Oracle® Communications
Integrated Diameter Intelligence Hub

IDIH 7.X Disaster Recovery Guide

Release 7.0

E56375-02

Feburary 2015

IDIH 7.x Disaster Recovery, Release 7.0

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*.

Table of Contents

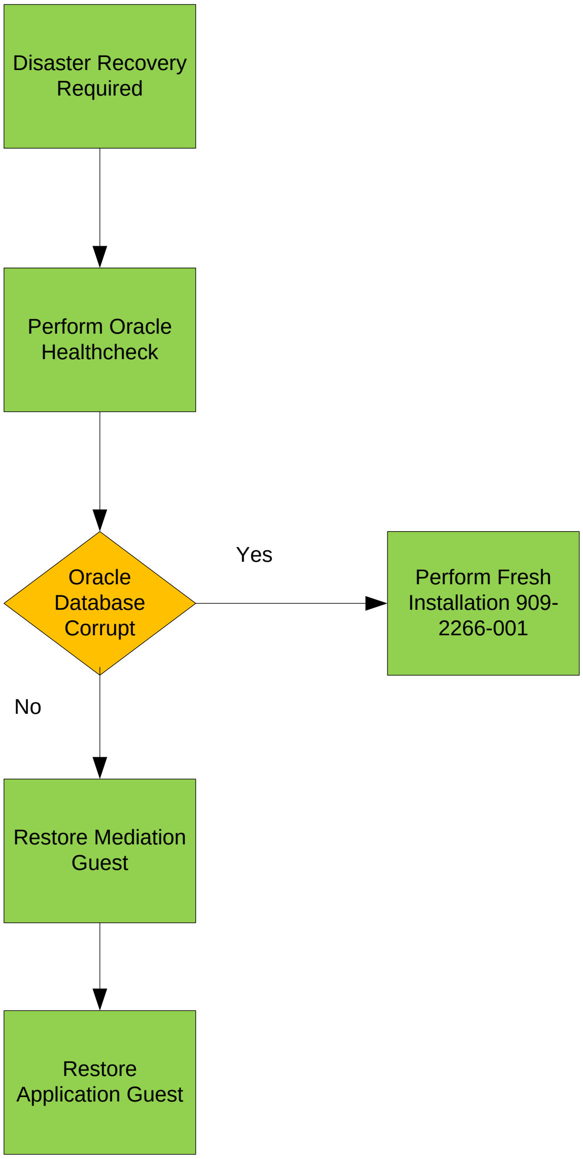
Chapter 1

Disaster Recovery Overview

Topics:

1.1 Disaster Recovery Overview

This section provides the disaster recovery overview for the IDIH system. The flowcharts below depict the flow of Disaster Recovery. You would use the trouble-shooting guide to determine when a disaster recovery is required. If you determine that the Oracle database is corrupt with the trouble-shooting guide or with the Oracle health-check then you need to perform a fresh installation as outlined in documentE56571-02.


Disaster Recovery Required
Perform Oracle Healthcheck
Oracle Database Corrupt
Yes
Perform Fresh Installation 909-2266-001
No
Restore Mediation Guest
Restore Application Guest

Chapter 2

Disaster Recovery Procedures

Topics:

2.1 Disaster Recovery Preparation

Note: The disaster recovery procedure enables the user to preserve the existing database data, However if the database is known to be corrupt follow the Installation ProcedureE56571-02.

1. **Verify the necessary IDIH software images are available on the PM&C server.**
   a) Open a web browser and log into the PM&C server as pmacadmin.
   b) Select the "Software" folder and click on the "Manage Software Images" link.
   c) Verify the current IDIH TVOE, TPD, Oracle, Application and Mediation images are listed.

   Note: If the necessary software images are not available please follow the instructions in the IDIH Installation Document E56571-02 and upload the necessary images.

