APM High Availability Installation and Upgrade
Version 4.8

Written by:
Ben Stern (bstern@us.ibm.com)
George McMullen (mcmulleg@us.ibm.com)
Executive IT Specialist: Application Performance Management Best Practices

Change activity 01/29/20 Changed “db2 connection” to “db2 connect” at 2 locations.

CONTENTS

High Level Description

The following section provides a high level description of how to

1. Install APM in an HA environment
2. Apply APM fixpacks to an HA environment
3. Migrate an APM HA environment from 8.1.3 to 8.1.4
4. Apply best practice recommendations.

Design Considerations

When setting up your APM HA solution you need to determine if you want to use VIPs (Virtual IP Addresses) or Proxy Servers. You also need to consider your options when upgrading your APM HA servers. There are several options to consider when designing your HA configuration for APM. The main differences are the DB2 setup and determining if you want to use Virtual IPs or use proxy servers.

DB2 Options

For DB2 we recommend DB2 HADR which has a Primary server and Standby server. Both servers have a complete copy of the database. One is the primary and the other is the standby database. The standby database is kept in sync with the primary database so the standby can quickly take control if the

primary fails. DB2 HADR requires Virtual IPs or manually updating the APM configuration files to configure ACR (Automatic Client Reroute). You can manually failover DB2 HADR or you can automate it by adding TSAMP (Tivoli System Automation for Multiple Platforms). TSAMP is include in the DB2 package and DB2 can be configured using db2haicu. This configuration will require either 3 VIPs (WAREHOUS, DATAMART, SCR32) or ACR. If you do not use TSAMP you can manually failover the database by running db2 takeover for the 3 database and manually moving the VIP or VIPs to the other server.

Another DB2 option is to use one set of databases that reside on shared storage. For example, RAID storage could be used. In the event of a failure the filesystems are unmounted on the failed server and mounted on the standby server and the VIP is moved to the standby server. DB2 with shared filesystems can be automated using TSAMP and configured using db2haicu. When using this configuration all the filesystems are moved together and all 3 databases are moved together. This configuration requires 1 VIP and ACR is not supported. Using a single database on a shared filesystem takes longer to failover but it saves the cost of the duplicate database and only requires one VIP for DB2.

DB2 License Agreement

DB2 license clarification: The DB2 10.5 AESE image is included with APM v8 as a supporting program, which means the APMv8 client is licensed to install and use DB2. The license is "only to support Licensee's use of the Principal Program under this Agreement and within the limits of the Proofs of Entitlement for the Program". The detail of this "supporting program" license restriction is in the APMv8 product license. The DB2 image in the APMv8.1.4 bundle is fine to use with APMv8 in order to install a remote DB2 server and as long as it complies with the license restriction, you don't have to purchase a DB2 license for this usage. Whether you use the locally-installed DB2 or the separately bundled DB2 with APMv8, the licensing is the same.

APM Options

For APM you have the option to use a Virtual IP to direct agents to the primary APM server or you can use a proxy server to direct agents to the primary APM server. The advantage of using a proxy server is that a proxy server can redirect the agents to an APM server on another subnet or even another data center. If you are using a proxy server, to make APM server “A” become the primary server you would need to redirect the forward proxy server and reverse proxy server to server “A”. **USING HTTPS OVER A PROXY SERVER IS NOT SUPPORTED**.

If you are using Virtual IPs for APM, both servers need to be on a common subnet. For example if “ifconfig –a “ indicates the subnet is 255.255.255.0 then there are only 256 IP addresses that can be assigned to that subnet. Both APM servers and the VIP must be part of that subnet. If you are using a virtual IP, you would use ifconfig to remove the VIP from server “B” and use ifconfig to assign the VIP to server “A”. Never assign the VIP to both servers at the same time and never make the VIP permanent which would automatically assign the VIP during a reboot of the server. You can also use multiple VIPs

for your APM servers; one for users to connect to the Web browser (apmus) and; one for agents to connect to the APM server (agents). Then if you wanted to move the agents from one APM server to another APM server you would move the VIP for those agents to the other APM server. Using a VIP for the agents to connect will also allow you to block the agents from connecting to APM during an APM upgrade. HTTPS works when using VIPs.

APM can connect to DB2 using a VIP with route. You can route the connection from APM to DB2 through an APM VIP. Then only the APM server that has the VIP assigned will be able to access DB2 through the firewalls. If you are using TSAMP, you can add a ServiceIP resource (VIP) to the TSAMP policy and use TSAMP to move your VIPs. TSAMP will automatically monitor the VIPs and prevent a VIP from being assigned to both servers at the same time.

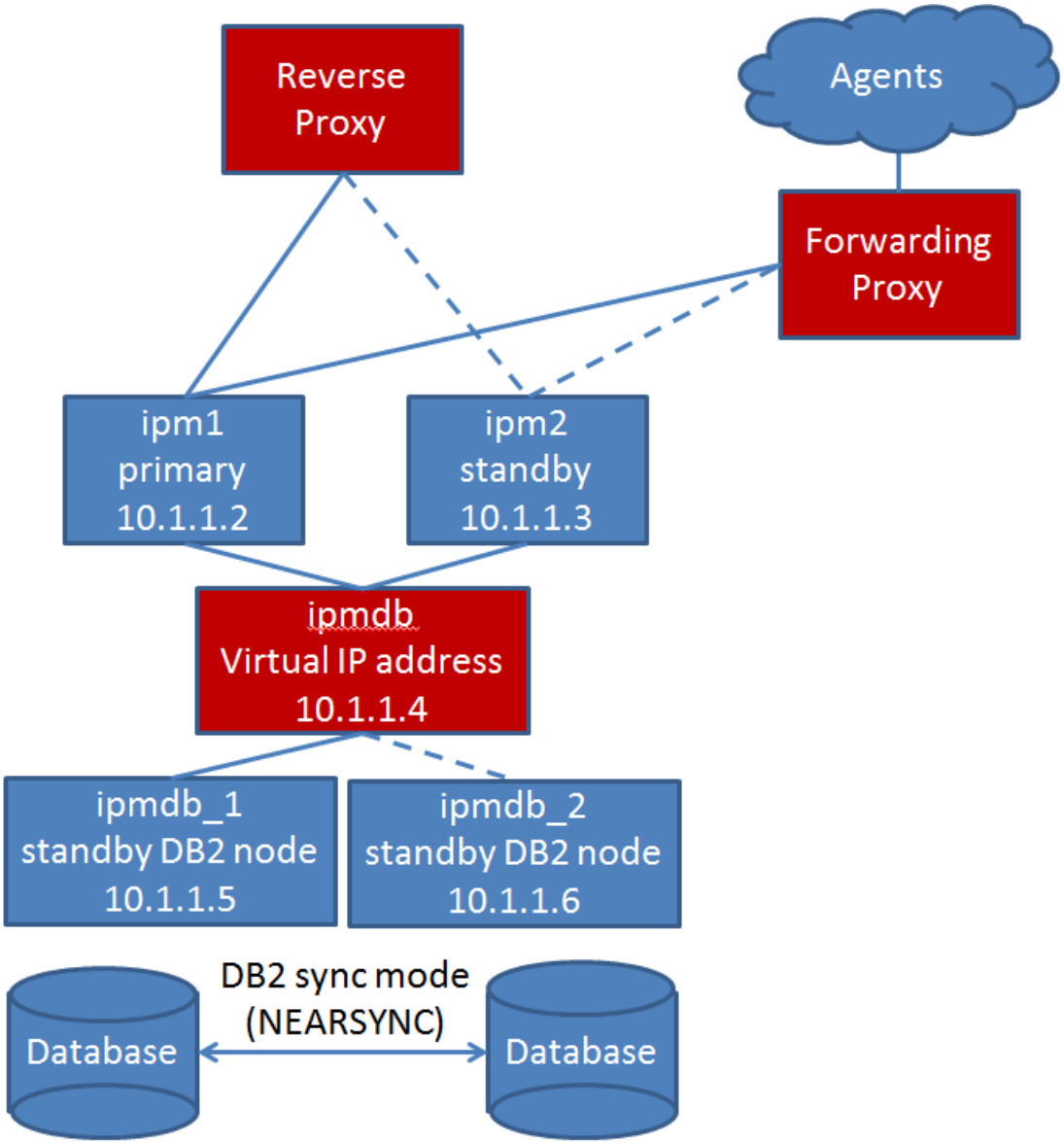
You must use firewalls to prevent both APM servers from accessing the database at the same time. There are no exceptions. If APM server "A" is the primary, then APM server "B" must be blocked from accessing the database. You do not need to change the firewall rules during an APM failover if you use a VIP on the APM server to route connections to DB2 and the firewalls only allow the VIP to access DB2.

An alternative to VIPs is using DNS entries and updating the DNS during a failover. Some customers use this option but we do not provide documentation for it here.

APM 8.1.4 interim fix 5 added support for customized database names and customized DB2 instance on the remote DB2 servers. You are not required to use the instance name db2apm or the database names WAREHOUS, DATAMART, SCR32 on your remote DB2 server.

The diagram below shows how the components communicate. In a single node DB2 deployment, the DB2 server would replace the component that is marked as the DB2 ipmdb VIP. The proxy servers can be replaced with VIPs.

Deployment Diagram:



Reference Documentation:

IBM Cloud Application Performance Management, Private
https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm

Upgrading the server on the same system
https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/upgrade_server_inplace.htm

Upgrading the server side-by-side
https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/upgrade_server_multiplesystems.htm

Forwarding proxy
https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/config_forwardproxy.htm

The latest version of this document is located at
https://developer.ibm.com/apm/resources/upgrading-a-high-availability-configuration/ under documentation

Installing APM 8.1.4 on a New Set of Servers

High Level Overview

1. Setup a remote DB2 server. This server can either be setup as a stand-alone DB2 server or as a DB2 HADR clustered environment. This will be used as the backend database for the IBM Performance Management environment. We recommend DB2 HADR as the mechanism used to achieve high availability within DB2.

2. You must setup firewalls. Setup a firewall on the database server(s) so that only one of the two APM servers can communicate with the databases. During the installation and execution of the APM environment, you will configure the firewall so that the active APM server is able to communicate with DB2, but the other APM server is blocked.

3. Setup 2 APM servers. Each of the APM servers will be configured to communicate with the same DB2 server or DB2 cluster.

a) You will initially setup the standby APM server using the shared DB2 server or cluster

b) After installing the standby APM server, do a db2 takeover to make the primary become the active DB2 server and install the SRC UDF routines on the DB2 server.

c) Install the primary APM server using the shared DB2 server or cluster

d) APM HA additional requirements

1. Firewalls are required. Both APM servers will be active and running, but communications to the DB2 server needs to be blocked from one of the two APM servers. During normal operations, traffic from the standby APM server will be blocked to the DB2 server(s). During failover operations, traffic from the primary APM server will be blocked to the DB2 server(s). This ensures that only one of the two APM servers is writing to the database.

2. All user interface (UI) communications to the APM server will be done through reverse proxy or a Virtual IP address so that it can be directed to the currently active APM server.

3. All Agent traffic will go through a forwarding proxy or Virtual IP address. The forwarding proxy will be configured to communicate to the currently "active" APM server. In lieu of a forwarding proxy the agents can be configured to use a virtual IP that is assigned to the primary APM server.

4. Periodically, you will run the backup.sh script on the primary APM server and restore the backed up configuration to the standby APM server using the restore.sh script.

5. Database backups will be performed on the database server, following best practices for your database configuration. These processes will differ depending on whether you are using a single server database, an HADR database with replication, or a database cluster.

Failover Process

The failover processes outlined in this document are manual steps, but it is possible to detect failures and automate the processes identified in this document.

Steps required for failover. During a failover the following things must happen.

e) To failover APM:

1. First, remove the VIPs on the APM server or stop the proxy servers to prevent the Agents and UI traffic from accessing the primary APM server. (The VIP for the Agent traffic and UI traffic can be the same VIP or you can have two separate VIPs. Two separate VIPs are recommended)

2. Next, update the firewalls to prevent the primary APM server from accessing DB2. In lieu of updating firewall rules you can remove the DB2 VIP from the primary APM server to prevent it from accessing DB2.

3. If you are updating firewalls, you also need to force applications using the db2 instance ID to terminate existing connections. Updating firewalls does not block existing connections. If this instance is dedicated to one APM server, you can run "db2 force applications all" to drop ALL connections to ALL databases owned by the instance ID.

4. Next, update the firewalls to allow the standby APM server to access DB2 or assign the DB2 VIP to the standby APM server to allow the standby APM server to access DB2.

5. Finally, add the APM VIPs to the standby APM server or update the proxy servers to allow the agents and UI traffic to connect to the standby APM server.

6. If this failover was unplanned, determine why APM failed, fix it, and fail back to the primary APM server or reverse your backup/restore process to keep the primary APM server in sync with the backup APM server.

f) To failover DB2:

1. First, remove the DB2 Virtual IPs from the primary DB2 server. If you are using ACR or TSAMP automation, skip this step.

2. Next, from the db2 instance ID on the standby DB2 server perform a DB2 takeover for all 3 databases by using a script like "db2takeover.sh". If you are manually entering the takeovers, do the takeovers one at a time waiting for the previous takeover to complete before starting the next takeover. If you are not using automation, as root add the DB2 Virtual IPs to the standby DB2 server. If you are using TSAMP to automate the DB2 failover process, skip this step to move the VIPs.

3. There is no APM requirement to failback. If your backup tools expect APM to be running on the primary node, then you should failback as soon as possible.

Best Practices

g) Recommendation for applying patches. You can eliminate some down time by patching the APM servers one at a time. First patch the standby APM server while it does not have access to DB2. Then do a failover and patch the other APM server. Normally the only outage that you should see is the short period of time that it takes to do a failover. See the section on "Applying fixes in an APM HA environment" for details.

h) Recommendation for backing up the APM server. A recommended set of steps and schedules are provided for backing up the configuration and event content on the primary APM server and restoring the content onto the standby APM server. These steps can be used to ensure that the two servers are in sync in case there is a failover. See "APM Server Synchronization via Backup/Restore" for details.

i) Recommendations for backing up DB2: With DB2, a good backup/restore strategy is important to ensure that the data can be restored in case there are any software or hardware failures. Typically, this includes setting up periodic full backups as well as incremental backups. We recommend DB2 HADR for the DB2 database. DB2 HADR will maintain a duplicate copy of your data on the standby server. We also recommend daily online backups of your Warehous, Datamart, and SCR32 databases. Depending on your preferred method of DB2 high availability, go to the appropriate section of the document for detailed instructions. Most of the documentation is written with references to the DB2 server. There is information in appendixes A, D, E,and G for DB2 HADR configurations:

   Appendix A: Setting up High Availability with DB2 HADR Cluster This appendix documents how to setup the APM database in a DB2 HADR configuration. It does not include information on setting up a VIP.

   Appendix D: Dropping Databases in a DB2 HADR Environment This appendix gives detailed information on dropping databases in a DB2 HADR environment. If you follow the recommendations in this document, you should not need to use this section.

   Appendix E: Accessing DB2 HADR without a VIP (ACR) This section of the documentation provides detailed information how to configure the APM components so that they use a primary and standby database by defining the hostname for the primary DB2 server and the hostname for the alternate DB2 server.

   Appendix E: Accessing DB2 HADR without a VIP This section of the documentation provides an example of how to setup HADR.

Setup DB2

Setup DB2 based on your desired level of high availability. DB2 can be setup as a single node or can be setup in a DB2 HADR cluster. If you choose to setup DB2 as a single node configuration, you will have some downtime required to setup a new DB2 server and restore the backed up database. If you setup a DB2 HADR cluster, there will be little downtime during many failure conditions.

IMPORTANT: The IBM Performance Management software requires DB2 Advanced Enterprise Edition 10.5 or higher. There are features that are only available in the advanced edition that are exploited by the APM software. When setting up the DB2 server, please use the DB2 Advanced Enterprise Server edition (AESE) or DB2 Advanced Workgroup Server edition (AWSE). DB2 AWSE 11.1.3.3 is currently recommended.

APM 8.1.4 interim fix 5 added support for customers to use their own name for the DB2 instance on the DB2 server and their own names for the databases on the DB2 server

When installing DB2, the following 4 accounts will be setup on the DB2 server. The Linux account "db2apm" will be the instance owner. The DB2 fenced user will be db2fenc1. The DB2 Administration Server (DAS) user for DB2 10.5 will be dasusr1. In addition, setup an itmuser OS account on the database server. This account will be used to access the data in the database. When you are done, you will have these 4 Linux OS accounts on the database server:

- db2apm (or a custom instance name on your remote DB2 server).
- db2fenc1
- dasusr1 (Not required for DB2 11.1)
- itmuser

Make note of the passwords for db2apm and itmuser. They will be used during the installation of the APM server and future operations.

Setup the APM databases on the primary DB2 server and setup the DB2 client on the APM server by following the instructions in IBM Performance Management for setting up a Remote DB2 database. https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/install_server_mydb2.htm

Note: The instructions may be missing a step to set **DB2_ATS_ENABLE=YES** on the remote DB2 server. If "db2set" does not have it set, then from the DB2 instance ID run

```
db2set DB2_ATS_ENABLE=YES
```

If you are using a DB2 HADR cluster or DB2 HADR cluster with VIP, setup the 3 databases on the primary DB2 node and then follow normal practices for configuring the databases in a cluster. Sample instructions on how to setup an HADR database are located in Appendix G.

If you plan on using DB2 HADR, at this point you should have completed the base DB2 install and installed the DB2 fixpack on both remote DB2 servers.

After following the instructions, you should have 3 databases created and tuned with some of the schemas populated. The three default databases are:

- WAREHOUS
- SCR32
- DATAMART

You can confirm that the databases are created by issuing the following command as the db2apm user or another user with database privileges.

```
db2 list database directory
```

You should see a list of the three databases and their home directories.

At this point you should be able to access the databases from the APM client. Verify you can access the databases.

DB2 HADR clustering is normally setup after the databases have been created and the second APM server has been installed. Detailed information on setting up a DB2 HADR Cluster can be found in **Appendix A**: Setting up High Availability with DB2 HADR Cluster

and additional instructions can be found online.

If you are setting up a standard high availability DB2 HADR clustered environment without a VIP, you should perform the entire IBM Performance Management server installation using the primary database node. Then, configure the HADR cluster after all of the software is installed. This is the easier than setting up DB2 HADR and then installing the software.

However, if you are using a DB2 HADR VIP, then the VIP must be setup before the APM software is installed. The APM installation will require the VIP to update the APM configuration files that are used to access DB2.

Verify TSAMP is ready.

If you plan to use TSAMP to automate the failover between DB2 servers you should perform the next step to verify TSAMP is ready. If you are not ready to setup a standby DB2 server at this time, you can do it at any time in the future.

To test TSAMP (Tivoli System Automation for MultiPlatforms), you should create a two node cluster to verify that TSAMP is working. When you install the DB2 base and install the DB2 fixpack it automatically installs TSAMP, the underlying RSCT code, and any efixes. You can verify TSAMP and RSCT were installed by running samversion and ctversion on both nodes. It should return the version of TSAMP and RSCT. For example,

```
[root@sapm-db2a ~]# samversion
rsa41svcs003g 4.1.0.3  Oct 24 2017 14:17:21
[root@sapm-db2a ~]# ctversion -Ab
RSCT_Build_Name=rrablxs001a 3.2.3.1 RSCT_Build_Time=17298.01:29:45
RSCT_Build_Context=amd64_linux_2
```

Both nodes should indicate the same version of TSAMP and RSCT

```
[root@sapm-db2b ~]# samversion
rsa41svcs003g 4.1.0.3  Oct 24 2017 14:17:21
[root@sapm-db2b ~]# ctversion -Ab
RSCT_Build_Name=rrablxs001a 3.2.3.1 RSCT_Build_Time=17298.01:29:45
RSCT_Build_Context=amd64_linux_2
```

If both nodes are not at the same version of TSAMP and RSCT, then you need to go back to the steps where you installed DB2 and install the exact same versions of DB2 on both of the remote DB2 servers.

Run samlicm -s to show the license information. The expiration date should be 2037

Run samlic –p; echo $?; to verify the license is permanent. The return code will be 0 if the license is permanent.

To test TSAMP, run the following steps to create a simple 2 node cluster.

1. Use the value that is returned from the hostname command as the node names of your DB2 servers. Then run preprpnode <node1> <node2> As root on one of the DB2 servers For example,

   ```
   [root@sapm-db2a ~]# hostname
   sapm-db2a
   [root@sapm-db2a ~]# preprpnode sapm-db2a sapm-db2b
   ```

2. Run the exact same preprnode command as root on the other server.

   ```
   [root@sapm-db2b ~]# preprpnode sapm-db2a sapm-db2b
   [root@sapm-db2b ~]#
   ```

3. On one of the two DB2 servers use the mkrpdomain command to create a domain. The domain can be any name. This sample domain is called APM_Domain. For example,

   ```
   [root@sapm-db2a ~]# mkrpdomain APM_Domain sapm-db2a sapm-db2b
   ```

4. On one of the two DB2 servers start the domain. For example,

   ```
   [root@sapm-db2b ~]# startrpdomain APM_Domain
   ```

5. Within a few seconds you should be able to verify the domain is online. For example,

   ```
   [root@sapm-db2a ~]# lsrpdomain
   Name      OpState RSCTActiveVersion MixedVersions TSPort GSPort
   APM_Domain Online  3.2.3.1          No            12347  12348
   [root@sapm-db2a ~]# lsrpnode
   Name     OpState RSCTVersion
   ```

```
sapm-db2a Online  3.2.3.1
sapm-db2b Online  3.2.3.1
```

6. The lsrpdomain command should indicate MixedVersions is “No”, If it is a “Yes” that means you upgraded RSCT or TSAMP and did not follow the steps to complete the migration. If it is “Yes” follow the steps on the internet to complete the migration and then rerun lsrpdomain to verify both nodes are at the same version

7. Do not leave the domain up and running because it is missing things like resources and a tie breaker. You do not want automation to take any action yet. Run stoprpdomain APM_Domain on either node then verify the domain is stopped. For example,

```
[root@sapm-db2a ~]# stoprpdomain APM_Domain
[root@sapm-db2a ~]# lsrpdomain
Name      OpState       RSCTActiveVersion MixedVersions TSPort GSPort
APM_Domain Pending offline 3.2.3.1          No          12347  12348
[root@sapm-db2a ~]# lsrpdomain
Name      OpState RSCTActiveVersion MixedVersions TSPort GSPort
APM_Domain Offline 3.2.3.1          No          12347  12348
```

DB2 Standby SCR UDF steps

1. You need to install the SCR UDF Routines on the standby DB2 server. Make the standby DB2 server become the active DB2 server and setup the SCR UDF Routines. The steps for setting up the SCR UDF routines are located in the section called "Setup SCR UDF Routines" near the bottom of Appendix G: “Example of How to Setup HADR" in this document. Run steps 8d "Run the setup-dbconfig program." and step 8e "Install tbsmdb and setup the SCR UDF routines" on the standby DB2 server.

