VERIFYING HIGH AVAILABILITY OF TIVOLI ACCESS MANAGER POLICY SERVER USING IBM TIVOLI SYSTEM AUTOMATION FOR MULTIPLATFORMS

BY Chinwe Edeani

Table of Contents

PRODUCTS USED

IBM Tivoli Directory Server version 6.1.0 (LDAP)
IBM Tivoli Access Manager version 6.1.0.1 (TAM)
WebSphere Application Server Edge Components version 7.0 (Load Balancer)
IBM Tivoli System Automation for Multiplatforms version 3.1.0.4 (TSAMP)

SYSTEMS USED

Name	Use
tiv023	LDAP, Edge (with unique cluster IP address)
tiv024	Primary policy server
tiv025	Backup policy server
tiv026	Runtime

All the systems used are SUSE Linux Enterprise Server (SLES) 10 SP2

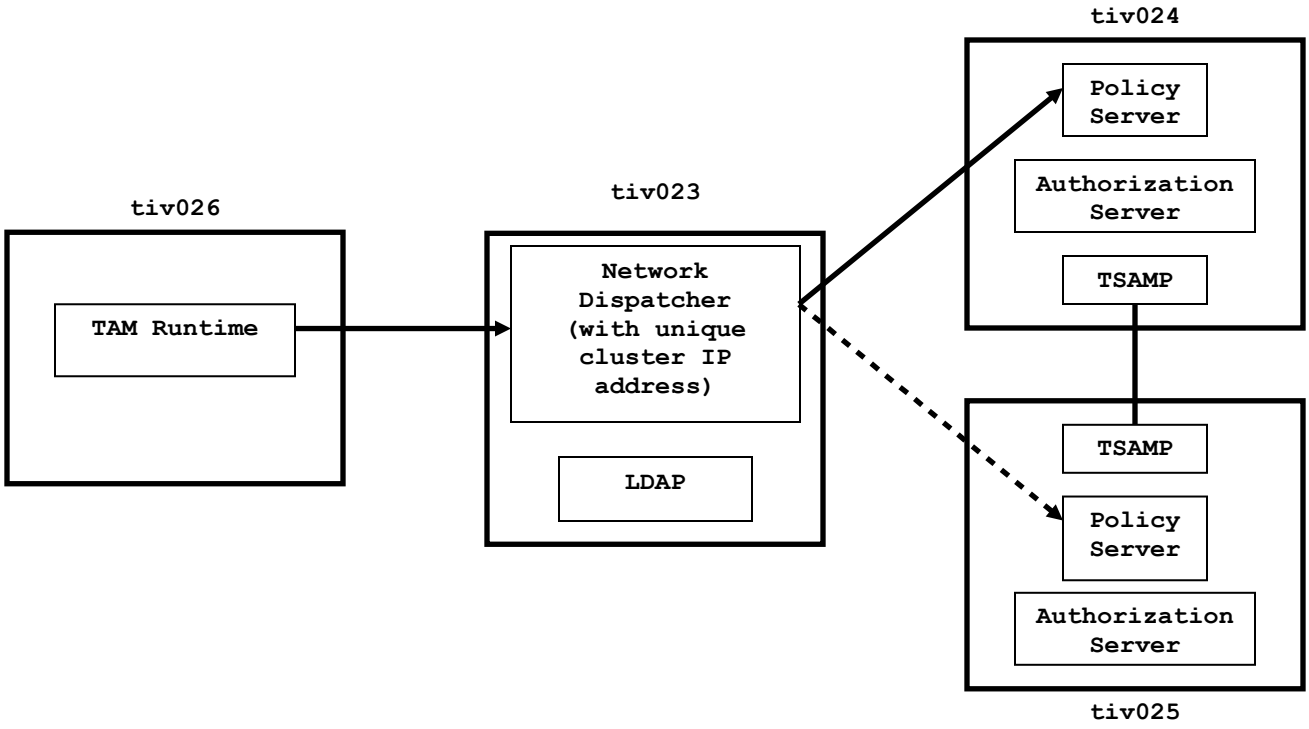


Figure 1: System Configuration
(The solid line is the normal path to the primary TAM system. The broken line is the failover path to the backup system.)

STEP 1: SET UP POLICY AND AUTHORIZATION SERVERS

1.1 Install LDAP on tiv023

Mount install ISOs:

```
tiv023:~ # mount -o loop /opt/amds610-1.LINUX_S390.iso /mnt/disk/
tiv023:~ # mount -o loop /opt/amds610-2.LINUX_S390.iso /mnt/disk2
```

Install Java from ISO, and modify environment variables:

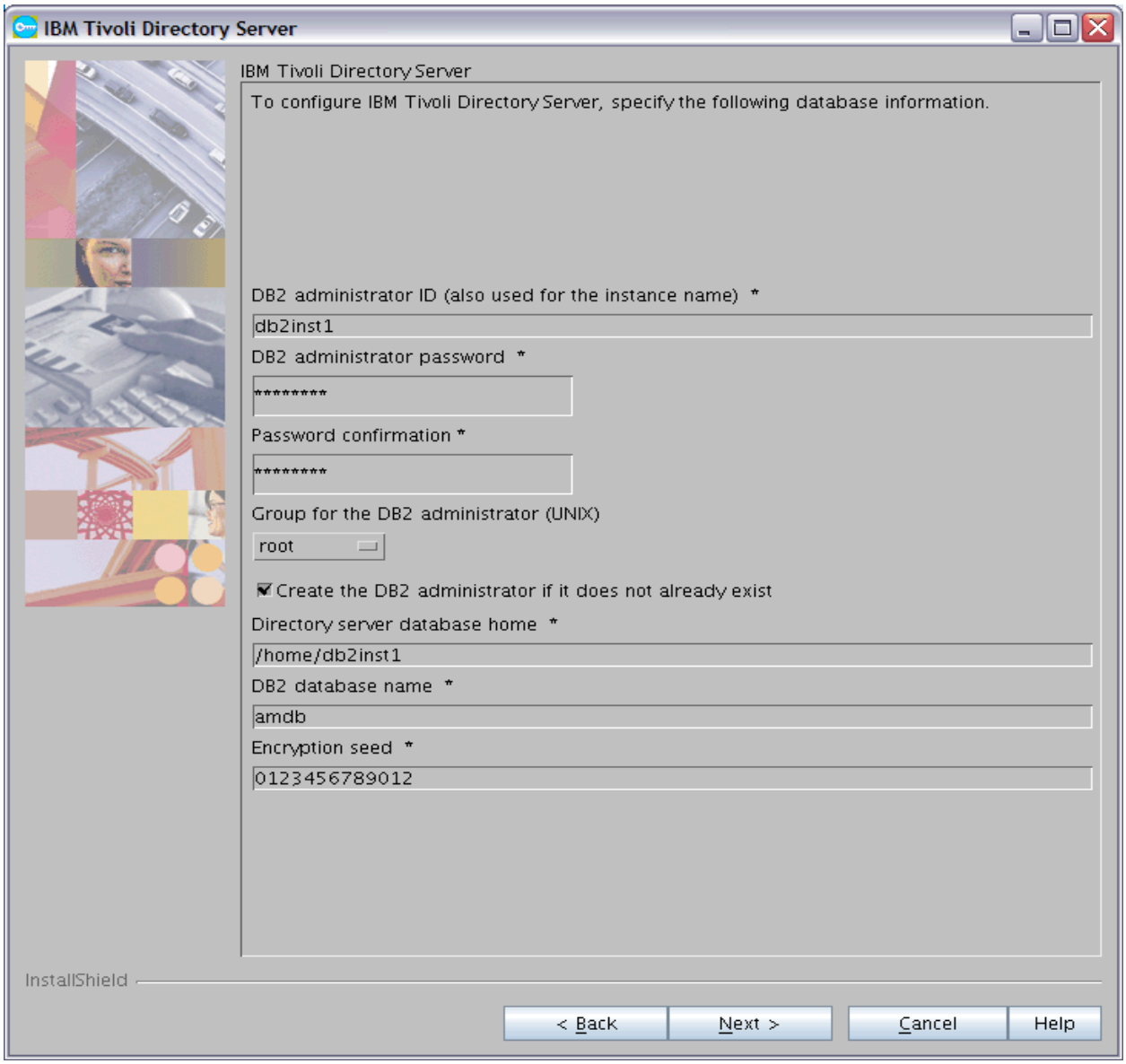
```
tiv023:~ # export JAVA_HOME=/opt/ibm/java2-s390-50/jre
tiv023:~ # export PATH=/opt/ibm/java2-s390-50/jre/bin:$PATH
```

Create and modify needed users and groups:

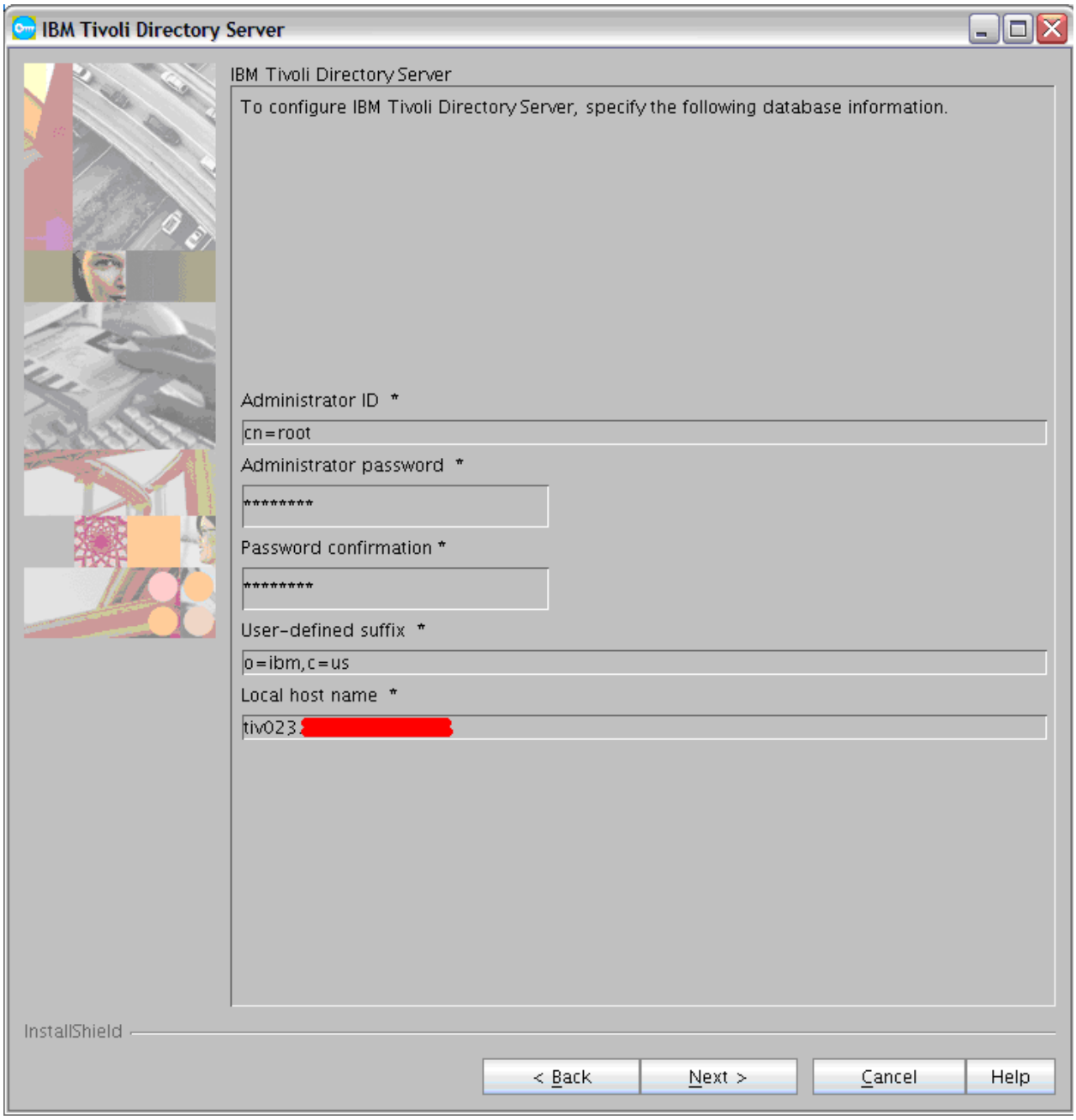
```
tiv023:~ # groupadd db2iadm1
tiv023:~ # groupadd idsldap
tiv023:~ # useradd -g db2iadm1 -G idsldap -d /home/db2inst1 -m db2inst1
tiv023:~ # passwd db2inst1
Changing password for db2inst1.
New Password:
Reenter New Password:
Password changed.
tiv023:~ # groups root
root : root
tiv023:~ # usermod -G db2iadm1,root root
usermod: `root' is primary group name.
tiv023:~ # groups root
root : root db2iadm1
```

Run LDAP installer:

