update the /etc/hosts file for the existing entries with the new Public network addresses. Also, the DNS should be updated with the new addresses for SCAN/VIP/and host names.

f. If the network service was stopped, check your work now and restart it:
(root)# service network start
If just the bondeth0 interface was changed, restart it:
(root)# ifup bondeth0
This will validate the above files were properly modified.

7. Using the new NETWORK number computed on the DB nodes for the bondeth0 interface. This command should be run as oracle on only one node in the cluster.
   (oracle)$ oifcfg setif -global bondeth0/198.51.100.0:public

8. Verify the new network configuration.
   (oracle)$ oifcfg getif

9. Modify the network resource to update the new network configuration. These commands should be run as root on only one node in the cluster. The NETWORK number for the Client Access network computed above. Use the fully qualified domain name for the <new-scan-name> in the follow command.
   (root)# srvctl modify network –netnum 1 –subnet 198.51.100.0/255.255.254.0/bondeth0 -pingtarget 198.51.100.1

10. Modify the scan to update its IP addresses as the oracle user on only one node in the cluster.
    (oracle)$ srvctl modify scan –netnum 1 –scanname scan.mycluster.example.com

11. Verify the current SCAN configuration. This command should be run as oracle on only one node in the cluster.
    (oracle)$ srvctl config scan

12. Depending on the system's original configuration, more advanced features, such as Valid Node Checking for Registration of services with the Listener may need to be reconfigured. For VNCR changes see note 1914282.1. For other features, please check their reference notes or documentation.

13. Restart the various Clusterware components:
    (oracle)$ srvctl start vip -node {each node}
    (oracle)$ srvctl start listener
    (oracle)$ srvctl start scan
    (oracle)$ srvctl start scan_listener
    In 12.2 and later, starting the Cluster Health Analyzer will start the Management database and its listener.
    (oracle)$ srvctl start cha

14. Validate the changes made:
    (oracle)$ srvctl status nodeapps
    (oracle)$ srvctl status scan_listener
    (oracle)$ srvctl status cha

15. For the last check, restart clusterware on all nodes. These commands should be run as root on only one node in the cluster.
    (root)# /u01/app/12.1.0.2/grid/bin/crsctl stop cluster -all
    (root)# /u01/app/12.1.0.2/grid/bin/crsctl start cluster -all

16. If Clusterware was set for auto start previously, re-enable it to auto start. This command should be run as root on only one node in the cluster.
    (root)# dcli -g dbs_group -l root /u01/app/12.1.0.2/grid/bin/crsctl enable crs

17. Restart the database(s). This command should be run as oracle on only one node in the cluster.
    (oracle)$ srvctl start database -d <dbname>

18. Start dbfs resource(s). This command should be run as oracle on only one node in the cluster.
    (oracle)$ crsctl start res dbfs_mount

19. The LOCAL_LISTENER parameter should not be set in the spfile and will automatically be set by the Clusterware. The SCAN name didn't change, so REMOTE_LISTENER parameter in the database(s) shouldn't need to change. If the SCAN name changes, you'll also need to update the instance initialization parameters for your database instance(s) as appropriate. Some instances might be using the LISTENER_NETWORKS parameter which may require separate updates as well if there are IP addresses embedded in it.

20. If you plan on using EM Cloud Control to monitor this cluster, please ensure that you re-generate onecommand configuration files with the new IP addresses. To re-generate these configuration files, use the Oracle Exadata Deployment Assistant as outlined in the Oracle Exadata Database Machine Owner's Guide.

Private Network Change

For changing the Private Infiniband network IP addresses please refer to the Oracle Exadata Database Machine Maintenance Guide, Chapter 4 "Maintaining Other Components of Oracle Exadata Racks" in the section titled "Changing InfiniBand IP Addresses and Host Names"

REFERENCES

NOTE:952903.1 - How to Update the IP Address of the SCAN VIP Resources (ora.scan{n}.vip)
NOTE:283684.1 - How to Modify Private Network Information in Oracle Clusterware
NOTE:972500.1 - How to Modify SCAN Setting or SCAN Listener Port after Installation
NOTE:1306154.1 - Configuring Exadata Database Server Routing
NOTE:1531298.1 - How To Change The Domain Name In An Exadata Environment
   Didn't find what you are looking for?