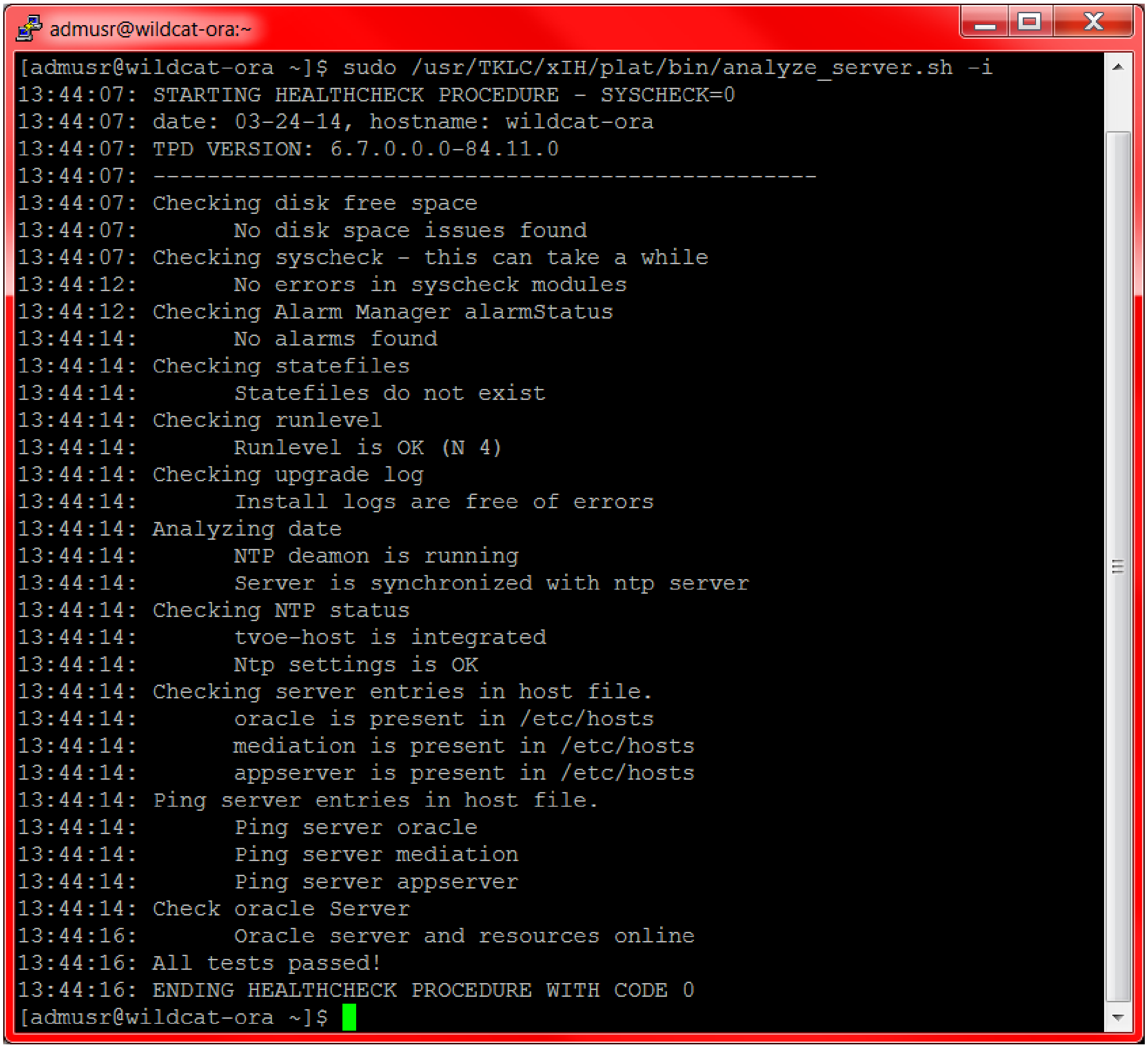
2.2 Database Health-check

Warning: If the Oracle Health-check fails you must perform a fresh installation.