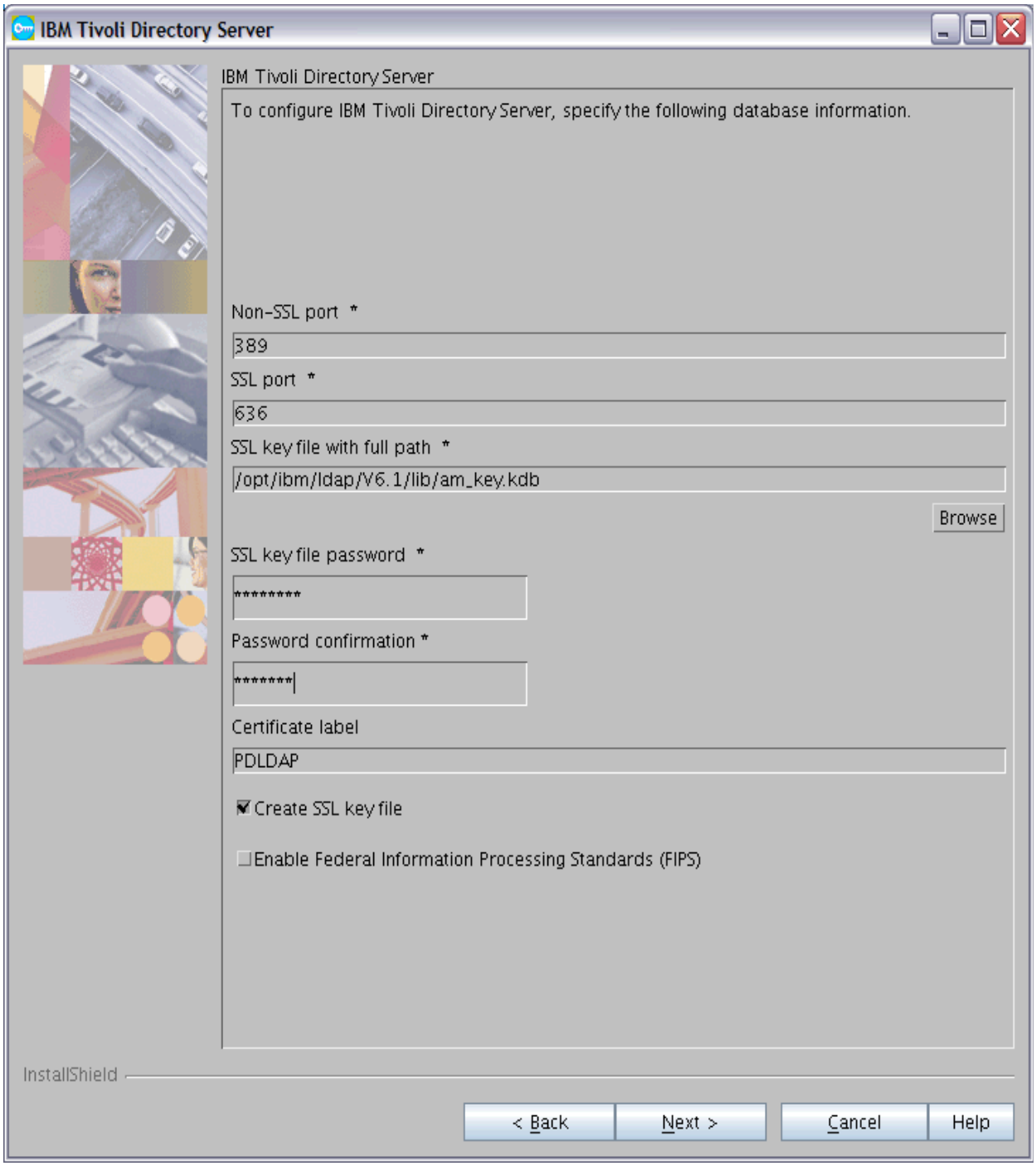
- Enter the DB2 instance name, password, and instance home directory. You can optionally edit the database name, but leave the default encryption seed value:



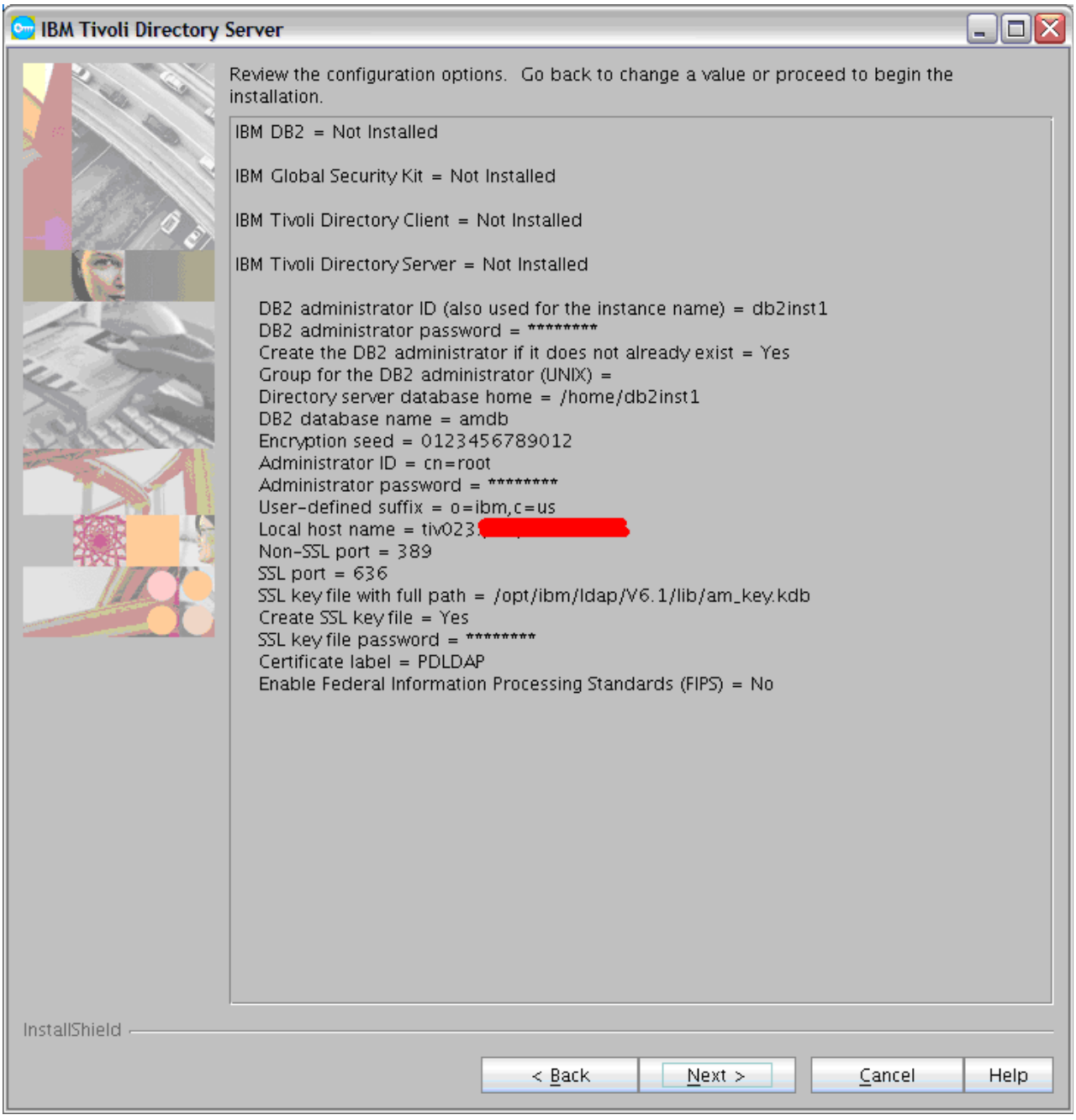
- Enter the LDAP administrator id, password, user suffix and hostname:



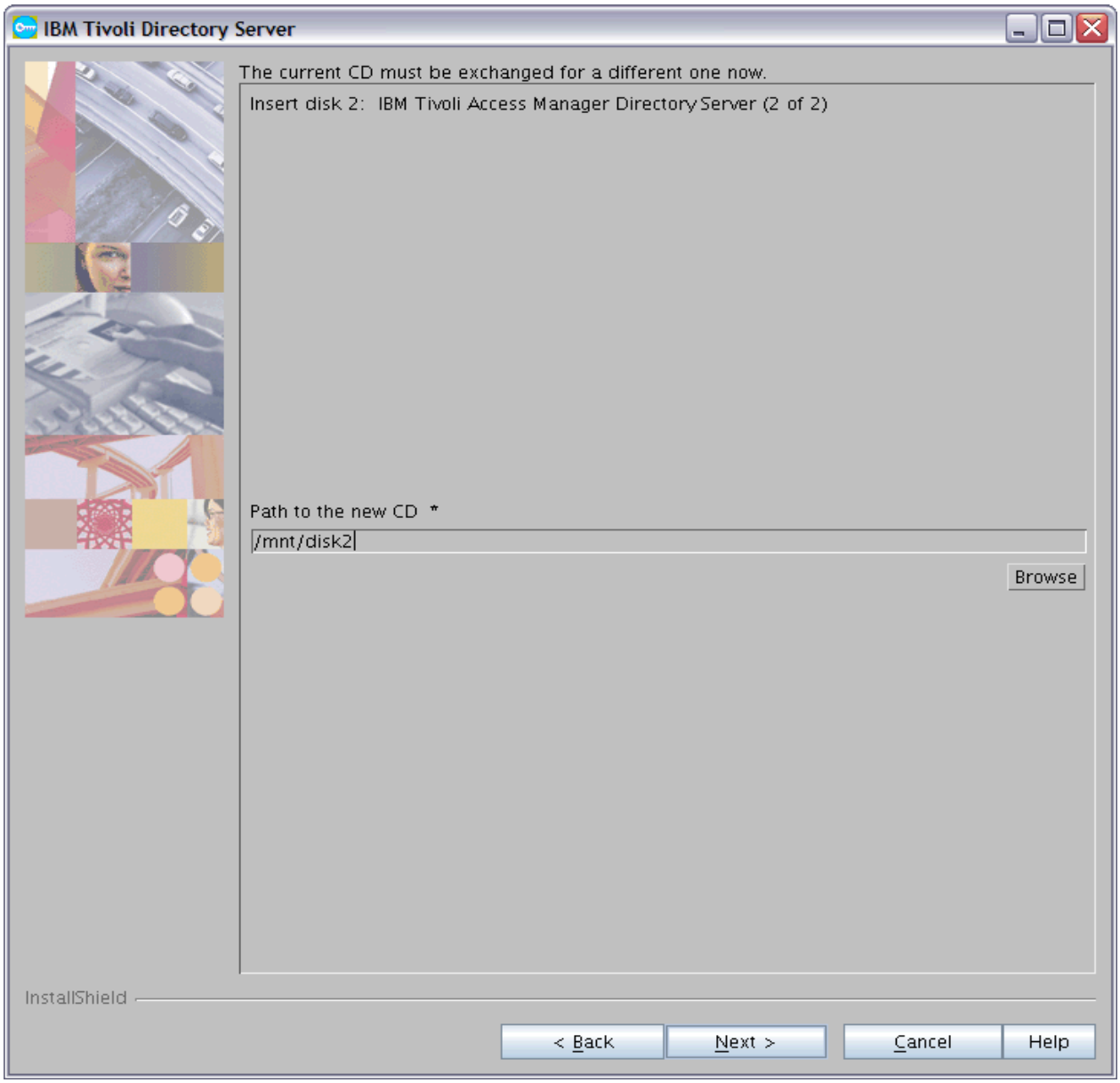
- Enter the SSL key password and leave all other default values:



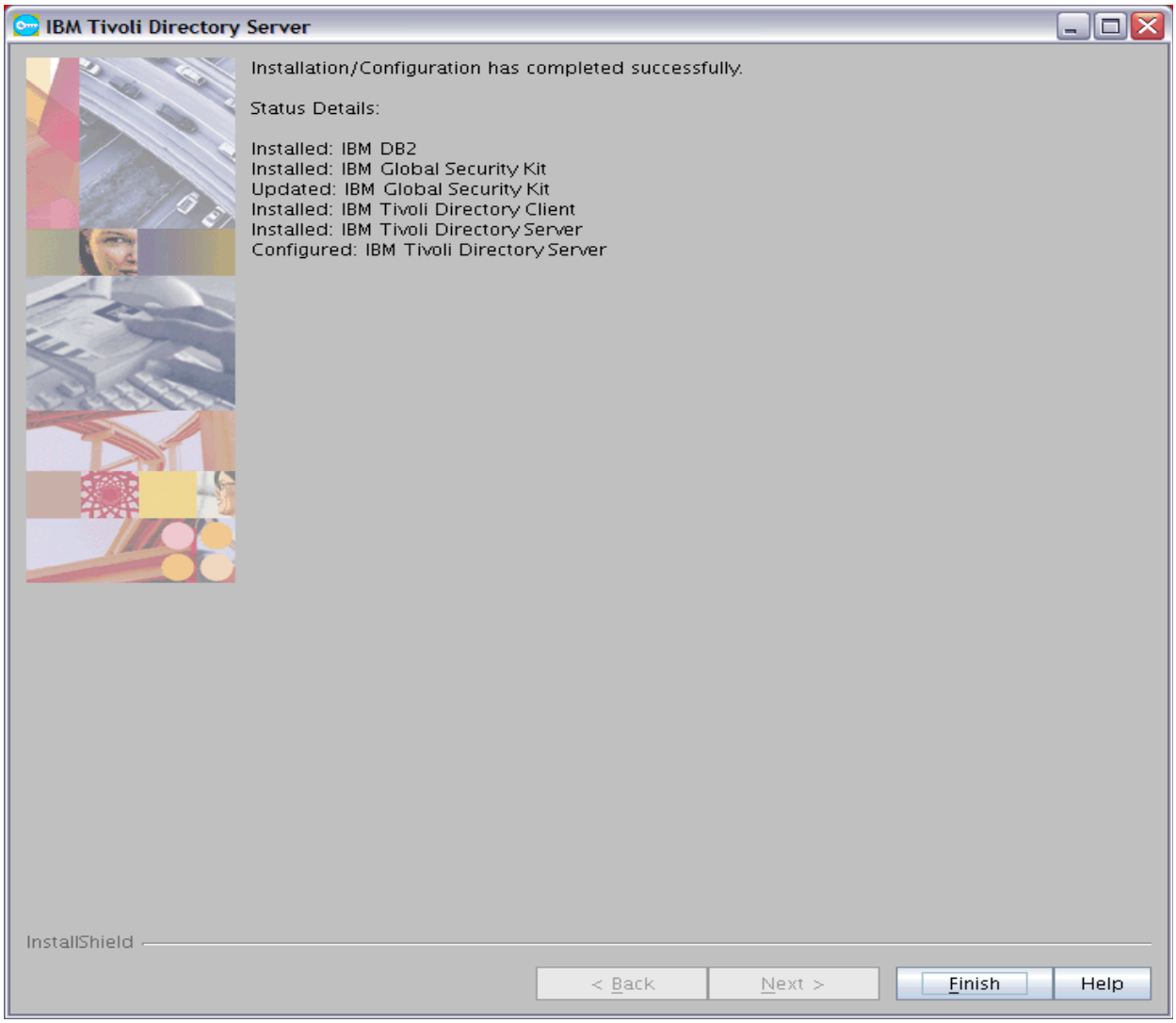
- The summary page will display all your selected values. You can click "Back" to modify unsatisfactory values. If you are satisfied, click "Next" and the installation will begin:



- The second stage of the installation requires the location of part two of the install ISO image. Enter the path and then click “Next”:



- Click “Finish” when the installation is complete:



1.2 Install and configure TAM on tiv024

Install IBM Java:

```
tiv024:/mnt # rpm -ivh ibm-java2-s390-sdk-5.0-5.0.s390.rpm
Preparing...                ########################################### [100%]
   1:ibm-java2-s390-sdk     ########################################### [100%]
tiv024:/mnt # export PATH=/opt/ibm/java2-s390-50/jre/bin:$PATH
tiv024:/mnt # which java
/opt/ibm/java2-s390-50/jre/bin/java
tiv024:/mnt # java -version
java version "1.5.0"
Java(TM) 2 Runtime Environment, Standard Edition (build pxz31dev-20070511(SR5))
IBM J9 VM (build 2.3, J2RE 1.5.0 IBM J9 2.3 Linux s390-31 j9vmxz3123-20070426 (JIT
enabled)
J9VM - 20070420_12448_bHdSMr
JIT  - 20070419_1806_r8
GC   - 200704_19)
JCL  - 20070511
```

Install GSK:

```
tiv024:/mnt # rpm -Uvh gsk7bas-7.0-4.11.s390.rpm
```

```
   Preparing...                ########################################### [100%]
      1:gsk7bas                ########################################### [100%]
```

Install PD packages:

```
   tiv024:/mnt # rpm -ivh TivSecUtl-TivSec-6.1.0-1.s390.rpm PDlic-PD-6.1.0-1.s390.rpm
   PDRTE-PD-6.1.0-1.s390.rpm PDAcld-PD-6.1.0-1.s390.rpm PDMgr-PD-6.1.0-1.s390.rpm
   PDMgrPrxy-PD-6.1.0-1.s390.rpm PDWebRTE-PD-6.1.0-1.s390.rpm PDWeb-PD-6.1.0-1.s390.rpm
   PDWPM-PD-6.1.0-1.s390.rpm PDJrte-PD-6.1.0-1.s390.rpm PDAuthADK-PD-6.1.0-1.s390.rpm
   Preparing...                ########################################### [100%]
   Adding ivmgr user
   Adding tivoli user
   usermod: `root' is primary group name.
   usermod: `root' is primary group name.
   usermod: `ivmgr' is primary group name.
      1:PDlic-PD               ########################################### [  9%]
      2:PDJrte-PD              ########################################### [ 18%]
      3:TivSecUtl-TivSec       ########################################### [ 27%]
      4:PDRTE-PD               ########################################### [ 36%]
      5:PDWebRTE-PD            ########################################### [ 45%]
      6:PDAcld-PD              ########################################### [ 55%]
      7:PDMgr-PD               ########################################### [ 64%]
      8:PDMgrPrxy-PD           ########################################### [ 73%]
      9:PDWeb-PD               ########################################### [ 82%]
     10:PDWPM-PD               ########################################### [ 91%]
     11:PDAuthADK-PD           ########################################### [100%]

   tiv024:/mnt # rpm -ivh idsldap-clt32bit61-6.1.0-6.s390.rpm idsldap-cltbase61-6.1.0-
   6.s390.rpm idsldap-cltjava61-6.1.0-6.s390.rpm
   Preparing...                ########################################### [100%]
      1:idsldap-cltbase61      ########################################### [ 33%]
      2:idsldap-clt32bit61     ########################################### [ 67%]
      3:idsldap-cltjava61      ########################################### [100%]
   Java tar extracted.
```

Configure Runtime:

```
   tiv024:/opt/PolicyDirector/bin # ./pdconfig
           Tivoli Access Manager Configuration Menu

           1. Access Manager Runtime Configuration
           2. Access Manager Policy Server Configuration
           3. Access Manager Policy Proxy Server Configuration
           4. Access Manager Authorization Server Configuration
           5. Access Manager WebSEAL Configuration
           6. Access Manager Web Portal Manager Configuration
           7. Access Manager Runtime for Java Configuration
           x. Return to the Tivoli Access Manager Setup Menu

   Select the menu item [x]: 1
   Tivoli Common Directory logging is not configured.
   This scheme provides a common location for log files for Tivoli products instead of
   separate locations determined by each application.

   Do you want to use Tivoli Common Directory logging (y/n) [No]?

   Log files for this application will be created in directory:
   /var/PolicyDirector/log
```

```
        1. LDAP

   Registry [1]:

   LDAP server host name: <ldap_server_host_name>

   LDAP server port [389]:
   The package has been configured successfully.
```

Configure Policy and Authorization servers:

```
   tiv024:/opt/PolicyDirector/bin # ./pdconfig

           Tivoli Access Manager Setup Menu

           1. Configure Package
           2. Unconfigure Package
           3. Display Configuration Status
           x. Exit

   Select the menu item [x]: 1

           Tivoli Access Manager Configuration Menu

           1. Access Manager Policy Server Configuration
           2. Access Manager Policy Proxy Server Configuration
           3. Access Manager Authorization Server Configuration
           4. Access Manager WebSEAL Configuration
           5. Access Manager Web Portal Manager Configuration
           6. Access Manager Runtime for Java Configuration
           x. Return to the Tivoli Access Manager Setup Menu

   Select the menu item [x]: 1
   LDAP administrator ID [cn=root]:
   LDAP administrator password:

   Management domain name [Default]:

   The LDAP management domain location DN is the location in the LDAP
   server where the management domain information is stored. If the
   LDAP management domain location DN is not specified, the
   management domain information is stored in its own suffix by
   default.  Whether the DN is specified or the default is used,
   the location must already exist in the LDAP server.

   LDAP management domain location DN []:

   Enable SSL between the Tivoli Access Manager policy server
   and the LDAP server (y/n) [Yes]? n

   Provide a password for the Tivoli Access Manager administrator account. The
   administrator login name is sec_master and cannot be changed.

   Tivoli Access Manager administrator password: ******
   Confirm password: ******

   User and group tracking information format
```

```
Selecting Minimal requires fewer LDAP objects to maintain user and group tracking
information.
Previous versions of Access Manager will not be supported in the Minimal environment.

Selecting Standard requires additional LDAP objects to maintain user and group
tracking information.
All versions of Access Manager can participate in the Standard environment.

Enable Minimal Data Format (y/n):[Yes]
Policy server SSL port [7135]:
SSL certificate lifecycle [1460]:

Enable Federal Information Processing Standards (FIPS) (y/n):[No]

* Configuring the server.

Generating the server certificates. This may take a few minutes.

Creating the SSL certificate.  This might take several minutes.
The SSL configuration of the Tivoli Access Manager policy server has completed
successfully.

The policy server's signed SSL certificate is base-64 encoded and saved in text file
"/var/PolicyDirector/keytab/pdcacert.b64."

This file is required by the configuration program on each machine in your secure
domain.
The SSL configuration of Access Control Runtime has completed successfully.
  Tivoli Access Manager policy server domain name:     Default
  Tivoli Access Manager policy server host name:       tiv024
  Tivoli Access Manager policy server listening port:  7135

* Starting the server.

The server has been started.
The package has been configured successfully.

Press Enter to continue.

        Tivoli Access Manager Configuration Menu

        1. Access Manager Policy Proxy Server Configuration
        2. Access Manager Authorization Server Configuration
        3. Access Manager WebSEAL Configuration
        4. Access Manager Web Portal Manager Configuration
        5. Access Manager Runtime for Java Configuration
        x. Return to the Tivoli Access Manager Setup Menu

Select the menu item [x]: 2
Enable SSL between the Tivoli Access Manager authorization
server and the LDAP server (y/n) [Yes]? n
Domain [Default]:
Policy server host name [tiv024]:
Policy server SSL port [7135]:
Tivoli Access Manager administrator ID [sec_master]:
Tivoli Access Manager administrator password: passw0rd
Local host name [tiv024]:
```

```
   Administration request port [7137]:
   Authorization request port [7136]:

   * Configuring the server.

   Configuration of application "ivacld" for host "tiv024" is in progress.
   This might take several minutes.
   The specified action completed successfully.

   * Starting the server.

   The server has been started.
   The package has been configured successfully.
```

Display server status:

```
   tiv024:/opt/PolicyDirector/bin # pd_start status

   Tivoli Access Manager servers

   Server                Enabled       Running
   ------------------------------------------
   pdmgrd                   yes        yes
   pdacld                   yes        yes
   pdmgrproxyd              no         no
```

1.3 Install and configure TAM on tiv025

Install packages as on tiv024...