APM HA Preparation Steps

1. APM requires firewalls to prevent both APM servers from accessing DB2 at the same time. Refer to Appendix K to create firewall scripts and test your firewall scripts

2. Agent and APM UI connections will need to be directed to the APM server that is acting as the Primary APM server. This can be done by using VIPs or Proxy servers. If you are using proxy servers, refer to Appendix L to setup proxy servers.

Installing the APM Servers

The next step is to install the two APM servers. One will be setup as the primary server and the other will be setup as the standby. Their functions and software will be identical. But, only one APM server can actively be used to monitor the agents connected to the environment. The other server will be active and ready to take over the workload in case the primary server goes down. Begin by installing the standby APM server.

Install the standby APM server

1. Before beginning the installation of the standby APM server, prevent the primary APM server from accessing db2 and allow the standby APM server to access DB2. If you are using VIPs, on the primary APM server remove the VIP that allows APM to access DB2. For example, on the primary APM server run **./block.sh db2**. This will remove the VIP that APM is using to access DB2 and drop the connections. Then on the standby APM server run **./allow.sh db2**. This will assign the VIP to the standby APM server and establish the routes for accessing DB2. If you are not using VIPs, then on the DB2 server update the firewalls to block the primary APM server, then as the DB2 instance ID run "db2 force applications all" to drop ALL connections to ALL databases owned by the instance ID, then on the DB2 server updatre the firewalls to allow the standby server to access DB2. If you are toggling the firewall rules you can use the scripts **./apm-fw.sh remove primary** script to prevent the primary APM server from accessing db2, then force applications all, and execute **./apm-fw.sh add standby** script to allow the standby APM server to access DB2. If you are using DB2 HADR, execute these scripts as root on both DB2 servers.

2. Since you will be connecting to a remote DB2 server, you must install either the IBM Data Server Client or the DB2 server software on the APM server machine. You do not need to create any databases on the APM server machine. Perform step 3 under "Connecting to a remote Db2 server" at https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/install_server_mydb2.htm

3. Refer to the installation instructions at https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/install_server.htm "Downloading and installing the server" Complete steps 1 thru 8

4. The following instructions are details for step 8g when editing the install.properties file.

   Note: APM install may fail if X11 is enabled. Do not use X11 on your putty session. See **https://www-01.ibm.com/support/docview.wss?uid=ibm10740409**

Before beginning the install, you must ensure that the database names that are set in the install.properties file match your DB2 database names. The install.sh script will read the install.properties file and use the values in the file as the defaults when it prompts you for answers. The Install script will create the catalog entries for the database names that are specified in that file. Unless you update the properties file APM will use the names WAREHOUS, DATAMART, and SCR32 when it configures APM. Since the install.sh script does not ask for the names of the databases you must update the install.properties file if you are not using the default names for the databases.

Update the following lines in install.properties:

a. db2.hostname=localhost Set it to the remote Warehous VIP. If you are not using VIPs set it to the primary db2 server Hostname.

b. db2.installdir=/opt/ibm/db2 If you did not use the default install directory for DB2 you should update this value.

c. db2.external.instance=db2apm You can enter the instance name here or enter it when prompted by the install script.

d. db2.nodename=APM_NODE This is the name that DB2 will use when cataloging the NODE. You can use this default or use any 8 character name.

e. db2apm.password= Leave the passwords blank. Do not record your passwords here.

f. If you are not using DB2 V10.5, make sure you complete the step to update KQZ_JDBC_JAR_PATHS= in <Install_dir>/serveragents/config/<ShortHostname>_te.cfg

5. If you wish to review an interactive example of the installation process on the Standby APM server before you attempt the install, go to Appendix B: Installation Prompts for Standby APM Server.

6. After completing steps 1 thru 8 continue to step 9 at https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/install_server.htm Follow the normal installation procedure as detailed in step 9 for installing the IBM Performance Management server with a few exceptions:

a. There is no need to configure the Agent packages during the install. That step will be executed when the primary APM node is installed.

b. If you are using DB2 HADR, during the database configuration section, specify the hostname or DB2 HADR VIP for accessing the WAREHOUS database. If you are not using VIPs, specify the hostname or IP address of the primary database server.

c. You will be asked to confirm the hostname and IP address of the server that will be used in a browser to connect to the APM server. In this section, you want to specify the hostname and IP address of the reverse proxy as seen below or the VIP for the UI to access APM. Do NOT accept the default values. If you accidentally accept the default values, you can execute the /opt/ibm/ccm/configure_server_address.sh script following the install.

   i. Fully qualified domain name: proxy1.ibm.com (or Hostname of the VIP for APM UI)

   ii. Short hostname: proxy1 (or Short hostname of the VIP for APM UI)

   iii. IP: 10.1.1.1 (or VIP for APM UI)

Completing the installation

After the APM install.sh script completes and before agents connect to the APM server and before you install the Interim Fix. Refer to the section on "Post APM Installation Steps" for details to complete the following steps.

1. Update as.environment
2. Add port 8093 to the reverse proxy server
3. Setup certificates for the reverse proxy server
4. LDAP requirements
5. Install Interim Fix
6. Verify KAS_HOSTNAME
7. Configure Agent Image Installation package
8. Allow users to access the APM UI.
9. Update vhost.xml files for APM alias.
10. Log into the APM server
11. Verify Host Name Overide IP address
12. Check the setting for My Components
13. Allow Agents to connect to the APM server.
14. Set up DB2 HADR
15. Add additional VIPS to DB2 HADR
16. Verify APM SCR is blocked.

Install the primary APM server

1. If you plan to use DB2 HADR and you have not setup HADR yet, that is OK. The instructions to set up HADR are located later in this document. Sample steps to create an HADR database are in Appendix A: "Setting up High Availability with DB2 HADR Cluster".

2. Before beginning the installation, verify your firewalls are blocking the standby APM server from accessing DB2 and allowing the primary APM server to access db2. If you are using VIPs, this can be done by running ./block.sh db2 on the standby APM server and running ./allow.sh db2 on the primary APM server. These scripts normally run as root.

3. On the primary APM server, extract the IBM Performance Management server software. The media is delivered as a tar file that can be extracted. After extacting the tar file, you will see an install.sh file. Do not execute the install.sh script yet. There are additional steps require when using a remote DB2 server.

4. Refer to "Install the standby APM server" in this document and complete steps 2 thru 5 to install the db2 client and prepare to install APM.

5. Refer to "Install the standby APM server" in this document and complete step 6 to install APM. This time, you DO want to configure the Agent packages. When prompted, specify the hostname or IP address of the forwarding proxy or VIP for the agents to connect to APM. This will configure the Agent packages so that they will send their traffic to the forwarding proxy. (proxy2.ibm.com) or directly to APM by using the VIP

Completing the installation

After the APM install.sh script completes and before agents connect to the APM server and before you install the Interim Fix. Refer to the section on "Post APM Installation Steps" for details to complete the following steps.

1. Update as.environment
2. Add port 8093 to the reverse proxy server
3. Setup certificates for the reverse proxy server
4. LDAP requirements
5. Install Interim Fix
6. Verify KAS_HOSTNAME
7. Configure Agent Image Installation package
8. Allow users to access the APM UI.
9. Update vhost.xml files for APM alias.
10. Log into the APM server
11. Verify Host Name Overide IP address
12. Check the setting for My Components

13. Allow Agents to connect to the APM server.
14. Set up DB2 HADR
15. Add additional VIPS to DB2 HADR
16. Verify APM SCR is blocked.

Post APM Installation Steps

1. Update as.environment
   The value of KAS_HOSTNAME on the standby and primary APM servers must match.
   a. apm stop oslc
   b. cd /opt/ibm/ccm/oslc_pm/config
   c. vi as.environment
   d. add the following to the end of the file: KAS_HOSTNAME=<fully-qualified primary hostname>
   e. save the file
   f. On the secondary APM server only
      1. - cd /opt/ibm/ccm/oslc_pm/lx8266/as
      2. – rm –f KASSTATE
   g. apm start oslc
   h. KASSTATE will be recreated when oslc restarts provided APM has access to the SCR database.

2. Add port 8093 to the reverse proxy server. If you are using a reverse proxy server, add a section for port 8093 that is similar to port 8099 to the /etc/httpd/conf/httpd.conf file. (Added for 8.1.4) See "Setup your Reverse Proxy" in this document.

3. Setup certificates for the reverse proxy server. If you are using a reverse proxy server for users to connect to the APM UI and you are not using custom certificates, then perform the following steps

   a. Before you can logon to the APM server, you must import the SSL certificates from your reverse proxy into the APM server.
      1. Export the *.crt file from your reverse proxy HTTP server. In my example, the file is named proxy1.crt.
      2. Copy the *.crt file to the APM server and place it in a temporary directory such as /tmp

3. For example, scp -p root@ Add port 8093 to the reverse proxy server9.42.12.249:/etc/pki/tls/certs.backup/localhost.crt /tmp/proxy1.crt

b. Backup the existing trust store
   - cp /opt/ibm/wlp/usr/shared/resources/security/trust.jks /opt/ibm/wlp/usr/shared/resources/security/trust.jks.sav

c. List the current contents of the trust store:
   - keytool -list -keystore /opt/ibm/wlp/usr/shared/resources/security/trust.jks -storepass ccmR0cKs!

d. Import the certificate file into the APM server using the following command:
   - keytool -import -trustcacerts -alias proxy1 -file /tmp/proxy1.crt -keystore /opt/ibm/wlp/usr/shared/resources/security/trust.jks -storepass ccmR0cKs

e. List the current contents of the trust store to confirm that the certificate was imported.
   - keytool -list -keystore /opt/ibm/wlp/usr/shared/resources/security/trust.jks -storepass ccmR0cKs!

f. After importing the certificate, restart the APM UI service using the following command:
   - apm restart apmui

4. If you are using a VIP for users to connect to the APM UI and you want custom UI certificates then see Appendix P: Creating custom certificates.

5. LDAP requirements. If you are using LDAP, you need to have either the IBM® Cloud Application Performance Management Private, V8.1.4.0 interim fix 6, or a later server interim fix, or the APAR fix for RTC PMR 133748 applied to both the primary and standby APM servers. Interim fixes for the Cloud APM server version 8.1.4 are available to download from IBM Fix Central. The fix is required when you are restoring to the standby server and also using LDAP.

6. Install Interim Fix. After you complete the Cloud APM server installation, install the **IBM Cloud Application Performance Management, Private V8.1.4.0 interim fix 9**, or a later server interim fix. Interim fixes for the Cloud APM server V8.1.4 are available to download from IBM Fix Central. No unique HA configuration options will need to be specified during the upgrade.

7. Verify KAS_HOSTNAME in /opt/ibm/ccm/oslc_pm/config/as.environment. If this is the install for the 2nd APM server, verify both APM servers have a line in the file to set KAS_HOSTNAME to the fully qualified hostname of the primary APM server.

8. Configure Agent Image Installation package. You can configure the agent images now or any time later. You only need to do this step once. To create the agent image for installing agents, run /opt/ibm/ccm/make_configuration_packages.sh.

    a. When you are asked "Enter the IP address/hostname that should be used by agents to communicate with the server." Enter the VIP that is used for the agents to connect to the server.
    b. And run /opt/ibm/ccm/configure_agent_images.sh.

9. Allow users to access the APM UI. If you are using VIPs, assign the VIP for users to access the APM UI to this server. For example, run ./allow.sh apmui as root on this server. If you are using a reverse proxy server, update the httpd.conf file to allow users to access the APM UI.

10. Update vhost.xml files for APM alias. IF08 added security to require users to access the APM server using the name that was used to configure the APM server. If your users are using an alias like "myapm:9443" to access APM, we recommend that they use the IP address or hostname that was used when APM was installed. If you decide to use an alias to access APM then the alias name must be added to the vhost.xml files and it may or may not work and it will not work if the user intends to open multiple sessions on their browser using an alias. Additional sessions can be opened using the hostname or IP address that was used when APM was installed. If you receive the following message, use the correct name in the URL to connect to the APM server. "This page isn't working"

    The following is not recommended. This is a test example. I configured the APM server using the VIP for the APM server. I also want to access the APM UI using an alias known as "testapm". I added an alias "testapm" to my /etc/hosts file to associate it with the VIP that I used when APM was installed. To be able to access the APM server as "testapm" I need to insert the following lines into the server-vhost.xml files.

    /opt/ibm/wlp/usr/servers/oidc/server-vhost.xml
    <hostAlias>testapm:8099</hostAlias>

    /opt/ibm/wlp/usr/servers/uviews/server-vhost.xml
    <hostAlias>testapm:8092</hostAlias>
    <hostAlias>testapm:8093</hostAlias>

    /opt/ibm/wlp/usr/servers/apmui/server-vhost.xml
    <hostAlias>testapm:9443</hostAlias>
    <hostAlias>testapm:8080</hostAlias>

    If the lines are not added, you may get the message "Context Root Not Found" when you attempt to access the APM server. Or "This page isn't working".

11. Log into the APM server. Log into the APM server's APM UI and ensure that it is functioning properly. When you login to the server, you will specify a URL using the reverse proxy or VIP.

Because we configured the APM server with the fully qualified and shortname of the reverse proxy or VIP, that is what the UI is expecting when requests come to the server. You will NOT be able to connect directly to the UI by specifying the hostname of the standby APM server.

a. Example: https://proxy1.ibm.com:9443

b. When prompted enter the administrator username and password. The username is apmadmin. The default password is apmpass. If you specified a different password during the install, use the password that you specified.

c. If you don't see the logon screen or are unable to logon to the APM server, look at two things:

1. First, confirm that the APM services are all running by typing: apm status

2. If the APM services are running and you are unable to see the login screen or are unable to login, it is probably a configuration problem with the reverse proxy or VIP

12. Verify the Host Name Override IP address. Logon to the APM UI. Select the "System Configuration" icon. Select "Advanced Configuration". Then select "Agent Central Configuration". The value in "Host Name Override" should be the VIP that the agents will use when connecting to the APM server. This value should match the VIP that is used when you configured the agent packages. It is used by the agents when reporting Agent CCS server connection status.

13. Check the setting for My Components. The setting for "My Components" is based on the size of your environment and is determined by the installation script. If the installation script determined this is a large server the option to select "My Components" was removed from the APM UI. You can add it back by setting ENABLE_MY_COMPONENTS=true for service apmui in file /opt/ibm/wlp/usr/servers/apmui/apps/customCfg/apmui.cfg Then "apm restart apmui". It may take a few minutes for "My Components" to appear under "All My Applications".

14. Allow Agents to connect to the APM server.. If you using a VIP for the Agents to connect to the APM server, add the agent VIP to the APM server to allow the agents to connect to the APM server. For example run ./allow.sh agents as root on this APM server. If you are using proxy servers, allow your forwarding proxy server to access APM.

15. Set up DB2 HADR. If you want to setup DB2 HADR, refer to Appendix G: Example of How to Setup HADR.

16. Add additional VIPS to DB2 HADR. If you are using a separate VIP for each database (3 VIPs), refer to Appendix H: Configuring APM to use 3 VIPs for DB2.

17. Verify APM SCR is blocked. IF09 added code to help prevent corruption of the database when both APM servers are accidentally allowed to access DB2. Verify IF09 is only allowing 1 SRC process to access DB2 by logging onto each APM server and checking the

messages in /opt/ibm/ccm/SCR/XMLtoolkit/log/msgGTM_XT.log.0 (where /opt/ibm is your install directory)

a. verify that one APM scr process has a message similar to this at the bottom of /opt/ibm/ccm/SCR/XMLtoolkit/log/msgGTM_XT.log.0

   [jcc][t4][2043][11550][3.69.24] Exception java.net.NoRouteToHostException: Error opening socket to server /10.21.5.73 on port 50,001 with message: No route to host (Host unreachable). ERRORCODE=-4499, SQLSTATE=08001

   Retry for 60 minutes. If this is a command line utility, press ctrl-c to stop the retry

b. And the other APM server has a messages like:

   GTMCL5319I: SQL file execution complete.

c. You may also see the following messages:

   GTMCL5600I: Disabling local heartbeat to the registry.

   GTMCL5598I: The SCR is relinquishing database control to another instance in an HA configuration.

d. If one of the APM servers is not being blocked from accessing DB2 then

   1. Determine why your firewalls are not blocking one of the APM servers.
   2. Fix your firewalls.
   3. If necessary, force the connections to be stopped
   4. Run "netstat –an | grep 50000" on the primary db2 server to verify there are no connections that have the IP address of the standby APM server. (where 50000 is the port that you assigned to DB2)
   5. On the APM server that is allowed to access DB2 run the following as root "apm restart oslc;"

18.

Install Monitoring Agents

You are now ready to install a small number of monitoring agents. The agent media has been preconfigured to connect to the forwarding proxy.

Using the Agent media that can be found in /opt/ibm/ccm/depot, install one or more agents.

- Note: Do NOT use the Agent media that you downloaded from Passport Advantage. You must use the Agent media that was reconfigured during the install process. The media found in /opt/ibm/ccm/depot has been configured to communicate using the forwarding proxy, or VIP.

Once an agent is installed, you will want to verify a couple of things:

1. Confirm that the agent is successfully connecting to the Primary APM server and is visible in the APM UI. Depending on the size of your environment, you might need to create a business application and add the agents to the application before they become visible.
2. View the /opt/ibm/apm/agent/localconfig/<2 letter code>/<2 letter code>_asfServer.xml file on one of the servers and check that the URL points to the forwarding proxy.
    - For the Linux OS Agent, this would be /opt/ibm/apm/agent/localconfig/lz/lz_asfServer.xml

You are now ready to start configuring and testing the failover between the two servers.

Configuring and Testing Failover

Now that the two APM servers are up and running, test to ensure that the failover and failback is working properly. Once you have ensured that the failover/failback is working properly, you need to create automation to automate as much of the process as possible..

Setup Customization and Synchronize the Content

In order to show that content is being synchronized properly between the two servers, it is important to make some changes. You might want to make the following types of changes:

- Create a new Threshold
- Create a new Resource Group
- Create a new business application or modify the contents of an existing application
- Customize Agent configuration settings that can be modified centrally via the UI…for example, define some log file monitoring or change the transaction tracking settings for an agent.
- Define some new Role Based Access Control (RBAC) settings
- Etc.

Now, you need to synchronize content between the servers. Some of the content is automatically synchronized by the fact that you're using a common DB2 server. But, some content must be synchronized by using the backup.sh/restore.sh scripts.

- Since the Primary APM server is now the active, server, run the /opt/ibm/ccm/backup.sh script. This will backup content and will save a file like:
    - /opt/ibm/backups/backup_20190129_123742.tar
- Your actual filename will be different, but will be identified when you run the backup.sh command.
- Copy the tar file to the Standby APM server. The file can be placed in any directory.
- Use the restore.sh script from 8.1.4 with the "-e scr" option. Do not use the restore.sh script from 8.1.3. When you restore the APM server you need to add the "-e scr" option because the scr component includes "./ccm/SCR/XMLtoolkit/bin/scr_restore.sh" which needs to access DB2 and it will hang because access to DB2 is blocked by the firewalls.
- You are now ready to restore the backup content. On the Standby server run the command "/opt/ibm/ccm/restore.sh –e scr -f <path to backup tar file>", where the path to the backup tar file is the file that you copied from the Primary APM sever.
    - Example: /opt/ibm/ccm/restore.sh –e scr -f /tmp/backup_20190129_123742.tar
- After a period of time, the restore will complete. You should pay attention to how long the restore takes. Later, as we automate the process, you'll need to understand how long this takes. However, the amount of time will grow as more agents are added to the environment and more customization is added. In a small environment a backup takes about 2 minutes and a restore takes about 30 minutes.
- You are now ready to perform a failover.

Content Not Backed Up

The backup restore procedures will back up the critical content to ensure that you can failover to the standby APM server. However, some data is not backed up.

- The DB2 server and the three databases are not backed up using the backup scripts. They should be backed up by your DBA according to your desired schedule. For example, weekly full backups + incremental backups.
- Deep Dive Diagnostic data is stored on the Agents and is not accessible within the APM server for backup and restore. However, during a failover, this data will not be lost because it is still available on the agent.
- Transaction Tracking data is stored within the MongoDB database. There is a large volume of transaction tracking data stored in the MongoDB database and it is not backed up by the backup.sh script. If desired, create a backup script to backup and restore the Transaction Tracking data that is stored in MongoDB.

Testing Failover/Failback

Before you begin

- Test your firewall. On some servers the firewalls will not block existing connections. To test your firewalls logon to the Primary DB2 server and execute the command to block the Primary APM server. Then on the DB2 server run "netstat –an | grep 50000" to see if connections between APM and DB2 are still active (where 50000 is the port that you assigned to DB2). If the connections are in a FIN_WAIT2 state, then they are being dropped. If they are in an ESTABLISHED state, then the firewalls are only blocking new connections. You may need to force the connections down by either running "apm stop min; apm stop server1; apm stop scr; apm stop txagent;" or running "db2 force applications all" to drop ALL connections to ALL databases owned by the instance ID.
- If you are using VIPs and the scripts provided for APM HA, you can do a fast failover by running the following 2 commands:

    1) On the Primary APM server run the following command as root
        - /scripts/block.sh all
    2) On the Standby APM server run the following command as root
        - /scripts/allow.sh all
    3) Allow Agent traffic by assigning the VIP to the APM server or updating the httpd.conf file on the Forwarding Proxy server and Reverse Proxy server.

Here are the details to test a graceful failover from the Primary APM server to the Standby APM server. Use the following steps to perform a failover.

- On the standby APM server as root and run "apm stop min; apm stop server1; apm stop scr; apm stop txagent;". This will stop any APM parts that may still be connect to DB2. Then block the Primary APM server from accessing DB2 by either updating the firewall rules (logon to your primary db2 server and block the Primary APM server by executing the "./apm-fw.sh remove primary" command on both DB2 servers or by running the "./block.sh db2" command on the APM servers. Then logon to the db2instance ID on the primary DB2 server and run "db2 list applications". If any of the applications have the IP address of the Primary APM server then your firewalls are only blocking new connections. If this is true then during a failover you will need to stop the Primary APM connections to DB2 before you allow the APM Standby server to connect to DB2. Or force the

connections to close by running something like “db2 force applications all” to drop ALL connections to ALL databases owned by the instance ID.

- To start a failover, on the Primary APM server run “apm stop min; apm stop server1; apm stop scr; apm stop txagent;” This will end the existing connections to the database and stop future connections.
- These same 4 processes need to restart after DB2 is available. On the APM Standby server
- Then reconfigure the firewall rules on the DB2 servers so that new traffic is now blocked from the primary APM server by running the “./apm-fw.sh remove primary” command on the DB2 servers. Or if you are using VIPs on the APM server run the “./block.sh db2” command on the APM server to prevent APM from accessing DB2.
- On the DB2 Primary server logon as db2apm and run “db2 list applications”. It may take a few minutes for the applications to stop. If any connections continue to exist from the Primary APM server run “db2 force applications all” to drop ALL connections to ALL databases owned by the instance ID.
- Allow the Standby APM server to connect to the database. You can do this by running the “./apm-fw.sh add standby” script on both the Primary and Standby DB2 servers or by running the “./allow.sh db2” on the standby APM server.
- On the Standby server start the 4 processes that were stopped earlier. Run “apm start_all”
- Next, redirect Agent traffic to the standby APM Server by either updating the forwarding proxy server or if you are using VIPs, you can run “./allow.sh agents” on the standby APM server.