1. Run the Oracle Health-check to verify the Oracle Database is not corrupt.

a) As admusr run the Oracle Health-Check and verify the database status.

- sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i



```
[admusr@wildcat-ora ~]$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i
13:44:07: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
13:44:07: date: 03-24-14, hostname: wildcat-ora
13:44:07: TPD VERSION: 6.7.0.0.0-84.11.0
13:44:07: -------------------------------------------------
13:44:07: Checking disk free space
13:44:07:       No disk space issues found
13:44:07: Checking syscheck - this can take a while
13:44:12:       No errors in syscheck modules
13:44:12: Checking Alarm Manager alarmStatus
13:44:14:       No alarms found
13:44:14: Checking statefiles
13:44:14:       Statefiles do not exist
13:44:14: Checking runlevel
13:44:14:       Runlevel is OK (N 4)
13:44:14: Checking upgrade log
13:44:14:       Install logs are free of errors
13:44:14: Analyzing date
13:44:14:       NTP deamon is running
13:44:14:       Server is synchronized with ntp server
13:44:14: Checking NTP status
13:44:14:       tvoe-host is integrated
13:44:14:       Ntp settings is OK
13:44:14: Checking server entries in host file.
13:44:14:       oracle is present in /etc/hosts
13:44:14:       mediation is present in /etc/hosts
13:44:14:       appserver is present in /etc/hosts
13:44:14: Ping server entries in host file.
13:44:14:       Ping server oracle
13:44:14:       Ping server mediation
13:44:14:       Ping server appserver
13:44:14: Check oracle Server
13:44:16:       Oracle server and resources online
13:44:16: All tests passed!
13:44:16: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
[admusr@wildcat-ora ~]$
```

b) Run the Oracle Health-Check and verify the database status, the screen should match the "Check oracle Server -> Oracle server and resources online". If they do not then the Oracle database is corrupt and the installation must be run. If the status matches the output seen above then continue to the next step.

2. **Shutdown each of the IDIH guest in an orderly fashion.**

   Warning: You must run "init 0" as root on each of the guest to preserve the Oracle Database.

   a) As root user on the TVOE host open a virsh console on the mediation guest.
      - virsh console mediation
   b) As root on the mediation console run the "init 0" command.
      - init 0
   c) Wait for the mediation guest to shutdown, when it is fully shutdown, it will kick you out of the mediation console and you once again be root on the TVOE host
   d) As root user on the TVOE host open a virsh console on the application guest.
      - virsh console application
   e) As root on the application console run the "init 0" command.
      - init 0
   f) Wait for the application guest to shutdown, when it is fully shutdown, it will kick you out of the application console and you once again be root on the TVOE host

   NOTE: Do NOT shutdown Oracle Database guest server.

2.3 Mediation and Application Guest Restore

1. **Verify the Mediation and Application guest state.**
   a) Open a web browser and log into the PM&C server as pmacadmin.
   b) On the Main Menu Select "VM Management".
   c) On the Virtual Machine Management Menu, Select the IDIH TVOE host.
   d) On the VM Entities Menu, Select the mediation guest.
      - Verify "Current Power State: Shutdown"
   e) On the VM Entities Menu, Select the application guest.
      - Verify "Current Power State: Shutdown"

2. **Verify the Disaster Recovery FDC files exists on the PMAC in the "/var/TKLC/smac/guest-dropin" directory.**
   a) As "admusr" user on the change directory to guest-dropin.
      - cd /var/TKLC/smac/guest-dropin
   b) If the FDC disaster recovery file exists move onto step 3.
   c) To create the FDC file run the following command as "admusr".
      - sudo /usr/TKLC/smac/html/TPD/mediation*/gen-dr_fdc_file.sh <idih>.xml
      - After the execution, a file of DisasterRecovery<idih>.xml will be generated.

        Note: The <idih>.xml file is the same fdconfig file used to fresh install the system from the PMAC server.