Check TAM servers status:

```
   tiv025:/opt/PolicyDirector/bin # pd_start status

   Tivoli Access Manager servers

   Server                Enabled       Running
   ------------------------------------------
   pdmgrd                   no         no
   pdacld                   no         no
   pdmgrproxyd              no         no
```

Configure TAM Runtime:

```
   tiv025:/opt/PolicyDirector/bin # ./pdconfig

           Tivoli Access Manager Setup Menu

           1. Configure Package
           2. Unconfigure Package
           3. Display Configuration Status
           x. Exit

   Select the menu item [x]: 1

           Tivoli Access Manager Configuration Menu

           1. Access Manager Runtime Configuration
           2. Access Manager Policy Server Configuration
           3. Access Manager Policy Proxy Server Configuration
```

```
        4. Access Manager Authorization Server Configuration
        5. Access Manager WebSEAL Configuration
        6. Access Manager Web Portal Manager Configuration
        7. Access Manager Runtime for Java Configuration
        x. Return to the Tivoli Access Manager Setup Menu

   Select the menu item [x]: 1
   Tivoli Common Directory logging is not configured.
   This scheme provides a common location for log files
   for Tivoli products instead of separate locations
   determined by each application.

   Do you want to use Tivoli Common Directory logging (y/n) [No]?

   Log files for this application will be created in directory:
   /var/PolicyDirector/log

        1. LDAP

   Registry [1]:

   LDAP server host name: tiv023

   LDAP server port [389]:
   The package has been configured successfully.
```

1.4 Clone policy and authorization servers on tiv024

Display policy and authorization server files on tiv024:

```
   tiv024:/var/PolicyDirector/db # ls -l
   total 844
   -rw------- 1 ivmgr ivmgr 540672 Oct 19 10:38 ivacld.db         -- Authorization server
   db file
   -rw------- 1 ivmgr ivmgr 540672 Oct 19 10:38 master_authzn.db  -- Policy server db file
```

Backup configuration on tiv024:

```
   tiv024:/var/PolicyDirector/db # pdbackup -action backup -list
   /opt/PolicyDirector/etc/pdbackup.lst -path /tmp -file pdbackup.tiv024

   The output was written to /tmp/msg__pdbackup.log
```

It created backup file, pdbackup.tiv024.tar, in /tmp

1.5 Restore configuration on tiv025

Get backup file from tiv024 and restore configuration on tiv025:

```
   tiv025:/opt/PolicyDirector/etc # pdbackup -action restore -file
   /tmp/pdbackup.tiv024.tar

   The output was written to /tmp/msg__pdbackup.log
```

Display policy and authorization server files on tiv025:

```
   tiv025:/var/PolicyDirector/db # ls -l
   total 1064
   -rw------- 1 ivmgr ivmgr 540672 Oct 19 10:38 ivacld.db
   -rw------- 1 ivmgr ivmgr 540672 Oct 19 10:38 master_authzn.db
```

Check configuration status of servers on tiv025:

```
   tiv025:/var/PolicyDirector/db # pdconfig status
```

```
            Tivoli Access Manager Setup Menu

            1. Configure Package
            2. Unconfigure Package
            3. Display Configuration Status
            x. Exit

   Select the menu item [x]: 3

            Tivoli Access Manager Configuration Status

            Package Name Configured?
            ____________________________________________________________

            Access Manager Runtime                          Yes
            Access Manager Policy Server                    Yes
            Access Manager Policy Proxy Server              No
            Access Manager Authorization Server             Yes
            Access Manager WebSEAL                          No
            Access Manager Web Portal Manager               No
            Access Manager Runtime for Java                 No

   tiv025:/var/PolicyDirector/db # pd_start status

   Tivoli Access Manager servers

   Server                 Enabled       Running
   ----------------------------------------
   pdmgrd                    yes       no
   pdacld                    yes       no
   pdmgrproxyd               no        no
```

1.6 Configure unique authorization server on tiv025

Delete authorization server files:

Main configuration file is /opt/PolicyDirector/etc/ivacld.conf. In here are the locations of other files to delete:

/opt/PolicyDirector/etc/ivacld.conf.obf (configuration-database file)
/var/PolicyDirector/keytab/ivacld.kdb (ssl-keyfile)
/var/PolicyDirector/keytab/ivacld.sth (ssl-keyfile-stash)
/var/PolicyDirector/db/ivacld.db (db-file)

Also delete /opt/PolicyDirector/.configure/PDAcld-PD
Finally, delete /opt/PolicyDirector/etc/ivacld.conf

Configure unique authorization server on tiv025:

```
   tiv025:/var/PolicyDirector/db # pdconfig

            Tivoli Access Manager Setup Menu

            1. Configure Package
            2. Unconfigure Package
            3. Display Configuration Status
            x. Exit

   Select the menu item [x]: 1
```

```
          Tivoli Access Manager Configuration Menu

          1. Access Manager Policy Proxy Server Configuration
          2. Access Manager Authorization Server Configuration
          3. Access Manager WebSEAL Configuration
          4. Access Manager Web Portal Manager Configuration
          5. Access Manager Runtime for Java Configuration
          x. Return to the Tivoli Access Manager Setup Menu

   Select the menu item [x]: 2
   Enable SSL between the Tivoli Access Manager authorization
   server and the LDAP server (y/n) [Yes]? n
   Domain [Default]:
   Policy server host name [tiv024]:
   Policy server SSL port [7135]:
   Tivoli Access Manager administrator ID [sec_master]:
   Tivoli Access Manager administrator password:
   Local host name [tiv025]:
   Administration request port [7137]:
   Authorization request port [7136]:

   * Configuring the server.

   Configuration of application "ivacld" for host "tiv025" is in progress.
   This might take several minutes.
   The specified action completed successfully.

   * Starting the server.

   The server has been started.

   The package has been configured successfully.

   tiv025:/var/PolicyDirector/db # pdadmin -a sec_master -p passw0rd
   pdadmin sec_master> server list
       ivacld-tiv024
       ivacld-tiv025
   pdadmin sec_master> exit
```

1.7 Perform update tests to verify TAM servers

The policy and authorization servers on both guests are all using the same policy database. Therefore, updates from either guest are replicated across the policy databases and should be accessible from both guests.

Create an ACL on tiv024 and check replication on tiv025

(tiv024) Make sure policy server (PS) and authorization server (AS) are started:

```
   tiv024:/opt/PolicyDirector/bin # ./pdmgrd
   Tivoli Access Manager policy server v6.1.0.1 (Build 080912b)
   Copyright (C) IBM Corporation 1994-2003.  All Rights Reserved.
   2009-10-19-11:36:09.676-04:00I----- 0x14C521D3 pdmgrd NOTICE mis ivcore cfgmgr.cp    p
   196 0x76be66b0
   HPDMS0467I   Server startup
   2009-10-19-11:36:09.676-04:00I----- 0x14C526F2 pdmgrd NOTICE mis ivmgrd cfgmgr.cp    p
   201 0x76be66b0
   HPDMS1778I   Loading configuration

   tiv024:/opt/PolicyDirector/bin # ./pdacld
```

```
Tivoli Access Manager authorization server v6.1.0.1 (Build 080912b)
Copyright (C) IBM Corporation 1994-2003.  All Rights Reserved.
2009-10-19-11:46:57.814-04:00I----- 0x14C521D3 pdacld NOTICE mis ivcore ivacld.cpp 443
0x76be66b0
HPDMS0467I   Server startup
2009-10-19-11:46:57.815-04:00I----- 0x14C526F2 pdacld NOTICE mis ivmgrd ivacld.cpp 448
0x76be66b0
HPDMS1778I   Loading configuration

tiv024:/opt/PolicyDirector/bin # pd_start status

Tivoli Access Manager servers

Server                 Enabled       Running
----------------------------------------
pdmgrd                    yes        yes
pdacld                    yes        yes
pdmgrproxyd               no         no
```

(tiv024) Create ACL, *testacl*:

```
tiv024:/opt/PolicyDirector/bin # pdadmin -a sec_master -p passw0rd
pdadmin sec_master> acl create testacl
pdadmin sec_master> acl show testacl
    ACL Name: testacl
    Description:
    Entries:
        User sec_master TcmdbsvaBRl
```

(tiv024) Stop both PS and AS:

```
tiv024:/opt/PolicyDirector/bin # pd_start stop
Stopping the: Access Manager policy server.
Stopping the: Access Manager authorization server.
```

(tiv025) Stop AS:

```
tiv025:/var/PolicyDirector/db # pd_start stop
Stopping the: Access Manager authorization server.
```

(tiv025) Change master-host in pd.conf:

```
tiv025:/opt/PolicyDirector/etc # vi pd.conf
# Hostname of the server.
# This parameter is set by the bassslcfg utility.
#master-host = <Server host name>
#master-host = tiv024
master-host = tiv025
```

(tiv025) Change database-path in ivmgrd.conf:

```
tiv025:/opt/PolicyDirector/etc # vi ivmgrd.conf
# Database file.
#database-path = /var/PolicyDirector/db/master_authzn.db
database-path = /var/PolicyDirector/db/ivacld.db
```

(tiv025) Start PS, but NOT AS:

```
tiv025:/opt/PolicyDirector/etc # pdmgrd
Tivoli Access Manager policy server v6.1.0.1 (Build 080912b)
Copyright (C) IBM Corporation 1994-2003.  All Rights Reserved.
2009-10-19-11:52:54.062-04:00I----- 0x14C521D3 pdmgrd NOTICE mis ivcore cfgmgr.cpp 196
0x76be66b0
```

```
   HPDMS0467I   Server startup
   2009-10-19-11:52:54.062-04:00I----- 0x14C526F2 pdmgrd NOTICE mis ivmgrd cfgmgr.cpp 201
   0x76be66b0
   HPDMS1778I   Loading configuration
```

(tiv025) Login to pdadmin and check for testacl:

```
   tiv025:/opt/PolicyDirector/etc # pdadmin -a sec_master -p passw0rd
   pdadmin sec_master> acl list
   default-management-proxy
   default-management
   testacl  <<---- Good!! The ACL created on tiv024 shows up here
   default-root
   default-gso
   default-policy
   default-config
   default-domain
   default-replica
```

Update ACL on tiv025 and check replication on tiv024

(tiv024) Change AS to point to tiv025 PS:

Change *master-host* in pd.conf:

```
      # Hostname of the server.
      # This parameter is set by the bassslcfg utility.
      #master-host = <Server host name>
      #master-host = tiv024
      master-host = tiv025
```

Change *master-host* in ivacld.conf:

```
      # Hostname of the server.
      # This parameter is set by the svrsslcfg utility.
      # master-host = <Server host name>
      #master-host = tiv024
      master-host = tiv025
```

(tiv024) Start AS, but NOT PS:

```
   tiv024:/opt/PolicyDirector/etc # pdacld
   Tivoli Access Manager authorization server v6.1.0.1 (Build 080912b)
   Copyright (C) IBM Corporation 1994-2003.  All Rights Reserved.
   2009-10-19-11:59:46.935-04:00I----- 0x14C521D3 pdacld NOTICE mis ivcore ivacld.cpp 443
   0x76be66b0
   HPDMS0467I   Server startup
   2009-10-19-11:59:46.935-04:00I----- 0x14C526F2 pdacld NOTICE mis ivmgrd ivacld.cpp 448
   0x76be66b0
   HPDMS1778I   Loading configuration
   tiv024:/opt/PolicyDirector/etc # pd_start status

   Tivoli Access Manager servers

   Server                Enabled       Running
   ------------------------------------------
   pdmgrd                    yes       no
   pdacld                    yes       yes
   pdmgrproxyd               no        no
```

(tiv025) Change *testacl* ACL:

```
   pdadmin sec_master> acl show testacl
       ACL Name: testacl
```

```
        Description:
        Entries:
            User sec_master TcmdbsvaBRl
    pdadmin sec_master> user create chinwe cn=chinwe,o=ibm,c=us Chinwe Smith passw0rd
    pdadmin sec_master> user modify chinwe account-valid yes
    pdadmin sec_master> acl modify testacl set user chinwe Tr
    pdadmin sec_master> acl show testacl
        ACL Name: testacl
        Description:
        Entries:
            User sec_master TcmdbsvaBRl
            User chinwe Tr
```

(tiv025) Stop PS:

```
    tiv025:/opt/PolicyDirector/bin # pd_start stop
    Stopping the: Access Manager policy server.
```

(tiv024) Stop AS:

```
    tiv024:/opt/PolicyDirector/bin # pd_start stop
    Stopping the: Access Manager authorization server.
```

(tiv024) Change PS to point to tiv024 AS database:

Update ivmgr.conf:

```
       # Database file.
       #database-path = /var/PolicyDirector/db/master_authzn.db
       database-path = /var/PolicyDirector/db/ivacld.db
```

Update pd.conf:

```
       # Hostname of the server.
       # This parameter is set by the bassslcfg utility.
       #master-host = <Server host name>
       master-host = tiv024
```

(tiv024) Start PS:

```
    tiv024:/opt/PolicyDirector/etc # pdmgrd
    Tivoli Access Manager policy server v6.1.0.1 (Build 080912b)
    Copyright (C) IBM Corporation 1994-2003.  All Rights Reserved.
    2009-10-19-12:04:47.334-04:00I----- 0x14C521D3 pdmgrd NOTICE mis ivcore cfgmgr.cpp 196
    0x76be66b0
    HPDMS0467I   Server startup
    2009-10-19-12:04:47.334-04:00I----- 0x14C526F2 pdmgrd NOTICE mis ivmgrd cfgmgr.cpp 201
    0x76be66b0
    HPDMS1778I   Loading configuration

    tiv024:/opt/PolicyDirector/etc # pd_start status
    Tivoli Access Manager servers
    Server                Enabled       Running
    ------------------------------------------
    pdmgrd                    yes       yes
    pdacld                    yes       no
    pdmgrproxyd               no        no
```

(tiv024) Login to pdadmin and check for modified testacl:

```
    tiv024:/opt/PolicyDirector/bin # pdadmin -a sec_master -p passw0rd
    pdadmin sec_master> acl show testacl
        ACL Name: testacl
        Description:
```

```
       Entries:
           User sec_master TcmdbsvaBRl
           User chinwe Tr     <<---- Yay!!
```

Restore initial configuration on tiv025:

- Set pd.conf master-host back to tiv024
- Start AS, NOT PS.
- Make sure pdadmin works correctly

1.8 Create failover scripts and test

NOTE: These failover scripts are NOT supported by IBM Support or supplied with the product, but were created from scratch, solely for the purposes of this testing.[1]