    1) To reconfigure the forwarding proxy so that Agent traffic is directed to the standby APM server. You should only need to change one line in the httpd.conf file as follows:
        - Change: ProxyPass / http://apm1.ibm.com/
        - To: ProxyPass / http://apm2.ibm.com/
        - Then, recycle the HTTP server in order for the changes to take effect. (service httpd restart)
    2) To manually move the VIP from the Primary server to the Standby server use the following commands
        - On the Primary server remove the VIP by running ifconfig
            - ifconfig ens192:0 del 9.42.12.3 where ens192:0 is the nic and 9.42.12.3 is the VIP

        - Or ip address del 9.42.12.3/22 dev ens192:0 where /22 is the subnet mask.
        - Then ping 9.42.12.3 to verify it was removed.
        - Note: If you add an alias using ip addr add, sometimes ifconfig –a will not show it. Use ip adder show to see the IPs that are assigned to the nics
    - On the Standby server add the VIP as an alias by running
        - ifconfig [nic]:0 [IP-Address] netmask [mask]
        - For example, ifconfig ens192:0 9.42.12.3 netmask 255.255.252.0
        - Or ip address add 9.42.12.3/22 dev ens192:0

- Finally, redirect the UI traffic to the standby server.

    1) If you are using a reverse proxy, reconfigure the reverse proxy so that UI traffic is directed to the standby APM server. You will need to change four entries in the file. You'll find two entries for proxyPass two entries for proxyPassReverse. Replace the hostname of the primary APM server with the hostname of the standby APM server. Then, recycle the HTTP server in order for the changes to take effect. You can avoid editing the files by creating an httpd.conf file for APM1 and an httpd.conf file for APM2. Then if you want to redirect the proxy server to APM2 you would run cp httpd.conf.apm2 httpd.conf and run service httpd restart .

    2) If you are using VIPs for UI and agent traffic, proceed to the next step. Otherwise move the VIP that is being used for UI traffic from the Primary Server to the Standby server using the same process that you used to move the VIP for Agent traffic. You can use the "./block.sh agents", "./block.sh apmui", "./allow.sh agents" ,and "./allow.sh apmui" commands to move the VIPs.

- You should also optionally restart the following APM processes when either APM or DB2 fails over: "apm stop min; apm stop server1; apm stop scr; apm stop txagent; apm start txagent; apm start scr; apm start server1; apm start min;" These processes should restart automatically and during IF09 testing this step was not necessary.

- Everything should be fully functional following the failover. You may need to log out and back into the APM user interface.

- Note: If you are using a DB2 HADR cluster, you can also test the failover between the two database nodes. Use the DB2 commands to failover the database nodes. You can find information here:

http://www.ibm.com/support/knowledgecenter/en/SSEPGG_10.5.0/com.ibm.db2.luw.admin.ha.doc/doc/c0059999.html

- After failing over, confirm the following:

    1) Confirm that you can log into the APM server. You might want to shutdown the primary APM server to prove that you are accessing the correct server.

    2) Confirm that key features/functions are working properly

    3) Confirm that agents are still sending data to the APM server even though you are now using the standby server. There might be a small gap in your data from the time that you reconfigured the firewall and the time that the DNS changes take effect.

    4) Confirm that the configuration modifications that you made on the Primary APM server are showing up on the Standby APM server. For example, do you see the new Thresholds and Resource Groups that you created? Do you see the RBAC changes that you made? Etc.

- If desired, you can cause a fail-back to the Primary APM server. This can be accomplished by reversing the steps:

    1) The following 3 backup and restore steps can be skipped if the standby has only been acting as the primary for a short period of time (less than 2 days) and no configuration changes were made while the standby was acting as the primary.

        - Backup the content on the Standby APM server by running the backup.sh script on the Standby server.

        - Copy the Backup tar file to the Primary APM server

        - Restore the content to the Primary APM server by running the restore.sh script

    2) Block the agents from accessing the standby APM server, block the users from accessing the APM UI on the standby APM server, and use the firewalls to block the Standby server from accessing DB2. If you are using VIPs, you can run the following on the standby APM server: "./block.sh agents; "./block.sh db2; "./block.sh apmui;".

    3) If you are updating firewall rules, existing connections from the standby APM server will not be blocked. You must verify there are no remaining connections to DB2 from the standby server by running "db2 list applications". Then run "db2 force applications all" to drop ALL connections to ALL databases owned by the instance ID.

    4) Use the firewalls to allow the primary APM server to access DB2. You can update firewall rules or run the "allow.sh db2" script on the primary APM server.

5) Reconfigure the forwarding proxy so that Agent traffic flows to the Primary APM server. If you are using VIPs you can run, "./allow agents; " on the Primary APM server.

6) Reconfigure the reverse proxy so that UI traffic flows to the Primary APM server. If you are using VIPs you can run, "./allow apmui; " on the Primary APM server.

Automation of the Synchronization and Failover

You now have an understanding of how data is backed up and restored between the two APM servers. You also understand what needs to change in the environment during a failover. It is now time to automate as much of that process as possible. During the following steps it is recommended that you bounce 4 parts of the APM server but, it is not necessary because the connections will automatically resume as needed over time. (apm stop min; apm stop server1; apm stop scr; apm stop txagent; apm start txagent; apm start scr; apm start server1; apm start min;)

- On the Primary APM server, create a cron job that will periodically backup the server by running the /opt/ibm/ccm/backup.sh script. Base the frequency of the cron job on how long it takes to execute the backup script. This duration will increase as more agents are added to the environment and more customization is added. So, be conservative initially until you have a good sense of how long the backups are going to take. Suggestion is to backup every 2 hours initially.

- Using the mechanism of your choice, automate the process of copying the backup tar files to the Standby APM server. Using something like rsync to synchronize the /opt/ibm/backups directory would work well.

- On the Standby APM server, create a cron job that will periodically restore the content that was copied from the Primary APM server. The cron job will need to execute the /opt/ibm/ccm/restore.sh –e scr –f <filename> command. You'll need to create a script that will ensure that you restore the most recent backup tar file. Suggestion is to restore no more than every 2 hours, but this interval will depend on the need for currency and duration of the restore.sh script your environment.

- If desired, setup automation to detect an outage on the primary server and trigger the failover process.

- If you are using VIPs and an APM failure is triggered, the automation should:

    - Remove the VIP for the Agent traffic. This will stop the agents from sending data.

    - Stop the following 4 processes if they are still running. apm stop min; apm stop server1; apm stop scr; apm stop txagent;

    - Wait a minute for existing connections to the database to complete.

- Block the Primary APM server from accessing DB2 and allow the Standby APM server to access DB2.
- Start the 4 APM processes on the Standby server (apm start_all)
- Assign the VIP for the Agent Traffic to the Standby server.

- If you are using VIPs and a DB2 failure is triggered, the automation should:
  - Execute db2 takeover hadr on db <db_name> for all 3 DBs
  - Move the VIP for DB2 to the Standby server

- If you are not using VIPs and a DB2 failure is triggered, the automation should:
  - Execute db2 takeover hadr on db <db_name> for all 3 DBs
  - On the APM server run "apm stop min; apm stop server1; apm stop scr; apm stop txagent; apm start txagent; apm start scr; apm start server1; apm start min;"
- If you are using proxy servers and an APM failure is triggered, the automation should:
  - Use firewalls to block the failing APM server.
  - Run "db2 force applications all" to drop ALL connections to ALL databases owned by the instance ID on the failing APM server.
  - Use firewalls to unblock the standby APM server. You should immediately see connections from the standby server (netstat –an | grep 50000 or db2 list applications) (where 50000 is the port that you assigned to DB2)
  - Reconfigure the reverse proxy so that UI traffic is directed to the Standby APM server. On an HTTP server, the easiest thing would be to create two different httpd.conf files. During a failover, copy the Standby httpd.conf file into place and recycle the HTTP server. If you are using a VIP move the VIP to the standby server.
  - Reconfigure the forwarding proxy so that UI traffic is directed to the Standby APM server. On an HTTP server, the easiest thing would be to create two different httpd.conf files. During a failover, copy the Standby httpd.conf file into place and recycle the HTTP server. If you are using a VIP for the Agents to connect, move the VIP and recycle the HTTP server.

Optional Configuration

There are some optional configurations the can be done as part of this high availability configuration. Those options are described here:

HTTPS Traffic from the Agents

1a) If you are using a VIP and you decide to configure HTTPS communication between the agents and the APM server and you do not want to use the default certificates created by APM, refer to the instructions in Appendix P: Creating custom certificates.

1b) CONFIGURING AGENTS TO USE HTTPS TO CONNECT TO THE APM SERVER THROUGH A FORWARD PROXY SERVER IS NOT SUPPORTED.

APM Server Synchronization via Backup and Restore

This section of the document provides recommendations on how to keep the two APM servers in sync. This will ensure that minimal data is lost during the failover from the primary to the standby APM server. You will use the product provided backup.sh script to periodically backup the configuration and event content on the primary APM server. The restore.sh script will be used to restore the configuration and event content to the standby APM server.

Backup Schedule

You should define a backup schedule that can be reliably executed in your environment. This is based on how long it takes to run the backup.sh and restore.sh scripts. More than likely, the restore.sh script will require longer than the backup.sh scripts. The duration of the backup is based on the quantity of data stored in the various repositories. Information includes data collected from the agents and configuration data. As more configuration data and agent data is added to the environment, the restore will take longer. So, monitor the duration that the restore.sh takes to execute and adjust your automation as required.

Applying fixes in an APM HA environment.

Overview

We normally recommend that you apply the latest Cloud APM 8.1.4.0 server interim fix that is available from Fix Central. Two things to consider when applying patches are: 1) Will any of the fixes/patches

require APM components to be restarted; and 2) Will any of the fixes/patches require access to DB2 to complete.

When you apply the interim fix first update the standby APM server while the standby server is blocked from accessing DB2. If the any of the patches in the interim fix need to restart APM components, it may take 10-20 minutes to complete depending on the number of APM components that need to be restarted. If any of the patches require access to DB2, the update for that patch will fail but the other patches will complete. If the interim fix contains a patch that requires access to DB2, the primary APM server will require an outage to apply the patch and the standby APM server will require an outage to apply the patch. Normally the second time that you run ./apmpatch.sh it will run quickly because it already installed the patches that required restarting APM components and it only needs to install the patches that require access to DB2.

Steps for Interim Fixes

- The steps to apply an interim fix in an HA environment are as follows:

    1. Apply the interim fix to the standby APM server.

    2. If the interim fix did not require any components to be restarted or access to DB2, apply the interim fix to the primary APM server.

    3. If the interim fix requires some of the APM components to be restarted or access to DB2, then schedule an outage for the primary APM server to be updated. This should be a short outage.

        a. Failover from the primary APM server to the standby APM server and rerun ./apmpatch.sh when the standby APM server has access to the DB2 database. ./apmpatch.sh should complete within a few seconds.

        b. Run ./apmpatch .sh on the primary APM server while the primary is blocked from accessing DB2. It may take 10-15 minutes for the script to restart APM components

        c. Fail back to the primary APM server and rerun ./apmpatch.sh when the primary APM server has access to the DB2 database.

- For example, when applying interim fix IF06 to the standby APM 8.1.4 server. It took 12 minutes to complete. Of the 22 component patches they all completed except 1. The one that failed required access to DATAMART. After doing a failover the rerun of ./apmpatch.sh completed in 5 seconds. In this case the outage was the time it takes to do a failover and failback plus a few seconds.

Appendix A: Setting up High Availability with DB2 HADR Cluster

Setting up a DB2 HADR cluster is the preferred method for achieving database high availability with IBM Performance Management. Assuming that your DBA is familiar with setting up DB2 in a clustered configuration with a virtual IP address (VIP), then the configuration and failover of APM will be very straightforward. When using a VIP, the high availability of the database server is completely transparent to the APM servers. If a VIP is not used, then additional configuration steps are required to configure the APM components so that they utilize a primary and secondary database.

Setup the DB2 HADR Cluster

Here are the steps require to setup APM with a DB2 HADR Cluster configuration.

- First, setup DB2 in a clustered configuration. Follow the DB2 documentation and configure DB2 as needed. DB2 has multiple HADR configurations. Documentation can be found here: for DB2 10.5 https://www.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.ha.doc/doc/c0006354.html or for DB2 11.1 https://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.ha.doc/doc/c0006354.html

  There are multiple ways to achieve the high availability including clustering where the standby node takes over the IP address of the primary node or through a Virtual IP address.

  Configuring APM to use a standard HADR cluster is a bit complex due to the fact that you have manually configure some of the components to use the primary and secondary database nodes. Setting up DB2 HADR with a Virtual IP (VIP) is much simpler. When using a VIP, the APM server treats the database servers the same as it would with a single database node. We highly recommend you use a VIP for your DB2 HADR configuration. You can find information about setting up a VIP at these links:

  http://download.boulder.ibm.com/ibmdl/pub/software/dw/data/dm-0908hadrdb2haicu/HADR_db2haicu.pdf

  http://www.ibm.com/developerworks/data/library/techarticle/dm-1409hadr-db2-tivoli/index.html

  Either way, you need to setup a cluster where your database clients, in this case the APM servers, can connect to a single IP address without knowledge of the backend DB2 servers. From an APM server perspective, both APM servers will be connected to a single hostname/IP

address, and behind the scenes, DB2 will ensure that the single hostname/IP address is connected to the active database server.

The APM servers are connected to the virtual IP address (VIP). At any point in time, the VIP will only be connect to one of the two clustered database servers. The recommendation for data synchronization is to setup the DB2 synchronization mode as "NEARSYNC", but other options are supported. The level of synchronization that you choose depends on the amount of risk you want to take in possibly losing a transaction. The higher the protection, the higher the overhead is on the database transactions. NEARSYNC is a good compromise that offers good performance with minimal risk of losing transactions.

In the "Deployment Diagram", you will notice that I have chosen the following hostnames. These will be used in the example commands used throughout this document:

- DNS Alias for the APM server: ipm.ibm.com
- Hostname of the primary APM server: apm1.ibm.com
- Hostname of the standby APM server: apm2.ibm.com
- Hostname or the VIP for the database cluster: apmdb.ibm.com
- Hostname of the primary DB2 node: apmdb_1.ibm.com
- Hostname of the standby DB2 node: apmdb_2.ibm.com

- Ensure that the DB2 Cluster is setup with a VIP (Virtual IP address). This will ensure that the APM server does not need any knowledge of the backend database topology and state. The APM servers will be configured using the VIP.
- Ensure that both DB2 nodes and all three databases are configured for online backups. Instructions for configuring online backups is documented here: http://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/admin_backup_online_dbs.htm

Example DB2 Commands for Setting up the APM Database in DB2 HADR

Here are some example commands for setting up the DB2 database in a DB2 HADR clustered environment:

- On both DB2 nodes, setup the following services in /etc/services. You may choose different port numbers, but the examples below will use these port numbers. These are ports that are used for the primary and standby database to communicate with each other. The service names do not have to be these specific names, but it will be more intuitive if the identify the database name and whether it is for the primary or standby node.
    - hadr_warehous_standby 51012/tcp
    - hadr_warehous_primary 51013/tcp
    - hadr_datamart_standby 51014/tcp
    - hadr_datamart_primary 51015/tcp
    - hadr_scr32_standby 51016/tcp
    - hadr_scr32_primary 51017/tcp
- On both database servers, make sure that the SVCENAME is set to match the database entry in /etc/services for the database instance. Using default configurations, the entry in /etc/services will be "db2c_db2apm 50000/tcp". Use the following command to update each of the database servers.
    - As the database instance owner (db2apm), issue this command:
        - db2 update dbm cfg using SVCENAME db2c_db2apm

Steps on Primary Node

- If you already have APM databases that you are using, you should take a backup of all 3 databases before you attempt to convert your existing databases to HADR databases.
- Create the 3 DB2 databases per the product documentation on the primary DB2 node. The instructions can be found here: http://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/install_server_mydb2.htm

Note: The instructions may be missing a step to set **DB2_ATS_ENABLE=YES** on the remote DB2 server. If "db2set" does not have it set, then from the DB2 instance ID run

db2set DB2_ATS_ENABLE=YES

- Configure the 3 database for log archiving using the following command:

- db2 update db cfg for <DBNAME> using LOGARCHMETH1 LOGRETAIN
- **Warning: LOGRETAIN puts the db into backup pending state and you cannot access the database until after HADR setup completes**
- Examples:

  db2 update db cfg for whous1 using LOGARCHMETH1 LOGRETAIN

  db2 update db cfg for dmart1 using LOGARCHMETH1 LOGRETAIN

  db2 update db cfg for scr1 using LOGARCHMETH1 LOGRETAIN

- For each of the 3 database (WAREHOUS, DATAMART, SCR32), setup the following optional parameters or use the defaults:

db2 UPDATE DB CFG FOR <database> USING AUTO_DEL_REC_OBJ ON

db2 UPDATE DB CFG FOR warehous USING AUTO_DEL_REC_OBJ ON

db2 UPDATE DB CFG FOR datamart USING AUTO_DEL_REC_OBJ ON

db2 UPDATE DB CFG FOR scr32 USING AUTO_DEL_REC_OBJ ON

db2 UPDATE DB CFG FOR <database> USING REC_HIS_RETENTN 1

db2 UPDATE DB CFG FOR warehous USING REC_HIS_RETENTN 1

db2 UPDATE DB CFG FOR datamart USING REC_HIS_RETENTN 1

db2 UPDATE DB CFG FOR scr32 USING REC_HIS_RETENTN 1

db2 UPDATE DB CFG FOR <database> USING NUM_DB_BACKUPS 1

db2 UPDATE DB CFG FOR warehous USING NUM_DB_BACKUPS 1

db2 UPDATE DB CFG FOR datamart USING NUM_DB_BACKUPS 1

db2 UPDATE DB CFG FOR scr32 USING NUM_DB_BACKUPS 1

db2 UPDATE DB CFG FOR <database> USING LOGARCHCOMPR1 OFF

db2 UPDATE DB CFG FOR warehous USING LOGARCHCOMPR1 OFF

db2 UPDATE DB CFG FOR datamart USING LOGARCHCOMPR1 OFF

db2 UPDATE DB CFG FOR scr32 USING LOGARCHCOMPR1 OFF

db2 UPDATE DB CFG FOR <database> USING INDEXREC RESTART

db2 UPDATE DB CFG FOR warehous USING INDEXREC RESTART

db2 UPDATE DB CFG FOR datamart USING INDEXREC RESTART

db2 UPDATE DB CFG FOR scr32 USING INDEXREC RESTART

db2 UPDATE DB CFG FOR <database> USING TRACKMOD ON

db2 UPDATE DB CFG FOR warehous USING TRACKMOD ON

db2 UPDATE DB CFG FOR datamart USING TRACKMOD ON

db2 UPDATE DB CFG FOR scr32 USING TRACKMOD ON

db2 UPDATE DB CFG FOR <database> USING DFT_DEGREE ANY

db2 UPDATE DB CFG FOR warehous USING DFT_DEGREE ANY

db2 UPDATE DB CFG FOR warehous USING DFT_DEGREE ANY

db2 UPDATE DB CFG FOR warehous USING DFT_DEGREE ANY

db2 UPDATE DB CFG FOR <database> USING LOGBUFSZ 1024

db2 UPDATE DB CFG FOR warehous USING LOGBUFSZ 1024

db2 UPDATE DB CFG FOR datamart USING LOGBUFSZ 1024

db2 UPDATE DB CFG FOR scr32 USING LOGBUFSZ 1024

db2 UPDATE DB CFG FOR <database> USING NUM_IOCLEANERS 14

db2 UPDATE DB CFG FOR warehous USING NUM_IOCLEANERS 14

db2 UPDATE DB CFG FOR datamart USING NUM_IOCLEANERS 14

db2 UPDATE DB CFG FOR scr32 USING NUM_IOCLEANERS 14

db2 UPDATE DB CFG FOR <database> USING NUM_IOSERVERS 24

db2 UPDATE DB CFG FOR warehous USING NUM_IOSERVERS 24

db2 UPDATE DB CFG FOR datamart USING NUM_IOSERVERS 24

db2 UPDATE DB CFG FOR scr32 USING NUM_IOSERVERS 24

- On the 3 databases, update the HADR_LOCAL_HOST to be the IP address of the primary DB2 server using the command: db2 update db cfg for <database> using HADR_LOCAL_HOST <IP of primary db2>
    - Examples:

      db2 update db cfg for warehous using HADR_LOCAL_HOST 10.1.1.5

db2 update db cfg for datamart using HADR_LOCAL_HOST 10.1.1.5

db2 update db cfg for scr32 using HADR_LOCAL_HOST 10.1.1.5

- On the 3 databases, update the service port based on the settings in /etc/services. Use the command: db2 update db cfg for <database> using HADR_LOCAL_SVC <unique port>
  - Examples:

    db2 update db cfg for warehous using HADR_LOCAL_SVC 51013

    db2 update db cfg for datamart using HADR_LOCAL_SVC 51015

    db2 update db cfg for scr32 using HADR_LOCAL_SVC 51017

- On the 3 databases, update the HADR_REMOTE_HOST parameter using the command: db2 update db cfg for <database> using HADR_REMOTE_HOST <IP of standby db2>
  - Examples:

    db2 update db cfg for warehous using HADR_REMOTE_HOST 10.1.1.6

    db2 update db cfg for datamart using HADR_REMOTE_HOST 10.1.1.6

    db2 update db cfg for scr32 using HADR_REMOTE_HOST 10.1.1.6

- On the 3 databases, update the remote service port using the HADR_REMOTE_SVC parameter and the command: db2 update db cfg for <database> using HADR_REMOTE_SVC <unique port>
  - Examples:

    db2 update db cfg for warehous using HADR_REMOTE_SVC 51012

    db2 update db cfg for datamart using HADR_REMOTE_SVC 51014

    db2 update db cfg for scr32 using HADR_REMOTE_SVC 51016

- On the 3 databases, update the HADR_TARGET_LIST. This parameter is a combination of the <hostname>:<port or service name> of the remote DB2 database.
  - Examples:

    db2 update db cfg for warehous using HADR_TARGET_LIST apmdb_2:51012

    db2 update db cfg for datamart using HADR_TARGET_LIST apmdb_2:51014

    db2 update db cfg for scr32 using HADR_TARGET_LIST apmdb_2:51016

- Update the remote instance for the 3 databases using the command: db2 update db cfg for <database> using HADR_REMOTE_INST <database instance>
    - Where db2apm is the instance name on the standby server
    - Examples:

      db2 update db cfg for warehous using HADR_REMOTE_INST db2apm

      db2 update db cfg for datamart using HADR_REMOTE_INST db2apm

      db2 update db cfg for scr32 using HADR_REMOTE_INST db2apm
- Issue the following command for each of the databases:
    - db2 update alternate server for database <DB Name> using hostname <alternate hostname> port <DB alternate port>
    - Examples:

      db2 update alternate server for database warehous using hostname apmdb_2 port 51012

      db2 update alternate server for database datamart using hostname apmdb_2 port 51014

      db2 update alternate server for database scr32 using hostname apmdb_2 port 51016
- Update the LOGINDEXBUILD parameter for the 3 databases and set it to “ON” using the following command: db2 update db cfg for <database> using LOGINDEXBUILD ON
    - Examples:

      db2 update db cfg for warehous using LOGINDEXBUILD ON

      db2 update db cfg for datamart using LOGINDEXBUILD ON

      db2 update db cfg for scr32 using LOGINDEXBUILD ON
- Update the HADR_TIMEOUT for the 3 database and set it to 120:

  db2 update db cfg for warehous using HADR_TIMEOUT 120

  db2 update db cfg for datamart using HADR_TIMEOUT 120

  db2 update db cfg for scr32 using HADR_TIMEOUT 120
- Update the HADR_SYNCMODE for the 3 database and set it to NEARSYNC:

  db2 update db cfg for warehous using HADR_SYNCMODE NEARSYNC

db2 update db cfg for datamart using HADR_ SYNCMODE NEARSYNC

db2 update db cfg for scr32 using HADR_ SYNCMODE NEARSYNC

- Update the HADR_PEER_WINDOW for the 3 database and set it to 120:

  db2 update db cfg for warehous using HADR_PEER_WINDOW 300

  db2 update db cfg for datamart using HADR_PEER_WINDOW 300

  db2 update db cfg for scr32 using HADR_PEER_WINDOW 300

- Take the 3 databases offline so that offline backups can be taken.