3. Update release numbers in the software section in the FDC file to make sure it has the version numbers equal to the release that you are upgrading to.

4. **As admusr user run the "fdconfig config" command, be sure you use the Disaster Recovery FDC file.**

   Warning: If you run the "fdconfig config" command with the installation FDC your oracle server will be overwritten.

   a) As "admusr" run the "fdconfig config" command.
      - sudo fdconfig config --file=DisasterRecovery<idih>.xml .

   b) Monitor the fdconfig configuration from the shell and from the PMAC GUI under "Task Monitoring"

   c) Verify all Healthchecks performed by fdconfig have passed in the Task Monitor window on the PMAC.

   Note: The IPM and Upgrade should take approximately 1 hour and 45 minutes.

Chapter 3

Post Disaster Recovery Procedures

Topics:

3.1 Post Disaster Recovery

Perform site configuration from the Application server GUI.

a) Verify all applications are deployed on the application server.

1. Open a web browser and login as idihadmin on the NSP application interfaces.
   a. URL http://10.240.15.118/idih
2. Verify the following applications are deployed. The will be displayed as icon choices on the application server home page.

   Alarm Forwarding
   Audit Viewer
   Log Viewer
   OAM
   ProTrace
   System Alarms

Configure DSR Reference Data Synchronization for IDIH

After an IDIH fresh installation, reference data synchronization is initially disabled. Reference data synchronization requires some initial configuration before it is enabled.

The Trace Ref Data Adapter application must retrieve data from web services hosted by the DSR SO web server, and this requires the DSR Site OAM virtual IP address (VIP) to be configured. The DSR SO VIP will be unique at each customer site because it is defined based on the customer's network configuration. Therefore, we have no standard default value for the DSR SO VIP.

1. Log into an IDIH app server terminal window as LINUX user **tekelec**.
2. Execute script: `apps/trda-config.sh`
3. For prompt "**Please enter DSR oam server IP address**", enter the virtual IP address of the DSR Site OAM and press Enter.
   - If the address entered is unreachable the script will exit with error "**Unable to connect to <*ip-address*>!**".
   - Entry of a reachable address causes the trace-refdata-adapter application to be enabled in the Weblogic server.
   - This is sample terminal output for a successful execution of script `apps/trda-config.sh`:

```
demo1-app:/usr/TKLC/xIH apps/trda-config.sh
dos2unix: converting file
/usr/TKLC/xIH/bea/user_projects/domains/tekelec/nsp/trace-refdata-
adapter.properties to UNIX format ...
Please enter DSR oam server IP address: 10.240.39.175
dos2unix: converting file /usr/TKLC/xIH/bea/user_projects/domains/tekelec/nsp/trace-refdata-adapter.properties
to UNIX format ...
Buildfile: build.xml

app.disable:

common.weblogic.stop:
     [echo]
     [echo]
     [echo] ====================================================================
     [echo] application: xihtra
     [echo] ====================================================================
     [echo] === stop application EAR
     [java] weblogic.Deployer invoked with options:  -adminurl http://appserver:7001 -userconfigfile
/usr/TKLC/xIH/bea/user_projects/domains/tekelec/configfile.secure -userkeyfile
/usr/TKLC/xIH/bea/user_projects/domains/tekelec/keyfile.secure -name xIH Trace Reference Data Adapter -stop
     [java] <Oct 17, 2013 11:35:32 AM EDT> <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating stop operation
for application, xIH Trace Reference Data Adapter [archive: null], to configured targets.>
     [java] Task 4 initiated: [Deployer:149026]stop application xIH Trace Reference Data Adapter on nsp.
     [java] Task 4 completed: [Deployer:149026]stop application xIH Trace Reference Data Adapter on nsp.
     [java] Target state: stop completed on Server nsp
     [java]

BUILD SUCCESSFUL
Total time: 1 minute 3 seconds
Buildfile: build.xml

app.enable:

common.weblogic.start:
     [echo]
     [echo]
     [echo] ====================================================================
     [echo] application: xihtra
     [echo] ====================================================================
     [echo] === start application EAR
     [java] weblogic.Deployer invoked with options:  -adminurl http://appserver:7001 -userconfigfile
/usr/TKLC/xIH/bea/user_projects/domains/tekelec/configfile.secure -userkeyfile
/usr/TKLC/xIH/bea/user_projects/domains/tekelec/keyfile.secure -name xIH Trace Reference Data Adapter -start
     [java] <Oct 17, 2013 11:36:36 AM EDT> <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating start
operation for application, xIH Trace Reference Data Adapter [archive: null], to configured targets.>
     [java] Task 5 initiated: [Deployer:149026]start application xIH Trace Reference Data Adapter on nsp.
     [java] Task 5 completed: [Deployer:149026]start application xIH Trace Reference Data Adapter on nsp.
     [java] Target state: start completed on Server nsp
     [java]

BUILD SUCCESSFUL
Total time: 1 minute 3 seconds
```