Fail over

tiv024down on tiv024

1. Stop PS on tiv024
2. Change the pd.conf file on tiv024 to point to master-host = tiv025
3. Unalias loopback interface
4. Start Auth Server on tiv024

tiv025up on tiv025

5. Stop AS on tiv025
6. Change the pd.conf file on tiv025 to point to master-host = tiv025
7. Alias loopback interface
8. Start Policy Server on tiv025

Fail back

tiv025down on tiv025

1. Stop PS on tiv025
2. Change the pd.conf file on tiv025 to point to master-host = tiv024
3. Unalias loopback interface
4. Start Auth Server on tiv025

tiv024up on tiv024

5. Stop AS on tiv024
6. Change the pd.conf file on tiv024 to master-host = tiv024
7. Alias loopback interface
8. Start Policy Server on tiv024

Run *tiv024down:*

```
tiv024:/opt/PolicyDirector/etc # ./tiv024down
Stopping the: Access Manager policy server.
Setting lo:1 interface DOWN...
Starting the Authorization server...
Tivoli Access Manager authorization server v6.1.0.1 (Build 080912b)
Copyright (C) IBM Corporation 1994-2003.  All Rights Reserved.
2009-10-23-13:10:55.638-04:00I----- 0x14C521D3 pdacld NOTICE mis ivcore ivacld.cpp 443
0x76be66b0
HPDMS0467I   Server startup
```

[1] THESE MATERIALS ARE PROVIDED "AS IS" AND, SUBJECT TO ANY STATUTORY WARRANTIES WHICH CAN NOT BE EXCLUDED, IBM MAKES NO WARRANTIES OR CONDITIONS EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, REGARDING THE FAILOVER SCRIPTS. IBM WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO ANY USE OR DISTRIBUTION OF THESE SCRIPTS.

```
2009-10-23-13:10:55.639-04:00I----- 0x14C526F2 pdacld NOTICE mis ivmgrd ivacld.cpp 448
0x76be66b0
HPDMS1778I   Loading configuration

tiv024:/opt/PolicyDirector/etc # pd_start status
Tivoli Access Manager servers
Server                Enabled       Running
-----------------------------------------
pdmgrd                    yes       no
pdacld                    yes       yes
pdmgrproxyd               no        no
```

Run *tiv025up:*

```
tiv025:/opt/PolicyDirector/etc # ./tiv025up
Stopping the: Access Manager authorization server.
Setting lo:1 interface UP...
Starting the policy server...
Tivoli Access Manager policy server v6.1.0.1 (Build 080912b)
Copyright (C) IBM Corporation 1994-2003.  All Rights Reserved.
2009-10-23-13:11:36.500-04:00I----- 0x14C521D3 pdmgrd NOTICE mis ivcore cfgmgr.cpp 196
0x76be66b0
HPDMS0467I   Server startup
2009-10-23-13:11:36.501-04:00I----- 0x14C526F2 pdmgrd NOTICE mis ivmgrd cfgmgr.cpp 201
0x76be66b0
HPDMS1778I   Loading configuration

tiv025:/opt/PolicyDirector/etc # pd_start status
Tivoli Access Manager servers
Server                Enabled       Running
-----------------------------------------
pdmgrd                    yes       yes
pdacld                    yes       no
pdmgrproxyd               no        no
```

Login to pdadmin on tiv025 and try updating *testacl:*

```
tiv025:/opt/PolicyDirector/etc # pdadmin -a sec_master -p passw0rd
pdadmin sec_master> user create ndidi cn=ndidi,o=ibm,c=us Ndidi Smith passw0rd
pdadmin sec_master> user modify ndidi account-valid yes
pdadmin sec_master> acl modify testacl set user ndidi Tr
pdadmin sec_master> acl show testacl
    ACL Name: testacl
    Description:
    Entries:
        User sec_master TcmdbsvaBRl
        User chinwe Tr
        User ndidi Tr
```

Run *tiv025down:*

```
tiv025:/opt/PolicyDirector/etc # ./tiv025down
Stopping the: Access Manager policy server.
Setting lo:1 interface DOWN...
Starting the authorization server...
Tivoli Access Manager authorization server v6.1.0.1 (Build 080912b)
Copyright (C) IBM Corporation 1994-2003.  All Rights Reserved.
2009-10-23-13:06:37.450-04:00I----- 0x14C521D3 pdacld NOTICE mis ivcore ivacld.cpp 443
0x76be66b0
HPDMS0467I   Server startup
```

```
2009-10-23-13:06:37.452-04:00I----- 0x14C526F2 pdacld NOTICE mis ivmgrd ivacld.cpp 448
0x76be66b0
HPDMS1778I   Loading configuration
```

Run *tiv024up:*

```
tiv024:/opt/PolicyDirector/etc # ./tiv024up
Stopping the: Access Manager authorization server.
Setting lo:1 interface UP...
Starting the policy server...
Tivoli Access Manager policy server v6.1.0.1 (Build 080912b)
Copyright (C) IBM Corporation 1994-2003.  All Rights Reserved.
2009-10-23-13:07:06.948-04:00I----- 0x14C521D3 pdmgrd NOTICE mis ivcore cfgmgr.cpp 196
0x76be66b0
HPDMS0467I   Server startup
2009-10-23-13:07:06.949-04:00I----- 0x14C526F2 pdmgrd NOTICE mis ivmgrd cfgmgr.cpp 201
0x76be66b0
HPDMS1778I   Loading configuration
```

Login to pdadmin on tiv024 and list *testacl:*

```
tiv024:/opt/PolicyDirector/etc # pdadmin -a sec_master -p passw0rd
pdadmin sec_master> acl show testacl
    ACL Name: testacl
    Description:
    Entries:
        User sec_master TcmdbsvaBRl
        User chinwe Tr
        User ndidi Tr      <-- Yay!!
```

Configuration for normal running mode

tiv024 (Primary)

```
Policy Server UP
Auth Server DOWN
pd.conf: master-host = tiv024
ivmgrd.conf: database-path = /var/PolicyDirector/db/ivacld.db
ivacld.conf: master-host = tiv025; db-file = /var/PolicyDirector/db/ivacld.db
```

tiv025 (Backup)

```
Policy Server DOWN
Auth Server UP
pd.conf: master-host = tiv024
ivmgrd.conf: database-path = /var/PolicyDirector/db/ivacld.db
ivacld.conf: master-host = tiv024
```

STEP 2: SET UP NETWORK DISPATCHER

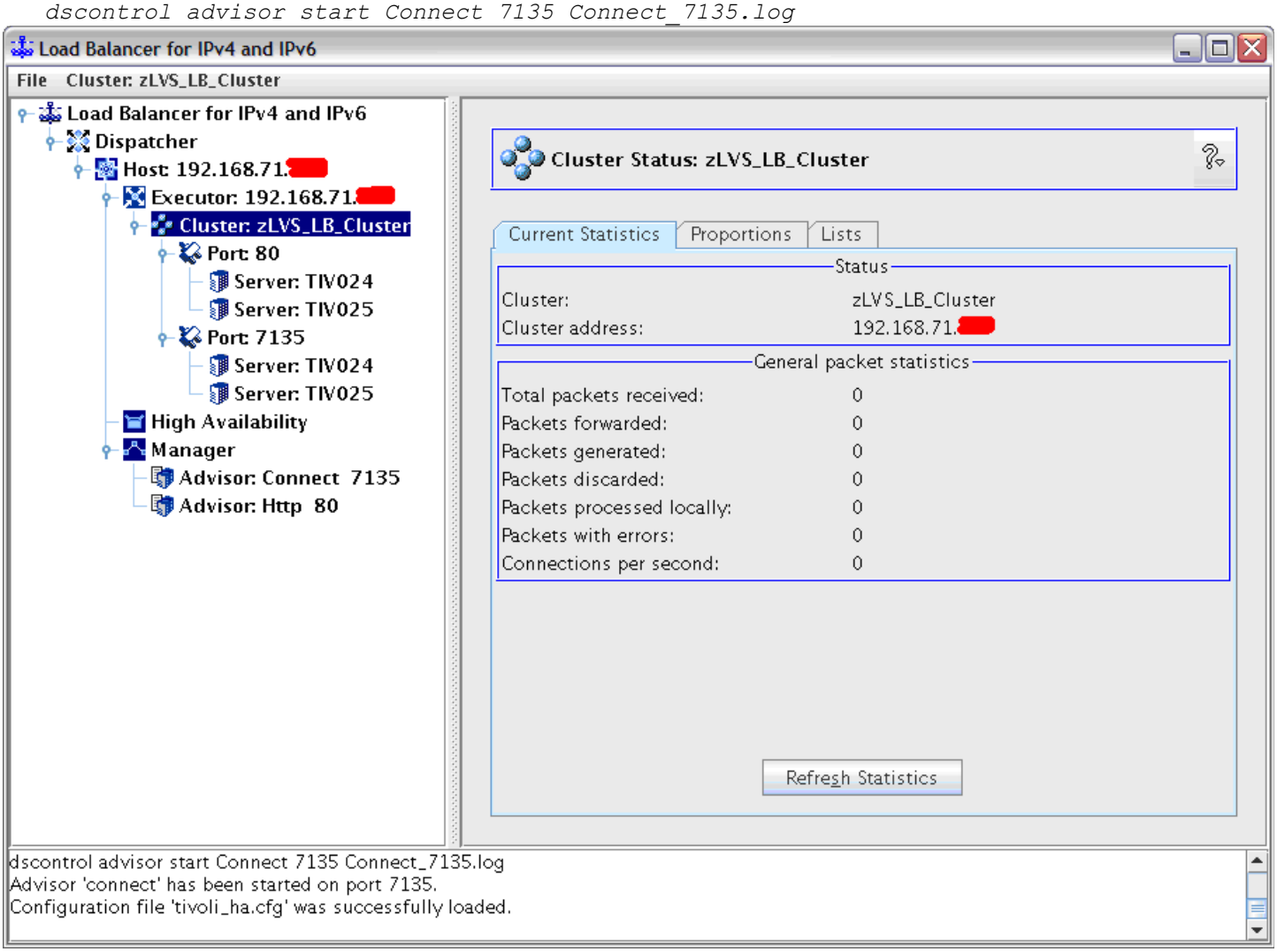
2.1 Configure Load Balancer

The Load Balancer serves as the mechanism to balance requests between the policy servers. The cluster IP address must be added as an alias to the loopback interface on both policy server guests.

Run the following commands to set up your configuration:

```
dscontrol set loglevel 3
dscontrol executor start
dscontrol executor set hatimeout 3

dscontrol cluster add zLVS_LB_Cluster address <cluster_ip_address>
dscontrol cluster set zLVS_LB_Cluster proportions 49 50 1 0
```

```
dscontrol port add zLVS_LB_Cluster@7135 selectionalgorithm connection
dscontrol port set zLVS_LB_Cluster@7135 staletimeout 6400

dscontrol server add zLVS_LB_Cluster@7135@tiv025 address <tiv025_ip_address>

dscontrol server add zLVS_LB_Cluster@7135@tiv024 address <tiv024_ip_address>

dscontrol port add zLVS_LB_Cluster@80 selectionalgorithm connection
dscontrol port set zLVS_LB_Cluster@80 staletimeout 6400

dscontrol server add zLVS_LB_Cluster@80@tiv025 address <tiv025_ip_address>

dscontrol server add zLVS_LB_Cluster@80@tiv024 address <tiv024 _ip_address>


dscontrol manager start manager.log 10004

dscontrol advisor start Http 80 HTTP_80.log

dscontrol advisor start Connect 7135 Connect_7135.log
```



Add cluster IP address as interface on both guests

```
tiv024:~ # ip -4 addr add <cluster_ip_address>/32 dev lo:1
tiv024:~ # ip add
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet <cluster_ip_address>/32 scope global lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: sit0: <NOARP> mtu 1480 qdisc noop
    link/sit 0.0.0.0 brd 0.0.0.0
3: eth0: <BROADCAST,MULTICAST,UP> mtu 1492 qdisc pfifo_fast qlen 1000
    link/ether 02:09:00:00:00:73 brd ff:ff:ff:ff:ff:ff
    inet <tiv024_ip_address>/24 brd <netmask> scope global eth0
    inet6 fe80::9:ff:fe00:73/64 scope link
       valid_lft forever preferred_lft forever

tiv025:~ # ip -4 addr add <cluster_ip_address>/32 dev lo:1
tiv025:~ # ip addr
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet <cluster_ip_address>/32 scope global lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: sit0: <NOARP> mtu 1480 qdisc noop
    link/sit 0.0.0.0 brd 0.0.0.0
3: eth0: <BROADCAST,MULTICAST,UP> mtu 1492 qdisc pfifo_fast qlen 1000
    link/ether 02:09:00:00:00:70 brd ff:ff:ff:ff:ff:ff
    inet <tiv025_ip_address>/24 brd <netmask> scope global eth0
    inet6 fe80::9:ff:fe00:70/64 scope link
       valid_lft forever preferred_lft forever
```