  db2 deactivate database warehous

  db2 deactivate database datamart

  db2 deactivate database scr32

- Take an offline backup of the 3 databases:

  db2 backup database warehous

  db2 backup database datamart

  db2 backup database scr32

- Activate the 3 databases:

  db2 activate database warehous

  db2 activate database datamart

  db2 activate database scr32

Steps On the Standby DB2 Node

- Run these steps and commands on the **standby** DB2 node as the db2 instance owner (db2apm)
  - Copy the offline database backup files from the primary DB2 server to the standby. By default, the backup files will be located in /home/db2apm. Place the files in /home/db2apm on the standby DB2 server.
  - Restore the 3 databases using the following command:

    db2 restore database warehous

    db2 restore database datamart

db2 restore database scr32

- For each of the 3 database (WAREHOUS, DATAMART, SCR32), setup the following parameters:

db2 UPDATE DB CFG FOR <database> USING AUTO_DEL_REC_OBJ ON

db2 UPDATE DB CFG FOR warehous USING AUTO_DEL_REC_OBJ ON

db2 UPDATE DB CFG FOR datamart USING AUTO_DEL_REC_OBJ ON

db2 UPDATE DB CFG FOR scr32 USING AUTO_DEL_REC_OBJ ON

db2 UPDATE DB CFG FOR <database> USING REC_HIS_RETENTN 1

db2 UPDATE DB CFG FOR warehous USING REC_HIS_RETENTN 1

db2 UPDATE DB CFG FOR datamart USING REC_HIS_RETENTN 1

db2 UPDATE DB CFG FOR scr32 USING REC_HIS_RETENTN 1

db2 UPDATE DB CFG FOR <database> USING NUM_DB_BACKUPS 1

db2 UPDATE DB CFG FOR warehous USING NUM_DB_BACKUPS 1

db2 UPDATE DB CFG FOR datamart USING NUM_DB_BACKUPS 1

db2 UPDATE DB CFG FOR scr32 USING NUM_DB_BACKUPS 1

db2 UPDATE DB CFG FOR <database> USING LOGARCHCOMPR1 OFF

db2 UPDATE DB CFG FOR warehous USING LOGARCHCOMPR1 OFF

db2 UPDATE DB CFG FOR datamart USING LOGARCHCOMPR1 OFF

db2 UPDATE DB CFG FOR scr32 USING LOGARCHCOMPR1 OFF

db2 UPDATE DB CFG FOR <database> USING INDEXREC RESTART

db2 UPDATE DB CFG FOR warehous USING INDEXREC RESTART

db2 UPDATE DB CFG FOR datamart USING INDEXREC RESTART

db2 UPDATE DB CFG FOR scr32 USING INDEXREC RESTART

db2 UPDATE DB CFG FOR <database> USING TRACKMOD ON

db2 UPDATE DB CFG FOR warehous USING TRACKMOD ON

db2 UPDATE DB CFG FOR datamart USING TRACKMOD ON

db2 UPDATE DB CFG FOR scr32 USING TRACKMOD ON

db2 UPDATE DB CFG FOR <database> USING DFT_DEGREE ANY

db2 UPDATE DB CFG FOR warehous USING DFT_DEGREE ANY

db2 UPDATE DB CFG FOR warehous USING DFT_DEGREE ANY

db2 UPDATE DB CFG FOR warehous USING DFT_DEGREE ANY

db2 UPDATE DB CFG FOR <database> USING LOGBUFSZ 1024

db2 UPDATE DB CFG FOR warehous USING LOGBUFSZ 1024

db2 UPDATE DB CFG FOR datamart USING LOGBUFSZ 1024

db2 UPDATE DB CFG FOR scr32 USING LOGBUFSZ 1024

db2 UPDATE DB CFG FOR <database> USING NUM_IOCLEANERS 14

db2 UPDATE DB CFG FOR warehous USING NUM_IOCLEANERS 14

db2 UPDATE DB CFG FOR datamart USING NUM_IOCLEANERS 14

db2 UPDATE DB CFG FOR scr32 USING NUM_IOCLEANERS 14

db2 UPDATE DB CFG FOR <database> USING NUM_IOSERVERS 24

db2 UPDATE DB CFG FOR warehous USING NUM_IOSERVERS 24

db2 UPDATE DB CFG FOR datamart USING NUM_IOSERVERS 24

db2 UPDATE DB CFG FOR scr32 USING NUM_IOSERVERS 24

- On the 3 databases, update the HADR_LOCAL_HOST to be the IP address of the standby DB2 server using the command: db2 update db cfg for <database> using HADR_LOCAL_HOST <IP of standby db2>
  - Examples:

    db2 update db cfg for warehous using HADR_LOCAL_HOST 10.1.1.6

    db2 update db cfg for datamart using HADR_LOCAL_HOST 10.1.1.6

    db2 update db cfg for scr32 using HADR_LOCAL_HOST 10.1.1.6

- On the 3 databases, update the service port based on the settings in /etc/services. Use the command: db2 update db cfg for <database> using HADR_LOCAL_SVC <unique port>
  - Examples:

db2 update db cfg for warehous using HADR_LOCAL_SVC 51012

db2 update db cfg for datamart using HADR_LOCAL_SVC 51014

db2 update db cfg for scr32 using HADR_LOCAL_SVC 51016

- On the 3 databases, update the HADR_REMOTE_HOST parameter using the command: db2 update db cfg for <database> using HADR_REMOTE_HOST <IP of standby db2>
  - Examples:

    db2 update db cfg for warehous using HADR_REMOTE_HOST 10.1.1.5

    db2 update db cfg for datamart using HADR_REMOTE_HOST 10.1.1.5

    db2 update db cfg for scr32 using HADR_REMOTE_HOST 10.1.1.5

- On the 3 databases, update the remote service port using the HADR_REMOTE_SVC parameter and the command: db2 update db cfg for <database> using HADR_REMOTE_SVC <unique port>
  - Examples:

    db2 update db cfg for warehous using HADR_REMOTE_SVC 51013

    db2 update db cfg for datamart using HADR_REMOTE_SVC 51015

    db2 update db cfg for scr32 using HADR_REMOTE_SVC 51017

- On the 3 databases, update the HADR_TARGET_LIST. This parameter is a combination of the <hostname>:<port or service name> of the remote DB2 database.
  - Examples:

    db2 update db cfg for warehous using HADR_TARGET_LIST apmdb_1:51013

    db2 update db cfg for datamart using HADR_TARGET_LIST apmdb_1:51015

    db2 update db cfg for scr32 using HADR_TARGET_LIST apmdb_1:51017

- Update the remote instance for the 3 databases using the command: db2 update db cfg for <database> using HADR_REMOTE_INST <database instance>
  - Where db2apm is the instance name on the standby server
  - Examples:

    db2 update db cfg for warehous using HADR_REMOTE_INST db2apm

db2 update db cfg for datamart using HADR_REMOTE_INST db2apm

db2 update db cfg for scr32 using HADR_REMOTE_INST db2apm

- Issue the following command for each of the databases:
  - db2 update alternate server for database <DB Name> using hostname <alternate hostname> port <DB alternate port>
    - Examples:

      db2 update alternate server for database warehous using hostname apmdb_1 port 51013

      db2 update alternate server for database datamart using hostname apmdb_1 port 51015

      db2 update alternate server for database scr32 using hostname apmdb_1 port 51017

- Update the HADR_TIMEOUT for the 3 database and set it to 120:

  db2 update db cfg for warehous using HADR_TIMEOUT 120

  db2 update db cfg for datamart using HADR_TIMEOUT 120

  db2 update db cfg for scr32 using HADR_TIMEOUT 120

- Update the HADR_SYNCMODE for the 3 database and set it to NEARSYNC:

  db2 update db cfg for warehous using HADR_SYNCMODE NEARSYNC

  db2 update db cfg for datamart using HADR_ SYNCMODE NEARSYNC

  db2 update db cfg for scr32 using HADR_ SYNCMODE NEARSYNC

- Update the HADR_PEER_WINDOW for the 3 database and set it to 120:

  db2 update db cfg for warehous using HADR_PEER_WINDOW 120

  db2 update db cfg for datamart using HADR_PEER_WINDOW 120

  db2 update db cfg for scr32 using HADR_PEER_WINDOW 120

- Update the LOGINDEXBUILD parameter for the 3 databases and set it to “ON” using the following command: db2 update db cfg for <database> using LOGINDEXBUILD ON
  - Examples:

db2 update db cfg for warehous using LOGINDEXBUILD ON

db2 update db cfg for datamart using LOGINDEXBUILD ON

db2 update db cfg for scr32 using LOGINDEXBUILD ON

- Start HADR for the 3 databases on the standby DB2 server
  - Examples:

    db2 start hadr on database warehous as standby

    db2 start hadr on database datamart as standby

    db2 start hadr on database scr32 as standby

Steps on Primary Node (part 2)

- On the primary DB2 node, start the 3 databases as DB2 HADR primary databases by issue these commands:

  db2 start hadr on database warehous as primary

  db2 start hadr on database datamart as primary

  db2 start hadr on database scr32 as primary

- Verify that the DB2 clustering is configured properly. You should only be able to write to the primary database server. In addition, if you are using a VIP, verify that you can access the databases via the VIP in both primary and standby configurations. You can also issue this command from the primary node:
  - db2pd -db <DBNAME> -hadr
    - Examples:

      db2pd –db warehous –hadr

      db2pd –db datamart –hadr

      db2pd –db scr32 –hadr

- Setup the three databases for online backups

- You can now test that failover is working:

- First verify that the primary database is accessible and the standby database is not accessible. This can be accomplished by attempting to issue the following command from both nodes:

  db2 connect to warehous

- On the primary node, you will be able to access the warehouse database and you will be able to run queries.
- On the standby node, you will receive the following message: SQL1776N The command cannot be issued on an HADR database. Reason code = "1".
- Now, force a failover of the DB2 HADR cluster.

  db2 takeover hadr on database warehous

  db2 takeover hadr on database datamart

  db2 takeover hadr on database scr32

- After the failover, two of the APM services must be restarted. Restart server1 and scr using the following steps:
  - apm stop server1
  - apm stop scr
  - apm start scr
  - apm start server1
- After forcing the failover, test that the databases are accessible on the standby node
- Now, reset the environment back to the default:
  - Start the primary DB2 server using db2start
  - On the primary DB2 server issue this command: db2 start hadr on database <dbname> as standby

    db2 start hadr on database warehous as standby

    db2 start hadr on database datamart as standby

    db2 start hadr on database scr32 as standby

  - On the primary DB2 server issue this command to take over control of the databases: db2 takeover hadr on database <dbname>

db2 takeover hadr on database warehous

db2 takeover hadr on database datamart

db2 takeover hadr on database scr32

- Test to make sure that the databases are accessible from the Primary DB2 node.

- If you are NOT using a VIP, you must not configure your APM server components to correctly use the clustered database. They must be configured so that they will failover from the primary to the standby DB2 database(s). Follow the instructions found in Appendix E: Accessing DB2 HADR without a VIP (ACR)

Example Commands

The following is an example of the commands that were used to setup DB2 HADR in a test environment. Your actual commands will differ.

steps that I used to setup hadr on db2a/db2b on 09/20/18

db2 update db cfg for whous1 using LOGARCHMETH1 LOGRETAIN # This puts the db into backup pending state and you cannot access until after HADR completes

db2 update db cfg for dmart1 using LOGARCHMETH1 LOGRETAIN #

db2 update db cfg for scr1 using LOGARCHMETH1 LOGRETAIN

On the primary

db2 update db cfg for whous1 using HADR_LOCAL_HOST 9.42.12.210

db2 update db cfg for whous1 using HADR_LOCAL_SVC 51013

db2 update db cfg for whous1 using HADR_REMOTE_HOST 9.42.12.234

db2 update db cfg for whous1 using HADR_REMOTE_SVC 51012

db2 update db cfg for whous1 using HADR_REMOTE_INST db2apm1

db2 update db cfg for dmart1 using HADR_LOCAL_HOST 9.42.12.210

db2 update db cfg for dmart1 using HADR_LOCAL_SVC 51015

db2 update db cfg for dmart1 using HADR_REMOTE_HOST 9.42.12.234

db2 update db cfg for dmart1 using HADR_REMOTE_SVC 51014

db2 update db cfg for dmart1 using HADR_REMOTE_INST db2apm1

db2 update db cfg for scr1 using HADR_LOCAL_HOST 9.42.12.210

db2 update db cfg for scr1 using HADR_LOCAL_SVC 51017

db2 update db cfg for scr1 using HADR_REMOTE_HOST 9.42.12.234

db2 update db cfg for scr1 using HADR_REMOTE_SVC 51016

db2 update db cfg for scr1 using HADR_REMOTE_INST db2apm1

db2 update db cfg for whous1 using HADR_TARGET_LIST sapm-db2b:51012

db2 update db cfg for dmart1 using HADR_TARGET_LIST sapm-db2b:51014

db2 update db cfg for scr1 using HADR_TARGET_LIST sapm-db2b:51016

db2 update alternate server for database whous1 using hostname sapm-db2b port 50000

db2 update alternate server for database dmart1 using hostname sapm-db2b port 50000

db2 update alternate server for database scr1 using hostname sapm-db2b port 50000

Do an online or offline db2 backup for all 3 databases

db2 backup db whous1 to /db2/backups/

db2 backup db scr1 to /db2/backups/

db2 backup db dmart1 to /db2/backups/

```
# On the standby

#Do a db2 restore for all 3 databases

su - db2inst1

cd /db2/backups

db2 restore db whous1

db2 restore db scr1

db2 restore db dmart1


db2 update db cfg for whous1 using HADR_LOCAL_HOST 9.42.12.234

db2 update db cfg for whous1 using HADR_LOCAL_SVC 51012

db2 update db cfg for whous1 using HADR_REMOTE_HOST 9.42.12.210

db2 update db cfg for whous1 using HADR_REMOTE_SVC 51013

db2 update db cfg for whous1 using HADR_REMOTE_INST db2apm1


db2 update db cfg for dmart1 using HADR_LOCAL_HOST 9.42.12.234

db2 update db cfg for dmart1 using HADR_LOCAL_SVC 51014

db2 update db cfg for dmart1 using HADR_REMOTE_HOST 9.42.12.210

db2 update db cfg for dmart1 using HADR_REMOTE_SVC 51015

db2 update db cfg for dmart1 using HADR_REMOTE_INST db2apm1


db2 update db cfg for scr1   using HADR_LOCAL_HOST 9.42.12.234

db2 update db cfg for scr1   using HADR_LOCAL_SVC 51016

db2 update db cfg for scr1   using HADR_REMOTE_HOST 9.42.12.210

db2 update db cfg for scr1   using HADR_REMOTE_SVC 51017
```

db2 update db cfg for scr1 using HADR_REMOTE_INST db2apm1

db2 update db cfg for whous1 using HADR_TARGET_LIST sapm-db2a:51013

db2 update db cfg for dmart1 using HADR_TARGET_LIST sapm-db2a:51015

db2 update db cfg for scr1 using HADR_TARGET_LIST sapm-db2a:51017

db2 update alternate server for database whous1 using hostname sapm-db2a port 50000

db2 update alternate server for database dmart1 using hostname sapm-db2a port 50000

db2 update alternate server for database scr1 using hostname sapm-db2a port 50000

Also need to setup logging This example uses a disk archive. Run these commands on both servers

db2 update db cfg for whous1 using LOGINDEXBUILD ON

db2 update db cfg for dmart1 using LOGINDEXBUILD ON

db2 update db cfg for scr1 using LOGINDEXBUILD ON

mkdir /home/db2apm1/log_arch

mkdir /home/db2apm1/log_arch/whous1

mkdir /home/db2apm1/log_arch/dmart1

mkdir /home/db2apm1/log_arch/scr1

db2 update db cfg for whous1 using logarchmeth1 DISK:/home/db2apm1/log_arch/whous1

db2 update db cfg for dmart1 using logarchmeth1 DISK:/home/db2apm1/log_arch/dmart1

db2 update db cfg for scr1 using logarchmeth1 DISK:/home/db2apm1/log_arch/scr1

To get it into peer mode.

On the standby server run

db2 start hadr on db whous1 as standby

db2 start hadr on db scr1 as standby

db2 start hadr on db dmart1 as standby

Then on the primary run

db2 start hadr on db whous1 as primary

db2 start hadr on db scr1 as primary

db2 start hadr on db dmart1 as primary

When SCR32 is the primary on db2b then you can add SCR UDF routines to the database. They are not included in the restore process.

db2 takeover hadr on db scr1

#Then follow the instructions to setup scr udf routines. (This only needs to be done when SCR is initially created.)

Appendix B: Installation Prompts for Standby APM Server

This section contains example prompts from the installation of the APM server. In the example below, the items in **BLUE** are the values specified for this demo scenario. I have entered a value for all prompts, but when you perform an install you only have to enter values if you do not want to use the default value.

./install.sh

Do you want to upgrade from an existing installation of the Performance Management server [1-yes or 2-no; "no" is default]? 2

This script will install IBM Application Performance Management Advanced (8.1.4.0).

Do you want to continue [1-yes or 2-no; "yes" is default]? 1

Do you want to change the default installation directory (/opt/ibm) [1-yes or 2-no; "no" is default]? no

Do you accept the license agreement(s) found in the /media/8.1.4/licenses/ipm_apm_advanced directory [1-accept or 2-decline]? 1

License agreement was accepted, installation will proceed...

Do you want to change the default password for the administrator account [1-yes or 2-no; "no" is default]? no

Agent installation images must be configured to connect to this server. If you have downloaded the agent images to the same system as the server, you can configure the agent images now.

Do you want to configure the compressed (*.zip or *.tar) agent installation files now [1-yes or 2-no; "yes" is default]? 1

Enter the path to the directory where you downloaded the compressed agent (and/or Hybrid Gateway) installation images (e.g. /opt/agents).

Enter the path: /media

Enter the path to the directory where configured agent installation images can be stored.

Enter the path or accept the default [/opt/ibm/ccm/depot]: /opt/ibm/ccm/depot

Enter the IP address/hostname that will be used by agents to communicate with the server.

Enter the IP address/hostname or accept the default [10.1.1.3]: proxy2.ibm.com

Enter the hostname and IP address of the server that will be used in a web browser to log in to the Performance Management console. Accept the default values or provide your own.

Default values:

Fully qualified domain name: apm2.ibm.com

Short hostname: apm2

IP: 10.1.1.3

Do you want to use these values [1-yes or 2-no; "yes" is default]? 2

Enter the fully qualified domain name or accept the default [apm2.ibm.com]: proxy1.ibm.com

Enter the short hostname or accept the default [apm2]: proxy1

Enter the IP address or accept the default [10.1.1.3]: 10.1.1.1

Do you want to install the database or connect to an existing DB2? [1-install database or 2-connect to existing database; "1-install database" is default]? 2

Enter configuration parameters to establish connection to the existing DB2 database.

Enter the hostname/IP address to the DB2 host or accept the default [localhost]: apmdb.ibm.com

Enter the port number of the DB2 instance or accept the default [50000]: 50000

Enter the password for the user "itmuser": Passw0rd2!

Enter the password for the instance user "db2apm": Passw0rd1!

Running Prerequisite Scanner. This may take a few minutes depending on the number of checked components and machine's performance.

Setting Prerequisite Scanner output directory to user defined directory: /opt/ibm/ccm/logs/apm-prs_20170128_121440

Reading Prerequisite Scanner configuration files from user defined directory: /opt/ibm/ccm/logs/apm-prs_20170128_121440/config

IBM Prerequisite Scanner

Version: 1.2.0.17

Build : 20150827

OS name: Linux

User name: root

Machine Information

Machine name: apm2

Serial number: VMware-42 25 1b e7 e7 59 ec b9-27 8c 24 d2 68 13 fd 9e

Scenario: Prerequisite Scan

APM - IBM Application Performance Management [version 08010300]:

Overall result: PASS

Detailed results are also available in /opt/ibm/ccm/logs/apm-prs_20170128_121440/result.txt

No further user input is required. The installation and configuration of components is now starting and may take up to one hour to complete. The installation log is available at "/opt/ibm/ccm/logs/apm-server-install_20170128_121440.log".

Installing the Performance Management server. Please wait...

/opt/ibm/ccm/server_size.sh small

Appendix C: Installation Prompts for the Primary APM Server:

This section contains example prompts from the installation of the APM server. In the example below, the items in **BLUE** are the values specified for this demo scenario. I have entered a value for all prompts, but when you perform an install you only have to enter values if you do not want to use the default value.

./install.sh

Do you want to upgrade from an existing installation of the Performance Management server [1-yes or 2-no; "no" is default]? 2

This script will install IBM Application Performance Management Advanced (8.1.4.0).

Do you want to continue [1-yes or 2-no; "yes" is default]? 1

Do you want to change the default installation directory (/opt/ibm) [1-yes or 2-no; "no" is default]? no

Do you accept the license agreement(s) found in the /media/8.1.4/licenses/apm_apm_advanced directory [1-accept or 2-decline]? 1

License agreement was accepted, installation will proceed...

Do you want to change the default password for the administrator account [1-yes or 2-no; "no" is default]? no

Agent installation images must be configured to connect to this server. If you have downloaded the agent images to the same system as the server, you can configure the agent images now.

Do you want to configure the compressed (*.zip or *.tar) agent installation files now [1-yes or 2-no; "yes" is default]? 1

Enter the path to the directory where you downloaded the compressed agent (and/or Hybrid Gateway) installation images (e.g. /opt/agents).