4. Monitor log file **`/var/TKLC/xIH/log/apps/weblogic/apps/application.log`** for log entries containing text "**Trace Reference Data Adapter**".

Setting up the SSO Domain.

a) Confirm that DNS has been configure in the DSR OAM.

1. Log into the DSR ACTIVE NETWORK OAM&P as user **guiadmin.**
2. Access menu **Administration→Remote Servers→DNS Configuration** to display the web page.
3. In the System Domain section of the page, Confirm that a value has been entered for field **Domain Name**.

4. In the External DNS Name Servers section of the page, confirm that field **Name Server 1** has a value.
5. In the Domain Search Order section of the page, confirm that field **Search Domain 1** has a value.
6. If any previously mentioned field is not configured, consult the network administrator for proper configuration values before proceeding with steps in this section.
7. Select the Cancel button.

b) Establish the SSO Local Zone in the DSR OAM.

1. Log into the DSR ACTIVE NETWORK OAM&P as user **guiadmin**.
2. Access menu **Administration→Access Control→Certificate Management**.
3. Select button **Establish SSO Zone**.
4. In the **Establish Single Sign-On Authentication Zone** page, enter a value for field **Zone Name**. Example: **dsr**.
5. Select the Ok button. Information for the new Certificate of type **SSO** Local is displayed.
6. Select the Report button. The Certificate Report is displayed. Select and copy the encoded certificate text to the clipboard for future access. Example:

```
-----BEGIN CERTIFICATE-----
MIIEPzCCAyegAwIBAgIBADANBgkqhkiG9w0BAQUFADCBuTELMAkGA1UEBhMCVVMx
FzAVBgNVBAgMDk5vcnRoIENhcm9saW5hMRQwEgYDVQQHDAtNb3JyaXN2aWxsZTEQ
MA4GA1UECgwHVGVrZWxlYzERMA8GA1UECwwIQXBwV29ya3MxMjAwBgNVBAMMKWRz
ci9kb21haW49bGFicy5uYy50ZWtlbGVjLmNvbS90eXBlPUFXU1NPMSIwIAYJKoZI
hvcNAQkBFhNzdXBwb3J0QHRla2VsZWMuY29tMB4XDTEzMDgyNjE3NDM1NVoXDTE0
MDgyNjE3NDM1NVowgbkxCzAJBgNVBAYTAlVTMRcwFQYDVQQIDA5Ob3J0aCBDYXJv
bGluYTEUMBIGA1UEBwwLTW9ycmlzdmlsbGUxEDAOBgNVBAoMB1Rla2VsZWMxETAP
BgNVBAsMCEFwcFdvcmtzMTIwMAYDVQQDDClkc3IvZG9tYWluPWxhYnMubmMudGVr
ZWxlYy5jb20vdHlwZT1BV1NTTzEiMCAGCSqGSIb3DQEJARYTc3VwcG9ydEB0ZWtl
bGVjLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANA7uB1JTv1x
hLKz7Fj7rcH0pqzNUKThUStQkAplOUuOYjMHz5gCBdRqu4LnHRtJ+fIHxAzIoksp
V1C0Ucsl4V+ptAySbQH4cv5swrzAZp2ntzdqqNs3EPFeRwy80Ok9mV4glM1c5ozq
V3EyjE37Bt0kBH1qhiqLhsepvqflGVboZok4zZoCFl4VKfYzCg4wIjhhSTx74o8G
cRG6mNt14xDBNOUaXvngnyrEjvb4ckwbH43hl+0zbBptFV+aRwPrcFpuZ3zaolaf