Display manager report

```
   tiv023:/opt/ibm/edge/ulb/bin # ./dscontrol manager report

   ------------------------------------------------------------------
   |                      SERVER                        |   STATUS   |
   ------------------------------------------------------------------
   |                                              tiv025 |     ACtivE |
   |                                              tiv024 |     ACtivE |
   ------------------------------------------------------------------
   ----------------------------
   |   MANAGER REPORT LEGEND   |
   ----------------------------
   | ACTV | Active Connections |
   | NEWC | New Connections    |
   | SYS  | System Metric      |
   | NOW  | Current Weight     |
   | NEW  | New Weight         |
   | CONN | Connections        |
   ----------------------------
   ------------------------------------------------------------------
   |   zLVS_LB_Cluster  |        |        |        |        |        |
   |                    | WEIGHT |  ACTV  |  NEWC  |  PORT  |   SYS  |
   |     PORT:  7135    |NOW  NEW|   49%  |   50%  |    1%  |    0%  |
   ------------------------------------------------------------------
```

```
|             tiv025 | 10  10 |      0 |      0 |     38 |      0 |
|             tiv024 |  0   0 |      0 |      0 |     -1 |      0 |
-------------------------------------------------------------------
-------------------------------------------------------------------
|   zLVS_LB_Cluster  |        |        |        |        |        |
|                    | WEIGHT |  ACTV  |  NEWC  |  PORT  |   SYS  |
|     PORT:    80    |NOW  NEW|   49%  |   50%  |    1%  |    0%  |
-------------------------------------------------------------------
|             tiv025 | 10  10 |      0 |      0 |    108 |      0 |
|             tiv024 |  0   0 |      0 |      0 |     -1 |      0 |
-------------------------------------------------------------------
-----------------------------------------------------
|    ADVISOR    |    CLUSTER@PORT     |  TIMEOUT  |
-----------------------------------------------------
|          http |                  80 | unlimited |
|       connect |                7135 | unlimited |
-----------------------------------------------------
```

2.2 Install and configure Runtime and LDAP on tiv026

Install TAM Runtime (for pdadmin):

```
tiv026:/mnt # rpm -ivh gsk7bas-7.0-4.11.s390.rpm PDlic-PD-6.1.0-1.s390.rpm TivSecUtl-
TivSec-6.1.0-1.s390.rpm PDRTE-PD-6.1.0-1.s390.rpm
Preparing...                ########################################### [100%]
   1:gsk7bas                ########################################### [ 25%]
   2:TivSecUtl-TivSec       ########################################### [ 50%]
Adding ivmgr user
Adding tivoli user
usermod: `root' is primary group name.
usermod: `root' is primary group name.
usermod: `ivmgr' is primary group name.
   3:PDlic-PD               ########################################### [ 75%]
   4:PDRTE-PD               ########################################### [100%]
```

Install LDAP client packages:

```
tiv026:/mnt # rpm -ivh idsldap-cltbase61-6.1.0-6.s390.rpm idsldap-clt32bit61-6.1.0-
6.s390.rpm
Preparing...                ########################################### [100%]
   1:idsldap-cltbase61      ########################################### [ 50%]
   2:idsldap-clt32bit61     ########################################### [100%]
tiv026:/mnt # rpm -ivh idsldap-cltjava61-6.1.0-6.s390.rpm
Preparing...                ########################################### [100%]
   1:idsldap-cltjava61      ########################################### [100%]
Java tar extracted.
```

Configure Runtime server:

```
tiv026:/opt/PolicyDirector/etc # pdconfig

            Tivoli Access Manager Setup Menu

        1. Configure Package
        2. Unconfigure Package
        3. Display Configuration Status
        x. Exit

Select the menu item [x]: 1

        Tivoli Access Manager Configuration Menu
```

```
        1. Access Manager Runtime Configuration
        x. Return to the Tivoli Access Manager Setup Menu

   Select the menu item [x]: 1

   Will the policy server be installed on this machine (y/n) [No]:  n

   Tivoli Common Directory logging is not configured.
   This scheme provides a common location for log files for Tivoli products instead of
   separate locations
   determined by each application.

   Do you want to use Tivoli Common Directory logging (y/n) [No]? n

   Log files for this application will be created in directory:
   /var/PolicyDirector/log

        1. LDAP
        2. Active Directory

   Registry [1]: 1

   LDAP server host name: tiv023

   LDAP server port [389]:

   Policy server host name: tiv024

   Policy server SSL port [7135]:
   Domain [Default]:

   Current status of Federal Information Processing Standards (FIPS)
   as enabled on the policy server: no

   Automatically download the pdcacert.b64 file
   from the policy server? (y/n) [Yes]:
   The SSL configuration of Access Control Runtime has completed successfully.
     Tivoli Access Manager policy server domain name:     Default
     Tivoli Access Manager policy server host name:       tiv024
     Tivoli Access Manager policy server listening port:  7135

   The package has been configured successfully.
```

2.3 Verify request forwarding by load balancer, using tiv026

Modify *master-host* in pd.conf to point to cluster IP address:

```
   # Hostname of the server.
   # This parameter is set by the bassslcfg utility.
   #master-host = <Server host name>
   #master-host = <tiv024_ip_address>
   master-host = <cluster_ip_address>
```

Login to pdadmin to verify:

```
   tiv026:/opt/PolicyDirector/etc # pdadmin -a sec_master -p passw0rd
   pdadmin sec_master> server list
       ivacld-tiv024
       ivacld-tiv025
```

```
pdadmin sec_master> acl list
default-management-proxy
default-management
testacl
default-root
default-gso
default-policy
default-config
default-domain
default-replica
pdadmin sec_master> acl show testacl
    ACL Name: testacl
    Description:
    Entries:
        User sec_master TcmdbsvaBRl
        User chinwe Tr
pdadmin sec_master> exit
```

Yay!! This means that the dispatcher is correctly routing to the policy server.

STEP 3: Configure TSAMP to perform automatic failover

3.1 Install TSAMP on tiv024 and tiv025

Run pre-req test:

```
tiv024:/opt/SAM3100MPLinux # ./prereqSAM
prereqSAM: All prerequisites for the ITSAMP installation are met on operating system:
SUSE Linux Enterprise Server 10 (s390x)
VERSION = 10
PATCHLEVEL = 2
```

Run install script:

```
tiv024:/opt/SAM3100MPLinux # ./installSAM
...
...
installSAM: The following license is installed:
Product ID: 101
Product Annotation:
Creation date: Wed Oct 24 20:00:00 2007
Expiration date: Thu Dec 31 18:59:59 2037
Subsystem         Group            PID     Status
 ctrmc            rsct             23579   active
 IBM.ERRM         rsct_rm          23618   active
 IBM.AuditRM      rsct_rm          23651   active
installSAM: Warning: Must set CT_MANAGEMENT_SCOPE=2

installSAM: All packages were installed successfully.
```

Set environment variable:

```
tiv024:/opt/SAM3100MPLinux # export CT_MANAGEMENT_SCOPE=2
tiv024:/opt/SAM3100MPLinux # echo $CT_MANAGEMENT_SCOPE
2
```

3.2 Create cluster and network tiebreaker

Create 2-node cluster:

- Run preprpnode **on both systems**

```
tiv024:~ # preprpnode tiv024 tiv025
tiv025:~ # preprpnode tiv024 tiv025
```

- Create a cluster, *SA_Domain*, from 1 system

```
tiv024:~ # mkrpdomain SA_Domain tiv024 tiv025
```

- Display cluster status

```
tiv024:~ # lsrpdomain SA_Domain
Name      OpState RSCTActiveVersion MixedVersions TSPort GSPort
SA_Domain Offline 2.5.1.2           No            12347  12348
```

- Bring cluster online

```
tiv024:~ # startrpdomain SA_Domain
```

- Check status again

```
tiv024:~ # lsrpdomain SA_Domain
Name      OpState        RSCTActiveVersion MixedVersions TSPort GSPort
SA_Domain Pending online 2.5.1.2           No            12347  12348
tiv024:~ # lsrpdomain SA_Domain
Name      OpState RSCTActiveVersion MixedVersions TSPort GSPort
SA_Domain Online  2.5.1.2           No            12347  12348
```

- Check status on tiv025

```
tiv025:~ # lsrpdomain SA_Domain
Name      OpState RSCTActiveVersion MixedVersions TSPort GSPort
SA_Domain Online  2.5.1.2           No            12347  12348
```

Set up network tiebreaker:

NOTE: This is an IP address that TSAMP checks; if it can't ping it, the node is taken down. I will use the real address of the network dispatcher machine.

- List available tiebreaker types on system

```
tiv024:~ # lsrsrc -c IBM.TieBreaker AvailableTypes
Resource Class Persistent Attributes for IBM.TieBreaker
resource 1:
        AvailableTypes = {["ECKD",""],["EXEC",""],["Operator",""],["Fail",""]}
```

- Create tiebreaker

```
tiv024:~ # mkrsrc IBM.TieBreaker Type="EXEC" Name="mynetwork"
DeviceInfo='PATHNAME=/usr/sbin/rsct/bin/samtb_net Address=<tiv023_ip_address>
Log=1' PostReserveWaitTime=30;
```

- Activate the tiebreaker

```
tiv024:~ # chrsrc -c IBM.PeerNode OpQuorumTieBreaker="mynetwork"
```

- Display the current tiebreaker info, from tiv025

```
tiv025:/opt/PolicyDirector/etc # lsrsrc IBM.TieBreaker
Resource Persistent Attributes for IBM.TieBreaker
resource 1:
        Name                = "Operator"
        Type                = "Operator"
        DeviceInfo          = ""
        ReprobeData         = ""
        ReleaseRetryPeriod  = 0
        HeartbeatPeriod     = 0
        PreReserveWaitTime  = 0
        PostReserveWaitTime = 0
        NodeInfo            = {}
        ActivePeerDomain    = "SA_Domain"
resource 2:
```

```
        Name                = "Fail"
        Type                = "Fail"
        DeviceInfo          = ""
        ReprobeData         = ""
        ReleaseRetryPeriod  = 0
        HeartbeatPeriod     = 0
        PreReserveWaitTime  = 0
        PostReserveWaitTime = 0
        NodeInfo            = {}
        ActivePeerDomain    = "SA_Domain"
resource 3:
        Name                = "mynetwork"
        Type                = "EXEC"
        DeviceInfo          = "PATHNAME=/usr/sbin/rsct/bin/samtb_net
Address=<tiv023_ip_address> Log=1"
        ReprobeData         = ""
        ReleaseRetryPeriod  = 0
        HeartbeatPeriod     = 0
        PreReserveWaitTime  = 0
        PostReserveWaitTime = 30
        NodeInfo            = {}
        ActivePeerDomain    = "SA_Domain"
```

3.3 Setup scripts for application resource:

An application resource will enable the failover automation by TSAMP and in order to create one, the following three scripts are needed:

- *polup*, the start script for bringing the resource online,
- *poldown*, the stop script for taking the resource offline, and
- *polmon*, the script for monitoring the resource.

tiv024 start script

```
tiv024:/opt/PolicyDirector/etc # cp tiv024up polup

tiv024:/opt/PolicyDirector/etc # cat polup
#!/bin/bash

#Stop authorization server
/opt/PolicyDirector/bin/pd_start stop >/dev/null 2>&1
logger -i -t "POLUP" "Authorization server stopped"

#Change pd.conf
sed 's/master-host = tiv025/master-host = tiv024/g' /opt/PolicyDirector/etc/pd.conf
   > /opt/PolicyDirector/etc/pd.conf.temp
mv /opt/PolicyDirector/etc/pd.conf.temp /opt/PolicyDirector/etc/pd.conf
logger -i -t "POLUP" "pd.conf modified: master-host set to tiv024"

#Alias loopback interface
ifconfig lo:1 <cluster_ip_address> netmask 255.255.255.255 up
logger -i -t "POLUP" "lo:1 interface UP"

#Start policy server
/opt/PolicyDirector/bin/pdmgrd >/dev/null 2>&1
logger -i -t "POLUP" "Policy server started"

exit 0
```

tiv024 stop script

```
tiv024:/opt/PolicyDirector/etc # cp tiv024down poldown

tiv024:/opt/PolicyDirector/etc # cat poldown
#!/bin/bash

#Stop policy server
/opt/PolicyDirector/bin/pd_start stop >/dev/null 2>&1
logger -i -t "POLDOWN" "Policy server stopped"

#Change pd.conf
sed 's/master-host = tiv024/master-host = tiv025/g' /opt/PolicyDirector/etc/pd.conf
   > /opt/PolicyDirector/etc/pd.conf.temp
mv /opt/PolicyDirector/etc/pd.conf.temp /opt/PolicyDirector/etc/pd.conf
logger -i -t "POLDOWN" "pd.conf modified: master-host set to tiv025"

#Unalias loopback interface
ifconfig lo:1 down
logger -i -t "POLDOWN" "lo:1 interface DOWN"

#Start authorization server
/opt/PolicyDirector/bin/pdacld >/dev/null 2>&1
logger -i -t "POLDOWN" "Authorization server started"

exit 0
```