Enter the path: /media

Enter the path to the directory where configured agent installation images can be stored.

Enter the path or accept the default [/opt/ibm/ccm/depot]: /opt/ibm/ccm/depot

Enter the IP address/hostname that will be used by agents to communicate with the server.

Enter the IP address/hostname or accept the default [10.1.1.3]: proxy2.ibm.com

Enter the hostname and IP address of the server that will be used in a web browser to log in to the Performance Management console. Accept the default values or provide your own.

Default values:

Fully qualified domain name: apm1.ibm.com

Short hostname: apm1

IP: 10.1.1.2

Do you want to use these values [1-yes or 2-no; "yes" is default]? 2

Enter the fully qualified domain name or accept the default [apm1.ibm.com]: proxy1.ibm.com

Enter the short hostname or accept the default [apm1]: proxy1

Enter the IP address or accept the default [10.1.1.2]: 10.1.1.1

Do you want to install the database or connect to an existing DB2? [1-install database or 2-connect to existing database; "1-install database" is default]? 2

Enter configuration parameters to establish connection to the existing DB2 database.

Enter the hostname/IP address to the DB2 host or accept the default [localhost]: apmdb.ibm.com

Enter the port number of the DB2 instance or accept the default [50000]: 50000

Enter the password for the user "itmuser": Passw0rd2!

Enter the password for the instance user "db2apm": Passw0rd1!

Running Prerequisite Scanner. This may take a few minutes depending on the number of checked components and machine's performance.

Setting Prerequisite Scanner output directory to user defined directory: /opt/ibm/ccm/logs/apm-prs_20170128_121440

Reading Prerequisite Scanner configuration files from user defined directory: /opt/ibm/ccm/logs/apm-prs_20170128_121440/config

IBM Prerequisite Scanner

Version: 1.2.0.17

Build : 20150827

OS name: Linux

User name: root

Machine Information

Machine name: apm1

Serial number: VMware-42 25 1b e7 e7 59 ec b9-27 8c 24 d2 68 13 fd 9e

Scenario: Prerequisite Scan

- IBM Performance Management [version 08010300]:

Overall result: PASS

Detailed results are also available in /opt/ibm/ccm/logs/apm-prs_20170128_121440/result.txt

No further user input is required. The installation and configuration of components is now starting and may take up to one hour to complete. The installation log is available at "/opt/ibm/ccm/logs/apm-server-install_20170128_121440.log".

Installing the Performance Management server. Please wait...

/opt/ibm/ccm/server_size.sh small

Appendix D: Dropping Databases in a DB2 HADR Environment

The following steps can be used to drop the databases in a DB2 HADR clustered environment. These steps should be performed on the primary and standby database nodes using the database instance owner (db2apm).

Use the following sequence to drop the databases. All commands should be issued as the db2apm user account.

- First, deactivate the databases on the standby node
    - Type: db2 deactivate database WAREHOUS

- Type: db2 deactivate database DATAMART
- Type: db2 deactivate database SCR32

- Stop HADR on the standby node
  - Type: db2 stop hadr on db WAREHOUS
  - Type: db2 stop hadr on db DATAMART
  - Type: db2 stop hadr on db SCR32
- Stop HADR on the primary node
  - Type: db2 stop hadr on db WAREHOUS
  - Type: db2 stop hadr on db DATAMART
  - Type: db2 stop hadr on db SCR32
- Drop the databases on the standby node
  - Type: db2 drop database warehous
  - Type: db2 drop database datamart
  - Type: db2 drop database scr32
- Drop the databases on the primary node
  - Note: It may be necessary to force the databases to be disconnected before dropping the databases. Issue these commands:
    - Type: db2 force applications all
    - Type: db2stop
    - Type: db2start
  - Type: db2 drop database warehous
  - Type: db2 drop database datamart
  - Type: db2 drop database scr32

Appendix E: Accessing DB2 HADR without a VIP (ACR)

Setting up an APM server, when using DB2 HADR without a VIP, is a bit complex. You must do some manual configuration of some components so that they communicate with the primary and secondary DB2 database node. If possible, setup a VIP. If it is not possible to setup a VIP, use the Alternate Client Reroute (ACR) function to define both DB2 servers to APM. The steps in this section ensure that the APM server components failover to the active DB2 node by adding the alternate db2 server (standby server) information to the APM server's configuration files.

Reconfigure the APM servers so that they use a Primary and Secondary database server using the following instructions. These instructions must be performed on both the Primary and Secondary APM servers.

- When executing these configuration steps on the Primary APM server, ensure that the DB2 firewall allows communications from the Primary APM server.
- When executing these configuration steps on the Standby APM server, ensure that the DB2 firewall allows communications from the Standby APM server.

In the instructions, items in **GREEN** are variables that you will need to replace. Items in **BLUE** are the actual commands you will type, but the examples given use the server names in the documentation environment. Replace those server names with the names in your environment.

It will be necessary to modify the configuration files for kafka, the XML toolkit, SCR, and the Summarization & Pruning component.

First, stop the APM services using apm stop_all

Reconfigure kafka to use the database cluster:

- Start kafka: apm start kafka
- Type: <apm-server-home>/kafka/bin/zkCli.sh –server localhost
    - Example: /opt/ibm/kafka/bin/zkCli.sh –server localhost
- View and record the current kafka settings for the DATAMART and WAREHOUS database:
    - To view your existing kafka setting, you can type:

      get /systemconfig/com.ibm.tivoli.ccm.datamart/dburl

      get /systemconfig/com.ibm.tivoli.ccm.saas.prefetch/DB_URL
        - You will get back results similar to the ones shown below:
            - {"duplicated":false,"uivisibility":false,"encrypted":false,"readonly":false,"datatype":"STRING","service":"com.ibm.tivoli.ccm.datamart","name":"dburl","

value":"jdbc:db2:\/\/apmdb_1:50000\/DATAMART","cfgrequired":false,"uiorder":1000}

- {"duplicated":false,"uivisibility":false,"encrypted":false,"readonly":false,"datatype":"STRING","service":"com.ibm.tivoli.ccm.saas.prefetch","name":"DB_URL","value":"jdbc:db2:\/\/apmdb_1:50000\/WAREHOUS","cfgrequired":true,"uiorder":0}

- Enter this command on a single line at the Zookeeper command prompt to set the URL connection string so that kafka can connect to primary and secondary DB2 server for the WAREHOUS database:

  set /systemconfig/com.ibm.tivoli.ccm.saas.prefetch/DB_URL {"duplicated":false,"uivisibility":false,"encrypted":false,"readonly":false,"datatype":"STRING","service":"com.ibm.tivoli.ccm.saas.prefetch","name":"DB_URL","value":"jdbc:db2:\/\/primary-db2-server-hostname:primary-db2-server-port\/WAREHOUS:clientRerouteAlternateServerName=backup-db2-server-hostname;clientRerouteAlternatePortNumber=backup-db2-server-port;maxRetriesForClientReroute=1;retryIntervalForClientReroute=15;","cfgrequired":true,"uiorder":0}

  - Where primary-db2-server-hostname, primary-db2-server-port, backup-db2-server-hostname, and backup-db2-server-port need to be replaced by the values for the DB2 HADR servers. In our example, the database server names are apmdb_1 and apmdb_2.

- Example:

  set /systemconfig/com.ibm.tivoli.ccm.saas.prefetch/DB_URL {"duplicated":false,"uivisibility":false,"encrypted":false,"readonly":false,"datatype":"STRING","service":"com.ibm.tivoli.ccm.saas.prefetch","name":"DB_URL","value":"jdbc:db2:\/\/apmdb_1:50000\/WAREHOUS:clientRerouteAlternateServerName=apmdb_2;clientRerouteAlternatePortNumber=50000;maxRetriesForClientReroute=3;retryIntervalForClientReroute=5;","cfgrequired":true,"uiorder":0}

- Enter this command on a single line at the Zookeeper command prompt to set the URL connection string so that kafka can connect to primary and secondary DB2 server for the WAREHOUS database:

  set /systemconfig/com.ibm.tivoli.ccm.datamart/dburl {"duplicated":false,"uivisibility":false,"encrypted":false,"readonly":false,"datatype":"STRING","service":"com.ibm.tivoli.ccm.datamart","name":"dburl","value":,"jdbc:db2:\/\/primary-db2-server-hostname:primary-db2-server-port\/DATAMART:clientRerouteAlternateServerName=primary-db2-server-hostname,backup-db2-server-hostname;clientRerouteAlternatePortNumber=primary-db2-server-port,backup-db2-server-port;maxRetriesForClientReroute=1;retryIntervalForClientReroute=15;","cfgrequired":false,"uiorder":1000}

- where primary-db2-server-hostname, primary-db2-server-port, backup-db2-server-hostname, and backup-db2-server-port need to be replaced by the values for the DB2 HADR servers.

- Example:

  set /systemconfig/com.ibm.tivoli.ccm.datamart/dburl {"duplicated":false,"uivisibility":false,"encrypted":false,"readonly":false,"datatype":"STRING","service":"com.ibm.tivoli.ccm.datamart","name":"dburl","value":"jdbc:db2:\/\/apmdb_1:50000\/DATAMART:clientRerouteAlternateServerName=apmdb_2;clientRerouteAlternatePortNumber=50000;maxRetriesForClientReroute=3;retryIntervalForClientReroute=5;","cfgrequired":false,"uiorder":1000}

Reconfigure SCR to use the DB2 HADR environment:

- Verify your current configuration.
  - cd <apm-server-home>/ccm/SCR/XMLtoolkit/bin/
  - grep DL_DBManager.ObjectURL xmltoolkitsvc.properties
  - The output should look something like this:
    - jdbc:db2://sapm-db2a.tivlab.raleigh.ibm.com:50001/SCR1
- Add the alternate DB2 server information to the line.
  - Run <apm-server-home>/ccm/SCR/XMLtoolkit/bin/scrdbconfig.sh -update -t DB2 -h sapm-db2a.tivlab.raleigh.ibm.com -p 50001 -d SCR1 -x sapm-db2b.tivlab.raleigh.ibm.com -y 50001
  - Where
    - The value for the –t parameter is “DB2”.
    - The value for the –h parameter is the hostname of the primary DB2 server.
    - The value for the –p parameter is the DB2 port used to connect to the primary DB2 server.
    - The value for the –d parameter is the name of the DB2 SCR database.
    - The value for the –x parameter is the hostname of the standby DB2 server.
    - The value for the –y parameter is the DB2 port used to connect to the standby DB2 server.

- After running the command the value returned from running
  - grep DL_DBManager.ObjectURL xmltoolkitsvc.properties
  - Should look similar to this example:
  - DL_DBManager.ObjectURL= jdbc:db2://sapm-db2a.tivlab.raleigh.ibm.com:50001/SCR1:clientRerouteAlternateServerName=sapm-db2a.tivlab.raleigh.ibm.com,sapm-db2b.tivlab.raleigh.ibm.com;clientRerouteAlternatePortNumber=50001,50001;maxRetriesForClientReroute=10;retryIntervalForClientReroute=30;

Reconfigure Server1 to use the DB2 HADR environment:

- Edit <apm-server-home>/wlp/usr/servers/server1/scr/conf/server_include.xml and make the following changes to the datasources to ensure that SCR uses the DB2 HADR environment.
- Copy the password value and then delete the following section that begins with "<!—DB2 datasource- -->" as shown below. Remove the entire section shown in red. Your password will be different from the entry shown in blue, so save your password.

```
<!-- DB2 datasource- -->
    <dataSource id="SCR_DB" jndiName="jdbc/scr">
        <connectionManager maxPoolSize="20" minPoolSize="5"
numConnectionsPerThreadLocal="1"  connectionTimeout="10s" agedTimeout="30m"/>
        <jdbcDriver libraryRef="SCRDB2JDBC"/>
        <properties.db2.jcc databaseName="SCR32" serverName="sapm-db2b"
portNumber="50000"
                    currentLockTimeout="30s" user="itmuser" password="{xor}HjIsa2YrOiwr"/>
    </dataSource>
    <!-- End DB2 datasource -->

<!-- DB2 with reroute datasource -
    <dataSource id="SCR_DB" jndiName="jdbc/scr">
        <connectionManager maxPoolSize="20" minPoolSize="5"
numConnectionsPerThreadLocal="1"  connectionTimeout="10s" agedTimeout="30m"/>
        <jdbcDriver libraryRef="SCRDB2JDBC"/>k
        <properties.db2.jcc databaseName="SCR32" serverName="sapm-db2b"
portNumber="50000"
                    currentLockTimeout="30s" user="itmuser" password="{xor}HjIsa2YrOiwr"
                    clientRerouteAlternateServerName="__DB2_REROUTE_HOST_NAME__"
                    clientRerouteAlternatePortNumber="__DB2_REROUTE_PORT__"
                    maxRetriesForClientReroute="__DB2_REROUTE_MAX_RETRIES__"
                    retryIntervalForClientReroute="__DB2_REROUTE_RETRY_INTERVAL__"
```

```
                    enableSeamlessFailover="1"
                    __DB2_REROUTE_ADDITIONAL_PARAMETERS__
                    />
            </dataSource>
            - End DB2 with reroute datasource -->
```

- Replace the comment out section with the following. Where you see items in blue, replace them with values that are appropriate for your environment. For the password, copy and paste the contents from the previous section that you deleted.

```
<!-- DB2 with reroute datasource- -->
    <dataSource id="SCR_DB" jndiName="jdbc/scr">
        <connectionManager maxPoolSize="20" minPoolSize="5"
numConnectionsPerThreadLocal="1" connectionTimeout="10s" agedTimeout="30m"/>
        <jdbcDriver libraryRef="SCRDB2JDBC"/>
        <properties.db2.jcc databaseName="scr32" serverName="apmdb_1.ibm.com"
portNumber="50000" currentLockTimeout="30s" user="db2apm" password="{xor}HjIsa2YrOiwr "
clientRerouteAlternateServerName="apmdb-2.ibm.com"
clientRerouteAlternatePortNumber="50000" maxRetriesForClientReroute="3"
retryIntervalForClientReroute="5" enableSeamlessFailover="1"/>
    </dataSource>
    <!-- End DB2 with reroute datasource -->
```

- Copy the password value and then delete the following section that begins with "<!-- Prefetch datasource- -->" as shown below. Remove the entire section shown in red. Your password will be different from the entry shown in blue, so save your password.

```
<!-- Prefetch datasource- -->
    <dataSource id="SCR_PREFETCH" jndiName="jdbc/scr_prefetch">
        <connectionManager maxPoolSize="3" minPoolSize="1" numConnectionsPerThreadLocal="1"
connectionTimeout="10s" agedTimeout="30m"/>
        <jdbcDriver libraryRef="SCRDB2JDBC"/>
        <properties.db2.jcc databaseName="WAREHOUS" serverName="sapm-db2b"
portNumber="50000"
                    currentLockTimeout="30s" user="itmuser" password="{xor}HjIsa2YrOiwr"/>
    </dataSource>
    <!-- End Prefetch datasource -->

<!-- Prefetch with reroute datasource -
    <dataSource id="SCR_PREFETCH" jndiName="jdbc/scr_prefetch">
        <connectionManager maxPoolSize="3" minPoolSize="1" numConnectionsPerThreadLocal="1"
connectionTimeout="10s" agedTimeout="30m"/>
        <jdbcDriver libraryRef="SCRDB2JDBC"/>
        <properties.db2.jcc databaseName="WAREHOUS" serverName="sapm-db2b"
portNumber="50000"
                    currentLockTimeout="30s" user="itmuser" password="{xor}HjIsa2YrOiwr"
                    clientRerouteAlternateServerName="__PREFETCH_REROUTE_HOST_NAME__"
                    clientRerouteAlternatePortNumber="__PREFETCH_REROUTE_PORT__"
```

```
                maxRetriesForClientReroute="__PREFETCH_REROUTE_MAX_RETRIES__"
                retryIntervalForClientReroute="__PREFETCH_REROUTE_RETRY_INTERVAL__"
                __PREFETCH_REROUTE_ADDITIONAL_PARAMETERS__
                enableClientAffinitiesList="1"/>
        </dataSource>
        - End Prefetch with reroute datasource -->
```

- Next, create a new section beginning with the information below. Where you see items in blue, replace them with values that are appropriate for your environment. For the password, copy and paste the contents from the previous section that you deleted.

```
<!-- Prefetch with reroute datasource -->
    <dataSource id="SCR_PREFETCH" jndiName="jdbc/scr_prefetch">
        <connectionManager maxPoolSize="3" minPoolSize="1" numConnectionsPerThreadLocal="1"
connectionTimeout="10s" agedTimeout="30m"/>
        <jdbcDriver libraryRef="SCRDB2JDBC"/>
        <properties.db2.jcc databaseName="warehous" serverName="apmdb_1.ibm.com"
portNumber="50000" currentLockTimeout="30s" user="itmuser" password="{xor}HjIsa2YrOiwr "
clientRerouteAlternateServerName="apmdb_2.ibm.com" clientRerouteAlternatePortNumber="50000"
maxRetriesForClientReroute="3" retryIntervalForClientReroute="5" enableSeamlessFailover="1"/>
    </dataSource>
    <!-- End Prefetch with reroute datasource -->
```

Modify the Summarization & Pruning to use the DB2 HADR environment

- Edit the <apm-server-home>/sy/config/.ConfigData/ksyenv file and change the KSY_DB_JDBCURL line to have this value:
    - lx8266|KSY_DB2_JDBCURL|jdbc:db2://primary-db2-server-hostname:primary-db2-server-port/WAREHOUS:clientRerouteAlternateServerName=primary-db2-server-hostname,backup-db2-server-hostname;clientRerouteAlternatePortNumber=primary-db2-server-port,backup-db2-server-port;maxRetriesForClientReroute=1;retryIntervalForClientReroute=15;|
    - Example:
        - lx8266|KSY_DB2_JDBCURL|jdbc:db2://apmdb_1.ibm.com:50000/WAREHOUS:clientRerouteAlternateServerName=apmdb_1,apmdb_2.ibm.com;clientRerouteAlternatePortNumber=50000,50000;maxRetriesForClientReroute=1;retryIntervalForClientReroute=15;|

- Edit the <apm-server-home>/sy/config/sy.ini file and change the KSY_WAREHOUSE_URL line to have this value. Note: There must be a semicolon at the end of the line:

- KSY_WAREHOUSE_URL='jdbc:db2://primary-db2-server-hostname:primary-db2-server-port/WAREHOUS:clientRerouteAlternateServerName=primary-db2-server-hostname,backup-db2-server-hostname;clientRerouteAlternatePortNumber=primary-db2-server-port,backup-db2-server-port;maxRetriesForClientReroute=1;retryIntervalForClientReroute=15;

- Example:

  - KSY_WAREHOUSE_URL='jdbc:db2://apmdb_1.ibm.com:50000/WAREHOUS:clientRerouteAlternateServerName=apmdb_1,apmdb_2.ibm.com;clientRerouteAlternatePortNumber=50000,50000;maxRetriesForClientReroute=1;retryIntervalForClientReroute=15;

Appendix F: Record Current values

Before you perform an upgrade record key information: (Userids, passwords, hostnames, keys, configuration files, VIP for APM and VIPs for DB2, installDB2 HADR values (ports, VIP, logindexbuild, logarchmeth1 and logarchmeth2), Userid and PW for logging on to the APM http GUI, the APM install path and DB2 version (db2ls shows the installed versions, db2level shows the version being used by the instance.)

Make note of the passwords for these accounts. They will be used during the installation of the APM server.

- db2apm (default instance ID)
- itmuser

If you are using a VIP for DB2 or APM, record the VIPs

The default username is apmadmin. The default password is apmpass.

Record the fully qualified names and IPs of the proxy servers.

You may also want to save a copy of the current configuration files that are used for connecting to DB2 Here is an example of a commands that you can use:

tar -cvf /root/apm.config.original.tar /opt/ibm/sy/config/.ConfigData/ksyenv /opt/ibm/sy/config/sy.ini /opt/ibm/ccm/SCR/XMLtoolkit/bin/xmltoolkitsvc.properties /opt/ibm/serveragents/config/`hostname`_te.cfg /opt/ibm/wlp/usr/servers/server1/scr/conf/server_include.xml /opt/ibm/ccm/properties/install.properties /opt/ibm/ccm/oslc_pm/config/as.environment

You should also backup a copy of the kafka output
apm start kafka
/opt/ibm/kafka/bin/zkCli.sh
Then "get /systemconfig/com.ibm.tivoli.ccm.datamart/dburl"
and "get /systemconfig/com.ibm.tivoli.ccm.saas.prefetch/DB_URL"
Cut and paste the above output into a file.

Appendix G: Example of How to Setup HADR.

DB2 HADR requires two servers. The servers should have the same amount of memory, CPUs, and disk space. Each server has the capability of being the primary server.