P7vOK5S8gSgYblnA/DZ2WrXmShxUp8bpH//rH6HS4TvVPSswUnnfyruK48uTogLP
E+v9Mi6UY8ECAwEAAaNQME4wHQYDVR0OBBYEFI9KwcaTlMyoZmNgC1snxjHsAQXM
MB8GA1UdIwQYMBaAFI9KwcaTlMyoZmNgC1snxjHsAQXMMAwGA1UdEwQFMAMBAf8w
DQYJKoZIhvcNAQEFBQADggEBAI96pB+IvJ8xN8agrhE4lVCqL0v2AlqYKRVnASGW
XUYRMkaBEX/soqCHEfj3tS79XOZVajgCcsga0Q/eMw8+1srqNpPJ/u5IwOxnmsE1
nph11+nV9ekUNtvKh53iVjHKYMtoCMEblgEc9O8/rUtxoVz9qIf2EEkSWlazx7UR
iAaB04C0lEXjReHPy0TIqPJzIIsOiAMAza/FdLLEukIqBk3Qg/jkCDe4uCC3zzTu
TGagLMW4oDYxhYuFs5B3m51rBI8arDx4j2TfJVu6Q1pHs0TQu+vRooH1YXxJoJc6
94UUa/UsuamVifGktkcOMenYQbgHvmUXQ/Hic+4adFkA6uE=
      -----END CERTIFICATE-----
```

c) Configure the SSO Domain in the IDIH App Server

1. Log into the IDIH App Server web interface as default user **idihadmin**.
2. Select the OAM portal icon to launch the OAM web application.
3. In the IDIH OAM application, select menu **System->Single Sign On**.
4. In the **System: Single Sign On** page, select the **SSO Parameters** tab.
5. In the **SSO Domain** data entry form, select the **Edit Value** icon button.

6. Enter a value for field **Domain Name**. This should be the same domain name assigned in the DSR OAM&P DNS configuration.
7. Select the **Save** icon button.

d) IDIH App Server, Configure an SSO Remote Zone for the DSR Network OAM&P

1. Log into the IDIH App Server web interface as default user **idihadmin**.
2. Select the OAM portal icon to launch the OAM web application.
3. In the IDIH OAM application, select menu **System->Single Sign On**.
4. In the **System: Single Sign On** page, select the **SSO Zones** tab.
5. In the **SSO Remote Zones** data entry form, select the **Add** icon button.
6. Enter a value for field **Remote Name**. This should be the name for the SSO Local Zone that was configured in the DSR Network OAM&P.
7. In field **X.509 Certificate**, paste the encoded certificate text from the clipboard that was previously copied from the DSR Network OAM&P.
8. Select the **Save** icon button.
9. Select the **Refresh** icon button to display data saved for the Remote Zone.

e) In DSR OAM, Configure the ProTrace Launch URL

1. Open a new web browser window/tab and login to the DSR System OAM.
2. Select menu **"Diameter→Troubleshooting with DIH→Configuration→Options"**.
3. In field **"DIH Visualization address"**, enter the fully qualified IDIH host name. This host name includes the domain as a suffix. The domain is the same as the domain configured in the DSR DNS Configuration.
4. Click the Apply button.