tiv024 monitor script

```
tiv024:/opt/PolicyDirector/etc # cat polmon
#!/bin/bash
OPSTATE_ONLINE=1
OPSTATE_OFFLINE=2

ps -ef | grep -v "grep" | grep "pdmgrd" >/dev/null

if [ $? == 0 ]
then
        RC=${OPSTATE_ONLINE}
else
        RC=${OPSTATE_OFFLINE}
fi
exit $RC
```

tiv025 start script

```
tiv025:/opt/PolicyDirector/etc # cat polup
#!/bin/bash

#Stop authorization server
/opt/PolicyDirector/bin/pd_start stop >/dev/null 2>&1
logger -i -t "POLUP" "Authorization server stopped"

#Change pd.conf
sed 's/master-host = tiv024/master-host = tiv025/g' /opt/PolicyDirector/etc/pd.conf
> /opt/PolicyDirector/etc/pd.conf.temp
mv /opt/PolicyDirector/etc/pd.conf.temp /opt/PolicyDirector/etc/pd.conf
logger -i -t "POLUP" "pd.conf modified: master-host set to tiv025"

#Alias loopback interface
```

```
ifconfig lo:1 <cluster_ip_address> netmask 255.255.255.255 up
logger -i -t "POLUP" "lo:1 interface UP"

#Start policy server
/opt/PolicyDirector/bin/pdmgrd >/dev/null 2>&1
logger -i -t "POLUP" "Policy server started"

exit 0
```

tiv025 stop script

```
tiv025:/opt/PolicyDirector/etc # cat poldown
#!/bin/bash

#Stop policy server
/opt/PolicyDirector/bin/pd_start stop >/dev/null 2>&1
logger -i -t "POLDOWN" "Policy server stopped"

#Change pd.conf
sed 's/master-host = tiv025/master-host = tiv024/g' /opt/PolicyDirector/etc/pd.conf
> /opt/PolicyDirector/etc/pd.conf.temp
mv /opt/PolicyDirector/etc/pd.conf.temp /opt/PolicyDirector/etc/pd.conf
logger -i -t "POLDOWN" "pd.conf modified: master-host set to tiv024"

#Unalias loopback interface
ifconfig lo:1 down
logger -i -t "POLDOWN" "lo:1 interface DOWN"

#Start authorization server
/opt/PolicyDirector/bin/pdacld >/dev/null 2>&1
logger -i -t "POLDOWN" "Authorization server started"

exit 0
```

tiv025 monitor script

```
tiv025:/opt/PolicyDirector/etc # cat polmon
#!/bin/bash
OPSTATE_ONLINE=1
OPSTATE_OFFLINE=2

ps -ef | grep -v "grep" | grep "pdmgrd" >/dev/null

if [ $? == 0 ]
then
        RC=${OPSTATE_ONLINE}
else
        RC=${OPSTATE_OFFLINE}
fi
exit $RC
```

3.4 Set up floating application resource

Create application resource:

```
tiv024:/opt/PolicyDirector/etc # cat pdmgrd-rs.def
PersistentResourceAttributes::
Name="pdmgrd-rs"
StartCommand="/opt/PolicyDirector/etc/polup"
StopCommand="/opt/PolicyDirector/etc/poldown"
MonitorCommand="/opt/PolicyDirector/etc/polmon"
```

```
MonitorCommandPeriod=5
MonitorCommandTimeout=30
NodeNameList={'tiv024','tiv025'}
StartCommandTimeout=30
StopCommandTimeout=30
UserName="root"
ResourceType=1
```

NOTE: ResourceType=1 means floating resource, so it can run on any node, but only one will be up at a time.

```
tiv024:/opt/PolicyDirector/etc # mkrsrc -f pdmgrd-rs.def IBM.Application
```

Make a resource group:

```
tiv024:/opt/PolicyDirector/etc # mkrg pdmgrd-rg
```

Add your resource to the resource group:

```
tiv024:/opt/PolicyDirector/etc # addrgmbr -g pdmgrd-rg IBM.Application:pdmgrd-rs
```

Bring resource online:

```
tiv024:/opt/PolicyDirector/etc # chrg -o online pdmgrd-rg
```

Display resource group info:

```
tiv024:/opt/PolicyDirector/etc # samdiag -g pdmgrd
   Displaying information for the following:
    Resource Group "pdmgrd-rg":

   Diagnosis::Resource: pdmgrd-rg/ResGroup/IBM.ResourceGroup
       type: CHARM Resource Group
     Status -
         Observed: Offline         - Soft Down
          Desired: Online          - Requested Online
         (Nominal: Online          - Nominal State: Online)
       Automation: Idle            - CharmBase trigger linked
        Startable: Yes             - Resource is startable
          Binding: Bound           - Bound
         Compound: Awaiting        - Awaiting Automation
             Move: Not_Supported   - Resource Move State is Not Supported

    Resource Based Quorum: Not Supported   - CharmBase trigger linked
     Members and Memberships:
         +---HasMember                      ---> pdmgrd-rs/Float/IBM.Application
     Group Constraint: Collocated
     Binding Constraints:
     Flags:
       None
     Orders:
       Outstanding Order: Online          - Make Available sent
               Progress: None            -
                  Reason: None            -
     Dependencies:
       Start: Satisfied
         +---InCluster                      ---> Cluster
       Stop: Satisfied
     Binding exceptions:
       None
     Static Relationships:
```

```
            +---InCluster                          ---> Cluster
         Dynamic Relationships:"
```

Check resource group attributes:

```
   tiv024:/opt/PolicyDirector/etc # lsrg -Ab -V -g pdmgrd
   Starting to list resource group information.
   lsrg: Executed on Wed Nov  4 16:48:47 2009 at "tiv024", master node "tiv025".

   Displaying Resource Group information:
   All Attributes
   For Resource Group "pdmgrd-rg".


   Resource Group 1:
           Name                              = pdmgrd-rg
           MemberLocation                    = Collocated
           Priority                          = 0
           AllowedNode                       = ALL
           NominalState                      = Online
           ExcludedList                      = {}
           Subscription                      = {}
           Owner                             =
           Description                       =
           InfoLink                          =
           ActivePeerDomain                  = SA_Domain
           OpState                           = Pending online
           TopGroup                          = pdmgrd-rg
           MoveStatus                        = [None]
           ConfigValidity                    =
           LockState                         = 0
           AutomationDetails[CompoundState] = Waiting
                            [DesiredState] = Online
                           [ObservedState] = Offline
                            [BindingState] = Bound
                         [AutomationState] = Idle
                            [ControlState] = Startable
                             [HealthState] = Not Applicable
   Completed listing resource group information.
```

Check application resource:

```
   tiv024:/opt/PolicyDirector/etc # lsrsrc -s "Name = 'pdmgrd-rs'" IBM.Application
   Resource Persistent Attributes for IBM.Application
      resource 1:
              Name                  = "pdmgrd-rs"
              ResourceType          = 0
              AggregateResource     = "0x2028 0xffff 0x5d05a7e4 0xaf01fa18 0x9172725b
      0x5eb9dc78"
              StartCommand          = "/opt/PolicyDirector/etc/polup"
              StopCommand           = "/opt/PolicyDirector/etc/poldown"
              MonitorCommand        = "/opt/PolicyDirector/etc/polmon"
              MonitorCommandPeriod  = 5
              MonitorCommandTimeout = 30
              StartCommandTimeout   = 30
              StopCommandTimeout    = 30
              UserName              = "root"
              RunCommandsSync       = 1
              ProtectionMode        = 0
```

```
        HealthCommand         = ""
        HealthCommandPeriod   = 10
        HealthCommandTimeout  = 5
        InstanceName          = ""
        InstanceLocation      = ""
        SetHealthState        = 0
        MovePrepareCommand    = ""
        MoveCompleteCommand   = ""
        MoveCancelCommand     = ""
        CleanupList           = {}
        CleanupCommand        = ""
        CleanupCommandTimeout = 10
        ActivePeerDomain      = "SA_Domain"
        NodeNameList          = {"tiv025"}
resource 2:
        Name                  = "pdmgrd-rs"
        ResourceType          = 0
        AggregateResource     = "0x2028 0xffff 0x5d05a7e4 0xaf01fa18 0x9172725b
0x5eb9dc78"
        StartCommand          = "/opt/PolicyDirector/etc/polup"
        StopCommand           = "/opt/PolicyDirector/etc/poldown"
        MonitorCommand        = "/opt/PolicyDirector/etc/polmon"
        MonitorCommandPeriod  = 5
        MonitorCommandTimeout = 30
        StartCommandTimeout   = 30
        StopCommandTimeout    = 30
        UserName              = "root"
        RunCommandsSync       = 1
        ProtectionMode        = 0
        HealthCommand         = ""
        HealthCommandPeriod   = 10
        HealthCommandTimeout  = 5
        InstanceName          = ""
        InstanceLocation      = ""
        SetHealthState        = 0
        MovePrepareCommand    = ""
        MoveCompleteCommand   = ""
        MoveCancelCommand     = ""
        CleanupList           = {}
        CleanupCommand        = ""
        CleanupCommandTimeout = 10
        ActivePeerDomain      = "SA_Domain"
        NodeNameList          = {"tiv024"}
resource 3:
        Name                  = "pdmgrd-rs"
        ResourceType          = 1
        AggregateResource     = "0x3fff 0xffff 0x00000000 0x00000000 0x00000000
0x00000000"
        StartCommand          = "/opt/PolicyDirector/etc/polup"
        StopCommand           = "/opt/PolicyDirector/etc/poldown"
        MonitorCommand        = "/opt/PolicyDirector/etc/polmon"
        MonitorCommandPeriod  = 5
        MonitorCommandTimeout = 30
        StartCommandTimeout   = 30
        StopCommandTimeout    = 30
        UserName              = "root"
        RunCommandsSync       = 1
```

```
ProtectionMode         = 0
HealthCommand          = ""
HealthCommandPeriod    = 10
HealthCommandTimeout   = 5
InstanceName           = ""
InstanceLocation       = ""
SetHealthState         = 0
MovePrepareCommand     = ""
MoveCompleteCommand    = ""
MoveCancelCommand      = ""
CleanupList            = {}
CleanupCommand         = ""
CleanupCommandTimeout = 10
ActivePeerDomain       = "SA_Domain"
NodeNameList           = {"tiv024","tiv025"}
```

3.5 Test TSAMP automation

Here are four possible options for testing failover:

1) Pull the power cable on the server that is currently hosting the "Online" pdmgrd-rs resource. This would be the same as a real life power failure.

2) Perform a reboot of the server that is currently hosting the "Online" pdmgrd-rs resource. This would be similar (though a lot more graceful) to a kernel panic causing an OS crash.

3) Kill the underlying pdmgrd process on the server that is currently hosting the "Online" pdmgrd-rs resource. This would simulate the pmgrd process crashing or unexpectedly terminating.

4) Rename '/opt/PolicyDirector/etc/polup' to something else on the server that is currently hosting the "Online" pdmgrd-rs resource and kill the underlying pdmgrd process on that same server. Since the startup script cannot be found using the expected name, the resource will not be able to start on this node. This should cause a failover. **Remember to rename the startup script after the test is done. This might simulate an unrecoverable crash of pdmgrd.**

Running option 2, doing a reboot of the master node (tiv024). Here are the log messages:

tiv025

Nov 16 18:43:19 tiv025 ConfigRM[1624]: (Recorded using libct_ffdc.a cv 2):::Error ID: :::Reference ID: :::Template ID: 0:::Details File: :::Location: RSCT,PeerDomain.C,1.99.18.12,17335 :::CONFIGRM_PENDINGQUORUM_ER The operational quorum state of the active peer domain has changed to PENDING_QUORUM. This state usually indicates that exactly half of the nodes that are defined in the peer domain are online. In this state cluster resources cannot be recovered although none will be stopped explicitly.

Nov 16 18:43:20 tiv025 RecoveryRM[2058]: (Recorded using libct_ffdc.a cv 2):::Error ID: 825....MCS.9/195/ZS2e.1.....:::Reference ID: :::Template ID: 0:::Details File: :::Location: RSCT,Protocol.C,1.54.1.32,2525 :::RECOVERYRM_INFO_4_ST A member has left. Node number = 1

Nov 16 18:43:20 tiv025 RecoveryRM[2058]: (Recorded using libct_ffdc.a cv 2):::Error ID: 825....MCS.9/kkc/ZS2e.1.....:::Reference ID: :::Template ID: 0:::Details File: :::Location: RSCT,Protocol.C,1.54.1.32,2553 :::RECOVERYRM_INFO_5_ST Master has left, this node is now the master.