Here is a line to basic instructions on how to setup HADR:
http://www.ibm.com/support/docview.wss?uid=swg21410648

An example of commands to setup HADR for APM follow:

```
After you have created databases on the primary server for Warehous, Datamart,
and SCR32.  Enable all 3 databases for log archiving using LOGRETAIN or
specifying the actual location for logs.

   db2 update db cfg for <DBNAME> using LOGARCHMETH1 LOGRETAIN
```

- **Warning: LOGRETAIN puts the db into backup pending state and you cannot access the database until after HADR setup completes**

```
Setup the HADR configuration

On the primary

db2 update db cfg for warehous using HADR_LOCAL_HOST 9.42.12.210
db2 update db cfg for warehous using HADR_LOCAL_SVC 51013
db2 update db cfg for warehous using HADR_REMOTE_HOST 9.42.12.234
db2 update db cfg for warehous using HADR_REMOTE_SVC 51012
db2 update db cfg for warehous using HADR_REMOTE_INST db2apm

db2 update db cfg for datamart using HADR_LOCAL_HOST 9.42.12.210
db2 update db cfg for datamart using HADR_LOCAL_SVC 51015
db2 update db cfg for datamart using HADR_REMOTE_HOST 9.42.12.234
db2 update db cfg for datamart using HADR_REMOTE_SVC 51014
db2 update db cfg for datamart using HADR_REMOTE_INST db2apm

db2 update db cfg for scr32 using HADR_LOCAL_HOST 9.42.12.210
db2 update db cfg for scr32 using HADR_LOCAL_SVC 51017
db2 update db cfg for scr32 using HADR_REMOTE_HOST 9.42.12.234
db2 update db cfg for scr32 using HADR_REMOTE_SVC 51016
db2 update db cfg for scr32 using HADR_REMOTE_INST db2apm

db2 update db cfg for warehous using HADR_TARGET_LIST sapm-db2b:51012
db2 update db cfg for datamart using HADR_TARGET_LIST sapm-db2b:51014
db2 update db cfg for scr32 using HADR_TARGET_LIST sapm-db2b:51016

db2 update alternate server for database warehous using hostname sapm-db2b
port 50000
db2 update alternate server for database datamart using hostname sapm-db2b
port 50000
```

```
db2 update alternate server for database scr32 using hostname sapm-db2b port
50000
```

Do an offline db2 backup for all 3 databases

On the standby

Do a db2 restore for all 3 databases

```
db2 update db cfg for warehous using HADR_LOCAL_HOST 9.42.12.234
db2 update db cfg for warehous using HADR_LOCAL_SVC 51012
db2 update db cfg for warehous using HADR_REMOTE_HOST 9.42.12.210
db2 update db cfg for warehous using HADR_REMOTE_SVC 51013
db2 update db cfg for warehous using HADR_REMOTE_INST db2apm

db2 update db cfg for datamart using HADR_LOCAL_HOST 9.42.12.234
db2 update db cfg for datamart using HADR_LOCAL_SVC 51014
db2 update db cfg for datamart using HADR_REMOTE_HOST 9.42.12.210
db2 update db cfg for datamart using HADR_REMOTE_SVC 51015
db2 update db cfg for datamart using HADR_REMOTE_INST db2apm

db2 update db cfg for scr32 using HADR_LOCAL_HOST 9.42.12.234
db2 update db cfg for scr32 using HADR_LOCAL_SVC 51016
db2 update db cfg for scr32 using HADR_REMOTE_HOST 9.42.12.210
db2 update db cfg for scr32 using HADR_REMOTE_SVC 51017
db2 update db cfg for scr32 using HADR_REMOTE_INST db2apm

db2 update db cfg for warehous using HADR_TARGET_LIST sapm-db2a:51013
db2 update db cfg for datamart using HADR_TARGET_LIST sapm-db2a:51015
db2 update db cfg for scr32 using HADR_TARGET_LIST sapm-db2a:51017

db2 update alternate server for database warehous using hostname sapm-db2a
port 50000
db2 update alternate server for database datamart using hostname sapm-db2a
port 50000
db2 update alternate server for database scr32 using hostname sapm-db2a port
50000
```

Also need to setup logging This example uses a disk archive. Run these commands on both servers

```
db2 update db cfg for warehous using LOGINDEXBUILD ON
db2 update db cfg for datamart using LOGINDEXBUILD ON
db2 update db cfg for scr32 using LOGINDEXBUILD ON
mkdir /home/db2apm/log_arch
mkdir /home/db2apm/log_arch/warehous
mkdir /home/db2apm/log_arch/datamart
mkdir /home/db2apm/log_arch/scr32
db2 update db cfg for warehous using logarchmeth1
DISK:/home/db2apm/log_arch/warehous
db2 update db cfg for datamart using logarchmeth1
```

```
DISK:/home/db2apm/log_arch/datamart
db2 update db cfg for scr32 using logarchmeth1
DISK:/home/db2apm/log_arch/scr32


To get it into peer mode.
On the standby server run   db2 start hadr on db <db> as standby
Then on the primary run db2 start hadr on db <db> as primary
```

Verify HADR is in peer mode by running db2pd –hadr –db <db>

The database might be in remote catchup pending mode but should reach peer mode after a few minutes depending on the size of the database and activity on the primary.

Setup SCR UDF Routines

The SCR UDF routines must exist on both DB2 HADR servers. You can verify they exist by running the following commands on the active DB2 server

db2 connect to scr32

where scr32 is the name of your SCR database.

db2 "select ROUTINE_CATALOG, ROUTINE_SCHEMA, ROUTINE_NAME, ROUTINE_TYPE from sysibm.routines " | grep -i TBSMUDF |wc –l

The result should be the number 32. If 32 routines exist on each DB2 servers, then do not perform the SCR UDF setup steps below.

Follow the instructions at https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/upgrade_server_inplace.htm step 8b thru 8e to setup SCR UDF routines. These instruction will have steps to setup the SCR UDF routines:

8. Step 8.

   If the SCR UDF routines are setup, you can skip this step 8. The SCR UDF routines must exist on both the primary and standby HADR DB2 databases. To list the APM routines run: db2 connect to scr32; db2 "select ROUTINE_CATALOG, ROUTINE_SCHEMA, ROUTINE_NAME, ROUTINE_TYPE from sysibm.routines " | grep -i TBSMUDF | wc –l The result line count should indicate 32. If you already have 32 UDF routines on each DB2 server, skip the rest of step 8.

   You need to verify the SCR UDF functions exist on the standby DB2 server. To do that you will need to do a “db2 takeover hadr on db SCR32” where SCR32 is the name of

your DB2 SCR32 database then “db2 connect to SCR32” and run the above command to verify the 32 SCR UDF functions exist on the standby APM server.

If the SCR UDF functions already exist on each DB2 server, then do not perform the SCR UDF setup steps below.

a. Do not run step 8a. The DB2 database was already backed up using the primary, side A.

If you need to create the UDF functions, complete steps 8b through 8e

b. (Copy the setup-dbconfig-*platform*_64.bin script) ….
c. (Login) ….
d. Run the setup-dbconfig program. The SCR UDF routines are not included in the database backup and restore process. If the SCR UDF routines do not exist, then you will need to run the setup-dbconfig program to create the tbsmdb directory and then use the tbsmdb directory to create the UDF routines. You should only run the setup-dbconfig program once for each instance. If the setup-dbconfig program has not been run for this instance,
    1. Login to the secondary DB2 server as the db2 instance user.
    2. Copy /installation_media/packages/SCR/setup-dbconfig-linux_64.bin to the secondary DB2 server
    3. As the DB2 instance user, run "setup-dbconfig-operating_system_64.bin -i console"
    4. --- when prompted, use /home/db2-instance/tbsmdb for the installation folder Where /home/db2-instance/ is the home directory for this instance. (Update Jan 28 2019) If you installed the TBSM product on this DB2 server, use a different directory when installing APM’s copy of TBSM, i.e. if TBSM databases are also installed on this Db2 server, ensure that the installation folder used for the setup-dbconfig program is different than the one used for the TBSM Database Configuration Utility.
    5. --- when prompted for “Select the product that will be using this database”

       select the default “ IBM Cloud Application Performance Management (APM)”

    6. --- When prompted for the type of install, select “Simple”
    7. --- When prompted whether to create the database or not, specify NO. The database already exists, we do not want to create it.
    8. --- Accept the defaults to complete the tbsmdb installation. (If you are using customized values, enter those values instead of SCR32 and 50000).
e. Install tbsmdb and setup the SCR UDF routines: If the routines do not exist,
    1. The SCR32 database must be in the Primary role. If not, run “db2 takeover hadr on db SCR32”. Performing the next step as the db2-instance user:
    2. Cd to the tbsmdb/bin directory for this instance. For example, cd /home/db2apm//tbsmdb/bin
    3. --- ./tbsm_db.sh -s sc -U <db2-instance-user> -f j
    4. --- This will install the Java UDF routines into the database as well as install the associated jar's into the secondary DB2 instance's file system.

f. Step f was already completed on the primary DB2 server. Skip this step.

The above steps are similar to steps 5 & 6 under **Moving Db2 databases to a different Db2 server or Db2 instance** Step 5 - Set up TBSMDB for SCR UDF functions and Step 6 - Set up the SCR UDF functions.

End of setting up SCR UDF routines on the standby DB2 server

Appendix H: Configuring APM to use 3 VIPs for DB2

DB2 HADR normally has one VIP for each database. APM installation only expects one VIP for all 3 databases. You can either use ACR or VIPs. If you use VIPs and you also want to use TSAMP to provide automation for DB2 failovers you will need to manually configure APM to use the 3 VIPs. The following steps are for customers that want to use 3 VIPs for DB2.

1) If you did not setup DB2 HADR yet, refer to Appendix G: Example of How to Setup HADR.

APM uses 3 dbs 1) Warehous AKA metric or prefetch, 2) SCR32 AKA SCR or topology, and Datamart.

When installing in an HA environment that uses HADR you will have 3 DBs on the primary DB2 server and 3 DBs on the standby DB2 server.

APM requires SCR UDF routines to be installed. These are setup as part of the steps for creating the SCR database. As part of the HADR setup process a backup is taken on the primary DB2 server and restored on the standby DB2 server. Backup and restore does not include UDF routines. You need to add the SCR UDF routines to the standby DB2 server.

.

2) Edit install.properties file (it is located in the same directory as install.sh).

Update the following fields in the install.properties file:

db2.hostname=db2wh1.tivlab.raleigh.ibm.com

db2.external.instance=db2apm1

db2.port=50001

#Authentication must match the values that you used to catalog the DB2 databases.(server is the default)

db2.authentication=server

#If you are not using the default names, update the names of the databases

datamartdb.name=Dmart1

metriccachedb.name=whOUS1

topologydb.name=scR1

3) update the db2 catalog db

For every db in install.properties verify the catalog entry does not exist. From the APM server su - db2apm and do a db2 uncatalog db <db_name>

For every custom db name that you are using you must create a cross reference catalog entry on the APM server

For example,

db2 CATALOG TCPIP NODE APM1 REMOTE db2wh1.tivlab.raleigh.ibm.com SERVER 50001

db2 CATALOG DB WHOUS1 as WAREHOUS at NODE APM1

You should only catalog the alias db names if you are using custom db2 names.

If you are using the default database names, the APM install will create the catalog entries for you.

If you are using 3 VIPs for HADR, the catalog entries will need to be updated after the installation completes.

After the installation completes you will have the 3 catalog entries that the installation created plus an optional 3 that you created as aliases for your custom DB names.

If the catalog entries for the DBs that are listed in the install.properties file exist prior to installation you may get this error.

SQL1005N The database alias "whOUS1" already exists in either the local database directory or system database directory.

(The install.sh will allow you to use the name APM_NODE but use a different name like APM1 when you catalog your node because uninstall will uncatalog APM_Node.)

4) block agents from accessing APM while the install.sh is running.

If possible use a separate VIP for the Agents to connect to the APM server and remove the VIP until after APM is ready for agents.

If you are using the same VIP for the APM UI and the agents. Then do not assign the VIP until after the installation completes and you have updated the configuration files.

5) Block APM from accessing DB2. If two APM servers access the same database at the same time the database will become corrupted.

Setup the firewall rules to prevent both APM servers from accessing the same DB2 databases.

6) Install APM on both servers

7) Install IF06 on both servers

7b) Backup both APM servers /opt/ibm/ccm/backup.sh

8) save a backup copy of the original config files

cd to install dir (/opt/ibm) then run

cd /opt/ibm; tar -cvf /root/apm.config.original.tar ./sy/config/.ConfigData/ksyenv ./sy/config/sy.ini ./ccm/SCR/XMLtoolkit/bin/xmltoolkitsvc.properties ./serveragents/config/`hostname`_te.cfg ./wlp/usr/servers/server1/scr/conf/server_include.xml ./ccm/properties/install.properties ./ccm/oslc_pm/config/as.environment

9) Update the config files. The only way to avoid updating APM config files is to use one VIP for DB2 and keep the primary for all 3 DBs on the same DB2 server. If you are using ACR you must add the alternate server to the jdbc config files. If you are using 3 VIPs for DB2, APM install only allowed you to enter one (the Warehous VIP) and you must update the config files for SCR and Datamart.

After install completes

a) Update /opt/ibm/ccm/oslc_pm/config/as.environment (For example, echo "KAS_HOSTNAME=sapm-apm.tivlab.raleigh.ibm.com" >> /opt/ibm/ccm/oslc_pm/config/as.environment)

Update the following 5 configuration files on the primary server to use the DB2 VIPs

Verify the following files are using the VIP for Warehous

b) (Verify one location in this file)

c) /opt/ibm/sy/config/sy.ini (Verify one location in this file)

Update the following file to use the VIP for SCR

d) /opt/ibm/ccm/SCR/XMLtoolkit/bin/xmltoolkitsvc.properties (Update one location in this file)

Update the following file to use the VIP for Datamart

e) /opt/ibm/serveragents/config/`hostname`_te.cfg (Update two locations in this file)

The following file uses both SCR and Warehous.

f) /opt/ibm/wlp/usr/servers/server1/scr/conf/server_include.xml (Verify the 2 entries for Warehous are correct and update the two entries for SCR.)

Run /opt/ibm/kafka/bin/zkCli.sh then

get /systemconfig/com.ibm.tivoli.ccm.saas.prefetch/DB_URL # verify the VIP for Warehous is being used

get /systemconfig/com.ibm.tivoli.ccm.datamart/dburl # Update it to use the VIP for Datamart

quit to exit

To update the datamart/dburl: Save the above output to a file and use the output to create one long line similar to:

set /systemconfig/com.ibm.tivoli.ccm.datamart/dburl {"duplicated":false,"uivisibility":false,"encrypted":false,"readonly":false,"datatype":"STRING","service":"com.ibm.tivoli.ccm.datamart","name":"dburl","value":"jdbc:db2:\/\/db2dm1.tivlab.raleigh.ibm.com:50001\/DMart1","cfgrequired":false,"uiorder":1000}

run /opt/ibm/kafka/bin/zkCli.sh then run the set cmd and then quit.

rerun the get cmds and verify the output matches the original with the exception of the VIP being updated for Datamart.

10) Tar up the 6 files that were updated.

tar -cvf /root/apm.config.updated.tar ./ccm/oslc_pm/config/as.environment ./sy/config/.ConfigData/ksyenv ./sy/config/sy.ini ./ccm/SCR/XMLtoolkit/bin/xmltoolkitsvc.properties ./serveragents/config/`hostname`_te.cfg ./wlp/usr/servers/server1/scr/conf/server_include.xml

11b) Backup the configuration files on the standby server

Backup the current configuration files like you did on the primary APM server. Save a backup copy of the original config files

cd to install dir (/opt/ibm) then run tar -cvf /root/apm.config.original.tar ./sy/config/.ConfigData/ksyenv ./sy/config/sy.ini ./ccm/SCR/XMLtoolkit/bin/xmltoolkitsvc.properties ./serveragents/config/`hostname`_te.cfg ./wlp/usr/servers/server1/scr/conf/server_include.xml ./ccm/properties/install.properties ./ccm/oslc_pm/config/as.environment

11c) If you updated the configuration files to use multiple DB2 vips or added ACR to the configuration files, **you should not run /opt/ibm/ccm/update_db_config.sh** because it will rewrite your configuation files using the default of 1 ip address.

mv /opt/itm/ccm/update_db_config.sh /opt/itm/ccm/update_db_config.sh.BlockedByHA # to prevent someone from accidentally running it.

12) Restore the standby server from the primary APM server.

Whenever you run a restore.sh on the standby server you must use the -e scr option on the restore.sh for APM and if using custom names you must specify the database names.

For example, [root@sapm-apm5 apm4]# /opt/ibm/ccm/restore.sh -e scr -j whous1 -k scr1 -l dmart1 -f /backups/apm4/backup_20180730_165223.tar

The standby APM server should be blocked from accessing DB2 during the restore.

12b) If you are using LDAP, the first time that you restore to the standby server you should copy this file: (/opt/ibm/wlp/usr/shared/config/oauthVariables-onprem.xml) from the primary APM server to the standby APM server.

If this is the first time that you are running restore.sh on the standby server, you need to setup the configuration files on the standby server.

13) Copy the configuration files from the primary to the standby server

scp root@sapm-apm4:/root/apm.config.updated.tar /root/apm.primary.config.files.tar

tar -xvf /root/apm.primary.config.files.tar -C /opt/ibm/

14) Update the configuration files on the standby server.

14b) cp -p ./serveragents/config/sapm-apm4_te.cfg ./serveragents/config/`hostname`_te.cfg

14c) Change the hostname in the following files to the hostname of this server

cd /opt/ibm

vi ./sy/config/.ConfigData/ksyenv update hostname on 2 or 3 locations

vi ./ccm/SCR/XMLtoolkit/bin/xmltoolkitsvc.properties 1 VIP update hostname in 2 locations

14d) Run db2_users_passwd.sh on the standby to fix passwords that may be encrypted differently on the standby (For example, server_include.xml.).

Setup HADR

15) block both APM servers from accessing DB2

See instructions for setting up HADR

Skip to step 21 (Verify HADR)

21) verify scr udf routines exist on both HADR DB2 servers

db2 connect to scr1

[db2apm1@sapm-db2a ~]$ db2 "select ROUTINE_CATALOG, ROUTINE_SCHEMA, ROUTINE_NAME, ROUTINE_TYPE from sysibm.routines " | grep -i TBSMUDF |wc -l

32

db2 connect reset

[db2apm1@sapm-db2b db2a]$ db2 takeover hadr on db scr1

db2 connect to scr1

[db2apm1@sapm-db2b db2a]$ db2 "select ROUTINE_CATALOG, ROUTINE_SCHEMA, ROUTINE_NAME, ROUTINE_TYPE from sysibm.routines " | grep -i TBSMUDF |wc -l

32

db2 connect reset

22) Verify db2 takeover works from the standby server for all 3 databases. Then Put all 3 databases back onto the primary node.

[db2apm1@sapm-db2a ~]$ db2 takeover hadr on db whous1

DB20000I The TAKEOVER HADR ON DATABASE command completed successfully.

[db2apm1@sapm-db2a ~]$ db2 takeover hadr on db scr1

DB20000I The TAKEOVER HADR ON DATABASE command completed successfully.

[db2apm1@sapm-db2a ~]$ db2 takeover hadr on db dmart1

DB20000I The TAKEOVER HADR ON DATABASE command completed successfully.

[db2apm1@sapm-db2a ~]$

Setup TSAMP

23) setup tsamp

If you want to add automation to your DB2 HADR databases,

a) Install tsamp on both nodes

cd /media/db211.3.3/db2fp3/server_t/db2/linuxamd64/tsamp

[root@sapm-db2a tsamp]# ./installSAM --silent

b) view the log.

ls -ltra /tmp | grep installSAM

c) install the efix if there is an efix directory in the tsamp directory

cd efix; ./install.sh

Installing efix DB2-4103-efix5 for RSCT 3.2.1.2 and SAMP 4.1.0.3 on x86_64_linux_2

[root@sapm-db2b efix]#

d) Record the version of tsamp and rsct.

[root@sapm-db2b tsamp]# samversion -Ab

rsa41svcs003g 4.1.0.3 Oct 24 2017 14:17:21

[root@sapm-db2b tsamp]# ctversion -Ab

RSCT_Build_Name=roots002a 3.2.1.2 RSCT_Build_Time=16097.22:05:47
RSCT_Build_Context=amd64_linux_2

e) if tsamp directory has a db2installSAM script. Run it to upgrade RSCT and TSAMP

[root@sapm-db2b tsamp]# ./db2installSAM

f) It will upgrade RSCT to version 3.2.3.1 and install the efix

[root@sapm-db2b tsamp]# ctversion -Ab

RSCT_Build_Name=rrablxs001a 3.2.3.1 RSCT_Build_Time=17298.01:29:45
RSCT_Build_Context=amd64_linux_2

[root@sapm-db2b tsamp]# samversion -Ab

rsa41svcs003g 4.1.0.3 Oct 24 2017 14:17:21

24) After TSAMP is installed verify both nodes are at the same tsamp and rsct version

[root@sapm-db2a ~]# ctversion

rrablxs001a 3.2.3.1 amd64_linux_2

[root@sapm-db2a ~]# samversion

rsa41svcs003g 4.1.0.3 Oct 24 2017 14:17:21

Create the TSAMP domain

25)now run preprpnode on both nodes

use the values from hostname when running preprpnode.

preprpnode sapm-db2a sapm-db2b

db2haicu will use the gateway as the quorum device. Normally netstat -ar | grep -i default will show you the gateway.

If that does not work, use traceroute <an IP on a different subnet> and the gateway should be the first hop in the sequence.

Normally it would be 9.42.12.1 but sometimes a different IP is used like 9.42.12.152

db2haicu will ask for the type of network you are using (public vs private network).

The public network is the network that is used to access DB2. If you are using VIPs, to access DB2 the VIPs are on the public network.

The private network (AKA backnet) is the network that is used for administrative purposes such as running backups.

The term public is just a name. It does not imply the network is not secure. If you only have one network, then it is called the public network.

a) Update the peer window and timeout settings. If the peer window is 0, change it to 300. It cannot be 0

db2 update db cfg for dmart1 using HADR_PEER_WINDOW 300 # (if it is 0 it cannot be automated.)

[db2apm1@sapm-db2b ~]$ db2pd -hadr -db dmart1 | grep -i timeout   # 120 is the default

HADR_TIMEOUT(seconds) = 120

b) if /usr/sbin/rsct/sapolicies/db2 does not exist, run

[root@sapm-db2a tsamp]# /opt/ibm/db2/V11.1/install/tsamp/db2cptsa

Note: Remove the VIPS before running db2haicu. If they already ping, the script will reject them.

26)run db2haicu on the standby server.

27) run db2haicu on the primary server.

At this point you should be able to run lssam on either DB2 node to see the resources that are managed by TSAMP.

Test connection from APM to DB2

28) setup the db2 catalog entries on APM4 and APM5 to use the 3 DB2 VIPs

For example,

su - db2apm

db2 catalog tcpip node APMwh1 REMOTE db2wh1.tivlab.raleigh.ibm.com SERVER 50001

catalog a tcpip node for each DB2 VIP and then catalog each database using the correct node

28) After a DB2 failover you should bounce the following components. Often the failover does not require restarting any APM components.

apm stop min; apm stop server1; apm stop scr; apm stop txagent;

apm start_all

Appendix I: Sample db2haicu on the standby DB2 server

Prior to running db2haicu you must run preprpnode node1 node2 on both DB2 servers as root.

Where: node1 is the hostname of the primary db2 server and node2 is the hostname of the standby db2 server. This sets up ACLs and allows communications between the two servers.

The follow is the output from running db2haicu on the standby db2 server as the db2 instance.

[db2apm1@sapm-db2b ~]$ db2haicu

Welcome to the DB2 High Availability Instance Configuration Utility (db2haicu).

You can find detailed diagnostic information in the DB2 server diagnostic log file called db2diag.log. Also, you can use the utility called db2pd to query the status of the cluster domains you create.

For more information about configuring your clustered environment using db2haicu, see the topic called 'DB2 High Availability Instance Configuration Utility (db2haicu)' in the DB2 Information Center.

db2haicu determined the current DB2 database manager instance is 'db2apm1'. The cluster configuration that follows will apply to this instance.

db2haicu is collecting information on your current setup. This step may take some time as db2haicu will need to activate all databases for the instance to discover all paths ...

When you use db2haicu to configure your clustered environment, you create cluster domains. For more information, see the topic 'Creating a cluster domain with db2haicu' in the DB2 Information Center. db2haicu is searching the current machine for an existing active cluster domain ...

db2haicu did not find a cluster domain on this machine. db2haicu will now query the system for information about cluster nodes to create a new cluster domain ...

db2haicu did not find a cluster domain on this machine. To continue configuring your clustered environment for high availability, you must create a cluster domain; otherwise, db2haicu will exit.

Create a domain and continue? [1]

1. Yes

2. No

1

Create a unique name for the new domain:

apmdb2

Nodes must now be added to the new domain.

How many cluster nodes will the domain 'apmdb2' contain?

2

Enter the host name of a machine to add to the domain:

sapm-db2a

Enter the host name of a machine to add to the domain:

sapm-db2b

db2haicu can now create a new domain containing the 2 machines that you specified. If you choose not to create a domain now, db2haicu will exit.