Checked for master node:

```
tiv025:~ # lssrc -ls IBM.RecoveryRM | grep -i master
   Master Node Name      : tiv025 (node number =  2)
```

After tiv024 came back up, I checked its logs:

tiv024

```
Nov 16 18:42:47 tiv024 shutdown[15933]: shutting down for system reboot
Nov 16 18:42:47 tiv024 init: Switching to runlevel: 6
Nov 16 18:42:48 tiv024 ConfigRM[1667]: (Recorded using libct_ffdc.a cv 2):::Error
ID: :::Reference ID:  :::Template ID: 0:::Details File:  :::Location:
RSCT,ConfigRMDaemon.C,1.13,188                :::CONFIGRM_STOPPED_ST IBM.ConfigRM
daemon has been stopped.
Nov 16 18:42:48 tiv024 cthags[1775]: (Recorded using libct_ffdc.a cv 2):::Error ID:
825....sBS.9/V510YS2e.1.....................:::Reference ID:  :::Template ID:
0:::Details File:  :::Location: RSCT,SRCSocket.C,1.75,482
:::GS_STOP_ST Group Services daemon stopped DIAGNOSTIC EXPLANATION Received
signal[SIGTERM]. Converted to normal stop
...
...
Nov 16 18:44:38 tiv024 ConfigRM[1634]: (Recorded using libct_ffdc.a cv 2):::Error
ID: :::Reference ID:  :::Template ID: 0:::Details File:  :::Location:
RSCT,PeerDomain.C,1.99.18.12,12287            :::CONFIGRM_ONLINE_ST The node is online
in the domain indicated in the detail data. Peer Domain Name SA_Domain
Nov 16 18:44:40 tiv024 StorageRM[1953]: (Recorded using libct_ffdc.a cv 2):::Error ID:
:::Reference ID:  :::Template ID: 0:::Details File:  :::Location:
RSCT,IBM.StorageRMd.C,1.41,142                :::STORAGERM_STARTED_ST IBM.StorageRM
daemon has started.
Nov 16 18:44:40 tiv024 RecoveryRM[1950]: (Recorded using libct_ffdc.a cv 2):::Error
ID: 824....cDS.9/y5U1YS2e.1.....................:::Reference ID:  :::Template ID:
0:::Details File:  :::Location: RSCT,IBM.RecoveryRMd.C,1.21.2.2,145
:::RECOVERYRM_INFO_0_ST IBM.RecoveryRM daemon has started.
Nov 16 18:44:41 tiv024 RecoveryRM[1950]: (Recorded using libct_ffdc.a cv 2):::Error
ID: 824....dDS.9/3E0.YS2e.1.....................:::Reference ID:  :::Template ID:
0:::Details File:  :::Location: RSCT,Protocol.C,1.54.1.32,369
:::RECOVERYRM_INFO_7_ST This node has joined the IBM.RecoveryRM group. My node number
=  1 ; Master node number =  2
```

Also, tiv025 shows tiv024 node joining the domain:

tiv025

```
Nov 16 18:44:41 tiv025 RecoveryRM[2058]: (Recorded using libct_ffdc.a cv 2):::Error
ID: 825....dDS.9/8ag0ZS2e.1.....................:::Reference ID:  :::Template ID:
0:::Details File:  :::Location: RSCT,Protocol.C,1.54.1.32,2513
:::RECOVERYRM_INFO_3_ST A new member has joined. Node number =  1
```

GOTCHAS

Here are a few items to keep in mind and watch out for when setting up this environment:

- The syntax for the NodeNameList variable in the resource definition file is critical. The node names must be enclosed in single quotes.

- Make sure to use file redirection for all file handles, for instance: /opt/PolicyDirector/bin/pd_start stop >/dev/null 2>&1

- Do not use echo statements in scripts, because there is nowhere for them to go as the script is run within the scope of TSAMP. Use logger statements to print to /var/log/messages.

- Use unique names for the application resource and the resource group. Best practice is to use suffixes of -rg and -rs for the group and resource respectively.

- Time-out values in the application resource definition file should not be too small. This causes the start, stop, and monitor commands not to detach from the shell, therefore hanging. Use a value such as 30 seconds for the MonitorCommandTimeout, StartCommandTimeout and StopCommandTimeout parameters.

- The start, stop, and monitor scripts must exit with a return code. The start and stop scripts can exit with 0 for success. The monitor script needs to exit with the actual operational state of the application resource, exit 1 for Online or 2 for Offline.

Upgrade TSAMP with fixpack 4 (version 3.1.0.4)

During the course of our testing, we needed to upgrade the TSAMP product to the latest code version. Here are the steps:

- Check installed version of RSCT on domain:

```
tiv024:~ # lsrpdomain
Name      OpState RSCTActiveVersion MixedVersions TSPort GSPort
SA_Domain Online  2.5.1.2           No            12347  12348
```

- Check version of RSCT on nodes:

```
tiv024:~ # lsrpnode
Name                    OpState RSCTVersion
tiv024 Online  2.5.1.2
tiv025 Online  2.5.1.2
```

NOTE: IBM Reliable Scalable Cluster Technology (RSCT) is the infrastructure used by System Automation for Multiplatforms to provide clusters with improved system availability, scalability, and ease of use.

- Check if SAMP end-to-end automation adapter is running:

```
tiv024:/ # samadapter status
samadapter is not running on tiv024

tiv025:/ # samadapter status
samadapter is not running on tiv025
```

- Stop the online resources:

```
tiv024:/ # chrg -o Offline pdmgrd-rg
```

- Stop the domain:

```
tiv024:/ # stoprpdomain SA_Domain
2632-110 The operation was rejected by one or more nodes, probably because one or more
resources are online or there was an error encountered in determining if any resources
are online.
tiv024: 2621-793 Node "tiv024" cannot be made offline. System Automation Manager
reports that there are resources online on this node.
```

- Stop the nodes:

```
tiv024:/ # lsrpnode
Name                    OpState RSCTVersion
tiv024 Online  2.5.1.2
tiv025 Online  2.5.1.2
```

```
tiv024:/ # stoprpnode tiv025
tiv024:/ # stoprpnode tiv024

tiv024:/ # lsrpnode
lsrpnode: There are no nodes in the peer domain or an online peer domain does not
exist.
tiv024:/ # stoprpdomain SA_Domain
The peer domain "SA_Domain" cannot be stopped because it is not online.
```

- Install update on tiv024 and tiv025:

```
tiv024:/SAM3104MPLinux # ./installSAM
prereqSAM: All prerequisites for the ITSAMP installation are met on operating system:
SUSE Linux Enterprise Server 10 (s390x)
VERSION = 10
PATCHLEVEL = 2
installSAM: Installing System Automation on platform: s390x
installSAM: Packages will be installed from directory:  ./Linux/s390

installSAM: Installing
 ./Linux/s390/src-1.3.0.4-09204.s390.rpm

installSAM: Installing
 ./Linux/s390/rsct.core.utils-2.5.3.3-09204.s390.rpm
 ./Linux/s390/rsct.core-2.5.3.3-09204.s390.rpm
 ./Linux/s390/rsct.basic-2.5.3.3-09204.s390.rpm
...
...
installSAM: The following license is installed:
Product ID: 101
Product Annotation:
Creation date: Wed Oct 24 20:00:00 2007
Expiration date: Thu Dec 31 18:59:59 2037
Subsystem         Group            PID     Status
 ctrmc            rsct             17361   active
 IBM.ConfigRM     rsct_rm          17443   active
 IBM.ERRM         rsct_rm          17449   active
 IBM.AuditRM      rsct_rm          17492   active

installSAM: All packages were installed successfully.

tiv025:/SAM3104MPLinux # ./installSAM
prereqSAM: All prerequisites for the ITSAMP installation are met on operating system:
SUSE Linux Enterprise Server 10 (s390x)
VERSION = 10
PATCHLEVEL = 2
installSAM: Installing System Automation on platform: s390x
installSAM: Packages will be installed from directory:  ./Linux/s390

installSAM: Installing
 ./Linux/s390/src-1.3.0.4-09204.s390.rpm

installSAM: Installing
 ./Linux/s390/rsct.core.utils-2.5.3.3-09204.s390.rpm
 ./Linux/s390/rsct.core-2.5.3.3-09204.s390.rpm
 ./Linux/s390/rsct.basic-2.5.3.3-09204.s390.rpm
...
```

```
...
installSAM: The following license is installed:
Product ID: 101
Product Annotation:
Creation date: Wed Oct 24 20:00:00 2007
Expiration date: Thu Dec 31 18:59:59 2037
Subsystem         Group            PID     Status
 ctrmc            rsct             2613    active
 IBM.ERRM         rsct_rm          2677    active
 IBM.ConfigRM     rsct_rm          2709    active
 IBM.AuditRM      rsct_rm          2741    active

installSAM: All packages were installed successfully.
```

- Start the domain:

```
tiv024:/ # startrpdomain SA_Domain
```

- Check installed code levels:

```
tiv024:/ # lssrc -ls IBM.RecoveryRM
Subsystem         : IBM.RecoveryRM
PID               : 18156
Cluster Name      : SA_Domain
Node Number       : 1
Daemon start time : 11/09/09 14:30:45

Information from malloc about memory use:
   Total Space    : 0x00108000 (1081344)
   Allocated Space: 0x000fafb8 (1028024)
   Unused Space   : 0x0000d048 (53320)
   Freeable Space : 0x0000c1a0 (49568)

Total Address Space Used : 0x01f71000 (32968704)
   Unknown               : 0x00000000 (0)
   Text                  : 0x00f93000 (16330752)
   Global Data           : 0x00115000 (1134592)
   Dynamic Data          : 0x0063c000 (6537216)
   Stack                 : 0x000f2000 (991232)
   Mapped Files          : 0x0079b000 (7974912)
   Shared Memory         : 0x00000000 (0)

Information about trace levels:
   _SEU Errors=255 Info=0 API=0 Buffer=0 SvcTkn=0 CtxTkn=0
   _SEL Errors=255 Info=0 API=0 Buffer=0 Perf=0
   _SEI Error=0 API=0 Mapping=0 Milestone=0 Diag=0
   _SEA Errors=255 Info=0 API=0 Buffer=0 SVCTKN=0 CTXTKN=0
   _MCA Errors=255 Info=0 API=0 Callbacks=0 Responses=0 RspPtrs=0
        Protocol=0 APItoProto=0 PrototoRsp=0 CommPath=0 Thread=0 ThreadCtrl=0
        RawProtocol=0 Signatures=0
   _RCA RMAC_SESSION=0 RMAC_COMMANDGROUP=0 RMAC_REQUEST=0 RMAC_RESPONSE=0 RMAC_C
ALLBACK=0
   _GSA Errors=255 Info=2 GSCL=0 Debug=0
   _SRA API=0 Errors=255 Wherever=0
   _RMA Errors=255 Info=0 API=0 Thread=0 Method=0 Object=0
        Protocol=0 Work=0 CommPath=0
   _SDK Errors=255 Info=0 Exceptions=0
   _RMF Errors=255 Info=2 Debug=0
   _RCD Errors=255 Info=2 Exceptions=0 Publisher=2 Audit=2
```

```
   Trace file spooling: OFF

   tiv024:/ # lsrpdomain
   Name      OpState RSCTActiveVersion MixedVersions TSPort GSPort
   SA_Domain Online  2.5.1.2           Yes           12347  12348

   tiv024:/ # lsrpnode
   Name                    OpState RSCTVersion
   tiv024 Online  2.5.3.3
   tiv025 Online  2.5.3.3
```

- Complete migration:

```
   tiv024:/ # runact -c IBM.PeerDomain CompleteMigration Options=0
   Resource Class Action Response for CompleteMigration

   tiv024:/ # lsrpdomain
   Name      OpState RSCTActiveVersion MixedVersions TSPort GSPort
   SA_Domain Online  2.5.3.3           No <--YAY!           12347  12348

   tiv024:/ # samctrl -m
   Ready to Migrate! Are you Sure? [Y|N]:.
   Y

   tiv024:/ # lssrc -ls IBM.RecoveryRM
   Subsystem         : IBM.RecoveryRM
   PID               : 18156
   Cluster Name      : SA_Domain
   Node Number       : 1
   Daemon start time : 11/09/09 14:30:45

   Daemon State:
      My Node Name          : tiv024
      Master Node Name      : tiv024 (node number =  1)
      Our IVN               : 3.1.0.4 <--YAY!
      Our AVN               : 3.1.0.4 <--YAY!
      Our CVN               : 214af86f14 (4af86f14)
      Total Node Count      : 2
      Joined Member Count   : 2
      Config Quorum Count   : 2
      Startup Quorum Count : 1
      Operational Quorum State: HAS_QUORUM
      In Config Quorum      : TRUE
      In Config State       : TRUE
      In Jeopardy           : FALSE
```

RESOURCES

- IBM Tivoli System Automation for Multiplatforms v3.1 Documentation: http://publib.boulder.ibm.com/tividd/td/IBMTivoliSystemAutomationforMultiplatforms3.1.html

- IBM Tivoli Information Center: http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc/toc.xml

- Edge Components v7.0 Documentation: http://publib.boulder.ibm.com/infocenter/wasinfo/fep/index.jsp?topic=/com.ibm.websphere.edge.doc/lb/info/ae/welcome_edge.html