Create the domain now? [1]

1. Yes

2. No

1

Creating domain 'apmdb2' in the cluster ...

Creating domain 'apmdb2' in the cluster was successful.

You can now configure a quorum device for the domain. For more information, see the topic "Quorum devices" in the DB2 Information Center. If you do not configure a quorum device for the domain, then a human operator will have to manually intervene if subsets of machines in the cluster lose connectivity.

Configure a quorum device for the domain called 'apmdb2'? [1]

1. Yes

2. No

1

The following is a list of supported quorum device types:

1. Network Quorum

Enter the number corresponding to the quorum device type to be used: [1]

1

Specify the network address of the quorum device:

9.42.12.152

Configuring quorum device for domain 'apmdb2' ...

Configuring quorum device for domain 'apmdb2' was successful.

The cluster manager found the following total number of network interface cards on the machines in the cluster domain: '4'. You can add a network to your cluster domain using the db2haicu utility.

Create networks for these network interface cards? [1]

1. Yes

2. No

1

Enter the name of the network for the network interface card: 'virbr0' on cluster node: 'sapm-db2a.tivlab.raleigh.ibm.com'

1. Create a new public network for this network interface card.

2. Create a new private network for this network interface card.

3. Skip this step.

Enter selection:

3

Enter the name of the network for the network interface card: 'virbr0' on cluster node: 'sapm-db2b.tivlab.raleigh.ibm.com'

1. Create a new public network for this network interface card.

2. Create a new private network for this network interface card.

3. Skip this step.

Enter selection:

3

Enter the name of the network for the network interface card: 'ens192' on cluster node: 'sapm-db2b.tivlab.raleigh.ibm.com'

1. Create a new public network for this network interface card.

2. Create a new private network for this network interface card.

3. Skip this step.

Enter selection:

1

Are you sure you want to add the network interface card 'ens192' on cluster node 'sapm-db2b.tivlab.raleigh.ibm.com' to the network 'db2_public_network_0'? [1]

1. Yes

2. No

1

Adding network interface card 'ens192' on cluster node 'sapm-db2b.tivlab.raleigh.ibm.com' to the network 'db2_public_network_0' ...

Adding network interface card 'ens192' on cluster node 'sapm-db2b.tivlab.raleigh.ibm.com' to the network 'db2_public_network_0' was successful.

Enter the name of the network for the network interface card: 'ens192' on cluster node: 'sapm-db2a.tivlab.raleigh.ibm.com'

1. db2_public_network_0

2. Create a new public network for this network interface card.

3. Create a new private network for this network interface card.

4. Skip this step.

Enter selection:

1

Are you sure you want to add the network interface card 'ens192' on cluster node 'sapm-db2a.tivlab.raleigh.ibm.com' to the network 'db2_public_network_0'? [1]

1. Yes

2. No

1

Adding network interface card 'ens192' on cluster node 'sapm-db2a.tivlab.raleigh.ibm.com' to the network 'db2_public_network_0' ...

Adding network interface card 'ens192' on cluster node 'sapm-db2a.tivlab.raleigh.ibm.com' to the network 'db2_public_network_0' was successful.

Retrieving high availability configuration parameter for instance 'db2apm1' ...

The cluster manager name configuration parameter (high availability configuration parameter) is not set. For more information, see the topic "cluster_mgr - Cluster manager name configuration parameter" in the DB2 Information Center. Do you want to set the high availability configuration parameter?

The following are valid settings for the high availability configuration parameter:

1.TSA

2.Vendor

Enter a value for the high availability configuration parameter: [1]

1

Setting a high availability configuration parameter for instance 'db2apm1' to 'TSA'.

Adding DB2 database partition '0' to the cluster ...

Adding DB2 database partition '0' to the cluster was successful.

Do you want to validate and automate HADR failover for the HADR database 'WHOUS1'? [1]

1. Yes

2. No

1

Adding HADR database 'WHOUS1' to the domain ...

Cluster node '9.42.12.210' was not found in the domain. Please re-enter the host name.

sapm-db2a

Cluster node '9.42.12.234' was not found in the domain. Please re-enter the host name.

sapm-db2b

Adding HADR database 'WHOUS1' to the domain ...

HADR database 'WHOUS1' has been determined to be valid for high availability. However, the database cannot be added to the cluster from this node because db2haicu detected this node is the standby for HADR database 'WHOUS1'. Run db2haicu on the primary for HADR database 'WHOUS1' to configure the database for automated failover.

Do you want to validate and automate HADR failover for the HADR database 'DMART1'? [1]

1. Yes

2. No

1

Adding HADR database 'DMART1' to the domain ...

Cluster node '9.42.12.210' was not found in the domain. Please re-enter the host name.

sapm-db2a

Cluster node '9.42.12.234' was not found in the domain. Please re-enter the host name.

sapm-db2b

Adding HADR database 'DMART1' to the domain ...

HADR database 'DMART1' has been determined to be valid for high availability. However, the database cannot be added to the cluster from this node because db2haicu detected this node is the standby for HADR database 'DMART1'. Run db2haicu on the primary for HADR database 'DMART1' to configure the database for automated failover.

Do you want to validate and automate HADR failover for the HADR database 'SCR1'? [1]

1. Yes

2. No

1

Adding HADR database 'SCR1' to the domain ...

Cluster node '9.42.12.210' was not found in the domain. Please re-enter the host name.

sapm-db2a

Cluster node '9.42.12.234' was not found in the domain. Please re-enter the host name.

sapm-db2b

Adding HADR database 'SCR1' to the domain ...

HADR database 'SCR1' has been determined to be valid for high availability. However, the database cannot be added to the cluster from this node because db2haicu detected this node is the standby for HADR database 'SCR1'. Run db2haicu on the primary for HADR database 'SCR1' to configure the database for automated failover.

All cluster configurations have been completed successfully. db2haicu exiting ...

[db2apm1@sapm-db2b ~]$ db2haicu

Appendix J: Sample db2haicu on the primary DB2 server

The follow is the output from running db2haicu on the primary DB2 server as the DB2 instance.

[db2apm1@sapm-db2a ~]$ db2haicu

Welcome to the DB2 High Availability Instance Configuration Utility (db2haicu).

You can find detailed diagnostic information in the DB2 server diagnostic log file called db2diag.log. Also, you can use the utility called db2pd to query the status of the cluster domains you create.

For more information about configuring your clustered environment using db2haicu, see the topic called 'DB2 High Availability Instance Configuration Utility (db2haicu)' in the DB2 Information Center.

db2haicu determined the current DB2 database manager instance is 'db2apm1'. The cluster configuration that follows will apply to this instance.

db2haicu is collecting information on your current setup. This step may take some time as db2haicu will need to activate all databases for the instance to discover all paths ...

When you use db2haicu to configure your clustered environment, you create cluster domains. For more information, see the topic 'Creating a cluster domain with db2haicu' in the DB2 Information Center. db2haicu is searching the current machine for an existing active cluster domain ...

db2haicu found a cluster domain called 'apmdb2' on this machine. The cluster configuration that follows will apply to this domain.

Retrieving high availability configuration parameter for instance 'db2apm1' ...

The cluster manager name configuration parameter (high availability configuration parameter) is not set. For more information, see the topic "cluster_mgr - Cluster manager name configuration parameter" in the DB2 Information Center. Do you want to set the high availability configuration parameter?

The following are valid settings for the high availability configuration parameter:

1.TSA

2.Vendor

Enter a value for the high availability configuration parameter: [1]

1

Setting a high availability configuration parameter for instance 'db2apm1' to 'TSA'.

Adding DB2 database partition '0' to the cluster ...

Adding DB2 database partition '0' to the cluster was successful.

Do you want to validate and automate HADR failover for the HADR database 'WHOUS1'? [1]

1. Yes

2. No

1

Adding HADR database 'WHOUS1' to the domain ...

Cluster node '9.42.12.234' was not found in the domain. Please re-enter the host name.

sapm-db2b

Cluster node '9.42.12.210' was not found in the domain. Please re-enter the host name.

sapm-db2a

Adding HADR database 'WHOUS1' to the domain ...

Adding HADR database 'WHOUS1' to the domain was successful.

Do you want to configure a virtual IP address for the HADR database 'WHOUS1'? [1]

1. Yes

2. No

1

Enter the virtual IP address:

9.42.13.1

Enter the subnet mask for the virtual IP address '9.42.13.1': [255.255.255.0]

255.255.252.0

Select the network for the virtual IP '9.42.13.1':

1. db2_public_network_0

Enter selection:

1

Adding virtual IP address '9.42.13.1' to the domain ...

Adding virtual IP address '9.42.13.1' to the domain was successful.

Do you want to configure mount point monitoring for the HADR database 'WHOUS1'? [2]

1. Yes

2. No

2

Do you want to validate and automate HADR failover for the HADR database 'DMART1'? [1]

1. Yes

2. No

1

Adding HADR database 'DMART1' to the domain ...

Cluster node '9.42.12.234' was not found in the domain. Please re-enter the host name.

sapm-db2b

Cluster node '9.42.12.210' was not found in the domain. Please re-enter the host name.

sapm-db2a

Adding HADR database 'DMART1' to the domain ...

Adding HADR database 'DMART1' to the domain was successful.

Do you want to configure a virtual IP address for the HADR database 'DMART1'? [1]

1. Yes

2. No

1

Enter the virtual IP address:

9.42.13.2

Enter the subnet mask for the virtual IP address '9.42.13.2': [255.255.255.0]

255.255.252.0

Select the network for the virtual IP '9.42.13.2':

1. db2_public_network_0

Enter selection:

1

Adding virtual IP address '9.42.13.2' to the domain ...

Adding virtual IP address '9.42.13.2' to the domain was successful.

Do you want to configure mount point monitoring for the HADR database 'DMART1'? [2]

1. Yes

2. No

2

Do you want to validate and automate HADR failover for the HADR database 'SCR1'? [1]

1. Yes

2. No

1

Adding HADR database 'SCR1' to the domain ...

Cluster node '9.42.12.234' was not found in the domain. Please re-enter the host name.

sapm-db2b

Cluster node '9.42.12.210' was not found in the domain. Please re-enter the host name.

sapm-db2a

Adding HADR database 'SCR1' to the domain ...

Adding HADR database 'SCR1' to the domain was successful.

Do you want to configure a virtual IP address for the HADR database 'SCR1'? [1]

1. Yes

2. No

1

Enter the virtual IP address:

9.42.13.3

Enter the subnet mask for the virtual IP address '9.42.13.3': [255.255.255.0]

255.255.252.0

Select the network for the virtual IP '9.42.13.3':

1. db2_public_network_0

Enter selection:

1

Adding virtual IP address '9.42.13.3' to the domain ...

Adding virtual IP address '9.42.13.3' to the domain was successful.

Do you want to configure mount point monitoring for the HADR database 'SCR1'? [2]

1. Yes

2. No

2

All cluster configurations have been completed successfully. db2haicu exiting ...

[db2apm1@sapm-db2a ~]$

Sample lssam –V output

After db2haicu completes on both servers your domain should be similar to the following:

[db2apm1@sapm-db2a ~]$ lssam -V

Online IBM.ResourceGroup:db2_db2apm1_db2apm1_DMART1-rg Nominal=Online -.

|- Online IBM.Application:db2_db2apm1_db2apm1_DMART1-rs -. :

|- Online IBM.Application:db2_db2apm1_db2apm1_DMART1-rs:sapm-db2a | :

'- Offline IBM.Application:db2_db2apm1_db2apm1_DMART1-rs:sapm-db2b | :

'- Online IBM.ServiceIP:db2ip_9_42_13_2-rs IP=9.42.13.2 | :

```
        |- Online IBM.ServiceIP:db2ip_9_42_13_2-rs:sapm-db2a            |    :
        '- Offline IBM.ServiceIP:db2ip_9_42_13_2-rs:sapm-db2b           |    :
Online IBM.ResourceGroup:db2_db2apm1_db2apm1_SCR1-rg Nominal=Online             |    :   -.
    |- Online IBM.Application:db2_db2apm1_db2apm1_SCR1-rs                | -. :    :
        |- Online IBM.Application:db2_db2apm1_db2apm1_SCR1-rs:sapm-db2a    | | :    :
        '- Offline IBM.Application:db2_db2apm1_db2apm1_SCR1-rs:sapm-db2b   | | :    :
    '- Online IBM.ServiceIP:db2ip_9_42_13_3-rs IP=9.42.13.3               | | :    :
        |- Online IBM.ServiceIP:db2ip_9_42_13_3-rs:sapm-db2a            | | :    :
        '- Offline IBM.ServiceIP:db2ip_9_42_13_3-rs:sapm-db2b           | | :    :
Online IBM.ResourceGroup:db2_db2apm1_db2apm1_WHOUS1-rg Nominal=Online           | | :    : -.
    |- Online IBM.Application:db2_db2apm1_db2apm1_WHOUS1-rs              | | : -. : :
        |- Online IBM.Application:db2_db2apm1_db2apm1_WHOUS1-rs:sapm-db2a  | | : | : :
        '- Offline IBM.Application:db2_db2apm1_db2apm1_WHOUS1-rs:sapm-db2b | | : | : :
    '- Online IBM.ServiceIP:db2ip_9_42_13_1-rs IP=9.42.13.1               | | : | : :
        |- Online IBM.ServiceIP:db2ip_9_42_13_1-rs:sapm-db2a            | | : | : :
        '- Offline IBM.ServiceIP:db2ip_9_42_13_1-rs:sapm-db2b           | | : | : :
Online IBM.ResourceGroup:db2_db2apm1_sapm-db2a_0-rg Nominal=Online              | | : | : : -.
    '- Online IBM.Application:db2_db2apm1_sapm-db2a_0-rs                | | : | : : :
        '- Online IBM.Application:db2_db2apm1_sapm-db2a_0-rs:sapm-db2a   | | : | : : :
Online IBM.ResourceGroup:db2_db2apm1_sapm-db2b_0-rg Nominal=Online              | | : | : : : -.
    '- Online IBM.Application:db2_db2apm1_sapm-db2b_0-rs                | | : | : : : :
        '- Online IBM.Application:db2_db2apm1_sapm-db2b_0-rs:sapm-db2b   | | AN | : : : :
Online IBM.Equivalency:db2_db2apm1_db2apm1_DMART1-rg_group-equ                | | <' | : : : :
    |- Online IBM.PeerNode:sapm-db2a:sapm-db2a                          | |    | : : : :
    '- Online IBM.PeerNode:sapm-db2b:sapm-db2b                          | |    | AN : : :
```

```
Online IBM.Equivalency:db2_db2apm1_db2apm1_SCR1-rg_group-equ                | |   | <' : : :
    |- Online IBM.PeerNode:sapm-db2a:sapm-db2a                              | |   |   : : :
    '- Online IBM.PeerNode:sapm-db2b:sapm-db2b                              | |   |  AN : :
Online IBM.Equivalency:db2_db2apm1_db2apm1_WHOUS1-rg_group-equ              | |   |  <' : :
    |- Online IBM.PeerNode:sapm-db2a:sapm-db2a                              | |   |     : :
    '- Online IBM.PeerNode:sapm-db2b:sapm-db2b                              | |   |    AN :
Online IBM.Equivalency:db2_db2apm1_sapm-db2a_0-rg_group-equ                 | |   |    <' :
    '- Online IBM.PeerNode:sapm-db2a:sapm-db2a                              | |   |      AN
Online IBM.Equivalency:db2_db2apm1_sapm-db2b_0-rg_group-equ                 | |   |      <'
    '- Online IBM.PeerNode:sapm-db2b:sapm-db2b                             DO DO   DO
Online IBM.Equivalency:db2_public_network_0                               <' <'   <'
    |- Online IBM.NetworkInterface:ens192:sapm-db2a
    '- Online IBM.NetworkInterface:ens192:sapm-db2b
[db2apm1@sapm-db2a ~]$
```

Save the policy

It is a good idea to save the policy that you just created. The command to save the policy is sampolicy –s For example,

```
[root@sapm-db2a scripts]# sampolicy -s /scripts/APM.policy.092218.xml   # save the current policy


.The current policy was saved to file /scripts/APM.policy.092218.xml.


[root@sapm-db2a scripts]#
```

Appendix K: Creating Firewall Scripts

Scripts are available as is on the internet at https://developer.ibm.com/apm/resources/upgrading-a-high-availability-configuration/ under download. There are two tar files contained in a .zip file. The one for APM is apmhascripts.tar. The one for db2 is db2hascripts.tar.

Create Firewall Scripts

In this high availability configuration, only one of the two APM servers can be allowed to communicate with the DB2 database. You must setup firewall rules to prevent both APM servers from accessing DB2 at the same time. There are two options for setting up firewall scripts. The first option is to create two scripts and place them on the DB2 server(s). One script allows APM server "A" to access DB2 and blocks APM server "B". The second script blocks APM server "A" and allows APM server "B" to access DB2. Each time you do an APM failover you would run the appropriate script to allow traffic on the database port from the desired APM server and block the other APM server. If you are using VIPs, a better option is to add another VIP to the APM server for DB2 traffic. The firewall rules will only allow traffic from the APM server that has the VIP assigned and only one APM server can have the VIP.

In a typical DB2 environment, the database is listening on port 50,000. The sample scripts below assume that is the default port.. If your database is setup for a different port, change the port number in the scripts. In addition, the IP addresses listed in the scripts are based on the IP addresses in the architecture diagram. Replace the IP addresses with the addresses of your database server(s) and APM servers.

Verify the firewalls startup automatically at boot time. Check for any errors in the log at /lib/systemd/system/firewalld.service . Sometimes there is a conflict between iptables and firewalld

You can check the status of iptables by running:

/bin/systemctl status iptables.service

It is very important to have the firewalls up before APM and DB2 start to prevent both APM servers from accessing DB2 and corrupting the database. The firewalls should start at boot up time.

In previous versions of this document the firewalls needed to be updated when APM fails over to allow the other APM server to access DB2. A better idea is to use a VIP on the APM server for DB2 traffic. The DB2 firewalls will only allow traffic from the VIP. Only the APM server that has the VIP can access DB2. With this approach the firewalls are initialized at boot startup and never need to be changed.

See "Firewall Scripts" in Appendix M for samples of the firewall settings.

Test your firewall scripts

Before you move to the next step in your setup, test to make sure that the scripts are working properly. This can easily be done using the telnet command. If telnet is not installed on your machines, it can be installed using "yum install telnet" or you can test the connectivity using the tool of your choice.

First, execute systemctl start firewalld.service

Then run "./allow-basic.sh" script. You can verify the firewall is active by running: "firewall-cmd --zone=internal --list-all"

On the primary APM server, execute the following command, specifying the hostname or IP address of your database server. In the case of an HADR cluster, use the VIP. Use the port number of your database server.

telnet <IP address of database server> <port number of database server>

Example: telnet 10.1.1.4 50000

If your firewall is configured correctly, at this point the primary APM server will not be able to connect to the database server and you'll see message like this:

Trying 10.1.1.4...

telnet: connect to address 10.1.1.4: No route to host

Next allow the primary APM server to connect to DB2. You can either update your firewall rules by running "./apm-fw.sh add primary" or if you are using VIPs run "./allow.sh db2" on the primary APM server. If your firewall is configured correctly, at this point the primary APM server should be able to connect to the database server and you'll see message like this:

Connected to 10.1.1.4.

Escape character is '^]'.

Type "Ctrl]" and then "quit" to return to the command prompt.

Next, attempt to telnet from the standby APM server to the database server

telnet <IP address of database server> <port number of database server>

Example: telnet 10.1.1.4 50000

If your firewall is configured correctly, you should see something like this:

Trying 10.1.1.4...

telnet: connect to address 10.1.1.4: No route to host

Next, block the primary APM server and allow the standby APM server to access DB2. If APM is already installed on the standby APM server, run apm stop_all to prevent it from making any updates to the database. If you are updating firewall rules during a failover, run "./apm-fw.sh remove primary"on the DB2 serves or if you are using VIPs, run "./block.sh db2" on the Primary APM server. Then use telnet to verify the primary is blocked. Then run either "./apm-fw.sh add standby" on both DB2 servers or run "./allow.sh db2" on the Standby APM server. Then use telnet to verify the standby server can access DB2. The primary APM server should not be able to connect to the database server and the standby APM server should succeed in connecting over port 50,000.

Appendix L: Setting up proxy servers

Setup your Reverse Proxy

When setting up the reverse proxy, there are a few things that are important. This section will give you an example of a working Apache 2.2 httpd.conf file. This does not include the entire configuration, but does highlight the required items.

In the configuration settings below, you'll notice a few key entries. First, we have the mod_proxy and mod_rewrite modules loaded. These are required for the reverse proxy.

In the configuration we have defined, all user interface communications are using HTTPS. Before beginning, you need to generate your own certificate for the reverse proxy. We'll later import those certificates into the APM servers. In the VirtualHost section, we have configured the reverse proxy to disable configure SSL v2, SSL v3, and all certificate validation against the backend APM servers.

We are using the proxyPreserveHost to ensure that hostnames are preserved.

Here are the sample httpd.conf file settings. If you choose to copy/paste the contents below, replace the following hostnames with the fully qualified hostnames in your environment:

apm2.ibm.com (standby APM server)

proxy1.ibm.com (reverse proxy server)

You'll notice that initially the reverse proxy is configured to proxy traffic to the standby APM server (apm2.ibm.com). This is because we will initially be installing the standby APM server. Later, you will reconfigure the reverse proxy so that it can proxy traffic to the primary APM server. During an HA

failover of IBM Performance Management, reconfiguring the reverse proxy will be the mechanism that is used to ensure that traffic is being directed to the active APM server.

httpd.conf file for APM UI

```
# Key modules to load
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
# The Reverse Proxy server must listen on both port 9443 and 8099 and 8093
Listen 9443
Listen 8099
Listen 8093
# The first VirtualHost defines the communications that are used on port 9443
<VirtualHost *:9443>
ServerName proxy1.ibm.com
ServerAlias *.proxy1.ibm.com
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCertificateKeyFile /etc/pki/tls/private/proxy1.key
SSLCertificateFile /etc/pki/tls/certs/proxy1.crt
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
ProxyRequests off
ProxyPreserveHost On
ProxyPass / https://apm2.ibm.com:9443/
ProxyPassReverse / https://apm2.ibm.com:9443/
</VirtualHost>
# The VirtualHost  for APM 8.1.4 uses communications on port 8093 (added for 8.1.4)
<VirtualHost *:8093>
ServerName proxy1.ibm.com
ServerAlias *.proxy1.ibm.com
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCertificateKeyFile /etc/pki/tls/private/proxy1.key
SSLCertificateFile /etc/pki/tls/certs/proxy1.crt
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
ProxyRequests off
ProxyPreserveHost On
```

```
ProxyPass / https://apm2.ibm.com:8093/
ProxyPassReverse / https://apm2.ibm.com:8093/
</VirtualHost>

# The second VirtualHost defines that communications on port 8099
<VirtualHost *:8099>
ServerName proxy1.ibm.com
ServerAlias *.proxy1.ibm.com
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCertificateKeyFile /etc/pki/tls/private/proxy1.key
SSLCertificateFile /etc/pki/tls/certs/proxy1.crt
SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
ProxyRequests off
ProxyPreserveHost On
ProxyPass / https://apm2.ibm.com:8099/
ProxyPassReverse / https://apm2.ibm.com:8099/
</VirtualHost>
```

Setup the Forwarding Proxy

The forward proxy HA configuration does not support HTTPS communication from the agents. This is a limitation until a solution is available where the HTTPS connection is terminated by the forward proxy server and then HTTP is used between the forward proxy server and the APM server.

The forwarding proxy will be used for Agents to connect. All Agent traffic will be sent to the forwarding proxy. The traffic will then be proxied to the APM server. Once the environment is up and running reconfiguration of the forwarding proxy will allow all the Agents to connect and send data to the active APM server. In the example given in the documentation below, the forwarding proxy is setup for HTTP communications from the Agents. This is the default configuration for IBM Performance Management. The assumption is that all communications happen within the LAN and it is not necessary to encrypt the traffic.

In the following example, you'll see the configuration settings for an Apache 2.x HTTP server that is setup as a forwarding proxy. You can setup any forwarding proxy that you want. The file below does not represent the entire httpd.conf file, but does represent the key parameters to load the modules for the proxy, define the listening ports, and In the configuration below, replace http://apm1.ibm.com/ with the hostname of your Primary APM server.

During a failover of APM, you will modify the httpd.conf to use the standby APM server and recycle the HTTP server.

httpd.conf file for agents

```
# Key modules to load
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
# The Forwarding Proxy server must listen on port 80 for Agent communications.  If you setup your APM environment for HTTPS, change the port to 443
Listen 80
<IfModule mod_proxy.c>
 ProxyRequests On
 ProxyVia On
 <Proxy *>
 Order deny,allow
 Allow from 10.0.0.0/24
 </Proxy>
 ProxyPass / http://apm1.ibm.com/
</IfModule>
```

You'll notice in the configuration that I'm allowing communication from any systems in the 10.0.0.0 subnet. You should setup that entry so that you only allow connectivity from the appropriate subnets in your environment.

Appendix M: Example failover scripts

These are sample scripts that were used during the testing of failovers.

Scripts are available as is on the internet at https://developer.ibm.com/apm/resources/upgrading-a-high-availability-configuration/ under download. There are two tar files contained in a .zip file. The one for APM is apmhascripts.tar. The one for db2 is db2hascripts.tar.

Scripts to define HA variables

This following script allows you to define all of your IPs, ports, database names, and other variables in one location. A copy of the script should exist on the APM server and a copy on the DB2 servers. These are variables to be exported and sourced by other scripts in this package. The variables are sourced by adding ". ./apmcommonha.sh" to the top of your scripts.

apmcommonha.sh

Scripts to add or remove a VIP

The following two scripts are used to manually move the VIPs on the APM and DB2 servers. If you are using TSAMP the DB2 VIPs should move automatically when the database moves. VIPs are temporarily assigned to the server. You should never permanently assign a VIP to a server because a reboot of that server would automatically assign the VIP when it could already be assigned to another server. The parameter passed is the VIP to be removed or added.

removevip.sh

addvip.sh

Scripts that run on the DB2 servers

Firewall Scripts

The following script is used to start, stop, and check firewall status. It is important to make sure the firewalls are up before APM starts. Sometimes firewalls do not automatically start at boot up time due to errors. Parameters are start, stop, status, detail, or reload

firewall.sh

The following script is used to setup firewall rules and open standard connections. This permanently opens firewalls for basic communications and cluster communications.

allowbasic.sh

The following firewall rules allow APM to access DB2 on the specified port using the VIP to route to DB2. This permanently opens the firewall for the APM server that has the "accessdb2ip" VIP assigned to it to communicate with DB2. This is the VIP that APM uses to access DB2. No parameters are required.

allowapm.sh

The following scripts are used to update firewall rules during an APM failover. This is for customers that are not using VIPs. Parameter 1 is "add or remove" where add allows the apm server to access DB2 and remove blocks the apm server from accessing DB2. PParameter 2 is the server. Parameter 3 is the port.

apm-fw.sh

apmfailover2standby.sh (no parameters required)

apmfailback2primary.sh (no parameters required)

Status Script

The following script reports the status of the 3 DB2.
db2status.sh

Script to move the DB2 Databases

The following script is used to move the 3 Databases as a group to the DB2 server where the script is executed. No parameters are required.
db2takeover.sh

Scripts that run on the APM servers

The following two scripts run on the APM server. They are used to either block connections or allow connections. Each script can be passed a parameter of db2, agents, or apmui. If you have 3 spare VIPs for the APM servers, you can control the access for each component separately.
allow.sh
block.sh

The following script is intended to be used as part of the backup.sh and restore.sh process that is used to keep the two APM servers in sync. Script to find latest backup and run the restore cmd. No parameters are required because it reads the values from apmcommonha.sh.
myrestore.sh

Status Script

The following script reports which VIPs are assigned to this server. No parameters are required.
hastatus.sh

IP Addresses for Use Case Servers

The above scripts were copied from test servers. The names and IPs used in the scripts are the actual names. To help avoid confusion the layout of those servers follows:

10.21.6.248 APM1 (Primary APM server)
10.21.8.83 APM2 (Standby APM server)
10.21.9.14 DB2A (Primary DB2 HADR server)
10.21.9.73 DB2B (Standby DB2 HADR server)
VIPs
10.21.16.20 APM (VIP for users to access the APM UI)
10.21.16.21 agents (VIP for agents to access APM)
10.21.16.22 DB2FW (VIP for APM to route connections to DB2)
10.21.16.23 whous1 (VIP for accessing DB2 whous1 database)
10.21.16.24 scr1 (VIP for accessing DB2 scr1 database)
10.21.16.25 dmart1 (VIP for accessing DB2 dmart1 database)

The /scripts/* directory on the APM servers contain the following scripts:

1) apmcommonha.sh (A common location for APM HA variables)
2) allow.sh (Script to allow users and agents to access APM and APM to access DB2)
3) block.sh (Script to block users and agents from accessing APM and block APM from accessing DB2)
4) hastatus.sh (Script to show current status of APM vips)
5) addvip.sh (Script to add a VIP)
6) removevip.sh (Script to remove a VIP)
7) myrestore.sh (Script to assist with backup and restore)

The /scripts/* directory on the DB2 servers contain the following scripts:

1) apmcommonha.sh (A common location for APM HA variables)
2) firewall.sh (script to start or stop firewalls and show detail)
3) allowbasic.sh (Script to add basic communications to your firewalls)
4) allowapm.sh (Script to add APM communications to your firewalls)
5) db2status.sh (Script to show the status of the 3 APM DB2 HADR databases)
6) db2takeover.sh (Script to make the 3 databases primary on the other DB2 server)
7) addvip.sh (Script to add a VIP)
8) removevip.sh (Script to remove a VIP)
9) apm-fw.sh (Script for changing firewall rules when you are not using a VIP to allow APM to access DB2)
10) apmfailover2standby.sh (Script to block the primary APM server from accessing DB2 and allow the standby to access DB2 (if you are not using an APM VIP))
11) apmfailback2primary.sh (Script to block the standby APM server from accessing DB2 and allow the primary to access DB2 (if you are not using an APM VIP)))

Appendix N: Failover Scenarios

The following are examples of the steps that occur as part of a failover.

Failover Scenarios for APM and DB2

Failing over DB2 from Primary to Standby:

1. If TSAMP is setup, run ./db2takeover.sh on the standby DB2 server. No additional steps are required.
2. If the DB2 failover is not automated,
    a. If you are using DB2 VIPs, manually remove them from the primary DB2 server.
    b. Run ./db2takeover.sh to move the 3 database or move them one at a time.
    c. If you are using DB2 VIPs, manually assign them to the new primary DB2 server.

APM will automatically reestablish connections to DB2. The above steps can easily be automated by using TSAMP as the cluster manager and using db2haicu to configure DB2 HADR automation.

Failing over APM from Primary to Standby:

1. If you are using VIPs,
    a. run ./block.sh all on the primary APM server
    b. run ./allow.sh all on the standby APM server
    c. No additional steps are required.
2. If you are not using VIPs
    a. On the primary and standby DB2 servers change the firewall rules to block the current APM server.
    b. Run “db2 force applications all” to drop ALL connections to ALL databases owned by the instance ID. This is required because changing the firewall rules will not block existing connections.
    c. On the primary and standby DB2 servers change the firewall rules to allow the standby APM server.
    d. Update /etc/httpd/conf/httpd.conf files on the forward and reverse proxy servers and restart httpd

Failing over both APM and DB2 from Primary to Standby:

1. If you are using VIPs,

a. Run "./block.sh all" on the Primary APM server. This prevents Agents from sending more data to APM and drops existing connections to DB2.
b. On the standby DB2 server run ./db2takeover.sh
c. On the standby APM server run ./allow.sh all

2. If you are not using VIPs, follow the steps listed above for "**Failing over DB2 from Primary to Standby" and "Failing over APM from Primary to Standby".**

Appendix O: Migrating APM HA from 8.1.3 to 8.1.4

upgrade a high availability configuration of IBM Application Performance Management (APM) version 8. These instructions are written for upgrading version 8.1.3 to 8.1.4, but should apply to subsequent minor releases. The following section outlines at a high level the steps that are used to upgrade APM. Detailed instructions will be provided in subsequent sections of the document.

Upgrade Options

When upgrading your existing APM HA environment there are 2 methods to consider.

You can upgrade in place which means you use the same 4 servers that are currently running 8.1.3 and APM is down while you do the upgrade. The advantage with this method is that a second system is not required for the upgrade. Customers with small to medium environments usually choose this method.

Customers with larger environments may want to create a new set of servers (side-by-side upgrade) and then run a backup from the 8.1.3 servers and restore to the new 8.1.4 servers. In a side-by-side upgrade the 8.1.3 servers continue to run while the 8.1.4 servers are being setup. After the new servers are setup a backup is performed using the 8.1.3 servers and restored to the 8.1.4 servers.

In the past an option was documented that created temporary databases W1, D1, and S1 during the upgrade. The option caused confusion and has been removed.

These instructions will focus on doing an in place upgrade of APM 8.1.3 to 8.1.4.

These HA instructions have steps that reference the base APM instructions. You should review the base instructions before attempting to setup a failover APM server.

Steps to Upgrade Side A

Preparation Steps

Before you begin record key information: See detailed steps in. Appendix F: Record Current values

Stop APM server on side B (apm stop_all)

Upgrade Side A

The steps to upgrade your existing APM 8.1.3 HA environment to 8.1.4 follow.

1. Initial state: APM Side A is the primary, DB2 HADR side A is the primary, The DB2 firewalls are blocking APM on side B from accessing DB2, and the DB2 firewalls are allowing APM side A to access DB2.
2. Backup key information. See appendix F
3. Download the software.
4. Follow the instructions at https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/upgrade_server_inplace.htm to upgrade side A of your HA environment. These instruction will have steps for the following tasks
    1. How to download the software
    2. If you have Mongo DB
    3. If you are using LDAP
    4. Download Interim Fix 10
    5. Verify umask
    6. Backup your 8.1.3 APM primary server
    7. Uninstall APM on the primary server
    8. Backup the DBs for Warehous, Datamart, and SCR32. Update SCR32 DB. Adjust the buffer pools. The 8.1.3 backup of DB2 is only used for recovery purposes. It is not used in these instructions.

        e. In step "e" the tbsmdb path should be under the home directory of the instance directory but it could also be /opt/ibm/scrdb/tbsmdb or /opt/ibm/db2/tbsmdb. If you have multiple DB2 instances, you should have a separate tbsmdb directory for each instance.

    9. Install the new version of APM on the primary server (side A)

        a. Follow the responses for steps 9a through 9f

        g. You have the option to configure new APM 8.1.4 agents. Skip this step for now because you may require a fix pack for some of your agents. You can configure the agent package later by running the /opt/ibm/ccm/make_configuration_packages.sh and /opt/ibm/ccm/configure_agent_images.sh scripts.

        h. When you are prompted to enter the host name and IP address of the server that will be used in a web browser to log into the Cloud APM console, use the VIP for the

APM servers or the hostname of the reverse proxy server. **Do not use the hostname of the APM server. Use the VIP for the fully qualified name, short name, and IP address.**

i. When responding to the prompts to connect to the remote Db2 database **use the VIP for DB2 HADR. If you are using multiple DB2 VIPs, use the VIP for the WAREHOUS DB2 HADR. The VIPs for SCR32 and DATAMART will be added later. If you are not using a VIP, use the hostname of the primary DB2 server and later follow the instruction for adding an alternate DB2 server (ACR) to the configuration files. See Appendix E: Accessing DB2 HADR without a VIP (ACR).**

10. Migrate the Hybrid Gateway configuration
11. Refer to the steps under what to do next for any steps that may pertain to your installation.

    a. Clear your web browser cache
    b. If you are using a Hybrid Gateway
    c. If you want to use the old agent configuration packages
    d. (d,e,f) If you configured HTTPS communication between the Cloud APM server and agents in your V8.1.3 Cloud APM server

    g. If the system where you installed the Cloud APM server is using LDAP, and you updated the passwords for the itmuser and the Db2 instances users
    h. If you need to reconfigure reports
    i. If you are using Tivoli Common Reporting and changed the VIP for DB2.
    j. Review the WAREHOUS database settings that were applied by the restore process.
    k. By default the settings for logarchmeth1 and logarchmeth2 are set to off. If you back up your Warehouse database and you support log pruning, modify these settings.

Completing the installation

After the APM install.sh script completes and before agents connect to the APM server and before you install the Interim Fix. Refer to the section on "Post APM Installation Steps" for details to complete the following steps.

1. Update as.environment
2. Add port 8093 to the reverse proxy server
3. Setup certificates for the reverse proxy server
4. LDAP requirements
5. Install Interim Fix
6. Verify KAS_HOSTNAME
7. Configure Agent Image Installation package
8. Allow users to access the APM UI.
9. Update vhost.xml files for APM alias.
10. Log into the APM server
11. Verify Host Name Overide IP address
12. Check the setting for My Components
13. Allow Agents to connect to the APM server.
14. Set up DB2 HADR

15. Add additional VIPS to DB2 HADR
16. Verify APM SCR is blocked.

Steps to Upgrade Side B

Preparation Steps

1. Before you begin record key information: See Appendix F
2. Stop APM server on side A and B (apm stop_all). (B should already be stopped.)
3. Change the firewalls to block Side A and Side B from accessing DB2.
4. Move the VIP for the UI traffic from Side A to Side B.

Upgrade Side B

Follow the instructions at https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/upgrade_server_inplace.htm to upgrade side B of your HA environment. These instruction will have steps for the following tasks

1. Review steps 1 through 6. You should not need to execute any of these steps because they were already done using side A. (You should already have a backup of the primary APM server and a backup of the DB2 database.)

7. Uninstall APM V8.1.3 on Side B
8. Remote DB2 server steps.
    a. Replace steps 8a thru 8e with the steps to setup SCR UDF routines located Appendix G under Setup SCR UDF Routines

    f. Skip step 8f. The db2 restore will create the databases on the standby DB2 server.

Before you install APM on the standby APM server you must block APM A from accessing DB2 and allow APM B to access DB2. This is done by either updating the firewalls to allow APM Side B to access DB2 and blocking APM Side A from accessing DB2 or if APM is using a VIP with route to access DB2 just move the VIP to the APM server that needs access to DB2. (When using a VIP the firewalls do not need to be changed because the firewalls will only allow access through the APM VIP and the VIP can only be assigned to one of the APM servers.)

9. Install the new version of APM on the standby server (side B)

    a. Follow the responses for steps 9a through 9f

g. Skip the step to configure new APM 8.1.4 agents during the initial installation. The depot directory was already created on the primary APM server.
h. When you are prompted to enter the host name and IP address of the server that will be used in a web browser to log into the Cloud APM console, use the same hostname or VIP that you entered when configuring the primary APM server. **Do not use the hostname of the APM server.**
i. When responding to the prompts to connect to the remote Db2 database use the same hostname or VIP that you used when configuring the primary APM server.

10. Migrate the Hybrid Gateway configuration
11. Refer to the steps under what to do next for any steps that may pertain to your installation.

    a. Clear your web browser cache
    b. If you are using a Hybrid Gateway
    c. If you want to use the old agent configuration packages
    d. (d,e,f) If you configured HTTPS communication between the Cloud APM server and agents in your V8.1.3 Cloud APM server

    g. If the system where you installed the Cloud APM server is using LDAP, and you updated the passwords for the itmuser and the Db2 instances users
    h. If you need to reconfigure reports
    i. If you are using Tivoli Common Reporting and changed the VIP for DB2.
    j. Review the WAREHOUS database settings that were applied by the restore process.
    k. By default the settings for logarchmeth1 and logarchmeth2 are set to off. If you back up your Warehouse database and you support log pruning, modify these settings.

Completing the installation

After the APM install.sh script completes and before agents connect to the APM server and before you install the Interim Fix. Refer to the section on "Post APM Installation Steps" for details to complete the following steps.

1. Update as.environment
2. Add port 8093 to the reverse proxy server
3. Setup certificates for the reverse proxy server
4. LDAP requirements
5. Install Interim Fix
6. Verify KAS_HOSTNAME
7. Configure Agent Image Installation package
8. Allow users to access the APM UI.
9. Update vhost.xml files for APM alias.
10. Log into the APM server
11. Verify Host Name Overide IP address
12. Check the setting for My Components
13. Allow Agents to connect to the APM server.
14. Set up DB2 HADR
15. Add additional VIPS to DB2 HADR

16. Verify APM SCR is blocked.

Appendix P: Creating custom certificates.

APM provides default certificates for connecting to the Cloud APM console and for agents to connect to the APM server using HTTPS. If you do not want to use the default certificates then you can either use a third party certificate authority or a private certificate authority to create custom certificates.

When creating custom UI certificates for use in a high availability environment with a VIP, you should specify the VIP hostname in place of apm_server_hostname in the instructions in the Knowledge Center topic below when configuring the primary APM server:

https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/on_prem_config_ca_console.html (Configuring certificates by using a Third-Party Root Certificate Authority)

or

https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/onprem_config_selfsigncert_console.html (Configuring certificates by using a private root certificate authority)

Also when creating custom agent certificates for use in a high availability environment with a VIP, you should specify the VIP hostname in place of serverhostname in the instructions in the Knowledge Center topic below when configuring the primary APM server:

https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/onprem_config_ca_custom.html (Configuring a Third-Party Root CA custom certificate for HTTPS agent communications)

or

https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/onprem_config_selfsigned_cert.html (Configuring a self-signed certificate)

You only need to submit CSR requests for certificates that use the VIP hostname and do not have to create CSR requests and certificates for the actual primary APM server hostname and secondary APM server hostname.

After you have followed the instructions to create custom certificates, configured the primary APM server and agents to use the custom certificates, and successfully connected to the APM UI and can see agent data in the UI then perform an APM backup on the primary APM server

and a restore on the backup APM server (per the instructions in this document under "APM Server Synchronization via Backup and Restore" so that the backup/secondary APM server is using the same certificates and configuration as the primary APM server).

Appendix Q: Trouble shooting

Agents missing from "My Components" or "Resource Groups" on APMUI

Check your firewalls. If both APM servers were allowed to access DB2, the SCR process on the standby APM server will delete agents after the "Remove Offline System Delay" period has been reached. To fix the problem refer to "Verify APM SCR is blocked" under "Post APM Installation Steps". Also if you are not using a VIP with route to block APM from accessing DB2 you must run something like "db2 force applications all" to stop the connections to DB2 because adding a firewall will not block existing connections. You can run "netstat –an | grep 50000" (where 50000 is the port that you assigned to DB2) to determine which APM server has connections to DB2. Only the primary APM server IP or the VIP for routing should be connecting to DB2. You can also use "db2 list applications" to see connections to DB2. After you fix the firewall problem issue "apm restart oslc" on the primary APM server.

Unable to access the APM UI.

IF08 added security to require users to access the APM UI using the hostname or IP address that was used when APM was installed. Browser connections using an alias or short name may be blocked and you may receive a message stating "This page isn't working". To access the APM server use the name that was used when APM was installed. See "Update vhost.xml files for APM alias" in section "Post APM Installation Steps".

Unable to establish a connection to APM UI when using an alias to access APM UI.

The user receives the following message when attempting to connect to the APM UI.

CWOAU0073E: An error was encountered while authenticating a user. Please try authenticating again, or contact the site administrator if the problem persists.

If this occurs logon using the hostname or IP address that appears in the URL. You can only establish one session using the alias. Part of the process for access in the APM server is authentication using oidc. The URL will automatically update to the hostname or IP address that was used when APM was installed for authentication. When this message is displayed use the server name that appears in the URL in front of the string "oidcclient" to access the APM server.

Agents missing after doing an APM failover.

Verify KAS_HOSTNAME has been set on both APM servers. See “Update as.environment” in section “Post APM Installation Steps”.

Agents are not removed from “My Components”.

This can occur if both APM Servers published resources before the oslc processes as.environment files were updated with matching KAS_HOSTNAME values. If this occurs, the agents published by the backup server before KAS_HOSTNAME was set will not be deleted because the provider that registered them is no longer a provider. These resources can be removed by executing the following process on the active (primary) APM server:

- cat /opt/ibm/ccm/oslc_pm/config/as.environment and retrieve the value of KAS_HOSTNAME

For this explanation KAS_HOSTNAME=rtp-primary.raleigh.ibm.com and the backup APM server in our HA configuration is rtp-backup.raleigh.ibm.com

- retrieve a list of registered providers and the number of resources associated with each from the SCR:

- cd /opt/ibm/ccm/SCR/XMLtoolkit/bin

- ./oslcmaint.sh -U itmuser -v

GTMCL5569I: Provider id: 0 Provider: SCR_OWNED_NAMING_STRINGS Resources published: 0

GTMCL5569I: Provider id: 0 Provider: SCR_Static_Meta_Resources Resources published: 80

GTMCL5569I: Provider id: 0 Provider: http://www.ibm.com/APMUI/provider/101 Resources published: 2

GTMCL5569I: Provider id: 4 Provider: http://rtp-primary.raleigh.ibm.com/localhost Resources published: 23

GTMCL5569I: Provider id: 21 Provider: http://delta02:16310/oslc/providers/1360103741670 Resources published: 9

GTMCL5569I: Provider id: 61 Provider: http://rtp-backup.raleigh.ibm.com/localhost Resources published: 20

- In this example, both the primary and backup servers have registered resources. The primary has 23 resources and the backup has 20. We only want resources associated with the primary since KAS_HOSTNAME is set to rtp-primary.raleigh.ibm.com on both APM servers.

- To remove the resources registered by rtp-backup.raleigh.ibm.com issue the following command:

- ./oslcmaint.sh -U itmuser -r 61

  Where 61 is the Provider id of the backup (standby) APM server.

- The oslcmaint.sh request to delete the resources will be queued for execution.

End of doc

IBM United States of America

Produced in the United States of America

IBM Director of Licensing
IBM Corporation
4205 South Miami Boulevard
Research Triangle Park, NC 27709 U.S.A.